Available online at http://scik.org
J. Math. Comput. Sci. 9 (2019), No. 6, 755-763
https://doi.org/10.28919/jmcs/4221
ISSN: 1927-5307

ABELIAN GROUP FACTORIZATION FROM PERFECT CODES

ABDULLA EID* AND KHALID AMIN

Department of Mathematics, University of Bahrain, Sakhir, Bahrain

Abstract. In this paper, we give a factorization of certain p–groups using non–trivial perfect codes (Hamming and Golay codes). The factorization consists of two sets, one corresponding to the perfect code and the other corresponding to the codewords in the Hamming sphere with center at the zero codeword and radius one (Hamming code) and three (Golay code). Non–perfect codes are also considered in such construction and we give the necessary condition for the factorization in terms of the parity check matrix of the code.

Keywords: Hamming codes; perfect codes; group factorization.

2010 AMS Subject Classification: 94B05, 20K25.

1. INTRODUCTION

A linear t–error correcting code (n,k,d) is a linear subspace C of $\mathbb{F}_q^n$ of dimension k and it is able to correct up to t errors in any received codeword. The Hamming distance between any two codewords in $\mathbb{F}_q^n$ is the number of positions in which the corresponding symbols are different. The minimum distance d of a linear code C is the minimum Hamming distance between the codewords in the code. For more details, the reader may refer to the book of MacWilliams and Sloane [4]. Error correcting codes have many applications in communications, networking, and

*Corresponding author

E-mail address: aeid@uob.edu.bh

Received July 15, 2019

in compact disc systems [3]. In this paper, we will use the properties of certain error correcting codes to solve some problems in group theory, in particular in group factorization.

Factorization of abelian groups into subsets was born in 1938, when G. Hajòs reformulated and eventually settled a long-standing conjecture by H. Minkowski about lattice tiling of $\mathbb{R}^n$ into a group-theoretical question about decomposition of a finite abelian group into subsets. The group-theoretical equivalence of Minkowski's conjecture is usually stated as follows:

Let G be a finite abelian group. If $G = A_1A_2 \dots A_n$ is a direct product of subsets of G, where each A_i is of the form $\{e, g, g^2, \dots, g^k\}$, where $g \in G$, and k is an integer less than order of g, then at least one of these subsets must be a subgroup of G.

This Hajòs reformulation turned out to provide not only a strong tool in the area of tiling but also in other areas of mathematics such as number theory, graph theory, geometry, functional analysis, and coding theory (more information on this can be found in [7]). In [1], the interconnection between factorization of abelian groups and Hamming codes was studied. In fact, factorization of abelian groups was used to construct the binary Hamming $(7,4,3)$ code. In this paper, we continue in this direction by showing that the reverse process is also possible and we generalize the result to all perfect codes.

This paper is organized as follows. In Section 2 we recall the basic definitions and properties of Hamming codes and abelian group factorizations. In Section 3 we use the Hamming code to obtain an abelian group factorization of certain p–group. In Section 4, we use the binary Golay code to obtain abelian group factorization of a 2–group of order 2^{23} and the ternary Golay code to obtain abelian group factorization of a 3–group of order 3^{11}. In Section 5 we give the necessary condition for the factorization to work for any linear code in terms of a condition in the parity check matrix of the code.

2. PRELIMINARIES

Hamming codes are linear error correcting codes that were first introduced by R. Hamming [2]. They are widely used in telecommunication, data compression, and in computer memory [5].

The Hamming code $\mathrm{HAM}(r,q)$ is defined as a linear $(n := \frac{q^r-1}{q-1}, n-r, 3)$ error correcting code over $\mathbb{F}_q$, where q is a prime power. The parity check matrix has the property that the columns

of the matrix are made up from the distinct nonzero vectors in $\mathbb{F}_q^r$ whose first entry is one. In the binary case, the columns are precisely the nonzero binary words of length r.

Note that any linear code with parameters $(n := \frac{q^r-1}{q-1}, n-r, 3)$ is a Hamming code, i.e., the Hamming code is characterized by its length, dimension, and minimum distance. Since the minimum distance of the Hamming code is 3, any two Hamming codewords differ in at least three positions. This will be crucial for us in Section 3.

Let G be a finite abelian group written multiplicatively and with identity e, and $A_1, A_2, \ldots, A_n$ subsets of G. We say that $G = A_1A_2 \ldots A_n$ is a factorization of G if each element g of G can be written uniquely as $g = a_1a_2 \ldots a_n$, where $a_i \in A_i$. If in addition, each of the subsets A_i contains e, we call $G = A_1A_2 \ldots A_n$ a normalized factorization. Since $G = (a_1^{-1}a_2^{-1} \ldots a_n^{-1})G = a_1^{-1}A_1 \ldots a_n^{-1}A_n$ is also a factorization of G, we may and shall only consider normalized factorization.

