Recognizing circulant graphs in polynomial time: An application of association schemes

Mikhail E. Muzychuk,*
Department of Computer Science and Mathematics,
Netanya Academic College, Netanya, 42365, Israel
muzy@netanya.ac.il

Gottfried Tinhofer,
Zentrum Mathematatik, Technical University of Munich,
80290 Munich, Germany
gottin@mathematik.tu-muenchen.de

Submitted: October 7, 2000; Accepted: May 26, 2001
MR subject classifications: 05C25, 05C85.

Abstract

In this paper we present a time-polynomial recognition algorithm for certain classes of circulant graphs. Our approach uses coherent configurations and Schur rings generated by circulant graphs for elucidating their symmetry properties and eventually finding a cyclic automorphism.

Key words: Circulant graphs, association schemes, Schur rings.

1 Introduction

We consider graphs of the form $G = (X, \gamma)$, where X is a finite set and γ is a binary relation on X, the *adjacency relation*. For $x \in X$ put $\gamma(x) = \{y : (x, y) \in \gamma\}$.

*Partially supported by DAAD fellowship A/00/24054

Let $\mathbf{G}$ be a group and $G = (X, \gamma)$ a graph with vertex set $X = \mathbf{G}$ and with adjacency relation γ defined with the aid of some subset $S \subset \mathbf{G}$ by

$$\gamma = \{(g, h) \, : \, g, h \in \mathbf{G} \wedge hg^{-1} \in S\}.$$

Then G is called *Cayley graph* over the group $\mathbf{G}$ and S is called *connection set* of G.

Let $\mathbf{Z}_n$, $n \in \mathbf{N}$, stand for a cyclic group of order n, written additively. A *circulant graph* G of order n (or a *circulant*, for short) is a *Cayley graph* over $\mathbf{Z}_n$. In this particular case, the adjacency relation γ has the form

$$\gamma = \bigcup_{i=0}^{n-1} \{i\} \times \{i + \gamma(0)\}$$

where $\gamma(0)$ is the set of successors of the vertex 0. Evidently, the set of successors $\gamma(i)$ of an arbitrary vertex i satisfies $\gamma(i) = i + \gamma(0)$. All arithmetic operations with vertex numbers are understood modulo n. We do not distinguish by notation between the element $z \in \mathbf{Z}_n$ and the integer $z \in \mathbf{Z}$. From the context, it will always be clear what is meant. For $a \in \mathbf{Z}_n$ and $S \subset \mathbf{Z}_n$ we write aS for the set $\{as \mid s \in S\}$.

For a circulant G the connection set is $\gamma(0)$. G is a simple undirected graph if $0 \notin \gamma(0)$ and if $j \in \gamma(0)$ implies $-j \in \gamma(0)$.

There are different equivalent characterizations of circulants. One of them is this: A graph G is a circulant iff its vertex set can be numbered in such a way that the resulting adjacency matrix $A(G)$ is a circulant matrix. We call such a numbering a *Cayley numbering.* Still another characterization is: G is a circulant iff a cyclic permutation of its vertices exists which is an automorphism of G. Such an automorphism we shall call a *full cycle.*

Cayley graphs, and in particular circulants, have been studied intensively in the literature. These graphs are vertex-transitive. In the case of a prime vertex number n, circulants are known to be the only vertex-transitive graphs. Because of their high symmetry, Cayley graphs are ideal models for communication networks. In this context, recently particular interest has been awaken for so-called geometric circulants. A *geometric circulant* $\mathcal{GC}(n, d)$ is a circulant on the vertex set $\mathbf{Z}_n$ possessing a connection set

$$\gamma(0) = \{\pm 1, \pm d, \pm d^2, \ldots, \pm d^m\},$$

consisting of a geometric progression in d and its inverses, where d is a natural number satisfying $1 < d \leq \frac{n}{2}$ and m is such that $d^m + 1 < n \leq d^{m+1} + 1$.

Certain geometric circulant graphs have been proposed in [22] as a new topology for multicomputer networks. The circulants in this paper have been called *recursive circulants*, they are geometric circulants with vertex number $n = cd^m$ for some c, $1 < c \leq d$.

The motivation for the attribute *recursive*, as pointed out in this paper, is the fact that circulants $\mathcal{G}C(cd^m, d)$ possess a hierarchical structure. If one drops all edges in $\mathcal{G}C(cd^m, d)$ which are of the form $(v, v \pm 1)$ then the remaining graph is a union of d graphs, each isomorphic to $\mathcal{G}C(cd^{m-1}, d)$. A hierarchy like this, however, may be observed also in more general situations. Cayley graphs showing a hierarchical structure have been investigated in [1] and [2] (and in many subsequent papers on Cayley graphs as models for interconnection networks) in a more general setting. A review on this topic is found in [14].

The problem we deal with in this paper is the *recognition problem* for circulants, in particular for geometric circulants. Assume that a graph G on the vertex set $X = \{0, \ldots, n-1\}$ is given by its diagram or by its adjacency matrix, or by some other data structure commonly used in dealing with graphs. Our task is *to decide whether G is a circulant graph or not.*

To our knowledge the first result towards recognizing circulants can be found in [23] where circulant tournaments have been considered. In the paper [21] we have settled the case of a prime number n of vertices, i. e. we have proposed a still somewhat complicated, but nevertheless time-polynomial method for recognizing arbitrary circulants of prime order.

In the present paper we first consider a reduction step which enables us to restrict our considerations to circulants with connection sets the stabilizer of which is trivial. Then we study the structure of geometric circulants in more detail and describe a time-polynomial recognition method for this class of circulants. Our method exploits the properties of algebraic-combinatorial structures which can be associated with graphs, namely *coherent configurations* [15], respectively, *coherent algebras* [16], also called *cellular algebra* [24], and *Schur rings* [25], and the interrelations between these structures when the automorphism group $\mathbf{Aut}(G)$ of G contains a full cycle. Since the coherent configuration generated by G has the same automorphism group as G, our method can be introduced as a method for recognizing coherent configurations having a full cyclic automorphism. Coherent configurations with this property will be called *circulant (coherent) configurations.*

As just mentioned, the method used for recognizing circulant graphs is based on the notions of coherent configurations and Schur rings generated by graphs and on the interrelations between these notions when the graph G possesses a cyclic automorphism. For reaching our aims it is therefore unavoidable to call the reader's attention to some particular facts concerning the interrelation between these two algebraic structures. This will be done in the appendix, part of the content of which has already been presented in [21]. However, for the convenience of the reader, this material must be included here again.

The main body of our paper starts with Section 2 where we explain the algebraic-combinatorial approach to the recognition problem for circulants we use and where the reduction to the case of trivial stabilizers of the connection set is described. In Section

3 basic properties of geometric circulants $\mathcal{G}C(n,d)$ are discussed. In most cases we can prove that the Schur ring generated by a geometric circulant contains $\{1,-1\}$ as a basic set. In such cases we are done, because such a basic set defines a Hamiltonian cycle of the graph under consideration, along which we can determine a Cayley numbering. The only case in which this does not happen is when n and d are relatively prime and $n|(d^{m+1}\pm 1)$, in which case the connection set $\gamma(0)$ is a subgroup of $\mathbf{Z}_n^*$.

In Section 4 we give a formal description of the recognition algorithm. Section 5 contains some concluding remarks.

2 An algebraic-combinatorial approach to the recognition problem for circulants

Let $G=(X,\gamma), X=\{0,1,\dots,n-1\}$, be an arbitrary graph, $\langle\langle\gamma\rangle\rangle=(X;\Gamma)$ its coherent configuration with basic relations $\gamma_0,\gamma_1,\dots,\gamma_s$. The basis of $(X;\Gamma)$ can be computed in time $O(n^3 \ln n)$ using an appropriate version of a so-called *graph stabilization algorithm* first described in [24], see [3], [4], [7][1]. If $(X;\Gamma)$ is not a commutative association scheme, then G is certainly not circulant.

If (X,γ) is an undirected circulant, then all basic relations γ_i in $(X;\Gamma)$ are symmetric, too. Hence, if starting with an undirected graph G we find a basic relation γ_i which is not symmetric, then again G cannot be circulant. Checking $(X;\Gamma)$ for being a commutative association scheme and, in the undirected case, for having symmetric basic relations needs time $O(n^2)$.

If G is a circulant with connection set $\gamma(0)$, then we may assume $X=\mathbf{Z}_n$ and, as pointed out in the appendix (Subsections 6.2 and 6.3), there is a mapping $log_g:\Gamma\longrightarrow 2^{Z_n}$ defined with the aid of a full cycle $g\in\mathbf{Aut}(X;\Gamma)$ relating the basic relations of the association scheme to a partition $T_0=log_g(\gamma_0), T_1=log_g(\gamma_1),\dots,T_s=log_g(\gamma_s)$ of $\mathbf{Z}_n$ such that $\underline{T_0},\underline{T_1},\dots,\underline{T_s}$ are the basic quantities of the S-ring $\mathcal{S}=\langle\langle\gamma(0)\rangle\rangle$ of G. Since we do not know this mapping, i. e. since we do not know a full cycle g (or a Cayley numbering of G), we are not able to compute $\mathcal{S}$. We only know the association scheme $(X;\Gamma)$ for the computation of which we do not need a Cayley numbering. Any numbering of the vertex set using e. g. the numbers $0,1,\dots,n-1$ is equally appropriate. To compute a Cayley numbering we can try to use properties the association scheme $(X;\Gamma)$ must have if G is a circulant. In general, it is yet not known how to find a sufficient set of properties of $(X;\Gamma)$ which would enable us to find a Cayley numbering for arbitrary circulants G in polynomial time. However, the search for such a sufficient set is simplified if we restrict

[1]The currently most efficient implementation can be obtained free of charge for non-commercial use from `http://www-m9.mathematik.tu-muenchen.de/~bastert/wl.html`.

the investigation to certain subclasses of circulants. It is in this context that S-ring theory becomes useful. Subclasses of circulants can be characterized by properties of their connection sets and/or the S-rings generated by them. For example, connection sets may have non-trivial or trivial stabilizers (either additive or multiplicative ones), or they may have other obvious structures, as it is the case for instance with geometric circulants. These features imply particular features on the corresponding S-rings and, vice versa, on the equivalent two-dimensional structures, i. e. the corresponding association schemes. The idea of working with the interplay between association schemes and S-rings has been successfully employed in [21] for the case of circulants on a prime number of vertices. In this paper we are going to demonstrate its usefulness in other cases.

2.1 Hamiltonian cycles

Let us start with the situation in which a Cayley numbering can be found directly from the shape of some basic graph (X, γ_i) of $(X; \Gamma)$. The following statement seems to be folklore. To be able to refer to it conveniently we present it as a proposition.

Proposition 2.1. *Let $G = (X, \gamma)$ be a graph such that its coherent configuration $(X; \Gamma)$ is an association scheme.*

(i) *Assume that some basic graph $G_i = (X, \gamma_i)$ is connected and has outdegree 1. Let $g = (x_0, x_1, \ldots, x_{n-1})$ where for $0 \le k \le n-2$ the vertex x_{k+1} is the only vertex satisfying $(x_k, x_{k+1}) \in \gamma_i$. Then G is circulant and $g \in \mathbf{Aut}(X, \gamma)$.*

(ii) *Assume that some symmetric basic graph $G_j = (X, \gamma_j)$ is connected and has degree 2. Let $g = (y_0, y_1, \ldots, y_{n-1})$ and g^{-1} be the two unique full cycles of G_j. Then, G is circulant if and only if $g \in \mathbf{Aut}(X, \gamma)$.*

Let $\mathbf{Z}_n^*$ denote the multiplicative group of units in $\mathbf{Z}_n$. Notice that if G is a circulant then $(X; \Gamma)$ has a connected basic graph G_i of outdegree 1 iff there is an $a \in \mathbf{Z}_n^*$ such that the S-ring of G has basic set $\{a\}$, and that there is a symmetric connected basic graph G_j of degree 2 iff there is a $q \in \mathbf{Z}_n^*$ such that the S-ring of G has a basic set $\{q, -q\}$.

