Non-Cayley-Isomorphic Self-Complementary Circulant Graphs

Valery Liskovets* and **Reinhard Pöschel***
Institut für Algebra
Technische Universität Dresden
D-01062 Dresden, Germany†
poeschel@math.tu-dresden.de

18.12.97; revised June 99

Abstract

Non-CI self-complementary circulant graphs of prime-squared order are constructed and enumerated. It is shown that for prime p, there exists a self-complementary circulant graph of order p^2 not Cayley isomorphic to its complement if and only if $p \equiv 1 \pmod 8$. Such graphs are also enumerated.

Keywords: self-complementary circulant graph; Cayley isomorphism; multiplier; graph enumeration; complementing permutation; Paley graph

Mathematics Subject Classifications (1991): 05C25, 05C30, 05C20.

1 Introduction

1.1. Outline. Self-complementary graphs are combinatorial objects that have been attracting a great attention of numerous researchers. Recently, several results were obtained for self-complementary circulant graphs, see for example [1, 2, 4, 6]. In the present paper we act in the same direction. For prime-squared orders $n = p^2$, by using a natural and simple construction and a known isomorphism theorem we describe a new family of self-complementary circulant

*This research was supported by the Grant No. I-0333-263.06/93 from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

†Current address of the first author: Institute of Mathematics, National Academy of Sciences, 220072, Minsk, Belarus; liskov@im.bas-net.by

graphs, called non-CI, and count their number. Here CI stands for *Cayley isomorphic*: a circulant graph Γ is said to be CI (or *one-multiplier equivalent*) if for any circulant graph Γ' isomorphic to Γ, there is an isomorphism between them which is induced by an automorphism of the underlying cyclic group. Such an automorphism can be identified with the multiplication by a number prime to the order.

We show that exactly in the case when $p-1$ is divisible by 8, there exists a *strongly* non-CI self-complementary circulant graph of order p^2, that is, one in which no isomorphism with its complementary graph is induced by an automorphism of the underlying cyclic group (Theorem 3.5). In the literature (see for example [2]), such an isomorphism is sometimes called Ádám complementarity. We will use the term *self-complementing multiplier*. Finally, all such graphs with p^2 vertices are counted exactly (Theorem 4.4 and formula (15)).

These considerations can be easily extended to arbitrary (admissible) orders by using *composition* (called also wreath product) of circulant graphs. In this case, however, the results are not exhaustive.

It is worth stressing that only a very small fraction of self-complementary circulant graphs (and circulant graphs in general) are non-CI. For example, calculations by formulas obtained in [6] show that there exist 56,385,212,104 non-isomorphic self-complementary circulant graphs of order $13^2 = 169$, and only 4 of them are non-CI. The corresponding numbers of all circulant graphs of order 169 and valency 84 are 21,524,493,412,979,864,466,188 and 16, respectively.

Our approach can be easily applied to self-complementary circulant digraphs. In particular, it turns out that strongly non-CI self-complementary circulant digraphs of order p^2 exist if and only if 4 divides $p-1$, and strongly non-CI circulant tournaments do not exist (see the extended preliminary version of the present work [11]).

After the present paper had been submitted for publication we learned about the paper [5] by Jajcay and Li containing the same result on the existence of strongly non-CI self-complementary circulant graph of order p^2 (announced also in the survey [9]). The authors call them not SC-CI-graphs and use the same main construction.

1.2. Connection sets and multipliers. For undefined notions we refer to [6]. Given a positive integer n, we denote $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ and $\mathbb{Z}'_n := \mathbb{Z}_n \setminus \{0\}$. $\mathbb{Z}^*_n$ stands for the set of numbers in $\mathbb{Z}_n$ relatively prime to n. It is an abelian group with respect to multiplication. In the sequel, all arithmetic operations are regarded *modulo* n unless otherwise stated.

A *graph* (*digraph*) will mean a finite *undirected* (resp., *directed*) graph without loops and multiple (directed) edges. Graphs may be considered as symmetric digraphs, i.e. consisting of pairs of oppositely directed arcs. A (di)graph is called *self-complementary* if it is isomorphic to its complement in the complete (di)graph.

An n-(di)graph means a graph of order n, i.e. a (di)graph with n vertices. By default, the set of vertices is assumed to be $\mathbb{Z}_n$.

A *circulant (di)graph* of order n, or simply a *circulant* (or an n-circulant) is a (di)graph Γ on $\mathbb{Z}_n$ for which the cyclic permutation $(0, 1, 2, \ldots, n-1)$ is an automorphism.

