

On Routing in Circulant Graphs of Degree Four

Domingo Gómez, Jaime Gutierrez,
Alvar Ibeas, Carmen Martínez and Ramón Beivide
Universidad de Cantabria
E-39071 Santander, Spain
jaime.gutierrez@unican.es

Abstract

In this paper we present the first polynomial time deterministic algorithm to compute the shortest path between two vertices of a circulant graph of degree four. Our spectacular algorithm only requires $O(\log^3 N)$ bit operations, where N is the number of the vertices and it is based on shortest vector problems in a special class of lattices for L_1 -norm. Moreover, the technique can be extended to weighted and directed circulant graphs, the so called double-loop networks. Our main tools are results and methods from the geometry of numbers and computer algebra.

1 Introduction

Two important tools in computer algebra are: Gröbner basis theory and the shortest vector problem. The first one was introduced by Buchberger [5] and it is very useful for manipulating multivariate polynomial ideals. The second one was used in the celebrated *LLL algorithm* of Lenstra, Lenstra and Lovász [12] for factoring polynomials. Both of them are related to an appropriate finite generator system: *reduced basis*. In this paper, we compute a certain reduced basis and applying the *basis reduction technique* we provide an algorithm to find the shortest path between two vertices in circulant graphs of degree four.

We recall that a *circulant (undirected) graph* with N vertices and jumps j_1, j_2, \dots, j_m is a graph in which each vertex n , $0 \leq n \leq N - 1$, is adjacent to all the vertices $n \pm j_i \text{ mod } N$, with $1 \leq i \leq m$. The family of circulant graphs includes the complete graph and the cyclic graph or ring among its members.

Circulant graphs have a vast number of applications in telecommunication networking, VLSI design and distributed computation [2, 3, 4, 14].

With every circulant graph $C_N(j_1, j_2, \dots, j_m)$ one can associate the lattice, which consist of integer solutions $(x_1, \dots, x_m) \in \mathbf{Z}^m$ to the system of congruences

$$j_1x_1 + \dots + j_mx_m \equiv 0 \pmod{N}.$$

Starting from any node or vertex r we arrive s if and only if

$$\sum_{i=1}^m x_i j_i \equiv r - s \pmod{N}.$$

It is natural to aim to minimize the L_1 -norm which is the length of the shortest path between r and s , that is, the routing from node r to s .

For general graphs finding the shortest path between two vertices is a well known problem. Efficient polynomial time algorithms have been developed for various shortest path problems. However, for the class of circulant graphs, there is an important distinction to be made, and that concerns the natural input size to a problem. For a general graph it is common to consider the input size to be $O(N^2)$, which is the number of elements in the adjacency matrix. However, any circulant graph can be described by only m integers. In this representation the input size is $O(m \log N)$. Thus polynomial time algorithms for general graphs may exhibit exponential complexity in the special case of circulant graphs.

In [6] the authors establish relations between several routing problems and the problem of finding the shortest vector in the L_1 - norm in a lattice. They show that the shortest-Path problem is NP-hard for circulant graphs of arbitrary degree.

In this paper we consider only the special case $m = 2$, that is, circulant graphs of degree four. There are several algorithmic results for circulant graphs of degree four, see [7, 8, 9, 15, 16]. The best known algorithm for the routing problem is exponential in the input size $\log N$. Typically, they require $O(\log N)$ time for preprocessing and constant processing time at each node on the route. But the lower bounds of the diameter is $\sqrt{N/2}$ for undirected circulant graph of degree four and $\sqrt{3N}$ for directed ones (see [3]), so in both cases are exponential in the input size $\log N$. On the other hand, these papers use quite elementary number theoretic considerations.

2 The algorithm

The main question of this paper is to compute the shortest path for two vertices of any connected circulant graph of degree four with jumps j_1, j_2 and N nodes. A useful tool is the *Ádam's Conjecture*, see [1], known to be a theorem for circulants of degree four, see [13].

Theorem 2.1. *Let N be a natural number. We have, $C_N(j_1, j_2) \cong C_N(i_1, i_2) \Leftrightarrow \exists u \in \mathbf{Z}, \gcd(u, N) = 1 \mid u\{\pm j_1, \pm j_2\} = \{\pm i_1, \pm i_2\} \pmod N$.*

So we can suppose that $\gcd(j_1, j_2) = 1$ and, instead of study them, we associate the two dimensional lattice \mathcal{L} :

$$j_1x + j_2y \equiv 0 \pmod N.$$

2.1 The reduction of a vector

For the rest of the paper we only consider the L_1 -norm $\|\cdot\|$ in two dimensional lattice of \mathbf{Z}^2 .

