ON ROUTING IN CIRCULANT GRAPHS

Jin-Yi Cai *
Dept. of Computer Science and Engineering
State University of NY at Buffalo, Buffalo, NY 14260-2000, USA
cai@cs.buffalo.edu

George Havas†
Dept. of Computer Science and Electrical Engineering
The University of Queensland, Qld 4072, Australia
havas@csee.uq.edu.au

Bernard Mans
Dept. of Computing, School of MPCE
Macquarie University, Sydney, NSW 2109, Australia
bmans@mpce.mq.edu.au

Ajay Nerurkar‡
Dept. of Computer Science and Engineering
State University of NY at Buffalo, Buffalo, NY 14260-2000, USA
apn@cs.buffalo.edu

Igor Shparlinski§
Dept. of Computing, School of MPCE
Macquarie University, Sydney, NSW 2109, Australia
igor@mpce.mq.edu.au

Abstract

We investigate various problems related to circulant graphs – finding the shortest path between two vertices, finding the shortest loop, and computing the diameter. These problems are related to shortest vector problems in a special class of lattices. We give matching upper and lower bounds on the length of the shortest loop. We prove NP-hardness results, and establish a worst-case/average-case connection for the shortest loop problem. A pseudo-polynomial time algorithm for these problems is also given. Our main tools are results and methods from the geometry of numbers.

Key Words Circulant graphs, Shortest paths, Loops, Diameter, Lattices

*Research supported in part by NSF grant CCR-9634665 and a J. S. Guggenheim Fellowship
†Research supported in part by ARC grants A49702337 and A49801415
‡Research supported in part by NSF grant CCR-9634665
§Research supported in part by ARC grant A69700294

1 Introduction

Circulant graphs have a vast number of applications to telecommunication network, VLSI design and distributed computation [5, 21, 23]. We study various routing problems in circulant graphs such as finding the shortest path between two vertices, finding the shortest loop and the diameter. We establish relations between these routing problems and the problem of finding the shortest vector in the L_1-norm in a lattice.

We recall that an n-vertex *circulant graph* G is a graph whose adjacency matrix $A = (a_{ij})_{i,j=0}^{n-1}$ is a circulant. That is, the ith row of A is the cyclic shift of the zeroth row by i,

$$a_{ij} = a_{0,j-i}, \qquad i, j = 0, \ldots, n-1,$$

(adjacency matrix subscripts are taken modulo n). We consider undirected graphs, that is, $a_{ij} = a_{ji}$ for $i, j = 0, \ldots, n-1$ and there are no self-loops ($a_{ii} = 0$ for $i = 0, \ldots, n-1$).

Therefore with every circulant graph one can associate a set S of positive integers which shows which pairs of nodes are connected. Two nodes u and v of the graph are connected if and only if $\pm(u - v) \pmod n \in S$. Given S we denote the corresponding n-vertex graph by $\langle S \rangle_n$. We denote the group of residues modulo n by $\mathbb{Z}_n$. Without loss of generality, we always assume that $S \subseteq \mathbb{Z}_n$.

Let $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$ with $1 \leq s_i \leq n/2$ for $i = 1, \ldots, m$. Given two vertices u and v of the graph $\langle S \rangle_n$, a path from u to v can be described by an integer vector $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ such that there are x_i steps of the form $w \to w + s_i$ if $x_i \geq 0$, or there are $|x_i|$ steps of the form $w \to w - s_i$ if $x_i < 0$, for $i = 1, \ldots, m$. It is easy to see that any permutation of a sequence of steps in a path from u to v produces another path from u to v.

Starting from u we arrive at v if and only if

$$\sum_{i=1}^{m} x_i s_i \equiv v - u \pmod n.$$

It is natural to aim to minimize the L_1-norm $|\mathbf{x}|_{L_1}$ which is the length of the shortest path between u and v. For any given n and $S = \{s_1, \ldots, s_m\}$, this minimal number depends only on $u - v$. Accordingly for $w \in \mathbb{Z}_n$ we denote by $\Omega(w) = \Omega_{n,S}(w)$ the set of solutions $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ of the congruence

$$\sum_{i=1}^{m} x_i s_i \equiv w \pmod n.$$

Define

$$D_{n,S}(w) = \min\{|\mathbf{x}|_{L_1} \ : \ \mathbf{x} \in \Omega(w), \mathbf{x} \neq 0\}.$$

The condition $\mathbf{x} \neq 0$ is relevant only when $w = 0$ and in this case

$$L(n, S) = D_{n,S}(0)$$

is the length of the shortest loop. We note that

$$D(n, S) = \max_{1 \leq w \leq n-1} D_{n,S}(w)$$

is the diameter of $\langle S \rangle_n$.

Let $a_1, \ldots, a_n$ be linearly independent vectors in $\mathbb{R}^n$. The set of all integral linear combinations of the a_i forms a (n-dimensional) lattice L, and the a_i are called a basis of L. A lattice can also be abstractly defined as a discrete additive subgroup of $\mathbb{R}^n$. The *determinant* of a lattice L is denoted by $\det(L)$. If $a_1, \ldots, a_n$ is a basis of L, then $\det(L) = |\det(a_1, \ldots, a_n)|$. It is invariant under a change of basis. We remark that $\Omega(0)$ is a lattice and $\Omega(w)$ is a shifted (affine) lattice, and so we can apply existing tools for studying short vectors in lattices and their shifts.

We formulate the following problems

Shortest-Path: Given a set $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$ and a residue $w \in \mathbb{Z}_n$, $w \neq 0$, find $D_{n,S}(w)$ and a vector $\mathbf{x} \in \Omega(w)$ for which $D_{n,S}(w) = |\mathbf{x}|_{L_1}$.

Shortest-Loop: Given a set $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$, find $L(n, S)$ and a vector $\mathbf{x} \in \Omega(0)$ for which $L(n, S) = |\mathbf{x}|_{L_1}$.

Diameter: Given a set $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$, find $D(n, S)$.

For general graphs these are well known problems. 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 that the input size is of order n^2, which is the number of elements in the adjacency matrix. However, any circulant graph can be described by only m integers $1 \leq s_1, \ldots, s_m \leq n/2$. In this representation the input size is of order $m \log n$. Thus polynomial time algorithms for general graphs may exhibit exponential complexity in the special case of circulant graphs.

Despite quite active interest in the above problems, motivated by various applications of circulant graphs, very few algorithmic results are known except for some special partial cases such as $m = 2$, see [10, 11, 19, 27]. These papers use quite elementary number theoretic considerations. Thus one of the purposes of this paper is to introduce new techniques in this area, namely the relatively modern theory of geometric lattices [1, 2, 3, 4, 6, 7, 8, 13, 15, 16, 17, 18, 20, 22, 24, 25, 26] as well as more classical tools from the geometry of numbers [9] and combinatorial number theory [12, 14].

First, we give estimates on the shortest loop length in terms of associated lattices. We provide upper and lower bounds which are close, within a factor of approximately two.

Then, we briefly discuss the case when the input n is given in unary. We provide an algorithm specifically tailored for the circulant graphs which solves the *Shortest-Loop* problem in polynomial time for this input measure. In contrast, we show that the *Shortest-Path* problem is NP-hard in the context of the more concise representation.

Finally, we prove that three lattice problems which are believed to be hard, are reducible to an average-case instance of the *Shortest Vector Problem* (**SVP**) for the homogeneous lattice family defined by circulant graphs, under a certain distribution on such lattices.

2 Estimates of Shortest Vectors

In this section we give estimates for the shortest loop length $L(n, S)$ in terms of the lattice defined by the congruence $\sum_{i=1}^{m} a_i x_i \equiv 0 \pmod{n}$. For simplicity we focus on the case where the modulus n is a prime p. This can be generalized to a composite modulus via the Chinese Remainder Theorem. In fact taking the lattice view, it is natural to consider the more general setting where a set of s congruences is given,

$$A\mathbf{x} \equiv 0 \pmod{p}, \qquad \mathbf{x} \in \mathbb{Z}^m,$$

where $A = (a_{ij}) \in \mathbb{Z}_p^{s \times m}$, which defines a lattice L of dimension m. The case with the circulant graph is $s = 1$. This lattice is of dimension m, independent of s, since $p \cdot e_i \in L$, for all i, where e_i is the ith canonical basis vector (for $\mathbb{Z}^m$). Note that in general $p \cdot e_i$ do not form a basis for L.

