Restricted shortest paths in 2-circulant graphs
T. Dobravec and B. Robič
Faculty of Computer and Information Science
University of Ljubljana, Slovenia
\{tomaz.dobravec, borut.robic\}@fri.uni-lj.si

Keywords: circulant graphs, routing, $\ell_1$-lattice, Diophantine equation, closest vector problem

Corresponding author:
Tomaž Dobravec
University of Ljubljana, Slovenia
Faculty of Computer and Information Science
e-mail: tomaz.dobravec@fri.uni-lj.si
Version: draft (Januar 2010)
Restricted shortest paths in 2-circulant graphs

Abstract

Semi-directed 2-circulant graph is a subgraph of an (undirected) 2-circulant graph in which the links of one type (i.e., short or long) are directed while the other links are undirected. The shortest paths in semi-directed circulant graphs are called the restricted shortest paths in 2-circulant graphs. In this paper we show that the problem of finding the restricted shortest paths is equivalent (1) to solving an optimization problem which involves Diophantine equations and (2) to the closest vector problem in a subset of a point lattice of all cyclic paths of the graph. We also present our new, efficient algorithm for constructing the restricted shortest paths which requires $O(\log n)$ arithmetic operations.

1 Introduction

Circulant graphs are well-known and frequently studied mathematical structures. Due to their powerful and useful properties (such as vertex symmetry, small diameter, scalability and efficient routing capabilities), they have been used in the development of VLSI technology as well as for connection schemes in computer networks [1, 4, 12, 16]. With a view to taking full advantage of the routing capabilities of the underlying topology in the famous computer ILLIAC IV, in FDDI-token, SILK and SONT rings [2, 15] as well as in some other parallel processing systems and projects (Intel Paragon, Cray T3D, MPP, MICROS), many theoretical studies concerning the routing problems in circulant graphs have been discussed [3, 5–8, 11, 13, 14].

A subgraph of a 2-circulant graph in which the links of one type (i.e., short or long) are changed from undirected to directed is called a semi-directed 2-circulant graph (see Fig. 1). In this way the node degrees are reduced from 4 to 3, thus making such graphs asymmetric (in terms of path reversibility) and hence diameter-related problems generally harder than for undirected graphs. The shortest paths (i.e., paths with the minimum number of links) in semi-directed 2-circulant graphs will be called restricted shortest paths of 2-circulant graphs, or simply RSPs.

The efficiency of constructing the RSPs is crucial to the time complexity of several optimal dynamic routing algorithms for circulant graphs [9]. Using RSPs these algorithms can dynamically decide where to send a given package in order to stay on one of the shortest paths to the destination node. The main advantage of RSP-based routing over static routing (where the routing path is constructed during the preprocessing phase) or over dynamic routing with the shortest paths (where the routing path is augmented on-the-fly at each routing step) is that RSP-based routing algorithms can often choose from a larger set of candidates for the next node to be visited. Specifically, while in static routing or dynamic routing with the shortest paths this set has at most two elements, in RSP-based routing it may contain 3 or even 4 elements. Using an RSP-based routing algorithm the systematic construction of the routing paths in all the circulant graphs consisting of up to
Figure 1: 2-circulants with 8 nodes and with hops of length 2 and 3. In the undirected case each node has in-degree 4 and every path can be simply reversed while in the semi-directed graph, in which nodes have in-degrees 3, this is not always possible.

50 nodes (i.e., 4165 graphs and 154687 routing paths) has revealed that in 8.3% of cases this set consists of 3 elements and in 2.9% of even 4 elements. Hence, in at least 11.2% of the cases the RSP-based routing algorithm can choose from more candidates for the next node to be visited than other algorithms [10]. This property is especially important in heavy-traffic networks where flexible routing algorithms are needed in order to avoid potential routing problems that arise from congestion or node/link faults.

In this paper we show that the problem of finding RSPs can be defined in at least three equivalent ways: (1) as a graph-theoretical problem, (2) as an optimization problem (involving a linear Diophantine equation with two restriction criteria), and (3) as a closest vector problem (in a point lattice of all cyclic paths of the corresponding graph). As the first definition offers no useful hints for solving the problem, we have focused on the third one, and in this way designed an efficient algorithm for constructing the RSPs. Consequently, this algorithm contributes not only to graph theory but also to number theory as well as to the theory and application of point lattices.

