© Algebra and Discrete Mathematics RESEARCH ARTICLE
Volume **35** (2023). Number 2, pp. 134–167
DOI:10.12958/adm2130

Overlaps in field generated circular planar nearrings

W.-F. Ke and H. Kiechle

Communicated by G. Pilz

Abstract. We investigate circular planar nearrings constructed from finite fields as well the complex number field using a multiplicative subgroup of order k, and characterize the overlaps of the basic graphs which arise in the associated 2-designs.

1. Introduction

Planar nearrings were defined to connect nearrings and geometry. The first three examples of planar nearrings were obtained by twisting the multiplication of the complex number field, $\mathbb{C}$. These examples provide many ideas for deriving geometrical and combinatorial objects from planar nearrings. One example even inspires the notion of circularity in planar nearrings (see [2] for details). In a circular planar nearring, "circles" are formed and one can discuss the radii and centers of these circles just as one would with circles in a complex plane. Understanding circular planar nearrings also enables the creation of more circular planar nearring structures in $\mathbb{C}$.

One direction of research on circular planar nearrings involves selecting equivalence classes, E_c^r, of circles with radius r and centers on another circle which has radius c and center on 0. Each E_c^r has an associated

2020 MSC: 05B05, 11D41.
Key words and phrases: Ferrero pair, 2-design, circularity, overlap.

graph, $G(E_c^r)$, which is naturally derived. This graph is sometimes the union of spanning subgraphs called "basic graphs". In other words, the "overlapping" of some basic graphs produces the graph $G(E_c^r)$. In [5], it is shown that if a circular planar nearring N is derived from a ring and r is fixed, then the total number of basic graphs that appear in $G(E_c^r)$, where $c \in N^* = N \setminus \{0\}$, is a function of k only, even if the nearring N is changed to a different one. Since several basic graphs can exist in a graph $G(E_c^r)$, the total number of the graphs $G(E_c^r)$, where $c \in N^*$, varies from one circular planar nearring to another.

In this work, we continue to study E_c^r's for circular planar nearrings constructed from finite fields as well the complex number field using a multiplicative subgroup of order k. We begin with a brief review of circular planar nearrings derived from fields, including some results in [5]. We then define the overlaps of basic graphs and show that for each k, there exists a finite set of primes, $\mathcal{Q}_k$, such that if $F = \mathrm{GF}(q)$ is a Galois field of order q with $\mathrm{char}F \notin \mathcal{Q}_k$ such that $k \mid (q-1)$, and N is a planar nearring constructed from F using the multiplicative subgroup of order k in F, then the overlapping of the basic graphs that occur in N is exactly the same as that in $\mathbb{C}$ when the regular polygon $C_k = \{z \in \mathbb{C} \mid z^k = 1\}$ is used.

In section 4, we discuss the normalized form for overlaps which provide us the base to compare. In sections 5 and 6, with the help of a theorem by Conway and Jones (Theorem 6.3), we classify all overlaps of basic graphs in $\mathbb{C}$. In the last two sections, we classify all triple overlaps of basic graphs in $\mathbb{C}$, and conclude that no further overlaps can be found.

The results we obtained in [5] have found applications (see [6–8]). An application of the results obtained in this paper to the number of solutions of equations $ax^m + by^m - cz^m = 1$ over a finite field is in preparation.

2. Preliminaries

On a (left) nearring $(N, +, \cdot)$, the relation $=_m$ on N given by $a =_m b$ if $ax = bx$ for all $x \in N$ is an equivalence relation. When $N/=_m$ has at least three distinct classes and if $ax = bx + c$ has a unique solution $x \in N$ for all $a, b, c \in N$ with $a \neq_m b$, we say that N is *planar*. Let N be a planar nearring. For each $a \in N$, denote l_a the map from N to N given by $l_a(x) = ax$ for all $x \in N$. Then the set $\Phi = \{l_a \mid a \in N, a \neq_m 0\}$ is a fixed point free automorphism group of the additive group $(N, +)$. The pair (N, Φ) is called the *Ferrero pair* associated to N.

Conversely, start with a Ferrero pair (N, Φ), where $(N, +)$ is a group and Φ a fixed point free automorphism group of N, one can construct planar nearrings $(N, +, \cdot)$. For example, if we take a field F and a multiplicative subgroup A of F with $|A| \geqslant 3$, then $\Phi = \{l_a \mid a \in A\}$ is a fixed point free automorphism group of $(F, +)$ and so (F, Φ) is a Ferrero pair. We simply identify Φ with the set A in this case. Any planar nearring obtained from this Ferrero pair is referred to as a *field generated* planar nearring (see [1] and [2]).

Each planar nearring N gives rise to certain combinatorial structures. The one that concerns us here is an incidence structure. Let (N, Φ) be the Ferrero associated to N. For any $r, c \in N$, denote $\Phi r + c = \{\varphi(r) + c \mid \varphi \in \Phi\}$. With $\mathcal{B}_\Phi = \{\Phi r + c \mid r, c \in N, r \neq 0\}$, $(N, \mathcal{B}_\Phi)$ is an incidence structure. If N is finite, then $(N, \mathcal{B}_\Phi)$ is actually a 2-design (balanced incomplete block design).

In what follows, let $k \geqslant 3$ be a fixed integer and N a field generated planar nearring with associated Ferrero (F, Φ) where $(F, +, \cdot)$ is a field and Φ a multiplicative subgroup of F of order k. Let φ be a generator of Φ. We will assume that

$$\big|(\Phi a + b) \cap \Phi c\big| \leqslant 2 \text{ for all } a, b, c \in F^*. \tag{2.1}$$

If this holds, N, as well as the Ferrero pair (F, Φ), is called *circular*.

Put $\boldsymbol{k} = \{1, 2, \ldots, k-1\}$ and $\boldsymbol{k}_0 = \{0, 1, 2, \ldots, k-1\}$, and set

$$\mathcal{I} = \{(i, j, s, t) \in \boldsymbol{k}^4 \mid (i, j) \neq (s, t) \text{ and } (i, s) \neq (j, t)\}.$$

Characterizations of circularity of (F, Φ) are given in [9] (see also [2, §5.3]).

Theorem 2.1 ([9, Theorem 4])**.** *The pair (F, Φ) is circular if and only $(\varphi^i - 1)(\varphi^t - 1) - (\varphi^j - 1)(\varphi^s - 1) \neq 0$ for all $(i, j, s, t) \in \mathcal{I}$. This is equivalent to that $(\alpha - 1)(\beta - 1) - (\gamma - 1)(\delta - 1) \neq 0$ for all $\alpha, \beta, \gamma, \delta \in \Phi \setminus \{1\}$ with $(\alpha, \beta) \neq (\gamma, \delta)$ and $(\alpha, \gamma) \neq (\beta, \delta)$.*

Theorem 2.2 ([9, Theorem 8])**.** *For each integer $k > 2$ there exists a finite set of primes $\mathcal{P}_k$ such that for all finite fields F and multiplicative subgroup Φ of F^* of order k, (F, Φ) is circular if and only if $\mathrm{char} F \notin \mathcal{P}_k$.*

The proof of Theorem 2.2 shows that $\mathcal{P}_k$ is the union of the prime divisors of k and those of the resultants $\mathrm{Res}(g_k, f_{i,j,s,t})$, where $g_k = x^k - 1$

and

$$f_{i,j,s,t} = (1-x^i)(1-x^t) - (1-x^j)(1-x^s),\ (i,j,s,t) \in \mathcal{I}. \tag{2.2}$$

Now Φ acts on $\mathcal{B}_\Phi$ naturally: $\lambda \cdot (\Phi r + c) = \Phi r + \lambda c$ for all $\lambda \in \Phi$ and $\Phi r + c \in \mathcal{B}_\Phi$. For $r, c \in F^*$, denote by $E_c^r = \{\Phi r + \lambda c \mid \lambda \in \Phi\}$ the Φ-orbit of $\Phi r + c$ in $\mathcal{B}_\Phi$. Then $|E_c^r| = |\Phi| = k$. It is known that for any $r, r', c, c' \in F^*$, $E_c^r = E_{c'}^{r'}$ if and only if $\Phi r' = \Phi r$ and $c' = \lambda c$ for some $\lambda \in \Phi$ (see [5, (4.2)]). As (F, Φ) is circular, $\Phi r + c$, $r, c \in F^*$ is regarded as a "circle" with radius r centered at c, and hence E_c^r is the family of circles of radius r centered at the points of the circle $\Phi c = \{\lambda c \mid \lambda \in \Phi\}$.

To visualize E_c^r consider $(\mathbb{C}, U)$ where $U = \{z \in \mathbb{C} \mid z^k = 1\}$, the regular k-gon inscribed in the unit circle $C = \{z \in \mathbb{C} \mid |z| = 1\}$. Thus, $\mathcal{B}_U$ is the collection of all regular k-gons in the complex plane, and for $r, c \in \mathbb{C}^*$, E_c^r is the collection of the k regular k-gons with radius $|r|$, centered at λc, $\lambda \in U$.

Figure 2.1(a) shows two E_c^r's with $k = 6$. So each of them have 6 hexagons with centers (crosses) on another hexagon.

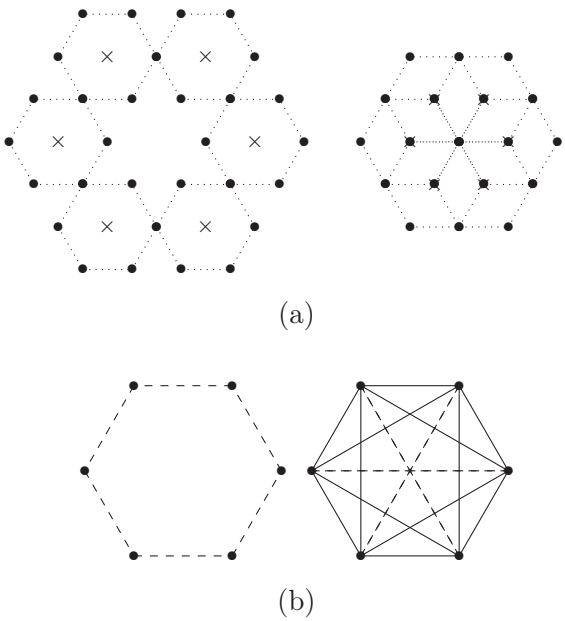

FIGURE 2.1. (a) Two E_c^r's and (b) the corresponding graphs

Two circles in an E_c^r may be disjoint, or intersect at one or two points. To make out such relations between the circles in E_c^r, a graph $G(E_c^r) = (\mathcal{V}, \mathcal{E})$ can be used. Here the vertex set $\mathcal{V}$ is simply Φ and the edge set is $\mathcal{E} = \{(\lambda, \mu) \mid (\Phi r + \lambda c) \cap (\Phi r + \mu c) \neq \varnothing\}$. For example, Figure 2.1(b) are the two graphs corresponding to the two E_c^r's on the left. In case that $(\lambda, \mu) \in \mathcal{E}$, the fact that $|(\Phi r + \lambda c) \cap (\Phi r + \mu c)| = 1$ or 2 is realized by coloring: an edge $(\lambda, \mu) \in \mathcal{E}$ is *even* if $|(\Phi r + \lambda c) \cap (\Phi r + \mu c)| = 2$ and *odd* if $|(\Phi r + \lambda c) \cap (\Phi r + \mu c)| = 1$. For $j \in \{1, 2, \ldots, k-1\}$, let $e_j = |(\Phi r + c) \cap (\Phi r + \varphi^j c)|$. Then the sequence $e(r, c) = (\epsilon_1, \epsilon_2, \ldots, \epsilon_{k-1})$ describes completely the edge structure of E_c^r. (See [5, (3.2)].)

