Recognizing circulant graphs of prime order in polynomial time *

Mikhail E. Muzychuk
Netanya Academic College
42365 Netanya, Israel
mikhail@netvision.net.il

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

Submitted: December 19, 1997; Accepted: April 1, 1998

Abstract

A circulant graph G of order n is a Cayley graph over the cyclic group $\mathbf{Z}_n$. Equivalently, G is circulant iff its vertices can be ordered such that the corresponding adjacency matrix becomes a circulant matrix. To each circulant graph we may associate a coherent configuration $\mathcal{A}$ and, in particular, a Schur ring $\mathcal{S}$ isomorphic to $\mathcal{A}$. $\mathcal{A}$ can be associated without knowing G to be circulant. If n is prime, then by investigating the structure of $\mathcal{A}$ either we are able to find an appropriate ordering of the vertices proving that G is circulant or we are able to prove that a certain necessary condition for G being circulant is violated. The algorithm we propose in this paper is a recognition algorithm for cyclic association schemes. It runs in time polynomial in n.

MR Subject Number: 05C25, 05C85, 05E30
Keywords: Circulant graph, cyclic association scheme, recognition algorithm

*The work reported in this paper has been partially supported by the German Israel Foundation for Scientific Research and Development under contract # I-0333-263.06/93

1 Introduction

The graphs considered in this paper are of the form (X, γ), where X is a finite set and γ is a binary relation on X which is not necessarily symmetric.

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

$$\gamma = \{(g, h) \,:\, g, h \in \mathcal{G} \wedge gh^{-1} \in C\}.$$

Then G is called *Cayley graph* over the group $\mathcal{G}$.

Let $\mathbf{Z}_n$, $n \in \mathbf{N}$, stand for a cyclic group of order n written additively. A *circulant graph* G over $\mathbf{Z}_n$ is a *Cayley graph* over this group. 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 $\gamma(i) = i + \gamma(0)$.

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

There are different equivalent characterizations of circulant graphs. One of them is this: A graph G is a circulant graph 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 graph iff a cyclic permutation of its vertices exists which is an automorphism of G.

Cayley graphs, and in particular, circulant graphs have been studied intensively in the literature. These graphs are easily seen to be vertex transitive. In the case of a prime vertex number n circulant graphs are known to be the only vertex transitive graphs. Because of their high symmetry, Cayley graphs are ideal models for communication networks. Routing and weight balancing is easily done on such graphs.

Assume that a graph G on the set $V(G) = \{0, \ldots, n-1\}$ is given by its diagram or by its adjacency matrix, or by some other data structure commonly used in dealing with graphs. How can we decide whether G is a Cayley graph or not? In such a generality, this decision problem seems to be far from beeing tractable efficiently. A recognition algorithm for Cayley graphs would have to involve implicitly checking all finite groups of order n. In the special case of circulant graphs, or in any other case where the group $\mathcal{G}$ is given, we could recognize Cayley graphs by checking all different numberings of the vertex set and comparing the corresponding adjacency matrix with the group table of $\mathcal{G}$. This *ad hoc* procedure is of course not efficient.

To our knowledge the first result towards recognizing circulant graphs can be found in [Pon92] where circulant tournaments have been considered. In the present paper we shall settle the case of a prime number n of vertices, i.e. we shall propose a still somewhat complicated, but nevertheless time-polynomial, method for recognizing arbitrary circulant graphs of prime order. Our method is based on the notions of *coherent configurations* ([Hig70]), the *Bose-Mesner algebra* of which is a *coherent algebra* ([Hig87]) (also called *cellular algebra*, [Wei76]), and *Schur rings* generated by G and on the interrelations between these notions when G possesses a cyclic automorphism. 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. The properties of coherent configurations and Schur rings we have to use in the construction of the recognition algorithm are presented basically in earlier papers of the first author or can be found in the literature. They have been exploited in joint work with the second author for the purpose of this paper.

In order to make this paper self-contained and readable not only for insiders in the theory of coherent configurations we start with a small collection of the basic notions in this theory. This is done in Section 2. In Section 3 we relate cyclic configurations to the corresponding Schur rings and list up the basic facts of these algebraic structures which are used in the remaining sections. In Section 4 the recognition algorithm for cyclic configurations of prime order is discussed. In Section 5 we give a more formal description of our algorithm and a rough estimation of its time complexity. We end up with some examples in order to demonstrate how our algorithm works.

2 Coherent configurations.

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* [Hig87] 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* and their graphs are called *basic graphs* of $(X;\Gamma)$.

For arbitrary two relations $\gamma,\rho\in\Gamma$ we define the *product* $\gamma\rho$ by

$$\gamma\rho=\{(x,y)\,|\,\exists z:(x,z)\in\gamma\wedge(z,y)\in\rho\}.$$

We shall write γ^2 for $\gamma\gamma$.

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

In the case of $(X;\Gamma)$ being homogeneous we write Γ^* for $\Gamma\setminus\{\varepsilon_X\}$.

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. Suppose that $\Gamma=\{\gamma_0,\gamma_1,\dots,\gamma_t\}$ with $\gamma_0=\varepsilon_X$. The matrix

$$Adj((X;\Gamma))=\sum_{i=0}^{t}i\cdot A(\gamma_i)$$

is called the *adjacency matrix* of $(X;\Gamma)$.

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* $\mathrm{Aut}(X;\Gamma)$ is a subgroup of the symmetric group $\mathrm{Sym}(X)$ defined as follows

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

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. We say that a coherent configuration $(X;\Pi)$ is a *fusion* of a coherent configuration $(X;\Gamma)$ (and $(X;\Gamma)$ is called a *fission* of $(X;\Pi)$) if $\mathrm{Rel}(\Pi)\subset\mathrm{Rel}(\Gamma)$ (see [BaI84]). The relation $\mathrm{Rel}(\Pi)\subset\mathrm{Rel}(\Gamma)$ is a partial ordering on the set of all coherent configurations defined on X.

An equivalence relation $\tau\subset X^2$ is said to be *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*.

If Φ is any set of binary relations defined on X, then by $(X;\langle\Phi\rangle)$ we denote the minimal coherent configuration $(X;\Gamma)$ satisfying the property: $\Phi\in\mathrm{Rel}(\Gamma)$. Such a configuration is unique and may be found by the *Weisfeiler-Leman* algorithm in time $O(|X|^3\log(|X|))$ (see [BBLT97]). A version of this algorithm with much higher time-complexity, but nevertheless very efficient in the range up to $n=1000$, is presented in [BCKP97].

For any $Y\subset X$ and $\gamma\in\Gamma$ we define $\Gamma_Y=\{\gamma\cap(Y\times Y)\ \mid\gamma\in\Gamma\}$. Given a point $x\in X$ and $\gamma\in\Gamma$, one can consider the coherent configuration $(\gamma(x);\langle\Gamma_{\gamma(x)}\rangle)$. In what follows we shall denote this configuration as $(\gamma(x);\Gamma^{\gamma(x)})$.

We say that a coherent configuration $(X;\Gamma)$ is *cyclic* 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 C_n generated by g acts transitively on X. Therefore, $\mathrm{Aut}(X;\Gamma)$ is a transitive permutation group and $(X;\Gamma)$ is homogeneous.

Note that a graph $G=(X,\gamma)$ is a circulant graph iff the coherent configuration $(X;\langle\{\gamma\}\rangle)$ is cyclic. Therefore, the main question considered in this paper can be reformulated in the following way:

Find an algorithm with time-complexity polynomial in $|X|$ that answers the question: Is a given homogenous coherent configuration cyclic?

To create such an algorithm one has first to study the properties of cyclic coherent configurations.

3 Properties of cyclic coherent configurations.

Let $(X;\Gamma)$ be a cyclic coherent configuration and $g\in\mathrm{Aut}(X;\Gamma)$ 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:

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

Proposition 3.1 *The mapping $log_{g,x}$ does not depend on the choice of the point $x\in X$.*

Proof. Take an arbitrary relation $\gamma\in\Gamma$ and two points $x,y\in X$. Clearly, $y=x^{g^l}$ for a suitable $l\in\mathbf{Z}_n$. By definition

$$k\in log_{g,x}(\gamma)\Leftrightarrow(x,x^{g^k})\in\gamma$$

Since $g \in Aut(X;\Gamma)$,

$$(x, x^{g^k}) \in \gamma \Leftrightarrow (x^{g^l}, x^{g^{k+l}}) \in \gamma \Leftrightarrow (y, y^{g^k}) \in \gamma \Leftrightarrow k \in log_{g,y}(\gamma)$$

finishing the proof. $\diamondsuit$

Thus we shall write $log_g(\gamma)$ instead of $log_{g,x}(\gamma)$. An easy check shows that $log_g(\varepsilon_X) = \{0\}$, where ε_X is the identical relation on X.

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

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.

Proposition 3.2 (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) *$\gamma \in \mathrm{Rel}(\Gamma)$ is an equivalence relation if and only if $log_g(\gamma)$ is a subgroup of $\mathbf{Z}_n$.*

The mapping log_g assigns to a cyclic 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.

3.1 Schur rings.

Let H be a finite group written multiplicatively and with identity e. Let $\mathbf{Z}H$ be the group algebra over the ring $\mathbf{Z}$ of integers. Given any subset $T \subset H$, we denote by $\underline{T}$ the following element of $\mathbf{Z}H$: $\underline{T} = \sum_{t \in T} t$. According to [Wie64] we call such elements *simple quantities.*

Definition.[Wie64] A $\mathbf{Z}$-subalgebra $\mathcal{S} \subset \mathbf{Z}H$ is called *Schur ring* (briefly *S-ring*) over 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 $\cup_{i=0}^{r} T_i = H$;
- (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 $\mathcal{S}$. We say that a subset $R \subset \mathbf{Z}_n$ *belongs* to an S-ring $\mathcal{S}$ if $\underline{R} \in \mathcal{S}$. It is clear that an S-ring $\mathcal{S}$ is closed under all set-theoretical operations over the subsets belonging to $\mathcal{S}$. An S-ring $\mathcal{S}'$ over the group H is an *S-subring* of an S-ring $\mathcal{S}$ defined over the same group H if $\mathcal{S}' \subset \mathcal{S}$.

