SIAM J. DISCRETE MATH.
Vol. 21, No. 3, pp. 763–784




# CAYLEY DIGRAPHS OF FINITE ABELIAN GROUPS AND MONOMIAL IDEALS*

DOMINGO GÓMEZ†, JAIME GUTIERREZ†, AND ÁLVAR IBEAS†

**Abstract.** In the study of double-loop computer networks, the diagrams known as *L-shapes* arise as a graphical representation of an optimal routing for every graph's node. The description of these diagrams provides an efficient method for computing the diameter and the average minimum distance of the corresponding graphs. We extend these diagrams to multiloop computer networks. For each Cayley digraph with a finite abelian group as vertex set, we define a monomial ideal and consider its representations via its minimal system of generators or its irredundant irreducible decomposition. From this last piece of information, we can compute the graph's diameter and average minimum distance. That monomial ideal is the initial ideal of a certain lattice with respect to a graded monomial ordering. This result permits the use of Gröbner bases for computing the ideal and finding an optimal routing. Finally, we present a family of Cayley digraphs parametrized by their diameter $d$, all of them associated to irreducible monomial ideals.

**Key words.** monomial ideals, Cayley digraph, Gröbner bases, multiloop networks

**AMS subject classifications.** 13P10, 05C25, 68M10

**DOI.** 10.1137/050646056

**1. Introduction.** Let $\Gamma$ be a group and $S \subseteq \Gamma$ a subset. The *Cayley digraph* associated to $(\Gamma, S)$ is a directed graph whose vertex set is $\Gamma$ and whose edge set is $\{(g,h) \in \Gamma^2 \mid g^{-1}h \in S\}$. Every Cayley digraph is vertex-symmetric and its degree equals the number of elements in $S$. These graphs are connected if and only if the set $S$ generates the group. We are dealing with digraphs associated to finite abelian groups, but we are mainly interested in those associated to cyclic groups. Let $N$ be a positive integer and $\mathbb{Z}_N$ the integers modulo $N$. For any subset $S = \{j_1, \ldots, j_r\}$ of this abelian group we denote by $C_N(S) = C_N(j_1, \ldots, j_r)$ the corresponding Cayley digraph (see Figure 1.1), which is called the *circulant digraph* or *multiloop computer network* of jumps $j_1, \ldots, j_r$. It is connected if and only if $\gcd(j_1, \ldots, j_r, N) = 1$. If $S$ is a subset of $\mathbb{Z}_N$ such that for every element in $S$ its inverse also lies in $S$, then $C_N(S)$ is an undirected graph called a *circulant graph* or *distributed multiloop computer network*.

Multiloop networks were first proposed in [32] for organizing multimodule memory services and have a vast number of applications in telecommunication networking, VLSI design, and distributed computation. Their properties, such as diameter and reliability, have been the focus of much research in computer network design; see, for instance, [5, 7, 12, 13, 19, 21, 25, 33].

The *single-loop network* or *ring network* is mathematically trivial. Digraphs with $r = 2$ or *double-loop networks* and their corresponding undirected graphs (*distributed double-loop networks*, with degree four) have been extensively studied; see the surveys [3, 20] and the references therein. When $C_N(j_1, j_2)$ is connected, one can define a *minimum distance diagram* (MDD) as an array with vertex 0 in cell $(0,0)$ and vertex $c$

*Received by the editors November 25, 2005; accepted for publication (in revised form) March 22, 2007; published electronically September 26, 2007. This research was partially supported by the Research Project MTM2004-07086 of the Spanish Ministry of Science. An extended abstract of part of this work appeared in [14].

http://www.siam.org/journals/sidma/21-3/64605.html

†University of Cantabria, E–39071 Santander, Spain (domingo.gomez@unican.es, jaime.gutierrez @unican.es, alvar.ibeas@unican.es).

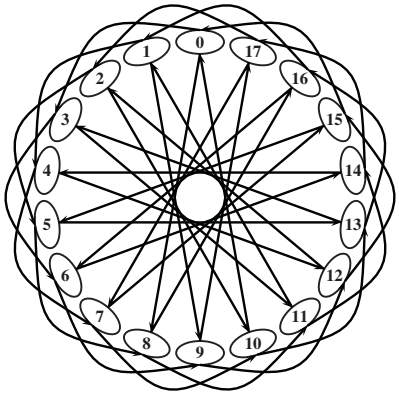


FIG. 1.1. $C_{18}(3,8)$.

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | | | | | | | | | | | |
| 27 | | | | | | | | | | | |
| 13 | | | | | | | | | | | |
| 32 | | | | | | | | | | | |
| 18 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 23 | | | | | | | | | | | |
| 9 | | | | | | | | | | | |
| 28 | | | | | | | | | | | |
| 14 | 19 | 24 | 29 | 1 | 6 | 11 | 16 | 21 | 26 | 31 | 3 |
| 0 | 5 | 10 | 15 | 20 | 25 | 30 | 2 | 7 | 12 | 17 | 22 |

FIG. 1.2. *MDD of* $C_{33}(5,14)$.

in cell $(x, y)$ ($x$ is the column index and $y$ the row index), for a particular choice satisfying $j_1x + j_2y \equiv c \bmod N$, and $x + y$ minimum. One example is shown in Figure 1.2.

The classical work of Wong and Coppersmith [32] presents an algorithm for constructing an MDD of $C_N(j_1, j_2)$ in $O(N^2)$ steps and shows it has an "L" shape. Several characterizations and applications of this idea for describing circulants with desirable properties appear in [1, 8, 9, 13]. However, they do not focus on higher degree digraphs.

Two notable parameters in a graph are the diameter $d$ and the average minimum distance $\bar{d}$. The former represents the worst delay in the communication between two nodes, and the latter represents the average delay. Given an L-shape, it is easy to compute $d$ and $\bar{d}$.

On the other hand, let $d_r(N) := \min\{d(C_N(j_1, \ldots, j_r) \mid j_1, \ldots, j_r \in \mathbb{Z}_N\}$. An important problem is to determine this value and find a specific $C_N(j_1, \ldots, j_r)$ attaining this minimum. The network $C_N(j_1, \ldots, j_r)$ is said to be *optimal* if its diameter equals $d_r(N)$. In some cases, it is difficult to obtain optimal networks; however, one can find general simple functions serving as upper and lower bounds for $d_r(N)$; see [3]. The paper [32] shows $d_2(N) \leq \sqrt{3N} - 2$ and presents a family of circulant digraphs with diameter $2\sqrt{N} - 2$.

In this article we present monomial ideals as a natural tool for studying the MDDs of arbitrary Cayley digraphs, provided that the vertex group is finite and

abelian. Given a graded monomial ordering and a Cayley digraph $(\Gamma, S)$, we build a monomial ideal in the polynomial ring $\mathbb{K}[X_1, \ldots, X_r]$, where $\mathbb{K}$ is an arbitrary field and $r = \#S$. We obtain some properties of this monomial ideal: in particular, a certain generalization of the two-dimensional L-shape is shown. On the other side, it is the initial ideal of a certain lattice. This result permits the use of Gröbner bases for computing the ideal and finding an optimal routing for each pair of nodes. Given the representation of the monomial ideal via its irreducible decomposition, we provide formulae to compute $d$ and $\bar{d}$. We also show a family of circulant digraphs of degree two which coincides with the family obtained in paper [32]. Finally, we present a new and attractive family of circulant digraphs of arbitrary degree parametrized by the diameter $d$, with average minimum distance $d/2$, and whose associated monomial ideals are irreducible.

The paper is divided into nine sections. In section 2 we collect several known facts about monomial ideals, presenting examples and fixing notation for later use. Section 3 presents the key idea of associating monomial ideals to digraphs in order to obtain an MDD, and it also provides an algorithm to construct an MDD for Cayley digraphs with a finite abelian group as vertex set. Section 4 is devoted to presenting the relation between MDDs and the ideal of a lattice. In section 5 we present an algorithm to compute a shortest path between two vertices by means of Gröbner bases. Section 6 presents an algorithm specifically tailored for degree three circulants. It computes the minimal system of generators in $O(s \log N)$ arithmetic operations, where $s$ is the number of generators and $N$ is the number of nodes. Section 7 is dedicated to providing formulae to find the diameter and the average minimum distance. Then section 8 presents a family of multiloop computer networks with an arbitrary number of jumps, parametrized by the diameter $d$, and all of them associated to irreducible monomial ideals. We conclude with a short summary and a discussion of open questions.

**2. Monomial ideals.** Monomial ideals form an important link between commutative algebra and combinatorics. Here we review several basic related results and definitions concerning monomial ideals; see, for instance, [2, 30].

Let $\mathbb{K}$ be an arbitrary field and $\mathbb{K}[X_1, \ldots, X_r]$ the polynomial ring in the variables $X_1, \ldots, X_r$. Throughout the paper, we very often identify monomials of $\mathbb{K}[X_1, \ldots, X_r]$ with vectors of $\mathbb{N}^r$ and use the following notation:

$$\mathbf{x}^{\mathbf{a}} = X_1^{a_1} \cdots X_r^{a_r} \longleftrightarrow \mathbf{a} = (a_1, \ldots, a_r),$$

$$\mathbf{x}^{\mathbf{a}} | \mathbf{x}^{\mathbf{b}} \iff \mathbf{a} = (a_1, \ldots, a_r) \leq \mathbf{b} = (b_1, \ldots, b_r) \overset{\text{def}}{\iff} a_i \leq b_i \quad \forall i = 1, \ldots, r,$$

$$\mathbf{a} = (a_1, \ldots, a_r) \sqsubset \mathbf{b} = (b_1, \ldots, b_r) \overset{\text{def}}{\iff} (b_i > 0 \Rightarrow a_i < b_i)\,,$$

$$\mathbf{e}_i := (0, \ldots, \overset{i}{\smile}{1}, \ldots, 0), \quad \mathfrak{m}^{\mathbf{a}} := (X_i^{a_i} \mid a_i > 0), \quad \mathbf{1} := (1, \ldots, 1).$$

The definition of $\sqsubset$ suits the characterization in (2.2), and when it is employed (in expressions like $\mathbf{a} \sqsubset \mathbf{b}$), we usually have $\mathbf{1} \leq \mathbf{b}$.

