International Journal of Quantum Information
Vol. 5, No. 3 (2007) 417–430
© World Scientific Publishing Company

World Scientific
www.worldscientific.com

PARAMETERS OF INTEGRAL CIRCULANT GRAPHS AND PERIODIC QUANTUM DYNAMICS

NITIN SAXENA
Centrum voor Wiskunde en Informatica,
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands
ns@cwi.nl

SIMONE SEVERINI
Institute for Quantum Computing,
University of Waterloo, N2L 3G1 Waterloo, Canada
simoseve@gmail.com

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University,
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Received 8 April 2007

The intention of the paper is to move a step towards a classification of network topologies that exhibit periodic quantum dynamics. We show that the evolution of a quantum system whose hamiltonian is identical to the adjacency matrix of a circulant graph is periodic if and only if all eigenvalues of the graph are integers (that is, the graph is *integral*). Motivated by this observation, we focus on relevant properties of integral circulant graphs. Specifically, we bound the number of vertices of integral circulant graphs in terms of their degree, characterize bipartiteness and give exact bounds for their diameter. Additionally, we prove that circulant graphs with odd order do not allow perfect state transfer.

Keywords: Circulant graphs; integral graphs; periodic dynamics; perfect state transfer.

1. Introduction

Circulant graphs have a vast number of uses and applications to telecommunication network, VLSI design, parallel and distributed computing (see Ref. 6 and references therein).

A graph is integral if all the eigenvalues of its adjacency matrix are integers (see Ref. 2 for a survey on integral graphs).

Here, we first show that the evolution of a quantum system, whose hamiltonian is identical to the adjacency matrix of a circulant graph, is periodic if and only if the graph is integral. Then, motivated by this observation, we focus on relevant properties of integral circulant graphs.

The intention of the paper is to move a step towards a classification of network topologies which exhibit periodic quantum dynamics. For certain quantum spin systems with fixed nearest-neighbour couplings, periodicity is a necessary condition for *perfect state transfer*, that is, for transferring a quantum state between sites of the system, with the use of a *free* evolution and without dissipating the information content of the state (see Ref. 3, for more information on this topic).

It is useful to study certain parameters of graphs that allow periodic dynamics, having in mind applications like perfect state transfer. Specifically, it is interesting to know *how far* information can be potentially transferred between sites of the system modeled by the graph. So, it is interesting to know the length of the longest geodesic in the graph, or, in other words, the *diameter* of the graph. Since many vertices means many particles and harder control, for the purpose of information transfer, a *good* network will have large diameter and a small number of vertices. Although path graphs would be the best candidates, it can be easily shown that these do not allow periodic dynamics and that one needs to add more and more vertices for constructing graphs with the desired dynamical properties. This is why we focus on order and diameter of integral circulant graphs.

The main mathematical results of the paper are the following:

- we bound the order of connected integral circulant graphs as a function of the degree (Sec. 4, Theorem 2);
- we characterize bipartite integral circulant graphs (Sec. 5, Theorem 3);
- we prove tight lower and upper bounds on the diameter of integral circulant graphs (Sec. 6, Theorems 4 and 5).

Given the properties of circulant graphs, the proofs are based on elementary number theory. In the last section, we show that circulant graphs with odd order do not allow perfect state transfer. However, we do not have a characterization of integral circulant graphs allowing perfect state transfer. This is left as an open problem.

2. Background on Circulant Graphs

A *graph* $\mathcal{G} = (V(\mathcal{G}), E(\mathcal{G}))$ is a pair whose elements are two sets, $V(\mathcal{G}) = \{1, 2, \ldots, n\}$ and $E(\mathcal{G}) \subset V(\mathcal{G}) \times V(G)$. The elements of $V(\mathcal{G})$ and $E(\mathcal{G})$ are called *vertices* and *edges*, respectively. We assume that $\{i, i\} \notin E(\mathcal{G})$ for all $i \in V(\mathcal{G})$. Two vertices i, j of a graph are said to be *adjacent* if $\{i, j\}$ is an edge; the edge $\{i, j\}$ is then *incident* with the vertices i, j.

The *adjacency matrix* of a graph $\mathcal{G}$ is the matrix $A(\mathcal{G})$ such that $A(\mathcal{G})_{i,j} = 1$ if $\{i, j\} \in E(\mathcal{G})$ and $A(\mathcal{G})_{i,j} = 0$ if $\{i, j\} \notin E(\mathcal{G})$. The *spectrum* of a graph $\mathcal{G}$ is the collection of eigenvalues of $A(\mathcal{G})$, or equivalently, the collection of zeros of the characteristic polynomial of $A(\mathcal{G})$; see Ref. 4. We denote by $\mathrm{sp}(\mathcal{G}) = (\lambda_0(\mathcal{G}), \ldots, \lambda_{n-1}(\mathcal{G}))$ the spectrum of a graph $\mathcal{G}$ in the non-increasing (with respect to modulus) ordering. We simply write $\lambda_0, \ldots, \lambda_{n-1}$ when $\mathcal{G}$ is clear from the context.