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

Lemma 3.3 *Let $g \in \mathrm{Sym}(X)$ be an arbitrary full cycle and $(X; \Gamma)$ be a g-invariant coherent configuration. 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.
It follows from Proposition 3.2 that the sets $\log_g(\gamma)$ form a partition of $\mathbf{Z}_n$. Thus we have to check that the $\mathbf{Z}$-module $\mathrm{sp}\{\underline{\log_g(\gamma)}\}_{\gamma \in \Gamma}$ is closed with respect to the group algebra multiplication.

Let $\alpha, \beta, \gamma \in \Gamma$ be an arbitrary triple of basic relations. Take an arbitrary $k \in \log_g(\gamma)$. To each pair $u \in \log_g(\alpha)$, $v \in \log_g(\beta)$ that satisfies $u + v = k$ one can associate a triple of points x, x^{g^u}, x^{g^k}. Clearly $(x, x^{g^u}) \in \alpha$, $(x^{g^u}, x^{g^k}) \in \beta$ and $(x, x^{g^k}) \in \gamma$. Thus the number of solutions of the equation $u + v = k$ where $u \in \log_g(\alpha)$, $v \in \log_g(\beta)$ does not depend on the choice of $k \in \log_g(\gamma)$ and is equal to $p_{\alpha,\beta}^{\gamma}$. Therefore, $\mathrm{sp}\{\underline{\log_g(\gamma)}\}_{\gamma \in \Gamma}$ is closed with respect to the group algebra multiplication and its structure constants coincide with those of the Bose-Mesner algebra of Γ. Hence

$$A(\gamma) \mapsto \underline{\log_g(\gamma)}$$

induces an isomorphism between the algebras. $\diamondsuit$

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

Proposition 3.4 *If $(X; \Gamma)$ is a cyclic 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* [BaI84]. For this reason we shall call a cyclic coherent configuration a *cyclic association scheme.*

Proposition 3.5 *Let* $(X;\Gamma)$ *be a non-trivial cyclic association scheme and let* $g \in \mathrm{Aut}(\Gamma)$ *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* $\pi \in \mathrm{Rel}(\Gamma)$ *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 cyclic scheme, then it has a unique non-trivial equivalence relation* $\tau \in \mathrm{Rel}(\Gamma)$ *with a maximal number of classes.*

Proof. (i) follows from Theorem 25.3 of [Wie64]. (ii) π is an equivalence relation invariant under $\mathrm{Aut}(X;\Gamma)$. 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. $\diamondsuit$

3.2 Cyclic association schemes of prime degree.

In this subsection we assume that $|X| = p$, where p is a prime. The structure of all cyclic schemes of prime degree is well-known since 1978 (see [KliP78]). To describe it we identify X with a finite field $\mathbf{F}_p$. We also assume that the full cycle $g = (0, 1, ..., p-1)$ is an automorphism of our scheme. Clearly, $x^g = x + 1$, $x \in \mathbf{F}_p$.

Fix an arbitrary subgroup $M \leq \mathbf{F}_p^*$, $|M| = d$. Then $\mathbf{F}_p^*$ is a union of M-cosets:

$$\mathbf{F}_p^* = Mt_1 \cup ... \cup Mt_r,\ t_1 = 1,\ r = (p-1)/d.$$

For each Mt_i we set $\gamma_i = \{(x, y) \mid x - y \in Mt_i\}$.

Theorem 3.1

(i) *The set* $\Gamma_M = \{\varepsilon_X, \gamma_1, ..., \gamma_r\}$ *of binary relations forms a cyclic association scheme on* $\mathbf{F}_p$, $g \in \mathrm{Aut}(\mathbf{F}_p;\Gamma_M)$.

(ii) $\mathrm{Aut}(\mathbf{F}_p;\Gamma_M) = \mathrm{Aff}(M, \mathbf{F}_p)$, *where* $\mathrm{Aff}(M, \mathbf{F}_p)$ *is the group of all permutations of the form* $f(x) = mx + a, m \in M, a \in \mathbf{F}_p$.

(iii) *Every cyclic association scheme* $(\mathbf{F}_p;\Gamma)$ *with* $g \in \mathrm{Aut}(\mathbf{F}_p;\Gamma)$ *coincides with* $(\mathbf{F}_p;\Gamma_M)$ *for a suitable* $M \leq \mathbf{F}_p^*$.

(iv) *The graphs* $(\mathbf{F}_p, \gamma_i), i = 1, ..., r$ *are pairwise isomorphic.*

(v) *The graph* $(\mathbf{F}_p, \gamma_1)$ *is symmetric if and only if* $|M|$ *is even.*

(vi) $(\mathbf{F}_p; \Gamma_M)$ *is a fusion scheme of* $(\mathbf{F}_p; \Gamma_{M'})$ *if and only if* $M' \leq M$.

Proof.
(i) Γ_M is the set of 2-orbits (= orbitals) of $\mathrm{Aff}(M, \mathbf{F}_p)$.
(ii) See [McC63], [FarIK92].
(iii) This follows from the classifications of S-rings over $\mathbf{F}_p$, see [FarIK92].
(iv) - (vi) These statements are trivial conclusions from (i) - (iii). $\diamondsuit$

The claim below contains the main properties of the association schemes $(\mathbf{F}_p; \Gamma_M)$, $M \leq \mathbf{F}_p^*$.

Lemma 3.6 *Assume* $M \leq \mathbf{F}_p^*$, $1 < |M| < p-1$. *For any* $x \in \mathbf{F}_p$ *and* $\gamma \in \Gamma_M^*$

(i) *all coherent configurations* $(\gamma(x); (\Gamma_M)^{\gamma(x)})$ *are pairwise isomorphic and*

(ii) *if* $|M| > 2$, *then* $(\gamma(x); (\Gamma_M)^{\gamma(x)})$ *is a non-trivial cyclic association scheme.*

Proof.
(i) Since $\mathrm{Aut}(\mathbf{F}_p; \Gamma_M)$ is transitive, $(\gamma(x); (\Gamma_M)^{\gamma(x)})$ and $(\gamma(y); (\Gamma_M)^{\gamma(y)})$ are isomorphic for any pair $x, y \in \mathbf{F}_p$. Thus we have to show that

$$(\gamma_1(0); (\Gamma_M)^{\gamma_1(0)}) \cong (\gamma_i(0); (\Gamma_M)^{\gamma_i(0)})$$

for each $i = 1, ..., r$. Take the permutation $x \to xt_i$. A direct check shows that $\gamma_1^{t_i} = \gamma_i$ and $\forall_{\gamma_j \in \Gamma}(\gamma_j^{t_i} \in \Gamma)$. Therefore, $(\gamma_1(0); (\Gamma_M)^{\gamma_1(0)})^{t_i} = (\gamma_i(0); (\Gamma_M)^{\gamma_i(0)})$, as desired.

(ii) It is enough to prove this part only for $\gamma = \gamma_1$ and $x = 0$. In this case $\gamma_1(0) = M$ and $(\gamma_1(0); (\Gamma_M)^{\gamma_1(0)}) = (M; (\Gamma_M)^M)$. Let us write Γ_M^0 instead of $(\Gamma_M)^M$.

The point stabilizer $(\mathrm{Aut}(\mathbf{F}_p; \Gamma_M))_0$ is a subgroup of $\mathrm{Aut}(M; \Gamma_M^0)$. It consists of all permutations of the form $x \to mx, m \in M$. Since $(\mathrm{Aut}(\mathbf{F}_p; \Gamma_M))_0$ acts regularly on M, $\mathrm{Aut}(M; \Gamma_M^0)$ contains a regular subgroup isomorphic to M. Since M is cyclic, $(M; \Gamma_M^0)$ is a cyclic association scheme.

To finish the proof we have to show that $(M; \Gamma_M^0)$ is non-trivial. Assume the contrary, *i.e.*, assume that $(M; \Gamma_M^0)$ has only two basic relations: ε_M and $M^2 \setminus \varepsilon_M$. Take $\gamma_i \in \Gamma^*$ such that $\gamma_i \cap M^2 \setminus \varepsilon_M \neq \emptyset$. Then, $\gamma_i \cap M^2 = M^2 \setminus \varepsilon_M$.

Take an arbitrary point $m \in M = \gamma_1(0)$. Then $(0, m) \in \gamma_1$. For each $m' \in \gamma_1(0)$ such that $m' \neq m$ we have that $(0, m') \in \gamma_1$ and $(m', m) \in \gamma_i$. Therefore,

$$p_{\gamma_1, \gamma_i}^{\gamma_1} = |M| - 1.$$

Since γ_i is of degree $|M|$, for each $m \in M$ there is a $z_m \notin M$ such that $\gamma_i(m) = M \setminus \{m\} \cup \{z_m\}$. Fix $m \in M$. From $p^{\gamma_1}_{\gamma_1,\gamma_i} = |M|-1$ it follows that for every $a \in \gamma_1^t(m)$ there is a $y_a \in M \setminus \{m\}$ such that $\gamma_1(a) = M \setminus \{y_a\} \cup \{z_m\}$. Moreover, $y_a \neq y_{a'}$ for $a \neq a'$ (for otherwise $\mathbf{F_p}$ would have a non-trivial subgroup). This implies that every two elements $m, m' \in M$ have exactly $|M|-1$ joint predecessors with respect to γ_1. From this it follows

$$p^{\gamma_i}_{\gamma_1^t,\gamma_1} = |M| - 1,$$

and

$$A(\gamma_1^t)A(\gamma_1) = |M|I_X + (|M|-1)A(\gamma_i) \tag{1}$$

where I_X is the unit matrix. Now the proof is completed by applying Theorem 2.3.10(i) from [FarKM94]. According to this theorem we have

$$|M| - 1 \leq \frac{|M|}{2}$$

which is true only for $|M| \leq 2$, a contradiction to our hypothesis.

4 How to recognize cyclic coherent configurations.

Let $(X;\Gamma)$ be a homogeneous coherent configuration with $|X| = p$, p a prime. We shall present a method for finding a full cyclic automorphism of $(X;\Gamma)$, provided this configuration is cyclic.

We set $r := |\Gamma| - 1$. If some relations have different valencies, then $(X;\Gamma)$ is not cyclic. Thus we may assume that $|\gamma(x)| = d, d = (p-1)/r$ for all $\gamma \in \Gamma$. The case $d = 1$ is trivial. In this case each basic graph (X, γ_i) is a full cycle which defines a full cyclic automorphism. Hence, assume $1 < d < p-1$. There are two possible cases: d is composite and d is prime.

