Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-020-00758-3

Subgroup perfect codes in Cayley sum graphs

Xuanlong Ma[1] · Min Feng[2] · Kaishun Wang[3]

Received: 22 April 2019 / Revised: 1 April 2020 / Accepted: 2 April 2020

Abstract

Let Γ be a graph with vertex set V. If a subset C of V is independent in Γ and every vertex in $V \setminus C$ is adjacent to exactly one vertex in C, then C is called a perfect code of Γ. Let G be a finite group and let S be a square-free normal subset of G. The Cayley sum graph of G with respect to S is a simple graph with vertex set G and two vertices x and y are adjacent if $xy \in S$. A subset C of G is called a perfect code of G if there exists a Cayley sum graph of G which admits C as a perfect code. In particular, if a subgroup of G is a perfect code of G, then the subgroup is called a subgroup perfect code of G. In this paper, we give a necessary and sufficient condition for a non-trivial subgroup of an abelian group with non-trivial Sylow 2-subgroup to be a subgroup perfect code of the group. This reduces the problem of determining when a given subgroup of an abelian group is a perfect code to the case of abelian 2-groups. As an application, we classify the abelian groups whose every non-trivial subgroup is a subgroup perfect code. Moreover, we determine all subgroup perfect codes of a cyclic group, a dihedral group and a generalized quaternion group.

Keywords Perfect code · Subgroup perfect code · Cayley sum graph · Finite group

Mathematics Subject Classification 05C25 · 05C69 · 94B25

Communicated by V. A. Zinoviev.

✉ Xuanlong Ma
xuanlma@xsyu.edu.cn

Min Feng
fengmin@njust.edu.cn

Kaishun Wang
wangks@bnu.edu.cn

1 School of Science, Xi'an Shiyou University, Xi'an 710065, China

2 School of Science, Nanjing University of Science and Technology, Nanjing 210094, China

3 School of Mathematical Sciences & Laboratory of Mathematical and Complex Systems, Beijing Normal University, Beijing 100875, China

Published online: 18 April 2020

1 Introduction

Throughout the paper, all graphs considered are finite and simple. For a graph Γ with vertex set V, a subset C of V is called a *perfect code* [17] of Γ if C is an independent set such that every vertex in $V \setminus C$ is adjacent to exactly one vertex in C. In graph theory, a perfect code of a graph is also called an *efficient dominating set* [6] or *independent perfect dominating set* [18]. Since the beginning of coding theory in the late 1940s, perfect codes have been important objects of study in information theory; see the surveys [12,23] on perfect codes and related definitions in the classical setting. In [3], Biggs showed that the proper setting for the perfect code problem is the class of distance-transitive graphs. Since the fundamental work of Delsarte [7], a great amount of work on perfect codes in distance-regular graphs and association schemes in general has been produced. Beginning with [17], perfect codes in general graphs have also attracted considerable attention in the community of graph theory; see [20,22,24] for example.

All groups considered in this paper are finite. Given a group G with identity element e and an inverse-closed subset S of G with $e \notin S$, the *Cayley graph* $\mathrm{Cay}(G, S)$ of G with respect to the connection set S is defined to be the graph with vertex set G such that two elements x, y are adjacent if $yx^{-1} \in S$, where the subset S of G is called *inverse-closed* if $S^{-1} := \{s^{-1} : s \in S\} = S$. Some perfect codes in the classical setting are also perfect codes in Cayley graphs. For example, the characterization of perfect code parameters in Hamming graphs (prime power q) and in Doob graphs, the nonexistence of perfect codes in bilinear form graphs (rank-metric codes) and the problem of existence of perfect codes in Hamming graphs for non-prime-power q. In recent years, perfect codes in Cayley graphs have received considerable attention, see, for example [8,10,13,18,25,26].

Let A be an abelian group and let T be a subset of A. The *Cayley sum graph* (also called *addition Cayley graph*) of A with respect to the connecting set T, denoted by $\mathrm{CayS}(A, T)$, is a graph with vertex set A and two elements x and y are joined by an edge if $xy \in T$. In 1989, Chung [5] first introduced the Cayley sum graphs of abelian groups. As pointed out in [11], the twins of the usual Cayley graphs, Cayley sum graphs are rather difficult to study, so that they received much less attention in the literature. Most results on Cayley sum graphs can be found in [1,4,9,16,19,21].

Let G be a group. An element x of G is called a *square* if $x = y^2$ for some element $y \in G$. A subset of G is called a *square-free subset* of G if it is a set without squares. A subset S of G is called a *normal subset* if S is a union of some conjugacy classes of G or equivalently, for every $g \in G$, $g^{-1}Sg := \{g^{-1}sg : s \in S\} = S$. Remark that any subset of an abelian group is normal. One can generalize the concept of Cayley sum graphs over arbitrary groups. Let S be a subset of G. The Cayley sum graph $\mathrm{CayS}(G, S)$ of G with respect to the connecting set S is a directed graph whose vertex set is G and two vertices x and y are joined by an arc if $xy \in S$. If S is a normal subset of G, then $xy \in S$ if and only if $yx \in S$, and so $\mathrm{CayS}(G, S)$ is an undirected graph. If there exists $g \in G$ with $g^2 \in S$, then $\{g, g\}$ is a semi-edge of $\mathrm{CayS}(G, S)$, where a semi-edge is an edge with one endpoint. A graph with no multiple edges and semi-edges is called a *simple graph*.

Note that all graphs considered in this paper are simple. Thus, we always consider a simple Cayley sum graph $\mathrm{CayS}(G, S)$, that is, the connecting set S needs to be normal and square-free. More explicitly, for a square-free normal subset S of G, the *Cayley sum graph* $\mathrm{CayS}(G, S)$ of G with respect to the connecting set S is a simple graph with vertex set G and two vertices x and y are adjacent if $xy \in S$. It is easy to see that $\mathrm{CayS}(G, S)$ is $|S|$-regular.

In 2016, Amooshahi and Taeri [2] first introduced the concept of the Cayley sum graph of a non-abelian group, and studied some basic properties of the graph.

In [13], Huang et al. introduced the following concept: A subset C of a group G is called a *perfect code* of G if there exists a Cayley graph $\mathrm{Cay}(G, S)$ of G which admits C as a perfect code. In particular, a perfect code of G which is also a subgroup of G is called a *subgroup perfect code* of G. In the same paper, Huang et al. obtained a necessary and sufficient condition for a normal subgroup of a group G to be a subgroup perfect code of G, and determined all subgroup perfect codes of dihedral groups and some abelian groups. As explained in [13], in some sense subgroup perfect codes are an analogue of linear perfect codes.

In this paper, we study perfect codes of Cayley sum graphs and define a subgroup perfect code of a group by using Cayley sum graphs instead of Cayley graphs. More precisely, a *subgroup perfect code* of a group G is a subgroup of G and a perfect code of some Cayley sum graph of G. We give a necessary and sufficient condition for a non-trivial subgroup of an abelian group with non-trivial Sylow 2-subgroup to be a subgroup perfect code of the group (see Theorem 3.1). This reduces the problem of determining when a given subgroup of an abelian group is a perfect code to the case of abelian 2-groups. As an application, we classify the abelian groups whose every non-trivial subgroup is a subgroup perfect code (see Theorem 3.5). Also, we determine all subgroup perfect codes of a cyclic group (see Theorem 3.7), a dihedral group (see Theorem 4.1) and a generalized quaternion group (see Theorem 5.1).