A *monomial ideal* is an ideal generated by monomials, i.e., $I \subset \mathbb{K}[X_1, \ldots, X_r]$ is a monomial ideal if there is a subset $A \subseteq \mathbb{N}^r$ such that

$$I = (\mathbf{x}^{\mathbf{a}} \mid \mathbf{a} \in A) = (A).$$

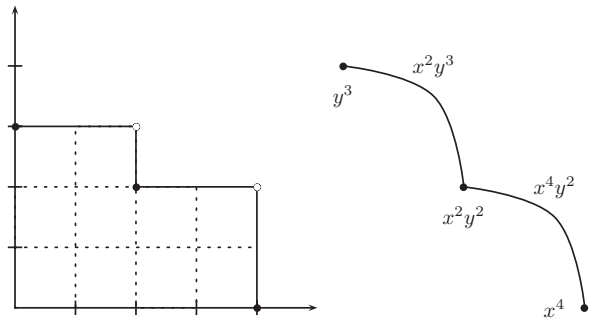


FIG. 2.1. *Staircase diagram and Buchberger's graph.*

There are two standard ways of describing a nontrivial monomial ideal:

- Via the (unique) minimal system of monomial generators $I = (\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s})$, we have

$$\mathbf{x}^{\mathbf{u}} \in I \iff \exists\, i \in \{1, \ldots, s\} \mid \mathbf{a}_i \leq \mathbf{u}. \tag{2.1}$$

- Via the (unique) irredundant decomposition by irreducible monomial ideals $I = \mathfrak{m}^{\mathbf{b}_1} \cap \cdots \cap \mathfrak{m}^{\mathbf{b}_n}$, we have

$$\mathbf{x}^{\mathbf{u}} \notin I \iff \exists\, i \in \{1, \ldots, n\} \mid \mathbf{u} \sqsubset \mathbf{b}_i. \tag{2.2}$$

The so-called staircase diagram is a useful graphical representation of monomial ideals.

*Example* 2.1. The monomial ideal $I_1 := (x^4, x^2y^2, y^3) = (x^2, y^3) \cap (x^4, y^2)$ is represented on the left in Figure 2.1.

There is an algorithm for finding the irredundant irreducible decomposition of a monomial ideal based on Alexander duality; see [27]. An irreducible component $\mathfrak{m}^{\mathbf{a}}$ can be associated to $\operatorname{lcm}(X_1^{a_1}, \ldots, X_r^{a_r}) = \mathbf{x}^{\mathbf{a}}$. On the other hand, if $\mathbb{K}[X_1, \ldots, X_r]/I$ is an artinian ring, then the monomial $\mathbf{x}^{\mathbf{a}}$ associated to the irreducible component $\mathfrak{m}^{\mathbf{a}}$ must coincide with the least common multiple of a subset of the minimal generators of $I$. In the above Example 2.1 we have

$$x^2y^3 = \operatorname{lcm}(x^2y^2, y^3),\ x^4y^2 = \operatorname{lcm}(x^4, x^2y^2).$$

The diagram on the right in Figure 2.1 is called *Buchberger's graph* of the monomial ideal $I_1$; see [28]. At any stage in Buchberger's algorithm for computing Gröbner bases, one considers the S-pairs among the current polynomials and removes those which are redundant; the minimal S-pairs define a graph on the generators of any monomial ideal.

THEOREM 2.2. *Let $I$ be a nontrivial monomial ideal given by a minimal system of generators $I = (\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s})$ and by the irredundant irreducible decomposition $I = \mathfrak{m}^{\mathbf{b}_1} \cap \cdots \cap \mathfrak{m}^{\mathbf{b}_n}$. The following are equivalent:*

1. *$\mathbb{K}[X_1, \ldots, X_r]/I$ is an artinian ring.*
2. *$\forall i = 1, \ldots, r$, one of the generators' exponents is $\mathbf{a}_j = \alpha_i \mathbf{e}_i$ for some $\alpha_i \in \mathbb{N}$.*
3. *$\forall i = 1, \ldots, n,\ \forall j = 1, \ldots, r,\ b_{i,j} > 0$.*

*Proof.* We need to prove that the number of monomials outside $I$ is finite if and only if either of the two last items is satisfied. We do that using the characterizations in (2.1) and (2.2).

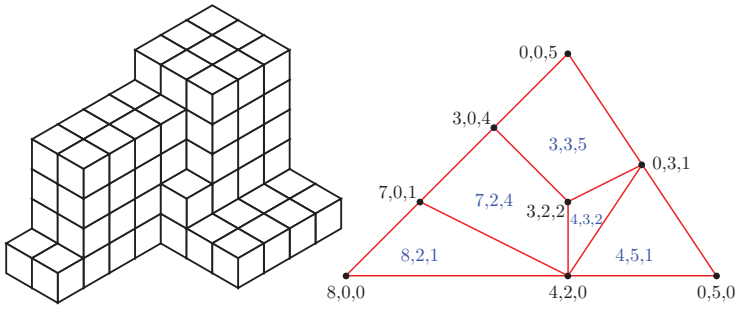


FIG. 2.2. *Planar graph associated to* $I_2$.

If the second item is true, then the number of monomials which do not lie in the ideal is bounded by the product $\prod \alpha_i$. Conversely, if that item is false, there exists an index $i \in \{1, \ldots, r\}$ such that $X_i^\alpha \notin I \ \forall \alpha \in \mathbb{N}$.

The third item is obviously equivalent to $\#\{\mathbf{u} \in \mathbb{N}^r \mid \mathbf{u} \sqsubset \mathbf{b}_i \text{ for some } i \in \{1, \ldots, r\}\} < \infty$. ∎

We conclude this section by illustrating those facts in the following example.

*Example* 2.3. In [28], a planar graph is associated to every monomial ideal in three variables satisfying the conditions in Theorem 2.2. The monomial $\mathbf{x}^\mathbf{b}$ associated to an irreducible component $\mathfrak{m}^\mathbf{b}$ is identified with a connected component in the graph's complement and can be obtained as the least common multiple of the generators in its boundary. In Figure 2.2 we show this construction for the ideal:

$$\begin{aligned} I_2 &:= (x^8, x^4y^2, y^5, y^3z, z^5, x^3z^4, x^7z, x^3y^2z^2) \\ &= (x^8, y^2, z) \cap (x^7, y^2, z^4) \cap (x^4, y^3, z^2) \cap (x^4, y^5, z) \cap (x^3, y^3, z^5). \end{aligned}$$

The description of those relations permits the simplification of some computations on Cayley digraphs, as pointed out in section 7.

**3. Minimum distance diagrams.** There are different ways to relate monomial ideals with graphs (see, for instance, [30]). In this section we propose a new approach to studying Cayley digraphs in which we associate a graph with a monomial ideal. The routing problem for Cayley digraphs reduces to studying paths originating at a fixed vertex, as these graphs are vertex-symmetric. Given a graph associated to $(\Gamma, \{s_1, \ldots, s_r\})$, where $\Gamma$ is finite and abelian, we are looking for the shortest path from node $0_\Gamma$ to node $c \ \forall c \in \Gamma$, i.e., a *minimum distance diagram* (MDD). We can construct the *routing mapping* $R$:

$$\begin{array}{rccc} R: & \mathbb{N}^r & \longrightarrow & \Gamma \\ & \mathbf{a} & \mapsto & a_1 s_1 + \cdots + a_r s_r. \end{array} \tag{3.1}$$

Thus, we need to find a right inverse map of $R$:

$$D: \quad \Gamma \quad \longrightarrow \quad \mathbb{N}^r,$$

such that

$$R(D(c)) = c \quad \forall c \in \Gamma \quad \text{and} \quad \|D(c)\|_1 = \min\{\|\mathbf{x}\|_1 \mid \mathbf{x} \in R^{-1}(c)\}.$$

In general, map $D$ is not unique; see Figure 3.1. This happens when the set $R^{-1}(c)$ contains two or more elements with minimum $\ell_1$-norm for some $c \in \Gamma$.

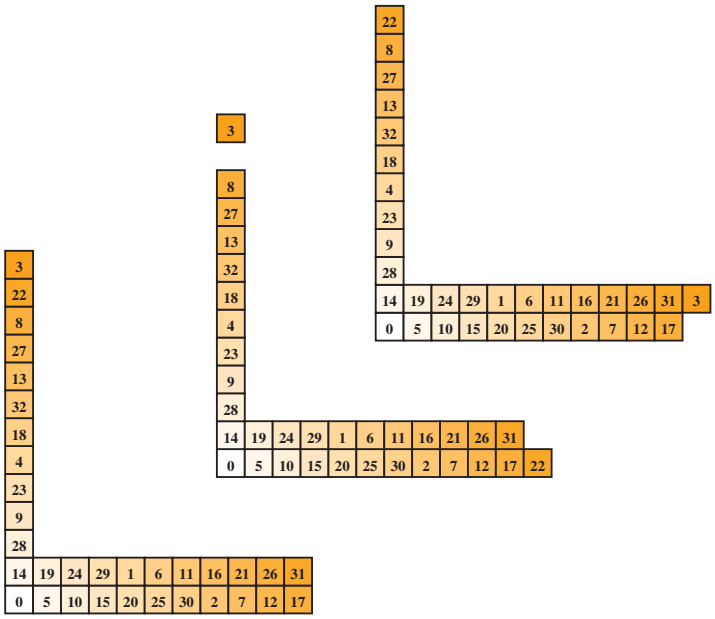


FIG. 3.1. *Different MDDs for* $C_{33}(5, 14)$.

In digraphs of degree two, we can characterize this situation in terms of lattices. Let $\bar{R}$ be the extended map of $R$ from $\mathbb{N}^r$ to $\mathbb{Z}^r$, and $\mathcal{L}$ the kernel of $\bar{R}$.

