On Congruence in Z^n and the Dimension of a Multidimensional Circulant

M.A. Fiol

Dpt. de Matemàtica Aplicada i Telemàtica
Universitat Politècnica de Catalunya

Abstract

From a generalization to Z^n of the concept of congruence we define a family of regular digraphs or graphs called multidimensional circulants, which turn out to be Cayley (di)graphs of Abelian groups. This paper is mainly devoted to show the relationship between the Smith normal form for integral matrices and the dimensions of such (di)graphs, that is the minimum ranks of the groups they can arise from. In particular, those 2-step multidimensional circulants which are circulants, that is Cayley (di)graphs of cyclic groups, are fully characterized. In addition, a reasoning due to Lawrence is used to prove that the cartesian product of n circulants with equal number of vertices $p > 2$, p a prime, has dimension n.

1   Introduction

Throughout this paper we make use of standard concepts and terminology of graph theory and group theory, see for instance [6] and [16] respectively. We will recall here the most relevant definitions. Let Γ be a group with identity element e, and let $A \subseteq \Gamma - \{e\}$ such that $A^{-1} = A$. The Cayley graph of Γ with respect to A, denoted by $G(\Gamma; A)$, is the graph whose vertices are labelled with the elements of Γ, and an edge (u, v) if and only if $u^{-1}v \in A$. The Cayley digraph $G(\Gamma; A)$ is defined similarly, but now we do not require $A^{-1} = A$. Since left translations in Γ are automorphisms of $G(\Gamma; A)$, a Cayley graph is always vertex-transitive. Moreover, the group of such automorphisms, $AutG(\Gamma; A)$, contains a regular subgroup (that is a transitive subgroup whose order coincides with the order of the graph) isomorphic to Γ. In fact, Sabidussi [17] first showed that this is also a sufficient

condition for a graph to be a Cayley graph (of the group Γ). Clearly, the same statements also hold for Cayley digraphs. In particular, this result or its digraph analog will be simply referred to as *Sabidussi's result*.

Because of both theoretical and practical reasons, the class of Cayley (di)graphs obtained from Abelian groups have deserved special attention in the literature. This is the case, for instance, for circulant (di)graphs the definition of which follows. Let m be a positive integer, and $A = \{a_1, a_2, \ldots, a_d\} \subseteq Z/mZ - \{0\}$. The *(d-step) circulant digraph* $G(m; A)$ has as set of vertices the integers modulo m, and vertex u is adjacent to the vertices $u + A = \{u + a_i \pmod{m} : a_i \in A\}$. The names *multiple loop digraph* and *multiple fixed step digraph* [3, 13] are also used. The *(d-step) circulant graph* $G(m; A)$ is defined analogously with $A = -A = \{\pm a_1, \pm a_2, \ldots, \pm a_d\}$. These graphs have also received other names such as *starred polygons* [18] and *multiple loop graphs* [4]. In both the directed and undirected case, the elements of A are called *jumps* or *steps*. Henceforth, we will use the word *circulant* to denote either a circulant digraph or a circulant graph. As stated above, notice that the circulant $G(m; A)$ is just the Cayley (di)graph of the cyclic group Z/mZ with respect to A. Therefore, from Sabidussi's result, *a (di)graph is a circulant iff its automorphism group contains a regular cyclic subgroup*. As Leighton showed in [14], this characterization can be used to easily prove Turner's result [18], which states that every transitive graph on a prime number of vertices is a circulant. (It suffices to use Cauchy's group theorem: "If a prime p divides the order of a finite group then it contains an element of order p.") In fact the same reasoning shows that Turner's result also holds for digraphs.

Recall that, given two graphs, $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$, their *cartesian product* $G_1 \times G_2$ is the graph with set of vertices $V_1 \times V_2$ and an edge between (u_1, u_2) and (v_1, v_2) iff either $(u_1, v_1) \in E_1$ and $u_2 = v_2$ or $u_1 = v_1$ and $(u_2, v_2) \in E_2$. The cartesian product of two digraphs is defined analogously. Another well known family of Cayley graphs of Abelian groups are the (Boolean) n-cubes, which are sometimes defined as the cartesian product of n copies of the complete graph K_2. From our point of view, the *n-cube* (or *binary n-dimensional hypercube*) is the Cayley graph $G(\Gamma; A)$, where $\Gamma = Z/2Z \times \cdots \times Z/2Z$ (n factors) and A is the set of unitary vectors $\mathbf{e}_i$, $1 \leq i \leq n$.

