Perfect state transfer between non-antipodal vertices in integral circulant graphs

Milan Bašić

Faculty of Sciences and Mathematics, University of Niš,

Višegradska 33, 18000 Niš, Serbia

E-mail: basic_milan@yahoo.com

Abstract

In this paper we investigate the existence of perfect state transfer in integral circulant graphs between non-antipodal vertices-vertices that are not at the diameter of a graph. Perfect state transfer is considered on circulant quantum spin networks with nearest-neighbor couplings. The network is described by a circulant graph G, which is characterized by its circulant adjacency matrix A. Formally, we say that there exists *perfect state transfer* (PST) between vertices $a, b \in V(G)$ if $|F(\tau)_{ab}| = 1$, for some positive real number τ, where $F(t) = \exp(\imath At)$. Saxena, Severini and Shparlinski (*International Journal of Quantum Information* 5 (2007), 417–430) proved that $|F(\tau)_{aa}| = 1$ for some $a \in V(G)$ and $\tau \in \mathbb{R}^+$ if and only if all the eigenvalues of G are integer (that is, the graph is integral). The integral circulant graph $\mathrm{ICG}_n(D)$ has the vertex set $Z_n = \{0, 1, 2, \dots, n-1\}$ and vertices a and b are adjacent if $\gcd(a - b, n) \in D$, where $D \subseteq \{d : d \mid n,\ 1 \leq d < n\}$. We characterize completely the class of integral circulant graphs having PST between non-antipodal vertices for $|D| = 2$. We have thus answered the question posed by Godsil on the existence of classes of graphs with PST between non-antipodal vertices. Moreover, for all values of n such that $\mathrm{ICG}_n(D)$ has PST ($n \in 4\mathbb{N}$), several classes of graphs $\mathrm{ICG}_n(D)$ are constructed such that PST exists between non-antipodal vertices.

AMS Subj. Class.: 05C12, 05C50

Keywords: Circulant graphs; Integral graphs; Perfect state transfer; Cayley graphs; Diameter.

1 Introduction

The transfer of a quantum state from one location to another is a crucial ingredient for many quantum information processing protocols. There are various physical systems that can serve as quantum channels, one of them being a quantum spin network. These networks consist of n qubits where some pairs of qubits are coupled via XY-interaction. The perfect transfer of quantum states from one qubit to another in such networks was first considered in [9]. There are two special qubits A and B representing the input and output qubit, respectively. The transfer is implemented by setting the qubit A in a prescribed quantum state and by retrieving the state from the output qubit B after some time. The transfer is called *perfect state transfer* (transfer with unit fidelity) if the initial state of the qubit A and the final state of the qubit B are equal up to a local phase rotation.

Every quantum spin network with fixed nearest-neighbor couplings is uniquely described by an undirected graph G on a vertex set $V(G) = \{1, 2, \dots, n\}$. The edges of the graph G specify which qubits are coupled. In other words, there is an edge between vertices i and j if i-th and j-th qubit are coupled.

In [9] a simple XY coupling is considered such that the Hamiltonian of the system has the form

$$H_G = \frac{1}{2} \sum_{(i,j)\in E(G)} \sigma_i^x \sigma_j^x + \sigma_i^y \sigma_j^y.$$

and σ_i^x, σ_i^y and σ_i^z are Pauli matrices acting on i-th qubit. The standard basis chosen for an individual qubit is $\{|0\rangle, |1\rangle\}$ and it is assumed that all spins initially point down ($|0\rangle$) along the prescribed z axis. In other words, the initial state of the network is $|\underline{0}\rangle = |0_A 0 \dots 0 0_B\rangle$. This is an eigenstate of Hamiltonian H_G corresponding to zero energy. The Hilbert space $\mathcal{H}_G$ associated with a network is spanned by the vectors $|e_1 e_2 \dots e_n\rangle$ where $e_i \in \{0, 1\}$ and, therefore, its dimension is 2^n.

The process of transmitting a quantum state from A to B begins with the creation of the initial state $\alpha|0_A 0 \dots 0 0_B\rangle + \beta|1_A 0 \dots 0 0_B\rangle$ of the network. Since $|\underline{0}\rangle$ is a zero-energy eigenstate of H_G, the coefficient α will not change in time. Since the operator of total z component of the spin $\sigma_{tot}^z = \sum_{i=1}^n \sigma_i^z$ commutes with H_G, state $|1_A 0 \dots 0 0_B\rangle$ must evolve into a superposition of the states $|i\rangle = |0 \dots 0 1_i 0, \dots, 0\rangle$ for $i = 1, \dots, n$. Denote by $\mathcal{S}_G$ the subspace of $\mathcal{H}_G$ spanned by the vectors $|i\rangle$, $i = 1, \dots, n$. Hence, the initial state of network evolves in time t into the state

$$\alpha|\underline{0}\rangle + \sum_{i=1}^{n} \beta_i(t)|i\rangle \in \mathcal{S}_G.$$

The previous equation shows that system dynamics is completely determined by the evolution in n-dimensional space $\mathcal{S}_G$. The restriction of the Hamiltonian H_G to the subspace $\mathcal{S}_G$ is an $n \times n$ matrix identical to the adjacency matrix A_G of the graph G.

