Note

# Perfect codes in circulant graphs

Rongquan Feng [a], He Huang [a,*], Sanming Zhou [b]

[a] *School of Mathematical Sciences, Peking University, Beijing 100871, China*
[b] *School of Mathematics and Statistics, The University of Melbourne, Parkville, VIC 3010, Australia*

## A R T I C L E   I N F O

## A B S T R A C T

A perfect code in a graph $\Gamma = (V, E)$ is a subset $C$ of $V$ that is an independent set such that every vertex in $V \setminus C$ is adjacent to exactly one vertex in $C$. A total perfect code in $\Gamma$ is a subset $C$ of $V$ such that every vertex of $V$ is adjacent to exactly one vertex in $C$. A perfect code in the Hamming graph $H(n, q)$ agrees with a $q$-ary perfect 1-code of length $n$ in the classical setting. In this paper we give a necessary and sufficient condition for a circulant graph of degree $p - 1$ to admit a perfect code, where $p$ is an odd prime. We also obtain a necessary and sufficient condition for a circulant graph of order $n$ and degree $p^l - 1$ to have a perfect code, where $p$ is a prime and $p^l$ the largest power of $p$ dividing $n$. Similar results for total perfect codes are also obtained in the paper.

© 2017 Elsevier B.V. All rights reserved.

## 1. Introduction

Since the beginning of coding theory in the late 1940s, perfect codes have been important objects of study in information theory; see the surveys [9,19] for a large number of results on perfect codes. Hamming and Golay codes are well known examples of perfect codes, and their importance is widely recognized. The notion of perfect codes can be generalized to graphs [2,13] in a natural way, such that $q$-ary perfect $e$-codes of length $n$ in the classical setting are precisely perfect $e$-codes in the corresponding Hamming graph $H(n, q)$. Since Hamming graphs are a particular family of Cayley graphs, perfect codes in Cayley graphs can be viewed as generalizations of perfect codes in the classical case. From a group theoretic point of view, the simplest Cayley graphs are circulant graphs, namely Cayley graphs on cyclic groups. However, even in this innocent-looking case, the question about when a general circulant graph admits a perfect 1-code is unsettled. Contributing to improvement of this unsatisfactory situation, we answer this question for two families of circulant graphs and give similar results for total perfect codes in this paper.

Let $\Gamma = (V, E)$ be a simple undirected graph and $e \geq 1$ an integer. The *ball* with radius $e$ and centre $u \in V$ is the set of vertices of $\Gamma$ with distance at most $e$ to $u$ in $\Gamma$. A subset $C$ of $V$ is called a *perfect $e$-code* [2,13] in $\Gamma$ if the balls with radius $e$ and centres in $C$ form a partition of $V$. As mentioned above, $q$-ary perfect $e$-codes of length $n$ in the classical setting [9,19] are simply perfect $e$-codes in the Hamming graph $H(n, q)$. In graph theory, perfect 1-codes in a graph are called efficient dominating sets or independent perfect dominating sets of the graph. In the rest of this paper a perfect 1-code is simply called a *perfect code*. A subset $C \subseteq V$ is called a *total perfect code* in $\Gamma$ (see e.g. [8]) if every vertex of $\Gamma$ has exactly one neighbour in $C$. This concept is related to diameter perfect codes, which were introduced in [1] for distance regular graphs and adapted in [7] for Lee metric over $\mathbb{Z}^n$ and $\mathbb{Z}_q^n$. As mentioned in [21], when the Manhattan (for $\mathbb{Z}^n$) or Lee (for $\mathbb{Z}_q^n$) distance is considered, total perfect codes coincide with diameter perfect codes of minimum distance four.

---

* Corresponding author.
  *E-mail addresses:* fengrq@math.pku.edu.cn (R. Feng), 811745023@qq.com (H. Huang), sanming@unimelb.edu.au (S. Zhou).