Let $S = \{s_1, s_2, \dots, s_k\}$ be a set of k integers in the range

$$1 \leq s_1, s_2, \dots, s_k < n.$$

Since we consider only *undirected graphs*, we assume that $s \in S$ if and only if $n - s \in S$.

A *circulant graph* $\mathcal{G} = G(n; S)$ is a graph on the set of n vertices $V(\mathcal{G}) = \{v_1, \dots, v_n\}$ with an edge incident with v_i and v_j whenever $|i - j| \in S$; see Ref. 6. The set S is said to be the *symbol* of $\mathcal{G}$. In particular, $k = \#S$ is the *degree* of a circulant graph $G(n; S)$.

Let $\mathbb{Z}_n$ denote the *residue ring* modulo n and let $\mathbb{Z}_n^*$ be the multiplicative group of $\mathbb{Z}_n$.

Notice that a circulant graph $G(n; S)$ is a *Cayley graph* of the additive group of $\mathbb{Z}_n$ with respect to the *Cayley set* S.

We recall that a Cayley graph with respect to a finite group $\mathfrak{G}$ and a set $S \subseteq \mathfrak{G}$, such that it contains $-w$ for every $w \in S$, is a graph on $n = \#\mathfrak{G}$ vertices, labeled by elements of $\mathfrak{G}$, where the vertices u and v are connected if and only if $u - v \in S$ (or equivalently, $v - u \in S$).

A *path* in a graph is a finite sequence of vertices which are connected by an edge. A *connected graph* is a graph such that there is a path between all pairs of vertices. It is easy to show that a circulant graph $G(n; S)$ with symbol $S = \{s_1, s_2, \dots, s_k\}$ is connected if and only if $\gcd(n, s_1, s_2, \dots, s_k) = 1$.

The adjacency matrix of a circulant graph is diagonalized by the Fourier transform at the irreducible representations over the group $\mathbb{Z}_n^*$ (which is a Vandermonde matrix). Lemma 1 is based on this observation.

Let $\omega_n = \exp(2\pi\iota/n)$, where $\iota = \sqrt{-1}$.

Lemma 1. *The spectrum of a circulant graph $\mathcal{G} = G(n; S)$ on n vertices with symbol S is*

$$\lambda_j = \sum_{s \in S} \omega_n^{js}, \tag{1}$$

where $0 \leq j \leq n - 1$.

By Lemma 1, the eigenvalues of a circulant graph are just the sum over S of the irreducible characters of $\mathbb{Z}_n^*$. The eigenvectors are also easily available. In fact, it is straightforward to see that the eigenvector corresponding to the eigenvalue λ_j has the form $v_j = [1, \omega^j, \dots, \omega^{j(n-1)}]^T$.

3. Integral Circulant Graphs and Periodic Quantum Dynamics

A *quantum spin system* associated to a graph $\mathcal{G}$ can be defined by attaching a spin-$\frac{1}{2}$ particle to each of the n vertices of $\mathcal{G}$. The Hilbert space assigned to the system is then $\mathcal{H} \cong (\mathbb{C}^2)^{\otimes n}$.

This system can be interpreted as a noiseless quantum channel, whose Hamiltonian is identical to the adjacency matrix of $\mathcal{G}$ itself. From another perspective, its evolution can be seen as a continuous-time quantum walk on $\mathcal{G}$. Some properties of such dynamics on circulant graphs have been studied in Ref. 1.

As observed in Ref. 3, the dynamics of the system is *periodic* if for every state $|\psi\rangle \in \mathcal{H}$, there exists $p \in \mathbb{R}$, $0 < p < \infty$, for which $|\langle\psi|e^{-\iota A(\mathcal{G})p}|\psi\rangle| = 1$. The number p is the *period* of the system.

In general, assuming that the initial state was $|\psi(0)\rangle = \sum_j \alpha_j|\lambda_j\rangle$, we can express as follows the state of the system at generic time t:

$$|\psi(t)\rangle = e^{-\iota H_G t}|\psi(0)\rangle = \sum_j \alpha_j e^{-\iota t\lambda_j}|\lambda_j\rangle,$$

where $|\lambda_j\rangle$ is an eigenvector of $A(\mathcal{G})$ with eigenvalue λ_j and $\alpha_j \in \mathbb{C}$. Thus, the periodicity condition $|\psi(t)\rangle = e^{-\iota\phi}|\psi(0)\rangle$ (ϕ is a phase) gives us that for every $\lambda_j \in \mathrm{sp}(G)$ we have:

$$\lambda_j t - \phi = 2\pi r_j, \quad \text{for some } r_j \in \mathbb{Z}.$$

Therefore, for every quadruple $\lambda_i, \lambda_j, \lambda_r, \lambda_s \in \mathrm{sp}(G)$ (with $\lambda_r \neq \lambda_s$), it follows that

$$\frac{\lambda_i - \lambda_j}{\lambda_r - \lambda_s} \in \mathbb{Q}. \tag{2}$$

We now show that Eq. (1) implies the integrality of the underlying graph.