Abstractly, a sequence $e = (\epsilon_1, \epsilon_2, \ldots, \epsilon_{k-1})$ with values 0, 1 and 2 satisfying $\epsilon_j = \epsilon_{k-j}$ for $j = 1, 2, \ldots, k-1$ gives rise to a colored graph $G(e)$. Here $G(e)$ has the vertex set $\{v_0, v_2, \ldots, v_{k-1}\}$ and edge set

$$\{(v_i, v_{i+t}) \mid 0 \leqslant i \leqslant k-1,\ 1 \leqslant t \leqslant k/2,\ \epsilon_t \neq 0\}.$$

An edge (v_i, v_{i+t}) is even if $\epsilon_t = 2$ and odd if $\epsilon_t = 1$. This way, one gets $G(E_c^r) = G(e(r, c))$. With such abstraction, basic graphs can be defined. Let $j \in \boldsymbol{k} = \{1, \ldots, k-1\}$. For the sequence $e = (\epsilon_1, \epsilon_2, \ldots, \epsilon_{k-1})$ with $\epsilon_i = 0$ if $i \notin \{j, k-j\}$ and $\epsilon_j = \epsilon_{k-j} = 1$, the graph $\mathit{\Gamma}_j^k = G(e)$ is called the jth odd basic k-graph. For the sequence $e = (\epsilon_1, \epsilon_2, \ldots, \epsilon_{k-1})$ with $\epsilon_i = 0$ if $i \notin \{j, k-j\}$ and $\epsilon_j = \epsilon_{k-j} = 2$, the graph $\mathit{\Pi}_j^k = G(e)$ is called the jth even basic k-graph. Specifically, if $\mathit{\Delta} \in \{\mathit{\Gamma}_j^k, \mathit{\Pi}_j^k\}$, then the edge set $\mathcal{E}(\mathit{\Delta})$ is $\{(v_i, v_{i+j}) \mid i \in \boldsymbol{k}_0\}$ and $i + j$ is carried out modulo k.

It turns out that each non-null graph $G(E_c^r)$ is the union of spanning subgraphs, each of them is an even basic k-graph, or an odd basic k-graph [5, (4.1)]. Figure 2.2 shows such a decomposition of the second graph in Figure 2.1(b) into three basic graphs, two even ones (with solid-line edges) and an odd one (with dotted-line edges).

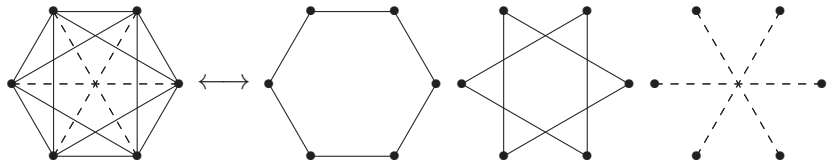

FIGURE 2.2. An $G(E_c^r)$ and the spanning basic graphs

Furthermore, an ith basic graph $\mathit{\Delta} \in \{\mathit{\Gamma}_i^k, \mathit{\Pi}_i^k\}$ is a spanning subgraph of $G(E_c^r)$ if and only if c is in $\Phi(\varphi^i - 1)^{-1}(\varphi^j - 1)$ for some $j \in \boldsymbol{k}$

[5, (4.3)]. Thus, the set $\mathcal{M}_r$ of E_c^r's with $G(E_c^r)$ non-null is given by $\mathcal{M}_r = \{E^r_{c_{i,j}} \mid i,j \in \boldsymbol{k}\}$, where each $c_{i,j} = (\varphi^i - 1)^{-1}(\varphi^j - 1)$.

Finally, for $i \in \boldsymbol{k}$, set $\gamma_i(r) = |\{E_c^r \in \mathcal{M}_r \mid \Gamma_i^k \prec G(E_c^r)\}|$ and $\pi_i(r) = |\{E_c^r \in \mathcal{M}_r \mid \Pi_i^k \prec G(E_c^r)\}|$, where "$\prec$" means "is a spanning subgraph of". It was shown in [5, (4.7), (4.9), (4.10)] that

1) if k is even, then $\gamma_i(r) = 1$ and $\pi_i(r) = k/2 - 1$, and
2) if k is odd, then $\gamma_i(r) = k - 1$ and $\pi_i(r) = 0$.

A natural question to ask now is what is the number of distinct graphs in $\{G(E_c^r) \mid E_c^r \in \mathcal{M}_r\}$? This amounts to learn when two or more basic graphs are at the same time the spanning subgraphs of some graph $G(E_c^r)$. In such a case, we say that *these two or more basic graphs overlap,* and that *an overlap occurs inside* $G(E_c^r)$.

From [5, (4.3)], one has

Theorem 2.3. *An overlap occurs inside $G(E_c^r)$ for some $r, c \in F^*$ if and only if there exist $w \in \boldsymbol{k}_0$, $i,j,s,t \in \boldsymbol{k}$, $i \neq s$, such that*

$$(\varphi^i - 1)^{-1}(\varphi^j - 1) = \varphi^w(\varphi^s - 1)^{-1}(\varphi^t - 1). \tag{2.3}$$

Remark 2.4. The situation $i = s$ and $j = k - t$ in the theorem gives the same ith basic graph, and so actually no overlap occurs. The situation $i = j$ and $s = t$ in the theorem describes the overlap of the ith and the sth basic graphs in $G(E_r^r)$. Therefore, the graph $G(E_r^r)$ is in fact a complete graph. Thus, there is always an overlap with $\lfloor \frac{k}{2} \rfloor$ edges. In fact, this is the only overlap with $\lfloor \frac{k}{2} \rfloor$ edges. The number $\lfloor \frac{k}{2} \rfloor$ comes from the fact that the edges (v_0, v_i) and (v_0, v_{k-i}) are the same for all $i \in \boldsymbol{k}$, as we have seen above. For obvious reasons, we'll later refer to these overlaps as trivial.

Our aim is to show in which situations overlaps can occur in (F, Φ). The following two lemmas from [7] will be needed.

Lemma 2.5 ([7, Lemma 9])**.** *Let (F, Φ) be circular, and let $\chi = (\psi - 1)^{-1}(\lambda - 1)$ where $\lambda, \psi \in \Phi \setminus \{1\}$. If $\chi \in \Phi$, then*

$$\textit{either } \chi = 1 \textit{ and } \psi = \lambda, \quad \textit{or } \chi = -\lambda \textit{ and } \psi = \lambda^{-1}.$$

The second case implies either $p = 2$, or that $|\Phi|$ is even.

Lemma 2.6 ([7, Lemma 10]). *Let (p,k) be circular. For $i,j,t \in \boldsymbol{k}$ we have*

1) *if k is even, then $c_{i,j} \in \Phi c_{i,t} \iff j = t$ or $i = k - t$, and*
2) *if k is odd, then $c_{i,j} \in \Phi c_{i,t} \iff j = t$ or, in case $p = 2$, $i = k - t$.*

3. Overlaps

We shall fix $r \in F^*$ and for $c \in F^*$ denote $\Gamma_c = G(E_c^r)$. Based on Theorem 2.3, we make the following definition.

Definition 3.1. We say that the quadruple $(i,j \mid s,t)$, where $i,j,s,t \in \boldsymbol{k}$, $i \neq s$, forms an *overlap* (with respect to (F,Φ), or (q,k)) if $c_{i,j} \in \Phi c_{s,t}$. In this case, we also say that $c_{i,j}$ is *involved in an overlap*.

We first collect some trivial cases, namely, an overlap $(i,j \mid s,t)$ with $j = i$, $j = t$ or $s = k - i$.

If $j = i$, then $c_{i,j} = 1$, which puts $c_{s,t}$ into $\Phi = \Phi c_{j,i}$. By Lemma 2.5, if $t \neq s$, then either $2 \mid k$ and $t = k - s$, or $p = 2$ and $t = k - s$.

If $j = t$, then

$$\frac{\varphi^j - 1}{\varphi^i - 1} \in \Phi \frac{\varphi^j - 1}{\varphi^s - 1} \iff \frac{\varphi^s - 1}{\varphi^i - 1} = c_{i,s} \in \Phi = \Phi c_{j,j}$$

so Lemma 2.5 applies again, and we have either $2 \mid k$ and $s = k - i$ where $i \neq \frac{k}{2}$, or $p = 2$ and $s = k - i$ with $i \neq s$.

If $s = k - i$, then we have $c_{i,j} \in \Phi c_{k-i,t} = \Phi c_{i,k-t}$ as well. Lemma 2.6 says that if $t \neq k - j$, then either $2 \mid k$ and $t = j$, or $p = 2$ and $t = j$.

When describing or applying overlaps later, we mostly exclude the instances above by referring to them as *trivial overlaps*. They are presented in compact form in Table 3.1, where the first row shows the forms of trivial overlaps and the second row (if present) shows the extra conditions for the trivial overlaps to occur.

TABLE 3.1. All trivial overlaps $(i,j,s \in \boldsymbol{k},\ i \neq s)$

$(i,i \mid s,s)$	$(i,i \mid s,k-s)$	$(i,j \mid k-i,j)$	$(i,j \mid k-i,k-j)$
	$2 \mid k \vee p = 2$	$(2 \mid k \vee p = 2) \wedge j \neq \frac{k}{2}$	$i \neq \frac{k}{2}$

Our aim is to determine the set of all nontrivial overlaps, namely,

$$\mathcal{O} = \mathcal{O}(F,k) = \left\{ (i,j \mid s,t) \;\middle|\; \Phi\frac{\varphi^j-1}{\varphi^i-1} = \Phi\frac{\varphi^t-1}{\varphi^s-1}, (i,j,s,t) \in \mathcal{I} \right\}.$$

As $s = t$ would create a trivial overlap (see Lemma 2.6), we have added the condition $s \neq t$ to the above definition of $\mathcal{O}$ for symmetry. Also, we could have used the notation $\mathcal{O}(F,\Phi)$ instead of $\mathcal{O}(F,k)$, since Φ is uniquely determined by k. As we will also consider the complex number field $\mathbb{C}$, this notation comes in handy. Actually, the biggest part of this chapter will be occupied by the case when $F = \mathbb{C}$.

After clearing denominators and expanding (2.3), we find

$$\varphi^{\omega+j+s} + \varphi^{\omega} - \varphi^{\omega+s} - \varphi^{\omega+j} - \varphi^{t+i} + \varphi^t + \varphi^i - 1 = 0, \text{ with } i \neq s. \tag{3.1}$$

For $i,j,s,t \in \boldsymbol{k}$, $i \neq s$, and $\omega \in \boldsymbol{k}_0$ define polynomials over F

$$f_{i,j,s,t,\omega}(x) = x^{\omega+j+s} + x^{\omega} - x^{\omega+s} - x^{\omega+j} - x^{t+i} + x^t + x^i - 1 \tag{3.2}$$
$$= x^{\omega}(x^j-1)(x^s-1) - (x^i-1)(x^t-1). \tag{3.3}$$

Obviously, when $i \neq s$, then we have $(i,j \mid s,t)$ is an overlap if and only if there exists some $\omega \in \boldsymbol{k}_0$ such that $f_{i,j,s,t,\omega}(\varphi) = 0$.

A direct consequence of this is

Lemma 3.2. *Let (F,Φ) be circular, and let K be an extension field of F. Then (K,k) is circular and $\mathcal{O}(K,k) = \mathcal{O}(F,k)$.*

Proof. The statement about circularity comes directly from Theorem 2.1. The second statement is clear. □

This means that we can reduce our discussions to the smallest subfield of F containing a k-th root of unity. In particular, if F is finite, the set $\mathcal{O}(F,k)$ only depends on the characteristic p. We therefore sometimes simply write $\mathcal{O}(p,k)$ for $\mathcal{O}(F,k)$.

