The aim of the journal **“Algebra and Discrete Mathematics”** (as $\mathcal{ADM}$ below) is to present timely the state-of-the-art accounts on modern research in all areas of algebra (general algebra, semigroups, groups, rings and modules, linear algebra, algebraic geometry, universal algebras, homological algebra etc.) and discrete mathematics (combinatorial analysis, graphs theory, mathematical logic, theory of automata, coding theory, cryptography etc.)

Languages:

Papers to be considered for publication in the $\mathcal{ADM}$ journal must be written in English.

Preparing papers:

Papers submitted to the $\mathcal{ADM}$ journal should be prepared in LaTeX. Authors are strongly encourages to prepare their papers using the $\mathcal{ADM}$ author package containing template, instructions, and $\mathcal{ADM}$ journal document class. $\mathcal{ADM}$ author package is available from the journal web-site `http://adm.luguniv.edu.ua`.

Graphical items should be prepared as eps (encapsulated PostScript) files and included by using the `graphicx` package. To avoid distortion from rescaling, figures must not be wider than 120 mm.

Submitting papers:

Authors who wish to submit their papers should send paper in PDF format directly to anyone of the Editors via electronic mail. E-mails of the Editors are listed on the Editorial Board page.

The source TeX-file of the paper will be needed if it accepted for publication.

Submission of a manuscript implies that the work described has not been published before and that it is not under consideration for publication elsewhere.

Required information:

The following information is required with the submission (note that all contact information, particularly email addresses, must be supplied to avoid delay):

1) *full postal address of each author;*
2) *e-mail of each author;*
3) *abstract (no more than 15 lines);*
4) *2010 Mathematics subject classification (can be accessible from* `http://www.ams.org/msc`*);*
5) *key words and phrases.*

Proof-sheets:

Authors receive only one set of proof-sheets in PDF format via e-mail for corrections. Only correction of misprints and minor changes can be made during proofreading.

Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **19** (2015). Number 2, pp. 145–161

Derived equivalence classification of generalized multifold extensions of piecewise hereditary algebras of tree type

Hideto Asashiba, Mayumi Kimura

Communicated by D. Simson

Abstract. We give a derived equivalence classification of algebras of the form $\hat{A}/\langle\phi\rangle$ for some piecewise hereditary algebra A of tree type and some automorphism ϕ of $\hat{A}$ such that $\phi(A^{[0]}) = A^{[n]}$ for some positive integer n.

Introduction

Throughout this paper we fix an algebraically closed field $\mathbb{k}$, and assume that all algebras are basic and finite-dimensional $\mathbb{k}$-algebras and that all categories are $\mathbb{k}$-categories.

The classification of algebras under derived equivalences seems to be first explicitly investigated by Rickard in [9], which gave the derived equivalence classification of Brauer tree algebras (implicitly there exists an earlier work [4] by Assem–Happel giving the classification of gentle tree algebras). After that the first named author gave the classification of representation-finite self-injective algebras (see also [1] and Membrillo-Hernández [7] for type A_n). The technique used there (a covering technique for derived equivalences developed in [1]) is applicable also for representation-infinite

2010 MSC: 16G30, 16E35, 16W22.
Key words and phrases: derived equivalence, piecewise hereditary, quivers, orbit categories.

algebras; it requires that the algebras in consideration have the form of orbit categories (usually of repetitive categories of some algebras having no oriented cycles in their ordinary quivers). In fact, it was applied in [3] to give the classification of twisted multifold extensions of piecewise hereditary algebras of tree type by giving a complete invariant. Here an algebra is called a *twisted multifold extension* of an algebra A if it has the form

$$T_\psi^n(A) := \hat{A}/\langle \hat{\psi}\nu_A^n \rangle \tag{0.1}$$

for some positive integer n and some automorphism ψ of A, where $\hat{A}$ is the repetitive algebra of A, ν_A is the Nakayama automorphism of $\hat{A}$ and $\hat{\psi}$ is the automorphism of $\hat{A}$ naturally induced from ψ (see Definition 1.1 and Lemma 1.2 for details); and an algebra A is called a *piecewise hereditary algebra of tree type* if A is an algebra derived equivalent to a hereditary algebra whose ordinary quiver is an oriented tree. In this paper we extend this classification to a wider class of algebras. To state this class of algebras we introduce the following terminologies. For an integer n we say that an automorphism ϕ of $\hat{A}$ has a *jump* n if $\phi(A^{[0]}) = A^{[n]}$. An algebra of the form

$$\hat{A}/\langle \phi \rangle$$

for some automorphism ϕ of $\hat{A}$ with jump n for some positive integer n is called a *generalized multifold extension* of A. Since obviously $\hat{\psi}\nu_A^n$ is an automorphism of $\hat{A}$ with jump n in the formula (0.1), twisted multifold extensions are generalized multifold extensions. We are now able to state our purpose. In this paper we will give the derived equivalence classification of generalized multifold extensions of piecewise hereditary algebras of tree type by giving a complete invariant. Note that most algebras in this class are wild and that the tame part of the class has a big intersection with the class of self-injective algebras of Euclidean type studied by Skowroński in [10] (see Remark 1.7).

The paper is organized as follows. After preparations in section 1 we first reduce the problem to the case of hereditary tree algebras in section 2. Then we investigate scalar multiples in the repetitive category of a hereditary tree algebras in section 3, which is a central part of the proof of the main result. In section 4 we show that any generalized multifold extension of a piecewise hereditary algebra of tree type is derived equivalent to a twisted multifold extension of the same type, which immediately yields the desired classification result.

1. Preliminaries

For a category R we denote by R_0 and R_1 the class of objects and morphisms of R, respectively. A category R is said to be *locally bounded* if it satisfies the following:

- Distinct objects of R are not isomorphic;
- $R(x,x)$ is a local algebra for all $x \in R_0$;
- $R(x,y)$ is finite-dimensional for all $x, y \in R_0$; and
- The set $\{y \in R_0 \mid R(x,y) \neq 0 \text{ or } R(y,x) \neq 0\}$ is finite for all $x \in R_0$.

A category is called *finite* if it has only a finite number of objects.

A pair (A, E) of an algebra A and a complete set $E := \{e_1, \dots, e_n\}$ of orthogonal primitive idempotents of A can be identified with a locally bounded and finite category R by the following correspondences. Such a pair (A, E) defines a category $R_{(A,E)} := R$ as follows: $R_0 := E$, $R(x,y) := yAx$ for all $x, y \in E$, and the composition of R is defined by the multiplication of A. Then the category R is locally bounded and finite. Conversely, a locally bounded and finite category R defines such a pair (A_R, E_R) as follows: $A_R := \bigoplus_{x,y \in R_0} R(x,y)$ with the usual matrix multiplication (regard each element of A as a matrix indexed by R_0), and $E_R := \{(\mathbb{1}_x \delta_{(i,j),(x,x)})_{i,j \in R_0} \mid x \in R_0\}$. We always regard an algebra A as a locally bounded and finite category by fixing a complete set A_0 of orthogonal primitive idempotents of A.

For a locally bounded category A, we denote by $\operatorname{Mod} A$ the category of all (right) A-modules (= contravariant functors from A to the category $\operatorname{Mod} \Bbbk$ of $\Bbbk$-vector spaces); by $\operatorname{mod} A$ the full subcategory of $\operatorname{Mod} A$ consisting of finitely presented objects; and by $\operatorname{prj} A$ the full subcategory of $\operatorname{Mod} A$ consisting of finitely generated projective objects. $\mathcal{K}^{\mathrm{b}}(\mathcal{A})$ denotes the bounded homotopy category of an additive category $\mathcal{A}$.

1.1. Repetitive categories

Definition 1.1. Let A be a locally bounded category.

(1) The *repetitive category* $\hat{A}$ of A is a $\Bbbk$-category defined as follows ($\hat{A}$ turns out to be locally bounded again):

- $\hat{A}_0 := A_0 \times \mathbb{Z} = \{x^{[i]} := (x, i) \mid x \in A_0, i \in \mathbb{Z}\}$.

- $\hat{A}(x^{[i]}, y^{[j]}) := \begin{cases} \{f^{[i]} \mid f \in A(x,y)\} & \text{if } j = i, \\ \{\phi^{[i]} \mid \phi \in DA(y,x)\} & \text{if } j = i+1, \\ 0 & \text{otherwise,} \end{cases}$

  for all $x^{[i]}, y^{[j]} \in \hat{A}_0$.
- For each $x^{[i]}, y^{[j]}, z^{[k]} \in \hat{A}_0$ the composition $\hat{A}(y^{[j]}, z^{[k]}) \times \hat{A}(x^{[i]}, y^{[j]}) \to \hat{A}(x^{[i]}, z^{[k]})$ is given as follows.

  (i) If $i = j, j = k$, then this is the composition of A $A(y,z) \times A(x,y) \to A(x,z)$.

  (ii) If $i = j, j+1 = k$, then this is given by the right A-module structure of DA: $DA(z,y) \times A(x,y) \to DA(z,x)$.

  (iii) If $i+1 = j, j = k$, then this is given by the left A-module structure of DA: $A(y,z) \times DA(y,x) \to DA(z,x)$.

  (iv) Otherwise, the composition is zero.

(2) We define an automorphism ν_A of $\hat{A}$, called the *Nakayama automorphism* of $\hat{A}$, by $\nu_A(x^{[i]}) := x^{[i+1]}$, $\nu_A(f^{[i]}) := f^{[i+1]}$, $\nu_A(\phi^{[i]}) := \phi^{[i+1]}$ for all $i \in \mathbb{Z}, x \in A_0, f \in A_1, \phi \in \bigcup_{x,y \in A_0} DA(y,x)$.

(3) For each $n \in \mathbb{Z}$, we denote by $A^{[n]}$ the full subcategory of $\hat{A}$ formed by $x^{[n]}$ with $x \in A$, and by $1\!\!1^{[n]} : A \xrightarrow{\sim} A^{[n]} \hookrightarrow \hat{A}, x \mapsto x^{[n]}$, the embedding functor.

We cite the following from [3, Lemma 2.3].

Lemma 1.2. *Let $\psi\colon A \to B$ be an isomorphism of locally bounded categories. Denote by $\psi_x^y\colon A(y,x) \to B(\psi y, \psi x)$ the isomorphism defined by ψ for all $x, y \in A$. Define $\hat{\psi}\colon \hat{A} \to \hat{B}$ as follows.*

- *For each $x^{[i]} \in \hat{A}, \hat{\psi}(x^{[i]}) := (\psi x)^{[i]}$;*
- *For each $f^{[i]} \in \hat{A}(x^{[i]}, y^{[i]}), \hat{\psi}(f^{[i]}) := (\psi f)^{[i]}$; and*
- *For each $\phi^{[i]} \in \hat{A}(x^{[i]}, y^{[i+1]}), \hat{\psi}(\phi^{[i]}) := (D((\psi_x^y)^{-1})(\phi))^{[i]} = (\phi \circ (\psi_x^y)^{-1})^{[i]}$.*

Then

(1) *$\hat{\psi}$ is an isomorphism.*

(2) *Given an isomorphism $\rho\colon \hat{A} \to \hat{B}$, the following are equivalent.*

  (a) *$\rho = \hat{\psi}$;*

  (b) *ρ satisfies the following.*

(i) $\rho\nu_A = \nu_B\rho$;
(ii) $\rho(A^{[0]}) = A^{[0]}$;
(iii) *The diagram*

$$\begin{array}{ccc} A & \xrightarrow{\psi} & B \\ {\scriptstyle \mathbb{1}^{[0]}}\downarrow & & \downarrow{\scriptstyle \mathbb{1}^{[0]}} \\ A^{[0]} & \xrightarrow[\rho]{} & B^{[0]} \end{array}$$

is commutative; and
(iv) $\rho(\phi^{[0]}) = (\phi \circ (\psi^y_x)^{-1})^{[0]}$ *for all* $x, y \in A$ *and all* $\phi \in DA(y, x)$.

Let R be a locally bounded category with the Jacobson radical J and with the ordinary quiver Q. Then by definition of Q there is a bijection $f\colon Q_0 \to R_0, x \mapsto f_x$ and injections $\bar{a}_{y,x}\colon Q_1(x, y) \to J(f_x, f_y)/J^2(f_x, f_y)$ such that $\bar{a}_{y,x}(Q_1(x, y))$ forms a basis of $J(f_x, f_y)/J^2(f_x, f_y)$, where $Q_1(x, y)$ is the set of arrows from x to y in Q for all $x, y \in Q_0$. For each $\alpha \in Q_1(x, y)$ choose $a_{y,x}(\alpha) \in J(f_x, f_y)$ such that $a_{y,x}(\alpha) + J^2(f_x, f_y) = \bar{a}_{y,x}(\alpha)$. Then the pair (f, a) of the bijection f and the family a of injections $a_{y,x}\colon Q_1(x, y) \to J(f_x, f_y)$ $(x, y \in Q_0)$ uniquely extends to a full functor $\Phi\colon \Bbbk Q \to R$, which is called a *display functor* for R.

A path μ from y to x in a quiver with relations (Q, I) is called *maximal* if $\mu \notin I$ but $\alpha\mu, \mu\beta \in I$ for all arrows $\alpha, \beta \in Q_1$. For a $\Bbbk$-vector space V with a basis $\{v_1, \dots, v_n\}$ we denote by $\{v_1^*, \dots, v_n^*\}$ the basis of DV dual to the basis $\{v_1, \dots, v_n\}$. In particular if $\dim_k V = 1$, $v^* \in DV$ is defined for all $v \in V\backslash\{0\}$.

An algebra is called a *tree algebra* if its ordinary quiver is an oriented tree.

Lemma 1.3. *Let* A *be a tree algebra and* $\Phi : \Bbbk Q \to A$ *a display functor with* $I := \operatorname{Ker}\Phi$. *Then*

(1) Φ *uniquely induces the display functor* $\hat{\Phi} : \Bbbk\hat{Q} \to \hat{A}$ *for* $\hat{A}$, *where*

(i) $\hat{Q} = (\hat{Q}_0, \hat{Q}_1, \hat{s}, \hat{t})$ *is defined as follows:*

- $\hat{Q}_0 := Q_0 \times \mathbb{Z} = \{x^{[i]} := (x, i) \mid x \in Q_0, i \in \mathbb{Z}\}$,
- $Q_1 \times \mathbb{Z} := \{\alpha^{[i]} := (\alpha, i) \mid \alpha \in Q_1, i \in \mathbb{Z}\}$,
  $\hat{Q}_1 := (Q_1 \times \mathbb{Z}) \sqcup \{\mu^{*[i]} \mid \mu$ *is a maximal path in* $(Q, I), i \in \mathbb{Z}\}$,
- $\hat{s}(\alpha^{[i]}) := s(\alpha)^{[i]}$, $\hat{t}(\alpha^{[i]}) := t(\alpha)^{[i]}$ *for all* $\alpha^{[i]} \in Q_1 \times \mathbb{Z}$, *and if* μ *is a maximal path from* y *to* x *in* (Q, I) *then,* $\hat{s}(\mu^{*[i]}) := x^{[i]}$, $\hat{t}(\mu^{*[i]}) := y^{[i+1]}$.

(ii) $\hat{\Phi}$ *is defined by* $\hat{\Phi}(x^{[i]}) := (\Phi x)^{[i]}$, $\hat{\Phi}(\alpha^{[i]}) := (\Phi\alpha)^{[i]}$, *and* $\hat{\Phi}(\mu^{*[i]}) := (\Phi(\mu)^*)^{[i]}$ *for all* $i \in \mathbb{Z}$, $x \in Q_0$, $\alpha \in Q_1$ *and maximal paths* μ *in* (Q, I).

(2) *We define an automorphism* ν_Q *of* $\hat{Q}$ *by* $\nu_Q(x^{[i]}) := x^{[i+1]}$, $\nu_Q(\alpha^{[i]}) := \alpha^{[i+1]}$, $\nu_Q(\mu^{*[i]}) := \mu^{*[i+1]}$ *for all* $i \in \mathbb{Z}, x \in Q_0, \alpha \in Q_1$, *and maximal paths* μ *in* (Q, I).

(3) $\operatorname{Ker}\hat{\Phi}$ *is equal to the ideal* $\hat{I}$ *defined by the full commutativity relations on* $\hat{Q}$ *and the zero relations* $\mu = 0$ *for those paths* μ *of* $\hat{Q}$ *for which there is no path* $\hat{t}(\mu) \rightsquigarrow \nu_Q(\hat{s}(\mu))$. (*Therefore note that if a path* $\alpha_n \cdots \alpha_1$ *is in* I, *then* $\alpha_n^{[i]} \cdots \alpha_1^{[i]}$ *is in* $\hat{I}$ *for all* $i \in \mathbb{Z}$.)

Let R be a locally bounded category. A morphism $f\colon x \to y$ in R_1 is called a *maximal nonzero morphism* if $f \neq 0$ and $fg = 0, hf = 0$ for all $g \in \operatorname{rad} R(z, x), h \in \operatorname{rad} R(y, z), z \in R_0$.

Lemma 1.4. *Let* A *be an algebra and* $x^{[i]}, y^{[j]} \in \hat{A}_0$. *Then there exists a maximal nonzero morphism in* $\hat{A}(x^{[i]}, y^{[j]})$ *if and only if* $y^{[j]} = \nu_A(x^{[i]})$.

Proof. This follows from the fact that $\hat{A}(\text{-}, x^{[i+1]}) \cong D\hat{A}(x^{[i]}, \text{-})$ for all $i \in \mathbb{Z}, x \in A_0$. □

Lemma 1.5. *Let* A *be an algebra. Then the actions of* $\phi\nu_A$ *and* $\nu_A\phi$ *coincide on the objects of* $\hat{A}$ *for all* $\phi \in \operatorname{Aut}(\hat{A})$.

Proof. Let $x^{[i]} \in \hat{A}_0$. Then there is a maximal nonzero morphism in $\hat{A}(x^{[i]}, \nu_A(x^{[i]}))$ by Lemma 1.4. Since ϕ is an automorphism of $\hat{A}$, there is a maximal nonzero morphism in $\hat{A}(\phi(x^{[i]}), \phi(\nu_A(x^{[i]})))$. Hence $\phi(\nu_A(x^{[i]})) = \nu_A(\phi(x^{[i]}))$ by the same lemma. □

The following is immediate by the lemma above.

Proposition 1.6. *Let* A *be an algebra,* n *an integer, and* ϕ *an automorphism of* $\hat{A}$. *Then the following are equivalent:*

(1) ϕ *is an automorphism with jump* n;

(2) $\phi(A^i) = A^{[i+n]}$ *for some integer* i;

(3) $\phi(A^j) = A^{[j+n]}$ *for all integers* j; *and*

(4) $\phi = \sigma\nu_A^n$ *for some automorphism* σ *of* $\hat{A}$ *with jump* 0.

Remark 1.7. Let A be an algebra.

(1) In Skowroński [10, 11] an automorphism ϕ of $\hat{A}$ is called *rigid* if $\phi(A^{[j]}) = A^{[j]}$ for all $j \in \mathbb{Z}$. Hence ϕ is rigid if and only if it is an automorphism with jump 0 by the proposition above. Therefore for an integer n, ϕ is an automorphism with jump n if and only if $\phi = \sigma\nu_A^n$ for some rigid automorphism σ of $\hat{A}$.

(2) Noting this fact we see by [11, Theorem 4.7] that the class of self-injective algebras of Euclidean type contains a lot of generalized multifold extensions of piecewise hereditary algebras of tree type.

In the sequel, we always assume that n is a positive integer when we consider a morphism with jump n.

1.2. Derived equivalences and tilting subcategories

Let R be a locally bounded category and $\phi \in \operatorname{Aut}(R)$. Then ϕ induces an equivalence ${}^{\phi}(\text{-}) : \operatorname{mod} R \to \operatorname{mod} R$ defined by ${}^{\phi}M := M \circ \phi^{-1} : R \to \operatorname{mod} \Bbbk$ for all $M \in \operatorname{mod} R$. In particular for $R(\text{-}, x)$ with $x \in R$, we have ${}^{\phi}(R(\text{-}, x)) = R(\phi^{-1}(\text{-}), x) \cong R(\text{-}, \phi x)$, and the last isomorphism is given by ϕ itself. Thus the identification ${}^{\phi}(R(\text{-}, x)) = R(\text{-}, \phi x)$ depends on ϕ, and the subset $\{R(\text{-}, x) \mid x \in R\}$ of $\operatorname{prj} R$ is not $\langle {}^{\phi}(\text{-}) \rangle$-stable in a strict sense. This makes it difficult to give explicitly a complete set of representatives of isoclasses of indecomposable objects of $\mathcal{K}^{\mathrm{b}}(\operatorname{prj} R)$ which is $\langle \mathcal{K}^{\mathrm{b}}({}^{\phi}(\text{-})) \rangle$-stable. To avoid this difficulty we used in [2] the formal additive hull $\operatorname{add} R$ ([5, 2.1 Example 8]) of R defined below instead of $\operatorname{prj} R$.

Definition 1.8. Let R be a locally bounded category. The *formal additive hull* $\operatorname{add} R$ of R is a category defined as follows.

- $(\operatorname{add} R)_0 := \{\bigoplus_{i=1}^{n} x_i := (x_1, \dots, x_n) \mid n \in \mathbb{N},\ x_1, \dots, x_n \in R_0\}$;
- For each $x = \bigoplus_{i=1}^{m} x_i, y = \bigoplus_{j=1}^{m} y_i \in (\operatorname{add} R)_0$,

$$\begin{aligned}(\operatorname{add} R)(x, y) := \{(\mu_{j,i})_{j,i} \mid \mu_{j,i} \in R(x_i, y_j) \\ \text{for all } i = 1, \dots, m, j = 1, \dots, n\};\ \text{and}\end{aligned}$$

- The composition is given by the matrix multiplication.

We regard that R is contained in $\operatorname{add} R$ by the embedding $(f \colon x \to y) \mapsto ((f) \colon (x) \to (y))$ for all f in R.

Remark 1.9. Let R and ϕ be as above.

(1) Define a functor $\eta_R\colon \operatorname{add} R \to \operatorname{prj} R$ by $(x_1, \dots, x_n) \mapsto R(\text{-}, x_1) \oplus \cdots \oplus R(\text{-}, x_n)$ and $(\mu_{ji})_{j,i} \mapsto (R(\text{-}, \mu_{ji}))_{j,i}$. Then η_R is an equivalence, called the *Yoneda* equivalence.

(2) Let $F\colon R \to S$ be a functor of locally bounded categories. Then F naturally induces functors $\operatorname{add} F\colon \operatorname{add} R \to \operatorname{add} S$ and $\tilde{F} := \mathcal{K}^{\mathrm{b}}(\operatorname{add} F)\colon \mathcal{K}^{\mathrm{b}}(\operatorname{add} R) \to \mathcal{K}^{\mathrm{b}}(\operatorname{add} S)$, which are isomorphisms if F is an isomorphism. Namely, $\operatorname{add} F$ is defined by $(x_1, \dots, x_n) \mapsto (Fx_1, \dots, Fx_n)$ and $(\mu_{ji}) \mapsto (F\mu_{ji})$ for all objects $(x_1, \dots, x_n)$ and all morphisms (μ_{ji}) in $\operatorname{add} R$; and $\tilde{F}$ is defined by $\operatorname{add} F$ componentwise. Further if $G\colon S \to T$ is a functor of locally bounded categories, then we have $(GF)\tilde{} = \tilde{G}\tilde{F}$.

(3) The automorphism ϕ acts on $\mathcal{K}^{\mathrm{b}}(\operatorname{add} R)$ as $\tilde{\phi}$, and ${}^{\phi}\mathcal{K}^{\mathrm{b}}(\eta_R)(X^{\boldsymbol{\cdot}}) \cong \mathcal{K}^{\mathrm{b}}(\eta_R)(\tilde{\phi}(X^{\boldsymbol{\cdot}}))$ for all $X^{\boldsymbol{\cdot}} \in \mathcal{K}^{\mathrm{b}}(\operatorname{add} R)$.

We cite the following from [2, Proposition 5.1] which follows from Keller [6] (Cf. Rickard [8], [1, Proposition 1.1]).

Proposition 1.10. *Let R and S be locally bounded categories. Then the following are equivalent:*

(1) *There is a triangle equivalence $\mathcal{D}(\operatorname{Mod} S) \to \mathcal{D}(\operatorname{Mod} R)$; and*

(2) *There is a full subcategory E of $\mathcal{K}^{\mathrm{b}}(\operatorname{add} R)$ such that*

  (a) *$\mathcal{K}^{\mathrm{b}}(\operatorname{add} R)(T, U[n]) = 0$ for all $T, U \in E$ and all $n \neq 0$;*

  (b) *R is contained in the smallest full triangulated subcategory of $\mathcal{K}^{\mathrm{b}}(\operatorname{add} R)$ containing E that is closed under direct summands and isomorphisms; and*

  (c) *E is isomorphic to S.*

Definition 1.11. We say that locally bounded categories R and S are *derived equivalent* if one of the equivalent conditions above holds. In (2) the triple (R, E, S) is called a *tilting triple* and $E \subseteq \mathcal{K}^{\mathrm{b}}(\operatorname{add} R)$ is called a *tilting subcategory* for R.

Theorem 1.5 in [1] is interpreted as follows.

Theorem 1.12. *If (A, E, B) is a tilting triple of locally bounded categories with an isomorphism $\psi\colon E \to B$, then $(\hat{A}, \hat{E}, \hat{B})$ is also a tilting triple with the isomorphism $\hat{\psi}\colon \hat{E} \to \hat{B}$, where $\hat{E}$ is isomorphic to (and identified with) the full subcategory of $\mathcal{K}^{\mathrm{b}}(\operatorname{add} \hat{A})$ consisting of the $(\mathbb{1}^{[n]})\tilde{}\,(T)$ with $T \in E$, $n \in \mathbb{Z}$.*

For a group G acting on a category S we say that a subclass E of the objects of S is *G-stable* (resp. *G-stable up to isomorphisms*) if $gx \in E$ (resp. if gx is isomorphic to some object in E) for all $g \in G$ and $x \in E$.

Proposition 1.13. *Let (A, E, B) be a tilting triple of locally bounded categories with an isomorphism $\psi\colon E \to B$, g an automorphism of $\hat{A}$ and h an automorphism of $\hat{B}$. Then $\hat{A}/\langle g\rangle$ is derived equivalent to $\hat{B}/\langle h\rangle$ if*

(1) *g is of infinite order and $\langle g\rangle$ acts freely on $\hat{A}$;*

(2) *$\hat{E}$ is $\langle \tilde{g}\rangle$-stable; and*

(3) *The following diagram commutes:*

$$\begin{array}{ccc} \hat{E} & \xrightarrow{\hat{\psi}} & \hat{B} \\ {\scriptstyle \tilde{g}}\big\downarrow & & \big\downarrow{\scriptstyle h} \\ \hat{E} & \xrightarrow[\hat{\psi}]{} & \hat{B}. \end{array}$$

Remark 1.14. Let E be a tilting subcategory for a locally bounded category R and G a group acting on R. If E is G-stable up to isomorphisms, then there exists a tilting subcategory E' for R such that $E \cong E'$ and E' is G-stable (see [1, Remark 3.2] and [2, Lemma 5.3.3 and Remark 5.3(2)]).

2. Reduction to hereditary tree algebras

Let Q be a quiver. We denote by $\bar{Q}$ the underlying graph of Q, and call Q *finite* if both Q_0 and Q_1 are finite sets. Each automorphism of Q is regarded as an automorphism of $\bar{Q}$ preserving the orientation of Q, thus $\mathrm{Aut}(Q)$ can be regarded as a subgroup of $\mathrm{Aut}(\bar{Q})$. Suppose now that Q is a finite oriented tree. Then it is also known that $\mathrm{Aut}(Q) \leqslant \mathrm{Aut}_0(\bar{Q}) := \{f \in \mathrm{Aut}(\bar{Q}) \mid f(x) = x \text{ for some } x \in Q_0\}$. We say that Q is an *admissibly oriented* tree if $\mathrm{Aut}(Q) = \mathrm{Aut}_0(\bar{Q})$. We quote the following from [3, Lemma 4.1]:

Lemma 2.1. *For any finite tree T there exists an admissibly oriented tree Q with a unique source such that $\bar{Q} = T$.*

We cite the following from [3, Lemma 5.4].

Lemma 2.2. *Let A be a piecewise hereditary algebra of type Q for an admissibly oriented tree Q. Then there is a tilting triple (A, E, kQ) such that E is $\langle\tilde{\phi}\rangle$-stable up to isomorphisms for all $\phi \in \mathrm{Aut}(A)$.*

By the following proposition we can reduce the derived equivalence classification of generalized multifold extensions of *piecewise hereditary* algebras of tree type to the corresponding problem of generalized multifold extensions of *hereditary* tree algebras. The second statement also enables us to compare the generalized multifold extension and a twisted version corresponding to it using the repetitive category of the common hereditary algebra.

Proposition 2.3. *Let A be a piecewise hereditary algebra of tree type $\bar{Q}$ for an admissibly oriented tree Q, and n a positive integer. Then we have the following:*

(1) *For any $\phi \in \mathrm{Aut}(\hat{A})$ with jump n, there exists some $\psi \in \mathrm{Aut}(\widehat{\Bbbk Q})$ with jump n such that $\hat{A}/\langle\phi\rangle$ is derived equivalent to $\widehat{\Bbbk Q}/\langle\psi\rangle$; and*

(2) *If we set $\phi' := \nu_A^n \hat{\phi_0} \in \mathrm{Aut}(\hat{A})$, where $\phi_0 := (\mathbb{1}^{[0]})^{-1}\nu_A^{-n}\phi\mathbb{1}^{[0]}$, then there exists some $\psi' \in \mathrm{Aut}(\widehat{\Bbbk Q})$ with jump n such that $\hat{A}/\langle\phi'\rangle$ is derived equivalent to $\widehat{\Bbbk Q}/\langle\psi'\rangle$, and that the actions of ψ and ψ' coincide on the objects of $\widehat{\Bbbk Q}$.*

Proof. (1) We set $\nu := \nu_A$ and $\phi_i := (\mathbb{1}^{[i]})^{-1}\nu_A^{-n}\phi\mathbb{1}^{[i]} \in \mathrm{Aut}(A)$ for all $i \in \mathbb{Z}$. By Lemma 2.2, there exists a tilting triple $(A, E, \Bbbk Q)$ with an isomorphism $\zeta\colon E \to \Bbbk Q$ such that E is $\langle\tilde{\eta}\rangle$-stable up to isomorphisms for all $\eta \in \mathrm{Aut}(A)$. In particular, E is $\langle\tilde{\phi_i}\rangle$-stable up to isomorphisms for all $i \in \mathbb{Z}$. Then $(\hat{A}, \hat{E}, \widehat{\Bbbk Q})$ is a tilting triple with the isomorphism $\hat{\zeta}$ by Theorem 1.12 and the following holds.

Claim 1. *$\hat{E}$ is $\langle\tilde{\phi}\rangle$-stable up to isomorphisms.*

Indeed, for each $T \in E_0$ and $i \in \mathbb{Z}$, we have

$$\begin{aligned}\tilde{\phi}(\mathbb{1}^{[i]})\tilde{}\,(T) &= (\nu^n\nu^{-n}\phi\mathbb{1}^{[i]})\tilde{}\,(T)\\ &= (\nu^n\mathbb{1}^{[i]}\phi_i)\tilde{}\,(T)\\ &= (\mathbb{1}^{[i+n]})\tilde{}\,\tilde{\phi}_i(T).\end{aligned} \tag{2.1}$$

Since E is $\langle\tilde{\phi}_i\rangle$-stable up to isomorphisms, we have $\tilde{\phi}_i(T) \cong T'$ for some $T' \in E$, and hence $\tilde{\phi}((\mathbb{1}^{[i]})\tilde{}\,(T)) \cong (\mathbb{1}^{[i+n]})\tilde{}\,(T') \in \hat{E}$, as desired.

By Remark 1.14, we have a $\langle\tilde{\phi}\rangle$-stable tilting subcategory $\hat{E}'$ and an isomorphism $\theta\colon \hat{E}' \xrightarrow{\sim} \hat{E}$. Therefore by Proposition 1.13 $\hat{A}/\langle\phi\rangle$ and $\hat{E}'/\langle\tilde{\phi}\rangle$ are derived equivalent. If we set $\psi := (\hat{\zeta}\theta)\tilde{\phi}(\hat{\zeta}\theta)^{-1}$, then (2.1) shows that ψ is an automorphism with jump n, and that $\hat{E}'/\langle\tilde{\phi}\rangle \cong \widehat{\Bbbk Q}/\langle\psi\rangle$. Hence $\hat{A}/\langle\phi\rangle$ and $\widehat{\Bbbk Q}/\langle\psi\rangle$ are derived equivalent.

(2) Note that ϕ' is also an automorphism with jump n. By the same argument we see that $\hat{E}$ is also $\langle\tilde{\phi}'\rangle$-stable up to isomorphisms; there exists a $\langle\tilde{\phi}'\rangle$-stable tilting subcategory $\hat{E}''$ and an isomorphism $\theta' \colon \hat{E}'' \xrightarrow{\sim} \hat{E}$; and $\hat{A}/\langle\phi'\rangle$ and $\hat{E}''/\langle\tilde{\phi}'\rangle$ are derived equivalent. Set $\psi' := (\hat{\zeta}\theta')\tilde{\phi}'(\hat{\zeta}\theta')^{-1}$, then ψ' is an automorphism with jump n, $\hat{E}''/\langle\tilde{\phi}'\rangle \cong \widehat{\Bbbk Q}/\langle\psi'\rangle$, and $\hat{A}/\langle\phi'\rangle$ and $\widehat{\Bbbk Q}/\langle\psi'\rangle$ are derived equivalent. Now for $i = 0$ the equality (2.1) shows that $\tilde{\phi}(\mathbb{1}^{[0]})\tilde{}\,(T) = (\mathbb{1}^{[n]})\tilde{}\,\tilde{\phi}_0(T)$ for all $T \in E_0$. Since $\phi'_0 = \phi_0$, the same calculation shows that $\tilde{\phi}'(\mathbb{1}^{[0]})\tilde{}\,(T) = (\mathbb{1}^{[n]})\tilde{}\,\tilde{\phi}_0(T)$ for all $T \in E_0$. Thus the actions of $\tilde{\phi}$ and $\tilde{\phi}'$ coincide on the objects of $E^{[0]}$, which shows that the actions of ψ and ψ' coincide on the objects of $\Bbbk Q^{[0]}$. Hence by Lemma 1.5 their actions coincide on the objects of $\widehat{\Bbbk Q}$. Indeed, $\psi(x^{[i]}) = \psi\nu^i(x^{[0]}) = \nu^i\psi(x^{[0]}) = \nu^i\psi'(x^{[0]}) = \psi'\nu^i(x^{[0]}) = \psi'(x^{[i]})$ for all $x \in Q_0$ and $i \in \mathbb{Z}$. □

3. Hereditary tree algebras

Remark 3.1. Let Q be an oriented tree.

(1) We may identify $\widehat{\Bbbk Q} = \Bbbk\hat{Q}/\hat{I}$ as stated in Lemma 1.3, and we denote by $\overline{\mu}$ the morphism $\mu + \hat{I}$ in $\widehat{\Bbbk Q}$ for each morphism μ in $\Bbbk\hat{Q}$.

(2) Let $x, y \in \hat{Q}_0$. Since $\hat{I}$ contains full commutativity relations, we have $\dim_{\Bbbk} \widehat{\Bbbk Q}(x, y) \leqslant 1$, and in particular $\hat{Q}$ has no double arrows.

(3) Let $\alpha \colon x \to y$ be in $\hat{Q}_1$ and $\phi \in \mathrm{Aut}(\widehat{\Bbbk Q})$. Then there exists a unique arrow $\phi x \to \phi y$ in $\hat{Q}$, which we denote by $(\hat{\pi}\phi)(\alpha)$, and we have $\phi(\overline{\alpha}) = \phi_\alpha \overline{(\hat{\pi}\phi)(\alpha)} \in \widehat{\Bbbk Q}(\phi x, \phi y)$ for a unique $\phi_\alpha \in \Bbbk^\times := \Bbbk \setminus \{0\}$. This defines an automorphism $\hat{\pi}\phi$ of $\hat{Q}$, and thus a group homomorphism $\hat{\pi} : \mathrm{Aut}(\widehat{\Bbbk Q}) \to \mathrm{Aut}(\hat{Q})$.

(4) Similarly, let $\alpha \colon x \to y$ be in Q_1 and $\psi \in \mathrm{Aut}(\Bbbk Q)$. Then there exists a unique arrow $\psi x \to \psi y$ in Q, which we denote by $(\pi\psi)(\alpha)$. This defines an automorphism $\pi\psi$ of Q, and thus a group homomorphism $\pi : \mathrm{Aut}(\Bbbk Q) \to \mathrm{Aut}(Q)$.

We cite the following from [3, Proposition 7.4].

Proposition 3.2. *Let R be a locally bounded category, and g, h automorphisms of R acting freely on R. If there exists a map $\rho \colon R_0 \to \Bbbk^\times$ such that $\rho(y)g(f) = h(f)\rho(x)$ for all morphisms $f \colon x \to y$ in R, then $R/\langle g\rangle \cong R/\langle h\rangle$.* □

Definition 3.3. (1) For a quiver $Q = (Q_0, Q_1, s, t)$ we set $Q[Q_1^{-1}]$ to be the quiver

$$Q[Q_1^{-1}] := (Q_0, Q_1 \sqcup \{\alpha^{-1} \mid \alpha \in Q_1\}, s', t'),$$

where $s'|_{Q_1} := s$, $t'|_{Q_1} := t$, $s'(\alpha^{-1}) := t(\alpha)$ and $t'(\alpha^{-1}) := s(\alpha)$ for all $\alpha \in Q_1$. A *walk* in Q is a path in $Q[Q_1^{-1}]$.

(2) Suppose that Q is a finite oriented tree. Then for each $x, y \in Q_0$ there exists a unique shortest walk from x to y in Q, which we denote by $w(x,y)$. If $w(x,y) = \alpha_n^{\varepsilon_n} \cdots \alpha_1^{\varepsilon_1}$ for some $\alpha_1, \cdots, \alpha_n \in Q_1$ and $\varepsilon_1, \dots, \varepsilon_n \in \{1, -1\}$, then we define a subquiver $W(x,y)$ of Q by $W(x,y) := (W(x,y)_0, W(x,y)_1, s', t')$, where $W(x,y)_0 := \{s(\alpha_i), t(\alpha_i) \mid i = 1, \dots, n\}$, $W(x,y)_1 := \{\alpha_1, \dots, \alpha_n\}$, and s', t' are restrictions of s, t to $W(x,y)_1$, respectively. Since Q is an oriented tree, $w(x,y)$ is uniquely recovered by $W(x,y)$. Therefore we can identify $w(x,y)$ with $W(x,y)$, and define a *sink* and a *source* of $w(x,y)$ as those in $W(x,y)$.

The following is a central part of the proof of the main result.

Proposition 3.4. *Let Q be a finite oriented tree and ϕ, ψ automorphisms of $\widehat{\Bbbk Q}$ acting freely on $\widehat{\Bbbk Q}$. If the actions of ϕ and ψ coincide on the objects of $\widehat{\Bbbk Q}$, then there exists a map $\rho\colon (\hat{Q}_0 =)\ \widehat{\Bbbk Q}_0 \to \Bbbk^\times$ such that $\rho(y)\psi(f) = \phi(f)\rho(x)$ for all morphisms $f\colon x \to y$ in $\widehat{\Bbbk Q}$. Hence in particular, $\widehat{\Bbbk Q}/\langle\phi\rangle$ is isomorphic to $\widehat{\Bbbk Q}/\langle\psi\rangle$.*

Proof. Assume that the actions of $\phi, \psi \in \operatorname{Aut}(\widehat{\Bbbk Q})$ coincides on the objects of $\widehat{\Bbbk Q}$. Then ϕ and ψ induce the same quiver automorphism $q = \hat{\pi}\phi = \hat{\pi}\psi$ of $\hat{Q}$, and there exist $(\phi_\alpha)_{\alpha \in \hat{Q}_1}, (\psi_\alpha)_{\alpha \in \hat{Q}_1} \in (k^\times)^{\hat{Q}_1}$ such that for each $\alpha \in \hat{Q}_1$ we have

$$\phi(\overline{\alpha}) = \phi_\alpha \overline{q(\alpha)}, \quad \psi(\overline{\alpha}) = \psi_\alpha \overline{q(\alpha)}.$$

For each path $\lambda = \alpha_n \cdots \alpha_1$ in $\hat{Q}$ with $\alpha_1, \dots, \alpha_n \in \hat{Q}_1$ we set $\phi_\lambda := \phi_{\alpha_n} \cdots \phi_{\alpha_1}$. Then we have

$$\phi(\overline{\lambda}) = \phi_\lambda \overline{q(\lambda)},$$

where $q(\lambda) := q(\alpha_n) \cdots q(\alpha_1)$ because

$$\phi(\overline{\alpha_n}) \cdots \phi(\overline{\alpha_1}) = \phi_{\alpha_n} \cdots \phi_{\alpha_1} \overline{q(\alpha_n) \cdots q(\alpha_1)}.$$

To show the statement we may assume that $\psi_\alpha = 1$ for all $\alpha \in \hat{Q}_1$. Since for each $x, y \in \hat{Q}_0$ the morphism space $\widehat{\Bbbk Q}(x,y)$ is at most 1-dimensional and has a basis of the form $\overline{\mu}$ for some path μ, it is enough to show that there exists a map $\rho : \hat{Q}_0 \to \Bbbk^\times$ satisfying the following condition:

$$\rho(v^{[j]}) = \phi_\beta \rho(u^{[i]}) \quad \text{for all } \beta : u^{[i]} \to v^{[j]} \text{ in } \hat{Q}_1. \tag{3.1}$$

We define a map ρ as follows:
Fix a maximal path $\mu\colon y \rightsquigarrow x$ in Q. Then x is a sink and y is a source in Q. We can write μ as $\mu = \alpha_l \cdots \alpha_1$ for some $\alpha_1, \dots, \alpha_l \in Q_1$. First we set $\rho(x^{[0]}) := 1$. By induction on $0 \leqslant i \in \mathbb{Z}$ we define $\rho(x^{[i]})$ and $\rho(x^{[-i]})$ by the following formulas:

$$\rho(x^{[i+1]}) := \phi_{\mu^{[i+1]}} \phi_{\mu^{*[i]}} \rho(x^{[i]}), \tag{3.2}$$
$$\rho(x^{[i-1]}) := \phi^{-1}_{\mu^{*[i-1]}} \phi^{-1}_{\mu^{[i]}} \rho(x^{[i]}). \tag{3.3}$$

Now for each $i \in \mathbb{Z}$ and $u \in Q_0$ if $w(u, x) = \beta_m^{\varepsilon_m} \cdots \beta_1^{\varepsilon_1}$ for some $\beta_1, \dots, \beta_m \in Q_1$ and $\varepsilon_1, \dots, \varepsilon_m \in \{1, -1\}$, then we set

$$\rho(u^{[i]}) := \phi^{-\varepsilon_1}_{\beta_1^{[i]}} \cdots \phi^{-\varepsilon_m}_{\beta_m^{[i]}} \rho(x^{[i]}). \tag{3.4}$$

We have to verify the condition (3.1).

Case 1. $\beta = \alpha^{[i]}\colon u^{[i]} \to v^{[i]}$ for some $i \in \mathbb{Z}$, and $\alpha\colon u \to v$ in Q_1. Since Q is an oriented tree, we have either $w(u, x) = w(v, x)\alpha$ or $w(v, x) = w(u, x)\alpha^{-1}$. In either case we have $\rho(v^{[i]}) = \phi_{\alpha^{[i]}} \rho(u^{[i]})$ by the formula (3.4).

Case 2. Otherwise, we have $\beta = \lambda^{*[i]} : u^{[i]} \to v^{[i+1]}$ for some maximal path $\lambda\colon v \rightsquigarrow u$ in Q and $i \in \mathbb{Z}$. In this case the condition (3.1) has the following form:

$$\rho(v^{[i+1]}) = \phi_{\lambda^{*[i]}} \rho(u^{[i]}). \tag{3.5}$$

Two paths are said to be *parallel* if they have the same source and the same target. We prepare the following for the proof.

Claim 2. *If ζ and η are parallel paths in $\hat{Q}$, then we have $\phi_\zeta = \phi_\eta$.*

Indeed, since $\zeta - \eta \in \hat{I}$, we have $\phi(\bar{\zeta}) = \phi(\bar{\eta})$, which shows

$$\phi_\zeta \overline{q(\zeta)} = \phi_\eta \overline{q(\eta)}.$$

Here we have $\overline{q(\zeta)} = \psi(\bar{\zeta}) = \psi(\bar{\eta}) = \overline{q(\eta)}$, and $\psi(\bar{\zeta}) \neq 0$ because $\bar{\zeta} \neq 0$. Hence $\phi_\zeta = \phi_\eta$, as required.

We now set $d(a, b)$ to be the number of sinks in $w(a, b)$ for all $a, b \in Q_0$. By induction on $d(y, v)$ we show that the condition (3.5) holds. Note that both v and y (resp. u and x) are sources (resp. sinks) in Q.

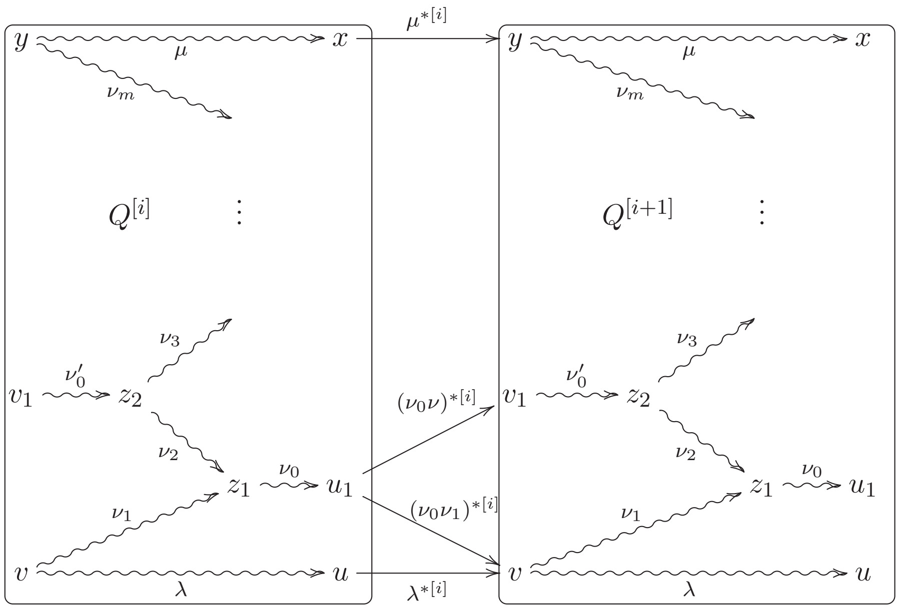

FIGURE 1.

Assume $d(y, v) = 0$. Then $y = v$ because these are sources in Q. By formulas (3.4) and (3.2) we have

$$\rho(v^{[i+1]}) = \rho(y^{[i+1]}) = \phi^{-1}_{\alpha_1^{[i+1]}} \cdots \phi^{-1}_{\alpha_l^{[i+1]}} \rho(x^{[i+1]}) = \phi_{\mu^{*[i]}} \rho(x^{[i]}).$$

If $u = x$, then $\lambda = \mu$ and hence $\phi_{\mu^{*[i]}} \rho(x^{[i]}) = \phi_{\lambda^{*[i]}} \rho(u^{[i]})$. Thus (3.5) holds.

If $u \neq x$, then $\phi_{\mu^{*[i]}} \phi_{\mu^{[i]}} = \phi_{\lambda^{*[i]}} \phi_{\lambda^{[i]}}$ by Claim 2. Since Q is an oriented tree, we have $w(u, x) = \mu\lambda^{-1}$, and $\rho(u^{[i]}) = \phi_{\lambda^{[i]}} \phi^{-1}_{\mu^{[i]}} \rho(x^{[i]})$. Therefore

$$\rho(v^{[i+1]}) = \phi_{\mu^{*[i]}} \rho(x^{[i]}) = \phi_{\lambda^{*[i]}} \phi_{\lambda^{[i]}} \phi^{-1}_{\mu^{[i]}} \rho(x^{[i]}) = \phi_{\lambda^{*[i]}} \rho(u^{[i]}),$$

and (3.5) holds.

Assume $d(y, v) \geqslant 1$. Then we can write $w(y, v) = \nu_1^{-1}\nu_2 \cdots \nu_{m-1}^{-1}\nu_m$ for some paths $\nu_1, \dots, \nu_m$ of length at least 1 and $m \geqslant 2$. Set $z_1 := t(\nu_2), z_2 := s(\nu_2)$. Then z_1 is a sink and z_2 is a source in $w(y, v)$. Since Q is a tree, there exists a unique maximal path of the form $\nu_0\nu_2\nu_0' \colon v_1 \rightsquigarrow u_1$ in Q for some paths ν_0, ν_0'. We set $\nu := \nu_2\nu_0'$. (See Figure 1, where we omitted the notations $[i], [i+1]$ for paths in $Q^{[i]}, Q^{[i+1]}$, respectively.) Since $d(v_1, y) = d(v, y) - 1$, we have

$$\rho(v_1^{[i+1]}) = \phi_{(\nu_0\nu)^{*[i]}} \rho(u_1^{[i]}) \tag{3.6}$$

by induction hypothesis. Since the paths $\nu^{[i+1]}(\nu_0\nu)^{*[i]}$ and $\nu_1^{[i+1]}(\nu_0\nu_1)^{*[i]}$ are parallel, we have

$$\phi_{\nu^{[i+1]}}\phi_{(\nu_0\nu)^{*[i]}} = \phi_{\nu_1^{[i+1]}}\phi_{(\nu_0\nu_1)^{*[i]}} \tag{3.7}$$

by Claim 1. Further by the result of Case 1 we have

$$\rho(v^{[i+1]}) = \phi^{-1}_{\nu_1^{[i+1]}}\phi_{\nu^{[i+1]}}\rho(v_1^{[i+1]}). \tag{3.8}$$

It follows from (3.6), (3.7) and (3.8) that

$$\rho(v^{[i+1]}) = \phi_{(\nu_0\nu_1)^{*[i]}}\rho(u_1^{[i]}).$$

(If $u_1 = u$, then $\nu_0\nu_1 = \lambda$ and this already gives (3.5).) Again by the result of Case 1 we have

$$\rho(u_1^{[i]}) = \phi_{(\nu_0\nu_1)^{[i]}}\phi^{-1}_{\lambda^{[i]}}\rho(u^{[i]}).$$

Since the paths $\lambda^{*[i]}\lambda^{[i]}$ and $(\nu_0\nu_1)^{*[i]}(\nu_0\nu_1)^{[i]}$ are parallel, we have

$$\phi_{\lambda^{*[i]}}\phi_{\lambda^{[i]}} = \phi(\nu_0\nu_1)^{*[i]}\phi(\nu_0\nu_1)^{[i]}$$

by Claim 1. The last three equalities give (3.5). □

4. Main result

Theorem 4.1. *Let A be a piecewise hereditary algebra of tree type and ϕ an automorphism of $\hat{A}$ with jump n. Then $\hat{A}/\langle\phi\rangle$ and $T^n_{\phi_0}(A)$ are derived equivalent, where we set $\phi_0 := (\mathbb{1}^{[0]})^{-1}\nu^{-n}\phi\mathbb{1}^{[0]}$.*

Proof. Let T be the tree type of A. Then by Lemma 2.1 there exists an admissibly oriented tree Q with $\bar{Q} = T$. We set $\phi' := \nu_A^n\hat{\phi}_0$ $(= \hat{\phi}_0\nu_A^n)$. Then $T^n_{\phi_0}(A) = \hat{A}/\langle\phi'\rangle$. By Proposition 2.3(2) there exist some $\psi, \psi' \in \operatorname{Aut}(\widehat{\Bbbk Q})$ both with jump n such that $\hat{A}/\langle\phi\rangle$ (resp. $\hat{A}/\langle\phi'\rangle$) is derived equivalent to $\widehat{\Bbbk Q}/\langle\psi\rangle$ (resp. $\widehat{\Bbbk Q}/\langle\psi'\rangle$), and the actions of ψ and ψ' coincide on the objects of $\widehat{\Bbbk Q}$. Then by Proposition 3.4 we have $\widehat{\Bbbk Q}/\langle\psi\rangle \cong \widehat{\Bbbk Q}/\langle\psi'\rangle$. Hence $\hat{A}/\langle\phi\rangle$ and $T^n_{\phi_0}(A)$ are derived equivalent. □

Definition 4.2. Let Λ be a generalized n-fold extension of a piecewise hereditary algebra A of tree type T, say $\Lambda = \hat{A}/\langle\phi\rangle$ for some $\phi \in \operatorname{Aut}(A)$ with jump n. Further let Q be an admissibly oriented tree with $\bar{Q} = T$.

Then by Proposition 2.3 there exists $\psi \in \mathrm{Aut}(\widehat{\Bbbk Q})$ with jump n such that $\hat{A}/\langle\phi\rangle$ is derived equivalent to $\widehat{\Bbbk Q}/\langle\psi\rangle$. We define the (*derived equivalence*) *type* $\mathrm{type}(\Lambda)$ of Λ to be the triple $(T, n, \overline{\pi}(\psi_0))$, where $\psi_0 := (\mathbb{1}^{[0]})^{-1}\nu_{\Bbbk Q}^{-n}\psi\mathbb{1}^{[0]}$ and $\overline{\pi}(\psi_0)$ is the conjugacy class of $\pi(\psi_0)$ in $\mathrm{Aut}(T)$. $\mathrm{type}(\Lambda)$ is uniquely determined by Λ.

By Theorem 4.1, we can extend the main theorem in [3] as follows.

Theorem 4.3. *Let Λ, Λ' be generalized multifold extensions of piecewise hereditary algebras of tree type. Then the following are equivalent:*

(i) *Λ and Λ' are derived equivalent.*

(ii) *Λ and Λ' are stably equivalent.*

(iii) $\mathrm{type}(\Lambda) = \mathrm{type}(\Lambda')$.

Finally we pose a question concerning a refinement of Theorem 4.1.

Question. Under the setting of Theorem 4.1, when are the algebras $\hat{A}/\langle\phi\rangle$ and $T^n_{\phi_0}(A)$ isomorphic?

By Proposition 3.4 this is affirmative if A is hereditary.

Acknowledgements

This work is partially supported by Grant-in-Aid for Scientific Research (C) 21540036 from JSPS.

References

[1] H. Asashiba, *A covering technique for derived equivalence*, J. Algebra **191**, (1997) 382–415.

[2] H. Asashiba, *The derived equivalence classification of representation-finite selfinjective algebras*, J. of Algebra **214**, (1999) 182–221.

[3] H. Asashiba, *Derived and stable equivalence classification of twisted multifold extensions of piecewise hereditary algebras of tree type*, J. Algebra **249**, (2002) 345–376.

[4] I.Assem, D. Happel, *Generalized tilted algebras of type A_n*, Comm. Algebra **9** (1981), no. 20, 2101–2125.

[5] P. Gabriel, A. V. Roiter, *Representations of finite-dimensional algebras*, Encyclopaedia of Mathematical sciences Vol. **73**, Springer, 1992.

[6] B. Keller, Deriving DG categories, *Ann. scient. Éc. Norm. Sup.*, (4) **27** (1994), 63–102.

[7] F. H. Membrillo-Hernández, *Brauer tree algebras and derived equivalence*, J. Pure Appl. Algebra **114** (1997), no. 3, 231–258.

[8] J. Rickard, *Morita theory for derived categories*, J. London Math. Soc., **39** (1989), 436–456.

[9] J. Rickard, *Derived categories and stable equivalence*, J. Pure and Appl. Alg. **61** (1989), 303–317.

[10] A. Skowroński, *Selfinjective algebras of polynomial growth*, Math. Ann. **285** (1989), 177–199.

[11] A. Skowroński, *Selfinjective algebras: finite and tame type*, *In* Trends in Representation Theory of Algebras and Related Topics, Contemporary Mathematics 406, Amer. Math. Soc., Providence, RI, 2006, 169–238.

Contact information

Hideto Asashiba, Mayumi Kimura
Faculty of Science, Shizuoka University,
836 Ohya, Suruga-ku, Shizuoka, 422-8529, Japan
E-Mail(s): asashiba.hideto@shizuoka.ac.jp,
f5144005@ipc.shizuoka.ac.jp

Received by the editors: 25.04.2013
and in final form 25.05.2013.

Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **19** (2015). Number 2, pp. 162–171

On inverse subsemigroups of the semigroup of orientation-preserving or orientation-reversing transformations

Paula Catarino*, Peter M. Higgins, Inessa Levi

Communicated by V. Mazorchuk

Abstract. It is well-known [16] that the semigroup $\mathcal{T}_n$ of all total transformations of a given n-element set X_n is covered by its inverse subsemigroups. This note provides a short and direct proof, based on properties of digraphs of transformations, that every inverse subsemigroup of order-preserving transformations on a finite chain X_n is a semilattice of idempotents, and so the semigroup of all order-preserving transformations of X_n is not covered by its inverse subsemigroups. This result is used to show that the semigroup of all orientation-preserving transformations and the semigroup of all orientation-preserving or orientation-reversing transformations of the chain X_n are covered by their inverse subsemigroups precisely when $n \leqslant 3$.

1. Introduction

In a regular semigroup S every element α has an inverse β in S meaning that $\alpha = \alpha\beta\alpha$ and $\beta = \beta\alpha\beta$. In an inverse semigroup S every element of S has a unique inverse in S. An inverse β of an element α in a

---

*The first author is a Member of the Research Center of Mathematics, CM-UTAD, Portugal.

2010 MSC: 20M20, 05C25.

Key words and phrases: semigroup, semilattice, inverse subsemigroup, strong inverse, transformation, order-preserving transformation, orientation-preserving transformation, orientation-reversing transformation.

semigroup S is said to be a *strong inverse* of α if the subsemigroup $\langle \alpha, \beta \rangle$ of S generated by α and β is an inverse subsemigroup of S. A semigroup S is covered by its inverse subsemigroups precisely when every element in S has a strong inverse in S.

