Algebra and Discrete Mathematics
Number 3. **(2003).** pp. 102 – 109

RESEARCH ARTICLE

On a group theoretical construction of expanding graphs

Vasyl A. Ustimenko

Communicated by V. M. Usenko

1. Introduction

Constructions of an infinite families of expanding graphs is an important and hard combinatorial problem. A few known examples had been formulated in terms of a Group Theory (special Cayley graphs of semisimple Lie groups satisfying Kazhdan property).

In this note we present a new construction. Both the construction of graphs and evaluation of their expansion properties are also group theoretical.

We construct for each $t \geq 3$, an infinite family of t-regular expanding graphs.

Let A be a set of vertices of a graph X. We define ∂A to be the set of all elements $b \in X - A$ such that b is adjacent to some $a \in A$.

We say that t-regular graph with n vertices has an expansion constant c if, for each set $A \subset X$ with $|A| \leq n/2$, $|\partial A| \geq c|A|$.

One says that the infinite family of graph X_i is a family of expanders constant c, if there exists a constant c such that every X_i has the expansion constant c.

Expander graphs are widely used in Computer Science, in areas ranging from parallel computation to complexity theory and cryptography [3].

An explicit construction of infinite families of t-regular expanders (t fixed) turns out to be difficult.

Gregory Margulis [4] constructed the first family of expanders. He used representation theory of semisimple groups.

It can be shown that if $\lambda_1(X)$ is the second largest eigenvalue of the adjacency matrix of the graph X, then $c \geq (t - \lambda_1)/2t$. Thus, if λ_1 is small, the expansion constant is large. A well-known result of Alon and Bopanna says that, if X_n is an infinite family of t-regular graphs (t fixed), then $\lim \lambda_1(X_n) \geq 2\sqrt{t-1}$. This statement was the motivation of Ramanujan graphs as special objects among t-regular graphs. A finite t-regular graph Y is called Ramanujan if, for every eigenvalue λ of Y, either $|\lambda| = t$ or $|\lambda| \leq 2\sqrt{t-1}$. So, Ramanujan graphs are, in some sense, best expanders.

Lubotzky, Phillips and Sarnak ([4]) proved that graphs defined by Margulis in [4] are Ramanujan graphs of degree $p+1$ for all primes p. Morgenstern [6] proved that, for each prime degree q, there exists a family of Ramanujan graphs of degree $q-1$.

In this note, we construct a family of graphs, which contains for each $t > 2$, infinitely many bipartite t-regular graphs Γ the eigenvalues of which are bounded from above by $2\sqrt{t}$. Eigenvalues of distance 2 graph for Γ, which has a degree $t(t-1)$, can be written as $2t\cos\alpha + t$, for some α.

This variety of "almost Ramanujan graphs" contains some well known families of graphs, which degrees q are prime powers, such as Wegner graphs $W_k(q)$, $k = 1, 2, \ldots$ [9] or $CD(k,q)$ [2]. They proved to be useful in Computer Science (see [9, 10, 11, 12, 13, 14]). For some of them list of the eigenvalues have been obtained via computer simulation [7, 8].

2. Preliminaries

The *girth* of a graph G, denoted by $g = g(G)$, is the length of the shortest cycle in G.

The distance $d(x,y)$ between vertices x and y of the graph is the number of edges in a minimal pass between x and y.

The *spectrum* $spec(A)$ of G is the set of all eigenvalues of the adjacency matrix A of graph G.

An incidence structure is a set $\Gamma = P \cup L$ where P and L are two disjoint sets (the set of points and set of lines, respectively) together with symmetric binary relation I on Γ (incidence relation). We will identify I with the related bipartite graph.