2 Preliminaries

This section contains some technical lemmas required for the proofs of our main results. We always use G to denote a finite group having at least two elements, and let e denote its identity element. The *order* of an element g of G is defined as the cardinality of the cyclic subgroup $\langle g\rangle$, and is denoted by $o(g)$. Let H be a subgroup of G. The *index* of H in G, denoted by $[G : H]$, is the number of right (or left) cosets of H in G. A *right transversal* of H in G is a subset of G which contains exactly one element from each right coset of H. If G is abelian, since every right coset of H is a left coset, we use the term “transversal” to refer to a right transversal. A subgroup K of G is called a *Hall* $2'$*-subgroup* if $[G : K]$ is the order of a Sylow 2-subgroup of G. Note that, for an abelian group G, the Sylow 2-subgroup consists of the elements of G with order a power of 2, and the Hall $2'$-subgroup consists of the elements of G with odd order. For subsets S, T of G, write

$$S^{-1} = \{s^{-1} : s \in S\}, \qquad ST = \{st : s \in S, t \in T\}.$$

If $S = \{s\}$, then we denote ST and TS simply by sT and Ts, respectively.

It is easy to see that every non-trivial element of a group is a non-square if and only if the group is an elementary abelian 2-group. So a Cayley sum graph $\mathrm{CayS}(G, S)$ is complete if and only if G is an elementary abelian 2-group and $S = G \setminus e$. This also means that the trivial subgroup $\{e\}$ of a group is a subgroup perfect code of the group if and only if the group is an elementary abelian 2-group. Moreover, the whole group G is a perfect code in the empty Cayley sum graph $\mathrm{CayS}(G, \emptyset)$. As a result, any group is a subgroup perfect code of the group. Thus, in the following we always consider the non-trivial subgroup perfect codes of a group.

Lemma 2.1 *Let S and H be a square-free normal subset and a subgroup of G, respectively. The following are equivalent.*

(i) *H is a perfect code of* $\mathrm{CayS}(G, S)$.
(ii) *$S \cup \{e\}$ is a right transversal of H in G.*
(iii) *$[G : H] = |S| + 1$ and $H \cap (S \cup SS^{-1}) = \{e\}$.*

Proof Assume (i), that is H is a perfect code of $\mathrm{CayS}(G, S)$. By the definitions of a perfect code and a Cayley sum graph, it is easy to see that

$$\bigcup_{s \in S \cup \{e\}} Hs = G. \tag{1}$$

Note that S is square-free in G. If $h_1 = h_2 s$ for two distinct $h_1, h_2 \in H$ and some $s \in S$, then $h_2^{-1} \neq h_1$ and $h_2^{-1} h_1 \in S$, and so h_2^{-1} and h_1 are adjacent in $\mathrm{CayS}(G, S)$, which contradicts that H is independent. We conclude that $H \cap HS = \emptyset$. If $h_1 s_1 = h_2 s_2$ for two distinct $s_1, s_2 \in S$ and some $h_1, h_2 \in H$, then $h_1 \neq h_2$, $h_1^{-1} \neq h_1 s_1$ and $h_2^{-1} \neq h_2 s_1$, which implies that both h_1^{-1} and h_2^{-1} are adjacent to $h_1 s_1$ in $\mathrm{CayS}(G, S)$, a contradiction. We deduce that $Hs_1 \cap Hs_2 = \emptyset$ for each two distinct $s_1, s_2 \in S$. It follows from (1) that (ii) holds. Also, by the definition of a perfect code, it is easy to check that (ii) implies (i). It follows that (i) and (ii) are equivalent.

In the following we show that (ii) and (iii) are equivalent. Suppose first that $S \cup \{e\}$ is a right transversal of H in G. Note that $e \notin S$. Then $[G : H] = |S| + 1$. Taking $h \in H \cap (S \cup SS^{-1})$, we have $h \notin S$. It follows that $h \in SS^{-1}$. Therefore, there exist $s_1, s_2 \in S$ such that $h = s_1 s_2^{-1}$, and so $Hs_2 = Hs_1$. This means that $s_1 = s_2$, and hence $h = e$. It follows that $H \cap (S \cup SS^{-1}) = \{e\}$, and so (iii) follows.

Suppose next that $[G : H] = |S| + 1$ and $H \cap (S \cup SS^{-1}) = \{e\}$. Let s_1 and s_2 be two distinct elements of S. If there exist $h_1, h_2 \in H$ such that $h_1 s_1 = h_2 s_2$, then $s_2 s_1^{-1} = h_2^{-1} h_1 \in H \cap (S \cup SS^{-1})$, so $s_2 s_1^{-1} = e$, and hence $s_1 = s_2$, a contradiction. It follows that $Hs_1 \neq Hs_2$. Also, if there exist $h_1, h_2 \in H$ such that $h_1 = h_2 s_1$, then $s_1 = h_2^{-1} h_1 \in H \cap (S \cup SS^{-1})$, and hence $s_1 = e$, a contradiction. We conclude that $H \neq Hs_1$. Now $[G : H] = |S| + 1$ implies that $S \cup \{e\}$ is a right transversal of H in G, and so (ii) follows. Thus, (ii) and (iii) are equivalent. The proof is now complete. □

Lemma 2.2 *If H is a subgroup perfect code of G, then for any $g \in G \setminus H$, Hg has at least one non-square element in G.*

Proof Suppose that H is a perfect code of $\mathrm{CayS}(G, S)$ for some square-free normal subset S of G. For any $g \in G \setminus H$, by Lemma 2.1, there exists $s \in S$ such that $g \in Hs$. Namely, $Hg = Hs$, which implies that Hg has a non-square element s in G, as desired. □

For a subset S of G, write

$$\overline{S} = \sum_{g \in G} \mu_S(g) g \in \mathbb{Z}[G],$$

where $\mathbb{Z}[G]$ is the group ring of G over the ring of integers $\mathbb{Z}$ and

$$\mu_S(g) = \begin{cases} 1, & \text{if } g \in S; \\ 0, & \text{if } g \notin S. \end{cases}$$

The following result is immediate by Lemma 2.1.

Lemma 2.3 *Let* $\mathrm{CayS}(G, S)$ *be a Cayley sum graph of* G*, and let* H *be a subgroup of* G*. Then* H *is a perfect code of* $\mathrm{CayS}(G, S)$ *if and only if* $\overline{H} \cdot \overline{S \cup \{e\}} = \overline{G}$*.*

The proof of the following result is straightforward.

Lemma 2.4 *Let* $G_1, G_2, \ldots, G_n$ *be* n *groups and let* H_i *be a subgroup of* G_i *for each* $1 \leq i \leq n$*. Suppose that* C_i *is a right transversal of* H_i *in* G_i *for each* $1 \leq i \leq n$*. Then* $C_1 \times C_2 \times \cdots \times C_n$ *is a right transversal of* $H_1 \times H_2 \times \cdots \times H_n$ *in* $G_1 \times G_2 \times \cdots \times G_n$*.*

Finally, we give a necessary condition for a normal subgroup of a group to be a perfect code in some Cayley sum graph of the group.

