International Electronic Journal of Algebra
Volume 10 (2011) 25-36

INTEGER t-SHIFT CODES AND FACTORING ABELIAN GROUPS

Sándor Szabó

Received : 22 January 2010; Revised : 1 March 2011
Communicated by Abdullah Harmancı

Abstract. Let p a be prime number. Using algebraic methods from the factorization theory of abelian groups we will prove a result about the structure of the 1-error correcting t-shift integer codes over the alphabet Z_p in the special case when t is a prime. The algorithms to construct such codes can take advantage of this extra structural information in a straightforward manner and the search for these codes can be speed up dramatically.

Mathematics Subject Classification (2010): Primary 94B60; Secondary 20K01
Keywords: integer codes, shift codes, single-error correcting perfect codes, splitting and factoring abelian groups

1. Introduction

In this section we describe the concepts of 1-error correcting t-shift codes over the alphabet $\{0, 1, \ldots, m-1\}$, splittings and factorizations of abelian groups. For more on t-shift codes see [3] and [11]. Further material on splitting groups can be found in [1], [2] and [5]. Some of the history of the factorization theory of abelian groups is presented in [7].

Let $f : A \to B$ be an injective function. The set $C = \mathrm{Im}f$ is called a code. Intuitively an element $a \in A$ is coded by the element $f(a) \in B$. In the most commonly encountered situation A, B are chosen to be F^k, F^n respectively, where F is the Galois field of order 2. In this case a 0, 1 sequence of length k is coded by a 0, 1 sequence of length n. When f is a linear map it is customary to consider the exact sequence

$$\{0\} \longrightarrow F^k \xrightarrow{f} F^n \xrightarrow{g} F^{n-k} \longrightarrow \{0\}$$

associated with a code. For us in this paper a similar exact sequence

$$\{0\} \longrightarrow Z_m^k \xrightarrow{f} Z_m^n \xrightarrow{g} Z_m^{n-k} \longrightarrow \{0\}$$

will be relevant, where Z_m is the ring of integers modulo m. The code $C = \mathrm{Im}f$ can be equivalently described as $C = \mathrm{Ker}g$. In other words an $a \in Z_m^n$ is a code

word if $g(a) = 0$. In general $g(a)$ is not equal to 0. Customarily $g(a)$ is called the syndrome of a. In order to further particularize the construction let $k = n - 1$ and let us fix the sequence of elements $s_1, \ldots, s_n$ of $Z_m \setminus \{0\}$ and define the function g by

$$g(a) = \sum_{i=1}^{n} s_i a_i,$$

where $a = (a_1, \ldots, a_n)$. The sequence $s_1, \ldots, s_n$ is called a weight sequence. The choice of the weights leads to various codes. For example when

$$(s_1, s_2, \ldots, s_n) = (1, 2, \ldots, n)$$

we get the Varshamov-Tenengolts code. This code is capable of correcting one asymmetric error. For more on the Varshamov-Tenengolts code see [10].

Suppose that a single substitution error occurs, say the letter a_i is replaced by a letter $a_i' = a_i + e_i$ in the code word $a = (a_1, \ldots, a_n)$, where e_i is coming from a fixed error set E. Then we receive the new word

$$a' = (a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$$

instead of a. The set of elements

$$a' = (a_1, \ldots, a_{i-1}, a_i + e, a_{i+1}, \ldots, a_n),$$

where i and e vary over the elements of the sets $\{1, \ldots, n\}$, $E \cup \{0\}$ independently, is defined to be the substitution error sphere centered at a and is denoted by $S(a, E)$. Clearly $S(a, E)$ has $n|E| + 1$ elements. A perfect single substitution error correcting code is a subset C of Z_m^n if the error spheres

$$S(c, E),\ c \in C$$

form a partition of Z_m^n.