Perfect codes in Cayley graphs are particularly charming objects. Given a finite group $G$ and an inverse-closed subset $X$ of $G$ not containing the identity element, the *Cayley graph* $\mathrm{Cay}(G, X)$ on $G$ relative to the *connection set $X$* is the graph with vertex set $G$ such that $u, v \in G$ are adjacent if and only if $vu^{-1} \in X$. This graph is connected if and only if $S$ is a generating set of $G$. In the special case when $G = \mathbb{Z}_n$ is the additive group of integers modulo $n$, a Cayley graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ on $\mathbb{Z}_n$ is called a *circulant graph*. In [15] sufficient conditions for Gaussian and Eisenstein–Jacobi graphs to contain perfect $e$-codes were given, and these conditions were proved to be necessary in [20] in a more general setting. In [18] it was proved that there is no perfect code in any Cayley graph on $\mathrm{SL}(2, 2^f), f > 1$ with respect to a conjugation-closed connection set. In [3] a methodology for constructing infinite families of E-chains of Cayley graphs on symmetric groups was given, where an E-chain is a countable family of nested graphs each containing a perfect code. In [6] perfect codes in a Cayley graph with a conjugation-closed connection set were studied by way of equitable partitions, yielding a nonexistence result in terms of irreducible characters of the underlying group. In [14] it was proved that a conjugation-closed subset $C$ of a group $G$ is a perfect code in a Cayley graph on $G$ if and only if there exists a covering projection from the Cayley graph to a complete graph with $C$ as a fibre. A similar result was obtained in [21] for total perfect codes in Cayley graphs. In a recent work [10], perfect codes in Cayley graphs were studied from the viewpoint of group rings, and among other results conditions for a normal subgroup of a finite group to be a perfect code in some Cayley graph of the group were obtained.

Perfect codes in circulant graphs have been studied by several researchers in recent years. In [16], 3- and 4-regular connected circulant graphs admitting a perfect code were characterized, and a sufficient condition for a general circulant graph to have a perfect code was given. In [4] a necessary and sufficient condition for a circulant graph to admit a perfect code with size a prime number was given and all such perfect codes were characterized. In [17] a few results on perfect codes in circulant graphs were proved. In [20] perfect $e$-codes in an interesting family of circulant graphs with degree twice an odd prime were studied in the more general setting of cyclotomic graphs.

In spite of the efforts above, our understanding of perfect codes in circulant graphs is still quite limited. In this paper we prove the following results with the help of cyclotomic polynomials.

**Theorem 1.1.** *Let $n$ be a positive integer and $p$ be an odd prime. A connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ of degree $p - 1$ admits a perfect code if and only if $p$ divides $n$ and $s \not\equiv s'$ mod $p$ for distinct $s, s' \in S \cup \{0\}$.*

**Theorem 1.2.** *Let $n, l$ be positive integers, and let $p$ be a prime such that $p^l$ divides $n$ but $p^{l+1}$ does not divide $n$. A connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ of degree $p^l - 1$ admits a perfect code if and only if $s \not\equiv s'$ mod $p^l$ for distinct $s, s' \in S \cup \{0\}$.*

**Theorem 1.3.** *Let $n$ be a positive integer and $p$ be an odd prime. A connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ of degree $p$ admits a total perfect code if and only if $p$ divides $n$ and $s \not\equiv s'$ mod $p$ for distinct $s, s' \in S$.*

**Theorem 1.4.** *Let $n, l$ be positive integers, and let $p$ be a prime such that $p^l$ divides $n$ but $p^{l+1}$ does not divide $n$. A connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ of degree $p^l$ admits a total perfect code if and only if $s \not\equiv s'$ mod $p^l$ for distinct $s, s' \in S$.*

## 2. Proofs

Let $\zeta_n$ be a primitive $n$th root of unity, say $\zeta_n = e^{2\pi i/n}$. The *$n$th cyclotomic polynomial* is defined [11] as

$$\lambda_n(x) = \prod_{1 \le d < n, (d,n)=1} (x - \zeta_n^d).$$

The roots of $\lambda_n(x)$ are precisely the primitive $n$th roots of unity, that is, $\lambda_n(x) = \prod_{\zeta \in E_n}(x - \zeta)$, where $E_n$ is the set of all primitive $n$th roots of unity. We will use the following well known results (see e.g. [11, Section 9.1]) in the proof of Theorems 1.1–1.4.