4.1 Case of d being composite.

If $(X;\Gamma)$ is a cyclic scheme corresponding to a subgroup $M \leq \mathbf{F}_p^*$, then it is a fusion of a cyclic scheme $(X;\Gamma')$ corresponding to some proper subgroup $M' \leq M, 1 < |M'| < |M|$ which exists, since $|M|$ is not prime.

The main idea is to build the fission (see [BaS93]) scheme $(X;\Gamma')$ by purely combinatorial methods and to apply the algorithm to a new scheme.

Step 1.
For each point $x \in X$ and each $\gamma \in \Gamma^*$ we compute, using the WL-algorithm, $(\gamma(x);\Gamma^{\gamma(x)})$. If $(\gamma(x);\Gamma^{\gamma(x)})$ is not homogeneous, then the initial scheme is not cyclic. Thus we may assume that $(\gamma(x);\Gamma^{\gamma(x)})$ is homogeneous for all $x \in X$.

If $(X;\Gamma)$ is cyclic, then, by Lemma 3.6, $(\gamma(x);\Gamma^{\gamma(x)})$ is a non-trivial cyclic scheme. Since $|M|$ is composite, $(\gamma(x);\Gamma^{\gamma(x)})$ is imprimitive and, therefore, there exists a unique equivalence relation $\tau_{x,\gamma} \in \mathrm{Rel}(\Gamma^{\gamma(x)})$ with a maximal number of classes (Proposition 3.5(ii)). The schemes $(\gamma(x);\Gamma^{\gamma(x)}), x \in X, \gamma \in \Gamma^*$ should be pairwise isomorphic. Therefore, the number of classes of $\tau_{x,\gamma}$ should not depend on the choice of $x \in X, \gamma \in \Gamma^*$.

Step 2.
For each $x \in X$ and $\gamma \in \Gamma^*$ we find a nontrivial equivalence relation $\tau_{x,\gamma} \in \mathrm{Rel}(\Gamma^{\gamma(x)})$ with a maximal number of classes. If for some pair x,γ the scheme $(\gamma(x);\Gamma^{\gamma(x)})$ has more than one such equivalence relation, then the initial scheme is not cyclic. If there are two pairs $(x,\gamma) \neq (x',\gamma')$ such that $\tau_{x,\gamma}$ and $\tau_{x',\gamma'}$ have different number of classes, then $(X;\Gamma)$ is not cyclic. So we may assume that $\tau_{x,\gamma}$ always has s classes of cardinality $d', sd' = d$. Since $\tau_{x,\gamma}$ should be non-trivial, $1 < d' < d$.

Every $\tau_{x,\gamma}$ is an equivalence relation on $\gamma(x)$. For each $x \in X$ we define an equivalence relation of X by setting

$$\tau_x = \bigcup_{\gamma\in\Gamma^*} \tau_{x,\gamma} \cup \{(x,x)\}. \qquad (2)$$

It follows from the definition that each equivalence class of τ_x distinct from $\{x\}$ contains exactly d' elements.

Proposition 4.1 *Assume $(X;\Gamma) \cong (\mathbf{F}_p;\Gamma_M), |M| = d$. Let $M' < M$ be the unique subgroup of order d'. Then for each $x \in \mathbf{F}_p$ the equivalence relation τ_x has the following form:*

$$\tau_x = \bigcup_{\gamma'\in\Gamma_{M'}} (\gamma'(x) \times \gamma'(x)).$$

Proof. Since $\mathrm{Aut}(\mathbf{F}_p;\Gamma_M)$ is transitive, we may assume $x = 0$. Let $(y,z) \in \tau_0$ be an arbitrary pair. Since the case $y = z = 0$ is trivial, we may assume that $y \neq 0 \neq z$. By definition of τ_x, there exists $\gamma \in \Gamma_M$ such that $y,z \in \gamma(0)$ and $(y,z) \in \tau_{0,\gamma}$. $(\mathrm{Aut}(X;\Gamma))_0$ is a cyclic subgroup of $\mathrm{Aut}(\gamma(0);\Gamma^{\gamma(0)})$ of order d. Its generator g is a product $g_1 \cdot \ldots \cdot g_r$ of $r = (p-1)/d$ disjoint cycles of the same length d. Thus $\gamma(0)$ is an orbit of a suitable group $\langle g_i\rangle$. WLOG we may assume that $\gamma(0)$ is an orbit of $\langle g_1\rangle$. Thus g_1 is a full cyclic automorphism of $(\gamma(0);\Gamma^{\gamma(0)})$. According to Proposition 3.5(ii) each equivalence class of $\tau_{0,\gamma}$ is an orbit of $\langle g_1^{d/d'}\rangle$. Hence the equivalence classes of $\tau_{0,\gamma}$ are the orbits of $\langle g_1^{d/d'}\rangle$, and, therefore, they are orbits of $\langle g^{d/d'}\rangle$. Thus, each equivalence class of τ_0 is an orbit of $\langle g^{d/d'}\rangle$. Since $g^{d/d'}$ is of order d', it generates M'. But the orbits of M' on $\mathbf{F}_p$ are exactly the sets $\gamma'(0), \gamma' \in \Gamma_{M'}$. $\diamondsuit$

Our next step is to show that the set $\{\tau_x\}_{x\in X}$ defines the association scheme $(\mathbf{F}_p;\Gamma_{M'})$ uniquely.

Lemma 4.2 *Let $(X;\Psi)$ be a primitive association scheme. Assume that all nontrivial valencies of Ψ are strictly greater than 1.*[1] *For each $x \in X$ we define an equivalence relation τ_x as follows*

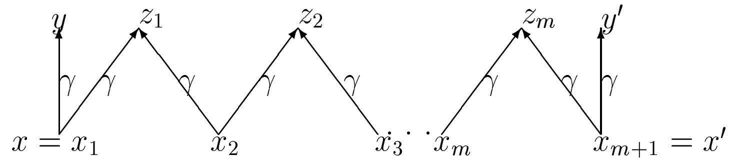
$$\tau_x = \bigcup_{\gamma \in \Psi^*} (\gamma(x) \times \gamma(x)).$$

Let Φ be a graph with node set $X^2 \setminus \varepsilon_X$ and with two nodes $(x,y),(z,w) \in X^2 \setminus \varepsilon_X$ connected by an edge iff either $x = z \wedge (y,w) \in \tau_x$ or $y = w \wedge (x,z) \in \tau_y$. Then the set of connected components of Φ coincides with the set of relations Ψ^*.

Proof. Let (x,y) and (z,w) be two nodes connected by an edge in Φ, If $x = z$, then $y, w \in \gamma(x)$ for some $\gamma \in \Psi^*$, or, equivalently, $(x,y),(z,w) \in \gamma$. If $w = y$, then $x, z \in \beta(y)$ for some $\beta \in \Psi^*$ implying $(x,y),(z,w) \in \beta^t$. Thus, any two nodes $(x,y),(z,w)$ connected by an edge in Φ lie at the same relation $\gamma \in \Psi^*$. Therefore, each relation from Ψ^* is a union of connected components of Φ.

Take now $(x,y),(x',y') \in \gamma \in \Psi^*$ and show that there exists a path in Φ starting in (x,y) and finishing at (x',y').

Since γ is non-trivial of valency greater than 1, $\gamma\gamma^t$ is a non-identical symmetric relation. Therefore $\gamma\gamma^t$ is connected and there exists a path $x = x_1, ..., x_{m+1} = x'$ with $(x_i, x_{i+1}) \in \gamma\gamma^t, i = 1, ..., m$. Since $(x_i, x_{i+1}) \in \gamma\gamma^t$, there exists $z_i \in X$ such that $(x_i, z_i) \in \gamma$, $(x_{i+1}, z_i) \in \gamma$. But now we have the following path in Φ :



$\diamondsuit$

Step 3.
For each $x \in X$ we build an equivalence relation according to formula (2). After that we find connected components of the graph $(X^2 \setminus \varepsilon_X; \Phi)$ defined in Lemma 4.2. If these components don't form an association scheme on X, then $(X;\Gamma)$ is not cyclic. Otherwise we obtain a new association scheme $(X;\Gamma')$. If there is a relation $\gamma' \in \Gamma'$ whose valency is not equal to d', then $(X;\Gamma)$ is not cyclic.

Suppose that all non-trivial relations of Γ' are of valency d'. If d' is composite, then we go to Step 1. If d' is prime, then we apply another method which is described in the next subsection.

4.2 Case of d being prime.

If $d = 2$, then the graph of every $\gamma \in \Gamma^*$ should be a non-oriented p-cycle. So, if some of these graphs has not this property, then the scheme is not cyclic. If all the

[1] A primitive association scheme that contains a basic relation of valency 1 is isomorphic to the full cyclic scheme on a prime number of points.

basic graphs are non-oriented cycles, then by orienting one of them we obtain the automorphism we searched for. Thus we may assume that d is odd. In this case, by Theorem 3.1(v), $\gamma \neq \gamma^t$ for all $\gamma \in \Gamma^*$.

Proposition 4.3 *Let $M \leq \mathbf{F}_p^*$ be a subgroup of odd order. Then for each $a \in \mathbf{F}_p$ the mapping i_a defined by $x^{i_a} = 2a - x$, $x \in \mathbf{F}_p$ is the only involution from* $\mathrm{Sym}(\mathbf{F}_p)$ *satisfying*

(i) $a^{i_a} = a$;

(ii) $\forall_{\gamma \in \Gamma}(\gamma^{i_a} = \gamma^t)$;

Proof. By direct check we can see that i_a really satisfies (i) and (ii). Let now $j \in S(\mathbf{F}_p)$ be an involution that satisfies (i) and (ii). Then $i_a j$ is an automorphism of $(\mathbf{F}_p; \Gamma_M)$. Therefore, $i_a j \in \mathrm{Aff}(M, \mathbf{F}_p)$, implying $j \in \mathrm{Aff}(\mathbf{F}_p^*, \mathbf{F}_p)$. That means there exist $b, c \in \mathbf{F}_p, b \neq 0$ such that $x^j = bx + c, x \in \mathbf{F}_p$. Since j is an involution that fixes a, we find $b = -1, c = 2a$. $\diamond$

The main idea of the algorithm is to reconstruct the involution $i_a, a \in X$ by purely combinatorial methods. After that we multiply i_a with i_b for some $b \neq a$. If the product is a full cycle that belongs to $\mathrm{Aut}(X; \Gamma)$, then we are done. Otherwise $(X; \Gamma)$ is not a cyclic scheme.