This note addresses the following question: what regular semigroups are covered by their inverse subsemigroups?

For example, the semigroup $\mathcal{T}_n$ of all total transformations of a given n-element set X_n and the semigroup $\mathcal{PT}_n$ of all total and partial transformations of X_n are both regular but not inverse. B. M. Schein [16] noted that the above question was formulated in 1964 during the VI Vsesouznyi Algebra Colloquium in Minsk, USSR, in terms of the semigroups $\mathcal{T}_n$ and $\mathcal{PT}_n$. In his 1971 paper [16], B. M. Schein showed, generalizing the results by L. M. Gluskin [9], that $\mathcal{T}_n$ and $\mathcal{PT}_n$ are covered by their inverse subsemigroups. A detailed proof of this result may be found in P. M. Higgins' book [11]. Note that this result does not hold for the semigroup of all total transformations of an infinite set, see, for example, [11, Exercise 6.2.8].

Let $X_n = \{1, 2, \cdots, n\}$ be a chain with respect to the standard order, and let $\mathcal{O}_n$ be the semigroup of all order-preserving transformations α on X_n, that is transformations satisfying the condition $x\alpha \leqslant y\alpha$ whenever $x < y$, for all $x, y \in X_n$. Let $\{i_n\}$ denote the identity permutation of X_n. The semigroup $\mathcal{O}_n$ was introduced by A. Ya. Aizenstat [1], where she gave a presentation for $\mathcal{O}_n \setminus \{i_n\}$ in terms of $2n-2$ idempotent generators. She described in [2] the congruences on $\mathcal{O}_n$. There is a large body of literature on properties of the semigroup $\mathcal{O}_n$. For example, it is shown in [10] that the minimal number of generators of $\mathcal{O}_n \setminus \{i_n\}$ is n; combinatorial properties of $\mathcal{O}_n$ were studied in [13], [12] and [14]. It is well known that $\mathcal{O}_n$ is a regular semigroup.

It was shown recently by A. Vernitski [18] that all the inverse subsemigroups of $\mathcal{O}_n$ are semilattices. Indeed he proved that a finite inverse semigroup can be represented by order-preserving mappings if and only if it is a semilattice of idempotents. Vernitski's paper is concerned with the study of the pseudovariety of all finite semigroups whose inverse subsemigroups consist of a single element, and the quasivariety of all finite semigroups whose inverse subsemigroups are semilattices. The proof uses the Krohn-Rhodes Theorem on wreath products of monoids. In the present paper we provide a simple self-contained proof of the result based on digraphs associated with transformations (Theorem 2.7).

A transformation $\alpha \in \mathcal{T}_n$ is said to be *orientation-preserving* (*orientation-reversing*) if the sequence $(1\alpha, 2\alpha, \ldots, n\alpha)$ is a cyclic permutation of a non-decreasing (non-increasing) sequence. The semigroup

$\mathcal{OP}_n$ of all orientation-preserving transformations and the semigroup $\mathcal{P}_n$ of all orientation-preserving or orientation-reversing transformations were introduced independently by D. B. McAlister [15] and P. M. Catarino and P. M. Higgins [5]. Clearly, $\mathcal{O}_n$ is a subsemigroup of $\mathcal{OP}_n$, which in turn is a subsemigroup of $\mathcal{P}_n$.

For a transformation $\alpha \in \mathcal{T}_n$ the rank of α, denoted by $\operatorname{rank}(\alpha)$, is the number of elements in the image set $X_n\alpha$ of α. It was shown in [4] and [15] that $\mathcal{OP}_n$ is generated by an idempotent in $\mathcal{O}_n$ of rank $n-1$ and the cyclic group generated by the n-cycle $(1, 2, 3, \dots, n)$. It was also shown [15] that $\mathcal{P}_n$ is generated by an idempotent in $\mathcal{O}_n$ of rank $n-1$ and the dihedral group D_n. It follows that minimal generating sets of $\mathcal{OP}_n$ and $\mathcal{P}_n$ have sizes 2 and 3 respectively. The semigroups $\mathcal{OP}_n$ and $\mathcal{P}_n$ are regular [5].

The introduction of the semigroups $\mathcal{OP}_n$ and $\mathcal{P}_n$ generated a large body of fruitful research by a number of authors. For example, P. M. Catarino [4] exhibited a presentation of $\mathcal{OP}_n$ in terms of $2n-1$ generators, by extending A. Ja. Aizenstat's [1] presentation for $\mathcal{O}_n$ by a single generator and $2n$ relations. R. E. Arthur and N. Ruškuc [3] gave a presentation for $\mathcal{OP}_n$ in terms of the minimal number of generators (two) and $n+2$ relations. In the same article they also gave a presentation of $\mathcal{P}_n$ on three generators and $n+6$ relations. The congruences of $\mathcal{OP}_n$ and $\mathcal{P}_n$ were described by V. H. Fernandes, G. M. S. Gomes and M. M. Jesus [8]. The pseudovariety generated by all semigroups of orientation-preserving transformations on a finite cycle was introduced and studied by P. M. Catarino and P. M. Higgins in [6]. More recently, combinatorial properties of semigroups of total and partial orientation-preserving transformations were studied by A. Umar [17], and all maximal subsemigroups of $\mathcal{OP}_n$ and $\mathcal{P}_n$ were described by I. Dimitrova, V. H. Fernandez and J. Koppitz [7].

In the present paper we use the result that every inverse subsemigroup of $\mathcal{O}_n$ is a semilattice of idempotents (Theorem 2.7 below) to show that $\mathcal{OP}_n$ and $\mathcal{P}_n$ are covered by their respective inverse subsemigroups if and only if $n \leqslant 3$.

2. Results

Every transformation α of X_n may be viewed as a digraph on n vertices, in which for $x, y \in X_n$ we have that xy is an arc of the digraph of α precisely when $x\alpha = y$. A comprehensive discussion on digraphs associated with transformations may be found in [11, Section 1.6]; we summarize here the results used in the proofs below.

The *orbits* of a mapping α in $\mathcal{T}_n$ are the classes of the equivalence relation $\sim$ on X_n defined by $x \sim y$ if and only if there exist non-negative integers k, m such that $x\alpha^k = y\alpha^m$. The sets of vertices of connected components of a digraph of α correspond to orbits of α. Each component of a digraph of a transformation is *functional*, that is, it consists of a unique cycle together with a number of trees rooted around this cycle. A cycle on m distinct vertices of X_n is to be referred to as an m-cycle. If the cycle of a component consists of a single vertex x, then x is a fixed point of α, that is $x\alpha = x$.

Lemma 2.1. *Let α be a transformation in $\mathcal{T}_n$ and suppose that all the cycles in the digraph of α are* 1*-cycles. Then for any positive integer k, the orbits and fixed points of α and α^k are identical.*

Proof. Assume that x and y are in the same orbit with respect to some power α^k of α, that is $x \sim y$ with respect to α^k. Then there exist positive integers s and t such that $x\,(\alpha^k)^s = y\,(\alpha^k)^t$, whence $x\,\alpha^{ks} = y\,\alpha^{kt}$ and so $x \sim y$ with respect to α. Conversely, assume that $x \sim y$ with respect to α. By our assumption, the component C of the digraph of α containing vertices x and y has a unique 1-cycle, say, with a vertex z. Therefore z is a fixed point of α, and so $x\,\alpha^t = y\,\alpha^t = z$ for any positive integer $t \geqslant l$, where l is the length of the longest directed path in C. Hence $x\,\alpha^{kl} = y\,\alpha^{kl} = z$ or $x\,(\alpha^k)^l = y\,(\alpha^k)^l$. Thus $x \sim y$ with respect to α^k also. We conclude that the vertex set of C is a common orbit for all positive powers of α. Moreover z is a fixed point of α if and only if the same is true of all such powers. $\square$

The following result follows directly from Lemma 2.1.

Corollary 2.2. *Let α be a transformation in $\mathcal{T}_n$ and suppose that all the cycles in the digraph of α are* 1*-cycles. Let ε be an idempotent in $\mathcal{T}_n$ such that $\varepsilon = \alpha^r$, for some positive integer r. Then the orbits and fixed points of α and ε are identical.*

Lemma 2.3. *Let α be a transformation in $\mathcal{T}_n$ and suppose that all the cycles in the digraph of α are* 1*-cycles. If $\beta \in \mathcal{T}_n$ is any strong inverse of α then the orbits and fixed points of α and β are identical.*

Proof. Observe that since β is a strong inverse of α, the subsemigroup $S = \langle \alpha, \beta \rangle$ of $\mathcal{T}_n$ generated by α and β is an inverse semigroup. Therefore for any positive integer t we have that β^t is the unique inverse of α^t in S. Taking $t = r$ so that $\varepsilon = \alpha^r$ is an idempotent as in Corollary 2.2 we have that β^r is the unique inverse of $\alpha^r = \varepsilon$. Since an idempotent is its own unique inverse in S, we have that $\beta^r = \varepsilon$ also, and so $\alpha^r = \beta^r$. It follows immediately from Lemma 2.1 that the orbits and fixed points of α, β and ε are identical. $\square$

It follows from the definition of an order-preserving transformation on a finite chain that the iterative sequence of images $x, x\,\alpha, \ldots, x\,\alpha^k, \ldots$ of a point $x \in X_n$ under a transformation $\alpha \in \mathcal{O}_n$ must terminate in a fixed point, whence it follows that the cycles of the components of the digraph of α are merely fixed points. This observation leads to Proposition 2.4 below, see a proof in [12, Proposition 1.5]. From this we also note that the semigroup $\mathcal{O}_n$ is *aperiodic*, meaning that all of its subgroups are trivial as it follows from the previous observation that the cyclic subgroup of the monogenic subsemigroup $\langle\alpha\rangle$ of $\mathcal{O}_n$ has only one member.

Proposition 2.4 ([12, Proposition 1.5]). *The cycle of each component of $\alpha \in \mathcal{O}_n$ consists of a unique fixed point.*

Therefore, as it was noted in [12], the digraph of a mapping in $\mathcal{O}_n$ consists of components, each of which is a directed tree with all arcs directed towards the root, which represents a fixed point of the mapping. The next result follows from Proposition 2.4 and Lemma 2.3.

Corollary 2.5. *Let α, β be transformations in $\mathcal{O}_n$. If β is a strong inverse of α then α and β have the same orbits and their components have the same roots.*

Recall that any order-preserving transformation has a strong inverse in $\mathcal{T}_n$. However, as the next result shows, an order-preserving transformation does not have an order-preserving strong inverse unless the transformation is an idempotent.

Theorem 2.6. *Let $\alpha \in \mathcal{O}_n$. Then*

1) *α has a strong inverse in $\mathcal{O}_n$ if and only if α is an idempotent.*
2) *If α is a non-idempotent with at least two fixed points, then α has no strong inverse in $\mathcal{OP}_n$.*

Proof. Since the first statement of the theorem is clearly true in the forward direction, we assume that there exists a non-idempotent $\alpha \in \mathcal{O}_n$ that has a strong inverse β in $\mathcal{OP}_n$. Moreover, since an idempotent transformation may be characterized as a transformation that fixes each element of its image, for a non-idempotent α there exist distinct $u, v \in X_n$ such that $u\alpha = v$, $v\alpha \neq v$. Let C be the component of the digraph of α containing vertices u, v. Since C is a directed tree with all arcs directed towards the root, say, $z \in X_n$, there exists a unique directed path in C from u through v to z. Therefore there exist distinct vertices x, y distinct from z in this path such that $x\alpha = y$, $y\alpha = z$, and $z\alpha = z$. We may assume without loss of generality that $x < y$. Then since α is order-preserving we have that $y = x\alpha \leqslant y\alpha = z$, so that $x < y < z$ since $y \neq z$.

Since β is an inverse of α, $\beta\alpha$ is an idempotent transformation with image $X_n\beta\alpha = X_n\alpha$, so $y \in X_n\beta\alpha$ and $y\beta\alpha = y$. Let w denote $y\beta$. If $y \leqslant w$, then since α is order-preserving we have that $z = y\alpha \leqslant w\alpha = y\beta\alpha = y$, a contradiction to our earlier observation that $y < z$. Therefore we have $y\beta = w < y$.

Assume first that β is order-preserving, so an application of β to both sides of the inequality $y\beta < y$ yields $y\beta^2 \leqslant y\beta < y$, so $y\beta^2 < y < z$. By using a similar argument we obtain that $y\beta^3 < y < z$, and indeed

$$y\beta^m < y < z \text{ for any integer } m \geqslant 2. \tag{1}$$

Let $k \geqslant 2$ be chosen such that α^k is an idempotent, say ε. Put $m = k$ in Equation (1) above. On one hand by Corollary 2.2 we have that $y\alpha^k$ is the root of the common component of y under α and under ε, so that $y\alpha^k = z$. On the other hand we now obtain by Lemma 2.3 and Equation (1) that $y\alpha^k = y\beta^k < y < z$, a contradiction. It follows that if $\beta \in \mathcal{O}_n$ then α is an idempotent, and so the first statement is proved.

Finally assume that α has at least two fixed points and $\beta \in \mathcal{OP}_n$. Consider the (common) components $C(1)$ and $C(n)$ associated with digraphs of α and β containing 1 and n respectively. Since the components of α are intervals of the standard chain X_n (see Lemma 2.8 of [5]), it follows that if $C(1) = C(n)$ then α would have just one component and so just one fixed point, contrary to hypothesis. Hence $C(1) = \{1, 2, \dots, i\}$ and $C(n) = \{j, j+1, \dots, n\}$, for some $i < j$. But since these are also components of β, and β maps each of its components into itself, it follows that $1\,\beta$ lies in $C(1)$ and $n\,\beta$ lies in $C(n)$; in particular $1\,\beta < n\,\beta$, whence it follows from Proposition 2.3 of [5] that β lies in $\mathcal{O}_n$. But that contradicts the first part of our theorem. Therefore α does not have a strong inverse in $\mathcal{OP}_n$. □

An immediate consequence of the above is the result of A. Vernitski [18, Corollary 4].

Theorem 2.7. *Any inverse subsemigroup of $\mathcal{O}_n$ is a semilattice. The union of all inverse subsemigroups of $\mathcal{O}_n$ is just the set of idempotents of $\mathcal{O}_n$, or equivalently, the set of group elements of $\mathcal{O}_n$.*

Next we apply the above results to the semigroups $\mathcal{OP}_n$ of all orientation-preserving transformations of X_n and $\mathcal{P}_n$ of all orientation-preserving or orientation-reversing transformations of X_n. Let $\mathcal{OR}_n$ denote the set of all orientation-reversing transformations in $\mathcal{T}_n$. It was shown in [5] that $\mathcal{P}_n = \mathcal{OP}_n \cup \mathcal{OR}_n$,

$$\mathcal{OP}_n \cap \mathcal{OR}_n = \{\alpha \in \mathcal{T}_n : \operatorname{rank}(\alpha) \leqslant 2\},$$

$$\mathcal{OP}_n \cdot \mathcal{OR}_n = \mathcal{OR}_n = \mathcal{OR}_n \cdot \mathcal{OP}_n \text{ and } (\mathcal{OR}_n)^2 = \mathcal{OP}_n = (\mathcal{OP}_n)^2. \quad (2)$$

Note that for $n \leqslant 2$ we have $\mathcal{OP}_n = \mathcal{T}_n$ and so every element of $\mathcal{OP}_n$ has a strong inverse in $\mathcal{OP}_n$. Now $|\mathcal{OP}_3| = 24$ (see [5], Corollary 2.7), and $\mathcal{T}_3 \setminus \mathcal{OP}_3$ consists of the three transpositions, which reverse orientation. It is easily seen that each member of $\mathcal{OP}_3$ has a strong inverse: indeed, $\mathcal{P}_3 = \mathcal{T}_3$ (see [5]), and so $\mathcal{P}_3$ is covered by its inverse subsemigroups. Since the elements of $\mathcal{P}_3$ and $\mathcal{OP}_3$ of rank at most two coincide, and the ranks of a transformation and its inverse are the same, we only need to observe that the three permutations in $\mathcal{OP}_3$ each have strong inverses in $\mathcal{OP}_3$ as together they form a (cyclic) group.

Let θ denote the n-cycle $(1, 2, 3, \ldots, n)$ in $\mathcal{OP}_n$. As a consequence of Theorem 2.7 we can prove the following result:

Lemma 2.8. *A non-idempotent transformation in $\mathcal{OP}_n$ with at least two fixed points does not have a strong inverse in $\mathcal{OP}_n$.*

Proof. Observe that if $n \leqslant 3$ then any transformation in $\mathcal{OP}_n$ with at least two fixed points is an idempotent. Hence assume that $n \geqslant 4$. By Theorem 4.9 in [5], the digraph of any member of $\mathcal{OP}_n$ cannot have two cycles of different length. It follows that all the cycles of α are fixed points. By Corollary 4.12 in [5], the mapping α can be written as $\theta^{-m}\delta\theta^{m}$ for some $\delta \in \mathcal{O}_n$ and a non-negative integer m.

Now assume by way of contradiction that $\beta \in \mathcal{OP}_n$ is a strong inverse of α. Take the mapping

$$\varphi : \mathcal{OP}_n \to \mathcal{OP}_n \text{ defined by } \kappa\varphi = \theta^{m}\kappa\theta^{-m}$$

for $\kappa \in \mathcal{OP}_n$. Since θ is a permutation in $\mathcal{OP}_n$, the mapping φ is an automorphism of $\mathcal{OP}_n$. Moreover, $\alpha\varphi = \delta$ and $\beta\varphi = \theta^{m}\beta\theta^{-m}$, so φ maps

$\langle \alpha, \beta \rangle$ isomorphically onto $\langle \delta, \theta^m \beta \theta^{-m} \rangle$. Since, by our assumption, β is a strong inverse of α, we have that $\langle \alpha, \beta \rangle$ and $\langle \delta, \theta^m \beta \theta^{-m} \rangle$ are isomorphic inverse subsemigroups of $\mathcal{OP}_n$ and $\theta^m \beta \theta^{-m}$ is a strong inverse of δ.

We now note that α and its conjugate δ have the same number of fixed points. Indeed for any $x \in X_n$ we have that $x\,\alpha = x$ if and only if $x\,\theta^{-m}\delta\theta^m = x$, that is $(x\,\theta^{-m})\delta = x\,\theta^{-m}$. Thus $\delta \in \mathcal{O}_n$ has at least two fixed points, and by Theorem 2.6(2), δ does not have a strong inverse in $\mathcal{OP}_n$, a contradiction. $\square$

Putting together the observations above that $\mathcal{OP}_n$ is covered by its inverse subsemigroups when $n \leqslant 3$, and that if $n \geqslant 4$ then $\mathcal{OP}_n$ contains non-idempotent transformations with at least two fixed points, an application of the above lemma yields the following result.

Theorem 2.9. *The semigroup $\mathcal{OP}_n$ is covered by its inverse subsemigroups if and only if $n \leqslant 3$.*

Example. In $\mathcal{OP}_3$ we have the pair of strong inverses $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{pmatrix}$. We note that neither α nor β are idempotents, and α is a member of $\mathcal{O}_3$, while β is a member of $\mathcal{OP}_3$. The semigroup $\langle \alpha, \beta \rangle$ is the five-element combinatorial Brandt (inverse) semigroup, yet neither of α nor β is a group element. Hence, although $\mathcal{OP}_n$ is not covered by its inverse subsemigroups, its set of strong inverses encompasses more than its group elements (so that Theorem 2.7 is not true if $\mathcal{O}_n$ is replaced by $\mathcal{OP}_n$). We note that α is a member of $\mathcal{O}_3$ and β is a member of the semigroup of order-preserving mappings on the chain $3 < 1 < 2$. This however does not contradict Lemma 2.8 as both α and β have just one fixed point.

If $n \leqslant 3$, it is observed in [5] that $\mathcal{P}_n = \mathcal{T}_n$, and so $\mathcal{P}_n$ is covered by its inverse semigroups. The result below demonstrates that these are the only instances when this is true.

Theorem 2.10. *The semigroup $\mathcal{P}_n$ of all orientation-preserving or orientation reversing mappings is covered by its inverse subsemigroups if and only if $n \leqslant 3$.*

Proof. Assume $n \geqslant 4$ and choose, using Theorem 2.6, a transformation $\alpha \in \mathcal{OP}_n$ of rank at least 3 that has no strong inverse in $\mathcal{OP}_n$. Assume $\beta \in \mathcal{P}_n$ is a strong inverse of α in $\mathcal{P}_n$. Now any inverse of α has the same rank as α, so $\beta \in \mathcal{OR}_n$ with rank at least 3. But then by [5, Corollary 5.2] $\alpha = \alpha\beta\alpha \in \mathcal{OP}_n \cdot \mathcal{OR}_n \cdot \mathcal{OP}_n = \mathcal{OR}_n$. Since the rank of α is at least 3, and, in accordance with [5, Lemma 5.4], $\mathcal{OR}_n \cap \mathcal{OP}_n$ consists of transformations of rank at most 2, $\alpha \in \mathcal{OR}_n \setminus \mathcal{OP}_n$, a contradiction to the assumption that $\alpha \in \mathcal{OP}_n$. This completes the proof. $\square$

Acknowledgement

The first author acknowledges support by the Portuguese Government through the Portuguese Foundation FCT under the project PEst-OE/MAT/UI4080/2014.

References

[1] A. Ja. Aizenštat, The defining relations of the endomorphism semigroup of a finite linearly ordered set, *Sibirsk. Mat. Ž.* **3** (1962), 161-169 (Russian).

[2] A. Ja. Aizenštat, On homomorphisms of semigroups of endomorphisms of ordered sets, *Leningrad. Gos. Pedagog. Inst. Učen. Zap.* **238** (1962), 38-48 (Russian).

[3] R. E. Arthur and N. Ruškuc, Presentations for two extensions of the monoid of order-preserving mappings on a finite chain, *Southeast Asian Bull. Math* **24** (2000), 1-7.

[4] P. M. Catarino, Monoids of orientation-preserving mappings of a finite chain and their presentation, *Semigroups and Applications, St. Andrews(1997)*, 39–46, World Sci. Publ., River Edge, NJ, 1998.

[5] P. M. Catarino and P. M. Higgins, The monoid of orientation-preserving mappings on a chain, *Semigroup Forum*, **58**, (1999), 190-206.

[6] P. M. Catarino and P. M. Higgins, The pseudovariety generated by all semigroups of orientation preserving transformations on a finite cycle, *Int. J. Algebra Comput.*, **12**(3), (2002), 387-405.

[7] I. Dimitrova, V. H. Fernandes and J. Koppitz, The maximal subsemigroups of semigroups of transformations preserving or reversing the orientation on a finite chain, *Publ. Math. Debrecen*, **81**, 1-2, (2012), 11-29.

[8] V. H. Fernandes, G. M. S. Gomes and M. M. Jesus, Congruences on monoids of transformations preserving the orientation on a finite chain, *J. Algebra*, **321**(2009), no. 3, 743-757.

[9] L. M. Gluskin, Elementary Generalized Groups, *Mat. Sb. N. S.*, **41(83)** (1957), 23-36.

[10] G. M. S. Gomes and J. M. Howie, On the ranks of certain semigroups of order-preserving transformations, *Semigroup Forum* **45** (1992), no. 3, 272-282.

[11] P. M. Higgins, *Techniques of semigroup theory*, Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1992.

[12] P. M. Higgins, Combinatorial results for semigroups of order-preserving transformations. *Math. Proc. Camb. Phil. Soc.*, (1993), **113**, pp 281-296.

[13] J. M. Howie, Products of idempotents in certain semigroups of transformations, *Proc. Edinburgh Math. Soc.*, (1971), **17**, pp 223-236.

[14] A. Laradji and A. Umar, Combinatorial results for semigroups of order-preserving full transformations, *Semigroup Forum* **72** (2006), 51-62.

[15] D. B. McAlister, Semigroups generated by a group and an idempotent. *Comm. Algebra*, **26**(2), (1998), 515-547.

[16] B. M. Schein, A symmetric semigroup of transformations is covered by its inverse subsemigroups, *Acta Mat. Acad. Sci. Hung.*, **22**, (1971) 163-171.

[17] A. Umar, Combinatorial results for semigroups of orientation-preserving partial transformations, *J. Integer Seq.* **14** (2011), Article 11.7.5.

[18] A. Vernitski, Inverse subsemigroups and classes of finite aperiodic semigroups, *Semigroup Forum*, **78**, (2009), 486-497.

Contact information

Paula Catarino
Departamento de Matemática
Universidade de Trás-os-Montes e Alto Douro
5001-801 Vila Real, Portugal
E-Mail(s): `pcatarin@utad.pt`

Peter M. Higgins
Department of Mathematical Sciences
University of Essex
Colchester CO4 3SQ U.K.
E-Mail(s): `peteh@essex.ac.uk`

Inessa Levi
Department of Mathematics
Columbus State University
Columbus, GA 31907, USA
E-Mail(s): `levi_inessa@columbusstate.edu`

Received by the editors: 04.06.2014
and in final form 04.08.2014.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 172–192 RESEARCH ARTICLE

Projectivity and flatness over the graded ring of normalizing elements

T. Guédénon

Communicated by V. Mazorchuk

Abstract. Let k be a field, H a cocommutative bialgebra, A a commutative left H-module algebra, $Hom(H, A)$ the k-algebra of the k-linear maps from H to A under the convolution product, $Z(H, A)$ the submonoid of $Hom(H, A)$ whose elements satisfy the cocycle condition and G any subgroup of the monoid $Z(H, A)$. We give necessary and sufficient conditions for the projectivity and flatness over the graded ring of normalizing elements of A. When A is not necessarily commutative we obtain similar results over the graded ring of weakly semi-invariants of A replacing $Z(H, A)$ by the set $\chi(H, Z(A)^H)$ of all algebra maps from H to $Z(A)^H$, where $Z(A)$ is the center of A.

0. Introduction

It is well known that projectivity and flatness over the ring of invariants are important in the theory of Hopf-Galois extensions. These properties reflect the notions of principal bundles and homogeneous spaces in a noncommutative setting. In [8], when C is a bialgebra, A is a C-comodule algebra and G is any subgroup of the monoid of the grouplike elements of the A-coring $A \otimes C$, we have adapted to the graded set-up the methods and techniques of [5] to give necessary and sufficient conditions for the projectivity and flatness over the graded ring $\mathcal{S}(A)$ of semi-coinvariants of

2010 MSC: 16D40, 16W50, 16W30.
Key words and phrases: projective module, flat module, bialgebra, smash product, graded ring, normalizing element, weakly semi-invariant element.

A. When A and C are commutative, we obtained similar results for the graded ring $\mathcal{N}(A)$ of conormalizing elements of A. In the present paper, we are concerned with the dual situation. Let H be a cocommutative bialgebra, A a commutative left H-module algebra. Then $Hom_k(H, A)$ is a commutative algebra under the convolution product. Let us denote by $Z(H, A)$ the submonoid of the algebra $Hom_k(H, A)$ whose elements satisfy the cocycle condition. Let G be any subgroup of the monoid $Z(H, A)$. We give necessary and sufficient conditions for the projectivity and flatness over the graded ring of normalizing elements of A. In an appendix, we establish similar results for the graded ring $\mathcal{S}(A)$ of weakly semi-invariants of A replacing $Z(H, A)$ by the set $\chi(H, Z(A)^H)$ of all k-algebra maps from H to the subring of invariants of the center $Z(A)$ of A. In this case we do not assume that A is commutative. If H is finite dimensional, our results are not new: we can derive them from [8] (see Proposition 3.8). This article is the continuation of the papers [3], [6] and [7]. In [3], with S. Caenepeel, we gave necessary and sufficient conditions for projectivity and flatness over the endomorphism ring of a finitely generated module. In [6] and [7], we obtained similar results for the endomorphism ring of a finitely generated comodule over a coring and for the colour endomorphism ring of a finitely generated G-graded comodule, where G is an abelian group with a bicharacter. For other related results we refer to [2], where, with S. Caenepeel, we gave necessary and sufficient conditions for the projectivity of a relative Hopf module over the subring of coinvariants.

Throughout we will be working over a field k. All algebras and coalgebras are over k. Except where otherwise stated, all unlabelled tensor products and Hom are tensor products and Hom over k, and all modules are left modules.

1. Preliminaries from graded ring theory

We will use the following well-known results of graded ring theory [13]. Let G be a group, B a G-graded ring and ${}_{gr-B}\mathcal{M}$, the category of left G-graded B-modules.

- Let N be a left G-graded B-module. For every x in G, $N(x)$ is the graded B-module obtained from N by a shift of the gradation by x. As vector spaces, N and $N(x)$ coincide, and the actions of B on N and $N(x)$ are the same, but the gradations are related by $N(x)_y = N_{xy}$ for all $y \in G$.

- An object of ${}_{gr-B}\mathcal{M}$ is projective (resp. flat) in ${}_{gr-B}\mathcal{M}$ if and only if it is projective (resp. flat) in ${}_{B}\mathcal{M}$, the category of left B-modules.
- An object of ${}_{gr-B}\mathcal{M}$ is free in ${}_{gr-B}\mathcal{M}$ if it has a B-basis consisting of homogeneous elements, equivalently, if it is isomorphic to some $\oplus_{i\in I}B(x_i)$, where I is an index set and $(x_i)_{i\in I}$ is a family of elements of G.
- Any object of ${}_{gr-B}\mathcal{M}$ is a quotient of a free object in ${}_{gr-B}\mathcal{M}$, and any projective object in ${}_{gr-B}\mathcal{M}$ is isomorphic to a direct summand of a free object of ${}_{gr-B}\mathcal{M}$.
- An object of ${}_{gr-B}\mathcal{M}$ is flat in ${}_{gr-B}\mathcal{M}$ if and only if it is the inductive limit of finitely generated free objects in ${}_{gr-B}\mathcal{M}$.

2. Main results

Let k be a field. For a bialgebra H with comultiplication Δ_H and counit ϵ_H we will use the version of Sweedler's sigma notation

$$\Delta_H(h) = h_1 \otimes h_2, \text{ for all } h \in H.$$

For unexplained concepts and notation on bialgebras and actions of bialgebras on rings, we refer the reader to [11], [12] and [14]. A bialgebra H is said to be cocommmutative if

$$h_1 \otimes h_2 = h_2 \otimes h_1 \quad \forall h \in H.$$

For every H-module M we denote by M^H the k-submodule of M whose elements are H-invariant, that is,

$$M^H = \{m \in M : h.m = \epsilon_H(h)m, \text{ for all } h \in H\}.$$

Note that M^H is a trivial H-submodule of M.

A k-algebra A is an H-module algebra if A is an H-module satisfying

$$h.(ab) = (h_1.a)(h_2.b) \quad \text{and} \quad h.1_A = \epsilon_H(h)1_A \quad \forall a, b \in A, \quad h \in H.$$

Let A be an H-module algebra. Then the smash product algebra $A\#H$ is the k-algebra which is equal to $A \otimes H$ as a k-vector space, and has its multiplication given by

$$(a \otimes h)(a' \otimes h') = a(h_1.a') \otimes h_2h', \quad \forall a, a' \in A, \quad h, h' \in H.$$

An element a of A is normal if for every $u \in A$ we have $au = va$ and $ua = v'a$ for some elements $v, v' \in A$.

An element a of A is H-normal if a is a normal element of A and for every $h \in H$ we have $h.a = u_h a$ for some element $u_h \in A$.

An $A\#H$-module M is both an A-module and an H-module such that the A- and H-actions are compatible in the sense that

$$h.(am) = (h_1.a)(h_2.m) \quad \forall h \in H, a \in A, m \in M.$$

It is easy to see that A is an $A\#H$-module whenever A is an H-module algebra. Let us denote by ${}_{A\#H}\mathcal{M}$ the category of $A\#H$-modules. The morphisms of ${}_{A\#H}\mathcal{M}$ are left A-linear and left H-linear maps. Note that A^H is a subalgebra of A called the subring of invariants of A.

From now A is an H-module algebra and $Hom(H, A)$ is the vector space of k-linear maps from H to A. Let us equip $Hom(H, A)$ with the convolution product; i.e.,

$$(\phi \star \phi')(h) = \phi(h_1)\phi'(h_2) \quad \forall \phi, \phi' \in Hom(H, A).$$

It is well known that $Hom(H, A)$ with this product is an algebra with identity ϵ_H. An element ϕ of $Hom(H, A)$ satisfies the cocycle condition if

$$\phi(hh') = [h_1.\phi(h')]\phi(h_2) \quad \text{for all} \quad h, h' \in H \quad (\star),$$

When A is commutative and H is cocommutative, it is easy to see that an element ϕ of $Hom(H, A)$ satisfies the cocycle condition if the k-linear map

$$A\#H \to A\#H, a \otimes h \mapsto a\phi(h_1) \otimes h_2 \quad \text{is an algebra endomorphism.}$$

If $\phi \in Hom(H, A)$ satisfies the cocycle condition then $\phi(h) = \phi(h)\phi(1_H)$ for all $h \in H$. Therefore $\phi(1_H) \neq 0$ if $\phi \neq 0$.

Denote by $Z(H, A)$ the subset of $Hom(H, A)$ whose elements satisfy the cocycle condition and send 1_H to 1_A.

For any $a \in A$, we denote by a_M the k-endomorphism of M which defines the action of a on M; i.e. $a_M(m) = am$ for all $m \in M$.

Let M be an $A\#H$-module and denote by h_M the endomorphism of M that corresponds to the action of $h \in H$ on M. For each $\phi \in Hom(H, A)$, set (see [9], where H is a cocommutative Hopf algebra)

$$\rho_\phi(h) = \phi(h_2)_M \circ (h_1)_M \quad \text{for all} \quad h \in H.$$

Then ρ_ϕ is a k-linear map from H to $End(M)$. For any $a \in A$ we have

$$\rho_\phi(h)(am) = \phi(h_3)(h_1.a)(h_2m).$$

A simple computation gives

$$\rho_\phi(hh')(m) = \phi(h_2h'_2)(h_1h'_1m)$$

and

$$\rho_\phi(h) \circ \rho_\phi(h')(m) = \phi(h_3)[h_1.\phi(h'_2)](h_2h'_1m)$$

for all $h, h' \in H$ and $m \in M$.

If we assume that A is commutative, H is cocommutative and ϕ belongs to $Z(H, A)$, then the two formulas just mentioned above show that ρ_ϕ is an algebra homomorphism. So in the case where A is commutative, H is cocommutative and ϕ belongs to $Z(H, A)$, we can define for every $A\#H$-module M a new $A\#H$-module M^ϕ, the underlying A-module of which is the same as that of M, while the action of H is new and is given by the rule

$$h._\phi m = \rho_\phi(h)m = \phi(h_2)(h_1m) \quad \forall h \in H, m \in M.$$

We call M^ϕ the twisted $A\#H$-module obtained from M and ϕ.

Let A be commutative and H be cocommutative. Then $Z(H, A)$ is a submonoid of $Hom(H, A)$ under the convolution product. The monoid $Z(H, A)$ is commutative since the algebra $Hom(H, A)$ is commutative. For every $A\#H$-module M, we have

$$M^{\epsilon_H} = M, \quad (M^\phi)^\psi = M^{\phi\star\psi}, \quad A^\phi \otimes_A M = M^\phi \quad \forall \phi, \psi \in Z(H, A).$$

In the remainder of the section, we assume that A is commutative, H is a cocommutative bialgebra and G is any subgroup of the monoid $Z(H, A)$.

The case of main interest is when H is a Hopf algebra. In this case, $Z(H, A)$ is a group and we can take G to be any subgroup of the group $Z(H, A)$. For every $\phi \in G$, we will denote by $\bar{\phi}$ its inverse with respect to the convolution product.

Let M be an $A\#H$-module and ϕ an element of G. Set

$$M_\phi = \{m \in M; hm = \phi(h)m \quad \text{for all } h \in H\}.$$

Then

$$A_\phi = \{a \in A; h.a = \phi(h)a \quad \text{for all } h \in H\}.$$

Clearly, $M_{\epsilon_H} = M^H$ and M_ϕ is a k-vector subspace of M. We have $1_A \in A_\phi$ if and only if $\phi = \epsilon_H$. An element of M_ϕ will be called an H-normal element of M with respect to G. Thus an H-normal element of A with respect to G is a particular H-normal element of A.

Lemma 2.1. *For every $A\#H$-module M and every $\phi \in G$, we have*

$$M_\phi \simeq {}_{A\#H}Hom(A^\phi, M) \quad \textit{as vector spaces.}$$

Proof. Let us define $F : Hom(A^\phi, M) \to M$ by $F(f) = f(1_A)$. If f is $A\#H$-linear, we have

$$\begin{aligned} h(F(f)) = h(f(1_A)) &= f(h._\phi 1_A) = f[\phi(h_2)(h_1.1_A)] \\ &= f[\phi(h_2)\epsilon_H(h_1)1_A] \\ &= f[\phi(h)1_A] \\ &= \phi(h)f(1_A) = \phi(h)(F(f)). \end{aligned}$$

So $F(f) \in M_\phi$, and F is a k-linear map from ${}_{A\#H}Hom(A^\phi, M)$ to M_ϕ. Let $m \in M_\phi$ and set $G(m)(a) = am$. Then $G(m) \in {}_AHom(A^\phi, M)$. We have

$$\begin{aligned} G(m)(h._\phi a) = (h._\phi a)m &= \phi(h_2)(h_1.a)m = (h_1.a)\phi(h_2)m \\ &= (h_1.a)(h_2 m) = h(am) = h[G(m)(a)]. \end{aligned}$$

So $G(m) \in {}_{A\#H}Hom(A^\phi, M)$. It is obvious that F and G are inverse of each other. $\square$

If ϕ and ψ are elements of G and if M is an $A\#H$-module, we have $A_\phi M_\psi \subseteq M_{\phi\star\psi}$. In particular, $A_\phi A_\psi \subseteq A_{\phi\star\psi}$ and every M_ϕ is an A^H-module. It is obvious that if M and M' are $A\#H$-modules, and $f : M \to M'$ is an $A\#H$-linear map, then $f(M_\phi) \subseteq M'_\phi$ for all ϕ in G.

For more information about the vector spaces M_ϕ and M^ϕ, we refer to [9], where H is a Hopf algebra and $G = Z(H, A)$.

For every $A\#H$-module M, let us denote by $\mathcal{N}(M)$ the direct sum of the family $(M_\phi)_{\phi\in G}$ in the category of vector spaces. Then $\mathcal{N}(A)$ is the direct sum of the family $(A_\phi)_{\phi\in G}$ in the category of vector spaces. We have

$$\mathcal{N}(M) = \oplus_{\phi\in G} M_\phi \quad \text{and} \quad \mathcal{N}(A) = \oplus_{\phi\in G} A_\phi.$$

This means that $M_\phi \cap M_\psi = 0$ if $\phi \neq \psi$. We call $\mathcal{N}(M)$ the set of the H-normal elements of M with respect to G.

It is easy to see that $\mathcal{N}(A)$ is a commutative G-graded algebra which we will call the graded algebra of H-normal (or normalizing) elements of A with respect to G and $\mathcal{N}(M)$ is a G-graded $\mathcal{N}(A)$-module called the graded $\mathcal{N}(A)$-module of H-normal (or normalizing) elements of M with respect to G. We will denote by ${}_{gr-\mathcal{N}(A)}\mathcal{M}$ the category of G-graded $\mathcal{N}(A)$-modules. The morphisms of this category are the graded morphisms, that is, the $\mathcal{N}(A)$-linear maps of degree ϵ_H.

If N is an object of ${}_{gr-\mathcal{N}(A)}\mathcal{M}$, $N = \oplus_{\phi\in G}N_\phi$, then $A \otimes_{\mathcal{N}(A)} N$ is an object of ${}_{A\#H}\mathcal{M}$: the A-module structure is the obvious one and the H-action is defined by

$$h(a \otimes n_\phi) = \phi(h_2)(h_1.a) \otimes n_\phi, \quad a \in A, h \in H, n_\phi \in N_\phi.$$

Thus we get an induction functor,

$$A \otimes_{\mathcal{N}(A)} (-) : {}_{gr-\mathcal{N}(A)}\mathcal{M} \to {}_{A\#H}\mathcal{M}; \quad N \mapsto A \otimes_{\mathcal{N}(A)} N.$$

To each element $\phi \in G$, we associate a functor

$$(-)^\phi : {}_{A\#H}\mathcal{M} \to {}_{A\#H}\mathcal{M}; \quad M \mapsto M^\phi :$$

this functor $(-)^\phi$ is an isomorphism with inverse $(-)^{\overline{\phi}}$. Since A is commutative, we can also associate to each $\phi \in G$ a functor

$$(-)_\phi : {}_{A\#H}\mathcal{M} \to {}_{A^H}\mathcal{M}; \quad M \mapsto M_\phi.$$

We define the normalizing functor to be

$$\mathcal{N}(-) : {}_{A\#H}\mathcal{M} \to {}_{gr-\mathcal{N}(A)}\mathcal{M}, \quad M \mapsto \mathcal{N}(M) = \oplus_{\phi\in G}M_\phi,$$

which is a covariant left exact functor.

Lemma 2.2. $(A \otimes_{\mathcal{N}(A)} (-), \quad \mathcal{N}(-))$ *is an adjoint pair of functors: in other words, for any* $M \in {}_{A\#H}\mathcal{M}$ *and* $N \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$, *we have an isomorphism of vector spaces*

$${}_{A\#H}Hom(A \otimes_{\mathcal{N}(A)} N, M) \cong {}_{gr-\mathcal{N}(A)}Hom(N, \mathcal{N}(M)).$$

Proof. Let $N = \oplus_{\phi\in G}N_\phi$ be an object of ${}_{gr-\mathcal{N}(A)}\mathcal{M}$, M an object of ${}_{A\#H}\mathcal{M}$ and $f \in {}_{A\#H}Hom(A \otimes_{\mathcal{N}(A)} N, M)$. Let $n_\phi \in N_\phi$, that is, n_ϕ is a homogeneous element of N of degree ϕ. Then $1_A \otimes_{\mathcal{N}(A)} n_\phi$ is an element of $(A \otimes_{\mathcal{N}(A)} N)_\phi$ and $f(1_A \otimes_{\mathcal{N}(A)} n_\phi) \in M_\phi$. Let us define k-linear maps

$$u : {}_{A\#H}Hom(A \otimes_{\mathcal{N}(A)} N, M) \to Hom(N, \mathcal{N}(M))$$

by $u(f)(n_\phi) = f(1_A \otimes_{\mathcal{N}(A)} n_\phi)$ and

$$v : {}_{gr-\mathcal{N}(A)}Hom(N, \mathcal{N}(M)) \to Hom(A \otimes_{\mathcal{N}(A)} N, M)$$

by $v(g)(a \otimes_{\mathcal{N}(A)} n_\phi) = ag(n_\phi)$. Note that $g(n_\phi) \in M_\phi$ since g is an $\mathcal{N}(A)$-linear map of degree ϵ_H from N to $\mathcal{N}(M)$. It is easy to show that $u(f) \in {}_{gr-\mathcal{N}(A)}Hom(N, \mathcal{N}(M))$, that is, $u(f)$ is $\mathcal{N}(A)$-linear of degree ϵ_H. It is clear that $v(g)$ is A-linear. Let us show that it is H-linear. Take $h \in H$. We have

$$\begin{aligned}
v(g)(h(a \otimes n_\phi)) &= v(g)[\phi(h_2)(h_1.a) \otimes n_\phi] \\
&= \phi(h_2)(h_1.a)[g(n_\phi)] \\
&= (h_1.a)\phi(h_2)[g(n_\phi)] \\
&= (h_1.a)(h_2.[g(n_\phi)]) \\
&= h.(ag(n_\phi)) \\
&= h[v(g)(a \otimes n_\phi)].
\end{aligned}$$

It follows that $v(g) \in {}_{A\#H}Hom(A \otimes_{\mathcal{N}(A)} N, M)$. Now we have

$$u[v(g)](n_\phi) = v(g)(1_A \otimes_{\mathcal{N}(A)} n_\phi) = g(n_\phi)$$

and

$$v[u(f)](a \otimes_{\mathcal{N}(A)} n_\phi) = a[u(f)(n_\phi)] = a[f(1_A \otimes_{\mathcal{N}(A)} n_\phi)] = f(a \otimes_{\mathcal{N}(A)} n_\phi).$$

Hence u and v are inverse of each other. $\square$

Let us denote by F' the functor $A \otimes_{\mathcal{N}(A)} (-)$. The unit and counit of the adjunction pair $\left(F', \quad \mathcal{N}(-)\right)$ are the following: for $N \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$ and $M \in {}_{A\#H}\mathcal{M}$:

$$u_N : N \to \mathcal{N}(A \otimes_{\mathcal{N}(A)} N), \quad u_N(n_\phi) = 1_A \otimes_{\mathcal{N}(A)} n_\phi; \phi \in G$$

$$c_M : A \otimes_{\mathcal{N}(A)} \mathcal{N}(M) \to M, \quad c_M(a \otimes_{\mathcal{N}(A)} m) = am.$$

The adjointness property means that we have

$$\mathcal{N}(c_M) \circ u_{\mathcal{N}(M)} = id_{\mathcal{N}(M)}, \quad c_{F'(N)} \circ F'(u_N) = id_{F'(N)} \qquad (\star\star).$$

Lemma 2.3. *The functor $\mathcal{N}(-)$ commutes with direct sums. It commutes with direct limits if $A\#H$ is left noetherian.*

Proof. We know that A is finitely generated as an $A\#H$-module (its generator is 1_A). So for every $\phi \in G$, A^ϕ is finitely generated as an $A\#H$-module. It follows that the functor ${}_{A\#H}Hom(A^\phi, -)$ commute with arbitrary direct sums for every $\phi \in G$. Let $(M_i)_{i\in I}$ be a family of objects in ${}_{A\#H}\mathcal{M}$. Using Lemma 2.1, we have

$$\begin{array}{rcl}\mathcal{N}(\oplus_{i\in I}M_i) & = & \oplus_{\phi\in G}(\oplus_{i\in I}M_i)_\phi \\ & = & \oplus_{\phi\in G}[{}_{A\#H}Hom(A^\phi, \oplus_{i\in I}M_i)] \\ & = & \oplus_{\phi\in G}\oplus_{i\in I}[{}_{A\#H}Hom(A^\phi, M_i)] \\ & = & \oplus_{\phi\in G}\oplus_{i\in I}(M_i)_\phi \\ & = & \oplus_{i\in I}\oplus_{\phi\in G}(M_i)_\phi \\ & = & \oplus_{i\in I}\mathcal{N}(M_i),\end{array}$$

and we get the first assertion. Assume that $A\#H$ is left noetherian. Then every A^ϕ is finitely presented as an $A\#H$-module since every A^ϕ is finitely generated as an $A\#H$-module and $A\#H$ is left noetherian. It follows that the functor ${}_{A\#H}Hom(A^\phi, -)$ commutes with arbitrary direct limits for every $\phi \in G$. Let $(M_i)_{i\in I}$ be a directed family of objects in ${}_{A\#H}\mathcal{M}$. Using Lemma 2.1, we have

$$\begin{aligned}\mathcal{N}(\varinjlim M_i) &= \oplus_{\phi\in G}(\varinjlim M_i)_\phi \\ &= \oplus_{\phi\in G}[{}_{A\#H}Hom(A^\phi, \varinjlim M_i)] \\ &= \oplus_{\phi\in G}\varinjlim[{}_{A\#H}Hom(A^\phi, M_i)] \\ &= \oplus_{\phi\in G}\varinjlim(M_i)_\phi \\ &= \varinjlim \oplus_{\phi\in G}(M_i)_\phi \\ &= \varinjlim \mathcal{N}(M_i).\end{aligned}$$ $\square$

Let A be projective in ${}_{A\#H}\mathcal{M}$. Then each A^ϕ is projective in ${}_{A\#H}\mathcal{M}$ because the functor $(-)^\phi$ is an isomorphism. So by Lemma 2.1, the functor $(-)_\phi$ is exact for every $\phi \in G$. It follows that the functor $\mathcal{N}(-)$ is exact when A is projective in ${}_{A\#H}\mathcal{M}$.

Lemma 2.4. *Let M be an $A\#H$-module. Then*

(1) $(M^\phi)_\psi = M_{\overline{\phi}\star\psi} \quad \forall \phi, \psi \in G$;

(2) $\mathcal{N}(M)(\phi) = \mathcal{N}(M^{\overline{\phi}})$ *for every* $\phi \in G$;

(3) *The k-linear map $f : A \otimes_{\mathcal{N}(A)} \mathcal{N}(A^\phi) \to A^\phi$; $a \otimes_{\mathcal{N}(A)} u \mapsto au$ is an isomorphism in ${}_{A\#H}\mathcal{M}$.*

Proof. (1) Let $m \in M_{\overline{\phi}\star\psi}$. Then $hm = (\overline{\phi}\star\psi)(h)m$, i.e., $hm = \overline{\phi}(h_1)\psi(h_2)m$. Since M is equal to M^ϕ as an A-module and H is cocommutative, we get

$$h._\phi m = \phi(h_2)(h_1 m) = \phi(h_3)\overline{\phi}(h_1)\psi(h_2)m = \epsilon_H(h_1)\psi(h_2)m = \psi(h)m.$$

This means that $m \in (M^\phi)_\psi$. Now let $m \in (M^\phi)_\psi$. Then $m \in M^\phi$ and $h._\phi m = \psi(h)m$. It follows that

$$(\overline{\phi}\star\psi)(h)m = \overline{\phi}(h_1)\psi(h_2)m = \overline{\phi}(h_1)(h_2._\phi m) = \overline{\phi}(h_1)\phi(h_3)(h_2 m) = hm,$$

because H is cocommutative. This means that $m \in M_{\overline{\phi}\star\psi}$. Thus we showed that $m \in M_{\overline{\phi}\star\psi}$ if and only if $m \in (M^\phi)_\psi$.

(2) We have $\mathcal{N}(M)(\phi) = \oplus_{\psi\in G} M_{\phi\star\psi}$ and using (1), we have

$$\mathcal{N}(M^{\overline{\phi}}) = \oplus_{\psi\in G}((M^{\overline{\phi}})_\psi) = \oplus_{\psi\in G} M_{\overline{\overline{\phi}}\star\psi} = \oplus_{\psi\in G} M_{\phi\star\psi}.$$

(3) Assume that u is homogeneous of degree ψ in $\mathcal{N}(A^\phi)$. This means that $u \in (A^\phi)_\psi = A_{\overline{\phi}\star\psi}$. Since H is cocommutative and A is commutative, we have

$$\begin{aligned} h.(au) = (h_1.a)(h_2._\phi u) &= (h_1.a)\phi(h_3)(h_2.u) \\ &= (h_1.a)\phi(h_3)[(\overline{\phi}\star\psi)(h_2)]u \\ &= (h_1.a)\phi(h_4)\overline{\phi}(h_2)\psi(h_3)u \\ &= (h_1.a)\psi(h_2)u = \psi(h_2)(h_1.a)u. \end{aligned}$$

On the other hand, we have

$$f(h.(a\otimes_{\mathcal{N}(A)} u)) = f\big(\psi(h_2)(h_1.a)\otimes_{\mathcal{N}(A)} u\big) = \psi(h_2)(h_1.a)u.$$

Therefore, f is H-linear. Clearly, f is A-linear.

Note that $a\otimes_{\mathcal{N}(A)} u = au\otimes_{\mathcal{N}(A)} 1_A$ for every $a \in A$. Then f is an isomorphism of $A\#H$-modules: the inverse of f is defined by $a \mapsto a\otimes_{\mathcal{N}(A)} 1_A$. $\square$

Lemma 2.5. *For every index set I,*

1. $c_{\oplus_{i\in I} A^{\overline{\phi_i}}}$ *is an isomorphism;*
2. $u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}$ *is an isomorphism;*
3. *if A is projective in ${}_{A\#H}\mathcal{M}$, then u is a natural isomorphism; in other words, the induction functor $F' = A\otimes_{\mathcal{N}(A)}(-)$ is fully faithful.*

Proof. (1) It is straightforward to check that the canonical isomorphism

$$A \otimes_{\mathcal{N}(A)} (\oplus_{i\in I}\mathcal{N}(A)(\phi_i)) \simeq \oplus_{i\in I} A^{\overline{\phi_i}} \quad \text{is just} \quad c_{\oplus_{i\in I} A^{\overline{\phi_i}}} \circ (id_A \otimes \kappa),$$

where κ is the isomorphism $\oplus_{i\in I}\mathcal{N}(A)(\phi_i) \cong \mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}})$, (see Lemmas 2.3 and 2.4). So $c_{\oplus_{i\in I} A^{\overline{\phi_i}}}$ is an isomorphism.

(2) Putting $M = \oplus_{i\in I} A^{\overline{\phi_i}}$ in $(\star\star)$, we find

$$\mathcal{N}(c_{\oplus_{i\in I} A^{\overline{\phi_i}}}) \circ u_{\mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}})} = id_{\mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}})}.$$

From Lemmas 2.3 and 2.4, we get

$$\mathcal{N}(c_{\oplus_{i\in I} A^{\overline{\phi_i}}}) \circ u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)} = id_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}.$$

From (1), $\mathcal{N}(c_{\oplus_{i\in I} A^{\overline{\phi_i}}})$ is an isomorphism, hence $u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}$ is an isomorphism.

(3) Since A is projective in ${}_{A\#H}\mathcal{M}$, we know that the functor $\mathcal{N}(A)$ is exact. Take a free resolution $\oplus_{j\in J}\mathcal{N}(A)(\phi_j) \to \oplus_{i\in I}\mathcal{N}(A)(\phi_i) \to N \to 0$ of a left graded $\mathcal{N}(A)$-module N. Since u is natural and the tensor product commutes with arbitrary direct sums, using Lemma 2.4, we have a commutative diagram

$$\begin{tikzcd}
\oplus_{j\in J}\mathcal{N}(A)(\phi_j) \arrow[r] \arrow[d, "u_{\oplus_{j\in J}\mathcal{N}(A)(\phi_j)}"'] & \oplus_{i\in I}\mathcal{N}(A)(\phi_i) \arrow[r] \arrow[d, "u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}"'] & N \arrow[r] \arrow[d, "u_N"'] & 0 \\
\mathcal{N}(\oplus_{j\in J} A^{\overline{\phi_j}}) \arrow[r] & \mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}}) \arrow[r] & \mathcal{N}(A \otimes_{\mathcal{N}(A)} N) \arrow[r] & 0
\end{tikzcd}$$

The top row is exact. The bottom row is exact, since the sequence

$$\oplus_{j\in J} A^{\overline{\phi_j}} \longrightarrow \oplus_{i\in I} A^{\overline{\phi_i}} \longrightarrow A \otimes_{\mathcal{N}(A)} N \longrightarrow 0$$

is exact in ${}_{A\#H}\mathcal{M}$ (because $A \otimes_{\mathcal{N}(A)} (-)$ is right exact) and $\mathcal{N}(-)$ is an exact functor. By (2), $u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}$ and $u_{\oplus_{j\in J}\mathcal{N}(A)(\phi_j)}$ are isomorphisms. It follows from the five lemma that u_N is an isomorphism. $\square$

Theorem 2.6. *For $P \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$, we consider the following statements.*

(1) *$A \otimes_{\mathcal{N}(A)} P$ is projective in ${}_{A\#H}\mathcal{M}$ and u_P is injective;*

(2) *P is projective as a graded $\mathcal{N}(A)$-module;*

(3) *$A \otimes_{\mathcal{N}(A)} P$ is a direct summand in ${}_{A\#H}\mathcal{M}$ of some $\oplus_{i\in I} A^{\overline{\phi_i}}$, and u_P is bijective;*

(4) *there exists* $Q \in {}_{A\#H}\mathcal{M}$ *such that* Q *is a direct summand of some* $\oplus_{i\in I} A^{\overline{\phi_i}}$, *and* $P \cong \mathcal{N}(Q)$ *in* ${}_{gr-\mathcal{N}(A)}\mathcal{M}$;

(5) $A \otimes_{\mathcal{N}(A)} P$ *is a direct summand in* ${}_{A\#H}\mathcal{M}$ *of some* $\oplus_{i\in I} A^{\overline{\phi_i}}$.

Then (1) $\Rightarrow$ *(2)* $\Leftrightarrow$ *(3)* $\Leftrightarrow$ *(4)* $\Rightarrow$ *(5).*

If A *is projective in* ${}_{A\#H}\mathcal{M}$, *then (5)* $\Rightarrow$ *(3)* $\Rightarrow$ *(1).*

Proof. (2) $\Rightarrow$ (3). If P is projective as a right graded $\mathcal{N}(A)$-module, then we can find an index set I and $P' \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$ such that $\oplus_{i\in I}\mathcal{N}(A)(\phi_i) \cong P \oplus P'$. Obviously $\oplus_{i\in I} A^{\overline{\phi_i}} \cong \oplus_{i\in I}(A \otimes_{\mathcal{N}(A)} \mathcal{N}(A)(\phi_i)) \cong (A \otimes_{\mathcal{N}(A)} P) \oplus (A \otimes_{\mathcal{N}(A)} P')$. Since u is a natural transformation, we have a commutative diagram:

$$\begin{tikzcd}
\oplus_{i\in I}\mathcal{N}(A)(x_i) \arrow[r, "\cong"] \arrow[d, "u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}"'] & P \oplus P' \arrow[d, "u_P \oplus u_{P'}"] \\
\mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}}) \arrow[r, "\cong"'] & \mathcal{N}(A \otimes_{\mathcal{N}(A)} P) \oplus \mathcal{N}(A \otimes_{\mathcal{N}(A)} P')
\end{tikzcd}$$

From the fact that $u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}$ is an isomorphism (Lemma 2.5), it follows that u_P (and $u_{P'}$) are isomorphisms.

(3) $\Rightarrow$ (4). Take $Q = A \otimes_{\mathcal{N}(A)} P$.