Thus, the time evolution operator can be written in the form $F(t) = \exp(\imath A_G t)$. The matrix exponential $\exp(M)$ is defined as usual

$$\exp(M) = \sum_{n=0}^{+\infty} \frac{1}{n!} M^n.$$

Perfect state transfer (PST) between different vertices (qubits) a and b ($1 \leq a, b \leq n$) is obtained in time τ, if $\langle a|F(t)|b\rangle = |F(\tau)_{ab}| = 1$. The graph (network) is *periodic* at a if $|F(\tau)_{aa}| = 1$ for some τ. A graph is *periodic* if it is periodic at each vertex a.

The existence of PST for some network topologies has already been considered in the literature. For example, PST occurs in paths of length one and two between their end-vertices and also in Cartesian powers of these graphs between vertices at maximal distance [10]. In the recent paper [13], Godsil constructed a class of distance-regular graphs of diameter three, with PST. Furthermore, some properties of quantum dynamics on circulant graphs were studied in [1]. In the recent papers [2, 21, 23], PST on circulant networks were examined and the main result is that there exists an integral circulant graph with n vertices having PST if and only if $4 \mid n$. Several classes of integral circulant graphs having PST were found as well and several others in [7]. In all known classes of graphs having PST *perfect quantum communication distances* (i.e. the distances between vertices where PST occurs) are considerably small compared to the order of the graph. One idea for the distance enlargement, is to consider networks with fixed but different couplings between qubits. These networks correspond to graphs with weighted adjacency matrices. For example, in [9, 10] the authors showed that PST can be achieved over arbitrarily long distances in a weighted linear paths. Many recent papers have proposed such an approach [7, 8, 19].

Studying PST in integral circulant graphs can also be interpreted as a contribution to the spectral theory of integral graphs. These graphs are highly symmetric and have some remarkable properties connecting graph theory and number theory. Integral circulant graphs found important applications in molecular chemistry [16, 18, 22]. The term 'integral circulant graph' first appears in the work of So [25], where a nice characterization of these graphs in terms of their symbol set is given. Various other properties of unitary Cayley graphs were recently investigated, such as the diameter, the size of the longest cycle, clique, chromatic number, bipartiteness ([2, 6, 17, 20, 23]).

In this paper we proceed with the study of circulant networks supporting PST initiated in [3, 4, 7, 13, 21, 23, 24]. Having in mind applications to PST, it is useful to study certain parameters of graphs that allow periodic dynamics. Specifically, it would be interesting to know how far information can potentially be transferred between sites of the system modelled by the graph. So, it is important to know the diameter of the graph and the perfect quantum communication distance. Especially, it is interesting to know if the perfect quantum communication distance is always equal to the diameter of a graph. In other words, are the involved vertices of a graph where PST exists, always antipodal? This question was posed by Godsil in [13] and we give negative answer to the question by characterizing all integral circulant graphs with a two element set of divisors having PST.

The plan of the paper is as follows. In Sections 2 and 3 we give formal mathematical definitions of integral circulant graphs and perfect state transfer. We also restate some results concerning the study of perfect state transfer in integral circulant graphs. In Section 4, the diameter of integral circulant graphs with one divisor is determined. This result is essential in calculating the diameter of integral circulant graphs with two divisors, which is performed in Section 5. We have also characterized all integral circulant graphs with a two element set of divisors having PST , and we have found two classes of graphs where PST occurs between non-antipodal vertices. These classes of integral circulant graphs are of the order divisible by eight. Furthermore, we have also found a class of integral circulant graphs with order in the set $8\mathbb{N}+4$. This way we prove that for any $n \in 4\mathbb{N}$ there is an integral circulant graph of order n such that PST occurs between non-antipodal vertices. Notice that PST exists in integral circulant graphs if the order of a graph is divisible by four. A class of integral circulant graphs of order $n \in 8\mathbb{N} + 4$ such that PST occurs between antipodal vertices is also found.

2 Integral circulant graphs

The *circulant graph* $G(n; S)$ is a graph on vertices $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ such that each vertex i is adjacent to vertices $i +_n s$ for all $s \in S$. The set $S \subseteq \mathbb{Z}_n$ is called the *symbol set* of the graph $G(n; S)$ and $+_n$ denotes addition modulo n. Note that the degree of $G(n; S)$ is $\#S$. A graph is *integral* if all its eigenvalues are integers. Wasin So has characterized integral circulant graphs [25] by the following theorem:

Theorem 1 [25] *A circulant graph $G(n; S)$ is integral if and only if*

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

for some set of divisors $D \subseteq D_n$. Here $G_n(d) = \{k \ : \ \gcd(k, n) = d, \ 1 \leq k \leq n-1\}$, and D_n is the set of all divisors of n, different from n.

Therefore an *integral circulant graph* $G(n; S)$ is defined by its order n and the set of divisors D. Such graphs are also known as *gcd-graphs* (see for example [20]). An integral circulant graph with n vertices, defined by the set of divisors $D \subseteq D_n$ will be denoted by $\mathrm{ICG}_n(D)$. Here, for the symbol set S of $\mathrm{ICG}_n(D)$ we use the notation from Theorem 1 and denote it by $G_n(D)$. From Theorem 1 we have that the degree of an integral circulant graph is $\deg \mathrm{ICG}_n(D) = \sum_{d \in D} \varphi(n/d)$. Here $\varphi(n)$ denotes the Euler-phi totient function [14].

The eigenvalues and eigenvectors of $\mathrm{ICG}_n(D)$ are given in [23] and can be expressed in terms of the *Ramanujan function* (see [14, p. 55] and [20], Theorem 16).