This paper studies the structure of the so-called $(d$-step$)$ multidimensional circulants (that is Cayley graphs or digraphs of Abelian groups), which are defined from integral matrices in Section 3. More precisely, given such a

(di)graph, we are interested in finding its "dimension", that is the minimum rank of the group(s) it can arise from. (The *rank* of a finitely generated Abelian group is the minimum number of elements which generate it.) For instance, from its definition it is clear that the n-cube has dimension not greater than n. As far as we know, this study was initialized by Leighton in [14], where it was shown that the dimension of the n-cube is in fact $\lfloor (n+1)/2 \rfloor$. Other results, concerning 2-step circulant digraphs (dimension 1) can be found in [10, 13]. In this paper we continue this study by deriving some new results, which are contained in Section 3. For instance, using some facts about integral matrices and a theorem in [7], we give a full characterization of those 2-step multidimensional circulants which are 1-dimensional. Moreover, it is proved that if $G_1, G_2, \ldots, G_n$ are circulant (di)graphs with $p > 2$ vertices, p a prime, then the cartesian product $G_1 \times G_2 \times \cdots \times G_n$ has dimension n.

As stated above, our approach uses some results of integral matrix theory which are summarized in the next section. In particular, we deal with the concept of congruence in Z^n, also discussed there. The reason is that, in the same way that congruence in Z (periodicity in one dimension) leads to the consideration of cyclic groups, congruence in Z^n (related to periodicity in n dimensions) induces quotient structures which are Abelian groups.

2 Congruences in Z^n and the Induced Abelian Groups

This section mainly deals with the concept of congruence in Z^n and its consequences to our study. In this context, the theory of integral matrices (that is matrices whose entries are integers) proves to be very useful and, hence, we begin by recalling some of its main results. The reader interested in the proofs is referred to [15].

Let Z^{n*n} be the ring of $n \times n$ matrices over Z. Given $A, B \in Z^{n*n}$, A is said to be *right equivalent* to B if there exists a unimodular (with determinant ± 1) matrix $V \in Z^{n*n}$ such that $A = BV$; and A is *equivalent* to B if $A = UBV$ for some unimodular matrices $U, V \in Z^{n*n}$. Clearly, both of them are equivalence relations.

Henceforth, $M = (m_{ij})$ will denote a nonsingular matrix of Z^{n*n} with columns $\mathbf{m}_j = (m_{1j}, m_{2j}, \ldots, m_{nj})^\top$, $j = 1, 2, \ldots, n$, and $m = |\det M|$. By the Hermite normal form theorem, M is right equivalent to an upper

triangular matrix $H(M) = H = (h_{ij})$ with positive diagonal elements h_{ii} and with each element above the main diagonal h_{ij}, $j > i$, $i = 1, 2, \ldots, n-1$, lying in a given complete set of residues modulo h_{ii} (for instance, $0 \le h_{ij} \le h_{ii} - 1$). This normal form is unique.

Let $k \in Z$, $1 \le k \le n$. The kth *determinantal divisor* of M, denoted by $d_k(M) = d_k$, is defined as the greatest common divisor of the $\binom{n}{k}^2$ $k \times k$ determinantal minors of M. Since M is nonsingular, not all of them are zero. Notice that $d_k | d_{k+1}$ for all $k = 1, 2, \ldots, n-1$ and $d_n = m$. For convenience, put $d_0 = 1$. The *invariant factors* of M are the quantities

$$s_k(M) = s_k = \frac{d_k}{d_{k-1}}, \quad k = 1, 2, \ldots, n.$$

It can be shown that $s_i | s_{i+1}$, $i = 1, 2, \ldots, n-1$.

By the Smith normal form theorem, M is equivalent to the diagonal matrix $S(M) = S = \mathrm{diag}(s_1, s_2, \ldots, s_n)$. This canonical form is unique.

For instance, the matrix $M = \mathrm{diag}(2, 2, 3)$, with determinantal divisors $d_1 = 1$, $d_2 = 2$, $d_3 = 12$, and invariant factors $s_1 = 1$, $s_2 = 2$, $s_3 = 6$, is equivalent to $S = \mathrm{diag}(1, 2, 6)$ since there exist the unimodular matrices

$$U = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ -3 & 0 & 2 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \tag{1}$$

such that $S = UMV$.

As usual, the greatest common divisor of the integers $a_1, a_2, \ldots, a_n$ will be denoted by $\gcd(a_1, a_2, \ldots, a_n)$. When they are the coordinates of a vector $\mathbf{a}$, we will simply write $\gcd(\mathbf{a})$.

Most of the remaining material in this section is drawn from [11] where additional details can be found.

Let Z^n denote the additive group of column n-vectors with integral coordinates. The set MZ^n, whose elements are linear combinations (with integral coefficients) of the (column) vectors $\mathbf{m}_j$, is said to be the lattice generated by M. Clearly, MZ^n with the usual vector addition is a normal subgroup of Z^n.

The concept of congruence in Z has the following natural generalization to Z^n. Let $\mathbf{a}, \mathbf{b} \in Z^n$. We say that $\mathbf{a}$ *is congruent with* $\mathbf{b}$ *modulo* M, and

write $\mathbf{a} \equiv \mathbf{b} \pmod{M}$, if

$$\mathbf{a} - \mathbf{b} \in MZ^n. \tag{2}$$

The quotient group Z^n/MZ^n can intuitively be called the *group of integral vectors modulo M*. Henceforth, we follow the usual convention of identifying each equivalence class by any of its representatives.