We now compute the determinant of L. The map $\mathbf{x} \mapsto A\mathbf{x} \pmod{p}$ defines a homomorphism from $\mathbb{Z}^m$ to $\mathbb{Z}_p^s$, the kernel of which is our lattice L. Thus the cardinality $|\mathbb{Z}^m / L| \leq p^s$ (equality holds if and only if A has rank m over $\mathbb{Z}_p$). Hence $\det(L) \leq p^s$, with equality if and only if A has rank m over $\mathbb{Z}_p$.

Let $B_m(r) = \{\mathbf{x} \in \mathbf{R}^m \ : \ |\mathbf{x}|_{L_1} \leq r\}$ be the L_1-norm ball of radius r in m-dimensional space. Then the volume

$$\mathrm{vol}(B_m(r)) = r^m \cdot \frac{2^m}{m!}.$$

By Minkowski's Theorem, see Theorem 2 of Chapter 3 of [9], if $\mathrm{vol}(B_m(r)) \geq 2^m \det(L)$, then there is a non-zero vector $x \in L \cap B_m(r)$. Because $2^m p^s \geq 2^m \det(L)$, a sufficient condition on r is

$$r \geq \sqrt[m]{m!}\, p^{s/m} \approx \frac{m}{e} p^{s/m},$$

(The approximation is based on $\sqrt[m]{m!} = \frac{m}{e}(1 + o(1))$ as $m \to \infty$.) Thus we have

Theorem 1. *For any system $A\mathbf{x} \equiv 0 \pmod{p}$, where $A \in \mathbb{Z}_p^{s \times m}$, there is a solution $\mathbf{x} \in \mathbb{Z}^m$, $\mathbf{x} \neq 0$, and $|\mathbf{x}|_{L_1} \leq \sqrt[m]{m!}\, p^{s/m}$. In particular, for any circulant graph $\langle S \rangle_p$,*

$$L(p, S) \leq \sqrt[m]{m!}\, p^{1/m},$$

where $m = |S|$.

Let $N_m(r) = |\{\mathbf{x} \in \mathbb{Z}^m : x_i \geq 0, \text{ and } x_1 + \cdots + x_m \leq r\}|$. It is elementary to show that

$$N_m(r) = \binom{r+m}{m}.$$

Thus $\mathbb{Z}^m \cap B_m(r) = \{\mathbf{x} \in \mathbb{Z}^m : |\mathbf{x}|_{L_1} \leq r\}$ has cardinality at most $2^m \binom{r+m}{m}$.

Now to each non-zero $\mathbf{x} \in \mathbb{Z}^m \cap B_m(r)$, there are exactly $p^{m-1} - 1$ non-zero coefficient sequences $(a_1, \ldots, a_m) \in \mathbb{Z}_p^m$ for which $\sum_{i=1}^{m} a_i x_i \equiv 0 \pmod{p}$. Altogether this can account for at most $(2^m \binom{r+m}{m} - 1)(p^{m-1} - 1)$ non-zero sequences $(a_1, \ldots, a_m) \in \mathbb{Z}_p^m$. Thus if

$$p^m - 1 > (2^m \binom{r+m}{m} - 1)(p^{m-1} - 1),$$

then some $(a_1, \ldots, a_m) \neq 0$ has no solution with norm at most r. The following bound is certainly a sufficient condition for this:

$$p \geq 2^m \binom{r+m}{m}.$$

Since $\binom{r+m}{m} \leq ((r+m)e/m)^m$, after some simple calculation, we have the sufficient condition

$$r < m\left(\frac{1}{2e}p^{1/m} - 1\right).$$

Theorem 2. *There are circulant graphs $\langle S\rangle_p$ with*

$$L(p, S) \geq m\left(\frac{1}{2e}p^{1/m} - 1\right).$$

We note that this lower bound almost matches the upper bound in Theorem 1, within a factor of about 2. Also the analysis here can be given in terms of a matrix $A \in \mathbb{Z}_p^{s\times m}$, in which case, we replace the quantity $p^{1/m}$ by $p^{s/m}$.

Unfortunately the above considerations do not seem to apply to the non-homogeneous case. Nevertheless, some number theoretic results of [12, 14] allow us to deal with this case as well. In particular, we obtain an upper bound on $D(n, S)$, which, in some cases, is quite tight.

Theorem 3. *For any circulant graph $\langle S\rangle_p$ with $m \geq 0.5\left\lfloor(4p-7)^{1/2}\right\rfloor + 1$,*

$$D(p, S) \leq 0.5\left\lfloor(4p-7)^{1/2} + 1\right\rfloor \sim p^{1/2},$$

where $|S| = m$.

Proof. It is shown in [12] that for any set $T \subseteq \mathbb{Z}_p^*$ of cardinality $|T| = \left\lfloor(4p-7)^{1/2}\right\rfloor + 1$, any element $w \in \mathbb{Z}_p$ can be represented in the form

$$w \equiv \sum_{t\in W} t \pmod p$$

for some subset $W \subseteq T$ of cardinality at most $|T|/2$. It is obvious that the cardinality of the set $R = S \cup -S$ is at least $2m - 1$. Thus selecting an arbitrary subset $T \subseteq R$ of cardinality $|T| = \left\lfloor(4p-7)^{1/2}\right\rfloor + 1 \leq 2m - 1$ we obtain the required result. □

We remark that if $m \sim p^{1/2}$ and $S = \{1, \ldots, m\}$ then, obviously, $D(p, S) \geq p/m \sim p^{1/2}$, thus Theorem 3 is tight for such circulant graphs.

3 Polynomial Time Algorithms for Small n

When n is given as a unary input and the time complexity is measured in terms of n, there are well known polynomial time algorithms to find both the length of the shortest path between

any two vertices of a graph with n vertices, as well as a shortest path itself. This applies to circulant graphs as a special case. However, even in this case, due to the symmetry present in any circulant graph, considerable savings can be realized in time complexity, compared to using a general graph algorithm.

We concentrate on the *Shortest-Loop* problem. The definition of a *loop* here is specifically tailored for the circulant graph, and is not merely a specialization of a loop in general graphs. This is because there is a "commutativity" of the underlying group $\mathbb{Z}_n$, and so we exclude certain "trivial loops". For example, suppose there are two distinct step sizes s_1 and $s_2 \in S$. The closed path $\langle 0, s_1, s_1+s_2, s_2, 0\rangle$, using steps $s_1, s_2, -s_1, -s_2$ respectively, would be considered a loop in a general graph, but is excluded here.

Assume we are given $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$. The idea of the following algorithm for finding loops is to try to compute all shortest paths connecting 0 and some $is_k \pmod n$, using only steps from $S' = \{s_1, \ldots, s_{k-1}\}$. We do this for all i and then for all k, and finally take the minimum.

Fix k, $1 \le k \le m$. Let $g_k = \gcd(s_k, n)$. Let $s'_k = s_k/g_k, n_k = n/g_k$. Then $\gcd(s'_k, n_k) = 1$, and we can solve integral linear equations

$$s'_k x - n_k y = \pm 1.$$

The general solution has the form $x = \pm[x_0 + tn_k]$ and $y = \pm[y_0 + ts'_k]$, for some x_0 and y_0, and where all $t \in \mathbb{Z}$ are admissible. Choose t so that the absolute value $|x| = |x_0 + tn_k|$ is minimum. This will set $|x| \le \lfloor n_k/2 \rfloor$ and the corresponding t is essentially unique. We denote this minimizing x by x_k.

Next, for each j, $1 \le j \le \lfloor n_k/2 \rfloor$, we compute the shortest path from 0 to $js_k \bmod(n)$, in the graph $\langle S'\rangle_n$ defined by $S' = \{s_1, \ldots, s_{k-1}\}$. The minimum path length in this graph is $D_{n,S'}(js_k)$.

Let

$$f(i,k) = \begin{cases} j + D_{n,S'}(js_k) & \text{if } i \equiv \pm js_k \pmod n, 1 \le j \le \lfloor n_k/2 \rfloor \\ \infty & \text{otherwise, that is, } g_k \not| \, i, \end{cases} \tag{1}$$

where $1 \le i \le n-1$, and let

$$f(0,k) = n_k.$$

Note that, for $1 \le i \le n-1$, $g_k = \gcd(s_k, n) \mid i$ if and only if there is some j, where $1 \le j \le \lfloor n_k/2 \rfloor$, such that $i \equiv \pm js_k \pmod n$. Moreover, in this case, such a $\pm j$ is unique, (except in the case where n_k is even and $i = \frac{n_k}{2}s_k$, in which case there are exactly two values $+\frac{n_k}{2}$ and $-\frac{n_k}{2}$.)