Let us compute the syndrome of the word a'.

$$\begin{aligned} g(a') &= s_1 a_1 + \cdots + s_{i-1} a_{i-1} + s_i a_i' + s_{i+1} a_{i+1} + \cdots + s_n a_n \\ &= s_1 a_1 + \cdots + s_n a_n + s_i (a_i' - a_i) \\ &= g(a) + s_i (a_i' - a_i) \\ &= s_i (a_i' - a_i) \\ &= s_i e_i. \end{aligned}$$

If all the possible syndromes are pair-wise distinct, then the distortion can be corrected. In other words a single substitution error can be corrected if

$$s_i e_i = s_j e_j,\ e_i, e_j \in E$$

imply that $s_i = s_j$ and $e_i = e_j$. When the error set is $E = \{\pm 1, \pm 2, \ldots, \pm t\}$, then the error correcting code is called a t-substitution code. The 1-error correcting t-substitution code is perfect if each element of $Z_m \setminus \{0\}$ is uniquely expressible in the form

$$is_j,\ 1 \leq |i| \leq t,\ 1 \leq j \leq n.$$

Let G be a finite abelian group written additively, let S be a subset of G, and let M be a set of integers. If each $g \in G \setminus \{0\}$ is uniquely expressible in the form

$$g = \mu s,\ \mu \in M,\ s \in S,$$

then we say that the equation $G \setminus \{0\} = MS$ is a splitting of $G \setminus \{0\}$. Here M is called the multiplier set and S is called the splitting set. The reader can verify that the multiplier set $M = \{\pm 1, \pm 2\}$ splits $Z_{13} \setminus \{0\}$ with the multiplier set $S = \{1, 3, 4\}$. Here of course Z_{13} is the additive group of the ring of integers modulo 13. The concept of splitting was introduced by S. K. Stein. There is a large body of results about splitting but our reference is merely the tip of the iceberg.

Let A and B be subsets of the finite abelian group G. If each $g \in G$ is uniquely expressible in the form

$$g = a + b,\ a \in A,\ b \in B,$$

then we say that the equation $G = A + B$ is a factorization of G. In the most well-known situation the factors A, B are subgroups of G. However, in our definition nothing is assumed about the subsets A and B. In the special case when G is the cyclic group of order m, we simply identify G with the additive part of Z_m, the ring of integers modulo m. Now a multiplier set M can be viewed as a subset of G. It is a well-know fact that if p is a prime, then the nonzero elements of Z_p form a cyclic group $Z_p^* = Z_p \setminus \{0\}$ under multiplication. Note that the splitting $Z_p \setminus \{0\} = MS$ of $Z_p \setminus \{0\}$ corresponds to the multiplicative factorization $Z_p^* = MS$ of Z_p^*.

We may sum up our previous considerations as follows. Let p be a prime and let $M = \{\pm 1, \pm 2, \ldots, \pm t\}$. If there is a subset S of Z_p^* such that $Z_p^* = MS$ is a multiplicative factorization of Z_p^*, then there is a perfect 1-error correcting t-substitution code word of length $|S|$ over the alphabet Z_p.

Let d, n, k be nonnegative integers such that $d \leq k$. The sequence $a = (a_1, \ldots, a_n)$ is called an (n, d, k)-sequence if $d \leq a_i \leq k$ holds for each i, $1 \leq i \leq n$. Plainly, if $a = (a_1, \ldots, a_n)$ is an (n, d, k)-sequence, then $b = (a_1 - d, \ldots, a_n - d)$ is an $(n, 0, k - d)$-sequence, that is, b can be viewed as a word of length n over the

alphabet $\{0, 1, \ldots, k-d\} = Z(m)$, where $m = k - d + 1$. The set of all (n, d, k)-sequences is denoted by $T(n, d, k)$. It can be checked that $T(n, d, k)$ has $(k-d+1)^n$ elements.