Theorem 1. *Let $\mathcal{G} = G(n; S)$ be a circulant graph on $n \geq 4$ vertices with symbol S. If $\mathcal{G}$ has at least four distinct eigenvalues and all of them satisfy the condition* (2) *then $\mathcal{G}$ is integral.*

Proof. Let $k = \#S$ be the degree of $\mathcal{G}$. By Lemma 1, $\lambda_0 = k$. It is clear then that $\lambda_1, \ldots, \lambda_{n-1}$ are all different from λ_0. If $\mathrm{sp}(\mathcal{G})$ satisfies (2), then for all $i \in \{1, \ldots, n-1\}$, we have

$$\frac{\lambda_i - k}{\lambda_1 - k} \in \mathbb{Q}.$$

Therefore, $\lambda_i = a_i\lambda_1 + b_i$ for some $a_i, b_i \in \mathbb{Q}$.

We now show that $\lambda_1 \in \mathbb{Q}$. For this we consider three cases:

Case 1. Suppose $n = p$, a prime.

Then the minimal polynomial of ω_n over $\mathbb{Q}$ is $1 + X + \cdots + X^{n-1}$. Since $\mathcal{G}$ has at least four distinct eigenvalues we can find $2 \leq j < h \leq (n-1)$ such that λ_0, λ_1, λ_j and λ_h are all distinct.

Suppose that $\lambda_1 \notin \mathbb{Q}$. From Eq. (1), we have that $\lambda_j = a_j\lambda_1 + b_j$ for some $a_j, b_j \in \mathbb{Q}$. Applying (1), we get

$$\sum_{s\in S} \omega_n^{js} = a_j \sum_{s\in S} \omega_n^s + b_j.$$

In the last identity we can replace each exponent js with its smallest positive residue $r_{j,s}$ modulo n, which in turn means the following divisibility of polynomials

$$1 + X + \cdots + X^{n-1} \Big| \sum_{s\in S} X^{r_{j,s}} - a_j \sum_{s\in S} X^s - b_j.$$

Since the nonzero polynomial on the right-hand side is of degree at most $n-1$ and since $\lambda_1 \neq \lambda_j$, we obtain

$$1 + X + \cdots + X^{n-1} = \sum_{s\in S} X^{r_{j,s}} - a_j \sum_{s\in S} X^s - b_j,$$

which implies $-a_j = -b_j = 1$. Thus, $\lambda_j = -\lambda_1 - 1$. Applying the same argument on λ_h we get, $\lambda_h = -\lambda_1 - 1$, thus implying $\lambda_h = \lambda_j$. This contradiction shows that $\lambda_1 \in \mathbb{Q}$ in this case.

Case 2. Suppose $n = p^r$, a power of a prime p, where $r \geq 2$.

Now focus on the set of eigenvalues:

$$\{\lambda_{p^{r-1}}, \lambda_{2p^{r-1}}, \ldots, \lambda_{(p-1)p^{r-1}}\}.$$

Suppose that $\lambda_1 \notin \mathbb{Q}$. Clearly, $\lambda_{p^{r-1}}$ cannot be rational (otherwise $\lambda_1 \in \mathbb{Q}$). The above eigenvalues can be described as:

$$\lambda_{ip^{r-1}} = \sum_{s\in S} \omega_n^{ip^{r-1}s} = \sum_{s\in S} \omega_p^{is}.$$

Thus, this case now reduces to the prime case above and shows that λ_1 is rational.

Case 3. Suppose n has two distinct prime factors p, q.

We have that for all $i \in \{1, \ldots, n-1\}$, $\lambda_i = a_i\lambda_1 + b_i$, for some $a_i, b_i \in \mathbb{Q}$. Thus,

$$\mathbb{Q}(\lambda_1) = \cdots = \mathbb{Q}(\lambda_{n-1}). \tag{3}$$

Observe that $\lambda_{n/p} \in \mathbb{Q}(\omega_p)$ and $\lambda_{n/q} \in \mathbb{Q}(\omega_q)$. But Eq. (3) implies that $\lambda_{n/p} \in \mathbb{Q}(\lambda_{n/q})$. Thus, $\lambda_{n/p} \in \mathbb{Q}(\omega_p) \cap \mathbb{Q}(\omega_q)$. It can be shown that $\mathbb{Q}(\omega_p) \cap \mathbb{Q}(\omega_q) = \mathbb{Q}$ since p, q are coprime. Thus, $\lambda_{n/p} \in \mathbb{Q}$ and then Eq. (3) forces $\lambda_1 \in \mathbb{Q}$.