Let now d be an odd prime and $(X; \Gamma)$ be a homogeneous coherent configuration, with $|\gamma(x)| = d$ for all $\gamma \in \Gamma^*$ and $x \in X$. Since the order and the valency of each $\gamma \in \Gamma$ are odd, Γ does not contain symmetric relations. So $\gamma \neq \gamma^t$ for all $\gamma \in \Gamma^*$. Fix an arbitrary point $a \in X$ and set $\overline{\gamma}(a) = \gamma(a) \cup \gamma^t(a)$. For each $\beta \in \Gamma^*$ we define the binary relation $\widehat{\beta} \subset (\overline{\gamma}(a))^2$ as follows

$$\widehat{\beta} = \beta \cap (\gamma(a) \times \gamma^t(a)).$$

By $\Phi(a, \gamma)$ we denote the following set of binary relations on $\overline{\gamma}(a)$:

$$\Phi(a, \gamma) = \{\varepsilon_{\overline{\gamma}(a)}, (\gamma(a))^2 \cup (\gamma^t(a))^2\} \cup \{\widehat{\beta} \cup (\widehat{\beta})^t\}_{\beta \in \Gamma^*}.$$

Proposition 4.4 *If $(X; \Gamma) \cong (\mathbf{F}_p; \Gamma_M)$, $|M| = d$, d is odd, then the coherent configuration $(\overline{\gamma}(a); \langle \Phi(a, \gamma) \rangle)$ is cyclic.*

Proof. The stabilizer $G_a := (\mathrm{Aut}(\mathbf{F}_p; \Gamma_M))_a$ consists of all permutations of the form $x \mapsto m(x - a) + a, m \in M$, and, therefore is a cyclic group of odd order d. Since i_a centralizes G_a, the group $\langle G_a, i_a \rangle$ is cyclic of order $2d$. Note that, if $\bar{m} \in M$ is a generator of M, then the mapping $x \to -\bar{m}(x - a) + a$ is a generator of $\langle G_a, i_a \rangle$. The orbits on $\mathbf{F}_p \setminus \{a\}$ of this group coincides with the sets $\overline{\gamma}(a), \gamma \in \Gamma^*$.

We claim that every relation from $\Phi(a, \gamma)$ is invariant under the group $\langle G_a, i_a \rangle$. Indeed, the invariance under G_a follows immediately from the definition of the set

$\Phi(a,\gamma)$.

Since $\overline{\gamma}(a)$ is i_a-invariant, $\varepsilon_{\overline{\gamma}(a)}^{i_a} = \varepsilon_{\overline{\gamma}(a)}$. By Proposition 4.3 $\gamma^{i_a} = \gamma^t$, therefore $((\gamma(a))^2 \cup (\gamma^t(a))^2)^{i_a} = ((\gamma(a))^2 \cup (\gamma^t(a))^2)$. All other relations from $\Phi(a,\gamma)$ are of the form $\widehat{\beta} \cup \widehat{\beta}^t$, where $\widehat{\beta} = \beta \cap (\gamma(a) \times \gamma^t(a))$. Therefore

$$\widehat{\beta}^{i_a} = \beta^{i_a} \cap (\gamma(a) \times \gamma^t(a))^{i_a} = \beta^t \cap (\gamma^t(a) \times \gamma(a)) = (\widehat{\beta})^t,$$

implying that $\widehat{\beta} \cup \widehat{\beta}^t$ is i_a-invariant.

Thus we have shown that all relations from $\Phi(a,\gamma)$ are invariant under the action of the cyclic group $\langle G_a, i_a \rangle$. Since the latter group acts transitively on the set $\overline{\gamma}(a)$, the coherent configuration $(\overline{\gamma}(a); \langle \Phi(a,\gamma) \rangle)$ is cyclic. $\diamondsuit$

The algorithm for the case of d being prime is based on the following claim.

Theorem 4.1 *If $(X;\Gamma) \cong (\mathbf{F}_p;\Gamma_M)$, $|M| = d$, d an odd prime, then for any $a \in \mathbf{F}_p$ and any $\gamma \in \Gamma^*$ the relation*

$$\pi_{a,\gamma} = i_a \cap (\overline{\gamma}(a))^2$$

(where i_a is viewed as $\{(x, x^{i_a}) \,|\, x \in \mathbf{F}_p\}$) is the unique basic relation ρ of the coherent configuration $(\overline{\gamma}(a); \langle \Phi(a,\gamma) \rangle)$ that satisfies the equality $\rho^2 = \varepsilon_{\overline{\gamma}(a)}$.

In order to prove this result we need two additional statements.

Proposition 4.5 *Let $(\mathbf{F}_p;\Gamma_M)$, $M \leq \mathbf{F}_p^*, |M| > 1$ be a non-trivial cyclic association scheme. Then for each point $a \in \mathbf{F}_p$ and any pair of non-trivial relations $\alpha, \beta \in \Gamma_M$ $(\alpha(a) \times \beta(a)) \not\subset \gamma$ for every $\gamma \in \Gamma_M$.*

Proof. Assume the contrary, *i.e.*, $(\alpha(a) \times \beta(a)) \subset \gamma$ for some $a \in \mathbf{F}_p$ and $\alpha, \beta, \gamma \in \Gamma_M$. Then $p_{\alpha,\gamma}^{\beta} = d$, implying $A(\alpha)A(\gamma) = d\,A(\beta)$. According to Lemma 2.3.8 of [FarKM94] the scheme $(\mathbf{F}_p;\Gamma_M)$ should be imprimitive in this case, a contradiction. $\diamondsuit$

Proposition 4.5 follows also from a more general statement in [EvdP98], Lemma 5.8.

Proposition 4.6 *Let $\mathcal{S} = \langle \underline{T}_0, ..., \underline{T}_r \rangle$ be an S-ring over $\mathbf{Z}_{2d}$ with d an odd prime. Let $H = 2\mathbf{Z}_{2d}$ and assume that $\underline{H} \in \mathcal{S}$ and $\mathbf{Z}_{2d} \setminus H$ is not a basic set of $\mathcal{S}$. Then $\underline{\{d\}} \in \mathcal{S}$.*

Proof. Let T be a basic set that contains the element $d \in \mathbf{Z}_{2d}$. Since d is odd we have $T \setminus H \neq \emptyset$. This implies $T \cap H = \emptyset$. Further, we have $m \cdot d = d$ for each $m \in \mathbf{Z}_{2d}^*$. Therefore $mT \cap T \neq \emptyset$ for all $m \in \mathbf{Z}_{2d}^*$. By Theorem 23.9 of [Wie64], mT is a basic set of $\mathcal{S}$. Hence $mT = T$ for every $m \in \mathbf{Z}_{2d}^*$. Note that $\mathbf{Z}_{2d} \setminus H = \mathbf{Z}_{2d}^* \cup \{d\}$. It follows that $1 \in T$ would imply $T = \mathbf{Z}_{2d} \setminus H$, which contradicts our assumption. Thus, $1 \notin T$. However, $x \in T$, $x \neq d$ implies $x \in \mathbf{Z}_{2d}^*$, and therefore $x^l \in T$ for arbitrary l. This contradicts $1 \notin T$. Thus, $T = \{d\}$, as desired. $\diamondsuit$

Now we are ready to prove Theorem 4.1.

Proof of Theorem 4.1. According to Proposition 4.4, $(\overline{\gamma}(a); \langle\Phi(a,\gamma)\rangle)$ is a cyclic coherent configuration on $2d$ points. Let g be a generator of the cyclic group $\langle\overline{G}_a, \overline{i}_a\rangle$ (here $^-$ means the restriction on the subset $\overline{\gamma}(a)$) and let $\mathcal{S} = log_g(\langle\Phi(a,\gamma)\rangle)$ be the corresponding S-ring over $\mathbf{Z}_{2d}$. Since $\langle\Phi(a,\gamma)\rangle$ contains the equivalence relation $(\gamma(a))^2 \cup (\gamma^t(a))^2$, the equivalence classes of which have size d, the subgroup $2\mathbf{Z}_{2d}$ of $\mathbf{Z}_{2d}$ is in $\mathcal{S}$.

We claim that $\mathbf{Z}_{2d} \setminus 2\mathbf{Z}_{2d}$ cannot be a basic set of $\mathcal{S}$. Indeed, if $\mathbf{Z}_{2d} \setminus 2\mathbf{Z}_{2d}$ is a basic set of $\mathcal{S}$, then

$$\begin{aligned} exp_g(\mathbf{Z}_{2d} \setminus 2\mathbf{Z}_{2d}) &= (\overline{\gamma}(a))^2 \setminus \left((\gamma(a))^2 \cup (\gamma^t(a))^2\right) \\ &= (\gamma(a) \times \gamma^t(a)) \cup (\gamma^t(a) \times \gamma(a)) \end{aligned}$$

is a basic relation of $\langle\Phi(a,\gamma)\rangle$. Take any pair $(x,y) \in \gamma(a) \times \gamma^t(a)$. Let $\alpha \in \Gamma_M^*$ be the basic relation that contains (x,y). Then $(x,y) \in \alpha \cap (\gamma(a) \times \gamma^t(a)) = \widehat{\alpha}$. But $\widehat{\alpha} \cup \widehat{\alpha}^t$ is a union of basic relations from $\langle\Phi(a,\gamma)\rangle$. Since (x,y) belongs to the basic relation $(\gamma(a) \times \gamma^t(a)) \cup (\gamma^t(a) \times \gamma(a))$, we have

$$(\gamma(a) \times \gamma^t(a)) \cup (\gamma^t(a) \times \gamma(a)) \subset \widehat{\alpha} \cup \widehat{\alpha}^t =$$

$$\left(\alpha \cap (\gamma(a) \times \gamma^t(a))\right) \cup \left(\alpha^t \cap (\gamma^t(a) \times \gamma(a))\right).$$

The latter inclusion implies $\gamma(a) \times \gamma^t(a) \subset \alpha$ contrary to Proposition 4.5.