3.1. The complex numbers

We now set the stage for $\mathbb{C}$. Let $\phi = \exp(2\pi\boldsymbol{i}/k)$ be a primitive k-th root of unity in $\mathbb{C}$ where $\boldsymbol{i}^2 = -1$, and let $U = U_k = \langle\phi\rangle$. Notice that $(\mathbb{C},U)$ is circular for all k as U is a subset of the unit circle. We will prove

Theorem 3.3. *Let p be a prime. Then $\mathcal{O}(\mathbb{C},k) \subseteq \mathcal{O}(p,k)$. Moreover, for $k \geqslant 3$, the set $\mathcal{Q}_k = \{p \text{ prime} \mid p \text{ divides } k \text{ or } \mathcal{O}(\mathbb{C},k) \neq \mathcal{O}(p,k)\}$ is finite.*

To prepare the proof we first show a proposition. All information on cyclotomic fields needed for this can be found in [4, Ch. 13, §2].

Proposition 3.4. *Let p be a prime, $k \in \mathbb{N}$, $k \geqslant 3$, and F a field of characteristic p which contains an element of order k in F^*. Let ϕ be a primitive k-th root of unity over $\mathbb{Q}$ and let $\mathcal{N} : \mathbb{Q}(\phi) \to \mathbb{Q}$, be the Galois norm. Let g be a polynomial in $\mathbb{Z}[x]$.*

1) *There exists an element φ of order k in F^* such that $g(\varphi) = 0$ if and only if $p \mid \mathcal{N}(g(\phi))$.*
2) *In case $g(\phi) = 0$ (which is equivalent to $\mathcal{N}(g(\phi)) = 0$), we have $g(\psi) = 0$ for all elements ψ of order k in F^*.*

Proof. There is no loss in generality to assume that F is the smallest field with the given properties. As $\mathbb{Z}[\phi]$ is the ring of integers inside the kth cyclotomic field $\mathbb{Q}(\phi)$, there exists a ring-epimorphism $\theta : \mathbb{Z}[\phi] \to F; u \mapsto u^\theta$ mapping ϕ to some primitive k-th roots of unity, i.e., an element of order k, inside F. (If F where not smallest, the image of θ would be this smallest field.) We note that the kernel P of θ is a prime ideal containing p, and the map θ extends naturally to a ring-epimorphism of the polynomial rings $\mathbb{Z}[\phi][x] \to F[x]$, which is also denoted by θ. Let $g \in \mathbb{Z}[x]$ be a polynomial and let G be the Galois group of $[\mathbb{Q}(\phi):\mathbb{Q}]$. As norms of elements of $\mathbb{Z}[\phi]$ are all in $\mathbb{Z}$, we have that $\mathcal{N}(g(\phi)) \in \mathbb{Z}$. Thus we find

$$\begin{aligned} p \mid \mathcal{N}(g(\phi)) &\iff \mathcal{N}(g(\phi)) = \prod_{\sigma\in G} (g(\phi))^\sigma = \prod_{\sigma\in G} g\left(\phi^\sigma\right) \in P \\ &\iff g\left(\phi^{\sigma_0}\right) \in P \quad \text{for some } \sigma_0 \in G \\ &\iff \left(g\left(\phi^d\right)\right)^\theta = 0 \quad \text{for some } d \in \mathbb{Z}_k^\times \end{aligned}$$

since P is a prime ideal, and the group G is naturally isomorphic to the group of units $\mathbb{Z}_k^\times$ of the ring $\mathbb{Z}_k$. (Indeed, if σ_0 and d correspond under this isomorphism, then $\phi^{\sigma_0} = \phi^d$.)

Now, assume that $p \mid \mathcal{N}(g(\phi))$. Then there exists a $d \in \mathbb{Z}_k^\times$ such that $\varphi = \left(\phi^d\right)^\theta$ is a root of g. Conversely, assume that φ exists. Then there exists a preimage of φ under θ, which is a primitive k-th roots of unity in $\mathbb{Q}(\phi)$. As G is transitive on the primitive k-th roots of unity, there exists $d \in \mathbb{Z}^\times$ with $\varphi = \left(\phi^d\right)^\theta$. Therefore, $\left(g\left(\phi^d\right)\right)^\theta = g(\varphi) = 0$, and so $p \mid \mathcal{N}(g(\phi))$. This proves (1).

Next, suppose that $g(\phi) = 0$. We have $g(\phi^d) = 0$ for all $d \in \mathbb{Z}_k^\times$. Therefore,

$$0 = g(\phi^d)^\theta = g((\phi^\theta)^d).$$

Here, $(\phi^\theta)^d$, $d \in \mathbb{Z}_k^\times$, are exactly the elements of order k inside F^*. This is (2). □

Remark 3.5. In the above proof, $\mathcal{N}(g(\phi)) = 0$ implies that there exists a conjugate ϕ^{d_0} of ϕ such that $g(\phi^{d_0}) = 0$. But then, by the action of G, $g(\phi^d) = 0$ for all $d \in \mathbb{Z}^\times$, and thus $g(\varphi) = 0$ for all elements $\varphi \in F$ of order k.

Proof of Theorem 3.3. We shall use the Galois norm $\mathcal{N}$ as introduced in Proposition 3.4.

For $(i, j \mid s, t) \in \mathcal{O}(\mathbb{C}, k)$ there exists $\omega \in \boldsymbol{k}_0$ such that $f_{i,j,s,t,\omega}(\phi) = 0$. Then $(i, j, s, t) \in \mathcal{I}$ and $\mathcal{N}(f_{i,j,s,t,\omega}(\phi)) = 0$, thus $(i, j \mid s, t) \in \mathcal{O}(p, k)$ by Proposition 3.4.

Suppose that $p \in \mathcal{Q}_k$ and $p \nmid k$. Thus there exists $(i, j \mid s, t) \in \mathcal{O}(p, k) \setminus \mathcal{O}(\mathbb{C}, k)$ with a corresponding ω. By Proposition 3.4 again, $\mathcal{N}(f_{i,j,s,t,\omega}(\phi)) \neq 0$ and $p \mid \mathcal{N}(f_{i,j,s,t,\omega}(\phi))$. There are only finitely many polynomials $f_{i,j,s,t,\omega}$ and each integer $\mathcal{N}(f_{i,j,s,t,\omega}(\phi))$ has only finitely many prime divisors. Thus the set $\mathcal{Q}_k$ is finite as well. □

Remark 3.6. $f_{i,j,s,t,\omega}(\phi)$ is a sum of 8 roots of unity. Let e be the number of elements in $\boldsymbol{k}$ coprime to k. To form $\mathcal{N}(g(\phi))$, we multiply e such sums. After expansion, we have a total of 8^e summands, each of which is a product of roots of unity and has absolute value 1. This yields the inequality $|\mathcal{N}(g(\phi))| \leqslant 8^e$. Thus for every prime $p \in \mathcal{Q}_k$ we have $p < 8^e$.

Note that this is a very crude bound as our data show, and is suggested from the proof, too.

For every $k \geqslant 3$, the set $\mathcal{Q}_k$ is referred to as the set of *exceptional primes*.

Corollary 3.7. *It holds that $\mathcal{P}_k \subseteq \mathcal{Q}_k$. Consequently, if (p, k) is a Ferrero pair with $p \notin \mathcal{Q}_k$, then (p, k) is circular.*

Proof. We notice that the polynomials (2.2) used for getting $\mathcal{P}_k$ are all of the form $f_{i,j,s,t,0}(x)$, $(i, j, s, t) \in \mathcal{I}$. As $(\mathbb{C}, U)$ is circular, $f_{i,j,s,t,0}(\phi) \neq 0$ for all $(i, j, s, t) \in \mathcal{I}$ by Lemma 2.1. From Proposition 3.4, it follows immediately that $\mathcal{P}_k$ consists exactly the prime divisors of $\mathcal{N}(f_{i,j,s,t,0}(\phi))$, $(i, j, s, t) \in \mathcal{I}$. Thus, in both $\mathcal{Q}_k$ and $\mathcal{P}_k$, we are determining primes dividing $\mathcal{N}(f_{i,j,s,t,\omega}(\phi))$ wherever $\mathcal{N}(f_{i,j,s,t,\omega}(\phi)) \neq 0$ for $(i, j, s, t) \in \mathcal{I}$: in the case of $\mathcal{Q}_k$, $\omega \in \boldsymbol{k}_0$ and in the case of $\mathcal{P}_k$, $\omega = 0$. Therefore, we have $\mathcal{P}_k \subseteq \mathcal{Q}_k$. □

We provide some examples of $\mathcal{Q}_k$ with elements of $\mathcal{P}_k$ underlined in Table 3.2. The algorithm to find the elements is based on the above proof.

TABLE 3.2. Exceptional primes; elements from $\mathcal{P}_k$ underlined

$$\begin{aligned}
\mathcal{Q}_4 &= \{\underline{2}, 3, \underline{5}\},\\
\mathcal{Q}_5 &= \{\underline{5}, \underline{11}\},\\
\mathcal{Q}_6 &= \{\underline{2}, \underline{3}, 5, \underline{7}, \underline{13}, \underline{19}, 31, 37\},\\
\mathcal{Q}_7 &= \{\underline{2}, \underline{7}, 13, \underline{29}, \underline{43}, 71\},\\
\mathcal{Q}_8 &= \{\underline{2}, \underline{3}, \underline{5}, 7, 13, \underline{17}, \underline{41}, 73, 89, 97, 113\},\\
\mathcal{Q}_9 &= \{2, \underline{3}, 17, \underline{19}, \underline{37}, \underline{73}, \underline{109}, \underline{127}, 163, 181, 199, \underline{271}, 397, 541\},\\
\mathcal{Q}_{10} &= \{\underline{2}, 3, \underline{5}, \underline{11}, 19, 29, \underline{31}, \underline{41}, \underline{61}, \underline{71}, \underline{101}, 131, 151, 181, 191, 211, 241,\\
&\quad 251, 271, 281, 311, 331, 401, 421, 541, 641, 761, 881, 941\},\\
\mathcal{Q}_{11} &= \{3, \underline{11}, \underline{23}, 43, \underline{67}, \underline{89}, 109, \underline{199}, 331, \underline{353}, \underline{397}, 419, 463, 617, 661,\\
&\quad \underline{683}, 727, 859, 881, 947, 991, 1277, 1453, 2069, 2311, 2399\},\\
\mathcal{Q}_{12} &= \{\underline{2}, \underline{3}, \underline{5}, \underline{7}, 11, \underline{13}, \underline{17}, \underline{19}, 23, 29, 31, \underline{37}, \underline{61}, \underline{73}, \underline{97}, \underline{109}, \underline{157}, \underline{181},\\
&\quad \underline{193}, 229, 241, 277, 313, 337, 349, 373, 397, 409, 421, 433, 541, 601,\\
&\quad 661, 769, 1009\}.
\end{aligned}$$

The following examples from [5] are some nontrivial overlaps for Ferrero pairs (q, k). Note that these are universal in the sense that they do not depend on q (or p), but only on the shape of k.

Example 3.8. If $k = 6\ell$, $\ell \in \mathbb{N}$, then φ^ℓ is a sixth root of unity, and $\varphi^{3\ell} = -1 = \varphi^{2\ell} - \varphi^\ell$. Therefore

$$\varphi^\ell \frac{\varphi^\ell - 1}{\varphi^i - 1} = \frac{-1}{\varphi^i - 1}$$

and

$$\varphi^i \frac{\varphi^{3\ell-i} - 1}{\varphi^{2i} - 1} = \frac{\varphi^{3\ell} - \varphi^i}{(\varphi^i - 1)(\varphi^i + 1)} = \frac{-1 - \varphi^i}{(\varphi^i - 1)(\varphi^i + 1)} = \frac{-1}{\varphi^i - 1}.$$

This yields $c_{2i,3\ell-i} = \varphi^{\ell-i} c_{i,\ell}$ for all $1 \leqslant i \leqslant k/4$. To put it short, we have that $(i, \ell \mid 2i, 3\ell - i)$ forms an overlap for every $i \in \{1, \dots, \lfloor k/4 \rfloor\}$.

