Algorithmica (2014) 70:301–325
DOI 10.1007/s00453-013-9810-3

# Random Walks, Bisections and Gossiping in Circulant Graphs

**Bernard Mans · Igor Shparlinski**

Received: 27 August 2012 / Accepted: 27 June 2013 / Published online: 11 July 2013


**Abstract** Circulant graphs are regular graphs based on Cayley graphs defined on the Abelian group $\mathbb{Z}_n$. They are popular network topologies that arise in distributed computing.

Using number theoretical tools, we first prove two main results for *random directed* $k$-regular circulant graphs with $n$ vertices, when $n$ is sufficiently large and $k$ is fixed. First, for any fixed $\varepsilon > 0$, $n = p$ prime and $L \geq p^{1/k}(\log p)^{1+1/k+\varepsilon}$, walks of length at most $L$ terminate at every vertex with asymptotically the same probability. Second, for any $n$, there is a polynomial time algorithm that for almost all undirected $2r$-regular circulant graphs finds a vertex bisector and an edge bisector, both of size less than $n^{1-1/r+o(1)}$. We then prove that the latter result also holds for all (rather than for almost all) $2r$-regular circulant graphs with $n = p$, prime, vertices, while, in general, it does not hold for composite $n$.

Using the bisection results, we provide lower bounds on the number of rounds required by any gossiping algorithms for any $n$. We introduce generic distributed algorithms to solve the gossip problem in any circulant graphs. We illustrate the efficiency of these algorithms by giving nearly matching upper bounds of the number of rounds required by these algorithms in the vertex-disjoint and the edge-disjoint paths communication models in particular circulant graphs.

**Keywords** Bisection · Circulant graphs · Gossiping · Random walks · Random graphs

B. Mans · I. Shparlinski (✉)
Department of Computing, Macquarie University, Sydney, Australia
e-mail: igor.shparlinski@mq.edu.au

B. Mans
e-mail: bernard.mans@mq.edu.au

## 1 Introduction and Main Results

### 1.1 Outline

In this section, we first introduce some basic definitions and notations, before providing the necessary definitions and our respective results for random walks, bisections and gossiping. In Sect. 2, we introduce the necessary number theoretic tools and methodologies using the theory of uniform distribution, linear congruences, equivalent sets and the shortest vector problem. We then provide the proofs of our main results on random walks and bisections in Sect. 3. Using our bisection results, we introduce lower bounds on the number of necessary rounds for gossiping in Sect. 4. We also present generic gossiping algorithms for any circulant graphs. We illustrate the efficiency of these algorithms by giving nearly matching upper bounds of the number of rounds required by these algorithms in particular circulant graphs. Finally, in Sect. 5, we provide the proofs on our lower bounds on the number of necessary rounds for gossiping. Concluding remarks are provided in Sect. 6.

We note that most of the results here are based on the arguments and ideas outlined in [23, 24].

### 1.2 Basic Definitions and Notations

For an integer $n \geq 2$ we use $\mathbb{Z}_n$ to denote the residue ring modulo $n$ that we assume to be represented by the set $\{0, 1, \ldots, n-1\}$. Let $\widetilde{\mathbb{Z}}_n$ be the set of non-zero elements of $\mathbb{Z}_n$. Thus, for a prime $n = p$ we have $\widetilde{\mathbb{Z}}_p = \mathbb{Z}_p^*$, the set of invertible elements in $\mathbb{Z}_p$.

A *circulant graph* is a directed $n$-vertex graph with an automorphism that is an $n$-cycle. Circulant graphs may be constructed as follows. Given a set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ we define the graph $\mathcal{C}_n(\mathcal{A})$ to be the directed graph with the vertex set $\mathbb{Z}_n$ where for $i, j \in \mathbb{Z}_n$ there is an edge from $i$ to $j$ if and only if $i - j \in \mathcal{A}$. It is not difficult to see that $\mathcal{C}_n(\mathcal{A})$ is an $n$-vertex directed circulant graph of regularity $\#\mathcal{A}$ (that is, both in-degree and out-degree are equal to $\#\mathcal{A}$)

We say that $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ is *symmetric* if $a \in \mathcal{A}$ if and only if $n - a \in \mathcal{A}$. Then $\mathcal{C}_n(\mathcal{A})$ is an undirected $k$-regular circulant graph, where $k = \#\mathcal{A}$. Clearly every symmetric set $\mathcal{A}$ of cardinality $k$ can be represented as

$$\mathcal{A} = \mathcal{S} \cup (n - \mathcal{S}) = \{s_1, n - s_1, \ldots, s_r, n - s_r\} \tag{1}$$

for some set $\mathcal{S} = \{s_1, \ldots, s_r\} \subseteq \widetilde{\mathbb{Z}}_n$, with $r = \lceil k/2 \rceil$ (for an odd $k$ we must have $n/2 \in \mathcal{S}$ and thus $n$ has to be even). We call $\mathcal{S}$ a *representative edge set* of $\mathcal{A}$. We also sometimes write a set $\mathcal{A}$ of the form (1) as

$$\mathcal{A} = \{\pm s_1, \ldots, \pm s_r\}.$$

Circulant graphs are special cases of so-called Abelian Cayley graphs and have been extensively studied in the literature (and we provide references when relevant).

For an integer $a$, we use $\|a\|_n$ to denote its minimal in absolute value residue modulo $n$, that is,

$$\|a\|_n = \min_{m \in \mathbb{Z}} |a - mn|.$$

Throughout the paper, the implied constants in the symbols '$O$', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on $k$, $r$ and $\varepsilon$. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \le c|V|$ holds for some constant $c > 0$.

### 1.3 Diameters and Random Walks

For a set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ we denote by $D_n(\mathcal{A})$ the *diameter* of the graph $\mathcal{C}_n(\mathcal{A})$, that is, the smallest $D$ such that any pair of vertices of the graph are connected by a walk of length at most $D$.

Improving some upper and lower bounds on $D_n(\mathcal{A})$ from [10], and answering an open question of Amir and Gurel-Gurevich [3], Marklof and Strombergsson [26] have given an explicit formula for the distribution function of the diameter $D_n(\mathcal{A})$ for a random set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ of a fixed cardinality $k$. In fact, the results of [26] are more general and apply to weighted circulant graphs and also to undirected circulant graphs. In particular, it is easy to see from the results of [26] that for any fixed real $\varepsilon > 0$ and an integer $k$, for almost all $n$ and almost all sets $\mathcal{A} = \{a_1, \ldots, a_k\} \subseteq \widetilde{\mathbb{Z}}_n$ of cardinality $\#\mathcal{A} = k$ and such that $\gcd(a_1, \ldots, a_k, n) = 1$, we have

$$D_n(\mathcal{A}) \le n^{1/k+\varepsilon}. \tag{2}$$

One of the possible interpretations of the estimate (2) is that for any $h \in \mathbb{Z}_n$ there is a walk from the vertex 0 to the vertex $h$ of length $L \le n^{1/k+\varepsilon}$. Let $N_n(\mathcal{A}, L; h)$ be the number of solutions to the congruence

$$m_1 a_1 + \cdots + m_k a_k \equiv h \pmod{n}, \tag{3}$$

where

$$m_1, \ldots, m_k \ge 0, \qquad m_1 + \cdots + m_k \le L. \tag{4}$$

One can easily see that if $\mathcal{A} = \{a_1, \ldots, a_k\}$ then $D_n(\mathcal{A})$ is the smallest value of $L$ such that for any $h \in \mathbb{Z}_m$ we have $N_n(\mathcal{A}, L; h) > 0$.

Here we show that for a prime $n = p$, the quantity $N_n(\mathcal{A}, L; h)$ is close to its expected value for every $h \in \mathbb{Z}_p$ starting with $L \sim p^{1/k+\varepsilon}$.

**Theorem 1** *For a prime $p$, a fixed integer $k \ge 1$ and a real $\varepsilon > 0$, for all integer $L \ge p^{1/k}(\log p)^{1/k+\varepsilon}$ and $h \in \mathbb{Z}_p$, the asymptotic formula*

$$N_p(\mathcal{A}, L; h) = \frac{1 + o(1)}{p} \binom{L+1}{k}$$

*holds for all sets $\mathcal{A} \subseteq \mathbb{Z}_p^*$ of cardinality $\#\mathcal{A} = k$ with $o(p^k)$ exceptions as $p \to \infty$.*

Clearly every solution to (3) defines a walk on $\mathcal{C}_n(\mathcal{A})$. Since the sequence of steps is not important, we say that the walk is *ordered* if it first makes $m_1$ jumps of length $a_1$, then $m_2$ jumps of length $a_2$ and so on, until at the end it makes $m_k$ jumps of length $a_k$.

We see that Theorem 1 implies that, for $L_0 = \lceil p^{1/k}(\log p)^{1/k+\varepsilon} \rceil$, for almost all circulant graphs $\mathcal{C}_p(\mathcal{A})$, a random ordered walk of length at most $L_0$ terminates at every vertex of $\mathcal{C}_p(\mathcal{A})$ with asymptotically the same frequency.

### 1.4 Bisections

For any *undirected* graph $G = (V(G), E(G))$, a *vertex bisector* of $G$ is a set of vertices $\mathcal{U}_v \subseteq V(G)$ such that the removal of the set of vertices $\mathcal{U}_v$ and their incident edges splits $G$ into two parts $G_1$ and $G_2$ of almost the same size, that is, for their vertex sets $V(G_1)$, $V(G_2)$ we have

$$\big|\#V(G_1) - \#V(G_2)\big| \le 1. \tag{5}$$

The graphs $G_1$ and $G_2$ are called the two *halves* of the bisection. The *vertex bisection width* $\mathrm{vw}(G)$ of $G$ is defined as:

$$\mathrm{vw}(G) = \min\{\#\mathcal{U} : \mathcal{U} \text{ is a vertex bisector of } G\}.$$

Similarly, the *edge bisection width* $\mathrm{ew}(G)$ of $G$ is the minimum size of the set of edges $\mathcal{F}_e \subseteq E(G)$, whose deletion yields two components $G_1$ and $G_2$ such that (5) holds.

The problems are not equivalent: the complete graph on $n$ vertices has no vertex bisector, whilst it has an edge bisection set of size $\lceil (n^2 - 1)/4 \rceil$. Both problems are **NP**-complete, but lower and upper bounds are known for most of the regular topologies of networks (see, for example, [20]).