PROPOSITION 3.1. *Let $D$ be an MDD for $(\Gamma, \{s_1, s_2\})$, where $\Gamma$ is finite and abelian. Then there is a different MDD for the same graph if and only if there exists a vector $(T, -T) \in \mathcal{L}$ with $T > 0$ and $T \leq \max\{a_1, a_2\}$ for some $\mathbf{a} = (a_1, a_2) \in D(\Gamma)$.*

In the example $C_{33}(5, 14)$ from Figure 1.2, the associated lattice is generated by $\{(-16, 1), (-1, -2)\}$:

$$(T, -T) = \alpha(-16, 1) + \beta(-1, -2) \in \mathcal{L} \iff \alpha = \frac{-T}{11},\ \beta = \frac{5T}{11} \in \mathbb{Z} \iff T \in (11).$$

In consequence, this graph admits exactly four MDDs: the L-shape one given in the introduction and the three shown in Figure 3.1. However, only two of them have an "L" shape. These correspond with the only two graded monomial orderings in $\mathbb{K}[X, Y]$.

In accordance with the previous discussion, a well-ordering in $\mathbb{N}^r$ compatible with the norm $\ell_1$ determines a unique MDD. Then, fixing a graded monomial ordering $\prec$, the obtained MDD is

$$D: \begin{array}{ccc} \Gamma & \longrightarrow & \mathbb{N}^r \\ c & \mapsto & \min(R^{-1}(c)). \end{array} \tag{3.2}$$

For each graded monomial ordering we can associate the bijective map $p : \mathbb{N} \longrightarrow \mathbb{N}^r$, such that $n < m \Rightarrow p(n) \prec p(m)$, that is, satisfying

$$p(i) = \min\left(\mathbb{N}^r \backslash \{p(j) \mid j < i\}\right).$$

This map provides a method of constructing the MDD with respect to a fixed monomial ordering. The procedure visits (through $p$) the elements in $\mathbb{N}^r$ corresponding with vertices (elements in $\Gamma$) until all of them are completed.

ALGORITHM 3.1: MDD construction.

**Input**: $\Gamma = \{c_i \mid 0 \le i < N\}$, abelian group, $\{s_1, \ldots, s_r\}$, generating set; $s$.
**Output**: $D(c_i),\ i = 0, \ldots, N-1$.

```
1 D[c_0, ..., c_{N-1}] := ∅̄, S := 0, a := 0;
2 while S < N do
3 |   c := R(a);
4 |   if D(c) = ∅ then
5 |   |   D(c) := a;
6 |   |   S := S + 1;
7 |   end
8 |   a := s(a);
9 end
```

We include in the MDD building method's input the mapping $s$, such that

$$\begin{array}{rccc} s: & \mathbb{N}^r & \longrightarrow & \mathbb{N}^r \\ & \mathbf{a} & \mapsto & p(p^{-1}(\mathbf{a})+1), \end{array}$$

$$\mathbf{a} \prec s(\mathbf{a}),\ (\mathbf{a} \prec \mathbf{b} \Rightarrow s(\mathbf{a}) \preceq \mathbf{b}).$$

Of course, computing the whole diagram $D[0, \ldots, N-1]$ of a circulant cannot be computationally efficient, its size being exponential in the input size. Furthermore, Algorithm 3.1 performs an exhaustive search that can last at most for $\binom{d+r}{d}$ loops until reaching its ending, where $d$ is the graph's diameter. When $r \ll d$, that bound is approximately $\frac{1}{r!}d^r$. The examples in Figure 3.2 illustrate the algorithm's output.

DEFINITION 3.2. *Let $\Gamma$ be a finite abelian group and $(\Gamma, S)$ an associated connected digraph. Let $\prec$ be a graded monomial ordering. The monomial ideal*

$$I_S := (\mathbb{N}^r \backslash D(\Gamma))$$

*is the ideal associated with the graph $(\Gamma, S)$ and the monomial ordering $\prec$.*

In the examples of Figure 3.2 we have two monomial ideals ($J_1$ and $J_2$) associated with $C_{104}(1, 5, 31)$ and with graded lex $x \prec y \prec z$ and $x \prec z \prec y$, respectively:

$$J_1 = (x^5, xy^6, y^7, y^3z^3, z^4, xy^2z^3) = (x^5, y^2, z^4) \cap (x^5, y^6, z^3) \cap (x, y^7, z^3) \cap (x, y^3, z^4),$$
$$J_2 = (x^5, y^4, y^3z^3, z^7, xy^2z^3) = (x^5, y^2, z^7) \cap (x^5, y^4, z^3) \cap (x, y^3, z^7).$$

PROPOSITION 3.3. *With the above notation, we have that $\mathbb{N}^r \backslash D(\Gamma)$ is an ideal of the semigroup $\mathbb{N}^r$.*

*Proof.* Let $\mathbf{a}$ be an element in the ideal generated by $\mathbb{N}^r \backslash D(\Gamma)$. Then $\exists \mathbf{b} \in \mathbb{N}^r$, $\exists \mathbf{z} \in \mathbb{N}^r \backslash D(\Gamma)$ such that $\mathbf{a} = \mathbf{b}+\mathbf{z}$. Now, $\mathbf{z} \notin D(\Gamma)$. Then $\exists \mathbf{u} \in \mathbb{N}^r$, with $R(\mathbf{u}) = R(\mathbf{z})$, $\mathbf{u} \prec \mathbf{z}$. Since $\mathbf{u}+\mathbf{b} \prec \mathbf{z}+\mathbf{b}$ and $R$ is a linear map, $R(\mathbf{u}+\mathbf{b}) = R(\mathbf{a})$ and $\mathbf{a} \notin D(\Gamma)$. ∎

Obviously, $D$ is an injective map and $\#\big(D(\Gamma)\big) = \#\Gamma < \infty$. So, the monomial ideal $I_S$ always contains generators of the form $X_1^{a_1}, \ldots, X_r^{a_r}$; that is, the quotient ring $\mathbb{K}[X_1 \ldots, X_r]/I_S$ is artinian (see Theorem 2.2). We say that an MDD built from a graded monomial ordering is *degenerated* if $I_S$ is an irreducible ideal, that is, when the minimal system of generators of $I_S$ contains only as many generators as the cardinal of $S$. In general, it is not the case as illustrated in the above examples. The paper [32] constructed MDDs in L-shape from circulant digraphs of degree two (i.e., $r = 2$). The following concept is the generalization of L-shapes to arbitrary dimension.

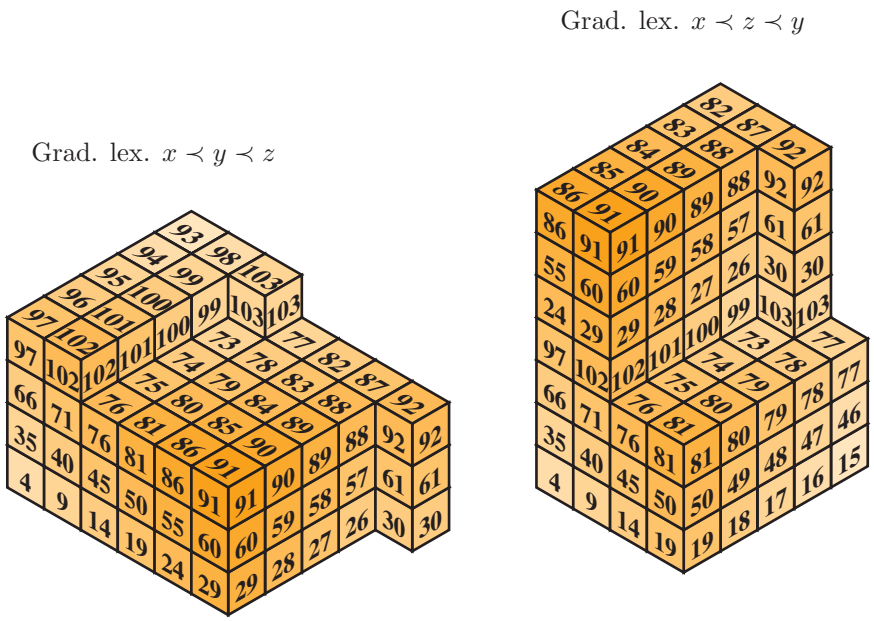


FIG. 3.2. *MDD of* $C_{104}(1, 5, 31)$.

DEFINITION 3.4. *Let $I$ be a monomial ideal and let $A$ be the minimal system of generators of $I$. We say that $I$ is an L-shape if there exists at most one element $\mathbf{x}^{\mathbf{a}} = X_1^{a_1} \cdots X_r^{a_r} \in A$ such that $a_i > 0 \ \forall i = 1, \ldots, r$.*

*We say that an MDD built following Algorithm* 3.1 *is an L-shape if the associated monomial ideal is an L-shape.*

In the examples of Figure 3.2 the generator involving every variable is $xy^2z^3$. We will prove that any MDD built with Algorithm 3.1 is an L-shape. First we need the following technical result.

LEMMA 3.5. *Let $A$ be the minimal system of generators of $I_S$. If the exponent of $\mathbf{x}^{\mathbf{a}} \in A$ has some component $a_i$ positive, then $\mathbf{b} = (b_1, \ldots, b_r) := D(R(\mathbf{a}))$ satisfies $b_i = 0$.*

*Proof.* Since $\mathbf{a}$ is an element of $A$, then $\mathbf{a} \notin D(\Gamma)$. We must have $\mathbf{a} - \mathbf{e}_i \in D(\Gamma)$, because otherwise $\mathbf{a}$ would not be a minimal generator. Now, $\mathbf{b} \prec \mathbf{a}$ and $R(\mathbf{b}) = R(\mathbf{a})$. If we suppose $b_i > 0$, then

$$R(\mathbf{b} - \mathbf{e}_i) = R(\mathbf{a} - \mathbf{e}_i), \ \mathbf{b} - \mathbf{e}_i \prec \mathbf{a} - \mathbf{e}_i,$$

which contradicts $\mathbf{a} - \mathbf{e}_i \in D(\Gamma)$. ∎

Now, we state the main result in this section.

PROPOSITION 3.6. *The output of Algorithm* 3.1 *is an L-shape.*

*Proof.* Let $A$ be the minimal system of generators of $I_S$. If $\mathbf{a} \in A$ is such that $a_i > 0 \ \forall i$, then by Lemma 3.5 we have $R(\mathbf{a}) = R(\mathbf{0}) = 0_\Gamma$.