Notice that the case $i = \ell$ is trivial, but all other cases are not. Thus nontrivial examples of this kind start with $k = 12$.

As we represent overlaps by the exponents with respect to a fixed generator, the actual quadruples will depend on this generator. We give examples for this in Examples 3.13 and 3.14.

The main concern of this paper is the determination of $\mathcal{O}(\mathbb{C}, k)$ and thus by Theorem 3.3 that of $\mathcal{O}(F, k)$ for all finite fields with characteristic not in $\mathcal{Q}_k$. We will now show that the set does not really depend on the generator in this case. In other words: a problem occurs only for exceptional primes.

Lemma 3.9. *Let $k \geqslant 3$ and let F be a field of characteristic $p \notin \mathcal{Q}_k$ such that F^* contains a subgroup Φ of order k, or $F = \mathbb{C}$. Then the set $\mathcal{O}(F, k)$ is independent of the choice of the generator for Φ. Specifically, let ψ and χ be generators of Φ, and let $(i, j \mid s, t) \in \mathcal{O}(F, k)$, i.e. there exists $w \in \boldsymbol{k}_0$ such that*

$$\psi^w \cdot \frac{\psi^j - 1}{\psi^i - 1} = \frac{\psi^s - 1}{\psi^t - 1} \iff \chi^w \cdot \frac{\chi^j - 1}{\chi^i - 1} = \frac{\chi^s - 1}{\chi^t - 1}.$$

Proof. We first treat the complex case. We can restrict to the kth cyclotomic field $F = \mathbb{Q}(\psi)$. There exists an automorphism σ of F such that

$\psi^\sigma = \chi$. The first equation implies $f_{i,j,s,t,\omega}(\psi) = 0$, then also

$$0 = f_{i,j,s,t,\omega}(\psi)^\sigma = f_{i,j,s,t,\omega}\,(\psi^\sigma) = f_{i,j,s,t,\omega}(\chi).$$

Now, the finite case follows directly with Proposition 3.4. □

3.2. The reduced form

To reduce complexity of the set $\mathcal{O}(F,k)$ we use some group actions on $\mathcal{O}(F,k)$. We consider the mappings $\kappa_\ell : \boldsymbol{k}^4 \to \boldsymbol{k}^4$, $\ell \in \{1,2,3,4\}$, which transforms the ℓ-th entry u_ℓ of a quadruple to $k - u_\ell$. These four mappings generate an elementary abelian 2-group $\mathcal{K}_0$ of order 16. The subgroup $\mathcal{K}_1 = \langle \kappa_1\kappa_4, \kappa_2\kappa_4, \kappa_3\kappa_4 \rangle$ generated by products of two such generators has index 2 in $\mathcal{K}_0$.

Let (F,k) be a circular Ferrero pair, then $\mathcal{K}_1$ acts on $\mathcal{O}(F,k)$. If k is even, then $\mathcal{K}_0$ acts on $\mathcal{O}(F,k)$ since $-1 = \varphi^{\frac{k}{2}} \in \Phi$.

If $o := (i,j \mid s,t) \in \mathcal{O}(F,k)$ is an overlap then the following permutations of the entries of o give more identities as in (2.3)

$$(i,t),\ (j,s),\ (i,t)(j,s),\ (i,s)(j,t),\ (i,j)(s,t),\ (i,j,t,s),\ (i,s,t,j). \tag{3.4}$$

These together with the identity map form a dihedral group D_4 acting on $\mathcal{O}(F,k)$, too. It is easy to see that D_4 normalizes $\mathcal{K}_1$ (and also $\mathcal{K}_0$). Thus the semidirect product of D_4 together with $\mathcal{K}_1$, or $\mathcal{K}_0$ form groups $\mathcal{G}_1$, or $\mathcal{G}_0$, respectively.

Lemma 3.10. *Let (F,k) be a circular Ferrero pair. If k is odd, then $\mathcal{G}_1$ acts on $\mathcal{O}(F,k)$, and if k is even, then $\mathcal{G}_0$ acts on $\mathcal{O}(F,k)$.*

Occasionally, we will write $o \sim o'$ if two overlaps $o, o' \in \mathcal{O}(F,k)$ are related by the group action of Lemma 3.10. Clearly, $\sim$ is an equivalence relation on the set of all overlaps. To describe this set it suffices to give a representative for each class. We will now describe a "reduced" representative for each class. Whenever situation allows, we will choose a reduced representative in our exposition.

Let $(i,j \mid s,t) \in \mathcal{O}(F,k)$ be a nontrivial overlap. By applying elements from $\mathcal{K}_1$, we can pass to an equivalent quadruple which has at most one entry greater than $\frac{k}{2}$. If k is even, we can even pass to an equivalent quadruple which has all of its entries less than or equal to $\frac{k}{2}$.

By applying the permutations (i,t) if necessary, we can assume that $i \leqslant t$. Applying (j,s) and/or $(i,j)(s,t)$ we may assume that i is the smallest

of the values among i, j, s, t. Now, applying (j, s), again, if necessary, we can assume with no loss of generality that

$$i < j \leqslant s \quad \text{and} \quad j \leqslant \frac{k}{2}. \tag{3.5}$$

An element $(i, j \mid s, t) \in \mathcal{O}(F, k)$ is called *reduced* if it satisfies the conditions in (3.5) and has at most one entry greater than $\frac{k}{2}$.

Lemma 3.11. *In each equivalence class of $\mathcal{O}(F, k)$ there exists a reduced element.*

Remark 3.12. The reduced form is not unique. E.g., let $k = 12$. From Example 3.8 we have an overlap $o = (1, 2 \mid 2, 5)$, which clearly is reduced. However, $(1, 2 \mid 2, 7) \sim o$ is also reduced; and so is $(1, 2 \mid 10, 5) \sim o$.

We emphasis again that for a prime $p \in \mathcal{Q}_k$, the representation of the overlaps as powers in the set $\mathcal{O}(F, k)$ depends on the choice of the generator for Φ.

Example 3.13. For $p = 13$ and $k = 7$, we have $13 \in \mathcal{Q}_7 \setminus \mathcal{P}_7$. Thus $(13^2, 7)$ is circular, but there exist exceptional overlaps such as $(1, 2 \mid 2, 6) \sim (1, 2 \mid 5, 1)$ both of which are reduced. This overlap works with the element φ of order k in the quadratic extension of $\mathbb{Z}_p$ with minimal polynomial $x^2 + 3x + 1$.[1] Indeed, a simple computation shows that

$$\begin{aligned} \varphi^5 \frac{\varphi^2 - 1}{\varphi - 1} = \frac{\varphi^6 - 1}{\varphi^2 - 1} &\iff (\varphi^2 - 1)^2 \varphi^{-2} = (\varphi^{-1} - 1)(\varphi - 1) \\ &\iff \varphi^2 + \varphi^{-2} - 2 = 2 - (\varphi^{-1} + \varphi). \end{aligned}$$

The last equation holds since the trace of φ is -3 and that of φ^2 is -6.

Another overlap which works with φ is $(1, 2 \mid 5, 1)$. In the same way we have $(1, 3 \mid 3, 6) \sim (1, 3 \mid 4, 1)$ working with φ^2. Notice that, however, $(1, 3 \mid 3, 6)$ does not work with φ.

Example 3.14. For $p = 11$ and $k = 12$ we again have $11 \in \mathcal{Q}_{12} \setminus \mathcal{P}_{12}$. Thus $(11^2, 12)$ is circular. Besides the natural overlaps $(1, 2 \mid 2, 5)$ and

[1] The minimal polynomial of the other generators are $x^2 + 5x + 1$ (for $\varphi^{\pm 3}$) and $x^2 + 6x + 1$ (for $\varphi^{\pm 2}$).

$(2,3 \mid 3,6)$ from Theorem 5.1 there exist exceptional overlaps such as $(2,4 \mid 5,3)$ which works with φ, a root of x^2+5x+1 (and $\omega = 4$). On the other hand, $(1,2 \mid 3,4)$ works with φ^5, which has minimal polynomial x^2-5x+1.

4. The normalized form

We will specialize to the realm of the complex numbers and consider only nontrivial overlaps. It turns out, as we shall see later, that there can be only trivial overlaps when k is odd. *From now on, we shall assume that k is even.* We come back to the odd case only in Theorem 5.2. By abuse of notation, we will write $\mathcal{O} = \mathcal{O}(\mathbb{C}, k)$.

As the group $\mathcal{G}_0$ acts on $\mathcal{O}$ for even k, we can assume that $i,j,s,t \in \{1,2,\dots,\frac{k}{2}\}$. Recall that $\phi = \exp(2\pi \boldsymbol{i}/k)$ is a primitive k-th root of unity in $\mathbb{C}$. We will use the polar decomposition of $\phi^r - 1$, $r \in \mathbb{R}$. This is easily computed using the identity $\phi^r - 1 = \left(\phi^{\frac{r}{2}} - \phi^{-\frac{r}{2}}\right)\phi^{\frac{r}{2}}$ and Euler's formula.

Lemma 4.1. *For $r \in \mathbb{R}$, it holds that*

$$\phi^r - 1 = 2\sin\frac{\pi r}{k} \cdot \exp \boldsymbol{i}\left(\frac{\pi}{2} + \frac{\pi r}{k}\right).$$

The following observations further reduces the overlap quadruples of interest.

Lemma 4.2. *Let $(i,j \mid s,t) \in \mathcal{O}$ with $i,j,s,t \in \{1,2,\dots,\frac{k}{2}\}$. Then*

$$i < j \iff s < t \text{ and } i < s \iff j < t.$$

Proof. By Lemma 4.1 and the monotonicity of sine on the interval $[0, \frac{\pi}{2}]$, we have

$$\left|\frac{\phi^j - 1}{\phi^i - 1}\right| = \frac{\sin\frac{\pi j}{k}}{\sin\frac{\pi i}{k}} > 1 \iff i < j.$$

As the same holds for (s,t), the first statement of the lemma follows. By exchanging the roles of j and s, the second statement follows immediately. □

Therefore (3.5) implies $s < t$ for a reduced quadruple $(i,j \mid s,t)$, $i,j,s,t \in \{1,2,\dots,\frac{k}{2}\}$. Summarizing we can assume

$$0 < i < j \leqslant s < t \leqslant \frac{k}{2}. \tag{4.1}$$

An element $(i, j \mid s, t) \in \mathcal{O}$ is called *normalized* if it satisfies the conditions in (4.1).

With these premises we find

Lemma 4.3. *If $(i, j \mid s, t) \in \mathcal{O}$ is normalized, then $j - i < t - s$, and so $j + s < i + t < k$.*

Proof. It suffices to compare the absolute values of the left and right hand side of (2.3). This gives, by Lemma 4.1,

$$\frac{\sin\frac{\pi j}{k}}{\sin\frac{\pi i}{k}} = \frac{\sin\frac{\pi t}{k}}{\sin\frac{\pi s}{k}}.$$

Set $f(x, y) = \frac{\sin(x+y)}{\sin x}$ on the set $\{(x, y) \mid 0 < x < x + y \leqslant \frac{\pi}{2}\}$. Simple calculus analysis reveals that, keeping y fixed, $f(x, y)$ strictly decreases as x increases, and, keeping x fixed, it strictly increases as y increases.

