AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **81(3)** (2021), Pages 474–479

On non-normal subgroup perfect codes

Angelot Behajaina

Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Normandie BP 5186, 14032 Caen Cedex, France
angelot.behajaina@unicaen.fr

Roghayeh Maleki

Department of Mathematics and Statistics
University of Regina
Saskatchewan, Canada
rmaleki@uregina.ca

Andriaherimanana Sarobidy Razafimahatratra

Department of Mathematics and Statistics
University of Regina
Saskatchewan, Canada
sarobidy@phystech.edu

Abstract

Let $X = (V, E)$ be a graph. A subset $C \subseteq V(X)$ is a *perfect code* of X if C is a coclique of X with the property that any vertex in $V(X) \setminus C$ is adjacent to exactly one vertex in C. Given a finite group G with identity element e and $H \leq G$, H is a *subgroup perfect code* of G if there exists an inverse-closed subset $S \subseteq G \setminus \{e\}$ such that H is a perfect code of the Cayley graph $\mathrm{Cay}(G, S)$ of G with connection set S. In this short note, we give an infinite family of finite groups G admitting a non-normal subgroup perfect code H such that there exists $g \in G$ with $g^2 \in H$ but $(gh)^2 \neq e$, for all $h \in H$, thus answering a question raised by Wang, Xia, and Zhou in [arXiv:2006.05100, 2020].

1 Introduction

The notion of perfect codes is fundamental to coding theory. In 1973, Biggs [2] extended this concept for distance-transitive graphs, which led to various generalizations for association schemes and simple graphs [1, 3, 5, 10]. The generalization

ISSN: 2202-3518

of perfect codes for simple graphs is of particular interest to us. Given a graph $X = (V, E)$ and $t \in \mathbb{N}$, a subset $C \subseteq V(X)$ is a *perfect t-code* if for every vertex $x \in V(X)$, there exists exactly one vertex $c \in C$ which is at distance at most t from the vertex x. In particular, C is a *coclique* or an *independent set* of the graph X. A perfect 1-code of X is called a *perfect code*.

One can also extend the concept of perfect codes for groups. Given a finite group G with identity element e and a subset $S \subseteq G \setminus \{e\}$ which is inverse-closed (i.e., if $x \in S$ then $x^{-1} \in S$), the Cayley graph $\mathrm{Cay}(G, S)$ is the graph whose vertex set is the group G and whose edge set consists of pairs $(g, h) \in G \times G$ such that $hg^{-1} \in S$. As S is inverse-closed, the graph $\mathrm{Cay}(G, S)$ is a simple graph. A subset C of G is a perfect code of G if C is a perfect code of a Cayley graph of G. In other words, there exists an inverse-closed subset S of $G \setminus \{e\}$ such that C is a perfect code of $\mathrm{Cay}(G, S)$. If $H \leq G$ is a perfect code of G, then we say that H is a *subgroup perfect code* of G.

Perfect codes for groups have been well-studied in the past decade [4, 6–8, 14]. For instance, Huang, Xia, and Zhou [6] gave a necessary and sufficient condition for a normal subgroup to be a perfect code.

Theorem 1.1 ([6]). *Let G be a group with identity element e, and let $H \lhd G$. Then, H is a perfect code of G if and only if the following formula, $\Phi(G, H)$, holds:*

$$\forall g \in G \ (g^2 \in H) \Rightarrow \exists h \in H, (gh)^2 = e.$$

Throughout this paper, we use G to denote a finite group and e to denote the identity of G. In [11], Wang, Xia, and Zhou asked the following question.

Question 1.2. Does Theorem 1.1 still hold when H is a non-normal subgroup of G?