(4) $\Rightarrow$ (2). Let $f : \oplus_{i\in I} A^{\overline{\phi_i}} \to Q$ be a split epimorphism in ${}_{A\#H}\mathcal{M}$. Then the map $\mathcal{N}(f) : \mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}}) \cong \oplus_{i\in I}\mathcal{N}(A)(\phi_i) \to \mathcal{N}(Q) \cong P$ is split surjective in ${}_{gr-\mathcal{N}(A)}\mathcal{M}$, hence P is projective as a right graded $\mathcal{N}(A)$-module.

(4) $\Rightarrow$ (5). We already proved that (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4). Since (5) is contained in (3), we get (4) $\Rightarrow$ (5).

(1) $\Rightarrow$ (2). Take an epimorphism $f : \oplus_{i\in I}\mathcal{N}(A)(\phi_i) \to P$ in ${}_{gr-\mathcal{N}(A)}\mathcal{M}$. Then

$$F(f) =: A \otimes_{\mathcal{N}(A)} (\oplus_{i\in I}\mathcal{N}(A)(\phi_i)) \cong \oplus_{i\in I} A^{\overline{\phi_i}} \to A \otimes_{\mathcal{N}(A)} P$$

is surjective because the functor $A \otimes_{\mathcal{N}(A)} (-)$ is right exact, and splits in ${}_{A\#H}\mathcal{M}$ since $A \otimes_{\mathcal{N}(A)} P$ is projective in ${}_{A\#H}\mathcal{M}$. Consider the commutative diagram

$$\begin{tikzcd}
\oplus_{i\in I}\mathcal{N}(A)(\phi_i) \arrow[r, "f"] \arrow[d, "u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}"'] & P \arrow[r] \arrow[d, "u_P"'] & 0 \\
\mathcal{N}(\oplus_{i\in I} A^{\overline{\phi_i}}) \arrow[r, "\mathcal{N}F(f)"'] & \mathcal{N}(A \otimes_{\mathcal{N}(A)} P) \arrow[r] & 0
\end{tikzcd}$$

The bottom row is split exact, since any functor, in particular $\mathcal{N}(-)$ preserves split exact sequences. By Lemma 2.5(2), $u_{\oplus_{i\in I}\mathcal{N}(A)(\phi_i)}$ is an isomorphism. A diagram chasing argument tells us that u_P is surjective. By assumption, u_P is injective, so u_P is bijective. We deduce that the top row is isomorphic to the bottom row, and therefore splits. Thus $P \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$ is projective.

(5) $\Rightarrow$ (3). Under the assumption that A is projective in ${}_{A\#H}\mathcal{M}$, (5) $\Rightarrow$ (3) follows from Lemma 2.5(3).

(3) $\Rightarrow$ (1). By (3), $A \otimes_{\mathcal{N}(A)} P$ is a direct summand of some $\oplus_{i\in I} A^{\overline{\phi_i}}$. If A is projective in ${}_{A\#H}\mathcal{M}$, then $\oplus_{i\in I} A^{\overline{\phi_i}}$ is projective in ${}_{A\#H}\mathcal{M}$. So $A \otimes_{\mathcal{N}(A)} P$ being a direct summand of a projective object of ${}_{A\#H}\mathcal{M}$ is projective in ${}_{A\#H}\mathcal{M}$. $\square$

Theorem 2.7. *Assume that $A\#H$ is left noetherian. For $P \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$, the following assertions are equivalent.*

(1) *P is flat as a graded $\mathcal{N}(A)$-module;*

(2) *$A \otimes_{\mathcal{N}(A)} P = \varinjlim Q_i$, where $Q_i \cong \oplus_{j\leqslant n_i} A^{\overline{\phi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$ for some positive integer n_i, and u_P is bijective;*

(3) *$A \otimes_{\mathcal{N}(A)} P = \varinjlim Q_i$, where $Q_i \in {}_{A\#H}\mathcal{M}$ is a direct summand of some $\oplus_{j\in I_i} A^{\overline{\phi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$, and u_P is bijective;*

(4) *there exists $Q = \varinjlim Q_i \in {}_{A\#H}\mathcal{M}$, such that $Q_i \cong \oplus_{j\leqslant n_i} A^{\overline{\phi_{ij}}}$ for some positive integer n_i and $\mathcal{N}(Q) \cong P$ in ${}_{gr-\mathcal{N}(A)}\mathcal{M}$;*

(5) *there exists $Q = \varinjlim Q_i \in {}_{A\#H}\mathcal{M}$, such that Q_i is a direct summand of some $\oplus_{j\in I_i} A^{\overline{\phi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$, and $\mathcal{N}(Q) \cong P$ in ${}_{gr-\mathcal{N}(A)}\mathcal{M}$.*

If A is projective in ${}_{A\#H}\mathcal{M}$, these conditions are also equivalent to conditions (2) and (3), without the assumption that u_P is bijective.

Proof. (1) $\Rightarrow$ (2). $P = \varinjlim N_i$, with $N_i = \oplus_{j\leqslant n_i}\mathcal{N}(A)(\phi_{ij})$. Take $Q_i = \oplus_{j\leqslant n_i} A^{\overline{\phi_{ij}}}$, then

$$\varinjlim Q_i \cong \varinjlim (A \otimes_{\mathcal{N}(A)} N_i) \cong A \otimes_{\mathcal{N}(A)} (\varinjlim N_i) \cong A \otimes_{\mathcal{N}(A)} P.$$

Consider the following commutative diagram:

$$\begin{tikzcd}
P = \varinjlim N_i \arrow[r, "\lim(u_{N_i})"] \arrow[d, "u_P"'] & \varinjlim \mathcal{N}(A \otimes_{\mathcal{N}(A)} N_i) \arrow[d, "f"] \\
\mathcal{N}(A \otimes_{\mathcal{N}(A)} (\varinjlim N_i)) \arrow[r, "\cong"'] & \mathcal{N}(\varinjlim (A \otimes_{\mathcal{N}(A)} N_i))
\end{tikzcd}$$

By Lemma 2.5(2), the u_{N_i} are isomorphisms. By Lemma 2.3, the natural homomorphism f is an isomorphism. Hence u_P is an isomorphism.

(2) $\Rightarrow$ (3) and (4) $\Rightarrow$ (5) are obvious.

(2) $\Rightarrow$ (4) and (3) $\Rightarrow$ (5). Put $Q = A \otimes_{\mathcal{N}(A)} P$. Then $u_P : P \to \mathcal{N}(A \otimes_{\mathcal{N}(A)} P)$ is the required isomorphism.

(5) $\Rightarrow$ (1). We have a split exact sequence $0 \to N_i \to P_i = \oplus_{j \in I_i} A^{\overline{\phi_{ij}}} \to Q_i \to 0$ in ${}_{A\#H}\mathcal{M}$. Consider the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & F\mathcal{N}(N_i) \arrow[r] \arrow[d, "c_{N_i}"'] & F\mathcal{N}(P_i) \arrow[r] \arrow[d, "c_{P_i}"'] & F\mathcal{N}(Q_i) \arrow[r] \arrow[d, "c_{Q_i}"'] & 0 \\
0 \arrow[r] & N_i \arrow[r] & P_i \arrow[r] & Q_i \arrow[r] & \mathbf{0}
\end{tikzcd}$$

We know from Lemma 2.5(1) that c_{P_i} is an isomorphism. Both rows in the diagram are split exact, so it follows that c_{N_i} and c_{Q_i} are also isomorphisms. Next consider the commutative diagram:

$$\begin{tikzcd}
A \otimes_{\mathcal{N}(A)} (\varinjlim \mathcal{N}(Q_i)) \arrow[r, "id_A \otimes f"] & A \otimes_{\mathcal{N}(A)} \mathcal{N}(Q) \arrow[d, "c_Q"] \\
\varinjlim (A \otimes_{\mathcal{N}(A)} \mathcal{N}(Q_i)) \arrow[u, "h"] \arrow[r, "\lim c_{Q_i}"] & Q
\end{tikzcd}$$

where h is the natural homomorphism and f is the isomorphism $\varinjlim \mathcal{N}(Q_i) \cong \mathcal{N}(\varinjlim(Q_i))$ (see Lemma 2.3). h is an isomorphism, because the functor $A \otimes_{\mathcal{N}(A)} (-)$ preserves inductive limits. $limc_{Q_i}$ is an isomorphism, because every c_{Q_i} is an isomorphism. It follows that c_Q is an isomorphism, hence $\mathcal{N}(c_Q)$ is an isomorphism. From ($\star\star$), we get $\mathcal{N}(c_Q) \circ u_{\mathcal{N}(Q)} = id_{\mathcal{N}(Q)}$. It follows that $u_{\mathcal{N}(Q)}$ is also an isomorphism. Since $\mathcal{N}(Q) \cong P$, u_P is an isomorphism. Consider the isomorphisms

$$P \cong \mathcal{N}(A \otimes_{\mathcal{N}(A)} P) \cong \mathcal{N}(A \otimes_{\mathcal{N}(A)} \mathcal{N}(Q)) \cong \mathcal{N}(Q) \cong \varinjlim \mathcal{N}(Q_i);$$

where the first isomorphism is u_P, the third is $\mathcal{N}(c_Q)$ and the last one is f. By Lemmas 2.3 and 2.4, each $\mathcal{N}(P_i) \cong \oplus_{j \in I} \mathcal{N}(A)(\phi_{ij})$ is projective as a right graded $\mathcal{N}(A)$-module, hence each $\mathcal{N}(Q_i)$ is also projective as a graded $\mathcal{N}(A)$-module, and we conclude that $P \in {}_{gr-\mathcal{N}(A)}\mathcal{M}$ is flat. The final statement is an immediate consequence of Lemma 2.5(3). $\square$

Let us examine some particular cases.

• Let H be a finite dimensional cocommutative bialgebra and A a commutative left H-module algebra. Then $H^* = Hom(H,k)$ is a commutative bialgebra: the product of H^* is the convolution product

$$(f \star f')(h) = f(h_1)f'(h_2); f, f' \in H^*, h \in H.$$

We know that A is a right H^*-comodule algebra. Denote by $\mathcal{C}$ the coring $A \otimes H^*$. Then $\mathcal{C}$ is a commutative algebra under the product

$$(a \otimes f)(a \otimes f') = aa' \otimes (f \star f'); a, a' \in A, f, f' \in H^*.$$

Denote by $G(\mathcal{C})$ the monoid of grouplike elements of $\mathcal{C}$. It is well known that the k-linear map $\eta : \mathcal{C} \to Hom(H,A)$ defined by

$$\eta(\sum a_i \otimes f_i)(h) = \sum a_i f_i(h); a_i \in A, f_i \in H^*, h_i \in H$$

is an isomorphism of k-algebras.

For the proof of the following proposition, we refer to [10], where H is a Hopf algebra.

Proposition 2.8. *With the above notations, let H be a finite dimensional cocommutative bialgebra and A a commutative left H-module algebra. Then*

$$\eta(G(\mathcal{C})) = Z(H,A).$$

Consequently, if G is a subgroup of the monoid $G(\mathcal{C})$, then $\eta(G)$ is a subgroup of the monoid $Z(H,A)$. Conversely, if G is a subgroup of the monoid $Z(H,A)$, then $\eta^{-1}(G)$ is a subgroup of the monoid $G(\mathcal{C})$.

It follows from Proposition 2.8 that our results are not new if H is finite-dimensional: they can be derived from [8]. We refer to [1] for more information on corings and comodules over corings.

•• Let g be a Lie algebra and $U(g)$ the enveloping algebra of g. It is well known that an algebra A is a $U(g)$-module algebra if and only if g acts on A by derivations. An element a of A is $U(g)$-normal if and only if it is g-normal, here a is a g-normal element if a is a normal element of A and for every $x \in g$ we have $x.a = u_x a$ for some u_x in A. Let A be a commutative $U(g)$-module algebra. Let us denote by $Z(g,A)$ the set of k-linear maps ϕ from g to A satisfying the cocycle condition $\phi([x,y]) = x.\phi(y) - y.\phi(x)$ for all $x, y \in g$. Clearly $Z(g,A)$ is an abelian additive group. It is easy to see that there is a bijection from $Z(g,A)$ to $Z(U(g),A)$. An element a of A is $U(g)$-normal with respect to $Z(U(g),A)$ if and only if it is g-normal with respect to $Z(g, A)$. So in the case of a Lie algebra g acting by derivations on a commutative algebra A, we can replace everywhere in our results $Z(U(g), A)$ by $Z(g, A)$.

• • • Let Γ be a group and $k\Gamma$ the group algebra of Γ. It is well known that an algebra A is a $k\Gamma$-module algebra if and only if Γ acts on A by automorphisms. An element a of A is $k\Gamma$-normal if and only if it is Γ-normal, here a is a Γ-normal element if a is a normal element of A and for every $x \in \Gamma$ we have $x.a = u_x a$ for some u_x in A. Let A be a commutative $k\Gamma$-module algebra. Let us denote by $Z(\Gamma, A)$ the set of maps ϕ from Γ to the set $U(A)$ of invertible elements of A satisfying the cocycle condition $\phi(xx') = [x.\phi(x')]\phi(x)$ for all $x, x' \in \Gamma$. Clearly $Z(\Gamma, A)$ is an abelian group $(\phi\phi')(x) = \phi(x)\phi'(x)$. It is easy to see that there is a bijection from $Z(\Gamma, A)$ to $Z(k\Gamma, A)$. An element a of A is $k\Gamma$-normal with respect to $Z(k\Gamma, A)$ if and only if it is Γ-normal with respect to $Z(\Gamma, A)$. So in the case of a group Γ acting by automorphisms on a commutative algebra A, we can replace everywhere in our results $Z(k\Gamma, A)$ by $Z(\Gamma, A)$.

• • •• Let Γ be an algebraic group and $k[\Gamma]$ the affine coordinate ring of Γ. It is well known that an affine variety X is a left Γ-module if and only if $k[X]$ is a right $k[\Gamma]$-comodule algebra. Note that $k[\Gamma]$ is a commutative Hopf algebra. Since a finite group is an algebraic group, our results are not new for a finite group acting by automorphisms on an affine variety: they can be derived from [8].

3. Appendix

We keep the conventions and notations of the preceding section. Let H be a bialgebra. Denote by $\chi(H, A^H)$ the set of all k-algebra maps from H to A^H. Clearly, $\chi(H, A^H)$ is a subset of $Hom(H, A)$. Let χ be an element of $\chi(H, A^H)$. It is easy to see that the map ρ_χ defined in the preceding section is an algebra homomorphism without the assumption that A is commutative and H is cocommutative. Likewise the set $\chi(H, A^H)$ is a monoid under the convolution product with identity ϵ_H. For χ in $\chi(H, A^H)$, we can define a new $A\#H$-module M^χ (exactly as in section 2), the underlying A-module of which is the same as that of M, while the action of H is new and is given by the rule

$$h._\chi m = \chi(h_2)(h_1 m) \quad \forall h \in H, m \in M.$$

We call M^χ the twisted $A\#H$-module obtained from M and χ.

If A is an H-module algebra, then the center $Z(A)$ of A is an H-module algebra and $Z(A)^H$ is a subalgebra of A^H. Let us denote by $\chi(H, Z(A)^H)$

the set of all k-algebra maps from H to $Z(A)^H$. It is a submonoid of $\chi(H, A^H)$.

A careful examination of the lemmas of section 2 shows that we have used the commutativity of A to get $\phi(H)$ contained in the center $Z(A)$ of A (see Lemmas 2.1 and 2.2). But this fact is always true for $\chi(H, Z(A)^H)$. Note also that it is only in Lemma 2.4 that the computations use the cocommutativity of H and that we have used Lemme 2.4 in the proof of Lemma 2.5. These remarks suggest that all the results of the preceding section are true replacing $Z(H, A)$ by $\chi(H, Z(A)^H)$ without the assumption that A is commutative.

Let us assume that G is any subgroup of the monoid $\chi(H, Z(A)^H)$.

For every $\chi \in G$ we will denote by $\bar{\chi}$ its inverse. Note that if H is a Hopf algebra, then $\chi(H, Z(A)^H)$ is a group and we can take $G = \chi(H, Z(A)^H)$ in our results. This group is commutative if H is cocommutative. Any element χ of $\chi(H, Z(A)^H)$ satisfies $\bar{\chi} = \chi S_H$ if H is a Hopf algebra with antipode S_H.

For an $A\#H$-module M and for an element χ of G, the elements of M_χ will be called the weakly H-semi-invariant elements of M.

The proofs of the following results are similar to those of the preceding section and we omit them.

Lemma 3.1. *Under the above notations, for every $A\#H$-module M and every $\chi \in G$, we have*

$$M_\chi \simeq {}_{A\#H}Hom(A^\chi, M) \quad \textit{as vector spaces.}$$

If χ and λ are elements of G and if M is an $A\#H$-module we have $A_\chi M_\lambda \subseteq M_{\chi\star\lambda}$. In particular, $A_\chi A_\lambda \subseteq A_{\chi\star\lambda}$ and every M_χ is an A^H-module.

It is obvious that if M and M' are $A\#H$-modules, and $f : M \to M'$ is $A\#H$-linear, then $f(M_\chi) \subseteq M'_\chi$ for all χ in G.

For every $A\#H$-module M, let us denote by $\mathcal{S}(M)$ the direct sum of the family $(M_\chi)_{\chi\in G}$ in the category of vector spaces. We have

$$\mathcal{S}(M) = \oplus_{\chi\in G} M_\chi \quad \text{and} \quad \mathcal{S}(A) = \oplus_{\chi\in G} A_\chi$$

We call $\mathcal{S}(M)$ (resp. $\mathcal{S}(A)$) the set of the weakly H-semi-invariant elements of M (resp. of A) with respect to G. It is easy to see that $\mathcal{S}(A)$ is a G-graded algebra and $\mathcal{S}(M)$ is a left G-graded $\mathcal{S}(A)$-module. We call

$\mathcal{S}(A)$ the graded algebra of weakly semi-invariants of A with respect to G and $\mathcal{S}(M)$ the graded $\mathcal{S}(A)$-module of weakly semi-invariants of M with respect to G. We will denote by ${}_{gr-\mathcal{S}(A)}\mathcal{M}$ the category of G-graded $\mathcal{S}(A)$-modules. The morphisms of this category are the graded morphisms, that is, the $\mathcal{S}(A)$-linear maps of degree ϵ_H. For any object $N \in {}_{gr-\mathcal{S}(A)}\mathcal{M}$, $A \otimes_{\mathcal{S}(A)} N$ is an object of ${}_{A\#H}\mathcal{M}$: the A-module structure is the obvious one and the H-action is defined by $h(a \otimes n_\chi) = \chi(h_2)(h_1.a) \otimes n_\chi$, where $a \in A$, $h \in H$ and $n_\chi \in N_\chi$. We have an induction functor,

$$A \otimes_{\mathcal{S}(A)} - : {}_{gr-\mathcal{S}(A)}\mathcal{M} \to {}_{A\#H}\mathcal{M}; \quad N \mapsto A \otimes_{\mathcal{S}(A)} N.$$

To each element $\chi \in G$, we associate a functor

$$(-)^\chi : {}_{A\#H}\mathcal{M} \to {}_{A\#H}\mathcal{M}; \quad M \mapsto M^\chi,$$

which is an isomorphim with inverse $(-)^{\overline{\chi}}$. We also associate to each $\chi \in G$ a functor

$$(-)_\chi : {}_{A\#H}\mathcal{M} \to {}_{A^H}\mathcal{M}; \quad M \mapsto M_\chi.$$

We define the weakly semi-invariant functor

$$\mathcal{S}(-) : {}_{A\#H}\mathcal{M} \to {}_{gr-\mathcal{S}(A)}\mathcal{M}, \quad M \mapsto \mathcal{S}(M) = \oplus_\chi M_\chi,$$

which is a covariant left exact functor.

Lemma 3.2. *Under the above notations, $(A \otimes_{\mathcal{S}(A)} (-), \quad \mathcal{S}(-))$ is an adjoint pair of functors; in other words, for any $M \in {}_{A\#H}\mathcal{M}$ and $N \in {}_{gr-\mathcal{S}(A)}\mathcal{M}$, we have an isomorphism of vector spaces*

$${}_{A\#H}Hom(A \otimes_{\mathcal{S}(A)} N, M) \cong {}_{gr-\mathcal{S}(A)}Hom(N, \mathcal{S}(M)).$$

Let us denote by F' the functor $A \otimes_{\mathcal{S}(A)} (-)$. The unit and counit of the adjunction pair $(F', \quad \mathcal{S}(-))$ are the following: for $N \in {}_{gr-\mathcal{S}(A)}\mathcal{M}$ and $M \in {}_{A\#H}\mathcal{M}$:

$$u_N : N \to \mathcal{S}(A \otimes_{\mathcal{S}(A)} N), \quad u_N(n) = 1_A \otimes_{\mathcal{S}(A)} n$$

$$c_M : A \otimes_{\mathcal{S}(A)} \mathcal{S}(M) \to M, \quad c_M(a \otimes_{\mathcal{S}(A)} m) = am.$$

The adjointness property means that we have

$$\mathcal{S}(c_M) \circ u_{\mathcal{S}(M)} = id_{\mathcal{S}(M)}, \quad c_{F'(N)} \circ F'(u_N) = id_{F'(N)} \qquad (\star\star\star).$$

Lemma 3.3. *Under the above notations, the functor $\mathcal{S}(-)$ commutes with direct sums. It commutes with direct limits if $A\#H$ is left noetherian.*

Let A be projective in ${}_{A\#H}\mathcal{M}$. Then each A^χ is projective in ${}_{A\#H}\mathcal{M}$ because the functor $(-)^\chi$ is an isomorphism. So by Lemma 3.1, the functor $(-)_\chi$ is exact for every $\chi \in G$. It follows that the functor $\mathcal{S}(-)$ is exact if A is projective in ${}_{A\#H}\mathcal{M}$.

Lemma 3.4. *Under the above notations, let H be cocommutative and let M be an $A\#H$-module. Then we have*

(1) $(M^\chi)_\lambda = M_{\overline{\chi}\star\lambda}$ *for every* $\chi \in G$.

(2) $\mathcal{S}(M)(\chi) = \mathcal{S}(M^{\overline{\chi}})$ *for every* $\chi \in G$;

(3) *The* k*-linear map* $f : A \otimes_{\mathcal{S}(A)} \mathcal{S}(A^\chi) \to A^\chi$; $a \otimes_{\mathcal{S}(A)} u \mapsto au$ *is an isomorphism in* ${}_{A\#H}\mathcal{M}$.

Lemma 3.5. *Under the above notations, let H be cocommutative. For every index set I,*

(1) $c_{\oplus_{i\in I} A^{\overline{\chi_i}}}$ *is an isomorphism;*

(2) $u_{\oplus_{i\in I}\mathcal{S}(A)(\chi_i)}$ *is an isomorphism;*

(3) *if A is projective in ${}_{A\#H}\mathcal{M}$, then u is a natural isomorphism; in other words, the induction functor $F' = A \otimes_{\mathcal{S}(A)} (-)$ is fully faithful.*

Theorem 3.6. *Let H be cocommutative. For $P \in {}_{gr-\mathcal{S}(A)}\mathcal{M}$, we consider the following statements.*

(1) $A \otimes_{\mathcal{S}(A)} P$ *is projective in* ${}_{A\#H}\mathcal{M}$ *and* u_P *is injective;*

(2) P *is projective as a graded* $\mathcal{S}(A)$*-module;*

(3) $A \otimes_{\mathcal{S}(A)} P$ *is a direct summand in* ${}_{A\#H}\mathcal{M}$ *of some* $\oplus_{i\in I} A^{\overline{\chi_i}}$, *and* u_P *is bijective;*

(4) *there exists* $Q \in {}_{A\#H}\mathcal{M}$ *such that* Q *is a direct summand of some* $\oplus_{i\in I} A^{\overline{\chi_i}}$, *and* $P \cong \mathcal{S}(Q)$ *in* ${}_{gr-\mathcal{S}(A)}\mathcal{M}$;

(5) $A \otimes_{\mathcal{S}(A)} P$ *is a direct summand in* ${}_{A\#H}\mathcal{M}$ *of some* $\oplus_{i\in I} A^{\overline{\chi_i}}$.

Then (1) $\Rightarrow$ (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4) $\Rightarrow$ (5).

If A is projective in ${}_{A\#H}\mathcal{M}$, then (5) $\Rightarrow$ (3) $\Rightarrow$ (1).

Theorem 3.7. *Let H be cocommutative. Assume that $A\#H$ is left noetherian. For $P \in {}_{gr-\mathcal{S}(A)}\mathcal{M}$, the following assertions are equivalent.*

(1) *P is flat as a graded $\mathcal{S}(A)$-module;*

(2) *$A \otimes_{\mathcal{S}(A)} P = \varinjlim Q_i$, where $Q_i \cong \oplus_{j \leqslant n_i} A^{\overline{\chi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$ for some positive integer n_i, and u_P is bijective;*

(3) *$A \otimes_{\mathcal{S}(A)} P = \varinjlim Q_i$, where $Q_i \in {}_{A\#H}\mathcal{M}$ is a direct summand of some $\oplus_{j \in I_i} A^{\overline{\chi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$, and u_P is bijective;*

(4) *there exists $Q = \varinjlim Q_i \in {}_{A\#H}\mathcal{M}$, such that $Q_i \cong \oplus_{j \leqslant n_i} A^{\overline{\chi_{ij}}}$ for some positive integer n_i and $\mathcal{S}(Q) \cong P$ in ${}_{gr-\mathcal{S}(A)}\mathcal{M}$;*

(5) *there exists $Q = \varinjlim Q_i \in {}_{A\#H}\mathcal{M}$, such that Q_i is a direct summand of some $\oplus_{j \in I_i} A^{\overline{\chi_{ij}}}$ in ${}_{A\#H}\mathcal{M}$, and $\mathcal{S}(Q) \cong P$ in ${}_{gr-\mathcal{S}(A)}\mathcal{M}$.*

If A is projective in ${}_{A\#H}\mathcal{M}$, these conditions are also equivalent to conditions (2) and (3), without the assumption that u_P is bijective.

Note that in all our results, G can be any subgroup of the set of characters $\chi(H)$ of H, that is the set of all k-algebra maps from H to k.

For further information about the vector space M_χ and the above functors we refer to [4], where H is a finite-dimensional Hopf algebra and χ is a character of H.

Acknowledgement

The author is grateful to the referee for his or her interesting remarks and helpful suggestions.

References

[1] T. Brzezinski and R. Wisbauer, “Comodules and corings", London Math. Soc. Lect. Note Series, *309*, Cambridge Univ. Press, Cambridge 2003.

[2] S. Caenepeel and T. Guédénon, Projectivity of a relative Hopf module over the subring of coinvariants, “ Hopf Algebras Chicago 2002", Lect. Notes in Pure and Appl. Math. *237*, Dekker, New York 2004, 97-108.

[3] S. Caenepeel and T. Guédénon, Projectivity and flatness over the endomorphism ring of a finitely generated module, Int. J. Math. Math. Sci. *30*, (2004), 1581-1588.

[4] S. Caenepeel, S. Raianu and F. Van Oystaeyen, Induction and coinduction for Hopf algebras: Applications, J. Algebra *165*, (1994), 204-222.

[5] J. J. Garcia and A. Del Rio, On flatness and projectivity of a ring as a module over a fixed subring, Math. Scand. *76* $n^\circ 2$, (1995), 179-193.

[6] T. Guédénon, Projectivity and flatness over the endomorphism ring of a finitely generated comodule, Beitrage zur Algebra und Geometrie *49* $n^\circ 2$, (2008), 399-408.

[7] T. Guédénon, Projectivity and flatness over the colour endomorphism ring of a finitely generated graded comodule, Beitrage zur Algebra und Geometrie *49* $n^\circ 2$, (2008), 399-408.

[8] T. Guédénon, Projectivity and flatness over the graded ring of semi-coinvariants, Algebra and Discrete Math. *10* $n^\circ 1$, (2010), 42-56.

[9] T. Guédénon, On the H-finite cohomology, Journ. of Algebra *273* $n^\circ 2$, (2004), 455-488.

[10] T. Guédénon, Picard groups of rings of coinvariants, Algebra and Represent. Theory *11* $n^\circ 1$, (2008), 25-42.

[11] C. Kassel, "Quantum groups' Graduate Texts in Mathematics *155*, Springer-Verlag, 1995.

[12] S. Montgomery, "Hopf algebra and their actions on rings", Providence, AMS, 1993.

[13] C. Nastasescu and F. Van Oystaeyen, "Methods of graded rings", Lecture Notes Math., Springer, 2004.

[14] M. Sweedler, "Hopf algebras", Benjamin New York, 1969.

Contact information

T. Guédénon

Département de Mathématiques
Université de Ziguinchor
B.P. 523 Ziguinchor, SENEGAL
E-Mail(s): Thomas.guedenon@univ-zig.sn

Received by the editors: 23.11.2013
and in final form 29.10.2014.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 193–199 RESEARCH ARTICLE

On one-sided interval edge colorings of biregular bipartite graphs

Rafayel Ruben Kamalian

Communicated by V. Mazorchuk

Abstract. A proper edge t-coloring of a graph G is a coloring of edges of G with colors $1, 2, \dots, t$ such that all colors are used, and no two adjacent edges receive the same color. The set of colors of edges incident with a vertex x is called a spectrum of x. Any nonempty subset of consecutive integers is called an interval. A proper edge t-coloring of a graph G is interval in the vertex x if the spectrum of x is an interval. A proper edge t-coloring φ of a graph G is interval on a subset R_0 of vertices of G, if for any $x \in R_0$, φ is interval in x. A subset R of vertices of G has an i-property if there is a proper edge t-coloring of G which is interval on R. If G is a graph, and a subset R of its vertices has an i-property, then the minimum value of t for which there is a proper edge t-coloring of G interval on R is denoted by $w_R(G)$. We estimate the value of this parameter for biregular bipartite graphs in the case when R is one of the sides of a bipartition of the graph.

We consider undirected, finite graphs without loops and multiple edges. $V(G)$ and $E(G)$ denote the sets of vertices and edges of a graph G, respectively. For any vertex $x \in V(G)$, we denote by $N_G(x)$ the set of vertices of a graph G adjacent to x. The degree of a vertex x of a graph G is denoted by $d_G(x)$, the maximum degree of a vertex of G by $\Delta(G)$. For a graph G and an arbitrary subset $V_0 \subseteq V(G)$, we denote by $G[V_0]$ the subgraph of G induced by the subset V_0 of its vertices.

2010 MSC: 05C15, 05C50, 05C85.

Key words and phrases: proper edge coloring, interval edge coloring, interval spectrum, biregular bipartite graph.

Using a notation $G(X, Y, E)$ for a bipartite graph G, we mean that G has a bipartition (X, Y) with the sides X, Y, and $E = E(G)$.

An arbitrary nonempty subset of consecutive integers is called an interval. An interval with the minimum element p and the maximum element q is denoted by $[p, q]$.

A function $\varphi : E(G) \to [1, t]$ is called a proper edge t-coloring of a graph G, if all colors are used, and no two adjacent edges receive the same color.

The minimum $t \in \mathbb{N}$ for which there exists a proper edge t-coloring of a graph G is denoted by $\chi'(G)$ [26].

For a graph G and any $t \in [\chi'(G), |E(G)|]$, we denote by $\alpha(G, t)$ the set of all proper edge t-colorings of G. Let

$$\alpha(G) \equiv \bigcup_{t=\chi'(G)}^{|E(G)|} \alpha(G, t).$$

If G is a graph, $x \in V(G)$, $\varphi \in \alpha(G)$, then let us set $S_G(x, \varphi) \equiv \{\varphi(e)/e \in E(G), e \text{ is incident with } x\}$.

We say that $\varphi \in \alpha(G)$ is persistent-interval in the vertex $x_0 \in V(G)$ of the graph G iff $S_G(x_0, \varphi) = [1, d_G(x_0)]$. We say that $\varphi \in \alpha(G)$ is persistent-interval on the set $R_0 \subseteq V(G)$ iff φ is persistent-interval in $\forall x \in R_0$.

We say that $\varphi \in \alpha(G)$ is interval in the vertex $x_0 \in V(G)$ of the graph G iff $S_G(x_0, \varphi)$ is an interval. We say that $\varphi \in \alpha(G)$ is interval on the set $R_0 \subseteq V(G)$ iff φ is interval in $\forall x \in R_0$.

We say that a subset R of vertices of a graph G has an i-property iff there exists $\varphi \in \alpha(G)$ interval on R; for a subset $R \subseteq V(G)$ with an i-property, the minimum value of t warranting existence of $\varphi \in \alpha(G, t)$ interval on R is denoted by $w_R(G)$.

Notice that the problem of deciding whether the set of all vertices of an arbitrary graph has an i-property is NP-complete [7, 8, 17]. Unfortunately, even for an arbitrary bipartite graph (in this case the interest is strengthened owing to the application of an i-property in timetablings [6, 17]) the problem keeps the complexity of a general case [3, 12, 25]. Some positive results were obtained for graphs of certain classes with numerical or structural restrictions [9, 11, 13–15, 17, 19–22, 28, 29]. The examples of bipartite graphs whose sets of vertices have not an i-property are given in [6, 13, 16, 23, 25].

The subject of this research is a parameter $w_R(G)$ of a bipartite graph $G = G(X, Y, E)$ in the case when R is one of the sides of the bipartition of G (the exact value of this parameter for an arbitrary bipartite graph is not known as yet). We obtain an upper bound of the parameter being discussed for biregular [2–5, 24] bipartite graphs, and the exact values of it in the case of the complete bipartite graph $K_{m,n}$ ($m \in \mathbb{N}, n \in \mathbb{N}$) as well.

The terms and concepts that we do not define can be found in [27].

First we recall some known results.

Theorem 1 ([7, 8, 17])**.** *If R is one of the sides of a bipartition of an arbitrary bipartite graph $G = G(X, Y, E)$, then: 1) there exists $\varphi \in \alpha(G, |E|)$ interval on R, 2) for $\forall t \in [w_R(G), |E|]$, there exists $\psi_t \in \alpha(G, t)$ interval on R.*

Theorem 2 ([1, 7, 8])**.** *Let $G = G(X, Y, E)$ be a bipartite graph. If for $\forall e = (x, y) \in E$, where $x \in X, y \in Y$, the inequality $d_G(y) \leqslant d_G(x)$ is true, then $\exists \varphi \in \alpha(G, \Delta(G))$ persistent-interval on X.*

Corollary 1 ([1, 7, 8])**.** *Let $G = G(X, Y, E)$ be a bipartite graph. If $\max_{y \in Y} d_G(y) \leqslant \min_{x \in X} d_G(x)$, then $\exists \varphi \in \alpha(G, \Delta(G))$ persistent-interval on X.*

Remark 1. Note that Corollary 1 follows from the result of [10].

Let $H = H(\mu, \nu)$ be a $(0,1)$-matrix with μ rows, ν columns, and with elements h_{ij}, $1 \leqslant i \leqslant \mu$, $1 \leqslant j \leqslant \nu$. The i-th row of H, $i \in [1, \mu]$, is called collected, iff $h_{ip} = h_{iq} = 1$, $t \in [p, q]$ imply $h_{it} = 1$, and the inequality $\sum_{j=1}^{\nu} h_{ij} \geqslant 1$ is true. Similarly, the j-th column of H, $j \in [1, \nu]$, is called collected, iff $h_{pj} = h_{qj} = 1$, $t \in [p, q]$ imply $h_{tj} = 1$, and the inequality $\sum_{i=1}^{\mu} h_{ij} \geqslant 1$ is true. If all rows and all columns of H are collected, then for i-th row of H, $i \in [1, \mu]$, we define the number $\varepsilon(i, H) \equiv \min\{j / h_{ij} = 1\}$.

H is called a collected matrix (see Figure 1), iff all its rows and all its columns are collected, $h_{11} = h_{\mu\nu} = 1$, and $\varepsilon(1, H) \leqslant \varepsilon(2, H) \leqslant \cdots \leqslant \varepsilon(\mu, H)$.

H is called a b-regular matrix ($b \in \mathbb{N}$), iff for $\forall i \in [1, \mu]$, $\sum_{j=1}^{\nu} h_{ij} = b$. H is called a c-compressed matrix ($c \in \mathbb{N}$), iff for $\forall j \in [1, \nu]$, $\sum_{i=1}^{\mu} h_{ij} \leqslant c$.

Lemma 1 ([18])**.** *If a collected n-regular ($n \in \mathbb{N}$) matrix $P = P(m, w)$ with elements p_{ij} ($1 \leqslant i \leqslant m, 1 \leqslant j \leqslant w$) is n-compressed, then $w \geqslant \lceil \frac{m}{n} \rceil \cdot n$.*

Proof. We use induction on $\lceil \frac{m}{n} \rceil$.

If $\lceil \frac{m}{n} \rceil = 1$, the statement is trivial.

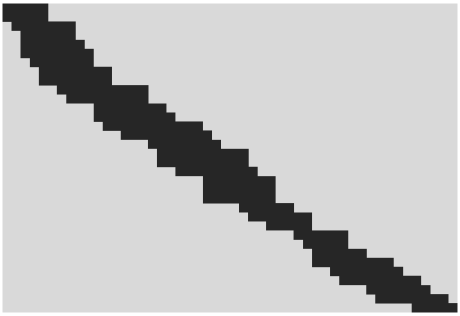

Figure 1. An example of the visual image of a collected matrix. The dark area is filled by 1s, the light area — by 0s.

Now assume that $\lceil \frac{m}{n} \rceil = \lambda_0 \geqslant 2$, and the statement is true for all collected n'-regular n'-compressed matrixes $P'(m', w')$ with $\lceil \frac{m'}{n'} \rceil \leqslant \lambda_0 - 1$.

First of all let us prove that $\varepsilon(n+1, P) \geqslant n+1$. Assume the contrary: $\varepsilon(n+1, P) \leqslant n$. Since P is a collected n-regular matrix, we obtain $\sum_{i=1}^{m} p_{in} \geqslant \sum_{i=1}^{n+1} p_{in} \geqslant n+1$, which is impossible because $P(m, w)$ is an n-compressed matrix. This contradiction shows that $\varepsilon(n+1, P) \geqslant n+1$.

Now let us form a new matrix $P'(m-n, w-(\varepsilon(n+1, P)-1))$ by deleting from the matrix P the elements p_{ij}, which satisfy at least one of the inequalities $i \leqslant n$, $j \leqslant \varepsilon(n+1, P) - 1$.

It is not difficult to see that $P'(m-n, w-(\varepsilon(n+1, P)-1))$ is a collected n-regular n-compressed matrix with $\lceil \frac{m-n}{n} \rceil = \lambda_0 - 1$. By the induction hypothesis, we have

$$w - (\varepsilon(n+1, P) - 1) \geqslant \left\lceil \frac{m-n}{n} \right\rceil \cdot n,$$

which means that

$$w \geqslant (\lambda_0 - 1)n + \varepsilon(n+1, P) - 1 \geqslant (\lambda_0 - 1)n + n = \lambda_0 n = \left\lceil \frac{m}{n} \right\rceil \cdot n. \quad \square$$

Now, for arbitrary positive integers m, l, n, k, where $m \geqslant n$ and $ml = nk$, let us define the class $Bip(m, l, n, k)$ of biregular bipartite graphs:

$$Bip(m, l, n, k) \equiv \left\{ G = G(X, Y, E) \,\middle|\, \begin{array}{l} |X| = m, |Y| = n, \\ \text{for } \forall x \in X, d_G(x) = l, \\ \text{for } \forall y \in Y, d_G(y) = k. \end{array} \right\}$$

Remark 2. Clearly, if $G \in Bip(m, l, n, k)$, then $\chi'(G) = k$.

Theorem 3. *If* $G = G(X,Y,E) \in Bip(m,l,n,k)$, *then* $w_Y(G) = k$, $w_X(G) \leqslant l \cdot \lceil \frac{m}{l} \rceil$.

Proof. The equality follows from Remark 2. Let us prove the inequality.

Let $X = \{x_1, \dots, x_m\}$. For $\forall r \in [1, \lfloor \frac{m}{l} \rfloor]$, define $X_r \equiv \{x_{(r-1)l+1}, \dots, x_{rl}\}$. Define $X_{1+\lfloor \frac{m}{l} \rfloor} \equiv X \setminus \left(\bigcup_{i=1}^{\lfloor \frac{m}{l} \rfloor} X_i \right)$. For $\forall r \in [1, \lfloor \frac{m}{l} \rfloor]$, define $Y_r \equiv \bigcup_{x \in X_r} N_G(x)$. Define $Y_{1+\lfloor \frac{m}{l} \rfloor} \equiv \bigcup_{x \in X_{1+\lfloor \frac{m}{l} \rfloor}} N_G(x)$. For $\forall r \in [1, \lceil \frac{m}{l} \rceil]$, define $G_r \equiv G[X_r \cup Y_r]$.

Consider the sequence $G_1, G_2, \dots, G_{\lceil \frac{m}{l} \rceil}$ of subgraphs of the graph G. From Corollary 1, we obtain that for $\forall i \in [1, \lceil \frac{m}{l} \rceil]$, there is $\varphi_i \in \alpha(G_i, l)$ persistent-interval on X_i.

Clearly, for $\forall e \in E(G)$, there exists the unique $\xi(e)$, satisfying the conditions $\xi(e) \in [1, \lceil \frac{m}{l} \rceil]$ and $e \in E(G_{\xi(e)})$.

Define a function $\psi : E(G) \to [1, l \cdot \lceil \frac{m}{l} \rceil]$. For an arbitrary $e \in E(G)$, set $\psi(e) \equiv (\xi(e) - 1) \cdot l + \varphi_{\xi(e)}(e)$.

It is not difficult to see that $\psi \in \alpha(G, l \cdot \lceil \frac{m}{l} \rceil)$ and ψ is interval on X. Hence, $w_X(G) \leqslant l \cdot \lceil \frac{m}{l} \rceil$. □

Theorem 4. *Let R be an arbitrary side of a bipartition of the complete bipartite graph $G = K_{m,n}$, where $m \in \mathbb{N}$, $n \in \mathbb{N}$. Then*

$$w_R(G) = (m + n - |R|) \cdot \left\lceil \frac{|R|}{m + n - |R|} \right\rceil.$$

Proof. Without loss of generality we can assume that G has a bipartition (X, Y), where $X = \{x_1, \dots, x_m\}$, $Y = \{y_1, \dots, y_n\}$, and $m \geqslant n$.

Case 1. $R = Y$. In this case the statement follows from Theorem 3; thus $w_Y(G) = m$.

Case 2. $R = X$.

The inequality $w_X(G) \leqslant n \cdot \lceil \frac{m}{n} \rceil$ follows from Theorem 3. Let us prove that $w_X(G) \geqslant n \cdot \lceil \frac{m}{n} \rceil$.

Consider an arbitrary proper edge $w_X(G)$-coloring φ of the graph G, which is interval on X.

Clearly, without loss of generality, we can assume that

$$\min(S_G(x_1, \varphi)) \leqslant \min(S_G(x_2, \varphi)) \leqslant \ldots \leqslant \min(S_G(x_m, \varphi)).$$

Let us define a $(0,1)$-matrix $P(m, w_X(G))$ with m rows, $w_X(G)$ columns, and with elements p_{ij}, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant w_X(G)$. For $\forall i \in [1, m]$, and for $\forall j \in [1, w_X(G)]$, set

$$p_{ij} = \begin{cases} 1, & \text{if } j \in S_G(x_i, \varphi) \\ 0, & \text{if } j \notin S_G(x_i, \varphi). \end{cases}$$

It is not difficult to see that $P(m, w_X(G))$ is a collected n-regular n-compressed matrix. From Lemma 1, we obtain $w_X(G) \geqslant n \cdot \lceil \frac{m}{n} \rceil$. $\square$

From Theorems 1 and 3, taking into account the proof of Case 2 of Theorem 4, we also obtain

Corollary 2. *If $G \in Bip(m, l, n, k)$, then*

1) *for $\forall t \in \left[l \cdot \lceil \frac{m}{l} \rceil, ml\right]$, there exists $\varphi_t \in \alpha(G, t)$ interval on X,*

2) *for $\forall t \in [k, nk]$, there exists $\psi_t \in \alpha(G, t)$ interval on Y.*

References

[1] A.S. Asratian, *Investigation of some mathematical model of Scheduling Theory*, Doctoral Dissertation, Moscow University, 1980 (in Russian).

[2] A.S. Asratian, C.J. Casselgren, *A sufficient condition for interval edge colorings of* $(4, 3)$*-biregular bipartite graphs*, Research report LiTH-MAT-R-2006-07, Linköping University, 2006.

[3] A.S. Asratian, C.J. Casselgren, *Some results on interval edge colorings of* (α, β)*-biregular bipartite graphs*, Research report LiTH-MAT-R-2006-09, Linköping University, 2006.

[4] A.S. Asratian, C.J. Casselgren, *On interval edge colorings of* (α, β)*-biregular bipartite graphs*, Discrete Math 307 (2007), pp.1951-1956.

[5] A.S. Asratian, C.J. Casselgren, J. Vandenbussche, D.B. West, *Proper path-factors and interval edge-coloring of* $(3, 4)$*-biregular bigraphs*, J. of Graph Theory 61 (2009), pp.88-97.

[6] A.S. Asratian, T.M.J. Denley, R. Haggkvist, *Bipartite graphs and their applications*, Cambridge Tracts in Mathematics, 131, Cambridge University Press, 1998.

[7] A.S. Asratian, R.R. Kamalian, *Interval colorings of edges of a multigraph*, Appl. Math. 5 (1987), Yerevan State University, pp.25-34 (in Russian).

[8] A.S. Asratian, R.R. Kamalian, *Investigation of interval edge-colorings of graphs*, Journal of Combinatorial Theory. Series B 62 (1994), N.**1**, pp.34-43.

[9] M.A. Axenovich, *On interval colorings of planar graphs*, Congr. Numer. 159 (2002), pp.77-94.

[10] D.P. Geller and A.J.W. Hilton, *How to color the lines of a bigraph*, Networks, 4(1974), pp.281-282.

[11] K. Giaro, *Compact task scheduling on dedicated processors with no waiting periods*, PhD thesis, Technical University of Gdansk, EIT faculty, Gdansk, 1999 (in Polish).

[12] K. Giaro, *The complexity of consecutive* Δ*-coloring of bipartite graphs:* 4 *is easy,* 5 *is hard*, Ars Combin. 47(1997), pp.287-298.

[13] K. Giaro, M. Kubale and M. Malafiejski, *On the deficiency of bipartite graphs*, Discrete Appl. Math. 94 (1999), pp.193-203.

[14] H.M. Hansen, *Scheduling with minimum waiting periods*, Master's Thesis, Odense University, Odense, Denmark, 1992 (in Danish).

[15] D. Hanson, C.O.M. Loten, B. Toft, *On interval colorings of bi-regular bipartite graphs*, Ars Combin. 50(1998), pp.23-32.

[16] T.R. Jensen, B. Toft, *Graph Coloring Problems*, Wiley Interscience Series in Discrete Mathematics and Optimization, 1995.

[17] R.R. Kamalian, *Interval Edge Colorings of Graphs*, Doctoral dissertation, the Institute of Mathematics of the Siberian Branch of the Academy of Sciences of USSR, Novosibirsk, 1990 (in Russian).

[18] R.R. Kamalian, *On one-sided interval colorings of bipartite graphs*, the Herald of the RAU, N.**2**, Yerevan, 2010, pp.3-11 (in Russian).

[19] R.R. Kamalian, *Interval colorings of complete bipartite graphs and trees*, Preprint of the Computing Centre of the Academy of Sciences of Armenia, Yerevan, 1989 (in Russian).

[20] M. Kubale, *Graph Colorings*, American Mathematical Society, 2004.

[21] P.A. Petrosyan, *Interval edge-colorings of complete graphs and n-dimensional cubes*, Discrete Math. 310 (2010), pp.1580-1587.

[22] P.A. Petrosyan, *On interval edge-colorings of multigraphs*, The Herald of the RAU, N.**1**, Yerevan, 2011, pp.12-21 (in Russian).

[23] P.A. Petrosyan, H.H. Khachatrian, *Interval non-edge-colorable bipartite graphs and multigraphs*, J. of Graph Theory 76 (2014), pp.200-216.

[24] A.V. Pyatkin, *Interval coloring of $(3,4)$-biregular bipartite graphs having large cubic subgraphs*, J. of Graph Theory 47 (2004), pp.122-128.

[25] S.V. Sevast'janov, *Interval colorability of the edges of a bipartite graph*, Metody Diskret. Analiza 50(1990), pp.61-72 (in Russian).

[26] V.G. Vizing, *The chromatic index of a multigraph*, Kibernetika 3 (1965), pp.29-39.

[27] D.B. West, *Introduction to Graph Theory*, Prentice-Hall, New Jersey, 1996.

[28] F. Yang, X. Li, *Interval coloring of $(3,4)$-biregular bigraphs having two $(2,3)$-biregular bipartite subgraphs*, Appl. Math. Letters 24(2011), pp.1574-1577.

[29] Y. Zhao and J.G. Chang, *Consecutive Edge-Colorings of Generalized θ-Graphs*, J. Akiyama et al. (Eds.): CGGA 2010, LNCS 7033, 2011, pp.214-225.

Contact information

R. R. Kamalian Institute for Informatics and Automation Problems of the National Academy of Sciences of RA, 0014 Yerevan, Republic of Armenia
E-Mail(s): rrkamalian@yahoo.com

Received by the editors: 17.12.2012
and in final form 10.02.2015.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 200–212

RESEARCH ARTICLE

On the cotypeset of torsion-free abelian groups

Fatemeh Karimi

Communicated by D. Simson

Abstract. In this paper the cotypeset of some torsion-free abelian groups of finite rank is studied. In particular, we determine the cotypeset of some rank two groups using the elements of their typesets.

Introduction

One of the important and known tools in the theory of torsion-free abelian groups is type and the typeset of a group. This set which is determined from the beginning of the the study the torsion-free groups, has allocated many papers which are about the identifying this set for torsion-free groups or applying it to determine the properties of these groups and the rings over them. Problems in this area are very diverse; for example, [3] is devoted to a determination of the representation type of indecomposables in the categories of almost completely decomposable groups, or in [6], the author is tried to construct indecomposable group with an special critical typeset, and some articles as well as [4], which are discussed about the representation of some categories of torsion-free abelian groups, are some of the works, which are done related to type. Moreover, [2], that provides perspectives on classification of almost completely decomposable groups and deals with the rank, regulator quotient and near-isomorphism types, is one of the major sources in [11], which is dealing with indecomposable $(1,2)-$groups with regulator quotient of

2010 MSC: 20K15.
Key words and phrases: typeset, cotypeset, type sequence, co-rank.

exponent $\leqslant 3$ and shows that there are precisely four near-isomorphism types of indecomposable groups. After much theorizing has been done about the type and continued more or less to the present, another concepts named "cotype" and "cotypeset" associated to the torsion-free groups. In fact, The study of cotypeset of torsion-free abelian groups begins mainly by Schultz [12]. This concept has been a focus of study between the years 1977 to 1987, and some of the works in this area are Arnold and Vinsonhaler [5], Metelli [9] and Mutzbauer[10]. In the past two decades there are only a few researches about this subject, such as Lafleur [8] in 1994. From that time better identification of cotypeset for different groups and its relation with type is considered. Moreover, always such a question is raised that: could we have some results for cotype similar to ones about the type? For example, similar results of [3], [4], [11] or [2] could be stated for cotype instead of types?

In this paper, we deal with the cotypeset of some torsion-free abelian groups of finite rank and show that the cotypeset of any completely decomposable group is closed under mutually union of its rank one direct summand's types. Moreover, we have some results about the relation between the elements of cotypeset and typeset and determine the cotypeset of some rank two groups using their typesets.

Finally, some of the other unsolved problems in this area are as follows:

(1) Identifying the cotypeset for a completely decomposable group of rank greater than 2.

(2) If $A = A_1 \oplus A_2$ is a group of rank three, with $r(A_2) = 2$, then can we obtain CT(A), (the cotypeset of A) using the cotypesets of A_1 and A_2?

(3) Is there any relation between the cardinality of the cotypeset of a torsion-free abelian group and the existance of a non-zero ring on a group?

1. Notation and Preliminaries

All groups considered in this paper are torsion-free and abelian, with addition as the group operation. Terminology and notation will mostly follow from [7]. By the typeset of a torsion-free group A we mean the partially ordered set of types, i.e.,

$$\mathrm{T(A)} = \{\mathrm{t(x)} \mid 0 \neq \mathrm{x} \in \mathrm{A}\},$$

and for two types $t_1 = [(m_i)_{i\in\mathbb{N}}]$ and $t_2 = [(k_i)_{i\in\mathbb{N}}]$ we define:

$$\inf\{t_1, t_2\} = [(\min\{m_i, k_i\})_{i\in\mathbb{N}}], \quad \sup\{t_1, t_2\} = [(\max\{m_i, k_i\})_{i\in\mathbb{N}}].$$

Moreover, if $t_2 \leqslant t_1$ then we set

$$t_1 - t_2 = [(m_i - k_i)_{i\in\mathbb{N}}].$$

We also may use the notations $t_1 \cap t_2$ and $t_1 \cup t_2$ instead of $\inf\{t_1, t_2\}$ and $\sup\{t_1, t_2\}$ respectively, for more convenience. A pure subgroup B of A is said to be of co-rank one if $rank(A/B) = 1$. The cotypeset of A, denoted by CT(A), is defined as

$$\mathrm{CT(A)} = \{\mathrm{t(A/B)} \mid \mathrm{B\ is\ a\ pure\ co\text{-}rank\ one\ subgroup\ of\ A}\}.$$

A torsion-free group A is called cohomogeneous if CT(A) has cardinality equal to one.

Let A is a torsion-free group of rank n and $S = \{x_1, x_2, \ldots, x_n\}$ a maximal independent set of A. For $X_i = \langle x_i \rangle_*$ and

$$Y_i = \langle x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n \rangle_*,$$

define the inner type of A to be

$$\mathrm{IT}(A) = \inf\{t(X_1), \ldots, t(X_n)\}.$$

Moreover, the outer type of A is as follows

$$\mathrm{OT}(A) = \sup\{t(A/Y_1), \ldots, t(A/Y_n)\}.$$

2. Cotypeset of rank two groups

As in [5], let A is a rank two group and $A_1, A_2, \cdots$ be an indexing of the pure rank one subgroups of A with $t_i = t(A_i)$, $\sigma_i = t(A/A_i)$ for each i. Define $T_A = (t_1, t_2, \cdots), CT_A = (\sigma_1, \sigma_2, \cdots)$ are two countable infinite sequences of types (repetition of types is allowed). We say two type sequences T and T' are equivalent, $T \approx T'$, if one is a permutation of the other, and by this, T_A and CT_A are unique up to equivalence.

Proposition 1. *Let A be a rank 2 group with $T_A = (t_1, t_2, \cdots)$ and $CT_A = (\sigma_1, \sigma_2, \cdots)$.*

(1) *There is a type t_0 such that $t_0 = inf\{t_i, t_j\}$ for each $i \neq j$ and if $T(A)$ is finite then $t_0 = t_i$ for some $i \geqslant 1$.*

(2) *There is a type σ_0 such that $\sigma_0 = sup\{\sigma_i, \sigma_j\}$ for each $i \neq j$ and if $CT(A)$ is finite then $\sigma_0 = \sigma_i$ for some $i \geqslant 1$.*

(3) *$t_i \leqslant \sigma_j$ for each $i \neq j$ and $t_0 \leqslant \sigma_0$.*

(4) *$\sigma_i - t_j = \sigma_j - t_i$ for each $i \neq j$ with $i \geqslant 0$ and $j \geqslant 0$.*

(5) *If $t_0 = t(\mathbb{Z})$ then $\sigma_i = \sigma_0 - t_i$ for each i.*

Proof. See ([5], Proposition 1.1). □

Using above Proposition and nothing the known fact from [13], which the typeset of any non-nil rank two torsion-free group has the cardinality at most three, it would be straight forward too check:

Proposition 2. *The cotypeset of a non-nil rank two torsion-free group A has one of this forms:*

(1) *If* $\mathrm{T(A)} = \{\mathrm{t}\}$ *and B is a pure subgroup of A with $t(B) = t$, then* $\mathrm{CT(A)} = \{\mathrm{t(A/B)}\}$.

(2) *If* $\mathrm{T(A)} = \{\mathrm{t_1, t_2}\}$ *with $t_1 < t_2$ and A_1 is a pure subgroup of A such that $t(A_1) = t_1$, then* $\mathrm{CT(A)} = \{\sigma_1, \sigma_2\}$ *such that $\sigma_1 = t(A/A_1), \sigma_2 = \sigma_1 - t_2 + t_1$.*

(3) *If* $\mathrm{T(A)} = \{\mathrm{t_0, t_1, t_2}\}$ *with $t_0 < t_1, t_2$ and A_1, A_2, A_3 are rank one pure subgroups of A in which $t(A_1) = t_1, t(A_2) = t_2, t(A_3) = t_3$, then* $\mathrm{CT(A)} = \{\sigma_1, \sigma_2, \sigma_3\}$ *such that $\sigma_3 = t(A/A_3), \sigma_1 = \sigma_3 + t_0 - t_1, \sigma_2 = \sigma_3 + t_0 - t_2$.*

Moreover, we could easily show that:

Corollary 1. *If A is a non-nil rank two group which is completely decomposable, then we have:*

(1) *If* $|\mathrm{T(A)}| = 1$ *or* 2, *then* $\mathrm{T(A)} = \mathrm{CT(A)}$.

(2) *If* $\mathrm{T(A)} = \{\mathrm{t_1, t_2, t_1 \cap t_2}\}$, *then* $\mathrm{CT(A)} = \{\mathrm{t_1, t_2, t_1 \cup t_2}\}$.