Proof. (i) Under the hypothesis, the adjacency matrix $A(\gamma_i)$ is a permutation matrix and commutes with $A(\gamma)$. This proves that g is a full cycle of G.

(ii) Here G_i is an undirected hamiltonian cycle which has exactly two full cycles g and g^{-1} which can be found by starting at an arbitrary vertex y_0 and traversing G_i first in one and then in reverse direction. Since $\mathbf{Aut}(X, \gamma)$ is a subgroup of $\mathbf{Aut}(X, \gamma_i)$, each full cycle of (X, γ) is a full cycle of (X, γ_i).

□

2.2 A reduction step

Next we describe a reduction step which is possible whenever G happens to be a circulant (directed or undirected) with a connection set the additive stabilizer of which is non-trivial.

Let $\tau \in \mathrm{Rel}(\Gamma)$ be an equivalence of $(X;\Gamma)$ and let $C_0, \ldots, C_{s-1}$ be the classes of τ. Define a new graph $\hat{G} = (\hat{X}, \hat{\gamma})$ by

$$\hat{X} = \{0, \ldots, s-1\},$$
$$(i,j) \in \hat{\gamma} \Longleftrightarrow (C_i \times C_j) \cap \gamma \neq \emptyset.$$

In other words, $\hat{G}$ is derived from G by replacing each class C_i by a single vertex i and drawing an arc from i to j exactly if in G there is some arc from a vertex in C_i to a vertex in C_j. The resulting graph $\hat{G}$ is called the factor graph of G *modulo* τ and is also denoted by G/τ. It is the combinatorial analogue to the coset graph of a Cayley graph over a group **G** with respect to some subgroup **H**.

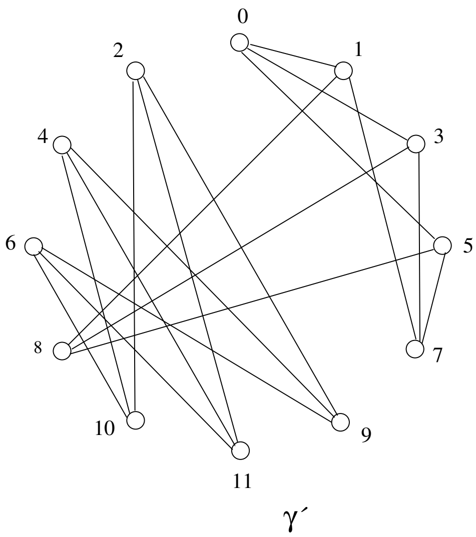

Figure 1a

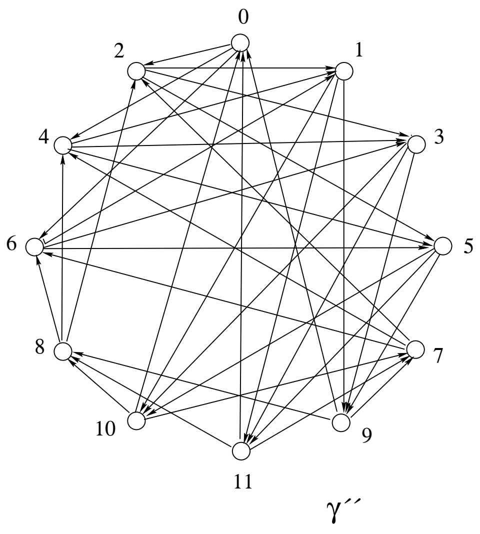

Figure 1b

Example. Consider the graph $G = (X, \gamma)$ on the vertex set $X = \{0, 1, \ldots, 11\}$ and with relation γ being the union of the symmetric relation γ' in Figure 1a and the antisymmetric relation γ'' in Figure 1b. The coherent configuration $\langle\langle\gamma\rangle\rangle$ has five basic relations $\gamma_0 = \epsilon_X$, γ_1, γ_2, γ_3 and γ_4, the latter four of them are shown in Figure 2. We have $\gamma_1 = \gamma'$, $\gamma_2 = \gamma''$, $\gamma_3 = \gamma_2^T$, $\gamma_4 = X \times X \setminus \gamma_0 \cup \gamma_1 \cup \gamma_2 \cup \gamma_3$.

It is obvious that the basic graphs (X, γ_2) and (X, γ_3) are connected. That means, γ_2 and γ_3 do not generate a non-trivial equivalence relation. Thus, the only non-trivial equivalences of $\langle\langle\gamma\rangle\rangle$ are

$$\tau_1 = \gamma_0 \cup \gamma_1 \cup \gamma_4 \text{ and } \tau_2 = \gamma_0 \cup \gamma_4.$$

The factor graph of G modulo τ_2 is shown in Figure 3.

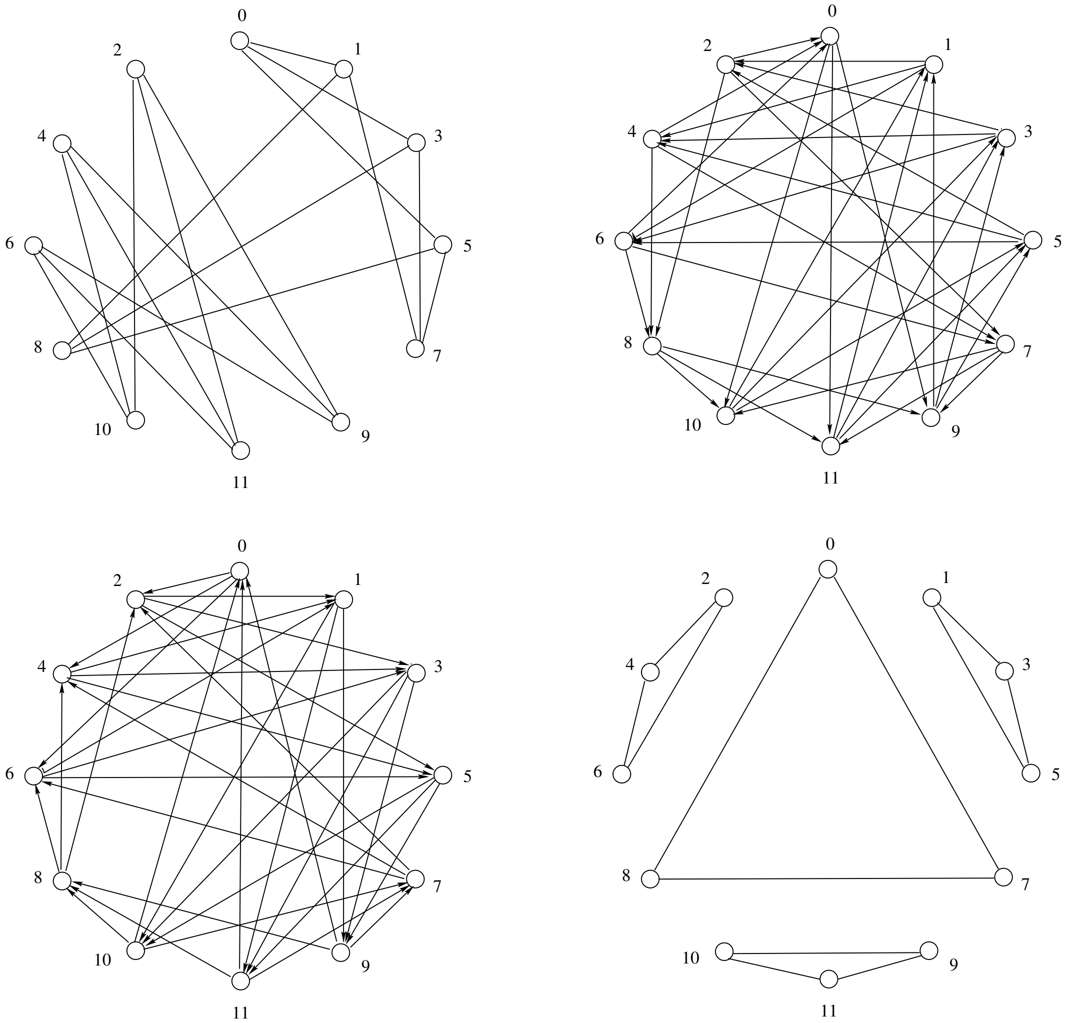

Figure 2

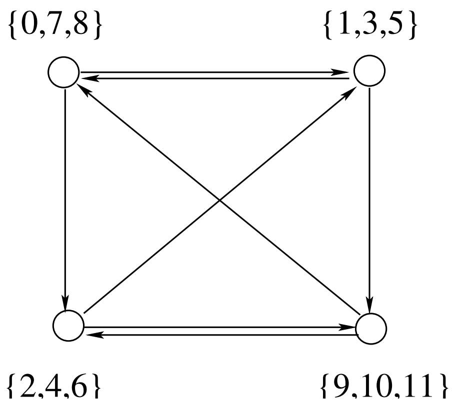

Figure 3

The graph G in our example and the equivalence τ_2 have the following property:

$$(C_i \times C_j) \cap \gamma \neq \emptyset \Longrightarrow C_i \times C_j \subset \gamma,\ i,j \in \hat{X}.$$

This is a useful property to which we return in Proposition 2.2.

Now, let again $G = (X, \gamma)$ be an arbitrary circulant of order n, $(X;\Gamma) = \langle\langle\gamma\rangle\rangle$ its association scheme and $\mathcal{S} = \langle\langle\gamma(0)\rangle\rangle$ its S-ring . According to Proposition 6.5(ii) the $\mathcal{S}$-subgroups of $\mathbf{Z}_n$ are in one-to-one correspondence with the equivalence relations of $(X;\Gamma)$. Assume that $\mathbf{F} = \langle f\rangle$ is an $\mathcal{S}$-subgroup (f the smallest generator) and τ the corresponding equivalence relation. Define $\hat{\gamma}(0) = \{i \bmod(f) \,:\, i \in \gamma(0)\}$. Then the factor graph G/τ is isomorphic to the graph $(Y, \hat{\gamma})$ where $Y = \mathbf{Z}_f$ and where by definition

$$(i,j) \in \hat{\gamma} \Longleftrightarrow j - i \in \hat{\gamma}(0),\ i,j \in \mathbf{Z}_f$$

$(Y, \hat{\gamma})$ is the *coset graph* of G *modulo* $\langle f\rangle$. From this observation we immediately find the following fact: *Let G be a graph and τ an equivalence of its coherent algebra. If G is a circulant, then also G/τ is a circulant graph.*

It may happen that we have to deal with the following situation: We choose a particular subgroup $\langle f\rangle$ of $\mathbf{Z}_n$ and want to derive the factor graph $G/\langle f\rangle$ from some input graph G without knowing a Cayley numbering of G. This operation can be executed on G provided we can identify the classes of the equivalence τ corresponding to $\langle f\rangle$. These classes are, however, easy to find. Different subgroups of $\mathbf{Z}_n$ are distinguished by their orders, hence, different equivalences of $(X;\Gamma)$ can be distinguished by the number of elements in their classes. In the appendix it will be discussed how the equivalences of $(X;\Gamma)$ can be listed in time $O(n^2)$. Thus, the graph G/τ can be constructed within this same time bound.

