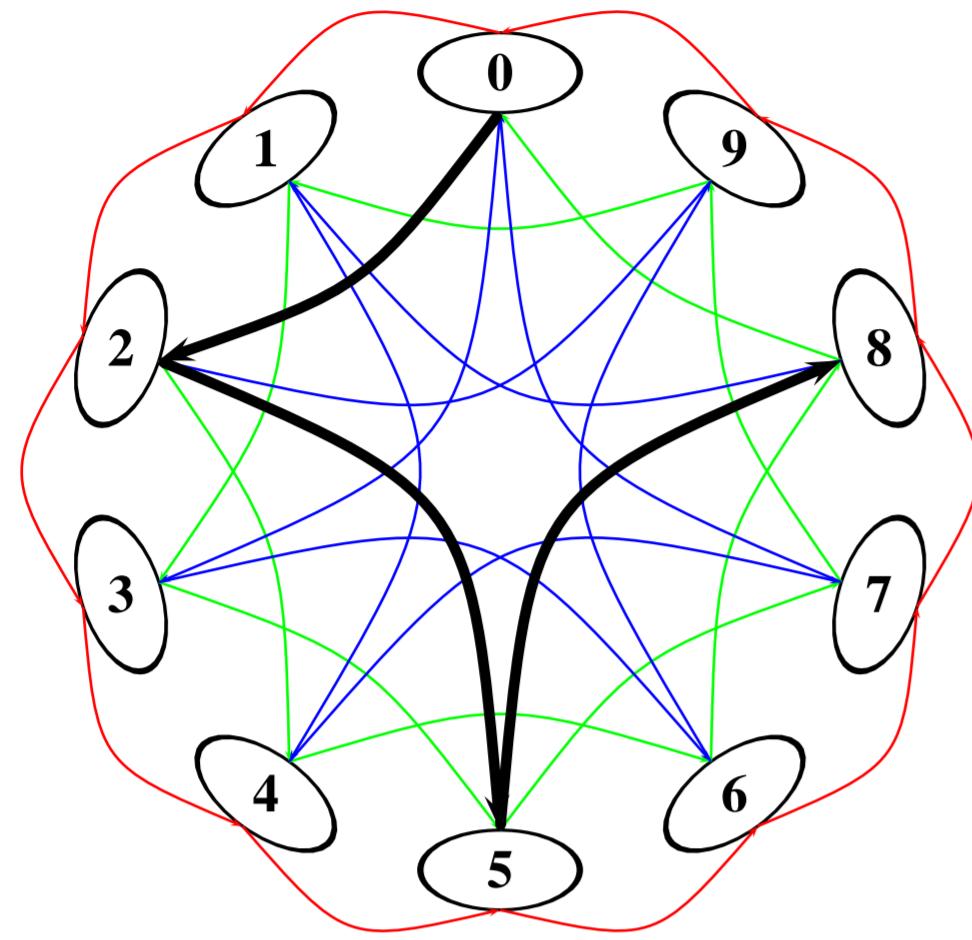


# Gröbner Bases and Cayley Digraphs of Cyclic Groups

Domingo Gómez, Jaime Gutierrez, Álar Ibeas  
University of Cantabria

A (directed) **circulant graph** is a Cayley Digraph with vertices group  $(\mathbb{Z}/N\mathbb{Z}, +)$ .



$\mathcal{C}_{10}(\mathbf{1}, \mathbf{2}, \mathbf{3})$

$R(0, \mathbf{1}, \mathbf{2}) = 8$

- Each graph is defined by its number of vertices  $N$  and a set of integers called **jumps**  $(j_1, \dots, j_r)$ .
- There are  $r$  edges leaving each node:  $c \rightsquigarrow c + j_i$ .

**Paths** in a circulant are described by monomials (elements in  $\mathbb{N}^r$ ), following the identification:

$$\mathbf{x}^{\mathbf{a}} \longleftrightarrow (a_1, \dots, a_r) \longleftrightarrow [c \rightsquigarrow c + j_1 a_1 + \dots + j_r a_r].$$

The **length** of a path (the number of edges it consists of) is:

$$\text{deg}(\mathbf{x}^{\mathbf{a}}) = \|\mathbf{a}\|_1.$$

The **routing** mapping relates each path with the vertex it reaches when applied to the origin:

$$R : \begin{array}{ccc} \mathbb{N}^r & \longrightarrow & \mathbb{Z}/N\mathbb{Z} \\ \mathbf{a} = (a_1, \dots, a_r) & \rightsquigarrow & a_1 j_1 + \dots + a_r j_r. \end{array}$$

Its extension  $\tilde{R} : \mathbb{Z}^r \rightarrow \mathbb{Z}/N\mathbb{Z}$ , (paths with negative components make sense in undirected graphs). Setting  $\mathcal{L} = \ker(\tilde{R})$  (an integer lattice), the set of paths joining two vertices is:

$$\text{Paths}(c \rightsquigarrow d) = (\mathbf{a} + \mathcal{L}) \cap \mathbb{N}^r,$$