Proposition 2.5 *Let* N *be a normal subgroup of* G*. Suppose that* N *is a perfect code of some Cayley sum graph* $\mathrm{CayS}(G, S)$*. Then for any* $g \in G \setminus (S \cup N)$*, there exists* $n \in N \setminus \{e\}$ *such that* $gn = ng$*.*

Proof By Lemma 2.1, $S \cup \{e\}$ is a right transversal of N in G. Since $g \notin N$, it follows that there exists an element s of S such that $g \in Ns$. Note that $g \notin S$. We may assume that $g = ns$ for some $n \in N \setminus \{e\}$. Then $Ng = Ns$. Also, since N is normal, we have $Ng^{-1} = Ns^{-1}$. It follows that

$$Ng^{-1}sg = (Ns^{-1})sg = Ng = Ns.$$

Since S is a normal subset, it follows that $g^{-1}sg \in S$, and hence $g^{-1}sg = s$. Note that $s = n^{-1}g$. We deduce $gn = ng$, as desired. □

3 Abelian groups

For any abelian group G of odd order, since $\{g^2 : g \in G\} = G$, we have that G has no non-square elements. Thus, in order to study the Cayley sum graph of an abelian group, we always assume that the abelian group has even order.

In this section, we give a necessary and sufficient condition for a non-trivial subgroup of an abelian group with non-trivial Sylow 2-subgroup to be a subgroup perfect code of the group (see Theorem 3.1). This reduces the problem of determining when a given subgroup of an abelian group is a perfect code to the case of abelian 2-groups. As an application, we classify the abelian groups whose every non-trivial subgroup is a subgroup perfect code (see Theorem 3.5). We also determine all subgroup perfect codes of a cyclic group (see Theorem 3.7).

Theorem 3.1 *Let* G *be an abelian group with non-trivial Sylow* 2*-subgroup* P*, and let* H *be a non-trivial subgroup of* G*. Then* H *is a subgroup perfect code of* G *if and only if one of the following occurs:*

(i) $P \subseteq H$.
(ii) $[G : H] = |P|$ *and* P *is elementary abelian.*
(iii) $H \cap P$ *is a non-trivial subgroup perfect code of* P*, and either* $[G : H]$ *is a power of* 2 *or* $H \cap P$ *has a non-square element in* G*.*

Proof Let $G = P \times Q$, where Q is the Hall $2'$-subgroup of G and consists of the elements of G with odd order. Clearly, $H \cap P$ is the Sylow 2-subgroup of H. Now let $H = P_1 \times Q_1$, where $P_1 = H \cap P$ and Q_1 consists of the elements of H with odd order. We have that Q_1 is a subgroup of Q.

We first prove the necessity. Suppose that H is a subgroup perfect code of G. Namely, G has a square-free subset S such that H is a perfect code of $\mathrm{CayS}(G, S)$. Write $S = \{(p_1, q_1), \ldots, (p_s, q_s)\}$, which is a subset of $P \times Q$. Lemma 2.1 implies that $S \cup \{(e, e)\}$ is a transversal of H in G. Observe that an element (a, b) of $P \times Q$ is a non-square if and only if a is a non-square in P.

Suppose that $|H \cap P| = 1$, that is, H is of odd order. If $H \subsetneq \{e\} \times Q$, choose $q \in Q \setminus Q_1$, it follows that every element of $H(e, q)$ is a square, contrary to Lemma 2.2. We conclude that $H = \{e\} \times Q$. Now take $x \in P \setminus \{e\}$. Then each element of $H(x, e)$ has form (x, q) for some $q \in Q$. Note that $H \neq H(x, e)$. It follows from Lemma 2.2 that x must be non-square in P. As a result, every non-trivial element of P is non-square, it follows that P has no elements of order 4, and hence we deduce that P is elementary abelian. So in this case (ii) occurs.

Suppose that $|H \cap P| \neq 1$. In order to prove the necessity, it suffices to show that if $P_1 \subsetneq P$, then (iii) occurs. So we now assume that $P_1 \subsetneq P$. Let S_1 be the set consisting of all elements in $\{p_1, \ldots, p_s\}$ satisfying that $P_1 \neq P_1 p_i$, $P_1 \neq P_1 p_j$ and $P_1 p_i \neq P_1 p_j$ for each two distinct indices $i, j \in \{1, \ldots, s\}$. Since $S \cup \{(e, e)\}$ is a transversal of H in G, we deduce that $S_1 \cup \{e\}$ is a transversal of P_1 in P. It follows that S_1 is a square-free subset of P, and hence P_1 is a subgroup perfect code of P by Lemma 2.1. Now suppose that $[G : H]$ is not a power of 2. It suffices to prove that $H \cap P$ has a non-square element in G. Note that $Q_1 \subsetneq Q$. Taking an element $q' \in Q \setminus Q_1$, we have $(e, q') \notin P_1 \times Q_1$. It follows by Lemma 2.2 that $H(e, q')$ has a non-square element in G, and so P_1 has a non-square element in P, which implies that $H \cap P$ has a non-square element in G, as desired.

We next prove the sufficiency. Take a transversal $S_2 = \{q_0, q_1, \ldots, q_t\}$ of Q_1 in Q, where $q_0 = e$. We consider the following cases.

Case 1. $P \subseteq H$, that is, $P_1 = P$.

Taking an element p in P such that $o(p) = \max\{o(g) : g \in P\}$, we see easily that p is a non-square element of P. Then $S = \{(p, q_1), \ldots, (p, q_t)\}$ is a square-free subset of G. Also, from Lemma 2.4, it follows that $\{(p, e)\} \cup S$ is a transversal H in G, and so H is a perfect code of $\mathrm{CayS}(G, S)$, as required.

Case 2. $[G : H] = |P|$ and P is elementary abelian.

Let $S = \{(p, e) : p \in P \setminus \{e\}\}$. Since P is elementary abelian, we deduce that S is square-free in G. Observe that $\{(e, e)\} \cup S$ is a transversal of H in G. So H is a perfect code of $\mathrm{CayS}(G, S)$, as required.

Case 3. $H \cap P$ is non-trivial and is a perfect code of P, and either $[G : H]$ is a power of 2 or $H \cap P$ has a non-square element in G.

In this case, there exists a square-free subset $S_1 = \{p_1, \ldots, p_l\}$ in P such that P_1 is a perfect code of $\mathrm{CayS}(P, S_1)$. Note that $P_1 \subsetneq P$. Suppose that P_1 has a non-square element p in G. Lemma 2.1 implies $p \notin S_1$. By Lemma 2.4,

$$S = \{(x, y) : x \in S_1 \cup \{p\}, y \in S_2\}$$

is a transversal of H in G. Observe that S is square-free in G. It follows that H is a perfect code of $\mathrm{CayS}(G, S \setminus \{(p, e)\})$, as required.

Suppose now that $[G : H]$ is a power of 2. Then $Q_1 = Q$. It is readily seen that

$$S' = \{(x, e) : x \in S_1 \cup \{e\}\}$$

is a transversal of H in G. Also, we have that $S' \setminus \{(e, e)\}$ is a square-free subset of G. We conclude that H is a perfect code of $\mathrm{CayS}(G, S' \setminus \{(e, e)\})$. The proof is now complete. □

The following result is immediate by Theorem 3.1.

Corollary 3.2 *An abelian group has a subgroup perfect code of odd order if and only if the Sylow 2-subgroup of the group is an elementary abelian 2-group and the subgroup perfect code is the Hall $2'$-subgroup of the group.*

As an application of Theorem 3.1, we determine all subgroup perfect codes of the direct product of an elementary abelian 2-group and an abelian group of odd order.