Lemma 1. *Let $T = (t_1, t_2, \cdots)$ and $C = (\sigma_1, \sigma_2, \cdots)$ be type sequences with $t_0 = inf\{t_i, t_j\}$ and $\sigma_0 = sup\{\sigma_i, \sigma_j\}$ whenever $i \neq j$. There is a rank two group A with $T_A = T$ and $CT_A = C$ if and only if there is a rank two group B with $T_B = (t_1 - t_0, t_2 - t_0, \cdots)$, $CT_B = (\sigma_1 - t_0, \sigma_2 - t_0, \cdots)$, $IT(B) = t(\mathbb{Z})$, $OT(B) = \sigma_0 - t_0$.*

Proof. See ([5], Lemma 1.3). □

Proposition 3. *Let $S = \{t_i \mid i \geqslant 1\}$ be a set of types with $t_0 = inf\{t_i, t_j\}$ whenever $i \neq j$. If there exists characteristic $h_i \in t_i$ for $i \geqslant 0$ with $h_0 = inf\{h_i, h_j\}$ for each $i \neq j$ then there exists a rank two group A with $T(A) = S$ and $OT(A) = [sup\{h_i \mid i \geqslant 1\}]$.*

Proof. See ([5], Corollary 2.14). □

Theorem 1. *Let $S = \{t_1, t_2, \cdots\}$ be a set of types with $t_0 = inf\{t_i, t_j\}$ for each $i \neq j$ and $t_0 \in S$ if S is finite. Then*

(1) *There exists $s_i \in t_i$ for $i \geqslant 0$ such that $s_0 = min\{s_i, s_j\}$ for $i \neq j$.*

(2) *There exists a rank two group A with $T(A) = S, IT(A) = t_0$, $OT(A) = [sup\{s_i \mid i \geqslant 1\}]$ and $CT(A) = \{OT(A) - (t_i - t_0) \mid i \geqslant 1\}$.*

Proof. (1) Let $n \geqslant 3$ be an arbitrary integer and let $s_i \in t_i$ for $0 \leqslant i \leqslant n-1$ with $s_0 = \min\{s_i, s_j\}$ for $1 \leqslant i \neq j \leqslant n-1$. Now choose $s_n \in t_n$ such that $s_0 = \min\{s_i, s_n\}$ for $1 \leqslant i \leqslant n-1$.

(2) By (1) and Proposition 3, let $\chi'_0 = \sup\{s_i \mid i \geqslant 1\}$, $\sigma'_0 = [\chi'_0]$ and $\gamma_i = \sigma'_0 - t_i$ for $i \geqslant 0$. Note that $\gamma_i = [\chi'_0 - s_i]$ for each $i \geqslant 0$. Now $\Gamma = \{\gamma_1, \gamma_2, \cdots\}$ with $\gamma_0 = \sup\{\gamma_i, \gamma_j\}$ if $i \neq j$, because $t_0 = \inf\{t_i, t_j\}$ hence $\sigma'_0 - t_0 = \sup\{\sigma'_0 - t_i, \sigma'_0 - t_j\}$. Moreover, $\gamma_0 \in \Gamma$ if Γ is finite. In fact if Γ is finite then S must be finite. This means $t_0 \in S$ which yields $t_0 = t_j$ for some $t_j \in S$. Now we have $\gamma_0 = \sigma'_0 - t_0 = \sigma'_0 - t_j = \gamma_j$, for some $\gamma_j \in \Gamma$. Define $\sigma_i = \gamma_0 - \gamma_i$ for $i \geqslant 0$. The next step is to show that there exists a rank two group B with $T(B) = \{\sigma_i \mid i \geqslant 1\}$ and $CT(B) = \{\gamma_i \mid i \geqslant 1\}$. For each $i \geqslant 1$, let $\chi_i = (\chi'_0 - s_0) - (\chi'_0 - s_i) \in \sigma_i = \gamma_0 - \gamma_i$. Note that

1) If $\chi_i(p)$, the $p-$component of χ_i, is equal to ∞, for some $i \geqslant 1$, then $s_i(p) = \infty, \quad s_0(p) < \infty$ and $\chi'_0(p) = \infty$.

2) $\chi_i(p) = s_i(p) - s_0(p)$.

3) $\min\{\chi_i, \chi_j\} = (0, 0, \cdots)$ whenever $i \neq j$. This is a consequence of 2) and the fact that $s_0 = \min\{s_i, s_j\}$.

By 3) and Proposition 3, there exists a rank two group B with $T(B) = \{\sigma_i \mid i \geqslant 1\}, \mathrm{OT}(B) = [\sup\{\chi_i \mid i \geqslant 1\}]$. Moreover, from 3) we deduce that $\mathrm{IT}(B) = t(\mathbb{Z})$. Now 2) implies

$$\begin{aligned}\sup\{\chi_i \mid i \geqslant 1\} &= \sup\{s_i - s_0 \mid i \geqslant 1\}\\ &= \sup\{s_i \mid i \geqslant 1\} - s_0\\ &= \chi'_0 - s_0,\end{aligned}$$

therefore $\mathrm{OT}(B) = \gamma_0$. Now by Proposition 1 (5), we deduce

$$CT(B) = \{\gamma_0 - \sigma_i \mid i \geqslant 1\} = \{\gamma_i \mid i \geqslant 1\}.$$

The last equality holds because of 3). In fact:

$$\gamma_0 - \sigma_i = [(\chi'_0 - s_0) - (s_i - s_0)] = [\chi'_0 - s_i] = \gamma_i.$$

Consequently, in view of Lemma 1, there exists a rank two group A with

$$\begin{aligned} T(A) &= \{\sigma_i + t_0 \mid i \geqslant 1\} = \{t_i \mid i \geqslant 1\}, \quad \mathrm{IT}(A) = t_0, \\ CT(A) &= \{\gamma_i + t_0 \mid i \geqslant 1\} = \{\sigma'_0 - t_i + t_0 \mid i \geqslant 1\}, \\ \mathrm{OT}(A) &= \mathrm{OT}(B) + t_0 = \gamma_0 + t_0 = \sigma'_0. \end{aligned}$$ □

3. Cotypeset of finite rank groups

We begin this section with an example of a cohomogeneous group of any arbitrary finite rank that is homogeneous too. First we need the following definition and two propositions:

Definition 1. A torsion-free group A is called coseparable if, given any pure subgroup B of A such that A/B reduced of finite rank, B contains a summand C of A which has a completely decomposable finite rank complement. Moreover, a torsion-free group A is finitely cohesive exactly if for every pure finite corank subgroup B of A, A/B is divisible.

Proposition 4. *A finite rank group is coseparable exactly if it is completely decomposable.*

Proof. See ([9], Proposition 1.2). □

Remark 1. By above definition, a finitely cohesive group A is cohomogeneous with

$$\mathrm{CT(A)} = \{(\infty, \infty, \cdots)\}.$$

Proposition 5. *Finitely cohesive groups are coseparable.*

Proof. See ([9], Proposition 1.5). □

Example 1. Let A be a finitely cohesive group of finite rank. Then by Proposition 5, A is coseparable and so completely decomposable group by Proposition 4. This yields $\mathrm{T(A)} = \{(\infty, \infty, \cdots)\}$ and so A is a homogeneous group.

Now we present the main results of this section.

Theorem 2. *Let A is a torsion-free group of finite rank n, A set $\{x_1, x_2, \cdots, x_n\}$ a maximal independent set of A and $A_1, A_2, \cdots$ is an indexing of the rank one pure subgroups of A. Define*

$$U_A = \{m_1x_1 + \cdots + m_nx_n \mid m_1, m_2, \cdots, m_n \in \mathbb{Z}, (m_1, m_2, \cdots, m_n) = 1\}$$

which is a subset of $\bigoplus_{i=1}^n \mathbb{Z}x_i \subseteq A$. Then

(1) *For each $i \geqslant 1$ there exists a unique $a_i \in U_A \bigcap A_i$. Moreover,*

$$A_i \bigcap (\bigoplus_{i=1}^{n} \mathbb{Z}x_i) = \mathbb{Z}(a_i), \quad t(a_i) = t(A_i).$$

(2) *$OT(A) = [sup\{\chi_A(a) \mid a \in U_A\}]$.*

Proof. (1) Let a_i' be a non-zero element of A_i with $t(a_i') = t_i = t(A_i)$. Then $A_i = \langle a_i' \rangle_*$ and $A_i \bigcap U_A \neq 0$. Now for all $i \geqslant n$, let $k, k_{i1}, k_{i2}, \cdots, k_{in}$ be some integers such that

$$0 \neq ka_i' = \sum_{j=1}^{n} k_{ij}x_j.$$

Suppose $(k_{i1}, k_{i2}, \cdots, k_{in}) = l$; if $l = 1$ then ka_i' has the stated properties in (1). If $l \neq 1 \in \mathbb{Z}$ then we could write $k_{ij} = lk_{ij}', (j = 1, 2, \cdots, n)$ and $ka_i' = l(\sum_{j=1}^n k_{ij}'x_j)$. Now by letting $a_i = \sum_{j=1}^n k_{ij}'x_j$ we obtain $a_i \in U_A \bigcap A_i$. To show that a_i is unique, let $a_i'' \in U_A \bigcap A_i$, then from $a_i, a_i'' \in A_i$, there exist some integers m, n such that $(n, m) = 1$ and $ma_i'' = na_i$. Now using the fact that $a_i'', a_i \in U_A$ we conclude the result and the other parts of (1) are easy to proof.

(2) We write

$$(A/\bigoplus_{i=1}^{n} \mathbb{Z}x_i) = \bigoplus_{p} [\mathbb{Z}(p^{i_{1p}}) \oplus \cdots \oplus \mathbb{Z}(p^{i_{np}})]$$

such that $0 \leqslant i_{1p} \leqslant \cdots \leqslant i_{np} \leqslant \infty$ for each p. Then $\mathrm{IT}(A) = [(i_{1p})]$ and $\mathrm{OT}(A) = [(i_{np})]$, (See [14]). If $a + (\bigoplus_{i=1}^n \mathbb{Z}x_i)$ is an element of the $p-$component of $A/\bigoplus_{i=1}^n \mathbb{Z}x_i$, then the order of $a + (\bigoplus_{i=1}^n \mathbb{Z}x_i)$ is the least j such that $p^j a = mu$ for some $u \in U_A$ and $m \in \mathbb{Z}$ with $(m, p) = 1$. Since i_{np} is the maximum of such j, in view of $j \leqslant h_p^A(u)$, we have

$$i_{np} \leqslant \sup\{h_p^A(a) \mid a \in U_A\}.$$

But

$$\frac{A}{\bigoplus_{i=1}^{n} \mathbb{Z}x_i} \supseteq \frac{A_i + (\bigoplus_{i=1}^{n} \mathbb{Z}x_i)}{\bigoplus_{i=1}^{n} \mathbb{Z}x_i} \cong \frac{A_i}{\mathbb{Z}a_i} = \bigoplus_{p} \mathbb{Z}(p^{l_p}),$$

such that $i_{np} \geqslant l_p = h_p^A(a_i)$. This means $\sup\{h_p^A(a) \mid a \in U_A\} \leqslant i_{np}$ and therefore

$$\mathrm{OT}(A) = [(i_{np})] = [\sup\{\chi_A(a) \mid a \in U_A\}]. \qquad \square$$

Theorem 3. *Let A is a torsion-free group of finite rank n and A_1, $A_2, \cdots, A_n$ are rank one subgroups such that $\{x_i | x_i \in A_i\}_{i=1}^{n}$ is an independent set of A. If $\sigma_i = t\left(\frac{A}{\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}\right)$ and $t(A_i) = t_i$, then $\sigma_i - t_i = \sigma_j - t_j$ for all $i \neq j \in \{1, 2, \cdots, n\}$.*

Proof. There is an exact sequence

$$0 \longrightarrow A_i \longrightarrow \frac{A}{\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*} \longrightarrow \frac{A}{\bigoplus_{j=1}^{n} A_j} \longrightarrow 0$$

for all $i = 1, 2, \cdots, n$. Choose $a_i \in A_i$ and $y_i \in \frac{A}{\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}$ with $a_i \longmapsto y_i$. Then

$$0 \longrightarrow \frac{A_i}{\mathbb{Z}a_i} \longrightarrow \frac{A/\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}{\mathbb{Z}y_i} \longrightarrow \frac{A}{\bigoplus_{j=1}^{n} A_j} \longrightarrow 0 \qquad (*)$$

is exact. Now since $A/\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*$ is a rank one torsion-free group, $\frac{A/\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}{\mathbb{Z}y_i}$ is torsion, so we have

$$\frac{A}{\bigoplus_{j=1}^{n} A_j} \cong \bigoplus_{p} \mathbb{Z}(p^{k_p}), \quad \frac{A_i}{\mathbb{Z}a_i} \cong \bigoplus_{p} \mathbb{Z}(p^{l_p})$$

and

$$\frac{A/\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}{\mathbb{Z}y_i} \cong \bigoplus_{p} \mathbb{Z}(p^{n_p}).$$

On the other hand the exactness of $(*)$ implies that

$$\bigoplus_{p} \mathbb{Z}(p^{k_p}) \cong \frac{\bigoplus_p \mathbb{Z}(p^{n_p})}{\bigoplus_p \mathbb{Z}(p^{l_p})},$$

hence $k_p = n_p - l_p$. Moreover,

$$n_p = h_p^{A/\langle \bigoplus_{i\neq j=1}^{n} A_j\rangle_*}(y_i) - h_p^{\mathbb{Z}y_i}(y_i), \quad l_p = h_p^{A_i}(a_i) - h_p^{\mathbb{Z}a_i}(a_i)$$

and $h_p^{\mathbb{Z}y_i}(y_i) = 0 = h_p^{\mathbb{Z}a_i}(a_i)$. Therefore

$$k_p = h_p^{A/\langle\bigoplus_{i\neq j=1}^{n} A_j\rangle_*}(y_i) - h_p^{A_i}(a_i),$$

which means $[(k_p)] = \sigma_i - t_i$. Similarly $[(k_p)] = \sigma_j - t_j$ and this completes the proof. $\square$

Proposition 6. *In any torsion-free abelian group of finite rank A with finite typeset, the intersection type and inner type coincide and this type is realized. This means there exists a rank one subgroup B of A such that* $\mathrm{IT(A)} = \mathrm{t(B)}$.

Proof. See ([10], Corollary 1.3). $\square$

Proposition 7. *Let A is a group of rank two and X, Y be different pure rational subgroups of A. Then*

$$t(A/X) - t(Y) = t(A/Y) - t(X).$$

Moreover, the outer type is realized if the inner type is realized; more precisely if $t(B) = \mathrm{IT(A)}$ for some subgroup B of A then $t(A/B) = \mathrm{OT(A)}$.

Proof. See ([10], Lemma 2.4). $\square$

Theorem 4. *Let A is a group such that any rank two torsion-free quotient of A is non-nil. Then* $\mathrm{CT(A)}$ *is closed under the union of its elements.*

Proof. Let $s, t \in \mathrm{CT(A)}$ be two arbitrary elements. Then there exist pure subgroups B, C of A such that A/B and A/C are of rank one and $t(A/B) = s, t(A/C) = t$. Now $D = \frac{A}{B\cap C}$ is a torsion-free group of rank two and $\frac{B}{B\cap C}, \frac{C}{B\cap C}$ are two co-rank one pure subgroups of D such that

$$t\left(\frac{D}{B/B\cap C}\right) = s, \qquad t\left(\frac{D}{C/B\cap C}\right) = t.$$

Hence $s, t \in \mathrm{CT(D)}$. Moreover, our assumption implies that $\mathrm{CT(D)} \subseteq \mathrm{CT(A)}$. Now it is sufficient to prove $s \cup t \in \mathrm{CT(D)}$. By Proposition 6 the inner type of D is realized in $\mathrm{T(D)}$, because $\mathrm{T(D)}$ is finite, so there is a pure subgroup Y of D with $r(Y) = 1, \mathrm{IT(D)} = \mathrm{t(Y)}$. Now by Proposition 7 we have $t(D/Y) = \mathrm{OT(D)} = \mathrm{s} \cup \mathrm{t} \in \mathrm{CT(D)}$ and this completes the proof. $\square$

Theorem 5. *Let $A = A_1 \oplus A_2$ be a group of rank three with A_2 a non-nil group of rank two. Then*

$$\mathrm{CT(A)} \supseteq \{\mathrm{t(A_1)}\} \cup \mathrm{CT(A_2)}$$

and $\mathrm{T(A)}$ *contains at most three maximal elements.*

Proof. The first part is obtained from the fact that for any pure co-rank one subgroup B of A_2, $A_1 \oplus B$ is a pure co-rank one subgroup of A such that

$$\frac{A}{A_1 \oplus B} \cong \frac{A_2}{B}.$$

Moreover,

$$\mathrm{T(A)} = \{\mathrm{t(A_1)}\} \cup \mathrm{T(A_2)} \cup \{\mathrm{t(A_1)} \cap \mathrm{t} \mid \mathrm{t} \in \mathrm{T(A_2)}\}.$$

But $\mathrm{T(A_2)}$ has at most two maximal elements since A_2 is a non-nil rank two group. □

Remark 2. At the proof of above theorem, if Y is any pure fully invariant subgroup of A with $r(A/Y) = 1$ and $Y \neq A_2$, then $Y \cap A_2 \neq 0$ and $Y \cap A_1 = A_1$. In fact if $Y \cap A_1 \neq A_1$,

$$\frac{A}{Y} = \frac{A_1 \oplus A_2}{(Y \cap A_1) \oplus (Y \cap A_2)}$$

is not a torsion-free group, (because $A_1/(Y \cap A_1)$ is torsion) which yields a contradiction.

Now $0 \neq Y \cap A_2$ is a pure subgroup of rank one of A_2. Let $pa_2 = y$ for some $a_2 \in A_2, y \in Y \cap A_2$ and a prime number p, then there exist an element $a \in Y$ such that $a = a_1 + a_2'$ for some $a_1 \in A_1$ and $a_2' \in A_2$ in which $pa_2 = y = pa = pa_1 + pa_2'$, because Y is a pure subgroup of A, but this yields $a_2 = a_2'$ and $a_1 = 0$. Therefore $a_2' \in Y \cap A_2$ and this completes this part of proof. So we have $Y = A_1 \oplus (Y \cap A_2)$ and $Y \cap A_2$ is a co-rank one pure subgroup of A_2.

But if Y is not a fully invariant subgroup, similar result couldn't be true.

Theorem 6. *Let $X = \bigoplus_{i=1}^{n} X_i$ is a completely decomposable group of rank n and B a torsion-free group with finite rank greater than one. If $A = X \otimes B$ and $B_i = X_i \otimes B$, then*

$$\mathrm{CT(A)} \supseteq \bigcup_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{CT(B_i)}$$

and $\mathrm{T(A)}$ *is equal to*

$$\bigcup_{i=1}^{n} \mathrm{T(B_i)} \bigcup \{\cap_{\mathrm{i \in I}} \mathrm{t_i} |\ \mathrm{I\ is\ a\ finite\ subset\ of} \{1, 2, \cdots, \mathrm{n}\}, \mathrm{t_i} \in \mathrm{T(B_i)}\}.$$

Proof. Let C_i is a pure rank (co-rank) one subgroup of B_i, then

$$C_i(\bigoplus_{i \neq j=1}^{n} B_j \bigoplus C_i)$$

is a pure rank (co-rank) one subgroup of A. Moreover,

$$\frac{A}{(\bigoplus_{i \neq j=1}^{n} B_j) \bigoplus C_i} \cong \frac{B_i}{C_i}$$

which yields the result. □

Theorem 7. *If $A = \bigoplus_{i=1}^{n} B_i$ with $r(B_i) \geqslant 2$, then the typeset of A is equal to*

$$\bigcup_{i=1}^{n} \mathrm{T(B_i)} \bigcup \{\cap_{\mathrm{i \in I}} \mathrm{t_i} \mid \mathrm{I\ is\ a\ finite\ subset\ of}\ \{1, 2, \cdots, \mathrm{n}\}, \mathrm{t_i} \in \mathrm{T(B_i)}\}$$

and

$$\mathrm{CT(A)} \supseteq \bigcup_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{CT(B_i)}.$$

Proof. Obvious. □

In this part we have some results about the cotypeset of completely decomposable groups.

Lemma 2. *Let A be a torsion-free group and $H \leqslant A$ then*

$$CT(A/H) \subseteq CT(A).$$

Proof. Obvious. □

Theorem 8. *Let $A = \bigoplus_{i \in I} A_i$ is a torsion-free group with $r(A_i) = 1$ and $t(A_i) = t_i$. Then the cotypeset of A is closed under mutually union of $t(A_i)$s. Moreover, if $t_i = t(A_i)$ and $t_j = t(A_j)$ are two incomparable types, then $(t_i \cup t_j) - t_k = t_k - (t_i \cap t_j)$ for $k = i, j$.*

Proof. We know $A/(\oplus_{(j\neq)i\in I} A_i) \cong A_j$, hence $t_j \in CT(A)$ for all $j \in I$. Now let t_i, t_j be two incomparable types and let $A' = A_i \oplus A_j$. Then A' is a pure subgroup of A and from $T(A') = \{t_i, t_j, t_i \cap t_j\} \subseteq T(A)$ and Proposition 1, we deduce that $CT(A') = \{t_i, t_j, t_i \cup t_j\}$. Let $t_i \cup t_j = t(A'/H)$ for some co-rank one subgroup H of A'. Now

$$\frac{A' \oplus (\bigoplus_{(i,j\neq)k\in I} A_k)}{H \oplus (\bigoplus_{(i,j\neq)k\in I} A_k)}$$

is a rank one torsion-free quotient of A. We let $G = H \oplus (\bigoplus_{(i,j\neq)k\in I} A_k)$, hence $A/G \cong A'/H$ which yields $t(A/G) = t(A'/H) = t_i \cup t_j \in CT(A)$. Moreover, by assuming $A' = A_i \oplus A_j$ we have $\mathrm{OT}(A') = t_i \cup t_j$ and $\mathrm{IT}(A') = t_i \cap t_j$. Now the result follows from Prposition 1(4) and the fact that $\mathrm{OT}(A') \in CT(A)$ and $\mathrm{IT}(A') \in T(A)$. $\square$

References

[1] A.M. Aghdam and A. Najafizadeh,*On torsion free rings with indecomposable additive group of rank two,* Southeast Asian Bull. Math., **32**, No. 2, 2008, 199-208.

[2] D.M. Arnold, *Abelian Groups and Representations of Partially Ordered Sets,* CMS Adv. Books Math., Springer-Verlag, New York, 2000.

[3] D. M. Arnold and M. Dugas, *Representation type of finite rank almost completely decomposable groups,* Forum Math., **10**, 1998, 729-749.

[4] D. M. Arnold and D. Simson, *Representations of Finite Posets Over Discrete Valuation Rings,* Comm. Algebra, **35**, Issue 10, 2007, 3128-3144.

[5] D.M. Arnold, C. Vinsonhaler,*The typesets and cotypesets rank two torsion-free abelian groups,* Pacific J. Math., **114**, No. 1, 1984, 1-21.

[6] M. Dugas, *BCD-groups with type set (1,2),* Forum Mathematicum., **13**, 2000, 143-148.

[7] L. Fuchs, *Infinite abelian groups,* Vol. **2**, Academic Press, New York - London, 1973.

[8] R. S. Lafleur, *Typesets and cotypesets of finite-rank torsion-free abelian groups,* Contemp. Math., **171**, Amer. Math. Soc., Providence, RI, 1994, 243-256.

[9] C. Metelli, *Coseparable torsion-free groups,* Arch. Math., **45**, 1985, 116-124.

[10] O. Mutzbauer, *Type invariants of torsion-free abelian groups,* Abelian Group Theory Proc. Perth, 1987, 133-153.

[11] O. Mutzbauer and E. Solak, $(1,2)-$*Groups with p^3-regulator quotient,* J. Algebra, **320**, 2008, 3821-3831.

[12] P. Schultz, *The type-set and cotype-set of a rank two abelian group,* Pacific J. Math., **78**, 1978, 503-517.

[13] A.E. Stratton, *The type-set of torsion-free rings of finite rank,* Comment. Math. Univ. Sancti Pauli, **27**, 1978, 199-211.

[14] R. Warfield, Jr., *Homomorphisms and duality of torsion-free groups,* J. Algebra, **83** No. 2, 1983, 380-386.

CONTACT INFORMATION

Fatemeh Karimi
Department of Mathematics,
Payame Noor University, PO BOX 19395-3697,
Tehran, I.R. of IRAN
E-Mail(s): karimi@pnu.ac.ir

Received by the editors: 08.07.2012
and in final form 09.06.2014.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 213–228

RESEARCH ARTICLE

Recursive formulas generating power moments of multi-dimensional Kloosterman sums and m-multiple power moments of Kloosterman sums*

Dae San Kim

Communicated by V. V. Kirichenko

Abstract. In this paper, we construct two binary linear codes associated with multi-dimensional and $m-$multiple power Kloosterman sums (for any fixed m) over the finite field $\mathbb{F}_q$. Here q is a power of two. The former codes are dual to a subcode of the binary hyper-Kloosterman code. Then we obtain two recursive formulas for the power moments of multi-dimensional Kloosterman sums and for the m-multiple power moments of Kloosterman sums in terms of the frequencies of weights in the respective codes. This is done via Pless power moment identity and yields, in the case of power moments of multi-dimensional Kloosterman sums, much simpler recursive formulas than those associated with finite special linear groups obtained previously.

1. Introduction and Notations

Let ψ be a nontrivial additive character of the finite field $\mathbb{F}_q$ with $q = p^r$ elements (p a prime), and let m be a positive integer. Then the

*This work was supported by National Research Foundation of Korea Grant funded by the Korean Government 2009-0072514.
2010 MSC: 11T23, 20G40, 94B05.
Key words and phrases: Index terms-recursive formula, multi-dimensional Kloosterman sum, Kloosterman sum, Pless power moment identity, weight distribution.

m-dimensional Kloosterman sum $K_m(\psi; a)$([10]) is defined by

$$K_m(\psi; a) = \sum_{\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*} \psi(\alpha_1 + \cdots + \alpha_m + a\alpha_1^{-1} \cdots \alpha_m^{-1}) \ (a \in \mathbb{F}_q^*).$$

For this, we have the Deligne bound

$$|K_m(\psi; a)| \leqslant (m+1)q^{\frac{m}{2}}. \tag{1.1}$$

In particular, if $m = 1$, then $K_1(\psi; a)$ is simply denoted by $K(\psi; a)$, and is called the Kloosterman sum. The Kloosterman sum was introduced in 1926 [8] to give an estimate for the Fourier coefficients of modular forms. It has also been studied to solve various problems in coding theory and cryptography over finite fields of characteristic two.

For each nonnegative integer h, we denote by $MK_m(\psi)^h$ the h-th moment of the m-dimensional Kloosterman sum $K_m(\psi; a)$, i.e.,

$$MK_m(\psi)^h = \sum_{a \in \mathbb{F}_q^*} K_m(\psi; a)^h.$$

If $\psi = \lambda$ is the canonical additive character of $\mathbb{F}_q$, then $MK_m(\lambda)^h$ will be simply denoted by MK_m^h. If futher $m = 1$, for brevity MK_1^h will be indicated by MK^h. The power moments of Kloosterman sums can be used, for example, to give an estimate for the Kloosterman sums.

Explicit computations on power moments of Kloosterman sums were initiated in the paper [17] of Salié in 1931, where it is shown that for any odd prime q,

$$MK^h = q^2 M_{h-1} - (q-1)^{h-1} + 2(-1)^{h-1} \quad (h \geqslant 1).$$

Here $M_0 = 0$, and, for $h \in \mathbb{Z}_{>0}$,

$$M_h = |\{(\alpha_1, \cdots, \alpha_h) \in (\mathbb{F}_q^*)^h | \sum_{j=1}^{h} \alpha_i = 1 = \sum_{j=1}^{h} \alpha_i^{-1}\}|.$$

For $q = p$ an odd prime, Salié obtained MK^1, MK^2, MK^3, MK^4 in that same paper by determining M_1, M_2, M_3. On the other hand, MK^5 can be expressed in terms of the p-th eigenvalue for a weight 3 newform on $\Gamma_0(15)$ (cf. [11], [16]). MK^6 can be expressed in terms of the p-th eigenvalue for a weight 4 newform on $\Gamma_0(6)$ (cf.[4]). Also, based on numerical evidence, in [3] Evans was led to propose a conjecture which expresses MK^7 in terms of Hecke eigenvalues for a weight 3 newform on $\Gamma_0(525)$ with quartic nebentypus of conductor 105.

From now on, let us assume that $q = 2^r$. Carlitz [1] evaluated MK^h for $h \leqslant 4$. Recently, Moisio was able to find explicit expressions of MK^h, for $h \leqslant 10$ (cf. [13]). This was done, via Pless power moment identity, by connecting moments of Kloosterman sums and the frequencies of weights in the binary Zetterberg code of length $q+1$, which were known by the work of Schoof and Vlugt in [18].

Also, Moisio considered binary hyper-Kloosterman codes $C(r, m)$ and determined the weight distributions of $C(r, m)$ and $C^\perp(r, m)$, for $r = 2$ and all $m \geqslant 2$, and for all $r \geqslant 2$ and $m = 3$ (cf. [14]). In [15], these results were further extended to the case of $r = 3, 4$ and all $m \geqslant 2$.

In this paper, we construct two binary linear codes C_{n-1} and D_m, respectively connected with multi-dimensional and m-multiple power Kloosterman sums (for any fixed m) over the finite field $\mathbb{F}_q$. Here q is a power of two. The code $C_{n-1}^\perp$ is a subcode of the hyper-Kloosterman code $C(r, n)$, which is mentioned above. Then we obtain two recursive formulas for the power moments of multi-dimensional Kloosterman sums and the m-multiple power moments of Kloosterman sums in terms of the frequencies of weights in the respective codes. This is done via Pless power moment identity and yields, in the case of power moments of multi-dimensional Kloosterman sums, much simpler recursive formulas than those obtained previously in [5]. As for the case of q a power of three, in [6] two infinite families of ternary linear codes associated with double cosets in the symplectic group $Sp(2n, q)$ were constructed in order to generate infinite families of recursive formulas for the power moments of Kloosterman sums with square arguments and for the even power moments of those in terms of the frequencies of weights in those codes.

Theorem 1.1. (1) *Let $n = 2^s$, $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$\begin{aligned} MK_{n-1}^h = &\sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{(n-1)(h-l)} MK_{n-1}^l \\ &+ q \sum_{j=0}^{\min\{(q-1)^{n-1},\ h\}} (-1)^{h+j} C_{n-1,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^{n-1} - j}{(q-1)^{n-1} - t}. \end{aligned} \tag{1.2}$$

Here $S(h, t)$ indicates the Stirling number of the second kind given by

$$S(h,t) = \frac{1}{t!} \sum_{j=0}^{t} (-1)^{t-j} \binom{t}{j} j^h. \tag{1.3}$$

In addition, $\{C_{n-1,j}\}_{j=0}^{(q-1)^{n-1}}$ *denotes the weight distribution of the binary linear code* C_{n-1}*, given by*

$$C_{n-1,j} = \sum \prod_{\beta\in\mathbb{F}_q} \binom{\delta(n-1,q;\beta)}{\nu_\beta}, \tag{1.4}$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q} (0 \leqslant \nu_\beta \leqslant \delta(n-1,q;\beta))$ *satisfying*

$$\sum_{\beta\in\mathbb{F}_q} \nu_\beta = j, \qquad \sum_{\beta\in\mathbb{F}_q} \nu_\beta \beta = 0 \tag{1.5}$$

and
$$\begin{aligned}\delta(n-1,q;\beta) &= |\{(\alpha_1,\cdots,\alpha_{n-1}) \in (\mathbb{F}_q^*)^{n-1}| \\ &\qquad\qquad \alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1}=\beta\}| \\ &= \begin{cases} q^{-1}\{(q-1)^{n-1}+1\}, & \text{if } \beta = 0, \\ K_{n-2}(\lambda;\beta^{-1}) + q^{-1}\{(q-1)^{n-1}+1\}, & \text{if } \beta \in \mathbb{F}_q^*. \end{cases}\end{aligned}$$

Here we understand that $K_0(\lambda;\beta^{-1}) = \lambda(\beta^{-1})$.

(2) *Let* $q = 2^r$. *For* $r \geqslant 3$, *and* $m, h = 1, 2, \cdots,$

$$\begin{aligned} MK^{mh} &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{m(h-l)} MK^{ml} \\ &+ q \sum_{j=0}^{\min\{(q-1)^m,h\}} (-1)^{h+j} D_{m,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^m - j}{(q-1)^m - t}. \end{aligned} \tag{1.6}$$

Here $\{D_{m,j}\}_{j=0}^{(q-1)^m}$ *is the weight distribution of the binary linear code* D_m*, given by*

$$D_{m,j} = \sum \prod_{\beta\in\mathbb{F}_q} \binom{\sigma(m,q;\beta)}{\nu_\beta}, \tag{1.7}$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q} (0 \leqslant \nu_\beta \leqslant \sigma(m,q;\beta))$ *satisfying (1.5), and*

$$\begin{aligned} \sigma(m,q;\beta) &= |\{(\alpha_1,\cdots,\alpha_m) \in (\mathbb{F}_q^*)^m| \\ &\qquad\qquad \alpha_1+\cdots+\alpha_m+\alpha_1^{-1}+\cdots+\alpha_m^{-1} = \beta\}| \\ &= \sum \lambda(\alpha_1+\cdots+\alpha_m) + q^{-1}\{(q-1)^m + (-1)^{m+1}\}, \end{aligned} \tag{1.8}$$

with the sum running over all $\alpha_1,\cdots,\alpha_m \in \mathbb{F}_q^*$, *satisfying* $\alpha_1^{-1}+\cdots+\alpha_m^{-1} = \beta$.

(1) and (2) of the following are respectively $n = 2$ and $n = 4$ cases of Theorem 1.1 (1) (cf. (3.3), (3.4)), and (3) and (4) are equivalent and $n = 2$ case of Theorem 1.1 (2) ((cf. (5.4), (5.8)).

Corollary 1.2. (1) *Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$\begin{aligned} MK^h &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{h-l} MK^l \\ &+ q \sum_{j=0}^{\min\{(q-1),h\}} (-1)^{h+j} C_{1,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{q-1-j}{q-1-t}, \end{aligned} \tag{1.9}$$

where $\{C_{1,j}\}_{j=0}^{q-1}$ is the weight distribution of the binary linear code C_1, with

$$C_{1,j} = \sum \binom{1}{\nu_0} \prod_{\mathrm{tr}(\beta^{-1})=0} \binom{2}{\nu_\beta} \quad (j = 0, \cdots, N_1).$$

Here the sum is over all the sets of nonnegative integers $\{\nu_0\} \bigcup \{\nu_\beta\}_{\mathrm{tr}(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{\mathrm{tr}(\beta^{-1})=0} \nu_\beta \beta = 0$.

(2) *Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$\begin{aligned} MK_3^h &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{3(h-l)} MK_3^l \\ &+ q \sum_{j=0}^{min\{(q-1)^3,h\}} (-1)^{h+j} C_{3,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^3 - j}{(q-1)^3 - t}, \end{aligned} \tag{1.10}$$

where $\{C_{3,j}\}_{j=0}^{(q-1)^3}$ is the weight distribution of the binary linear code C_3, with

$$C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta}.$$

Here the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying (1.5),

$$m_0 = q^2 - 3q + 3,$$

and

$$m_t = t^2 + q^2 - 4q + 3,$$

for every integer t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1(4)$.

(3) *Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$\begin{aligned} MK^{2h} &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q-1)^{2(h-l)} MK^{2l} \\ &+ q \sum_{j=0}^{\min\{(q-1)^2, h\}} (-1)^{h+j} D_{2,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^2 - j}{(q-1)^2 - t}, \end{aligned} \tag{1.11}$$

where $\{D_{2,j}\}_{j=0}^{(q-1)^2}$ is the weight distribution of the binary linear code D_2, with

$$\begin{aligned} D_{2,j} &= \sum \binom{2q-3}{\nu_0} \prod_{\beta \in \mathbb{F}_q^*} \binom{K(\lambda; \beta^{-1}) + q - 3}{\nu_\beta} \\ &= \sum \binom{2q-3}{\nu_0} \prod_{\substack{|t| < 2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda; \beta^{-1}) = t} \binom{t + q - 3}{\nu_\beta}, \end{aligned} \tag{1.12}$$

with the sum running over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying (1.5).

(4) *Let $q = 2^r$. For $r \geqslant 3$, and $h = 1, 2, \cdots$,*

$$\begin{aligned} MK_2^h &= \sum_{l=0}^{h-1} (-1)^{h+l+1} \binom{h}{l} (q^2 - 3q + 1)^{(h-l)} MK_2^l \\ &+ q \sum_{j=0}^{\min\{(q-1)^2, h\}} (-1)^{h+j} D_{2,j} \sum_{t=j}^{h} t! S(h,t) 2^{h-t} \binom{(q-1)^2 - j}{(q-1)^2 - t}, \end{aligned} \tag{1.13}$$

where $D_{2,j} (0 \leqslant j \leqslant (q-1)^2)$'s are just as in (1.12).

The next two theorems will be of use later.

Theorem 1.3 ([9]). *Let $q = 2^r$, with $r \geqslant 2$. Then the range R of $K(\lambda; a)$, as a varies over $\mathbb{F}_q^*$, is given by*

$$R = \{t \in \mathbb{Z} \mid |t| < 2\sqrt{q},\ t \equiv -1(mod 4)\}.$$

In addition, each value $t \in R$ is attained exactly $H(t^2 - q)$ times, where $H(d)$ is the Kronecker class number of d.

Theorem 1.4 ([2]). *For the canonical additive character λ of $\mathbb{F}_q$, and $a \in \mathbb{F}_q^*$,*

$$K_2(\lambda; a) = K(\lambda; a)^2 - q. \tag{1.14}$$

Before we proceed further, we will fix the notations that will be used throughout this paper:

$$\begin{aligned} q &= 2^r \ (r \in \mathbb{Z}_{>0}), \\ \mathbb{F}_q &= \textit{the finite field with } q \textit{ elements}, \\ \mathrm{tr}(x) &= x + x^2 + \cdots + x^{2^{r-1}} \textit{ the trace function } \mathbb{F}_q \ \rightarrow \ \mathbb{F}_2, \\ \lambda(x) &= (-1)^{\mathrm{tr}(x)} \textit{ the canonical additive character of } \mathbb{F}_q. \end{aligned}$$

Note that any nontrivial additive character ψ of $\mathbb{F}_q$ is given by $\psi(x) = \lambda(ax)$, for a unique $a \in \mathbb{F}_q^*$.

2. Construction of codes associated with multi-dimensional Kloosterman sums

We will construct binary linear codes C_{n-1} of length $N_1 = (q-1)^{n-1}$, connected with the $(n-1)$-dimensional Kloosterman sums. Here $n = 2^s$, with $s \in \mathbb{Z}_{>0}$.

Let

$$v_{n-1} = (\cdots, \alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}, \cdots), \tag{2.1}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ run respectively over all elements of $\mathbb{F}_q^*$. Here we do not specify the ordering of the components of v_{n-1}, but we assume that some ordering is fixed.

Proposition 2.1 ([5], Proposition 11). *For each $\beta \in \mathbb{F}_q$, let*

$$\begin{aligned} &\delta(n-1, q; \beta) \\ &\quad = |\{(\alpha_1, \cdots, \alpha_{n-1}) \in (\mathbb{F}_q^*)^{n-1} | \alpha_1 + \cdots, +\alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1} = \beta\}| \end{aligned}$$

(Note that $\delta(n-1, q; \beta)$ is the number of components with those equal to β in the vector v_{n-1}(cf.(2.1))). Then

$$\delta(n-1, q; 0) = q^{-1}\{(q-1)^{n-1} + 1\},$$

and, for $\beta \in \mathbb{F}_q^*$,

$$\delta(n-1, q; \beta) = K_{n-2}(\lambda; \beta^{-1}) + q^{-1}\{(q-1)^{n-1} + 1\},$$

where $K_0(\lambda; \beta^{-1}) = \lambda(\beta^{-1})$ by convention.

Corollary 2.2.

$$(1)\quad \delta(1,q;\beta)=\begin{cases}2, & \textit{if} \ \ \mathrm{tr}(\beta^{-1})=0,\\ 1, & \textit{if} \ \ \beta=0,\\ 0, & \textit{if} \ \ \mathrm{tr}(\beta^{-1})=1.\end{cases} \tag{2.2}$$

$$(2)\quad \delta(3,q;\beta)=\begin{cases}q^2-3q+3, & \textit{if} \ \beta=0,\\ K(\lambda;\beta^{-1})^2+q^2-4q+3, & \textit{if} \ \beta\in\mathbb{F}_q^* \ (cf.(1.14)).\end{cases} \tag{2.3}$$

The binary linear code C_{n-1} is defined as

$$C_{n-1}=\{u\in\mathbb{F}_2^{N_1}|u\cdot v_{n-1}=0\}, \tag{2.4}$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_1}$.

The following Delsarte's theorem is well-known.

Theorem 2.3 ([12])**.** *Let B be a linear code over $\mathbb{F}_q$. Then*

$$(B|_{\mathbb{F}_2})^{\perp}=\mathrm{tr}(B^{\perp}).$$

In view of this theorem, the dual $C_{n-1}^{\perp}$ of C_{n-1} is given by

$$C_{n-1}^{\perp}=\{c(a)=(\cdots,\mathrm{tr}(a(\alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1})),\cdots)|a\in\mathbb{F}_q\}. \tag{2.5}$$

Lemma 2.4. *$(q-1)^{n-1}>nq^{\frac{n-1}{2}}$, for all $n=2^s$ $(s\in\mathbb{Z}_{>0})$, and $q=2^r\geqslant 8$.*

Proof. This can be proved, for example, by induction on s. □

Proposition 2.5. *For $q=2^r$, with $r\geqslant 3$, the map $\mathbb{F}_q\to C_{n-1}^{\perp}(a\mapsto c(a))$ is an $\mathbb{F}_2$-linear isomorphism.*

Proof. The map is clearly $\mathbb{F}_2$-linear and onto. Let a be in the kernel of the map. Then $\mathrm{tr}(a(\alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1}))=0$, for all $\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*$. Suppose that $a\neq 0$. Then, on the one hand,

$$\sum_{\alpha_1,\cdots,\alpha_{n-1}\in\mathbb{F}_q^*}(-1)^{\mathrm{tr}(a(\alpha_1+\cdots+\alpha_{n-1}+\alpha_1^{-1}\cdots\alpha_{n-1}^{-1}))}=(q-1)^{n-1}=N_1. \tag{2.6}$$

On the other hand, (2.6) is equal to $K_{n-1}(\lambda;a)$ (cf. proof of Proposition 11 in [5]), and so from Deligne's estimate in (1.1) we get

$$(q-1)^{n-1}\leqslant nq^{\frac{n-1}{2}}.$$

But this is impossible for $q\geqslant 8$, in view of Lemma 2.4. □

3. Recursive formulas for power moments of multi-dimensional Kloostermann sums

We are now ready to derive, via Pless power moment identity, a recursive formula for the power moments of multi-dimensional Kloosterman sums in terms of the frequencies of weights in C_{n-1}.

Theorem 3.1 (Pless power moment identity, [12]). *Let B be an q-ary $[n,k]$ code, and let B_i(resp. $B_i^{\perp}$) denote the number of codewords of weight i in B(resp. in $B^{\perp}$). Then, for $h = 0, 1, 2, \cdots$,*

$$\sum_{i=0}^{n} i^h B_i = \sum_{i=0}^{\min\{n,h\}} (-1)^i B_i^{\perp} \sum_{t=i}^{h} t! S(h,t) q^{k-t} (q-1)^{t-i} \binom{n-i}{n-t}, \quad (3.1)$$

where $S(h,t)$ is the Stirling number of the second kind defined in(1.3).

For the following lemma, observe that $(n, q-1) = 1$.

Lemma 3.2. *The map $a \mapsto a^n : \mathbb{F}_q^* \to \mathbb{F}_q^*$ is a bijection.*

Lemma 3.3. *For $a \in \mathbb{F}_q^*$, the Hamming weight $w(c(a))$(cf. (2.5)) of $c(a)$ can be expressed as follows:*

$$w(c(a)) = \frac{N_1}{2} - \frac{1}{2} K_{n-1}(\lambda; a), \text{ with } N_1 = (q-1)^{n-1}. \quad (3.2)$$

Proof.

$$\begin{aligned} w(c(a)) &= \frac{1}{2} \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} (1 - (-1)^{\mathrm{tr}(a(\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}))}) \\ &= \frac{1}{2} \{N_1 - \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} \lambda(a(\alpha_1 + \cdots + \alpha_{n-1} + \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}))\} \\ &= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} \lambda(\alpha_1 + \cdots + \alpha_{n-1} + a^n \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}) \\ &= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} \lambda(\alpha_1^n + \cdots + \alpha_{n-1}^n + a^n \alpha_1^{-n} \cdots \alpha_{n-1}^{-n}) \end{aligned}$$

(by Lemma 3.2)

$$\begin{aligned} &= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} \lambda((\alpha_1 + \cdots + \alpha_{n-1} + a \alpha_1^{-1} \cdots \alpha_{n-1}^{-1})^n) \\ &= \frac{N_1}{2} - \frac{1}{2} \sum_{\alpha_1, \cdots, \alpha_{n-1} \in \mathbb{F}_q^*} \lambda(\alpha_1 + \cdots + \alpha_{n-1} + a \alpha_1^{-1} \cdots \alpha_{n-1}^{-1}) \end{aligned}$$

([10], Theorem 2.23(v))

$$= \frac{N_1}{2} - \frac{1}{2} K_{n-1}(\lambda; a). \qquad \square$$

Denote for the moment v_{n-1} in (2.1) by $v_{n-1} = (g_1, g_2, \cdots, g_{N_1})$. Let $u = (u_1, \cdots, u_{N_1}) \in \mathbb{F}_2^{N_1}$, with ν_β 1's in the coordinate places where $g_l = \beta$, for each $\beta \in \mathbb{F}_q$. Then we see from the definition of the code C_{n-1} (cf. (2.4)) that u is a codeword with weight j if and only if $\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j$ and $\sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0$ (an identity in $\mathbb{F}_q$). As there are $\prod_{\beta \in \mathbb{F}_q} \binom{\delta(n-1,q;\beta)}{\nu_\beta}$ (cf. Proposition 2.1) many such codewords with weight j, we obtain the following result.

Proposition 3.4. *Let $\{C_{n-1,j}\}_{j=0}^{N_1}$ be the weight distribution of C_{n-1}, where $C_{n-1,j}$ denotes the frequency of the codewords with weight j in C_{n-1}. Then*

$$C_{n-1,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\delta(n-1, q; \beta)}{\nu_\beta},$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ $(0 \leqslant \nu_\beta \leqslant \delta(n-1, q; \beta))$ satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \text{ and } \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.$$

Corollary 3.5. (1) *Let $\{C_{1,j}\}_{j=0}^{q-1}$ be the weight distribution of C_1. Then*

$$C_{1,j} = \sum \binom{1}{\nu_0} \prod_{\operatorname{tr}(\beta^{-1})=0} \binom{2}{\nu_\beta} \quad (j = 0, \cdots, q-1), \tag{3.3}$$

where the sum is over all the sets of nonnegative integers $\{\nu_0\} \cup \{\nu_\beta\}_{\operatorname{tr}(\beta^{-1})=0}$ satisfying $\nu_0 + \sum_{\operatorname{tr}(\beta^{-1})=0} \nu_\beta = j$ and $\sum_{\operatorname{tr}(\beta^{-1})=0} \nu_\beta \beta = 0$ (cf.(2.2)).

(2) *Let $\{C_{3,j}\}_{j=0}^{(q-1)^3}$ be the weight distribution of C_3. Then*

$$C_{3,j} = \sum \binom{m_0}{\nu_0} \prod_{\substack{|t|<2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda;\beta^{-1})=t} \binom{m_t}{\nu_\beta}, \tag{3.4}$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \text{ and } \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0,$$

$$m_0 = q^2 - 3q + 3,$$

and

$$m_t = t^2 + q^2 - 4q + 3,$$

for every integer t satisfying $|t| < 2\sqrt{q}$ and $t \equiv -1(4)$ (cf. Theorem 1.3, (2.3)).

Remark 3.6. This shows that the weight distribution of C_1 is the same as that of $C(SO^+(2,q))$ (cf. [7]).

From now on, we will assume that $r \geqslant 3$, and hence every codeword in $C_{n-1}^{\perp}$ can be written as $c(a)$, for a unique $a \in \mathbb{F}_q$ (cf. Proposition 2.5).

We now apply the Pless power moment identity in (3.1) to $C_{n-1}^{\perp}$, in order to obtain the result in Theorem 1.1 (1) about a recursive formula. Then the left hand side of that identity in (3.1) is equal to

$$\sum_{a \in \mathbb{F}_q^*} w(c(a))^h, \tag{3.5}$$

with $w(c(a))$ given by (3.2). So (3.5) is

$$\begin{aligned} \sum_{a \in \mathbb{F}_q^*} w(c(a))^h &= \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} (N_1 - K_{n-1}(\lambda; a))^h \\ &= \frac{1}{2^h} \sum_{a \in \mathbb{F}_q^*} \sum_{l=0}^{h} (-1)^l \binom{h}{l} N_1^{h-1} K_{n-1}(\lambda; a)^l \qquad (3.6) \\ &= \frac{1}{2^h} \sum_{l=0}^{h} (-1)^l \binom{h}{l} N_1^{h-1} M K_{n-1}^l. \end{aligned}$$

On the other hand, noting that $dim_{\mathbb{F}_2} C_{n-1} = r$ (cf. Proposition 2.5) the right hand side of the Pless moment identity(cf. (3.1)) becomes

$$q \sum_{j=0}^{\min\{N_1,h\}} (-1)^j C_{n-1,j} \sum_{t=j}^{h} t! S(h,t) 2^{-t} \binom{N_1 - j}{N_1 - t}. \tag{3.7}$$

Our result in (1.2) follows now by equating (3.6) and (3.7).

Remark 3.7. A recursive formula for the power moments of multi-dimensional Kloosterman sums was obtained in [5] by constructing binary linear codes $C(SL(n,q))$ and utilizing explicit expressions of Gauss sums for the finite special linear group $SL(n,q)$. However, our result in (1.2) is better than that in (1) of [5]. Because our formula here is much simpler than the one there. Indeed, the length of the code C_{n-1} here is $N_1 = (q-1)^{n-1}$, whereas that of $C(SL(n,q))$ there is $N = q^{\binom{n}{2}} \prod_{j=2}^{n} (q^j - 1)$, both of which appear in their respective expressions of recursive formulas.

4. Construction of codes associated with powers of Kloosterman sums

We will construct binary linear codes D_m of length $N_2 = (q-1)^m$, connected with the m-th powers of (the ordinary) Kloosterman sums. Here $m \in \mathbb{Z}_{>0}$.

Let

$$w_m = (\cdots, \alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1}, \cdots), \tag{4.1}$$

where $\alpha_1, \alpha_2, \cdots, \alpha_m$ run respectively over all elements of $\mathbb{F}_q^*$. Here we do not specify the ordering of the components of w_m, but we assume that some ordering is fixed.

Theorem 4.1 ([7]). *Let λ be the canonical additive character of $\mathbb{F}_q$, and let $\beta \in \mathbb{F}_q^*$. Then*

$$\sum_{\alpha \in \mathbb{F}_q - \{0,1\}} \lambda\left(\frac{\beta}{\alpha^2 + \alpha}\right) = K(\lambda; \beta) - 1. \tag{4.2}$$

Proposition 4.2. *For each $\beta \in \mathbb{F}_q$, let*

$$\sigma(m, q; \beta) = |\{(\alpha_1, \cdots, \alpha_m) \in (\mathbb{F}_q^*)^m | \alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta\}|$$

(Note that $\sigma(m, q; \beta)$ is the number of components with those equal to β in the vector w_m (cf. (4.1)). Then

$$(1) \quad \sigma(m, q; \beta) = \sum \lambda(\alpha_1 + \cdots + \alpha_m) + q^{-1}\{(q-1)^m + (-1)^{m+1}\}, \tag{4.3}$$

where the sum in (4.3) runs over all $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \cdots + \alpha_m^{-1} = \beta$.

$$(2) \quad \sigma(2, q; \beta) = \begin{cases} 2q - 3, & \text{if } \beta = 0, \\ K(\lambda; \beta^{-1}) + q - 3, & \text{if } \beta \neq 0. \end{cases} \tag{4.4}$$

Proof. (1) can be proved just as Proposition 2.1(cf. [5], Proposition 11). The details are left to the reader.

(2) If $m = 2$, from (4.3)

$$\sigma(2, q; \beta) = \sum \lambda(\alpha_1 + \alpha_2) + q - 2, \tag{4.5}$$

where α_1 and α_2 run over all elements in $\mathbb{F}_q^*$, satisfying $\alpha_1^{-1} + \alpha_2^{-1} = \beta$.

If $\beta = 0$, then the result is clear. Assume now that $\beta \neq 0$. Then the sum in (4.5) is

$$\begin{aligned}
&\sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta^{-1}\}} \lambda(\alpha_1 + (\alpha_1^{-1} + \beta)^{-1}) \\
&\qquad = \sum_{\alpha_1 \in \mathbb{F}_q - \{0, \beta\}} \lambda(\alpha_1^{-1} + (\alpha_1 + \beta)^{-1}) \quad (\alpha_1 \to \alpha_1^{-1}) \\
&\qquad = \sum_{\alpha_1 \in \mathbb{F}_q - \{0, 1\}} \lambda(\frac{\beta^{-1}}{\alpha_1^2 + \alpha_1}) \quad (\alpha_1 \to \beta\alpha_1) \\
&\qquad = K(\lambda; \beta^{-1}) - 1 \ (cf.(4.2)).
\end{aligned}$$ □

The binary linear code D_m is defined as

$$D_m = \{u \in \mathbb{F}_2^{N_2} | u \cdot w_m = 0\},$$

where the dot denotes the usual inner product in $\mathbb{F}_q^{N_2}$.

Remark 4.3. Clearly, the binary linear codes C_1 and D_1 coincide.

In view of Theorem 2.3, the dual $D_m^{\perp}$ of D_m is given by

$$D_m^{\perp} = \{d(a) = (\cdots, \mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1})), \cdots) | a \in \mathbb{F}_q\}. \tag{4.6}$$

Lemma 4.4. *$(q-1)^m > 2^m q^{\frac{m}{2}}$, for all $m \in \mathbb{Z}_{>0}$ and $q = 2^r \geqslant 8$.*

Proof. This can be shown, for example, by induction on m. □

Proposition 4.5. *For $q = 2^r$, with $r \geqslant 3$, the map $\mathbb{F}_q \to D_m^{\perp}(a \mapsto d(a))$ is an $\mathbb{F}_2$-linear isomorphism.*

Proof. The map is clearly $\mathbb{F}_2$-linear and onto. Let a be in the kernel of the map. Then $\mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1})) = 0$, for all $\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*$. Suppose that $a \neq 0$. Then, on the one hand,

$$\sum_{\alpha_1, \cdots, \alpha_m \in \mathbb{F}_q^*} (-1)^{\mathrm{tr}(a(\alpha_1 + \cdots + \alpha_m + \alpha_1^{-1} + \cdots + \alpha_m^{-1}))} = (q-1)^m = N_2. \tag{4.7}$$

On the other hand, (4.7) is equal to $K(\lambda; a)^m$, and so from Weil's estimate (i.e. (1.1) with $m = 1$) we get

$$(q-1)^m \leqslant 2^m q^{\frac{m}{2}}.$$

But this is impossible for $q \geqslant 8$, in view of Lemma 4.4. □

5. Recursive formulas for m-multiple power moments of Kloostermann sums

We are now ready to derive, via Pless power moment identity, a recursive formula for the m-multiple power moments of Kloosterman sums in terms of the frequencies of weights in D_m.

Lemma 5.1. *For $a \in \mathbb{F}_q^*$, the Hamming weight $w(d(a))$ of $d(a)$ (cf. (4.6)) can be expressed as follows:*

$$w(d(a)) = \frac{N_2}{2} - \frac{1}{2}K(\lambda; a)^m, \ \text{with } N_2 = (q-1)^m. \tag{5.1}$$

Proof. This can be shown exactly as the proof of Lemma 3.3. □

Corollary 5.2. *For $m = 2$,*

$$w(d(a)) = \frac{1}{2}(q^2 - 3q + 1 - K_2(\lambda; a)) \ (cf.(1.14)). \tag{5.2}$$

The same argument leading to Proposition 3.4 shows the next proposition.

Proposition 5.3. *Let $\{D_{m,j}\}_{j=0}^{N_2}$ be the weight distribution of D_m, where $D_{m,j}$ denotes the frequency of the codewords with weight j in D_m. Then*

$$D_{m,j} = \sum \prod_{\beta \in \mathbb{F}_q} \binom{\sigma(m, q; \beta)}{\nu_\beta}, \tag{5.3}$$

where the sum runs over all the sets of integers $\{\nu_\beta\}_{\beta \in \mathbb{F}_q}$ $(0 \leqslant \nu_\beta \leqslant \sigma(m, q; \beta))$, satisfying

$$\sum_{\beta \in \mathbb{F}_q} \nu_\beta = j, \ \text{and} \ \sum_{\beta \in \mathbb{F}_q} \nu_\beta \beta = 0.$$

Corollary 5.4. *Let $\{D_{2,j}\}_{j=0}^{(q-1)^2}$ be the weight distribution of D_2, and let $q = 2^r$, with $r \geqslant 2$. Then, in view of Theorem 1.3 and (4.4), we have*

$$\begin{aligned} D_{2,j} &= \sum \binom{2q-3}{\nu_0} \prod_{\beta \in \mathbb{F}_q^*} \binom{K(\lambda; \beta^{-1}) + q - 3}{\nu_\beta} \\ &= \sum \binom{2q-3}{\nu_0} \prod_{\substack{|t| < 2\sqrt{q} \\ t \equiv -1(4)}} \prod_{K(\lambda; \beta^{-1}) = t} \binom{t + q - 3}{\nu_\beta}, \end{aligned} \tag{5.4}$$

where the sum runs over all the sets of nonnegative integers $\{\nu_\beta\}_{\beta\in\mathbb{F}_q}$ *satisfying*

$$\sum_{\beta\in\mathbb{F}_q}\nu_\beta = j \quad \textit{and} \quad \sum_{\beta\in\mathbb{F}_q}\nu_\beta\beta = 0.$$

From now on, we will assume that $r \geqslant 3$, *and hence every codeword in* $D_m^\perp$ *can be written as* $d(a)$, *for a unique* $a\in\mathbb{F}_q$ *(cf. Proposition 4.5).*

We now apply the Pless power moment identity in (3.1) to $D_m^\perp$, in order to obtain the result in Theorem 1.1 (1) about a recursive formula. Then the left hand side of that identity in (3.1) is equal to

$$\sum_{a\in\mathbb{F}_q^*} w(d(a))^h, \tag{5.5}$$

with $w(d(a))$ given by (5.1). So (5.5) is seen to be equal to

$$\sum_{a\in\mathbb{F}_q^*} w(d(a))^h = \frac{1}{2^h}\sum_{l=0}^{h}(-1)^l\binom{h}{l}N_2^{h-l}MK^{ml}. \tag{5.6}$$

On the other hand, noting that $dim_{\mathbb{F}_2}D_m = r$(cf. Proposition 4.5) the right hand side of the Pless moment identity(cf. (3.1)) becomes

$$q\sum_{j=0}^{\min\{N_2,h\}}(-1)^jD_{m,j}\sum_{t=j}^{h}t!S(h,t)2^{-t}\binom{N_2-j}{N_2-t}. \tag{5.7}$$

Our result in (1.6) follows now by equating (5.6) and (5.7).