Note that whenever $M = \text{diag}(m_1, m_2, \ldots, m_n)$ the vectors $\mathbf{a} = (a_1, a_2, \ldots, a_n)^\top$ and $\mathbf{b} = (b_1, b_2, \ldots, b_n)^\top$ are congruent modulo M iff the system of congruences in Z

$$a_i \equiv b_i \pmod{m_i}, \;\; i = 1, 2, \ldots, n$$

holds. In this case Z^n/MZ^n is the direct product of the cyclic groups Z/m_iZ, $i = 1, 2, \ldots, n$.

If A and B are $n \times r$ matrices over Z with columns $\mathbf{a}_j$ and $\mathbf{b}_j$, $j = 1, 2, \ldots, r$, respectively, we will write $A \equiv B \pmod{M}$ to denote that $\mathbf{a}_j \equiv \mathbf{b}_j \pmod{M}$ for all $j = 1, 2, \ldots, r$.

Let $H = MV$ be the Hermite normal form of M. Then (2) holds iff $\mathbf{a} - \mathbf{b} \in HV^{-1}Z^n = HZ^n$ since V, and hence V^{-1}, are unimodular. Therefore we conclude that

$$\mathbf{a} \equiv \mathbf{b} \pmod{M} \;\; \Leftrightarrow \;\; \mathbf{a} \equiv \mathbf{b} \pmod{H} \tag{3}$$

or, what is the same,

$$Z^n/MZ^n \cong Z^n/HZ^n. \tag{4}$$

Let us now consider the Smith normal form of M, $S = \text{diag}(s_1, s_2, \ldots, s_n) = UMV$. Then (2) holds iff $U\mathbf{a} \equiv U\mathbf{b} \pmod{S}$ or, equivalently,

$$\mathbf{u}_i\mathbf{a} \equiv \mathbf{u}_i\mathbf{b} \pmod{s_i}, \;\; i = 1, 2, \ldots, n \tag{5}$$

where $\mathbf{u}_i$ stands for the ith row of U. Moreover, if r is the smallest integer such that $s_{n-r} = 1$ (thus, $s_1 = s_2 = \cdots = s_{n-r-1} = 1$), (if there is no such a r, let $r = n$), the first $n - r$ equations in (5) are irrelevant, and we only need to consider the other ones. This allows us to write

$$\mathbf{a} \equiv \mathbf{b} \pmod{M} \;\; \Leftrightarrow \;\; U'\mathbf{a} \equiv U'\mathbf{b} \pmod{S'} \tag{6}$$

where U' stands for the $r \times n$ matrix obtained from U by leaving out the first $n - r$ rows, and $S' = \text{diag}(s_{n-r+1}, s_{n-r+2}, \ldots, s_n)$. So, the (linear) mapping

ϕ from the vectors modulo M to the vectors modulo S' given by $\phi(\mathbf{a}) = U'\mathbf{a}$ is a group isomorphism, and we can write

$$Z^n/MZ^n \cong Z^r/S'Z^r = Z/s_{n-r+1}Z \times \cdots \times Z/s_nZ. \qquad (7)$$

Analogously, it may be shown that the $n \times r$ matrix of the inverse mapping ϕ^{-1} is obtained from U^{-1} by leaving out its first $n - r$ columns.

The next proposition contains some easy consequences of the above results. For instance, (b) follows from the fact that $s_1 s_2 \cdots s_n = d_n = m$ and $s_i | s_{i+1}$, $i = 1, 2, \ldots, n - 1$.

Proposition 2.1 *(a) The number of equivalence classes modulo M is $|Z^n/MZ^n| = m = |\det M|$.*
(b) If $p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ is the prime factorization of m, then $Z^n/MZ^n \cong Z^r/S'Z^r$ for some $r \times r$ matrix S' with $r \le \max\{r_i : 1 \le i \le t\}$.
(c) The (Abelian) group of integral vectors modulo M is cyclic iff $d_{n-1} = 1$.
(d) Let r be the smallest integer such that $s_{n-r} = 1$. Then r is the rank of Z^n/MZ^n and the last r columns of U^{-1} form a basis of Z^n/MZ^n. $\square$

Given any element $\mathbf{a}$ of Z^n/MZ^n, simple reasoning shows that its order is given by the formula

$$\mathrm{o}(\mathbf{a}) = \frac{m}{\gcd(m, \gcd(mM^{-1}\mathbf{a}))}, \qquad (8)$$

(see [11]). For instance, if $M = (m_{ij})$ is a 2×2 matrix and $\mathbf{a} = (a_1, a_2)^\top$ we have

$$\mathrm{o}(\mathbf{a}) = \frac{m}{\gcd(m, a_1 m_{22} - a_2 m_{12}, a_2 m_{11} - a_1 m_{21})}. \qquad (9)$$