An important example of the above is the so-called group incidence structure $\Gamma(G, G_i)_{i\in\{1,2\}}$. Here G is an abstract group and $\{G_s\}_{s\in\{1,2\}}$ is a pair of distinct subgroups of G. The objects of $\Gamma(G, G_i)_{i\in\{1,2\}}$ are the cosets of G_i in G for $i = 1, 2$. Cosets α and β are incident precisely when $\alpha \cap \beta \neq \emptyset$. The type function is defined by $t(\alpha) = i$ where $\alpha = xG_i$ for some $x \in G$.

A definition of unipotent-like factorisation, i.e. a factorisation of a group U into 3 subgroups U_1, U_2 and U_3 such that $U_1 \cap U_2 = 1$, $U_1 \cap U_3 =$

1, $U_2 \cap U_3 = 1$, and U_3 contains $[U_1, U_2]$ was given in [11]. In this case, there are unique decompositions $u \in U$ of the kinds $u = u_1u_2u_3$ and $u = u_2u_1u_3'$ where $u_1 \in U_1$, $u_2 \in U_2$, and $u_3, u_3' \in U_3$.

The following statement gives us a natural examples.

Proposition 2.1. *Let G be a free product of finite nontrivial groups G_1 and G_2. Let G_3 be the group $[G_1, G_2]$. Then $G = G_1G_2G_3$ is a unipotent-like factorization.*

Proof. It is well known that the group $[G_1, G_2]$ is normalised by the both subgroups G_1 and G_2 hence is normal in G. Since $G/[G_1, G_2] = \bar{G}_1 \times \bar{G}_2$ where $\bar{G}_i = G_i[G_1, G_2]/[G_1, G_2]$ for $i = 1, 2$, the desired result follows immediately. □

Let $G = G_1G_2G_3$ be a unipotent-like factorization and $F < G_3$ be a normal subgroup of G. It is clear that $(G/F) = G_1G_2(G_3/F)$ is also a unipotent-like factorization.

Let us consider the following *navigation function* n from $\Gamma(G) = \Gamma(G)_{G_1,G_2}$ onto the set $C = G_1 \cup G_2$ of *colors* $C = G_1 \cup G_2$: $n(G_1x) = g_2$, where $x = x_1x_2x_3$, $x_i \in G_i$, and $n(G_2y) = y_1$, where $y = y_2y_1y_3$, $y_i \in G_i$.

Term *navigation* is used because each vertex has a uniquely defined neighbor of chosen color. Let $F < G_3$ be a normal subgroup of G . It is clear that $G/F = G_1G_2(G_3/F)$ is also a unipotent-like factorization and canonical homomorphism $\eta : G \to G/F$ induces natural graph homomorphism indη:$\Gamma(G) \to \Gamma(G/F)$, which preserves navigation function.

Proposition 2.2. *Let $G = G_1G_2G_3$ be a unipotent-like factorization of finite group G and F be a normal subgroup of G such that $F < G_3$. Then*

$$\mathrm{spec}(\Gamma(G/F)_{G_1,G_2}) \subset \mathrm{spec}(\Gamma(G)_{G_1,G_2})$$

Proof. Let $i = \mathrm{ind}(\eta)$ be a natural homomorphism of $\Gamma_1 = \Gamma(G)$ onto $\Gamma_2 = \Gamma(G/F)$, V_i be the set of vertices of the graph Γ_i with the adjacency matrix A_i, F_i be a vector space of real functions on V_i and ϕ_i be a linear operator on F_i with the standard matrix A_i. Let us put $H_1 = G$ and $H_2 = (G/F)$. and $F = \{f \in F_1 | [i(x) = i(y)] \to [f(x) = f(y)]\}$.

The value of $\phi_i(f(x)$ for $x \in (H_i : G_1)$ $((H_i : G_2))$ is the sum of elements $f(y_g)$, where y_g is the neighbor of x of color g, $g \in G_2$ (G_1, respectively). The map i preserves navigation function and type function. Thus F is an invariant subspace of ϕ_1 and the induced operator $\phi_1|F$ is similar to ϕ_2.