We consider edge and vertex bisection widths of random circulant graphs (that is, graphs $\mathcal{C}_n(\mathcal{A})$ with the generating set $\mathcal{A}$ chosen uniformly at random among all subsets of $\widetilde{\mathbb{Z}}_n$ of given cardinality). We also note that in [12] a similar problem has been studied for directed $r$-regular Cayley graph constructed on an Abelian group. Here we give a constructive proof, that leads to a polynomial time algorithm of constructing small edge and vertex bisections, which satisfy the bounds similar to Theorem 2 (below).

**Theorem 2** *For an arbitrary integer $n \ge 2$, a fixed integer $r \ge 1$, a real $\varepsilon > 0$, and for all but $o(n^r)$ symmetric sets $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ of the form (1), one can find in time $n^{1-1/r+o(1)}$ a vertex bisector $\mathcal{U}_v \subseteq V(\mathcal{C}_n(\mathcal{A}))$ and an edge bisector $\mathcal{F}_e \subseteq E(\mathcal{C}_n(\mathcal{A}))$ of $\mathcal{C}_n(\mathcal{A})$ with*

$$\#\mathcal{U}_v \le n^{1-1/r+o(1)} \quad \text{and} \quad \#\mathcal{F}_e \le n^{1-1/r+o(1)},$$

*as $n \to \infty$.*

We also consider edge and vertex bisection widths of circulant graphs which satisfy the bounds similar to Theorem 2, for all circulant graphs over $\mathbb{Z}_p$ with $p$ prime.

**Theorem 3** *For a prime $p$, a fixed integer $r \ge 1$, and for all symmetric sets $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_p$ of the form (1), one can find in time $n^{1-1/r+o(1)}$ a vertex bisector $\mathcal{U}_v \subseteq V(\mathcal{C}_p(\mathcal{A}))$ and an edge bisector $\mathcal{F}_e \subseteq E(\mathcal{C}_p(\mathcal{A}))$ of $\mathcal{C}_p(\mathcal{A})$ with*

$$\#\mathcal{U}_v = O\big(p^{1-1/r}\big) \quad \text{and} \quad \#\mathcal{F}_e = O\big(p^{1-1/r}\big).$$

In [23] the following more explicit but non-constructive estimates

$$\mathrm{vw}\big(\mathcal{C}_p(\mathcal{A})\big) \le 4p^{1-\frac{1}{r}} \quad \text{and} \quad \mathrm{ew}\big(\mathcal{C}_p(\mathcal{A})\big) \le \big(r^{\log r + C\log\log r} r!\big)^{1/r} p^{1-1/r} \tag{6}$$

have been shown to hold uniformly for $r = o(\log p)$ (with some absolute constant $C$).

*Remark 4* The first estimate in (6) gives an improvement by the factor $2er^{-1}\log(n/2)$ compared to the previously best known bound for Abelian Cayley graphs, see [12]. It is also easy to see that if $r = o(\log p)$ then $\mathrm{vw}(\mathcal{C}_p(\mathcal{A})) \le (2+o(1))p^{1-\frac{1}{r}}$, as $p \to \infty$.

*Remark 5* By using the known inequality $r! < r^{r+1}e^{-r}$ which holds for all integers $r \ge 7$ the second estimate in (6) gives that, provided that $r$ is large enough, we have $\mathrm{ew}(\mathcal{C}_p(\mathcal{A})) \le 0.4rp^{1-1/r}$.

*Remark 6* If $r \to \infty$ such that $r = o(\log p)$ then the second estimate in (6) becomes of the form $\mathrm{ew}(\mathcal{C}_p(\mathcal{A})) \le (r/e + o(1))p^{1-1/r}$, as $p \to \infty$.

We also show that the statement of Theorem 3 fails for composite $n$ in general, in the sense that there are generating sets for which the stated bounds on the bisectors do not hold.

### 1.5 Gossiping

Circulant graphs are popular network topologies that arise in distributed computing. Due to an uncoordinated literature, numerous terms to name similar network topologies are commonly used (for example, *distributed loop networks* [8] or *chordal rings* [5, 22]). They are used in point-to-point as well as in advanced networks (such as optical networks [28, 30]). However, unlike other highly regular network topologies, computing the shortest paths and routing is NP-hard in general (see [10]).

Our results above have an immediate impact on the effectiveness of gossiping algorithms when circulant graphs are used as network topologies. For the problem of gossiping, each node has a piece of information and wants to communicate this information to all the other nodes (such that all nodes learn the cumulative message), that is an all-to-all dissemination problem. A communication algorithm consists of a number of communication *rounds* during which nodes are involved in communications.

The communication algorithm necessary to solve these problems depends on the communication model. Several communication modes exist. The *vertex-disjoint paths mode* (VDP) assumes:

(i) a communication involves exactly two nodes which can be at distance more than 1,
(ii) any two paths corresponding to simultaneous communications must be vertex-disjoint.

Similarly, the *line mode* or *edge-disjoint paths mode* (EDP) assumes:

(i) a communication involves exactly two nodes which can be at distance more than 1,
(ii) any two paths corresponding to simultaneous communications must be edge-disjoint.

The mode of communication also depends on the type of communication links available: (a) *half-duplex* (or *1-way*) or (b) *full-duplex mode* (or *2-way*).

In the 2-VDP mode (respectively, 2-EDP), two nodes involved in a 2-way VDP communication (respectively, EDP communication) can exchange their information.

In the 1-VDP mode (respectively, 1-EDP), the information flows in the 1-way direction from one node to the other. More information about gossiping is given in Sect. 5.1.

Given a graph $G$ and a gossiping algorithm $\mathfrak{G}$, let $g_{\mathfrak{G}}(G)$ denote the number of rounds of this algorithm for $G$.

There are known explicit lower bounds for the number of rounds of gossip algorithms in terms of bisection widths, see [16, 18], which are reproduced in Lemmas 20 and 21 below. By inserting our bounds on the bisection width into these lower bounds we obtain the following results.

**Theorem 7** *For an arbitrary integer $n \geq 2$, a fixed integer $r \geq 1$, for all but $o(n^r)$ symmetric sets $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ of the form (1), in both the 2-EDP mode and the 2-VDP mode, for any gossip algorithm $\mathfrak{G}$, we have*

$$g_{\mathfrak{G}}\big(\mathcal{C}_n(\mathcal{A})\big) \geq \left(1 + \frac{1}{r} + o(1)\right) \log n,$$

*as $n \to \infty$.*

For prime $n = p$ we have "individual" bounds:

**Theorem 8** *Let $n = p$ be prime. For a fixed integer $r \geq 1$, and any symmetric set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_p$ of the form (1):*

- *In the 2-EDP mode, for any gossip algorithm $\mathfrak{G}$, we have*

$$g_{\mathfrak{G}}\big(\mathcal{C}_p(\mathcal{A})\big) \geq \left(1 + \frac{1}{r} + o(1)\right) \log p,$$

  *as $p \to \infty$, provided that $r = o(\log p)$.*
- *In the 2-VDP mode, For any gossip algorithm $\mathfrak{G}$ we have*

$$g_{\mathfrak{G}}\big(\mathcal{C}_p(\mathcal{A})\big) \geq \left(1 + \frac{1}{r}\right) \log p - \log\log p - 8.$$

Let

$$\vartheta = \big(\log\big(1 + 5^{1/2}\big) - 1\big)^{-1} = 1.440\ldots.$$

With the 1-VDP mode, we consider "well-structured" gossip algorithms (as originally defined in [14] and explained in Sect. 4.2). We have

**Theorem 9** *For an arbitrary integer $n \geq 2$, a fixed integer $r \geq 1$, for all but $o(n^r)$ symmetric sets $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ of the form (1), and for any "well-structured" gossip algorithm $\mathfrak{G}$ in the 1-VDP mode, we have*

$$g_{\mathfrak{G}}\big(\mathcal{C}_n(\mathcal{A})\big) \geq \left(\vartheta + \frac{2-\vartheta}{r} + o(1)\right) \log n,$$

*as $n \to \infty$.*

Finally, we also have the following completely explicit bound:

**Theorem 10** *Let $n = p$ be prime. For a fixed integer $r \geq 1$, and any symmetric set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_p$ of the form (1) and for any "well-structured" gossip algorithm $\mathfrak{G}$ in the 1-VDP mode, we have*

$$g_{\mathfrak{G}}\big(\mathcal{C}_p(\mathcal{A})\big) \geq \left(\vartheta + \frac{2-\vartheta}{r}\right) \log p - (2-\vartheta) \log\log p - 17.$$

It is worth noting that by exploiting the knowledge of the bisection width of the network topology combined with the generic algorithms presented in Sect. 4, one can obtain near-optimal performance for gossiping for some circulant graphs. Similarly algorithms can be obtained in the 1-VDP mode for any "well-structured" gossiping algorithm, and are also presented in Sect. 4.

## 2 Preparations and Methodology

### 2.1 Tools from the Theory of Uniform Distribution

For a finite set $\mathcal{F} \subseteq [0,1]^k$ of the $k$-dimensional unit cube, we define its *discrepancy with respect to a domain* $\Xi \subseteq [0,1]^k$ as

$$\Gamma(\mathcal{F}, \Xi) = \left| \frac{\#\{\mathbf{f} \in \mathcal{F} \cap \Xi\}}{\#\mathcal{F}} - \lambda(\Xi) \right|,$$

where $\lambda$ is the Lebesgue measure on $[0,1]^k$.

We now define the *discrepancy* of $\mathcal{F}$ as

$$\Delta(\mathcal{F}) = \sup_{\Pi \subseteq [0,1]^k} \Gamma(\mathcal{F}, \Pi),$$

where the supremum is taken over all boxes $\Pi = [0, \alpha_1] \times \cdots \times [0, \alpha_k]$ with $0 \leq \alpha_1, \ldots, \alpha_k < 1$.