If $G = AB$ is a factorization of G, then we call $A($ or $B)$ a *periodic* set, if there exists $g \in G$ different than the identity, such that $gA = A (gB = B)$. A group G is called a Hajòs group if from each factorization $G = AB$ of G, it follows that either A or B is periodic. Hajòs gave a method for constructing all factorizations of such groups, a result which was later generalized by Sands [6] to the case $n \geq 2$. In this paper, we use perfect codes to construct normalized factorization of certain p–groups.

In this paper, we will concentrate only on perfect codes, i.e., the spheres of radius $t := (d-1)/2$ centered at the codewords cover the whole space without an overlap, i.e., the parameters of the code satisfy the sphere packing condition

$$q^k \sum_{i=0}^{t} (q-1)^i \binom{n}{i} = q^n$$

By Tietäväinen–Van Lint theorem [8, 9], the only nontrivial perfect codes are those with parameters of the Hamming and Golay codes and we will just focus on these two classes of codes in this paper.

Let G be a finite abelian p–group, i.e., G is a product of cyclic groups:

$$G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$$

where each x_i has order p. Let $g = x_1^{c_1} x_2^{c_2} \dots x_n^{c_n} \in G$, then we get a correspondence between g and a codeword in $\mathbb{F}_p^n$ by setting $c := (c_1, c_2, \dots, c_n) \in \mathbb{F}_p^n$. This also works in reverse direction, i.e., each codeword in $\mathbb{F}_p^n$ gives a group element in G.

3. GROUP FACTORIZATION FROM HAMMING CODES

In this section, we will use a binary Hamming code $(n := 2^r - 1, n - r, 3)$ to find a factorization for the 2–group

$$G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$$

Starting with a subset A of G consisting of monomials of length one or less in $x_1, \dots, x_n$, i.e. A corresponds to the codewords in $\mathbb{F}_2^n$ in the Hamming sphere of radius one centered at the zero codeword. Explicitly, A is given by

$$A = \{e, x_1, x_2, \dots, x_n\}.$$

Next we use the Hamming code to construct another subset B of G of size 2^{n-r} consisting of elements in G that correspond to the codewords of the Hamming code.

Proposition 1. *The sets A and B provide a factorization of G.*

Proof. We need to prove that each element $g \in G$ can be written uniquely as a product of two elements, one in A and the other one in B.

Recall that the Hamming codes are perfect codes with $t = 1$ and every element $g \in G$ corresponds to a codeword in $\mathbb{F}_2^n$. This codeword is either a Hamming codeword or a codeword that is differs only in one position from a Hamming codeword, in the later case, we can recover the error position and this gives us directly the existence of the factorization.

For uniqueness, assume w.l.o.g. that

$$g = x_1 b_1 = x_2 b_2$$

where $b_1, b_2 \in B$ are two group elements corresponding to two Hamming codewords that are different in at least 3 positions. Note that $x_1 b_1$ means that only the first position in the codeword corresponding to b_1 is changed and similarly $x_2 b_2$ means that only the second position in the

codeword corresponding to b_2 is changed, but since $x_1 b_1 = x_2 b_2$ this means that the codewords corresponding to b_1 and b_2 differ in at most 2 positions which is a contradiction to the fact that the minimum distance of the Hamming code is 3.

□

Now we generalize the argument above to the non–binary Hamming codes. We start with a Hamming code HAM(r,p) with parameters $(n := \frac{p^r-1}{p-1}, n-r, 3)$ over $\mathbb{F}_p$, where p is a prime integer. Consider the p–group

$$G = \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_n \rangle$$

The next proposition gives a factorization for the group G.

Proposition 2. *The group G can be factored into $G = AB$, where $A = \{e\} \cup \{x_i^j \mid, j = 0,1,\ldots,p-1, i = 1,2,\ldots,n\}$ and B is the subgroup generated by the codewords of the Hamming code* HAM(r,p).

Proof. We need to prove that each element $g \in G$ can be written uniquely as products of two element, one in A and the other one in B.

For the existence part, we note that the Hamming code HAM(r,p) is a perfect non–binary code with $t = 1$. This means that every element $g \in G$ is corresponding to a codeword in $\mathbb{F}_p^n$ which turns out to be either a Hamming codeword or a codeword that is differ in one position from a Hamming codeword. Assume the latter case and that position is i, we have then that g is corresponding to a codeword of the form $x_i^j b$, where b is a group element that is corresponding to a Hamming codeword and $j = 0,1,\ldots,p-1$. This gives us the existence of the factorization.