Moreover, $\mathbf{a} - \mathbf{e}_1 \in D(\Gamma)$, and $R(\mathbf{a} - \mathbf{e}_1) = -s_1$. So, if $\mathbf{a} \in A$ and $\mathbf{b} \in A$ are two generators with every component positive, then $\mathbf{a} - \mathbf{e}_1 = D(-s_1) = \mathbf{b} - \mathbf{e}_1$. That completes the proof. ∎

Now, the problem is to find the list of generators describing the ideal associated to a circulant digraph in a convenient way. The following section answers this question.

**4. Lattice ideals and L-shapes.** In this section we study the initial ideal of the lattice defined by the kernel of the extended routing map $\bar{R}$ and the monomial ideal associated to a circulant graph.

An integral lattice $\mathcal{L}$ of $\mathbb{Z}^r$ is the set of integer linear combinations of some integral vectors; in other words, an integral lattice is a $\mathbb{Z}$-submodule of $\mathbb{Z}^r$. This object has been used to solve many problems in mathematics and computer science (see, for instance, [4, 16, 24, 26]).

For any integral lattice $\mathcal{L} \subset \mathbb{Z}^r$ there is an associated binomial ideal (see [10, 31]):

$$I_{\mathcal{L}} := (\mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} \mid \mathbf{a} \in \mathcal{L}) \subseteq \mathbb{K}[X_1, \ldots, X_r],$$

where $\mathbf{a}^+$ and $\mathbf{a}^-$ are the *positive* and *negative parts* of vector $\mathbf{a}$, that is, the unique vectors with no negative component and such that $\mathbf{a} = \mathbf{a}^+ - \mathbf{a}^-$.

The interesting articles [10, 31] study the combinatorics, geometry, and complexity of Gröbner bases for the ideals $I_{\mathcal{L}}$. In particular, they show that

$$\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I_{\mathcal{L}} \iff \mathbf{a} - \mathbf{b} \in \mathcal{L}. \tag{4.1}$$

Given a Cayley digraph $(\Gamma, S = \{s_1, \ldots, s_r\})$ associated to a finite abelian group, we can extend the routing map $R$ defined in (3.1) from $\mathbb{N}^r$ to $\mathbb{Z}^r$:

$$\begin{array}{rccc} \bar{R}: & \mathbb{Z}^r & \longrightarrow & \Gamma \\ & \mathbf{a} & \mapsto & a_1 s_1 + \cdots + a_r s_r. \end{array}$$

The kernel $\mathcal{L}_S$ of the map $\bar{R}$, i.e.,

$$\mathcal{L}_S := \{(a_1, \ldots, a_r) \in \mathbb{Z}^r \mid a_1 s_1 + \cdots + a_r s_r = 0_\Gamma\},$$

is the lattice associated to $(\Gamma, \{s_1, \ldots, s_r\})$.

Given an integral lattice $\mathcal{L}$ and a monomial ordering $\prec$, for every nonzero binomial $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}} \in I_{\mathcal{L}}$, the *leading* or *initial monomial* with respect to $\prec$ is given by

$$LM(\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}) := \begin{cases} \mathbf{x}^{\mathbf{a}} & \text{if } \mathbf{x}^{\mathbf{a}} \succ \mathbf{x}^{\mathbf{b}}, \\ \mathbf{x}^{\mathbf{b}} & \text{otherwise.} \end{cases}$$

As usual, given a polynomial ideal $J$ in $\mathbb{K}[X_1, \ldots, X_r]$ we denote by $LM(J)$ the monomial ideal generated by the leading monomials of all nonzero elements of $J$, that is,

$$LM(J) := (LM(f) \mid f \in J^*).$$

The following is one of the main results in this section.

PROPOSITION 4.1. *For every graded monomial ordering $\prec$, we have that*

$$LM(I_{\mathcal{L}_S}) = I_S.$$

*Proof.* The ideal $I_{\mathcal{L}_S}$ is generated by binomials of the form $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$. Then it has a Gröbner basis $G$ also consisting of that kind of binomial. Let $\mathbf{x}^{\mathbf{a}}$ be a monomial in $LM(I_{\mathcal{L}_S})$. There exists a binomial $\mathbf{x}^a - \mathbf{x}^b$ in the basis $G$, and by (4.1), $\mathbf{a} - \mathbf{b} \in \mathcal{L}_S$. Now, since $\mathbf{a} \succ \mathbf{b}$ and both paths have the same image by $R$, then $\mathbf{a} \notin D(\mathbb{Z}_N)$. Conversely, let $\mathbf{x}^{\mathbf{a}} \in I_S$. We take $\mathbf{b} := D(R(\mathbf{a})) \prec \mathbf{a}$. It is clear that $\mathbf{a} - \mathbf{b} \in \mathcal{L}_S$, and so $\mathbf{x}^{\mathbf{a}} - \mathbf{x}^{\mathbf{b}}$ is a binomial in $I_{\mathcal{L}_S}$, whose leading monomial is $\mathbf{x}^{\mathbf{a}}$. ∎

Gröbner bases were introduced by Buchberger in his thesis [6] and their use has become widespread in commutative algebra and algebraic geometry. The theory of Gröbner bases is related to several areas in mathematics and computer science; see, for instance, [2, 17, 30]. As a consequence of the previous result we have that if $G$ is a minimal or reduced Gröbner basis of the ideal $I_{\mathcal{L}_S}$, then the leading monomials of the elements of $G$ constitute a minimal system of generators of our MDD. In order to apply Buchberger's algorithm for computing a finite Gröbner basis of an ideal, we need to start with a finite set of generators. In this sense, we must point out that every generating set of binomials for $I_{\mathcal{L}_S}$ corresponds to a generating set of $\mathcal{L}_S$ (see (4.1)), but the converse is not true. Lemma 2.1 of [31] provides a sufficient condition for this converse result to be true.

PROPOSITION 4.2. *Let $C_N(j_1, \ldots, j_r)$ be a connected circulant graph with associated lattice $\mathcal{L}$. We have $I_{\mathcal{L}} = (X_1^N X_2^N \cdots X_r^N - 1, \quad \mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} \mid \mathbf{a} \in U)$, where*

$$U := \{(N\alpha_1, \ldots, N\alpha_r), (\alpha_1 j_1 - 1, \alpha_2 j_2, \ldots, \alpha_r j_r), (\alpha_1 j_1, \alpha_2 j_2 - 1, \ldots, \alpha_r j_r), \ldots, (\alpha_1 j_1, \ldots, \alpha_{r-1} j_{r-1}, \alpha_r j_r - 1)\},$$

*and $\beta, \alpha_i \in \mathbb{Z}, (i = 1, \ldots, r)$, satisfying $1 = \alpha_1 j_1 + \cdots + \alpha_r j_r + \beta N$.*

*Proof.* The proof follows from [31, Lemma 2.1] and a simple linear algebra exercise. ∎

Using Propositions 4.1 and 4.2 we can compute a minimal system of generators of $I_S$ for circulant digraphs. The paper [31] also contains results on the complexity of computing the reduced Gröbner basis of lattice ideals and on its size. In particular, it provides an upper bound for the number of elements and shows an example lattice $\mathcal{L}$ with exponential size in the bit complexity of a basis of $\mathcal{L}$. Nevertheless, we must cite program 4*ti*2, which is extremely efficient in computing the reduced Gröbner basis of binomials ideals. That software is available at http://www.4ti2.de; see [18].

**5. Optimal routing.** In this section we show an algorithm for computing a shortest path between two vertices for any Cayley digraph with a finite abelian group as vertex set using a finite Gröbner basis of $I_{\mathcal{L}_S}$.

Message routing is a basic function in communication networks. The problem is to find a route along which messages should be sent. The routing algorithm dictates token passing strategies in communication networks.

Given a pair of nodes $(t, s)$ in a graph, there are several paths which join the origin $t$ and the destination $s$. We are interested in *optimal paths*, i.e., those with minimum length. For general graphs, finding a shortest path between two vertices is a well-known and important problem. Efficient polynomial time algorithms have been developed for various routing problems. However, for the family of circulant graphs, there is an important distinction to be made, and that concerns the natural input size to a problem. For an arbitrary graph it is common to consider the input size to be $O(N^2)$, which is the number of bits in its adjacency matrix. However, any circulant graph can be described by only $r$ integers. In this representation the input size is $O(r \log N)$. Thus, polynomial time algorithms for general graphs may exhibit exponential complexity in the special case of circulant graphs for this compact input representation. In [7] it is shown that the shortest path problem is NP-hard for this concise representation. The paper [15] presents very efficient algorithms for computing a shortest path for circulants with two jumps.

As we have already pointed out, in our case the routing problem is reduced to pairs of nodes $(0_\Gamma, j)$ where the starting point is fixed. Using the well-known extended Euclidean algorithm we compute a path $\mathbf{c}$ from vertex $0_\Gamma$ to vertex $j$ if it exists.

We can apply the general integer programming techniques (see [29]) to find a shortest path for circulant digraphs as follows.

LEMMA 5.1. *Any shortest path from* 0 *to* $j$ *in* $C_N(j_1, j_2, \ldots, j_r)$ *is a solution to the following integer program:* $\min\{\mathbf{d}\cdot\mathbf{x} | A\mathbf{x} \geq \mathbf{b}, \mathbf{x} \in \mathbb{Z}^{r+1}\}$, *where* $\mathbf{x} = (x_1, x_2, \ldots, x_r, y) \in \mathbb{Z}^{r+1}$, $\mathbf{d} = (1, 1, \ldots, 1, 0) \in \mathbb{Z}^{r+1}$, $\mathbf{b} = (j, -j, 0, \ldots, 0) \in \mathbb{Z}^{r+2}$, *and*

$$A = \begin{pmatrix} j_1 & j_2 & \ldots & j_r & N \\ -j_1 & -j_2 & \ldots & -j_r & -N \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \in \mathbb{Z}^{(r+2)\times(r+1)},$$

*and conversely.*

So, with the number of jumps $r$ fixed, we can derive an algorithm to compute a shortest path in circulant digraphs requiring $O(r + \log r \log N)$ arithmetic operations on rational numbers of size $O(\log N)$; see [11, 15, 22, 23].