As usual, we define the distance between a vector $\mathbf{u} \in [0,1]^k$ and a set $\Xi \subseteq [0,1]^k$ by

$$\operatorname{dist}(\mathbf{u}, \Xi) = \inf_{\mathbf{w} \in \Xi} \|\mathbf{u} - \mathbf{w}\|,$$

where $\|\mathbf{v}\|$ denotes the Euclidean norm of $\mathbf{v}$. Given $\varepsilon > 0$ and a domain $\Xi \subseteq [0,1]^k$, we define the sets

$$\Xi_\varepsilon^+ = \left\{\mathbf{u} \in [0,1]^k \setminus \Xi\colon \operatorname{dist}(\mathbf{u}, \Xi) < \varepsilon\right\}$$

and

$$\Xi_\varepsilon^- = \left\{\mathbf{u} \in \Xi\colon \operatorname{dist}\left(\mathbf{u}, [0,1]^k \setminus \Xi\right) < \varepsilon\right\}.$$

Let $h(\varepsilon)$ be an arbitrary increasing function defined for $\varepsilon > 0$ and such that $\lim_{\varepsilon \to 0} h(\varepsilon) = 0$. As in [19, 29], we define the class $\mathcal{S}_h$ of domains $\Xi \subseteq [0,1]^k$ for which $\lambda(\Xi_\varepsilon^+) \le h(\varepsilon)$ and $\lambda(\Xi_\varepsilon^-) \le h(\varepsilon)$.

A relation between $\Delta(\mathcal{F})$ and $\Gamma(\mathcal{F}, \Xi)$ for $\Xi \in \mathcal{S}_h$ is given by the following inequality of [19] (see also [29]).

**Lemma 11** *For any domain $\Xi \in \mathcal{S}_h$, we have*

$$\Gamma(\mathcal{F}, \Xi) \ll h\left(k^{1/2} \Delta(\mathcal{F})^{1/k}\right).$$

## 2.2 Distribution of Solutions of Linear Congruences

For positive integers $M_1, \dots, M_k$ we let $R_n(\mathcal{A}, M_1, \dots, M_k; h)$ be the number of solutions to the congruence (3) with $0 \le m_i \le M_i - 1$, $i = 1, \dots, k$.

We use exponential sums to estimate $R_n(\mathcal{A}, M_1, \dots, M_k; h)$.

Let $\mathbf{e}_n(z) = \exp(2\pi i z/n)$. We recall, that for any integers $z$ and $n \ge 1$, we have the orthogonality relation

$$\frac{1}{n} \sum_{-n/2 \le \lambda < n/2} \mathbf{e}_n(\lambda z) = \begin{cases} 1, & \text{if } z \equiv 0 \pmod n, \\ 0, & \text{if } z \not\equiv 0 \pmod n, \end{cases} \tag{7}$$

see [17, Sect. 3.1].

We now assume that $n = p$ is prime.

**Lemma 12** *For a prime $p$ we have*

$$\frac{1}{p^k} \sum_{\substack{\mathcal{A} \subseteq \mathbb{Z}_p^* \\ \#\mathcal{A} = k}} \max_{1 \le M_1, \dots, M_k \le p} \max_{h \in \mathbb{Z}_p} \left| R_p(\mathcal{A}, M_1, \dots, M_k; h) - \frac{M_1 \cdots M_k}{p} \right| \ll (\log p)^k.$$

*Proof* For a fixed set $\mathcal{A} = \{a_1, \dots, a_k\} \subseteq \mathbb{Z}_p^*$, using (7), we write

$$\begin{aligned} &R_p(\mathcal{A}, M_1, \dots, M_k; h) \\ &\quad = \sum_{m_1=0}^{M_1-1} \cdots \sum_{m_k=0}^{M_k-1} \frac{1}{p} \sum_{-(p-1)/2 \le \lambda \le (p-1)/2} \mathbf{e}_p\left(\lambda(m_1 a_1 + \cdots + m_k a_k - h)\right) \end{aligned}$$

(we can certainly assume that $p \ge 3$). Changing the order of summation and separating the term $M_1 \cdots M_k/p$ corresponding to $\lambda = 0$, we derive

$$R_p(\mathcal{A}, M_1, \ldots, M_k; h) - \frac{M_1 \cdots M_k}{p} = \frac{1}{p} \sum_{1 \le |\lambda| \le (p-1)/2} \mathbf{e}_p(-\lambda h) \prod_{i=1}^{k} \sum_{m_i=0}^{M_i-1} \mathbf{e}_p(\lambda m_i a_i).$$

We also recall the bound

$$\sum_{u=K+1}^{K+H} \mathbf{e}_n(cu) \ll \frac{n}{\|c\|_n + 1}, \tag{8}$$

which holds for any integers $c$, $n$, $K$ and $H$ with $n \gg H \ge 1$, see [17, Bound (8.6)]. Therefore, if $1 \le M_1, \ldots, M_k \le p$ then

$$R_p(\mathcal{A}, M_1, \ldots, M_k; h) - \frac{M_1 \cdots M_k}{p} \ll p^{k-1} \sum_{1 \le |\lambda| \le (p-1)/2} \prod_{a \in \mathcal{A}} \frac{1}{\|\lambda a\|_p}. \tag{9}$$

Let

$$W = \frac{1}{p^k} \sum_{\substack{\mathcal{A} \subseteq \mathbb{Z}_p^* \\ \#\mathcal{A} = k}} \max_{1 \le M_1, \ldots, M_k \le p} \max_{h \in \mathbb{Z}_p} \left| R_p(\mathcal{A}, M_1, \ldots, M_k; h) - \frac{M_1 \cdots M_k}{p} \right|.$$

Since the right hand side of (9) does not depend on $M_1, \ldots, M_k$ and $h$, we obtain

$$W \ll \frac{1}{p} \sum_{\substack{\mathcal{A} \subseteq \mathbb{Z}_p^* \\ \#\mathcal{A} = k}} \sum_{1 \le |\lambda| \le (p-1)/2} \prod_{a \in \mathcal{A}} \frac{1}{\|\lambda a\|_p} \ll \frac{1}{p} \sum_{a_1, \ldots, a_k \in \mathbb{Z}_p^*} \sum_{1 \le |\lambda| \le (p-1)/2} \prod_{i=1}^{k} \frac{1}{\|\lambda a_i\|_p}$$

$$= \frac{1}{p} \sum_{1 \le |\lambda| \le (p-1)/2} \sum_{a_1, \ldots, a_k \in \mathbb{Z}_p^*} \prod_{i=1}^{k} \frac{1}{\|\lambda a_i\|_p}.$$

It is obvious that the inner sum does not depend on $\lambda \in \mathbb{Z}_p^*$. Hence

$$W \ll \sum_{a_1, \ldots, a_k \in \mathbb{Z}_p^*} \prod_{i=1}^{k} \frac{1}{\|a_i\|_p} = \prod_{i=1}^{k} \sum_{a_i \in \mathbb{Z}_p^*} \frac{1}{\|a_i\|_p} = \left( \sum_{a \in \mathbb{Z}_p^*} \frac{1}{\|a\|_p} \right)^k \ll \left( 2 \sum_{1 \le a \le p/2} \frac{1}{a} \right)^k$$

and the result follows. □

For a fixed $\varepsilon > 0$ we denote by $\mathfrak{A}_p(k, \varepsilon)$ the collection of sets $\mathcal{A} \subseteq \mathbb{Z}_p$ with $\#\mathcal{A} = k$ and such that

$$\max_{1 \le M_1, \ldots, M_k \le p} \max_{h \in \mathbb{Z}_p} \left| R_p(\mathcal{A}, M_1, \ldots, M_k; h) - \frac{M_1 \cdots M_k}{p} \right| \le (\log p)^{k+\varepsilon}. \tag{10}$$

We immediately derive from Lemma 12 that for any $\varepsilon > 0$, almost all sets $\mathcal{A} \subseteq \mathbb{Z}_p$ with $\#\mathcal{A} = k$ belong to $\mathfrak{A}_p(k, \varepsilon)$. More precisely,

**Corollary 13** *For any fixed $\varepsilon > 0$, we have*

$$\#\mathfrak{A}_p(k,\varepsilon) = \big(1+o(1)\big)\binom{p}{k},$$

*as $p \to \infty$.*

*Proof* Let $\mathfrak{F}_p(k,\varepsilon)$ the collection of sets $\mathcal{A} \subseteq \mathbb{Z}_p$ with $\#\mathcal{A} = k$ for which (10) fails. By Lemma 12

$$\begin{aligned}
&\#\mathfrak{F}_p(k,\varepsilon)(\log p)^{k+\varepsilon} \\
&\quad < \sum_{\substack{\mathcal{A}\subseteq\mathbb{Z}_p^* \\ \#\mathcal{A}=k}} \max_{1\le M_1,\dots,M_k\le p} \max_{h\in\mathbb{Z}_p} \left| R_p(\mathcal{A}, M_1,\dots,M_k; h) - \frac{M_1\cdots M_k}{p} \right| \\
&\quad \ll p^k(\log p)^{-\varepsilon} \ll \binom{p}{k}(\log p)^{-\varepsilon}.
\end{aligned}$$

Thus $\#\mathfrak{F}_p(k,\varepsilon) \le p^k(\log p)^{-\varepsilon}$ which concludes the proof. □

In particular, Corollary 13 means that in the proof of Theorem 1 it is now enough to only consider sets $\mathcal{A} \in \mathfrak{A}_p(k,\varepsilon)$.