**Lemma 2.1.**

(a)

$$x^n - 1 = \prod_{d \mid n} \lambda_d(x);\tag{1}$$

(b) $\lambda_n(x) \in \mathbb{Z}[x]$;
(c) $\lambda_n(x)$ is irreducible in $\mathbb{Z}[x]$.

In particular, by (1), for any prime $p$ and integer $j \ge 1$,

$$\lambda_{p^j}(x) = \frac{x^{p^j} - 1}{x^{p^{j-1}} - 1} = (x^{p^{j-1}})^{p-1} + (x^{p^{j-1}})^{p-2} + \cdots + x^{p^{j-1}} + 1.\tag{2}$$

Define

$$f_A(x) = \sum_{a \in A} x^a$$

for any non-empty finite set $A$ of nonnegative integers. For a subset $S$ of $\mathbb{Z}_n$, denote

$$S_0 = S \cup \{0\}.$$

The following lemma reduces the perfect code problem for circulant graphs to a number theoretic problem.

**Lemma 2.2.** *A subset $C$ of $\mathbb{Z}_n$ is a perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$ if and only if there exists $q(x) \in \mathbb{Z}[x]$ such that*

$$f_C(x)f_{S_0}(x) = (x^n - 1)q(x) + (x^{n-1} + \cdots + x + 1). \tag{3}$$

**Proof.** By the definition of a perfect code, $C$ is a perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$ if and only if every integer in $\{0, 1, \ldots, n - 1\}$ can be written in a unique way as $(c + s) \bmod n$ with $c \in C$ and $s \in S_0$, which is equivalent to $f_C(x)f_{S_0}(x) = \sum_{c \in C, s \in S_0} x^{c+s} \equiv x^{n-1} + \cdots + x + 1 \bmod (x^n - 1)$. Thus $C$ is a perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$ if and only if (3) holds for some $q(x) \in \mathbb{Z}[x]$. $\square$

The next lemma was proved in [16, Remark 1]. We give a different proof using Lemma 2.2 for the completeness of the present paper.

**Lemma 2.3** ([16, Remark 1]). *A connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ of order $n \geq 4$ and degree $k = |S|$ admits a perfect code provided that $k + 1$ divides $n$ and $s \not\equiv s' \bmod (k + 1)$ for distinct $s, s' \in S \cup \{0\}$.*

**Proof.** Consider a connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$ with order $n \geq 4$ and degree $k = |S|$. Suppose that $k + 1$ divides $n$, say $n = m(k + 1)$ for some integer $m \geq 1$, and $s \not\equiv s' \bmod (k + 1)$ for distinct $s, s' \in S \cup \{0\}$. We may write $S_0 = S \cup \{0\} = \{s_0, s_1, \ldots, s_k\}$, where $s_0, s_1, \ldots, s_k$ are pairwise distinct modulo $(k + 1)$. Without loss of generality we may assume $s_0 = 0$ and $s_i \equiv i \bmod (k + 1)$ for $i \in \{1, 2, \ldots, k\}$. Then $x^{s_i} \equiv x^i \bmod (x^{k+1} - 1)$ for $i \in \{0, 1, \ldots, k\}$ and $f_{S_0}(x) = \sum_{s \in S_0} x^s \equiv x^k + \cdots + x + 1 \bmod (x^{k+1} - 1)$. So there exists $q(x) \in \mathbb{Z}[x]$ such that $f_{S_0}(x) = (x^{k+1} - 1)q(x) + (x^k + \cdots + x + 1)$.