Remark 5.5. If $m=2$, from the alternative expression of $w(d(a))$ in (5.2) we see that (5.5) can also be given as

$$\sum_{a\in\mathbb{F}_q^*} w(d(a))^h = \frac{1}{2^h}\sum_{l=0}^{h}(-1)^l\binom{h}{l}(q^2-3q+1)^{h-l}MK_2^l. \tag{5.8}$$

References

[1] L. Carlitz, *Gauss sums over finite fields of order* 2^n, Acta. Arith. **15**(1969), 247–265.

[2] L. Carlitz, *A note on exponential sums*, Pacific J. Math. **30**(1969), 35–37.

[3] R. J. Evans, *Seventh power moments of Kloosterman sums*, Israel J. Math. **175**(2010), 349–362.

[4] K. Hulek, J. Spandaw, B. van Geemen, and D. van Straten, *The modularity of the Barth-Nieto quintic and its relatives*, Adv. Geom. **1**(2001), 263-289.

[5] D. S. Kim, *Codes associated with special linear groups and power moments of multi-dimensional Kloosterman sums,* Ann. Mat. Pura Appli. **190**(2011), 61-76.

[6] D. S. Kim, *Infinite families of recursive formulas generating power moments of ternary Kloosterman sums with square arguments arising from symplectic groups,* Adv. Math. Commun. **3**(2009), 167–178.

[7] D. S. Kim, *Codes associated with $O^+(2n, 2^r)$ and power moments of Kloosterman sums*, Integers **12**(2012), 237–257.

[8] H. D. Kloosterman, *On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$*, Acta Math. **49**(1926), 407-464.

[9] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory **36**(1990), 686-692.

[10] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl.**20**, Cambridge University Pless, Cambridge, 1987.

[11] R. Livné, *Motivic orthogonal two-dimensional representations of Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$, Israel J. Math. **92**(1995), 149-156.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1998.

[13] M. Moisio, *The moments of a Kloosterman sum and the weight distribution of a Zetterberg-type binary cyclic code*, IEEE Trans. Inform. Theory **53**(2007), 843-847.

[14] M. Moisio, *On the duals of binary hyper-Kloosterman codes*, SIAM J. Disc. Math. **22**(2008), 273-287.

[15] M. Moisio, K. Ranto, M. Rinta-aho and Väänänen, *On the weight distribution of the duals of irreducible cyclic codes, cyclic codes with two zeros and hyper-Kloosterman codes*, Adv. Appl. Discrete Math. **3**(2009), 155-164.

[16] C. Peters, J. Top, and M. van der Vlugt, *The Hasse zeta function of a K3 surface related to the number of words of weight 5 in the Melas codes*, J. Reine Angew. Math. **432**(1992), 151-176.

[17] H. Salié, *Über die Kloostermanschen Summen* $\mathcal{S}(u, v; q)$,Math. Z. **34**(1931), 91-109.

[18] R. Schoof and M. van der Vlugt, *Hecke operators and the weight distributions of certain codes*, J. Combin. Theory Ser. A **57**(1991), 163-186.

Contact information

Dae San Kim Department of Mathematics, Sogang University,
Seoul 121-742, South Korea
E-Mail(s): dskim@sogang.ac.kr

Received by the editors: 23.10.2010
and in final form 25.01.2015.

Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **19** (2015). Number 2, pp. 229–242

On fibers and accessibility of groups acting on trees with inversions

Rasheed Mahmood Saleh Mahmood*

Communicated by V. A. Artamonov

Abstract. Throughout this paper the actions of groups on graphs with inversions are allowed. An element g of a group G is called inverter if there exists a tree X where G acts such that g transfers an edge of X into its inverse. A group G is called accessible if G is finitely generated and there exists a tree on which G acts such that each edge group is finite, no vertex is stabilized by G, and each vertex group has at most one end.

In this paper we show that if G is a group acting on a tree X such that if for each vertex v of X, the vertex group G_v of v acts on a tree X_v, the edge group G_e of each edge e of X is finite and contains no inverter elements of the vertex group $G_{t(e)}$ of the terminal $t(e)$ of e, then we obtain a new tree denoted $\widetilde{X}$ and is called a fiber tree such that G acts on $\widetilde{X}$. As an application, we show that if G is a group acting on a tree X such that the edge group G_e for each edge e of X is finite and contains no inverter elements of $G_{t(e)}$, the vertex G_v group of each vertex v of X is accessible, and the quotient graph G/X for the action of G on X is finite, then G is an accessible group.

*The author would like to thank the referee for his(her) help and suggestions to improve the first draft of this paper.

2000 MSC: 20E06, 20E086, 20F05.

Key words and phrases: Ends of groups, groups acting on trees, accessible groups.

Introduction

The theory of groups acting on trees without inversions known Bass-Serre theory is introduced in [2] and [10], and with inversions is introduced in [9]. The concepts of the fibers of groups acting on trees without inversions were introduced in ([2], p. 78). In this paper we generalize such concepts to the case where the actions of groups on trees with inversions are allowed, and have applications. This paper is divided into 3 sections. In section 1, we introduce the concept of groups acting on trees with inversions. In section 2, we use the results of section 1 to obtain new trees called the fibers of groups acting on trees with inversions. In section 3, we use the results of section 2 to have applications.

1. Groups acting on trees

We begin with general background. A graph X consists of two disjoint sets $V(X)$, (the set of vertices of X) and $E(X)$, (the set of edges of X), with $V(X)$ non-empty, together with three functions $\partial_0 : E(X) \to V(X)$, $\partial_1 : E(X) \to V(X)$, and $\eta : E(X) \to E(X)$ is an involution satisfying the conditions that $\partial_0\eta = \partial_1$ and $\partial_1\eta = \partial_0$. For simplicity, if $e \in E(X)$, we write $\partial_0(e) = o(e)$, $\partial_1(e) = t(e)$, and $\eta(e) = \overline{e}$. This implies that $o(\overline{e}) = t(e)$, $t(\overline{e}) = o(e)$, and $\overline{\overline{e}} = e$. The case $\overline{e} = e$ is allowed. For the edge e, $o(e)$ and $t(e)$ are called the ends of e, and $\bar{e}$ is called the inverse of e. By a path P of X we mean a sequence $y_1, ..., y_n$ of edges of X such that $t(y_j) = o(y_{j+1})$ for $j = 1, \ldots, n-1$. P is reduced if $y_{i+1} \neq \overline{y}_i$, $i = 1, \ldots, n-1$.

The origin $o(P)$ and the terminal $t(P)$ of P are defined as $o(P) = o(y_1)$, and $t(P) = t(y_n)$. There are obvious definitions of subgraphs, circuits, morphisms of graphs and $Aut(X)$, the set of all automorphisms of the graph X which is a group under the composition of morphisms of graphs. For more details, the interested readers are referred to [2], [9], and [10]. We say that a group G acts on a graph X, (or X is a G-graph) if there is a group homomorphism $\phi : G \to Aut(X)$. In this case, if $x \in X$ (vertex or edge) and $g \in G$, we write $g(x)$ for $(\phi(g))(x)$. Thus, if $g \in G$, and $y \in E(X)$, then $g(o(y)) = o(g(y))$, $g(t(y)) = t(g(y))$, and $g(\overline{y}) = \overline{g(y)}$. The case the actions with inversions are allowed. That is; $g(y) = \overline{y}$ is allowed for some $g \in G$, and $y \in E(X)$. In this case we say that g is an inverter element of G and y is called an inverted edge of X.

If X and Y are G-graphs, and $\mu : V(X) \to V(Y)$ is a map, then μ is called G-map if $\mu(g(x)) = g(\mu(x))$ for all $x \in V(X)$.

Convention. If the group G acts on the graph X and $x \in X$, (x is a vertex or edge), then

1. The stabilizer of x, (or the x group) denoted G_x is defined to be the set $G_x = \{g \in G\colon g(x) = x\}$. It is clear that $G_x \leqslant G$, and if $x \in E(X)$, and $u \in \{o(x),\ t(x)\}$, then $G_{\overline{x}} = G_x$ and $G_x \leqslant G_u$.

2. The orbit of x denoted $G(x)$ and is defined to be the set $G(x) = \{g(x) : g \in G\}$. It is clear that G acts on the graph X without inversions if and only if $G(\overline{e}) \neq G(e)$ for any $e \in E(X)$.

3. The set of the orbits G/X of the action of G on X is defined as $G/X = \{G(x) : x \in X\}$. G/X forms a graph called the quotient graph of the action of G on X, where $V(G/X) = \{G(v) : v \in V(X)\}$, $E(G/X) = \{G(e) : e \in E(X)\}$, and if $e \in E(X)$, then $o(G(e)) = G(o(e))$, $t(G(e)) = G(t(e))$, and $\overline{G(e)} = G(\overline{e})$. The map $p : X \to G/X$ given by $p(x) = G(x)$ is an onto morphism of graphs. If X is connected, then G/X is connected.

4. The set of elements of X fixed by G is the set $X^G = \{x \in X : G_x = G\}$.

Definition 1. Let G be a group acting on a tree X with inversions and let T and Y be two subtrees of X such that $T \subseteq Y$, and each edge of Y has at least one end in T. Assume that T and Y are satisfying the following.

(i) T contains exactly one vertex from each vertex orbit.

(ii) Y contains exactly one edge y(say) from edge orbit if $G(y) \neq G(\overline{y})$ and exactly one pair x, $\overline{x}$ from each edge orbit if $G(x) = G(\overline{x})$. Then

(1) T is called a tree of representatives for the action of G on X,

(2) Y is called a transversal for the action of G on X.

For simplicity we say that $(T;Y)$ is a fundamental domain for the action of G on X.

For the existence of fundamental domains we refer the readers to [5]. For the rest of this section, G is a group acting on a tree X with inversions, and $(T;Y)$ is a fundamental domain for the action of G on X.

The properties of T and Y imply the following that for any $v \in V(X)$ there exists a unique vertex denoted v^* of T and an element g (not unique) of G such that $g(v^*) = v$; that is, $G(v^*) = G(v)$. Moreover, if $v \in V(T)$, then $v^* = v$.

Definition 2. For each $y \in E(Y)$, let $[y]$ be an element of G chosen as follows.

(a) if $o(y) \in V(T)$, then $[y]((t(y))^*) = t(y)$, $[y] = 1$ in case $y \in E(T)$, and $[y](y) = \overline{y}$ if $G(y) = G(\overline{y})$,

(b) if $t(y) \in V(T)$, then $[y](o(y)) = (o(y))^*$, $[y] = [\overline{y}]^{-1}$ if $G(y) \neq G(\overline{y})$, and $[y] = [\overline{y}]$ if $G(y) = G(\overline{y})$.

Proposition 1. *G is generated by G_v and $[e]$, where v runs over $V(T)$ and e runs over $E(Y)$.*

Proof. See Lemma 4.4 of [9]. □

The proof of the following proposition is clear.

Proposition 2. *For each edge $y \in E(Y)$,let $[y][\overline{y}] = \delta_y$. Then $\delta_y = 1$ if $G(y) \neq G(\overline{y})$, and $\delta_y = [y]^2 \in G_y$ if $G(y) = G(\overline{y})$. Moreover $[y] \notin G_{(t(y))^*}$, if $y \notin E(T)$.*

Definition 3. For each $y \in E(Y)$, let $+y$ be the edge $+y = y$ if $o(y) \in V(T)$, and $+y = [y](y)$ if $t(y) \in V(T)$.

It is clear that if $G(y) = G(\overline{y})$ or $y \in E(T)$, then $G_{+y} = G_y$. Furthermore, if x and y are two edges of Y such that $+x = +y$, then $x = y$ or $x = \overline{y}$.

Definition 4. By a word w of G we mean an expression of the form $w = g_0$, $g_0 \in G_v$, $v \in V(T)$, or, $w = g_0.y_1.g_1...y_n.g_n$, $n > 0$, $y_i \in E(Y)$ for $i = 1, \ldots, n$ such that the following hold.

(1) $g_0 \in G_{\ (o(y_1))^*}$,

(2) $(t(y_i))^* = (o(y_{i+1}))^*$, for $i = 1, 2, \ldots, n-1$,

(3) $g_i \in G_{\ (t(y_i))^*}$, for $i = 1, 2, \ldots, n$.

We define $o(w) = (o(y_1))^*$ and $t(w) = (t(y_n))^*$. If $o(w) = t(w) = v$, then w is called a closed word of G.

We have the following concepts related to the word w defined above.

(i) The value of w is denoted by $[w]$ and defined to be the element of

$$[w] = g_0[y_1]g_1...[y_n]g_n \text{ of } G.$$

(ii) w reduced if either $n = 0$ and $g_0 \neq 1$, or else $n > 0$ and w contains no subword of the following forms:

$$y_i.g_i.\overline{y}_i \text{ if } g_i \in G_{+(y_i)}, \text{and } +y_{i+1} = +(\overline{y}_i)\,,\ i = 1, \ldots n.$$

(iii) For each $i, i = 1, \ldots, n$, let $w_i = g_0.y_1.g_1...y_{i-1}.g_{i-1}$with convention $w_1 = g_0$.

Definition 5. For $g \in G$ and $e \in E(Y)$ let $[g; e]$ be the ordered pair $[g; e] = (gG_{+e}; +e)$.

Remark 1. If w is a reduced word of G and $y \in E(Y)$, no confusion will be confused by $[w]$, the value of w, and the ordered pair $[[w]; y]$.

Proposition 3. *Let $w = g_0.y_1.g_1...y_n.g_n$ and $w' = h_0.x_1.h_1...x_m.h_m$ be two reduced words of G such that $o(w) = o(w')$, $t(w) = t(w')$, and $[w] = [w']$. Then $m = n$ and, $[[w_i]; y_i] = [[w'_i]; x_i]$ for $i = 1, \dots, n$.*

Proof. We have $[w'][w]^{-1} = 1$. Let $\widetilde{w} = g_n^{-1}\delta_{y_n}^{-1}.\overline{y}_n...g_1^{-1}\delta_{y_1}^{-1}.\overline{y}_1.g_0^{-1}$.

It is clear that $\widetilde{w}$ is a reduced word of G and $[\widetilde{w}] = [w]^{-1}$. Then $w_0 = \widetilde{w}w' = g_n^{-1}\delta_{y_n}^{-1}.\overline{y}_n.....g_1^{-1}\delta_{y_1}^{-1}.\overline{y}_1.g_0^{-1}h_0.x_1.h_1.....x_m.h_m$ is a word of G.

For each $i = 0, 1, \dots, n$, let

$$L_i = g_i^{-1}\delta_{y_i}^{-1}\left[\overline{y}_i\right].....g_1^{-1}\delta_{y_1}^{-1}\left[\overline{y}_1\right]g_0^{-1}h_0\left[x_1\right]h_1...\left[x_i\right]h_i$$

with convention that $L_0 = g_0^{-1}h_0$. Since $[y]\left[\overline{y}\right] = \delta_y$ for every $y \in E(Y)$, therefore $L_i = g_i^{-1}\left[y_i\right]^{-1}.....g_1^{-1}\left[y_1\right]^{-1}g_0^{-1}h_0\left[x_1\right]h_1...\left[x_i\right]h_i$. Moreover, $L_i = g_i^{-1}\left[y_i\right]^{-1}L_{i-1}\left[x_i\right]h_i$. Since $[w_0] = 1$, the identity element of G, therefore by Corollary 1 of [8], w_0 is not reduced. Since $\widetilde{w}$ and w' are reduced, the only way that the indicated word w_0 can fail to be reduced is that $m = n$, and for $i = 1, \dots, n$, $+x_i = +\overline{\overline{y_i}} = +y_i$ and $L_{i-1} \in G_{+(x_i)} = G_{+(y_i)}$.

The case $L_{i-1} \in G_{+(x_i)} = G_{+(y_i)}$ implies that $[w_i]^{-1}[w'_i] \in G_{+(\overline{x_i})} = G_{+(\overline{y_i})}$. Then $[w_i]G_{+(y_i)} = [w'_i]G_{+(x_i)}$. Consequently $[[w_i]; y_i] = [[w'_i]; x_i]$, $i = 1, \dots, n-1$. This completes the proof. □

2. Fibers of groups acting on trees

We begin some general background taken from ([2], p. 78).

Definition 6. Let H be a subgroup of the group G and H acts on the set X. Define $\equiv$ to be the relation on $G \times X$ defined as $(f, u) \equiv (g, v)$, if there exists $h \in H$ such that $f = gh$ and $u = h^{-1}(v)$. It is easy to show that $\equiv$ is an equivalence relation on $G \times X$. The equivalence class containing (f, u) is denoted by $f \otimes_H u$. Thus, $f \otimes_H u = \left\{(fh, h^{-1}(u)) : h \in H\right\}$.

Consequently, if $f \otimes_H u = g \otimes_H v$, then $f = gh$ and $u = h^{-1}(v)$, $h \in H$. So $f \otimes_H u = fh \otimes_H h^{-1}(u)$ for all $h \in H$.

Let $g \in G$ and $A \subseteq H$. Define $g \otimes_H A = \{g \otimes_H a : a \in A\}$, and

$$G \otimes_H X = \{g \otimes_H x : g \in G, x \in X\}.$$

It is clear that $1 \otimes_H x = h \otimes_H x$ for all $h \in H_x$, the stabilizer of x under the action of H on X. It is easy to show that the rule $f(g \otimes_H x) = fg \otimes_H x$ for all $f, g \in G$, and all $x \in X$ defines an action of G on $G \otimes_H X$. The stabilizer $G_{g \otimes_H} x$ of $g \otimes_H x$ under the action of G on $G \otimes_H X$ is $G_{g \otimes_H} x = gH_x g^{-1}$ and the orbit $G(g \otimes_H x)$ of $g \otimes_H x$ under the action of G on $G \otimes_H X$ is $G \otimes_H H(x)$ where $H(x)$ is the orbit of x under the action of H on X.

Remark 2. $x \in X$ means x is a vertex or an edge of X.

Definition 7. Let G be a group acting on a tree X and $(T; Y)$ be a fundamental domain for the action of G on X. For each $v \in V(T)$, let X_v be a tree on which G_v acts; (X_v could consist of the single vertex $\{v\}$) and let $\widehat{X}$ be the set $\widehat{X} = \{[g; e] : g \in G, e \in E(Y)\}$, and $\widetilde{X}$ be the set $\widetilde{X} = \widehat{X} \cup (\bigcup_{v \in V(T)} (G \otimes_{G_v} X_v))$.

The following lemma is a generalization of Corollary 4.9 of ([2], p. 18) and is essential for the proof of the main result of this section.

Lemma 1. *Let G be a group acting on a tree X and H be a finite subgroup of G such that H contains no inverter elements of G. Then H is in G_v for some $v \in V(X)$.*

Proof. If G acts on X without inversions, then G contains no inverter elements and by ([2], p. 18) H is in G_v for some v∈V(X). Let G act on X with inversions and $g \in H$ be an inverter element. Then $g(e) = \overline{e}$ for some $e \in E(X)$. This implies that $g(o(e)) = t(e)$. Now we show that $g \notin G_v$ for any $v \in V(X)$. If $g \in G_v$, then there is a unique reduced path $e_1, e_2, ..., e_n$ in X joining $o(e)$ and v. Then $g(e_1), g(e_2), ..., g(e_n)$ is a unique reduced path in X joining $g(o(e)) = t(e)$ and $g(v) = v$. Then $\overline{e}, g(e_1), g(e_2), ..., g(e_n)$ is a path in X joining $g(o(e)) = t(e)$ and $g(v) = v$ but not reduced because X is a tree. Therefore $e = g(e_1)$ and $g(e_2), ..., g(e_n)$ is a reduced path in X joining $t(e)$ and v. Thus, the vertices $t(e)$ and v are joined in X by two distinct reduced paths. This contradicts the assumption that X is tree. This completes the proof. □

Remark 3. In Lemma 1 if $g \in G$ and $e \in E(X)$ such that $g(e) = \overline{e}$, then $g^2(e) = g(\overline{e}) = \overline{g(e)} = \overline{\overline{e}} = e$. This implies that $g \notin G_e$ and $g^2 \in G_e$.

If $G_e = \{1\}$, then the subgroup $H = \{1, g\}$ is finite, but H is not contained in G_e for any $v \in V(X)$.

Theorem 1. *Let G be a group acting on a tree X and $(T; Y)$ be a fundamental domain for the action of G on X. For each $v \in V(T)$, let X_v be a tree on which G_v acts such that for each $e \in E(X)$, $o(e) \in V(T)$, the stabilizer G_e is in a vertex stabilizer $(G_{o(e)})_w$, $w \in V(X_{o(e)})$.*

Then $\widetilde{X}$ forms a tree and G acts on $\widetilde{X}$. Furthermore, if G acts on X with inversions, or for some $v \in V(T), G_v$ acts on X_v with inversions, then G acts on $\widetilde{X}$ with inversions.

Proof. For each edge $e \in E(Y)$ it is clear that $o(+e) = (o(e))^* \in V(T)$ and $G_{+y} \leqslant G_{(o(y))^*}$. By assumption there exists a vertex denoted v_e such that $v_e \in V(X_{o(e)})$ and $G_e \leqslant (G_{o(e)})_{v_e}$, where $(G_{o(e)})_{v_e}$ is the vertex stabilizer of the vertex v_e under the action of $G_{o(e)}$ on $X_{o(e)}$. Now we show that $\widetilde{X}$ forms a graph. The set of vertices $V(\widetilde{X})$ of $\widetilde{X}$ is defined to be the set $V(\widetilde{X}) = \underset{v \in V(T)}{\cup}(G \otimes_{G_v} V(X_v))$ and the set of edges $E(\widetilde{X})$ of $\widetilde{X}$ is defined to be the set $E(\widetilde{X}) = \widehat{X} \cup (\underset{v \in V(T)}{\cup}(G \otimes_{G_v} E(X_v))$. It is clear that $V(\widetilde{X}) \neq \phi$ and $V(\widetilde{X}) \cap E(\widetilde{X}) = \phi$. The ends and the inverses of the edges of $\widetilde{X}$ are defined as follows. Let $g \in G$, $v \in V(T)$, and $e \in E(X_v)$.

Define the ends and the inverse of the edge $g \otimes_{G_v} e$ as follows.

$$t(g \otimes_{G_v} e) = g \otimes_{G_v} t(e), o(g \otimes_{G_v} e) = g \otimes_{G_v} o(e) \text{ and } \overline{g \otimes_{G_v} e} = g \otimes_{G_v} \overline{e},$$

where $t(e), o(e)$, and $\overline{e}$ are the ends and the inverse of the edge e in X_v.

If $e \in E(Y)$, we define the ends and the inverse of the edge $[g;e]$ as follows. $o[g;e] = g \otimes_{G_{(o(e))^*}} v_e, t[g;e] = g[e] \otimes_{G_{(t(e))^*}} v_{\overline{e}}$ and $\overline{[g;e]} = [g[e];\overline{e}]$. Then $\overline{\overline{[g;e]}} = [g[e][\overline{e}];\overline{\overline{e}}] = [g;e]$ because $[e][\overline{e}] \in G_{+e}$. These definitions show that $\widetilde{X}$ forms a graph. For $g \in G$ and $v \in V(T)$, let $g \otimes_{G_v} X_v = \{g \otimes_v u : u \in X_v\}$. It is clear that the elements of $g \otimes_{G_v} X_v$ are distinct and $g \otimes_{G_v} X_v$ forms a subtree of $\widetilde{X}$, where $V(g \otimes_{G_v} X_v) = g \otimes_{G_v} V(X_v)$ and $E(g \otimes_{G_v} X_v\ ) = g \otimes_{G_v} E(X_v)$. Then $g \otimes_{G_v} X_v = 1 \otimes_{G_v} X_v$, $g \in G_v$. We observe that if $g \in G$, $v \in V(T)$, v_1 and v_2 are two vertices of $V(X_v)$, and $P : e_1, e_2, ..., e_n$ is a reduced path in X_v joining v_1 and v_2 then it is clear that $g \otimes_{G_v} P : g \otimes_{G_v} e_1, g \otimes_{G_v} e_2, ..., g \otimes_{G_v} e_n$ is a reduced path in $g \otimes_{G_v} X_v$ joining the vertices $g \otimes_{G_v} v_1$ and $g \otimes_{G_v} v_2$ of $g \otimes_{G_v} X_v$. We call $g \otimes_{G_v} P$ the reduced path in $g \otimes_{G_v} X_v$ joining the vertices $g \otimes_{G_v} v_1$ and $g \otimes_{G_v} v_2$ in $g \otimes_{G_v} X_v$ induced by the reduced path in X_v joining v_1 and v_2. We note that P could consist of a single vertex. Now we show that $\widetilde{X}$ forms a tree. First we show that $\widetilde{X}$ contains no loops.

For, if $g \in G$ and $e \in E(Y)$ such that $o[g;e] = t[g;e]$, then $g \otimes_{G_{(o(e))^*}} v_e = g[e] \otimes_{G_{(t(e))^*}} v_{\overline{e}}$. This implies that $(o(e))^* = (t(e))^*$ and $[e] \in G_{(o(e))^*}$. If $e \in E(T)$ then $[e] = 1$ and the case $(o(e))^* = (t(e))^*$ implies that $o(e) = t(e)$. So e is a loop. This is impossible because X is a tree. So $e \notin E(T)$ and $[e] \in G_{(o(e))^*}$. This contradicts Proposition 2. If $g \in G$ and $e \in E(X_v)$ such that $t(g \otimes_{G_{(t(e))^*}} e) = o(g \otimes_{G_{(o(e))^*}} e)$, then $g \otimes_{G_{(t(e))^*}} t(e) = g \otimes_{G_{(o(e))^*}} o(e)$.

This implies that $t(e) = o(e)$. So e is a loop in X_v. This contradicts the fact that X_v is a tree. Let $g \in G$ and, u and v be two vertices of T. We need to show that the subtrees $1 \otimes_{G_u} X_u$ and $g \otimes_{G_v} X_v$ of $\widetilde{X}$ are joined by exactly one reduced path in $\widetilde{X}$. By Lemma 2.7 of [7], there exists a reduced word $w = g_0.y_1.g_1.....y_n.g_n$ of G such that $o(w) = u$, $t(w) = v$, and $[w] = g = g_0[y_1]g_1.....[y_n]g_n$. Then $(o(y_1))^* = u$, $(t(y_n))^* = v$, $g_0 \in G_u$, $g_i \in G_{(t(y_i))^*}$, $i = 1, \ldots, n$.

Furthermore, $(t(y_i))^* = (o(y_{i+1}))^*$, and, v_{y_i} and $v_{\overline{y}_{i+1}}$ are in $X_{(o(y_{i+1}))^*}$ for $i = 1, \ldots, n-1$. For $i = 1, \ldots, n$, let $[w_i] = g_0[y_1]g_1.....[y_{i-1}]g_{i-1}$ with convention that $[w_1] = g_0$, and let p_i be the edge $p_i = [[w_i]; y_i]$. Let P_i be the unique reduced path in $[w_{i+1}] \otimes_{G_{(o(y_{i+1}))^*}} X_{(o(y_{i+1}))^*}$ joining the vertices and $[w_{i+1}] \otimes_{G_{(o(y_{i+1}))^*}} v_{\overline{y}_i}$ and $[w_{i+1}] \otimes_{G_{(o(y_{i+1}))^*}} v_{y_{i+1}}$ induced by the unique reduced path in $X_{(o(y_{i+1}))^*}$ joining the vertices $v_{\overline{y}_i}$ and $v_{y_{i+1}}$ for $i = 1, \ldots, n-1$. Let P be the sequence of edges $P : p_1, P_1, p_2, P_2, ..., p_{n-1}, P_{n-1}, p_n$. We need to show that P is a unique reduced path in $\widetilde{X}$ joining the subtrees $1 \otimes_{G_u} X_u$ and $g \otimes_{G_v} X_v$.

$$
\begin{aligned}
o(p_1) &= o[[w_1]; y_1] = o[g_0; y_1] = g_0 \otimes_{G_{(o(y_1))^*}} v_{y_1} \in 1 \otimes_{G_u} X_u,\\
t(p_n) &= t[[w_n]; y_n] = [w_n][y_n] \otimes_{G_{(t(y_n))^*}} v_{\overline{y}_n} = [w_n][y_n]g_n \otimes_{G_{(t(y_n))^*}} v_{\overline{y}_n}\\
&= g \otimes_{G_v} v_{\overline{y}_n} \in g \otimes_{G_v} X_v.\\
t(p_i) &= t[[w_i]; y_i] = [w_i][y_i] \otimes_{G_{(t(y_i))^*}} v_{\overline{y}_i} = [w_i][y_i]g_i \otimes_{G_{(t(y_i))^*}} v_{\overline{y}_i}\\
&= [w_{i+1}] \otimes_{G_{(o(y_{i+1}))^*}} v_{\overline{y}_i} = o(p_i).t(p_i) = [w_{i+1}] \otimes_{G_{(o(y_{i+1}))^*}} v_{y_{i+1}}\\
&= o(p_{i+1}).
\end{aligned}
$$

Thus, P is a path in $\widetilde{X}$ joining the subtrees $1 \otimes_{G_u} X_u$ and $g \otimes_{G_v} X_v$. Now we show that P is reduced. Since the paths $p_1, p_2, ..., p_{n-1}$ are reduced and $Y \cap X_z = \phi$ for all $z \in V(T)$, we need to show that $p_{i+1} \neq \overline{p}_i$ for $i = 1, \ldots, n-1$. For if $p_{i+1} = \overline{p}_i$, then $[g_0[y_1]g_1.....[y_i]g_i; y_{i+1}] = [g_0[y_1]g_1.....[y_{i-1}]g_{i-1}; \overline{y}_i]$.

This implies that $g_i G_{+y_{i+1}} = G_{+(y_i)}$ and $+y_{i+1} = +(\overline{y}_i)$. So $g_i \in G_{+y_{i+1}}$.

This contradicts above that w is a reduced word of G. Hence P is a reduced path in $\widetilde{X}$ joining the vertices $1 \otimes_{G_{(o(y_1))^*}} v_{y_1}$ and $g \otimes_{G_v} v_{\overline{y}_i}$.

Now we show that P is unique.

Let $Q : q_1, Q_1, q_2, Q_2, ..., q_{m-1}, Q_{m-1}, q_m$ be a reduced path in $\widetilde{X}$ joining the vertices $1 \otimes_{G_{(o(y_1))^*}} v_{y_1}$ and $g \otimes_{G_v} v_{\overline{y}_i}$, where $q_j = [a_j; x_j]$, $a_j \in G$, $x_j \in E(Y)$, $j = 1, \ldots, m$, and Q_i is defined similarly as P_i above. We need to show that $Q = P$. We have $o[a_1; x_1] = 1 \otimes_{G_u} v_{y_1}$, $t[a_i; x_i] =$

$o[a_{i+1};x_{i+1}]$, $[a_{i+1};x_{i+1}] \neq \overline{[a_i;x_i]}$ for $i = 1,\ldots,n-1$, and $t[a_m;x_m] = g \otimes_{G_v} v_{\overline{y}_n}$. This implies that $a_1 \otimes_{G_{(o(x_1))^*}} v_{x_1} = 1 \otimes_{G_u} v_{y_1}$, $a_i[x_i] \otimes_{G_{(t(x_i))^*}} v_{\overline{x}_i} = a_{i+1} \otimes_{G_{(o(x_{i+1}))^*}} v_{x_{i+1}}$, $a_{i+1}G_{+x_{i+1}} \neq a_i[x_i]G_{+x_i}$ or $x_{i+1} \neq +\overline{x}_i$, and $a_m[x_m] \otimes_{G_{(t(x_m))^*}} v_{\overline{x}_m} = g \otimes_{G_v} v_{\overline{y}_n}$. Consequently $(o(x_1))^* = u$, $(t(x_i))^* = (o(x_{i+1}))^*$, $(t(x_m))^* = v$, $a_1 = h_0 \in G_u$, $a_{i+1} = a_i[x_i]h_i, h_i \in G_{(t(x_i))^*}$ and $g = a_m[x_m]h_m, h_m \in G_v$. We get the word $w\prime = h_0.x_1.h_1.\ldots.x_m.h_m$ such that $o(w\prime) = u, t(w\prime) = v$, and $[w\prime] = g$. $w\prime$ is reduced because $x_{i+1} \neq +\overline{x}_i$ or $h_i \notin G_{+x_i}$. By Proposition 3 we have $m = n$ and $[[w_i];y_i] = [[w\prime_i];x_i]$, $i = 1,\ldots,n-1$. So $Q = P$. Consequently $\widetilde{X}$ forms a tree. If G acts on X with inversions, then there exists $y \in E(Y)$ such that $G(y) = G(\overline{y})$ and $[y](y) = \overline{y}$. Then $+y = +\overline{y}$ and $\overline{[1;y]} = [[y];\overline{y}] = [y][1;y]$. So the element $[y]$ transfers the edge $[1;y]$ into its inverse $[[y];y]$. If $v \in V(T)$ and G_v acts on X_v with inversions, there exist $g \in G_v$ and $e \in E(X_v)$ such that $g(e) = \overline{e}$. The definition of $\otimes$ implies that $g \otimes_{G_v} e = 1 \otimes_{G_v} \overline{e}$. Then $g \otimes_{G_v} e = g(1 \otimes_{G_v} e) = 1 \otimes_{G_v} \overline{e} = \overline{1 \otimes_{G_v} e}$. Consequently, G acts on $\widetilde{X}$ with inversions. This completes the proof. □

Corollary 1. *Let G, X, and X_v, $v \in V(T)$ be as in Theorem 1. For each $e \in E(X)$, let G_e be finite and contains no inverter elements of $G_{t(e)}$. Then the conclusions of Theorem 1 hold. Moreover, the mapping $\mu : V(\widetilde{X}) \to V(X)$ given by $\mu(g \otimes_{G_v} w) = g(v)$, for all $w \in X_v$ is surjective, and is a G-map.*

Proof. Since G_e is finite and contains no inverter elements of $G_{t(e)}$, therefore by Lemma 1, there exists a vertex $w \in V(X_{t(e)})$ such that $G_e \leqslant (G_{t(e)})_w$. Then by Theorem 1, G acts on $\widetilde{X}$, and if G acts on X with inversions, or for some $v \in V(T)$, G_v acts on X_v with inversions, then G acts on $\widetilde{X}$ with inversions. Now if $f, g \in G$, and $u, w \in V(X_v)$ such that $f \otimes_{G_v} u = g \otimes_{G_v} w$, then $g^{-1}f \in G_v$. This implies that $g^{-1}f(v) = v$, or equivalently, $f(v) = g(v)$. Then $\mu(f \otimes_{G_v} u) = \mu(g \otimes_{G_v} w)$, and μ is well-defined. If $v \in V(X)$, and $u \in V(X_v)$, then it is clear that $\mu(1 \otimes_{G_v} u) = v$. So μ is surjective. If $f, g \in G$, $v \in V(X)$ and $u \in V(X_v)$, then $\mu(f(g \otimes_{G_v} u)) = \mu(fg \otimes_{G_v} u) = fg(v) = f(\mu(g \otimes_{G_v} u))$. This implies that μ is surjective, and is a G-map. This completes the proof. □

Corollary 2. *Let G, X, and X_v, $v \in V(T)$ be as in Corollary 1. If the stabilizer of each edge of X_v is finite, then the stabilizer of each edge of $\widetilde{X}$ is finite.*

Proof. $E(\widetilde{X}) = \widehat{X} \cup (\underset{v \in V(T)}{\cup}(G \otimes_{G_v} E(X_v)))$. Let $g \in G$, $v \in V(T), p \in E(X_v)$, and $e \in E(Y)$. It is clear that the stabilizer $G_{g \otimes_{G_v} p}$ of the edge

$g \otimes_{G_v} p$ under the action of G on $\widetilde{X}$ is $G_{g\otimes_{G_v} p} = g(G_v)_p g^{-1}$, where $(G_v)_p$ is the stabilizer of the edge p under the action of G_v on X_v. Since $(G_v)_p$ is finite, therefore $G_{g\otimes_{G_v} p}$ is finite. Similarly, that the stabilizer $G_{[g;e]}$ of the edge $[g;e]$ under the action of G on $\widetilde{X}$ is $G_{[g;e]} = gG_{+e}g^{-1}$. This completes the proof. □

Now we end this section the following definition.

Definition 8. Let G be a group acting on a tree X and $(T;Y)$ be a fundamental domain for the action of G on X. For each $v \in V(T)$, let X_v be a tree on which G_v acts, and for each $e \in E(Y)$, let G_e be finite and contains no inverter elements of $G_{t(e)}$. Then $\widetilde{X}$ is called a fibered G-tree of base X and fibers X_v, $v \in V(T)$.

3. Accessibility of groups acting on trees

For the study of the concepts of the ends of groups we refer the readers to ([1], p. 17), or ([2], p. 124, 126), or ([11], p. 171).

The number of the ends of a group G is denoted by $e(G)$.

A finitely generated group G is called accessible on the tree X if G acts on X and satisfies the following.

1. $X^G = \phi$,
2. G_e is finite for any $e \in E(X)$,
3. $e(G_v) \leqslant 1$ for all $v \in V(X)$.

A group is G called accessible if there exists a tree X on which G is accessible on X.

If G is an accessible group on the tree X, then by Proposition 7.4 ([2], p. 132), there exists a tree X' such that G acts on X' and G is not accessible on X'. In this case we say that G is inaccessible.

The main result of this section is the following theorem.

Theorem 2. *Let G be a group acting on the tree X such that for each edge e of X, G_e is finite and contains no elements of $G_{t(e)}$, and for each vertex v of X, G_v is an accessible, and the quotient graph G/X is finite. Then G is an accessible group, and G is inaccessible on X.*

Proof. The accessibility of G_v, $v \in V(X)$ implies that G_v is finitely generated. Since the quotient graph G/X is finite, therefore similar to the proof of Theorem 4.1 of [2, p. 15], we can show that G is finitely generated. Let $(T;Y)$ be a fundamental domain for the action of G on X. Then there exists a tree X_v on which G_v acts such that $X_v^{G_v} = \phi$,

$(G_v)_y$ is finite for every $y \in E(X_v)$, and $e(G_v) \leqslant 1$. The condition G_e is finite and contains no inverter elements of $G_{t(e)}$, $e \in E(Y)$ implies that G acts on the fiber tree $\widetilde{X}$. If $g \in G$ and $u \in V(X_v)$ such that $G_{g\otimes_{G_v} u} = g(G_v)_u g^{-1} = G$, then $(G_v)_u = G_v$. This contradicts the condition that $X_v^{G_v} = \phi$. So $\widetilde{X}^G = \phi$. If $e \in E(Y)$ and $p \in E(X_v), v \in V(X)$, then G_e and $(G_v)_p$ are finite. Then for every $g \in G$, $G_{[g;e]} = gG_{+e}g^{-1}$ and $G_{g\otimes_{G_v} p} = g(G_v)_p g^{-1}$ are finite. For $g \in G$, $v \in V(T)$ and $u \in V(X_v)$, $e(G_{g\otimes u}) = e(g(G_v)_u g^{-1}) = e((G_v)_u) \leqslant 1$. This implies that G is accessible on $\widetilde{X}$. Consequently G is accessible. If G is accessible on X, then for every $v \in V(T)$, $e(G_v) \leqslant 1$. Since G_v is accessible, then by Theorem 6.10 of ([2], p. 128), $e(G_v) \geqslant 2$. Contradiction. So G is inaccessible on X. This completes the proof. $\square$

Now we apply Theorem 2 to tree product of groups $A = \prod^*_{i\in I}(A_i; U_{ij} = U_{ji})$ of the groups A_i, $i \in I$, with amalgamation subgroups U_{ij}, $i, j \in I$ introduced in [3], and to a new class of groups called quasi-HNN groups introduced in [4], and defined as follows.

Let G be a group, I and J be two indexed sets such that $I \cap J = \phi$ and $I \cup J \neq \phi$. Let $\{A_i : i \in I\}$, $\{B_i : i \in I\}$, and $\{C_j : j \in J\}$ be families of subgroups of G. For each $i \in I$, let $\phi_i : A_i \to B_i$ be an onto isomorphism and for each $j \in J$, let $\alpha_j : C_j \to C_j$ be an automorphism such that α_j^2 is an inner automorphism determined by $c_j \in C$ and c_j is fixed by α_j; that is, $\alpha_j(c_j) = c_j$ and $\alpha_j^2(c) = c_j c c_j^{-1}$ for all $c \in C_j$.

The group G^* of the presentation

$$\Big\langle gen(G), t_i, t_j \mid rel(G), t_i a t_i^{-1} = \phi_i(a),\ t_j c t_j^{-1} = \alpha_j(c), \\ t_j^2 = c_j,\ a \in A_i,\ c \in C_j \Big\rangle,$$

where $i \in I, j \in J$, or simply,

$$G^* = \Big\langle gen(G), t_i, t_j \mid rel(G), t_i A_i t_i^{-1} = B_i,\ t_j C_j t_j^{-1} = C_j, \\ t_j^2 = c_i,\ i \in I, j \in J \Big\rangle$$

is called a quasi HNN group of base H and associated pairs (A_i, B_i), and (C_j, C_j) of subgroups of G.

The tree product $A = \prod^*_{i\in I}(A_i; U_{ij} = U_{ji})$ of the groups $A_i, i \in I$, acts on the tree X without inversions defined as follow.

$$V(X) = \{(gA_i, i) : g \in A, i \in I\}, \\ \text{and } E(X) = \{(gU_{ij}, ij) : g \in A, i, j \in I\}.$$

If y is the edge $y = (gU_{ij}, ij)$, then $o(y) = (gA_i, i), t(y) = (gA_j, j)$, and $\overline{y} = (gU_{ji}, ji)$. A acts on X as follows.

Let $f \in A$. Then $f((gA_i, i)) = (fgA_i, i)$ and $f((gU_{ij}, ij)) = (fgU_{ij}, ij)$.

If $v = (gA_i, i) \in V(X)$ and $y = (gU_{ji}, ij) \in E(X)$, then the stabilizer of v is $A_v = gA_i g^{-1} \cong A_i$, a conjugate of A_i, and then the stabilizer of y is $A_y = gU_{ij}g^{-1} \cong U_{ij}$, a conjugate of U_{ij}. The orbit of v is $A(v) = \{(agA_i, i) : a \in A, i \in I\}$, and the orbit of y is $A(y) = \{(agU_{ij}, ij) : a \in A, i, j \in I\}$.

So the quotient graph A/X is finite if I is finite. This leads the following proposition as an application to Theorem 2.

Proposition 4. *Let $A = \prod^*_{i \in I}(A_i; U_{ij} = U_{ji})$ be a tree product of the groups A_i, $i \in I$, such that A_i is accessible, and U_{ij} is finite and contains no inverter element of A_i for all i, $j \in I$. If I is finite, then A is accessible.*

A free product of groups with amalgamated subgroup is a special case of tree product of the groups, we state the following corollary of Proposition 4.

Corollary 3. *Let $A = *_c A_i$, $i \in I$, be the free product of the groups A_i, $i \in I$ with amalgamation subgroup C such that A_i is accessible, and C is finite and contains no inverter element of A_i for all $i, j \in I$. If I is finite, then A is accessible.*

It is shown in [6] that the quasi-HNN group

$$G^* = \Big\langle gen(G), t_i, t_j \mid rel(G), t_i A_i t_i^{-1} = B_i,\ t_j C_j t_j^{-1} = C_j,$$
$$t_j^2 = c_i,\ i \in I, j \in J \Big\rangle$$

acts on the tree X with inversions defined as follow.

$$V(X) = \{gG : g \in G^*\},\ \text{and}\ E(X) = \{(gB_i, t_i), (gA_i, t_i), (gC_j, t_j)\},$$

where $g \in G^*, i \in I$,and $j \in J$. For the edges $(gB_i,\ t_i), (gA_i, t_i)$, and (gC_j, t_j), $i \in I, j \in J$, define $o(gB_i,\ t_i) = o(gA_i, t_i) = o(gC_j, t_j) = gG$, $t(gB_i, t_i) = gt_iG, t(gA_i, t_i) = gt_i^{-1}G$, and $t(gC_j, t_j) = gt_jG$, and $\overline{(gB_i, t_i)} = (gt_iA_i, t_i^{-1})$, $\overline{(gA_i, t_i^{-1})} = (gt_i^{-1}B_i, t_i)$, and $\overline{(gC_j, t_j)} = (gt_jC_j, t_j)$.

G^* acts on X as follows. Let $f \in G^*$. Then for the vertex gG and the edges $(gB_i,\ t_i), (gA_i, t_i^{-1})$, and (gC_j, t_j) of X, define $f(gG) = fgG$, $f(gB_i, t_i) = (fgB_i, t_i)$, $f(gA_i, t_i^{-1}) = (fgA_i, t_i^{-1})$, and $f(gC_j, t_j) = (fgC_j, t_j)$.

The action of G^* on X is with inversions because the element $t_j \in G^*$ maps the edge (C_j, t_j) to its inverse $\overline{(C_j, t_j)}$; that is, $t_j(C_j, t_j) = (t_jC_j, t_j) = \overline{(C_j, t_j)}$

The stabilizer of the vertex $v = gG$ is, $G^*_v = gGg^{-1}$, a conjugate of G, the stabilizers of the edges (gB_i, t_i), $f(gA_i, t_i^{-1})$, and (gC_j, t_j) are gB_ig^{-1}, conjugates of B_i, gA_ig^{-1}, a conjugate of A_i, and gC_jg^{-1}, a conjugate of C_j respectively, for all $i \in I$, and all $j \in J$.

The orbits of gG, (gB_i, t_i), $f(gA_i, t_i^{-1})$, and (gC_j, t_j) are $\{fG : f \in G^*\}$, $\{(fB_i, t_i) : f \in G^*\}$, and $\{(fC_j, t_j) : f \in G^*\}$. Then the quotient graph $G^* \diagup X$ is finite if $I \cup J$ is finite. This leads the following proposition as an application to Theorem 2.

Proposition 5. *Let G^* be the quasi-HNN group*

$$G^* = \Big\langle gen(G), t_i, t_j \mid rel(G),\, t_iA_it_i^{-1} = B_i,\, t_jC_jt_j^{-1} = C_j,\\ t_j^2 = c_i,\, i \in I, j \in J \Big\rangle$$

such that G is accessible, A_i, B_i, and C_j are finite and contain no inverter elements of G. If $I \cup J$ is finite, then G^* is accessible.

By taking $J = \phi$ in the group G^* defined above, yields the the following corollary of Proposition 5.

Corollary 4. *Let G^* be the HNN group*

$$G^* = \Big\langle gen(G), t_i \mid rel(G), t_iA_it_i^{-1} = B_i,\ i \in I \Big\rangle$$

such that G is accessible, A_i, and B_i are finite and contain no inverter elements of G. If I is finite, then G^* is accessible.

References

[1] D. E. Cohen, *Groups of cohomological dimension one*, Springer Lecture Notes 245, 1972.

[2] W. Dicks and M. J. Dunwoody, *Groups acting on graphs*, Cambridge University Press, 1989.

[3] A. Karrass and D. Solitar, *The subgroups of a free product of two groups with an amalgamated subgroup*, Trans. Amer. Math. Soc., 150, 1970, pp.227-255.

[4] M. I. Khanfar and R. M. S. Mahmood, *On quasi HNN groups*, Kuwait J. Sci. Engrg. 29, 2002, no.2, pp.13-24.

[5] M. I. Khanfar and R. M. S. Mahmud, *A note on groups acting on connected graphs*, J. Univ. Kuwait Sci. 16, 1989, no.2, pp.205-208.

[6] R. M. S. Mahmood and M. I. Khanfar, *On invertor elements and finitely generated subgroups of groups acting on trees with inversions.* Int. J. Math. Math. Sci. 23, 2000, no.9, pp.585-595.

[7] R. M. S. Mahmood and M. I. Khanfar, *Subgroups of quasi-HNN groups*, Int. J. Math. Math. Sci. 31, 2002, no.12, pp.731-743.

[8] R. M. S. Mahmud, *The normal form theorem of groups acting on trees with inversions.* J. Univ. Kuwait Sci. 18, 1991, pp.7-16.

[9] R. M. S. Mahmud, *Presentation of groups acting on trees with inversions*, Proc. R. Soc. Edinb., Sect. A, 113, 1989, no.3-4, pp.235-241.

[10] J-P. Serre, Trees, *Translated by John Stillwell*, Springer-Verlag, 1980.

[11] C. T. C. Wall, *Homological Group Theory, London Mathematical Society*, Lecture Notes Series, vol.36, Cambridge University Press, Cambridge, 1979.

Contact information

R. M. S. Mahmood Department of Mathematics,
Irbid National University,
P. O. Box 2600, Irbid, Jordan.
E-Mail(s): rasheedmsm@yahoo.com

Received by the editors: 16.04.2013
and in final form 07.11.2014.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 243–253 RESEARCH ARTICLE

On various parameters of $\mathbb{Z}_q$-simplex codes for an even integer q

P. Chella Pandian* **and C. Durairajan****

Communicated by V. Artamonov

Abstract. In this paper, we defined the $\mathbb{Z}_q$-linear codes and discussed its various parameters. We constructed $\mathbb{Z}_q$-Simplex code and $\mathbb{Z}_q$-MacDonald code and found its parameters. We have given a lower and an upper bounds of its covering radius for q is an even integer.

1. Introduction

A code C is a subset of $\mathbb{Z}_q^n$, where $\mathbb{Z}_q$ is the set of integer modulo q and n is any positive integer. Let $x, y \in \mathbb{Z}_q^n$, then the distance between x and y is the number of coordinates in which they differ. It is denoted by $d(x, y)$. Clearly $d(x, y) = wt(x - y)$, the number of non-zero coordinates in $x - y$. wt(x) is called *weight of x*. The minimum distance d of C is defined by

$$d = \min\{d(x, y) \ \mid x, y \in C \textit{ and } x \neq y\}.$$

The minimum weight of C is $\min\{wt(c) \mid c \in C$ and $c \neq 0\}$. A code of length n cardinality M with minimum distance d over $\mathbb{Z}_q$ is called $(n, M, d)q$-ary code. For basic results on coding theory, we refer [16].

*The first author would like to gratefully acknowledge the UGC-RGNF[Rajiv Gandhi National Fellowship], New Delhi for providing fellowship.
**The second author was supported by a grant(SR/S4/MS:588/09) for the Department of Science and Technology, New Delhi.
2010 MSC: 94B05, 11H31.
Key words and phrases: codes over finite rings, $\mathbb{Z}_q$-linear code, $\mathbb{Z}_q$-simplex code, $\mathbb{Z}_q$-MacDonald code, covering radius.

We know that $\mathbb{Z}_q$ is a group under addition modulo q. Then $\mathbb{Z}_q^n$ is a group under coordinatewise addition modulo q. A subset C of $\mathbb{Z}_q^n$ is said to be a *q-ary code*. If C is a subgroup of $\mathbb{Z}_q^n$, then C is called a *$\mathbb{Z}_q$-linear code*. Some authors are called this code as *modular code* because $\mathbb{Z}_q^n$ is a module over the ring $\mathbb{Z}_q$. In fact, it is a free $\mathbb{Z}_q$-module. Since $\mathbb{Z}_q^n$ is a free $\mathbb{Z}_q$-module, it has a basis. Therefore, every $\mathbb{Z}_q$-linear code has a basis. Since $\mathbb{Z}_q$ is finite, it is finite dimension.

Every k dimension $\mathbb{Z}_q$-linear code with length n and minimum distance d is called $[n, k, d]$ *$\mathbb{Z}_q$-linear code*. A matrix whose rows are a basis elements of the $\mathbb{Z}_q$-linear code is called a *generator matrix* of C. There are many researchers doing research on code over finite rings [4, 9–11, 13, 14, 18]. In the last decade, there are many researchers doing research on codes over $\mathbb{Z}_4$ [1–3, 8, 15].

In this correspondence, we concentrate on code over $\mathbb{Z}_q$ where q is even. We constructed some new codes and obtained its various parameters and its covering radius. In particular, we defined $\mathbb{Z}_q$-Simplex code, $\mathbb{Z}_q$-MacDonald code and studied its various parameters. Section 2 contains basic results for the $\mathbb{Z}_q$-linear codes and we constructed some $\mathbb{Z}_q$-linear code and given its parameters. $\mathbb{Z}_q$-Simplex code is given in section 3 and finally, section 4 we determined the covering radius of these codes and $\mathbb{Z}_q$-MacDonald code.

2. $\mathbb{Z}_q$-linear code

Let C be a $\mathbb{Z}_q$-linear code. If $x, y \in C$, then $x - y \in C$. Let us consider the minimum distance of C is $d = \min\{d(x, y) \mid x, y \in C \text{ and } x \neq y\}$. Then

$$d = \min\{wt(x - y) \mid x, y \in C \text{ and } x \neq y\}.$$

Since C is $\mathbb{Z}_q$-linear code and $x, y \in C$, $x - y \in C$. Since $x \neq y$,

$$\min\{wt(x - y) \mid x, y \in C \ \text{ and } x \neq y\} = \min\{wt(c) \mid c \in C \ \text{ and } c \neq 0\}.$$

Thus, we have

Lemma 1. *In a $\mathbb{Z}_q$-linear code, the minimum distance is the same as the minimum weight.*

Let q be an even integer and let $x, y \in \mathbb{Z}_q^n$ such that $x_i, y_i \in \{0, \frac{q}{2}\}$, then $x_i \pm y_i \in \{0, \frac{q}{2}\}$.

Lemma 2. *Let q be an integer even. If $x, y \in \mathbb{Z}_q^n$ such that $x_i, y_i \in \{0, \frac{q}{2}\}$, then the coordinates of $x \pm y$ are either 0 or $\frac{q}{2}$.*

Now, we construct a new code and discuss its parameters. Let C be an [n, k, d] $\mathbb{Z}_q$-linear code. Define

$$D = \{(c0c\cdots c)+\alpha(\mathbf{0112\cdots q-1}) \mid \alpha \in \mathbb{Z}_q, c \in C \text{ and } \mathbf{i} = ii\cdots i \in \mathbb{Z}_q^n\}.$$

Then, $D = \{c0c\cdots c, c0c\cdots c+\mathbf{0112\cdots q-1}, c0c\cdots c+2(\mathbf{0112\cdots q-1})$ $,\cdots, c0c\cdots c+(q-1)(\mathbf{0112\cdots q-1}) \mid c \in C$ and $\mathbf{i} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}\}$. Since any $\mathbb{Z}_q$-linear combination of D is again an element in D, therefore the minimum distance of D is $d(D) = \min\{wt(c0c\cdots c), wt(c0c\cdots c+\mathbf{0112\cdots q-1}),$ $wt(c0c\cdots c+2(\mathbf{0112\cdots q-1})), \cdots, wt(c0c\cdots c+(q-1)(\mathbf{0112\cdots q-1}))$ $\mid c \in C$ and $\mathbf{i} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}\}$.

Clearly $\min\{wt(c0c\cdots c) \mid c \in C \& c \neq 0\} \geqslant qd$.

Let $c \in C$. Let us take c has r_i $i's$ where $i = 0, 1, 2, \cdots, q-1$. Then for $1 \leqslant i \leqslant q-1$,

$$wt(c+\mathbf{i}) = \sum_{j=0}^{q-1} r_j - r_{q-i}.$$

That is $wt(c+\mathbf{i}) = n - r_{q-i}$. Therefore

$$\begin{aligned} &wt(c0c\cdots c+\mathbf{0112\cdots q-1}) \\ &\qquad = wt(c+\mathbf{0}) + 1 + wt(c+\mathbf{1}) + wt(c+\mathbf{2}) + \cdots + wt(c+\mathbf{q-1}) \\ &\qquad = n - r_0 + 1 + n - r_{q-1} + n - r_{q-2} + \cdots + n - r_1 \\ &\qquad = (q-1)n + 1. \end{aligned}$$

Similarly, for every integer i which is relatively prime to q

$$wt((c0c\cdots c) + i(\mathbf{0112\cdots q-1})) \quad = \quad (q-1)n+1.$$

For other i's

$$\begin{aligned} &\min_{i\in\mathbb{Z}_q}\{wt(c0c\cdots c+i(\mathbf{0112\cdots q-1}))\} \\ &\qquad = wt(c+\mathbf{0}) + 1 + wt(c\cdots c + \frac{q}{2}(\mathbf{12\cdots q-1})) \\ &\qquad = wt(c+\mathbf{0}) + 1 + wt(c\cdots c + (\frac{\mathbf{q}}{\mathbf{2}}\mathbf{0}\frac{\mathbf{q}}{\mathbf{2}}\mathbf{0}\cdots\frac{\mathbf{q}}{\mathbf{2}}\mathbf{0}\frac{\mathbf{q}}{\mathbf{2}})) \\ &\qquad = \frac{q}{2}wt(c+\mathbf{0}) + 1 + \frac{q}{2}wt(c+\frac{\mathbf{q}}{\mathbf{2}}) \\ &\qquad = \frac{q}{2}(n-r_0) + 1 + \frac{q}{2}(n - r_{\frac{q}{2}}) \\ &\qquad = \frac{q}{2}n + 1 + \frac{q}{2}(n - r_0 - r_{\frac{q}{2}}). \end{aligned}$$

Hence, $d(D) = \min\{qd, (q-1)n+1, \frac{q}{2}n + 1 + \frac{q}{2}(n - r_0 - r_{\frac{q}{2}})\}$. Thus, we have

Theorem 1. *Let C be an $[n, k, d]$ $\mathbb{Z}_q$-linear code, then the*

$$D = \{c0c \cdots c + \alpha(\mathbf{0112} \cdots \mathbf{q-1}) \mid \alpha \in \mathbb{Z}_q, c \in C \textit{ and } \mathbf{i} = ii \cdots i \in \mathbb{Z}_q^n\}$$

is a $[qn+1, k+1, d(D)]$ $\mathbb{Z}_q$-linear code.