Our proof also relies on the following upper bound on the discrepancy $\Delta_p(\mathcal{A}, L; h)$ of the set of points

$$\mathcal{M}_p(\mathcal{A}, L; h) = \left\{ \left( \frac{m_1}{L}, \dots, \frac{m_k}{L} \right) \right\}$$

taken over all solutions $m_1, \dots, m_k \in \mathbb{Z}_n$ to (3) with $0 \le m_1, \dots, m_k \le L$. In particular, for $\mathcal{A} \in \mathfrak{A}_p(k,\varepsilon)$, we have

$$\#\mathcal{M}_p(\mathcal{A}, L; h) = R_p(\mathcal{A}, L+1, \dots, L+1; h) = \frac{(L+1)^k}{p} + O\big((\log p)^{k+\varepsilon}\big). \quad (11)$$

**Lemma 14** *For a prime $p$ and $\mathcal{A} \in \mathfrak{A}_p(k,\varepsilon)$, we have*

$$\Delta_p(\mathcal{A}, L; h) \ll L^{-1} + pL^{-k}(\log p)^{k+\varepsilon}.$$

*Proof* Clearly the number of points $(m_1/L, \dots, m_k/L) \in \mathcal{M}_n(\mathcal{A}, L; h)$ with $m_i/L \le \alpha_i$, $i = 1, \dots, k$ is given by $R_p(\mathcal{A}, \lfloor \alpha_1 L \rfloor + 1, \dots, \lfloor \alpha_k L \rfloor + 1; h)$. Hence, recalling the definition of the discrepancy in Sect. 2.1, we conclude that

$$\Delta_p(\mathcal{A}, L; h) \le \max_{0\le\alpha_1,\dots,\alpha_k<1} \left| \frac{R_p(\mathcal{A}, \lfloor \alpha_1 L \rfloor + 1, \dots, \lfloor \alpha_k L \rfloor + 1; h)}{\#\mathcal{M}_n(\mathcal{A}, L; h)} - \alpha_1, \dots, \alpha_k \right|$$

Clearly, for $\mathcal{A} \in \mathfrak{A}_p(k,\varepsilon)$, we have

$$
\begin{aligned}
&R_p\big(\mathcal{A}, \lfloor \alpha_1 L \rfloor + 1, \ldots, \lfloor \alpha_k L \rfloor + 1; h\big) \\
&\quad = \frac{1}{p} \prod_{i=1}^{k} \big(\lfloor \alpha_i L \rfloor + 1\big) + O\big((\log p)^{k+\varepsilon}\big) \\
&\quad = \frac{(L+1)^k \alpha_1 \cdots \alpha_k}{p} + O\big(L^{k-1} p^{-1} + (\log p)^{k+\varepsilon}\big),
\end{aligned}
$$

which together with (11) implies

$$
\frac{R_p(\mathcal{A}, \lfloor \alpha_1 L \rfloor + 1, \ldots, \lfloor \alpha_k L \rfloor + 1; h)}{\#\mathcal{M}_p(\mathcal{A}, L; h)} = \alpha_1 \cdots \alpha_k + O\big(L^{-1} + pL^{-k} (\log p)^{k+\varepsilon}\big)
$$

uniformly over $0 \le \alpha_1, \ldots, \alpha_k < 1$ which concludes the proof. □

### 2.3 Bisections of Circulant Graphs and Equivalent Sets

Upper bounds on the vertex-bisection width $\widetilde{\mathrm{vw}}(G)$ of a Cayley graph $G$ (with a generating set of cardinality $r$), in the relaxed case where

$$
\#V\big(G^1\big) \ge \frac{1}{3} n \quad \text{and} \quad \#V\big(G^2\big) \ge \frac{1}{3} n
$$

have been given in [4] and then improved in [9] to $\widetilde{\mathrm{vw}}(G) \le c(r) n^{1-1/r}$, where $c(r)$ is a constant depending only on $r$. In [12], it has been proved that an Abelian Cayley graph $G$ can be separated into two equal parts by deleting less than $8er^{-1}n^{1-\frac{1}{r}} \log(n/2)$ vertices. Here, we improve these results for circulant graphs.

An upper bound of the edge-bisection width of any undirected circulant graph of $n$ vertices can be given from the partitioning of vertex set (cyclically labelled $\{0, \ldots, n-1\}$) into two halves: $V(G^1) = \{0, \ldots, \lfloor n/2 \rfloor - 1\}$ and $V(G^2) = \{\lfloor n/2 \rfloor, \ldots, n-1\}$ or any rotation of such a cut, as shown in Fig. 1, say $V(G^1) = \{a, \ldots, b\}$ and $V(G^2) = \{b+1, \ldots, a-1\}$ where all operations are taken modulo $n$ and $b = a + \lfloor n/2 \rfloor - 1 \pmod{n}$. Without loss of generality, let us label the nodes on the ring cyclically and clockwise, and let us assume $1 \le s_1 < s_2 < \cdots < s_r < n/2$.

**Lemma 15** *For a symmetric set $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ of the form* (1)*, the edge-bisection width of $\mathcal{C}_n(\mathcal{A})$ is at most $2(|s_1| + \cdots + |s_r|)$.*

*Proof* Let us partition the vertex set $\{0, \ldots, n-1\}$ into two disjoint sets with the same order (within one), as described above (see Fig. 1). We count the number of chords of type $s_i$ which are "*cut*" at $a$ and $b$. Clearly, all the positive chords (going clockwise on the picture) outgoing from node $b$ are cut. In particular, the largest positive chord $s_r$ outgoing from node $b$ is cut. In fact, the same type of chord $s_r$ outgoing from nodes $\{b+1-s_r, \ldots, b\}$ is cut. Similarly, in the neighbouring of node $a$, all the nodes $\{a-s_r, \ldots, a-1\}$ have their outgoing chord $s_r$ cut. Clearly, no other node have their outgoing chord $s_r$ cut (otherwise, it requires their $s_r$ chords to be larger than $s_r$). Hence, the number of chords of type $s_r$, of length $s_r$, which need to be deleted to

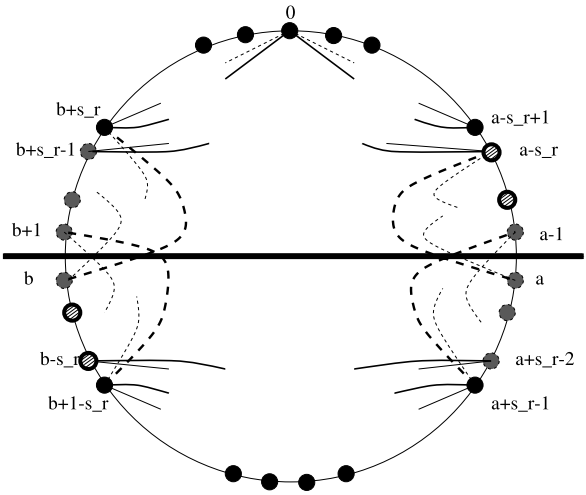


**Fig. 1** Bisection of a circulant graph

bisect the graph is: $\#\{b+1-s_r,\ldots,b\}+\#\{a-s_r,\ldots,a-1\}=s_r+s_r=2s_r$. Similarly, the edge bisecting set includes $2s_i$ of each type of chord $s_i$, and the lemma follows. Note that "negative" chords (that is, $\{-s_1,-s_2,\ldots,-s_r\}$) have been already counted as they correspond to incoming edges while labelling clockwise. □

Similarly, we give an upper bound of the vertex-bisection width.

**Lemma 16** *For a symmetric set* $\mathcal{A}\subseteq\widetilde{\mathbb{Z}}_n$ *of the form* (1), *the vertex-bisection width of* $\mathcal{C}_n(\mathcal{A})$ *is at most* $2\max_{1\le i\le r}|s_i|$.

*Proof* Let $G=\mathcal{C}_n(\mathcal{A})$. Let us partition the vertex set $\{0,\ldots,n-1\}$ into three disjoint subsets of $V$: $U$, $V(G^1)$ and $V(G^2)$ such as $U$ is a vertex bisector. Our proof is constructive. Initially, set $U=\emptyset$ and let $V(G^1)$ and $V(G^2)$ be the two sets of vertices obtained by an edge-bisection of $G$ (as described in Lemma 15). We remove the nodes $b+1,\ldots,b+s_r-1$ from $V^2$ and add them to $U$ (and delete all incident edges accordingly). Similarly, remove the nodes $a,\ldots,a+s_r-2$ from $V(G^1)$ and add them to $U$ (and delete all incident edges accordingly). Any path between a node of $V(G^1)$ and a node of $V(G^2)$ must either include the chord $s_r$ from node $b$ to node $b+s_r$, or include the chord $s_r$ from node $a-1$ to node $a+s_r-1$. Indeed, the path can neither use a chord larger than $s_r$, nor use an intermediate node (as they are all in $U$ now). By adding nodes $a-1$ and $b$ to $U$, and deleting all incident edges accordingly, we bisect $G$ as desired. As we removed the same number of vertices in the original sets $V(G^1)$ and $V(G^2)$, it is easy to verify that they are of the same size (within one). Clearly, $\#U=\#\{b,\ldots,b+s_r-1\}+\#\{a-1,\ldots,a+s_r-2\}=s_r+s_r=2s_r$. □

We say that sets $\mathcal{S},\mathcal{T}\subseteq\mathbb{Z}_n$ are *equivalent*, and write $\mathcal{S}\sim_n\mathcal{T}$, if for some integer $\lambda$ with $\gcd(\lambda,n)=1$, $\mathcal{A}\equiv\lambda\mathcal{B}\pmod n$ where the multiplication is taken element-wise and $\mathcal{S}$ (respectively $\mathcal{T}$) are representative edge sets of $\mathcal{A}$ (respectively $\mathcal{B}$).

The following statement is obvious (see also [25, 27] for results circulant isomorphism related to Ádám's conjecture [1]).

**Lemma 17** *Let $\mathcal{A} \subseteq \widetilde{\mathbb{Z}}_n$ be of the form (1). If $\mathcal{T} \sim_n \mathcal{S}$ then $\mathcal{C}_n(\mathcal{A})$ is isomorphic to $\mathcal{C}_n(\mathcal{B})$, where $\mathcal{B} = \mathcal{T} \cup (n - \mathcal{T})$.*

Hence, using Lemma 17, we prove that for almost all sets $\mathcal{S} \subseteq \widetilde{\mathbb{Z}}_n$ we can construct a set $\mathcal{T} \sim_n \mathcal{S}$ with small elements.

### 2.4 Equivalent Sets with Small Elements

For a given set $\mathcal{S} = \{s_1, \ldots, s_r\} \subseteq \widetilde{\mathbb{Z}}_n$ and a positive integer $h < n$ we denote by $T_n(\mathcal{S}; h)$ the number of solutions to the following system of congruences

$$\lambda s_i \equiv t_i \pmod{n}, \quad \lambda \in \mathbb{Z}_n^*, \ |t_i| \le h, \ i = 1, \ldots, r.$$

Note that when $\lambda \in \mathbb{Z}_n^*$ is fixed, the values of the variables $t_1, \ldots, t_r$ are uniquely defined. Since, $\lambda$ takes $\varphi(n)$ possible values, where $\varphi(n) = \#\mathbb{Z}_n^*$ is the Euler function, and the vector $(t_1, \ldots, t_n)$ can take $(2h+1)^r$ values out of the total number of possible $n^r$ values, it is natural to expect that $T_n(\mathcal{S}; h) > 0$ is close to $\varphi(n)(2h+1)^r/n^r$.