To an (n, d, k)-sequence $a = (a_1, \ldots, a_n)$ we assign the 0, 1 sequence

$$h(a) = (\underbrace{0, \ldots, 0}_{a_1}, 1, \underbrace{0, \ldots, 0}_{a_2}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1).$$

The sequence $h(a)$ has

$$a_1 + 1 + \cdots + a_n + 1 = n + a_1 + \cdots + a_n$$

components. The 1's in $h(a)$ are called peaks and consecutive 0's are called runs. If the first peak is shifted to the right by j digits, then we get the sequence

$$(\underbrace{0, \ldots, 0}_{a_1+j}, 1, \underbrace{0, \ldots, 0}_{a_2-j}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1)$$

from $h(a)$, provided of course that $a_2 - j \geq 0$ holds. If the first peak is shifted to the left by j digits, then we get the sequence

$$(\underbrace{0, \ldots, 0}_{a_1-j}, 1, \underbrace{0, \ldots, 0}_{a_2+j}, 1, \ldots, \underbrace{0, \ldots, 0}_{a_n}, 1)$$

from $h(a)$. Naturally, we must assume that $a_1 - j \geq 0$. Similarly, we can speak of shifting the ith peak to the left or to the right by j digits in $h(a)$ for each i, $1 \leq i \leq n-1$.

Let $a = (a_1, \ldots, a_n)$ be an (n, d, k)-sequence and let the error set E be

$$\{\pm 1, \pm 2, \ldots, \pm t\}.$$

Suppose that a single shift error occurs in $h(a)$, say the letter a_i is replaced by $a'_i = a_i - j$ and a_{i+1} is replaced by $a'_{i+1} = a_{i+1} + j$, where $j \in E$ and $1 \leq i \leq n-1$. We get a new sequence

$$a' = (a_1, \ldots, a_{i-1}, a'_i, a'_{i+1}, a_{i+2}, \ldots, a_n).$$

The set of elements

$$(a_1, \ldots, a_{i-1}, a_i - e, a_{i+1} + e, a_{i+2}, \ldots, a_n),$$

where i, e ranges over the elements of $\{1, \ldots, n-1\}$, $E \cup \{0\}$ is called a single shift error sphere with radius t centered at a. We denote it by $S(a, t)$. Clearly, if a is of length n, then $S(a, t)$ has $2nt + 1$ elements. Note that if a is an (n, d, k)-sequence, then the elements of $S(a, t)$ are $(n, d-t, k+t)$ sequences. A subset C of

$T(n, d-t, k+t)$ is called a perfect single t-shift error correcting code if the shift error spheres

$$S(c,t),\ a \in C$$

form a partition of $T(n, d-t, k+t)$.

Next we show that the existence of shift error correcting codes is related to splitting of abelian groups. The syndrome of a' is

$$\begin{aligned} g(a') &= s_1a_1 + \cdots + s_ia'_i + s_{i+1}a'_{i+1} + \cdots + s_na_n \\ &= s_1a_1 + \cdots + s_na_n - s_ij + s_{i+1}j \\ &= g(a) + j(s_{i+1} - s_i) \\ &= j(s_{i+1} - s_i). \end{aligned}$$

If all the possible syndromes are pair-wise distinct, then the distortion can be corrected. Let $W = \{w_1, \ldots, w_{n-1}\}$ be a subset of $Z(m)$. If each element of $Z(m) \setminus \{0\}$ is uniquely expressible in the form

$$jw_i,\ 1 \le |j| \le t,\ 1 \le i \le n-1,$$

that is if $Z(m) \setminus \{0\} = EW$ is a splitting, then there is a 1-error correcting perfect t-shift code. We just have to choose

$$s_2 - s_1, s_3 - s_2, \ldots, s_n - s_{n-1}$$

to be $w_1, \ldots, w_{n-1}$ respectively.

2. The complementer factor problem

The complementer factor problem is the following.