The *connection set* $X = X(\Gamma) \subseteq \mathbb{Z}_n'$ of a circulant (di)graph Γ is defined to be the set of all vertices adjacent to the vertex 0. The set X completely specifies Γ: two vertices $a, b \in \mathbb{Z}_n$ are adjacent if and only if $a - b \in X$. Correspondingly, we write $\Gamma = \Gamma(\mathbb{Z}_n, X)$, or simply $\Gamma = \Gamma(X)$. The circulant graph $\Gamma(X)$ is undirected if and only if X is *symmetric*, that is, $X = -X$ where $-X := \{-a \mid a \in X\}$.

The following simple statement plays a key role in the theory of circulants: *If the connection sets X and X' are* one-multiplier equivalent*, i.e. if*

$$X' = mX \qquad (*)$$

for some integer m prime to n, then the n-circulant (di)graphs $\Gamma(X)$ and $\Gamma(X')$ are isomorphic.

Condition (*) describes the induced element-wise action of the multiplicative group $\mathbb{Z}_n^*$ on connection sets. With respect to this action, the elements of $\mathbb{Z}_n^*$ are called *multipliers*. The connection sets X and X' satisfying condition (*), as well as their corresponding circulants, are called *Cayley isomorphic*, or CI.

If X presents a self-complementary circulant (di)graph and X' its complement, then

$$X \cup X' = \mathbb{Z}_n' \quad \text{and} \quad X \cap X' = \emptyset.$$

If the condition (*) holds for them, then m is called a *self-complementing multiplier* for X (and for $\Gamma(X)$).

(*) is often referred to as *Ádám's condition* in view of the famous opposite assertion conjectured by A. Ádám (which, however, turned out valid only in particular cases):

Ádám's conjecture. *The connection sets of isomorphic circulant n-(di)graphs are one-multiplier equivalent, i.e. all circulant (di)graphs of order n are CI.*

1.3. Non-CI orders and admissible primes. Recently ([12], see also [14]) it became known ultimately for which orders there exist non-CI circulant (di)graphs (that is, Ádám's conjecture is false): these are the numbers divisible by 8 or by a square of an odd prime for digraphs and the same numbers with the exception of 8, 9 and 18 for undirected graphs.

On the other hand, undirected self-complementary circulant graphs exist if and only if the order n is divisible only by primes $p \equiv 1 \pmod 4$, see [4, 1]. In what follows, such numbers n will be called *admissible*.

2 Prime-order self-complementary circulant graphs

In this section we characterize constructively self-complementary circulant graphs of prime order $n = p$. They will be used later as building blocks for non-CI self-complementary circulant graphs of order p^2.

2.1. Main construction. Let p be an admissible prime. Recall that $\mathbb{Z}_p^*$ is a *cyclic* multiplicative group of order $p-1$. Since Ádám's conjecture is valid for prime orders, each self-complementary circulant p-graph has a self-complementing multiplier m. Therefore it suffices to construct all such graphs for every multiplier m. This can be done by the following simple construction (it is well known in the literature ([16, 15, 17]) though possibly in less detail).

Let $m \in \mathbb{Z}_p^*$ be a multiplier of order $o(m) := 4k$ dividing $p-1$. The action of m on the set $\mathbb{Z}_p^*$ gives a permutation π_m consisting of $(p-1)/4k$ independent cycles of length $4k$. Since $m^{2k} \equiv -1$, the permutation π_m has the form

$$\pi_m = (a_1, a_2, \ldots, a_{2k}, -a_1, -a_2, \ldots, -a_{2k})(b_1, b_2, \ldots, b_{2k}, -b_1, -b_2, \ldots, -b_{2k}) \ldots$$

The elements of each cycle of π_m can be partitioned into two alternative parts (*"semi-orbits"*) according to the "odd" or "even" positions they occupy in the cycle. Let us arbitrarily select one, and only one, part from every cycle and consider the union of the selected parts. Let $\mathcal{U}_m$ denote the set of all connection sets obtained as such unions.

2.2. Proposition.

1. *A circulant p-graph Γ is self-complementary with m as a self-complementary multiplier if and only if $\Gamma = \Gamma(X)$ for some $X \in \mathcal{U}_m$.*
2. *The order $o(m)$ of every self-complementing multiplier m divides $p-1$ and is divisible by 4.*
3. $|\mathcal{U}_m| = 2^{(p-1)/o(m)}$.

The first two statements are well-known (see, for example, [16]). Statement 3 is evident. □

For $X \in \mathcal{U}_m$, let $\mathrm{Stab}(X) := \{m' \mid m'X = X,\ m' \in \mathbb{Z}_p^*\}$ be the *stabilizer* of 0 in the automorphism group $\mathrm{Aut}(\Gamma(X))$. It is of even order since it contains $m' = -1$ of order 2. Since m is a self-complementing multiplier, we have $m^2 \in \mathrm{Stab}(X)$. Moreover, the set of all self-complementing multipliers of $\Gamma(X)$ is just the coset $m \cdot \mathrm{Stab}(X)$ in the subgroup $\langle m \rangle$ of $\mathbb{Z}_p^*$ generated by m.