Clearly if $T_n(\mathcal{S}; h) > 0$ then $\mathcal{S}$ is equivalent to some set with elements of size at most $h$.

We consider the average deviation of $T_n(\mathcal{S}; h)$ from its expected value

$$\Delta_r(n; h) = \sum_{\substack{\mathcal{S} \subseteq \widetilde{\mathbb{Z}}_n \\ \#\mathcal{S} = r}} \left| T_n(\mathcal{S}; h) - \frac{\varphi(n)(2h+1)^r}{n^r} \right|.$$

Note that the question about estimating $T_n(\mathcal{S}; h)$ can be re-casted as a question about the distribution of the following vectors of fractional parts

$$\left( \left\{ \frac{\lambda s_1}{n} \right\}, \ldots, \left\{ \frac{\lambda s_r}{n} \right\} \right), \quad \lambda \in \mathbb{Z}_n^*,$$

which naturally links that question with the notion of discrepancy from Sect. 2.1. Thus, we use exponential sums to estimate $T_n(\mathcal{S}; h)$, which is a common tool used to estimate the discrepancy of sequences.

As usual, we use $\tau(d)$ to denote the number of integer positive divisors of an integer $d \ge 1$.

**Lemma 18** *For $1 \le h \le n$, we have $\Delta_r(n; h) \ll n^r \tau(n)^2 (\log n)^r$.*

*Proof* Using (7) and then changing the order of summation, we write

$$\begin{aligned} T_n(\mathcal{S}; h) &= \sum_{|t_1|, \ldots, |t_r| \le h} \sum_{\lambda \in \mathbb{Z}_n^*} \frac{1}{n^r} \sum_{-n/2 \le c_1, \ldots, c_r \in \mathbb{Z}_n < n/2} \mathbf{e}_n\left( \sum_{j=1}^{r} c_j (\lambda s_j - t_j) \right) \\ &= \frac{1}{n^r} \sum_{\lambda \in \mathbb{Z}_n^*} \sum_{c_1, \ldots, c_r \in \mathbb{Z}_n} \mathbf{e}_n\left( \lambda \sum_{j=1}^{r} c_j s_j \right) \prod_{j=1}^{r} \sum_{|t_i| \le h} \mathbf{e}_n(-c_j t_j). \end{aligned}$$

Separating the term $\varphi(n)(2h+1)^r/n^r$ corresponding to $c_1 = \cdots = c_r = 0$ and changing the order of summation, we derive

$$T_n(\mathcal{S};h) - \frac{\varphi(n)(2h+1)^r}{n^r} = \frac{1}{n^r} \sum_{\substack{-n/2 \le c_1,\ldots,c_r < n/2 \\ (c_1,\ldots,c_r)\neq \mathbf{0}}} R_n\left(\sum_{j=1}^{r} c_j s_j\right) \prod_{j=1}^{r} \sum_{|t_i|\le h} \mathbf{e}_n(-c_j t_j), \tag{12}$$

where $\mathbf{0}$ is the zero-vector and $R_n(a)$ is the *Ramanujan sum*

$$R_n(a) = \sum_{\lambda \in \mathbb{Z}_n^*} \mathbf{e}_n(\lambda a) = \varphi(n) \frac{\mu(n/\gcd(a,n))}{\varphi(n/\gcd(a,n))},$$

see [13, Theorem 272], where $\mu(k)$ is the Möbius function. In particular, from the trivial inequality $\varphi(k_1k_2) \le \varphi(k_1)k_2$, we derive

$$|R_n(a)| \le \gcd(a,n). \tag{13}$$

Substituting (8) (which applies as $1 \le h \le n$) and (13) in (12) we derive

$$\left| T_n(\mathcal{S};h) - \frac{\varphi(n)(2h+1)^r}{n^r} \right| \ll \sum_{\substack{-n/2 \le c_1,\ldots,c_r < n/2 \\ (c_1,\ldots,c_r)\neq \mathbf{0}}} \gcd\left(\sum_{j=1}^{r} c_j s_j, n\right) \prod_{j=1}^{r} \frac{1}{|c_j|+1}.$$

Therefore, extending the summation over all $s_1,\ldots,s_r \in \mathbb{Z}_n$, we obtain

$$\Delta_r(n;h) \ll \sum_{\substack{-n/2 \le c_1,\ldots,c_r < n/2 \\ (c_1,\ldots,c_r)\neq \mathbf{0}}} \prod_{j=1}^{r} \frac{1}{|c_j|+1} \sum_{\lambda s_i \in \mathbb{Z}_n} \gcd\left(\sum_{j=1}^{r} c_j s_j, n\right).$$

Now, for each divisor $d \mid n$ we collect together the terms with

$$\gcd(c_1 s_1 + \cdots + c_r s_r, n) = d,$$

getting

$$\Delta_r(n;h) \ll \sum_{d\mid n} d\,\Sigma_r(n;d), \tag{14}$$

where

$$\Sigma_r(n;d) = \sum_{\substack{-n/2 \le c_1,\ldots,c_r < n/2 \\ (c_1,\ldots,c_r)\neq \mathbf{0}}} \prod_{j=1}^{r} \frac{1}{|c_j|+1} \sum_{\substack{s_1,\ldots,s_r \in \mathbb{Z}_n \\ \gcd(\sum_{j=1}^{r} c_j s_j, n) = d}} 1.$$

Clearly, if $\gcd(c_1, \dots, c_r, d) = e$ then with $e_i = c_i/e$, $i = 1, \dots, r$ we derive

$$\sum_{\substack{s_1,\dots,s_r \in \mathbb{Z}_n \\ \gcd(\sum_{j=1}^r c_j s_j, n) = d}} 1 \le \sum_{\substack{s_1,\dots,s_r \in \mathbb{Z}_n \\ \sum_{j=1}^r c_j s_j \equiv 0 \pmod d}} 1 = \sum_{\substack{s_1,\dots,s_r \in \mathbb{Z}_n \\ \sum_{j=1}^r e_j s_j \equiv 0 \pmod{d/e}}} 1$$

$$= (ne/d)^r \sum_{\substack{s_1,\dots,s_r \in \mathbb{Z}_{d/e} \\ \sum_{j=1}^r e_j s_j \equiv 0 \pmod{d/e}}} 1 = n^r e/d.$$

Therefore,

$$\Sigma_r(n; d) \le n^r d^{-1} \sum_{e \mid d} e \sum_{\substack{-n/2 \le c_1,\dots,c_r < n/2 \\ (c_1,\dots,c_r) \ne \mathbf{0} \\ \gcd(c_1,\dots,c_r,d) = e}} \prod_{j=1}^r \frac{1}{|c_j| + 1}$$

$$\le n^r d^{-1} \sum_{e \mid d} e \sum_{\substack{-n/2e \le b_1,\dots,b_r < n/2e \\ (b_1,\dots,b_r) \ne \mathbf{0}}} \prod_{j=1}^r \frac{1}{e|b_j| + 1}$$

$$\le r n^r d^{-1} \sum_{e \mid d} e \sum_{1 \le |b_1| \le n/2e} \sum_{|b_2|,\dots,|b_r| \le n/2e} \prod_{j=1}^r \frac{1}{e|b_j| + 1}$$

$$= r n^r d^{-1} \sum_{e \mid d} e \sum_{1 \le |b_1| \le n/2e} \frac{1}{e|b_1| + 1} \left( \sum_{|b_2| \le n/2e} \frac{1}{e|b_2| + 1} \right)^{r-1}.$$

Clearly the sum over $b_1$ is at most $O(e^{-1} \log n)$ and the sum over $b_2$ is at most $O(\log n)$. Thus $\Sigma_r(n; d) \ll n^r d^{-1} \tau(d) (\log n)^r$. Substituting in (14), using the trivial bound $\tau(d) \le \tau(n)$, we derive the result. □

Since $\tau(n) = n^{o(1)}$, see [13, Theorem 317], we deduce from Lemma 18:

**Corollary 19** *We have,* $\Delta_r(n; h) \le n^{r+o(1)}$, *as* $n \to \infty$.

## 3 Proofs of Bounds for Walks and Bisectors

### 3.1 Proof of Theorem 1

By Corollary 13, it is enough to only consider the sets $\mathcal{A} \in \mathfrak{A}_p(k, \varepsilon)$.

Let us fix $\mathcal{A} \in \mathfrak{A}_p(k, \varepsilon)$.

The idea is to interpret counting solutions to (3) with the condition (3) as question of counting the vectors of fractional parts

$$\left( \left\{ \frac{m_1}{n} \right\}, \dots, \left\{ \frac{m_k}{n} \right\} \right), \tag{15}$$

that belong to the simplex

$$\Sigma = \big\{(\alpha_1, \dots, \alpha_k) \in [0,1]^k \mid \alpha_1 + \cdots + \alpha_k \le 1\big\},$$

where the vector $(m_1, \dots, m_k)$ runs through all solutions to (3). Since $\Sigma$ is convex, one easily sees that $\Sigma$ belongs to the class $\mathcal{S}_h$ (defined in Sect. 2.1) for some linear function $h(\varepsilon) = C\varepsilon$. Now Lemma 11 allows to reduce this question to counting the vectors (15) in aligned rectangles. In turn this question, for a prime $n = p$, has been addressed in Lemma 14

More precisely, combining Lemma 11 with Lemma 14, we estimate the discrepancy $\Gamma_p(\mathcal{A}, L, \Sigma; h)$ of the set $\mathcal{M}_p(\mathcal{A}, L; h)$ with respect to the simplex $\Sigma$ of volume $\lambda(\Sigma) = 1/k!$ as $O(L^{-1/k} + p^{1/k}L^{-1}(\log p)^{1+\varepsilon/k})$. Now, from (11), we obtain that

$$\begin{aligned} N_p(\mathcal{A}, L; h) &= L^k\lambda(\Sigma) + O\big(L^{k-1/k}p^{-1} + p^{1/k}L^{k-1}(\log p)^{1+\varepsilon/k}\big) \\ &= \binom{L+1}{k}\frac{1}{p} + O\big(L^{k-1/k}p^{-1} + p^{1/k}L^{k-1}(\log p)^{1+\varepsilon/k}\big). \end{aligned} \tag{16}$$

Therefore

$$N_p(\mathcal{A}, L; h) = \big(1 + o(1)\big)\binom{L+1}{k}\frac{1}{p}$$

for $L \ge p^{1/k}(\log p)^{1/k+\varepsilon}$.