The main result of this section is the following.

PROPOSITION 5.2. *Let* $G$ *be a Gröbner basis of the ideal* $I_{\mathcal{L}_S}$ *with respect to any graded monomial ordering* $\prec$, *and let* $\mathbf{c}$ *be a path (not necessarily a shortest one) in* $R^{-1}(j)$. *Then the normal form of* $\mathbf{x}^{\mathbf{c}} - 1$ *with respect to* $G$ *is* $\mathbf{x}^{\mathbf{d}} - 1$, *where* $\mathbf{d}$ *is the shortest path from vertex* $0_\Gamma$ *to vertex* $j$ *with respect to the monomial ordering* $\prec$.

*Proof.* We have $\mathbf{c} - \mathbf{d} \in I_{\mathcal{L}}$, which implies $(\mathbf{x}^{\mathbf{c}} - 1) - (\mathbf{x}^{\mathbf{d}} - 1) \in I_{\mathcal{L}_S}$. Clearly, $\mathbf{x}^{\mathbf{d}} - 1$ is a normal form, because $\mathbf{x}^{\mathbf{d}} \notin I_S$. ∎

This result provides a convenient algorithm to compute a shortest path and then to design optimal routings.

**6. An algorithm of MDD for triple-loop computer networks.** In this section we provide an algorithm specifically tailored for computing the minimal system of generators for a triple-loop computer network, which requires $O(s \log N)$ arithmetic operations, where $s$ is the number of generators of the minimal system.

The case of degree two circulants is very simple. We always have two generators of the form $x^a, y^b$, and there are two possibilities: there is one other generator $x^c y^d$ ($c < a,\ d < b$) or those two are the only generators (irreducible ideal case). We can obtain this representation in an efficient way, for instance, using the algorithm in [8].

We present Algorithm 6.1 to compute the minimal generators of the ideal $I_S$ associated to a circulant digraph of degree three. Once we have fixed a graded monomial ordering, we need as an intermediate step a procedure to decide, given a path $\mathbf{b}$, whether or not it lies in the MDD. For $\mathbf{b} \in \mathbb{N}^3$, we define the Boolean function $P(\mathbf{b})$ to be the truth value of $D(R(\mathbf{b})) = \mathbf{b}$.

Algorithm 6.1 works by computing, one by one, every generator in the ideal's minimal system. For each generator we use one or two binary searches. So, its complexity is $O(s\ \log N)$ steps, where $s$ is the number of generators. In the worst case, an upper bound for $s$ is $2N + 1$; see [31]. In practice, most of the time consumed in each step is used calling up the boolean function $P$, which will be proved to be computable in polynomial time.

PROPOSITION 6.1. *Algorithm* 6.1 *is correct.*

*Proof.* By Theorem 2.2, among the generators of $I_S$ are monomials of the form $x^a$, $y^b$, and $z^c$. These are computed in lines 2–14 (part I). Lines 15–44 (part II) find every

ALGORITHM 6.1: MDD description. The three jumps case. (I)

**Input**: $j_1, j_2, j_3, N \in \mathbb{N},\ \gcd(j_1, j_2, j_3, N) = 1,\ P$.
**Output**: $\mathbf{a}_1, \ldots, \mathbf{a}_s \in \mathbb{N}^3 \mid (\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_s}) = (\mathbb{N}^3 \backslash D(\mathbb{Z}_N))$; $a_i \not\leq a_j$ if $i \neq j$.

```
1  k := 1;
2  for i = 1, 2, 3 do
3  |  m := 0, M := N.;
4  |  while M − m > 1 do
   |  |  l := ⌊(m + M)/2⌋;
5  |  |
6  |  |  if P(l e_i) then
7  |  |  |  m := l;
8  |  |  else
9  |  |  |  M := l;
10 |  |  end
11 |  end
12 |  a_k := M e_i;
13 |  k := k + 1;
14 end
```

generator involving two variables, and lines 45–54 (part III) work for the (possibly missing) generator with all three variables.

The key fact is that if $(a, 0, 0)$ is one of the generators we are looking for in the first part, then for any $l \in \mathbb{N}$, $P(l, 0, 0) \iff l < a$. We can perform a binary search to obtain the three generators.

In the second part, we start with generators involving the first two variables, continue with the one without the $y$, and so on. For instance, for the first case, we look at the generator $(0, a, 0)$ found in the previous step. Then if $(q, *, 0)$ is the generator with lowest first component involving the first two variables, we can use $P(l, a-1, 0) \iff l < q$ to find $q$ by a binary search. Once this is done, we fix the generator's second component $*$, aided by $P(q, l, 0) \iff l < *$. In a similar way, we continue to discover all the generators in this form.

Finally, there is only one generator possibly missing, which must satisfy $R(\mathbf{b}) = 0$. So, steps 45–47 find a candidate. This possible generator is checked for possible irredundancy in the remaining lines. □

To finish the method, we need a way to decide $P(\mathbf{b})$. In fact, we can use integer programming to solve the problem of finding a shortest path; see Lemma 5.1.

However, we need to find the minimum element according to the ordering $\prec$. We can follow Algorithm 6.2, which takes as input a matrix $A$ to represent the monomial ordering (see [2]) in this way:

$$\mathbf{x} \prec \mathbf{y} \iff A\mathbf{x} \underset{\text{lex}}{<} A\mathbf{y}.$$

We represent the matrix rows with subindices: $A_1, \ldots, A_m$. Then we obtain Algorithm 6.2.

PROPOSITION 6.2. *Algorithm* 6.2 *is correct.*

*Proof.* Steps 1–6 are clear. The only trouble arises when the vector that we get as result of the integer programming–type search $\mathbf{c}$ has the same $\ell_1$-norm as $\mathbf{b}$,

ALGORITHM 6.1: MDD description. The three jumps case. (II)

```
for i = {(1,2),(1,3),(2,3)} do
    T := a_{i[2]}[i[2]] − 1;
    Q := 0;
    repeat
        m := Q, M := a_{i[1]}[i[1]];
        while M − m > 1 do
            l := ⌊(m + M)/2⌋;
            if P(l e_{i[1]} + T e_{i[2]}) then
                m := l;
            else
                M := l;
            end
        end
        Q := M;
        if Q < a_{i[1]}[i[1]] then
            m := 0, M := T;
            while M − m > 1 do
                l := ⌊(m + M)/2⌋;
                if P(Q e_{i[1]} + l e_{j[2]}) then
                    m := l;
                else
                    M := l;
                end
            end
            a_k := Q e_{i[1]} + l e_{i[2]};
            k := k + 1;
            T := l − 1;
        end
    until Q = a_{i[1]}[i[1]] ;
end
```

ALGORITHM 6.1: MDD description. The three jumps case. (III)

```
c := N − j_1 mod N;
b := D(c);
b[1] := b[1] + 1;
for i = 1, ..., k − 1 do
    if a_i ≤ b then
        k := k − 1;
        STOP;
    end
    a_k := b;
end
```

ALGORITHM 6.2: Deciding if a given path lies in an MDD.

**Input**: $j_1, \ldots, j_r, N \in \mathbb{N},\ \gcd(j_1, \ldots, j_r, N) = 1,\ A \in \mathbb{R}^{m \times r},\ \mathbf{b} \in \mathbb{N}^r$.
**Output**: Boolean value $P(\mathbf{b}) := (\mathbf{b} = D(R(\mathbf{b})))$.

```
1  Execute an integer programming–type algorithm to get c, an element with
   minimum ℓ1-norm in R^{-1}(R(b));
2  if ||c||_1 < ||b||_1 then
3  |  OUTPUT false;
4  else
5  |  if c ≺ b then
6  |  |  OUTPUT false;
7  |  else
8  |  |  Compute a basis for the lattice
   |  |  L := {c ∈ N^r | < c, (j_1, ..., j_r) >= 0, < c, (1, ..., 1) >= 0};
9  |  |  for i = 1, ..., m do
10 |  |  |  Set * = (< A_i, b > −(min A)/2);
11 |  |  |  Set the boolean value α, depending on whether there is a point in
   |  |  |  the set (b + L) ∩ N^r ∩ {c ∈ N^r | < c, A_1 >=< b, A_1 >, ..., <
   |  |  |  c, A_{i−1} >=< b, A_{i−1} >, < c, A_i >≤ *};
12 |  |  |  if α then
13 |  |  |  |  OUTPUT false;
14 |  |  |  end
15 |  |  end
16 |  |  OUTPUT true;
17 |  end
18 end
```

and $\mathbf{b} \preceq \mathbf{c}$. In this case, we have to decide whether there is another vector $\mathbf{d} \in \mathbb{N}^r$, satisfying

$$\|\mathbf{d}\|_1 = \|\mathbf{b}\|_1 = \|\mathbf{c}\|_1,\ \mathbf{d} \prec \mathbf{b}.$$

Obviously, if such a vector $\mathbf{d}$ does exist, it lies in the set $(\mathbf{b} + \mathcal{L}) \cap \mathbb{N}^r$. So, we check in steps 9–14 if there is another path $\mathbf{c}$ such that $A\mathbf{c} <_{\text{lex}} A\mathbf{b}$. ∎

**7. Diameter and average minimum distance.** Two notable parameters in a digraph are the diameter and the average minimum distance. The former represents the worst delay in the communication between two nodes, and the latter represents the average delay. In this section we show formulae to compute those parameters in a circulant digraph given by the irredundant irreducible decomposition of the monomial ideal $I_S$.

**7.1. Diameter.** Given an MDD of a digraph $(\Gamma, S)$, it is easy to obtain the diameter

$$d = \max\{\|\mathbf{a}\|_1 \mid \mathbf{a} \in D(\Gamma)\}.$$

The description of the monomial ideal $I_S$ in terms of its irreducible components permits a simplification.