The sets $\mathcal{U}_m$ can be used to determine self-complementary circulant graph *up to isomorphism* and to find their full sets of self-complementing multipliers. To that end, several useful properties of $\mathcal{U}_m$ can be easily established based on properties of cyclic groups (cf. [3]). They are formulated below.

2.3. Interconnections between the sets $\mathcal{U}_m$.

M1. $\mathcal{U}_{m'} = \mathcal{U}_m$ if and only if $o(m') = o(m)$.

M2. $\mathcal{U}_m$ and $\mathcal{U}_{m'}$ are disjoint if the orders $o(m)$ and $o(m')$ contain factor 2 in different powers.

M3. If $o(m)$ and $o(m')$ contain 2 in the same power, then $\mathcal{U}_m \cap \mathcal{U}_{m'} = \mathcal{U}_{m_0}$ where m_0 is a multiplier of order $\mathsf{lcm}(o(m), o(m'))$ (least common multiple).

M4. $\mathcal{U}_{m'} \subsetneqq \mathcal{U}_m$ if and only if $o(m')/o(m)$ is an odd integer greater 1.

2.4. Additional properties. From properties M2 and M4, one can easily establish:

M5. Let $\Gamma = \Gamma(X)$ be a self-complementary circulant graph with the stabilizer $\mathrm{Stab}(X)$ of order $2k$ dividing $\frac{p-1}{2}$. Then $X \in \mathcal{U}_{m'}$ if and only if
$m' = m^s$ for some odd s where m is an element of $\mathbb{Z}_p^*$ of order $4k$.

Finally, we need the following easily derivable properties of the stabilizers:

M6. Let $\Gamma = \Gamma(X)$ be a self-complementary circulant graph and $4k$ be the greatest order of its self-complementing multipliers. Then $\mathrm{Stab}(X)$ is of order $2k$.

M7. There exists a self-complementary circulant p-graph with the stabilizer of order $2k$ if and only if $4k$ divides $p - 1$.

Property M7 follows directly from M5 and M6 and the fact that $|\mathcal{U}_{m'}| < |\mathcal{U}_m|$ if $o(m) < o(m')$.

2.5. Definition. Two integers k and ℓ are called 2-*concordant*, denoted $k \overset{2}{\asymp} \ell$, if they contain 2 in the same power, i.e. $k = 2^r a$ and $\ell = 2^r b$ with some non-negative r and odd a and b.

Now we are in position to formulate a statement most important for the following.

2.6. Proposition. *Two self-complementary circulant p-graphs $\Gamma(X)$ and $\Gamma(X_1)$ possess a common self-complementing multiplier m_0 if and only if the orders $|\mathrm{Stab}(X)|$ and $|\mathrm{Stab}(X_1)|$ are 2-concordant.*

Proof. Let $|\mathrm{Stab}(X)| = 2^r a$ and $|\mathrm{Stab}(X_1)| = 2^r a_1$ with odd numbers a and a_1. By property M5, we have $X \in \mathcal{U}_m$ and $X_1 \in \mathcal{U}_{m_1}$ where m and m_1 are elements of orders $2^{r+1}a$ and $2^{r+1}a_1$, respectively. Therefore $m^{a_1} = m_1^a$.

Again, by M5 we conclude that $m_0 := m^{a_1}$ is a self-complementing multiplier of both $\Gamma(X)$ and $\Gamma(X_1)$. The converse statement
follows directly from M2 and M5. □

2.7. Reduced connection sets. To simplify practical calculations, we adopt the following agreement. It is clear that the connection sets of an undirected circulant graph of odd order is determined by its *reduced* ("halved") *connection set* $\check{X} := X \cap \mathbb{Z}_{\frac{n-1}{2}}$. Therefore, all calculations modulo p can be done up to altering the sign. Consequently, one may not distinguish between numbers a and b whenever $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$. This will be denoted as $a \simeq b$, for instance, $8 \simeq 5$ modulo 13.

In the subsequent examples we will often operate with $\check{X}$ instead of X (writing $\Gamma = \check{\Gamma}(\check{X})$), and with the *reduced permutation* $\check{\pi}_m = (a_1, a_2, \dots, a_{2k})\,(b_1, b_2, \dots, b_{2k}) \dots$ and its *reduced order* $\check{o}(m) := o(m)/2$. To avoid ambiguity, the elements of reduced connection sets are enclosed in brackets: $\check{X} = [a_1, a_2, \dots]$.

Up to equivalence, both, a connection set and its complement, present the same self-complementary circulant p-graph. By construction, if one of them belongs to $\mathcal{U}_m$, then the other does it too. Thus, we can additionally reduce lists to the half by considering only the reduced sets that contain 1. Correspondingly, let $\check{\mathcal{U}}_m := \{\check{X} \mid 1 \in \check{X}\}$.