The integral circulant graph $\mathrm{ICG}_n(D)$ is connected if and only if

$$\gcd(n, d_1, \ldots, d_k) = 1,$$

where $D = \{d_1, \ldots, d_k\}$ [15]. In the rest of the paper we will only consider connected integral circulant graphs.

3 Perfect state transfer

Let G be an undirected graph and denote by A_G its adjacency matrix. Let $F(t) = \exp(iA_G t)$. There is a *perfect state transfer* (PST) in graph G if there are distinct vertices a and b and a positive real number t such that $|F(t)_{ab}| = 1$ [9, 13, 23].

Let $\lambda_0, \lambda_2, \ldots, \lambda_{n-1}$ be the eigenvalues (not necessarily distinct) of A_G and $u_0, u_1, \ldots, u_{n-1}$ be the corresponding normalized eigenvectors. We use spectral decomposition of the real symmetric matrix A_G (see for example [12] (Theorem 5.5.1) for more details). The matrix function $F(t)$ can be represented as

$$F(t) = \sum_{k=0}^{n-1} \exp(\imath \lambda_k t) u_k u_k^*. \tag{1}$$

Now let $G = \mathrm{ICG}_n(D)$ be an integral circulant graph. By simple calculation and using the formula of eigenvalues, we see that $\|v_k\| = \sqrt{n}$ and hence $u_k = v_k / \sqrt{n}$. Expression (1) now becomes

$$F(t) = \frac{1}{n} \sum_{k=0}^{n-1} \exp(\imath \lambda_k t) v_k v_k^*.$$

In particular, from the last expression and the formula of eigenvectors it directly follows

$$F(t)_{ab} = \frac{1}{n} \sum_{k=0}^{n-1} \exp(\imath \lambda_k t) \omega_n^{k(a-b)}.$$

This expression is given in [23] (Proposition 1). Finally, our goal is to check whether there exist distinct integers $a, b \in \mathbb{Z}_n$ and a positive real number t such that $|F(t)_{ab}| = 1$, i.e.

$$\left| \frac{1}{n} \sum_{k=0}^{n-1} \exp(\imath \lambda_k t) \omega_n^{k(a-b)} \right| = 1. \tag{2}$$

Since the left-hand side of (2) depends on a and b only as a function of $a - b$ we can, without any loss of generality, assume that $b = 0$. Therefore, throughout the paper we consider the existence of PST only between vertices a and 0.

We restate some results proved in [4]. These results establish necessary and sufficient conditions for (2).

Theorem 2 [4] *There is no PST in* $\mathrm{ICG}_n(D)$ *if* n/d *is odd for every* $d \in D$*. For* n *even, if there exists PST in* $\mathrm{ICG}_n(D)$ *between vertices* a *and* 0*, then* $a = n/2$*.*

According to Theorem 2, PST may exist in $\mathrm{ICG}_n(D)$ only between vertices $n/2$ and 0 (i.e., between b and $n/2+b$ as mentioned in [23]). Hence we will avoid referring to the input and output vertex and will just say that there exists PST in $\mathrm{ICG}_n(D)$.

Theorem 3 [5] *An integral circulant graph* $\mathrm{ICG}_n(D)$*, where* D *has exactly two divisors, has PST if and only if* $S_2(n) \geq 3$ *and* $D = \{1, n/2\}$*,* $D = \{1, n/4\}$ *.*

We end this section with the following results concerning nonexistence of PST in $\mathrm{ICG}_n(D)$ for $n \in 4\mathbb{N}+2$ and existence of PST in $\mathrm{ICG}_n(D)$ for $n \in 4\mathbb{N}$.

Theorem 4 [21] *There is no PST in* $\mathrm{ICG}_n(D)$ *for an arbitrary set of divisors* D *for* $n \in 4\mathbb{N}+2$*.*

Theorem 5 [21] *Let* n *be a positive integer such that* $S_2(n) = 2$*. Then graphs* $\mathrm{ICG}_n(1,2,4,n/4)$ *and* $\mathrm{ICG}_n(1,2,4,n/2)$ *have PST.*

4 The diameter of integral circulant graphs with one divisor

The distance $d(u,v)$ between two vertices u and v of a graph is the minimum length of the paths connecting them (i.e., the length of a graph geodesic between u and v). The diameter of a graph is the maximum distance of any pair of vertices in the graph.

Definition 1 *Let* l *and* N *be given integers. If there exist integers* $s_1, s_2, \ldots s_k$ *with* $gcd(s_i, N) = 1$*, for* $1 \leqslant i \leqslant k$*, and* $l \equiv s_1 + s_2 + \ldots + s_k \pmod{N}$ *then the k-tuple* $(s_1, s_2, \ldots, s_k)$ *is called a reduced decomposition of* l *modulo* N *(*$RD_N(l)$*) on* k *elements.*

Lemma 6 *For any positive integers* m *and* l *such that* $l < m$ *and* $gcd(l,m) = 1$*, the following conditions hold:*

(i) There exists $RD_m(l)$ *on three elements.*

(ii) If m *is odd then there exists* $RD_m(l)$ *on two elements.*

(iii) If m *is even there is no* $RD_m(l)$ *on two elements.*

Proof.
(i) Since $gcd(l,m) = 1$ it follows that $gcd(m-l, m) = 1$ and thus we have $l \equiv (m-l) + l + l \pmod{m}$.

(ii) If m is odd then $gcd(2l, m) = 1$ and thus $l \equiv (m - l) + 2l \pmod{m}$.