Thus, we have shown that $2\mathbf{Z}_{2d} \in \mathcal{S}$ and $\mathbf{Z}_{2d} \setminus 2\mathbf{Z}_{2d}$ is not a basic set of $\mathcal{S}$. By Proposition 4.6 $\{d\}$ is a basic set of $\mathcal{S}$. Therefore $\{(x, x^{g^d}) \mid x \in \overline{\gamma}(a)\}$ is a basic relation $\langle\Phi(a,\gamma)\rangle$. However, this set equals $\pi_{a,\gamma}$. The remaining part of the proof follows from the fact that $\{d\}$ is the unique basic set T of $\mathcal{S}$ that satisfies $T^2 = \{0\}$. $\diamondsuit$

Now we can formulate how to proceed in the case of d being prime. First, for each $a \in X$ and $\gamma \in \Gamma$ we use the WL-algorithm in order to find the set of basic relations of the coherent configuration $(\overline{\gamma}(a); \langle\Phi(a,\gamma)\rangle)$. If this configuration is not homogeneous, then the scheme $(X;\Gamma)$ is not cyclic.

If $(\overline{\gamma}(a); \langle\Phi(a,\gamma)\rangle)$ is homogeneous, then we find all basic relations $\rho \subset (\overline{\gamma}(a))^2$ that satisfies the equality $\rho^2 = \varepsilon_{\overline{\gamma}(a)}$. If for some $a \in X$ and $\gamma \in \Gamma$ the number of such relations is different from 1, then $(X;\Gamma)$ is not cyclic.

Thus we may assume that for each $a \in X$ and every $\gamma \in \Gamma$ there exists a unique involution $\rho_{a,\overline{\gamma}(a)} \in \mathrm{Sym}(\overline{\gamma}(a))$ with $\rho_{a,\overline{\gamma}(a)} \in \langle\Phi(a,\gamma)\rangle$. Write $\Gamma = \{\varepsilon_X, \gamma_1, \gamma_1^t, ..., \gamma_l, \gamma_l^t\}$. For each point $a \in X$ define $i_a \in \mathrm{Sym}(X)$ as follows $a^{i_a} = a$ and $b^{i_a} = \rho_{a,\overline{\gamma}_j(a)}(b), b \neq a$ where γ_j is defined by the inclusion $b \in (\gamma_j(a) \cap \gamma_j^t(a))$. Now we take the product

$g = i_a i_b$ for some $a, b \in X$, $a \neq b$. If g is a full cycle and is an automorphism of $(X;\Gamma)$, then we are done, otherwise $(X;\Gamma)$ is not cyclic.

Note that in the case where d is prime the final step has to be performed only for two different vertices a and b.

5 The algorithm.

In this section we first give a compact description of the recognition algorithm for circulant graphs of prime order p which is based on the method developed in the last section. Afterwards we shall estimate the time complexity of the algorithm.

Algorithm CGR

INPUT: The adjacency matrix A of a graph G on the vertex set $\{0, \ldots, p-1\}$.

STEP 1. (*Initialization*)

1.1 **Apply** the WL-algorithm to A and **find** the basic relations of the coherent configuration $(X;\Gamma)$ generated by G;

1.2 **If** this configuration is not homogeneous, **then goto** STEP 4 **else let** $\mathcal{B} = \{\varepsilon_X, \gamma_1, \ldots, \gamma_r\}$ be the set of basic relations;

1.3 **Define** $d = |\gamma_1(0)|$; **If** $|\gamma_i(0)| \neq d$ for some $i > 1$, **then goto** STEP 4;

1.4 **If** d is prime, **then goto** STEP 3;

STEP 2.1

2.1.1 **Apply** the WL-algorithm to $(\gamma_1(0); \Gamma_{\gamma_1(0)})$ and **find** the basic relations of the coherent configuration $(\gamma_1(0); \Gamma^{\gamma_1(0)})$;

2.1.2 **If** this configuration is not homogeneous, **then goto** STEP 4 **else let** $\mathcal{B}_{\gamma_1}(0) = \{\varepsilon_{\gamma_1(0)}, \beta_1, \ldots, \beta_s\}$ be the set of basic relations;

2.1.3 **Find** the connected components $C_1, \ldots, C_q$ of $(\gamma_1(0), \beta_1 \cup \beta_1^t)$;
If some of these components have different size **then goto** STEP 4 **else define** $\mathcal{C}_{\gamma_1}(0) = \{C_1, \ldots, C_q\}$;

2.1.4 **For** $\alpha \in \mathcal{B}_{\gamma_1}(0) \setminus \{\varepsilon_{\gamma_1(0)}, \beta_1\}$ **do**
begin
Find the connected components $C_{\alpha,1}, \ldots, C_{\alpha,q_\alpha}$ of $(\gamma_1(0), \alpha \cup \alpha^t)$;

If some of these components are of different size, **then goto** STEP 4 **else do**
begin
If $q_\alpha > |\mathcal{C}_{\gamma_1}(0)|$ **then** $\mathcal{C}_{\gamma_1}(0) = \{C_1, \ldots, C_{q_\alpha}\}$;
If $q_\alpha = |\mathcal{C}_{\gamma_1}(0)|$ and $\mathcal{C}_{\gamma_1}(0) \neq \{C_1, \ldots, C_{q_\alpha}\}$ **then goto** STEP 4;
end;
end;

STEP 2.2

For $x \in X$ and $\gamma \in \mathcal{B} \setminus \{\varepsilon_X\}$ **do**
if $(x, \gamma) \neq (0, \gamma_1)$ **then**
begin

2.2.1 **Apply** the WL-algorithm to $(\gamma(x); \Gamma_{\gamma(x)})$ and **find** the basic relations of the coherent configuration $(\gamma(x); \Gamma^{\gamma(x)})$;

2.2.2 **If** this configuration is not homogeneous, **then goto** STEP 4 **else let** $\mathcal{B}_\gamma(x) = \{\varepsilon_{\gamma(x)}, \beta_1, \ldots, \beta_s\}$ be the set of basic relations;

2.2.3 **Find** the connected components $C_1, \ldots, C_q$ of $(\gamma(x), \beta_1 \cup \beta_1^t)$;
If some of these components have different size, **then goto** STEP 4 **else define** $\mathcal{C}_\gamma(x) = \{C_1, \ldots, C_q\}$;

2.2.4 **For** $\alpha \in \mathcal{B}_\gamma(x) \setminus \{\varepsilon_{\gamma(x)}, \beta_1\}$ **do**
begin
Find the connected components $C_1, \ldots, C_{q_\alpha}$ of $(\gamma(x), \alpha \cup \alpha^t)$;
If some of these components are of different size, **then goto** STEP 4
else do
begin
If $q_\alpha > |\mathcal{C}_\gamma(x)|$, **then** $\mathcal{C}_\gamma(x) = \{C_1, \ldots, C_{q_\alpha}\}$;
If $q_\alpha = |\mathcal{C}_\gamma(x)|$ and $\mathcal{C}_\gamma(x) \neq \{C_1, \ldots, C_{q_\alpha}\}$ **then goto** STEP 4;
end;
end;
If $|\mathcal{C}_\gamma(x)| \neq |\mathcal{C}_{\gamma_1}(0)|$, **then goto** STEP 4;
end;

STEP 2.3

2.3.1 **For** $x \in X$ **define**

$$\tau_x = \bigcup_{\gamma \in \Gamma^*} \bigcup_{C \in \mathcal{C}_\gamma(x)} C \times C;$$

2.3.2 **Find** the components $\phi_1, \ldots, \phi_s$ of the relation Φ on $X^2 \setminus \varepsilon_X$ defined in Lemma 4.2;

2.3.3 **If** $\mathcal{B}' = \{\varepsilon_X, \phi_1, \ldots, \phi_s\}$ is not the basis of an association scheme **then goto** STEP 4;

2.3.4 **Define** $\mathcal{B} = \mathcal{B}'$ and **goto** STEP 1.3;

STEP 3

For $a \in \{0, 1\}$ **do**
begin

3.1 **For** $\gamma \in \mathcal{B}$ **do**
begin

3.1.1 **Define**

$$\begin{array}{rcl} \overline{\gamma}(a) & = & \gamma(a) \cup \gamma^t(a); \\ W(a,\gamma) & = & \gamma(a) \times \gamma^t(a); \\ \Gamma(a,\gamma) & = & \{\beta \cap W(a,\gamma) \mid \beta \in \Gamma\}; \\ \widehat{\Gamma}(a,\gamma) & = & \{\beta \cup \beta^t \mid \beta \in \Gamma(a,\gamma) \wedge \beta \neq \emptyset\}; \\ \Phi(a,\gamma) & = & \{\varepsilon_{\overline{\gamma}(a)}, (\gamma(a))^2 \cup (\gamma^t(a))^2\} \cup \widehat{\Gamma}(a,\gamma); \end{array}$$

3.1.2 **Apply** the WL-algorithm to $(\overline{\gamma}(a), \Phi(a,\gamma))$ in order to find the set of basic relations $\mathcal{B}(a,\gamma)$ for $(\overline{\gamma}(a), \langle\Phi(a,\gamma)\rangle)$

3.1.3 **If** this configuration is not homogeneous, **then goto** STEP 4;

3.1.4 **Find** all basic relations $\rho \in \mathcal{B}(a,\gamma)$ with the property $\rho^2 = \varepsilon_{\overline{\gamma}(a)}$;
If there is more than one or no such relation, **then goto** STEP 4;

3.1.5 **Let** $\{(y, \rho_{a,\gamma}(y)) \,:\, y \in \overline{\gamma}(a)\}$ be the unique relation found in the last step;

end;

3.2 **Define** the involution i_a by $x^{i_a} = \begin{cases} a & \text{if } x = a \\ \rho_{a,\gamma}(x) & \text{if } x \in \overline{\gamma}(a); \end{cases}$

end;
Goto STEP 5;

STEP 4

STOP; COMMENT: 'G is not a circulant graph';

STEP 5

Compute the permutation $g = i_0 i_1$ of X;
If g is not a cyclic automorphism, **then goto** STEP 4;
Output $(0, 0^g, \ldots, 0^{g^{n-1}})$;
Stop;

REMARKS:

The mapping $0^{g^k} \to k,\ 0 \leq k \leq p-1$ defines a Cayley numbering of the input graph.

Note that the steps 2.1 to 2.3 correspond to Step 1 to Step 3 in Subsection 4.1. The most time consuming step in Algorithm CGR is Step 2 which is the iteration step. Its complexity is $O(p^5 \ln(p))$. Since d decreases to at least $\frac{d}{2}$ in each iteration the overall worst case time complexity of the algorithm is at most $O(p^5 \ln(p)^2)$.