2.8. Example. $\boxed{p = 17}$ 3 is a primitive root modulo 17, i.e. it is of reduced order 8. A repeated multiplication of 3 by itself gives us the permutation

$$\pi_3 = (1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6),$$

so that $\check{\pi}_3 = (1, 3, 8, 7, 4, 5, 2, 6)$. According to Section 2.1, the corresponding "odd/even" partition is such: $[1, 2, 4, 8]$ or $[3, 5, 6, 7]$. Thus, $\check{\mathcal{U}}_3$ consists of one connection set (containing 1). Moreover, 3, 5, 6 and 7 are all self-complementing multipliers of the corresponding circulant, they are of reduced order 8 and $\check{\pi}_5$, $\check{\pi}_6$ and $\check{\pi}_7$ give rise to the same partition.

Further, $\check{\pi}_2 = (1, 2, 4, 8)(3, 6, 5, 7)$ with the partition ($[1, 4]$ or $[2, 8]$) and ($[3, 5]$ or $[6, 7]$). The same partition arises for $\check{\pi}_8$. Finally, $\check{\pi}_4 = (1, 4)(2, 8)(3, 5)(6, 7)$ with ($[1]$ or $[4]$), ($[2]$ or $[8]$), ($[3]$ or $[5]$) and ($[6]$ or $[7]$).

Now, applying all possible multipliers to the constructed reduced connection sets in order to reveal isomorphic graphs, after some calculations we obtain four non-isomorphic self-complementary circulant graphs:

No	graph	self-complementing multipliers	stabilizer
1	$\check{\Gamma}([1,2,4,8])$	[3,5,6,7]	$[1,2,4,8] = \langle 2 \rangle$
2	$\check{\Gamma}([1,3,4,5])$ $\cong \check{\Gamma}([1,4,6,7])$	[2,8]	[1,4]
3	$\check{\Gamma}([1,2,3,6])$ $\cong \check{\Gamma}([1,2,5,6])$ $\cong \check{\Gamma}([1,3,6,8])$ $\cong \check{\Gamma}([1,3,7,8])$	[4]	[1]
4	$\check{\Gamma}([1,2,3,7])$ $\cong \check{\Gamma}([1,2,5,7])$ $\cong \check{\Gamma}([1,5,6,8])$ $\cong \check{\Gamma}([1,5,7,8])$		

2.9. The Paley graph of prime order. As a by-product of the descriptions given in Sections 2.1 – 2.4, two useful and possibly new properties of the well-known Paley graphs $\mathrm{P}(p)$ can be easily deduced ($\mathrm{P}(p)$ is defined on the field $\mathrm{GF}(p)$ as follows: two vertices are adjacent if their difference is a square).

If m is a generator of $\mathbb{Z}_p^*$, i.e. $o(m) = p-1$, then by Proposition 2.2(3), $\check{\mathcal{U}}_m$ contains a single connection set $\check{X}_0$. The corresponding self-complementary circulant graph $\check{\Gamma}(\check{X}_0)$ is known to be isomorphic to $\mathrm{P}(p)$ (see, e.g., [2]).

Definition. The minimal order of self-complementing permutations of a self-complementary graph is called its (self-complementary) *rank*.

Clearly, the rank is always a power of 2 (and it is greater than 2 according to Proposition 2.2(2)).

P1. The self-complementary rank of the Paley graph $\mathrm{P}(p)$ of prime order p is equal to the maximal power of 2 dividing $p-1$.

P2. $\mathrm{P}(p)$ is the unique self-complementary circulant p-graph having $\frac{p-1}{2}$ self-complementing multipliers.

For a simple proof and other details we refer to [11].

2.10. Remark on arbitrary orders. Just the same construction as in Section 2.1 generates all self-complementary circulant graphs which are *one-multiplier equivalent* (CI) to their complement for an *arbitrary* admissible order n. The number of such graphs (possibly, isomorphic to each other) is greater than or equal to $2^{\frac{n-1}{4}-1}$, where equality holds if $\frac{n-1}{4}$ is odd: in this and only in this case all self-complementary circulant graphs arise from the multiplier of order 4 (by properties M2 and M4, which are also valid for arbitrary orders). $2^{\frac{n-1}{4}-1}$ self-complementary circulants have been constructed for an arbitrary order n in [2]. Thus, our construction yields additional self-complementary graphs whenever 8 divides $n-1$.