Thus, in all the cases $\lambda_1 \in \mathbb{Q}$ and hence all the n eigenvalues are rational. Since they are also algebraic integers, this further implies the desired result. □

It is plausible that the method of proof of Theorem 1 can be extended to other classes of Cayley graphs.

In the light of Theorem 1, in the next sections we consider parameters of circulant integral graphs. Before doing that, we now give a characterization of these graphs, which is due to So (Ref. 9), (and which is naturally based on Lemma 1). This is our main technical tool.

Let

$$G_n(d) = \{k \,|\, 1 \leq k \leq n-1, \gcd(k,n) = d\}$$

be the set of all integers less than n having the same greatest common divisor d with n. In particular, $\#G_n(d) = \varphi(n/d)$, where, as usual,

$$\varphi(m) = \#\{1 \le s \le m \,|\, \gcd(s, m) = 1\}$$

denotes the Euler totient function of a positive integer m (see, for example, Ref. 5).

Notice that the collection $\{G_n(d) \mid d \text{ divides } n\}$ is a partition of the set $\{1, 2, \ldots, n-1\}$. Notice that $k \in G_n(d)$ if and only if $n - k \in G_n(d)$, since $\gcd(k, n) = \gcd(n - k, n)$.

Let D_n be the set of all $(\tau(n) - 1)$ divisors $d \mid n$ with $d \le n/2$, where, as usual, $\tau(n)$ is the number of positive integer divisors of n.

Lemma 2. *A circulant graph $\mathcal{G} = G(n; S)$ on n vertices with symbol S is integral if and only if*

$$S = \bigcup_{d \in D} G_n(d) \tag{4}$$

for some set of divisors $D \subseteq D_n$.

Throughout the paper, the implied constants in the symbols "O", "$\ll$" and "$\gg$" are absolute. We recall that $A \ll B$ and $B \gg A$ is equivalent to the statement that $A = O(B)$ for positive functions A and B.

4. Degree and Order

In this section, we prove an upper bound on the number of vertices of an integral circulant graph in terms of its degree.

Theorem 2. *There is an absolute constant $c > 0$ such that for any $k \ge 2$, the largest number $N(k)$ of vertices of an integral connected circulant graph $\mathcal{G} = G(n; S)$ having degree k is bounded by*

$$N(k) \le \exp(c\sqrt{k \log\log(k+2)} \log k).$$

Proof. By Lemma 2, we see that $S = \bigcup_{d \in D} G_n(d)$, for some set of divisors $D \subseteq D_n$. Therefore,

$$k = \#S = \sum_{f \in F} \varphi(f), \tag{5}$$

where $F = [n|d|d \in D]$.

Given that $\mathcal{G}$ is connected, we have $\gcd(\{d \,|\, d \in D\}, n) = 1$.

Noting that for any two divisors $f, F \mid n$ we have

$$\gcd(n/f, F) \ge \gcd(F/f, F) \ge F/f,$$

it is easy to prove by induction on m that for any sequence $f_1, \ldots, f_m$ of divisors of n, we have

$$\gcd(n/f_1, \ldots, n/f_m, n) \ge \frac{n}{f_1 \cdots f_m}.$$

Therefore

$$1 = \gcd(\{d \,|\, d \in D\}, n) = \gcd\left(\{n/f \,|\, f \in F\}, n\right) \geq n \prod_{f \in F} f^{-1},$$

which leads us to the bound

$$n \leq \prod_{f \in F} f. \tag{6}$$

We now recall the well-known bound that for some absolute constant $C > 0$,

$$\varphi(f) \gg \frac{f}{\log\log(f+2)} \tag{7}$$

(see Ref. 5, Theorem 328). Thus, we see from (5) that

$$\frac{f}{\log\log(f+2)} \ll k$$

for every $f \in F$, which obviously implies that

$$f \ll k \log\log(k+2).$$

Now, using this bound together with (7) and (5) again, we derive

$$k = \sum_{f \in F} \varphi(f) \gg \sum_{f \in F} \frac{f}{\log\log(f+2)} \gg \sum_{f \in F} \frac{f}{\log\log(k+2)}.$$