Corollary 3.3 *Let $G = \mathbb{Z}_2^n \times Q$, where $n \geq 1$ and Q is a non-trivial abelian group of odd order. Then a non-trivial subgroup of G is a subgroup perfect code of G if and only if the subgroup is not a proper subgroup of Q.*

Proof The necessity follows trivially from Theorem 3.1. We now prove the sufficiency. Let H be a non-trivial subgroup of G. Suppose that H is not a proper subgroup of Q. It is clear that if $H = Q$, then by Theorem 3.1, H is a subgroup perfect code of G. Thus, in the following we may assume that $H = P_1 \times Q_1$, where P_1 is the Sylow 2-subgroup of H and Q_1 is the Hall $2'$-subgroup of H. Note that $P_1 \neq \{e\}$ and $Q_1 \subseteq Q$. Let P be the Sylow 2-subgroup of G. Then $P \cong \mathbb{Z}_2^n$, $P_1 \subseteq P$ and $H \cap P = P_1$. If $P_1 = P$, then $P \subseteq H$, and so H is a subgroup perfect code of G by Theorem 3.1. We now assume that $P_1 \subsetneq P$. Notice that P is elementary abelian. It follows that P_1 is a non-trivial subgroup perfect code of P. Taking a non-identity element $x \in P_1$, we have that x is non-square in G, and so H is a subgroup perfect code of G by Theorem 3.1. $\square$

The following result determines a family of subgroup perfect codes of an abelian 2-group.

Lemma 3.4 *Suppose that $G_1, G_2, \ldots, G_n$ are n cyclic 2-groups. Let $G = G_1 \times G_2 \times \cdots \times G_n$ and $H = H_1 \times H_2 \times \cdots \times H_n$ is a non-trivial subgroup of G, where H_i is a subgroup of G_i for all $1 \leq i \leq n$. Then H is a subgroup perfect code of G if and only if either $|G_i| = 2|H_i|$ for all $1 \leq i \leq n$ or there exists j in $\{1, 2, \ldots, n\}$ such that $H_j = G_j$.*

Proof For every $1 \leq i \leq n$, let $G_i = \langle g_i \rangle$ and $C_i = \{e, g_i\}$. We first prove the sufficiency. Suppose that $|G_i| = 2|H_i|$ for each $1 \leq i \leq n$. Clearly, C_i is a transversal of H_i in G_i. Let $C = C_1 \times C_2 \times \cdots \times C_n$. By Lemma 2.4, C is a transversal of H in G. Since g_i is non-square in G_i, it follows that $C \setminus \{(e, \cdots, e)\}$ is a square-free subset of G. By Lemma 2.1, it follows that H is a perfect code of $\mathrm{CayS}(G, C \setminus \{(e, \cdots, e)\})$, as desired.

Now suppose that there exists j in $\{1, 2, \ldots, n\}$ such that $H_j = G_j$. Without loss of generality, we may assume $j = 1$. For every $2 \leq t \leq n$, let D_t be a transversal of H_t in G_t such that $e \in D_t$. Write $D = \{g_1\} \times D_2 \times D_3 \times \cdots \times D_n$. It follows from Lemma 2.4 that D is a transversal of H in G. Observe that D is square-free in G. So H is a perfect code of $\mathrm{CayS}(G, D \setminus \{(g_1, e, \cdots, e)\})$ by Lemma 2.1, as required.

We next prove the necessity. Suppose that H is a perfect code of G. Assume that $H_i \subsetneq G_i$ for each $1 \leq i \leq n$. It suffices to prove that $[G_i : H_i] = 2$ for each $1 \leq i \leq n$. Assume, to the contrary, that there exists $j \in \{1, 2, \ldots, n\}$ such that $[G_j : H_j] \neq 2$. Without loss of generality, say $j = 1$. Then $g_1^2 \notin H_1$, and so $(g_1^2, e, \cdots, e) \notin H$. Note that for every $1 \leq i \leq n$, every element of H_i is a square in G_i. It is easy to see that every element of $H(g_1^2, e, \cdots, e)$ is a square in G. Now from Lemma 2.2, it follows that H is not a perfect code of G, a contradiction. $\square$

As mentioned before, every non-trivial element of an elementary abelian 2-group $\mathbb{Z}_2^n$ is a non-square. Thus, for any non-trivial subgroup H of $\mathbb{Z}_2^n$, we choose a transversal $S \cup \{e\}$ of H in $\mathbb{Z}_2^n$, Lemma 2.1 implies that H is a perfect code of $\mathrm{CayS}(G, S)$. This means that it may happen that every non-trivial subgroup of a given abelian group is a subgroup perfect code of the group.

We now classify the abelian groups whose every non-trivial subgroup is a subgroup perfect code.

Theorem 3.5 *Let G be an abelian group. Every non-trivial subgroup of G is a subgroup perfect code of G if and only if G is isomorphic to one of the following groups:*

(a) $\mathbb{Z}_2^n$*, where* $n \geq 2$*;*
(b) $\mathbb{Z}_2^n \times \mathbb{Z}_4$*, where* $n \geq 1$*;*
(c) $\mathbb{Z}_2^n \times \mathbb{Z}_p$*, where* $n \geq 1$ *and p is an odd prime.*

Proof We first prove the sufficiency. We already know that every non-trivial subgroup of an elementary abelian 2-group is a subgroup perfect code. Also, by Corollary 3.3, every non-trivial subgroup of a group in (c) is a subgroup perfect code of the group. Now we suppose that $G \cong \mathbb{Z}_2^n \times \mathbb{Z}_4$, where $n \geq 1$. It follows that G has precisely one non-trivial square element, say x. Then $o(x) = 2$. Let H be a non-trivial subgroup of G. Take a transversal S of H in G such that $e \in S$. If $x \notin S$, then $S \setminus \{e\}$ is square-free, and so by Lemma 2.1, H is a perfect code of $\mathrm{CayS}(G, S \setminus \{e\})$, as desired. Assume now that $x \in S$. Then $Hx \neq H$. Taking a non-identity element $h \in H$, we have that $hx \neq x$ and $hx \in Hx$. It follows that $(S \cup \{hx\}) \setminus \{x\}$ is a transversal S of H in G and is square-free, and so H is a perfect code of $\mathrm{CayS}(G, (S \cup \{hx\}) \setminus \{e, x\})$, as required.

We now prove the necessity. Suppose that every non-trivial subgroup of G is a subgroup perfect code of G. Suppose that G is not a 2-group. Then G has a non-trivial subgroup Q of odd prime order, which is a subgroup perfect code of G. By Corollary 3.2, we have that $G \cong \mathbb{Z}_2^n \times Q \cong \mathbb{Z}_2^n \times \mathbb{Z}_p$, where $n \geq 1$ and p is an odd prime, as desired.

Suppose that G is a 2-group and has some elements of order 4. It is enough to show that G is isomorphic to a group in (b). Note that G is abelian. Note that every finite abelian group is a direct product of some cyclic groups. Thus, we may assume that

$$G \cong \mathbb{Z}_2^{t_1} \times \mathbb{Z}_{2^2}^{t_2} \times \cdots \times \mathbb{Z}_{2^k}^{t_k}, \tag{2}$$

where $k \geq 2$, $t_k > 0$ and $t_i \geq 0$ for all $1 \leq i \leq k-1$. Suppose for a contradiction that $k \geq 3$. Then we may say $G \cong G_1 \times G_2 \times \cdots \times G_n$, where G_i is a cyclic 2-group for each $1 \leq i \leq n$, and $G_n \cong \mathbb{Z}_{2^k}$. Let H_n be a subgroup of G_n of order 2. For each $1 \leq j \leq n$, let E_j be the trivial subgroup of G_j of order 1. Then $H = E_1 \times E_2 \times \cdots \times E_{n-1} \times H_n$ is a subgroup of $G_1 \times G_2 \times \cdots \times G_{n-1} \times G_n$. It follows from Lemma 3.4 that H is not a subgroup perfect code of G, a contradiction.