If there is a codeword $c \in C$ such that it has only 0 and $\frac{q}{2}$ as coordinates, then

$$\begin{aligned} wt(c0c \cdots c + \mathbf{0}\frac{\mathbf{q}}{\mathbf{2}}\frac{\mathbf{q}}{\mathbf{2}}\mathbf{0}\frac{\mathbf{q}}{\mathbf{2}} \cdots \mathbf{0}\frac{\mathbf{q}}{\mathbf{2}}) & \\ &= wt(c+0) + 1 + wt(c+\frac{q}{2}) + wt(c+0) + \cdots + w(c+\frac{q}{2}) \\ &= 1 + r_{\frac{q}{2}} + r_0 + r_{\frac{q}{2}} + \cdots + r_0 \\ &= \frac{q}{2}(r_0 + r_{\frac{q}{2}}) + 1 = \frac{q}{2}n + 1. \end{aligned}$$

Hence, $d(D) = \min\{qd, \frac{q}{2}n + 1\}$. Thus, we have

Corollary 1. *If there is a codeword $c \in C$ such that $c_i = 0$ or $\frac{q}{2}$ and if $n \leqslant 2d - 1$, then $d(D) = \frac{q}{2}n + 1$.*

3. $\mathbb{Z}_q$-simplex codes

Let G be a matrix over $\mathbb{Z}_q$ whose columns are one non-zero element from each 1-dimensional submodule of $\mathbb{Z}_q^2$. Then this matrix is equivalent to

$$G_2 = \left[\begin{array}{c|c|cccc} 0 & 1 & 1 & 2 & \cdots & q-1 \\ \hline 1 & 0 & 1 & 1 & \cdots & 1 \end{array}\right].$$

Clearly G_2 generates $[q+1, 2, \frac{q}{2}+1]$ code. Inductively, we define

$$G_{k+1} = \left[\begin{array}{c|c|c|c|c|c} 00\cdots 0 & 1 & 11\cdots 1 & 22\cdots 2 & \cdots & q-1q-1\cdots q-1 \\ \hline & 0 & & & & \\ G_k & \vdots & G_k & G_k & \cdots & G_k \\ & 0 & & & & \end{array}\right]$$

for $k \geqslant 2$. Clearly this G_{k+1} matrix generates $[n_{k+1} = \frac{q^{k+1}-1}{q-1},\ k+1,\ d]$ code. We call this code as $\mathbb{Z}_q$-*Simplex code.* This type of k-dimensional code is denoted by $S_k(q)$. For simplicity, we denote it by S_k.

Theorem 2. *$S_k(q)$ is an $[n_k = \frac{q^k-1}{q-1},\ k,\ \frac{q}{2}n_{k-1} + 1]$ $\mathbb{Z}_q$-linear code.*

Proof. We prove this theorem by induction on k. For $k = 2$, from the generator matrix G_2, it is clear that $d = \frac{q}{2}+1$ and the theorem is true. Since there is a codeword $c = 0\frac{q}{2}\frac{q}{2}0\frac{q}{2}\cdots 0\frac{q}{2}0\frac{q}{2} \in S_2$ and $n = q+1 \leqslant 2(\frac{q}{2}+1)-1 = 2d-1$, by Corollary 1 implies $d(S_3) = \frac{q}{2}n_2 + 1$ and hence the S_3 is $[n_3 = \frac{q^3-1}{q-1}, 3, \frac{q}{2}n_2+1]$ code. Since $c0c\cdots c+\frac{q}{2}(\mathbf{0112\cdots q-1}) \in S_3$ whose coordinates are either 0 or $\frac{q}{2}$ and satisfies the conditions of the Corollary 1, therefore $d(S_4) = \frac{q}{2}n_3+1$ and hence the S_4 is $[n_4 = \frac{q^4-1}{q-1}, 4, \frac{q}{2}n_3+1]$ code. By induction we can assume that this theorem is true for all less than k. That is, there is a code $c \in S_{k-1}$ whose coordinates are either 0 or $\frac{q}{2}$ and $n_{k-1} \leqslant 2d_{k-1} - 1$. By Corollary 1, $d_k = \frac{q}{2}n_{k-1} + 1$. Therefore $S_k(q)$ is an $[\frac{q^k-1}{q-1},\ k,\ \frac{q}{2}n_{k-1} + 1]$ $\mathbb{Z}_q$-linear code. Thus we proved. □

Now, we are going to see the minimum distance of the dual code of this $\mathbb{Z}_q$-Simplex code. Since the matrix $G_k(q)$ has no zero columns, therefore, the minimum distance of its dual is greater than or equal to 2. Since in the first block of the matrix G_k, there are two columns whose transpose matrices are $(0, 0, \cdots, 0, 1, 1)$ and $(0, 0, \cdots, 0, a, 1)$. Since addition and multiplications are modulo q and q is even, $\frac{q}{2}(0, 0, \cdots, 0, 1, 1) + \frac{q}{2}(0, 0, \cdots, 0, q-1, 1) = 0$. That is, there are two linearly dependent columns. Therefore, the minimum distance of the dual code is less than or equal to 2. Hence the dual of S_k is $[n_k = \frac{q^k-1}{q-1}, n_k - k, 2]$ $\mathbb{Z}_q$-linear code.

4. Covering radius

The *covering radius* of a code C over $\mathbb{Z}_q$ with respect to the Hamming distance d is given by

$$R(C) = \max_{u\in\mathbb{Z}_q^n}\left\{\min_{c\in C}\{d(u,c)\}\right\}.$$

It is easy to see that $R(C)$ is the least positive integer r such that

$$\mathbb{Z}_q^n = \cup_{c\in C} S_r(c)$$

where

$$S_r(u) = \left\{v \in \mathbb{Z}_q^n\} \mid d(u,v) \leqslant r\right\}$$

for any $u \in \mathbb{Z}_q^n$.

Proposition 1 ([5]). *If appending(puncturing) r number of columns in a code C, then the covering radius of C is increased(decreased) by r.*

Proposition 2 ([17]). *If C_0 and C_1 are codes over $\mathbb{Z}_q^n$ generated by matrices G_0 and G_1 respectively and if C is the code generated by*

$$G = \left(\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array}\right),$$

then $r(C) \leqslant r(C_0) + r(C_1)$ and the covering radius of C satisfy the following

$$r(C) \geqslant r(C_0) + r(C_1).$$

Since the covering radius of C generated by

$$G = \left(\begin{array}{c|c} 0 & G_1 \\ \hline G_0 & A \end{array}\right),$$

is greater than or equal to $r(C_0) + r(C')$ where C_0 and C' are codes generated by $\left[\begin{array}{c} 0 \\ \hline G_0 \end{array}\right] = \left[\begin{array}{c} G_0 \end{array}\right]$ and $\left[\begin{array}{c} G_1 \\ \hline A \end{array}\right]$, respectively, this implies $r(C) \geqslant r(C_0) + r(C_1)$ because C_1 is a subcode of the code C'.

A q-ary repetition code C over a finite field $\mathbb{F}_q$ with q elements is an $[n, 1, n]$ linear code. The covering radius of C is $\left\lfloor \frac{n(q-1)}{q} \right\rfloor$ [12]. For basic results on covering radius, we refer to [5], [6]. Now, we consider the repetition code over $\mathbb{Z}_q$. There are two types of repetition codes.

Type I. Unit repetition code generated by $G_u = [\overbrace{uu\ldots u}^{n}]$ where u is an unit element of $\mathbb{Z}_q$. This matrix generates C_u is $[n, 1, n]$ $\mathbb{Z}_q$-linear code. That is, C_u is (n, q, n) q-ary repetition code. We call this as *unit repetition code.*

Type II. Zero divisor repetition code is generated by the matrix $G_v = [\overbrace{vv\ldots v}^{n}]$ where v is a zero divisor in $\mathbb{Z}_q$. That is, v is not a relatively prime to q. This is an $(n, \frac{q}{v}, n)$ code over $\mathbb{Z}_q$. This code is denoted by C_v. This code is called *zero divisor repetition code.*

With respect to the Hamming distance the covering radius of C_u is $\left\lfloor \frac{n(q-1)}{q} \right\rfloor$ [12] but clearly the covering radius of C_v is n because code symbols appear in this code are zero divisors only. Thus, we have

Theorem 3. *$R(C_v) = n$ and $R(C_u) = \left\lfloor \frac{(q-1)n}{q} \right\rfloor$.*

Let $\phi(q) = \#\{i \mid 1 \leqslant i < q \;\&\; (i, q) = 1\}$ be the Euler ϕ-function. Let $U = \{i \in \mathbb{Z} \mid 1 \leqslant i < q \;\&\; (i, q) = 1\}$ be the set of all units in $\mathbb{Z}_q$ and let

$O = \mathbb{Z}_q \setminus U$ be the set which contains all zero divisors and 0. Let C be a $\mathbb{Z}_q$-linear code generated by the matrix

$$[\overbrace{11\dots1}^{n}\overbrace{22\dots2}^{n}\cdots\overbrace{q-1q-1\dots q-1}^{n}],$$

then this code is equivalent to a code whose generator matrix is

$$[u_1u_1\cdots u_1u_2u_2\cdots u_2\cdots u_{\phi(q)}u_{\phi(q)}\cdots u_{\phi(q)}o_1o_1\cdots o_1o_2o_2\cdots o_2\cdots o_ro_r\cdots o_r]$$

where $r = q-1-\phi(q)$. Let A be a code equivalent to the unit repetition code of length $\phi(q)n$ generated by $[u_1u_1\cdots u_1u_2u_2\cdots u_2\cdots u_{\phi(q)}u_{\phi(q)}\cdots u_{\phi(q)}]$, then by the above theorem, $R(A) = \left\lfloor \frac{(q-1)\phi(q)n}{q} \right\rfloor$. Let B be a code equivalent to the zero divisor repetition code of length $(q-1-\phi(q))n$ generated by $[o_1o_1\cdots o_1o_2o_2\cdots o_2\cdots o_ro_r\cdots o_r]$, then by the above theorem, $R(B) = (q-1-\phi(q))n$. By Proposition 2, $R(C) \geqslant \left\lfloor \frac{(q-1)\phi(q)n}{q} \right\rfloor + (q-1-\phi(q))n$.

Without loss of generality we can assume that the generator matrix of A as $[111\cdots1]$. Since $R(A) = \left\lfloor \frac{(q-1)\phi(q)n}{q} \right\rfloor$ and C is obtained by appending some $(q-1-\phi(q))n$ columns to A, by Proposition 1 the covering radius of C is increased by at most $(q-1-\phi(q))n$. Therefore, $R(C) \leqslant \left\lfloor \frac{(q-1)\phi(q)n}{q} \right\rfloor + (q-1-\phi(q))n$. Thus, we have

Theorem 4. *Let C be a $\mathbb{Z}_q$-linear code generated by the matrix*

$$[\overbrace{11\dots1}^{n}\ \overbrace{22\dots2}^{n}\cdots\overbrace{q-1q-1\dots q-1}^{n}].$$

Then C is a $[(q-1)n, 1, \frac{q}{2}n]$ $\mathbb{Z}_q$-linear code with $R(C) = \left\lfloor \frac{(q-1)\phi(q)n}{q} \right\rfloor + (q-1-\phi(q))n$.

Now, we see the covering radius of $\mathbb{Z}_q$-Simplex code. The covering radius of Simplex codes and MacDonald codes over finite field and finite rings were discussed in [12], [14].

Theorem 5. *For $k \geqslant 2$,*

$$R(S_{k+1}) \leqslant \frac{(k-1)(q-1)\phi(q) + (q^2-q-\phi(q))(q^{k+1}-q^2)}{q(q-1)^2} + R(S_2).$$

Proof. For $k \geqslant 2$, S_{k+1} is $[n_{k+1} = \frac{q^{k+1}-1}{q-1}, k+1, \frac{q}{2}n_k + 1]$ $\mathbb{Z}_q$-linear code. By Proposition 2 and Theorem 4 give

$$R(S_{k+1}) \leqslant (1 + \left\lfloor \frac{(q-1)\phi(q)n_k}{q} \right\rfloor + (q-1-\phi(q))n_k) + R(S_k)$$

$$\begin{aligned}
&\leqslant (1+\frac{(q-1)\phi(q)n_k}{q}+(q-1-\phi(q))n_k)+R(S_k)\\
&\leqslant \left(1+\frac{q^2-q-\phi(q)}{q}n_k\right)+R(S_k).
\end{aligned}$$

This implies

$$R(S_k)\leqslant (1+\frac{q^2-q-\phi(q)}{q}n_{k-1})+R(S_{k-1}).$$

Combining these two, we get

$$R(S_{k+1})\leqslant (1+\frac{q^2-q-\phi(q)}{q}n_k)+(1+\frac{q^2-q-\phi(q)}{q}n_{k-1})+R(S_{k-1})$$

Similarly, if we continue, we get

$$\begin{aligned}
R(S_{k+1})\leqslant{}& (1+\frac{q^2-q-\phi(q)}{q}n_k)+(1+\frac{q^2-q-\phi(q)}{q}n_{k-1})+\cdots\\
&+(1+\frac{q^2-q-\phi(q)}{q}n_2)+R(S_2).
\end{aligned}$$

Since $n_k=\frac{q^k-1}{q-1}$, for $k\geqslant 2$, therefore

$$\begin{aligned}
R(S_{k+1})&\leqslant (k-1)+\frac{q^2-q-\phi(q)}{q}\left(\frac{q^k-1}{q-1}+\frac{q^{k-1}-1}{q-1}+\cdots+\frac{q^2-1}{q-1}\right)+R(S_2)\\
&\leqslant (k-1)+\frac{q^2-q-\phi(q)}{q}\left(\frac{q^k+q^{k-1}+\cdots+q^2-(k-1)}{q-1}\right)+R(S_2)\\
&\leqslant \frac{(k-1)\phi(q)+(q^2-q-\phi(q))((q^{k+1}-1)/(q-1)-(q+1))}{q(q-1)}+R(S_2)\\
&\leqslant \frac{(k-1)(q-1)\phi(q)+(q^2-q-\phi(q))(q^{k+1}-q^2)}{q(q-1)^2}+R(S_2).
\end{aligned}$$

Hence the proof is complete. □

In particular, for $q=4$, $R(S_{k+1})\leqslant \frac{5.4^{k+1}+3k-29}{18}$ for $k\geqslant 2$ because of simple calculation $R(S_2)=3$.

Now, we can define a new code which is similar to the $\mathbb{Z}_q$-MacDonald code. Let

$$G_{k,u}=\left(G_k\setminus\begin{pmatrix}0\\G_u\end{pmatrix}\right)$$

for $2 \leqslant u \leqslant k-1$ where 0 is a $(k-u) \times \frac{q^u-1}{q-1}$ zero matrix and $\Big(A \setminus B\Big)$ is a matrix obtained from the matrix A by removing the matrix B. The code generated by $G_{k,u}$ is called $\mathbb{Z}_q$-*MacDonald* code. It is denoted by $M_{k,u}$. The Quaternary MacDonald codes were discussed in [7].

Theorem 6. *For* $2 \leqslant u \leqslant r \leqslant k$,

$$R(M_{k+1,u}) \leqslant \frac{(k-r+1)(q-1)\phi(q)+(q^2-q-\phi(q))q^r(q^{k-r+1}-1)}{q(q-1)^2} + R(M_{r,u}).$$

Proof. By using, Proposition 2, we get

$$\begin{aligned} R(M_{k+1,u}) &\leqslant (1 + \left\lfloor \frac{(q-1)\phi(q)n_k}{q} \right\rfloor + (q-1-\phi(q))n_k) + R(M_{k,u}) \\ &\leqslant (1 + \frac{(q-1)\phi(q)n_k}{q} + (q-1-\phi(q))n_k) + R(M_{k,u}) \\ &\leqslant \left(1 + \frac{q^2-q-\phi(q)}{q} n_k\right) + R(M_{k,u}). \end{aligned}$$

This implies $R(M_{k,u}) \leqslant (1 + \frac{q^2-q-\phi(q)}{q} n_{k-1}) + R(M_{k-1,u})$. Combining these two, we get

$$R(M_{k+1,u}) \leqslant (1+\frac{q^2-q-\phi(q)}{q} n_k) + (1+\frac{q^2-q-\phi(q)}{q} n_{k-1}) + R(M_{k-1,u}).$$

Similarly, if we continue, we get

$$\begin{aligned} R(M_{k+1,u}) \leqslant (1 + \frac{q^2-q-\phi(q)}{q} n_k) + (1 + \frac{q^2-q-\phi(q)}{q} n_{k-1}) \\ + \cdots + (1 + \frac{q^2-q-\phi(q)}{q} n_r) + R(M_{r,u}). \end{aligned}$$

Since $n_k = \frac{q^k-1}{q-1}$, for $k \geqslant 2$, therefore

$$\begin{aligned} &R(M_{k+1,u}) \\ &\quad \leqslant (k-r+1) + \frac{q^2-q-\phi(q)}{q} \left(\frac{q^k-1}{q-1} + \frac{q^{k-1}-1}{q-1} + \cdots + \frac{q^r-1}{q-1}\right) + R(M_{r,u}) \\ &\quad \leqslant (k-r+1) + \frac{q^2-q-\phi(q)}{q} \left(\frac{q^k+q^{k-1}+\cdots+q^r-(k-r+1)}{q-1}\right) + R(M_{r,u}) \\ &\quad \leqslant \frac{(k-r+1)\phi(q)+(q^2-q-\phi(q))q^r(q^{k-r}+q^{k-r-1}+\cdots+1)}{q(q-1)} + R(M_{r,u}) \end{aligned}$$

$$\leqslant \frac{(k-r+1)(q-1)\phi(q)+(q^2-q-\phi(q))q^r(q^{k-r+1}-1)}{q(q-1)^2}+R(M_{r,u}). \qquad \square$$

If $u = k$, then

$$R(M_{k+1,k}) \leqslant \left\lfloor \frac{(q-1)\phi(q)n_k}{q} \right\rfloor + (q-1-\phi(q))n_k + 1 \text{ for } k \geqslant 2.$$

In the above theorem, if we replace r by $u+1$, we get

$$R(M_{k+1,u}) \leqslant \frac{(k-u)(q-1)\phi(q)+(q^2-q-\phi(q))q^{u+1}(q^{k-u}-1)}{q(q-1)^2} + \frac{(q-1)\phi(q)n_u}{q} + (q-1-\phi(q))n_u + 1 \text{ for } u \geqslant 2.$$

Thus, we have

Corollary 2. *For $k \geqslant u \geqslant 2$,*

$$R(M_{k+1,u}) \leqslant \frac{(k-u)(q-1)\phi(q)+(q^2-q-\phi(q))q^{u+1}(q^{k-u}-1)}{q(q-1)^2} + \frac{(q-1)\phi(q)n_u}{q} + (q-1-\phi(q))n_u + 1.$$

References

[1] Aoki T., Gaborit P., Harada M., Ozeki M. and Solé P. *On the covering radius of $\mathbb{Z}_4$ codes and their lattices,* vol. 45, IEEE Trans. Inform. Theory no. 6,1999, pp. 2162–2168.

[2] Bhandari M. C., Gupta M. K. and Lal A. K. *On $\mathbb{Z}_4$ Simplex codes and their gray images,* Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-13, Lecture Notes in Computer Science, 1719, 1999, pp. 170–180.

[3] Bonnecaze A., Solé P., Bachoc C. and Mourrain B. *Type II codes over $\mathbb{Z}_4$,* IEEE Trans. Inform. Theory, 43, 1997, pp. 969–976.

[4] Bonnecaze A. and Udaya P. *Cyclic Codes and Self-Dual Codes over $F_2 + uF_2$,* IEEE Trans. Inform. Theory, 45(4), 1999, pp. 1250–1254.

[5] Cohen G. D. Karpovsky M. G., Mattson H. F. and Schatz J. R. *Covering radius-Survey and recent results,* vol. 31 IEEE Trans. Inform. Theory, no. 3, 1985, pp. 328–343.

[6] Cohen C., Lobstein A. and Sloane N. J. A. *Further Results on the Covering Radius of Codes,* vol. 32, IEEE Trans. Inform. Theory, no. 5, 1986, pp. 680–694.

[7] Colbourn C. J. and Gupta M. K. *On quaternary MacDonald codes,* Proc. Information Technology : Coding and Computing (ITCC), April, 2003, pp. 212–215.

[8] Conway J. H. and Sloane N. J. A. *Self-dual codes over the integers modulo 4,* Journal of Combinatorial Theory Series A, 62, 1993, pp. 30–45.

[9] Dougherty S. T., Gulliver T. A. and Harada M. *Type II codes over finite rings and even unimodular lattices,* J. Alg. Combin., 9, 1999, pp. 233–250.

[10] Dougherty S. T., Gaborit P., Harda M. and Sole P. *Type II codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45, 1999, pp. 32–45.

[11] Dougherty S. T., Harada M. and Solé P. *Self-dual codes over rings and the Chinese Remainder Theorem,* Hokkaido Math. J., 28, 1999, pp. 253–283.

[12] Durairajan C. *On Covering Codes and Covering Radius of Some Optimal Codes,* PhD Thesis, Department of Mathematics, IIT, Kanpur, 1996.

[13] El-Atrash M. and Al-Ashker M. Linear Codes over $F_2 + uF_2$, Journal of The Islamic University of Gaza, 11(2), 2003, 53-68.

[14] Gupta M. K. and Durairajan C. On the Covering Radius of some Modular Codes, Communicated.

[15] Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A. and Solé P. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes, IEEE Trans. Inform. Theory, 40, 1994, 301–319.

[16] MacWilliam F. J and Sloane N. J. A. *Theory of Error-Correcting codes,* The Netherlands : Amsterdom, North-Holland, 1977.

[17] Mattson H. F. Jr. An Improved upper bound on covering radius. Lecture Notes in Computer Science, vol. 228, Springer, 1986, pp. 90–106.

[18] Vazirani V. V., Saran H. and SundarRajan B. An efficient algorithm for constructing minimal trellises for codes over finite abelian groups. IEEE Trans. Inform. Theory, vol. 42, no. 6, 1996, pp. 1839–1854.

Contact information

P. Chella Pandian, C. Durairajan
Department of Mathematics,
Bharathidasan University,
Tiruchirappalli - 620 024, Tamilnadu, India.
E-Mail(s): chellapandianpc@gmail.com, cdurai66@rediffmail.com
Web-page(s): http://www.bdu.ac.in/schools/mathematical_sciences/mathematics

Received by the editors: 17.07.2013
and in final form 31.07.2013.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 254–269

RESEARCH ARTICLE

Ultrafilters on G-spaces

O. V. Petrenko, I. V. Protasov

Abstract. For a discrete group G and a discrete G-space X, we identify the Stone-Čech compactifications βG and βX with the sets of all ultrafilters on G and X, and apply the natural action of βG on βX to characterize large, thick, thin, sparse and scattered subsets of X. We use G-invariant partitions and colorings to define G-selective and G-Ramsey ultrafilters on X. We show that, in contrast to the set-theoretical case, these two classes of ultrafilters are distinct. We consider also universally thin ultrafilters on ω, the T-points, and study interrelations between these ultrafilters and some classical ultrafilters on ω.

By a G-space, we mean a set X endowed with the action $G \times X \to X : (g, x) \mapsto gx$ of a group G. All G-spaces are supposed to be transitive: for any $x, y \in X$, there exists $g \in G$ such that $gx = y$. If $X = G$ and the action is the group multiplication, we say that X is a regular G-space.

Several intersting and deep results in combinatorics, topological dynamics and topological algebra, functional analysis were obtained by means of ultrafilters on groups (see [5–7, 12, 27, 28]).

The goal of this paper is to systematize some recent and prove some new results concerning ultrafilters on G-spaces, and point out the key open problems.

In sections 1,2 and 3, we keep together all necessary definitions of filters, ultrafilters and the Stone-Čech compactification βX of the discrete space X. We extend the action of G on X to the action of βG on βX, characterize the minimal invariant subsets of βX, define the corona $\check{X}$ of X and the ultracompanions of subsets of X.

2010 MSC: 05D10, 22A15, 54H20.

Key words and phrases: G-space, ultrafilters, ultracompanion, G-selective ultrafilter, G-Ramsey ultrafilter, T-point, ballean, asymorphism.

In section 4, we give ultrafilter charecterizations of large, thick, thin, sparse and scattered subsets of X.

In section 5, we use G-invariant partitions and colorings to define G-selective and G-Ramsey ultrafilters on X, and show that, in contrast to the set-theoretical case, these two classes are essentially different.

In section 6, we use countable group of permutatious of $\omega = \{0, 1, \ldots\}$ to define thin ultrafilters on ω. We prove that some classical ultrafilters on ω (for example, P- and Q-points) are thin ultrafilters.

We conclude the paper, showing in section 7, how all above results can be considered and interpreted in the frames of general asymptology.

1. Filters and ultrafilters

A family $\mathcal{F}$ of subsets of a set X is called a *filter* if $X \in \mathcal{F}, \varnothing \notin \mathcal{F}$ and

$$A, B \in \mathcal{F}, A \subseteq C \Rightarrow A \cap B \in \mathcal{F}, C \in \mathcal{F}$$

The family of all fillters on X is partially ordered by inclusion $\subseteq$. A filter $\mathcal{U}$ that is maximal in this ordering is called an *ultrafilter*. Equivalentely, $\mathcal{U}$ is ultrafilter if $A \cup B \in \mathcal{U}$ implies $A \in \mathcal{U}$ or $B \in \mathcal{U}$. This characteristic of ultrafilters plays the key role in the Ramsey Theory: to prove that, under any finite partition of X, at least one cell of the partition has a given property, it suffices to construct an ultrafilter $\mathcal{U}$ such that each member of $\mathcal{U}$ has this property.

An ultrafilter $\mathcal{U}$ is called *principal* if $\{x\} \in \mathcal{U}$ for some $x \in X$. Nonprincipal ultrafilters are called *free* and the set of all free ultrafilters on X is denoted by X^*.

We endow a set X with the discrete topology. The Stone-Čech compactification βX of X is a compact Hausdorff space such that X is a subspace of βX and any mapping $f : X \to Y$ to a compact Hausdorff space Y can be extended to the continuous mapping $f^\beta : \beta X \to Y$. To work with βX, we take the points of βX to be the ultrafilters on X, with the points of X identified with the principal ultrafilters, so $X^* = \beta X \setminus X$.

The topology of βX can be defined by stating that the sets of the form $\overline{A} = \{p \in \beta X : A \in p\}$, where A is a subset of X, are base for the open sets. For a filter φ on X, the set $\overline{\varphi} = \{\overline{A} : A \in \varphi\}$ is closed in βX, and each non-empty closed subset of βX is of the form $\overline{\varphi}$ for an appropriate filter φ on X.

2. The action of βG on βX

Given a G-space X, we endow G and X with the discrete topologies and use the universal property of the Stone-Čech compactification to define the action of βG on βX.

Given $g \in G$, the mapping $x \mapsto gx : X \to \beta X$ extends to the continuous mapping

$$p \mapsto gp : \beta X \to \beta X.$$

We note that $gp = \{gP : P \in p\}$, where $gP = \{gx : x \in P\}$.

Then, for each $p \in \beta X$, we extend the mapping $g \mapsto gp : G \to \beta X$ to the continuous mapping

$$q \mapsto qp : \beta G \to \beta X.$$

Let $q \in \beta G$ and $p \in \beta X$. To describe a base for the ultrafilter $qp \in \beta X$, we take any element $Q \in q$ and, for every $g \in Q$, choose some element $P_g \in p$. Then $\bigcup_{g \in Q} gP_g \in qp$ and the family of subsets of this form is a base for qp.

By the construction, for every $g \in G$, the mapping $p \mapsto gp : \beta X \to \beta X$ is continuous and, for every $p \in \beta X$, the mapping $q \mapsto qp : \beta G \to \beta X$ is continuous. In the case of the regular G-space X, $X = G$, we get well known (see [7]) extention of multiplication from G to βG making βG a compact right topological semigroup. For plenty applications of the semigroup βG to combinatorics and topological algebra see [6, 7, 12, 28]. It should be marked that, for any $q, r \in \beta G$, and $p \in \beta X$, we have $(qr)p = q(rp)$ so semigroup βG acts on βX.

Now we define the main technical tool for study of subsets of X by means of ultrafilters.

Given a subset A of X and an ultrafilter $p \in \beta X$ we define the *p-companion* of A by

$$A_p = \{\overline{A} \cap Gp\} = \{gp : g \in G, A \in gp\}.$$

Systematically, p-companions will be used in section 4. Here we demonstrate only one appication of p-companion to characterize minimal invariant subsets of βX. A closed subset S of βX is called *invariant* if $g \in G$ and $p \in S$ imply $gp \in S$. Clearly, S is invariant if and only if $(\beta G)p \subseteq S$ for each $p \in S$. Every invariant subset S of βX contains minimal by inclusion invariant subset. A subset M is minimal invariant if and only if $M = (\beta G)p$ for each $p \in S$. In the case of the regular G-space, the minimal invariant subsets coincide with minimal left ideals of βG so the following theorem generalizes Theorem 4.39 from [7].

Theorem 2.1. *Let X be a G-space and let $p \in \beta X$. Then $(\beta G)p$ is minimal invariant if and only if, for every $A \in p$, there exists a finite subset F of G such that $G = FA_p$.*

Proof. We suppose that $(\beta G)p$ is a minimal invariant subset and take an arbitary $r \in \beta G$. Since $(\beta G)rp = (\beta G)p$ and $p \in (\beta G)p$, there exists $q_r \in \beta G$ such that $q_r rp = p$. Since $A \in q_r rp$, there exists $x_r \in G$ such that $A \in x_r rp$ so $x_r^{-1}A \in rp$. Then we choose $B_r \in r$ such that $\overline{x_r^{-1}A} \supseteq \overline{B_r}p$ and consider the open cover $\{\overline{B_r} : r \in \beta G\}$ of βG. By compactness of βG, there is its finite subcover $\{\overline{B_{r_1}}, \dots, \overline{B_{r_n}}\}$, so $G = B_{r_1} \cup \ldots \cup B_{r_n}$. We put $F^{-1} = \{x_{r_1}, \dots, x_{r_n}\}$. Then $G = (FA)_p$ and it suffices to observe that $(FA)_p = FA_p$.

To prove the converse statement, we suppose on the contrary that $(\beta G)p$ is not minimal and choose $r \in \beta G$ such that $p \notin (\beta G)rp$. Since $(\beta G)rp$ is closed in βX, there exists $A \in p$ such that $\overline{A} \cap (\beta G)rp = \varnothing$. It follows that $A \notin qrp$ for every $q \in \beta G$. Hence, $G \setminus A \in qrp$ for each $q \in \beta G$ and, in particular, $x(G \setminus A) \in rp$ for each $x \in G$. By the assumption, $gA_p \in r$ for some $g \in G$ so $A \in g^{-1}rp$, $gA \in rp$ and we get a contradiction. □

3. Dynamical equivalences and coronas

For an infinite discrete G-space, we define two basic equivalences on the space X^* of all free ultrafilter on X.

Given any $r, q \in X^*$, we say that r, q are *parallel* (and write $r \parallel q$) if there exists $g \in G$ such that $q = gr$. We denote by $\sim$ the minimal (by inclusion) closed in $X^* \times X^*$ equivalences on X^* such that $\parallel \subseteq \sim$. The quotient $X^*/\sim$ is a compact Hausdorff space. It is called the corona of X and is denoted by $\check{X}$.

For every $p \in X^*$, we denote by $\check{p}$ the class of the equivalence $\sim$ containing p, and say that $p, q \in X^*$ are corona equivalent if $\check{p} = \check{q}$. To detect whether two ultrafilters $p, q \in X^*$ are corona equivalent, we use G-slowly oscillating functions on X.

A function $h : X \to [0, 1]$ is called *G-slowly oscillating* if, for any $\varepsilon > 0$ and finite subset $K \subset G$, there exists a finite subset F of X such that

$$diam\ h(Kx) < \varepsilon,$$

for each $x \in X \setminus F$, where $diam\ h(Kx) = \sup\{|h(y) - h(z)| : y, z \in Kx\}$.

Theorem 3.1. *Let $q, r \in X^*$. Then $\check{q} = \check{r}$ if and only if $h^\beta(r) = h^\beta(q)$ for every G-slowly oscillating function $h : X \to [0, 1]$.*

For more detailed information on dynamical equivalences and topologies of coronas see [14] and [1, 13, 17, 19].

In the next section, for a subset A of X and $p \in X^*$, we use the *corona p-companion* of A

$$A_{\check{p}} = A^* \cap \check{p}.$$

4. Diversity of subsets of G-spaces

For a set S, we use the standard notation $[S]^{<\omega}$ for the family of all finite subsets of S.

Let X be a G-space, $x \in X, A \subseteq X, K \in [G]^{<\omega}$. We set

$$B(x, K) = Kx \cup \{x\}, B(A, K) = \bigcup_{a \in A} B(a, K),$$

and say that $B(x, K)$ is a *ball of radius* K around x. For motivation of this notation, see the section 7.

Our first portion of definitions concerns the upward directed properties: $A \in \mathcal{P}$ and $A \subseteq B$ imply $B \in \mathcal{P}$.

A subset A of a G-space X is called

- *large* if there exists $K \in [G]^{<\omega}$ such that $X = KA$;
- *thick* if, for every $K \in [G]^{<\omega}$, there exists $a \in A$ such, that $Ka \subseteq A$;
- *prethick* if there exists $F \in [G]^{<\omega}$ such that FA is thick.

In the dynamical terminology [7], large and prethick subsets are known as syndedic and piecewise syndedic subsets.

Theorem 4.1. *For a subset A of an infinite G-space X, the following statements hold:*

(i) *A is large if and only if $A_p \neq \varnothing$ for each $p \in X^*$;*

(ii) *A is thick if and only if, there exists $p \in X^*$ such that $A_p = Gp$.*

Proof. (i) We suppose that A is large and choose $F \in [G]^{<\omega}$ such that $X = FA$. Given any $p \in X^*$, we choose $g \in F$ such that $gA \in p$. Then $A \in g^{-1}p$ and $A_p \neq \varnothing$.

To prove the converse statement, for every $p \in X^*$, we choose $g_p \in G$ such that $A \in g_p p$ so $g_p^{-1}A \in p$. We consider an open covering of X^* by the subsets $\{g_p^{-1}A^* : p \in X^*\}$ and choose its finite subcovering $g_{p_1}^{-1}A^*, \ldots, g_{p_n}^{-1}A^*$. Then the set $H = X \setminus (g_{p_1}^{-1}A^* \cup \ldots \cup g_{p_n}^{-1}A^*)$ is finite.

We choose $F \in [G]^{<\omega}$ such that $H \subset FA$ and $\{g_{p_1}^{-1}, \dots, g_{p_n}^{-1}\} \subset F$. Then $X = FA$ so A is large.

(ii) We note that A is thick if and only if $X \setminus A$ is not large and apply (i). □

Theorem 4.2. *A subset A of an infinite G-space X is prethick if and only if there exists $p \in X^*$ such that $A \in p$ and $(\beta G)p$ is a minimal invariant subsets of βX.*

Proof. The theorem was proved for regular G-spaces in [7, Theorem 4.40]. This proof can be easily adopted to the general case if we use Theorem 2.1 in place of Theorem 4.39 from [7]. □

Corollary 4.1. *For every finite partition of a G-space X, at least one cell of the partition is prethick.*

Remark 4.1. For a subset A of an infinite G-space X, we set

$$\Delta(A) = \{g \in G : g^{-1}A \cap A \text{ is infinite}\}.$$

Let $\mathcal{P}$ be a finite partition of X. We take $p \in X^*$ such that the set $(\beta G)p$ is minimal invariant and choose $A \in \mathcal{P}$ such that $A \in p$. By Theorem 2.1, A_p is large in G. If $g \in A_p$ then $g^{-1}A \in p$ and $A \in p$. Hence, $g^{-1}A \cap A$ is infinite, so $A_p \subseteq \Delta(A)$ and $\Delta(A)$ is large.

In fact, this statement can be essentially strengthened: there is a function $f : \mathbb{N} \to \mathbb{N}$ such that, for every n-partition $\mathcal{P}$ of a G-space X, there are $A \in \mathcal{P}$ and $F \subset G$ such that $G = F\Delta(A)$ and $|F| \leqslant f(n)$. This is an old open problem (see the surveys [2, 22] whether the above statement is true with $f(n) = n$).

In the second part of the section, we consider the downward directed properties $A \in \mathcal{P}$, $B \subseteq A$ imply $B \in P$) and present some results from [3, 23] A subset A of a G-space X is called

- *thin* if, for every $F \in [G]^{<\omega}$, there exists $K \in [X]^{<\omega}$, such that $B_A(a, F) = \{a\}$ for each $a \in A \setminus K$, where $B_A(a, F) = B(a, F) \cap A$;
- *sparse* if, for every infinite subset Y of X, there exists $H \in [G]^{<\omega}$ such that, for every $F \in [G]^{<\omega}$, there is $y \in Y$ such that $B_A(y, F) \setminus B_A(y, H) = \varnothing$;
- *scattered* if, for every infinite subset Y of X, there exists $H \in [G]^{<\omega}$, such that, for every $F \in [G]^{<\omega}$, there is $y \in Y$ such that $B_Y(a, F) \setminus B_Y(a, H) = \varnothing$.

Theorem 4.3. *For a subset A of a G-space X, the following statements hold:*

(i) *A is thin if and only if $|A_p| \leqslant 1$ for each $p \in X^*$;*

(ii) *A is sparse if and only if A_p is finite for every $p \in X^*$;*

Let $(g_n)_{n\in\omega}$ be a sequence in G and let $(x_n)_{n\in\omega}$ be a sequence in X such that

(1) $\{g_0^{\varepsilon_0} \dots g_n^{\varepsilon_n} x_n : \varepsilon_i \in \{0,1\}\} \cap \{g_0^{\varepsilon_0} \dots g_m^{\varepsilon_m} x_m : \varepsilon_i \in \{0,1\}\} = \varnothing$ for all distinct $m, n \in \omega$;

(2) $|\{g_0^{\varepsilon_0} \dots g_n^{\varepsilon_n} x_n : \varepsilon_i \in \{0,1\}\}| = 2^{n+1}$ for every $n \in \omega$.

We say that a subset Y of X is a *piecewise shifted FP-set* if there exist $(g_n)_{n\in\omega}$, $(x_n)_{n\in\omega}$ satisfying (1) and (2) such that

$$Y = \{g_0^{\varepsilon_0} \dots g_n^{\varepsilon_n} x_n : \varepsilon_n \in \{0,1\}, n \in \omega\}.$$

For definition of an FP-set in a group see [7].

Theorem 4.4. *For a subset A of a G-space X, the following statements are equivalent:*

(i) *A is scattered;*

(ii) *for every infinite subset Y of A, there exists $p \in Y^*$ such that Y_p is finite;*

(iii) *$A_p p$ is discrete in X^* for every $p \in X^*$;*

(iv) *A contains no piecewise shifted FP-sets.*

Theorem 4.5. *Let G be a countable group and let X be a G-space. For a subset A of X, the following statements hold:*

(i) *A is large if and only if $A_{\check{p}} \neq \varnothing$ for each $p \in X^*$;*

(ii) *A is thick if and only if $\check{p} \subseteq A^*$ for some $p \in X^*$;*

(iii) *A is thin if and only if $|A_{\check{p}}| \leqslant 1$ for each $p \in X^*$;*

(iv) *if $A_{\check{p}}$ is finite for each $p \in X^*$ then A is sparse;*

(v) *if, for every infinite subset Y of A, there is $p \in Y^*$ such that $Y_{\check{p}}$ is finite then A is scattered.*

Question 4.1. *Does the conversion of Theorem 4.5 (iv) hold?*

Question 4.2. *Does the conversion of Theorem 4.5 (v) hold?*

Remark 4.2. If G is an uncountable Abelian group then the corona $\check{G}$ is a singleton [13]. Thus, Theorem 4.5 does not hold (with $X = G$) for uncountable Abelian groups.

5. Selective and Ramsey ultrafilters on G-spaces

We recall (see [4]) that a free ultrafilter $\mathcal{U}$ on an infinite set X is said to be *selective* if, for any partition $\mathcal{P}$ of X, either one cell of $\mathcal{P}$ is a member of $\mathcal{U}$, or some member of $\mathcal{U}$ meets each cell of $\mathcal{P}$ in at most one point. Selective ultrafilters on ω are also known under the name *Ramsey ultrafilters* because $\mathcal{U}$ is selective if and only if, for each colorings $\chi : [\omega]^2 \to \{0,1\}$ of 2-element subsets of ω, there exists $U \in \mathcal{U}$ such that the restriction $\chi|_{[U]^2} \equiv const.$

Let G be a group, X be a G-space with the action $G \times X \to X$, $(g,x) \mapsto gx$. All G-spaces under consideration are supposed to be transitive: for any $x, y \in X$, there exists $g \in G$ such that $gx = y$. If $G = X$ and gx is the product of g and x in G, X is called a *regular G-space*. A partition $\mathcal{P}$ of a G-space X is *G-invariant* if $gP \in \mathcal{P}$ for all $g \in G$, $P \in \mathcal{P}$.

Let X be an infinite G-space. We say that a free ultrafilter $\mathcal{U}$ on X is *G-selective* if, for any G-invariant partition $\mathcal{P}$ of X, either some cell of $\mathcal{P}$ is a member of $\mathcal{U}$, or there exists $U \in \mathcal{U}$ such that $|P \cap U| \leqslant 1$ for each $P \in \mathcal{P}$.

Clearly, each selective ultrafilter on X is G-selective. Selective ultrafilters on ω exist under some additional to ZFC set-theoretical assumptions (say, CH), but there are models of ZFC with no selective ultrafilters on ω.

Let X be a G-space, $x_0 \in X$. We put $St(x_0) = \{g \in G : gx_0 = x_0\}$ and identify X with the left coset space $G/St(x_0)$. If $\mathcal{P}$ is a G-invariant partition of $X = G/S, S = St(x_0)$, we take $P_0 \in \mathcal{P}$ such that $x_0 \in P_0$, put $H = \{g \in G : gS \in P_0\}$ and note that the subgroup H completely determines $\mathcal{P}$: xS and yS are in the same cell of $\mathcal{P}$ if and only if $y^{-1}x \in H$. Thus, $\mathcal{P} = \{x(H/S) : x \in L\}$ where L is a set of representatives of the left cosets of G by H.

Theorem 5.1. *For every infinite G-space X, there exists a G-selective ultrafilter $\mathcal{U}$ on X in ZFC.*

Proof. We take $x_0 \in X$, put $S = St(x_0)$ and identify X with G/S. We choose a maximal filter $\mathcal{F}$ on G/S having a base consisting of subsets of the form A/S where A is a subgroup of G such that $S \subset A$ and $|A : S| = \infty$. Then we take an arbitrary ultrafilter $\mathcal{U}$ on G/S such that $\mathcal{F} \subseteq \mathcal{U}$.

To show that $\mathcal{U}$ is G-selective, we take an arbitrary subgroup H of G such that $S \subseteq H$ and consider a partition $\mathcal{P}_H$ of G/S determined by H.

If $|H \cap A : S| = \infty$ for each subgroup A of G such that $A/S \in \mathcal{F}$ then, by the maximality of $\mathcal{F}$, we have $H/S \in \mathcal{F}$. Hence, $H/S \in \mathcal{U}$.

Otherwise, there exists a subgroup A of G such that $A/S \in \mathcal{F}$ and $|H \cap A : S|$ is finite, $|H \cap A : S| = n$. We take an arbitrary $g \in G$ and denote $T_g = gH \cap A$. If $a \in T_g$ then $a^{-1}T_g \subseteq A$ and $a^{-1}T_g \subseteq H$. Hence, $a^{-1}T_g/S \subseteq A \cap H/S$ so $|T_g/S| \leqslant n$. If x and y determine the same coset by H, then they determine the same set T_g. Then we choose $U \in \mathcal{U}$ such that $|U \cap x(H \cap A/S)| \leqslant 1$ for each $x \in G$. Thus, $|U \cap P| \leqslant 1$ for each cell P of the partition $\mathcal{P}_H$. □

The next theorem characterizes all G-spaces X such that each free ultrafilter on X is G-selective.

Theorem 5.2. *Let G be a group, S be a subgroup of G such that $|G : S| = \infty$, $X = G/S$. Each free ultrafilter on X is G-selective if and only if, for each subgroup T of G such that $S \subset T \subset G$, either $|T : S|$ is finite or $|G : T|$ is finite.*

Applying Theorem 2, we conclude that each free ultrafilter on an infinite Abelian group G (as a regular G-space) is selective if and only if $G = \mathbb{Z} \oplus F$ or $G = \mathbb{Z}_{p^\infty} \times F$, where F is finite, $\mathbb{Z}_{p^\infty}$ is the Prüffer p-group. In particular, each free ultrafilter on $\mathbb{Z}$ is $\mathbb{Z}$-selective.

For a G-space X and $n \geqslant 2$, a coloring $\chi : [X]^n \to \{0, 1\}$ is said to be *G-invariant* if, for any $\{x_1, \dots, x_n\} \in [X]^n$ and $g \in G$, $\chi(\{x_1, \dots, x_n\}) = \chi(\{gx_1, \dots, gx_n\})$. We say that a free ultrafilter $\mathcal{U}$ on X is *(G, n)-Ramsey* if, for every G-invariant coloring $\chi : [X]^n \to \{0, 1\}$, there exists $U \in \mathcal{U}$ such that $\chi|_{[U]^n} \equiv const$. In the case $n = 2$, we write "G-Ramsey" instead of $(G, 2)$-Ramsey.

Theorem 5.3. *For any G-space X, each G-Ramsey ultrafilter on X is G-selective.*

The following three theorems show that the conversion of Theorem 5.3 is very far from truth. Let G be a discrete group, βG is the Stone-Čech compactification of G as a left topological semigroup, $K(\beta G)$ is the minimal ideal of βG.

Theorem 5.4. *Each ultrafilter from the closure cl $K(\beta\mathbb{Z})$ is not $\mathbb{Z}$-Ramsey.*

A free ultrafilter $\mathcal{U}$ on an Abelian group G is said to be a *Schur ultrafilter* if, for any $U \in \mathcal{U}$, there are distinct $x, y \in U$ such that $x + y \in U$.

Theorem 5.5. *Each Schur ultrafilter $\mathcal{U}$ on $\mathbb{Z}$ is not $\mathbb{Z}$-Ramsey.*

A free ultrafilter $\mathcal{U}$ on $\mathbb{Z}$ is called *prime* if $\mathcal{U}$ cannot be represented as a sum of two free ultrafilters.

Theorem 5.6. *Every $\mathbb{Z}$-Ramsey ultrafilter on $\mathbb{Z}$ is prime.*

Question 5.1. *Is each $\mathbb{Z}$-Ramsey ultrafilter on $\mathbb{Z}$ selective?*

Some partial positive answers to this question are in the following two theorems.

Theorem 5.7. *Assume that a free ultrafilter $\mathcal{U}$ on $\mathbb{Z}$ has a member A such that $|g + A \cap A| \leqslant 1$ for each $g \in \mathbb{Z} \setminus \{0\}$. If $\mathcal{U}$ is $\mathbb{Z}$-Ramsey then $\mathcal{U}$ is selective.*

Theorem 5.8. *Every $(\mathbb{Z}, 4)$-Ramsey ultrafilter on $\mathbb{Z}$ is selective.*

All above results are from [9].

Remark 5.1. Let G be an Abelian group. A coloring $\chi : [G]^2 \to \{0, 1\}$ is called a PS-*coloring* if $\chi(\{a, b\}) = \chi(\{a - g, b + g\})$ for all $\{a, b\} \in [G]^2$, equivalently, $a + b = c + d$ implies $\chi(\{a, b\}) = \chi(\{c, d\})$. A free ultrafilter $\mathcal{U}$ on G is called a *PS-ultrafilter* if, for any PS-coloring χ of $[G]^2$, there is $U \in \mathcal{U}$ such that $\chi|_{[U]^2} \equiv const$. The following statements were proved in [18], see also [6, Chapter 10].

If G has no elements of order 2 then each PS-ultrafilter on G is selective. A strongly summable ultrafilter on the countable Boolean group $\mathbb{B}$ is a PS-ultrafilter but not selective. If there exists a PS-ultrafilter on some countable Abelian group then there is a P-point in ω^*.

Clearly, an ultrafilter $\mathcal{U}$ on $\mathbb{B}$ is a PS-ultrafilter if and only if $\mathcal{U}$ is $\mathbb{B}$-Ramsey. Thus, a $\mathbb{B}$-Ramsey ultrafilter needs not to be selective, but such an ultrafilter cannot be constructed in ZFC with no additional assumptions.

6. Thin ultrafilters

A free ultrafilter $\mathcal{U}$ on ω is said to be

- *P-point* if, for any partition $\mathcal{P}$ of ω, either $A \in \mathcal{U}$ for some cell A of $\mathcal{P}$ or there exists $U \in \mathcal{U}$ such that $U \cap A$ is finite for each $A \in \mathcal{P}$;
- *Q-point* if, for any partition $\mathcal{P}$ of ω into finite subsets, there exists $U \in \mathcal{U}$ such that $|U \cap A| \leqslant 1$ for each $A \in \mathcal{P}$.

Clearly, $\mathcal{U}$ is selective if and only if $\mathcal{U}$ is a P-point and a Q-point. It is well known that the existence of P- or Q-points is independent of the system of axioms ZFC.

We say that a free ultrafilter $\mathcal{U}$ on ω is a *T-point* if, for every countable group G of permutations of ω, there is a thin subset $U \in \mathcal{U}$ in the G-space ω.

To give a combinatorical characterization of T-points (see [8, 9]), we need some definitions.

A covering $\mathcal{F}$ of a set X is called uniformly bounded if there exists $n \in \mathbb{N}$ such that $|\cup\{F \in \mathcal{F} : x \in F\}| \leqslant n$ for each $x \in X$.

For a metric space (X, d) and $n \in \mathbb{N}$, we denote $B_d(x, n) = \{y \in X : d(x, y) \leqslant n\}$. A metric d is called *locally finite (uniformly locally finite)* if, for every $n \in \mathbb{N}$, $B_d(x, n)$ is finite for each $x \in X$ (there exists $c(n) \in \mathbb{N}$ such that $|B_d(x, n)| \leqslant c(n)$ for each $x \in X$).

A subset A of (X, d) is called *d-thin* if, for every $n \in \mathbb{N}$ there exists a bounded subset B of X such that $B_d(a, n) \cap A = \{a\}$ for each $a \in A \setminus B$.

Theorem 6.1. *For a free ultrafilter $\mathcal{U}$ on ω, the following statement are equivalent:*

(i) *$\mathcal{U}$ is a T-point;*

(ii) *for any sequence $(\mathcal{F}_n)_{n\in\omega}$ of uniformly bounded coverings of ω, there exists $U \in \mathcal{U}$ such that, for each $n \in \omega$, $|F \cap U| \leqslant 1$ for all but finitely many $F \in \mathcal{F}_n$;*

(iii) *for each uniformly locally finite metric d on ω, there is a d-thin member $U \in \mathcal{U}$.*

We do not know if a sequence of coverings in (ii) can be replaced to a sequence of partitions.

Remark 6.1. By [10, Theorem 3], a free ultrafilter $\mathcal{U}$ on ω in selective if and only if, for every metric d on ω, there is a d-thin member of $\mathcal{U}$.

Remark 6.2. By [10, Theorem 8], a free ultrafilter $\mathcal{U}$ on ω is a Q-point if and only if, for every locally finite metric d on ω, there is a d-thin member of $\mathcal{U}$.

Remark 6.3. It is worth to be mentioned the following metric characterization of P-points: a free ultrafilter $\mathcal{U}$ on ω is a P-point if and only if, for every metric d on ω, either some member of $\mathcal{U}$ is bounded or there is $U \in \mathcal{U}$ such that (U, d) is locally finite.

A free ultrafilter $\mathcal{U}$ on ω is said to be a *weak P-point* (a *NWD-point*) if $\mathcal{U}$ is not a limit point of a countable subset in ω^* (for every injective mapping $f:\omega\to\mathbb{R}$, there is $U\in\mathcal{U}$ such that $f(U)$ is nowhere dense in $\mathbb{R}$). We note that a weak P-point exists in ZFC.

In the next theorem, we summarize the main results from [8].

Theorem 6.2. *Every P-point and every Q-point is a T-point. Under CH, there exists a T-point which is neither P-point, nor NWD-point, nor Q-point. For every ultrafilter $\mathcal{V}$ on ω, there exist a T-point $\mathcal{U}$ and a mapping $f:\omega\to\omega$ such that $\mathcal{V}=f^{\beta}(\mathcal{U})$.*

Question 6.1. *Does there exist a T-point in ZFC?*

Question 6.2. *Is every weak P-point a T-point?*

Question 6.3. *(T. Banakh). Let $\mathcal{U}$ be a free ultrafilter on ω such that, for any metric d on ω, some member of $\mathcal{U}$ is discrete in (X,d). Is $\mathcal{U}$ a T-point?*

A free ultrafilter $\mathcal{U}$ on ω is called a $T_{\aleph_0}$-point if, for each minimal well ordering $<$ of ω, there is a $d_<$-thin member of $\mathcal{U}$, where $d_<$ is the natural metric on ω defined by $<$. By Theorem 6.1, each T-point is $T_{\aleph_0}$-point.

Question 6.4. *Is every $T_{\aleph_0}$-point a T-point? Does there exist a $T_{\aleph_0}$-point in ZFC?*

Remark 6.4. An ultrafilter $\mathcal{U}$ on ω is called *rapid* if, for any partition $\{P_n : n\in\omega\}$ of ω into finite subsets, there exists $U\in\mathcal{U}$ such that $|U\cap P_n|\leqslant n$ for every $n\in\omega$. Jana Flašková (see [10, p.350]) noticed that, in contrast to Q-points, a rapid ultrafilter needs not to be a T-point.

Remark 6.5. A family $\mathcal{F}$ of infinite subsets of ω is *coideal* if $M\subseteq N, M\in\mathcal{F}\Rightarrow N\in\mathcal{F}$ and $M=N_0\cup N_1, M\in\mathcal{F}\Rightarrow N_0\in\mathcal{F}\vee N_1\in\mathcal{F}$. Clearly, the family of all infinite subsets of ω is a coideal.

Following [27], we say that a coideal F is

- *P-coideal* if, for every decreasing sequence $(A_n)_{n\in\omega}$ in $\mathcal{F}$ there is $B\in\mathcal{F}$ such that $B\setminus A_n$ is finite for each $n\in\omega$;
- *Q-coideal* if, for every $A\in\mathcal{F}$ and every partition $A=\cup_{n\in\omega}F_n$ with F_n finite, there is $B\in\mathcal{F}$ such that $B\subseteq A$ and $|B\cap F_n|\leqslant 1$ for each $n\in\omega$.

We say that a coideal $\mathcal{F}$ is a *T-coideal* if, for every countable group G of permutations of ω and every $M \in \mathcal{F}$ there exists a G-thin subset $N \in \mathcal{F}$ such that $N \subseteq M$.

Generalizing the first statement in Theorem 6.2, we get: every P-coideal and every Q-coideal is a T-coideal.

Remark 6.6. We say that $\mathcal{U} \in \omega^*$ is sparse (scattered) if, for every countable group G of permutations of ω, there is sparse (scattered) in (G, w) member of $\mathcal{U}$. Clearly, T-point $\Rightarrow$ sparse ultrafilter $\Rightarrow$ scattered ultrafilter.

Question 6.5. *Does there exist sparse (scattcred) ultrafilter in ZFC? Is every weak P-point scattered ultrafilter?*

Question 6.6. *Let $\mathcal{U}$ be a free ultrafilter on ω such that, for every countable group G of permutations of ω, the orbit $\{g\mathcal{U} : g \in G\}$ is discrete in ω^*. Is $\mathcal{U}$ a weak P-point?*

7. The ballean context

Following [21,25], we say that a *ball structure* is a triple $\mathcal{B} = (X, P, B)$, where X, P are non-empty sets and, for every $x \in X$ and $\alpha \in P$, $B(x, \alpha)$ is a subset of X which is called a *ball of radius* α around x. It is supposed that $x \in B(x, \alpha)$ for all $x \in X$ and $\alpha \in P$. The set X is called the *support* of $\mathcal{B}$, P is called the set of *radii*.