The paper is organized as follows. In the next Section we define new terms and state three equivalent definitions of the RSP problem. In Section 3 we introduce the integer lattice environment with its properties and tools. In Section 4 we present our new, efficient algorithm for constructing RSPs and prove its correctness as well as its $O(\log n)$ time complexity.
2 Problem definition

Let \( \mathbb{N} \) be the set of positive integers, \( \mathbb{Z}_n = \{0, 1, \ldots, n-1\} \), and \( I = \{-2, -1, 1, 2\} \).

**Definition 1** Let \( n, h_1, h_2 \in \mathbb{N} \) be such that \( 0 < h_1 < h_2 < \lfloor n/2 \rfloor \) and \( \text{gcd}(n, h_1, h_2) = 1 \). A double-loop graph \( G(n; h_1, h_2) \) is a directed graph \( G(V, E) \), where the node set \( V = \mathbb{Z}_n \) and the arc set \( E \) is the union of sets \( E_1 = \{(u, u + h_1 \pmod{n}) \mid u \in \mathbb{Z}_n\} \) and \( E_2 = \{(u, u + h_2 \pmod{n}) \mid u \in \mathbb{Z}_n\} \). In the undirected case, which is known as a 2-circulant graph and is denoted by \( G(n; \pm h_1, \pm h_2) \), arcs are changed into (undirected) edges.

Note that a circulant graph is connected if and only if \( \text{gcd}(n, h_1, h_2) = 1 \). In 2-circulant graphs, besides \( E_1 \) and \( E_2 \), the set of edges also consists of the sets \( E_{-1} = \{(u, u - h_1 \pmod{n}) \mid u \in \mathbb{Z}_n\} \) and \( E_{-2} = \{(u, u - h_2 \pmod{n}) \mid u \in \mathbb{Z}_n\} \), i.e.,

\[
E = \bigcup_{j \in I} E_j.
\]

Let, for each \( i \in I \), \( \epsilon_i \) denote a hop of type \( i \) (i.e., a hop from set \( E_i \)). Each path in a 2-circulant graph of length \( l \) corresponds to a sequence \( \epsilon_{i_1}, \epsilon_{i_2}, \ldots, \epsilon_{i_l} \), where \( i_1, i_2, \ldots, i_l \in I \). For example, a path \( 1 \to 3 \to 6 \to 4 \to 7 \) in \( G(8; \pm 2, \pm 3) \) corresponds to a sequence \( \epsilon_1, \epsilon_2, \epsilon_{-1}, \epsilon_2 \). A path that does not contain hops of opposite types (i.e., \( \epsilon_i \) and \( \epsilon_{-i} \) for some \( i \in I \)) is called a simple path. Clearly, when considering shortest paths, only simple paths need to be taken into account.

If \( p = \epsilon_{i_1}, \epsilon_{i_2}, \ldots, \epsilon_{i_l} \) is a path from \( u \) to \( v \), then any permutation of hops \( \epsilon_{i_j} \) is also a path from \( u \) and \( v \). Furthermore, any such permutation is also a path from the node \( 0 \) to the node \( w = v - u \pmod{n} \). This is because the path \( p = \epsilon_{i_1}, \epsilon_{i_2}, \ldots, \epsilon_{i_l} \) is closely related to the linear Diophantine equation

\[
u + t_{i_1} + t_{i_2} + \cdots + t_{i_l} \equiv v \pmod{n},
\]

where \( t_i = \text{sign}(i) \cdot h_{|i|} \). Thus, when only the number of links of a particular type on a path is important (not their ordering), the path can be represented by a quadruplet of integers, one for each hop type. In particular, when considering simple paths, which is the case in this paper, a path can be represented by a pair \((x_1, x_2)\), where \( |x_i| \) is the number of hops of type \( \epsilon_j \) and \( j = \text{sign}(x_i) \cdot i \).

The following definition introduces semi-directed circulant graphs, which are circulant graphs having no links of a particular type.