3 Self-complementary p^2-circulants

3.1. Layers. For composite orders, it is natural to partition the elements of connection sets according to their divisors common to the order n: the layers thus obtained are invariant with respect to the multiplicative action of $\mathbb{Z}_n^*$. For $n = p^2$, two layers arise:

$$X = X_{(0)} \dot\cup X_{(1)}, \tag{1}$$

where the 0-*layer* $X_{(0)}$ is a subset of $\mathbb{Z}_{p^2}^*$ and the 1-layer $X_{(1)} = \{x \in X \mid p \text{ divides } x\}$ is a subset of $p\mathbb{Z}_p^*$.

3.2. Isomorphism theorem for p^2-circulants ([7], see also [13])**.** *Two circulant (di)graphs $\Gamma = \Gamma(X)$ and $\Gamma' = \Gamma(X')$ with $n = p^2$ vertices are isomorphic if and only if their respective layers are multiplicatively equivalent, i.e.*

$$X'_{(0)} = m_0 X_{(0)}, \quad X'_{(1)} = m_1 X_{(1)}, \tag{2}$$

for a pair of multipliers $m_0, m_1 \in Z_{p^2}^*$ where

$$m_0 = m_1 \tag{3}$$

whenever

$$(1+p)X_{(0)} \neq X_{(0)}. \tag{4}$$

3.3. Non-CI circulants. According to Theorem 3.2, the condition

$$(1+p)X_{(0)} = X_{(0)} \tag{5}$$

is necessary in order for $\Gamma(X)$ to be a non-CI circulant (di)graph. Moreover, this condition is also sufficient whenever both layers $X_{(0)}$ and $X_{(1)}$ are *proper* subsets of $\mathbb{Z}_{p^2}^*$ and $p\mathbb{Z}_p^*$,

respectively. Clearly, this is the case for self-complementary circulants.

For non-empty $X_{(0)}$, condition (5) means that

$$X_{(0)} = \{\alpha + \lambda \cdot p \mid \lambda = 0, 1, 2, \ldots, p-1;\ \alpha \in X_*\}$$

for some non-empty subset X_* of $\mathbb{Z}'_p$. Moreover, X_* is symmetric if and only if X is symmetric. Thus, X_* presents a circulant (di)graph of order p. In turn, up to the multiple p, the layer $X_{(1)}$ can be considered as the connection set of a circulant (di)graph of order p as well. Therefore any non-CI circulant (di)graph $\Gamma(X)$ of order p^2 can be presented by the pair

$$(X_*, X_1) \tag{6}$$

of connection sets of circulants of order p where $X_1 := p^{-1}X_{(1)} = \{\dfrac{m}{p} \mid m \in X_{(1)}\}$.

3.4. Proposition. *The mapping $\Gamma(X) \mapsto (\Gamma(X_*), \Gamma(X_1))$ is a one-to-one correspondence between non-isomorphic non-CI self-complementary circulant (di)graphs*

of order p^2 (p an admissible prime) and pairs of self-complementary circulant (di)graphs of order p. In this correspondence, strongly non-CI self-complementary circulant p^2-(di)graphs correspond to pairs of those self-complementary circulant p-(di)graphs which do not possess a self-complementing multiplier in common.

PROOF. If two non-CI circulant (di)graphs of order p^2 are isomorphic, then they are layer-wise isomorphic by a pair of multipliers (2). It is evident that m_0 defines an isomorphism between the corresponding p-circulants $\Gamma(X_*)$ and m_1 defines an isomorphism between the corresponding p-circulants $\Gamma(X_1)$. Vice versa, non-isomorphic p^2-circulants give rise to pairs of p-circulants which are non-isomorphic in at least one of the components.

It is clear that self-complementary circulant (di)graphs of order p^2 correspond to pairs of self-complementary circulant (di)graphs of order p. Conversely, any pair of self-complementary p-circulants gives rise to a non-CI self-complementary p^2-circulant (with the pair (X'_*, X'_1) corresponding to the complement $\Gamma(X')$). This proves the first assertion.

Now, let $\Gamma(X)$ be a non-CI self-complementary circulant (di)graph of order p^2 such that $\Gamma(mX)$ is its complement for some multiplier m. This means that m is a *common* self-complementing multiplier for both p-circulants, $\Gamma(X_*)$ and $\Gamma(X_1)$. □

It is easy to see that

$$\Gamma(X) \cong \Gamma(X_*) \circ \Gamma(X_1), \tag{7}$$

where $\circ$ denotes the *composition* of two graphs defined as follows: in the first graph we replace each vertex by a copy of the second graph; each edge of the first graph gives rise to edges connecting pairwise all the vertices of the corresponding copies of the second graph.

3.5. Theorem. *Strongly non-CI self-complementary circulant graphs of order p^2 exist if and only if $p-1$ is divisible by 8. On the contrary, a non-CI self-complementary circulant graph of order p^2 which is one-multiplier equivalent to its complement exists for any admissible p.*

PROOF. By property M7, there exists a pair of self-complementary circulant p-graphs with non-2-concordant orders of their stabilizers (Definition 2.5) if and only if 8 divides $p-1$. Now, applying Proposition 2.6 to the last statement of Proposition 3.4, we obtain the first assertion of the corollary.