To see this, one direction is trivial: if $i \equiv \pm js_k \pmod n$ for some j, then $g_k = \gcd(s_k, n) \mid i$. Now suppose $g_k \mid i$. Then i belongs to the subgroup generated by g_k in $\mathbb{Z}_n$, which is also generated by s_k. This subgroup has order n_k. Hence there is some j within the specified range $1 \le j \le \lfloor n_k/2 \rfloor$, such that

$$i \equiv \pm js_k \pmod n. \tag{2}$$

$j \ne 0$ since $i \not\equiv 0 \pmod n$. In the general case when $g_k \mid i$, except when n_k is even and $i = \frac{n_k}{2}s_k$, the uniqueness of such a $\pm j$ is quite obvious. For otherwise we have $((\pm j) - (\pm j'))s_k \equiv 0 \pmod n$ which implies that $n_k \mid ((\pm j) - (\pm j'))$. And the only possibility for this to hold is $j = j' = n_k/2$ but they took opposite signs in (2), and $i = \frac{n_k}{2}s_k$. Indeed in this case the $\pm j$ in (2) is not unique, but nonetheless the value of $f(i,k)$ is uniquely defined.

This shows that the function $f(i,k)$ is well defined, and given any algorithm for finding shortest paths, this gives us an algorithm to compute $f(i,k)$. In particular this gives a polynomial time algorithm for $f(i,k)$.

Now we claim that the minimum loop size

$$L(n,S) = \min_{0 \le i \le n-1, 1 \le k \le m} f(i,k). \tag{3}$$

Clearly the minimum value on the right in (3) produces the length of some loop. Since all $s_k \neq 0$, using s_k alone, one can form a loop with exactly $f(0,k) = n_k$ steps (and no less). Thus the minimum is finite. In the case $1 \le i \le n-1$, the value $f(i,k)$ gives the length of some loop, if such a loop exists, that consists of step sizes $s_1, \ldots, s_k$ only, with a non-zero number of step size s_k.

Let $\mathcal{L}$ be a loop achieving $L(n,S)$. We show that our minimum value on the right of (3) is at least as small. This establishes (3).

If $\mathcal{L}$ involves only one step size s_k, then $f(0,k) = n_k$ gives the shortest loop in this case. Let $\mathcal{L}$ involve more than one step size, and let k be the largest ℓ such that $\mathcal{L}$ involves a non-zero number x_ℓ of steps of size s_ℓ. Since $\mathcal{L}$ is minimal, $s_k x_k \not\equiv 0 \pmod{n}$, for otherwise, by deleting the steps involving s_k we still have a non-trivial loop.

Let i be the least modulus of $-s_k x_k \pmod{n}$, where $1 \le i \le n-1$, then $\sum_{\ell=1}^{k-1} s_\ell x_\ell \equiv i \pmod{n}$, and x_ℓ is the number of steps in $\mathcal{L}$ involving s_ℓ. Since the subgroup of $\mathbb{Z}_n$ generated by s_k has order n_k, there is a j, $1 \le j \le \lfloor n_k/2 \rfloor$, such that $-s_k x_k \equiv \pm j s_k \pmod{n}$. This implies that $-x_k \equiv \pm j \pmod{n_k}$. Since $|\mathbf{x}|_{L_1}$ is minimal, $x_k = \pm j$.

After taking away the steps involving s_k, what remains is a path from 0 to $i \equiv -s_k x_k \pmod{n}$ using only steps $s_1, \ldots, s_{k-1}$, the minimum length of which has been found in the equation (1) defining $f(i,k)$.

This completes the description of our algorithm to compute $L(n,S)$. Now, we estimate its time complexity. Let $\langle S_l \rangle_n$ be the graph defined by $S_l = \{s_1, \ldots, s_l\}$, where $1 \le l \le m$. To compute $f(i,k)$, where $i \equiv \pm j s_k \pmod{n}$, we need to know the value of $D_{n,S_{k-1}}(j s_k)$. We first do a breadth-first search on $\langle S_l \rangle_n$, for $l = 1, \ldots, m$, to compute the length of the shortest path from 0 to every other vertex in each of these graphs. This can be done in a total time of $O(nm^2)$. The rest of the computation takes time $O(nm \text{ polylog}(n))$. Therefore we have the following result

Theorem 4. *The Shortest-Loop Problem can be solved in time* $O(nm^2 + nm \log^{O(1)} n)$.

A more careful design of the algorithm can be shown to reduce the time to $O(nm)$.

4 NP-hardness for the *Shortest-Path* problem

In this section we show that the *Shortest-Path* problem is NP-hard. We can also show NP-hardness and quasi NP-hardness of the approximation version of this problem. These will be discussed in the full paper. We first state a decision problem version of the *Shortest-Path* problem. We show that this problem is NP-complete, and the NP-hardness of the optimization problem follows easily.

Shortest-Path Decision Problem(SPDP)
Instance: Given in binary an integer n, a set $S = \{s_1, \ldots, s_m\} \subseteq \mathbb{Z}_n$, a residue $w \in \mathbb{Z}_n$, $w \neq 0$, and a bound b.
Question: Is $D_{n,S}(w) \leq b$?
Size: $\text{length}(n) + \sum_{i=1}^{m} \text{length}(s_i) + \text{length}(w) + \text{length}(b)$.

Theorem 5. *The Shortest-Path Decision Problem (SPDP) is NP-complete.*

Proof. We reduce the following well-known NP-complete decision problem to the Shortest-Path Decision Problem.

Exact-3-Cover(X3C)
Instance: A positive integer q and a collection C of 3-element subsets of the set $X = \{1, 2, 3, ..., 3q\}$.
Question: Is there an exact cover $C' \subseteq C$ for X (so that each element of X belongs to exactly one member of C')?
Size: $q + |C|$, where $|C|$ is the cardinality of C.

Details of the proof are in Appendix A. □

5 The Hardness for Homogeneous Systems

In the last section we showed that the optimization problem of finding $D_{n,S}(w)$ for a general right hand side w is NP-hard. This corresponds to the SVP in a special class of *affine* lattices. The homogeneous case where $w = 0$ is the SVP in a special class of *homogeneous* lattices, namely those definable by a single congruence of the form $\sum_{i=1}^{m} s_i x_i \equiv 0 \pmod{n}$.

There has been a considerable amount of work on the SVP for homogeneous lattices. Van Emde Boas [26] showed that it is NP-hard for the L_∞-norm (see also [20]). The NP-hardness for every other L_p-norm, especially for the L_2-norm, was open until a recent breakthrough by Ajtai [2], who showed that the problem for the L_2-norm is NP-hard under randomized reductions. Moreover Ajtai [2] also showed that it is NP-hard to approximate the shortest non-zero vector in an m-dimensional lattice within a factor of $(1 + 2^{-m^k})$, for a sufficiently large constant k. This was improved by Cai and Nerurkar [8] to a factor of $\left(1 + \frac{1}{m^\epsilon}\right)$, for any $\epsilon > 0$. They [8] also noted explicitly that the proof works for arbitrary L_p-norms, $1 \leq p < \infty$. Micciancio further improved this factor to $\sqrt{2} - \epsilon$ [24]. Approximations to the closest vector in a lattice were considered in [4, 13]. However, in all these reductions, the lattices constructed do not fall into the category of lattices defined in terms of circulant graphs, that is, definable by a single congruence. Nevertheless, we show (in Appendix C) that the SVP for such lattices is, in fact, NP-hard under randomized reductions. We prove the following theorem:

Theorem 6. *The SVP for the class of (homogeneous) lattices defined by circulant graphs is NP-hard under randomized reductions. Moreover, it remains NP-hard to find an approximate shortest vector in this class of lattices within a factor of $\sqrt{2} - \epsilon$, for any constant $\epsilon > 0$.*

In this section, we focus on a worst-case/average-case connection.