**Definition 2** Let \( n, h_1, h_2 \) be as in Definition 1. For a given \( i \in I \), the semi-directed 2-circulant graph \( G'(n; \pm h_1, \pm h_2) \) is a graph with the node set \( V = \mathbb{Z}_n \) and the arc set

\[
E = \bigcup_{j \in I \setminus \{i\}} E_j.
\]
Definition 3  The shortest path from \( u \) to \( v \) in semi-directed 2-circulant graph \( G^i(n; \pm h_1, \pm h_2) \) is said to be a restricted shortest path of type \( i \) in \( G(n; \pm h_1, \pm h_2) \) and is denoted by \( p_i(u, v) \). The length of \( p_i(u, v) \) is denoted by \( d_i(u, v) \).

The main goal of this paper is to show how to solve the following problem.

**Problem 1** Given \( n, h_1, h_2, u, v \) and \( i \), find the restricted shortest path \( p_i(u, v) \).

As the definition of Problem 1 offers no hints about solving it, we will reformulate the problem in an algebraic and therefore more descriptive form. To do this we will use the following lemma.

**Lemma 1** Let \( n, h_1, h_2 \) be as in Definition 1, let \( i \in I \) and \( u, v \in \mathbb{Z}_n \). If \( p_i(u, v) \) is a simple path from \( u \) to \( v \) represented by \((x_1, x_2)\), then

\[ a. \quad u + x_1h_1 + x_2h_2 \equiv v \pmod{n}, \]
\[ b. \quad \text{the length of } p_i(u, v) \text{ is } d_i(u, v) = |x_1| + |x_2|, \]
\[ c. \quad \text{if } p_i(u, v) \text{ does not contain hops of type } i \in I, \text{ then } \text{sign}(i) \cdot x_{|i|} \leq 0. \]

Using Lemma 1, whose proof will be omitted due to its simplicity, Problem 1 can be reformulated in the following algebraic form.

**Problem 2** Let \( n, h_1, h_2 \) be as in Definition 1 and let \( i \in I, u, v \in \mathbb{Z}_n \) and \( w = v - u \pmod{n} \). Find a solution \((x_1, x_2)\) of the equation

\[ x_1h_1 + x_2h_2 \equiv w \pmod{n}, \tag{1} \]

which minimizes the sum

\[ |x_1| + |x_2| \tag{2} \]

subject to the restriction that

\[ \text{sign}(i) \cdot x_{|i|} \leq 0. \tag{3} \]

Instead of solving the problem analytically, which turned out to be difficult, we will show how to solve Problem 2 by transforming it into an equivalent geometric problem in the 2-dimensional integer lattice \( \mathbb{Z} \times \mathbb{Z} \), where each point \( x = (x_1, x_2) \) is labelled with the labeling function

\[ l(x) = x_1h_1 + x_2h_2 \pmod{n}. \]

It is obvious that (a) the solutions of equation (1) are points in \( \mathbb{Z} \times \mathbb{Z} \) with the label \( w \) (and vice versa), (b) the solutions of the inequality (3) are in the half-plane \( \mathbb{Z}^2_{-1} \) (see Fig. 2) and (c) the sum (2) is the Manhattan norm \( \ell_1 \) of element \( x = (x_1, x_2) \in \mathbb{Z} \times \mathbb{Z} \). Hence, we can reformulate Problem 2 as follows.
Problem 3 Let $n, h_1, h_2 \in \mathbb{N}$ such that $0 < h_1 < h_2 < [n/2]$ and $\gcd(n, h_1, h_2) = 1$. Let $i \in I$, $u, v \in \mathbb{Z}_n$ and $w = v - u \pmod{n}$. Among all points of the half-plane $\mathbb{Z}^2_{-i}$ that are labelled $w$ find the one with minimal $\ell_1$-norm.

In the following we will show how to solve Problem 3 and thus, since the three formulations of the problem are equivalent, how to find RSPs in 2-circulant graphs and also how to find a solution of the Diophantine equation (1) satisfying the restrictions (2) and (3).