(iii) Suppose that there are two element $RD_m(l)$. This means that there exist integers a and b both relatively prime to m and $l \equiv a + b \pmod{m}$. As m is an even integer, the last equation yields that $l - a - b$ is also even. On the other hand, since a, b and l are relatively prime to m, they are all odd and thus $l - a - b \in 2\mathbb{N} + 1$, which leads to a contradiction. □

Lemma 7 *Let $m = p^\alpha$, where p is a prime number and $\alpha > 1$. For any positive integer $l < m$ divisible by p, there exists $RD_m(l)$ on two elements and for $p > 2$ there is $RD_m(l)$ on three elements.*

Proof. The numbers m and $m - 1$ are relatively prime and for $p > 2$ the number $m - 2$ is not divisible by p. Under the conditions of the lemma, both $((m - 1), 1)$ and $((m - 2), 1, 1)$ represent $RD_m(l)$ on two and three elements, respectively. □

Lemma 8 *For any positive integer l less than a given positive integer N, there is $RD_N(l)$ of at most three elements.*

Proof.
(i) Let N be a prime number. Since all integers smaller than N are relatively prime to N, each of them trivially satisfies the assertion of the lemma.

(ii) Now let $N = p^\alpha$ for an arbitrary prime number $p \geq 2$ and $\alpha > 1$. Then for all numbers not relatively prime to N there is $RD_N(l)$ on two elements by Lemma 7.

(iii) Suppose that $N = nm$, where $n, m > 1$ are relatively prime integers. Also assume $m = p^\alpha$ for an odd prime p and $\alpha \geq 1$. Consider the congruent classes modulo m, $C_i = \{tm + i \mid 0 \leqslant t \leqslant n - 1\}$ for $0 \leqslant i \leqslant m - 1$.

The proof is further carried out using induction on N. For $N = p^\alpha$ where p is prime, the assertion holds according to part (i) and (ii) of the proof. Suppose the assertion holds for all $n < N$.

Consider an arbitrary class C_k for $0 \leqslant k \leqslant m - 1$. By the assumption, for each element $l \in C_k$ we have that there exists an integer $1 \leqslant x \leqslant 3$ such that

$$l \equiv s_1 + s_2 + \cdots + s_x \pmod{n}, \tag{3}$$

and $gcd(s_i, n) = 1$ for $1 \leqslant i \leqslant x$.

In the case where $2 \leqslant x \leqslant 3$ according to Lemma 6 (parts (i) and (ii)) and Lemma 7 there exist numbers $r_1, r_2, \ldots, r_x$ such that

$$l \equiv k \equiv r_1 + r_2 + \cdots + r_x \pmod{m}, \tag{4}$$

and $gcd(r_i, m) = 1$ for $1 \leqslant i \leqslant x$.

The proof of the assertion for $x = 1$, i.e. $gcd(l, n) = 1$, is easily reduced to that for $x = 3$, using part (i) of Lemma 6.

Since $gcd(n, m) = 1$, the elements of an arbitrary class form a complete residue system modulo n. This implies that for each element s_i there exists an integer $s'_i \in C_{r_i}$, such that $s'_i \equiv s_i \pmod{n}$ for $1 \leqslant i \leqslant x$. Thus, according to (3) and (4) we obtain $l \equiv s'_1 + s'_2 + \cdots + s'_x \pmod{n, m}$ or equivalently $l \equiv s'_1 + s'_2 + \cdots + s'_x$ (mod $N = nm$), since $gcd(n, m) = 1$. Due to the choice of the integers s'_i, they are relatively prime to both n and m and thus to $N = nm$. □

Now, we are ready to prove the main result of this section, concerning the diameter of integral circulant graphs with divisor set $D = \{1\}$.

Theorem 9 *For a given* $\mathrm{ICG}_n(1)$ *and* $n \geqslant 2$, *we have that*

$$diam\ (\mathrm{ICG}_n(1)) = \begin{cases} 1, & n \textit{ is a prime} \\ 2, & n \textit{ is an odd composite integer or a power of } 2 \\ 3, & \textit{otherwise.} \end{cases}$$

Proof. Consider two arbitrary vertices $u, v \in \mathbb{Z}_n$ such that $u < v$ and let $l = v - u$. According to Lemma 8 there is $RD_n(l)$ on at most three elements implying that *diam* $(\mathrm{ICG}_n(1)) \leqslant 3$.

(i) The diameter of a graph equals one if and only if it is complete. Equivalently, the degree of regularity $\varphi(n)$ must be equal to $n-1$. The last equation is satisfied if and only if n is a prime number. Therefore, in the rest of the proof we assume that n is a composite number and $diam(\mathrm{ICG}_n(1)) \geqslant 2$.

(ii) If n is a power of 2, according to part (ii) of Lemma 8, we have $diam(\mathrm{ICG}_n(1)) = 2$.

Now, assume that n is an odd composite integer. Let $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be a prime factorization of n. Using induction on k, as in the proof of Lemma 8, we can conclude that there exists $RD_{p_i^{\alpha_i}}(l)$ on two elements (according to part (ii) of Lemma 7), for $1 \leq i \leq k$. Thus, there is $RD_n(l)$ on two elements and *diam* $(\mathrm{ICG}_n(1)) = 2$.