Problem 2.1. *Given a finite abelian group G and a subset A of G such that $|A|$ divides $|G|$. Decide if there is a subset B of G such that $G = A+B$ is a factorization of G.*

Let us introduce a graph Γ. The nodes of Γ are the elements of G and two nodes g, g' are connected with an undirected edge if $g' - g \notin A - A$. Here $A - A$ stands for $\{a' - a :\ a', a \in A\}$. Let $l = |G|/|A|$. We claim that if Γ has a clique of size l, then there is a $B \subset G$ such that $G = A + B$ is a factorization of G. In order to prove the claim assume that Γ has a clique of size l and that B is the set of vertices of this clique. Now $(A - A) \cap (B - B) = \{0\}$ and so from

$$a + b = a' + b',\ a, a' \in A,\ b, b' \in B$$

it follows that $a - a' = b' - b$. Therefore $a - a' = b' - b = 0$ and so $a = a'$, $b = b'$. On the other hand the equation $|G| = |A||B|$ clearly holds which implies that each $g \in G$ can be represented in the form

$$g = a + b,\ a \in A,\ b \in B.$$

Therefore $G = A + B$ is a factorization of G.

One can see that the graph Γ has no clique of size larger than l. So the complementer factor problem can be reduced to finding a maximum clique in Γ. It is known that the maximum clique problem belongs to the NP complete class. If one could reduce the maximal clique problem to the complementer factor problem then this would prove that the complementer factor problem is also in the NP complete complexity class. We do not have such reduction at our disposal. On the other hand, numerical experiments indicate that the complementer factor problem is computationally hard. We will show that in fact it is hard.

Let A be an alphabet of q elements and let $S_r(a)$ be the Hamming sphere in A^n centered at a with radius r. A subset $C \in A^n$ is a called a perfect error correcting code with parameters (n, e, q) if the Hamming spheres

$$S_e(c),\ c \in C$$

form a partition of A^n. The problem of deciding if a perfect error correcting code with given parameters (n, e, q) exist is indeed computationally hard. We claim that the existence problem of the perfect error correcting codes is an instance of the complementer factor problem. In order to verify the claim note that the alphabet A can be equipped with the structure of an abelian group. Then A^n becomes the direct sum of n copies of A. The problem now is if there is a subset $C \subset A^n$ such that $A^n = S_e(0) + C$ is a factorization of A^n. Here 0 is the zero element of A^n.

The complementer subgroup problem is the following.

Problem 2.2. *Given a finite abelian group G and a subset A of G such that $|A|$ divides $|G|$. Decide if there is a subgroup H of G such that $G = A + H$ is a factorization of G.*

The complementer subgroup problem is computationally less demanding than the complementer factor problem, but still can be hard if G has too many subgroups. However, for cyclic groups it is definitely easy since there is only one subgroup of each given order. For a given subgroup H of G it is straightforward to check if $G = A + H$ is a factorization of G. Say one checks if the elements of A are pair-wise incongruent modulo H.

3. Coset splittings

Let p be a prime. S. K. Stein [6] calls a splitting $Z_p \setminus \{0\} = MS$ a coset splitting if S is a multiplicative subgroup of Z_p^* and consequently M is a complete set of representatives modulo S which explains the name. We saw in the previous section that deciding if a given M coset splits $Z_p \setminus \{0\}$ is computationally simpler than to decide if M splits $Z_p \setminus \{0\}$.

Let G be a finite abelian group. A subset A of G is called normalized if $0 \in A$. The factorization $G = A + B$ is defined to be normalized if both A and B are normalized. For a subset A of G the span of A in G is denoted by $\langle A \rangle$. In other words $\langle A \rangle$ is the smallest subgroup of G that contains A. We will prove the following theorem.

Theorem 3.1. *Let $G = A + B$ be a normalized factorization of the finite cyclic group G. If $|A| = q$ is a prime, $\langle A \rangle = G$, then B is a subgroup of G.*

The message in Theorem 3.1 is that in a class of splitting problems we may focus our attention to coset splittings. For the details of the proof of Theorem 3.1 we need two lemmas.