According to (7), for any given $M \in Z^{n*n}$ there exists an Abelian group Γ such that $\Gamma = Z^n/MZ^n$. Conversely, let Γ be a finite Abelian group generated by the elements $g_1, g_2, \ldots g_n$. Then Γ is isomorphic to Z^n/K, where K is the kernel of the surjective homomorphism $\Psi : Z^n \longrightarrow \Gamma$ defined by $\Psi(\mathbf{x}) = \mathbf{g}\mathbf{x}$, where $\mathbf{g}$ denotes the row vector $(g_1, g_2, \ldots, g_n)$ and $\mathbf{x} \in Z^n$. (Note that $\Psi(\mathbf{e}_i) = g_i$, $1 \le i \le n$, where $\mathbf{e}_i$ stands for the ith unitary vector.) More precisely, K is the lattice of Z^n generated by the upper triangular $n \times n$ matrix $H = (m_{ij})$ defined as follows:
$m_{11} = \mathrm{o}(g_1) = |<g_1>|$;
$m_{jj} = \min\{\mu \in Z^+ : \mu g_j \in <g_1, g_2, \ldots, g_{j-1}>\}$, $j = 2, 3, \ldots, n$;
and

$m_{ij}, j = 2, 3, \ldots, n, i < j$, are any integers such that $m_{1j}g_1 + m_{2j}g_2 + \cdots + m_{jj}g_j = 0$, (they can be chosen in a given complete set of residues modulo h_{ii}, e.g., $0 \leq m_{ij} \leq h_{ii} - 1$), where, as usual, $< g_1, g_2, \ldots, g_j >$ denotes the group generated by $g_1, g_2, \ldots, g_j$, and 0 is the identity element of Γ. Clearly, H is the Hermite normal form of any matrix M which generates the lattice K.

3 Multidimensional circulants and their dimension

Congruence in Z^n leads to the following generalization of circulants. Let M be an $n \times n$ integral matrix as in Section 2. Let $A = \{\mathbf{a}_j = (a_{1j}, a_{2j}, \ldots, a_{nj})^\top : 1 \leq j \leq d\} \subseteq Z^n/MZ^n$. The *multidimensional (d-step) circulant digraph* $G(M;A)$ has as vertex-set the integral vectors modulo M, and every vertex $\mathbf{u}$ is adjacent to the vertices $\mathbf{u} + A \pmod{M}$. As in the case of circulants, the *multidimensional (d-step) circulant graph* $G(M;A)$ is defined similarly just requiring $A = -A$.

In [14], Leighton considered multidimensional circulant graphs with diagonal matrix M, and characterized them by showing that *the automorphism group of these graphs must contain a regular Abelian subgroup.* Clearly, a multidimensional circulant (digraph or graph) is a Cayley (di)graph of the Abelian group Z^n/MZ^n. As a consequence, Sabidussi's result implies that Leighton's statement holds in fact for a multidimensional circulant obtained from any matrix M.

As another consequence of the above, if α is the index of the subgroup $\Gamma = < \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d >$ in Z^n/MZ^n, the multidimensional circulant $G(M;A)$ consists of α copies of the Cayley (di)graph of Γ generated by A. Besides, from the comments in the last paragraph of Section 2, $\Gamma \cong Z^d/HZ^d$, where H is an upper triangular $d \times d$ matrix, and each such copy is isomorphic to $G(H; \mathbf{e}_1, \mathbf{e}_2, \ldots \mathbf{e}_d)$.

In particular, $G(M; \mathbf{a}_1, \mathbf{a}_2, \ldots \mathbf{a}_d)$ (respectively $G(M; \pm\mathbf{a}_1, \pm\mathbf{a}_2, \ldots \pm\mathbf{a}_d)$) is strongly connected (respectively connected), that is $\alpha = 1$, iff $\{\mathbf{a}_1, \mathbf{a}_2, \ldots \mathbf{a}_d\}$ generates Z^n/MZ^n, that is, there exist n integral d-vectors $\mathbf{x}^j = (x_{1j}, x_{2j}, \ldots, x_{dj})^\top, j = 1, 2, \ldots, n$, such that

$$x_{1j}\mathbf{a}_1 + x_{2j}\mathbf{a}_2 + \cdots + x_{dj}\mathbf{a}_d \equiv \mathbf{e}_j \pmod{M}, \quad j = 1, 2, \ldots, n$$

or, in matrix form,

$$AX \equiv I \pmod{M}$$

where A now denotes the $n \times d$ matrix (a_{ij}), X is the $d \times n$ matrix (x_{ij}), and I stands for the identity matrix.

A certain (di)graph may be a multidimensional circulant for several different values of n. For instance, the digraph $G(M; A)$ with $M = \text{diag}(2, 2, 3)$ and $A = \{(1, 0, 0)^\top, (0, 1, 0)^\top, (0, 0, 2)^\top\}$ is isomorphic to the digraph $G(M'; A')$ with $M' = \text{diag}(2, 6)$ and $A' = \{(0, 3)^\top, (1, 0)^\top, (0, 4)^\top\}$ since, if U' is the 2×3 matrix obtained by taking the two last rows of the matrix U in (1), we have $U'A \equiv A' \pmod{M'}$. Following Leighton's terminology [14], if k is the smallest value of such n we will say that the multidimensional circulant has *dimension k* or that it is *k-dimensional*. Notice that this parameter is in fact the minimum rank of the groups such a (di)graph can arise from. Then the class of circulants is precisely the class of 1-dimensional circulants.