(iii) Let n be an even number divisible by an odd prime number. Hence, it can be represented as $n = 2^{\alpha_1} m$, where m is an odd number greater than one. Suppose that *diam* $(\mathrm{ICG}_n(1)) = 2$. Choose vertices u and v such that l is an odd number not relatively prime to m. Since m is an odd number, according to part (ii) there exists $RD_m(l)$ on two elements. On the other hand, according to the part (iii) of Lemma 6 there is no $RD_{2^{\alpha_1}}(l)$ on two elements. Thus there is no $RD_n(l)$ on two elements or equivalently *diam* $(\mathrm{ICG}_n(1)) \neq 2$, which leads to a contradiction. The only remaining possibility is *diam* $(\mathrm{ICG}_n(1)) = 3$, which completes the proof of the theorem.

□

5 Perfect quantum communication distance and diameter of integral circulant graphs

In the first part of the section we consider the diameter of $\mathrm{ICG}_n(D)$ for $D = \{1, d\}$. We calculate the diameter in Theorem 14 and the proof of this result is naturally divided into a sequence of lemmas. Throughout the section, we let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, where $p_1 < p_2 < \ldots < p_k$ are distinct primes, and $\alpha_i \geq 1$. The proof of the following Lemma is omitted since it is simple.

Lemma 10 $\mathrm{ICG}_n(D)$ *is complete if and only if* $n = p^2$ *and* $d = p$ *where* p *is an arbitrary prime number.*

Lemma 11 *Let* n *be an even number and* $k \geq 2$. *Then* $diam(\mathrm{ICG}_n(D)) = 2$ *if one of the following conditions is satisfied*

(i) d *is a power of* 2

(ii) $n = 2^{\alpha_1} p$ *and* $d = p$ *for a odd prime number* p.

Proof. Let $u, v \in \mathbb{Z}_n$ be two arbitrary vertices such that $l = v - u$.
(i) Suppose also that $d = 2^\alpha$ where $1 \leq \alpha \leq \alpha_1$. Now we will prove the existence of numbers $s_1, s_2 \in \mathbb{Z}_n$ such that $l \equiv s_1 + s_2 \pmod{n}$ and $s_1, s_2 \in G_n(D)$.

If $l \in 2\mathbb{N}$ then we will find $s_1, s_2 \in \mathbb{Z}_n$ such that there exists $RD_n(l)$ on two elements. Let $n = 2^{\alpha_1} m$ where m is odd. According to the part (ii) of Theorem 9, the existence of $RD_m(l)$ on two elements is guaranteed. On the other hand, from Lemma 8 (part (ii)) it holds that there exists $RD_{2^{\alpha_1}}(l)$ on two elements and thus there is $RD_n(l)$ on two elements. Notice that there exists $RD_n(l)$ on x elements if and only if there exists $RD_n(l')$ on x elements, where l' represents the residue of l modulo n. It is true since $l \equiv l' \equiv s_1 + s_2 + \ldots + s_x \pmod{n}$, where $\gcd(s_i, n) = 1$. This means that the above consideration also holds when $l > m$ or $l > 2^{\alpha_1}$.

If $l \in 2\mathbb{N} + 1$ then without loss of generality, suppose that $s_1 \in 2\mathbb{N} + 1$ and $s_2 \in 2\mathbb{N}$. This yields that $gcd(s_1, n) = 1$ and $gcd(s_2, n) = 2^\alpha$. We conclude that $p_i \nmid s_1$ for $1 \leq i \leq k$ and if $\alpha < \alpha_1$ we have $2^\alpha \mid s_2$, $2^{\alpha+1} \nmid s_2$ and $p_i \nmid s_2$ for $2 \leq i \leq k$. The last relations can be rewritten in the following form: $s_1 \not\equiv 0 \pmod{p_i}$ for $1 \leq i \leq k$, $s_2 \equiv 0 \pmod{2^\alpha}$, $s_2 \not\equiv 0 \pmod{2^{\alpha+1}}$ and $s_2 \not\equiv 0 \pmod{p_i}$ for $2 \leq i \leq k$. Since $s_1 \equiv l - s_2 \pmod{n}$, using the above relations we obtain $s_2 \equiv 0 \pmod{2^\alpha}$, $s_2 \not\equiv 0 \pmod{2^{\alpha+1}}$ and $s_2 \not\equiv \{0, l\} \pmod{p_i}$ for $2 \leq i \leq k$. Notice that, when we join the first two relations together we finally have the following system

$$\begin{aligned} s_2 &\equiv 2^\alpha \pmod{2^{\alpha+1}} \\ s_2 &\not\equiv \{0, l\} \pmod{p_i} \text{ for } 2 \leq i \leq k. \end{aligned}$$

According to the Chinese remainder theorem, it follows that there exists a solution s of the above system of congruences such that $0 \leq s < M$ and $s_2 \equiv s \pmod{M}$ where $M = 2^{\alpha+1} p_2 \ldots p_k$. Notice that the relation $M \leq n$ holds since $\alpha < \alpha_1$.

If $\alpha = \alpha_1$ then the condition $gcd(s_2, n) = 2^\alpha$ is equivalent to $s_2 \equiv 0 \pmod{2^{\alpha_1}}$ and $s_2 \not\equiv 0 \pmod{p_i}$ for $2 \leq i \leq k$. Thus, the above system is reduced to

$$\begin{aligned} s_2 &\equiv 0 \pmod{2^{\alpha_1}} \\ s_2 &\not\equiv \{0, l\} \pmod{p_i} \text{ for } 2 \leq i \leq k. \end{aligned}$$

Using the Chinese remainder theorem again, the system has a solution s such that $0 \leq s < M$ and $s_2 \equiv s \pmod{M}$ where $M = 2^{\alpha_1} p_2 \dots p_k$.