Lemma 3.2. *Let $G = A + B$ be a factorization of the abelian group G and let $H = \langle A \rangle$. Then $H = A + (B \cap H)$ is a factorization H.*

Proof. Choose a $h \in H$. Since $h \in G$ and $G = A + B$ is a factorization of G it follows that h can be represented uniquely in the form

$$h = a + b,\ a \in A,\ b \in B.$$

From $b = h - a$, $h \in H$, $a \in H$ we get that $b \in H$ and so $b \in B \cap H$. Therefore each h can be represented uniquely in the form

$$h = a + b,\ a \in A,\ b \in B \cap H$$

which completes the proof. □

We will refer to the result in Lemma 3.2 by saying that the factorization $G = A + B$ can be restricted to H to get the factorization $H = A + (B \cap H)$.

Lemma 3.3. *Let $G = A + B$ be a normalized factorization of the abelian group G. If $A = C + H$ is a factorization of A, where H is a subgroup G, then*

$$G/H = (C + H)/H + (B + H)/H$$

is a normalized factorization of the factor group G/H, where

$$(C+H)/H = \{c+H:\ c\in C\},$$

$$(B+H)/H = \{b+H:\ b\in B\}.$$

Proof. Choose a $g\in G$. Since $G=A+B$ is a factorization of G, a can be represented in the form

$$g=a+b,\ a\in A,\ b\in B.$$

Since $A=C+H$ is a factorization of A, a can be represented in the form

$$a=c+h,\ c\in C,\ h\in H.$$

Consequently, $g=c+h+b$ and so

$$\begin{aligned} g+H &= (c+h+b)+H \\ &= (c+H)+(b+H). \end{aligned}$$

Thus $g+H$ can be represented in the required form. Now assume that

$$(c+H)+(b+H)=(c'+H)+(b'+H),\ c,c'\in C,\ b,b'\in B,$$

that is $(c+b)+H=(c'+b')+H$. So there are $h,h'\in H$ such that $c+b+h=c'+b'+h'$. As $G=A+B$ is a factorization of G, from

$$\underbrace{(\ c+h\ )}_{\in A}+\underbrace{(\ b\ )}_{\in B}=\underbrace{(\ c'+h'\ )}_{\in A}+\underbrace{(\ b'\ )}_{\in B}$$

it follows that $c+h=c'+h'$, $b=b'$. Now using the fact that $A=C+H$ is a factorization we can conclude that $c=c'$ which completes the proof. □

We will refer to the result in Lemma 3.3 by saying that considering the factor group G/H the factorization $G=(C+H)+B$ gives the factorization

$$G/H=(C+H)/H+(B+H)/H$$

of the factor group G/H.

Theorem 3.1 greatly simplifies the search for the 1-error correcting t-substitution and t-shift codes in the case when t is a prime. To see how let $M=\{\pm1,\pm2,\dots,\pm t\}$ and let $Z_p\backslash\{0\}=MS$ be a splitting. The splitting corresponds to the multiplicative factorization $Z_p^*=MS$. Note that $L=\{-1,1\}$ is a subgroup of Z_p^*. Set $A=\{1,2,\dots,t\}$. Clearly, $M=AL$ is a multiplicative factorization of M. Considering the factor group $G=Z_p^*/L$ from $Z_p^*=(AL)S$ we get the factorization $G=AB$, where $B=\{sL:\ s\in S\}$. By our assumption, $|A|=t$ is a prime. Choose $a\in A$,

$b \in B$. Multiplying the factorization $G = AB$ by $a^{-1}b^{-1}$ we get the normalized factorization

$$G = Ga^{-1}b^{-1} = (Aa^{-1})(Bb^{-1}).$$

By renaming we may assume that the original factorization $G = AB$ is normalized. Set $H = \langle A \rangle$. If $H \neq G$, then restricting the factorization $G = AB$ to H we get the factorization $H = G \cap H = A(B \cap H)$. Choose a complete set of representatives $c_1, \ldots, c_s$ in G modulo H. Set $C = \{c_1, \ldots, c_s\}$. It is clear that $G = HC$ is a factorization of G. Then

$$G = [A(B \cap H)]C = A[(B \cap H)C]$$

is a factorization of G. From this we can read off that the problem to decide if A has a complementer factor in G can be reduced to the problem to decide if A has a complementer factor in $H = \langle A \rangle$.