In studying the dimension of a given multidimensional circulant $G(M; A)$ we only need to consider the connected case. Indeed suppose that the α disjoint components of $G(M; A)$ are, say, k-dimensional and isomorphic to $G(M'; A'), M' \in Z^{k*k}$. Then $G(M; A)$ is isomorphic to $G(\alpha M'; \alpha A')$ where $\alpha M'$ and $\alpha A'$ denote the matrix and set obtained from M' and A' by simply multiplying by α any, say the first, component of the corresponding (column) vectors. As a corollary, the dimension of $G(M; A)$ cannot be greater than the cardinality of the minimum subset of A that generates $\Gamma = \langle \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d \rangle$.

To obtain other results about the dimension of multidimensional circulants it is useful to introduce the concept of Ádám isomorphism. Let $M \in Z^{n*n}$ and $M' \in Z^{n'*n'}$. Then the multidimensional circulants $G(M; A)$ and $G(M'; A')$ are said to be *Ádám isomorphic* if there exists an isomorphism ϕ between the groups Z^n/MZ^n and $Z^{n'}/M'Z^{n'}$ such that $\phi(A) = A'$. For instance, if u is a unit of Z/mZ, that is $\gcd(u, m) = 1$, the circulants $G(m; A)$ and $G(m; uA)$ are Ádám isomorphic. In [1] it was first conjectured that any two isomorphic circulant digraphs are Ádám isomorphic, but in subsequent papers more attention was paid to the corresponding statement for circulant graphs. For instance, Djokovic [8] and Turner [18] independently proved that Ádám's conjecture is true for circulant graphs with prime order, and this is also the case for circulant digraphs [9]. The first counterexamples to this conjecture, both for graphs and digraphs were given by

Elpas and Turner in [9]. In [2], Alspach and Parsons characterized, in terms of a condition on automorphism groups, the validity of Ádám's conjecture for a given order m. In particular, the authors used this characterization to show that it holds for $m = p_1 p_2$ where p_1 and p_2 are different primes. In [5], Boesch and Tindell conjectured that all isomorphic 2-step circulant graphs are Ádám isomorphic. This was independently proved in [7] and [20]. The same result for 2-step circulant digraphs was given in [12]. In fact, Delorme, Favaron and Mahéo [7] proved some more general results concerning Cayley (di)graphs of Abelian groups. Using our terminology, they are stated in the following theorem.

Theorem 3.1 ([7]) *Let $M \in Z^{n*n}$ and $M' \in Z^{n'*n'}$ and suppose that $A = \{\mathbf{a}_1, \mathbf{a}_2\}$ and $A' = \{\mathbf{b}_1, \mathbf{b}_2\}$ are generating sets for Z^n/MZ^n and $Z^{n'}/M'Z^{n'}$, respectively. Then the two (connected) multidimensional circulant digraphs $G(M; A)$ and $G(M'; A')$ are isomorphic iff they are Ádám isomorphic, except in the case when there exist two group isomorphisms*

$$\phi : Z^n/MZ^n \longrightarrow Z/2\eta Z \times Z/2Z, \ \ \eta \in Z^+$$

and

$$\phi' : Z^{n'}/M'Z^{n'} \longrightarrow Z/4\eta Z$$

such that $\phi(A) = \{(1,0)^\top, (1,1)^\top\}$ and $\phi'(A') = \{1, 2\eta+1\}$. (In this case the two digraphs are isomorphic but, clearly, they are not Ádám isomorphic.) Moreover, this result is also true for connected multidimensional circulant graphs if we change A and A' by $\pm A$ and $\pm A'$, respectively. $\square$

Note that the exceptional case $\{Z/2\eta Z \times Z/2Z, \ \mathbf{a}_1 = (1,0)^\top, \mathbf{a}_2 = (1,1)^\top\}$ could also be characterized by the defining relations $\mathbf{a}_1 + \mathbf{a}_2 = \mathbf{a}_2 + \mathbf{a}_1$ (Abelian group), $2\eta\mathbf{a}_1 = 0$ and $2\mathbf{a}_1 = 2\mathbf{a}_2$. Moreover, this last relation is equivalent to writing $o(\mathbf{a}_1 - \mathbf{a}_2) = 2$ (which holds indeed if we substitute the above values in (9)).

Let $H = MV$ be the Hermite normal form of the matrix $M \in Z^{n*n}$. Let $S = \mathrm{diag}(s_1, s_2, \ldots, s_n) = UMV$ be its Smith normal form with $s_1 = s_2 = \cdots = s_{n-r} = 1$ and consider the $r \times r$ and $r \times n$ matrices S' and U' defined as in Section 2. From the results (3), (4), (6) and (7) given there we have the following theorem.