Now, given the circulant $G = (X, \gamma)$, consider a particular subgroup of $\mathbf{Z}_n$, the *stabilizer*

$$\mathbf{F} = Stab_+(\gamma(0)) = \{z \in \mathbf{Z}_n \,:\, z + \gamma(0) = \gamma(0)\}$$

of the connection set $\gamma(0)$. Let again τ be the equivalence of $(X;\Gamma)$ corresponding to $\mathbf{F}$. Note that in this particular case, if (i,j) is an arc of G then G contains every arc from any vertex in $i+F$ to any vertex in $j+F$. This simple fact can be used in order to reduce the task of constructing a Cayley numbering of G to the task of finding such a numbering for the factor graph G/τ and extending it to G.

Proposition 2.2. *Let $G = (X, \gamma)$ a graph, $|X| = n$, $\langle\langle\gamma\rangle\rangle = (X;\Gamma)$ a homogeneous coherent algebra, and τ an equivalence of $(X;\Gamma)$. Let $C_0, \ldots, C_{s-1}$ be the equivalence classes of τ. Assume that*

$$\gamma \cap C_i \times C_j \neq \emptyset \Longrightarrow C_i \times C_j \subset \gamma,\ \ 0 \leq i,j \leq s-1.$$

Then

(i) *G is a circulant graph iff the factor graph G/τ is a circulant graph.*

(ii) *Any Cayley numbering $\hat{\varphi}$ of G/τ can be lifted up to a Cayley numbering of G defining*

$$\varphi(z) = \sum_{i=0}^{s-1} \varphi_i(z) I_{C_i}(z)$$

where I_{C_i} is the characteristic function of the set C_i and φ_i is an arbitrary bijection from C_i onto the set

$$\{\hat{\varphi}(i), \hat{\varphi}(i) + f, \hat{\varphi}(i) + 2f, \ldots, \hat{\varphi}(i) + (\frac{n}{f} - 1)f\}.$$

Proof. The necessity of (i) has already been shown above. The sufficiency follows from (ii). (ii) is proved easily using the definition of a circulant and the property of τ stated in the hypothesis of the proposition.

□

To finish our example, consider Figure 4 where on the left part a Cayley numbering of the factor graph G/τ_2 is indicated. This numbering is extended to a Cayley numbering of the original graph G and indicated on the right part of the picture.

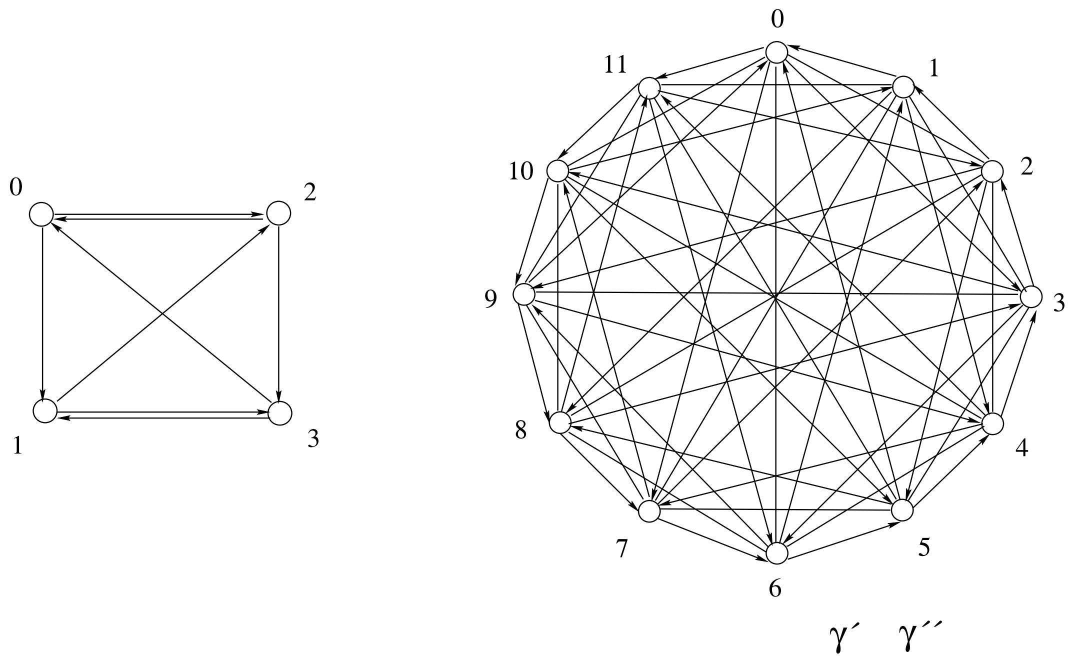

Figure 4

Here, we have indicated the Cayley numbering

z	0	1	2	3	4	5	6	7	8	9	10	11
$\varphi(z)$	0	6	1	2	9	10	5	4	8	3	11	7

However, every mapping φ satisfying

$$\varphi(\{0,7,8\}) = \{0,4,8\},\ \varphi(\{2,4,6\}) = \{1,5,9\},$$

$$\varphi(\{1,3,5\}) = \{2,6,10\},\ \varphi(\{9,10,11\}) = \{3,7,11\}$$

would be a Cayley numbering, too.

Replacing G by G/τ for finding a Cayley numbering, if such a numbering exists, is an efficient step in the process of recognizing circulants, which can be applied to any graph G, provided its coherent configuration is an association scheme and contains an equivalence τ which satisfies the hypothesis of Proposition 2.2. Notice that τ corresponds to a non-trivial stabilizer of the connection set $\gamma(0)$ iff each set of neighbours $\gamma(x)$ of the input graph (X,γ) is a union of equivalence classes of τ. This shows that we can find τ or prove that no such τ exists in time $O(n^2)$. Since a non-trivial stabilizer contains at least two elements, each reduction step reduces the size of the input graph at least by a factor $\frac{1}{2}$.

We summarize the considerations in this subsection presenting the following complexity statement.

Proposition 2.3. *The recognition problem for arbitrary circulant graphs is polynomially reducible to the recognition problem of circulants the connection set of which has trivial additive stabilizer.*

2.3 A simple recognition algorithm for exceptional cases

In a very few exceptional cases, when the connection set $\gamma(0)$ is of a special type, a Cayley numbering for a circulant graph G can be found without computing its coherent configuration. Since such exceptional cases appear also when dealing with geometric circulants we discuss them here and present an appropriate recognition algorithm which in the general case may be used as a subroutine.

Here we consider undirected graphs only. As before, let $G = (X,\gamma)$ be the undirected graph we want to test for being circulant and put

$$\psi = \{(x,y)\ :\ (A(\gamma)^2)_{xy} = 1\}.$$

Notice that ψ belongs to $(X;\Gamma)$. Consider the following procedure.

Algorithm 1

Input: An undirected graph $G = (X, \gamma)$

1. Compute ψ. If ψ is not regular of positive degree, then STOP with answer NO.

2. Choose $x \in X$ and do:
   Set $\rho = \gamma(x)$;
   2.1 If $\rho = \emptyset$ then STOP with answer NO
   else choose $y \in \gamma(x)$ and do:
   Set $x_0 = x$ and $x_1 = y$;
   For $0 \leq i < n - 2$ do:
   If $|\psi(x_i) \cap \gamma(x_{i+1})| \neq 1$, then delete y from ρ and goto 2.1.
   If $|\psi(x_i) \cap \gamma(x_{i+1})| = 1$, then define x_{i+2} to be the unique point in $\psi(x_i) \cap \gamma(x_{i+1})$.

3. Check whether $(x_0, x_1, \ldots, x_{n-1})$ is a full cycle for G;

In the positive case STOP with answer YES and output this cycle.
$\varphi(x_i) = i,\ 0 \leq i \leq n - 1$, defines a Cayley numbering;
In the negative case STOP with answer NO.

Proposition 2.4. *Let $G = (X, \gamma)$, be a circulant the connection set $S = \gamma(0)$ of which contains 1 and satisfies the following conditions:*

$$\forall_{s,s' \in S} \quad s + s' = 2 \iff s = 1 \wedge s' = 1; \tag{1}$$

$$\forall_{t \in 2S, s' \in S} \quad t - s' = 1 \iff t = 2 \wedge s' = 1 \tag{2}$$

where $2S = \{s + s \mid s \in S\}$. Then Algorithm 1 yields a Cayley numbering for G.

Proof. It follows from (1) that $\{(x, x+2) \mid x \in \mathbf{Z}_n\} \subseteq \psi$. Therefore (X, ψ) is a circulant having some connection set $T \subseteq \mathbf{Z}_n$ with $2 \in T$. In particular, $\psi \neq \emptyset$. Arguing as in part 1 of Lemma 6.3, we obtain that $T \subset 2S$.

In order to prove the claim it is sufficient to show that for each x, y with $y = x + 1$ the following holds

$$\psi(x) \cap \gamma(y) = \{y + 1\}.$$

We have $x + 2 \in \psi(x), x + 2 \in \gamma(x + 1)$. Thus, $y + 1 \in \psi(x) \cap \gamma(y)$. Conversely, let $z \in \psi(x) \cap \gamma(y)$. Then

$$z - x - (z - y) = y - x = 1,$$

$$z - x \in T \subseteq 2S,\ z - y \in S.$$

Now by (2) $z - y = 1$. This shows that, once the vertices x_0 and x_1 are correctly determined, the remaining numbering done by the algorithm is correct, too. Since a Cayley numbering remains a Cayley numbering if we subtract a constant c from each vertex x, we may choose x_0 arbitrarily, x_1 however must be a neighbor of x_0. To find the correct pair x_0, x_1 we have to try all possibilities for x_1. Algorithm 1 does it.

□

As a corollary we have the following

Proposition 2.5. *Let $G = (X, \gamma)$ be a recursive circulant with connection set $S = \{\pm 1, \pm d, ..., \pm d^m\}$ and $n = cd^m$ for some c, $1 < c \leq d$. If $d \geq 4$, then Algorithm 1 will determine a Cayley labeling of G.*

Proof. It is sufficient to show that S satisfies (1)-(2). Consider the equation $s+s' = 2$. Since all the elements of $S \setminus \{1, -1\}$ are contained in a subgroup of index $d \geq 4$, we have $2 \notin \langle d \rangle$. Therefore at least one of the elements s, s' is equal to ± 1. Without loss of generality $s = \pm 1$. If $s = 1$, then we are done. If $s = -1$, then $s' = 3$ which is impossible, since $d \geq 4$. Thus (1) holds.

Consider now the equation $2s - s' = 1, s, s' \in S$. As before, at least one of the elements $2s, s'$ is not contained in $\langle d \rangle$. Therefore $2s \in \{\pm 1\}$ or $s' \in \{\pm 1\}$. If $2s = 1$, then $s' = 0$ which is impossible. If $2s = -1$, then $s' = -2$ which is also impossible, since $d \geq 4$. If $s' = 1$, then $2s = 2$ and we are done. If $s' = -1$, then $2s = 0$, which is possible only in the case $c = 2, n = 2d^m$. But in this case $0 \notin T$, since 0 appears $|S|$ times in $\underline{S} + \underline{S}$. Hence the algorithm will work in this case as well.

□

Algorithm 1 involves matrix multiplication for the determination of ψ. However, since we easily can transform an adjacency matrix $A(\gamma)$ into a set of sorted adjacency lists for γ, we can compute $A(\psi)$ in time $O(n^2\delta)$ where δ is the degree of the (regular) input graph G. Let m be the edge number of G. We have $2m = n\delta$. Hence, using sorted adjacency lists for ψ, too, the overall complexity of Algorithm 1 is $O(nm)$.