Ajtai, in a separate work [1], established a reduction from the worst-case complexity of some problems believed to be hard, to the average-case complexity of the approximate SVP for a certain class of random lattices. This worst-case/average-case connection is the only such provable

reduction known for a problem in NP believed to be hard and has generated a lot of interest [3, 6, 7, 15, 16, 17, 18]. We state below three problems which are believed to be hard for any constants c_1, c_2 and c_3:

(P1) Find $\lambda_1(L)$, the length of a shortest non-zero vector in an m-dimensional lattice L, up to a polynomial factor m^{c_1}.

(P2) Find the shortest non-zero vector in an m-dimensional lattice, where the shortest vector is unique up to a polynomial factor m^{c_2}.

(P3) Find a basis in an m-dimensional lattice whose maximum length is the smallest possible, up to a polynomial factor m^{c_3}.

Let $\mathbb{Z}_q^{r\times l}$ denote the set of $r \times l$ matrices over $\mathbb{Z}_q$. For every r, l, q, $\Omega_{r,l,q}$ denotes the uniform distribution on $\mathbb{Z}_q^{r\times l}$. For every $X \in \mathbb{Z}_q^{r\times l}$, the set $\Lambda(X) = \{y \in \mathbb{Z}^l \mid Xy \equiv 0 \pmod q\}$ defines a lattice of dimension l. $\Lambda_{r,l,q}$ denotes the probability space of lattices consisting of $\Lambda(X)$ by choosing X according to $\Omega_{r,l,q}$. Let $q = r^c$ be an arbitrary but fixed polynomial of r. By Minkowski's Theorem, see Theorem 2 of Chapter 3 of [9], it can be proved that, $\forall c\ \exists c'$ such that $\forall \Lambda(X) \in \Lambda_{r,c'r,r^c},\ \lambda_1(\Lambda(X)) \leq r$. (In fact, this bound can be improved to $\Theta(r^{1/2+\epsilon})$.) Let $l = c'r$ where c' depends on c as indicated above. Let $\Lambda = \Lambda_{r,l,q}$. Ajtai showed:

Theorem 7 (Ajtai). *Let γ be any constant. If there is a probabilistic polynomial time algorithm $\mathcal{A}$ such that, with non-trivial probability $1/r^{O(1)}$, $\mathcal{A}$ finds a short non-zero vector v, $|v|_{L_2} \leq r^\gamma$, for a uniformly chosen lattice in the class Λ indexed by r, then there is a probabilistic polynomial time algorithm $\mathcal{B}$ that solves the three problems* **(P1)**, **(P2)** *and* **(P3)** *in the worst case, with high probability, for some constants c_1, c_2 and c_3.*

We prove here that these problems are also reducible to an average-case instance of the SVP for the lattice family defined by circulant graphs, under a certain distribution on such lattices. This is not quite an NP-hardness proof, since these problems **(P1)**, **(P2)** and **(P3)** are not known to be NP-hard. In fact there is evidence that they are not. Goldreich and Goldwasser showed that approximating the shortest lattice vector within a factor of $O(\sqrt{m/\log m})$ is not NP-hard assuming the polynomial time hierarchy does not collapse [15]. Cai showed that finding an $m^{1/4}$-unique shortest lattice vector is not NP-hard unless the polynomial time hierarchy collapses [6]. On the other hand, these problems have resisted all attempts at finding a (probabilistic) polynomial time algorithm to date. The best polynomial time algorithm is essentially the L^3 basis reduction algorithm [22] which achieves an approximation factor of $2^{m/2}$ for the SVP. Schnorr improves this factor to $(1+\epsilon)^m$, still exponential in m and with the running time depending badly on ϵ in the exponent [25]. Thus it is reasonable to assume that these problems **(P1)**, **(P2)** and **(P3)** are computationally hard.

The following proof establishes that for a certain distribution of circulant graphs, or equivalently for the special class of lattices, the average-case complexity of approximating the shortest vector in a lattice within any polynomial factor is at least as hard as these three problems in the worst-case. We first present a construction that reduces the problem of finding a short vector in a lattice $\Lambda(X)$ to the problem of finding a short solution vector to an appropriate congruence.

Given numbers q, β and a matrix $X \in \mathbb{Z}_q^{r\times l}$, we construct in polynomial time, a sequence $s_1, \ldots, s_{l+r}$ of $l + r$ integers and an integer n. The congruence we consider is $\sum_{i=1}^{l+r} s_i x_i \equiv 0 \pmod n$.

Define $k = \lceil \log_2 \beta \rceil + \lceil \log_2 q \rceil + 1$. For $i = 1, \ldots, l$, let $s_i = \sum_{j=1}^{r} X_{ji} 2^{(j-1)k}$. Essentially, s_i is a concatenation of padded versions of the entries in the i^{th} column of X. For $i = l+1, \ldots, l+r$, define $s_i = 2^{(i-l-1)k} q$. Define n to be any integer larger than $2^{rk}\beta$. The next theorem shows that the above construction is a reduction. This theorem can be tightened to get rid of the multiplicative factor r below. As our main goal in this section is to prove Theorem 9, we defer the stronger version to the full paper.

Theorem 8. *Let α be any number. Given a vector $\mathbf{v} \in \Lambda(X)$, $0 < |\mathbf{v}|_{L_1} \leq \alpha$, a solution vector $\mathbf{x}$ to the congruence $\sum_{i=1}^{l+r} s_i x_i \equiv 0 \pmod{n}$, with $0 < |\mathbf{x}|_{L_1} \leq (r+1)\alpha$, can be computed in polynomial time, and given a solution $\mathbf{x}$ to the congruence, $0 < |\mathbf{x}|_{L_1} \leq \beta$, a vector $\mathbf{v} \in \Lambda(X)$ with $0 < |\mathbf{v}|_{L_1} \leq \beta$, can be computed in linear time.*

Proof. Let $\mathbf{v} = (v_1, \ldots, v_l) \in \Lambda(X)$, $0 < |\mathbf{v}|_{L_1} \leq \alpha$. By the definition of $\Lambda(X)$, there are integers $a_1, \ldots, a_r$, such that for $j = 1, \ldots, r$,

$$\sum_{i=1}^{l} v_i X_{ji} = a_j q.$$

From this it follows that $|a_j| \leq |\mathbf{v}|_{L_1} \leq \alpha$ because for all i, j, $0 \leq X_{ji} < q$. We claim that the vector $\mathbf{x} = (v_1, \ldots, v_l, -a_1, \ldots, -a_r)$ is a solution to the congruence. This is because

$$\begin{aligned}
\sum_{i=1}^{l} v_i s_i + \sum_{j=1}^{r} (-a_j) s_{l+j} &= \sum_{i=1}^{l} v_i \left(\sum_{j=1}^{r} X_{ji} 2^{(j-1)k} \right) + \sum_{j=1}^{r} (-a_j) q 2^{(j-1)k} \\
&= \sum_{j=1}^{r} 2^{(j-1)k} \left(\sum_{i=1}^{l} v_i X_{ji} - a_j q \right) \\
&= 0.
\end{aligned}$$

Clearly $\mathbf{x}$ is non-zero, and $|\mathbf{x}|_{L_1} = |\mathbf{v}|_{L_1} + \sum_{j=1}^{r} |a_j| \leq \alpha + \alpha r = (r+1)\alpha$.

Now, let $\mathbf{x} = (x_1, \ldots, x_{l+r})$ be a solution to the congruence $\sum_{i=1}^{l+r} s_i x_i \equiv 0 \pmod{n}$, such that $|\mathbf{x}|_{L_1} \leq \beta$. Every s_i is at most 2^{rk} and so the sum $\sum_{i=1}^{l+r} s_i x_i$ is at most $2^{rk}\beta$ in absolute value, and since n has been chosen to be bigger than this quantity, $\sum_{i=1}^{l+r} s_i x_i = 0$. We claim that $\mathbf{v} = (x_1, \ldots, x_l)$ belongs to $\Lambda(X)$, that is, $X\mathbf{v} \equiv 0 \pmod{q}$.