Theorem 3.2 *The multidimensional circulants $G(M; A)$, $G(H; A)$ and $G(S'; \phi(A))$, where $\phi(A) = \{U'\mathbf{a} : \mathbf{a} \in A\}$, are Ádám isomorphic.* $\square$

9

As an example of application of this theorem, we can again consider the two isomorphic multidimensional circulants with matrices $M = \text{diag}(2, 2, 3)$ and $M' = \text{diag}(2, 6)$ mentioned before.

Corollary 3.3 *Let $G(M; A)$ be a k-dimensional circulant. Then $k \leq r$. In particular, if $r = 1$ ($d_{n-1} = s_{n-1} = 1$) such a (di)graph is a circulant.* $\square$

From the above corollary and Proposition 2.1(b) we get

Corollary 3.4 *Let $G(M; A)$ be a k-dimensional circulant with $m = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ vertices. Then $k \leq \max\{r_i : 1 \leq i \leq t\}$. In particular, if m is square free (that is, m is not divisible by the square of a prime) $G(M; A)$ is a circulant.* $\square$

This coincides with the result obtained by Leighton in [14] for a multidimensional circulant graph $G(M; A)$ with M a diagonal matrix.

In the case of multidimensional 2-step circulants we can give a complete characterization of circulants and, hence, of their dimension.

Theorem 3.5 *Let M be an $n \times n$ matrix with $(n-1)$th determinantal divisor d_{n-1}. Let $A = \{\mathbf{a}_1, \mathbf{a}_2\}$ be a generating set of Z^n/MZ^n. Then the (connected) multidimensional 2-step circulant digraph $G(M; A)$ (respectively, graph $G(M; \pm A)$), on $m = |\det M|$ vertices, is a circulant iff one of the following conditions hold:*
(a) $d_{n-1} = 1$;
or (b) $d_{n-1} = 2$ and $m = 2 \gcd(m, \gcd(mM^{-1}(\mathbf{a}_1 - \mathbf{a}_2)))$;
(respectively, or (c) $d_{n-1} = 2$ and $m = 2 \gcd(m, \gcd(mM^{-1}(\mathbf{a}_1 + \mathbf{a}_2))))$.

Proof. From Theorem 3.1 and Corollary 3.3 it is clear that (a) is a necessary and sufficient condition for $G(M; A)$ or $G(M; \pm A)$ to be a circulant except in the case $Z^n/MZ^n \cong Z/2\eta Z \times Z/2Z$ and $\text{o}(\mathbf{a}_1 - \mathbf{a}_2) = 2$ (or possibly, in the case of graphs, $\text{o}(\mathbf{a}_1 + \mathbf{a}_2) = 2$.) (According to this theorem, in this case we also have a circulant.) But then from the results of Section 2, and in particular (8), condition (b) (or condition (c), in the case of graphs) must hold. $\square$

In [13, 10] it was shown that the study of some distance-related parameters, such as the diameter, of 2-step circulant digraphs is best accomplished by considering them as particular instances of multidimensional circulants digraphs $G(M; \mathbf{e}_1, \mathbf{e}_2)$ with M a 2×2 matrix. Such (strongly connected)

digraphs have been called *commutative 2-step digraphs* [12]. The reason is that the matrix $M = (m_{ij})$ can always be chosen so that the studied parameter is easily related to its entries m_{ij}. (In some cases the same fact is true for 2-step circulant graphs, see [4] and [19].) Hence, it is of some interest to characterize those commutative 2-step (di)graphs which are circulants. As a particular case of Theorem 3.5, the next corollary gives a complete answer to this question.

Corollary 3.6 *Let $M = (m_{ij})$ be a 2×2 integer matrix with $|\det M| = m$. Then the commutative 2-step digraph $G(M; \mathbf{e}_1, \mathbf{e}_2)$ is a circulant digraph iff either*

$$d_1 = \gcd(m_{11}, m_{12}, m_{21}, m_{22}) = 1$$

or

$$d_1 = 2 \ and \ m = 2 \gcd(m, m_{22} + m_{12}, m_{11} + m_{21}). \ \square$$

Theorem 3.5 illustrates the fact that, although the knowledge of the structure of $Z^n / M Z^n$ (Proposition 2.1) gives an upper bound for the dimension of a multidimensional circulant (Corollary 3.3), the computation of its exact value may require more sophisticated and particular techniques. This is also made apparent for the next result, which gives the dimension of the direct product of n circulants, all of them with equal prime number of vertices. The proof is similar to that of Lemma 1 in [14], which was suggested by Lawrence (personal communication to Leighton.)