3 Properties of geometric circulants

In the remaining part of the paper we restrict ourselves to geometric circulants $\mathcal{GC}(n, d) = (X, \gamma)$. For such graphs, by definition,

$$\gamma(0) = \pm\{1, d, d^2, \dots, d^m\} \tag{3}$$

where

$$d^m + 1 < n \leq d^{m+1} + 1,\ 1 < d \leq \frac{n}{2}. \tag{4}$$

For convenience, from now on we shorten the term *geometric circulant graph* to simply *gc-graph.*

Given numbers n and δ, in most cases, there are more than one gc-graphs with vertex number n and degree δ. In particular cases, n and δ determine d and m uniquely. Unfortunately, the knowledge of n, d and m, in general, does not simplify the recognition problem.

3.1 The association schemes of geometric circulants

Let again $\mathbf{Z}_n^*$ denote he multiplicative group of units in $\mathbf{Z}_n$. Our notation does not distinguish between arithmetic modulo n and normal integer arithmetic. It will be clear from the context which arithmetic is used. For $B \subset \mathbf{Z}_n$ and $k \in \mathbf{Z}_n$ define $\{B\}_k = \{b \bmod(k) \mid b \in B\}$. The following theorem shows the main features of the association schemes, respectively, the S-rings of gc-graphs and presents the basic knowledge necessary for the construction of an efficient recognition algorithm for such graphs.

Theorem 3.1. *Let (X,γ) be a gc-graph $\mathcal{G}C(n,d)$. Then either*

(i) *$\langle\langle\gamma\rangle\rangle$ has basic set $\{1,-1\}$ or*

(ii) *the stabilizer $Stab_+(\gamma(0))$ is a non-trivial subgroup $\langle f\rangle$ of $\mathbf{Z}_n$ and $\{\gamma(0)\}_f = \{1,-1\}$ or*

(iii) *$\gamma(0)$ is a subgroup of $\mathbf{Z}_n^*$.*

Proof. Let $\mathcal{G}C(n,d)$ and its S-ring $\mathcal{S} = \langle\langle\gamma\rangle\rangle$ be given. By (S7), $a\gamma(0)$ is an $\mathcal{S}$-set for every $a \in \mathbf{Z}_n^*$. Assume that there is an $a \in \mathbf{Z}_n^* \setminus \{1\}$, satisfying $ad = d$. For such a we find

$$\gamma(0) \setminus a\gamma(0) = \{1,-1\}$$

is an $\mathcal{S}$-set and therefore must be a basic set of $\mathcal{S}$. Therefore, (i) happens if

$$xf = f$$

has a non-trivial solution $x \in \mathbf{Z}_n^*$. Here, $f = gcd(n,d)$. For $x \in \mathbf{Z}_n^*$ we have $gcd(xf,n) = f$. The number of elements $y \in \mathbf{Z}_n$ satisfying $gcd(y,n) = f$ equals $\varphi(\frac{n}{f})$ (where φ is the Euler function). Therefore, if $\varphi(\frac{n}{f}) < \varphi(n)$, then $xf = f$ has a non-trivial solution in $\mathbf{Z}_n^*$. From well-known properties of the Euler function it can be seen that $\varphi(\frac{n}{f}) < \varphi(n)$ always holds except when $f = 1$ or when $f = 2$ and $\frac{n}{f}$ is odd. Thus, $xf = f$ has a non-trivial solution in $\mathbf{Z}_n^*$ except in the two following cases:

- **Case 1:** $f = 2$ and $n = fq$ where q is odd.
- **Case 2:** $f = 1$.

Assume that we are in Case 1 and $m \geq 2$. The sets

$$[\mathbf{Z}_n]_h = \{x \in \mathbf{Z}_n \,:\, gcd(n,x) = h\}$$

are the orbits of $\mathbf{Z}_n^*$ acting on $\mathbf{Z}_n$ by multiplication. Thus, since $d^2 < n$ and $gcd(n,d) = gcd(n,d^2) = 2$ there exists an $l \in \mathbf{Z}_n^*$ satisfying $dl = d^2$. Put $K = \gamma(0) \cap l\gamma(0)$. Then $\pm\{d^2,\ldots,d^m\} \subseteq K \subseteq \pm\{d,d^2,\ldots,d^m\}$. By (S7) and (S8) K is a non-empty $\mathcal{S}$-set. Thus, $\langle K\rangle$ is an $\mathcal{S}$-group. Since $\langle d^2\rangle \leq \langle K\rangle \leq \langle d\rangle$ and $\langle d^2\rangle = \langle d\rangle = \langle 2\rangle$, we find $\langle K\rangle = \langle 2\rangle$. Therefore $\gamma(0) \setminus \langle 2\rangle = \{-1,1\}$ is a basic set $\mathcal{S}$-set.

If $m = 1$, then $d^2 \geq n-1$ such that $\gamma(0) = \{1,d,-d,-1\}$. Here, we should consider Table 1 which shows the entries in $\gamma(0)+\gamma(0)$.

Table 1	1	-1	d	$-d$
1	2	0	$1+d$	$1-d$
-1	0	-2	$-1+d$	$-1-d$
d	$d+1$	$d-1$	$2d$	0
$-d$	$-d+1$	$-d-1$	0	$-2d$

Note that, since d and n are even numbers,

$$\{2,-2,2d,-2d\} \cap \{1+d, 1-d, -1+d, -1-d\} = \emptyset.$$

Thus, unless $2d = -2$ ($2d = 2$ would contradict $d \leq \frac{n}{2}$), the elements of Table 1 determine two simple quantities $\underline{K}$ and $\underline{L}$ of $\mathcal{S}$ with $K = \{2,-2,2d,-2d\}$ and $L = \{d+1,-d-1,d-1,-d+1\}$ (since the frequency of the elements in K is 1, while the elements of L appear exactly twice). Since $2 \in K$, the subgroup $\langle 2\rangle = \langle K\rangle$ is an $\mathcal{S}$-group. Therefore, $\{1,-1\} = \gamma(0) \setminus \langle 2\rangle$ is a basic set of $\mathcal{S}$.

Finally, consider the case $2d = n-2$. We have

$$\underline{\gamma(0)} + \underline{\gamma(0)} = 4\cdot\underline{\{0\}} + 4\cdot\underline{\{q\}} + 2\cdot\underline{\{2,-2,q+2,q-2\}}$$

and $Stab_+(\gamma(0)) = \langle d+1\rangle = \langle q\rangle$, which implies $\gamma(0) = \{1,-1\} + \langle q\rangle$. This proves that in Case 1 we meet one of the situations (i) or (ii).

Notice that $m = 1, 2d = n-2$ always leads to case (ii), no matter whether $xf = f, x \in \mathbf{Z}_n^*$ has a non-trivial solution or not.

Finally, assume $gcd(n,d) = 1$ (Case 2). Then either

$$\gamma(0) \setminus (d\gamma(0)) = \{1,-1\},$$

and is therefore a basic set of $\mathcal{S}$, or $d\gamma(0) = \gamma(0)$ which implies that $\gamma(0)$ is a subgroup of $\mathbf{Z}_n^*$ and that either $n|(d^{m+1}-1)$ or $n|(d^{m+1}+1)$. This observation completes the proof of the theorem.

$\square$

3.2 Cyclotomic geometric circulants

We call a circulant (X,γ) a *cyclotomic circulant* if its connection set $\gamma(0)$ is a subgroup $\mathbf{H}$ of $\mathbf{Z}_n^*$. The term *cyclotomic* was introduced in [10] in connection with association schemes, see also [8], p. 66. Let $a_1\mathbf{H}, a_2\mathbf{H}, \ldots, a_r\mathbf{H}$, $a_1 = 1$, be the orbits of $\mathbf{H}$ acting on $\mathbf{Z}_n$ by multiplication. Then

$$\underline{T_0} = \underline{\{0\}}, \underline{T_1} = \underline{a_1\mathbf{H}}, \ldots \underline{T_r} = \underline{a_r\mathbf{H}}$$

are the basic quantities of an S-ring $\mathcal{S}$, and

$$\{(x,y) \,:\, y - x \in T_i\},\ 0 \le i \le r,$$

are the basic relations of an association scheme.

The S-ring $\mathcal{S}$ is not necessarily generated by $\mathbf{H}$. In general, $\langle\langle \mathbf{H} \rangle\rangle$ is some fusion of $\mathcal{S}$. However, it is known that $\langle\langle \mathbf{H} \rangle\rangle = \mathcal{S}$ iff $Stab_+(\mathbf{H})$ is trivial (see [19]). Therefore, with the help of Proposition 2.2, the recognition problem for general cyclotomic circulants coincides with the recognition problem for cyclotomic association schemes. This is a challenging problem on its own with which we plan to deal in a forthcoming paper. Here we restrict our attention to the case of cyclotomic geometric circulants, for which subclass recognition is much easier than for general cyclotomic circulants.

In this section we assume that the parameters of the graph $\mathcal{GC}(n,d)$ satisfy the conditions

$$\begin{gathered} d^m + 1 < n \le d^{m+1} + 1 \\ 1 < d \le \tfrac{n}{2},\ m > 0,\ n \ge 4, \\ n \mid (d^{m+1}+1) \text{ or } n \mid (d^{m+1}-1), \\ \mathcal{GC}(n,d) \text{ is not complete.} \end{gathered} \tag{5}$$

such that the connection set

$$\mathbf{H} = \pm\{1, d, \ldots, d^m\}$$

is a subgroup of $\mathbf{Z}_n^*$. Our assumptions imply that $|\mathbf{H}| > 2$. Otherwise the graph $\mathcal{GC}(n,d)$ would be a Hamiltonian cycle and the recognition problem would be trivial. If $Stab_+(\mathbf{H}) \ne \{0\}$, then let f be its smallest generator. A simple calculation shows that $\mathbf{H}_f = \pm\{1, \ldots, d^{a-1}\}$ for some $a \in \{1, 2, \ldots, m\}$. Thus, the factor graph of $\mathcal{GC}(n,d)$ modulo the equivalence τ which corresponds to $Stab_+(\mathbf{H})$ is again a cyclotomic geometric circulant. So we may assume that $Stab_+(\mathbf{H})$ is trivial.

For each $i \in \mathbf{Z}_n$ we set $\gamma_i = \{(x,y) \in \mathbf{Z}_n \times \mathbf{Z}_n \mid x - y \in i\mathbf{H}\}$. Obviously, in the current context, $\gamma_1 = \gamma$. The S-ring of $\mathcal{GC}(n,d)$ has basic sets $i\mathbf{H}$, $i \in J$, and its circulant association scheme has basic relations γ_i, $i \in J$, where $J = \{0, 1, a_2, \ldots, a_r\}$ is a set of representatives of the orbits of $\mathbf{H}$ considered as acting on $\mathbf{Z}_n$ by multiplication.

Remark: It is easy to see that, if $\varphi : \mathbf{Z}_n \longrightarrow \mathbf{Z}_n$ is a Cayley numbering for a cyclotomic circulant $G = \mathcal{G}C(n,d)$, then for $b \in \mathbf{Z}_n$ and $a \in \mathbf{H}$ also $\varphi_{a,b}$ defined by $\varphi_{a,b}(z) = a \cdot \varphi(z) + b$ is a Cayley numbering. For this reason, if $(x,y) \in \gamma$ is arbitrary and if a Cayley numbering for the candidate graph G exists, then there is also one which assigns 0 to x and 1 to y. We shall make freely use of this property in this subsection. Note that each $\varphi_{a,b}(z)$ is an automorphism of G, hence, a cyclotomic circulant is arc-transitive.

For the discussion of cyclotomic geometric circulants we need some auxiliary statements the proof of which is moved to the appendix.