We prove by induction on j, $j = 1, \ldots, r$, that $\sum_{i=1}^{l} X_{ji} x_i + q x_{l+j} = 0$. This proves that $\sum_{i=1}^{l} X_{ji} x_i \equiv 0 \pmod{q}$. First the base case. We can rewrite $\sum_{i=1}^{l+r} s_i x_i = 0$ as

$$\sum_{i=1}^{l} s_i x_i + \sum_{i=l+1}^{l+r} s_i x_i = 0.$$

We know that $s_i \equiv X_{1i} \pmod{2^k}$ for $i = 1, \ldots, l$, $s_{l+1} \equiv q \pmod{2^k}$, and for all other i, $s_i \equiv 0 \pmod{2^k}$. Writing the above equation mod 2^k gives us

$$\sum_{i=1}^{l} X_{1i} x_i + q x_{l+1} \equiv 0 \pmod{2^k}.$$

Since $0 \leq X_{1i} < q$ and $|\mathbf{x}|_{L_1} \leq \beta$, the above sum is at most $q\beta$ in absolute value. By definition, $q\beta < 2^k$. Therefore, $\sum_{i=1}^{l} X_{1i} x_i + q x_{l+1} = 0$.

Now, let us assume that $\sum_{i=1}^{l} X_{ji}x_i + qx_{l+j} = 0$ for $j = 1, 2, \ldots, j'$. We show that $\sum_{i=1}^{l} X_{ji}x_i + qx_{l+j} = 0$ for $j = j' + 1$. Let s'_i be the quotient obtained by dividing s_i by $2^{j'k}$. In other words, s'_i is the number got by removing the $j'k$ least significant bits of s_i. We claim (details in Appendix B) that

$$\sum_{i=1}^{l+r} s'_i x_i = 0. \tag{4}$$

Clearly, for $i = 1, \ldots, l$, $s'_i \equiv X_{j'+1,i} \pmod{2^k}$, $s'_{l+j'+1} \equiv q \pmod{2^k}$, and for all other i, $s'_i \equiv 0 \pmod{2^k}$. Therefore, taking (4) modulo 2^k, we see that $\sum_{i=1}^{l} X_{j'+1,i}x_i + qx_{l+j'+1} = 0$. This completes the induction. Therefore, for $j = 1, \ldots, r$, $\sum_{i=1}^{l} X_{ji}x_i + qx_{l+j} = 0$, and so $\sum_{i=1}^{l} X_{ji}x_i \equiv 0 \pmod{q}$. Clearly, $|\mathbf{v}|_{L_1} \leq |\mathbf{x}|_{L_1} \leq \beta$. □

We now apply this reduction to show that, to solve a congruence of the form $\sum_{i=1}^{r} s_i x_i \pmod{n}$ is as hard on the average, under a suitable distribution on the s_i and n, as problems **(P1)**, **(P2)** and **(P3)** are in the worst case. We first define the random distribution used.

The distribution takes two parameters, r and β. Let $q = r^{O(1)}$ and $l = \Theta(r)$ be as in the definition of Λ in Theorem 7. Define the set $S = S_{r,\beta}$ to be the set of positive integers less than 2^{rk}, where $k = \lceil \log_2 \beta \rceil + \lceil \log_2 q \rceil + 1$. Define the following distribution $D_{r,\beta}$ on integers $(s_1, \ldots, s_{l+r}, n) \in S^{l+r} \times \mathbb{Z}$. $D_{r,\beta}$ is obtained by first picking uniformly an $r \times l$ matrix X with entries in $\mathbb{Z}_q$, and then letting $s_i = \sum_{j=1}^{r} X_{ji} 2^{(j-1)k}$ for $i = 1, \ldots, l$, $s_i = 2^{(i-l-1)k} q$, for $i = l+1, \ldots, l+r$ and n be an integer greater than $2^{rk}\beta$, chosen according to any fixed distribution.

We get the following worst-case/average-case connection.

Theorem 9. *Let $\gamma > 2.5$ be any constant in Theorem 7 and let $l = \Theta(r)$ as above. If there is a probabilistic polynomial time algorithm $\mathcal{C}$ such that, with non-trivial probability $1/r^{O(1)}$, $\mathcal{C}$ finds a solution vector x of L_1-norm length at most r^γ for the congruence $\sum_{i=1}^{l+r} s_i x_i \equiv 0$ (mod n), where the s_i and n are chosen according to distribution D_{r,r^γ}, then there is a probabilistic polynomial time algorithm $\mathcal{D}$ that solves the three problems* **(P1)**, **(P2)** *and* **(P3)** *in the worst case, with high probability, for some constants c_1, c_2 and c_3.*

Proof. We show that the hypothesis implies that there is an algorithm which, with non-trivial probability $1/r^{O(1)}$, finds a short non-zero vector v of L_1-norm length at most r^γ, for a lattice $\Lambda(X)$ defined by a uniformly chosen matrix $X \in \mathbb{Z}_q^{r \times l}$, that is, a lattice chosen uniformly from Λ.

Given such a matrix X, we apply the reduction with $\beta = r^\gamma$, and construct an integer n and a sequence $s_1, \ldots, s_{l+r}$. Note that $s_1, \ldots, s_{l+r}, n$ have the distribution D_{r,r^γ}. By Minkowski's Theorem, see Theorem 2 of Chapter 3 of [9], there exists $\mathbf{v} \in \Lambda(X)$, $|\mathbf{v}|_{L_2} \leq r$. Therefore, by the Cauchy-Schwarz inequality, $|\mathbf{v}|_{L_1} \leq r\sqrt{l} = O(r^{1.5})$. By Theorem 8, there exists a solution vector $\mathbf{x}$ to the congruence $\sum_{i=1}^{l+r} s_i x_i \equiv 0 \pmod{n}$ with $|\mathbf{x}|_{L_1} = O(r^{2.5})$. Thus, our assumption about $\mathcal{C}$ is not vacuous, since $\gamma > 2.5$. By Theorem 8 again, given a solution $\mathbf{x}$ to the congruence, $|\mathbf{x}|_{L_1} \leq r^\gamma$, a vector $\mathbf{v} \in \Lambda(X)$ with $|\mathbf{v}|_{L_1} \leq r^\gamma$ can be constructed. The result now follows by Theorem 7 because $|\mathbf{v}|_{L_2} \leq |\mathbf{v}|_{L_1}$. □

References

[1] M. Ajtai. Generating hard instances of lattice problems. In *Proc. 28th Annual ACM Symposium on the Theory of Computing* (1996) 99–108. Available as TR96-007 from *Electronic Colloquium on Computational Complexity* at `http://www.eccc.uni-trier.de/eccc/`.

[2] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. In *Proc. 30th Annual ACM Symposium on the Theory of Computing* (1998) 10–19. Available as TR97-047 from *Electronic Colloquium on Computational Complexity* at `http://www.eccc.uni-trier.de/eccc/`.

[3] M. Ajtai and C. Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proc. 29th ACM Symposium on Theory of Computing* (1997) 284–293. Available as TR96-065 from *Electronic Colloquium on Computational Complexity* at `http://www.eccc.uni-trier.de/eccc/`.

[4] S. Arora, L. Babai, J. Stern, and Z. Sweedyk. The hardness of approximate optima in lattices, codes, and systems of linear equations. In *Proc. 34th IEEE Symposium on Foundations of Computer Science (FOCS)*, 724-733, 1993.

[5] J.-C. Bermond, F. Comellas and D. F. Hsu. Distributed loop computer networks: A survey. *Journal of Parallel and Distributed Computing* **24** (1995) 2–10.

[6] J-Y. Cai. A relation of primal-dual lattices and the complexity of shortest lattice vector problem. *Theoretical Computer Science* **207** (1998) 105–116.

[7] J-Y. Cai and A. Nerurkar. An improved worst-case to average-case connection for lattice problems. In *Proc. 38th IEEE Symposium on Foundations of Computer Science* (1997) 468–477.

[8] J-Y. Cai and A. Nerurkar. Approximating the SVP to within a factor $\left(1 + \frac{1}{\dim^\epsilon}\right)$ is NP-hard under randomized reductions. In *Proc. 13th Annual IEEE Conference on Computational Complexity* (1998) 46–55.

[9] J. W. S. Cassels. *An introduction to the geometry of numbers*. Springer-Verlag, 1959.

[10] N. Chalamaiah and B. Ramamurty. Finding shortest paths in distributed loop networks. *Inform. Proc. Letters* **67** (1998) 157–161.

[11] Y. Cheng and F. K. Hwang. Diameters of weighted loop networks. *J. of Algorithms* **9** (1988) 401–410.

[12] J. A. Dias da Silva and Y. O. Hamidoune. Cyclic spaces for Grassmann derivatives and additive theory *Bull. Lond. Math. Soc.* **26** (1994) 140–146.