Theorem 3.7 *Let $G_1 = G(p; A_1), G_2 = G(p; A_2), \ldots, G_n = G(p; A_n)$ be (connected) circulants with $p > 2$ vertices, p a prime. Let $M \in Z^{n*n}$ be the diagonal matrix $\mathrm{diag}(p, p, \ldots p)$ and $A = \{a\mathbf{e}_i : a \in A_i, 1 \le i \le n\}$. Then the multidimensional circulant $G(M; A)$ has dimension n.*

Proof. First note that the (di)graph $G(M; A)$, with vertex-set $V = Z/pZ \times \cdots \times Z/pZ$ (n factors), is nothing more than the cartesian product $G_1 \times \cdots \times G_n$. Let Ω be any regular Abelian subgroup of $AutG(M; A)$, $|\Omega| = |V| = p^n$. By Sabidussi's result it suffices to show that $\Omega \cong Z^n / M Z^n \cong Z/pZ \times \cdots \times Z/pZ$. For some fixed $1 \le i \le n$ and $j \in Z/pZ$, let G_{ij} denote the sub(di)graph of $G(M; A)$ spanned by the vertices whose labels have their ith component equal to j. Now, let us consider the group Ω as acting on the set $\mathcal{G} = \{G_{ij} : 1 \le i \le n, 0 \le j < p\}$. To show that any automorphism $\omega \in \Omega$ preserves the set $\mathcal{G}$ (that is, either $\omega(G_{ij}) \bigcap G_{kl} = \emptyset$ or $\omega(G_{ij}) = G_{kl}$), it suffices to prove that ω preserves the set of n directions. (As expected,

a *direction* is defined as the set of edges whose endvertices only differ in a given coordinate.) To know whether different edges belong to the same direction we can apply the following algorithm:

Choose a vertex $\mathbf{u} \in V$ and consider any shortest odd cycle containing it. Then, all the edges of this cycle clearly belong to one direction, say i. If the cycle has length p, then the sub(di)graph spanned by its p vertices, $G_i(\mathbf{u})$, is the copy of $G_i = G(p; A_i)$ that contains vertex $\mathbf{u}$ and whose edges belong to direction i. Otherwise, we consider an edge of the cycle and look for a different shortest odd cycle (of the same length as before) containing it. In this way we successively find the edges (and vertices) of $G_i(\mathbf{u})$. If, in some step, there is no such a shortest cycle we consider another of the (already found) edges of $G_i(\mathbf{u})$. Because of the nature of G_i, it is not difficult to realize that we eventually find the searched p vertices spanning $G_i(\mathbf{u})$. To find the other sub(di)graphs $G_j(\mathbf{u})$, $j \neq i$, we start again from vertex $\mathbf{u}$ and look, in the same way as before, for shortest odd cycles not containing edges in the already found directions. This is done until no edge incident to $\mathbf{u}$ is left out of discovered directions. To identify the directions of the edges incident to other vertices, different from $\mathbf{u}$, we can apply the following procedure: Consider two adjacent edges with endvertex $\mathbf{u}$ and different directions, say $(\mathbf{z}, \mathbf{u}) \in G_j(\mathbf{u})$ and $(\mathbf{u}, \mathbf{v}) \in G_i(\mathbf{u})$. Look for a shortest cycle containing them, $\mathbf{u}$, $\mathbf{v}$, ..., $\mathbf{z}$, $\mathbf{u}$, (note that its length must be at least 4). Then, the first edge (of the cycle) not in $G_i(\mathbf{u})$ has direction j and, similarly, the last edge not in $G_j(\mathbf{u})$ has direction i. Finally, once the directions of a sufficient number of edges incident to a vertex, say $\mathbf{w}$, have been determined, we can search again for appropriates odd cycles going through it, in order to locate the (di)graphs $G_i(\mathbf{w})$, $i = 1, 2, \ldots, n$.

From the above, the action of an automorphism $\omega \in \Omega$ on V completely determines its action on $\mathcal{G}$. Conversely, let $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in V$. Then $\mathbf{u}$ is the only vertex the sub(di)graphs $G_{iu_i}, 1 \leq i \leq n$, have in common. Hence, the action of ω on $\mathcal{G}$ also determines its action on V.

Let $\mathcal{G}_1, \ldots, \mathcal{G}_k$ be the orbits of $\mathcal{G}$ under the action of Ω. Let Ω_h, $1 \leq h \leq k$, be the restriction of Ω to $\mathcal{G}_h$ with duplicates eliminated. Then, $\Omega \subseteq \Omega_1 \times \cdots \times \Omega_k$ and hence

$$\prod_{h=1}^{k} |\Omega_h| \geq |\Omega| = p^n. \tag{10}$$

Moreover, since Ω_h is Abelian and transitive on $\mathcal{G}_h$, it is also regular. There-

fore $|\Omega_h| = |\mathcal{G}_h|$, $1 \le h \le k$, and then

$$\sum_{h=1}^{k} |\Omega_h| = \sum_{h=1}^{k} |\mathcal{G}_h| = |\mathcal{G}| = np. \qquad (11)$$