Now, from

$$\begin{aligned} f\left(\frac{\pi}{k}s, \frac{\pi}{k}(j-i)\right) &< f\left(\frac{\pi}{k}i, \frac{\pi}{k}(j-i)\right) \\ &= \frac{\sin\frac{\pi j}{k}}{\sin\frac{\pi i}{k}} = \frac{\sin\frac{\pi t}{k}}{\sin\frac{\pi s}{k}} = f\left(\frac{\pi}{k}s, \frac{\pi}{k}(t-s)\right) \end{aligned}$$

we infer that $j - i < t - s$. □

Remark 4.4. A reduced quadruple is not necessarily normalized, but the converse is true. Over finite fields there do exist reduced quadruples which cannot be normalized as Example 3.14 shows. This phenomenon can only occurs if the characteristic of the field is an exceptional prime.

4.1. Beyond the normalized form

Not all permutations in D_4 viewed as a subgroup of $\mathcal{G}_0$ give distinct elements from $\mathcal{O}$. Indeed

Lemma 4.5. *If $o := (i, j \mid s, t) \in \mathcal{O}$ is normalized then there are at most four values modulo Φ derived from this by permutations, namely,*

$$\frac{\phi^j - 1}{\phi^i - 1},\ \frac{\phi^s - 1}{\phi^i - 1},\ \frac{\phi^i - 1}{\phi^j - 1} \text{ and } \frac{\phi^i - 1}{\phi^s - 1}.$$

The action of $\mathcal{K}_0$ does not change the cosets.

Proof. Starting from the first value in the theorem, the first permutation from (3.4) produces the last entry, the second and third produce the second and third entry, respectively.

The permutation $(i, s)(j, t)$ only interchanges the left hand side with the right hand side of (2.3) up to an factor in Φ. Therefore the other three permutations in (3.4) cannot give more solutions either. □

5. The main theorem

Finally, in this section we reach our principal goal, the determination of the set $\mathcal{O} = \mathcal{O}(\mathbb{C}, k)$ of nontrivial overlaps over $\mathbb{C}$. For any finite field F with characteristic not in $\mathcal{Q}_k$ this set coincides with $\mathcal{O}(F, k)$, cf. Theorem 3.3.

Later in Theorem 7.4 we also determine the triple overlaps and prove that there are no quadruple overlaps. For the sake of easy reference, we include the findings of the triple overlaps in Theorem 7.4 into the following theorem (the last column, marked with T_r).

Theorem 5.1. *Let k be even and $\mathcal{O}$ nonempty, then there exists $\ell \in \mathbb{N}$ such that $k = 6\ell$. Depending on the shape of k, $\mathcal{O}$ is a union of the corresponding sets $\mathcal{O}_1$, $\mathcal{O}_{30}$, $\mathcal{O}_{42}$, and $\mathcal{O}_{60}$ described below. When we write $k = N\ell_r$ for $N \in \{30, 42, 60\}$, we mean that k is divisible by N.*

1) *For $k = 6\ell$, we have*

$$\phi^{\ell-u} \cdot \frac{\phi^\ell - 1}{\phi^u - 1} = \frac{\phi^{3\ell-u} - 1}{\phi^{2u} - 1}$$

for $1 \leqslant u \leqslant \left\lfloor \frac{k}{4} \right\rfloor$ with $u \neq \frac{k}{6} = \ell$. Namely, $\mathcal{O}_1$ consists of those $(i, j, s, t) \sim (u, \ell \mid 2u, 3\ell - u)$, where $1 \leqslant u \leqslant \left\lfloor \frac{k}{4} \right\rfloor$ and $u \neq \frac{k}{6} = \ell$.

2) *For $k = 30\ell_1$, the normalized forms of the elements in $\mathcal{O}_{30}$ are*

$(\ell_1, 3\ell_1 \mid 3\ell_1, 11\ell_1)$ *with* $\omega = 3\ell_1$,
$(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1)$ *with* $\omega = \ell_1$, $\quad T_1 : (3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1 \mid 6\ell_1, 12\ell_1)$,
$(7\ell_1, 9\ell_1 \mid 9\ell_1, 13\ell_1)$ *with* $\omega = \ell_1$,

$(\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1)$ *with* $\omega = 2\ell_1$, $\quad T_2 : (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1)$,
$(2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1)$ *with* $\omega = \ell_1$, $\quad T_3 : (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1 \mid 7\ell_1, 14\ell_1)$,
$T_4 : (2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1)$,
$(8\ell_1, 9\ell_1 \mid 11\ell_1, 14\ell_1)$ *with* $\omega = \ell_1$, $\quad T_5 : (4\ell_1, 5\ell_1 \mid 8\ell_1, 11\ell_1 \mid 9\ell_1, 14\ell_1)$,
$(2\ell_1, 3\ell_1 \mid 7\ell_1, 14\ell_1)$ *with* $\omega = 3\ell_1$, $\quad T_3 : (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1 \mid 7\ell_1, 14\ell_1)$,
$(3\ell_1, 4\ell_1 \mid 8\ell_1, 13\ell_1)$ *with* $\omega = 2\ell_1$, $\quad T_4 : (2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1)$,
$(4\ell_1, 5\ell_1 \mid 9\ell_1, 14\ell_1)$ *with* $\omega = 2\ell_1$, $\quad T_2 : (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1)$,
$T_5 : (4\ell_1, 5\ell_1 \mid 8\ell_1, 11\ell_1 \mid 9\ell_1, 14\ell_1)$.

3) *For $k = 42\ell_2$, the normalized forms of the elements in $\mathcal{O}_{42}$ are*

$$(2\ell_2, 3\ell_2 \mid 9\ell_2, 16\ell_2) \quad \text{with } \omega = 3\ell_2,$$
$$(3\ell_2, 4\ell_2 \mid 10\ell_2, 15\ell_2) \quad \text{with } \omega = 2\ell_2,$$
$$(8\ell_2, 9\ell_2 \mid 15\ell_2, 20\ell_2) \quad \text{with } \omega = 2\ell_2.$$

4) *For $k = 60\ell_3$, the normalized forms of the elements in $\mathcal{O}_{60}$ are*

$$(3\ell_3, 4\ell_3 \mid 16\ell_3, 27\ell_3) \quad \text{with } \omega = 5\ell_3,$$
$$(5\ell_3, 6\ell_3 \mid 18\ell_3, 25\ell_3) \quad \text{with } \omega = 3\ell_3,$$
$$(8\ell_3, 9\ell_3 \mid 21\ell_3, 28\ell_3) \quad \text{with } \omega = 3\ell_3.$$

Notice that inside every expression in the above list at least one of the exponents i, j, s, and t is odd when ℓ, ℓ_1, ℓ_2, or ℓ_3, respectively, are odd. We have

Theorem 5.2. *If k is odd, only the trivial overlaps occurs.*

Proof. Assume on the contrary that $(i, j \mid s, t) \in \mathcal{O}(\mathbb{C}, k)$ is reduced with k odd. Then $o := (2i, 2j \mid 2s, 2t) \in \mathcal{O}(\mathbb{C}, 2k)$, where we refer to a $2k$-th root of unity ψ with $\psi^2 = \phi$. Normalizing o would require at most one

transformation of the form $\kappa_i : x \mapsto 2k - x$, which results in an even entry. The same holds for permutations when applying to o. Thus, the normalized form of o has four even entries.

By Theorem 5.1 we have $2k = 6\ell$. Since k is odd, ℓ is also odd. As we have noted, in this case, the list in Theorem 5.1 shows no instance having four even entries. Thus there cannot be such $(i, j \mid s, t)$ in $\mathcal{O}(\mathbb{C}, k)$. □

6. The proof

The working of the case (1) in the Theorem 5.1 has already been verified in Example 3.8. It is also in [5]. All others can be verified by similar methods based on the corresponding cyclotomic polynomials. The main part of this section is to prove that there are no more. We give some

6.1. Preparations

It will turn out to be convenient to make the following substitution

$$a := \frac{s+j}{2},\ b := \frac{s-j}{2},\ c := \frac{t+i}{2},\ d := \frac{t-i}{2},$$

therefore

$$i = c - d,\ j = a - b,\ s = a + b,\ t = c + d. \tag{6.1}$$

We collect some easy consequences.

Lemma 6.1. *Our assumptions on i, j, s, t give*

1) $0 \leqslant b < a < c$, $0 \leqslant b < d < c$, and $0 \leqslant b < d < \frac{k}{4}$;
2) $\frac{2\pi}{k}b < \frac{2\pi}{k}d \leqslant \pi - \frac{2\pi}{k}c < \pi - \frac{2\pi}{k}a$;
3) $\pi - \frac{2\pi}{k}a + \frac{2\pi}{k}b < \pi - \frac{2\pi}{k}c + \frac{2\pi}{k}d$.

Proof. (1) follows easily from $0 < i < j \leqslant s < t \leqslant \frac{k}{2}$ and $j + s < i + t$. See Lemma 4.3.

(2) Only $\frac{2\pi}{k}d \leqslant \pi - \frac{2\pi}{k}c$ needs explanation. We have

$$(\pi - \frac{2\pi}{k}c) - \frac{2\pi}{k}d = \pi - \frac{2\pi}{k}(c+d) = \pi - \frac{2\pi}{k}t \geqslant 0.$$

(3) $\pi - \frac{2\pi}{k}a + \frac{2\pi}{k}b = \pi - \frac{2\pi}{k}j < \pi - \frac{2\pi}{k}i = \pi - \frac{2\pi}{k}c + \frac{2\pi}{k}d.$ □

By Lemma 4.1 the principle argument of $(\phi^s-1)^{-1}(\phi^t-1)$ is $(t-s)\pi/k$ while that of $(\phi^i-1)^{-1}(\phi^j-1)$ is $(j-i)\pi/k$. Thus, $\phi^\omega = \exp\big(((t-s)-(j-i))\pi\boldsymbol{i}/k\big)$ and so

$$\omega = \frac{(t+i)-(s+j)}{2} = c-a. \tag{6.2}$$

Remark 6.2. It turns out that ω is an integer. If $p \notin \mathcal{Q}_k$ and $F = \mathrm{GF}(q)$, where q is a power of p with $k \mid (q-1)$, we have $\mathcal{O}(F,k) = \mathcal{O}(\mathbb{C},k)$. Moreover, if $\varphi \in F$ is a primitive k-th root of unity, and $(i,j \mid s,t) \in \mathcal{O}(F,k)$, then $\omega = \frac{(t+i)-(s+j)}{2}$ satisfies $\varphi^\omega \frac{1-\varphi^j}{1-\varphi^i} = \frac{1-\varphi^t}{1-\varphi^s}$. Thus we know exactly how to compute ω from i,j,s,t. This is not the case when $p \in \mathcal{Q}_k$. Examples 3.13 and 3.14 show such situations.

Now, we expand (2.3) to obtain (see also (3.1))

$$1+\phi^{t+i}-\phi^t-\phi^i = \phi^\omega+\phi^{\omega+j+s}-\phi^{\omega+s}-\phi^{\omega+j}. \tag{6.3}$$

Using a,b,c,d and rearranging, we have

$$1+\phi^{2c}+\phi^{c+b}+\phi^{c-b} = \phi^{c+d}+\phi^{c-d}+\phi^{c-a}+\phi^{c+a}. \tag{6.4}$$

Multiply ϕ^{-c} to (6.4) and rearrange again to get

$$\phi^{-a}+\phi^a+\phi^{-d}+\phi^d = \phi^{-b}+\phi^b+\phi^{-c}+\phi^c.$$

As ϕ^{-x} is the complex conjugate of ϕ^x for all x, after dividing the last equation by 2, we obtain

$$\cos\frac{2\pi}{k}a+\cos\frac{2\pi}{k}d = \cos\frac{2\pi}{k}b+\cos\frac{2\pi}{k}c. \tag{6.5}$$

This suggests that we shall be able to apply the following theorem of Conway and Jones.