[13] I. Dinur, G. Kindler and S. Safra. Approximating-CVP to within almost-polynomial factors is NP-hard. 1998. Available as TR98-048 from *Electronic Colloquium on Computational Complexity* at `http://www.eccc.uni-trier.de/eccc/`.

[14] P. Erdös and H. Heilbronn On the addition of residue classes mod p *Acta Arithm.* **9** (1964) 149–159.

[15] O. Goldreich and S. Goldwasser. On the limits of non-approximability of lattice problems. In *Proc. 30th Annual ACM Symposium on the Theory of Computing* (1998) 1–9.

[16] O. Goldreich, S. Goldwasser and S. Halevi. Collision-free hashing from lattice problems. 1996. Available as TR96-042 from *Electronic Colloquium on Computational Complexity* at `http://www.eccc.uni-trier.de/eccc/`.

[17] O. Goldreich, S. Goldwasser and S. Halevi. Eliminating decryption errors in the Ajtai-Dwork cryptosystem. *Advances in Cryptology - CRYPTO '97* (editor B. Kaliski Jr.), Lecture Notes in Computer Science 1294 (Springer Verlag, 1997) 105–111.

[18] O. Goldreich, S. Goldwasser and S. Halevi. Public-key cryptosystems from lattice reduction problems. Advances in Cryptology - CRYPTO '97 (editor B. Kaliski Jr.), Lecture Notes in Computer Science 1294 (Springer Verlag, 1997) 112–131.

[19] D. J. Guan. Finding shortest paths in distributed loop networks. *Inform. Proc. Letters* **65** (1998) 255–260.

[20] J. C. Lagarias. The computational complexity of simultaneous diophantine approximation problems. In *Proc. 23rd IEEE Symposium on Foundations of Computer Science* (1982) 32–39.

[21] F. T. Leighton. *Introduction to parallel algorithms and architectures: Arrays, trees, hypercubes*. M. Kaufmann, 1992.

[22] A. K. Lenstra, H. W. Lenstra and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen* **261** (1982) 515–534.

[23] B. Mans. Optimal Distributed algorithms in unlabeled tori and chordal rings. *Journal on Parallel and Distributed Computing* **46** (1997) 80–90.

[24] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. To appear in proceedings of FOCS 1998. Available as TR98-016 from *Electronic Colloquium on Computational Complexity* at `http://www.uni-trier.de/eccc/`.

[25] C. P. Schnorr. A hierarchy of polynomial time basis reduction algorithms. *Theoretical Computer Science* **53** (1987) 201–224.

[26] P. van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in lattices. *Technical Report 81-04*, Mathematics Department, University of Amsterdam, 1981.

[27] J. Žervonik and T. Pisanski. Computing the diameter in multi-loop networks. *J. of Algorithms* **14** (1993) 226–243.

A Proof of Theorem 5

Given X and C in X3C, we construct in polynomial time an instance $\varphi(X, C)$ for SPDP such that X has an exact cover $C' \subseteq C$ if and only if $\varphi(X, C)$ is a positive instance for SPDP.

Let $\ell = \text{length}(q) + 1 = \lceil \log_2(q+1) \rceil + 1$, one more than the binary length of the integer q. Then $q \leq 2^{\ell-1} - 1$. Let B be the set of all binary strings of length $(3q+1) \cdot \ell + 1$. Each $x \in B$ is considered as a binary number with $3q+1$ blocks of bit sequences of length ℓ, plus one more leading (most significant) bit. $\forall i, 1 \leq i \leq 3q$, let $a_i = 2^{(i-1)\ell}$, a binary number with exactly one 1 in the i th block, i counting from the right. Let $M = 2^{3q\ell}$. For each $\tau \in C$, let $s_\tau = M + \sum_{i \in \tau} a_i$. s_τ is M plus a binary number with exactly one 1 in each of the three locations corresponding to the three elements of τ. Let $w = qM + \sum_{i=1}^{3q} a_i$. Finally let $n = 2^{(3q+1)\ell}$ and let $b = q$. This completes the definition of $\varphi(X, C)$.

If there is an exact cover $C' \subseteq C$ of X, then $|C'| = q$, and $\forall i, 1 \leq i \leq 3q, \sum_{\tau \in C'} \chi_\tau(i) = 1$. Let

$$x_\tau = \begin{cases} 1 & \text{if } \tau \in C' \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{\tau \in C} s_\tau x_\tau = qM + \sum_{\tau \in C'} \sum_{i \in \tau} a_i = qM + \sum_{i=1}^{3q} \left(\sum_{\tau \in C'} \chi_\tau(i) \right) a_i = qM + \sum_{i=1}^{3q} a_i = w.$$

In particular, $\sum_{\tau \in C} s_\tau x_\tau \equiv w \pmod{n}$ and $|\mathbf{x}|_{L_1} = q$. Hence $\varphi(X, C)$ is a positive instance for SPDP.

Suppose now $\sum_{\tau \in C} s_\tau x_\tau \equiv w \pmod{n}$ for some $\mathbf{x} = (x_\tau)_{\tau \in C}$ with $|\mathbf{x}|_{L_1} \leq q$. Suppose first $\sum_{\tau \in C} s_\tau x_\tau = w + kn$ for some integer $k \neq 0$. Then

$$\left| \sum_{\tau \in C} s_\tau x_\tau \right| \leq |\mathbf{x}|_{L_1} \cdot \max_{\tau \in C} \{s_\tau\} \leq q\overline{s},$$

where we denote by $\overline{s} = M + \sum_{i=1}^{3q} a_i$, an upper bound for all s_τ. Meanwhile $|w + kn| \geq n - w$ if $k \neq 0$. Thus

$$n \leq w + q\overline{s} = 2qM + (q+1) \sum_{i=1}^{3q} a_i < (2q+1)M < n,$$

since $q + 1 \leq 2^{\ell-1}$ and $2q + 1 < 2^\ell$. This is a contradiction. Thus $k = 0$ and

$$\sum_{\tau \in C} s_\tau x_\tau = w.$$

We wish to show next that among the x_τ's exactly q of them are 1 and the rest are all 0.

Consider $w = \sum_{\tau \in C} s_\tau x_\tau = \left(\sum_{\tau \in C} x_\tau \right) M + \sum_{\tau \in C} (s_\tau - M) x_\tau$. Let $r = \sum_{\tau \in C} x_\tau$. We claim $r = q$. Otherwise,

$$(r - q)M = \sum_{i=1}^{3q} a_i - \left(\sum_{\tau \in C} (s_\tau - M) x_\tau \right).$$

Thus

$$M \leq |(r-q)M| \leq \sum_{i=1}^{3q} a_i + q \max_{\tau \in C} \{s_\tau - M\} \leq (q+1) \sum_{i=1}^{3q} a_i < M.$$

Again a contradiction.

Thus $\sum_{\tau \in C} x_\tau = q$. But $|\mathbf{x}|_{L_1} = \sum_{\tau \in C} |x_\tau| \leq q$, hence, all $x_\tau \geq 0$.

Let $s'_\tau = s_\tau - M = \sum_{i\in\tau} a_i$, and let $w' = w - qM = \sum_{i=1}^{3q} a_i$. Then

$$\sum_{\tau\in C} s'_\tau x_\tau = w',$$

where $x_\tau \geq 0$ and $\sum_{\tau\in C} x_\tau = q$.

In the binary representation of $\sum_{\tau\in C} s'_\tau x_\tau$, each $a_i = 2^{(i-1)\ell}$ has a coefficient exactly equal to the number of times $i \in \tau$, each counting x_τ times. There can be no carries, since $x_\tau \geq 0$ and $\sum_{\tau\in C} x_\tau \leq q$.