6 Examples

To see how the algorithm works let us discuss some examples.

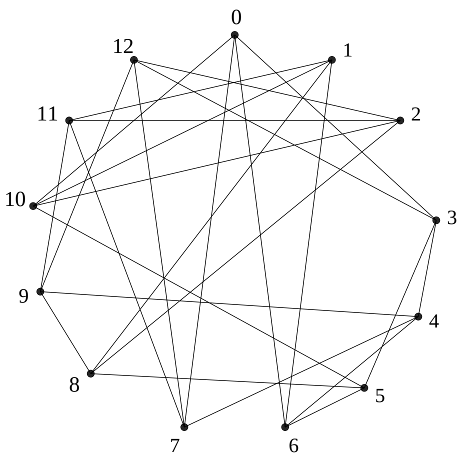


Figure 1

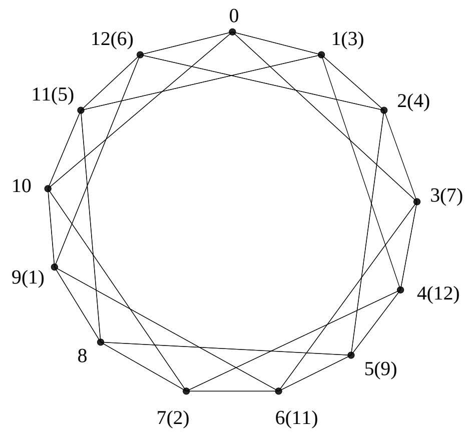


Figure 2

EXAMPLE 1: Consider the graph in Figure 1. Its coherent configuration has adjacency matrix

$$Adj(\mathcal{A}) = \begin{pmatrix} 0 & 4 & 3 & 1 & 2 & 2 & 1 & 6 & 5 & 5 & 6 & 3 & 4 \\ 4 & 0 & 2 & 5 & 3 & 2 & 6 & 3 & 1 & 4 & 1 & 6 & 5 \\ 3 & 2 & 0 & 3 & 5 & 4 & 5 & 4 & 1 & 2 & 6 & 1 & 6 \\ 1 & 5 & 3 & 0 & 1 & 6 & 2 & 2 & 3 & 4 & 4 & 5 & 6 \\ 2 & 3 & 5 & 1 & 0 & 4 & 6 & 1 & 3 & 6 & 5 & 4 & 2 \\ 2 & 2 & 4 & 6 & 4 & 0 & 1 & 5 & 6 & 3 & 1 & 5 & 3 \\ 1 & 6 & 5 & 2 & 6 & 1 & 0 & 4 & 4 & 3 & 2 & 3 & 5 \\ 6 & 3 & 4 & 2 & 1 & 5 & 4 & 0 & 5 & 2 & 3 & 6 & 1 \\ 5 & 1 & 1 & 3 & 3 & 6 & 4 & 5 & 0 & 6 & 2 & 2 & 4 \\ 5 & 4 & 2 & 4 & 6 & 3 & 3 & 2 & 6 & 0 & 5 & 1 & 1 \\ 6 & 1 & 6 & 4 & 5 & 1 & 2 & 3 & 2 & 5 & 0 & 4 & 3 \\ 3 & 6 & 1 & 5 & 4 & 5 & 3 & 6 & 2 & 1 & 4 & 0 & 2 \\ 4 & 5 & 6 & 6 & 2 & 3 & 5 & 1 & 4 & 1 & 3 & 2 & 0 \end{pmatrix}.$$

Since the diagonal is uniformly colored, the coherent configuration is homogeneous. We have six non-trivial symmetric basic relations. Each of the corresponding basic graphs has degree 2. Consider the first basic relation γ_1. It is the union of two antiparallel cycles

$$(0,3,4,7,12,9,11,2,8,1,10,5,6),(0,6,5,10,1,8,2,11,9,12,7,4,3).$$

Renumbering the vertices according to

$$0 \longrightarrow 0,\ \ 3 \longrightarrow 1,\ \ 4 \longrightarrow 2,\ \ 7 \longrightarrow 3,\ \ 12 \longrightarrow 4,\ \ 9 \longrightarrow 5,\ \ 11 \longrightarrow 6,\ \ 2 \longrightarrow 7,$$

$$8 \longrightarrow 8,\ \ 1 \longrightarrow 9,\ \ 10 \longrightarrow 10,\ \ 5 \longrightarrow 11,\ \ 6 \longrightarrow 12$$

and rearranging the vertices along a cycle changes the graph in Figure 1 into the graph in Figure 2. Note that each of the other basic graphs defines a full cyclic automorphism, too.

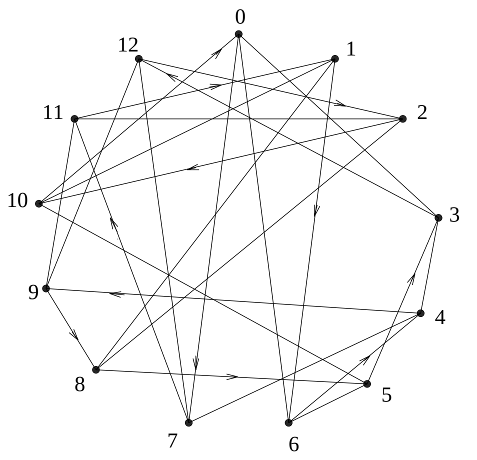


Figure 3

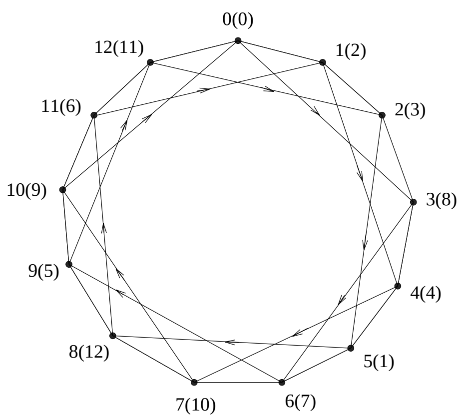


Figure 4

EXAMPLE 2: The graph in Figure 3 is the same as in Figure 1, however, some of its edges are oriented. The remaining non-oriented edges are considered to be pairs of anti-parallel oriented edges. The adjacency matrix of the associated coherent configuration is

$$Adj(\mathcal{A}) = \begin{pmatrix} 0 & 5 & 7 & 1 & 2 & 3 & 11 & 12 & 8 & 9 & 10 & 6 & 4 \\ 4 & 0 & 3 & 9 & 6 & 2 & 12 & 7 & 11 & 5 & 1 & 10 & 8 \\ 6 & 2 & 0 & 7 & 8 & 4 & 9 & 5 & 1 & 3 & 12 & 11 & 10 \\ 11 & 8 & 6 & 0 & 1 & 10 & 3 & 2 & 7 & 4 & 5 & 9 & 12 \\ 3 & 7 & 9 & 11 & 0 & 5 & 10 & 1 & 6 & 12 & 8 & 4 & 2 \\ 2 & 3 & 5 & 12 & 4 & 0 & 1 & 9 & 10 & 7 & 11 & 8 & 6 \\ 1 & 10 & 8 & 2 & 12 & 11 & 0 & 4 & 5 & 6 & 3 & 7 & 9 \\ 10 & 6 & 4 & 3 & 11 & 8 & 5 & 0 & 9 & 2 & 7 & 12 & 1 \\ 9 & 1 & 11 & 6 & 7 & 12 & 4 & 8 & 0 & 10 & 2 & 3 & 5 \\ 8 & 4 & 2 & 5 & 10 & 6 & 7 & 3 & 12 & 0 & 9 & 1 & 11 \\ 12 & 11 & 10 & 4 & 9 & 1 & 2 & 6 & 3 & 8 & 0 & 5 & 7 \\ 7 & 12 & 1 & 8 & 5 & 9 & 6 & 10 & 2 & 11 & 4 & 0 & 3 \\ 5 & 9 & 12 & 10 & 3 & 7 & 8 & 11 & 4 & 1 & 6 & 2 & 0 \end{pmatrix}.$$

Obviously, the configuration is homogeneous. All basic relations are full cycles. Take for instance γ_7. The corresponding cycle is

$$(0, 2, 3, 8, 4, 1, 7, 10, 12, 5, 9, 6, 11).$$

Renumbering the vertices according to

$$0 \longrightarrow 0,\ \ 2 \longrightarrow 1,\ \ 3 \longrightarrow 2,\ \ 8 \longrightarrow 3,\ \ 4 \longrightarrow 4,\ \ 1 \longrightarrow 5,\ \ 7 \longrightarrow 6,$$

$$10 \longrightarrow 7,\ \ 12 \longrightarrow 8,\ \ 5 \longrightarrow 9,\ \ 9 \longrightarrow 10,\ \ 6 \longrightarrow 11,\ \ 11 \longrightarrow 12,$$

and rearranging the vertices along a cycle changes the graph of Figure 3 into the graph of Figure 4.

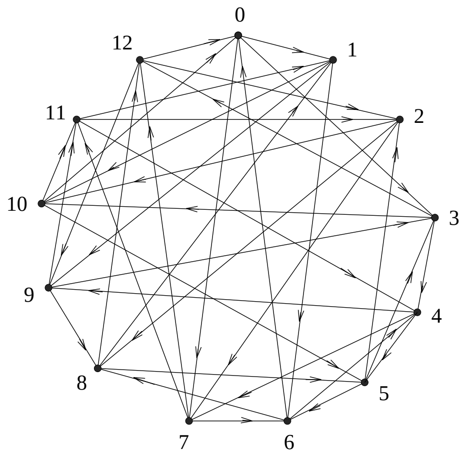


Figure 5

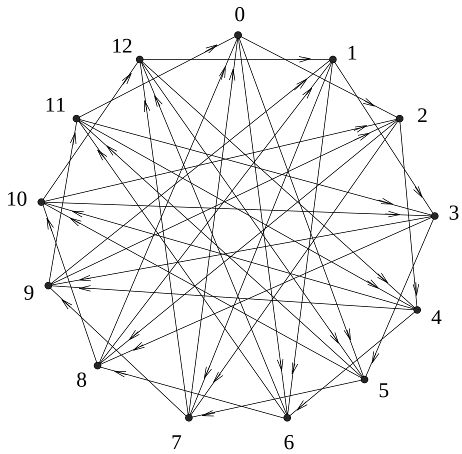


Figure 6

EXAMPLE 3: Consider the digraph in Figure 5. It looks like a circulant graph. What is the appropriate numbering of the vertices?