□

Let us consider a Coxeter system (W, S) for $W = D_\infty$ i. e. set of generators $S = \{s_1, s_2\}$ together with the set defining relations ${s_1}^2 = 1$, ${s_2}^2 = 1$.

Let q_s, $s \in S$ be a system of indeterminates, $R = Z[q_s|s \in S]$ and $F = Frac(R)$. Then there exists a *Tits generic algebra* $H(S, R)$, i.e., an F-algebra, for which $\{T_w|w \in W\}$ is a basis, and where multiplication is uniquely determined by the following formulas

$T_sT_w = T_{sw}$ if $l(sw) > l(w)$,

$T_sT_w = q_sT_{sw} + (q_s - 1)T_w$ if $l(sw) < l(w)$,

where $s \in S$, $g \in W$, and $l(g)$ is the length of a reduced decomposition of g.

The algebra $H(S, R)$ has a presentation as an R algebra with generators T_s, $s \in S$, and relations as follows:

$(T_s)^2 = q_sT_1 + (q_s - 1)T_s$,

Let $H(s, R)$ be an R-subalgebra of $H(S, R)$ defined as follows.

$H(s, R) = \{a \in H(S, R)|T_sa = aT_s = q_sa\}$

We will refer to $H(s, R)$ as the *parabolic Tits algebra* with respect to D_∞ and $s \in S$.

Let $W_s =< s >$ and $\{O_0, O_1, \cdots, \}$ be the totality of all double cosets of W by W_s. For each double coset O_i, put

$b_i = \sum_{w \in O_i} T_w$

The set $\{b_i|i = 0, 1, \cdots\}$ is a basis of the algebra $H(s, R)$.

For each $s \in S$, let $q_s = q$, $q \in Z$ be the specialization for our indeterminates, such that $q > 1$. Then this specialization induces morphisms of algebras $H(S, R)$ and $H(s, R)$ onto Q-algebras $IH(q)$ and $IH(s, q)$. We will refer to $IH(q$ and $IH(s, q)$ as the *Iwahory-Hecke algebra* and *Iwahory-Hecke parabolic subalgebra* of D_∞, respectively.

We can treat elements of group algebra $C(G)$ as functions from G to C. Let G_1 and G_2 be subgroups of G. Functions which are invariant on double cosets G_1gG_2 form the *double coset algebra* $D(G)_{G_1,G_2}$. If $G_1 = G_2$ instead of this term we will use the more popular term *Hecke algebra.*

A C^* algebra is a pair $(A, *)$ where A is an algebra over the field C of comlex numbers and $x \to x^*$ is an idempotent bijective map on A (unary operation). A represenration of C^* algebra A is a representations of A which agrees with the operation $*$. When * is fixed we will use the term *unitary represantations* instead of representations of C^* algebra. Let URep(A) stands for the set of all unitary finitedimensional representations of A.

We will consider the group algebra $C(G)$ as C^* algebra is a group algebra $C(G)$ with the standard * operation $f(g)^* = f(g^{-1})$. For evaluation of the second largest eigenvalue of the graph in our construction we will use the following result: the finitedimensional unitary represantations of the D_∞ are of dimensions 1 or 2. In fact, all initary representations of D_∞ are finidimensional (see [15]).

3. Main results

Theorem 3.1. *Let G be a finite group, let G_1 and G_2 be isomorphic subgroups of G such that $G =< G_1, G_2 >$, $G = G_1G_2G'$ be a unipotent-like factorization, and set $T = |G_1|$.*

(i) *Set $\Gamma^2 = (G/G_1, \{(x,y)|d_\Gamma(x,y) = 2\}$ for $\Gamma = \Gamma(G)_{G_1,G_2}$. Then each eigenvalue of Γ^2 can be written in the form $t + 2t\cos(\phi)$ or $t(t-1)$*

(ii) *If Γ has no cycles of length 4 then the second largest eigenvalues of Γ are bounded by $2\sqrt{t}$.*

Proof. In the group algebra $C(G)$ of G, form the elements

$$S_i = \sum_{w \in G_i \setminus 1} w \quad \text{and} \quad Q_i = \sum_{w \in G_i} w, i = 1, 2,$$

and let $B = B(S_1, S_2)$ be the subalgebra generated by S_1 and S_2.