We conclude that $k = 2$. Suppose for a contradiction that $t_2 \geq 2$. Then we may assume that $G \cong G_1 \times G_2 \times \cdots \times G_{n-2} \times G_{n-1} \times G_n$, where G_i is either a cyclic group of order 2 or a cyclic group of order 4 for each $1 \leq i \leq n-2$, and $G_{n-1} \cong G_n \cong \mathbb{Z}_4$. Let H_n be a subgroup of G_n of order 2. Then $H = E_1 \times E_2 \times \cdots \times E_{n-1} \times H_n$ is a subgroup of $G_1 \times G_2 \times \cdots \times G_{n-1} \times G_n$. From Lemma 3.4, it follows that H is not a subgroup perfect code of G, a contradiction.

We conclude that $k = 2$ and $t_2 = 1$ in (2), which implies that G is isomorphic to a group in (b), as desired. □

The next result is obtained by applying Lemma 3.4 to a cyclic 2-group.

Lemma 3.6 *Let G be a cyclic group of order* 2^k *with* $k \geq 2$*, and let H be a non-trivial subgroup of G. Then H is a subgroup perfect code of G if and only if* $[G : H] = 2$.

The following result determines all subgroup perfect codes of a cyclic group.

Theorem 3.7 *Let $G = \langle x \rangle$ be the cyclic group of even order n, and let $H = \langle x^t \rangle$ be a non-trivial subgroup of G with t dividing n. Then H is a subgroup perfect code of G if and only if t is either an odd number or 2.*

Proof We first prove the necessity. Suppose that H is a subgroup perfect code of G. Then there exists a square-free subset S of G such that H is a perfect code of $\mathrm{CayS}(G, S)$. It suffices to show that if t is even, then $t = 2$. Now Let t be even. Assume, to the contrary, that $t \geq 4$. By Lemma 2.1, $S \cup \{e\}$ is a transversal of H in G. Note that an element x^l of G is non-square if and only if l is odd. Since $x^2 \notin H$, we deduce $x^2 \in Hs$ for some $s \in S$. It follows that $x^2 = hx^l$ for some odd positive integer l and $h \in H$, which is impossible as t is even. We conclude that $t = 2$, as desired.

We next prove the sufficiency. If G is a 2-group, then $t = 2$, and so H is a subgroup perfect code of G by Lemma 3.6, as desired. Thus, in the following we may assume that $G \cong \mathbb{Z}_{2^m} \times \mathbb{Z}_r$, where $m \geq 1$ and r is an odd number at least 3. Since H is a non-trivial subgroup of G, we have $t \neq 1$. Let P be the Sylow 2-subgroup of G. If t is odd, then $P \subseteq H$, and so H is a subgroup perfect code of G by Theorem 3.1, as desired. Now suppose that $t = 2$. If $m = 1$, then H is the Hall $2'$-subgroup of G and P is elementary abelian, and Theorem 3.1 implies that H is a subgroup perfect code of G. Thus, we may assume that $m \geq 2$. Then $[P : H \cap P] = 2$ and $[G : H]$ is a power of 2. Combining Theorem 3.1 and Lemma 3.6, we have that H is a subgroup perfect code of G, as desired. □

We conclude the section by the following example to illustrate Theorem 3.7.

Example 3.8 Let $G = \mathbb{Z}_{12}$. Then by Theorem 3.7, $\langle 3 \rangle$ and $\langle 2 \rangle$ are all non-trivial subgroup perfect codes of G. In particular, $\langle 3 \rangle$ is a perfect code of $\mathrm{CayS}(G, \{1, 5\})$, and $\langle 2 \rangle$ is a perfect code of $\mathrm{CayS}(G, \{1\})$.

4 Dihedral groups

The dihedral group D_{2n} of order $2n$ is defined by

$$D_{2n} = \langle a, b : a^n = b^2 = e, bab = a^{-1} \rangle, \quad n \geq 3. \tag{3}$$

This section will determine all subgroup perfect codes of a dihedral group, the main result is as follows.

Theorem 4.1 *Let H be a non-trivial subgroup of D_{2n}. Then H is a subgroup perfect code of D_{2n} if and only if one of the following holds:*

(i) *$\frac{n}{2}$ is odd and either $H = \langle a^{\frac{n}{2}} \rangle$ or $H = \langle a^2, a^s b \rangle$ with $0 \leq s \leq 1$.*
(ii) *n is even and $H = \langle a^t, a^s b \rangle$ with an odd integer t dividing n, $t > 1$ and $0 \leq s \leq t - 1$.*

In this section, the letters a, b and D_{2n} are always as refer to (3). Remark that $o(a^i b) = 2$ for each $1 \leq i \leq n$ and

$$D_{2n} = \langle a \rangle \cup \{b, ab, a^2 b, \ldots, a^{n-1} b\}.$$

Furthermore, it is not hard to see that the subgroups of D_{2n} are the cyclic subgroups $\langle a^t \rangle$ with t dividing n, and the groups $\langle a^t, a^s b \rangle$ with t dividing n and $0 \leq s \leq t - 1$, where $\langle a^t, a^s b \rangle$ is either an abelian group (isomorphic to $\mathbb{Z}_2$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$) or a dihedral group.

Lemma 4.2 ([14, p. 108]) *Suppose that $n = 2m$ for some positive integer m at least 2. Then D_{2n} has $m + 3$ conjugacy classes as follows:*

$$\{e\}, \{a^m\}, \{a^{i-1}, a^{-i+1}\}, [b] = \{a^{2j}b : 0 \le j \le m-1\}, [ab] = \{a^{2j+1}b : 0 \le j \le m-1\},$$

where $2 \le i \le m$.

Lemma 4.3 *Let n be an even integer at least 4, and let $\langle a^t, a^s b\rangle$ be a non-trivial subgroup of D_{2n}, where t divides n and $0 \le s \le t-1$. Then $\langle a^t, a^s b\rangle$ is a subgroup perfect code of D_{2n} if and only if either t is odd, or $t = 2$ and $\frac{n}{2}$ is odd.*

Proof Write $G = D_{2n}$ and $H = \langle a^t, a^s b\rangle$. Let $n = 2m$ for some $m \ge 2$. Note that $|H| = \frac{2n}{t}$ and $[G : H] = t$.

Suppose first that t is an odd integer. Note that

$$\overline{H} = (e + a^t + a^{2t} + \cdots + a^{n-t})(e + a^s b).$$

Let $S = \{a, a^{-1}, a^3, a^{-3}, \ldots, a^{t-2}, a^{-(t-2)}\}$. Observe that $|S| = t-1$ and S is a square-free subset of G. Also, Lemma 4.2 implies that S is a normal subset of G. Furthermore, we have

$$\begin{aligned}
&\overline{H} \cdot \overline{S \cup \{e\}}\\
&= (e + a^t + a^{2t} + \cdots + a^{n-t})(e + a^s b)\\
&\quad \times (e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{2-t})\\
&= (e + a^t + a^{2t} + \cdots + a^{n-t})(e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{2-t})\\
&\quad + (e + a^t + a^{2t} + \cdots + a^{n-t})a^s b(e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{2-t})\\
&= (e + a + a^2 + \cdots + a^{n-1}) +\\
&\quad + a^s(e + a^t + a^{2t} + \cdots + a^{n-t})(e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{2-t})b\\
&= (e + a + a^2 + \cdots + a^{n-1}) + a^s(e + a + a^2 + \cdots + a^{n-1})b\\
&= \overline{G}.
\end{aligned}$$

It follows from Lemma 2.3 that H is a perfect code of $\mathrm{CayS}(G, S)$, as desired.