Set $C = \{0, k + 1, 2(k + 1), \ldots, (m - 1)(k + 1)\}$. Then

$$f_C(x) = x^{(m-1)(k+1)} + \cdots + x^{k+1} + 1 = \frac{x^{m(k+1)} - 1}{x^{k+1} - 1} = \frac{x^n - 1}{x^{k+1} - 1}$$

and hence

$$f_C(x)f_{S_0}(x) = (x^n - 1)q(x) + (x^{n-1} + \cdots + x + 1).$$

Therefore, by Lemma 2.2, $C$ is a perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$. $\square$

As shown in [16,17] by counterexamples, the sufficient condition for the existence of a perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$ given in Lemma 2.3 may not be necessary. However, it is indeed necessary when $k = 4$ (see [16]) or when $n/(k+1)$ is a prime and $S \cup \{0\}$ is aperiodic (see [4] for definition).

**Proof of Theorem 1.1.** By Lemma 2.3, it remains to prove the 'only if' part. Suppose that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is connected of degree $|S| = p - 1$ and admits a perfect code $C$, where $p$ is an odd prime. Then by Lemma 2.2, (3) holds for some $q(x) \in \mathbb{Z}[x]$. Setting $x = 1$ in (3), we obtain $p|C| = |C||S_0| = f_C(1)f_{S_0}(1) = n$. Hence $p$ divides $n$. Write $n = p^l m$ with $l \geq 1$ and $m$ not divisible by $p$. Then $|C| = p^{l-1}m$ and $p^l$ does not divide $|C|$.

By Lemma 2.1, $\lambda_p(x), \lambda_{p^2}(x), \ldots, \lambda_{p^l}(x)$ are distinct irreducible polynomials each dividing $x^n - 1$ and $(x^n - 1)/(x - 1) = x^{n-1} + \cdots + x + 1$. Combining this with (3), we obtain that $\lambda_{p^j}(x)$ divides $f_C(x)$ or $f_{S_0}(x)$ for each $j \in \{1, 2, \ldots, l\}$.

**Claim 1.** *There exists at least one $j \in \{1, 2, \ldots, l\}$ such that $\lambda_{p^j}(x)$ divides $f_{S_0}(x)$.*

Suppose otherwise. Then $\lambda_p(x), \lambda_{p^2}(x), \ldots, \lambda_{p^l}(x)$ all divide $f_C(x)$. Since they are irreducible and hence pairwise coprime, it follows that $\prod_{j=1}^{l} \lambda_{p^j}(x)$ divides $f_C(x)$. That is,

$$f_C(x) = g(x) \prod_{j=1}^{l} \lambda_{p^j}(x) \tag{4}$$

for some $g(x) \in \mathbb{Z}[x]$. Since $p$ is a prime, by (2) we have $\lambda_{p^j}(1) = p$ for each $j \geq 1$. Setting $x = 1$ in (4), we then obtain $|C| = f_C(1) = p^l \cdot g(1)$. Since $g(1)$ is an integer, it follows that $p^l$ divides $|C|$, which is a contradiction. This proves Claim 1.

Since $|S_0| = p$, we may write $S_0 = \{s_0, s_1, \ldots, s_{p-1}\}$, where $s_0 = 0$ and $s_1, s_2, \ldots, s_{p-1}$ are pairwise distinct. Denote by $t_i$ the unique integer in $\{0, 1, \ldots, p - 1\}$ such that $s_i \equiv t_i \bmod p$, for $0 \leq i \leq p - 1$. In particular, $t_0 = 0$ as $s_0 = 0$. We have

$$f_{S_0}(x) = \sum_{i=0}^{p-1} x^{s_i} \equiv \sum_{i=0}^{p-1} x^{t_i} \bmod (x^p - 1). \tag{5}$$