Lemma 3.1. *If (m,d,n) satisfies (5), then*

(i) $n \geq 1 + d + ... + d^m$ *and*

(ii) *if $d = 2$, then $n = 2^{m+1} \pm 1$.*

Lemma 3.2. *If $(m,n) \neq (1, 2d+2)$ and satisfies (5), then $|2\mathbf{H}| = |\mathbf{H}|$.*

Lemma 3.3. *If $(m,d,n) \notin \{(1,d,2d+2),(2,3,14)\}$ and satisfies (5), then*

(i) *the structure constant $p^{\gamma_i}_{\gamma_1,\gamma_1}$ is odd if and only if $\gamma_i = \gamma_2$;*

(ii)

$$p^{\gamma_2}_{\gamma_1,\gamma_1} = \begin{cases} 1, & \text{if } d \geq 4; \\ 3, & \text{if } d = 2,3. \end{cases}$$

(iii)

$$2\mathbf{H} \cap (1+\mathbf{H}) = \begin{cases} \{2\} & \text{if } d \geq 4; \\ \{2, \frac{2}{3}, -2\}, & \text{if } d = 3; \\ \{2, \frac{1}{2}, -1\}, & \text{if } d = 2 \end{cases}$$

(where $\frac{1}{3} = \pm 3^m$ and $\frac{1}{2} = \pm 2^m$, the signs $\pm$ distinguishing the two cases $n \mid (d^{m+1}-1)$ and $n \mid (d^{m+1}+1)$, respectively).

Note that If $(m,d,n) = (1,2,2d+2)$, then we are in the case discussed at the end of the proof of Theorem 3.1 in which $Stab_+(\gamma(0))$ is non-trivial.

The first part of Lemma 3.3 implies that γ_2 is uniquely determined by γ_1. More precisely, $\gamma_2 = \{(x,y) \mid (A(\gamma_1)A(\gamma_1))_{xy} \equiv 1 \pmod 2\}$.

Consider at first the case when $d \geq 4$. In this case $p^{\gamma_2}_{\gamma_1\gamma_1} = 1$. Since γ_1 and γ_2 are of the same valency Lemma 3.2 implies that $p^{\gamma_1}_{\gamma_2\gamma_1} = 1$. Pick an arbitrary pair $(x_0, x_1) \in \gamma_1$ and define the sequence $x_k, 2 \leq n-1$, recursively as follows:

$$\{x_k\} = \gamma_2(x_{k-2}) \cap \gamma_1(x_{k-1}). \tag{6}$$

This definition is correct, since $|\gamma_2(x_{k-2}) \cap \gamma_1(x_{k-1})| = p^{\gamma_1}_{\gamma_2\gamma_1} = 1$.

Proposition 3.4. *If (X, γ) is a cyclotomic geometric circulant with $d \geq 4$ and $x_0 = 0, x_1 = 1$, then $x_k = k,\ 2 \leq k \leq n-1$.*

Proof. The proof is by induction on k. The statement holds by assumption for $k = 0, 1$. Hence let $k \geq 2$. Assume that $x_{k-2} = k-2$ and $x_{k-1} = k-1$. Set $a = x_k - x_{k-2}, b = x_k - x_{k-1}$. By construction $a \in 2\mathbf{H}, b \in \mathbf{H}$ and $1 + b = a$. Clearly that $b = 1, a = 2$ is a solution of this equation. By Lemma 3.3 it is unique. Hence $x_k = x_{k-2} + 2 = k$, as desired.

Note that the proof just given shows that $S = \gamma(0)$ fulfills the conditions (1)-(2) of Proposition 2.4.

□

Proposition 3.4 enables us to reconstruct a Cayley numbering of a cyclotomic gc-graph, provided $d \geq 4$. Recall that according to the remark above the pair $(x_0, x_1) \in \gamma_1$ may be chosen arbitrarily. The remaining cases are more complicated. The problem is that the point x_k cannot be determined by (6), since $\gamma_2(x_{k-2}) \cap \gamma_1(x_{k-1})$ contains three points. In this case x_k should be separated by using a configuration with more than three points. The method we propose is based on the following proposition. It does not work in the case of a few small *exceptional graphs* defined by triples (m, d, n) in the set

$$\mathcal{K} = \{(1,3,8), (1,3,10), (2,2,9), (2,3,13), (2,3,14),$$

$$(2,3,26), (2,3,28), (3,2,15)\}.$$

Proposition 3.5. *Assume $d \in \{2, 3\}$ and $(m, d, n) \notin \mathcal{K}$. Let $(x, y) \in \gamma_1$ be arbitrary. Then $z_1 = 2y - x$ is the unique point of X which satisfies the following conditions:*

$$\begin{array}{c} z_1 \in \gamma_2(x) \cap \gamma_1(y); \\ Min\{|\gamma_2(y) \cap \gamma_1(z_1) \cap \gamma_1(z_2)|, |\gamma_2(y) \cap \gamma_1(z_1) \cap \gamma_1(z_3)|\} > \\ |\gamma_2(y) \cap \gamma_1(z_2) \cap \gamma_1(z_3)| \end{array} \tag{7}$$

where z_2 and z_3 are defined by $\{z_2, z_3\} = \gamma_2(x) \cap \gamma_1(y) \setminus \{z_1\}$.

Proof. The proof is given in the appendix.

□

Remarks.

1. If $(m, d, n) = (1, 3, 8)$, then $G = K_{4,4}$, the complete bipartite graph on two sets of four vertices each.

2. If $(m, d, n) = (2, 3, 13)$, then G is a Paley graph (see [9], p. 35).

3. If $(m, d, n) = (2, 3, 26)$, then G is a bipartite graph the coherent configuration of which contains an equivalence with 13 classes of size 2. The factor graph with respect to this equivalence is isomorphic to the Paley graph on 13 vertices just mentioned.

4. If $(m, d, n) = (3, 2, 15)$, then G is a tensor product of K_3 and K_5.

5. The remaining exceptional graphs have a similar simple structure.

In analogy to the case $d \geq 4$ we may construct a Cayley labeling for a cyclotomic gc-graph with $d \in \{2, 3\}$ proceeding in the following way. Pick an arbitrary pair $(x_0, x_1) \in \gamma = \gamma_1$ and define the sequence x_k, $2 \leq k \leq n-1$, recursively as follows:

> *x_k is the unique vertex z_1 which satisfies* (7) *in Proposition 3.5 with $x = x_{k-2}$ and $y = x_{k-1}$.*

The following proposition completes our discussion of cyclotomic gc-graphs.

Proposition 3.6. *Let (X, γ) be a cyclotomic gc-graph satisfying the assumption of Proposition 3.5. If $x_0 = 0$, $x_1 = 1$, then $x_k = k$, $2 \leq k \leq n-1$.*

4 The algorithm

Since there are only a finite number of exceptional graphs, given an arbitrary input graph G, we can decide in a preprocessing phase whether G is exceptional or not, and if yes, determine a Cayley numbering for G. This preprocessing needs constant time and does not influence the theoretical complexity of our recognition method. Therefore we formulate the following recognition algorithm for processing non-exceptional graphs only.

Algorithm 2

INPUT: A connected undirected regular non-exceptional graph $G = (X, \gamma)$ of degree δ, $2 \leq \delta < |X| - 1$;

STEP 1:
1.1 Compute the coherent configuration $(X; \Gamma) = \langle\langle \gamma \rangle\rangle$;
1.2 If $(X; \Gamma)$ is not a symmetric association scheme, then goto 6.2;
1.3 Otherwise let $\gamma_0 = \varepsilon_X, \gamma_1, \ldots, \gamma_s$ be the basic relations of $(X; \Gamma)$
with $\gamma_i \subseteq \gamma$ for $1 \leq i \leq t$ and $\gamma_i \cap \gamma = \emptyset$ for $t+1 \leq i \leq s$;

Put $i = 1$;

Step 2:

2.1 If $i < s$ compute the connected components $C_0, C_1, \ldots, C_{f-1}$ of the basic graph $G_i = (X, \gamma_i)$ else goto 4.1;

2.2 If G_i is connected, then
If G_i has degree 2, then do:
Choose arbitrarily x_0 and one of the two possible orientations of the undirected cycle G_i, determine its sequence of vertices $(x_0, x_1, \ldots, x_{n-1})$ and consider this as cyclic permutation g;
If g is a full cycle for G, then define $\varphi(x_j) = j,\ 0 \leq j \leq n-1$, and goto 6.1 else goto 6.2;
Otherwise, put $i = i + 1$ and goto 2.1;

2.3 If G_i is not connected, then
for $0 \leq k \leq f - 1$ do:
Choose $x \in C_k$ and compute $\gamma(x)$;
Put $\hat{\gamma}_k = \emptyset$;
For $0 \leq j \leq f - 1$ do
If $\gamma(x) \cap C_j \neq \emptyset$ and $C_j \not\subset \gamma(x)$ then put $i = i + 1$ and goto 2.1;
If $C_j \subseteq \gamma(x)$, then put $\hat{\gamma}_k = \hat{\gamma}_k \cup \{j\}$;

Step 3:

3.1 Define

$$\hat{X} = \{0, \ldots, f-1\};\ \ \hat{\gamma} = \bigcup_{k=0}^{f-1} \{k\} \times \gamma_k;$$

3.2 If $|\hat{\gamma}(0)| > 2$, then goto 6.2;

3.3 Let $(\hat{X}, \hat{\gamma})$ be the undirected cycle $(i_0, i_1, \ldots, i_{f-1})$ and define $\hat{\varphi}(i_s) = s,\ 0 \leq s \leq f - 1$;

3.4 For $0 \leq k \leq f - 1$ renumber all vertices of C_k arbitrarily using the numbers in $\hat{\varphi}(k) + \langle f \rangle$;

3.5 For $x \in X$ denote its new number by $\varphi(x)$ and goto 6.1;

Step 4:

4.1 Compute $\psi = \{(x, y) \,|\, (A(\gamma)^2)_{x,y} = 1\}$;
If ψ is not regular of positive degree, then goto 5.1;

4.2 Choose $(x, y) \in X$ and do:
Set $x_0 := x, x_1 := y$.
For $0 \leq i < n - 2$ do:
If $|\psi(x_i) \cap \gamma(x_{i+1})| \neq 1$, then goto 5.1;
If $|\psi(x_i) \cap \gamma(x_{i+1})| = 1$, then define x_{i+2} as the unique point in $\psi(x_i) \cap \gamma(x_{i+1})$

4.3 If $g = (x_0, x_1, \ldots, x_{n-1})$ is a full cycle of (X, γ), then define $\varphi(x_i) = i,\ 0 \le i \le n-1$, and goto 6.1;

STEP 5:
5.1 Compute $\psi = \{(x,y)\,|(A(\gamma)^2)_{x,y} = 3\}$;
If ψ is not regular of positive degree, then goto 6.2;
5.2 Choose $(x,y) \in X$ and do:
Set $x_0 := x, x_1 := y$.
For $0 \le i < n-2$ do:
If $|\psi(x_i) \cap \gamma(x_{i+1})| \ne 3$, then goto 6.2;
If $|\psi(x_i) \cap \gamma(x_{i+1})| = 3$, then do
if there is a unique vertex in $\psi(x_i) \cap \gamma(x_{i+1})$
which satisfies condition (7) in Proposition 3.5,
then denote this vertex by x_{i+2} else goto 6.2;
5.3 If $g = (x_0, x_1, \ldots, x_{n-1})$ is a full cycle of (X, γ), then
define $\varphi(x_i) = i,\ 0 \le i \le n-1$, and goto 6.1
else goto 6.2;

STEP 6:
6.1 STOP with answer YES and output the Cayley numbering φ;
6.2 STOP with answer NO;

---

5 Concluding Remarks

The most time consuming step of Algorithm 2 is Step 1, thus, this algorithm has time complexity $O(n^3 \ln n)$. If in Step 2 a connected basic graph G_i of degree 2 is found, then we are in Case (i) of Theorem 3.1, G_i is an undirected cycle which possibly determines a full cycle $\mathbf{Aut}(G)$. If in Step 2 an equivalence relation is found such that each $\gamma(x)$ is a union of equivalence classes, then we are in Case (ii) of Theorem 3.1. From the proof of this theorem it follows that the reduction step leads to a quotient graph which is a cycle. Therefore, in Step 3, Algorithm 2 checks whether a cycle has been found, and if yes, then it constructs the corresponding Cayley numbering. If this case does not happen, then the algorithm continues with Step 4, which is basically Algorithm 1, with the difference that here, because of the arc transitivity of cyclotomic gc-graphs, we need only consider a single choice for (x_0, x_1). If this step does not lead to a Cayley numbering, then Step 5 is entered in which the case of Proposition 3.5 is checked. This step is analogous to Step 4, only the search for the next vertex in the sequence is more involved. Finally, if Step 5 does not end with the determination of a Cayley numbering, then Algorithm 2 stops with answer NO. A stop with answer NO is also reached, when (X, Γ) is not a symmetric association scheme or when the reduction in Step 3 leads not to a cycle, a situation which cannot happen for a gc-graph. In all other cases, Algorithm 2 yields a Cayley numbering for the input graph G. Summarizing we can now state the main result of our paper in the following theorem.