Suppose now that $t = 2$ and m is odd. Let $S' = \{a^m\}$. Clearly, S' is a square-free normal subset of G. Moreover,

$$\begin{aligned}
&\overline{H} \cdot \overline{S' \cup \{e\}}\\
&\quad = (e + a^2 + a^4 + \cdots + a^{n-2})(e + a^s b)(e + a^m)\\
&\quad = (e + a^2 + a^4 + \cdots + a^{n-2})(e + a^m) + (e + a^2 + a^4 + \cdots + a^{n-2})a^s b(e + a^m)\\
&\quad = (e + a + a^2 + \cdots + a^{n-1}) + a^s(e + a^2 + a^4 + \cdots + a^{n-2})(e + a^{-m})b\\
&\quad = (e + a + a^2 + \cdots + a^{n-1}) + a^s(e + a + a^2 + \cdots + a^{n-1})b\\
&\quad = \overline{G}.
\end{aligned}$$

By Lemma 2.3, we deduce that H is a perfect code of $\mathrm{CayS}(G, S')$, as required.

For the converse, let S be a square-free normal subset of G such that H is a perfect code of $\mathrm{CayS}(G, S)$. Suppose that t is an even integer. It suffices to show that $t = 2$ and m is odd.

Suppose that $|H| = 2$, that is, $H = \{e, a^s b\}$. Then $|S| = 2m-1$. From Lemma 4.2, it follows that m is odd, and so S is the union of

$$T = \{a^i : i \ne m, i = 2j+1, 0 \le j \le m-1\}$$

and one of $[b]$ and $[ab]$. Note that $a^{s-l} \in Ha^l b$ for any $0 \le l \le n-1$. Assume that s is even. Since $S \cup \{e\}$ is a right transversal of H in G by Lemma 2.1, we have $a^s b \notin S$, and so

$[ab] \subseteq S$. It follows that there exists an odd integer $k \in \{0, 1, \ldots, n-1\}$ such that $a^{s-k} \in T$, which implies that $Ha^kb = Ha^{s-k}$. However, $\{a^{s-k}, a^kb\} \subseteq S$, contrary to Lemma 2.1 (ii). Similarly, if s is odd, we obtain also a contradiction.

We conclude that $|H| \geq 4$. It follows that

$$|S| + 1 = t = \frac{4m}{|H|} \leq m,$$

and so $|S|$ is odd. Note that S is a square-free normal subset of G. By Lemma 4.2, we deduce

$$S \subseteq \{a^i : i = 2j + 1, 0 \leq j \leq m - 1\},$$

which implies that $a^m \in S$ and so m is odd.

Now it is enough to prove $t = 2$. Assume, to the contrary, that $t \geq 4$. Then $|S| \geq 3$. By Lemma 2.1, it is easy to see $S \cup \{e\}$ is a right transversal of $\langle a^t \rangle$ in $\langle a \rangle$. It follows that $a^2 \in \langle a^t \rangle a^i$ for some $a^i \in S$. Consequently, we may assume that $a^2 = a^{kt+i}$ for some $1 \leq k \leq \frac{n}{t} - 1$. Note that i is odd. Since t is even, we deduce that n does not divide $kt + i - 2$, contrary to $a^2 = a^{kt+i}$. Thus, we have $t = 2$, as desired. The proof is now complete. □

Lemma 4.4 *Let n be an even integer at least 4, and let $\langle a^t \rangle$ be a non-trivial subgroup of D_{2n} with t dividing n. Then $\langle a^t \rangle$ is a subgroup perfect code of D_{2n} if and only if $n = 2t$ and t is odd.*

Proof Let $n = 2m$ for some $m \geq 2$. Suppose that $\langle a^t \rangle$ is a subgroup perfect code of D_{2n}. Then $\langle a^t \rangle$ is a perfect code of $\mathrm{CayS}(D_{2n}, S)$ for some square-free normal subset S of D_{2n}. By Lemmas 2.1 and 4.2, we deduce that only one of $[ab]$ and $[b]$ is contained in S. Set $S = T \cup L$, where $T = [ab]$ or $[b]$, and $L \subseteq \langle a \rangle$.

Suppose that $T = [ab]$. Then $b \in G \setminus (S \cup \langle a^t \rangle)$. Note that $\langle a^t \rangle$ is a normal subgroup of D_{2n}. By Proposition 2.5, we have that there exists $a^{rt} \in \langle a^t \rangle$ such that $ba^{rt} = a^{rt}b$, where r is a positive integer with $a^{rt} \neq e$. It follows that $a^{rt} = a^m \in \langle a^t \rangle$. If $T = [b]$, then $ab \in G \setminus (S \cup \langle a^t \rangle)$, and similarly, we have also $a^m \in \langle a^t \rangle$ by Proposition 2.5.

We conclude $a^m \in \langle a^t \rangle$. Now Lemma 2.1 also implies that $L \cup \{e\}$ is a right transversal of $\langle a^t \rangle$ in $\langle a \rangle$, and so $|L| = t - 1$. Since $[D_{2n} : \langle a^t \rangle] = 2t$, we conclude that

$$|S| = m + t - 1 = 2t - 1.$$

This means $m = t$, and so $\langle a^t \rangle = \{a^m, e\}$. Note that now $\langle a^t \rangle$ is a subgroup perfect code of $\langle a \rangle$. It follows from Theorem 3.7 that m is odd or $m = 2$. Now it suffices to prove $m \neq 2$. Suppose for a contradiction that $m = 2$. Then $n = 4$, and so $\langle a^2 \rangle$ is a perfect code of $\mathrm{CayS}(G, S)$. If $[b] = \{b, a^2b\} \subseteq S$, then $\langle a^2 \rangle b = \langle a^2 \rangle a^2b$, contrary to Lemma 2.1. Similarly, if $[ab] \subseteq S$, we obtain also a contradiction.

Conversely, suppose that $n = 2t$ and t is odd. Let

$$S = \{a, a^{-1}, a^3, a^{-3}, \ldots, a^{t-2}, a^{-(t-2)}, b, a^2b, \ldots, a^{n-2}b\}.$$

Observe that $|S| = 2t - 1$ and S is a square-free subset of D_{2n}. Also, Lemma 4.2 implies that S is a normal subset of G. Since t is odd, we have

$$\begin{aligned}
&\overline{\langle a^t \rangle} \cdot \overline{S \cup \{e\}} \\
&\quad = (e + a^t)(e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{-(t-2)} + b + a^2 b + \cdots + a^{n-2} b) \\
&\quad = (e + a^t)(e + a + a^{-1} + a^3 + a^{-3} + \cdots + a^{t-2} + a^{2-t}) \\
&\qquad + (e + a^t)(b + a^2 b + \cdots + a^{n-2} b) \\
&\quad = (e + a + a^2 + \cdots + a^{n-1}) + e(b + a^2 b + \cdots + a^{n-2} b) + a^t (b + a^2 b + \cdots + a^{n-2} b) \\
&\quad = (e + a + a^2 + \cdots + a^{n-1}) + (b + a^2 b + \cdots + a^{n-2} b) + (ab + a^3 b + \cdots + a^{n-1} b) \\
&\quad = \overline{D_{2n}}.
\end{aligned}$$