PROPOSITION 7.1. *Let* $\mathfrak{m}^{\mathbf{b}_1} \cap \cdots \cap \mathfrak{m}^{\mathbf{b}_n}$ *be the irredundant irreducible decomposition of the ideal* $I_S$. *Then*

$$d = \max\{\|\mathbf{b}_i\|_1 - r \mid i = 1, \ldots, r\}.$$

*Proof.* If we define the *corners* of $I_S$ as

$$E(D) := \{\mathbf{a} \in D(\Gamma) \mid \mathbf{a} + \mathbf{e}_i \notin D(\Gamma)\ \forall i = 1, \dots, r\},$$

then it is clear that $d = \max\{\|\mathbf{a}\|_1 \mid \mathbf{a} \in E(D)\}$. We will prove that $\{\mathbf{a} + \mathbf{1} \mid \mathbf{a} \in E(D)\} = \{\mathbf{b}_1, \dots, \mathbf{b}_n\}$.

Let $i \in \{1, \dots, n\}$. By Theorem 2.2, we have $\mathbf{b}_i \geq \mathbf{1}$. Let us check that $\mathbf{a} := \mathbf{b}_i - \mathbf{1} \in E(D)$. If $\mathbf{x}^{\mathbf{a}} \in I_S$, we would have $\mathbf{x}^{\mathbf{a}} \in \mathfrak{m}^{\mathbf{b}_i} \Rightarrow \exists j \in \{1, \dots, r\} \mid a_j \geq b_{ij} = a_j + 1$. So, $\mathbf{x}^{\mathbf{a}} \notin I_S$. Further, if $\exists j \in \{1, \dots, r\}$ such that $\mathbf{x}^{\mathbf{a}+\mathbf{e}_j} \notin I_S$, then $\exists k \in \{1, \dots, n\},\ k \neq i \mid \mathbf{x}^{\mathbf{a}+\mathbf{e}_j} \notin \mathfrak{m}^{\mathbf{b}_k} \Rightarrow \mathbf{a} + \mathbf{e}_j \sqsubset \mathbf{b}_k \Rightarrow \mathbf{b}_i \leq \mathbf{b}_k \Rightarrow \mathfrak{m}^{\mathbf{b}_k} \subseteq \mathfrak{m}^{\mathbf{b}_i}$. So, $\mathbf{x}^{\mathbf{a}+\mathbf{e}_j} \in I_S$ and $\mathbf{a} \in E(D)$.

On the other hand, let $\mathbf{a} \in E(D)$. First we will see that $I_S \subseteq \mathfrak{m}^{\mathbf{a}+\mathbf{1}}$. Suppose that $\mathbf{x}^{\mathbf{u}} \in I_S \backslash \mathfrak{m}^{\mathbf{a}+\mathbf{1}}$. Then $\mathbf{a} + \mathbf{1} > \mathbf{u} \Rightarrow \mathbf{a} \geq \mathbf{u}$. Since $\mathbf{x}^{\mathbf{u}} \in I_S$, then $\mathbf{x}^{\mathbf{a}} \in I_S$; this is a contradiction because $\mathbf{a} \in E(D)$. If $\mathfrak{m}^{\mathbf{a}+\mathbf{1}}$ were not an irreducible component in the decomposition of $I_S$, it would be satisfied:

$$\exists j \in \{1, \dots, n\} \mid \mathfrak{m}^{\mathbf{b}_j} \supsetneq \mathfrak{m}^{\mathbf{a}+\mathbf{1}} \Rightarrow \left\{ \begin{array}{l} \mathbf{a} + \mathbf{1} \leq \mathbf{b}_j \\ \mathbf{a} + \mathbf{1} \neq \mathbf{b}_j \end{array} \right\}$$
$$\Rightarrow \exists i \in \{1, \dots, r\} \mid \mathbf{x}^{\mathbf{a}+\mathbf{e}_i} \in D(\Gamma). \qquad \square$$

**7.2. Average minimum distance.** Again, given an MDD of a digraph, it is easy to obtain the average minimum distance. Let $N$ be the number of nodes.

$$\bar{d} = \frac{\sum_{c \in \Gamma} \|D(c)\|_1}{N} = \frac{\sum_{\mathbf{x}^{\mathbf{u}} \notin I_S} \|\mathbf{u}\|_1}{N}.$$

The following result provides a formula for computing $\bar{d}$ in digraphs with a degenerated MDD.

LEMMA 7.2. *Let* $I_S = \mathfrak{m}^{\mathbf{a}+\mathbf{1}} = \mathfrak{m}^{\mathbf{b}}$. *Then*

$$\sum_{\mathbf{x}^{\mathbf{u}} \notin I_S} \|\mathbf{u}\|_1 = \frac{b_1 \cdots b_r}{2}(b_1 + \cdots + b_r - r) = \frac{a_1 + \cdots + a_r}{2} \prod_{i=1}^{r} (a_i + 1).$$

*Proof.* By Proposition 7.1, we have

$$d = \|\mathbf{b}\|_1 - r = \|\mathbf{a}\|_1.$$

On the other hand,

$$\mathbf{u} = (u_1, \dots, u_r) \in D(\Gamma) \iff \forall i \in \{1, \dots, r\},\ u_i < b_i.$$

We define the following relation in $D(\Gamma)$: $(u_1, \dots, u_r) \equiv (a_1 - u_1, \dots, a_r - u_r)$. So, every equivalence class contains two elements (whose degrees add up to $\|\mathbf{a}\|_1$) or only one. This last happens if and only if $\forall i \in \{1, \dots, r\},\ u_i = a_i - u_i \Rightarrow 2\|\mathbf{u}\|_1 = \|\mathbf{a}\|_1$. We can state the following:

$$\sum_{\mathbf{x}^{\mathbf{u}} \notin I} \|\mathbf{u}\|_1 = \frac{N}{2} d,$$

and the proof is complete. $\square$

*Note* 7.3. In the above case, that is, when $I_S$ is an irreducible ideal, we have $\bar{d} = d/2$.

To discuss the general case we introduce some new notation. Let $\mathfrak{m}^{\mathbf{b}_1} \cap \cdots \cap \mathfrak{m}^{\mathbf{b}_n}$ be the irreducible decomposition of the monomial ideal $I_S$; so we define

$$\mathbf{d}_\Delta := \text{exponent}\left(\gcd(\mathbf{x}^{\mathbf{b}_i} \mid i \in \Delta)\right) \ \forall \Delta \subseteq \{1, \ldots, n\},\ \Delta \neq \emptyset.$$

$$\sigma(\mathbf{u}) := \frac{u_1 \cdots u_r}{2}(u_1 + \cdots + u_r - r).$$

Our next goal is to find a formula for the average minimum distance. We will apply the general inclusion-exclusion principle as follows.

PROPOSITION 7.4. *Let $\mathfrak{m}^{\mathbf{b}_1} \cap \cdots \cap \mathfrak{m}^{\mathbf{b}_n}$ be the irreducible decomposition of the ideal $I_S$. We have*

$$\sum_{\mathbf{x}^{\mathbf{u}} \notin I_S} \|\mathbf{u}\|_1 = \sum_{\emptyset \subsetneq \Delta \subseteq \{1,\ldots,n\}} (-1)^{\#\Delta+1} \sigma(\mathbf{d}_\Delta).$$

*Proof.* Applying Lemma 7.2, we obtain

$$\sum_{\emptyset \subsetneq \Delta \subseteq \{1,\ldots,n\}} (-1)^{\#\Delta+1} \sigma(\mathbf{d}_\Delta) = \sum_{\Delta} (-1)^{\#\Delta+1} \sum_{\mathbf{x}^{\mathbf{u}} \notin \mathfrak{m}^{\mathbf{b}_i} \ \forall i \in \Delta} \|\mathbf{u}\|_1.$$

If $\mathbf{x}^{\mathbf{u}} \notin I_S$, that is, if $\exists i \in \{1, \ldots, n\} \mid \mathbf{x}^{\mathbf{u}} \notin \mathfrak{m}^{\mathbf{b}_i}$, then the above sum includes $\|\mathbf{u}\|_1$ exactly once, as seen in the following equation, where $j = \#\{j \in 1, \ldots, n\} \,|\, \mathbf{x}^{\mathbf{u}} \notin \mathfrak{m}^{\mathbf{b}_i}$:

$$\binom{j}{1} - \binom{j}{2} + \cdots + (-1)^{j+1} \binom{j}{j} = 1.$$

This completes the proof. ∎

Considering the ideal $I_1 = (x^4, x^2y^2, y^3)$ from Example 2.1, the sum of the degrees of the monomials outside this ideal is (see Figure 7.1)

$$\sum_{\mathbf{x}^{\mathbf{u}} \notin I_1} \|\mathbf{u}\|_1 = \sigma(2,3) + \sigma(4,2) - \sigma(2,2) = 9 + 16 - 4 = 21.$$

The several results introduced in section 2 permit a strong reduction in the number of sum terms we need to consider in the expression of Proposition 7.4. For instance, if we consider Example 2.3, Proposition 7.4 solves (see Figure 7.2)

$$\begin{aligned}
\sum_{\mathbf{x}^{\mathbf{u}} \notin I} \|\mathbf{u}\|_1 = {} & \sigma(8,2,1) + \sigma(7,2,4) + \sigma(3,3,5) + \sigma(4,3,2) + \sigma(4,5,1) \\
& - [\sigma(7,2,1) + \sigma(3,2,1) + \sigma(4,2,1) + \sigma(4,2,1) + \sigma(3,2,4) \\
& + \sigma(4,2,2) + \sigma(4,2,1) + \sigma(3,3,2) + \sigma(3,3,1) + \sigma(4,3,1)] \\
& + \sigma(3,2,1) + \sigma(4,2,1) + \sigma(4,2,1) + \sigma(3,2,1) + \sigma(3,2,1) \\
& + \sigma(4,2,1) + \sigma(3,2,2) + \sigma(3,2,1) + \sigma(4,2,1) + \sigma(3,3,1) \\
& - [\sigma(3,2,1) + \sigma(3,2,1) + \sigma(4,2,1) + \sigma(3,2,1) + \sigma(3,2,1)] + \sigma(3,2,1) \\
= {} & \sigma(8,2,1) + \sigma(7,2,4) + \sigma(3,3,5) + \sigma(4,3,2) + \sigma(4,5,1) \\
& - [\sigma(7,2,1) + \sigma(3,2,4) + \sigma(4,2,2) + \sigma(3,3,2) + \sigma(4,3,1)] \\
& + s(3,2,2) = 454.
\end{aligned}$$

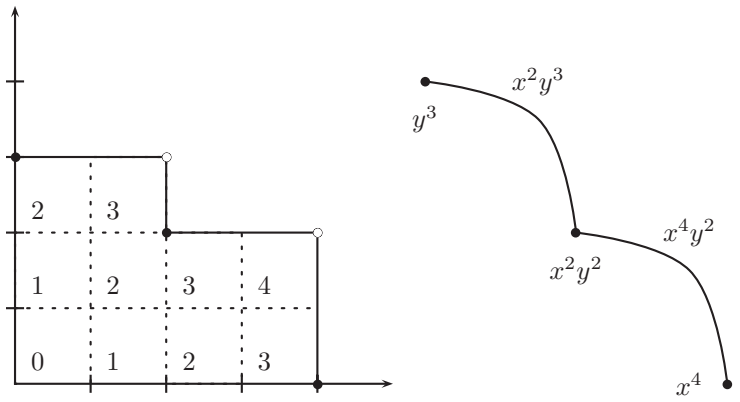


FIG. 7.1.