By Theorem 3.1, from the normalized factorization $H = AD$ it follows that D is a subgroup of H. This means that A can have only a subgroup complementer factor in H.

4. Proof of Theorem 3.1

We say that in the factorization $G = A + B$ the factor A can be replaced by A' if $G = A' + B$ is also a factorization of G. A subset A of G is called a cyclic subset if its elements are in the form

$$0, a, 2a, \ldots, (q-1)a$$

for some element $a \in G \setminus \{0\}$ and some integer q. We assume that $q \geq 2$ and the order of a is at least q. In the $|a| = q$ case A is equal to $\langle a \rangle$. A subset A of G is called periodic if there is an element $g \in G \setminus \{0\}$ such that $A + g = A$. We also say that g is a period of A. Clearly if g is a period of A then so is mg for each integer m unless $mg = 0$. The periods of A together with the zero form a subgroup H of G. We refer to H as the subgroup of periods of A. We can partition G into cosets modulo H. The subset A is a union of complete cosets. In other words there is a subset D of G such that $A = D + H$ is a factorization of A. The subset D here is not necessarily unique.

We are ready to prove Theorem 3.1.

Proof. In order to prove Theorem 3.1 assume on the contrary that there is a finite cyclic group G such that $G = A + B$ is a normalized factorization, $|A| = q$ is a

prime, $\langle A\rangle = G$, and B is not a subgroup of G. We choose such a counter-example for which $|G|$ is minimal.

We claim that in a minimal counter-example none of the factors is periodic. To verify the claim assume on the contrary that A or B is periodic. If A is periodic, then since $|A| = q$ is a prime and $0 \in A$ it follows that A is a subgroup of G of order q. As $\langle A\rangle = G$, we get that $B = \{0\}$. This contradicts to our assumption that B is not a subgroup of G. Thus we may assume that B is periodic. Let H be the subgroup of periods of B. There is a subset C of B such that $B = C + H$ is a factorization of B. From the factorization $G = A + (C + H)$ by considering the factor group G/H we get the factorization

$$G/H = (A + H)/H + (C + H)/H.$$

Note that the factor $(A + H)/H$ spans the whole of G/H. Indeed as $\langle A\rangle = G$, for each $g \in G$ there are elements $a_1, \dots, a_r \in A$ and integers $\alpha_1, \dots, \alpha_r$ such that $g = \alpha_1 a_1 + \cdots + \alpha_r a_r$. This means

$$\begin{aligned} g + H &= (\alpha_1 a_1 + \cdots + \alpha_r a_r) + H \\ &= (\alpha_1 a_1 + H) + \cdots + (\alpha_r a_r + H) \\ &= \alpha_1(a_1 + H) + \cdots + \alpha_r(a_r + H) \end{aligned}$$

and so $(A+H)/H$ spans the whole of G/H. The minimality of the counter-example $G = A + B$ implies that $(C + H)/H$ is a subgroup of G/H. So for each $c_1, c_2 \in C$ there is a $c_3 \in C$ such that $(c_1 + H) - (c_2 + H) = c_3 + H$. Hence for each $c_1, c_2 \in C$, $h_1, h_2 \in H$ there are $c_3 \in C$, $h_3 \in H$ such that $(c_1 + h_1) - (c_2 + h_2) = c_3 + h_3$. It follows that $B = C + H$ is a subgroup of G contrary to our assumption.

In the remaining part of the proof we will establish that in the factorization $G = A + B$ one of the factors is periodic.