Given any $x \in X, A \subseteq X$ and $\alpha \in P$ we set

$$B^*(x, \alpha) = \{y \in X : x \in B(y, \alpha)\},\ B(A, \alpha) = \bigcup_{a \in A} B(a, \alpha)$$

A ball structure $\mathcal{B} = (X, P, B)$ is called a *ballean* if

- for any $\alpha, \beta \in P$, there exist α', β' such that, for every $x \in X$,

$$B(x, \alpha) \subseteq B^*(x, \alpha'),\ B^*(x, \beta) \subseteq B(x, \beta');$$

- for any $\alpha, \beta \in P$, there exists $\gamma \in P$ such that, for every $x \in X$,

$$B(B(x, \alpha), \beta) \subseteq B(x, \gamma);$$

A ballean $\mathcal{B}$ on X can also be determined in terms of entourages of the diagonal of $X \times X$ (in this case it is called a coarse structure [26]) and can be considered as an asymptotic counterpart of a uniform topological space.

Let $\mathcal{B}_1 = (X_1, P_1, B_1)$, $\mathcal{B}_2 = (X_2, P_2, B_2)$ be balleans. A mapping $f : X_1 \to X_2$ is called a *$\prec$-mapping* if, for every $\alpha \in P_1$, there exists $\beta \in P_2$ such that, for every $x \in X_1$, $f(B_1(x, \alpha)) \subseteq B_2(f(x), \beta)$. A bijection $f : X_1 \to X_2$ is called an *asymorphism* if f and f^{-1} are $\prec$-mappings.

Every metric space (X, d) defines the metric ballean $(X, \mathbb{R}^+, B_d)$, where $B_d(x, r) = \{y \in X : d(x, y) \leqslant r\}$. By [25, Theorem 2.1.1], a ballean (X, P, B) is metrizable (i.e. asymorphic to some metric ballean) if and only if there exists a sequence $(\alpha_n)_{n\in\omega}$ in P such that, for every $\alpha \in P$, one can find $n \in \omega$ such that $B(x, \alpha) \subseteq B(x, \alpha_n)$ for each $x \in X$.

Let G be a group, $\mathcal{I}$ be an ideal in the Boolean algebra $\mathcal{P}_G$ of all subsets of G, i.e. $\varnothing \in \mathcal{I}$ and if $A, B \in \mathcal{I}$ and $A' \subseteq A$ then $A \cup B \in \mathcal{I}$ and $A' \in \mathcal{I}$. An ideal $\mathcal{I}$ is called a *group ideal* if, for all $A, B \in \mathcal{I}$, we have $AB \in \mathcal{I}$ and $A^{-1} \in \mathcal{I}$. For construction of group ideals see [16].

For a G-space X and a group ideal $\mathcal{I}$ on G, we define the ballean $\mathcal{B}(G, X, \mathcal{I})$ as the triple $(X, \mathcal{I}, B)$ where $B(x, A) = Ax \cup \{x\}$. In the case where $\mathcal{I}$ is the ideal of all finite subsets of G, we omit $\mathcal{I}$ and return to the notation $B(x, A)$ used from the very beginning of the paper.

The following couple of theorems from [10, 15] demonstrate the tight interrelations between balleans and G-spaces.

Theorem 7.1. *Every ballean $\mathcal{B}$ with the support X is asymorphic to the ballean $\mathcal{B}(G, X, \mathcal{I})$ for some subgroup G of the group S_X of all permutations of X and some group ideal $\mathcal{I}$ on G.*

Theorem 7.2. *Every metrizable ballean $\mathcal{B}$ with the support X is asymorphic to the ballean $\mathcal{B}(G, X, \mathcal{I})$ for some subgroup G of S_X and some group ideal $\mathcal{I}$ on G with countable base such that, for all $x, y \in X$, there is $A \in \mathcal{I}$ such that $y \in Ax$.*

A ballean $\mathcal{B} = (X, P, B)$ is called *locally finite (uniformly locally finite)* if each ball $B(x, \alpha)$ is finite (for each $\alpha \in P$, there exists $n \in \mathbb{N}$ such that $|B(x, \alpha)| \leqslant n$ for every $x \in X$.

Theorem 7.3. *Every locally finite ballean $\mathcal{B}$ with the support X is asymorphic to the ballean $\mathcal{B}(G, X, \mathcal{I})$ for some subgroup G of S_X and some group ideal $\mathcal{I}$ on G with a base consisting of subsets compact in the topology of pointwise convergence on S_X.*

Theorem 7.4. *Every uniformly locally finite ballean $\mathcal{B}$ with the support X is asymorphic to the ballean $\mathcal{B}(G, X, [G]^{<\omega})$ for some subgroup G of S_X.*

We note that Theorem 7.4 plays the key part in the proof of Theorem 6.1.

For ultrafilters on metric spaces and balleans we address the reader to [12, 20, 24].

References

[1] T. Banakh, O. Chervak, L. Zdomskyy, *On character of points in the Higson corona of a metric space*, Comment. Math. Univ. Carolin. **54** (2013), no 2, 159–178.

[2] T. Banakh, I. Protasov, S. Slobodianiuk, *Densities, submeasures and partitions of groups*, Algebra Discrete Math. **17** (2014), no 2, 193–221.

[3] T. Banakh, I. Protasov, S. Slobodianiuk, *Scattered subsets of groups*, Ukr. Math. J. **67** (2015), 304–312.

[4] W.W. Comfort, *Ultrafilters: some old and some new results*, Bull. Amer. Math. Soc. **83**(1977), 417-455.

[5] H. Dales, A. Lau, D. Strauss, *Banach Algebras on a Semigroups and Their Compactifications*, Mem. Amer. Math. Soc., vol. 2005, 2010.

[6] M. Filali, I. Protasov, *Ultrafilters and Topologies on Groups*, Math. Stud. Monogr. Ser., Vol. 13, VNTL Publishers, Lviv, 2011.

[7] N. Hindman, D. Strauss, *Algebra in the Stone-Čech compactification: Theory and Applications*, Walter de Gruyter, Berlin, New York, 1998.

[8] O. Petrenko, I. Protasov, *Thin ultrafilters*, Notre Dame J. Formal Logic **53** (2012), 79–88.

[9] O. Petrenko, I. Protasov, *Selective and Ramsey ultrafilters on G-spaces*, Notre Dame J. Formal Logic (to appear).

[10] O.V. Petrenko, I.V. Protasov, *Balleans and G-spaces*, Ukr. Math. J. **64** (2012), 344–350.

[11] O.V. Petrenko, I.V. Protasov, *Balleans and filters*, Matem. Stud. **38** (2012), 3–11.

[12] I. Protasov, *Combinatorics of Numbers*, Math. Stud. Monogr. Ser, Vol. 2, VNTL Publisher, Lviv, 1997.

[13] I. Protasov, *Coronas of balleans*, Topology Appl. **149** (2005), 149–160.

[14] I. Protasov, *Dynamical equivalences on G^**, Topology Appl. **155** (2008), 1394–1402.

[15] I.V. Protasov, *Balleans of bounded geometry and G-spaces*, Mat. Stud. **30** (2008), 61–66.

[16] I. Protasov, *Counting Ω-ideals*, Algebra Universalis **62** (2010), 339–343.

[17] I. Protasov, *Coronas of ultrametric spaces*, Comment. Math. Univ. Carolin. **52** (2011), no 2, 303–307.

[18] I. Protasov, *Ultrafilters and partitions of Abelian groups*, Ukr. Math. J. **53** (2011), 99–107.

[19] I. Protasov, *Weak P-points in coronas of G-spaces*, Topology Appl. **159** (2012), 587–592.

[20] I. Protasov, *Ultrafilters on metric spaces*, Topology Appl. **164** (2014), 207–214.

[21] I. Protasov, T. Banakh, *Ball Structures and Colorings of Graphs and Groups*, Math. Stud. Monogr. Ser, Vol. 11, VNTL Publisher, Lviv, 2003.

[22] I. Protasov, S. Slobodianiuk, *Partitions of groups*, Math. Stud., **42** (2014), 115–128.

[23] I. Protasov, S. Slobodianiuk, *On the subset combinatorics of G-spaces*, Algebra Discrete Math. **17** (2014), 98–109.

[24] I. Protasov, S. Slobodianiuk, *Ultrafilters on balleans*, Ukr. Math. J. (to appear).

[25] I. Protasov, M. Zarichnyi, *General Asymptology*, Math. Stud. Monogr. Ser., Vol. 12, VNTL Publishers, Lviv, 2007.

[26] J. Roe, *Lectures on Coarse Geometry*, Amer. Math. Soc., Providence, R.I. 2003.

[27] S. Todorcevic, *Introduction to Ramsey Spaces*, Princeton Univ. Press, 2010.

[28] Y. Zelenyuk, *Ultrafilters and Topologies on Groups*, de Grueter, 2012.

Contact information

O. V. Petrenko,
I. V. Protasov

Department of Cybernetics,
Taras Shevchenko National University,
Volodymyrs'ka St., 64, 01601 Kyiv, Ukraine
E-Mail(s): `opetrenko72@gmail.com`,
`i.v.protasov@gmail.com`

Received by the editors: 26.06.2015
and in final form 26.06.2015.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 270–282 RESEARCH ARTICLE

On c-normal and hypercentrally embeded subgroups of finite groups*

Ning Su and Yanming Wang

Communicated by L. A. Kurdachenko

Abstract. In this article, we investigate the structure of a finite group G under the assumption that some subgroups of G are c-normal in G. The main theorem is as follows:

Theorem A. *Let E be a normal finite group of G. If all subgroups of E_p with order d_p and $2d_p$ (if $p = 2$ and E_p is not an abelian nor quaternion free 2-group) are c-normal in G, then E is p-hypercyclically embedded in G.*

We give some applications of the theorem and generalize some known results.

1. Introduction

All groups considered in this paper are finite. We use conventional notions and notation, as in [3]. G always denotes a finite group, $|G|$ the order of G, $\pi(G)$ the set of all primes dividing $|G|$, G_p a Sylow p-subgroup of G for any prime $p \in \pi(G)$.

A well know result is that G is nilpotent if and only if every maximal subgroup of G is normal in G. In [11], Wang defined c-normality of a subgroup and prove that a finite group G is solvable if and only if every maximal subgroup of G is c-normal in G.

---

*The research has been supported by NSF China (11171353).
2010 MSC: 20D10.
Key words and phrases: c-normal, hypercenter, p-supersolvable, p-nilpotent.

Definition 1.1 ([11], Definition 1.1)**.** Let G be a group. We call a subgroup H is c-normal in G if there exit a normal subgroup N of G such that $HN = G$ and $H \cap N \leqslant H_G$.

The basic properties of c-normality are as follows.

Lemma 1.2 ([11], Lemma 2.1)**.** *Let G be a group. Then*

(1) *If H is normal in G , then H is c-normal in G.*

(2) *G is c-simple if and only if G is simple.*

(3) *If H is c-normal in G , $H \leqslant K \leqslant G$, then H is c-normal in K.*

(4) *Let $K \trianglelefteq G$ and $K \leqslant H$, Then H is c-normal in G if and only if H/K-normal in G/K.*

Several authors successfully use the c-normal property of some p-subgroups of G to determine the structure of G. (see [2],[5], [8-10]). Many results in previous papers have the following form: Suppose that G/E is supersolvable (or $G/E \in \mathcal{F}$, where $\mathcal{F}$ is a formation containing the class of all supersolvable groups), if some subgroups of E with prime power order are c-normal G , then G is supersolvable (or $G \in \mathcal{F}$). Actually, in a more general case, if we can get a criterion that E lies in the $\mathcal{F}$-hypercenter, then $G/E \in \mathcal{F}$ implies that $G \in \mathcal{F}$. In order to get good results, many authors have to impose the c-normal hypotheses on all the prime divisors or the minimal or maximal divisor p of $|G|$ rather than any prime divisor.

Let p be a fixed prime. In this paper, we mainly focus on how a normal subgroup E has the above property provided every p-subgroup of E with some fix order is c-normal in G. For this purpose, we introduce the concept of p-hypercentrally embeded:

Definition 1.3. A normal subgroup E is said to be p-hypercentrally embedded in G if every p-chief factor of G below E is cyclic.

It is of a lot interest to determine the structure of G with hypothesis that some p-subgroups are well suited in G. Many results on minimal p-subgroups and maximal subgroups of Sylow subgroups were obtained. Recently, people have more interest to get unified and general results ([8],[12]). That is, to consider the p-subgroups with the same order. For simplicity, we give the following notation of d_p .

Let E be a normal finite group of G. d_p is a prime power divisor of $|E_p|$ satisfying the following properties:If $|E_p| = p$ then $d_p = |E_p| = p$; if $|E_p| > p$ then $1 < d_p < |E_p|$.

In this paper, we will prove the following theorem:

Theorem A. *Let E be a normal finite group of G. If all subgroups of E_p with order d_p and $2d_p$ (if $p = 2$ and E_p is not an abelian nor quaternion free 2-group) are c-normal in G, then E is p-hypercyclically embedded in G.*

As an application of Theorem A, we have the following:

Theorem B. *Let E be a normal finite group of G such that both $N_G(E_p)$ and G/E are p-nilpotent. If either E_p is abelian or every subgroup of E_p with order d_p (d_p is a prime power divisor of $|E_p|$ and $1 < d_p < |E_p|$) and $2d_p$ (if $p = 2$ and E_p is not quaternion free) is c-normal in E, then G is p-nilpotent.*

2. Proof of the theorems

In this section, we will investigate how a normal subgroup E embedded in G if, for a fixed prime p, some subgroups of E_p are c-normal in G. First, we need some results about a normal subgroup with some subgroups being c-supplemented in G. Following [10], a group H is said to be c-supplemented in G if there exists a subgroup K of G such that $G = HK$ and $H \cap K \leqslant H_G$. It is clear from the definition that if a subgroup H is c-normal in G, then H is c-supplemented in G.

Lemma 2.1. *If N is a minimal abelian normal subgroup of G then all proper subgroups of N are not c-supplement in G.*

Proof. Suppose this Lemma is not true and let H be a proper subgroup of N which is c-supplemented in G. Obviously $H_G = 1$ since $H_G < N$ and N is a minimal normal subgroup of G. By the definition of c-supplement, there exit a proper subgroup M of G such that $G = HM$ with $H \cap M \leqslant H_G = 1$. Hence $NM \geqslant HM = G$. Since N is abelian, we know that $N \cap M \trianglelefteq G$. Hence $N \cap M = 1$. Therefore we have $|G| = |NM| = |N||M| > |H||M| = |HM|$, a contradiction to $G = HM$. □

For a saturated formation $\mathcal{F}$, the $\mathcal{F}$-hypercenter of a group G is denoted by $Z_{\mathcal{F}}(G)$ (see [3, p 389, Notation and Definitions 6.8(b)]). Let $\mathcal{U}$ denote the class of all supersolvable groups. In [2], Asaad gave the following result: Let p be a nontrivial normal p-subgroup, where p is an odd prime, if every minimal subgroup of P is c-supplemented in G, then $P \leqslant Z_{\mathcal{U}}(G)$. It is helpful to give a result for $p = 2$. In fact, we have the following property:

Property 2.2. *Let P be a normal 2-subgroup of G. If all minimal subgroups of P and all cyclic subgroups of P with order 4 (if P is neither abelian nor quaternion free) are c-supplemented in G, then $P \leqslant Z_\infty(G)$.*

Proof. Let Q be a Sylow q-subgroup of G $(q \neq p)$, we are going to show that PQ is 2-nilpotent. Suppose PQ is not 2-nilpotent, then PQ contains a minimal non 2-nilpotent subgroup H. By Ito's famous result, we know that $H = [H_2]H_q$, $exp(H_2) \leqslant 4$ and $H_2/\Phi(H_2)$ is a minimal normal subgroup of $H/\Phi(H_2)$. If $|H_2/\Phi(H_2)| = 2$, then we have $|H/\Phi(H_2) : H_q\Phi(H_2)/\Phi(H_2)| = |H_2/\Phi(H_2)| = 2$ and thus $H_q\Phi(H_2)/\Phi(H_2)$ is normal in $H/\Phi(H_2)$, which will lead to the nilpotent of H. Therefore $|H_2/\Phi(H_2)| > 2$. We distinguish the three cases:

Case 1. Every minimal subgroup of P and every cyclic subgroups with order 4 of P is c-supplemented in G. Let $\langle x\rangle$ be a subgroup of H_2 not contained In $\Phi(H_2)$, then $\langle x\rangle\Phi(H_2)/\Phi(H_2)$ is a nontrivial subgroup of $H/\Phi(H_2)$. Since $exp(H_2) \leqslant 4$, we know that $\langle x\rangle$ is c-supplemented in G and thus c-supplemented in H by [10, Lemma 2.1(1)]. By Lemma 2.1, we have $\langle x\rangle\Phi(H_2)/\Phi(H_2) = H_2/\Phi(H_2)$. But then $|H/\Phi(H_2) : H_q\Phi(H_2)/\Phi(H_2)| = |\langle x\rangle\Phi(H_2)/\Phi(H_2)| = 2$, a contradiction.

Case 2. Every minimal subgroup of P is c-supplemented in G and P is an abelian 2-group. Let $\langle x\rangle$ be a subgroup of H_2 not contained In $\Phi(H_2)$. If $|x| = 2$, then we can get a contradiction by using exactly the same argument as we did in Case 1.Therefore we may assume that $\Omega_1(H_2) \leqslant \Phi(H_2)$, where $\Omega_1(H_2)$ is a subgroup generated by all minimal subgroup of H_2. Since H is a minimal non 2-nilpotent group and $\Phi(H_2)H_q < H$, $\Phi(H_2)H_q$ is a nilpotent group. As a result, H_q acts trivially on $\Omega_1(H_2)$. Note that H_2 is also an abelian 2-group, by [4, Theorem2. 4] H_q also acts trivially on H_2, a contradiction.

Case 3. Every minimal subgroup of P is c-supplemented in G and P is a non-abelian quaternion free 2-group. If H_2 is abelian, then we can get the same contradiction as Case 2. Hence we may assume that H_2 is also a non-abelian quaternion free 2-group. Applying [6, Theorem 2.7], H_q acts on $H_2/\Phi(H_2)$ with at least one fixed point. Bare in mind that $H_2/\Phi(H_2)$ is a minimal normal subgroup of $H/\Phi(H_2)$, we have $|H_2/\Phi(H_2)| = 2$, again a contradiction.

The above proof shows that PQ is 2-nilpotent and thus $Q \trianglelefteq PQ$. Note that P is a normal subgroup of G, we have $[P, Q] = 1$. Note that we can choose Q to be a Sylow q-subgroup of G for any $q \neq p$, we have $[P, O^2(G)] = 1$. Let H/K be a G-chief factor of P. The fact $[P, O^{2'}(G)] = 1$ yields that $G/C_G(H/K)$ is a 2-group. But by [3, A, Lemma 13.6], we have $O_2(G/C_G(H/K)) = 1$. Consequently $G/C_G(H/K) = 1$ for any G-chief factor of P, in other words, $P \leqslant Z_\infty(G)$. □

As an application of Property 2.2, we have:

Corollary 2.3. *If all minimal subgroups of G_2 and all cyclic subgroups of G_2 with order 4 (if G_2 is neither abelian nor quaternion free) are c-supplemented in G, then G is 2-nilpotent.*

Proof. Suppose this corollary is not true and let G be a counterexample with minimal order. Obviously the hypothesis is inhered by all subgroups of G, G is actually a minimal non 2-nilpotent group. Hence G_2 is a normal subgroup in G. Applying Property 2.2 to G_2, we get a contradiction. □

By combining [2, Theorem 1.1] and Property 2.2, we have:

Lemma 2.4. *Let P be a normal p-subgroup of G. If all cyclic subgroups of P with order p or 4 (if P is a non-abelian and not quaternion free 2-group) are c-supplement in G, then $P \leqslant Z_{\mathcal{U}}(G)$.*

Next, we will show that if that some class of p-subgroup is c-normal in G, then G is p-solvable.

Lemma 2.5. *If G_p is c-normal in G then G is p-solvable.*

Proof. Suppose this Lemma is not true and considered G to be a counterexample with minimal order. Clearly the hypothesis holds for any quotient group of G, the minimal choice of G implies that $O_p(G) = O_{p'}(G) = 1$. By the definition of c-normal, there exit a normal subgroup H of G such that $G = G_pH$ and $H \cap G_p \leqslant (G_p)_G$. But $(G_p)_G = O_p(G) = 1$, hence H is a p' normal subgroup of G. The fact $O_{p'}(G) = 1$ indicates that $H = 1$ and thus $G = G_p$, a contradiction. □

Lemma 2.6. *Let d_p be a prime power divisor of $|G_p|$ with $d_p > 1$. If every subgroup of $|G_p|$ with order d_p and $2d_p$ (If $p = 2$ and G_2 is neither abelian nor quaternion free)) is c-normal in G then G is p-solvable.*

Proof. Suppose this Lemma is not true and considered G to be a counterexample with minimal order. According to Lemma 2.5 we may assume that $1 < d_p < |G_p|$.

(1) $O_{p'}(G) = 1$.
Since the hypothesis holds for $G/O_{p'}(G)$, the minimal choice of G yields that $O_{p'}(G) = 1$.

(2) *Every subgroup with order d_p and $2d_p$ (if $p = 2$ and G_2 is neither abelian nor quaternion free) is normal in G. In particular, $O_p(G) > 1$.*
Suppose there exit a subgroup K with order d_p or $2d_p$ (if $p = 2$) that is not normal in G. Then there exit a proper normal subgroup

L such that $G = KL, K \cap L \leqslant K_G$. Since G/L is a p-group, we can find a normal subgroup M containing L such that $|G/M| = p$. But $d_p < |G_p|$ so M still satisfies the hypothesis of this Lemma, thus M is p-solvable by the minimal choice of G and so is G.

(3) *Let N is a minimal normal subgroup contained in $O_p(G)$, then $|N| = d_p$.*
If $d_p > |N|$, then G/N satisfies the hypotheses of this Lemma and thus is p-solvable by the minimal choice of G. Since N is a p-group we can get that G is p-solvable, a contradiction.

(4) *$d_p = p$.*
Suppose $d_p > p$. From (3) we know that $|N| = d_p > p$ and thus N is not cyclic. Let H be a subgroup of G_p containing N such that $|H : N| = p$. Let M_1 and M_2 be two different maximal subgroup of H. By (2), both M_1 and M_2 are normal in G. Consequently $H/N = M_1M_2/N$ is also normal in G/N. Hence every subgroup of G/N with order p is normal in G/N. If $p = 2$ and and G_2 is neither abelian nor quaternion free, then by using a similar argument we know that every subgroup of G/N with order 4 is also normal in G/N. As a result, we see that G/N satisfies the hypothesis of this Lemma and the choice of G implies that G/N is p-solvable, thus G is p-solvable, a contradiction.

(5) *Final contradiction.*
If $p = 2$, then from (4) and Corollary 2.3, G is 2-nilpotent. So we may assume p is an odd prime. By (2) and (4) we know that every subgroup with order p is normal. Take a subgroup $\langle x\rangle$ with order p , it's easy to see that $G_p \leqslant C_G\langle x\rangle$. If $C_G\langle x\rangle < G$ then from the choice of G we know that $C_G\langle x\rangle < G$ is p-solvable. But $G/C_G\langle x\rangle < G$ is cyclic and thus G is p-solvable, contradict to the choice of G. Therefore we have $C_G\langle x\rangle = G$, that is, every minimal subgroup of order p is contained $Z(G)$. From Ito's theorem G is p-nilpotent, a contradiction. □

Now, we will study the properties of p-hypercyclically embedding. In [7, p. 217], a normal subgroup E is said to be hypercyclically embedded in G if every chief factor of G below E is cyclic. If a normal subgroup E is hypercyclically (p-hypercyclically) embedded in G, then E is solvable (p-solvable) and every normal subgroup of G contained in E is also hypercyclically (p-hypercyclically) embedded in G. The following lemma shows that for a p-solvable normal subgroup E, we can deduce that E

is hypercyclically (p-hypercyclically) embedded in G from the maximal p-nilpotent normal subgroup of E $F_p(E)$.

Lemma 2.7. *A p-solvable normal subgroup E is hypercyclically (p-hypercyclically) embedded in G if and only if $F_p(E)$ is hypercyclically (p-hypercyclically) embedded in G. In particular, if E is a p-solvable normal subgroup with $O_{p'}(E) = 1$, then E is hypercyclically embedded in G if and only if $O_p(E)$ is hypercyclically embedded in G.*

Proof. We only need to prove the sufficiency. Suppose the assertion is false and let (G, E) be a counterexample with $|G||E|$ minimal. We claim that $O_{p'}(E) = 1$. Indeed, since $F_p(E/O_{p'}(E)) = F_p(E)/O_{p'}(E)$, it's easy to verify that the hypothesis still holds for $(G/O_{p'}(E), E/O_{p'}(E))$. If $O_{p'}(E) \neq 1$, then the the minimal choice of (G, E) implies that $E/O_{p'}(E)$ hypercyclically (or p-hypercyclically) embedded in $G/O_{p'}(E)$. Since we have that $O_{p'}(E)$ is a normal subgroup of G contained in E, $O_{p'}(E)$ is hypercyclically (or p-hypercyclically) embedded in G . Therefore we have E hypercyclically (or p-hypercyclically) embedded in G, a contradiction.

Let N be a minimal normal subgroup of G contained in E. N is an abelian normal p-subgroup since E is p-solvable and $O_{p'}(E) = 1$. Consider the group $C_E(N)/N$. Let $L/N = O_{p'}(C_E(N)/N)$ and K be the Hall p' subgroup of L. Then $L = KN$. Since $K \leqslant L \leqslant C_E(N)$, we have $K = O_{p'}(L) \leqslant O_{p'}(G) = 1$. Consequently $O_{p'}(C_E(N)/N) = 1$ and we have $F_p(C_E(N)/N) = O_p(C_E(N)/N) \leqslant O_p(E)/N = F_p(E)/N$. As a result, we know that the hypothesis holds for $(G/N, C_E(N)/N)$ and the minimal choice of (G, E) yields that $C_E(N)/N$ is hypercyclically (or respectively p-hypercyclically) embedded in G/N. But $N \leqslant F_p(G)$ and thus N is also hypercyclically (or p-hypercyclically) embedded in G. Thus $C_E(N)$ is hypercyclically (or p-hypercyclically) embedded in G.

Since N is a normal p-subgroup which is hypercyclically (or respectively p-hypercyclically) embedded in G, we have that $|N| = p$. It yields $G/C_G(N)$ is a cyclic group. As a result, $EC_G(N)/C_G(N)$ is hypercyclically embedded in $G/C_G(N)$. Note that $E/C_E(N) = E/E \cap C_G(N)$ is G-isomorphic with $EC_G(N)/C_G(N)$, therefore $E/C_E(N)$ is hypercyclically embedded in $G/C_E(N)$. But $C_E(N)$ is also hypercyclically (or p-hypercyclically) embedded in G hypercyclically (or p-hypercyclically) embedded in G and thus E is hypercyclically (or p-hypercyclically) embedded in G, a final contradiction. □

Denote $\mathcal{A}(p-1)$ as the formation of all abelian groups of exponent divisible by $p-1$. The following proposition is well known:

Lemma 2.8 ([12], Theorem 1.4)**.** *Let H/K be a chief factor of G, p is a prime divisor of $|H/K|$, then $|H/K| = p$ if and only if $G/C_G(H/K) \in \mathcal{A}(p-1)$.*

Let f be a formation function, and N be a normal subgroup of G. We say that G acts f-centrally on E if $G/C_G(H/K) \in f(p)$ for every chief factor H/K of G below E and every prime p dividing $|H/K|$ ([3], p. 387, Definitions 6.2). Fixing a prime p, define a formation function g_p as follows:

$$g_p(q) = \begin{cases} \mathcal{A}(p-1) & (\text{if } q = p) \\ \text{all finite group} & (\text{if } q \neq p) \end{cases}$$

From Lemma 2.8, we can see that E is p-hypercyclically embedded in G if and only if G acts g_p-centrally on E. By applying [3, p. 388, Theorem 6. 7], we get the following useful results:

Lemma 2.9. *A normal subgroup E of G is p-hypercyclically embedded in G if and only if $E/\Phi(E)$ is p-hypercyclically embedded in $G/\Phi(E)$.*

Lemma 2.10. *Let K and L be two normal subgroup of G contained in E. If E/K is p-hypercyclically embedded in G/K and E/L is p-hypercyclically embedded in G/L, then $E/L \cap K$ is p-hypercyclically embedded in $G/L \cap K$.*

The following proposition indicates that when $d_p = p$, the conclusion of Theorem A holds.

Proposition 2.11. *Let E be a normal subgroup of G. If all cyclic subgroups of E_p with order p and 4 (if $p = 2$ and E_p is not an abelian nor quaternion free 2-group) are c-normal in G, then E is p-hypercyclically embedded in G.*

Proof. Suppose this Theorem is not true and let (G, E) be a counterexample such that $|G| + |P|$ is minimal. Suppose $O_{p'}(E) \neq 1$, it's easy to verifies that $(G/O'_p(E), E/O'_p(E))$ satisfies the hypothesis of this Theorem and thus $E/O'_p(E)$ is p-hypercyclically embedded in $G/O_{p'}(E)$ by the minimal choice of (G, E). But then E is p-hypercyclically embedded in G. This contradiction implies that $O_{p'}(E) = 1$.

From Lemma 2.6 and Lemma 1.2(3) we know that E is p-solvable and from Corollary F we know that $O_p(E) \leqslant Z_{\mathcal{U}}(G)$, thus $E \leqslant Z_{\mathcal{U}}(G)$ by Lemma 2.7, a contradiction. □

With the aid of all the preceding results, we can now prove the main theorem of this section.

Proof of Theorem A. Suppose this is not true and let (G, E) be a counterexample such that $|G| + |E|$ is minimal. If $|E_p| = p$, then E_p itself is c-normal in G and by Lemma 1.2, E_p is also c-normal in E. By Lemma 2.5 we know that E is p-solvable and consequently E is p-hypercyclically embedded in G since $|E_p| = p$. Therefore we may assume that $|E_p| > p$ and $1 < d_p < |E_p|$. By Proposition 2.11, we may further assume that $d_p > p$. Similar to step (1) in the proof of Lemma 2.6, we have $O_{p'}(E) = 1$. By Lemma 2.6, E is p-solvable. Let N be a minimal normal subgroup of G contained in E, then obviously $N \leqslant O_p(E)$.

(1) $|N| > p$.
Suppose $|N| = p$, then $d_p > |N|$ by our assumption that $d_p > p$. Hence $(G/N, E/N)$ also satisfies the hypothesis of this Theorem and therefore E/N is p-hypercyclically embedded in G/N by the choice of (G, E). If $|N| = p$, then E is p-hypercyclically embedded in G, a contradiction.

(2) $d_p > |N|$.
By Lemma 2.1 we have $d_p \geqslant |N|$. Suppose that $d_p = |N|$. Since $d_p < |E_p|$ by our assumption, let H be a subgroup of E_p such that N is a maximal subgroup of H . By (1), N is not cyclic and so is H. Hence we can choose a maximal subgroup K of H other than N . Obviously we have $H = NK$. If $N \cap K = 1$, then $|N| = |H|/|K| = p$, contradict to (1). Thus $N \cap K \neq 1$ and $|K : K \cap N| = |KN : N| = |H : N| = p$. Since $K_G \cap N \leqslant K \cap N < N$, we have $K_G \cap N = 1$. If $K_G \neq 1$, then $H = NK_G$ and $K = K \cap K_G N = (K \cap N)K_G$. As a result, $|K_G| = |K|/|K \cap N| = p$. But this contradicts to (1) because now we find a normal subgroup of G contained in $O_p(G)$ with order p. Therefore we have $K_G = 1$. Since $|K| = |N| = d_p$, K is c-normal in G by the hypothesis of this theorem. So there exists a proper normal subgroup L of G such that $G = KL$ and $K \cap L \leqslant K_G = 1$. Since $K \cap N \neq 1$ and $K \cap L = 1$, we have $N \neq L$ and thus $N \cap L = 1$. Consequently $|NL| = |N||L| = |K||L| = |KL| = |G|$ and thus $G = NL$. Let M an maximal subgroup of G containing L , then $|G : M| = p$ since G/L is a p-group. Obviously $G = NM$ and $N \cap M = 1$. But then $|N| = |G : M| = p$, a contradiction to (1).

(3) *N is the unique minimal normal subgroup of G contained in E and $N \nleqslant \Phi(E)$.*
Since $d_p > |N|$ by (2), it's easy to verify that $(G/N, E/N)$ still satisfies the hypothesis of this theorem. The minimal choice of (G, E) implies E/N is p-hypercyclically embedded in G/N. From

Lemma 2.10, N must be the unique minimal normal subgroup of G contained in E. From Lemma 2.9, we have $N \nleq \Phi(E)$.

(4) *Final contradiction.*
By (3), there exit a maximal subgroup M of E such that $E = NM$. $E_p = E_p \cap NM = N(E_p \cap M)$. Clearly $E_p \cap M < E_p$ since N is not contained in M, so we can choose a maximal subgroup K of E_p such that $E_p \cap M \leqslant K$. Note that now $E_p = NK$, if $N \cap K = 1$, then by simple calculation we know that $|N| = p$, contradict to (1). Hence $1 < N \cap K < N$. Clearly $|N| < d_p \leqslant |K|$, so we can choose a subgroup H with order d_p such that $1 < N \cap K < H \leqslant K$. Because $N \neq H$ and N is the unique minimal normal subgroup of G contained in E, we have $H_G = 1$. By the hypothesis of this Theorem, H is c-normal in E and hence there exit a normal subgroup L of G such that $G = HL$ and $H \cap L \leqslant H_G = 1$. Therefore $E = E \cap HL = H(E \cap L)$ and $E \cap L$ is a non trivial normal subgroup of G contained in E. But since $H \cap (E \cap L) \leqslant H \cap L = 1$ and $H \cap N \neq 1$, we have $N \nleq E \cap L$, contradicts to N being the unique minimal normal subgroup of G contained in E. □

Remark. The conclusion of Theorem A does not hold if we replace "c-normal" with "c-supplemented" in the hypothesis. One can take A_5 for a example. Obviously every subgroup of A_5 with order 5 is c-supplemented in A_5, but A_5 is not 5-hypercyclically embedded in itself.

Corollary 2.12. *Let $d_p(G)$ be a prime power divisor of $|G_p|$ satisfying the following properties: If $|G_p| = p$ then $d_p(G) = |G_p| = p$; if $|G_p| > p$ then $1 < d_p(G) < |G_p|$. Suppose that all of the subgroups of G_p with order $d_p(G)$ and $2d_p(G)$ (if $p = 2$ and G_p is not an abelian nor a quaternion free 2-group) are c-normal in G. Then G is p-supersolvable.*

Corollary 2.13. *Let E be a normal finite group of G and suppose that G/E is p-supersolvable. Suppose that all of the subgroups of E_p with order d_p and $2d_p$ (if $p = 2$ and E_p is not an abelian nor quaternion free 2-group) are c-normal in G. Then G is p-supersolvable.*

It is clear that G is p-nilpotent implies G is p-supersolvable but the converse is not true. However, The following lemma reveals a connection between p-nilpotent and p-supersolvable through the p-nilpotency of $N_G(G_p)$.

Lemma 2.14. *G is p-nilpotent if and only if G is p-supersolvable and $N_G(G_p)$ is p-nilpotent.*

Proof. Suppose this lemma is not true and let G be a minimal counterexample. Since $N_{G/O_{p'}(G)}(G_pO_{p'}(G)/O_{p'}(G)) = N_G(G_p)O_{p'}(G)/O_{p'}(G)$, we have that $O_{p'}(G) = 1$ by induction.

Let N be a minimal normal subgroup of G. Then $|N| = p$ since G is p-supersolvable and $O_{p'}(G) = 1$. It's easy to verify that G/N still satisfy the hypothesis of this lemma. Again from induction we know that N is the unique minimal normal subgroup of G, $\Phi(G) = 1$ and $N = C_G(N)$. But the fact $|N| = p$ implies that $G_p \leqslant C_G(N)$. Therefore we have $G_p = N$. It follows that $G = N_G(G_p)$ is p-nilpotent, a contradiction. □

Now we can prove Theorem B by using Theorem A and Lemma 2.14.

Proof of Theorem B. Suppose this is not true. Let (G, E) be a counterexample such that $|G| + |E|$ is minimal. We first claim that E is p-nilpotent. Since $N_G(E_p)$ is p-nilpotent, $N_E(E_p) = N_G(E_p) \cap E$ is also p-nilpotent. If E_p is abelian, then $N_E(E_p) = C_E(E_p)$ and hence E is p-nilpotent by Burnside's theorem. If E_p is not abelian, then every subgroup of E_p with order d_p (d_p is a prime power divisor of E_p and $1 < d_p < |E_p|$) and $2d_p$ (if $p = 2$ and E_p is not quaternion free) is c-normal in E by hypothesis and Lemma 1.2(3). We know from Corollary 2.12 that E is p-supersolvable. It follows from Lemma 2.14 that E is p-nilpotent.

By induction, we have $O_{p'}(E) = 1$ and thus E must be a p-group. Therefore $G = N_G(E) = N_G(E_p)$ is p-nilpotent, a contradiction. □

Remark. In Theorem A we ask E_p to be c-normal in G provided that $|E_p| = p$. But we don't impose the c-normality on E_p in Theorem B under the same circumstance because E_p is abelian if $|E_p| = p$.

Corollary 2.15. *Suppose $N_G(G_p)$ is p-nilpotent. If either G_p is abelian or every subgroup of G_p with order d_p (d_p is a prime power divisor of G_p and $1 < d_p < |G_p|$) and $2d_p$ (if $p = 2$ and G_p is not quaternion free) is c-normal in G, then G is p-nilpotent.*

3. Applications

In this section, we give some applications to show that we can apply our results to generalize some known results.

Corollary 3.1 ([1, Theorem 3.4])**.** *Let $\mathcal{F}$ be a saturated formation containing $\mathcal{U}$. If all minimal subgroups and all cyclic subgroups with order 4 of $G^{\mathcal{F}}$ are c-normal in G, then $G \in \mathcal{F}$.*

Proof. From Theorem A, we know that $G^{\mathcal{F}}$ is p-hypercentrally embedded in G for all $p \in \pi(G^{\mathcal{F}})$ and thus $G^{\mathcal{F}} \leqslant Z_{\mathcal{U}}(G)$. Since $\mathcal{F}$ be a saturated formation containing $\mathcal{U}$, we have that $Z_{\mathcal{U}}(G) \leqslant Z_{\mathcal{F}}(G)$. Consequently $G \in \mathcal{F}$ because $G/G^{\mathcal{F}} \in \mathcal{F}$ and $G^{\mathcal{F}} \leqslant Z_{\mathcal{U}}(G) \leqslant Z_{\mathcal{F}}(G)$. □

Corollary 3.2 ([8, Theorem 0.1]). *Let E be a normal subgroup of a group G of odd order such that G/E is supersolvable. Suppose that every non-cyclic Sylow subgroup P of E has a subgroup D such that $1 < |D| < |P|$ and all subgroups H of P with order $|H| = |D|$ are c-normal in G. Then G is supersolvable.*

Proof. Let p be the minimal prime divisor of $|E|$. If E_p is cyclic, then E is p-nilpotent by [13, Lemma 2.8]. If E_p is not cyclic, then by Corollary B, E is p-supersolvable and thus p-nilpotent since now p is the minimal prime divisor of $|E|$. By repeating this argument we know that E has a Sylow-tower and therefore E is solvable. Let p be any prime divisor of $|E|$, If E_p is cyclic, then E is p-hypercentrally embedded in G since now E is p-solvable. If E_p is not cyclic, E is also p-hypercentrally embedded in G by Theorem A. As a result we have $E \leqslant Z_{\mathcal{U}}(G)$. It follows that G is supersolvable since G/E is supersolvable and $E \leqslant Z_{\mathcal{U}}(G)$. □

Corollary 3.3 ([5, Theorem 3.1]). *Let p be an odd prime dividing the order of a group G and P a Sylow-subgroup of G. If $N_G(P)$ is p-nilpotent and every maximal subgroup of P is c-normal in G, then G is p-nilpotent.*

By noting the fact that if p is a prime such that $(|G|, p-1) = 1$, then G is p-nilpotent if and only if G is p-supersolvable, we have the following two corollary:

Corollary 3.4 ([5, Theorem 3.4]). *Let p be the smallest prime number dividing the order of a group G and P a Sylow p-subgroup of G. If every maximal subgroup of P is c-normal in G, then G is p-nilpotent.*

Proof. If $|P| = p$, then G is p-nilpotent by [13, Lemma 2.8]. If $|P| > p$, then by Corollary 2.12, G is p-supersolvable. Hence G is p-nilpotent. □

Corollary 3.5 ([5, Theorem 3.6]). *Let p be the smallest prime number dividing the order of group G and P a Sylow p-subgroup of G. If every minimal subgroup of $P \cap G'$ is c-normal in G and when $p = 2$, either every cyclic subgroup of $P \cap G'$ with order 4 is also c-normal in or P is quaternion-free, then G is p-nilpotent.*

Corollary 3.6 ([5, Corollary 3.9]). *Let p be an odd prime number dividing the order of a group G and P a Sylow p-subgroup of G. If every minimal subgroup of $P \cap G'$ is c-normal in G, then G is p-supersolvable.*

References

[1] Ballester-Bolinches, A.; Wang, Yanming, Finite groups with some C-normal minimal subgroups. J. Pure Appl. Algebra 153 (2000), no. 2, 121-127.

[2] Asaad, M.; Ramadan, M., Finite groups whose minimal subgroups are c-supplemented. *Comm. Algebra* 36 (2008), no. 3, 1034-1040.

[3] Doerk,R. and Hawkes, T., Finite soluble groups, Walter De Gruyter, Berlin-New York, 1992.

[4] Terence M. Gagen, *Topics in finite groups*, Cambridge University press, London, 1976.

[5] Guo, Xiuyun; Shum, K. P., On c-normal maximal and minimal subgroups of Sylow p-subgroups of finite groups. *Arch. Math. (Basel)* 80 (2003), no. 6, 561-569.

[6] Dornhoff, Larry, M-groups and 2-groups. *Math. Z.* 100 1967 226-256.

[7] R. Schmidt, Subgroup Lattices of Groups, *de Gruyter*, Berlin, 1994.

[8] Skiba, Alexander N., A note on c-normal subgroups of finite groups. Algebra Discrete Math. 2005, no. 3, 85-95.

[9] Jaraden, Jehad J.; Skiba, Alexander N., On c-normal subgroups of finite groups. *Comm. Algebra* 35 (2007), no. 11, 3776-3788

[10] Ballester-Bolinches, A.; Wang, Yanming; Xiuyun, Guo, c-supplemented subgroups of finite groups. *Glasg. Math. J.* 42 (2000), no. 3, 383-389.

[11] Wang, Yanming, c-normality of groups and its properties. *J. Algebra* 180 (1996), no. 3, 954-965.

[12] Weinstein, M., etl.(editor), Between nilpotent and solvable. *Polygonal Publishing House*, Passaic (1982).

[13] Wei, Huaquan; Wang, Yanming, On c*-normality and its properties. *J. Group Theory* 10 (2007), no. 2, 211-223.

Contact information

N. Su School of Mathematics, Sun Yatsen University, Guangzhou, 510275, China
E-Mail(s): `mc04sn@mail2.sysu.edu.cn`

Y. Wang Lingnan College and School of Mathematics, Sun Yatsen University, Guangzhou, 510275, China
E-Mail(s): `stswym@mail.sysu.edu.cn`

Received by the editors: 08.02.2013
and in final form 22.04.2013.

Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **19** (2015). Number 2, pp. 283–294

Symmetric modules over their endomorphism rings

B. Ungor, Y. Kurtulmaz, S. Halicioglu, A. Harmanci

Communicated by V. Mazorchuk

Abstract. Let R be an arbitrary ring with identity and M a right R-module with $S = \mathrm{End}_R(M)$. In this paper, we study right R-modules M having the property for $f, g \in \mathrm{End}_R(M)$ and for $m \in M$, the condition $fgm = 0$ implies $gfm = 0$. We prove that some results of symmetric rings can be extended to symmetric modules for this general setting.

1. Introduction

Throughout this paper R denotes an associative ring with identity, and modules are unitary right R-modules. All right-sided concepts and results have left-sided counterparts. For a module M, $S = \mathrm{End}_R(M)$ denotes the ring of right R-module endomorphisms of M. Then M is a left S-module, right R-module and (S, R)-bimodule. In this work, for the (S, R)-bimodule M, $r_R(.)$ and $l_M(.)$ denote the right annihilator of a subset of M in R and the left annihilator of a subset of R in M, respectively. Similarly, $l_S(.)$ and $r_M(.)$ are the left annihilator of a subset of M in S and the right annihilator of a subset of S in M, respectively.

A ring is *reduced* if it has no nonzero nilpotent elements. In [13], Krempa introduced the notion of the rigid endomorphism of a ring. An

2010 MSC: 13C99, 16D80.

Key words and phrases: symmetric modules, reduced modules, rigid modules, semicommutative modules, abelian modules, Rickart modules, principally projective modules.

endomorphism α of a ring R is said to be *rigid* if $a\alpha(a) = 0$ implies $a = 0$ for $a \in R$. According to Hong-Kim-Kwak [11], R is said to be an *α-rigid ring* if there exists a rigid endomorphism α of R. In [15], a ring R is *symmetric* if for any $a, b, c \in R$, $abc = 0$ implies $bac = 0$. This is equivalent to $abc = 0$ implies $acb = 0$. A ring R is called *semicommutative* if for any $a, b \in R$, $ab = 0$ implies $aRb = 0$. A ring R is called *abelian* if every idempotent is central, that is, $ae = ea$ for any $e^2 = e$, $a \in R$.

The reduced ring concept was extended to modules by Lee and Zhou in [16], that is, a right R-module M is called *reduced* if for any $m \in M$ and any $a \in R$, $ma = 0$ implies $mR \cap Ma = 0$. Similarly, in [2] and [3], Harmanci et al. extended the rigid ring notion to modules. A right R-module M is called *rigid* if for any $m \in M$ and any $a \in R$, $ma^2 = 0$ implies $ma = 0$. Reduced modules are certainly rigid, but the converse is not true in general. A right R-module M is said to be *semicommutative* if for any $m \in M$ and any $a \in R$, $ma = 0$ implies $mRa = 0$. Abelian modules are introduced in the context by Roos in [21] and studied by Goodearl and Boyle in [9]. A module M is called *abelian* if for any $f \in S$, $e^2 = e \in S$, $m \in M$, we have $fem = efm$. Note that M is an abelian module if and only if S is an abelian ring. The concept of (quasi-)Baer rings was extended by Rizvi and Roman [19] to the general module theoretic setting, by considering a right R-module M as an (S, R)-bimodule. A module M is called *Baer* if for all submodules N of M, $l_S(N) = Se$ with $e^2 = e \in S$. A submodule N of M is said to be *fully invariant* if it is also a left S-submodule of M. Then the module M is said to be *quasi-Baer* if for all fully invariant submodules N of M, $l_S(N) = Se$ with $e^2 = e \in S$. Motivated by Rizvi and Roman's work on (quasi-)Baer modules, the notion of principally quasi-Baer modules initially appeared in [22]. The module M is called *principally quasi-Baer* if for any $m \in M$, $l_S(Sm) = Sf$ for some $f^2 = f \in S$. Finally, the concept of right Rickart rings (or right principally projective rings) was extended to modules in [20], that is, the module M is called *Rickart* if for any $f \in S$, $r_M(f) = eM$ for some $e^2 = e \in S$, equivalently, $\mathrm{Ker} f$ is a direct summand of M.

In this paper, we investigate some properties of symmetric modules over their endomorphism rings. We prove that if M is a symmetric module, then S is a symmetric ring. The converse is true for Rickart or 1-epiretractable (in particular, free or regular) or principally projective modules. Among others it is shown that M is a symmetric module in one of the cases: (1) S is a strongly regular ring, (2) $E(M)$ is a symmetric module where $E(M)$ is the injective hull of M. Also, we give a characterization of symmetric rings in terms of symmetric modules, that is, a ring is symmetric if and only if every cyclic projective module is symmetric.

In what follows, by $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$ and $\mathbb{Z}/n\mathbb{Z}$ we denote, respectively, integers, rational numbers, the ring of integers modulo n and the $\mathbb{Z}$-module of integers modulo n.

2. Symmetric modules

Let M be a simple module. By Schur's Lemma, $S = \mathrm{End}_R(M)$ is a division ring and clearly for any $m \in M$ and f, $g \in S$, $fgm = 0$ implies $gfm = 0$. Also every module with a commutative endomorphism ring satisfies this property. A right R-module M is called *R-symmetric* ([15] and [18]) if whenever $a, b \in R$, $m \in M$ satisfy $mab = 0$, we have $mba = 0$. R-symmetric modules are also studied by the last two authors of this paper in [2]. Motivated by this we investigate properties of the class of modules which are symmetric over their endomorphism rings.

Definition 2.1. Let M be an R-module with $S = \mathrm{End}_R(M)$. The module M is called *S-symmetric* whenever $fgm = 0$ implies $gfm = 0$ for any $m \in M$ and f, $g \in S$.

From now on *S-symmetric* modules will be called *symmetric* for the sake of shortness. Note that a submodule of a symmetric module need not be symmetric. Therefore we can give the following definition.

Definition 2.2. Let M be an R-module with $S = \mathrm{End}_R(M)$ and N an R-submodule of M. The module N is called a *symmetric submodule* of M whenever $fgn = 0$ implies $gfn = 0$ for any $n \in N$ and f, $g \in S$.

We mention some examples of modules that are symmetric over their endomorphism rings.

Examples 2.3. (1) Let M be a cyclic torsion $\mathbb{Z}$-module. Then M is isomorphic to the $\mathbb{Z}$-module $(\mathbb{Z}/\mathbb{Z}p_1^{n_1}) \oplus (\mathbb{Z}/\mathbb{Z}p_2^{n_2}) \oplus \ldots \oplus (\mathbb{Z}/\mathbb{Z}p_t^{n_t})$ where p_i $(i = 1, \ldots, t)$ are distinct prime integers and n_i $(i = 1, \ldots, t)$ are positive integers. $\mathrm{End}_{\mathbb{Z}}(M)$ is isomorphic to the commutative ring $(\mathbb{Z}_{p_1^{n_1}}) \oplus (\mathbb{Z}_{p_2^{n_2}}) \oplus \ldots \oplus (\mathbb{Z}_{p_t^{n_t}})$. So M is a symmetric module.

(2) Let p be any prime integer and $M = (\mathbb{Z}/p\mathbb{Z}) \oplus \mathbb{Q}$ a $\mathbb{Z}$-module. Then S is isomorphic to the matrix ring $\left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a \in \mathbb{Z}_p, b \in \mathbb{Q} \right\}$ and so M is a symmetric module.

There are symmetric modules of which their endomorphism rings are symmetric, namely simple modules and vector spaces. Our next endeavor is to find conditions, under which the property of M being symmetric is equivalent to S being symmetric. A module M is called *n-epiretractable* [8] if every n-generated submodule of M is a homomorphic image of M. We show that Rickart modules and 1-epiretractable modules play an important role in this direction.

Theorem 2.4. *If M is a symmetric module, then S is a symmetric ring. The converse holds if M satisfies any of the following conditions.*

(1) *M is a Rickart module.*

(2) *M is a 1-epiretractable module.*

Proof. Let $f, g, h \in S$ with $fgh = 0$. Since M is symmetric, $0 = (fg)hm = (gf)hm$ for all $m \in M$. Then $gfh = 0$. Hence S is symmetric. Conversely, let M be a Rickart module with $fgm = 0$ for $f, g \in S$ and $m \in M$. Since M is a Rickart module, there exists $e^2 = e \in S$ such that $r_M(fg) = eM$. Hence $fge = 0$. There exists $m' \in M$ such that $m = em'$. By multiplying em' from the left by e, we have $em = eem' = em' = m$. By using symmetricity of S repeatedly, it can be easily seen that $0 = fge = 1f(ge)$ implies $1(ge)f = gef = 0$ and then $gfe = 0$. Hence $gfm = gfem = 0$. Thus M is symmetric. Assume now that M is 1-epiretractable. Then there exists $h \in S$ such that $mR = hM$. Then we have $fghM = 0$, and so $fgh = 0$. Since S is symmetric, $gfh = 0$. This implies that $gfm = 0$. Therefore M is symmetric. $\square$

Corollary 2.5. *A free R-module is symmetric if and only if its endomorphism ring is symmetric.*

Proof. Let F be a free R-module. Clearly, for any $m \in F$ there exists $f \in \mathrm{End}_R(F)$ such that $fF = mR$. Thus F is a 1-epiretractable module. Therefore Theorem 2.4(2) completes the proof. $\square$

Recall that a ring R is said to be *regular* if for any $a \in R$ there exists $b \in R$ with $a = aba$, while a ring R is called *strongly regular* if for any $a \in R$ there exists $b \in R$ such that $a = a^2b$. It is well known that a ring is strongly regular if and only if it is reduced and regular (see [14]). Also every reduced ring is symmetric by [5, Theorem I.3]. Then we have the following result.

Corollary 2.6. *If S is a strongly regular ring, then M is a symmetric module.*

Proof. Assume that S is a strongly regular ring. Then S is a symmetric and regular ring. By [4, Proposition 2.6], M is a Rickart module. The rest is clear from Theorem 2.4. $\square$

A module M is called *regular* (in the sense of Zelmanowitz [23]) if for any $m \in M$ there exists a right R-homomorphism $M \stackrel{\phi}{\to} R$ such that $m = m\phi(m)$. Then we have the following result.

Corollary 2.7. *If M is a regular module, then the following are equivalent.*

(1) *M is a symmetric module.*

(2) *S is a symmetric ring.*

Proof. Every cyclic submodule of a regular module is a direct summand, and so it is 1-epiretractable. It follows from Theorem 2.4. $\square$

In [7], Evans introduced principally projective modules as follows: An R-module M is called *principally projective* if for any $m \in M$, $r_R(m) = eR$, where $e^2 = e \in R$. The ring R is called *right principally projective* [10] if the right R-module R is principally projective. The concept of left principally projective rings is defined similarly.

In this note, we call the module M *principally projective* if M is principally projective as a left S-module, that is, for any $m \in M$, $l_S(m) = Se$ for some $e^2 = e \in S$.

It is straightforward that all Baer modules are principally projective. However quasi-Baer modules need not be principally projective. Namely, matrix rings over a commutative domain R are quasi-Baer rings; but if the commutative domain R is not Prüfer, matrix rings over R will not be principally projective rings. And every quasi-Baer module is principally quasi-Baer. There are principally projective modules which may not be quasi-Baer or Baer (see [6, Example 8.2]).

Example 2.8. Let R be a Prüfer domain (a commutative ring with an identity, no zero divisors, and all finitely generated ideals are projective) and M denote the right R-module $R \oplus R$. By ([12], page 17), S is a 2×2 matrix ring over R and it is a Baer ring. Hence M is Baer and so a principally projective module.

Note that the endomorphism ring of a principally projective module may not be a right principally projective ring in general. For if M is a principally projective module and $g \in S$, then we distinguish the two cases: Ker$g = 0$ and Ker$g \neq 0$. If Ker$g = 0$, then for any $f \in r_S(g)$, $gf = 0$ implies $f = 0$. Hence $r_S(g) = 0$. Assume that Ker$g \neq 0$. There exists a nonzero $m \in M$ such that $gm = 0$. By hypothesis, $g \in l_S(m) = Se$ for some $e^2 = e \in S$. In this case $g = ge$ and so $r_S(g) \leqslant (1-e)S$. The following example shows that this inclusion is strict.

Example 2.9. Let Q be the ring and N the Q-module constructed by Osofsky in [17]. Since Q is commutative, we can just as well think of N as a right Q-module. If $S = \mathrm{End}_Q(N)$, then N is a principally projective module. Identify S with the ring $\begin{bmatrix} Q & 0 \\ Q/I & Q/I \end{bmatrix}$ in the obvious way, and consider $\varphi = \begin{bmatrix} 0 & 0 \\ 1+I & 0 \end{bmatrix} \in S$. Then $r_S(\varphi) = \begin{bmatrix} I & 0 \\ Q/I & Q/I \end{bmatrix}$. This is not a direct summand of S because I is not a direct summand of Q. Therefore S is not a right principally projective ring.

Theorem 2.10. *If M is a principally projective module, then the following are equivalent.*

(1) *M is a symmetric module.*

(2) *S is a symmetric ring.*

Proof. (2) $\Rightarrow$ (1) Let S be a symmetric ring and assume that $fgm = 0$ for some $f, g \in S$ and $m \in M$. Since M is principally projective, there exists $e^2 = e \in S$ such that $l_S(gm) = Se$. Due to $f \in l_S(gm)$, we have $f = fe$ and $egm = 0$. Similarly, there exists an idempotent $e_1 \in S$ such that $l_S(m) = Se_1$. Since $eg \in l_S(m)$, $eg = ege_1$ and $e_1 m = 0$. By hypothesis, $Se_1 m = 0$ implies $e_1 Sm = 0$ and so $ege_1 Sm = egSm = 0$. Note that symmetric rings are abelian (indeed, since $ae(1-e) = 0 = a(1-e)e$ for any $e = e^2, a \in S$, we have $ea(1-e) = 0 = (1-e)ae$. This implies that $ea = ae$). Hence $0 = egfm = gfem = gfm$. Therefore M is symmetric.

(1) $\Rightarrow$ (2) Clear. $\square$

A proof of the following proposition can be given in the same way as the proof of [3, Lemma 2.12].

Proposition 2.11. *If M is a symmetric module and $m \in M, f_i \in S$ for $1 \leqslant i \leqslant n$, then $f_1 \dots f_n m = 0$ if and only if $f_{\sigma(1)} \cdots f_{\sigma(n)} m = 0$, where $n \in \mathbb{N}$ and $\sigma \in S_n$.*

Lemma 2.12 is a corollary to Lemma 2.18. But we give a proof in detail.