For uniqueness, assume w.l.o.g. that

$$g = x_1^j b_1 = x_2^k b_2$$

where $b_1, b_2 \in B$ are two group elements corresponding to two Hamming codewords that are different in at least 3 positions. Note that $x_1^j b_1$ means that only the first position in the codeword corresponding to b_1 is changed and similarly $x_2^k b_2$ means that only the second position in the codeword corresponding to b_2 is changed, but since $x_1^j b_1 = x_2^k b_2$ this means that the codewords

corresponding to b_1 and b_2 differ in at most 2 positions which is a contradiction to the fact that the minimum distance of the Hamming code is 3.

□

Example 1. *Let $p = 3$, $r = 2$, the Hamming code* $\mathrm{HAM}(2,3)$ *is a perfect* $(4,2,3)$*–linear code with two basis codewords* $\{1012, 0111\}$. *The* 3*-group* $G = \langle x_1\rangle \times \langle x_2\rangle \times \langle x_3\rangle \times \langle x_4\rangle$ *can be factored into*

$$A = \{e, x_1, x_1^2, x_2, x_2^2, x_3, x_3^2, x_4, x_4^2\}$$

and

$$B = \langle x_1 x_3 x_4^2, x_2 x_3 x_4\rangle$$

Next we prove the necessary part in Proposition 1 that if we have the factorization as constructed above, then we actually have the binary Hamming code. The argument below works also for the non–binary case.

Proposition 3. *Let C be a binary $(n,k,d = 3)$ code. Set A to be the set of all monomials of length* 1 *with the identity in $x_1, \ldots, x_n$, i.e., A corresponds to the Hamming sphere centered at* 0 *of radius* 1. *Let B be the set that corresponds to the codewords of C. If the set AB is closed under multiplication, then C is equivalent to a Hamming code.*

Proof. Assume that the set AB is closed under multiplication, then any element $g \in AB$ corresponds to $c + e$, where $c \in C$ is a codeword in the code C and e is an error vector of weight 0 or 1. For any $g_1, g_2 \in AB$, we have also $g_1 g_2 \in AB$. This means $(c_1 + e_1) + (c_2 + e_2) = c_3 + e_3$. if H is the parity check matrix of the code, we would have

$$e_1 H + e_2 H = e_3 H \tag{1}$$

Since eH corresponds to the syndrome in the column of H with entries e. Equation (1) means that columns of H must be closed under the column addition. Since the number of rows of H is k and the minimum distance of the code is 3, this means that all binary representations of length k of the numbers $1, 2, \ldots, 2^k - 1$ appears as columns of H. This leads to $n = 2^k - 1$ and so we have a code with parameters $(2^k - 1, n - k, 3)$ and by Tietäväinen–Van Lint theorem, it is equivalent to a Hamming code.

□

4. GROUP FACTORIZATION FROM THE GOLAY CODES

In this section we use the same idea as in Section 3 to construct a factorization for the 2–group

$$G_{23} := \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_{23} \rangle$$

using the binary Golay code $(23,12,7)$. The set A is the set of all monomials of length less than or equal 3 including the identity element of G_{23}, i.e.,

$$A := \{e, x_i x_j x_k \,|\, i,j,k \in \{1,\ldots,23\}\}$$

The set B is generated by elements in G_{23} that correspond to codewords in the binary Golay code. Then by a similar argument as in the proof of Proposition 1, we will have factorization $G = AB$, where

$$\begin{aligned} B = \langle & x_1x_{14}x_{15}x_{16}x_{17}x_{18}x_{19}x_{20}x_{21}x_{22}x_{23}, \; x_2x_{13}x_{14}x_{15}x_{17}x_{18}x_{19}x_{23}, \\ & x_3x_{13}x_{14}x_{16}x_{17}x_{18}x_{22}, \qquad\qquad x_4x_{13}x_{15}x_{16}x_{17}x_{21}x_{23}, \\ & x_5x_{13}x_{14}x_{15}x_{16}x_{20}x_{22}x_{23}, \qquad x_6x_{13}x_{14}x_{15}x_{16}x_{20}x_{22}x_{23}, \\ & x_7x_{13}x_{14}x_{15}x_{19}x_{21}x_{22}, \qquad\qquad x_9x_{15}x_{17}x_{18}x_{20}x_{21}x_{22}x_{23}, \\ & x_8x_{13}x_{17}x_{19}x_{20}x_{22}x_{23}, \qquad\qquad x_{10}x_{13}x_{15}x_{17}x_{18}x_{20}x_{21}x_{22}, \\ & x_{11}x_{13}x_{14}x_{16}x_{17}x_{19}x_{20}x_{21}, \qquad\qquad x_{12}x_{14}x_{15}x_{17}x_{18}x_{19}x_{20}\rangle \end{aligned}$$