Theorem 6.3 ([3, Theorem 7])**.** *Suppose we have at most four distinct rational multiples of π lying strictly between 0 and $\frac{\pi}{2}$ for which some rational linear combination of their cosines is rational but no proper subset has this property. Then the appropriate linear combination is proportional*

to one from the following list:

$$\cos\frac{\pi}{3} = \frac{1}{2}, \tag{6.6}$$

$$-\cos\theta + \cos\left(\frac{\pi}{3} - \theta\right) + \cos\left(\frac{\pi}{3} + \theta\right) = 0, \quad \left(0 < \theta < \frac{\pi}{6}\right), \tag{6.7}$$

$$\cos\frac{\pi}{5} - \cos\frac{2\pi}{5} = \frac{1}{2}, \tag{6.8}$$

$$\cos\frac{\pi}{5} - \cos\frac{\pi}{15} + \cos\frac{4\pi}{15} = \frac{1}{2}, \tag{6.9}$$

$$-\cos\frac{2\pi}{5} + \cos\frac{2\pi}{15} - \cos\frac{7\pi}{15} = \frac{1}{2}, \tag{6.10}$$

$$\cos\frac{\pi}{7} - \cos\frac{2\pi}{7} + \cos\frac{3\pi}{7} = \frac{1}{2}. \tag{6.11}$$

All other sums with four cosines equal $\frac{1}{2}$.

Since (6.5) has exactly four terms, we listed only the relevant identities in the above theorem. In order to match (6.5) with the equations in this theorem, we will have to rearrange the equations so that all arguments to the cosine are in the range $[0, \pi/2]$, and all terms nonnegative. For (6.5), there are three cases to consider.

Lemma 6.4. 1) *If* $c \leqslant \frac{k}{4}$, *we just keep terms in* (6.5) *as they are.*

2) *If* $a \geqslant \frac{k}{4}$ *and* $c \geqslant \frac{k}{4}$, *then* (6.5) *must be transformed into*

$$\cos\left(\pi - \frac{2\pi}{k}c\right) + \cos\frac{2\pi}{k}d = \cos\frac{2\pi}{k}b + \cos\left(\pi - \frac{2\pi}{k}a\right). \tag{6.12}$$

3) *If* $a < \frac{k}{4} \leqslant c$, *then* (6.5) *must be transformed into*

$$\cos\frac{2\pi}{k}a + \cos\frac{2\pi}{k}d + \cos\left(\pi - \frac{2\pi}{k}c\right) = \cos\frac{2\pi}{k}b. \tag{6.13}$$

Proof. By Lemma 6.1 (1), if $c \leqslant \frac{k}{4}$, then all terms in (6.5) are nonnegative; and, if $c > \frac{k}{4}$, then according to $a < \frac{k}{4}$ and $a \geqslant \frac{k}{4}$, the other two instances follow. □

With Lemma 6.4, we understand that we have to investigate an expression of the form

$$e_1\cos\alpha_1 + e_2\cos\alpha_2 + e_3\cos\alpha_3 + e_4\cos\alpha_4 = 0, \tag{6.14}$$

where $e_i \in \{1, -1\}$ and α_i are rational multiples of π in the range $[0, \pi/2]$. By Theorem 6.3, equation (6.14) must have subsums matching with equations (6.6)–(6.11). Notice that besides these possibilities there are always the trivial equations

$$\cos 0 = 1 \quad \text{and} \quad \cos \frac{\pi}{2} = 0,$$

which can be used to fill up to four terms. By Lemma 6.1(1), b is the single smallest value, thus $\cos 0$ can occure at most once in a sum.

We now go through the cases that can occur according to Theorem 6.3.

6.2. Cases (6.6) and (6.7)

We combine the first two equations of Theorem 6.3 to obtain

$$\cos\left(\frac{\pi}{3} - \theta\right) + \cos\left(\frac{\pi}{3} + \theta\right) = \cos\theta + \cos\frac{\pi}{2}, \text{ where } 0 \leqslant \theta < \tfrac{\pi}{6}, \quad (6.15)$$

or

$$\cos\frac{\pi}{2} + \cos\left(\frac{\pi}{3} - \theta\right) + \cos\left(\frac{\pi}{3} + \theta\right) = \cos\theta, \text{ where } 0 \leqslant \theta < \tfrac{\pi}{6}. \quad (6.16)$$

Notice that (6.6) corresponds to the case $\theta = 0$. Furthermore, we have put in trivial terms to fill up to four. We also have

$$\theta \leqslant \frac{\pi}{3} - \theta \leqslant \frac{\pi}{3} + \theta < \frac{\pi}{2}.$$

By Lemma 6.1(b), $\frac{2\pi}{k}b$ is the smallest value in all three cases of Lemma 6.4. Thus, $\theta = \frac{2\pi}{k}b$, or $b = \frac{k\theta}{2\pi}$. For convenience, we define $\ell = \frac{k}{6}$. This gives us $0 \leqslant b < \frac{k}{12} = \frac{\ell}{2}$. It will turn out that ℓ is actually an integer.

Suppose that $c \leqslant \frac{k}{4}$. By Lemmas 6.1 (1), c is the largest value. Therefore, 6.4 implies $\frac{2\pi}{k}c = \frac{\pi}{2}$, and so $c = \frac{k}{4}$. Hence we can assume that $c \geqslant \frac{k}{4}$. Now there are the following three possibilities:

$$b < a \leqslant d < \frac{k}{4} \leqslant c, \; b < d < a < \frac{k}{4} \leqslant c \;\text{ or }\; b < d < \frac{k}{4} \leqslant a < c.$$

(1) $b < a \leqslant d < \frac{k}{4} \leqslant c$. In this case, (6.13) applies, and we have

$$\cos\frac{2\pi}{k}a + \cos\frac{2\pi}{k}d + \cos\frac{2\pi}{k}\left(\frac{k}{2} - c\right) = \cos\frac{2\pi}{k}b.$$

Matching up the arguments of this with those in (6.16), we have

$$\frac{2\pi}{k}\left(\frac{k}{2} - c\right) = \frac{\pi}{2}, \quad \frac{2\pi}{k}d = \frac{\pi}{3} + \theta \text{ and } \frac{2\pi}{k}a = \frac{\pi}{3} - \theta.$$

Therefore, remembering that $\theta = \frac{2\pi}{k}b$, one gets

$$c = \frac{k}{4} = \frac{3}{2}\ell,\ d = \frac{k}{6} + b = \ell + b \text{ and } a = \frac{k}{6} - b = \ell - b.$$

By (6.1), we get

$$i = c - d = \frac{1}{2}\ell - b,\ j = a - b = \ell - 2b$$

and

$$s = a + b = \ell,\ t = c + d = \frac{5}{2}\ell + b.$$

Put $b' = \frac{1}{2}\ell - b$ to get

$$(i, j \mid s, t) = (b', 2b' \mid \ell, 3\ell - b') \in \mathcal{O},\ 0 < b' \leqslant \frac{1}{2}\ell.$$

Now $\omega = c - a = \frac{3\ell - b' + b' - (\ell + 2b')}{2} = \ell - b'$, and so

$$\phi^{\ell - b'} \cdot \frac{\phi^{2b'} - 1}{\phi^{b'} - 1} = \frac{\phi^{3\ell - b'} - 1}{\phi^{\ell} - 1}. \tag{6.17}$$

(2) $b < d < a < \frac{k}{4} \leqslant c$. Again, (6.13) is used to match up with (6.16), and

$$\frac{2\pi}{k}\left(\frac{k}{2} - c\right) = \frac{\pi}{2},\ \frac{2\pi}{k}a = \frac{\pi}{3} + \theta \text{ and } \frac{2\pi}{k}d = \frac{\pi}{3} - \theta.$$

Therefore,

$$c = \frac{k}{4} = \frac{3}{2}\ell,\ a = \frac{k}{6} + b = \ell + b \text{ and } d = \frac{k}{6} - b = \ell - b.$$

By (6.1), we get

$$i = c-d = \frac{1}{2}\ell+b,\ j = a-b = \ell,\ s = a+b = \ell+2b \ \text{ and } \ t = c+d = \frac{5}{2}\ell-b.$$

Put $b'' = \frac{1}{2}\ell + b$ to get

$$(i, j \mid s, t) = (b'', \ell \mid 2b'', 3\ell - b'') \in \mathcal{O},\ \frac{1}{2}\ell \leqslant b'' < \ell.$$

Notice that $b' = \frac{\ell}{2}$ in the previous case and $b'' = \frac{\ell}{2}$ here give the same $(i, j \mid s, t)$.

Now $\omega = c - a = \frac{3\ell-b''+b''-(\ell+2b'')}{2} = \ell - b''$ and

$$\phi^{\ell-b''} \cdot \frac{\phi^{\ell} - 1}{\phi^{b''} - 1} = \frac{\phi^{3\ell-b''} - 1}{\phi^{2b''} - 1}. \tag{6.18}$$

(3) $b < d < \frac{k}{4} \leqslant a < c$. In this case, (6.12) applies, and we have

$$\cos\frac{2\pi}{k}d + \cos\frac{2\pi}{k}\left(\frac{k}{2} - c\right) = \cos\frac{2\pi}{k}b + \cos\frac{2\pi}{k}\left(\frac{k}{2} - a\right).$$

Matching up the arguments of this with those in (6.15), we have

$$\frac{2\pi}{k}d = \frac{\pi}{3} - \theta,\ \frac{2\pi}{k}\left(\frac{k}{2} - c\right) = \frac{\pi}{3} + \theta \ \text{ and } \ \frac{2\pi}{k}\left(\frac{k}{2} - a\right) = \frac{\pi}{2}.$$

Therefore,

$$d = \frac{k}{6} - \frac{k\theta}{2\pi} = \ell - b,\ c = \frac{k}{3} - \frac{k\theta}{2\pi} = 2\ell - b \ \text{ and } \ a = \frac{k}{4} = \frac{3}{2}\ell.$$

By (6.1), we get

$$i = c - d = \ell,\ j = a - b = \frac{3}{2}\ell - b,$$

and

$$s = a + b = \frac{3}{2}\ell + b,\ t = c + d = 3\ell - 2b.$$

Put $b''' = \frac{3}{2}\ell - b$ to obtain

$$(i, j \mid s, t) = (\ell, b''' \mid 3\ell - b''', 2b''') \in \mathcal{O},\ \ell < b''' \leqslant \frac{3}{2}\ell.$$

As $\omega = c - a = \frac{2b'''+\ell-(b'''+3\ell-b''')}{2} = b''' - \ell$, we find

$$\phi^{b'''-\ell} \cdot \frac{\phi^{b'''} - 1}{\phi^{\ell} - 1} = \frac{\phi^{2b'''} - 1}{\phi^{3\ell-b'''} - 1},$$

or equivalently,

$$\phi^{\ell-b'''} \cdot \frac{\phi^{\ell} - 1}{\phi^{b'''} - 1} = \frac{\phi^{3\ell-b'''} - 1}{\phi^{2b'''} - 1}. \tag{6.19}$$

Note that b', b'', b''' must be integers, as they are equal to one of i or j. Likewise, ℓ is an integer. Note also that the ranges fit. Putting (6.17), (6.18), and (6.19) together, we therefore obtain

$$\phi^{\ell-u} \cdot \frac{\phi^{\ell} - 1}{\phi^{u} - 1} = \frac{\phi^{3\ell-u} - 1}{\phi^{2u} - 1},\ 1 \leqslant u \leqslant \left\lfloor \frac{k}{4} \right\rfloor,\ u \neq \frac{k}{6}.$$

This is $\mathcal{O}_1$.

Remark 6.5. In (1) and (2), when ℓ is even,

$$\left(\frac{1}{2}\ell + b, \ell \;\middle|\; \ell + 2b, \frac{5}{2}\ell - b\right) = \left(\frac{1}{2}\ell - b, \ell - 2b \;\middle|\; \ell, \frac{5}{2}\ell + b\right)$$

if and only if $b = 0$. Obviously, the expression in (3) cannot be equal to one from (1) or (2).