**Claim 2.** *If $j \in \{2, \ldots, l\}$, then $\lambda_{p^j}(x)$ does not divide $f_{S_0}(x)$.*

Suppose to the contrary that $\lambda_{p^j}(x)$ divides $f_{S_0}(x)$ for some $j \in \{2, \ldots, l\}$, say, $f_{S_0}(x) = \lambda_{p^j}(x)h(x)$, where $h(x) \in \mathbb{Z}[x]$. Since $j \geq 2$, $x^{p^{j-1}} \equiv 1 \bmod (x^p - 1)$. This together with (2) implies $\lambda_{p^j}(x) \equiv p \bmod (x^p - 1)$. Thus,

$$f_{S_0}(x) \equiv p \cdot \bar{h}(x) \bmod (x^p - 1), \tag{6}$$

where $\bar{h}(x)$ is the unique polynomial of degree less than $p$ such that $h(x) \equiv \bar{h}(x) \bmod (x^p - 1)$. Combining (5) and (6), we have

$$\sum_{i=0}^{p-1} x^{t_i} \equiv p \cdot \bar{h}(x) \bmod (x^p - 1).$$

Since both sides of this equation are polynomials of degree less than $p$ whilst $x^p - 1$ has degree $p$, it follows that

$$\sum_{i=0}^{p-1} x^{t_i} = p \cdot \bar{h}(x). \tag{7}$$

Since $0 \leq t_i \leq p - 1$ and $t_0 = 0$, this implies that all $t_i = 0$, that is, every element of $S$ is a multiple of $p$. However, this implies that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is disconnected, which contradicts our assumption. This proves Claim 2.

Combining Claims 1 and 2, we know that $\lambda_p(x)$ divides $f_{S_0}(x)$. Thus, by (5) and $x^p - 1 = (x - 1)\lambda_p(x)$, we obtain $\sum_{i=0}^{p-1} x^{t_i} \equiv 0 \bmod \lambda_p(x)$. Since $\sum_{i=0}^{p-1} x^{t_i}$ has degree at most $p-1$ whilst $\lambda_p(x)$ has degree $p-1$, it follows that $\sum_{i=0}^{p-1} x^{t_i} = a\lambda_p(x)$ for some integer $a$. Setting $x = 1$, we obtain $p = ap$ and so $a = 1$. Therefore, $\sum_{i=0}^{p-1} x^{t_i} = \lambda_p(x) = x^{p-1} + \cdots + x + 1$. In other words, $\{t_0, t_1, \ldots, t_{p-1}\} = \{0, 1, \ldots, p-1\}$, or equivalently, $s \not\equiv s' \bmod p$ for distinct $s, s' \in S_0$. $\square$

**Proof of Theorem 1.2.** Again, by Lemma 2.3, it remains to prove the 'only if' part. Suppose that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is connected of degree $|S| = p^l - 1$ and admits a perfect code $C$, where $n, l$ are positive integers and $p$ a prime such that $p^l$ divides $n$ but $p^{l+1}$ does not. Then by Lemma 2.2, (3) holds for some $q(x) \in \mathbb{Z}[x]$. Setting $x = 1$ in (3), we obtain $p^l|C| = |C||S_0| = f_C(1)f_{S_0}(1) = n$. Since $p^{l+1}$ does not divide $n$, $p$ does not divide $|C|$.

Similar to the proof of Theorem 1.1, we see that $\lambda_{p^j}(x)$ divides $f_C(x)$ or $f_{S_0}(x)$ for each $j \in \{1, 2, \ldots, l\}$. We prove further that:

**Claim 3.** $\lambda_{p^j}(x)$ divides $f_{S_0}(x)$ for each $j \in \{1, 2, \ldots, l\}$.

To prove this, let $J$ denote the set of integers $j \in \{1, 2, \ldots, l\}$ such that $\lambda_{p^j}(x)$ divides $f_C(x)$. Since $\lambda_p(x), \lambda_{p^2}(x), \ldots, \lambda_{p^l}(x)$ are irreducible and hence pairwise coprime,

$$f_C(x) = g(x) \prod_{j \in J} \lambda_{p^j}(x) \tag{8}$$

for some $g(x) \in \mathbb{Z}[x]$. By (2), we have $\lambda_{p^j}(1) = p$ for each $j \geq 1$. Thus, setting $x = 1$ in (8), we obtain $|C| = f_C(1) = p^{|J|} \cdot g(1)$. Since $g(1)$ is an integer, it follows that $p^{|J|}$ divides $|C|$. Since $p$ does not divide $|C|$, we must have $J = \emptyset$ and so Claim 3 is proved.