### 3.2 Proof of Theorem 2

We now fix a sufficiently small $\varepsilon > 0$ and assume that $n$ is sufficiently large.

Corollary 19 means that for almost all sets $\mathcal{S} \subseteq \widetilde{\mathbb{Z}}_n$ there is $\lambda \in \mathbb{Z}_n^*$ with

$$\max_{i=1,\dots,r} \|\lambda s_i\|_n = n^{1-1/r+\varepsilon}. \tag{17}$$

We also see from the bound $\tau(n) = n^{o(1)}$ on the divisor function, see [13, Theorem 317], that for almost all sets $\mathcal{S} \subseteq \widetilde{\mathbb{Z}}_n$ we have $\gcd(s_1, n) = n^{o(1)}$. Indeed, the number of sets $\mathcal{S} \subseteq \widetilde{\mathbb{Z}}_n$ with, say, $\gcd(s_1, n) \ge \tau(n)\log n$ is at most

$$\sum_{\substack{d \mid n \\ d \ge \tau(n)\log n}} \frac{n^r}{d} \le \frac{n^r}{\log n}.$$

Now, for each of the remaining sets we search through all solutions $\lambda \in \mathbb{Z}_n^*$ to the congruences

$$\lambda s_1 \equiv t_1 \pmod{n}$$

with $|t_1| \le n^{1-1/r+\varepsilon}$. Since $\gcd(s_1, n) = n^{o(1)}$ each of these congruences has $n^{o(1)}$ possible solutions. So in time $n^{1-1/r+\varepsilon+o(1)}$ we find $\lambda \in \mathbb{Z}_n^*$ that satisfies (17). Recalling that $\varepsilon$ is arbitrary, together with Lemmas 16 and 17, we conclude the proof.

### 3.3 Proof of Theorem 3

Let us set $N = \lceil p^{1/r} \rceil - 1$ and consider the family of $p$ points

$$(\ell s_1, \ldots, \ell s_r), \quad \ell \in \mathbb{Z}_p. \tag{18}$$

Separating this cube into $N^r < p$ equal subcubes with the side length $h = p/N$, we see that there is at least one subcube that contains at least two points (18) corresponding to some $0 \le \ell_1 < \ell_2 \le p-1$. Therefore, putting $\lambda = \ell_2 - \ell_1$, we obtain

$$\|\lambda s_i\|_p \le h, \quad i = 1, \ldots, r.$$

Therefore, in time $p^{1-1/r+o(1)}$ (see the proof of Theorem 2) we can comput $\lambda \not\equiv 0 \pmod p$ such that

$$\left(\sum_{i=1}^{r} \|\lambda s_i\|_p^2\right)^{1/2} \le \left(\sum_{i=1}^{r} \|\lambda s_i\|_p^2\right)^{1/2} \le r^{1/2} h.$$

Hence, using the Cauchy inequality, we derive

$$\max_{i=1,\ldots,r} \|\lambda s_i\|_p \le \sum_{i=1}^{r} \|\lambda s_i\|_p \le \left(r \sum_{i=1}^{r} \|\lambda s_i\|_p^2\right)^{1/2} \le rh$$

As in the proof of Theorem 2, using Lemmas 16 and 17, we conclude the proof.

### 3.4 Composite Values of $n$

It is natural to try to extend our method to composite values of $n$. Unfortunately, this does not seem to be possible. It is easy to show that if $n = 2m$ is even, and $S_0 = \{\pm 1, \pm(m+1)\}$ then

$$\min_{T \sim_n S_0} \max_{i=1,2} |t_i| \ge n/4.$$

Indeed, let $T = \lambda S$. If $|\lambda| = |t_1| < m/2 = n/4$, then, because the condition $\gcd(l, n) = 1$ implies that $\lambda$ is odd, we have $|t_2| = m + \lambda > m/2 = n/4$. Thus any method using our Lemmas 15 and 16 leads to very weak results. This however does not mean that appropriate bisectors do not exist in this case.

The difficulty of finding a precise bisection width when $n$ is composite is not really surprising. There is nothing new in the fact that the arithmetic structure of $n$ (for example, primality) plays an important role. Let us recall that the simple isomorphism rule only holds for special cases, including circulant graphs with prime number of vertices [11], but is not true for most of values of $n$ (see previous section).

## 4 Gossiping Algorithms in Circulant Graphs

### 4.1 Background on Gossiping

Information dissemination is the most important communication problem in interconnection networks. Three basic communication problems are:

- *Broadcast* (one-to-all): one node has a piece of information and has to communicate this information to all the other nodes.
- *Accumulation* (all-to-one): all the nodes have a different piece of information and want to communicate this information to the same particular node.
- *Gossip* (all-to-all): each node has a piece of information and wants to communicate this information to all the other nodes (such that all nodes learn the cumulative message). Clearly, gossiping can be achieved by combining solutions to both previous problems (as shown in Sect. 4.2).

### 4.2 Generic and "Well-Structured" VDP Gossiping

It is clear that "specialised" algorithms must be used to obtain tight complexity bounds for specific chord sets. (For example, it is easy to see that a circulant graph of $n = 2^r$ nodes with chord set $\mathcal{A} = \{\pm 1, \pm 2, \pm 2^2, \ldots, \pm 2^{r-1}\}$ perfectly embeds a hypercube, and thus, can gossip with the minimum number of rounds.)

Here, we only focus on "generic" algorithms that work correctly for any circulant graph given as input. Although, we can only bound the number of rounds required by the algorithm when $n$ is prime, let us emphasize that the algorithms described below completes the gossip correctly even if $n$ is composite.

A popular strategy, introduced in [15], to solve the gossip problem is to use a 3-phase algorithm described as follows. Let $G(V, E)$ be the graph corresponding to the topology of the network. Let $a(G)$ be any subset of nodes of $G$ (called the *accumulation set*). Divide $G$ into $m = |a(G)|$ connected components (called *accumulation components*) of size $\lceil n/m \rceil$, such that each connected component contains exactly one accumulation node of $a(G)$.

The 3-phase gossip algorithm for $G$ with respect to $a(G)$ follows the phases, (where $1 \leq i \leq m$):

1. **Accumulation**: each accumulation node $a_i$ accumulates the information from the nodes lying in its accumulation component $A_i$.
2. **Gossip**: performs a gossip algorithm among the nodes $a_i$ of $a(G)$.
3. **Broadcast**: each node $a_i$ broadcasts the cumulative message in its component $A_i$.

For the 2-VDP mode, the accumulation problem can be considered as the reverse of broadcast problem, and hence, a similar strategy can be used. In [15], the authors proved that, with the 2-VDP mode, broadcasting (resp. accumulating) in a Hamiltonian path of $k$ nodes can be done in $\lceil \log k \rceil$ rounds.

For the 1-VDP mode, we use the same notations as in [14] and call a 3-phase algorithm *well-structured* if the gossip phase is an implementation of an optimal gossip algorithm (for example, in the complete graph $K_m$, or a hypercube $Q_{\lceil \log m \rceil}$), and takes $\lceil \log m \rceil$.

Under the 2-VDP mode, when the accumulating components are Hamiltonian paths, a well-structured gossip algorithm $\mathfrak{G}$ on $G$ only requires

$$\lceil \log n/m \rceil + \lceil \log m \rceil + \lceil \log n/m \rceil \leq 2\lceil \log n \rceil - \lceil \log m \rceil \tag{19}$$

rounds. A straightforward upper bound on the number of rounds of gossiping can be obtained by constructing a well-structured gossip algorithm $\mathfrak{G}$ by taking the $m$ nodes of the vertex bisector as accumulation nodes. It is easy to see that, when $m = \lceil n^{1-1/r} \rceil$, the number of rounds is nearly optimal:

$$g_{\mathfrak{G}}(G) \leq \left(1 + \frac{1}{r}\right) \log n.$$

In the following, we exploit the knowledge of the existence of such $m$ nodes when $n$ is prime by computing (in polynomial time) a bisector set of size $m$ (as described in Theorem 3). We first describe a well-structured gossip algorithm for a specific infinite family of circulant graphs of degree four with $n$ prime. We then show how to extend this strategy to other circulant graphs. Let us consider the circulant graph $G$ of degree 4 with $n$ vertices and chord set $\mathcal{A} = \{\pm 1, \pm s_2\}$ (that is, $r = 2$) with $s_2 = 2^d$ and $s_2(s_2 - 1) \leq n \leq s_2^2$ (that is, $s_2 \sim n^{1/2}$). Without loss of generality we can label the nodes $[0, \ldots, (n-1)]$ cyclically along the chord $+1$. We partition $G$ into $m = s_2$ connected components of, up to, $\lceil n/s_2 \rceil \leq s_2 = 2^d$ nodes:

$$\begin{aligned} A_i &= \{i, s_2 + i, 2s_2 + i, \ldots, (s_2 - 1)s_2 + i\}, \quad 0 \leq i < n - (s_2 - 1)s_2, \\ A_i &= \{i, s_2 + i, 2s_2 + i, \ldots, (s_2 - 2)s_2 + i\}, \quad n - (s_2 - 1)s_2 \leq i \leq s_2 - 1, \end{aligned} \tag{20}$$

where each component has an accumulating node $a_i = i$, $0 \leq i \leq s_2 - 1$. This also defines $s_2$ consecutive segments $S_k$, $0 \leq k \leq s_2 - 1$ along the $+1$ chords. The first segment, $S_0$, corresponds to the accumulation nodes, and all segments, but possibly the last one $S_{s_2-1}$, are of size $s_2$. Clearly, each accumulating component is connected by a Hamiltonian path along the chord $+s_2$. With the 2-VDP mode, the accumulating phase and the broadcasting phase take at most

$$\lceil \log s_2 \rceil = d \leq \log n^{1/2} + 1 = \frac{1}{2} \log n + 1$$

rounds respectively.