Problem 3 can be solved by a brute-force algorithm that systematically searches the half-plane, i.e., it searches $\ell_1$-spheres by incrementing their radius until the first element with the label $w$ is found. However, this algorithm has a time complexity polynomial in $n$ and is therefore prohibitively slow. This is because a 2-circulant graph $G(n; h_1, h_2)$ can be described only by the numbers $n, h_1$ and $h_2$. Since the input takes only $O(\log n)$ space, the polynomial in $n$ is in fact exponential in terms of the size of the input. In Section 4 we will present an algorithm for solving Problem 3 which requires only $O(\log n)$ arithmetic operations. However, before that we must introduce some additional technical notions and tools.

3 The integer lattice environment

The integer lattice $\mathbb{Z} \times \mathbb{Z} = \{(x_1, x_2); x_1, x_2 \in \mathbb{Z}\}$ with its modular properties has turned out to be an environment in which Problem 1 can be clearly presented and solved with a reasonable amount of effort.

The labeling function

Integer lattices and circulant graphs are connected in a natural way: each point in the lattice represents a simple path in a graph and vice versa. If the lattice is equipped with a labeling function $l(x) = x_1 h_1 + x_2 h_2 \pmod{n}$ for each $x = (x_1, x_2) \in \mathbb{Z} \times \mathbb{Z}$, then this connection is even stronger since each lattice point with label $w$ represents a path from node 0 to $w$ in the corresponding graph $G(n; \pm h_1, \pm h_2)$.

Example: Fig. 3 depicts a labeled integer lattice that represents the graph $G(8; \pm 2, \pm 3)$. The lattice point $z=(5,4)$, for example, corresponds to a path with 5 short and 4 long hops. The label of point $z$ (i.e. 6) corresponds to the node that is reached from the node 0: $0 + 5 \times 2 + 4 \times 3 = 6$.
The set \( X \)

We will denote with \( X \) the set of elements of the lattice \( \mathbb{Z} \times \mathbb{Z} \) that are labelled with \( w \),

\[ X := \{ x \in \mathbb{Z} \times \mathbb{Z}; \ l(x) = w \}. \]

For each \( w \in \mathbb{Z}_n \) and \( i \in I \) the intersection of \( X \) and \( \mathbb{Z}_i^2 \) will be denoted by \( X^i \). The set \( X \) of elements with the label 0 (note that this set represents all cyclic paths) is a submodule of \( \mathbb{Z} \times \mathbb{Z} \).

**Example:** Every lattice point with label 5 belongs to the set \( X \); among these elements all that are in the right half-plane belong to \( X^+ \), in the left half-plane to \( X^- \), and so forth. In Fig. 3 the labels of the members of \( X^\pm \) are underlined.

**Basis, parallelograms, and elements**

Let \( \{ a, b \} \) be a basis of the module \( X \) (i.e., a set of linearly independent vectors that spans \( X \)). The set of points

\[ \{ x \in \mathbb{Z} \times \mathbb{Z}; \ x = \alpha a + \beta b; \ 0 \leq \alpha, \beta < 1 \} \]

is denoted by \( [a, b] \) and called the *main base parallelogram*. With base parallelograms we denote the parallelograms \( [a, b], [a, b] - a, [a, b] - b \) and \( [a, b] - (a + b) \). Every other parallelogram, i.e., every parallelogram of the form \( [a, b] + sa + tb (s, t \in \mathbb{Z}) \), is called a *parallelogram of the basis \( \{ a, b \} \).*

**Example:** One of possible bases of module \( X \) for the graph \( G(8; \pm 2, \pm 3) \) is \( \{ a, b \} = \{(4, 0), (1, 2)\} \). This basis and the corresponding base parallelograms are depicted in Fig. 3 in bold; the main base parallelogram is shaded.

We will use the following lemma, which was proved in [17].

**Lemma 2** For each \( w \in \mathbb{Z}_n \) there exists \( x \in [a, b] \) such that \( l(x) = w \).

Since there are \( n \) points in each parallelogram, for each \( w \in \mathbb{Z}_n \) there is exactly one \( x \in [a, b] \) with the label \( w \). This element, called a *main base element*, will be denoted \( x \). The elements in the four base parallelograms with the label \( w \) (i.e., \( x, x - a, x - b, x - (a + b) \)) are called *base elements*.