It follows from Lemma 2.3 that $\langle a^t \rangle$ is a perfect code of $\mathrm{CayS}(D_{2n}, S)$, as desired. □

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Combining Lemmas 4.3 and 4.4, we only need to show that if n is odd, then D_{2n} has no subgroup perfect codes. Now suppose that $n = 2m + 1$ for some positive integer m. Then D_{2n} has $m + 2$ conjugacy classes (cf. [14, p. 108]), as follows

$$\{e\}, \quad \{a^i, a^{-i}\}, \quad \{a^j b : 0 \leq j \leq 2m\},$$

where $1 \leq i \leq m$. It follows that if S is a square-free normal subset of D_{2n}, then $S = \{a^j b : 0 \leq j \leq 2m\}$. Suppose for a contradiction that H is a perfect code of $\mathrm{CayS}(D_{2n}, S)$. Then $|S| = 2m + 1$. Now Lemma 2.1 implies $[D_{2n} : H] = |S| + 1$. It follows that $|H|(m + 1) = 2m + 1$, which is impossible. □

We use the following example to illustrate Theorem 4.1.

Example 4.5 (i) Let $G = D_{24}$. Then by Theorem 4.1, $\langle a^3, b \rangle$, $\langle a^3, ab \rangle$ and $\langle a^3, a^2 b \rangle$ are all non-trivial subgroup perfect codes of G. In particular, by the proof of Lemma 4.3, we have that each of $\langle a^3, b \rangle$, $\langle a^3, ab \rangle$ and $\langle a^3, a^2 b \rangle$ is a perfect code of $\mathrm{CayS}(G, \{a, a^{11}\})$.

(ii) Let $G = D_{20}$. It follows from Theorem 4.1 that $\langle a^5 \rangle$, $\langle a^2, b \rangle$, $\langle a^2, ab \rangle$ and $\langle a^5, a^t b \rangle$ $(0 \leq t \leq 4)$ are all non-trivial subgroup perfect codes of G. Particularly, by the proofs of Lemmas 4.3 and 4.4, we have that $\langle a^5 \rangle$ is a perfect code of $\mathrm{CayS}(G, \{a, a^9, a^3, a^7, b, a^2 b, a^4 b, a^6 b, a^8 b\})$, each of $\langle a^2, b \rangle$ and $\langle a^2, ab \rangle$ is a perfect code of $\mathrm{CayS}(G, \{a^5\})$, and $\mathrm{CayS}(G, \{a, a^9, a^3, a^7\})$ admits $\langle a^5, a^t b \rangle$ as a perfect code for each $0 \leq t \leq 4$.

5 Generalized quaternion groups

We use Q_{4n} to denote the generalized quaternion group of order $4n$, where $n \geq 2$. It is well known (see, for example, [15, pp. 44–45]) that

$$Q_{4n} = \langle a, b : a^n = b^2, a^{2n} = 1, b^{-1} a b = a^{-1} \rangle, \quad n \geq 2. \tag{4}$$

The main result of this section determines all subgroup perfect codes of Q_{4n}.

Theorem 5.1 *Let H be a non-trivial subgroup of Q_{4n}. Then H is a subgroup perfect code of Q_{4n} if and only if one of the following holds:*

(i) *n is odd and $H = \langle a^n \rangle$.*

(ii) $H = \langle a^t, a^s b\rangle$ *with an odd integer* t *dividing* $2n$, $t > 1$ *and* $0 \leq s \leq t-1$.

In this section, the letters a, b and Q_{4n} are always as refer to (4). Remark that $o(a^i b) = 4$ for each $i \in \{1, \ldots, 2n\}$, and Q_{4n} has a unique involution a^n, and

$$Q_{4n} = \{e, a, \ldots, a^{2n-1}\} \cup \Big(\bigcup_{i=0}^{n-1}\{a^i b, (a^i b)^{-1}\}\Big).$$

It is not hard to see that the subgroups of Q_{4n} are $\langle a^t\rangle$ with t dividing $2n$, and $\langle a^t, a^s b\rangle$ with t dividing $2n$ and $0 \leq s \leq t-1$, where $\langle a^t, a^s b\rangle$ is either the cyclic group $\langle b\rangle$ or a generalized quaternion group.

Lemma 5.2 ([14, p. 420]) *Q_{4n} has $n+3$ conjugacy classes as follows:*

$$\{e\}, \{a^n\}, \{a^i, a^{-i}\}, [b] = \{a^{2j}b : 0 \leq j \leq n-1\}, [ab] = \{a^{2j+1}b : 0 \leq j \leq n-1\},$$

where $1 \leq i \leq n-1$.

Lemma 5.3 *Let $\langle a^t\rangle$ be a non-trivial subgroup of Q_{4n}, where t divides $2n$. Then $\langle a^t\rangle$ is a subgroup perfect code of Q_{4n} if and only if n is odd and $t = n$.*

Proof Let $G = Q_{4n}$ and $H = \langle a^t\rangle$. Suppose that H is a subgroup perfect code of G. Let S be a square-free normal subset of G such that H is a perfect code of $\mathrm{CayS}(G, S)$. By Lemma 2.1, $S \cup \{e\}$ is a right transversal of H in G, and according to Lemma 5.2, we may assume that

$$S = A \cup B,$$

where A consists of some non-square elements of $\langle a\rangle$, and B is exactly one of $[a]$ and $[ab]$. Thus, we have

$$|S| + 1 = n + |A| + 1 = [G : H] = 2t. \tag{5}$$

Moreover, it is easy to see that H is a perfect code of $\mathrm{CayS}(\langle a\rangle, A)$. Now Theorem 3.7 implies that t is either an odd integer or 2. If $t = 2$, then $n = 2$ and $|A| = 1$ by (5), and so $A = \{a^2\}$ by Lemma 5.2, which is impossible since a^2 is a square. We conclude that t is odd.

Suppose that $B = [b]$. If $|H| \geq 3$, then $b \neq a^{2t}b$ and $Ha^{2t}b = Hb$, which is impossible since $S \cup \{e\}$ is a right transversal of H in G. It follows that $|H| = 2$. Similarly, if $B = [ab]$, we obtain also $|H| = 2$. As a result, we have $t = n$, as desired.

Conversely, suppose that n is odd and $t = n$. Then $H = \{a^n, e\}$. Let

$$K = [ab], \quad L = \{a^{2i+1} : 0 \leq i \leq n-1\} \setminus \{a^n\}.$$

Then $L^{-1} = L$. Note that $(a^t b)^{-1} = a^{n+t}b$ for any $1 \leq t \leq 2n$. It is easy to see that

$$a^n \notin KL^{-1} \cup LK^{-1} \cup LL^{-1}. \tag{6}$$

Let i and j be two odd integers such that $a^i b \in K$ and $a^{n+j}b \in K^{-1}$, respectively. We have that $a^i b a^{n+j} b = a^i b b a^{-n-j} = a^{i-j}$, and so $a^i b a^{n+j} b \neq a^n$ since $i - j$ is even. It follows that

$$a^n \notin KK^{-1}. \tag{7}$$

Now let $S = K \cup L$. Observe that $|S| = 2n-1$ and $H \cap S = \emptyset$. Furthermore, S is a square-free normal subset of G by Lemma 5.2. Combining (6) and (7), we have $H \cap (S \cup SS^{-1}) = \{e\}$, which implies that H is a perfect code of $\mathrm{CayS}(G, S)$ by Lemma 2.1, as desired. ◻