We conclude this construction by using the last nontrivial perfect code, the ternary Golay code $(11,6,5)$ over $\mathbb{F}_3$ to obtain factorization to the 3–group

$$G_{11} := \langle x_1 \rangle \times \langle x_2 \rangle \times \cdots \times \langle x_{11} \rangle$$

into AB, where A is the set consisting of all monomials of length 2 or less including the identity element of G_{11}, i.e.,

$$A := \{e, x_i, x_i x_j \,|\, i,j \in \{1,\ldots,11\}\}$$

and the set B is generated by elements in G_{11} that correspond to codewords in the ternary Golay code, i.e.,

$$B = \langle x_1x_2x_3x_4^2x_5^2x_7, x_1x_2x_3^2x_4x_6^2x_8, x_1x_2^2x_3x_5x_6^2x_9, x_1x_2^2x_4x_5^2x_6x_{10},$$
$$x_1x_3^2x_4^2x_5x_6x_{11}\rangle$$

5. GROUP FACTORIZATION FROM NON–PERFECT CODES

In this section, we generalize our construction above by giving a condition on the parity check matrix H of the any linear $(n,k,d=2t+1)$–code C to provide a factorization of a 2–group. The factorization into two sets will be as above, one set corresponds to the codewords in the Hamming sphere of radius t centered at the zero codeword and the other set corresponds to the code C.

Proposition 4. *Let C be a binary $(n,k,d=2t+1)$ code. Set A to be the set of all monomials of length less than or equal to t in $x_1,\ldots,x_n$, i.e., A corresponds to the Hamming sphere centered at 0 of radius t. Let B be the set that corresponds to the codewords of C. If the set AB is closed under multiplication, then the parity check matrix is closed under the addition of any t-columns or less.*

Proof. Assume that the set AB is closed under multiplication, then any element $g \in AB$ corresponds to $c+e$, where $c \in C$ is a codeword in the code C and e is an error vector of weight t. Since $g_1g_2 \in AB$, we have also $g_1g_2 \in AB$. This means $(c_1+e_1)+(c_2+e_2) = c_3+e_3$. if H is the parity check matrix of the code, we would have

$$e_1H + e_2H = e_3H \tag{2}$$

Since e_iH can be written as sum of t-columns or less. Equation (2) means that columns of H must be closed under the addition of any t-columns or less.

□

6. CONCLUSION

In this paper, the link between linear codes over $\mathbb{F}_p$ and certain p–groups allows us to use non trivial perfect linear error correcting codes (Hamming and Golay codes) to obtain abelian

group factorization of certain groups. The corresponding subsets in the factorization is given by the codewords in the code and the codewords in the Hamming sphere of radius t centered at the zero codeword. We also showed that in the binary cases, the factorization works only if the code is perfect and we find the necessary condition in terms of parity check matrix for our construction to work.

Conflict of Interests

The author(s) declare that there is no conflict of interests.

REFERENCES

[1] K. Amin, *Constructing single-error-correcting codes using factorization of finite abelian groups*, Int. J. Algebra **8** (2014), no. 7, 311–315.

[2] R.W. Hamming, *Error detecting and error correcting codes*, Bell Labs Techn. J. **29** (1950), no. 2, 147–160.

[3] H. Hoeve, J. Timmermans and L.J. Vries, *Error correction and concealment in the compact disc system*, Origins and Successors of the Compact Disc (1982), 82.

[4] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, 2nd ed., North-holland Publishing Company, 1978.

[5] R.J. McEliece, *The reliability of computer memories*, Sci. Amer. **252** (1985), no. 1, 88–95.

[6] A. Sands, *On the factorisation of finite abelian groups. ii*, Acta Math. Hung. **13** (1962), no. 1-2, 153–169.

[7] S. Stein, S. Szabó, and Mathematical Association of America, *Algebra and tiling: Homomorphisms in the service of geometry*, Carus Mathematical Monographs, Mathematical Association of America, 1994.

[8] A. Tietäväinen, *On the nonexistence of perfect codes over finite fields*, SIAM J. Appl. Math. **24** (1973), no. 1, 88–96.

[9] J.H. Van Lint, *A survey of perfect codes*, J. Math. **5** (1975), no. 2, 199–224.