Since $|S_0| = p^l$, we may write $S_0 = \{s_0, s_1, \ldots, s_{p^l-1}\}$, where $s_0 = 0$. Denote by $t_i$ the unique integer in $\{0, 1, \ldots, p^l - 1\}$ such that $s_i \equiv t_i \bmod p^l$, for $0 \leq i \leq p^l - 1$. In particular, $t_0 = 0$ as $s_0 = 0$. We have

$$f_{S_0}(x) = \sum_{i=0}^{p^l-1} x^{s_i} \equiv \sum_{i=0}^{p^l-1} x^{t_i} \bmod (x^{p^l} - 1). \tag{9}$$

On the other hand, by Claim 3,

$$f_{S_0}(x) = h(x) \prod_{j=1}^{l} \lambda_{p^j}(x) \tag{10}$$

for some $h(x) \in \mathbb{Z}[x]$. By (1), $\prod_{j=1}^{l} \lambda_{p^j}(x) = (x^{p^l} - 1)/(x - 1) = \sum_{j=0}^{p^l-1} x^j$ divides $x^{p^l} - 1$. This together with (9) and (10) implies that $\sum_{j=0}^{p^l-1} x^j$ divides $\sum_{i=0}^{p^l-1} x^{t_i}$. Since the former has degree $p^l - 1$ whilst the latter has degree at most $p^l - 1$, it follows that the latter must have degree $p^l - 1$ and moreover $\sum_{i=0}^{p^l-1} x^{t_i} = a\sum_{j=0}^{p^l-1} x^j$ for some integer $a$. Setting $x = 1$, we obtain $p^l = ap^l$ and so $a = 1$. That is, $\sum_{i=0}^{p^l-1} x^{t_i} = \sum_{j=0}^{p^l-1} x^j$. Therefore, $\{t_0, t_1, \ldots, t_{p^l-1}\} = \{0, 1, \ldots, p^l - 1\}$ and the proof is complete. $\square$

Similar to Lemma 2.2, one can easily verify the following result.

**Lemma 2.4.** A subset $C$ of $\mathbb{Z}_n$ is a total perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$ if and only if there exists $q(x) \in \mathbb{Z}[x]$ such that

$$f_C(x)f_S(x) = (x^n - 1)q(x) + (x^{n-1} + \cdots + x + 1). \tag{11}$$

Similar to [16, Remark 1] (see Lemma 2.3), we have the following observation.

**Lemma 2.5.** *A connected circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *of order* $n \geq 4$ *and degree* $k = |S|$ *admits a total perfect code provided that* $k$ *divides* $n$ *and* $s \not\equiv s' \bmod k$ *for distinct* $s, s' \in S$.

In fact, since all elements of $S$ are pairwise distinct modulo $k$, for any $v \in \mathbb{Z}_n$ there exists a unique $s \in S$ such that $v \equiv s \bmod k$, implying that $\{ki : 0 \leq i < n/k\}$ is a total perfect code in $\mathrm{Cay}(\mathbb{Z}_n, S)$.

Theorem 1.3 can be proved using Lemmas 2.4 and 2.5 and following the proof of Theorem 1.1 but with $S \cup \{0\}$ replaced by $S = \{s_0, s_1, \ldots, s_{p-1}\}$. (Since $s_0 \neq 0$ in the current case, $t_0$ may not be 0, but one can see that not all elements of $S$ are congruent to each other modulo $p$ as $p$ is odd and each $n - s_i \in S$. So from (7) we can still derive that all $t_i = 0$.)

Theorem 1.4 can be proved using Lemmas 2.4 and 2.5 and following the proof of Theorem 1.2 but with $S \cup \{0\}$ replaced by $S = \{s_0, s_1, \ldots, s_{p^l-1}\}$.

## 3. Remarks

We remark that our method in the previous section can be adapted to give a totally different proof of the following known result.