**Example:** For the basis \( \{ a, b \} = \{(4, 0), (1, 2)\} \) and \( w = 7 \) the main base element is \( x = (2, 1) \); the other three base elements are \( x - a = (-2, 1), x - b = (1, -1), \) and \( x - (a + b) = (-3, -1) \) (in Fig. 3 these elements are circled).

**Packed basis**

A basis \( \{ a, b \} \) of a module \( X \) for which

\[ \max\{||a||, ||b||\} \leq \min\{||a + b||, ||a - b||\} \]

(mod 8).

The set \( X \)

We will denote with \( X \) the set of elements of the lattice \( \mathbb{Z} \times \mathbb{Z} \) that are labelled with \( w \),

\[ X := \{ x \in \mathbb{Z} \times \mathbb{Z}; \ l(x) = w \}. \]
The minimal projection. The set of base stripes is denoted by \( \text{base stripes} \). In Fig. 4 the base stripes for the graph \( G \) are depicted.

For each stripe \( (x, e) \) the half-plane is denoted by \( T \). The direction of the base vectors (i.e., \( \ell \)). The basis \( O \) found in previous examples is packed.

Example: The basis \( \{a, b\} = \{(4, 0), (1, 2)\} \) from previous examples is packed.

Stripes

For each \( x, e \in \mathbb{Z} \times \mathbb{Z} \) a discrete line \( x + ke \); \( k \in \mathbb{Z} \) is called a stripe through \( x \) in direction \( e \) and denoted by \( t(x, e) \). For each \( w \in \mathbb{Z}_0 \) the stripes through the base elements in the direction of the base vectors (i.e., \( t(x_w, a), t(x_w, b), t(x_w - b, a) \) and \( t(x_w - a, b) \)) are called base stripes. The set of base stripes is denoted by \( T_w \), while its intersection with the \( i \)-th half-plane is denoted by \( T_{wi} \).

Example: In Fig. 4 the base stripes for the graph \( G(8; \pm 2, \pm 3) \) with packed basis \( \{a, b\} = \{(4, 0), (1, 2)\} \) and \( w = 8 \) are depicted.

Minimal projection

The \( \ell_1 \)-smallest element on the stripe \( t(x, e) \) in the half-plane \( \mathbb{Z}_i^2 \) is called a minimal projection of \( x \) in the direction of \( e \) to \( \mathbb{Z}_i^2 \) and denoted \( P_i(x, e) \). For each \( x, e \in \mathbb{Z} \times \mathbb{Z} \) and \( i \in I \) the minimal projection \( P_i(x, e) \) can be found in constant time [10].

Example: The minimal projection \( P_1(x_w, b) \) is the element \((1, -1)\) since its norm (2) is smaller than the norms of all the other elements of the stripe \( t(x_w, b) \) (see Fig. 4).
Figure 4: The base stripes and the four sections of the set $X_w \ (w = 7)$ for the graph $G(8; \pm 2, \pm 3)$ with packed basis $\{a, b\} = \{(4, 0), (1, 2)\}$

**Sections of $X_w$**

Each element $x \in X_w$ can be expressed as $x = x_w + ma + nb; m, n \in \mathbb{Z}$. According to the signs of the integers $m$ and $n$ the set $X_w$ can be split into four sections,

$$X_w = [1]_w \cup [2]_w \cup [3]_w \cup [4]_w,$$

where

$$
\begin{align*}
&x \in [1]_w \iff m_x \geq 0 \land n_x \geq 0, \\
&x \in [2]_w \iff m_x < 0 \land n_x \geq 0, \\
&x \in [3]_w \iff m_x \geq 0 \land n_x < 0, \\
&x \in [4]_w \iff m_x < 0 \land n_x < 0.
\end{align*}
$$

For each $P \in \{1, 2, 3, 4\}$ the set of elements from $[P]_w$ not lying on the base stripes will be denoted by $(P)_w$.

**Example:** In Fig. 4 the four sections of the set $X_w \ (w = 7)$ for the graph $G(8; \pm 2, \pm 3)$ with the packed basis $\{a, b\} = \{(4, 0), (1, 2)\}$ are shaded.