Thus, if we denote

$$\sigma = \sum_{f \in F} f,$$

then we have

$$\sigma \ll k \log\log(k+2). \tag{8}$$

Let $s = \#F$. Then, we deduce from (6) that

$$n \leq (\sigma/s)^s. \tag{9}$$

Since

$$\sigma = \sum_{f \in F} f \geq \sum_{j=1}^{s} j = \frac{s(s+1)}{2},$$

we see that

$$s \ll \sqrt{\sigma}. \tag{10}$$

Since the function $(\sigma/x)^x$ monotonically increases for $1 \leq x \leq \sigma/e$, we obtain from (8) and (9) that

$$n \leq \exp(O(\sqrt{\sigma} \log \sigma)),$$

and recalling (8), we conclude the proof. □

On the basis of the arguments used in the proof of Theorem 2, we can construct the following table, in which we list the maximum order of an integral circulant graph of fixed degree $k = 2, \dots, 11$ (this is the sequence A126857 in Ref. 8):

Degree k	Maximum Order $N(k)$
$2, 3$	6
$4, 5$	12
$6, 7$	30
$8, 9$	42
$10, 11$	120

Notice that the cycle with six vertices is the largest cycle with integral eigenvalues.

5. Bipartiteness

In this section, we characterize bipartite integral circulant graphs.

Let us denote by $\mu(m)$ the Möbius function of a positive integer m:

$$\mu(m) = \begin{cases} 0, & \text{if } m \text{ has repeated prime factors;} \\ 1, & \text{if } m = 1; \\ (-1)^k, & \text{if } m \text{ is a product of } k \text{ distinct primes.} \end{cases}$$

For a fixed k, there exists a set $F \subset \mathbb{N}$ such that we have (5). Writing

$$n = \operatorname{lcm}\{f \,|\, f \in F\}$$

and

$$S = \bigcup_{f \in F} G_n\left(\frac{n}{f}\right), \tag{11}$$

it is not hard to see that that the above defines an integral circulant graph $\mathcal{G} = G(n; S)$. As discussed in Ref. 9, the eigenvalues of $\mathcal{G} = G(n; S)$ are then: for $0 \le j \le n - 1$,

$$\lambda_j = \sum_{f \in F} \varphi(f) \cdot \frac{\mu\left(f/\gcd(f, j)\right)}{\varphi\left(f/\gcd\left(f, j\right)\right)}. \tag{12}$$

By (12), we can determine which integral circulant graphs are bipartite.

Theorem 3. *An integral circulant graph $\mathcal{G} = G(n; S)$ on n vertices with symbol S is bipartite if and only if n is even and $S = \cup_{f \in F} G_n(\frac{n}{f})$, where for some number ℓ_0, the set $\{2\ell_0/f \,|\, f \in F\}$ contains only odd integers.*

Proof. Having degree k, the graph $\mathcal{G}$ is bipartite if and only if it has an eigenvalue $\lambda_\ell = -k$; see Ref. 4.

Suppose $\mathcal{G}$ is bipartite. On the basis of (11) and (12),

$$\lambda_\ell = -k = \sum_{f \in F} \varphi\,(f) \cdot \frac{\mu\,(f/\gcd(f,\ell))}{\varphi\,(f/\gcd\,(f,\ell))}.$$

Given (5), the above equation can hold only if for every $f \in F$:

$$\frac{\mu\,(f/\gcd(f,\ell))}{\varphi\,(f/\gcd\,(f,\ell))} = -1.$$

This implies that

$$\mu\left(\frac{f}{\gcd(f,\ell)}\right) = -1 \quad \text{and} \quad \varphi\left(\frac{f}{\gcd\,(f,\ell)}\right) = 1, \tag{13}$$

whence

$$\frac{f}{\gcd(f,\ell)} \in \{1,2\}. \tag{14}$$

So, (13) together with (14) gives:

$$\frac{f}{\gcd\,(f,\ell)} = 2,$$

implying that for every $f \in F$ the ratio $2\ell/f$ is an odd integer.

Also, it follows that n is even as $n = \operatorname{lcm}\{f \,|\, f \in F\}$. Thus, the theorem is true in one direction.

Conversely, suppose that n is even and $2\ell_0/f$ is odd for every $f \in F$. Consequently, the ℓ_0th eigenvalue is:

$$\begin{aligned}\lambda_{\ell_0} &= \sum_{f \in F} \varphi(f) \cdot \frac{\mu(f/\gcd(f,\ell_0))}{\varphi(f/\gcd(f,\ell_0))} \\ &= \sum_{f \in F} \varphi(f) \cdot \frac{\mu(2)}{\varphi(2)} = \sum_{f \in F} \varphi(f) \cdot (-1) = -k.\end{aligned}$$

Thus, $\mathcal{G}$ is bipartite and the theorem is proved. □

6. Diameter

In this section, we prove tight lower and upper bounds on the diameter of integral circulant graphs.