Theorem. *Geometric circulants can be recognized in time $O(n^3 \ln n)$ using the above Algorithm 2.*

Algorithm 2 solves not only the recognition problem for gc-graphs but also for all graphs generating an association scheme having a connected basic graph (X, γ_i) of degree ≤ 2 and for graphs having a factor graph which is a cycle. The algorithm could easily be extended to recognize all circulants having a coset graph which is a gc-graph.

While the cases (i) and (ii) of Theorem 3.1 can be handled in a straightforward manner, the treatment of case (iii), where the connection set is a subgroup of $\mathbf{Z}_n^*$, needs additional knowledge of the structure of the association scheme, respectively, the S-ring generated by cyclotomic circulants. Every recognition algorithm for a class of circulants containing cyclotomic circulants will need such knowledge, too. For this reason it seems reasonable to look more closely to the structure of general cyclotomic circulants and try to find a polynomial time recognition algorithm for them. In our eyes, this is a challenging task which we plan to undertake in a forthcoming publication.

6 Appendix

6.1 Coherent configurations

We now summarize briefly the properties of coherent configurations and Schur rings which we have used in the main body of this paper. Most of them have been developed basically in earlier papers of the first author and have already been used in [21]. We use the same notation as in this latter publication.

Let X be a finite set. We use small Greek letters for binary relations on X and capital Greek letters for sets of such relations. A set Γ of binary relations on X is called *a coherent configuration* [16] if it satisfies the following axioms:

- (CC1) There exists a subset $\Pi \subset \Gamma$ such that the identical relation $\varepsilon_X = \{(x,x) \mid x \in X\}$ is a union of $\pi \in \Pi$, $\varepsilon_X = \bigcup_{\pi \in \Pi} \pi$.
- (CC2) The relations from Γ form a partition of X^2;
- (CC3) $\forall \gamma \in \Gamma, \gamma^t = \{(x,y) \mid (y,x) \in \gamma\} \in \Gamma$;
- (CC4) For each triple $\alpha, \beta, \gamma \in \Gamma$ and a pair $(x,y) \in \gamma$ the number

$$p^{\gamma}_{\alpha,\beta} = |\{z \in X \mid (x,z) \in \alpha, (z,y) \in \beta\}|$$

does not depend on the choice of the pair $(x,y) \in \gamma$.

The elements of Γ are called *basic relations*, their graphs *basic graphs*, and the numbers $p^{\gamma}_{\alpha,\beta}$ are called the *structure constants* of the coherent configuration $(X;\Gamma)$.

For any relation $\gamma \in \Gamma$ and a point $x \in X$ we set

$$\gamma(x) = \{y \in X \mid (x,y) \in \gamma\}.$$

For $\Pi \subset \Gamma$, let $\Pi(x) = \bigcup_{\pi\in\Pi} \pi(x)$.

A coherent configuration $(X;\Gamma)$ is called *homogeneous* if

- (CC5) $\forall_{\gamma\in\Gamma}\forall_{x,y\in X}(|\gamma(x)| = |\gamma(y)|)$.

An *adjacency matrix* $A(\gamma), \gamma \in \Gamma$, is an $X \times X$ matrix whose (x,y)-entry is 1 if $(x,y) \in \gamma$ and 0 otherwise. The complex vector subspace of $M_X(\mathbf{C})$ spanned by the adjacency matrices $A(\gamma), \gamma \in \Gamma$, is a complex matrix algebra of dimension $|\Gamma|$ which is known as *the Bose-Mesner* algebra of $(X;\Gamma)$.

The automorphism group $\mathbf{Aut}(X;\Gamma)$ of a coherent configuration is a subgroup of the symmetric group $\mathbf{S}(X)$ defined as follows

$$\mathbf{Aut}(X;\Gamma) = \{g \in S(X) \,|\, \forall_{\gamma\in\Gamma}(\gamma^g = \gamma)\,\}.$$

We set $\mathrm{Rel}(\Gamma) = \{\bigcup_{\gamma\in\Pi}\gamma \mid \Pi \subset \Gamma\}$. In other words, $\mathrm{Rel}(\Gamma)$ is the set of all binary relations that may be obtained as unions of those belonging to Γ.

If Φ is any set of binary relations defined on X, then by $\langle\langle\Phi\rangle\rangle$ we denote the minimal coherent configuration $(X;\Gamma)$ satisfying the property: $\Phi \in \mathrm{Rel}(\Gamma)$. We say that this configuration is *generated* by Φ. It is uniquely determined by Φ and may be found by an appropriate version of the *Weisfeiler-Leman* method in time $O(|X|^3\log(|X|))$ (see [3]). A version of this algorithm with much higher worst case time-complexity, but which is nevertheless very efficient in the range up to $n = 1000$, is presented in [4].

An equivalence relation $\tau \subset X \times X$ is said to be an equivalence of $(X;\Gamma)$ if $\tau \in \mathrm{Rel}(\Gamma)$. It is called *non-trivial* if the number of equivalence classes is strictly greater than 1 and less than $|X|$. A homogeneous coherent configuration $(X;\Gamma)$ is called *imprimitive* if $\mathrm{Rel}(\Gamma)$ contains a non-trivial equivalence relation. If $\mathrm{Rel}(\Gamma)$ does not contain such a relation, then $(X;\Gamma)$ is said to be *primitive.*

The equivalence classes of an equivalence relation τ coincide with the connected components of the graph $(X;\tau)$. If $(X;\Gamma)$ is homogeneous, then each equivalence class of τ has the same number of elements (see for example [24], page 48). Denote this number by $\nu(\tau)$.

Every basic relation γ of a homogeneous coherent configuration $(X;\Gamma)$ *generates* an equivalence relation $\tau(\gamma) \in \mathrm{Rel}(\Gamma)$. Let $V_1,\ldots,V_{p(\gamma)}$ be the components of (X,γ) and put

$$\Pi(\gamma) = \{\gamma' \,:\, \gamma' \cap (V_i \times V_i) \neq \emptyset\}$$

for some $i \in \{1,\ldots,p(\gamma)\}$. Then $\Pi(\gamma)$ is independent of i and

$$\tau(\gamma) = \bigcup_{\gamma' \in \Pi(\gamma)} \gamma'.$$

The connected components of (X,γ) can be found in time $O(|X| + |\gamma|)$. This implies the validity of the following lemma, which we present here for easy reference in later sections.

Lemma 6.1. *For a homogeneous coherent configuration $(X;\Gamma)$ a list of all equivalence relations generated by basic relations can be computed in time $O(n^2)$.*

We say that a coherent configuration $(X;\Gamma)$ is *circulant* if its automorphism group contains a *full cycle*, *i.e.,* a permutation of the form $g = (x_1,...,x_n)$, where $n = |X|$. The cyclic group $\langle g\rangle$ generated by g acts transitively on X. Therefore, if $(X;\Gamma)$ is circulant then $\mathbf{Aut}e(X;\Gamma)$ is a transitive permutation group and $(X;\Gamma)$ is homogeneous.

For any graph $G = (X,\gamma)$ the coherent configuration generated by $\Phi = \{\gamma\}$ is called the *coherent configuration of* G and denoted by $\langle\!\langle\gamma\rangle\!\rangle$. Note that a graph $G = (X,\gamma)$ is a circulant graph iff its coherent configuration $\langle\!\langle\gamma\rangle\!\rangle$ is circulant. In particular, each basic graph of $\langle\!\langle\gamma\rangle\!\rangle$ is a circulant graph. For this reason, we have to prepare ourselves to deal conveniently with circulant coherent configurations.

6.2 Properties of circulant coherent configurations.

Let $(X;\Gamma)$ be a circulant coherent configuration and $g \in \mathbf{Aut}(X;\Gamma)$ be a full cycle. Fix an arbitrary point $x \in X$ and consider the mapping

$$log_{g,x} : \Gamma \to 2^{\mathbf{Z}_n}$$

defined as follows:

$$log_{g,x}(\gamma) = \{k \in \mathbf{Z}_n \mid (x, x^{g^k}) \in \gamma\}.$$

It is easy to see ([21]) that $log_{g,x}$ does not depend on the choice of the point $x \in X$. Thus we shall write $log_g(\gamma)$ instead of $log_{g,x}(\gamma)$. Obviously, $log_g(\varepsilon_X) = \{0\}$.

It should be mentioned that in general $log_g(\gamma)$ depends on the choice of the full cycle $g \in \mathbf{Aut}(X;\Gamma)$.

Given a subset $T \subset \mathbf{Z}_n$, we define a binary relation $exp_g(T)$ as follows:

$$exp_g(T) = \{(z, z^{g^k}) \mid k \in T, z \in X\}.$$

The following proposition is easy to check (see [21]).

Proposition 6.2. (i) *$exp_g(log_g(\gamma)) = \gamma$, $log_g(exp_g(T)) = T$;*

(ii) *Let $\gamma \neq \sigma \in \Gamma$ be two arbitrary relations. Then $log_g(\gamma) \cap log_g(\sigma) = \emptyset$;*

(iii) *For arbitrary $\gamma \in \Gamma$ we have $log_g(\gamma^t) = -log_g(\gamma)$;*

(iv) *If $A(\gamma), \gamma \in \Gamma$, is the adjacency matrix of $\gamma \in \Gamma$ and P_g is the permutation matrix of g, then $A(\gamma) = \sum_{k \in \log_g(\gamma)} P_g^k$;*

(v) *$\bigcup_{\gamma \in \Gamma} log_g(\gamma) = \mathbf{Z}_n$;*

(vi) *$\gamma \in Rel(\Gamma)$ is an equivalence relation if and only if $log_g(\gamma)$ is a subgroup of $\mathbf{Z}_n$. The classes of an equivalence γ are the connected components of (X, γ). They correspond bijectively to the cosets of $log_g(\gamma)$ in $\mathbf{Z}_n$.*

The mapping log_g assigns to a circulant coherent configuration a certain partition of $\mathbf{Z}_n$. To characterize all partitions obtainable in this way from coherent configurations we need the notion of a Schur ring.