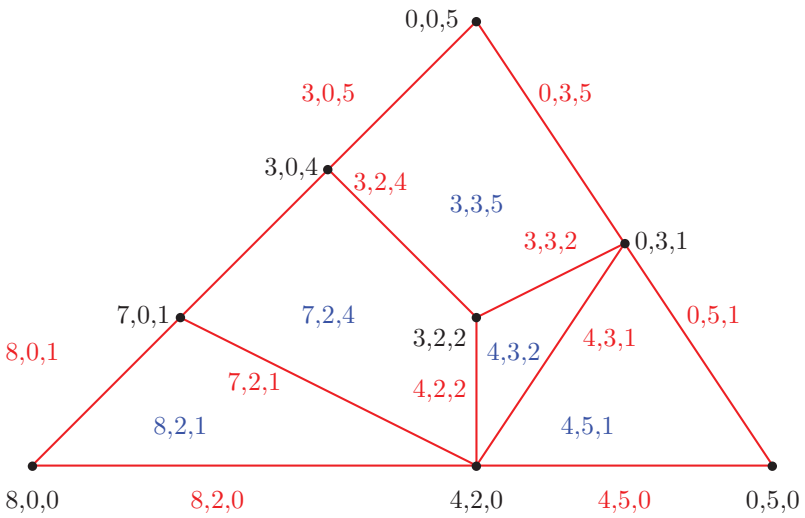


FIG. 7.2.

Clearly, if $\mathbf{b} \in \mathbb{N}^r$ has a zero coordinate, then $\sigma(\mathbf{b}) = 0$. This fact produces several cancellations in the formula of Proposition 7.4. We end up with a sum of the simplex labels, affected with the sign: + for faces, − for edges, and + for nodes.

In Cayley digraphs of degree two the associated monomial ideal has only one or two irreducible components (see Proposition 3.6). Then the computation of the average minimum distance is immediate. For digraphs of degree three we can follow this strategy:

- Construct the Miller–Sturmfels graph $G$ as in the previous examples such that each irreducible component corresponds with the least common multiple of some generators of the minimal system.
- Let $E$ be the set of all edges, $F$ the set of faces, and $N$ the set of vertices of $G$:

$$\bar{d} = \frac{1}{N}\left(\sum_{e\in F}\sigma(e) - \sum_{e\in E}\sigma(e) + \sum_{e\in N}\sigma(e)\right).$$

**8. Degenerated L-shapes.** We recall that an MDD is degenerated if the associated monomial ideal is irreducible, that is, of the form $\left(X_1^{\alpha_1}, \ldots, X_r^{\alpha_r}\right)$. In general, the family of graphs having this property does not have optimal properties according to the ratio nodes/diameter. In this section we present families of circulant digraphs having a degenerated MDD and with a relatively small diameter.

PROPOSITION 8.1. *Let $a, s, k$ be natural numbers such that $\gcd(a, s) = 1$ and $a < s$. The monomial ideal associated with $C_{sk}(a, s)$ is $I_S = (x^s, y^k)$ for any monomial ordering.*

*Proof.* Since $\mathbb{K}[x, y]/I_S$ is an artinian ring (see Theorem 2.2), the minimal system of generators of $I_S$ contains monomials of the form $x^\alpha,\ y^\beta$. We claim that $\beta = k$. In order to prove it, we note that $D(si) = (0, i)\ \forall i = 0, \ldots, k-1$. In fact, let $i \in \{0, \ldots, k-1\}$ and suppose that $\exists (u, v) \in \mathbb{N}^2,\ \mid u + v \leq i$ with $R(u, v) = si$. Then

$$si \equiv_{sk} au + sv \Rightarrow \exists h \in \mathbb{N}\ /\ si = au + sv + hsk \Rightarrow s|au \Rightarrow s|u$$

$$\Rightarrow \begin{cases} u = 0 \\ \vee \\ \exists t \in \mathbb{N}^*\ /\ u = st. \end{cases}$$

In the first case, we have

$$i = v + kh \leq k - 1 \Rightarrow h = 0 \Rightarrow v = i.$$

In the second,

$$i = at + v + kh \leq k - 1 \Rightarrow h = 0, \qquad i = at + v \geq u + v \Rightarrow at \geq u,$$

but this a contradiction because $a < s$. So, $\beta \geq k$. On the other hand, $D(0, k) = 0 = D(0, 0)$ implies $\beta = k$. Finally, suppose that (see Figure 8.1)

$$I_S = (x^\alpha, x^\gamma y^\delta, y^k), \quad \gamma < \alpha,\ \delta < k, \quad R(\gamma, \delta) = R(0, k) = 0.$$

Thus,

$$R(\gamma, k) = R(\gamma, \delta) + R(0, k - \delta) = R(0, k - \delta),$$

$$R(\gamma, k) = R(\gamma, 0) + R(0, k) = R(\gamma, 0).$$

Therefore, one of the two vectors $(0, k - \delta),\ (\gamma, 0)$ should be in $I_S$, but this is false.

Consequently, $I_S$ is degenerated and

$$sk = \dim\left({}^{\mathbb{K}[x,y]}/_{(x^\alpha, y^k)}\right) = \alpha k \Rightarrow s = \alpha. \qquad \square$$

The following example shows that we cannot omit from the above result hypotheses the requirement $a < s$.

*Example* 8.2. The monomial ideal $I_S$ associated with $C_{60}(7, 6)$ and any graded monomial ordering in $\mathbb{K}[x, y]$ is not degenerated: $I_S = (x^{12}, x^6y^3, y^7)$.

Using the Gröbner bases theory and previous results we can generalize Proposition 8.1 from two jumps to an arbitrary number of them.

PROPOSITION 8.3. *Let $\alpha_1, \ldots, \alpha_r$ be positive integers, neither of them equal to one. Setting $N := \alpha_1 \cdots \alpha_r$, the circulant digraph $\mathcal{C}_N(1, \alpha_1, \alpha_1\alpha_2, \ldots, \alpha_1 \cdots \alpha_{r-1})$*

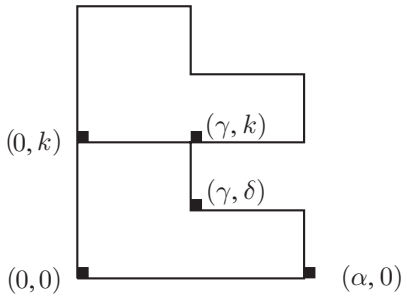


FIG. 8.1.

*is associated to the—incidentally, irreducible—monomial ideal* $(X_1^{\alpha_1},\dots,X_r^{\alpha_r})$*, with any graded monomial ordering. The Gröbner basis of the associated binomial ideal is* $\{X_i^{\alpha_i}-X_{i+1} \mid \ i=1,\dots,r-1\}\cup\{X_r^{\alpha_r}-1\}$.

*Proof.* First of all, every element of the proposed basis lies in the binomial ideal. This is because their associated lattice points,

$$\{(0,\dots,\overset{i}{\overset{\smile}{\alpha_i}},-1,\dots,0) \mid i=1,\dots,r-1\}\cup\{(0,\dots,0,\alpha_r)\},$$

are paths for node 0. Then the initial ideal of this lattice ideal must contain the following one:

$$(X_1^{\alpha_1},\dots,X_r^{\alpha_r})\subseteq I_S.$$

We know that the dimension of the quotient vector space $\mathbb{K}[\mathbf{x}]/I_S$ equals the number of nodes $N=\alpha_1\cdots\alpha_r$. Moreover, the dimension of $\mathbb{K}[\mathbf{x}]/(X_i^{\alpha_i} \mid i=1,\dots,r)$ is $N$, so both ideals must coincide. In order to obtain a reduced Gröbner basis, we must have one binomial for each generator in the initial ideal. That is, the reduced Gröbner basis is

$$\{X_i^{\alpha_i}-m_i(\mathbf{x}) \mid i=1,\dots,r\},$$

where $m_i$ is a monomial satisfying $m_i\notin(X_1^{\alpha_1},\dots,X_r^{\alpha_r})$. Then $m_i=\mathbf{x}^{\mathbf{a}}$, with $a_i<\alpha_i, i=1,\dots,r$. Set $X_{r+1}:=1$. Then $(X_i^{\alpha_i}-X_{i+1})-(X_i^{\alpha_i}-m_i)=m_i-X_{i+1}$ belongs to the ideal. If $m_i\neq X_{i+1}$, we would have $\alpha_{i+1}=1$, which is a contradiction. ∎

The following result is an immediate consequence.