We say that the nodes $i$ and $j$ exchange information through the segment $S_k$, if the information is passed first through $k$ chords $(+s_2)$, then through the chord $(\pm 1)$ between the nodes $ks_2 + i$ and the node $ks_2 + j$ (in the segment $S_k$ of nodes $\{ks_2, \ldots, ks_2 + s_2 - 1\}$), and finally back through $k$ chords $(-s_2)$. For the gossip phase of the accumulating nodes, we present the recursive Algorithm in Fig. 2 (see also Fig. 3) similar to the algorithm presented in [14] for square grids of $n = 2^{2d}$ nodes and side-length $n^{1/2} = 2^d$. Initially, the algorithm is started by running `Gossip`$(0, s_2 - 1)$.

By induction, it is easy to see that each node learns the cumulative message and the communication at each round is vertex-disjoint. Any two pairs of nodes $(i_1, j_1)$

Procedure `Gossip`$(a, b)$
if $(b-a) > 1$ do in parallel
  Gossip$(a, a + \lfloor \frac{b-a}{2} \rfloor)$ and Gossip$(a + \lceil \frac{b-a}{2} \rceil, b)$
endo in parallel
for $a \le i \le a + \lfloor \frac{b-a}{2} \rfloor$ do in parallel
  exchange information between $i$ and $j = b - i$ through segment $S_k$, $k = \lfloor \frac{j-i}{2} \rfloor$
endo in parallel

**Fig. 2** Gossip procedure for the algorithm in the 2-VDP mode

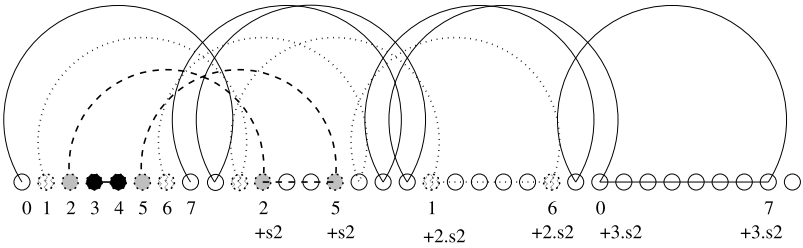


**Fig. 3** The communication paths in the 2-VDP mode

and $(i_2, j_2)$ exchanging information through a segment $k$ define two non-intersecting sections in the segment $S_k$, as

$$k = \left\lfloor \frac{j_1 - i_1}{2} \right\rfloor = \left\lfloor \frac{j_2 - i_2}{2} \right\rfloor$$

we have $i_1 < j_1 < i_2 < j_2$. In the case $i_1 < i_2 < j_2 < j_1$, we have

$$\left\lfloor \frac{j_1 - i_1}{2} \right\rfloor = k_1 \neq k_2 = \left\lfloor \frac{j_2 - i_2}{2} \right\rfloor.$$

Obviously,

$$\log s_2 \le \frac{1}{2} \log n + 1$$

rounds are sufficient to gossip among the accumulating nodes, and thus, the total number of rounds of this well-structured gossip algorithm $\mathfrak{G}$ is

$$g_{\mathfrak{G}}(G) \le \left(1 + \frac{1}{2}\right) \log n + 3 = \frac{3}{2} \log n + 3.$$

This is near optimal as it almost match the lower bound of Theorems 7 and 8 and can be generalised to other cases. Note that the last section $S_{s_2-1}$ is not used and does not require to be full. In fact, only the first $k$ segments, $k = \lfloor (n-1)/2 \rfloor$, are used by the algorithm. Hence the algorithm can be adapted to run correctly for $s_2^2/2 \le n \le s_2^2$, and takes either $\frac{3}{2} \log n$ or $\frac{3}{2} \log n + 3$ rounds.

In the case that $s_2$ is not a power of 2 (that is, $2^d < s_2 < 2^{d+1}$ for some $d$), a similar algorithm can be used with two extra rounds. After the accumulation phase, each accumulation node $j$, $2^d \le j \le s_2 - 1$, gossips its information to the accumulation node $i$, $2^d - 1 \ge i \ge 2^d - 1 - (s_2 - 1 - 2^d)$, through the segment $S_k$, $k = (j - i)/2$. After the gossip phase $\texttt{Gossip}(0, 2^d - 1)$, and before the broadcast phase, each node $i$ sends the cumulative message to the respective node $j$.

When considering circulant graphs with $n = p$ prime and a chord set $\mathcal{A} = \{\pm s_1, \pm s_2\}$, $s_1 < s_2$, (instead of the specific chord set $\mathcal{B} = \{\pm 1, \pm s_2\}$), Theorem 3 implies that for circulant graphs $G$ of degree 4 with $n$ vertices, it is possible to generate a representation of $G$ with a chord set $\mathcal{B} = \{\pm t_1, \pm t_2\}$ such that $\langle \mathcal{A} \rangle_n \simeq \langle \mathcal{B} \rangle_n$ and $t_1 < t_2 \le 4n^{1-\frac{1}{2}} = 4n^{1/2}$. Using $\mathcal{B}$ as the chord set, and if $\gcd(t_1, t_2) = 1$, we can partition $G$ into $m = \lceil n/t_2 \rceil$ connected components (along the chord $+t_1$) of, up to, $t_2$ nodes. Each component has an accumulating node $a_i = it_2$, $0 \le i \le (m - 1)$. Clearly, each accumulating component is connected by a Hamiltonian path along the chord $+t_1$. With the 2-VDP mode, the accumulating phase and the broadcasting phase take at most $\lceil \log t_2 \rceil$. Representing $G$ with chord set $\mathcal{C} = \{\pm 1, \pm w_2\}$ where $w_2 \equiv t_1 t_2^{-1} \pmod{n}$, the accumulating nodes $a_i$, $0 \le i \le m - 1$, are now consecutive along the chord $+1$. It is easy to see that if $2n/w_2 < m < w_2$, the generic $\texttt{Gossip}$ algorithm runs correctly within a number of rounds close to the minimum.

For circulant graphs with chord set $\mathcal{A} = \{\pm 1, \pm n^{1/r}, \pm n^{2/r}, \ldots, \pm n^{(r-1)/r}\}$, with $r \ge 3$, we can give tight upper bounds on the gossiping complexity in the 2-VDP mode using an algorithm similar to [14] for $r$-dimensional grids of $n$ nodes and side-length $n^{1/r}$, $r \ge 3$, when $n$ is an $r$th power, and extend from these algorithms otherwise.

### 4.3 2-EDP Gossiping

In this section, we describe a gossiping algorithm in the 2-EDP mode for almost all circulant graphs.

As in Sect. 4.2, we first consider a specific circulant graph $G$ of degree 4 with $n$ vertices and chord set $\mathcal{A} = \{\pm 1, \pm s_2\}$ (that is, $r = 2$) with $s_2$ and $s_2(s_2 - 1) \le n \le s_2^2$ (that is, $s_2 \sim n^{1/2}$). (In this case, we do not need to assume that $s_2$ is a power of 2.)

Without loss of generality we can label the nodes $[0, \ldots, n - 1]$ cyclically along the chord $+1$. We partition $G$ into $m = s_2$ connected components of, up to, $\lceil n/s_2 \rceil \le s_2$ nodes as described in (20). Again, each accumulating component is connected by a Hamiltonian path along the chord $+s_2$. With the 2-EDP mode, the accumulating phase and the broadcasting phase take at most $\log s_2 \le \log n^{1/2} + 1 = \frac{1}{2} \log n + 1$ rounds respectively.

For the gossip phase of the accumulating nodes, the algorithm is described in Figs. 4 and 5 for the case $m$ even and $m$ odd respectively. (This algorithm has originally been designed for complete graphs and has also been used for chordal rings of degree three [6, 7], which are not circulant graphs.)

In our case, a communication exchange between nodes $i$ and $j$ in the algorithm is replaced by a call between $a_i$ and $a_j$ through the segment $S_j$. We say that the nodes $a_i$ and $a_j$ exchange information through the segment $S_j$, if the information is passed first through $j$ chords $(+s_2)$, then through $(j - i)$ chords $(\pm 1)$ between the

For $j := 1$ to $\lfloor \log m \rfloor$ do
  For each node $i$, $i$ even, do in parallel
    exchange information between node $i$ and node $i + 2^j - 1 \pmod m$

**Fig. 4** Gossip algorithm in $K_m$, $m$ even [7]

$q := \lfloor m/2 \rfloor$
For each node $i$, $0 < i < m/2$, do in parallel
  exchange information between node $i$ and node $i + q \pmod n$
If $q$ odd then $m_0 := q + 1$ else $m_0 := q + 2$
Gossip in $K_{m_0}$ ($m_0$ even)
For each node $i$, $0 < i < m/2$, do in parallel
  exchange information between node $i$ and node $i + q \pmod n$

**Fig. 5** Gossip algorithm in $K_m$, $m$ odd [7]

nodes $js_2 + i$ and $js_2 + j$ (in the segment of nodes $S_j$), and finally back through $j$ chords $(-s_2)$.

At each round, any two pairs of nodes $(a_{i_1}, a_{j_1})$ and $(a_{i_2}, a_{j_2})$ use different segments (namely, $j_1$ and $j_2$), and thus the communication at each round is edge-disjoint.

Obviously, $\log s_2 \leq \frac{1}{2} \log n + 1$ rounds are sufficient to gossip among the accumulating nodes, and thus, the total number of rounds of this well-structured gossip algorithm $\mathfrak{G}$ is

$$g_{\mathfrak{G}}(G) \leq \left(1 + \frac{1}{2}\right) \log n + 3 = \frac{3}{2} \log n + 3.$$

In fact, this gossiping algorithm runs correctly with any chordal ring of degree four with $n$ vertices and chord set $\mathcal{A} = \{\pm 1, \pm s_2\}$ if $s_2 \leq n^{1/2}$ (but near optimal when $s_2 \sim n^{1/2}$). It can be extended to any circulant graph with chord set $\mathcal{A} = \{\pm t_1, \pm t_2\}$, $t_1 < t_2$, and for $r \geq 3$ with chord set $\mathcal{B} = \{\pm 1, \pm n^{1/r}, \pm n^{2/r}, \ldots, \pm n^{(r-1)/r}\}$ using an algorithm for $r$-dimensional grids $\mathrm{Gr}_n^r$ of $n$ nodes and sidelength $n^{1/r}$, $r \geq 3$ [16] to obtain asymptotically optimal number of rounds.