**Theorem 3.1** ([16, Theorem 2]). *A cubic connected circulant graph of order* $n \geq 4$ *admits a perfect code if and only if* $n \equiv 4 \bmod 8$.

**Proof.** It can be verified that, for a cubic connected circulant graph $\mathrm{Cay}(\mathbb{Z}_n, S)$, where $n \geq 4$ and $S = \{n/2, s, n - s\}$ for some $1 \leq s \leq (n/2) - 1$, $n$ must be even and moreover $n \equiv 4 \bmod 8$ if and only if 4 divides $n$ and the elements of $S \cup \{0\}$ are pairwise distinct modulo 4. Thus, by Lemma 2.3, if $n \equiv 4 \bmod 8$, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ admits a perfect code $C$.

Suppose that $\mathrm{Cay}(\mathbb{Z}_n, S)$ admits a perfect code $C$. Similar to the proof of Theorem 1.1, by Lemma 2.2, (3) holds and so $4|C| = |C||S_0| = f_C(1)f_{S_0}(1) = n$. This together with the connectedness of $\mathrm{Cay}(\mathbb{Z}_n, S)$ implies that $n$ is a multiple of 4 and $s$ must be odd. Write $n = 2^l m$ with $l \geq 2$ and $m$ odd. Then $|C| = 2^{l-2} m$. Since $2^{l-1}$ does not divide $|C|$, similar to Claim 1 in the proof of Theorem 1.1 one can show that exactly two of $\lambda_2(x), \lambda_{2^2}(x), \ldots, \lambda_{2^l}(x)$ divide $f_{S_0}(x)$. So there is at least one $j \in \{2, \ldots, l\}$ such that $\lambda_{2^j}(x)$ divides $f_{S_0}(x)$. Note that $\lambda_{2^j}(x) = x^{2^{j-1}} + 1$ by (2).

Write $s = 2^{j-1} q + r$, where $q$ and $r$ are integers and $0 \leq r \leq 2^{j-1} - 1$. Since $s$ is odd and $j \geq 2$, $r$ is odd and so $1 \leq r \leq 2^{j-1} - 1$. We have

$$
\begin{aligned}
f_{S_0}(x) &= x^0 + x^{n/2} + x^s + x^{n-s} \\
&= 1 + (x^{2^{j-1}})^{2^{l-j}m} + (x^{2^{j-1}})^q \cdot x^r + (x^{2^{j-1}})^{2^{l-j+1}m-q-1} \cdot x^{2^{j-1}-r} \\
&\equiv 1 + (-1)^{2^{l-j}m} + (-1)^q \cdot x^r + (-1)^{2^{l-j+1}m-q-1} \cdot x^{2^{j-1}-r} \bmod (x^{2^{j-1}} + 1) \\
&\equiv 1 + (-1)^{2^{l-j}m} + (-1)^q \cdot (x^r - x^{2^{j-1}-r}) \bmod (x^{2^{j-1}} + 1).
\end{aligned}
$$

Thus, since $x^{2^{j-1}} + 1$ divides $f_{S_0}(x)$, it also divides $1 + (-1)^{2^{l-j}m} + (-1)^q \cdot (x^r - x^{2^{j-1}-r})$. However, this polynomial has degree at most $2^{j-1} - 1$ as $1 \leq r \leq 2^{j-1} - 1$. Therefore, $1 + (-1)^{2^{l-j}m} + (-1)^q \cdot (x^r - x^{2^{j-1}-r}) = 0$, yielding $1 + (-1)^{2^{l-j}m} = 0$ and $r = 2^{j-1} - r$. Hence $l = j$ and $r = 2^{j-2}$. Since $r$ is odd, we then have $l = j = 2$. So $n = 4m$ with odd $m$. Thus $n \equiv 4 \bmod 8$ and the proof is complete. $\square$