COROLLARY 8.4. *Let* $d,r$ *be two positive integers. Let* $k$ *be the residue class of* $d$ *modulo* $r$*. Then, if we fix*

$$\alpha_1=\cdots=\alpha_k=\frac{d-k}{r}+2,\quad \alpha_{k+1}=\cdots=\alpha_r=\frac{d-k}{r}+1,$$

*the following is a directed circulant graph with* $r$ *jumps,* $N:=\alpha_1\cdots\alpha_r$ *nodes, and diameter* $d$*:*

$$\mathcal{C}_N(1,\alpha_1,\alpha_1\alpha_2,\dots,\alpha_1\cdots\alpha_{r-1}).$$

We note that the number of vertices is

$$N=\left(\frac{d-k}{r}+2\right)^k\left(\frac{d-k}{r}+1\right)^{r-k}.$$

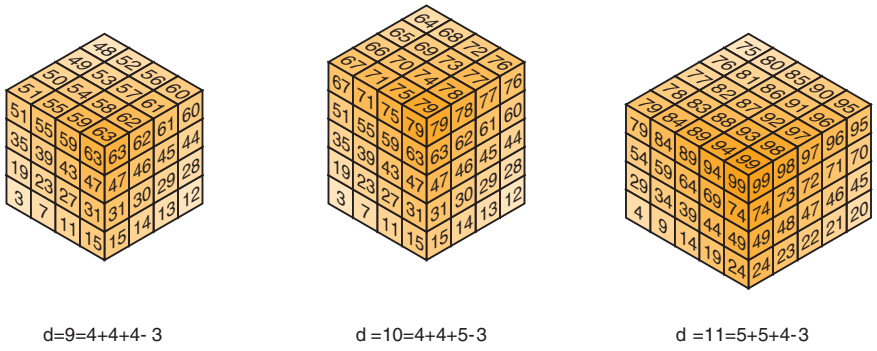


FIG. 8.2. *Family of circulant digraphs.*

Once $r$ is fixed, increasing the diameter $d$ makes the number of nodes in this graph family increase as $O(d^r)$.

Proposition 8.1 provides a family with diameter $2\sqrt{N}-2$ and average minimum distance $\sqrt{N}-1$. Let $d>1$ be a natural number:

$$C_{\left(\frac{d+2}{2}\right)^2}\left(1,\frac{d+2}{2}\right) \text{ if } d\equiv 0 \bmod 2 \quad \text{and} \quad C_{\frac{(d+1)(d+3)}{4}}\left(1,\frac{d+1}{2}\right) \text{ if } d\equiv 1 \bmod 2.$$

Basically, this family was discovered in the paper [32]. However, determining $d_2(N)$ and finding the optimal $C_N(j_1,j_2)$ is an open problem.

In the case of undirected circulant graphs of degree four, i.e., $C_N(j_1,-j_1,j_2,-j_2)$, several papers have shown that the lower bound $\frac{1}{2}\left(\sqrt{2N-1}-1\right)$ can be achieved by taking $j_1=\frac{1}{2}\left(\sqrt{2N-1}-1\right)$ and $j_2=\frac{1}{2}\left(\sqrt{2N-1}-1\right)+1$; see the survey [3]. In the middle, that is, between circulant digraphs of degree two and circulant graphs of degree four, Proposition 8.3 and the above corollary provide a very attractive family of circulant graph of degree three; see Figure 8.2. Let $d>2$ be a natural number:

$$C_{\left(\frac{d+3}{3}\right)^3}\left(1,\frac{d+3}{3},\left(\frac{d+3}{3}\right)^2\right) \text{ if } d\equiv 0 \bmod 3,$$

$$C_{\frac{(d+2)^2(d+5)}{27}}\left(1,\frac{d+2}{3},\left(\frac{d+2}{3}\right)^2\right) \text{ if } d\equiv 1 \bmod 3,$$

$$C_{\frac{(d+4)^2(d+1)}{27}}\left(1,\frac{d+4}{3},\left(\frac{d+4}{3}\right)^2\right) \text{ if } d\equiv 2 \bmod 3.$$

Graphs in this family have diameter $d$ and average minimum distance $d/2$.

**9. Conclusions.** In this paper we have proposed monomial ideals as a natural tool for studying Cayley digraphs with a finite abelian group as vertex set. We have generalized the L-shape concept in the plane to L-shape in the $r$-dimensional affine space. We think that this new point of view may shed light on problems in multiloop computer networks. We also have introduced the Gröbner bases theory in this context, which seems very useful. Many interesting questions remain unsolved. We would like to provide fault tolerance routing algorithms. From a more practical point of view, it would be interesting to investigate the implementation in computer networks of the family of circulant graphs of degree three under parameters such as routing, fault tolerance, etc.

**Acknowledgment.** We would like to thank Prof. B. Sturmfels, who gave us the ideal of a lattice point of view.



REFERENCES

[1] F. Aguiló and M. A. Fiol, *An efficient algorithm to find optimal double loop networks*, Discrete Math., 138 (1995), pp. 15–29.
[2] T. Beker and V. Weispfenning, *Gröbner Bases. A Computational Approach to Commutative Algebra*, Grad. Texts in Math. 141, Springer-Verlag, New York, 1993.
[3] J.-C. Bermond, F. Comellas, and D. F. Hsu, *Distributed loop computer networks: A survey*, J. Parallel Distrib. Comput., 24 (1995), pp. 2–10.
[4] S. R. Blackburn, D. Gomez-Perez, J. Gutierrez, and I. E. Shparlinski, *Predicting nonlinear pseudorandom number generators*, Math. Comp., 74 (2005), pp. 1471–1494.
[5] F. T. Boesch and R. Tindell, *Circulants and their connectivity*, J. Graph Theory, 8 (1984), pp. 487–499.
[6] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, University of Innsbruck, Austria, 1965.
[7] J.-Y. Cai, G. Havas, B. Mans, A. Nerurkar, J.-P. Seifert, and I. Shparlinski, *On routing in circulant graphs*, in Computing and Combinatorics (Tokyo, 1999), Lecture Notes in Comput. Sci. 1627, Springer-Verlag, Berlin, 1999, pp. 360–369.
[8] Y. Chen and F. K. Hwang, *Diameters of weighted double-loop networks*, J. Algorithms, 9 (1988), pp. 401–410.
[9] D. Z. Du, D. F. Hsu, and F. K. Hwang, *Double-linked ring networks*, IEEE Trans. Comput., 34 (1985), pp. 853–877.
[10] D. Eisenbud and B. Sturmfels, *Binomial ideals*, Duke Math. J., 84 (1996), pp. 1–45.
[11] F. Eisenbrand, *Fast integer programming in fixed dimension*, in Algorithms—ESA 2003, Lecture Notes in Comput. Sci. 2832, Springer-Verlag, Berlin, 2003, pp. 196–207.
[12] P. Erdös and D. F. Hsu, *Distributed loop networks with minimum transmission delay*, Theoret. Comput. Sci., 100 (1992), pp. 223–241.
[13] M. Fiol, J. L. Yebra, I. Alegre, and M. Valero, *A discrete optimization problem in local networks and data alignment*, IEEE Trans. Comput., C-36 (1987), pp. 702–713.
[14] D. Gomez, J. Gutierrez, and A. Ibeas, *Circulant digraphs and monomial ideals*, in Computer Algebra in Scientific Computing, Lecture Notes in Comput. Sci. 3718, Springer-Verlag, Berlin, 2005, pp. 196–207.
[15] D. Gomez, J. Gutierrez, and A. Ibeas, *Optimal routing in double loop networks*, Theoret. Comput. Sci., 381 (2007), pp. 68–85.
[16] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Berlin, 1993.
[17] J. Gutierrez and R. Rubio, *Reduced Groebner bases under composition*, J. Symbolic Comput., 26 (1999), pp. 433–444.
[18] R. Hemmecke, R. Hemmecke, and P. Malkin, *4ti2 Version* 1.2*—Computation of Hilbert Bases, Graver Bases, Toric Gröbner Bases, and More*, 2005; available online from www.4ti2.de.
[19] D. F. Hsu and X.-D. Jia, *Extremal problems in the construction of distributed loop networks*, SIAM J. Discrete Math, 7 (1994), pp. 57–71.
[20] F. K. Hwang, *A complementary survey on double-loop networks*, Theoret. Comput. Sci., 263 (2001), pp. 211–229.
[21] F. K. Hwang, *A survey on multi-loop networks*, Theoret. Comput. Sci., 299 (2003), pp. 107–121.
[22] R. Kannan, *Minkoswski's convex body theorem and integer programing*, Math. Oper. Res., 12 (1987), pp. 415–440.
[23] H. W. Lenstra, *Integer programming with a fixed number of variables*, Math. Oper. Res., 8 (1983), pp. 538–548.
[24] A. K. Lenstra, H. W. Lenstra, and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann., 261 (1982), pp. 515–534.
[25] B. Mans, *Optimal distributed algorithms in unlabeled tori and chordal rings*, J. Parallel Distrib. Comput., 46 (1997), pp. 80–90.
[26] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems*, Kluwer Internat. Ser. Engrg. Comput. Sci. 671, Kluwer Academic, Boston, MA, 2002.
[27] E. Miller, *Resolutions and Duality for Monomial Ideals*, Ph.D. Thesis, University of California, Berkeley, 2000.

[28] E. Miller and B. Sturmfels, *Monomial ideal and planar graphs*, in Proceedings of AAECC-13, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Honolulu, HI, 1999), Lecture Notes in Comput. Sci. 1719, Springer-Verlag, Berlin, 1999, pp. 19–28.
[29] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Intersci. Ser. Discrete Math, Wiley-Interscience, Chichester, UK, 1986.
[30] B. Sturmfels, *Gröbner Bases and Convex Polytopes*, Univ. Lecture Ser. 8, AMS, Providence, RI, 1996.
[31] B. Sturmfels, R. Weismantel, and G. M. Ziegler, *Gröbner bases of lattices, corner polyhedra, and integer programming*, Beiträge Algebra Geom., 36 (1995), pp. 281–298.
[32] C. K. Wong and D. Coppersmith, *A combinatorial problem related to multimodule memory organizations*, J. ACM, 21 (1974), pp. 392–402.
[33] J. Žerovnik and T. Pisanski, *Computing the diameter in multiple-loop networks*, J. Algorithms, 14 (1993), pp. 226–243.