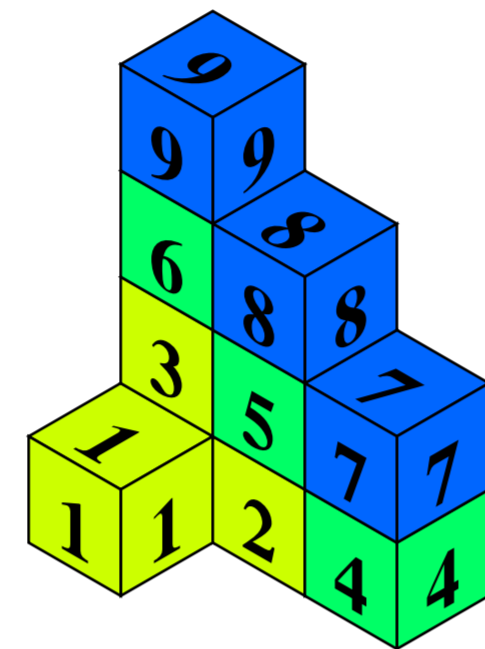
being  $\mathbf{a}$  a particular path with  $R(\mathbf{a}) = d - c$ .

So, the **Routing Problem** in circulants (finding a shortest path) can be solved as an Integer Programming problem.

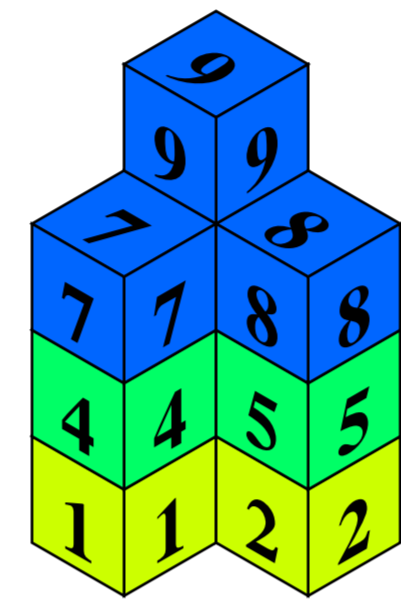
A **Minimum Distance Diagram** can be associated to a circulant,

$$D : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{N}^r, \quad R \circ D = id$$

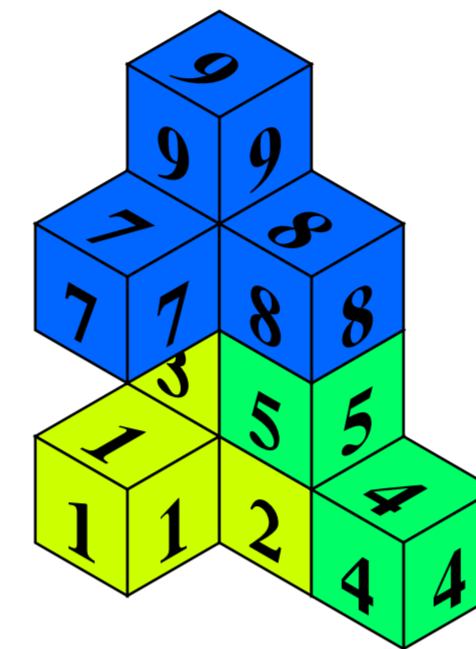
such that  $D(c)$  is minimum in  $R^{-1}(c)$ , with  $\ell_1$  norm.



grad.lex.  $X \succ Y \succ Z$



grad.rev.lex.  $X \succ Y \succ Z$



A graded monomial ordering  $\preceq$  in  $\mathbb{N}^r$  provides a MDD:

$$D(c) = \min (R^{-1}(c)).$$

This way, the diagram is the complement of a monomial ideal.

The third diagram also verifies the minimum distance condition, but it doesn't follow a monomial ordering.

If the diagram is constructed following a monomial ordering, its complement as the initial ideal of the binomial ideal associated to  $\mathcal{L}$  and  $\preceq$ :

$$J := (\mathbf{x}^{\mathbf{a}^+} - \mathbf{x}^{\mathbf{a}^-} / \mathbf{a} \in \mathcal{L}),$$

$$\mathbb{N}^r \setminus D(\mathbb{Z}_N) = \text{init}_{\preceq}(J)$$

A Gröbner basis of  $J$  is useful to compute optimal routings.