It is clear that double coset algebra $D = D(G)_{G_1,G_2}$ (Hecke algebra) for the action of $(G, (G : G_1) \cup (G : G_2))$ and the Hecke algebra D^2 corresponding to the action $(G, (G : G_1))$ are subalgebras of algebra $B = B(S_1, S_2)$. Element of D^2 corresponding to Γ^2 is $2Q_1Q_2Q_1$. In case of unipotent-like factorization we can consider both D and B as C^* subalgebras of C(G) with operation $*$ induced by $f(g)^* = f(g^{-1})$:

$$S_1{}^* = S_1 \quad \text{and} \quad S_2{}^* = S_2 \tag{1}$$

By direct checking, we got

$$(S_i)^2 = (t-1)E + (t-2)S_i, i = 1, 2 \tag{2}$$

We could identify the algebra D^2 with the quotient I of the Iwahori-Hecke parabolic subalgebra $IH(s_1, t-1)$ of D_∞ .

Relations (2) can be written as

$$a_i{}^2 = E,\ a_i = 2/t(S_i - (t-2)/2E),\ i = 1, 2,\ a_i{}^* = a_i$$

Thus, the map ϕ defined by the rules $\phi(s_i) = (2/t(S_i - (t-2)/2)$ is an epimorphism of the group algebra $C(D_\infty)$ onto C^*-algebra B. So, there is an embedding of $URep(B(G))$ and $URep(C(D_\infty))$, $(D^2))$ is the image of parabolic subalgebra $IH(s_1, 1)$ of $C(D_\infty)$. The descriptions of all finite-dimensional representations of group algebras for D_n, $n \le \infty$, and its parabolic subalgebras can be written uniformly for all possible $n \in N \cup \infty$. There are one-dimensional representations and those of dimension 2 of the kind $A = (a_{ij})$, $a_{11} = \cos(\alpha)$, $a_{12} = \sin(\alpha)$, $a_{22} = a_{11}$, $a_{21} = -a_{12}$. The eigenvalue of a_2 is the trace $2\cos(\alpha)$ of matrix A. We have that $a_2 = ((2Q_2)/t - 1)$, Eigenvalues of matrix $2Q_1Q_2Q_1$ (same with $2Q_2$) form a $Spec(D^2)$. Thus, any element λ from $Spec(D^2)$ which is different from the valency can be written in the form

$$t + \mathrm{tr}(tA) = t + 2t\cos(\alpha). \tag{3}$$

If the graph does not contains cycles of length 4 then a path of length 2 between given vertices is unique, and the matrix of de Morgan's square of Γ is a $0,1$-matrix), and its eigenvalues are t, $-t$ and trace$(\sqrt{(tA)})$, (see [1]), i.e.

$$2\sqrt{t}\cos(\alpha). \tag{4}$$

□

Remark. Relations for the generators S_1 and S_2, different from (1) and (2) have a trigonometric nature. They determine the angles α in Equations(3) and (4) for eigenvalues of the graphs Γ and Γ^2.