It is well known that Cayley graphs are vertex-transitive. In general, perfect codes in vertex-transitive graphs are also of considerable interest. For example, the problem of characterizing vertex-transitive graphs admitting a perfect code was posed in [12]. In the same paper it was proved that a connected cubic vertex-transitive graph of order $2^m$ ($m \geq 3$) has a perfect code if and only if it is not isomorphic to the Möbius ladder $M_{2^{m-1}}$. (Since $M_{2^{m-1}}$ is isomorphic to the cubic circulant graph $\mathrm{Cay}(\mathbb{Z}_{2^m}, \{2^{m-1}, 1, -1\})$ and $2^m$ is divisible by 8 when $m \geq 3$, the fact that $M_{2^{m-1}}$ has no perfect codes can be thought as a special case of Theorem 3.1.) Since $2^m \equiv 0 \bmod 8$ when $m \geq 3$, this implies that, in contrast to Theorem 3.1, a connected cubic Cayley graph of order $n$ admitting a perfect code may not satisfy $n \equiv 4 \bmod 8$, as shown also in [12, Table 1]. It would be interesting to give a characterization of cubic Cayley graphs (or cubic vertex-transitive graphs) admitting at least one perfect code.

## Acknowledgements

# References

[1] R. Ahlswede, H.K. Aydinian, L.H. Khachatrian, On perfect codes and related concepts, Des. Codes Cryptogr. 22 (2001) 221–237.
[2] N. Biggs, Perfect codes in graphs, J. Combin. Theory Ser. B 15 (1973) 288–296.
[3] I.J. Dejter, O. Serra, Efficient dominating sets in Cayley graphs, Discrete Appl. Math. 129 (2003) 319–328.
[4] Y.-P. Deng, Efficient dominating sets in circulant graphs with domination number prime, Inform. Process. Lett. 114 (2014) 700–702.
[5] Y.-P. Deng, Y.-Q. Sun, Q. Liu, H.-C. Wang, Efficient dominating sets in circulant graphs, Discrete Math. (2017). http://dx.doi.org/10.1016/j.disc.2017.02.014, in press.
[6] G. Etienne, Perfect codes and regular partitions in graphs and groups, European J. Combin. 8 (1987) 139–144.
[7] T. Etzion, Product constructions for perfect Lee codes, IEEE Trans. Inform. Theory 57 (2011) 7473–7481.
[8] A.-A. Ghidewon, R.H. Hammack, D.T. Taylor, Total perfect codes in tensor products of graphs, Ars Combin. 88 (2008) 129–134.
[9] O. Heden, A survey of perfect codes, Adv. Math. Commun. 2 (2008) 223–247.
[10] H. Huang, B. Xia, S. Zhou, Perfect codes in Cayley graphs, preprint, https://arxiv.org/abs/1609.03755.
[11] F. Jarvis, Algebraic Number Theory, Springer, 2014.
[12] M. Knor, P. Potočnik, Efficient domination in cubic vertex-transitive graphs, European J. Combin. 33 (8) (2012) 1755–1764.
[13] J. Kratochvíl, Perfect codes over graphs, J. Combin. Theory Ser. B 40 (1986) 224–228.
[14] J. Lee, Independent perfect domination sets in Cayley graphs, J. Graph Theory 37 (2001) 213–219.
[15] C. Martínez, R. Beivide, E. Gabidulin, Perfect codes for metrics induced by circulant graphs, IEEE Trans. Inform. Theory 53 (2007) 3042–3052.
[16] N. Obradović, J. Peters, G. Ružić, Efficient domination in circulant graphs with two chord lengths, Inform. Process. Lett. 102 (2007) 253–258.
[17] K. Reji Kumar, G. MacGillivray, Efficient domination in circulant graphs, Discrete Math. 313 (2013) 767–771.
[18] S. Terada, Perfect codes in $SL(2, 2^f)$, European J. Combin. 25 (2004) 1077–1085.
[19] J.H. van Lint, A survey of perfect codes, Rocky Mountain J. Math. 5 (1975) 199–224.
[20] S. Zhou, Cyclotomic graphs and perfect codes, preprint, http://arxiv.org/abs/1502.03272.
[21] S. Zhou, Total perfect codes in Cayley graphs, Des. Codes Cryptogr. 81 (2016) 489–504.