(ii) Suppose that $n = 2^{\alpha_1} p$ and $d = p$. If $l \in 2\mathbb{N}+1$ we have that either $p \mid l$ or $p \nmid l$. It follows that either $gcd(l,n) = p$ or $gcd(l,n) = 1$. In either case we conclude that $l \in G_n(D)$.

For $l \in 2\mathbb{N}$ there is $RD_n(l)$ on two elements as we have already proved in (i).

□

Lemma 12 *Let p_i be an arbitrary prime divisor of n for $2 \leq i \leq k$. We have that $k = i = 2$ and $\alpha_2 = 1$ if and only if for all odd $l \in \mathbb{Z}_n$ $l \in G_n(1, p_i)$ holds.*

Proof.
($\Rightarrow$:) For $l \in 2\mathbb{N}+1$ we have that either $p_i \mid l$ or $p_i \nmid l$. It follows that either $gcd(l,n) = p_i$ or $gcd(l,n) = 1$. In either case we conclude that $l \in G_n(D)$.

($\Leftarrow$:) Suppose that for all odd $l \in \mathbb{Z}_n$ we have that $l \in G_n(1, p_i)$ holds. This implies that for any odd $l \in \mathbb{Z}_n$ either $gcd(l,n) = 1$ or $gcd(l,n) = p_i$ holds. Since the number of odd $l \in \mathbb{Z}_n$ such that $gcd(l,n) = 1$ is equal to $\varphi(n)$ and the number of odd $l \in \mathbb{Z}_n$ such that $gcd(l,n) = p_i$ is equal to $\varphi(n/p_i)$, we have that

$$\varphi(n) + \varphi(n/p_i) = \frac{n}{2}. \tag{5}$$

Let $\alpha_i \geq 2$. Using the Euler's totient function formula we obtain that

$$\begin{aligned} 2^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_k^{\alpha_k} &= 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) \\ &+ 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_i^{\alpha_i - 2}(p_i - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) \Leftrightarrow \\ p_2 \dots p_i^2 \dots p_k &= (p_2 - 1) \dots (p_i - 1) \dots (p_k - 1)(p_i + 1) \\ &= (p_2 - 1) \dots (p_i^2 - 1) \dots (p_k - 1). \end{aligned}$$

We see that the above equation does not have a solution since the left hand side is obviously greater than the right hand side.

Now suppose that $\alpha_i = 1$. The relation (5) now becomes

$$\begin{aligned} &2^{\alpha_1 - 1} p_2^{\alpha_2} \dots p_i \dots p_k^{\alpha_k} = 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1}(p_2 - 1) \dots (p_i - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) \\ &+ 2^{\alpha_1 - 1} p_2^{\alpha_2 - 1}(p_2 - 1) \dots p_{i-1}^{\alpha_{i-1} - 1}(p_{i-1} - 1) p_{i+1}^{\alpha_{i+1} - 1}(p_{i+1} - 1) \dots p_k^{\alpha_k - 1}(p_k - 1) \\ &\Leftrightarrow p_2 \dots p_i \dots p_k = (p_2 - 1) \dots (p_{i-1} - 1)(p_{i+1} - 1) \dots (p_k - 1) p_i. \end{aligned}$$

It can be concluded that the equality holds if and only if $k = 2$, since for $k \geq 3$ the left hand side is obviously greater than the right hand side. Then $i = 2$ and so $\alpha_2 = 1$.

□

Lemma 13 *Let $n > 4$ be an even number and $k \geq 2$. Then $diam(\mathrm{ICG}_n(D)) = 3$ if and only if the following conditions are satisfied*

(i) *d is not a power of 2*

(ii) *$n \neq 2^{\alpha_1}p$ or $d \neq p$ for any odd prime number p.*

Proof.
($\Rightarrow$:) Suppose that $diam(\mathrm{ICG}_n(D)) = 3$ and that either (i) or (ii) of the assertion of the lemma is false. This implies that either assertion (i) or (ii) of Lemma 11 holds which yields that $diam(\mathrm{ICG}_n(D)) = 2$. This contradicts our assumption.
($\Leftarrow$:) Suppose now that both (i) and (ii) hold. This implies that for $2 \leq i \leq k$ there is an odd prime common divisor p_i of n and d.

If $d \neq p_i$ then $gcd(p_i, n) = p_i \notin \{1, d\}$. From this it follows that $p_i \notin G_n(D)$. Let $u, v \in \mathbb{Z}_n$ be two arbitrary vertices such that $p_i = v - u$. Suppose that the distance of vertices u and v is equal to two. It means that there exist $s_1, s_2 \in G_n(D)$ such that $s_1 + s_2 \equiv p_i \pmod n$. Since $p_i \in 2\mathbb{N}+1$ and $n \in 2\mathbb{N}$ then s_1 and s_2 have different parity and thus $gcd(s_1, n) \neq gcd(s_2, n)$. Without loss of generality, assume that $gcd(s_1, n) = 1$ and $gcd(s_2, n) = d$. We further obtain that $p_i \nmid s_1$ and $p_i \mid s_2$ and thus $p_i \nmid s_1 + s_2$, which is impossible. We conclude that the distance between vertices u and v is greater than two.