Lemma 5.4 *Let $\langle a^t, a^s b\rangle$ be a non-trivial subgroup of Q_{4n}, where t divides $2n$ and $0 \le s \le t-1$. Then $\langle a^t, a^s b\rangle$ is a subgroup perfect code of Q_{4n} if and only if t is an odd integer.*

Proof Note that t is a divisor of $2n$. Since $\langle a^n, a^s b\rangle = \langle a^{2n}, a^s b\rangle = \langle a^s b\rangle$, we may assume that $t \le n$. Write $G = Q_{4n}$ and $H = \langle a^t, a^s b\rangle$. Then $|H|$ is even and $[G : H] = t$. Suppose that H is a subgroup perfect code of G. Then there exists a square-free normal subset S in G such that H is a perfect code of $\mathrm{CayS}(G, S)$. It follows from Lemma 2.1 that $|S| = t - 1 \le n - 1$, and so $S \subseteq \{a^{2i+1} : 0 \le i \le n-1\}$ by Lemma 5.2. Note that in this case $S \cup \{e\}$ is a right transversal of H in G. We deduce that $S \cup \{e\}$ is a right transversal of $\langle a^t\rangle$ in $\langle a\rangle$. By Theorem 3.7, t is either an odd integer or 2. Suppose for a contradiction that $t = 2$. Since H is a proper subgroup of G, we have $|H| = 2n$, and so $|S| = 1$. It follows that $S = \{a^n\}$ by Lemma 5.2, which is impossible since a^n is a square. We conclude that t is an odd integer.

For the converse, suppose that t is odd. By Theorem 3.7, there exists a square-free normal subset S in $\langle a\rangle$ such that $\langle a^t\rangle$ is a perfect code of $\mathrm{CayS}(\langle a\rangle, S)$. Lemma 2.1 implies $\langle a^t\rangle \cap (S \cup SS^{-1}) = \{e\}$, and so $H \cap (S \cup SS^{-1}) = \{e\}$. Since t is odd and divides $2n$, we have that t divides n. This implies that $a^n \in \langle a^t\rangle$, and so $a^n \notin S$. Observe that $|S| = t - 1$ and S is a square-free normal subset of G. In view of Lemma 2.1, H is a perfect code of $\mathrm{CayS}(G, S)$, as desired. The proof is now complete. □

Combining Lemmas 5.3 and 5.4, we complete the proof of Theorem 5.1.

We conclude the paper by the following example to illustrate Theorem 5.1.

Example 5.5 Let $G = Q_{20}$. By Theorem 5.1, $\langle a^5\rangle$ and $\langle a^5, a^s b\rangle$ $(0 \le s \le 4)$ are all non-trivial subgroup perfect codes of G. Also, it is easy to see that $\langle a^5\rangle$ is a perfect code of $\mathrm{CayS}(G, \{a, a^9, a^3, a^7, b, a^2b, a^4b, a^6b, a^8b\})$, and $\mathrm{CayS}(G, \{a, a^9, a^3, a^7\})$ admits $\langle a^5, a^s b\rangle$ as a perfect code for each $0 \le s \le 4$.

Acknowledgements We are grateful to the anonymous referees for their helpful comments which led to improvement of Section 3 and betterment of presentation of the paper. Ma was supported by the National Natural Science Foundation of China (Grant Nos. 11801441 and 61976244), the Natural Science Basic Research Program of Shaanxi (Program No. 2020JQ-761), and the Young Talent fund of University Association for Science and Technology in Shaanxi, China (Grant No. 20190507). Feng was supported by the National Natural Science Foundation of China (11701281), the Natural Science Foundation of Jiangsu Province (BK20170817) and the Grant of China Postdoctoral Science Foundation. Wang was supported by the National Natural Science Foundation of China (11671043).

References

1. Alon N.: Large sets in finite fields are sumsets. J. Number Theory **126**, 110–118 (2007).
2. Amooshahi M., Taeri B.: On Cayley sum graphs of non-abelian groups. Graphs Combin. **32**, 17–29 (2016).
3. Biggs N.L.: Perfect codes in graphs. J. Combin. Theory Ser. B **15**, 289–296 (1973).
4. Cheyne B., Gupta V., Wheeler C.: Hamilton cycles in addition graphs. Rose-Hulman Undergrad. Math J. **4**, 1–17 (2003). (electronic).
5. Chung F.R.K.: Diameters and eigenvalues. J. Am. Math. Soc. **2**, 187–196 (1989).
6. Dejter I.J., Serra O.: Efficient dominating sets in Cayley graphs. Discrete Appl. Math. **129**, 319–328 (2003).
7. Delsarte P.: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. **10**, 165, 171, 173 (1973).
8. Deng Y.-P., Sun Y.-Q., Liu Q., Wang H.-C.: Efficient dominating sets in circulant graphs. Discret. Math. **340**, 1503–1507 (2017).
9. DeVos M., Goddyn L., Mohar B., Šámal R.: Cayley sum graphs and eigenvalues of (3, 6)-fullerenes. J. Combin. Theory Ser. B **99**, 358–369 (2009).

10. Feng R., Huang H., Zhou S.: Perfect codes in circulant graphs. Discret. Math. **340**, 1522–1527 (2017).
11. Grynkiewicz D., Levb V.F., Serra O.: Connectivity of addition Cayley graphs. J. Combin. Theory Ser. B **99**, 202–217 (2009).
12. Heden O.: A survey of perfect codes. Adv. Math. Commun. **2**, 223–247 (2008).
13. Huang H., Xia B., Zhou S.: Perfect codes in Cayley graphs. SIAM J. Discret. Math. **32**, 548–559 (2018).
14. James G., Liebeck M.: Representations and Characters of Groups. Cambridge University Press, Cambridge (2001).
15. Johnson D.L.: Topics in the Theory of Group Presentations. London Mathematical Society Lecture Note Series, vol. 42. Cambridge University Press, Cambridge (1980).
16. Konyagin S.V., Shkredov I.D.: On subgraphs of random Cayley sum graphs. Eur. J. Comb. **70**, 61–74 (2018).
17. Kratochvíl J.: Perfect codes over graphs. J. Comb. Theory Ser. B **40**, 224–228 (1986).
18. Lee J.: Independent perfect domination sets in Cayley graphs. J. Graph Theory **37**, 213–219 (2001).
19. Lev V.F.: Sums and differences along Hamiltonian cycles. Discret. Math. **310**, 575–584 (2010).
20. Li C.-K., Nelson I.: Perfect codes on the towers of Hanoi graph. Bull. Aust. Math. Soc. **57**, 367–376 (1998).
21. Ma X., Wang K.: Integral Cayley sum graphs and groups. Discuss. Math. Graph Theory **36**, 797–803 (2016).
22. Mollard M.: On perfect codes in Cartesian products of graphs. Eur. J. Comb. **32**, 398–403 (2011).
23. van Lint J.H.: A survey of perfect codes. Rocky Mt. J. Math. **5**, 199–224 (1975).
24. Žerovnik J.: Perfect codes in direct products of cycles—a complete characterization. Adv. Appl. Math. **41**, 197–205 (2008).
25. Zhou S.: Total perfect codes in Cayley graphs. Des. Codes Cryptogr. **81**, 489–504 (2016).
26. Zhou S.: Cyclotomic graphs and perfect codes. J. Pure Appl. Algebra **223**, 931–947 (2019).