Before presenting the algorithm for constructing the RSPs, let us reformulate our problem as a special kind of a closest vector problem and prove that resulting formulation is equivalent to Problem 1.

**Problem 4** Given $n, h_1, h_2, w = v - u \pmod{n}$ and $i$, take any $x \in X_w$ and find the element of $X^x_0 := \{z \in X_0; z_{[i]} \geq \text{sign}(i)x_{[i]}\}$ which is closest to the $x$. 

9
Lemma 3 Let $x \in X_w$ and let $z \in X_0^w$ such that $||z - x|| \leq ||z' - x||$, $\forall z' \in X_0^w$. Then $p_i(u, v) = x - z$.

Proof (Lema 3)
Since $z_i \geq \text{sign}(i)x_i$ it is obvious that $x - z \in X_i^w$. We only have to prove that among all the elements of $X_i^w$, $(x - z)$ is the smallest one. Suppose that there exists $x' \in X_i^w$ such that $||x'|| < ||x - z||$. Then $x - x' \in X_0^w$ and $||x - (x - x')|| = ||x'|| < ||x - z||$ which contradicts the assumption that $z$ is among all elements of $X_0^w$ the closest to the $x$.

4 Finding the RSPs

The RSPs $p_i(u, v)$, i.e., the shortest path from $u$ to $v$ with no hops of type $\epsilon_i$, is the $\ell_1$-smallest element of the set $X_i^w$, i.e., the smallest of the elements of the half-plane $\mathbb{Z}_i^2$ with the label $w$. Thus, to find the $p_i(u, v)$, one has to select from among all the elements in $\mathbb{Z}_i^2$ with the label $w$ the one with minimal $\ell_1$ norm. However, to reduce the number of candidates we use the following theorem.

Theorem 4 Let $\{a, b\}$ be a packed basis of a module $X_0$ for graph $G(n; \pm h_1, \pm h_2)$ and let $i \in I$, $w \in \mathbb{Z}_n$. Then the smallest element of $X_i^w$ is in $T_i^w$, i.e.,

$$\min_{x \in X_i^w} ||x|| = \min_{x \in T_i^w} ||x||.$$

Proof (Theorem 4)
To prove Theorem 4 it is sufficient to show that for each $x \in X_i^w$ there exists $y \in T_i^w$ whose norm is not bigger than the norm of $x$, i.e.,

$$\forall x \in X_i^w, \exists y \in T_i^w : ||y|| \leq ||x||. \tag{4}$$

For the elements $x$ that are already on one of the base stripes, the above statement is obviously true (take $y = x$), so we focus only on the elements in $X_i^w$ that are not in $T_i^w$, i.e., on the elements of the set

$$D_i^w := X_i^w - T_i^w.$$

We need to show that there exists a transformation $\tau : D_i^w \to X_i^w$ that decreases the distance from the base stripes $T_i^w$ and, at the same time, it does not increase the norm. Applying $\tau$ on $x \in D_i^w$ several times, i.e.,

$$y = \tau^n(\tau(\cdots \tau(x)),$$

for some $n$, decreases the distance to zero ($y \in T_i^w$) while $||y|| \leq ||x||$. This observation is formally stated in the following proposition where the distance of the element $x \in D_i^w$ from
the base stripes is denoted by \( r(x) \). The existence of a transformation \( \tau \) proves statement (4) and consequently Theorem 4.

**Proposition.** Let \( \{a, b\} \) be the packed basis of the module \( X_0 \) for the graph \( G(n; \pm h_1, \pm h_2) \), \( w \in \mathbb{Z}_n \) and \( x_w \) main base element. For each halfplane \( i \in I \), for each \( P \in \{1, 2, 3, 4\} \) and for each element \( x = x_w + m_x a + n_x b \in (P)_w^i \) there exists a transformation \( \tau : (P)_w^i \rightarrow [P]^i_w \), for which \( r(\tau(x)) < r(x) \) and \( ||\tau(x)|| \leq ||x|| \).