The *diameter* of a graph $\mathcal{G}$, denoted by $\operatorname{diam} \mathcal{G}$, is the longest among the shortest paths between any two vertices. If $\mathcal{G}$ is a circulant graph on n vertices, then it is clear that $1 \leq \operatorname{diam} \mathcal{G} \leq n/2$.

For a given degree k, the number of vertices of an integral circulant graph $\mathcal{G}$ is $n = \operatorname{lcm}\{f \,|\, f \in F\}$, where F is as given in Eq. (5).

Assuming that the columns (and rows) of the adjacency matrix $A_\mathcal{G}$ of $\mathcal{G}$ are labeled from $0, \ldots, (n-1)$ then the first row of $A_\mathcal{G}$ is:

$$S = \bigcup_{f \in F} G_n\left(\frac{n}{f}\right) = \bigcup_{f \in F} \left\{ i \mid 1 \leq i \leq n,\ \gcd(i,n) = \frac{n}{f} \right\}.$$

A right shift of row S gives the subsequent rows of $A_{\mathcal{G}}$.

Let $X \subseteq \mathbb{Z}_n$ then, for a positive integer, we define

$$iX = \underbrace{X + \cdots + X}_{i \text{ times}} = \{x_1 + \cdots + x_i \mid x_1, \ldots, x_i \in X\}$$

(where the elements are added modulo n). Note that the vertices in $\mathcal{G}$ reachable from the vertex 0 in 1 step are exactly the vertices of S; the vertices reachable from the vertex 0 in 2 steps are those of $2S$, and so on. Similarly, if we define $T = S \cup \{0\}$ then the vertices reachable from the vertex 0 in i or smaller steps are iT. Thus, we have:

Lemma 3. *The diameter of the circulant graph $\mathcal{G} = G(n; S)$ is the least index i such that $iT = \mathbb{Z}_n$.*

Theorem 4. *Let D be a set of divisors of n such that $\gcd(D, n) = 1$ and let t be the size of the smallest set of additive generators of $\mathbb{Z}_n$ contained in D. Then, for the circulant graph $\mathcal{G} = G(n; S)$, where $S = \cup_{d \in D} G_n(d)$, we have*

$$t \leq \operatorname{diam} \mathcal{G} \leq 2t + 1.$$

Proof. It is very simple to show the lower bound. By the hypothesis, it is easy to see that t is the size of the smallest set of generators of $\mathbb{Z}_n$ contained in T. Thus, by Lemma 3, we deduce that $\operatorname{diam} \mathcal{G} \geq t$.

We now turn to the upper bound. Let $d_1, \ldots, d_t \in D$ be the additive generators of $\mathbb{Z}_n$. Without loss of generality, we can assume that d_1 is odd. Clearly, $\gcd(d_1, \ldots, d_t, n) = 1$. We intend to show that, given any $\ell \in \mathbb{Z}_n$, there exist $x_0, x_1, \ldots, x_{2t} \in (\mathbb{Z}_n)^*$ such that either

$$d_1 x_0 + d_1(x_1 + x_{t+1}) + \cdots + d_t(x_t + x_{2t}) \equiv \ell \pmod{n}$$

or

$$d_1(x_1 + x_{t+1}) + \cdots + d_t(x_t + x_{2t}) \equiv \ell \pmod{n}. \tag{15}$$

Note that this would mean that $(2t+1)T = \mathbb{Z}_n$. We now solve one of the above congruences modulo prime factors of n and then "lift" that solution modulo n.

If $2|n$, then we can put

$$x_0 \equiv x_1 \equiv \cdots \equiv x_{2t} \equiv 1 \pmod{2}$$

and then, depending on the parity of ℓ, one of the above equations, say (15), holds modulo 2. Suppose α_2 is the largest index of 2 dividing n. Then this solution can be Hensel lifted[7] to a solution $(x_0, \ldots, x_{2t})$ modulo 2^{α_2}.

Next, let p be an odd prime dividing n. Since $\gcd(d_1, \ldots, d_t, n) = 1$, without loss of generality, we can assume that $p \nmid d_1$. Now, we substitute

$$x_2 \equiv \cdots \equiv x_t \equiv 1 \equiv -x_{2+t} \equiv \cdots \equiv -x_{2t} \pmod{p}$$

and then (15) simply becomes

$$d_1(x_1 + x_{t+1}) \equiv \ell \pmod{p}$$

or

$$x_1 + x_{t+1} \equiv \ell \cdot d_1^{-1} \pmod{p}$$

and we can easily find nonzero values of x_1 and x_{t+1} modulo p. So we have a solution of Eq. (15) modulo p and it can be Hensel lifted to a solution modulo p^{α_p}, where α_p is the largest index of p dividing n.