If $d = p_i$, according to Lemma 12, there exists an odd $l \in \mathbb{Z}_n$ such that $gcd(l, n) \notin \{1, p_i\}$. Consider the vertices u and v such that $l = v - u$ and $v > u$. Suppose that the distance of vertices u and v is equal to two. It means that there exist $s_1, s_2 \in G_n(D)$ such that $s_1 + s_2 \equiv l \pmod n$. Since $l \in 2\mathbb{N} + 1$, s_1 and s_2 have different parity and thus without loss of generality we can assume that $s_1 \in 2\mathbb{N}$. On the other hand, we have $gcd(s_1, n) \in \{1, p_i\}$ which implies $s_1 \in 2\mathbb{N} + 1$. This is a contradiction and the distance between vertices u and v is greater than two.

In both cases we have found two vertices such that the distance between them is greater than or equal to three, which yields that $diam(\mathrm{ICG}_n(D)) \geq 3$. According to Theorem 9 we conclude $diam(\mathrm{ICG}_n(D)) \leq diam(\mathrm{ICG}_n(1)) \leq 3$, which completes the proof. □

Now we can formulate our main result which has important application in Theorem 15. It is a direct consequence of Lemmas 10, 11 and 13.

Theorem 14 *For a given $\mathrm{ICG}_n(1, d)$ and $n \geqslant 4$ we have that*

$$diam(\mathrm{ICG}_n(1,d)) = \begin{cases} 1, & n = p^2,\ d = p,\ p \textit{ is prime} \\ 2, & n \textit{ is odd other than prime or} \\ & n \textit{ is even and } d \textit{ is a power of } 2 \textit{ or} \\ & n \textit{ is even, } k = 2, \alpha_2 = 1 \textit{ and } d = p_2 \\ 3, & \textit{otherwise.} \end{cases} \qquad (6)$$

Perfect quantum communication distance (PQCD) of an arbitrary pair of vertices u and v is the distance $d(u, v)$ if perfect state transfer exists between them. If we consider a circulant network with identical couplings PST occurs only between vertices b and $b+n/2$ for $0 \leq b \leq n/2-1$ (Theorem 2). For the integral circulant graph $\mathrm{ICG}_n(D)$ where $D = \{1, n/2\}$, PQCD of b and $b + n/2$ is equal to one. In the other case, we have that $D =$

$\{1, n/4\}$ (Theorem 3) and thus the existence of the path $b, b+n/4, b+n/2$ shows that PQCD is equal to two. The above discussion leads us to the conclusion that PST exists between antipodal vertices if and only if $1 \leq diam(\mathrm{ICG}_n(1,d)) \leq 2$.

Theorem 15 *PST exists between non-antipodal vertices in* $\mathrm{ICG}_n(D)$ *for* $|D| = 2$ *if and only if one of the following conditions is satisfied*

(i) $n \in 8\mathbb{N}$ *and* $D = \{1, n/2\}$

(ii) $n \in 8\mathbb{N}$ *other than a power of* 2 *and* $D = \{1, n/4\}$.

Proof.
(i) PST exists in $\mathrm{ICG}_n(1, n/2)$ between antipodal vertices b and $b+n/2$ for $0 \leq b \leq n/2-1$ if and only if $diam(\mathrm{ICG}_n(1, n/2)) = d(b, b+n/2) = 1$. This implies that $\mathrm{ICG}_n(1, n/2)$ for $n \in 8\mathbb{N}$ has to be complete. But, according to Theorem 14 this is true if and only if n is a square of a prime. This is a contradiction since $8 \mid n$. Thus we conclude that there are no antipodal vertices b and $b+n/2$ for $0 \leq b \leq n/2-1$ in $\mathrm{ICG}_n(1, n/2)$ for $8 \mid n$, which completes the first part of the proof.

(ii) Similarly, we conclude that PST exists in $\mathrm{ICG}_n(1, n/4)$ between antipodal vertices b and $b+n/2$ for $0 \leq b \leq n/2-1$ if and only if the diameter of $\mathrm{ICG}_n(1, n/4)$ for $n \in 8\mathbb{N}$ is equal to two. Since n is even, using Theorem 14 we have two possibilities such that $diam(\mathrm{ICG}_n(1, n/4)) = 2$.

If $d = n/4$ is a power of two, then we have that n is also a power of two. Thus we conclude that the vertices b and $b+n/2$ are antipodal for $0 \leq b \leq n/2-1$ in $\mathrm{ICG}_n(1, n/4)$ for $n = 2^{\alpha_1}$ and $\alpha_1 \geq 3$.

If $n = 2^{\alpha_1} p_2$ and $d = p_2$, it follows that $d = n/4 = p_2$ and hence that $n = 4p_2$. According to the assumption we have $n \in 8\mathbb{N}$ which is a contradiction and consequently $diam(\mathrm{ICG}_n(1, n/4)) \neq 2$. Thus we conclude that there are no antipodal vertices b and $b+n/2$ for $0 \leq b \leq n/2-1$ in $\mathrm{ICG}_n(1, n/4)$ for $8 \mid n$. □

6 Concluding remarks

We have thus found two classes of integral circulant graphs $\mathrm{ICG}_n(D)$ having PST between a pair of non-antipodal vertices for $n \in 8\mathbb{N}$. On the other hand, Theorems 3, 4 and 5 show that there exists an integral circulant graph with n vertices having PST if and only if $n \in 4\mathbb{N}$. Thus, we will examine the classes of graphs given in Theorem 5 and answer the question of PST existence between non-antipodal vertices for any $n \in 4\mathbb{N}$.