The second assertion is evident (for example, take a pair $(\Gamma(X'), \Gamma(X'))$ with an arbitrary self-complementary circulant p-graph $\Gamma(X')$). □

The first five primes p permitting strongly non-CI self-complementary circulant p^2-graphs are the following: 17, 41, 73, 89, 97.

3.6. Example. According to Example 2.8 and Proposition 3.4, one of strongly non-CI self-complementary circulant graphs of order $n = 17^2$ is $\Gamma = \Gamma(X)$ with

$$X_{(0)} = \{1, 2, 4, 8, -1, -2, -4, -8\} + 17 \cdot \{0, 1, \dots, 16\}$$

and

$$X_{(1)} = 17 \cdot \{1, 3, 4, 5, -1, -3, -4, -5\}$$

(+ and $\cdot$ are the element-wise addition and multiplication). In terms of composition (and the adopted reduced notations) it can be presented as follows:

$$\Gamma = \check{\Gamma}([1, 2, 4, 8]) \circ \check{\Gamma}([1, 3, 4, 5]). \tag{8}$$

3.7. Remark on admissible orders. Non-CI self-complementary circulant graphs exist for all admissible non-square-free orders. Indeed, let p^2 divides n, let Γ be a non-CI self-complementary circulant of order p^2 and let Δ be a self-complementary circulant graph

of order n/p^2. Then, as can be easily seen, their composition $\Gamma \circ \Delta$ is also a self-complementary non-CI circulant graph, and it is of order n. Moreover, if Γ is a strongly non-CI self-complementary circulant graph, the resulting composition is also strongly non-CI.

4 Enumeration

4.1. Prime order self-complementary circulant graphs. Properties M1 – M4 given in Section 2.3 are sufficient for counting self-complementary circulant p-graphs by the order of their stabilizer. Denote by $C_{\mathrm{su}}(p, k)$ the number of non-isomorphic self-complementary circulant graphs with p vertices whose stabilizer is of order $2k$ where $4k$ divides $p - 1$ (here 'su' stands for self-complementary, undirected). Then $C_{\mathrm{su}}(p, k)$ can be calculated by the following formula, slightly modifying one given in [3]:

$$C_{\mathrm{su}}(p, k) = \frac{2k}{p-1} \sum_{\substack{\ell \mid (p-1), k \mid \ell \\ \ell/k \text{ odd}}} \mu\left(\frac{\ell}{k}\right) 2^{\frac{p-1}{4\ell}}, \tag{9}$$

where $\mu(\ell)$ is the number-theoretic Möbius function.

Summing up the expressions (9) over k, one can calculate the number $C_{\mathrm{su}}(p)$ of all non-isomorphic self-complementary circulant p-graphs [3]. But there is, instead, a much simpler enumerative formula obtained in [6]:

$$C_{\mathrm{su}}(p) = \frac{2}{p-1} \sum_{\ell \mid \frac{p-1}{4}} \phi(2\ell) 2^{\frac{p-1}{4\ell}}, \tag{10}$$

where $\phi(2\ell)$ is the Euler totient function.

4.2. Non-CI and weakly self-complemetary circulant graphs. Based on the preceding formulas and Theorem 3.2 we can obtain several new enumerative results supplementing those given in [6]. We mean the counting of all weakly self-complementary circulant graphs of order p^2 (not necessarily non-CI) and strongly non-CI

circulant graphs. Hereafter we will use the term *'weakly'* as the property opposite to 'strongly'. Thus, a circulant is referred to as weakly self-complementary if it is one-multiplier equivalent to its complement.

All self-complementary circulant graphs can be separated into three disjoint classes:

- CI (necessarily weakly self-complementary);
- weakly non-CI self-complementary (ws);
- strongly non-CI self-complementary (ss).

Let $F_{\mathrm{CI}}(p^2)$, $F_{\mathrm{ws}}(p^2)$ and $F_{\mathrm{ss}}(p^2)$ denote the numbers of the corresponding circulants considered up to isomorphism and let $F_{CI}^{\mathrm{weak}}(p^2)$, $F_{\mathrm{ws}}^{\mathrm{weak}}(p^2)$ and $F_{\mathrm{ss}}^{\mathrm{weak}}(p^2)$ denote the numbers of them up to one-multiplier equivalence. In fact, by definition, $F_{\mathrm{CI}}^{\mathrm{weak}}(p^2) = F_{\mathrm{CI}}(p^2)$.