To prove this proposition one has to deal with 16 special cases (\( |I| \ast |P| = 16 \)) and for each of them there are 11 subcases (depending on the type of the packed basis). Some of these 176 cases are decomposed further on depending on the position of the element \( x \). The complete proof that extends over more than 25 pages (\([10] \), pages 55–65 and 79–95) treats all of these cases by proving (a) for \( i = 1, P = 1 \) it is true that \( ||x|| \geq \min ||x - a||, ||x - b|| \), therefore one of the transformations \( x \mapsto x - a \) and \( x \mapsto x - b \) has the desired properties, (b) for \( i = 1, P = 2 \) one of the transformations \( x \mapsto x - a \), \( x \mapsto x + b \), \( x \mapsto x + b - a \), \( x \mapsto x - [b/2a]a + b \) and \( x \mapsto x - [b_1/a_1]a + b \) has the desired properties, (c) for \( i = 1, P = 4 \) the domain is empty \( ([4]^1_w = \emptyset) \), therefore all conditions are improved by any \( \tau \), and (d) by applying reflection and rotation on a packed basis and the domain \([P]^i_w \) for all the other cases one can obtain the known and already proved case (a), (b) or (c). This completes the proof of the proposition and of Theorem 4.

Let us now show how to apply Theorem 4 in constructing RSPs. Since \( T_w^i \) is composed of the stripes \( t^i(x_w, a), t^i(x_w, b), t^i(x_w - b, a) \) and \( t^i(x_w - a, b) \), by Theorem 4 the smallest element of \( X_w^i \) is one of the smallest elements on these stripes, i.e.

\[
\min_{x \in X_w^i} ||x|| = \min_{x \in P} ||x||,
\]

where

\[
P = \{P^i(x_w, a), P^i(x_w, b), P^i(x_w - b, a), P^i(x_w - a, b)\}.
\]

Consequently, the RSPs can be constructed with the Algorithm A.

**Algorithm A**

input: \( n, h_1, h_2, i, u, v \)
output: RSP \( p_i(u, v) \)

begin

\{ \( a, b \) := packed basis of module \( X_0 \) for \( G(n; \pm h_1, \pm h_2) \); \}
\( w := v - u \mod n \); \( x_w := \text{main base element} \);
\( P := \{P^{-i}(x_w, a), P^{-i}(x_w, b), P^{-i}(x_w - b, a), P^{-i}(x_w - a, b)\} \); 

return \( \min_{t_i} P \);

end.

11
The correctness of Algorithm A follows from Theorem 4. The time complexity (expressed in the number of arithmetic operations) of Algorithm A is $O(\log n)$ since the packed basis and the main base element can be found in logarithmic time and minimal projections in constant time (see Section 3).

5 Conclusions

In this paper we introduced a subfamily of circulant graphs, called semi-directed circulant graphs, and defined their shortest paths as restricted shortest paths, RSPs. RSPs can be used for the indirect construction of general (i.e., unrestricted) shortest paths and to perform optimal dynamic routing. When routing a package from a given source to a given destination, RSPs are used at each intermediate node to determine the next node on one of the shortest paths. When heavy traffic is present RSP-based routing performs better than static routing since it can offer larger set of possible candidates for the next node.

In the paper we designed an optimal, $O(\log n)$ algorithm for constructing RSPs in 2-circulants. To do this we reformulated the problem in two algebraic forms: first by using linear Diophantine equations with two conditions, and then by using an integer lattice with a Manhattan norm. Thus, besides solving the graph theoretical problem the algorithm can also be used to solve optimization problems on linear Diophantine equations and to solve a special kind of closest vector problem in a point lattice.

Our RSP-based dynamic routing can be used in every topology in which the set of edges can be decomposed in $k > 1$ subsets of related edges (i.e., each node is connected to the rest of the graph with $k$ types of edges) and in which the routing destination depends only on the number of edges of a certain type (not on their ordering). In these topologies RSPs can be defined similarly as in 2-circulant graphs and the same routing algorithm can be used. What are these topologies (besides $k$-circulant graphs, mesh topology with wraparound connections and hyper-cubes) and how fast can one find their RSPs are the questions open for further research.

References