Using a similar approach as in the proof of Lemma 10 we can prove that $\mathrm{ICG}_n(1, d_1, d_2, d_3)$ is complete if and only if $n = p^4$ and $d_i = p^i$ for $1 \leq i \leq 3$ for an arbitrary prime number p. This implies that $\mathrm{ICG}_n(1, 2, 4, n/2)$ for $n \in 8\mathbb{N}+4$ is not complete and thus PST only exists between non-antipodal vertices.

Since $diam(\mathrm{ICG}_n(1, 2, 4, n/4) \leq diam(\mathrm{ICG}_n(1, 2)) = 2$ by Lemma 11 (part (i)), it can be concluded that

$diam(\mathrm{ICG}_n(1,2,4,n/4)) = 2$ for $n \in 8\mathbb{N}+4$. This leads us to the final conclusion that PST only exists between antipodal vertices in $\mathrm{ICG}_n(1,2,4,n/4)$ for $n \in 8\mathbb{N}+4$. Following the above discussion, we can now formulate our final result.

Theorem 16 *There exists an integral circulant graph with n vertices having PST between non-antipodal vertices if and only if $n \in 4\mathbb{N}$.*

It would be interesting to characterize integral circulant graphs of diameter equal to two, especially graphs having PST and we leave it as open problem. Even the special case when the divisor set consists of a small number of divisors of n seems difficult to solve elegantly. Graphs with small diameter also have application in molecular graph theory. Also, a class of self-complementary integral circulant graphs should be searched among those with diameter two.

Acknowledgement: The author gratefully acknowledges the support from the research project 144011 of the Serbian Ministry of Science.

References

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

[2] M. Bašić, A. Ilić, *On the clique number of integral circulant graphs*, Appl. Math. Lett. 22 (2009) 1406–1411.

[3] M. Bašić, M.D. Petković, *Some classes of integral circulant graphs allowing and not allowing perfect state transfer*, Appl. Math. Lett. 22 (2009) 1609–1615.

[4] M. Bašić, M.D. Petković, D. Stevanović, *Perfect state transfer in integral circulant graphs*, Appl. Math. Lett. 22 (2009) 1117–1121.

[5] M. Bašić, M.D. Petković, *Perfect state transfer in integral circulant graphs of non-square-free order*, Lin. Algebra Appl. 433 (2010) 149–163.

[6] P. Berrizbeitia, R.E. Giudic, *On cycles in the sequence of unitary Cayley graphs*, Discrete Math. 282 (2004), 239–243.

[7] R.J. Angeles-Canul, R.M. Norton, M.C. Opperman, C.C. Paribello, M.C. Russell, C. Tamonk, *Perfect state transfer, integral ciculants and join of graphs*, Quant. Inform. Comput. 10 (2010) 325-342.

[8] R.J. Angeles-Canul, R.M. Norton, M.C. Opperman, C.C. Paribello, M.C. Russell, C. Tamonk, *Quantum perfect state transfer on weighted join graphs*, Int. J. Quantum Inf. 7 (2009), 1429–1445.

[9] 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].

[10] M. Christandl, N. Datta, T.C. Dorlas, A. Ekert, A. Kay, and A.J. Landahl, *Perfect transfer of arbitrary states in quantum spin networks*, Phys. Rev. A 71:032312, 2005.

[11] E. Fuchs, *Longest induced cycles in circulant graphs*, The Electronic J. Comb. 12 (2005), 1-12.

[12] C.D. Godsil, *Algebraic combinatorics*, Chapman and Hall mathematics, 1993.

[13] C.D. Godsil, *Periodic Graphs*, arXiv:0806.2074v1 [math.CO] 12 Jun 2008.

[14] G.H. Hardy, E.M. Wright, An introduction to the Theory of Numbers, 5th ed, Clarendon Press, Oxford University Press, New York, 1979.

[15] F.K. Hwang, *A survey on multi-loop networks*, Theor. Comput. Sci. 299 (2003), 107–121.

[16] A. Ilić, *The energy of unitary Cayley graphs*, Lin. Algebra Appl. 431 (2009), 1881–1889.

[17] A. Ilić, M. Bašić, *On the chromatic number of integral circulant graphs*, Comput. Math. Appl. 60 (2010) 144–150.

[18] A. Ilić, M. Bašić, I Gutman, *Triply Equienergetic Graphs*, MATCH Commun. Math. Comput. Chem. 64 (2010) 189–200.

[19] M.A. Jafarizadeh, R. Sufiani, *Perfect state transfer over distance- regular spin networks*, Phys. Rev. A 77, 022315 (2008).

[20] W. Klotz, T. Sander, *Some properties of unitary Cayley graphs*, The Electronic J. Comb. 14 (2007), #R45.

[21] M.D. Petković, M. Bašić, *Further results on the perfect state transfer in integral circulant graphs*, submitted for publication.

[22] H. N. Ramaswamy, C. R. Veena, *On the Energy of Unitary Cayley Graphs*, The Electronic J. Comb. 16 (2007) #N24

[23] N. Saxena, S. Severini, I. Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, Int. J. Quantum Inf. 5 (2007), 417–430.

[24] D. Stevanović, M. Petković, M. Bašić, *On the diametar of integral circulant graphs*, Ars Comb. accepted for publication.

[25] W. So, *Integral circulant graphs*, Discrete Math. 306 (2006), 153–158.