Lemma 2.12. *If M is a symmetric module and N a direct summand of M, then N is a symmetric module.*

Proof. Let S_1 =End$_R(N)$ and $M = N \oplus K$ for some submodule K of M. Let $f, g \in S_1$ and $n \in N$ with $fgn = 0$. Define $f_1(n,k) = (fn, 0)$ and $g_1(n,k) = (gn, 0)$ where $f_1, g_1 \in S = \mathrm{End}_R(M)$, $k \in K$. Then $f_1g_1(n,0) = f_1(gn,0) = (fgn,0) = (0,0)$. Since M is symmetric and $f_1, g_1 \in S$, $g_1f_1(n,0) = (0,0)$. But $(0,0) = g_1f_1(n,0) = g_1(fn,0) = (gfn,0)$. Hence $gfn = 0$. Therefore N is symmetric. □

Corollary 2.13. *Let R be a symmetric ring and $e \in R$ an idempotent. Then eR is a symmetric module.*

Theorem 2.14. *Let R be a ring. Then the following conditions are equivalent.*

(1) *Every free R-module is symmetric.*

(2) *Every projective R-module is symmetric.*

Proof. (1) ⇒ (2) Let M be a projective R-module. Then M is a direct summand of a free R-module F. By (1), F is symmetric and so is M from Lemma 2.12.

(2) ⇒ (1) Clear. □

Theorem 2.15. *A ring R is symmetric if and only if every cyclic projective R-module is symmetric.*

Proof. The sufficiency is clear. For the necessity, let M be a cyclic projective R-module. Then $M \cong I$ for some direct summand right ideal I of R. Since R is symmetric, by Lemma 2.12, I is symmetric and so is M. □

Any direct sum of symmetric modules need not be symmetric, as the following example shows.

Example 2.16. Consider the $\mathbb{Z}$-modules $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$. Clearly, these modules are symmetric. Let M denote the $\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Then the endomorphism ring $\mathrm{End}_{\mathbb{Z}}(M)$ of M is $\begin{bmatrix} \mathbb{Z}_2 & \mathbb{Z}_2 \\ \mathbb{Z}_2 & \mathbb{Z}_4 \end{bmatrix}$. Consider $f = \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{0} & \bar{1} \end{bmatrix}$, $g = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}$ and $e = \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}$ of $\mathrm{End}_{\mathbb{Z}}(M)$. Then $fge = 0$ but $gfe \neq 0$. Hence $\mathrm{End}_{\mathbb{Z}}(M)$ is not a symmetric ring. By Theorem 2.4, M is not a symmetric module.

Proposition 2.17. *Let M_1 and M_2 be modules over a ring R. If M_1 and M_2 are symmetric and $Hom_R(M_i, M_j) = 0$ for $i \neq j$, then $M_1 \oplus M_2$ is a symmetric module.*

Proof. Let $M = M_1 \oplus M_2$ and $S_i = \mathrm{End}_R(M_i)$ for $i = 1, 2$. We may describe S as $\begin{bmatrix} S_1 & 0 \\ 0 & S_2 \end{bmatrix}$. Let $f = \begin{bmatrix} f_1 & 0 \\ 0 & f_2 \end{bmatrix}, g = \begin{bmatrix} g_1 & 0 \\ 0 & g_2 \end{bmatrix} \in S$ with $f_1, g_1 \in S_1$ and $f_2, g_2 \in S_2$ and $m = (m_1, m_2) \in M$ with $m_1 \in M_1, m_2 \in M_2$ such that $fgm = 0$. Then we have $f_1g_1m_1 = 0$ and $f_2g_2m_2 = 0$. Since M_1 and M_2 are symmetric, $g_1f_1m_1 = 0$ and $g_2f_2m_2 = 0$. This implies that $gfm = 0$. Therefore M is symmetric. □

Lemma 2.18. *Let M be an R-module and N a submodule of M. If M is symmetric and every endomorphism of N can be extended to an endomorphism of M, then N is also symmetric.*

Proof. Let $S = \mathrm{End}_R(M)$ and $f, g \in \mathrm{End}_R(N), n \in N$ with $fgn = 0$. By hypothesis, there exist $\alpha, \beta \in S$ such that $\alpha|_N = f$ and $\beta|_N = g$. Then $\alpha|_N\beta|_Nn = 0$, and so $\alpha\beta n = 0$. Since M is symmetric, we have $\beta\alpha n = 0$. This and $\alpha n \in N$ imply that $0 = \beta|_N\alpha|_Nn = gfn$. Therefore N is a symmetric module. □

It is well known that every endomorphism of any module M can be extended to an endomorphism of the injective hull $E(M)$ of M. By considering this fact, we can say the next result.

Theorem 2.19. *Let M be a module. If $E(M)$ is symmetric, then so is M.*

Proof. Clear from Lemma 2.18. □

Recall that a module M is *quasi-injective* if it is M-injective. Then we have the following.

Theorem 2.20. *Let M be a quasi-injective module. If M is symmetric, then so is every submodule of M.*

Proof. Let N be a submodule of M and $f \in \mathrm{End}_R(N)$. By quasi-injectivity of M, f extends to an endomorphism of M. Lemma 2.18 completes the proof. □

Let M be an R-module with $S = \mathrm{End}_R(M)$. Consider

$$T({}_SM) = \{m \in M \mid fm = 0 \text{ for some nonzero } f \in S\}.$$

The subset $T({}_SM)$ of M need not be a submodule of the modules ${}_SM$ and M_R in general, as the following example shows.

Example 2.21. Let e_{ij} denote 3×3 matrix units and consider the ring $R = \{(e_{11} + e_{22} + e_{33})a + e_{12}b + e_{13}c + e_{23}d : a, b, c, d \in \mathbb{Z}_2\}$ and the R-module $M = \{e_{12}a + e_{13}b + e_{23}c : a, b, c \in \mathbb{Z}_2\}$. Let $f, g \in S$ defined by $f(e_{12}a + e_{13}b + e_{23}c) = e_{12}a + e_{13}b$ and $g(e_{12}a + e_{13}b + e_{23}c) = (e_{13} + e_{23})c$. For $m = e_{23}1, m' = e_{12}1 \in M$, $fm = 0$ and $gm' = 0$. But no nonzero elements of S annihilate $m + m'$ since $(m + m')R = M$. Therefore $T({}_SM)$ is not a submodule of the modules ${}_SM$ and M_R.

In the symmetric case we have the following.

Proposition 2.22. *If M is a symmetric module and S is a domain, then $T({}_SM)$ is a left S-submodule of M.*

Proof. Let m_1, $m_2 \in T({}_SM)$. There exist nonzero f_1, $f_2 \in S$ with $f_1m_1 = 0$ and $f_2m_2 = 0$. Then $f_1f_2m_2 = 0$. By hypothesis, $0 = f_2f_1m_1 = f_1f_2m_1$. Since S is a domain, $f_1f_2 \neq 0$ and so $f_1f_2(m_1 - m_2) = 0$ or $m_1 - m_2 \in T({}_SM)$. If $g \in S$, then $gf_1m_1 = 0$. Since M is symmetric, $gf_1m_1 = 0$ implies $f_1gm_1 = 0$. Hence $gm_1 \in T({}_SM)$ and so $T({}_SM)$ is a left S-submodule of M. □

Theorem 2.23. *Let M be an R-module with S a domain. Then M is a symmetric module if and only if $T({}_SM)$ is a symmetric submodule of M.*

Proof. Assume that M is a symmetric module and $m \in T({}_SM)$. There exists a nonzero $f \in S$ with $fm = 0$. For any $r \in R$, $f(mr) = (fm)r = 0$. So $mr \in T({}_SM)$. Therefore $T({}_SM)$ is an R-submodule of M. Let $f, g \in S$ and $m \in T({}_SM)$ with $fgm = 0$. Since M is symmetric, $gfm = 0$ and so $T({}_SM)$ is a symmetric submodule of M.

Conversely, let $m \in M$ and f, g be nonzero elements of S with $fgm = 0$. If $m \in T({}_SM)$, by the symmetry condition on $T({}_SM)$, we have $gfm = 0$. If $m \notin T({}_SM)$, then $fg = 0$. Since S is a domain, we have a contradiction. Therefore M is a symmetric module. □

Let M be an R-module with $S = \mathrm{End}_R(M)$ and N a submodule of M. The quotient module M/N is called *S-symmetric* if $fgm \in N$ implies $gfm \in N$ for any $m \in M$ and $f, g \in S$.

Theorem 2.24. *Let M be an R-module with S a domain. If M is symmetric, then the quotient module $M/T({}_SM)$ is S-symmetric.*

Proof. Let $m \in M$ and $f, g \in S$ with $fgm \in T({}_SM)$. So there exists nonzero $h \in S$ such that $hfgm = 0$. By Proposition 2.11, we have $hfgm = hgfm = 0$. Then $gfm \in T({}_SM)$. Hence $M/T({}_SM)$ is S-symmetric. □

Recall that a module M is called *quasi-projective* if it is M-projective.

Theorem 2.25. *Let M be a module and N a submodule of M.*

(1) *If M is a quasi-projective module and M/N is S-symmetric, then M/N is symmetric as a left $End_R(M/N)$-module.*

(2) *If N is a fully invariant submodule of M and M/N is symmetric as a left $End_R(M/N)$-module, then M/N is S-symmetric.*

Proof. (1) Let $f_1, g_1 \in \mathrm{End}_R(M/N)$ and $m \in M$ with $f_1 g_1(m+N) = 0+N$ and π denote the natural projection from M to M/N. Since M is quasi-projective, there exist $f, g \in S$ such that $f_1\pi = \pi f$ and $g_1\pi = \pi g$. Then we have $0 + N = f_1 g_1(m + N) = f_1 g_1 \pi m = f_1 \pi g m = \pi f g m$, and so $fgm \in N$. Hence $gfm \in N$ by hypothesis. This implies that $\pi g f m = g_1 \pi f m = g_1 f_1 \pi m = g_1 f_1(m + N) = 0 + N$. Therefore M/N is symmetric as a left $\mathrm{End}_R(M/N)$-module.

(2) Let $f, g \in S$ and $m \in M$ with $fgm \in N$ and π denote the natural projection from M to M/N. Since N is fully invariant, there exist $\overline{f}, \overline{g} \in \mathrm{End}_R(M/N)$ such that $\overline{f}\pi = \pi f$ and $\overline{g}\pi = \pi g$. It follows that $\overline{f}\overline{g}(m + N) = \overline{0}$, and so $\overline{g}\overline{f}(m + N) = \overline{0}$. Therefore $gfm \in N$. □

Proposition 2.26 follows from [1, Theorem 2.14] and [4, Theorem 2.25].

Proposition 2.26. *If M is a principally projective module, then the following conditions are equivalent.*

(1) *M is a rigid module.*

(2) *M is a reduced module.*

(3) *M is a symmetric module.*

(4) *M is a semicommutative module.*

(5) *M is an abelian module.*

Remark 2.27. It follows from Theorem 2.14 of [1], every reduced module is semicommutative, and every semicommutative module is abelian. The converses hold for principally projective modules. Note that for a prime integer p the cyclic group M of p^2 elements is a $\mathbb{Z}$-module for which $S = \mathbb{Z}_{p^2}$. The module M is neither reduced nor principally projective although it is semicommutative.

Every symmetric module has a symmetric endomorphism ring. However, despite all our efforts we have not succeeded in answering positively the following question for an arbitrary module.

Question. Is any module symmetric if its endomorphism ring is symmetric?

The answer is positive for simple modules, vector spaces and the modules which satisfy the conditions in Theorem 2.4. But if the answer is negative for an arbitrary module, then what is the counterexample?

Acknowledgements

The authors would like to thank the referee(s) for careful reading of the manuscript and valuable suggestions. The first author thanks the Scientific and Technological Research Council of Turkey (TUBITAK) for the grant.

References

[1] N. Agayev, G. Güngöroğlu, A. Harmanci and S. Halicioglu, *Abelian modules*, Acta Math. Univ. Comenianae 78(2)(2009), 235-244.

[2] N. Agayev, S. Halicioglu and A. Harmanci, *On symmetric modules*, Riv. Mat. Univ. Parma 8(2)(2009), 91-99.

[3] N. Agayev, S. Halicioglu and A. Harmanci, *On reduced modules*, Commun. Fac. Sci. Univ. Ank. Series A1 58(1)(2009), 9-16.

[4] N. Agayev, S. Halicioglu and A. Harmanci, *On Rickart modules*, Bull. Iran. Math. Soc. 38(2)(2012), 433-445.

[5] D. D. Anderson and V. Camillo, *Semigroups and rings whose zero products commute*, Comm. Algebra 27(6)(1999), 2847-2852.

[6] A. W. Chatters and C. R. Hajarnavis, Rings with chain conditions, Pitman, Boston, 1980.

[7] M. W. Evans, *On commutative p.p. rings*, Pacific J. Math. 41(1972), 687-697.

[8] A. Ghorbani and M. R. Vedadi, *Epi-retractable modules and some applications*, Bull. Iran. Math. Soc. 35(1)(2009), 155-166.

[9] K. R. Goodearl and A. K. Boyle, Dimension theory for nonsingular injective modules, Memoirs Amer. Math. Soc. 7(177), 1976.

[10] A. Hattori, *A foundation of the torsion theory over general rings*, Nagoya Math. J. 17(1960), 147-158.

[11] C. Y. Hong, N. K. Kim and T. K. Kwak, *Ore extensions of Baer and p.p.-rings*, J. Pure Appl. Algebra 151(3)(2000), 215-226.

[12] I. Kaplansky, Rings of operators, Math. Lecture Note Series, Benjamin, New York, 1965.

[13] J. Krempa, *Some examples of reduced rings*, Algebra Colloq. 3(4)(1996), 289-300.

[14] T. Y. Lam, Exercises in classical ring theory, Springer-Verlag, New York, 1995.

[15] J. Lambek, *On the representation of modules by sheaves of factor modules*, Canad. Math. Bull. 14 (3)(1971), 359-368.

[16] T. K. Lee and Y. Zhou, *Reduced modules*, Rings, modules, algebras and abelian groups, 365-377, Lecture Notes in Pure and Appl. Math., 236, Dekker, New York, (2004).

[17] B. L. Osofsky, *A counter-example to a lemma of Skornjakov*, Pacific J. Math. 15(1965), 985-987.

[18] R. Raphael, *Some remarks on regular and strongly regular rings*, Canad. Math. Bull. 17(5)(1974/75), 709-712.

[19] S. T. Rizvi and C. S. Roman, *Baer and quasi-Baer modules*, Comm. Algebra 32(2004), 103-123.

[20] S. T. Rizvi and C. S. Roman, *On direct sums of Baer modules*, J. Algebra 321(2009), 682-696.

[21] J. E. Roos, *Sur les categories spectrales localement distributives*, C. R. Acad. Sci. Paris 265(1967), 14-17.

[22] B. Ungor, N. Agayev, S. Halicioglu and A. Harmanci, *On principally quasi-Baer modules*, Albanian J. Math. 5(3)(2011), 165-173.

[23] J. M. Zelmanowitz, *Regular modules*, Trans. Amer. Math. Soc. 163(1972), 341-355.

CONTACT INFORMATION

Burcu Ungor, Sait Halicioglu
Department of Mathematics,
Ankara University, Turkey
E-Mail(s): bungor@science.ankara.edu.tr, halici@ankara.edu.tr

Yosum Kurtulmaz
Department of Mathematics,
Bilkent University, Turkey
E-Mail(s): yosum@fen.bilkent.edu.tr

Abdullah Harmanci
Department of Maths,
Hacettepe University, Turkey
E-Mail(s): harmanci@hacettepe.edu.tr

Received by the editors: 05.01.2013
and in final form 05.12.2014.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 295–301

RESEARCH ARTICLE

A commutative Bezout PM^* domain is an elementary divisor ring

B. Zabavsky, A. Gatalevych

Communicated by V. V. Kirichenko

Abstract. We prove that any commutative Bezout PM^* domain is an elementary divisor ring.

The aim of this paper is to study the question of diagonalizability for matrices over a ring. It is well-known that any elementary divisor domain is a Bezout domain and it is a classical open question to determine whether the converse statement is true?

The notion of an elementary divisor ring was introduced by Kaplansky in [6]. There are a lot of researches that deal with the matrix diagonalization in different cases (the most comprehensive history of these researches can be found in [10]). It is an open question dating back at least to Helmer [5] in 1942 to decide, whether a commutative Bezout domain is always an elementary divisor domain. Helmer showed that not only does the domain of entire functions is an elementary divisor domain, it also has a property which he labeled adequate. Henriksen [4] appears to be the first person to have given an example to show that being adequate is a stronger property than that of being an elementary divisor ring. In proving this, Henriksen observed that in an adequate domain each nonzero prime ideal is contained in a unique maximal ideal [4]. It is a natural question to ask whether or not the converse holds and this question is explicitly raised in [7]. The negative answer to this question is given in [1]. Furthermore, it is shown that there exists an elementary divisor ring

2010 MSC: 13F99.

Key words and phrases: Bezout domain, PM-ring, clean element, neat element, elementary divisor ring, stable range 1, neat range 1.

which is not adequate but which does have the property that each nonzero prime ideal is contained in a unique maximal ideal. In this paper we show that a commutative Bezout domain in which each nonzero prime ideal is contained in a unique maximal ideal is an elementary divisor ring. Note that these results are responses to open questions work [12, Questions 10, Problem 6].

We introduce the necessary definitions and facts.

All rings considered will be commutative and have identity. A ring is a *Bezout ring*, if every its finitely generated ideal is principal. A ring R is *an elementary divisor ring* if every matrix A (not necessarily square one) over R admits diagonal reduction, that is, there exist invertible square matrices P and Q such that PAQ is a diagonal matrix, say (d_{ij}), for which d_{ii} is a divisor of $d_{i+1,i+1}$ for each i. A ring R to be *right Hermite* if every 1×2 matrix over R admits diagonal reduction. Any Hermite ring is a Bezout ring. For domains, the notions of Hermite and Bezout ring are equivalent. Gillman and Henriksen showed that any commutative ring R is an Hermite ring if and only if for all $a, b \in R$ there exist $a_1, b_1, d \in R$ such that $a = a_1 d$, $b = b_1 d$ and $a_1 R + b_1 R = R$ [10]. Furthermore, they proved the following result, which we state formally.

Proposition 1. *Let R be a commutative Bezout ring. R is an elementary divisor ring if and only if R is an Hermite ring that satisfies the extra condition that for all $a, b, c \in R$ with $aR+bR+cR = R$ there exist $p, q \in R$ such that $paR + (pb + qc)R = R$.*

Definition 1. Let R be a commutative Bezout domain. A nonzero element a in R is called an adequate element if for every $b \in R$ there exist $r, s \in R$ such that $a = rs$, $rR + bR = R$, and if s' is a non-unit divisor of s, then $s'R + bR \neq R$. If every nonzero element of the ring R is adequate, then R is called an adequate ring [5, 10].

Definition 2. Let R be a commutative ring. An element $a \in R$ is called a clean element if a can be written as the sum of a unit and an idempotent. If every element of R is clean, then we say that R is a clean ring [8, 9].

Any clean ring is a Gelfand ring. Recall that a ring R is called a *Gelfand ring* if for every $a, b \in R$ such that $a + b = 1$ there are $r, s \in R$ such that $(1 + ar)(1 + bs) = 0$. A ring R is called a *PM-ring* if each prime ideal is contained in a unique maximal ideal. It had been asserted that a commutative ring is a Gelfand ring if and only if it is a PM-ring [2, 3]. A ring R is called a *PM^*-ring* if each nonzero prime ideal is contained in a unique maximal ideal [9]. A ring R is said to be *a ring of stable range 1*, if for any $a, b \in R$ such that $aR + bR = R$ there exist $t \in R$ such that $(a + bt)R = R$.

Definition 3. An element $a \in R \setminus \{0\}$ of a commutative ring R is called a PM-element if the factor ring R/aR is a PM-ring.

Proposition 2. *For a commutative ring R the following are equivalent:*

1) $a \in R$ is a PM-element;

2) for each prime ideal P such that $a \in P$ there exists a unique maximal ideal M such that $P \subset M$.

Proof. This is obvious, since $\overline{P}$ is a prime ideal of R/aR if and only if there exists a prime ideal P such that $aR \subset P$ and $\overline{P} = P/aR$. □

As a consequence of Proposition 2 we obtain the following result.

Proposition 3. *A commutative domain R is a domain in which each nonzero prime ideal is contained in a unique maximal ideal of R if and only if every nonzero element of R is a PM-element.*

Proposition 4. *An element a of a commutative Bezout domain is a PM-element if and only if, for every elements $b, c \in R$ such that $aR + bR + cR = R$, an element a can be represented as $a = rs$, where $rR + bR = R$, $sR + cR = R$.*

Proof. Denote $\overline{R} = R/aR$, $\overline{b} = b + aR$, $\overline{c} = c + aR$. Since $aR + bR + cR = R$, we see that $\overline{bR} + \overline{cR} = \overline{R}$. Therefore, if $a = rs$ where $rR + bR = R$, $sR + cR = R$, then $\overline{bR} + \overline{cR} = \overline{R}$ and $\overline{0} = \overline{rs}$ where $\overline{r}\overline{R} + \overline{bR} = \overline{R}$, $\overline{s}\overline{R} + \overline{c}\overline{R} = \overline{R}$. By [2], $\overline{R}$ is a PM-ring.

If $\overline{R}$ is a PM-ring then, by [9], $\overline{0} = \overline{rs}$ where $\overline{r}\overline{R} + \overline{bR} = \overline{R}$, $\overline{s}\overline{R} + \overline{c}\overline{R} = \overline{R}$ for arbitrary $\overline{b}, \overline{c} \in \overline{R}$ such that $\overline{bR} + \overline{cR} = \overline{R}$. Whence we obtain $aR + bR + cR = R$. Because $\overline{0} = 0 + aR = \overline{rs}$, we have $rs \in aR$, where $\overline{r} = r + aR$, $\overline{s} = s + aR$. Let $rR + aR = r_1R$, $sR + aR = s_1R$. From this $r = r_1r_0$, $a = r_1a_0$, $s = s_1s_2$, $a = s_1a_2$, where $r_0R + a_0R = R$, $s_2R + a_2R = R$. Since $r_0R + a_0R = R$, we obtain $r_0u + a_0v = 1$ for some $u, v \in R$. Since $rs \in aR$, we see that $rs = at$ for some $t \in R$. Then $r_1r_0s = r_1a_0t$, because R is a domain, and we have $a_0t = r_0s$. By the equality, $r_0u + a_0v = 1$ we have $sr_0u + sa_0v = s$, $a_0(tu + a_0v) = s$. Therefore $a = r_1a_0$, where $r_1R + bR + r_1a_0R = R$. Then $r_1R + bR = R$. Since $a_0(tu + a_0v) = s$ and $a_0R + cR + aR = R$, we obtain $a_0R + cR = R$. The proposition is proved. □

Theorem 1. *A commutative Bezout domain in which each nonzero prime ideal is contained in a unique maximal ideal is an elementary divisor ring.*

Proof. Let R be a commutative Bezout domain with the property that each nonzero prime ideal is contained in a unique maximal ideal. According to Proposition 4, let $a, b, c \in R$ be such that $aR+bR+cR = R$. According to the restrictions imposed on R, by Proposition 4, we have $b = rs$ where $rR+aR = R$, $sR+cR = R$. Let $p \in R$ be such that $sp+ck = 1$ for some $k \in R$. Hence $rsp + rck = r$ and $bp + crk = r$. Denoting $rk = q$ and we obtain $(br + cq)R + aR = R$. Let $pR + qR = dR$ and $d = pp_1 + qq_1$ with $p_1R + q_1R = R$. Hence $p_1R + (p_1b + q_1c)R = R$ and, since $pR \subset p_1R$, we obtain $p_1R + cR = R$ and $p_1R + (p_1b + q_1c)R = R$.

Since $bp + cq = d(bp_1 + cq_1)$, and $(bp + cq)R + aR = R$ we obtain $(bp_1 + cq_1)R + aR = R$. Finally, we have $ap_1R + (bp_1 + cq_1)R = R$. By Proposition 1, we obtain that R is an elementary divisor ring. The theorem is proved. □

Remark 1. Note that in order to prove this theorem, it is necessary that only the element $b \in R$ is a PM-element.

Let R be a commutative Bezout domain. We denote by $S = S(R)$ the set of all PM-elements of R. Since $1 \in R$, the set S is nonempty. Furthermore, we obtain the following result.

Proposition 5. *The set $S(R)$ of all PM-elements of a commutative domain R is a saturated multiplicatively closed set.*

Proof. Let $a, b \in S(R)$. We show that $ab \in S(R)$. Suppose the contrary. Then there exist a prime ideal P and maximal ideals M_1, M_2 such that $M_1 \neq M_2$ and $ab \in P \subset M_1 \cap M_2$. Since $ab \in P$, we obtain that $a \in P$ or $b \in R$. It is impossible because $a \in S(R)$, $b \in S(R)$ and $P \subset M_1 \cap M_2$. Therefore $S(R)$ is a multiplicatively closed set.

Let $ab \in S(R)$ for some $a, b \in R$. If $a \notin S(R)$ then there exists a prime ideal P such that $a \in P$ and $P \subset M_1 \cap M_2$ for some maximal ideals M_1, M_2 and $M_1 \neq M_2$. Therefore, $ab \in P$ and $P \subset M_1 \cap M_2, M_1 \neq M_2$. It is impossible because $ab \in S(R)$. Hence $S(R)$ is a saturated multiplicatively closed set. The Proposition is proved. □

Let R be a commutative Bezout domain and $S(R)$ be the set of all PM-elements of R. Since $S(R)$ is a saturated multiplicatively closed set, we can consider the localization of R with denominators from $S(R)$ i.e. the ring of fractious R_S. We have:

Theorem 2. *Let R be a commutative elementary divisor domain. Then a ring R_S is an elementary divisor ring.*

Proof. Suppose that R is an elementary divisor ring. We need to show that R_S is also an elementary divisor ring. Let $as^{-1}, bs^{-1}, cs^{-1}$ be any elements from R_S such that

$$as^{-1}R_S + bs^{-1}R_S + cs^{-1}R_S = R_S.$$

Then $aR+bR+cR = dR$, for some element $d \in S(R)$. Let $a = a_1d$, $b = b_1d$, $c = c_1d$ for some elements $a_1, b_1, c_1 \in R$ such that $a_1R + b_1R + c_1R = R$. Since R is an elementary divisor ring, there are elements $u, v, p, q \in R$ such that

$$a_1pu + (b_1p + c_1q)v = 1.$$

Then

$$apR_S + (bp + cq)R_S = R_S.$$

By [6], R_S is an elementary divisor ring. Theorem is proved. □

Let R be a commutative Bezout domain and $S = S(R)$ be the set of all PM-elements of R. Since $S(R)$ is a saturated multiplicatively closed set, we can construct by transfinite induction a natural chain

$$\{R^\alpha | \alpha \text{ is an ordinal}\}$$

of the saturated multiplicatively closed sets in R as follows. Let $R^0 = S(R)$. Let α be an ordinal greater than zero and assume R^β has been defined and is a saturated multiplicatively closed set in R, whenever $\beta < \alpha$ and let $K_\beta = R_{R_\beta}$. Then K_β is a commutative Bezout domain (see [10]) and hence $S(K_\beta)$ is a saturated multiplicatively closed set by Proposition 5.

We define R^α by $R^\alpha = \bigcup_{\beta<\alpha} R^\beta$ if α is a limit ordinal and $R^\alpha = S(K_{\alpha-1}) \cap R$ otherwise. It is obvious that R^α is a saturated multiplicatively closed set. If α, β are ordinals such that $\alpha \leqslant \beta$ then $R^\alpha \subset R^\beta \subset R$. Also $R^\alpha = R^{\alpha+1}$ for some ordinal α. In case, when $R^\alpha \neq R^{\alpha+1}$ for each ordinal α, then

$$\operatorname{card}(R^\alpha) > \operatorname{card}(\alpha).$$

Choosing β such that $\operatorname{card}(\beta) > \operatorname{card}(R)$ we obtain

$$\operatorname{card}(\beta) > \operatorname{card}(R) > \operatorname{card}(R^\beta),$$

a contradiction. We let α_0 denote the least ordinal such that

$$R^{\alpha_0} = R^{\alpha_0+1}$$

and we call

$$\{R^\alpha | 0 \leqslant \alpha \leqslant \alpha_0\}$$

a D-chain in R. In this situation R^{-1} will denote the group of units of R.

By Theorem 2 and the fact that union of elementary divisor rings are an elementary divisor ring and using D-chain of a commutative Bezout domain we can conclude that the problem of being a commutative Bezout domain an elementary divisor ring is reduced to the case of a commutative Bezout domain where PM-elements are the only units, when $U(R) = S(R)$.

Definition 4. Let R be a commutative Bezout domain. An element $a \in R$ is called a neat element if R/aR is a clean ring.

Obvious examples of neat elements are units of a ring, and adequate elements of a ring [11]. If R is a commutative Bezout domain and a is a neat element of R, then R/aR is a clean ring [9], that is R/aR is a PM-ring. Hence we obtain the following result.

Proposition 6. *Every neat element of a commutative Bezout domain is a PM-element.*

Definition 5. A commutative ring R is said to be of the neat range 1 if for any $a, b \in R$ such that $aR + bR = R$ there exists $t \in R$ such that for the element $a + bt = c$ the ring R/cR is a clean ring [11].

Theorem 3 ([11])**.** *A commutative Bezout domain is an elementary divisor ring if and only if R is a ring of the neat range 1.*

From this we obtain the following result.

Theorem 4. *Let R be a commutative Bezout domain and $U(R) = S(R)$. Then R is an elementary divisor ring if and only if stable range of R is equal to 1.*

Proof. Since every neat element is a PM-element and $U(R) = S(R)$, then only units in a ring are neat elements. Then by Theorem 3, R is an elementary divisor ring if and only if R is a ring of stable range 1. Theorem is proved. □

Let R be a commutative Bezout domain and $a \in R$ is a neat element of R. By [9] the stable range of R/aR is equal to 1. Consequently by Theorem 4, we have a next result.

Theorem 5. *Let R be a commutative Bezout domain such that for every nonzero element $a \in R$ stable range of R/aR is not equal 1. Then R is not an elementary divisor ring.*

References

[1] *J. W. Brewer, P. F. Conrad, P. R. Montgomery.* Lattice-ordered groups and a conjecture for adequate domains, Proc. Amer. Math. Soc, 43(1) (1974), pp.31–34. pp.93–108.

[2] *M. Contessa*, On pm-rings, Comm. Algebra, 10(1) (1982), pp.93–108.

[3] *G. De Marco, A. Orsatti.* Commutative rings in which every prime ideal is contaned in a unigue maximal ideal, Proc. Amer. Math. Soc, 30(3) (1971), pp.459–466.

[4] *M. Henriksen*, Some remarks about elementary divisor rings, Michigan Math. J., 3(1955/56) pp.159-163.

[5] *O. Helmer*, The elementary divisor for certain rings without chain conditions, Bull. Amer. Math. Soc., 49(2)(1943), pp.225–236.

[6] *I. Kaplansky.* Elementary divisors and modules, Trans. Amer. Math. Soc., 66(1949), pp. 464–491.

[7] *M. Larsen, W. Lewis, T. Shores*, Elementary divisor rings and finitely presented modules, Trans. Amer. Mat. Soc. 187(1974) pp.231–248.

[8] *W. K. Nicholson*, Lifting idempotents and exchange rings, Trans. Amer. Math. Soc., 229(1977) pp. 269–278.

[9] *W. McGovern*, Neat rings, J. of Pure and Appl. Algebra, 205(2)(2006) pp. 243–266.

[10] *B.V. Zabavsky*, Diagonal reduction of matrices over rings, Mathematical Studies, Monograph Series, v. XVI, Lviv (2012), 251p.

[11] *B.V. Zabavsky*, Diagonal reduction of matrices over finite stable range, Mat. Stud., 41(1)(2014) pp.101–108.

[12] *B.V. Zabavsky*, Questions related to the K-theoretical aspect of Bezout rings with various stable range conditions, Mat.Stud. 42(1)(2014), pp. 89–109.

Contact information

B. V. Zabavsky,
A. Gatalevych

Department of Mechanics and Mathematics,
Ivan Franko National Univ., Lviv, Ukraine
E-Mail(s): `zabavskii@gmail.com`,
`gatalevych@ukr.net`

Received by the editors: 07.03.2015
and in final form 13.07.2015.

Algebra and Discrete Mathematics
Volume **19** (2015). Number 2, pp. 302–312
RESEARCH ARTICLE

Towards practical private information retrieval from homomorphic encryption

Dmitry Zhuravlev*

Communicated by V. V. Kirichenko

Abstract. Private information retrieval (PIR) allows a client to retrieve data from a remote database while hiding the client's access pattern. To be applicable for practical usage, PIR protocol should have low communication and computational costs. In this paper a new generic PIR protocol based on somewhat homomorphic encryption (SWHE) is proposed. Compared to existing constructions the proposed scheme has reduced multiplicative depth of the homomorphic evaluation circuit which allows to cut down the total overhead in schemes with ciphertext expansion. The construction results in a system with $O(\log n)$ communication cost and $O(n)$ computational complexity for a database of size n.

Introduction

Confidentiality of queries to publicly accessible on-line data sources is becoming increasingly important for retrieving up-to-date information in many domains, such as patent and media databases, real-time stock quotes, Internet domain names, location-based services, on-line behavioral profiling and advertising, e-commerce and search engines. The *private information retrieval* (PIR) technology allows to protect client's query

*The author would like to thank Ihor Samoilovych for his helpful discussions in the process of this work.

2010 MSC: 11T71.

Key words and phrases: protocols, encryption, servers, complexity theory, private information retrieval, homomorphic encryption.

in such a way that server (or database administrator) cannot infer the purpose of the query while still being able to return the desired data (see Fig. 1).

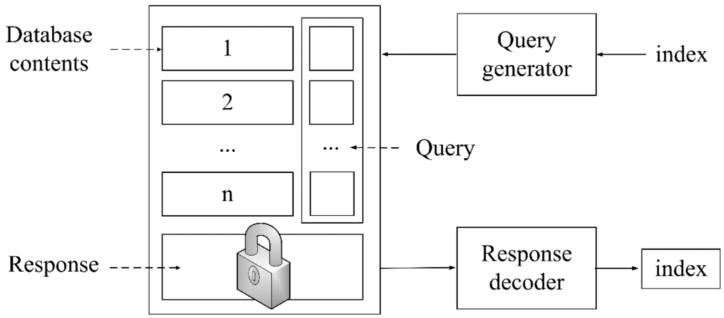

FIGURE 1. PIR scheme.

PIR was introduced by Chor et al. [1] in non-colluding multi-server settings. In [2] it was proposed the first single database PIR protocol based on hardness computationally assumptions. Namely, the security of the proposed scheme relies on quadratic residuosity problem. The communication complexity of the protocol is $O(2^{\sqrt{\log n \log\log N}})$, where n is the number of bits in the database and N is a composite modulus.

Recent progress in homomorphic cryptography gives rise for new approaches to PIR. In [3] Gentry constructed the first *fully homomorphic encryption* (FHE) scheme — an encryption scheme that supports arbitrary number of additions and multiplications over ciphertexts, and therefore admits to compute arbitrary boolean circuits over encrypted data. In particular, the selection circuit to access the database can be computed over ciphertexts. Hence, one can encrypt the index bitwise and then apply the selection circuit to the encrypted database.

All existing FHE schemes are too expensive to be practical. On the other hand, there exist [4] more practical *somewhat homomorphic encryption* (SWHE) schemes that preserve only limited number of operations. In [5] Brakerski et al. proposed a generic PIR protocol that utilizes a SWHE scheme and a symmetric encryption scheme as building blocks. In their protocol the client uses the symmetric scheme to encrypt the index, and then the server homomorphically decrypts it during query evaluation. Thus, the client's query is short but the server computational cost and response size can be quite large because of the deep response generation circuit.

In [6] Yi et al. constructed a PIR protocol with communication complexity $O(\log n)$ and computational complexity $O(n \log n)$ using the SWHE scheme from [7]. Similar approach is presented in [8] where the SWHE scheme from [9] is exploited to privately retrieve the data. In their protocol a tree-based compression scheme is used to reduce the communication complexity.

Contribution. The presented approach improves both computational and communication costs compared to the previous SWHE based PIR protocols. To adopt PIR for using SWHE, in the proposed protocol the multiplication depth (the number of nested multiplications) of response generation circuit was decreased. For example, a SWHE that can evaluate circuits of depth 5 is sufficient to retrieve the data from a database containing more than 8 billion rows. This multiplication depth is practical for state-of-the-art SWHE [4]. Moreover, the proposed PIR protocol utilizes the recursive retrieval algorithm from [10], which allows to reduce computational complexity from $O(n \log n)$ to $O(n)$. The security of proposed generic protocol is based on the security of the underlying SWHE scheme.

1. Preliminaries

In this section the concepts of PIR protocol and SWHE scheme will be introduced.

1.1. Notations

Throughout the paper we will use the following notation. In the sequel, n denotes the database size in bits and $l = \lceil \log_2 n \rceil$ gives the bit capacity of database indexes. Vector indexes always start from 0, e.g. $a = (a_0, a_1, \ldots, a_{n-1})$. For nonnegative l-bit integer $i = \sum_{k=0}^{l-1} i_{(k)} \cdot 2^k$ we denote $(k+1)$-th bit of i as $i_{(k)}$ for all $k \in \{0, 1, \ldots, l-1\}$.

For all $a \in \{0, 1\}$ we use $a^{\mathcal{R}}$ to denote corresponding additive identity $0_{\mathcal{R}}$ and multiplicative identity $1_{\mathcal{R}}$ of unitary ring $\mathcal{R}$, namely

$$a^{\mathcal{R}} \stackrel{\text{def}}{=} \begin{cases} 0_{\mathcal{R}}, & \text{if } a = 0; \\ 1_{\mathcal{R}}, & \text{othewise.} \end{cases}$$

For some unitary ring $\mathcal{R}$ and all $b = (b_0, b_1, \ldots, b_{l-1}) \in \mathcal{R}^l$ we define associated element to $(k+1)$-th bit of nonnegative l-bit integer t as

$$b_k^t \stackrel{\text{def}}{=} \begin{cases} b_k + 1_{\mathcal{R}}, & \text{if } t_{(k)} = 0; \\ b_k, & \text{othewise.} \end{cases}$$

If $\mathcal{A}$ is a *probabilistic polynomial time* (PPT) Turing machine, by $\Pr[\mathcal{A}(x) = y]$, we denote the probability that y is equal to answer generated by $\mathcal{A}$ on input x. By $\mathcal{A}^{\mathcal{B}}(\cdot)$, we denote an algorithm that can make oracle queries to $\mathcal{B}$.

1.2. Definitions

We are now ready to define a single database computational private information retrieval. PIR protocols consist of two interactive PPT Turing machines $\mathcal{C}, \mathcal{S}$ which are called the *client* and the *server*, respectively. Each will take as input the security parameter λ and the size of the database n. The server will take as input the database $d = (d_0, d_1, \ldots, d_{n-1}) \in \{0,1\}^n$. The client will take as input an index $i \in \{0, \ldots, n-1\}$, and at the end of the protocol the client will output a bit d_i. This notion can be formally described by the following definition:

Definition 1 (PIR Correctness)**.** A PIR protocol $(\mathcal{C}, \mathcal{S})$ is correct if for any λ, n, i and d as specified above, if

$$(out_{\mathcal{C}}, out_{\mathcal{S}}) \leftarrow \langle \mathcal{C}(1^\lambda, n, i), \mathcal{S}(1^\lambda, n, d) \rangle$$

then $out_{\mathcal{C}} = d_i$.

One of the most important properties of the private information retrieval protocol is the possibility of non-revealing of the index i to the server. In this paper, we consider a PIR scheme to be secure in the sense that it is computationally infeasible for an adversary to distinguish two queries.

Definition 2 (Negligible function)**.** A positive function μ is *negligible in* λ, or just *negligible*, if for every positive polynomial p and any sufficiently large λ it holds that $\mu(\lambda) \leqslant 1/p(\lambda)$.

Formally the security of PIR protocol is defined as follows:

Definition 3 (PIR Security)**.** A PIR protocol $(\mathcal{C}, \mathcal{S})$ is secure if for all i and j from $\{0, 1, \ldots, n-1\}$ and all non-uniform PPT Turing machines $\mathcal{A}$ there exists a negligible function μ such that

$$\Big| \Pr\left[(out_{\mathcal{C}}, out_{\mathcal{A}}) \leftarrow \langle \mathcal{C}(1^\lambda, n, i), \mathcal{A}(state) \rangle : out_{\mathcal{A}} = i\right] - \\ - \Pr\left[(out_{\mathcal{C}}, out_{\mathcal{A}}) \leftarrow \langle \mathcal{C}(1^\lambda, n, j), \mathcal{A}(state) \rangle : out_{\mathcal{A}} = i\right] \Big| \leqslant \mu(\lambda) \quad (1)$$

The basis of our PIR protocol is encryption that allows to securely compute polynomial functions of bounded degree.

Definition 4 (Somewhat homomorphic encryption)**.** A symmetric *somewhat homomorphic encryption* (SWHE) scheme is a tuple of three PPT algorithms $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ in which its spaces of plaintexts and ciphertexts are rings and exists a positive number M such that for all polynomial p with $\deg(p) \leqslant M$, all plaintexts $m_0, \ldots, m_k$, and all outputs $sk \leftarrow \mathrm{KeyGen}(1^\lambda)$, we have

$$\mathrm{Dec}\left(sk, p(\mathrm{Enc}(sk, m_0)), \ldots, \mathrm{Enc}(sk, m_k))\right) = p(m_0, \ldots, m_k). \tag{2}$$

We say that the cryptosystem is secure, if the adversary unable to distinguish pairs of ciphertexts based on the message is encrypted by them.

Definition 5 (IND-CPA Security)**.** A symmetric encryption scheme $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ is *indistinguishable chosen plaintext attack secure (IND-CPA)* if for any PPT adversary $\mathcal{A}$, there is a negligible function μ such that

$$\Big| \Pr\left[sk \leftarrow \mathrm{KeyGen}(1^\lambda) : \mathcal{A}^{\mathrm{Enc}(sk, \mathrm{Select}(\cdot,\cdot,0))} = 1\right] - \\ - \Pr\left[sk \leftarrow \mathrm{KeyGen}(1^\lambda) : \mathcal{A}^{\mathrm{Enc}(sk, \mathrm{Select}(\cdot,\cdot,1))} = 1\right] \Big| \leqslant \mu(\lambda), \tag{3}$$

where $\mathrm{Select}(m_0, m_1, b) = m_b$ for $b \in \{0, 1\}$.

2. From SWHE to PIR

In this section we describe the construction of PIR from [5, 6, 8] based on homomorphic cryptography with computational optimization from [10].

2.1. The basic scheme

Let $d = (d_0, d_1, \ldots, d_{n-1})$ be the client's database, where $d_i \in \{0, 1\}$. We take a SWHE scheme $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ on bits (the message space is residue ring $\mathbb{Z}_2 = \{0, 1\}$), which is used as a "black-box" module. The parameters of the scheme are specified to allow below computations.

The idea of retrieving data is based on the observation that one can algebraically realize the comparison of homomorphically encrypted indexes. Let i be an index of an element in the database d, $0 \leqslant i < n$, where $i_{(k)} \in \{0, 1\}$ are the bits of i. The client encrypts index i bitwise,

$Enc(sk, i) = (c_0, \ldots, c_{l-1})$, $c_i \leftarrow Enc(sk, i_{(k)})$, and sends the result to the server. The server can compare the encrypted address $Enc(sk, i)$ with a given index j, algebraically:

$$e_j = (c_0 + \mathrm{Enc}(j_{(0)}) + \mathrm{Enc}(1)) \cdot \ldots \cdot (c_{l-1} + \mathrm{Enc}(j_{(l-1)}) + \mathrm{Enc}(1)),$$

where Enc (0) and Enc (1) are predetermined encryption of 0 and 1. Since the ciphertext space $\mathcal{R}$ is a ring, $0_{\mathcal{R}}$ and $1_{\mathcal{R}}$ are a valid encryption of 0 and 1.

The homomorphic properties of the scheme $\mathcal{E}$ imply that

$$\mathrm{Dec}\,(sk, e_j) = \begin{cases} 1, & \text{if } j = i; \\ 0, & \text{othewise.} \end{cases}$$

The server computes the auxiliary encrypted choice-bits e_k for every $0 \leqslant k < n$. Then, in order to access the data with encrypted index $End(i)$, the server computes the linear combination over all database

$$r = e_0 \cdot \mathrm{Enc}\,(d_0) + \ldots + e_{n-1} \cdot \mathrm{Enc}\,(d_{n-1}), \tag{4}$$

where $\mathrm{Enc}\,(d_i) = d_i^{\mathcal{R}}$ is the deterministic bit encryption. The client decrypts the result and gets the requested value

$$\mathrm{Dec}\,(r) = \sum_{k=0}^{n-1} \mathrm{Dec}\,(e_k) \cdot \mathrm{Dec}\,(d_k^{\mathcal{R}}) = d_i.$$

2.2. Efficiency

Direct computation in formula (4) requires approximately $l + n$ homomorphic additions and $l \cdot n$ multiplications with depth $\lceil \log_2 l \rceil$ on the server side per request. In [10] efficient method that combines calculation of e_i and the linear combination (4) was proposed. The main idea of this method is to consequently reduce the database so that at the end there is only one element left which is the correct requested element after decryption. Construct elements

$$f_i = c_0 \cdot (d_{2i}^{\mathcal{R}} + d_{2i+1}^{\mathcal{R}}) + d_{2i}^{\mathcal{R}},\ i = 0, 1, \ldots, l-1,$$

where addition and multiplication are the homomorphic operations from the encryption scheme. Note that

$$\mathrm{Dec}\,(sk, f_i) = \begin{cases} d_{2i}, & \text{if } \mathrm{Dec}\,(sk, c_0) = 0; \\ d_{2i+1}, & \text{if } \mathrm{Dec}\,(sk, c_0) = 1. \end{cases}$$

Therefore the requested element is the element of the database $(f_0, \ldots, f_{2^{l-1}-1})$ with encrypted index $(c_1, \ldots, c_{n-1})$ after decryption. We can repeat the same construction for the new database and index. After l steps we obtain only one element, which is d_i after decryption. The scheme of the algorithm is shown on Fig. 2.

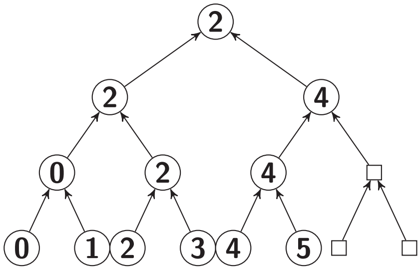

FIGURE 2. Retrieving element with index 010_2 from database of size 6.

This algorithm reduces the number of operations from $O(n \log n)$ to $O(n)$ while calculating server response. Notice that the multiplicative depth of polynomial remains $\lceil \log_2 l \rceil$ as well as in direct computation.

3. Our protocol

In this section, we will show how to decrease the degree of the polynomial in the formula (4) to allow more effective using of server resources.

3.1. PIR with reduced depth

Without loss of generality it is assumed that the database content is represented as an n-bit string $d = (d_0, d_1, \ldots, d_{n-1})$ from which the client wishes to obtain the bit d_i while keeping the index i private. Let $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ be a symmetric SWHE scheme such that its plaintexts form the residue ring $\mathbb{Z}_2$, its ciphertexts form some unitary ring $(\mathcal{R}, +, \cdot)$ and this scheme admits correct evaluation of polynomials of degree $l - 1$, where $l = \lceil \log_2 n \rceil$.

The proposed PIR protocol consists of initialization, query, answering and reconstruction algorithms:

1) Init (λ, n): Given a security parameter λ and the database of size n, the client invokes KeyGen (1^λ) to generate a secret key sk of the scheme $\mathcal{E}$.

2) QGen $(n, i, 1^\lambda)$: The client encrypts an index i bitwise as $c_k \leftarrow \mathrm{Enc}(sk, i_{(k)})$, where $i = i_{(l-1)} \dots i_{(1)} i_{(0)}$ in binary representation. Let $c = (c_0, \dots, c_{l-1})$.
3) RGen (d, c): The server generates and returns a response consisting of two parts, i.e $(r, s) \in \mathcal{R} \times \mathbb{Z}_2$.
   - The server computes r in the ring $\mathcal{R}$:
   $$r = \sum_{t=0}^{n-1} \left(d_t^{\mathcal{R}} \cdot \prod_{k=0}^{l-1} c_k^t \right) - \sum_{t=0}^{n-1} d_t^{\mathcal{R}} \cdot \prod_{k=0}^{l-1} c_k, \tag{5}$$
   where
   $$d_i^{\mathcal{R}} \stackrel{\text{def}}{=} \begin{cases} 0_{\mathcal{R}}, & \text{if } d_i = 0 \\ 1_{\mathcal{R}}, & \text{othewise} \end{cases} \quad \text{and } c_k^t \stackrel{\text{def}}{=} \begin{cases} c_k + 1_{\mathcal{R}}, & \text{if } t_{(k)} = 0 \\ c_k, & \text{othewise} \end{cases}$$
   - The server computes the sum s of the database elements as elements of the ring $\mathbb{Z}_2$, i.e. $s = \sum_{t=0}^{n-1} d_i$.
4) RExt (r, s, i): Given the response $(r, s) \in \mathcal{R} \times \mathbb{Z}_2$ and index i, the client:
   - Decrypts r to obtain $\mathrm{Dec}(sk, r) = r' \in \mathbb{Z}_2$
   - Computes the bit $d_i = r' + s \cdot \prod_{k=0}^{l-1} i_{(k)} \in \mathbb{Z}_2$.

Theorem 1 (Correctness). *The generic PIR protocol described above is correct for any SWHE sheme on bits $\mathcal{E}$ which can evaluate polynomial of degree $l-1$, any security parameter λ, any database d with any size n and index $0 \leqslant i < n-1$.*

Proof. The degree of polynomial with respect to ciphertext in equation (5) is $l-1$. Thus the homomorphic property of $\mathcal{E}$ implies that

$$\mathrm{Dec}(sk, r) + s \cdot \prod_{k=0}^{l-1} i_{(k)} = \sum_{t=0}^{n-1} \left(d_t \cdot \prod_{k=0}^{l-1} {i_{(k)}}_k^t \right) - s \cdot \prod_{k=0}^{l-1} i_{(k)} + s \cdot \prod_{k=0}^{l-1} i_{(k)} = d_i. \quad \square$$

3.2. Security proof

Based on the formal definition of security for PIR protocol given in Section 1, we have

Theorem 2 (Security). *If the SWHE scheme $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ is IND-CPA secure, then PIR protocol described above is secure.*

Proof. We show that if a PPT adversary $\mathcal{A}$ against the PIR scheme can distinguish two queries, than there is an adversary $\mathcal{A}'$ that can distinguish two ciphertexts.

Assume $\mathcal{A}$ distinguishes i^0 and i^1 with probability ϵ. That is,

$$\left|\Pr\left[\mathcal{A}(1^\lambda, c^0, state) = i^1\right] - \Pr\left[\mathcal{A}(1^\lambda, c^1, state) = i^1\right]\right| > \epsilon,$$

where $c^i = (c^i_0, \ldots, c^i_{n-1})$ such that $c^k_j \leftarrow \mathrm{Enc}\left(sk, i^k_{(j)}\right)$. This implies,

$$\sum_{k=0}^{l-1}\Big|\Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k)) = \mathrm{Hyb}\,(i^0, i^1, k-1)\right] -$$
$$- \Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k-1)) = \mathrm{Hyb}\,(i^0, i^1, k-1)\right]\Big| \geqslant$$
$$\geqslant \Big|\sum_{k=0}^{l-1}\big(\Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k)) = \mathrm{Hyb}\,(i^0, i^1, k-1)\right] -$$
$$- \Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k-1)) = \mathrm{Hyb}\,(i^0, i^1, k-1)\right]\big)\Big| > \epsilon,$$

where $\mathrm{Hyb}\,(a, b, k) \stackrel{\mathrm{def}}{=} (a_0, \ldots, a_{k-1}, b_k, \ldots, b_{l-1})$.

Therefore, there must exist $k^\star$ such that

$$\Big|\Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k^\star)) = \mathrm{Hyb}\,(i^0, i^1, k^\star-1)\right] -$$
$$- \Pr\left[\mathcal{A}(\mathrm{Hyb}\,(c^0, c^1, k^\star-1)) = \mathrm{Hyb}\,(i^0, i^1, k^\star-1)\right]\Big| > \frac{\epsilon}{l}.$$

Consider the algorithm

$$\mathcal{A}'(c^\star) \stackrel{\mathrm{def}}{=} \begin{cases} i^0_{(k^\star)}, & \text{if } \mathcal{A}(1^\lambda, (c^0_0, \ldots, c^0_{k-1}, c^\star, c^1_{k+1}, \ldots, c^1_{l-1})) = i^0; \\ i^1_{(k^\star)}, & \text{othewise.} \end{cases}$$

$\mathcal{A}'$ runs in polynomial time since $\mathcal{A}$ does. Furthermore, $\mathcal{A}'$ will distinguish $c^\star$ with probability $\frac{\epsilon}{l^2}$. □

4. Efficiency analysis

Since the construction described above can potentially be used with any SWHE scheme, the number of homomorphic operations per request and the size of ciphertexts were used as an efficiency metric.

The most time consuming step of the response generation is computing the linear combination (5). An efficient algorithm of encrypted memory reading proposed in [10] requires approximately $O(n)$ homomorphic additions and $O(n)$ multiplications on the server side per request.

Current SWHE schemes have a ciphertext expansion property. It means that the size of server response grows with the multiplicative depth of the circuit. Unlike previous construction, in the proposed PIR protocol the multiplicative depth is $\lceil \log_2 (l-1) \rceil$. So overall, the server side computational complexity and communication overhead in our protocol is lower.

The current implementation (based on the SWHE scheme from [9]) of the proposed protocol has the response time 1.88 seconds for a query to a database with 10-bit indexes and 1-Kb records (the benchmarks were measured on an i7 @ 2.20 GHz machine).

Conclusion

This research makes another step towards making *private information retrieval* applicable for the market use-cases. Nowadays the computation and communication overhead are the major issues. We have shown how to improve existing approaches by reducing multiplicative depth of the response generation circuit and utilization recursive retrieval algorithm.

As the future work, we will test our generic protocol with suitable SWHE scheme. Recently, Tian et al. [11] showed that the SWHE scheme from [7] can be effectively realized on GPU. This result gives a way to significantly improve the performance, because a compute-intensive retrieval of multi-bit records admits massively parallel computations. Thus, the speed-up of PIR can be achieved by using parallel computations.

References

[1] B. Chor, E. Kushilevitz, O. Goldreich, M. Sudan, *Private Information Retrieval*, ACM, 45, 1998.

[2] E. Kushilevitz, R. Ostrovsky, *Replication is not needed: single database, computationally-private information retrieval*, In FOCS, 1997, pp 364.

[3] C. Gentry, *A fully homomorphic encryption scheme*, PhD thesis, Stanford University, 2009.

[4] K. Lauter, M. Naehrig, V. Vaikuntanathan, *Can homomorphic encryption be practical?*, Technical Report MSR-TR-2011-61, *Microsoft Research*, 2011.

[5] Z. Brakerski, V. Vaikuntanathan, *Efficient fully homomorphic encryption from (standard) LWE*, FOCS, 2011, pp. 97-106.

[6] X. Yi, M. Kaosar, R. Paulet, E. Bertino, *Single-database private information retrieval from fully homomorphic encryption*, IEEE Trans. Knowl. Data Eng. 25(5), 2013, pp. 1125-1134.

[7] M. Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan, *Fully Homomorphic Encryption over the Integers* Gilbert, H., ed.: EUROCRYPT. Volume **6110** of Lecture Notes in Computer Science, *Springer*, 2010, pp. 24-43.

[8] C. Dong, C. Chen, *A Fast Single Server Private Information Retrieval Protocol with Low Communication Cost*, ESORICS, Lecture Notes in Computer Science, Volume **8712**, 2014, pp 380-399.

[9] Z. Brakerski, C. Gentry, V. Vaikuntanathan, *(Leveled) fully homomorphic encryption without bootstrapping*, ITCS, 2012, pp. 309-325.

[10] D. Zhuravlev, I. Samoilovych, R. Orlovskyi, I. Bondarenko, Y. Lavrenyuk, *Encrypted Program Execution*, TrustCom, 2014.

[11] Y. Tian, M. Al-Rodhaan, B. Song, A. Al-Dhelaan, H. Ma, *Somewhat homomorphic cryptography for matrix multiplication using GPU acceleration*, ISBAST, 2014.

Contact information

D. Zhuravlev
Department of Mechanics and Mathematics
Kyiv National Taras Shevchenko University
Volodymyrska, 64, Kyiv 01033, Ukraine
E-Mail(s): `dzhuravlev@ukr.net`

Received by the editors: 11.03.2015
and in final form 16.07.2015.

Contents

Наукове видання

АЛГЕБРА ТА ДИСКРЕТНА МАТЕМАТИКА
ТОМ 19, НОМЕР 2, 2015

Заснований у 2002 році.
Свідоцтво про державну реєстрацію
КВ № 14443-3414ПР від 14.08.2008.
Виходить чотири рази на рік англійською мовою.

Журнал внесений до переліку наукових фахових видань України (фізико-математичні науки)
Постанова президії ВАК України від 14 жовтня 2009 р. № 1-05/4.

Засновник і видавець:

"Луганський національний університет імені Тараса Шевченка"

Підписано до друку рішенням Вченої ради механіко-математичного факультету Київського національного університету імені Тараса Шевченка (протокол № 8 від 2 червня 2015 р.)

Здано до складання 02.04.2015р. Підписано до друку 02.06.2015р.
Формат 60x84 1/16. Папір офсетний. Гарнітура Times New Roman.
Друк лазерний. Умов. друк. арк. 10,00.
Тираж 125 екз.

Видавництво Державного закладу
"Луганський національний університет імені Тараса Шевченка"
пл. Гоголя, 1, м. Старобільськ, 92703. Тел.: (06461) 2-26-70

Надруковано у типографії ТОВ "Цифра принт".
Свідоцтво про реєстрацію Серія А01 N 432705 від 03.08.2009р.
61058 м. Харків, вул. Данилевського, 30.