6.3. Case (6.8)

We can use $\cos 0 = 1$ or $\cos \frac{\pi}{2} = 0$, to fill up (6.8) to four terms. By Lemma 6.1 (1), b is the smallest values that appear among the arguments of cos, if $\cos 0$ is used, we have $b = 0$; otherwise, $b \neq 0$.

In the case when $b \neq 0$, (6.8) from Theorem 6.3 reads

$$\cos\frac{\pi}{5} + \cos\frac{\pi}{2} = \cos\frac{2\pi}{5} + \cos\frac{\pi}{3}. \tag{6.20}$$

To simplify notation we let $k = 60\ell_3$.

If $c \leqslant \frac{k}{4} = 15\ell_3$, we can match (6.20) with (6.5). Using Lemma 6.1(1), we obtain

$$b = \frac{k}{10} = 6\ell_3,\ c = \frac{k}{4} = 15\ell_3, \quad \text{and} \quad \{a, d\} = \{10\ell_3, 12\ell_3\}.$$

From this we get

$$(i, j \mid s, t) = (3\ell_3, 4\ell_3 \mid 16\ell_3, 27\ell_3) \text{ or } (5\ell_3, 6\ell_3 \mid 18\ell_3, 25\ell_3).$$

If $c > \frac{k}{4} = 15\ell_3$ we match (6.20) with (6.12). Using Lemma 6.1 (2), we obtain

$$b = 6\ell_3,\ d = 10\ell_3,\ \frac{k}{2} - a = \frac{k}{4} \Longrightarrow a = 15\ell_3 \quad \text{and} \quad c = 18\ell_3,$$

leading to $(i, j \mid s, t) = (8\ell_3, 9\ell_3 \mid 21\ell_3, 28\ell_3)$.

We have all possibilities in $\mathcal{O}_{60}$. Notice that ℓ_3 must be an integer, as the entries inside our three quadruples are relatively prime.

Now we do the case $b = 0$. In this case $\cos 0$ has to be added to (6.8) from Theorem 6.3 to make it an equation with four terms, which then reads

$$\cos\frac{\pi}{5} + \cos\frac{\pi}{3} = \cos\frac{2\pi}{5} + \cos 0. \tag{6.21}$$

To simplify notation we let $k = 30\ell_1$.

If $c \leqslant \frac{k}{4}$, we can match (6.21) with (6.5). Using Lemma 6.1(1), we obtain

$$b = 0\ell_1,\ c = 6\ell_1 \quad \text{and} \quad \{a, d\} = \{3\ell_1, 5\ell_1\}.$$

From this we get $(i, j \mid s, t) = (\ell_1, 3\ell_1 \mid 3\ell_1, 11\ell_1)$ or $(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1)$.

If $c > \frac{k}{4}$ we can match (6.21) with (6.12). Using Lemma 6.1(2) we obtain

$$b = 0\ell_1,\ d = 3\ell_1,\ a = 9\ell_1 \quad \text{and} \quad c = 10\ell_1,$$

leading to $(i, j \mid s, t) = (7\ell_1, 9\ell_1 \mid 9\ell_1, 13\ell_1)$.

We have obtained the first three possibilities in $\mathcal{O}_{30}$.

6.4. Case (6.9)

Slightly rewriting the equation (6.9) from Theorem 6.3 reads

$$\cos\frac{\pi}{5} + \cos\frac{4\pi}{15} = \cos\frac{\pi}{15} + \cos\frac{\pi}{3}. \tag{6.22}$$

To simplify notation again we let $k = 30\ell_1$.

If $c \leqslant \frac{k}{4}$, we can match (6.22) with (6.5). Using Lemma 6.1(1) we obtain

$$b = \ell_1,\ c = 5\ell_1 \ \text{ and } \ \{a, d\} = \{3\ell_1, 4\ell_1\}.$$

From this we get $(i, j \mid s, t) = (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1)$ or $(2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1)$.

If $c > \frac{k}{4}$ we can match (6.22) with (6.12). Using Lemma 6.1(2) we obtain

$$b = \ell_1,\ d = 3\ell_1,\ a = 10\ell_1 \ \text{ and } \ c = 11\ell_1,$$

leading to $(i, j \mid s, t) = (8\ell_1, 9\ell_1 \mid 11\ell_1, 14\ell_1)$.

These make the second block of three in $\mathcal{O}_{30}$.

6.5. Case (6.10)

Slightly rewriting the equation (6.10) from Theorem 6.3 reads

$$\cos\frac{2\pi}{15} = \cos\frac{5\pi}{15} + \cos\frac{6\pi}{15} + \cos\frac{7\pi}{15}. \tag{6.23}$$

For simple notation we stay with $k = 30\ell_1$.

Now, the equation (6.23) can only match with (6.13), thus $c \geqslant \frac{k}{4}$ and $a < \frac{k}{4}$.

First matching $\frac{2\pi b}{k}$ with $\frac{2\pi}{15}$, we get $b = 2\ell_1$. From Lemma 6.1 (2), we have $d \leqslant \frac{k}{2} - c$. Thus, there are three possibilities.

- If $d \leqslant \frac{k}{2} - c < a$, then $a = 7\ell_1$, $15\ell_1 - c = 6\ell_1$ and $d = 5\ell_1$. In this case, the element in $\mathcal{O}_{30}$ (the third block) is $(4\ell_1, 5\ell_1 \mid 9\ell_1, 14\ell_1)$.
- If $d < a < \frac{k}{2} - c$, then $15\ell_1 - c = 7\ell_1$, $a = 6\ell_1$ and $d = 5\ell_1$. In this case, the element in $\mathcal{O}_{30}$ (the third block) is $(3\ell_1, 4\ell_1 \mid 8\ell_1, 13\ell_1)$.
- If $a < d \leqslant \frac{k}{2} - c$, then $15\ell_1 - c = 7\ell_1$, $d = 6\ell_1$ and $a = 5\ell_1$. In this case, the element in $\mathcal{O}_{30}$ (the third block) is $(2\ell_1, 3\ell_1 \mid 7\ell_1, 14\ell_1)$.

As before we emphasize the point that the entries inside all nine quadruples involving ℓ_1 are relatively prime. Thus ℓ_1 turns out to be an integer.

6.6. Case (6.11)

Slightly rewriting the equation (6.11) in Theorem 6.3 we get

$$\cos\frac{\pi}{7} + \cos\frac{3\pi}{7} = \cos\frac{2\pi}{7} + \cos\frac{\pi}{3}. \tag{6.24}$$

To simplify notation here, we let $k = 42\ell_2$.

If $c \leqslant \frac{k}{4}$, we can match the terms of (6.24) with (6.5) and obtain

$$b = 3\ell_2,\ c = 9\ell_2,\ \{a, d\} = \{6\ell_2, 7\ell_2\}.$$

From this we get

$$(i, j \mid s, t) = (2\ell_2, 3\ell_2 \mid 9\ell_2, 16\ell_2) \text{ or } (3\ell_2, 4\ell_2 \mid 10\ell_2, 15\ell_2).$$

If $c > \frac{k}{4}$, we can use Lemma 6.1(2) again to match (6.24) with (6.12) and get

$$b = 3\ell_2,\ d = \frac{1}{7}k = 6\ell_2,\ c = 14\ell_2 \ \text{ and } \ a = 12\ell_2.$$

Therefore we obtain one more solution $(i, j \mid s, t) = (8\ell_2, 9\ell_2 \mid 15\ell_2, 20\ell_2)$ to form $\mathcal{O}_{42}$.

Again, ℓ_3 must be an integer.

We have now exhibited all possible nontrivial overlaps. There are no more than those listed in the theorem as we have claimed.

7. Triple overlaps

We say that a nontrivial *triple overlap* occurs if for some $s_i, t_i \in \boldsymbol{k}$, $i = 1, 2, 3$, $(s_1, t_1 \mid s_2, t_2)$, $(s_2, t_2 \mid s_3, t_3)$, and $(s_1, t_1 \mid s_3, t_3)$ are in $\mathcal{O}$. In this case, we write $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$ and call it a *nontrivial* triple overlap.

We collect all nontrivial triple overlaps in the set $\mathcal{T}$, i.e.,

$$\begin{aligned}&(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T}\\ &\qquad \Longleftrightarrow (s_1, t_1 \mid s_2, t_2), (s_2, t_2 \mid s_3, t_3), (s_1, t_1 \mid s_3, t_3) \in \mathcal{O}.\end{aligned}$$

We are interested in nontrivial overlaps only. So if $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$ is in $\mathcal{T}$, we simply use the phrase "there is a triple overlap $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$," or "$(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$ is a triple overlap", and the like to refer to a nontrivial triple overlap.

Recall that when k is odd, no nontrivial overlaps can occur by Theorem 5.2. We are only dealing with even k. Thus, we may assume that $s_i \leqslant \frac{k}{2}$ and $t_i \leqslant \frac{k}{2}$ for all i.

For a triple overlap $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T}$, we denote

$$o_1 = (s_1, t_1 \mid s_2, t_2), \quad o_2 = (s_2, t_2 \mid s_3, t_3), \quad o_3 = (s_1, t_1 \mid s_3, t_3),$$

and call them the *constituents* of the triple overlap.

The following are easy consequences from the definition.

Lemma 7.1. *It holds that*

$$\begin{aligned}(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T} &\iff (s_2, t_2 \mid s_1, t_1 \mid s_3, t_3) \in \mathcal{T} \\ &\iff (s_3, t_3 \mid s_2, t_2 \mid s_1, t_1) \in \mathcal{T}.\end{aligned}$$

Lemma 7.2. *It holds that*

$$(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T} \iff (t_1, s_1 \mid t_2, s_2 \mid t_3, s_3) \in \mathcal{T}.$$

To obtain all the triple overlaps in $\mathcal{T}$, we can therefore restrict to the case when $s_1 < s_2 < s_3$ and $s_1 < t_1$. More precisely, if there is a triple overlap $(s_1', t_1' \mid s_2', t_2' \mid s_3', t_3')$, then there is also a triple overlap $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$ with $s_1 < s_2 < s_3$ and $s_1 < t_1$, and this one is referred to as *normalized*.

Lemma 7.3. *Let $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T}$ be a normalized triple overlap. Then $s_i < t_i$ and $t_1 < t_2 < t_3$.*

Proof. Lemma 4.2 implies $s_i < t_i$ for all i and $t_1 < t_2 < t_3$. □

Theorem 7.4. *Let $T = (s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T}$ be a normalized triple overlap. Then k is divisible by 30, i.e., $k = 30\ell$, and T is one of the following*

$$\begin{aligned} T_1 &:(3\ell, 5\ell \mid 5\ell, 9\ell \mid 6\ell, 12\ell), & T_4 &:(2\ell, 5\ell \mid 3\ell, 8\ell \mid 4\ell, 13\ell), \\ T_2 &:(\ell, 2\ell \mid 4\ell, 9\ell \mid 5\ell, 14\ell), & T_5 &:(4\ell, 5\ell \mid 8\ell, 11\ell \mid 9\ell, 14\ell). \\ T_3 &:(2\ell, 3\ell \mid 5\ell, 8\ell \mid 7\ell, 14\ell), \end{aligned}$$

Any other triple overlap in $\mathcal{T}$ can be obtained from these by applying the operations from Lemmas 7.1 and 7.2.

By inspection, we derive from this an immediate consequence.

Corollary 7.5. *There do not exist nontrivial "quadruple" overlaps.*

8. Proof of Theorem 7.4

By Lemmas 7.1, 7.2 and 7.3 every triple overlap $(s_1', t_1' \mid s_2', t_2' \mid s_3', t_3')$ in $\mathcal{T}$ can be normalized into a triple overlap $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3)$ with $s_1 < s_2 < s_3$, $t_1 < t_2 < t_3$, and $s_i < t_i$ for $i = 1, 2, 3$. This accounts for the last statement.