The adjacency matrix of the corresponding coherent configuration is given below. The configuration is homogeneous. Each basic graph has outdegree 3. Hence, we are in the case where d is a prime. Therefore, we have to perform STEP 3 of the algorithm. We have $\gamma_3 = \gamma_1^t$ and $\gamma_4 = \gamma_2^t$. Further,

$$\overline{\gamma}_1(0) = \{1,3,7\} \cup \{6,10,12\},\ \overline{\gamma}_2(0) = \{4,9,11\} \cup \{2,5,8\}$$

$$\overline{\gamma}_1(1) = \{6,9,10\} \cup \{0,8,11\},\ \overline{\gamma}_2(1) = \{3,4,5\} \cup \{2,7,12\}.$$

$$Adj(\mathcal{A}) = \begin{pmatrix} 0 & 1 & 4 & 1 & 2 & 4 & 3 & 1 & 4 & 2 & 3 & 2 & 3 \\ 3 & 0 & 4 & 2 & 2 & 2 & 1 & 4 & 3 & 1 & 1 & 3 & 4 \\ 2 & 2 & 0 & 4 & 4 & 3 & 2 & 1 & 1 & 4 & 1 & 3 & 3 \\ 3 & 4 & 2 & 0 & 1 & 3 & 4 & 2 & 4 & 3 & 1 & 2 & 1 \\ 4 & 4 & 2 & 3 & 0 & 1 & 3 & 1 & 2 & 1 & 4 & 3 & 2 \\ 2 & 4 & 1 & 1 & 3 & 0 & 1 & 2 & 3 & 4 & 3 & 4 & 2 \\ 1 & 3 & 4 & 2 & 1 & 3 & 0 & 3 & 1 & 2 & 4 & 4 & 2 \\ 3 & 2 & 3 & 4 & 3 & 4 & 1 & 0 & 2 & 2 & 4 & 1 & 1 \\ 2 & 1 & 3 & 2 & 4 & 1 & 3 & 4 & 0 & 3 & 2 & 4 & 1 \\ 4 & 3 & 2 & 1 & 3 & 2 & 4 & 4 & 1 & 0 & 2 & 1 & 3 \\ 1 & 3 & 3 & 3 & 2 & 1 & 2 & 2 & 4 & 4 & 0 & 1 & 4 \\ 4 & 1 & 1 & 4 & 1 & 2 & 2 & 3 & 2 & 3 & 3 & 0 & 4 \\ 1 & 2 & 1 & 3 & 4 & 4 & 4 & 3 & 3 & 1 & 2 & 2 & 0 \end{pmatrix}.$$

The adjaceny matrices $A(a,j)$ of the configurations generated by the sets of relations $\langle \Phi(a,\gamma_j) \rangle,\ \ a \in \{0,1\},\ j \in \{1,2\}$ are

$$A(0,1) = \begin{pmatrix} 0 & 3 & 3 & 1 & 1 & 2 \\ 3 & 0 & 3 & 2 & 1 & 1 \\ 3 & 3 & 0 & 1 & 2 & 1 \\ 1 & 2 & 1 & 0 & 3 & 3 \\ 1 & 1 & 2 & 3 & 0 & 3 \\ 2 & 1 & 1 & 3 & 3 & 0 \end{pmatrix},\ A(0,2) = \begin{pmatrix} 0 & 3 & 3 & 2 & 1 & 2 \\ 3 & 0 & 3 & 2 & 2 & 1 \\ 3 & 3 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 3 & 3 \\ 1 & 2 & 2 & 3 & 0 & 3 \\ 2 & 1 & 2 & 3 & 3 & 0 \end{pmatrix},$$

$$A(1,1) = \begin{pmatrix} 0 & 3 & 3 & 1 & 1 & 2 \\ 3 & 0 & 3 & 2 & 1 & 1 \\ 3 & 3 & 0 & 1 & 2 & 1 \\ 1 & 2 & 1 & 0 & 3 & 3 \\ 1 & 1 & 2 & 3 & 0 & 3 \\ 2 & 1 & 1 & 3 & 3 & 0 \end{pmatrix},\ A(1,2) = \begin{pmatrix} 0 & 3 & 3 & 2 & 2 & 1 \\ 3 & 0 & 3 & 2 & 1 & 2 \\ 3 & 3 & 0 & 1 & 2 & 2 \\ 2 & 2 & 1 & 0 & 3 & 3 \\ 2 & 1 & 2 & 3 & 0 & 3 \\ 1 & 2 & 2 & 3 & 3 & 0 \end{pmatrix}.$$

We find the following involutions:

$$i_0 : (1,12)(3,6)(7,10)(4,5)(9,8)(11,2),$$

$$i_1 : (6, 11)(9, 0)(10, 8)(3, 12)(4, 7)(5, 2).$$

Thus, $i_0 i_1$ gives the cyclic permutation

$$(0, 8, 7, 5, 11, 3, 1, 12, 6, 2, 4, 10, 9).$$

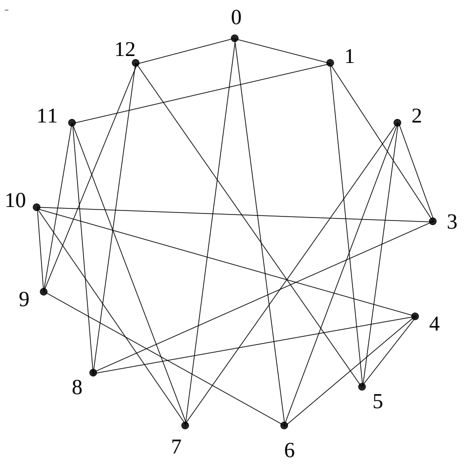


Figure 7

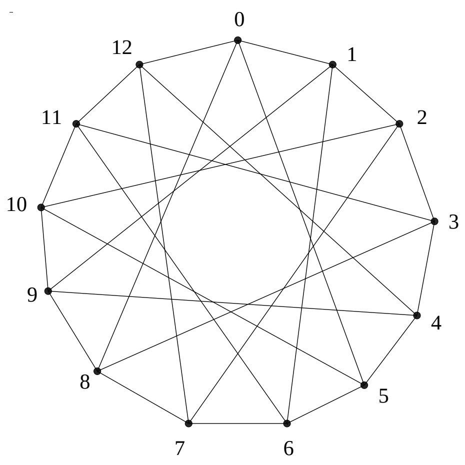


Figure 8

Renumbering the vertices according to

$$0 \longrightarrow 0,\ \ 8 \longrightarrow 1,\ \ 7 \longrightarrow 2,\ \ 5 \longrightarrow 3,\ \ 11 \longrightarrow 4,\ \ 3 \longrightarrow 5,\ \ 1 \longrightarrow 6,$$

$$12 \longrightarrow 7,\ \ 6 \longrightarrow 8,\ \ 2 \longrightarrow 9,\ \ 4 \longrightarrow 10,\ \ 10 \longrightarrow 11,\ \ 9 \longrightarrow 12$$

changes the graph in Figure 5 to the graph in Figure 6.

Example 4: Consider the graph in Figure 7. Its associated coherent configuration has adjacency matrix

$$Adj(\mathcal{A}) = \begin{pmatrix} 0 & 1 & 2 & 3 & 3 & 2 & 1 & 1 & 3 & 2 & 3 & 2 & 1 \\ 1 & 0 & 2 & 1 & 3 & 1 & 3 & 2 & 2 & 3 & 3 & 1 & 2 \\ 2 & 2 & 0 & 1 & 2 & 1 & 1 & 1 & 3 & 3 & 2 & 3 & 3 \\ 3 & 1 & 1 & 0 & 2 & 2 & 3 & 2 & 1 & 3 & 1 & 2 & 3 \\ 3 & 3 & 2 & 2 & 0 & 1 & 1 & 3 & 1 & 2 & 1 & 3 & 2 \\ 2 & 1 & 1 & 2 & 1 & 0 & 2 & 3 & 2 & 3 & 3 & 3 & 1 \\ 1 & 3 & 1 & 3 & 1 & 2 & 0 & 2 & 3 & 1 & 2 & 3 & 2 \\ 1 & 2 & 1 & 2 & 3 & 3 & 2 & 0 & 3 & 2 & 1 & 1 & 3 \\ 3 & 2 & 3 & 1 & 1 & 2 & 3 & 3 & 0 & 2 & 2 & 1 & 1 \\ 2 & 3 & 3 & 3 & 2 & 3 & 1 & 2 & 2 & 0 & 1 & 1 & 1 \\ 3 & 3 & 2 & 1 & 1 & 3 & 2 & 1 & 2 & 1 & 0 & 2 & 3 \\ 2 & 1 & 3 & 2 & 3 & 3 & 3 & 1 & 1 & 1 & 2 & 0 & 2 \\ 1 & 2 & 3 & 3 & 2 & 1 & 2 & 3 & 1 & 1 & 3 & 2 & 0 \end{pmatrix}.$$

The configuration is homogeneous. There are three symmetric non-trivial basic relations γ_1, γ_2 and γ_3, each of non-prime degree 4. Let us perform STEP 2 of the algorithm. The first table below shows the sets $\gamma_i(a)$:

	γ_1	γ_2	γ_3
0	1,6,7,12	2,5,9,11	3,4,8,10
1	0,3,5,11	2,7,8,12	4,6,9,10
2	3,5,6,7	0,1,4,10	8,9,11,12
3	1,2,8,10	4,5,7,11	0,6,9,12
4	5,6,8,10	2,3,9,12	0,1,7,11
5	1,2,4,12	0,3,6,8	7,9,10,11
6	0,2,4,9	5,7,10,12	1,3,8,11
7	0,2,10,11	1,3,6,9	4,5,8,12
8	3,4,11,12	1,5,9,10	0,2,6,7
9	6,10,11,12	0,4,7,8	1,2,3,5
10	3,4,7,9	2,6,8,11	0,1,5,12
11	1,7,8,9	0,3,10,12	2,4,5,6
12	0,5,8,9	1,4,6,11	2,3,7,10