We claim that in the factorization $G = A + B$ the factor A can be replaced by the cyclic subset

$$C = \{0, a, 2a, \dots, (q - 1)a\}$$

for each $a \in A \setminus \{0\}$. To verify the claim assume that $A = \{a_0, a_1, \dots, a_{q-1}\}$ with $a_0 = 0$. The factorization $G = A + B$ is equivalent to that the sets

$$a_0 + B,\ a_1 + B, \dots, a_{q-1} + B$$

form a partition of G. We would like to show that the sets

$$0 + B,\ a + B,\ 2a + B, \dots, (q - 1)a + B$$

form a partition of G. For the sake of definiteness we suppose that $a = a_1$. By Proposition 3 of [4], in the factorization $G = A + B$ the factor A can be replaced by $tA = \{ta : \ a \in A\}$ to get the factorization $G = tA + B$ for each integer t which is relatively prime to q. This means that the sets

$$ta_0 + B,\ ta_1 + B, \ldots, ta_{q-1} + B$$

form a partition of G for each t, $1 \leq t \leq q-1$. In particular $(0+B) \cap (ta_1 + B) = \emptyset$. If $(ia_1 + B) \cap (ja_1 + B) \neq \emptyset$ for some i, j, $1 \leq i < j \leq q-1$, then we get the

$$(0 + B) \cap [(j - i)a_1 + B] \neq \emptyset,\ 1 \leq i < j \leq q - 1$$

contradiction. Therefore $G = C + B$ is a factorization of G.

We claim that if $G = C + B$ is a factorization of G, where C is the cyclic subset

$$C = \{0, a, 2a, \ldots, (q-1)a\},$$

then $B + qa = B$. In particular if $qa \neq 0$, then B is periodic. In order to prove the claim note that the factorization $G = C + B$ is equivalent to that the sets

$$0 + B,\ a + B,\ 2a + B, \ldots, (q-1)a + B$$

form a partition of G. Adding a to the factorization $G = C + B$ we get the factorization $G = G + a = (C + a) + B$. This is equivalent to that the sets

$$a + B,\ 2a + B, \ldots, qa + B$$

form a partition of G. Comparing the two partitions gives that $B = qa + B$ as claimed.

To complete the proof replace the factor A in a minimal counter-example $G = A + B$ by the cyclic subset $C = \{0, a, 2a, \ldots, (q-1)a\}$ to get the factorization $G = C + B$. It follows that $B + qa = B$. If $qa \neq 0$, then B is periodic. Thus we may assume $|a| = q$ for each $a \in A \setminus \{0\}$. But in this case A is equal to the unique subgroup of G of order q and so A is periodic.

This completes the proof. □

References

[1] J. Charlebois, *Tiling by (k, n)-crosses*, Furman University, Electronic J. Undergraduate Math., 7 (2001), 1–11.

[2] D. R. Hickerson, *Splittings of finite abelian groups*, Pacific J. Math., 107 (1983), 141–171.

[3] A. Munemasa, *On perfect t-shift codes in abelian groups*, Des. Codes Cryptogr., 5 (1995), 253–259.

[4] A. D. Sands, *Replacement of factors by subgroups in the factorization of abelian groups*, Bull. London Math. Soc., 32 (2000), 297–304.

[5] S. K. Stein, *Tiling, packing and covering by clusters*, Rocky Mount. J. Math., 16 (1986), 277–321.

[6] S. K. Stein, *Splitting groups of prime order*, Aequationes Math., 33 (1987), 62–71.

[7] S. K. Stein and S. Szabó, Algebra and Tiling: Homomorphisms in the Service of Geometry, The Mathematical Association of America, 1994.

[8] S. Szabó, *On decomposing finite abelian groups*, Acta Math. Acad. Sci. Hung., 36 (1980), 105–114.

[9] S. Szabó, *Some problems of splitting of groups*, Aequationes Math., 30 (1986), 70–79.

[10] R. R. Varshamov and G. M. Tenengolts, *Codes which correct single asymmetric errors (in Russian)*, Autamatika i Telemekhanika 26 (1965), 288–292. English translation in Automation and Remote Control 26 (1965), 286–290.

[11] U. Tamm, *Splittings of cyclic groups and perfect shift codes*, IEEE Trans. Inform. Theory, 44 (1998), 2003–2009.

Sándor Szabó
Institute of Mathematics and Informatics
University of Pécs
Ifjúság u. 6
7624 Pécs, Hungary
e-mail: sszabo7@hotmail.com