Theorem 3.2. *Let G_1, G_2 are two copies of finite group G of order $|t|$. Then the free product $F = G_1 * G_2$ contains infinitely many normal subgroups H of finite index, such that graphs $\Gamma(F/H)_{G_1,G_2}$ form an infinite family of expanders with embedded spectra for which second largest eigenvalue is bounded by $2\sqrt{t}$.*

Proof. It is clear that we have the unipotent factorization $F = G_1G_2F'$, where $F' = [G_1, G_2]$ is the commutator of G_1 and G_2. Let us consider a filtration H_i of F such that $H_i \cap G_j = 1$ for $i = 2, 3, \dots,$ $j = 1, 2$ and H_i are invariant for automorphism of F which permutes G_1 and G_2. Let Γ_i be the incidence structure $\Gamma_i = \Gamma(F/H_i)_{G_1,G_2}$, $i = 2, 3, \dots$. The canonical homomorphism of F/H_{i+1} onto F/H_i induces the graph homomorphism of Γ_{i+1} onto Γ_i. The projective limit of Γ_i is the infinite tree $\Gamma(F)_{G_1,G_2}$. Thus the Γ_i, $i = 2, 3, \dots$, form an infinite family of graphs of unbounded girth and there are infinitely many subgroups H_i such that the girth of Γi is greater than 4. Spectra of the graph Γ_I are eigenvalues of Γ_{i+1} according to Proposition 2.2.

□

4. Acknowledgements

The author is deeply grateful to A. V. Borovik for useful remarks and support of this research. I am indebted to the referee for a careful reading and his help to improve style and prepare this note for a wider audience.

References

[1] D. Cvetcovic', M. Doob, *Graph Spectra*, North Holland (1988).

[2] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A New Series of Dense Graphs of High Girth*, Bull (New Series) of AMS, 32, no. 1 (1995), 73–79.

[3] A. Lubotzky, *Discrete Groups, Expanding graphs and Invariant Measures*, Progr. in Math., 125, Birkhoiser, 1994.

[4] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica, 8 (3) (1988), 261–277.

[5] G. Margulis, *Explicit construction of graphs without short cycles and low density codes*, Combinatorica 2 (1982), 71–78.

[6] M. Morgenstern, *Ramanujan graphs and diagrams, function field approach*, in DIMACS Series in Discrete Math. and Theor. Comp. Sci., vol. 10, 111–116.

[7] V. Gounder, *Algebraic graphs and their spectra*. Master Thesis, Department of Math and Computing, The University of the South Pacific, 2001, 176 pp.

[8] V. Ustimenko, V. Gounder, *Algebraic constructions of expanding graphs of given valency*, in Proceedings of Conference on Algebraic Systems, Sumy, Ukraine, 2001, pp. 54–57.

[9] R. Wegner, Extremal graphs with no C^4, C^6, or C^{10}'s, J. of Combinatorial Theory, Series B, 52 (1991), 113–116.

[10] V. A. Ustimenko, *Random Walks on special graphs and Cryptography*, AMS Meeting, Louisville, March, 1998, 3 pp.

[11] V. A. Ustimenko, *Coordinatization of regular tree and its quotients*, In the volume "Voronoi's Impact in Modern Science": (Proceedings of Memorial Voronoi Conference, Kiev, 1998), Kiev, IM AN Ukraine, July, 1998, pp. 125–152.

[12] V. Ustimenko and D. Sharma, *Special Graphs in Cryptography*, in Proceedings of 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC 2000), Melbourne, December 1999, 5 pp.

[13] V. Ustimenko and D. Sharma, *CRYPTIM: The system to encrypt text and image data*, in Proceedings of International ICSC congress on Intelligent Systems and Applications, December 2000, University of Wollongong, 14 pp.

[14] V. Ustimenko. *CRYPTIM: Graphs as Tools for Symmetric Encryption*, in Lecture Notes in Computer Science, Springer, v. 2227, 278-287.

[15] V. Ostrovskyi, Yu Samojlenko, *Introduction to the theory of representations of finitely presented* * *algebras ,1. Representations by bounded operators*, Rev. Math. and Math. Phys, 1999, v11, 1- 261.

Contact information

V. A. Ustimenko Department of Mathematics and Statistics
Sultan Quaboos University
Sultanate of Oman
E-Mail: vasyl@squ.edu.om

Received by the editors: 05.08.2003.