Given two vectors \vec{u} and \vec{v} , we can find $\alpha \in \mathbf{Z}$ such that the value $\|\vec{u} - \alpha\vec{v}\|$ is minimal, that is, we want to make \vec{u} as short as possible by subtracting an integer multiple of \vec{v} . The algorithms in [10, 11] require only $O(\log(\max(\|u\|, \|v\|)^2))$ bit operations. The main goal of this subsection is to obtain, on polynomial time, a such smallest vector with extra properties.

Definition 2.2. *Given two vectors $\vec{u} = (u_1, u_2)$ and $\vec{v} = (v_1, v_2)$ in \mathbf{Z}^2 such that $(v_1, v_2) \neq (0, 0)$, the reduction \vec{w} of \vec{u} with respect to \vec{v} is defined as follows:*

- If $|v_1| \geq |v_2|$, let q be the quotient of the division of u_1 into v_1 :
 - If $v_1 > 0$, then \vec{w} is the vector with minimum norm between the norm of the vectors $\vec{u} - q\vec{v}$ and $\vec{u} - (q + 1)\vec{v}$. If they have same norm, then $\vec{w} = \vec{u} - q\vec{v}$.
 - If $v_1 < 0$, then \vec{w} is the vector with minimum norm between the norm of the vectors $\vec{u} - q\vec{v}$ and $\vec{u} - (q - 1)\vec{v}$. If they have same norm, then $\vec{w} = \vec{u} - q\vec{v}$.
- If $|v_2| > |v_1|$, let q be the quotient of the Euclidean division of u_2 into v_2 :
 - If $v_2 > 0$, then \vec{w} is the vector with minimum norm between the norm of the vectors $\vec{u} - q\vec{v}$ and $\vec{u} - (q + 1)\vec{v}$. If they have same norm, then $\vec{w} = \vec{u} - q\vec{v}$.

- If $v_2 < 0$, then \vec{w} is the vector with minimum norm between the norm of the vectors $\vec{u} - q\vec{v}$ and $\vec{u} - (q - 1)\vec{v}$. If they have same norm, then $\vec{w} = \vec{u} - q\vec{v}$.

We denote the reduction of \vec{u} with respect \vec{v} by $\text{Reduce}_{\vec{v}}(\vec{u})$. By definition $\text{Reduce}_{(0,0)}(\vec{u}) = \vec{u}$.

Theorem 2.3. *With the above definition, let $M = \max(\|\vec{u}\|, \|\vec{v}\|)$:*

(i) *The vector $\text{Reduce}_{\vec{v}}(\vec{u})$ can be computed only with $O(\log^2 M)$ bit operations.*

(ii) *$\|\text{Reduce}_{\vec{v}}(\vec{u})\|$ is minimal in the set $\{\|\vec{u} + \alpha\vec{v}\|, \alpha \in \mathbf{Z}\}$.*

(iii) *Let $(w_1, w_2) = \text{Reduce}_{\vec{v}}(\vec{u})$:*

- *If $|v_1| \geq |v_2|$ then $|w_1| < |v_1|$; if $|v_1| > |v_2|$ and $|u_1| \geq |v_1|$ then $\|\text{Reduce}_{\vec{v}}(\vec{u})\| < \|\vec{u}\|$.*
- *If $|v_2| > |v_1|$ then $|w_2| < |v_2|$; and if $|u_2| \geq |v_2|$ then $\|\text{Reduce}_{\vec{v}}(\vec{u})\| < \|\vec{u}\|$.*

2.2 Reduced basis

The following concept is the generalization of reduced lattice basis in the celebrated algorithm [12] for lattices of rank 2 to an arbitrary norm [10].

Definition 2.4. *Given two vectors $\vec{u}, \vec{v} \in \mathbf{Z}^2$ spanning a two-dimensional lattice ($\text{rank}(\vec{u}, \vec{v}) = 2$), we say that $\langle \vec{u}, \vec{v} \rangle$ is a reduced basis if:*

$$\|\vec{u}\|, \|\vec{v}\| \leq \|\vec{u} - \vec{v}\|, \|\vec{u} + \vec{v}\|$$

The algorithm in [10, 11] computes a reduced base from a base $\langle \vec{u}, \vec{v} \rangle$ of the lattice \mathcal{L} in $O(\log M)$ arithmetic steps where $M = \max(\|\vec{u}\|, \|\vec{v}\|)$. The main goal in this subsection is to find a reduced basis of the lattice \mathcal{L} with extra properties.