Adhering the general enumerative scheme and nomenclature proposed in [6], we introduce the following enumerators (the order p^2 is dropped for brevity):

- $A_{\mathrm{su}} := F_{\mathrm{CI}}^{\mathrm{weak}} + F_{\mathrm{ws}}^{\mathrm{weak}} + F_{\mathrm{ss}}^{\mathrm{weak}}$: self-complementary circulants up to one-multiplier equivalence;
- $B_{\mathrm{su}} := F_{\mathrm{ws}}^{\mathrm{weak}} + F_{\mathrm{ss}}^{\mathrm{weak}}$: non-CI self-complementary circulants up to one-multiplier equivalence;
- $D_{\mathrm{su}} := F_{\mathrm{ws}} + F_{\mathrm{ss}}$: non-CI self-complementary circulants up to isomorphism;
- $A_{\mathrm{su}}^{\mathrm{weak}} := F_{\mathrm{CI}}^{\mathrm{weak}} + F_{\mathrm{ws}}^{\mathrm{weak}}$: weakly self-complementary circulants up to one-multiplier equivalence;
- $B_{\mathrm{su}}^{\mathrm{weak}} := F_{\mathrm{ws}}^{\mathrm{weak}}$: weakly non-CI self-complementary circulants up to one-multiplier equivalence;
- $D_{\mathrm{su}}^{\mathrm{weak}} := F_{\mathrm{ws}}$: weakly non-CI self-complementary circulants up to isomorphism.

The right-hand interpretations of the above quantities are evident.

4.3. Proposition.

$$C_{\mathrm{su}}^{\mathrm{weak}}(p^2) = C_{\mathrm{su}}(p^2) - F_{\mathrm{ss}}(p^2). \tag{11}$$

PROOF. According to Theorem 3.2,

$$C_{\mathrm{su}} = A_{\mathrm{su}} - B_{\mathrm{su}} + D_{\mathrm{su}} \tag{12}$$

is the number of non-isomorphic self-complementary circulant graphs of order $n = p^2$ and

$$C_{\mathrm{su}}^{\mathrm{weak}} = A_{\mathrm{su}}^{\mathrm{weak}} - B_{\mathrm{su}}^{\mathrm{weak}} + D_{\mathrm{su}}^{\mathrm{weak}} \tag{13}$$

is the number of non-isomorphic weakly self-complementary circulant graphs.

From the expressions given above we see that

$$A_{\mathrm{su}}^{\mathrm{weak}} - B_{\mathrm{su}}^{\mathrm{weak}} = A_{\mathrm{su}} - B_{\mathrm{su}} \tag{14}$$

and

$$D_{\mathrm{su}}^{\mathrm{weak}} = D_{\mathrm{su}} - F_{\mathrm{ss}}.$$

These equalities complete the proof. □

Now we can count strongly non-CI self-complementary circulant graphs. In view of the equality

$$F_{\mathrm{ss}}(p^2) = D_{\mathrm{su}}(p^2) - F_{\mathrm{ws}}(p^2) \tag{15}$$

(see above), this amounts to the counting of non-CI and weakly non-CI self-complementary circulant graphs.

4.4. Theorem. *The numbers of non-isomorphic non-CI self-complementary and weakly non-CI self-complementary circulant graphs of admissible order p^2 are expressed by the following formulas:*

$$D_{\mathrm{su}}(p^2) = C_{\mathrm{su}}(p)^2 \tag{16}$$

and

$$F_{\mathrm{ws}}(p^2) = \sum_{k,\ell \mid \frac{p-1}{4},\, k \overset{2}{\asymp} \ell} C_{\mathrm{su}}(p,k) C_{\mathrm{su}}(p,\ell), \tag{17}$$

where $C_{\mathrm{su}}(p)$ and $C_{\mathrm{su}}(p,k)$ are determined by formulas (10) *and* (9)*, and the relation $\overset{2}{\asymp}$ is defined in* Section 2.5.

PROOF. These formulas follow directly from Propositions 3.4 and 2.6. □

Clearly, if 8 does not divide $p-1$, we may use, instead of (17), the formula

$$F_{\mathrm{ws}}(p^2) = C_{\mathrm{su}}(p)^2. \tag{17$'$}$$

Expression (16) was established in [6] though without an explicitly formulated enumerative meaning of the left-hand term.

Specifically, for $p = 17$ we obtain $F_{\mathrm{ws}}(17^2) = 1^2 + 1^2 + 2^2 = 6$ by formulas (9) (or by the data presented in Section 2.8), (10) and (17). So that, there are $F_{\mathrm{ss}}(17^2) = 4^2 - 6 = 10$ non-isomorphic strongly non-CI self-complementary

circulant graphs of order 17^2. Similarly, for $p = 41$, $F_{\rm ws}(41^2) = 1^2 + 1^2 + 3^2 + 51^2 + 2 \cdot 1 \cdot 3 + 2 \cdot 1 \cdot 51 = 2720$ and $F_{\rm ss}(41^2) = 56^2 - 2720 = 416$.