In this short note, we show that $\Phi(G, H)$ is no longer a necessary condition when H is not normal. Consequently, we give a negative answer to Question 1.2. To do this, we provide an infinite family of examples. Fix a positive integer $n \geq 1$. Set $q = 2^n$ and let α be a primitive element of the quadratic extension $\mathbb{F}_{q^2}/\mathbb{F}_q$. We have $\mathbb{F}_{q^2} = \mathbb{F}_q \oplus \mathbb{F}_q\alpha$. Consider the affine group

$$\mathrm{AGL}(2, q^2) := \left\{(a, A) \mid a \in \mathbb{F}_{q^2}^2 \text{ and } A \in \mathrm{GL}_2(\mathbb{F}_{q^2})\right\},$$

with multiplication $(a, A)(b, B) = (a + Ab, AB)$, for any $(a, A),\ (b, B) \in \mathrm{AGL}(2, q^2)$.

For any $T \subseteq \mathbb{F}_{q^2}$, we let $\begin{pmatrix} T \\ T \end{pmatrix}$ be the set of all vectors of $\mathbb{F}_{q^2}^2$ with entries in T. Let H_q be the subgroup of $\mathrm{AGL}(2, q^2)$ given by

$$H_q := \left\{ (b, \mathrm{I}_2) \in \mathrm{AGL}(2, q^2) \;\middle|\; b \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix} \right\},$$

where I_2 is the identity matrix. Our main result is stated as follows.

Theorem 1.3. *The subgroup H_q is a non-normal subgroup of $\mathrm{AGL}(2, q^2)$ which is a perfect code but $\Phi\left(\mathrm{AGL}(2, q^2), H_q\right)$ does not hold.*

2 Proof of Theorem 1.3

2.1 Main lemmas

We recall that when G is a group and H is a subgroup of G, then a subset $S \subset G$ is a *left transversal* of H in G if for any $g \in G$, we have $|gH \cap S| = 1$. A few general characterizations of subgroup perfect codes are given next.

Lemma 2.1 ([9]). *Let G be a group and $H \leq G$. Then, H is a perfect code of G if and only if H has an inverse-closed left transversal.*

Lemma 2.2. *[13, Corollary 3.3] Let G be a group and let $H \leq G$ be a 2-group. Then, H is a perfect code of G if and only if $\Phi(N_G(H), H)$ holds, where $N_G(H)$ is the normalizer of H in G.*

We note that a much stronger statement than Lemma 2.2 was first proved in [12, Theorem 3.1, Theorem 3.2]; however the proof contained an error. This was subsequently corrected in [13].

2.2 Proof of the main theorem

We first note that there exists $s \in \mathbb{F}_q$ and $t \in \mathbb{F}_q^*$ such that $\alpha^2 + s\alpha + t = 0$, or equivalently, $\alpha^2 = s\alpha + t$.

Lemma 2.3. *The property $\Phi\left(\mathrm{AGL}(2, q^2), H_q\right)$ does not hold.*

Proof. Let $g = \left(\begin{pmatrix} 0 \\ \alpha + s \end{pmatrix}, \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\right) \in \mathrm{AGL}(2, q^2)$. We have

$$g^2 = \left(\begin{pmatrix} \alpha^2 + s\alpha \\ 0 \end{pmatrix}, \mathrm{I}_2\right) = \left(\begin{pmatrix} s\alpha + t + s\alpha \\ 0 \end{pmatrix}, \mathrm{I}_2\right) = \left(\begin{pmatrix} t \\ 0 \end{pmatrix}, \mathrm{I}_2\right) \in H_q.$$

Let $h = \left(\begin{pmatrix} u \\ v \end{pmatrix}, \mathrm{I}_2\right) \in H_q$ with $u, v \in \mathbb{F}_q$. As $t \neq 0$, we have

$$\begin{aligned}(gh)^2 &= \left[\left(\begin{pmatrix} 0 \\ \alpha + s \end{pmatrix}, \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\right)\left(\begin{pmatrix} u \\ v \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\right]^2 \\ &= \left(\begin{pmatrix} u + v\alpha \\ \alpha + s + v \end{pmatrix}, \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\right)^2 \\ &= \left(\begin{pmatrix} v\alpha + t \\ 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq (0, \mathrm{I}_2).\end{aligned}$$