In addition, the order of an orbit, $|\Omega_h| = |\mathcal{G}_h|$, divides the order of the permutation group $|\Omega| = p^n$, see [16]. Thus there exist integers $r_h \ge 0$, $1 \le h \le k$, such that $|\Omega_h| = p^{r_h}$, and formulas (10), (11) yield

$$\sum_{h=1}^{k} r_h \ge n; \quad \sum_{h=1}^{k} p^{r_h} = np$$

respectively. Hence, we must have $\sum_{h=1}^{k} pr_h \ge pn = \sum_{h=1}^{k} p^{r_h}$. But, for $p > 2$, $pr_h < p^{r_h}$ if $r_h \ne 1$ and $pr_h = p^{r_h}$ otherwise. Thus $|\Omega_h| = p$ for any $1 \le h \le k$, so that Ω_h is isomorphic to the cyclic group Z/pZ and, from (10), $\Omega \cong Z/pZ \times \cdots \times Z/pZ$ (n factors) as claimed. $\square$

As an example of application of the above theorem, we can state the following special case:

Corollary 3.8 *The cartesian product $K_p \times \cdots \times K_p$ (n factors), and the cartesian product of n p-cycles (directed or not) both have dimension n.* $\square$

In the above examples there is an easy way to know whether edges incident to a given vertex $\mathbf{u}$ belong to the same direction (or to locate the (di)graphs $G_i(\mathbf{u})$), owing to the connected components of the neighbourhood of $\mathbf{u}$ in the case of complete graphs K_p, and to the (shortest) p-cycles in the case of cycles. Another example comes when each set A_i has the property that if $x, y \in A_i$, $x \ne y$, then one at least of the elements $x - y$, $x + y$, $-x + y$, $-x - y$ belongs to A_i (for example, if A_i is stable under multiplication by 2): the directions are then given by the connected components of the neigbourhood of $\mathbf{u}$.

Acknowledgment

References

[1] A. Ádám, Research problem 2-10, *J. Combin. Theory* **2** (1967) 393.

[2] B. Alspach and T.D. Parsons, Isomorphism of circulant graphs and digraphs, *Discrete Math.* **25** (1979) 97-108.

[3] J.-C. Bermond, F. Comellas and D.F. Hsu, Distributed loop computer networks: a survey, to appear in *J. Parallel and Distributed Computing*.

[4] J.-C. Bermond, G. Illiades and C. Peyrat, An optimization problem in distributed loop computer networks, *3rd Int. Conf. Combin. Math.*, New York, U.S.A. June 1985. *Annals of the New York Acad. Science* **555** (1989) 45-55.

[5] F. Boesch and R. Tindell, Circulants and their connectivities, *J. Graph Theory* **8** (1984) 487-499.

[6] G. Chartrand and L. Lesniak, *Graphs and Digraphs*, Wadsworth, Monterrey (1986).

[7] C. Delorme, O. Favaron and M. Mahéo, Isomorphisms of Cayley multigraphs of degree 4 on finite Abelian groups, *European J. Combin.* **13** (1992), *no.* 1, 59-61.

[8] D.Z. Djokovic, Isomorphism problem for a special class of graphs, *Acta Math. Acad. Sci.* Hung. **21** (1970) 267-270.

[9] B. Elpas and J. Turner, Graphs with circulant adjacency matrices, *J. Combin. Theory* **9** (1970) 297-307.

[10] P. Esqué, F. Aguiló and M.A. Fiol, Double commutative-step digraphs with minimum diameters, *Discrete Math.* **114** (1993) 147-157.

[11] M.A. Fiol, Congruences in Z^n, finite Abelian groups and the Chinese remainder theorem, *Discrete Math.* **67** (1987) 101-105.

[12] M.A. Fiol and P. Morillo, Congruences in Z^2 and commutative two step digraphs, *3ème Coll. Int. Theorie des Graphes et Combinatoire*, Marseille, France, June 1986.

[13] M.A. Fiol, J.L.A. Yebra, I. Alegre and M. Valero, A discrete optimization problem in local networks and data alignment, *IEEE Trans. Comput.* **C-36** (1987) 702-713.

[14] F.T. Leighton, Circulants and the characterization of vertex-transitive graphs, *J. Res. Natl. Bur. Stand.* **88** (1983), no. 6, 395-402.

[15] M. Newman, *Integral Matrices*, Pure and Appl. Math. Series Vol. **45**, Ac. Press (1972), New York.

[16] D.J.S. Robinson, *A Course in the Theory of Groups*, Springer- Verlag, New York (1982).

[17] G. Sabidussi, On a class of fixed-point-free graphs, *Proc. Amer. Math. Soc.* **9** (1958) 800-804.

[18] J. Turner, Point-symmetric graphs with a prime number of points, *J. Combin. Theory* **3** (1967) 136-145.

[19] J.L.A. Yebra, M.A. Fiol, P. Morillo and I. Alegre, The diameter of undirected graphs associated to plane tessellations, *Ars Combin.* **20B** (1985) 159-171.

[20] S.C. Zhou, On Ádám isomorphism of circulants, *J. Changsha Railway Inst.* **5** (1987), no. 2, 11-18.