4.5. Remark. Due to equality (14), in order to find $C_{\rm su}(p^2)$ by formula (12), one can equally well use either the pairs of auxiliary quantities $A_{\rm su}$ and $B_{\rm su}$ or $A_{\rm su}^{\rm weak}$ and $B_{\rm su}^{\rm weak}$. In fact, it was the latter that was used in the paper [6] though the definition concerned the former. This misinterpretation does not affect the final formula for $C_{\rm su}(p^2)$ but should be taken into account with respect to the intermediate numerical results given in Table 1 loc. cit. (reproduced also as Table 4 in our paper [10]).

For instance, by characteristics of the four self-complementary circulant graphs of order 17 given in Section 2.8, one can easily calculate $B_{\rm su}^{\rm weak}(17^2) = \frac{2^2}{2} + \frac{4^2}{4} + \frac{(8+8)^2}{8} = 38$. This coincides with the value calculated in [6] in another, analytical, way. At the same time, $B_{\rm su}(17^2)$ is greater by $F_{\rm ss}^{\rm weak}(17^2) = 2\frac{2\cdot 4}{4} + 2\frac{(2+4)\cdot(8+8)}{8} = 28$. And just $28 = A_{\rm su}^{\rm weak}(17^2) - A_{\rm su}(17^2)$.

Acknowledgements

We thank the anonymous referees for helpful suggestions.

References

[1] B. Alspach, Isomorphism and Cayley graphs on abelian groups. *Graph symmetry: algebraic methods and applications*, Proc. NATO ASI Ser., Montréal, 1996 (G. Hahn ed.), Ser. C, Math. Phys. Sci. 497, Kluwer Acad. Publ., Dordrecht (1997), 1–22.

[2] I. Broere and J. H. Hattingh, On the construction of self-complementary circulant graphs. *Graph Th., Combin. and Algorithms*, Proc. 7-th Intern. Conf., Western Mich. Univ., Kalamazoo, 1992 (Y. Alavi and A. Schwenk eds.), Vol. **1**, Wiley, NY (1995), 123–129.

[3] G. L. Chia and C. K. Lim, A class of self-complementary vertex-transitive digraphs. *J. Graph Th.*, **10** (1986), No 2, 241–249.

[4] D. Fronček, A. Rosa and J. Širáň, The existence of selfcomplementary circulant graphs. *Europ. J. Combin.*, **17** (1996), No 7, 625–628.

[5] R. Jajcay and C. H. Li, Constructions of self-complementary circulants with no multiplicative isomorphisms. (submitted, 1997).

[6] M. Klin, V. Liskovets and R. Pöschel, Analytical enumeration of circulant graphs with prime-squared number of vertices. *Sém. Lothar. Combin.*, **36** (1996), B36d, 36 pp.

[7] M. H. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings. *Preprint* AdWDDR, ZIMM, Berlin (1978), 43 p. A shortened version in: *Colloq. Math. Soc. J. Bolyai*, **25**. *Algebr. Methods in Graph Theory. Szeged, 1978*, part 2, North-Holland, Amsterdam (1981), 405–434.

[8] M. Ch. Klin and R. Pöschel, The isomorphism problem for circulant digraphs with p^n vertices. *Preprint* P-34/80, Akad. der Wiss. der DDR, ZIMM, Berlin (1980), 40 pp.

[9] C. H. Li, On finite graphs that are self-complementary and vertex-transitive. *Australas. J. Combin.*, **18** (1998), 147–155.

[10] V. Liskovets and R. Pöschel, On the enumeration of circulant graphs of prime-power and square-free orders. *Preprint* MATH-AL-8-1996, TU-Dresden, 37 pp.

[11] V. Liskovets and R. Pöschel, Non-Cayley-isomorphic self-complementary circulant graphs, *Preprint* MATH-AL-18-1997, TU-Dresden, 16 pp.

[12] M. Muzychuk, Ádám's conjecture is true in the square-free case. *J. Combin. Th.*, **A72** (1995), No 1, 118–134.

[13] M. Muzychuk and R. Pöschel, Isomorphism criteria for circulant graphs. *Preprint* MATH-AL-9-1999, TU-Dresden, 43 pp.

[14] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism. *Europ. J. Combin.*, **8** (1987), No 1, 35–43.

[15] G. Ringel, Selbstkomplementäre Graphen. *Arch. Math.*, **14** (1963), 354–358.

[16] H. Sachs, Über selbstkomplementäre Graphen. *Publ. Math.*, **9** (1962), No 2, 269–288.

[17] D. A. Suprunenko, Self-complementary graphs. *Cybernetics*, **21** (1985), 559–567 (translation from *Kibernetika* (1985), No 5, 1–6).