6.3 Schur rings.

Let $\mathbf{H}$ be a finite group written multiplicatively and with identity e. Let $\mathbf{ZH}$ be the group algebra over the ring $\mathbf{Z}$ of integers. Given any subset $T \subset \mathbf{H}$, we denote by $\underline{T}$ the following element of $\mathbf{ZH}$: $\underline{T} = \sum_{t \in T} t$. According to [25] we call such elements *simple quantities.*

Definition.[25] A $\mathbf{Z}$-subalgebra $\mathcal{S} \subset \mathbf{ZH}$ is called *Schur ring* (briefly *S-ring*) over $\mathbf{H}$ if it satisfies the following conditions:

- (S1) There exists a basis of $\mathcal{S}$ consisting of simple quantities $\underline{T}_0, \underline{T}_1, ..., \underline{T}_r$;
- (S2) $T_0 = \{e\}$ and $\cup_{i=0}^r T_i = \mathbf{H}$;
- (S3) $T_i \cap T_j = \emptyset$ if $i \neq j$;
- (S4) For each $i \in \{0, 1, ..., r\}$ there exists $i' \in \{0, 1, ..., r\}$ such that $T_{i'} = \{t^{-1} | t \in T_i\}$.

The basis $\underline{T}_0, ..., \underline{T}_r$ is called the *standard basis* and the simple quantities $\underline{T}_i$ (resp. the sets T_i) are called *basic quantities* (resp. *basic sets*) of $\mathcal{S}$. The notation $\mathcal{S} = \langle \underline{T}_0, ..., \underline{T}_r \rangle$ means that $\underline{T}_0, ..., \underline{T}_r$ is the standard basis of $\mathcal{S}$.

Assume now that an S-ring $\mathcal{S}$ over $\mathbf{H}$ is given. A subset (or subgroup) B of $\mathbf{H}$ is called *$\mathcal{S}$-subset* (*$\mathcal{S}$-subgroup*) if $\underline{B} \in \mathcal{S}$. It is clear that the set of $\mathcal{S}$-subsets is closed under all set-theoretical operations.

For any subset C of the group $\mathbf{H}$ let $\langle\langle C \rangle\rangle$ denote the S-ring *generated* by C, i. e. the smallest S-ring containing $\underline{C}$. An S-ring $\mathcal{S}'$ over the group $\mathbf{H}$ is an *S-subring* of $\mathcal{S}$ defined over the same group $\mathbf{H}$ if $\mathcal{S}' \subset \mathcal{S}$.

For a circulant graph $G = (X, \gamma)$ the S-ring $\langle\langle \gamma(0) \rangle\rangle$ which is generated by the connection set of G is called the *S-ring generated by* G, or shortly, the S-ring of G.

For convenient reference we list here some fundamental properties of S-rings which are proved elsewhere in the literature. Since in the next sections we have to deal with S-rings over $\mathbf{Z}_n$ exclusively, we formulate these properties under the assumption that $\mathbf{H} = \mathbf{Z}_n$.

(S5) For any $B \subseteq \mathbf{Z}_n$ let

$$Stab_+(B) = \{h \in \mathbf{Z}_n \,:\, h + B = B\}$$

(the stabilizer of B). If B is an $\mathcal{S}$-subset, then $Stab_+(B)$ is an $\mathcal{S}$-subgroup.

(S6) For any $B \subseteq \mathbf{Z}_n$ let $\langle B \rangle$ denote the subgroup of $\mathbf{Z}_n$ generated by B. If B is an $\mathcal{S}$-subset, then $\langle B \rangle$ is an $\mathcal{S}$-subgroup.

(S7) For any $\mathcal{S}$-subset B and any $a \in \mathbf{Z}_n^*$ also $aB = \{ab \,:\, b \in B\}$ is an $\mathcal{S}$-subset.

(S8) If two subsets K and L of $\mathbf{Z}_n$ are $\mathcal{S}$-sets then their intersection $K \cap L$ and their differences $K \setminus L$ and $L \setminus K$ are $\mathcal{S}$-sets, too.

Proofs of (S5) - (S8) can be found in [25] (Proposition 23.5, Proposition 23.6, Proposition 23.9).

The connection between Schur rings and cyclic coherent configurations is given by the following statement.

Lemma 6.3. *Let g be an arbitrary cyclic permutation of X. Then the map $\Gamma \mapsto log_g(\Gamma)$ is a bijection between g-invariant coherent configurations and Schur rings over $\mathbf{Z}_n$. Moreover, the map $A(\gamma) \mapsto \underline{log_g(\gamma)}$ defines an isomorphism between the Bose-Mesner algebra of $(X;\Gamma)$ and the Schur ring $\langle \underline{log_g(\gamma)} \rangle_{\gamma\in\Gamma}$.*

Proof. See [21] ☐

As a first consequence of this claim we obtain the following property of circulant coherent configurations.

Proposition 6.4. *If $(X;\Gamma)$ is a circulant coherent configuration, then its Bose-Mesner algebra is commutative.*

A coherent configuration the Bose-Mesner algebra of which is commutative is known as *association scheme* [5]. For this reason we shall call a circulant coherent configuration a *circulant association scheme.*

Proposition 6.5. *Let $(X;\Gamma)$ be a non-trivial circulant association scheme and let $g \in$ $\mathbf{Aut}(\Gamma)$ be a full cycle. Then the following statements hold:*

(i) *$(X;\Gamma)$ is primitive iff $|X|$ is prime.*

(ii) *Assume that $(X;\Gamma)$ is imprimitive and let $\pi \in Rel(\Gamma)$ be a non-trivial equivalence relation. Then each equivalence class $\pi(x), x \in X$ is an orbit of a subgroup $\langle g^{n/d}\rangle$ where $d = |\pi(x)|$.*

(iii) *If $(X;\Gamma)$ is an imprimitive circulant scheme, then it has a unique non-trivial equivalence relation $\tau \in Rel(\Gamma)$ with a maximal number of classes.*

Proof. (i) follows from Theorem 25.3 of [25]. (ii) π is an equivalence relation invariant under $\mathbf{Aut}(X;\Gamma)$. Therefore, π is invariant under the action of $C_n = \langle g\rangle$ which acts regularly on X. Now the claim becomes evident. Part (iii) is a direct consequence of the previous part.

□

Proposition 6.6. *Let $G = (X,\gamma)$ be a circulant graph and g one of its full cycles. Let $\gamma_0,\ldots,\gamma_r$ be the basic relations of its circulant association scheme $\langle\langle\gamma\rangle\rangle$ and $\underline{T_0},\ldots,\underline{T_r}$ the basic quantities of S-ring its $\langle\langle\gamma(0)\rangle\rangle$. Then*

(i) *$\langle\langle\gamma(0)\rangle\rangle = log_g(\langle\langle\gamma\rangle\rangle)$, respectively, $\langle\langle\gamma\rangle\rangle = exp_g(\langle\langle\gamma(0)\rangle\rangle)$.*

(ii) *If G is an undirected graph, then all basic relations are symmetric, i. e. all basic graphs are undirected circulants, and all basic quantities satisfy $T_i = -T_i$.*

Proof. (i) is obvious. (ii) follows easily from the definition of $\langle\langle\gamma\rangle\rangle$.

□

6.4 Proofs

Proof of Lemma 3.1.

1. Since $n \mid (d^{m+1} \pm 1)$, $\frac{d^{m+1}\pm 1}{n}$ is an integer. By assumption $d^m + 1 < n$. Therefore

$$\frac{d^{m+1} \pm 1}{n} < \frac{d^{m+1} \pm 1}{d^m + 1} < d$$

which implies
$$\frac{d^{m+1}\pm 1}{n} \leq d-1 \Rightarrow n \geq \frac{d^{m+1}\pm 1}{d-1}.$$
Thus,
$$n \geq 1+d+d^2+\ldots+d^m.$$

2. (ii) is a direct consequence of (i) which implies $n \geq 2^{m+1} \pm 1$. If n is a proper divisor of $2^{m+1} \pm 1$, then $n < 2^m \pm 1 = d^m \pm 1$, a contradiction to (5).

□

Proof of Lemma 3.2.

Assume $|2\mathbf{H}| < |\mathbf{H}|$. Then obviously $d \geq 3$, n is even and $2\varepsilon_a d^a \equiv_n 2$ for some $\varepsilon_a \in \{1,-1\}$ with $\varepsilon_a d^a \neq 1$. Therefore $n \mid 2(\varepsilon_a d^a - 1) \neq 0$.

If n is a proper divisor of $2(\varepsilon_a d^a - 1)$, then $n \leq |\varepsilon_a d^a - 1| \leq d^m + 1$, which contradicts (5). Hence, $n = 2|\varepsilon_a d^a - 1|$.

If $a \leq m-1$, then $n \leq 2(d^{m-1}+1) < d^m + 2$, again a contradiction. Hence $a = m$ and either $n = 2(d^m - 1)$ or $n = 2(d^m + 1)$.

If $n = 2(d^m - 1)$, $n \,|\, (d^{m+1} - 1)$, then $\frac{n}{2} \mid \gcd(d^m - 1, d^{m+1} - 1) = d - 1$, which implies $m = 1, n = 2(d-1)$, a contradiction to $d \leq \frac{n}{2}$.

If $n = 2(d^m - 1)$, $n \,|\, (d^{m+1} + 1)$ or $n = 2(d^m + 1)$, $n \,|\, (d^{m+1} \pm 1)$, then we have $\frac{n}{2} \mid \gcd(d^m - 1, d^{m+1} + 1) \,|\, d + 1$. Due to (5) this yields $n \,|\, 2(d+1)$ which implies $m = 1, n = 2(d+1)$, a contradiction to $(m,n) \neq (1, 2d+2)$.

□

Proof of Lemma 3.3.

1. Assume $i\mathbf{H} \neq 2\mathbf{H}$. Take an arbitrary $t \in i\mathbf{H}$ and let $(x,y) \in \mathbf{H}^2$ be a pair with $x + y = t$. Since $i\mathbf{H} \cap 2\mathbf{H} = \emptyset$, $x \neq y$ and, therefore, since the pair (y,x) also satisfies $y + x = t$, we always have an even number of solutions which implies $p^{\gamma_i}_{\gamma_1,\gamma_1} \equiv_2 0$.

2. The structure constant $p^{\gamma_2}_{\gamma_1,\gamma_1}$ is equal to the number of ordered pairs $(x,y) \in \mathbf{H}^2$ which satisfy $x + y = 2$. Let $\varepsilon_a d^a + \varepsilon_b d^b \equiv_n 2$ where $\varepsilon_a = \pm 1$, $\varepsilon_b = \pm 1$. Since
$$|\varepsilon_a d^a + \varepsilon_b d^b - 2| \leq 2d^m + 2,$$
and $|\varepsilon_a d^a + \varepsilon_b d^b - 2| = kn$, we have
$$k \leq \frac{2d^m + 2}{n} \leq \frac{2d^m + 2}{d^m + 2} < 2.$$
Therefore either $|\varepsilon_a d^a + \varepsilon_b d^b - 2| = n$ or $\varepsilon_a d^a + \varepsilon_b d^b - 2 = 0$.

Case 1. $|\varepsilon_a d^a + \varepsilon_b d^b - 2| = n$.

If $d = 2$, then by Lemma 3.1 n is odd, and, therefore, either a or b is zero. This implies $2^{m+1} \pm 1 = n = |\varepsilon_a d^a + \varepsilon_b d^b - 2| \leq 2^m + 3$. Since $m = 1$ would imply $n = 2^{m+1} + 1 = 5$ and since (1,2,5) defines the complete graph K_5, it follows that $m = 2$, $n = 2^{m+1} - 1 = 7$. But $(m, d, n) = (2, 2, 7)$ defines the complete graph K_7. This shows that $d = 2$ contradicts the hypothesis if the lemma.