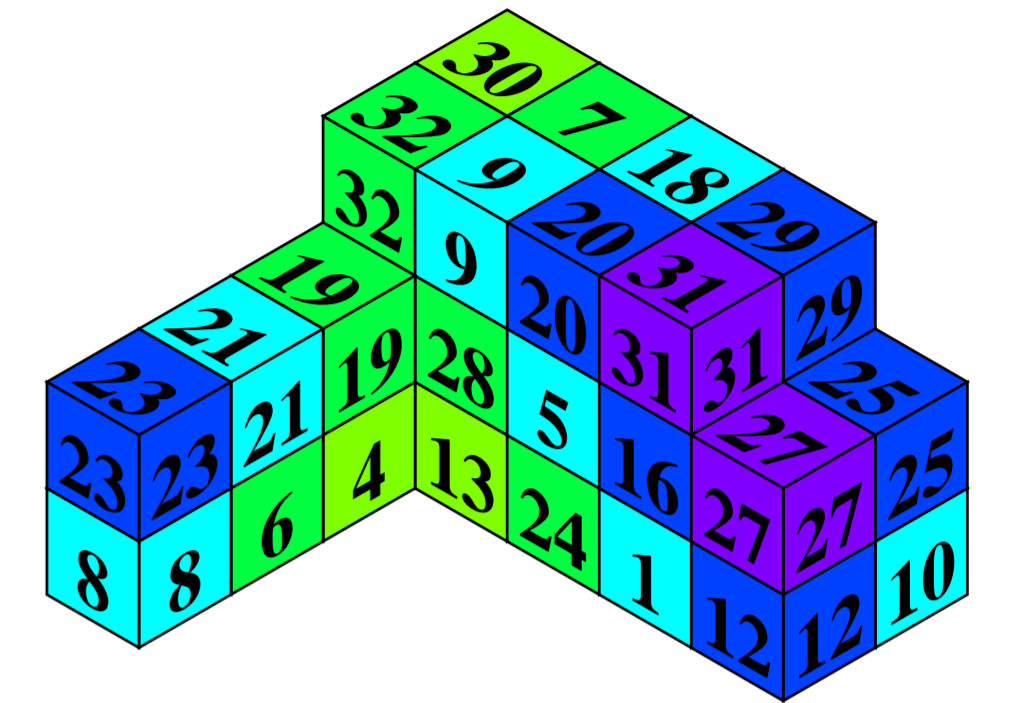
- Select any path  $\mathbf{a} \in R^{-1}(c)$ . (in  $\mathbb{N}^r$ )
- Reduce  $\mathbf{x}^{\mathbf{a}} - 1$  by the GB, obtaining  $\mathbf{x}^{\mathbf{b}} - 1$ .
- $\mathbf{b}$  is a shortest path (by the way, it is  $D(c)$ ).

Moreover, from a GB of  $J$  we obtain the minimal system of generators of  $\mathbb{N}^r \setminus D$ . The leading monomial of each basis element is a generator.

The irredundant decomposition by irreducible ideals is useful to compute the graph's **diameter** and **average minimum distance**.

As an example:

$\mathcal{C}_{34}(2, 11, 15)$



The binomial ideal associated to the lattice  $\ker(\tilde{R})$  is:

$$(X^2 Y - Z, X^2 Z^2 - 1, Y^5 Z - X, X^{34} Y^{34} Z^{34} - 1)$$

Using the graded monomial ordering  $X \succ Y \succ Z$ , we obtain the reduced Gröbner basis:

$$\{Z^3 - Y, X^2 Y - Z, X^2 Z^2 - 1, Y^5 - Z X^3, X^5 - Y^4, Y^4 Z^2 - X^3\}$$

We obtain the description of the diagram's complement:

$$\begin{aligned} I &= (Z^3, X^2 Y, X^2 Z^2, Y^5, X^5, Y^4 Z^2) = \\ &= (X^2, Y^4, Z^3) \cap (X^2, Y^5, Z^2) \cap (X^5, Y, Z^2). \end{aligned}$$

Writting  $\mathfrak{m}^{\mathbf{a}} := (X_i^{a_i} / a_i > 0)$ ,  $I = \mathfrak{m}^{\mathbf{a}_1} \cap \dots \cap \mathfrak{m}^{\mathbf{a}_n}$  the diameter  $d$  and average distance  $\bar{d}$  satisfy:

$$d = \max \|\mathbf{a}_i\|_1 - r,$$

$$\bar{d} = \frac{1}{N} \sum_{\emptyset \subsetneq \Delta \subseteq \{1, \dots, n\}} (-1)^{\#\Delta+1} \sigma(\text{gcd}(\mathbf{x}^{\mathbf{a}_i}, i \in \Delta)),$$

$$\sigma(\mathbf{x}^{\mathbf{a}}) := \frac{a_1 \cdots a_r}{2} (a_1 + \dots + a_r - r).$$

[1] J.C. Bermond, F. Comellas, D.F. Hsu: "Distributed loop computer networks: a survey". J. Parallel and Distributed Computing, **24**, 2-10, 1995.

[2] D. Gómez, J. Gutiérrez, A. Ibeas: "Cayley digraphs of finite cyclic groups and monomial ideals". Preprint, 2005.

[3] E. Miller, B. Sturmfels: "Monomial Ideal and Planar Graphs". Proc. AAECC-13, LNCS **1719**, 19-28, 1999.