Definition 2.5. *We say that a basis $\langle \vec{u}, \vec{v} \rangle$ of the lattice \mathcal{L} is an extra-reduced basis if*

$$\text{Reduce}_{\vec{v}}(\vec{u}) = \vec{u} \quad \& \quad \text{Reduce}_{\vec{u}}(\vec{v}) = \vec{v}.$$

The following is an important result:

Theorem 2.6. *Any extra-reduced basis is a reduced basis. Moreover, given a reduced basis $\langle \vec{u}, \vec{v} \rangle$ we can compute an extra-reduced basis in $O(\log^2 M)$ bit operations, where $M = \max(\|\vec{u}\|, \|\vec{v}\|)$.*

2.3 The shortest path

We start with an extra-reduced basis $\langle \vec{u}, \vec{v} \rangle$ of the lattice \mathcal{L} and an arbitrary path \vec{w} from the vertex 0 to any vertex $i \in \mathbf{Z}_N$. Using the previous results we can prove the following:

Theorem 2.7. *We can compute a shortest path on cubic polynomial time in the input size $\log N$.*

Sketch of the proof. Consider the following REDUCTION procedure

1. *Reduce* $_{\vec{v}}$ (\vec{w}) = $\vec{w}^{(1)}$.
2. *Reduce* $_{\vec{u}+\vec{v}}$ ($\vec{w}^{(1)}$) = $\vec{w}^{(2)}$.
3. *Reduce* $_{\vec{u}-\vec{v}}$ ($\vec{w}^{(2)}$) = $\vec{w}^{(3)}$.
4. *Reduce* $_{\vec{u}}$ ($\vec{w}^{(3)}$) = $\vec{w}^{(4)}$.
5. Repeat $\vec{w} := \vec{w}^{(4)}$.

3 Conclusions

In this extended abstract we have presented the first polynomial time algorithm to compute the shortest path for a circulant (undirected) graph of degree four. The method can be easily extended to directed circulant graph, the fundamental idea of the extension is find a path very close to a shortest one, then we have bounds for his components.

Acknowledgments.– The second author is partially supported by the Spanish project BFM2001-1294.

References

- [1] A. Adam. *Research problem 2-10*. J. Combinatorial Theory, 393, 1109-1124, 1991.
- [2] R. Beivide, E. Herrada, J.L. Balcázar and A. Arruabarrena. *Optimal Distance Networks of Low Degree for Parallel Computers*. IEEE Transactions on Computers, Vol. C-40, No. 10, pp. 1109-1124, 1991.
- [3] J.-C. Bermond, F. Comellas and D.F. Hsu. *Distributed Loop Computer Networks: A Survey*. Journal of Parallel and Distributed Computing, Vol. 24, pp. 2-10, 1995.

- [4] W.J. Bouknight, S.A. Denenberg, D.E. McIntyre, J.M. Randall, A.H. Sameh and D.L. Slotnick. *The Illiac IV System*. Proc. IEEE, Vol. 60, No. 4, pp. 369-388, 1972.
- [5] B. Buchberger. *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*. Aequationes Math. 4, 374–383, 1970.
- [6] J.-Y. Cai, G. Havas, B. Mans, A. Nerurkar, J.-P. Seifert and I. Shparlinski. *On Routing in Circulant Graphs*. Proc. Fifth Annual International Computing and Combinatorics Conference, Tokyo, Japan, July 26-28, 1999, LNCS vol. 1627, Springer-Verlag, T. Asano, H. Imai, D.T. Lee, S. Nakano, and T. Tokuyama (Eds.), pp. 360-369.
- [7] Y. Cheng and F. K. Hwang, *Diameters of Weighted Double Loop Networks*, Journal of Algorithms 9, 401-410, 1988.
- [8] D. J. Guan: *An Optimal Message Routing Algorithm for Double-Loop Networks*. Information Processing Letters 65(5): 255-260, 1998.
- [9] F. K. Hwang, *A complementary survey on double-loop networks*, Theoretical Computer Science 263, 2001. 211-229.
- [10] M. Kaib and C.P. Schnorr. *The generalized Gauss reduction algorithm*. J. Algorithms 21(3): 565-578, 1996.
- [11] R. Kannan, ‘Algorithmic geometry of numbers’, *Annual Review of Comp. Sci.*, **2**, 231–267, 1987.
- [12] A. K. Lenstra, H. W. Lenstra and L. Lovász, ‘Factoring polynomials with rational coefficients’, *Mathematische Annalen*, **261**, 515–534, 1982.
- [13] B. Mans, F. Pappalardi and I. Shparlinski. *On the Ádám Conjecture on Circulant Graphs*. Discrete Math., v.254, 309-329, 2002.
- [14] R. S. Wilkov. *Analysis and Design of Reliable Computer Networks*. IEEE Trans. Communications, Vol. 20, 660-678, 1972.
- [15] Yu-Liang Liu, Yue-Li Wang, D. J. Guan: *An Optimal Fault-Tolerant Routing Algorithm for Double-Loop Networks*. IEEE Transactions on Computers 50(5): 500-505, 2001.
- [16] Janez Zerovnik, Tomaz Pisanski. *Computing the Diameter in Multiple-Loop Networks*. J. Algorithms 14(2): 226-243, 1993.