Vertex	Classes
0	$\{0\},\{1,6\},\{2,5\},\{3,4\},\{7,12\},\{8,10\},\{9,11\}$
1	$\{1\},\{0,3\},\{2,7\},\{4,9\},\{5,11\},\{6,10\},\{8,12\}$
2	$\{2\},\{0,1\},\{3,6\},\{4,10\},\{5,7\},\{8,9\},\{11,12\}$
3	$\{3\},\{0,9\},\{1,10\},\{2,8\},\{4,5\},\{6,12\},\{7,11\}$
4	$\{4\},\{0,11\},\{1,7\},\{2,3\},\{5,10\},\{6,8\},\{9,12\}$
5	$\{5\},\{0,6\},\{1,4\},\{2,12\},\{3,8\},\{7,9\},\{10,11\}$
6	$\{6\},\{0,4\},\{1,8\},\{2,9\},\{3,11\},\{5,12\},\{7,10\}$
7	$\{7\},\{0,10\},\{1,3\},\{2,11\},\{4,12\},\{5,8\},\{6,9\}$
8	$\{8\},\{0,2\},\{1,5\},\{3,12\},\{4,11\},\{6,7\},\{9,10\}$
9	$\{9\},\{0,7\},\{1,2\},\{3,5\},\{4,8\},\{6,11\},\{10,12\}$
10	$\{10\},\{0,5\},\{1,12\},\{2,6\},\{3,9\},\{4,7\},\{8,11\}$
11	$\{11\},\{0,12\},\{1,9\},\{2,4\},\{3,10\},\{5,6\},\{7,8\}$
12	$\{12\},\{0,8\},\{1,11\},\{2,10\},\{3,7\},\{4,6\},\{5,9\}$

For a matrix A and a set W of indices write A_W for the submatrix of A consisting of all rows and columns index with elements of W. It is easy to see by inspection that each of the blocks $Adj(\mathcal{A})_{\gamma_i(a)}$ is of one of the following forms

$$\begin{pmatrix} 0 & x & y & y \\ x & 0 & y & y \\ y & y & 0 & x \\ y & y & x & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & x & y & x \\ x & 0 & x & y \\ y & x & 0 & x \\ x & y & x & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & x & x & y \\ x & 0 & y & x \\ x & y & 0 & x \\ y & x & x & 0 \end{pmatrix},$$

where $x, y \in \{1,2,3\}$, $x \neq y$. Using this we find the equivalence relations given in the second table above. Now, this table at hand, determining the components of Φ according to Lemma 4.2 is straight-forward. We get 6 components, which are represented by the following joint adjacency matrix:

$$\begin{pmatrix}
0 & 1 & 3 & 5 & 5 & 3 & 1 & 2 & 6 & 4 & 6 & 4 & 2 \\
1 & 0 & 3 & 1 & 6 & 2 & 5 & 3 & 4 & 6 & 5 & 2 & 4 \\
3 & 3 & 0 & 2 & 4 & 1 & 2 & 1 & 6 & 6 & 4 & 5 & 5 \\
5 & 1 & 2 & 0 & 4 & 4 & 6 & 3 & 2 & 5 & 1 & 3 & 6 \\
5 & 6 & 4 & 4 & 0 & 2 & 1 & 6 & 1 & 3 & 2 & 5 & 3 \\
3 & 2 & 1 & 4 & 2 & 0 & 3 & 5 & 4 & 5 & 6 & 6 & 1 \\
1 & 5 & 2 & 6 & 1 & 3 & 0 & 4 & 5 & 2 & 4 & 6 & 3 \\
2 & 3 & 1 & 3 & 6 & 5 & 4 & 0 & 5 & 4 & 2 & 1 & 6 \\
6 & 4 & 6 & 2 & 1 & 4 & 5 & 5 & 0 & 3 & 3 & 1 & 2 \\
4 & 6 & 6 & 5 & 3 & 5 & 2 & 4 & 3 & 0 & 1 & 2 & 1 \\
6 & 5 & 4 & 1 & 2 & 6 & 4 & 2 & 3 & 1 & 0 & 3 & 5 \\
4 & 2 & 5 & 3 & 5 & 6 & 6 & 1 & 1 & 2 & 3 & 0 & 4 \\
2 & 4 & 5 & 6 & 3 & 1 & 3 & 6 & 2 & 1 & 5 & 4 & 0
\end{pmatrix}.$$

In addition, this matrix is already the adjacency matrix of the coherent configuration generated by the components of Φ. The configuration is homogeneous. We have six non-trivial basic relations of degree $d = 2$ each. Each of them defines an undirected cycle, i.e. a full cycle and its inverse. For instance, γ_1 defines the cycle

$$(0, 1, 3, 10, 9, 12, 5, 2, 7, 11, 8, 4, 6).$$

Renumbering the vertices of the graph according to

$$0 \longrightarrow 0,\quad 1 \longrightarrow 1,\quad 3 \longrightarrow 2,\quad 10 \longrightarrow 3,\quad 9 \longrightarrow 4,\quad 12 \longrightarrow 5,\quad 5 \longrightarrow 6,$$

$$2 \longrightarrow 7,\quad 7 \longrightarrow 8,\quad 11 \longrightarrow 9,\quad 8 \longrightarrow 10,\quad 4 \longrightarrow 11,\quad 6 \longrightarrow 12$$

changes the picture of the graph in Figure 7 to the one in Figure 8.

EXAMPLE 5: Not every association scheme on a prime number of vertices is cyclic. To have an example consider the adjacency matrix below. It is the adjacency matrix of a homogeneous and commutative coherent configuration generated by an antisymmetric strongly regular graph Γ on 23 vertices. However, the automorphism group of this scheme is not transitive. Changing the first diagonal entry from 0 to 3 and applying the WL-algorithm to the resulting matrix yields a coherent configuration with 17 basic relations, while changing the second diagonal entry from 0 to 3 and applying the WL-algorithm yields 113 basic relations. This proves that 0 and 1 are not in the same orbit. Our algorithm, applied to the above matrix, will perform Step 1 and afterwards turn to Step 3. It will decide that the input is not cyclic at the first arrival at 3.1.4.

$$\begin{pmatrix}
0&2&2&2&2&2&2&2&2&2&2&2&1&1&1&1&1&1&1&1&1&1&1\\
1&0&2&1&2&2&2&1&1&1&2&1&2&1&2&1&1&1&2&2&2&1&2\\
1&1&0&2&1&2&2&2&1&1&1&2&2&2&1&2&1&1&1&2&2&2&1\\
1&2&1&0&2&1&2&2&2&1&1&1&1&2&2&1&2&1&1&1&2&2&2\\
1&1&2&1&0&2&1&2&2&2&1&1&2&1&2&2&1&2&1&1&1&2&2\\
1&1&1&2&1&0&2&1&2&2&2&1&2&2&1&2&2&1&2&1&1&1&2\\
1&1&1&1&2&1&0&2&1&2&2&2&2&2&2&1&2&2&1&2&1&1&1\\
1&2&1&1&1&2&1&0&2&1&2&2&1&2&2&2&1&2&2&1&2&1&1\\
1&2&2&1&1&1&2&1&0&2&1&2&1&1&2&2&2&1&2&2&1&2&1\\
1&2&2&2&1&1&1&2&1&0&2&1&1&1&1&2&2&2&1&2&2&1&2\\
1&1&2&2&2&1&1&1&2&1&0&2&2&1&1&1&2&2&2&1&2&2&1\\
1&2&1&2&2&2&1&1&1&2&1&0&1&2&1&1&1&2&2&2&1&2&2\\
2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1&2&2&2&1&2\\
2&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1&2&2&2&1\\
2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1&2&2&2\\
2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1&2&2\\
2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1&2\\
2&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1&1\\
2&1&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1&1\\
2&1&1&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2&1\\
2&1&1&1&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1&2\\
2&2&1&1&1&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0&1\\
2&1&2&1&1&1&2&2&2&1&2&1&1&2&1&1&1&2&2&2&1&2&0
\end{pmatrix}.$$

The example considered here is from an infinite series of examples of non-cyclic association schemes. It is found by the so-called *doubling method* described in [FarKM94], Theorem 2.6.6. A different way to arrive at this example is by using the one-to-one correspondence between skew-symmetric Hadamard matrices of order 4n and association schemes with two non-symmetric classes on 4n-1 points (regular tournaments) described in [Ito84].

7 Concluding remarks.

The described algorithm is based on the fact that the automorphism group of any circulant association scheme on p points is a Frobenius group. There is a more general class of association schemes the automorphism group of which is a Frobenius group, namely: the cyclotomic schemes on p^n points. So one can try to modify the algorithm in order to recognize this class of schemes. Results in this direction will be published in a forthcoming paper.

8 Acknowledgment

The authors wish to express their gratitude to the anonymous referee for pointing out some inconsistencies in the first draft of the paper and for giving various valuable suggestions and remarks.

References

[BBLT97] 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.*

[BCKP97] 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.*

[BaI84] E. Bannai, T. Ito, *Algebraic Combinatorics I, Association Schemes. Benjamin/Cummings, Menlo Park 1984*

[BaS93] E. Bannai, Y. S. Song, *Character table of fission schemes and fusion schemes. Europ. J. of Combin. 14, (1993), 385-396.*

[EvdP98] S. Evdokimov, I. Ponomarenko, *On Primitive Cellular Algebras. Zapiski POMI, 1998*, to appear.

[FarIK92] I. A. Faradžev, A. A. Ivanov, M. H. Klin, *Galois correspondence between permutation groups and cellular rings (association schems). Graphs and Comb. 6, (1992), 202-224.*

[FarKM94] 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.*

[Hig70] D. G. Higman, *Coherent configurations. I. Rend. Sem. Mat. Univ. Padova 44, (1970), 1-25.*

[Hig87] D. G. Higman, *Coherent algebras. Linear Algebra Appl. 93, (1987), 209-239.*

[Ito84] N. Ito, *Tournaments with transitive automorphism group. Europ. J. of Comb. 5, (1984), 37-42.*

[KliP78] 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.*

[McC63] R. McConnel, *Pseudo-ordered polynomial over a finite field. Acta Arith. 8, (1963), 127-151.*

[Pon92] I. Ponomarenko, *Polynomial-Time Algorithms for Recognizing and Isomorphism Testing of Cyclic Tournaments. Acta Appl. Math. 29, (1992), 139-160.*

[Wei76] B. J. Weisfeiler (Ed.), On construction and identification of graphs, *Springer Lecture Notes* 558 (1976).

[Wie64] H. W. Wielandt, *Finite permutation groups. Academic Press, N.Y., 1964.*