Finally, the solutions of (15) modulo q^{α_q} for every prime $q|n$ can be combined using Chinese Remaindering to get a solution modulo n. □

It is natural to try to obtain bounds on the diameter of $\mathcal{G} = G(n; S)$ in terms of $\#D$. By the above, we have bounds

$$2 \leq \operatorname{diam} \mathcal{G} \leq 2\#D + 1.$$

The following result shows that in general no better bounds are possible.

Theorem 5. *The following statements are true for integral circulant graphs*:

(i) *For $r \geq 3$, let n be the product of distinct odd primes $p_1, \ldots, p_r$ and let $D = \{p_1, \ldots, p_r\}$. The graph corresponding to these parameters has diameter 2.*

(ii) *Let m be the product of distinct odd primes $p_1, \ldots, p_r$. Let $n = 2m^2$ and*

$$D = \{(m/p_1)^2, \ldots, (m/p_r)^2\}.$$

The graph corresponding to these parameters has diameter $(2r + 1)$.

Proof. (i) By the hypothesis $n = p_1 \cdots p_r$, $D = \{p_1, \ldots, p_r\}$. Recall that $T = \{0\} \cup_{d \in D} G_n(d)$. Let $\mathcal{G}$ be the corresponding graph. We show that given any $\ell \in \mathbb{Z}_n$, we have $\ell \in T + T$.

Suppose ℓ is coprime to n. Then, using the methods of Theorem 4, we can find a solution $x_1, x_2 \in \mathbb{Z}_n^*$, such that $p_1 x_1 + p_2 x_2 \equiv \ell \pmod{n}$. Thus, $\ell \in T + T$. If ℓ is not coprime to n, then without loss of generality, we can assume that $p_1|\ell$. Again, using the methods of Theorem 4, we can find a solution $x_1,\ x_2 \in \mathbb{Z}_n^*$ such that $p_1 x_1 + p_1 x_2 \equiv \ell \pmod{n}$. Thus, $\ell \in T + T$.

Therefore, $T + T = \mathbb{Z}_n$. As the smallest additive generator set contained in D is of size 2, we deduce from Lemma 3 that $\operatorname{diam} \mathcal{G} = 2$.

(ii) We recall that $T = \{0\} \cup_{d \in D} G_n(d)$. Let $\mathcal{G}$ be the corresponding graph. We show that $m \notin 2rT$.

Suppose that $m \in 2rT$. This means that there are

$d_1, \ldots, d_{2r} \in D$ such that $m \in G_n(d_1) + \cdots + G_n(d_{2r})$. Since $p_j^2 \nmid m$, we deduce that $(m/p_j)^2 \in \{d_1, \ldots, d_{2r}\}$, $j = 1, \ldots, r$.

Without loss of generality, we can assume that $d_1 = (m/p_1)^2, \ldots, d_r = (m/p_r)^2$. In other words, there are $x_1, \ldots, x_{2r} \in \mathbb{Z}_n^*$ such that

$$\frac{m^2}{p_1^2} x_1 + \cdots + \frac{m^2}{p_r^2} x_r + d_{r+1} x_{r+1} + \cdots + d_{2r} x_{2r} \equiv m \pmod{n}. \tag{16}$$

Taking the above congruence modulo p_1, we deduce that

$$\frac{m^2}{p_1^2} x_1 + d_{r+1} x_{r+1} + \cdots + d_{2r} x_{2r} \equiv 0 \pmod{p_1}.$$

As $\gcd(x_1, p_1) = 1$, the above congruence implies $(m/p_1)^2 \in \{d_{r+1}, \ldots, d_{2r}\}$. Similarly, taking (16) modulo primes $p_2, \ldots, p_r$ and repeating the argument we deduce

$$(m/p_1)^2, \ldots, (m/p_r)^2 \in \{d_{r+1}, \ldots, d_{2r}\}.$$

Without loss of generality, we can assume that

$$d_{r+1} = \frac{m^2}{p_1^2}, \ldots, d_{2r} = \frac{m^2}{p_r^2}.$$

Thus, the congruence (16) becomes

$$\frac{m^2}{p_1^2}(x_1 + x_{r+1}) + \cdots + \frac{m^2}{p_r^2}(x_r + x_{2r}) \equiv m \pmod{n}.$$

Recall that $x_1, \ldots, x_{2r}$ are coprime to n. So, looking at the above equation modulo 2, we deduce $m \equiv 0 \pmod 2$, which is a contradiction as m is odd.

This shows that $m \notin 2rT$ and hence $\operatorname{diam} \mathcal{G} > 2r$. Since the smallest additive generator set of $\mathbb{Z}_n$ in D is of size r, by Theorem 4, we have that $\operatorname{diam} \mathcal{G} = 2r + 1$. □

7. Conclusion

We have proved that a quantum system whose hamiltonian is identical to the adjacency matrix of a circulant graph is periodic if and only if the graph is integral.

