Splittings of Cyclic Groups and Perfect Shift Codes

Ulrich Tamm

Department of Mathematics, University of Bielefeld, P. O. Box 100131, 33501 Bielefeld, Germany
tamm@mathematik.uni-bielefeld.de

Abstract. A splitting of an additive Abelian group $\mathcal{G}$ is a pair $(\mathcal{M}, \mathcal{S})$, where $\mathcal{M}$ is a set of integers and $\mathcal{S}$ is a subset of $\mathcal{G}$ such that every nonzero element $g \in \mathcal{G}$ can be uniquely written as $m \cdot h$ for some $m \in \mathcal{M}$ and $h \in \mathcal{S}$. Splittings of groups by the set $\mathcal{M} = \{\pm 1, \dots, \pm k\}$ are intimately related to tilings of the n– dimensional Euclidean space. Further, such a splitting corresponds to a perfect shift code used in the analysis of run–length limited codes correcting single peak shifts. We shall give the structure of the splitting set $\mathcal{S}$ for splittings of cyclic groups Z_p of prime order by sets of the form $\mathcal{M} = \{1, a, \dots, a^r, b, \dots, b^s\}$ and $\mathcal{M} = \{\pm 1, \pm a, \dots, \pm a^r, \pm b, \dots, \pm b^s\}$. This yields new conditions on the existence of perfect shift codes for $\mathcal{M} = \{\pm 1, \pm 2, \pm 3\}$ and $\mathcal{M} = \{\pm 1, \pm 2, \pm 3, \pm 4\}$ by the special choice $a = 2, b = 3, r = 1, 2, s = 1$. Further, it can be shown that splittings of Z_p by the set $\{\pm 1, \pm 2, \pm 3\}$ exist if and only if Z_p is also split by $\{1, 2, 3\}$.

Index terms. Shift codes, shift designs, splitting of groups, factorization of groups, peak-shift correction, tiling of Euclidean space, perfect codes

I. Introduction

Let $(\mathcal{G}, +)$ be an additive Abelian group. For any element $g \in \mathcal{G}$ and any positive integer m we define $m \cdot g = \underbrace{g + \ldots + g}_{m}$ and for a negative integer m it is $m \cdot g = -((-m) \cdot g)$. A *splitting* of an additive Abelian group $\mathcal{G}$ is a pair $(\mathcal{M}, \mathcal{S})$, where $\mathcal{M}$ is a set of integers and $\mathcal{S}$ is a subset of the group $\mathcal{G}$ such that every nonzero element $g \in \mathcal{G}$ can be uniquely written as $m \cdot h$ for some $m \in \mathcal{M}$ and $h \in \mathcal{S}$. It is also said that $\mathcal{M}$ *splits* $\mathcal{G}$ with *splitting set* $\mathcal{S}$. The notation here is taken from [1] which may also serve as an excellent survey on splittings of groups and its relation to tiling the Euclidean space by special clusters (see later on). Further surveys are [2], [3], [4]. In [5] Levenshtein and Vinck investigated perfect run–length–limited codes which are capable of correcting single peak shifts. As a basic combinatorial tool for the construction of such codes they introduced the concept of a *k–shift code*, which is defined to be a subset $\mathcal{H}$ of a finite additive Abelian group $\mathcal{G}$, with the property that for any $m = 1, \dots, k$ and any $h \in \mathcal{H}$ all elements $\pm m \cdot h$ are different and not equal to zero. Such a code is said to be *perfect* if for every nonzero element $g \in \mathcal{G}$ there are exactly one $h \in \mathcal{H}$ and $m \in \{1, \dots, k\}$ such that $g = m \cdot h$ or $g = -m \cdot h$. Hence a perfect shift code just is a splitting of a group $\mathcal{G}$ by the set

$$F(k) = \{\pm 1, \pm 2, \dots, \pm k\}$$

Levenshtein and Vinck [5] also gave explicit constructions of perfect shift codes for the special values $k = 1, 2$ and for the case $k = \frac{p-1}{2}$, where p is a prime number. Later Munemasa [6] gave necessary and sufficient conditions for the existence of perfect shift codes for the parameters $k = 3$ and $k = 4$. Munemasa also introduced the notion shift code (originally in [5] it was called shift design). One may think of the elements $h \in \mathcal{H}$ as codewords and the set $\{\pm h, \pm 2h, \dots, \pm kh\}$ as the sphere around the codeword h. Implicitly, this code concept is already contained in [7]. Here Golomb refers to Stein's paper [8], in which splittings by $F(k)$ and

$$S(k) = \{1, 2, \dots, k\}$$

had been introduced to study an equivalent geometric problem concerning tiling of R^n by certain star bodies (this will be presented in Section IV). These star bodies just correspond to the error spheres which have been discussed in [7] under the names Stein sphere and Stein corner, respectively (without giving an application in Coding Theory). We shall also use the notion *sphere* around h for the set $h \cdot \mathcal{M}, h \in \mathcal{S}$ for any splitting $(\mathcal{M}, \mathcal{S})$.

In this paper we shall investigate splittings of cyclic groups Z_p of prime order p by sets of the form

$$\mathcal{M}_1 = \{1, a, a^2, \ldots, a^r, b, b^2, \ldots, b^s\}, \tag{1}$$

and

$$\mathcal{M}_2 = \{\pm 1, \pm a, \pm a^2, \ldots, \pm a^r, \pm b, \pm b^2, \ldots, \pm b^s\},$$

where $r \geq 1$ and $s \geq 1$ are nonnegative integers smaller than the orders of a and b in Z_p, respectively, which we shall denote by $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$.