Consequently, $\Phi\left(\mathrm{AGL}(2, q^2), H_q\right)$ does not hold. ∎

Lemma 2.4. *The normalizer of H_q in $\mathrm{AGL}(2, q^2)$ is given by:*

$$N_{\mathrm{AGL}(2,q^2)}(H_q) = \left\{(a, A) \mid a \in \mathbb{F}_{q^2}^2, A \in \mathrm{GL}_2(\mathbb{F}_q)\right\}.$$

Proof. For any $g = (a, A) \in \mathrm{AGL}(2, q^2)$ and $h = (b, \mathrm{I}_2) \in H_q$, we have

$$ghg^{-1} = (a, A)(b, \mathrm{I}_2)(a, A)^{-1} = (Ab, \mathrm{I}_2). \tag{1}$$

Let $g = (a, A) \in N_{\mathrm{AGL}(2,q^2)}(H_q)$, where $A = \begin{pmatrix} u & v \\ w & z \end{pmatrix}$. Since $g \in N_{\mathrm{AGL}(2,q^2)}(H_q)$, we know that $g(b, \mathrm{I}_2)g^{-1} = (Ab, \mathrm{I}_2) \in H_q$, for $(b, I_2) \in H_q$ (see (1)). In particular,

$$Ab \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}, \text{ for } b \in \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

Therefore, the columns of A are elements of $\begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$ and so $A \in \mathrm{GL}_2(\mathbb{F}_q)$. In other words, $N_{\mathrm{AGL}(2,q^2)}(H_q) \subseteq \left\{ (a, A) \mid a \in \mathbb{F}_{q^2}^2, A \in \mathrm{GL}_2(\mathbb{F}_q) \right\}$.

Conversely, if $A \in \mathrm{GL}_2(\mathbb{F}_q)$ and $a \in \mathbb{F}_{q^2}^2$ then, by (1), it is easy to see that $(a, A) \in N_{\mathrm{AGL}(2,q^2)}(H)$. This completes the proof. $\square$

An immediate consequence of Lemma 2.4 is that H_q is not a normal subgroup of $\mathrm{AGL}(2, q^2)$.

Theorem 2.5. *The subgroup H_q of $\mathrm{AGL}(2, q^2)$ is a perfect code.*

Proof. Since H_q is a 2-group, we may apply Lemma 2.2. Consequently, we only need to show that $\Phi\left(N_{\mathrm{AGL}(2,q^2)}(H_q), H_q\right)$ holds. Let $g = (a, A) \in N_{\mathrm{AGL}(2,q^2)}(H_q)$ such that $(a, A)^2 = ((A + \mathrm{I}_2)a, A^2) \in H_q$, that is, $(A + \mathrm{I}_2)a \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$ and $A^2 = \mathrm{I}_2$. Let us prove that there exists $b \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$ such that $\left((a, A)(b, \mathrm{I}_2)\right)^2 = (0, \mathrm{I}_2)$.

First we note that if $A = \mathrm{I}_2$, then $(a, A)^2 = (a, \mathrm{I}_2)^2 = (a + a, \mathrm{I}_2) = (0, \mathrm{I}_2)$. Thus, for $b = 0$, we have $\left((a, A)(b, \mathrm{I}_2)\right)^2 = (0, \mathrm{I}_2)$. Therefore, we assume henceforth that $A \neq \mathrm{I}_2$.

Suppose that $(A + \mathrm{I}_2)a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$. Recall that the spectrum of a square matrix is the multiset consisting of all its eigenvalues. Since $A^2 = \mathrm{I}_2$, the spectrum of A is the multiset $\{1, 1\}$ and $\mathrm{tr}(A) = 0$. Thus, we may write $A = \begin{pmatrix} t & v \\ u & t \end{pmatrix}$, for some $t, u, v \in \mathbb{F}_q$. As $\det(A) = t^2 + uv = 1$, we obtain the equality $(t - 1)^2 = uv$.