We have bounded the number of vertices of integral circulant graph in terms of their degree, characterized bipartiteness and given exact bounds for the diameter.

It is a natural problem to extend Theorems 1, 3 and 4 to other classes of Cayley graphs, for example, Cayley graphs of Abelian groups.

We conclude with a partial result about perfect state transfer. We say that there is *perfect state transfer* (see Ref. 3) in a graph $\mathcal{G}$ between the vertices a and vertices b if there is $0 < t < \infty$, such that

$$|\langle a| e^{-\iota A(\mathcal{G})t} |b\rangle| = 1.$$

For an integral circulant graph $\mathcal{G} = G(n; S)$, we have the following setting: for all $0 \le j \le n-1$, $v_j = [1, \omega^j, \ldots, \omega^{j(n-1)}]^T$ is an eigenvector of $A(\mathcal{G})$ corresponding to the eigenvalue λ_j given by (1). Thus,

$$A(\mathcal{G}) = \frac{1}{n}\sum_{j=0}^{n-1} \lambda_j v_j v_j^\dagger.$$

We have then the next question: are there $0 \le a, b \le (n-1)$ and $t \in \mathbb{R}$ such that $|\langle a|e^{-iA(\mathcal{G})t}|b\rangle| = 1$?

Proposition 1. *If n is odd then there do not exist $0 \le a < b \le (n-1)$ and $t \in \mathbb{R}^{>0}$ such that $|\left\langle a|e^{\iota At}|b\right\rangle| = 1$. In other words, an integral circulant graph having odd number of vertices cannot have perfect state transfer.*

Proof. Recall

$$e^{\iota At} = \frac{1}{n}\sum_{\ell=0}^{n-1} e^{\iota\lambda_\ell t} v_\ell v_\ell^\dagger.$$

Therefore,

$$\begin{aligned}\langle a|e^{\iota At}|b\rangle &= \frac{1}{n}\sum_{\ell=0}^{n-1} e^{\iota\lambda_\ell t}\omega^{\ell a}\omega^{-\ell b}\\ &= \frac{1}{n}\sum_{\ell=0}^{n-1} e^{\iota\lambda_\ell t}\omega^{\ell(a-b)}.\end{aligned}$$

Now, the magnitude of the above expression is clearly ≤ 1. The equality holds if and only if each term is 1 implying that $e^{\iota\lambda_\ell t} = \pm 1$ and $\omega^{\ell(a-b)} = \pm 1$ for all ℓ. Now if n is odd then $\omega^{\ell(a-b)} = \pm 1$ happens only when $a \equiv b \pmod{n}$. Thus, there is no perfect state transfer when n is odd. □

When n is even there is perfect state transfer (between vertices a and $a + \frac{n}{2}$) if there exists a $t \in \mathbb{R}^{>0}$ such that $e^{\iota\lambda_\ell t} = (-1)^\ell$ for all $\ell \in \{0, \ldots, n-1\}$. For example, this happens in the case of $n = 4$ and $S = \{1, 3\}$. However, we do not know whether there are other such instances.

Acknowledgments

Part of this work has been carried out while S. Severini was visiting CWI. This was possible thanks to the financial support of CWI and the kind hospitality of Harry Buhrman. The authors would like to thank Harry Buhrman, Ronald de wolf, Leong-Chuan Kwek and Ben Toner for interesting discussions concerning the subject of this paper.

References

1. A. Ahmadi, R. Belk, C. Tamon and C. Wendler, On mixing of continuous-time quantum walks on some circulant graphs, *Quant. Inform. Comput.* **3** (2003) 611–618.

2. K. Balińska, D. Cvetković, Z. Radosavljević, S. Simić and D. Stevanović, A survey on integral graphs, *Univ. Beograd. Publ. Elektrotehn. Fak. Ser. Mat.* **13** (2003) 42–65.
3. M. Christandl, N. Datta, A. Ekert and A. J. Landahl, Perfect state transfer in quantum spin networks, *Phys. Rev. Lett.* **92** (2004) 187902 [quant-ph/0309131].
4. D. Cvetković, M. Doob and H. Sachs, *Spectra of Graphs — Theory and Application* (Academic Press, New York, 1980).
5. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn. (Clarendon Press, Oxford University Press, New York, 1979).
6. F. K. Hwang, A survey on multi-loop networks, *Theor. Comput. Sci.* **299**(1–3) (2003) 107–121.
7. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications* (Cambridge University Press, 1986).
8. N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, www.research.att.com/njas/sequences/ (2006).
9. W. So, Integral circulant graphs, *Discrete Math.* **306** (2006) 153–158.