Throughout this proof, overlaps and triple overlaps are not necessarily normalized. Thus, when doing inspection below, this fact has to be taken into account. Let $(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T}$. Whenever we are dealing with overlaps from $\mathcal{O}_{30}$, or $\mathcal{O}_{42}$, or $\mathcal{O}_{60}$, we assume that $k = 30\ell_1$, $k = 42\ell_2$, $k = 60\ell_3$, respectively.

The cases are organized by the number of constituents inside $\mathcal{O}_1$.

8.1. Triple overlaps with no constituents in $\mathcal{O}_1$

(1) Assume that there is a constituent, o_1 say, in $\mathcal{O}_{60}$. Then using Theorem 5.1 one easily sees that the others are not in $\mathcal{O}_{60}$.

If another constituent is to be in $\mathcal{O}_{30}$, then $\ell_1 = 2\ell_3$ and o_1 must have one instance of the form $(2m, 2m' \mid ., .)$. However, this is not the case according to Theorem 5.1. Similarly, if another constituent is to be in $\mathcal{O}_{42}$, then ℓ_2 is a multiple of 10 and so two entries of o_1 must be multiples of 10, which is not the case either.

Therefore, no constituents can be in $\mathcal{O}_{60}$.

(2) Assume that there is a constituent, o_1 say, in $\mathcal{O}_{42}$. Then from the list in Theorem 5.1 one easily sees that the others are not in $\mathcal{O}_{42}$. Hence, other constituents o_2 and o_3 have to be in $\mathcal{O}_{30}$. But then ℓ_1 is a multiple of 7 and so two entries of o_2, say, must be multiples of 7, which does not happen.

Therefore, no constituents can be in $\mathcal{O}_{42}$.

(3) We are left with the case that there are two constituents in $\mathcal{O}_{30}$. A tedious inspection (see the Remark 8.1 below) reveals two normalized triple overlaps:

$$(\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1) \quad \text{and} \quad (2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1), \tag{8.1}$$

as well as one not normalized: $(4\ell_1, 5\ell_1 \mid 9\ell_1, 14\ell_1 \mid 8\ell_1, 11\ell_1)$. Here $k = 30\ell_1$.

In each of the three triple overlaps found, there is one constituent (in fact o_3) from $\mathcal{O}_1$. Thus, these triple overlaps do not meet the condition of the present case, and will show up again in the sequel.

Remark 8.1. Here we describe an efficient strategy to find normalized triple overlaps from the list of overlaps.

- Start with a normalized overlap $(s_1, t_1 \mid s_2, t_2)$.
- Look for normalized overlaps $(s_2, v \mid s, t)$ and check
  if $t_2 = v$, then $(s_1, t_1 \mid s_2, t_2 \mid s, t) \in \mathcal{T}$, and
  if $t_2 = s$, then $(s_1, t_1 \mid s_2, t_2 \mid v, t) \in \mathcal{T}$.

Notice that the last of the triple overlaps given above cannot be found this way. Yet, it is spotted during the inspection. A normalized one for it will be found later.

8.2. Triple overlaps with exactly one constituent in $\mathcal{O}_1$

Putting $k = 6\ell$, we can assume that $o_1 = (i, \ell \mid 2i, 3\ell - i)$. This means that o_2 or o_3 must contain ℓ. Furthermore, we have $o_2, o_3 \in \mathcal{O}_{30} \cup \mathcal{O}_{42} \cup \mathcal{O}_{60}$.

In the cases $k = 60\ell_3$ and $k = 42\ell_2$ this implies that $10\ell_3$ or $7\ell_2$, respectively, must occur as an entry of an overlap. Yet there is no such overlap in the list of Theorem 5.1.

In the case $k = 30\ell_1$, the entry $5\ell_1$ must occur in an overlap inside $\mathcal{O}_{30}$. There are three normalized candidates:

$$(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1),\ (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1),\ (4\ell_1, 5\ell_1 \mid 9\ell_1, 14\ell_1). \tag{8.2}$$

If we assume that the first entry is smaller than the second, then three pairs of this form $(i, 5\ell_1)$, $(5\ell_1, i)$, $(5\ell_1, 15\ell_1 - i)$ can be found in the overlaps in $\mathcal{O}_1$. Note that $5\ell_1 < 15\ell_1 - i$, as $i \leqslant 15\ell_1/2$.

From the first quadruple of (8.2), we get $i = 3\ell_1$, or $i = 9\ell_1$ (too large), or $15\ell_1 - i = 9\ell_1$, hence $i = 3\ell_1$ or $6\ell_1$. Both yield

$$(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1 \mid 6\ell_1, 12\ell_1).$$

Since this triple overlap has two constituents inside $\mathcal{O}_1$, it does not fit the condition we are considering, and will show up again in the next case.

From the second quadruple of (8.2), we get $i = 2\ell_1$, or $i = 8\ell_1$ (too large), or $15\ell_1 - i = 8\ell_1$, hence (already normalized)

$i = 2\ell_1$, giving $(2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1)$,

and

$$i = 7\ell_1, \text{ giving } (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1 \mid 7\ell_1, 14\ell_1).$$

Notice that the first one here is the second in (8.1), and both triple overlaps here have one constituent in $\mathcal{O}_1$ and two constituents in $\mathcal{O}_{30}$.

From the third quadruple of (8.2), we have $i = 4\ell_1$, or $i = 14\ell_1$ (too large), or $15\ell_1 - i = 14\ell_1$, hence

$$i = 1\ell_1, \text{ giving } (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1),$$

and

$$i = 4\ell_1, \text{ giving } (4\ell_1, 5\ell_1 \mid 8\ell_1, 11\ell_1 \mid 9\ell_1, 14\ell_1).$$

The first one here is the first one in (8.1) while the second one is the nonnormalized triple overlap we had after (8.1). Both of them have one constituent in $\mathcal{O}_1$ and two constituents in $\mathcal{O}_{30}$.

Note that we have now found all the triple overlaps listed in the theorem, including $(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1 \mid 6\ell_1, 12\ell_1)$ which did not fit the current case condition. The following discussions will only show this one, but not any new ones.

8.3. Triple overlaps with at least two constituents in $\mathcal{O}_1$

Assume $k = 6\ell$ and start out with a triple overlap $o \in \mathcal{T}$ with at least two constituents from $\mathcal{O}_1$ (may not be normalized nor reduced, and the numbering may not be the actual order):

$$o_1 = (i, \ell \mid 2i, 3\ell - i) \quad \text{and} \quad o_2 = (j, \ell \mid 2j, 3\ell - j),$$

where $1 \leqslant i \leqslant \lfloor \frac{k}{4} \rfloor = \lfloor \frac{3\ell}{2} \rfloor < 2\ell$, $1 \leqslant j \leqslant \lfloor \frac{3\ell}{2} \rfloor$, $i \neq \ell$, $j \neq \ell$, and $i \neq j$. Thus, we have $2i \leqslant 3\ell$, $2j \leqslant 3\ell$, and $i + j \leqslant 3\ell$. There is no loss of generality in assuming that $i < j$. Then from $i < j \leqslant \frac{3\ell}{2}$, we infer that $i + j < 3\ell$. Summarizing, we obtain the following four inequalities:

$$i < j, \quad i < 3\ell - i, \quad \ell < 3\ell - i, \quad \text{and} \quad i < 3\ell - j.$$

From these, we see that either i or ℓ is the smallest among all entries involved in the triple overlap.

In both cases, $3\ell - i$ is the largest entry in o_1, and must appear in o_2. That is, $3\ell - i$ must be one of j, ℓ, $2j$ and $3\ell - j$. The first, second and fourth cases lead to contradictions $i + j = 3\ell$, $i = 2\ell$ and $i = j$, respectively. The third case makes $3\ell - i = 2j$. Also, since $i < j$, we have $3\ell = i + 2j < 3j$, and so $\ell < j$. Consequently, $i < \ell$.

Either $(i, \ell \mid 2i, 3\ell - i) = (i, \ell \mid 2i, 2j)$ or $(i, \ell \mid 2i, 3\ell - i) \sim (i, 2i \mid \ell, 2j)$ is the normalized form of o_1. Assume the later is normalized. In order to match it, we have to rearrange $o_2 = (j, \ell \mid 2j, 3\ell - j)$ into the form $(j, 2j \mid \ell, 3\ell - j)$ or $(3\ell - j, 2j \mid \ell, j)$. Then either $\ell = j$ or $\ell = 3\ell - j$, contradicting the fact that $\ell < j \leqslant \lfloor \frac{3\ell}{2} \rfloor$.

Therefore, $o_1 = (i, \ell \mid 2i, 2j)$ is in normalized form. And again, one of the rearrangements $(j, 2j \mid \ell, 3\ell - j)$ or $(3\ell - j, 2j \mid \ell, j)$ of o_2 matches o_1. If $2i = 3\ell - j$, then, together with $3\ell - i = 2j$, we arrive at the contradiction $i = j$. Thus we are left with $2i = j$. This yields $i = \frac{3}{5}\ell$ and $j = \frac{6}{5}\ell$. Putting $k = 30\ell_1$, we obtain the triple overlap $(3\ell_1, 5\ell_1 \mid 6\ell_1, 12\ell_1 \mid 5\ell_1, 9\ell_1)$, which already showed up earlier.

After rearranging into normalized form we obtain $o_1 \in \mathcal{O}_{30}$, $o_2 \in \mathcal{O}_1$ and $o_3 \in \mathcal{O}_1$.

Finally, there are no triple overlaps with all three constituents inside $\mathcal{O}_1$. We are done with the proof.

Acknowledgement

The authors thank the reviewer for his/her careful reading and comments.

References

[1] J. R. Clay. *Circular block designs from planar near-rings.* Combinatorics '86 (Trento, 1986), 95–105, Ann. Discrete Math., **37**, North-Holland, Amsterdam, 1988.

[2] J. R. Clay. Nearrings: Geneses and Applications. Oxford Univ. Press, Oxford, 1992.

[3] J. H. Conway and A. J. Jones. *Trigonometric diophantine equations*, Acta Arith. **30** (1976), 229–240.

[4] K. F. Ireland and M. I. Rosen. *A classical introduction to modern number theory*, 2nd ed., Springer-Verlag, Berlin-Heidelberg-New York, 1990.

[5] W.-F. Ke and H. Kiechle, *Combinatorial properties of ring generated circular planar nearrings*, J. Combin. Theory Ser. A **73** (1996), 286–301.

[6] W.-F. Ke and H. Kiechle, *On the solutions of the equation $x^m + y^m - z^m = 1$ in a finite field,* Proc. Amer. Math. Soc. 128 (1995), 1331–1339.

[7] W.-F. Ke and H. Kiechle, *Circularity in Finite Fields and Solutions of the Equations $x^m + y^m - z^m = 1$.* Submitted; arXiv:2307.05586.

[8] H. Kiechle, *Points on Fermat curves over finite fields,* in "Proc. Conference on Finite Fields: Theory, Applications, and Algorithms, Las Vegas, NV, 1993," Contemp. Math. 168 (1994), 181–183.

[9] M. C. Modisett. *A characterization of the circularity of balanced incomplete block designs.* Utilitas Math. **35** (1989), 83–94.

Contact information

Wen-Fong Ke Department of Mathematics, National Cheng Kung University, Tainan 701, Taiwan
E-Mail(*s*): wfke@mail.ncku.edu.tw

Hubert Kiechle Universität Hamburg, Fachbereich Mathematik, Bundesstr. 55, D-20146 Hamburg, Germany
E-Mail(*s*): hubert.kiechle@uni-hamburg.de

Received by the editors: 17.06.2023
and in final form 22.06.2023.