For any $h = (b, \mathrm{I}_2) \in H_q$, we have

$$(gh)^2 = \left((a, A)(b, \mathrm{I}_2)\right)^2 = (a + Ab, A)^2 = \left((A + \mathrm{I}_2)(a + b), \mathrm{I}_2\right). \tag{2}$$

1. *Assume that $t = 1$.*

In this case, $uv = (t - 1)^2 = 0$ and so $u = 0$ or $v = 0$. Without loss of generality, assume that $u = 0$. Then, $A = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$ and since $A \neq \mathrm{I}_2$, we must have $v \neq 0$.

Hence, $A + \mathrm{I}_2 = \begin{pmatrix} 0 & v \\ 0 & 0 \end{pmatrix}$. Consequently, $(A + \mathrm{I}_2)a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ implies that $a_2 = 0$. Taking $b = \begin{pmatrix} 0 \\ -v^{-1}a_1 \end{pmatrix} \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$ in (2), we have $(gh)^2 = (0, \mathrm{I}_2)$.

2. Assume that $t \neq 1$.

Let $t' = t - 1$. Since $uv = (t-1)^2 = t'^2 \neq 0$, we know that $u \neq 0$, $v \neq 0$, and $A + I = \begin{pmatrix} t' & u^{-1}t'^2 \\ u & t' \end{pmatrix}$. Note that $(A + \mathrm{I}_2)a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ implies $a_1 = u^{-1}t'a_2$. By letting $b = \begin{pmatrix} 0 \\ -t'^{-1}a_2 \end{pmatrix} \in \begin{pmatrix} \mathbb{F}_q \\ \mathbb{F}_q \end{pmatrix}$ in (2), we have $(gh)^2 = (0, \mathrm{I}_2)$.

We conclude that $\Phi\left(N_{\mathrm{AGL}(2,q^2)}(H_q), H_q\right)$ holds, therefore H_q is a subgroup perfect code of $\mathrm{AGL}(2, q^2)$. □

Acknowledgments

We are grateful to the anonymous reviewers for their insightful comments, which helped improve this paper.

References

[1] E. Bannai, On perfect codes in the Hamming schemes $H(n, q)$ with q arbitrary, *J. Combin. Theory Ser. A* **23** (1) (1977), 52–67.

[2] N. Biggs, Perfect codes in graphs, *J. Combin. Theory Ser. B* **15** (3) (1973), 289–296.

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* **10** (1973), vi+–97.

[4] R. Feng, H. Huang and S. Zhou, Perfect codes in circulant graphs, *Discrete Math.* **340** (7) (2017), 1522–1527.

[5] P. Hammond and D. H. Smith, Perfect codes in the graphs O_k, *J. Combin. Theory Ser. B* **19** (3) (1975), 239–255.

[6] H. Huang, B. Xia and S. Zhou, Perfect codes in Cayley graphs, *SIAM J. Discrete Math.* **32** (1) (2018), 548–559.

[7] J. Lee, Independent perfect domination sets in Cayley graphs, *J. Graph Theory* **37** (4) (2001), 213–219.

[8] X. Ma, M. Feng and K. Wang, Subgroup perfect codes in Cayley sum graphs, *Des. Codes Cryptogr.* **88** (7) (2020), 1447–1461.

[9] X. Ma, G. L. Walls, K. Wang and S. Zhou, Subgroup perfect codes in Cayley graphs, *SIAM J. Discrete Math.* **34** (3) (2020), 1909–1921.

[10] D. H. Smith, Perfect codes in the graphs O_k and $L(O_k)$, *Glasgow Math. J.* **21** (1) (1980), 169–172.

[11] Y. Wang, B. Xia and S. Zhou, Perfect sets in Cayley graphs, `arXiv:2006.05100` (2020).

[12] J. Zhang and S. Zhou, On subgroup perfect codes in Cayley graphs, *European J. Combin.* **91** (2020), 103228. (See `arXiv:2006.11104`, v2, 2021, for a corrected version.)

[13] J. Zhang and S. Zhou, Corrigenda: On subgroup perfect codes in Cayley graphs, submitted.

[14] S. Zhou, Cyclotomic graphs and perfect codes, *J. Pure Appl. Algebra* **223** (3) (2019), 931–947.

(Received 2 Apr 2021; revised 26 Aug 2021)