More precisely, consider any i, $1 \leq i \leq 3q$. Let

$$\tau^* = \tau - \{1, 2, \ldots, i-1\},$$

and let

$$s^*_\tau = \sum_{j\in\tau^*} a_j.$$

Then

$$w' = \sum_{\tau\in C} s'_\tau x_\tau = \sum_{\tau\in C} s^*_\tau x_\tau + \sum_{\tau\in C} (s'_\tau - s^*_\tau) x_\tau. \tag{5}$$

We note that $0 \leq s'_\tau - s^*_\tau \leq \sum_{j=1}^{i-1} a_j$. Thus

$$0 \leq \sum_{\tau\in C} (s'_\tau - s^*_\tau) x_\tau \leq |\mathbf{x}|_{L_1} \sum_{j=1}^{i-1} a_j \leq q \sum_{j=1}^{i-1} a_j < a_i = 2^{(i-1)\ell}.$$

Hence by (5)

$$\left\lfloor \frac{w'}{2^{(i-1)\ell}} \right\rfloor = \sum_{\tau\in C} \left(\frac{s^*_\tau}{2^{(i-1)\ell}} \right) x_\tau,$$

where term by term $\frac{s^*_\tau}{2^{(i-1)\ell}}$ is an integer. Meanwhile by definition

$$\left\lfloor \frac{w'}{2^{(i-1)\ell}} \right\rfloor = \sum_{j=0}^{3q-i} 2^{j\ell}.$$

Taking the last two right hand sides modulo 2^ℓ, we have

$$\sum_{\tau\in C} \left(\frac{s^*_\tau}{2^{(i-1)\ell}} \right) x_\tau \equiv 1 \pmod{2^\ell}.$$

Note that

$$\frac{s^*_\tau}{2^{(i-1)\ell}} \equiv \begin{cases} 1 \pmod{2^\ell} & \text{if } i \in \tau \\ 0 \pmod{2^\ell} & \text{if } i \notin \tau. \end{cases}$$

So we get

$$\sum_{\tau:\ i\in\tau} x_\tau \equiv 1 \pmod{2^\ell}.$$

But $0 \leq \sum_\tau x_\tau \leq q < 2^\ell$, so

$$\sum_{\tau:\ i\in\tau} x_\tau = 1.$$

Finally, since all $x_\tau \geq 0$, exactly one $x_\tau = 1$, and all other $x_\tau = 0$, among all τ containing i. This is true for all i, $1 \leq i \leq 3q$. Thus overall, among all x_τ's, exactly q of them are 1, the rest are 0, and

$$\{\tau \in C : x_\tau = 1\}$$

forms an exact cover of X.

B Proof of Equation (4)

This can be seen as follows. For $i = 1, \ldots l$,

$$s_i = 2^{j'k} s'_i + r_i,$$

where $r_i = \sum_{d=1}^{j'} X_{di} 2^{(d-1)k}$. Therefore,

$$\begin{aligned} \sum_{i=1}^{l} s_i x_i &= \sum_{i=1}^{l} \left[2^{j'k} s'_i + \sum_{d=1}^{j'} X_{di} 2^{(d-1)k} \right] x_i \\ &= \sum_{i=1}^{l} 2^{j'k} s'_i x_i + \sum_{d=1}^{j'} 2^{(d-1)k} \sum_{i=1}^{l} X_{di} x_i. \end{aligned}$$

By the inductive hypothesis, for $d = 1, \ldots, j'$,

$$\sum_{i=1}^{l} X_{di} x_i = -q x_{l+d}.$$

Thus,

$$\sum_{i=1}^{l} s_i x_i = \sum_{i=1}^{l} 2^{j'k} s'_i x_i - \sum_{d=1}^{j'} 2^{(d-1)k} q x_{l+d}. \tag{6}$$

For $i = l+1, \ldots, l+j'$, $s_i = 2^{(i-l-1)k} q$, for $i = l+j'+1, \ldots, l+r$, $s_i = 2^{j'k} s'_i$, and for $i = l+1, \ldots, l+j'$, $s'_i = 0$. Thus,

$$\begin{aligned} \sum_{i=l+1}^{l+r} s_i x_i &= \sum_{i=l+1}^{l+j'} s_i x_i + \sum_{i=l+j'+1}^{l+r} s_i x_i \\ &= \sum_{d=1}^{j'} 2^{(d-1)k} q x_{l+d} + \sum_{i=l+1}^{l+r} 2^{j'k} s'_i x_i. \end{aligned} \tag{7}$$

From equations (6) and (7), we get

$$0 = \sum_{i=1}^{l+r} s_i x_i = 2^{j'k} \sum_{i=1}^{l+r} s'_i x_i,$$

thus proving (4).

C Proof of NP-hardness of the SVP for the homogeneous case

In this section we denote by $\lambda_1(L)$ the L_1-norm length of a shortest non-zero vector in a lattice L. We also denote by $[b_1, \ldots, b_n]$ the matrix whose columns are the vectors b_i. Let L be an n-dimensional integral lattice in $\mathbb{R}^n$. Note that any n-dimensional lattice in some $\mathbb{R}^m$ given by $n^{O(1)}$ bits can be sufficiently approximated by an n-dimensional rational lattice in $\mathbb{R}^n$ whose basis can be described by $n^{O(1)}$ bits. By scaling, any rational lattice can be converted to an integral lattice. So there is no loss of generality in assuming L is integral.

Let L^* be the dual of L. Let $b_1, \ldots, b_n$ be a basis of L^*. In general, $b_i \in \mathbb{Q}^n$ even though L is integral. Let $B = [b_1, \ldots, b_n]^T$, the matrix with b_i^T as row vectors. Then, $L = L^{**} = \{z \in \mathbb{Z}^n \mid Bz \text{ is an integral vector}\}$. Let $b_{ij} = \frac{p_{ij}}{q_{ij}}$ and let k be the least common multiple of all the q_{ij}. Clearly, $b_{ij}k \in \mathbb{Z}$. Let $a_{ij} = b_{ij}k \pmod k$ and $A = (a_{ij})_{1 \le i,j \le n}$. By the definition of a dual lattice, for an integral $z \in \mathbb{Z}^n$, $z \in L \iff Bz$ is integral $\iff \forall i \sum_{j=1}^n b_{ij} z_j$ is an integer $\iff \forall i \sum_{j=1}^n a_{ij} z_j \equiv 0 \pmod k$. That is, $L = \{z \in \mathbb{Z}^n \mid Az \equiv 0 \bmod k\}$. The determinant of L is at most k^n. By Minkowski's First Theorem applied to the L_1-norm,

$$\lambda_1(L) \le \gamma n (\det L)^{1/n} \le \gamma n k,$$

where γ is a universal constant.

Let p be a prime bigger than $k^n(n!)$ and $\alpha = p\left(1 + \frac{n}{p}\right)\gamma n k$. Let $l = \lceil \log_2(pk\alpha) \rceil + 1$. Note that $l \le n^{O(1)}$. Let M be any integer $> 2^{nl}\alpha$. Let

$$s_i = \sum_{j=1}^n a_{ji} 2^{(j-1)l} \quad \text{for } i = 1, \ldots, n$$

and

$$s_i = 2^{(i-1-n)l} pk \quad \text{for } i = n+1, \ldots, 2n.$$

It is clear that $\forall i \ |s_i| \le 2^{nl}$. It is also obvious that all the quantities defined above have polynomial bit length. Let L' be the lattice $L' = \{x \in \mathbb{Z}^{2n} \mid \sum_{i=1}^{2n} s_i x_i \equiv 0 \pmod M\}$.

Lemma 10. *Given a non-zero vector $z \in L$, a non-zero vector $x \in L'$ can be computed so that $|x|_{L_1} \le p\left(1 + \frac{n}{p}\right)|z|_{L_1}$, and given a non-zero vector $x \in L'$, $|x|_{L_1} \le \alpha$, a non-zero vector $z \in L$ can be computed such that, $|z|_{L_1} \le \frac{|x|_{L_1}}{p}$. It follows that,*

$$p\lambda_1(L) \ \le \ \lambda_1(L') \ \le \ p\left(1 + \frac{n}{p}\right)\lambda_1(L).$$

Proof. Let $|z|_{L_1} = \beta$. By definition, $Az \equiv 0 \pmod k$. In other words, for $j = 1, \ldots, n$, $\exists d_j \in \mathbb{Z}$ such that $\sum_{i=1}^n a_{ji} z_i = d_j k$. Because $0 \le a_{ji} < k$, $|d_j| < |z|_{L_1} = \beta$. Let $y = pz$. This means that $Ay \equiv 0 \pmod{pk}$. Define $x = (y_1, \ldots, y_n, -d_1, \ldots, -d_n)$. We now show that $x \in L'$.