## 5 Proofs of Bounds on Gossiping

### 5.1 Proofs of Theorems 7 and 8

Here, we give lower bounds of the gossip complexity for the circulant graphs of $|V| = n = p$ vertices with $p$ prime. A direct relationship exists between the bisection width and the gossip complexity. The following statement gives a summary of several known bounds from [16] (for the EDP mode) and from [18] (for the VDP mode):

**Lemma 20** *Let $G$ be a network of edge-bisection* $\mathrm{ew}(G)$ *and of vertex-bisection* $\mathrm{vw}(G)$.

- *In the* 2*-EDP mode, for any gossip algorithm* $\mathfrak{G}$*, we have*

$$g_{\mathfrak{G}}(G) \geq 2\log n - \log \mathrm{ew}(G) - \log\log n - 4.$$

- *In the* 2*-VDP mode, for any gossip algorithm* $\mathfrak{G}$*, we have*

$$g_{\mathfrak{G}}(G) \geq 2\log n - \log \mathrm{vw}(G) - \log\log \mathrm{vw}(G) - 6.$$

Obviously, combining Lemma 20 with Theorems 2 and 3, we obtain the lower bounds of Theorems 7 and 8, respectively.

### 5.2 Proof of Theorems 9 and 10

Let as before define $\vartheta = (\log(1+5^{1/2})-1)^{-1}$. We now recall the following result from [18] (using their definition of "well-structured" gossip algorithms, reminded in Sect. 4.2).

**Lemma 21** *Let* $G$ *be a network of* $n$ *nodes and of vertex-bisection* $\mathrm{vw}(G)$*. In the* 1*-VDP mode, for any "well-structured" gossip algorithm* $\mathfrak{G}$*,*

$$g_{\mathfrak{G}}(G) \geq 2\log n - (2-\vartheta)\big(\log \mathrm{vw}(G) + \log\log \mathrm{vw}(G)\big) - 15.$$

Combining Lemma 21 with the bounds of Theorems 2 and 3 (see also (6)), we conclude the proofs of Theorems 9 and 10, respectively.

*Remark 22* Most of the optimal algorithms known for gossiping in the 1-way mode, VDP or EDP, (see [14, 16, 18]), are *well-structured*. The lower bounds obtained in Theorems 9 and 10 suggest that a well-structured algorithm, inspired from known algorithms in grids, could achieve similar results.

## 6 Concluding Remarks

We conclude by providing some open questions.

It is certainly an interesting problem to obtain an asymptotic formula for the number $\overline{N}_p(\mathcal{A}, L; h)$ of ordered walks of length *exactly* $L$ which end at $h \in \mathbb{Z}_p$. Clearly, $\overline{N}_p(\mathcal{A}, L; h) = N_p(\mathcal{A}, L; h) - N_p(\mathcal{A}, L-1; h)$, however the bound on the error term in the asymptotic formula (16) is not strong enough to get any meaningful results about $\overline{N}_p(\mathcal{A}, L; h)$.

Studying undirected circulant graphs that correspond to sets $\mathcal{A}$ of the form (1), is also of interest. Our technique can be easily adjusted to deal with this case as well.

One can also use our approach of Sect. 2.2 to study circulant graphs over $\mathbb{Z}_n$ with a composite $n$, although the argument becomes more technically cluttered due to the presence of zero-divisors in $\mathbb{Z}_n$.

It is natural to study traditional (that is, unordered) walks, where at each step any of the jump lengths $a_1, \ldots, a_k$ can be chosen with probability $1/k$. It is easy to see

that the number $M_p(\mathcal{A}, L; h)$ of such walks of length at most $L$ which end at $h \in \mathbb{Z}_p$ is given by the sum

$$M_p(\mathcal{A}, L; h) = \sum_{(m_1,\ldots,m_k)\in\mathcal{N}_p(\mathcal{A},L;h)} \frac{(m_1 + \cdots + m_k)!}{m_1! \cdots m_k!}$$

where $\mathcal{N}_p(\mathcal{A}, L; h)$ is the set of solutions to (3) satisfying the conditions (4). It seems plausible that our methods can be used to investigate such sums as well.

Another interesting direction is to study the cover time of random walks on circulant graphs, see [21] for general results the cover time of arbitrary and regular graphs. Studying multiple random walks on circulant graphs is also of interest, see [2].

Finally, we note that the argument of [10], essentially based on the Dirichlet pigeon-hole principle, has also been used here to show that for a prime $p$, any graph $\mathcal{C}_p(\mathcal{A})$ is isomorphic to another circulant graph $\mathcal{C}_p(\widetilde{\mathcal{A}})$ where all elements of $\widetilde{\mathcal{A}}$ are "small" (of size $O(p^{1-1/k})$). It is certainly interesting to investigate whether the technique of Marklof and Strombergsson [26] can be used to get more insight on this question.

**Acknowledgements** The authors are very grateful to the referees for constructive and thorough comments.

The research of B.M. by Australian Research Council Grant DP110104560, and that of I.E.S. by Australian Research Council Grants DP130100237 and Macquarie University Grant MQRDG1465020.

## References

1. Ádám, A.: Research problem 2–10. J. Comb. Theory **3**, 393 (1967)
2. Alon, N., Avin, C., Kouck, M., Kozma, G., Lotker, Z., Tuttle, M.R.: Many random walks are faster than one. Comb. Probab. Comput. **20**, 481–502 (2011)
3. Amir, G., Gurel-Gurevich, O.: The diameter of a random Cayley graph of $\mathbb{Z}_q$. In: Groups Complex. Crypto, vol. 2, pp. 59–65 (2010)
4. Annexstein, F., Baumslag, M.: On the diameter and bisector size of Cayley graphs. Math. Syst. Theory **26**, 271–291 (1993)
5. Attiya, H., van Leeuwen, J., Santoro, N., Zaks, S.: Efficient elections in chordal ring networks. Algorithmica **4**, 437–446 (1989)
6. Barrière, L., Fàbrega, J.: Edge-bisection of chordal rings. In: Proc. 25th MFCS. LNCS, pp. 162–171. Springer, Berlin (2004)
7. Barrière, L., Cohen, J., Mitjana, M.: Gossiping in chordal rings under the line model. Theor. Comput. Sci. **264**, 53–64 (2001)
8. Bermond, J.-C., Comellas, F., Hsu, D.F.: Distributed loop computer networks: a survey. J. Parallel Distrib. Comput. **24**, 2–10 (1995)
9. Blackburn, S.R.: Node bisectors of Cayley graphs. Math. Syst. Theory **29**, 589–598 (1996)
10. Cai, J.-Y., Havas, G., Mans, B., Nerurkar, A., Seifert, J.-P., Shparlinski, I.: On routing in circulant graphs. In: Proc. 5th COCOON. LNCS, pp. 370–378. Springer, Berlin (1999)
11. Elspas, B., Turner, J.: Graphs with circulant adjacency matrices. J. Comb. Theory **9**, 229–240 (1970)
12. Hamidoune, Y.O., Serra, O.: On small cuts separating an Abelian Cayley graph into two equal parts. Math. Syst. Theory **29**, 407–409 (1996)
13. Hardy, G.H., Wright, E.M.: An Introduction to the Theory of Numbers, 5th edn. Clarendon, New York (1979)
14. Hromkovič, J., Klasing, R., Stöhr, E.A., Wagener, H.: Gossiping in vertex-disjoint paths mode in d-dimensional grids and planar graphs. Inf. Comput. **123**, 17–28 (1995)
15. Hromkovič, J., Klasing, R., Stöhr, E.A.: Dissemination of information in generalized communication modes. Comput. Artif. Intell. **15**, 295–318 (1996)

16. Hromkovič, J., Klasing, R., Unger, W., Wagener, H.: Optimal algorithms for broadcast and gossip in the edge-disjoint path modes. Inf. Comput. **133**, 1–33 (1997)
17. Iwaniec, H., Kowalski, E.: Analytic Number Theory. Am. Math. Soc., Providence (2004)
18. Klasing, R.: The relationship between the gossip complexity in the vertex-disjoint paths mode and the vertex bisection width. Discrete Appl. Math. **83**, 229–246 (1998)
19. Laczkovich, M.: Discrepancy estimates for sets with small boundary. Studia Sci. Math. Hung. **30**, 105–109 (1995)
20. Leighton, F.T.: Introduction to Parallel Algorithms and Architectures: Arrays, Trees, Hypercubes. Morgan Kaufmann, San Mateo (1992)
21. Lovász, L.: Random Walks on Graphs: a Survey. Combinatorics, Paul Erdös Is Eighty, pp. 1–46. Bolyai Soc., Hungary (1993)
22. Mans, B.: Optimal distributed algorithms in unlabeled tori and chordal rings. J. Parallel Distrib. Comput. **46**, 80–90 (1997)
23. Mans, B., Shparlinski, I.E.: Bisecting and gossiping in circulant graphs. In: Proc. 6th LATIN. LNCS, pp. 589–598. Springer, Berlin (2004)
24. Mans, B., Shparlinski, I.E.: Random walks and bisections in random circulant graphs. In: Proc. 10th LATIN. LNCS, pp. 542–555. Springer, Berlin (2012)
25. Mans, B., Pappalardi, F., Shparlinski, I.: On the spectral Ádám property for circulant graphs. Discrete Math. **254**, 309–329 (2002)
26. Marklof, J., Strombergsson, A.: Diameters of random circulant graphs. Combinatorica. Available from: http://arxiv.org/abs/1103.3152 (2011, to appear)
27. Muzychuk, M.: On Ádám's conjecture for circulant graphs. Discrete Math. **167/168**, 497–510 (1997). Erratum: Discrete Math. **176**, 285–298 (1997)
28. Narayanan, L., Opatrny, J., Sotteau, D.: All-to-all optical routing in optimal chordal rings of degree 4. Algorithmica **29**, 396–409 (2001)
29. Niederreiter, H., Wills, J.M.: Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen. Math. Z. **144**, 125–134 (1975)
30. Opatrny, J.: Uniform multi-hop all-to-all optical routings in rings. Theor. Comput. Sci. **297**(1–3), 385–397 (2003)