Assume now that $d \geq 3$. If both a and b are at most $m-1$, then $n = |\varepsilon_a d^a + \varepsilon_b d^b - 2| \leq 2d^{m-1} + 2 < d^m + 2$, a contradiction. Assume therefore $a = m$. This implies $n = d^m \pm d^b \pm 2$. If $b = m$, then $2(d^m \pm 1) = n \mid (d^{m+1} \pm 1)$ which implies $m = 1, n = 2d \pm 2$, contradicting either $d \leq \frac{n}{2}$ or $(m, d, n) \neq (1, d, 2d + 2)$. Thus we may assume that $b \leq m - 1$.

If $m = 1$, then $n = d \pm 1 \pm 2 \in \{d+3, d+1, d-1, d-3\}$ which together with $n \geq d^m + 2$ implies $n = d + 3$. But $(d + 3) \mid (d^2 - 1) \iff d = 5 \iff (m, d, n) = (1, 5, 8)$, whereas $(d + 3) \mid (d^2 + 1) \iff d = 7 \iff (m, d, n) = (1, 7, 10)$, such that in both cases we get a contradiction to $d \leq \frac{n}{2}$.

In the remaining case the triple (m, d, n) satisfies the conditions

$$1 + d + ... + d^{m-1} + d^m \leq n = d^m \pm d^b \pm 2,\ b \leq m - 1,$$

$$m \geq 2,\ d \geq 3$$

which imply $m = 2$ and $n = d^2 + d + 2 = 14$, such that $n \mid d^{m+1} + 1$ for $d = 3$. This case is excluded by assumption.

Case 2. $\varepsilon_a d^a + \varepsilon_b d^b - 2 = 0$.

We may assume that $\varepsilon_a = 1$. If $\varepsilon_b = 1$, then $a = 0, b = 0$ is the unique solution. If $\varepsilon_b = -1$, then $d^a = d^b + 2$ which implies that $a > b$, and consequently $2 = d^b(d^{a-b} - 1)$. If $d \geq 4$, then this equation has no solution. If $d = 3$, then it has the unique solution $b = 0, a = 1$, if $d = 2$, then it has the unique solution $b = 1, a = 2$.

Thus we see that under the assumptions of the lemma the equation $2 = x + y, (x, y) \in \mathbf{H}^2$ has the following solutions:
$(1, 1)$ if $d \geq 4$;
$(1, 1), (3, -1), (-1, 3)$ if $d = 3$;
$(1, 1), (4, -2), (-2, 4)$ if $d = 2$.

3. $x \in 2\mathbf{H} \cap (1 + \mathbf{H})$ if and only if there exists $h_1, h_2 \in \mathbf{H}$ such that $x = 2h_1 = 1 + h_2$. Therefore, we have to find all pairs $(h_1, h_2) \in \mathbf{H}^2$ which satisfies $1 = 2h_1 - h_2$, or, equivalently, $2 = h_1^{-1} + h_1^{-1}h_2$. Since $\mathbf{H}$ is a multiplicative group, $h_1, h_2 \in \mathbf{H}$ implies $h_1^{-1} \in \mathbf{H}, h_1^{-1}h_2 \in \mathbf{H}$. All solutions of the equation $2 = x_1 + x_2$, $x_i \in \mathbf{H}$ were found in the

previous part. Using these solutions one can easily finish the proof.

$\square$

Proof of Proposition 3.5.

We distinguish two cases $d = 2$ and $d = 3$.

Case 1. $d = 3$.

According to the remark at the beginning of Subsection 3.2 we may assume $x = 0$, $y = 1$. Then, by Lemma 3.3, $\gamma_2(0) \cap \gamma_1(1) = \{2, \frac{2}{3}, -2\}$.Now

$$\gamma_2(1) \cap \gamma_1(2) = \left\{3, \frac{5}{3}, -1\right\}$$

$$\gamma_2(1) \cap \gamma_1(2/3) = \left\{\frac{7}{9}, \frac{1}{3}, \frac{5}{3}\right\}$$

$$\gamma_2(1) \cap \gamma_1(-2) = \{-1, -5, 7\}$$

If $U = \gamma_2(1) \cap \gamma_1(\frac{2}{3}) \cap \gamma_1(-2) = \emptyset$, then $z_1 = 2$ is the unique point which satisfies (7). Hence, consider the case when U is not empty. Then at least one of the following congruences hold:

$$\begin{array}{lll} \frac{7}{9} \equiv_n -1 & \frac{1}{3} \equiv_n -1 & \frac{5}{3} \equiv_n -1 \\ \frac{7}{9} \equiv_n -5 & \frac{1}{3} \equiv_n -5 & \frac{5}{3} \equiv_n -5 \\ \frac{7}{9} \equiv_n 7 & \frac{1}{3} \equiv_n 7 & \frac{5}{3} \equiv_n 7 \end{array}$$

Therefore, n divides one of the numbers $4, 8, 16, 20, 52, 56$ which implies

$$n \in \{2, 4, 5, 7, 8, 10, 13, 14, 16, 20, 26, 28, 52, 56\}.$$

The conditions $3^m + 1 < n$, $n|(3^{m+1} - 1)$ or $n\,|\,(3^{m+1} + 1)$ and $3 \leq \frac{n}{2}$ imply $n \in \{8, 10, 13, 14, 26, 28\}$. Since, in our case, m is uniquely determined by n, the set U is empty unless

$$(m, d, n) \in \{(1, 3, 8), (1, 3, 10), (2, 3, 13), (2, 3, 14), (2, 3, 26), (2, 3, 28)\}.$$

Thus, our assertion is true for $d = 3$.

Case 2. $d = 2$.

We note that in this case $2\mathbf{H} = \mathbf{H}$. Therefore $\gamma_2 = \gamma_1$. Again, we may assume that $x = 0$, $y = 1$. Then, by Lemma 3.3, $\gamma_2(x) \cap \gamma_1(y) = \{2, \frac{1}{2}, -1\}$. Now

$$\gamma_2(1) \cap \gamma_1(2) = \left\{\frac{3}{2}, 3, 0\right\}$$

$$\gamma_2(1) \cap \gamma_1(-1) = \{-3, 3, 0\}$$

$$\gamma_2(1) \cap \gamma_1(1/2) = \left\{0, \frac{3}{2}, \frac{3}{4}\right\}$$

Our statement is correct if

$$|\gamma_1(1) \cap \gamma_1(\frac{1}{2}) \cap \gamma_1(-1)| \leq 1.$$

If this number is larger than 1, then at least one of the following congruences holds:

$$\begin{array}{ll} \frac{3}{2} \equiv_n -3 & \frac{3}{2} \equiv_n 3 \\ \frac{3}{4} \equiv_n -3 & \frac{3}{4} \equiv_n 3. \end{array}$$

Therefore, n divides one of the numbers 9 and 15, and, consequently, since $n = 3$ is excluded by (5), we have

$$n \in \{5, 9, 15\}.$$

Since $n = 2^{m+1} \pm 1$, the possible triples (m, d, n) are (1,2,5), (2,2,9) and (3,2,15). The first triple defines the complete graph K_5. The remaining two are excluded by assumption. This proves the assertion for $d = 2$.

References

[1] S. B. Akers, Balakrishnan Krishnamurthy, *Group Graphs as Interconnection Networks. Proc. 14th Int. Conf. Fault Tolerant Computing* (1984), 422-427.

[2] S. B. Akers, Balakrishnan Krishnamurthy, *A Group-Theoretical Model for Symmetric Interconnection Networks. IEEE Transactions on Computers* **38** (1989), 555-566.

[3] L. Babel, S. Baumann, M. Lüdecke, G. Tinhofer, *STABCOL: Graph isomorphism testing based on the Weisfeiler-Leman algorithm. Preprint. TUM-M9702, Munich* (1997), 33 pp.

[4] L. Babel, I.V. Chuvaeva, M. Klin, D.V. Pasechnik, *Algebraic Combinatorics in Mathematical Chemistry. Methods and Algorithms. II. Program implementation of the Weisfeiler-Leman algorithm. (A preliminary version). Preprint* TUM-M9701, Munich (1997), 45 pp.

[5] E. Bannai, T. Ito, *Algebraic Combinatorics I, Association Schemes. Benjamin/Cummings*, Menlo Park, 1984.

[6] E. Bannai, Y. S. Song, *Character table of fission schemes and fusion schemes. Europ. J. of Combin.* **14** (1993), 385-396.

[7] O. Bastert, *Stabilization procedures and applications.* Doctoral thesis, Zentrum Mathematik, Technical University Munich, 2000.

[8] A. E. Brouwer, A. M. Cohen, A.Neumaier, *Distance - Regular Graphs. Springer-Verlag*, Berlin, 1989.

[9] P. J. Cameron, J. H. van Lint, *Designs, Graphs, Codes and Their Links.* Cambridge University Press, Cambridge, 1991.

[10] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory. Philips Research Reports Suppl.* **10** (1973).

[11] S. Evdokimov, I. Ponomarenko, *On Primitive Cellular Algebras. Zapiski POMI, 1998*, to appear.

[12] I. A. Faradžev, A. A. Ivanov, M. H. Klin, *Galois correspondence between permutation groups and cellular rings (association schemes). Graphs and Combinatorics* **6** (1992), 202-224.

[13] I. A. Faradžev, M. H. Klin, M. E. Muzychuk, *Cellular rings and groups of automorphisms of graphs.* In: Faradžev I.A. et al. (eds.): *Investigations in algebraic theory of combinatorial objects. Kluwer Acad. Publ.*, Dordrecht, 1994, 1-152.

[14] L. Heydemann, *Cayley Graphs as Interconnection Networks.* In: G. Hahn, G. Sabidussi (eds.), *Graph Symmetry: Algebraic Methods and Applications.* Kluwer, Amsterdam, 1997

[15] D. G. Higman, *Coherent configurations. I. Rend. Sem. Mat. Univ. Padova* **44** (1970), 1-25.

[16] D. G. Higman, *Coherent algebras. Linear Algebra Appl.* **93** (1987), 209-239.

[17] N. Ito, *Tournaments with transitive automorphism group. Europ. J. of Comb.* **5** (1984), 37-42.

[18] M. Ch. Klin, R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the characterization of Schur rings. Report Zentralinst. für Math.und Mech.*, Akademie der Wissenschaften der DDR, Berlin, 1978.

[19] K. H. Leung, S. L. Ma, *On Schur rings over cyclic groups. Israel Journal of Mathematics* **106** (1988), 251-267.

[20] R. McConnel, *Pseudo-ordered polynomial over a finite field. Acta Arith.* **8**, (1963), 127-151.

[21] M. Muzychuk, G. Tinhofer, *Recognizing Circulant Graphs of Prime Order in Polynomial Time. Electronic Journal of Combinatorics*, R25 of Volume **5(1)** (1998).

[22] Jung-Heum Park, Kyung-Yong Chwa, *Recursive Circulant: A New Topology for Multicomputer Networks* (Extended Abstract) *Proc. Internat. Symp. Parallel Architectures, Algorithms and Networks* (ISPAN'94), Japan, IEEE Press, New York, (1994) 73-90.

[23] I. Ponomarenko, *Polynomial-Time Algorithms for Recognizing and Isomorphism Testing of Cyclic Tournaments. Acta Appl. Math.* **29** (1992), 139-160.

[24] B. J. Weisfeiler (Ed.), On construction and identification of graphs, *Springer Lecture Notes* 558 (1976).

[25] H. W. Wielandt, *Finite permutation groups. Academic Press*, N.Y., 1964.