This is because

$$\begin{aligned}
\sum_{i=1}^n y_i s_i + \sum_{j=1}^n (-d_j) s_{n+j} &= \sum_{i=1}^n y_i \left(\sum_{j=1}^n a_{ji} 2^{(j-1)l}\right) + \sum_{j=1}^n (-d_j) pk 2^{(j-1)l} \\
&= \sum_{j=1}^n 2^{(j-1)l} \left(\sum_{i=1}^n y_i a_{ji} - d_j pk\right) \\
&= 0.
\end{aligned}$$

We get,

$$\begin{aligned} |x|_{L_1} &= |y|_{L_1} + \sum_{j=1}^{n} |d_j| \\ &\leq p\beta + n\beta \\ &= p\ (1 + \frac{n}{p})\ \beta. \end{aligned}$$

Because y is non-zero, x is a non-zero vector in L'. When z is the shortest non-zero vector in L, we get the following inequality,

$$\lambda_1(L') \leq |x|_{L_1} \leq p(1 + \frac{n}{p})\,|z|_{L_1} = p(1 + \frac{n}{p})\lambda_1(L). \tag{8}$$

Now for the second part of the lemma. By Minkowski's First Theorem, $\lambda_1(L) \leq \gamma nk$. Therefore, by what was proved above, $\lambda_1(L') \leq p\ (1 + \frac{n}{p})\ \gamma nk = \alpha$, which means our assumption in the second part $|x|_{L_1} \leq \alpha$ is not vacuous.

We have, $\sum_{i=1}^{2n} s_i x_i \equiv 0 \pmod{M}$, and because $\left|\sum_{i=1}^{2n} s_i x_i\right| \leq 2^{nl}\alpha < M$, $\sum_{i=1}^{2n} s_i x_i = 0$. We will now show that

$$A\hat{x} \equiv 0 \pmod{pk}, \tag{9}$$

where $\hat{x} = (x_1, \ldots, x_n)^T$, the first n components of x.

We prove by induction on j, $j = 1, \ldots, n$, that $\sum_{i=1}^{n} a_{ji}x_i + pkx_{n+j} = 0$. This proves that $\sum_{i=1}^{n} a_{ji}x_i \equiv 0 \pmod{pk}$. First the base case. We can rewrite $\sum_{i=1}^{2n} s_i x_i = 0$ as

$$\sum_{i=1}^{n} s_i x_i + \sum_{i=n+1}^{2n} s_i x_i = 0. \tag{10}$$

We know that $s_i \equiv a_{1i} \pmod{2^l}$ for $i = 1, \ldots, n$, $s_{n+1} \equiv pk \pmod{2^l}$, and for all other i, $s_i \equiv 0 \pmod{2^l}$. Writing the above equation mod 2^l gives us

$$\sum_{i=1}^{n} a_{1i}x_i + pkx_{n+1} \equiv 0 \pmod{2^l}.$$

Since $0 \leq a_{1i} < k$ and $|x|_{L_1} \leq \alpha$, the above sum is at most $pk\alpha$ in absolute value. By definition, $pk\alpha < 2^l$. Therefore, $\sum_{i=1}^{n} a_{1i}x_i + pkx_{n+1} = 0$.

Let $1 \leq j' < n$ and assume that $\sum_{i=1}^{n} a_{ji}x_i + pkx_{n+j} = 0$ for $j = 1, 2, \ldots, j'$. We show that $\sum_{i=1}^{n} a_{ji}x_i + pkx_{n+j} = 0$ for $j = j' + 1$. Let s'_i be the quotient obtained by dividing s_i by $2^{j'l}$. In other words, s'_i is the number got by removing the $j'l$ least significant bits of s_i. We claim that

$$\sum_{i=1}^{2n} s'_i x_i = 0. \tag{11}$$

This can be seen as follows. For $i = 1, \ldots n$,

$$s_i = 2^{j'l}s'_i + r_i,$$

where $r_i = \sum_{d=1}^{j'} a_{di} 2^{(d-1)l}$. Therefore,

$$\begin{aligned}\sum_{i=1}^{n} s_i x_i &= \sum_{i=1}^{n} \left[2^{j'l} s'_i + \sum_{d=1}^{j'} a_{di} 2^{(d-1)l} \right] x_i \\ &= \sum_{i=1}^{n} 2^{j'l} s'_i x_i + \sum_{d=1}^{j'} 2^{(d-1)l} \sum_{i=1}^{n} a_{di} x_i.\end{aligned}$$

By the inductive hypothesis, for $d = 1, \ldots, j'$,

$$\sum_{i=1}^{n} a_{di} x_i = -pkx_{n+d}.$$

Thus,

$$\sum_{i=1}^{n} s_i x_i = \sum_{i=1}^{n} 2^{j'l} s'_i x_i - \sum_{d=1}^{j'} 2^{(d-1)l} pkx_{n+d}. \tag{12}$$

For $i = n+1, \ldots, n+j'$, $s_i = 2^{(i-n-1)l} pk$, for $i = n+j'+1, \ldots, 2n$, $s_i = 2^{j'l} s'_i$, and for $i = n+1, \ldots, n+j'$, $s'_i = 0$. Thus,

$$\begin{aligned}\sum_{i=n+1}^{2n} s_i x_i &= \sum_{i=n+1}^{n+j'} s_i x_i + \sum_{i=n+j'+1}^{2n} s_i x_i \\ &= \sum_{d=1}^{j'} 2^{(d-1)l} pkx_{n+d} + \sum_{i=n+1}^{2n} 2^{j'l} s'_i x_i. \end{aligned} \tag{13}$$

From equations (10), (12) and (13), we get

$$0 = \sum_{i=1}^{2n} s_i x_i = 2^{j'l} \sum_{i=1}^{2n} s'_i x_i,$$

thus proving (11).

Clearly, for $i = 1, \ldots, n$, $s'_i \equiv a_{j'+1,i} \pmod{2^l}$, $s'_{n+j'+1} \equiv pk \pmod{2^l}$, and for all other i, $s'_i \equiv 0 \pmod{2^l}$. Therefore, taking (11) modulo 2^l, we see that $\sum_{i=1}^{n} a_{j'+1,i}\, x_i + pkx_{n+j'+1} = 0$. This completes the induction. Therefore, for $j = 1, \ldots, n$, $\sum_{i=1}^{n} a_{ji} x_i + pkx_{n+j} = 0$, and so $\sum_{i=1}^{n} a_{ji} x_i \equiv 0 \pmod{pk}$. This proves (9).

Let $A\hat{x} = (pm_1, \ldots, pm_n)^T$, where $m_i \in k\mathbb{Z}$. Then, $(\det A)\, x \equiv 0 \pmod{p}$. Since, $p > k^n(n!) \geq |\det A|$, p is relatively prime to $|\det A|$ and so $p \mid x_i$, for $i = 1, \ldots, n$. Let $z = (z_1, \ldots, z_n)$ where $z_i = \frac{1}{p} x_i$. Then $Az \equiv 0 \pmod{k}$. Also, since x is non-zero, not all $x_1, \ldots, x_n$ are zero, by the definition of L'. Therefore, z is a non-zero vector in L. Clearly, $|z|_{L_1} \leq \frac{1}{p} |x|_{L_1}$. We get the following inequality when x is the shortest non-zero vector in L',

$$\lambda_1(L) \leq |z|_{L_1} \leq \frac{1}{p} |x|_{L_1} = \frac{1}{p} \lambda_1(L'). \tag{14}$$

From (8) and (14) we establish,

$$p\lambda_1(L) \ \leq \lambda_1(L') \ \leq p \left(1 + \frac{n}{p}\right) \lambda_1(L).$$

□

Theorem 6. *The SVP for the class of (homogeneous) lattices defined by circulant graphs is NP-hard under randomized reductions. Moreover, it remains NP-hard to find an approximate shortest vector in this class of lattices within a factor of* $\sqrt{2} - \epsilon$*, for any constant* $\epsilon > 0$*.*

Proof. From the second part of Lemma 10, if x is the shortest vector in L', then the computed z satisfies $\lambda_1(L) \leq |z| \leq \left(1 + \frac{n}{p}\right) \lambda_1(L)$. It is known that it is NP-hard, under randomized reductions, to approximate the SVP for a general (homogeneous) lattice within a factor of $\sqrt{2} - \epsilon$ for the L_1-norm [24]. Hence, the NP-hardness, under randomized reductions, of the SVP for the homogeneous case follows. It also follows that for any constant $\epsilon > 0$, it remains NP-hard to approximate within a factor of $\sqrt{2} - \epsilon$.