Observe that for the special choice $a = 2, b = 3$ and $r = 1, s = 1$ (or $r = 2, s = 1$, respectively) the sets $S(3)$ and $F(3)$ (or $S(4)$ and $F(4)$) arise. It was shown by Galovich and Stein [9] and by Munemasa [6], respectively, that the analysis of splittings of finite Abelian groups by $S(k)$ and $F(k)$, respectively, for the parameters $k = 3, 4$ can essentially be reduced to the analysis of splittings by the same sets in cyclic groups Z_p of prime order (the exact results are presented in Section IV).

In this case a splitting of the additive group $(Z_p, +)$ corresponds to a *factorization* of the multiplicative group $(Z_p^* = Z_p \backslash \{0\}, \cdot)$. A factorization of a (multiplicative) group $\mathcal{G}$ is a representation $\mathcal{G} = \mathcal{A} \cdot \mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are subsets of $\mathcal{G}$ such that every element $g \in \mathcal{G}$ can be uniquely written as a product $a \cdot b$ for some $a \in \mathcal{A}$ and $b \in \mathcal{B}$. So for p prime a splitting $(\mathcal{M}, \mathcal{S})$ in Z_p yields the factorization $Z_p^* = \mathcal{M} \cdot \mathcal{S}$ and vice versa, since now $\mathcal{M}$ is also a subset of Z_p^*.

Further, the splittings $(\mathcal{M}_2, \mathcal{S})$ of the cyclic group Z_p by the set $\mathcal{M}_2$ correspond to factorizations of the group $Z_p^*/\{1, -1\} = \mathcal{M}_1 \cdot \mathcal{S}$. Since only one of the elements g and $-g$ can be contained in the splitting set $\mathcal{S}$ and since both elements must be simultaneously contained in the same sphere around an element of the splitting set $\mathcal{S}$, we can identify them by considering Z_p^* modulo the units $\{1, -1\}$. On the other hand, every factorization $Z_p^*/\{1, -1\} = \mathcal{M}_1 \cdot \mathcal{S}$ yields a factorization $Z_p^* = \mathcal{M}_2 \cdot \mathcal{S}'$ with the elements of the factor $\mathcal{S}'$ in Z_p^* regarded as the coset representatives for the cosets belonging to $\mathcal{S}$ in $Z_p^*/\{1, -1\}$. Hence, in the search for splittings of Z_p by the sets $\mathcal{M}_1$ and $\mathcal{M}_2$ we can concentrate on finding factorizations $\mathcal{G} = \mathcal{M}_1 \cdot \mathcal{S}$, where $\mathcal{G} = Z_p^*$ or $\mathcal{G} = Z_p^*/\{1, -1\}$.

In order to characterize the structure of a splitting set $\mathcal{S}$ for splittings by $\mathcal{M}_1$ or $\mathcal{M}_2$ we first need some further notation. As usual, we denote by

$$< a, b >= \{a^i \cdot b^j, i = 1, \ldots, \mathrm{ord}(a), j = 1, \ldots, \mathrm{ord}(b)\} \tag{2}$$

the subgroup of $\mathcal{G}$ generated by the elements a and b. Furthermore let

$$\mathcal{F} = \{a^i \cdot b^j, i - j \equiv 0 \bmod (r + s + 1)\}. \tag{3}$$

Observe that $\mathcal{F}$ is the subgroup in $\mathcal{G}$ generated by the elements a^{r+s+1}, b^{r+s+1}, and ab. It can be shown that a splitting by the set $\mathcal{M}_1$ (by the set $\mathcal{M}_2$) in Z_p exists exactly if for each element $f \in \mathcal{F}$, where $\mathcal{F}$ is a subgroup of $\mathcal{G} = Z_p^*$ (a subgroup of $\mathcal{G} = Z_p^*/\{1, -1\}$ for splittings by $\mathcal{M}_2$) all possible representations $f = a^i \cdot b^j$ as a product of powers of a and b are such that $i - j \equiv 0 \bmod (r + s + 1)$. Necessary and sufficient conditions are given in the following theorem.

THEOREM 1: Let $\mathcal{M}_1 = \{1, a, a^2, \ldots, a^r, b, b^2, \ldots, b^s\}$. A factorization $\mathcal{G} = \mathcal{M}_1 \cdot \mathcal{S}$ of the group $\mathcal{G} = Z_p^*$ ($\mathcal{G} = Z_p^*/\{1, -1\}$) by the set $\mathcal{M}_1$ and hence a splitting of Z_p by $\mathcal{M}_1 (\mathcal{M}_2 = \{\pm 1, \pm a, \ldots, \pm a^r, \pm b, \ldots, \pm b^s\})$ exists if and only if the splitting set $\mathcal{S}$ is of the form

$$\mathcal{S} = x_0 \cdot \mathcal{F} \cup x_1 \cdot \mathcal{F} \cup \ldots \cup x_{\rho-1} \cdot \mathcal{F}, \tag{4}$$

where ρ is the number of cosets of the subgroup $< a, b >$ of $\mathcal{G}$ and the $x_i, i = 0, \ldots, \rho - 1$ are representatives of each of these cosets and where

$$\mathrm{ord}(a) \text{ and } \mathrm{ord}(b) \text{ are divisible by } r + s + 1. \tag{5}$$

Further, if $b^{l_1} = a^{l_2}$ for some integers l_1 and l_2, then

$$l_1 + l_2 \equiv 0 \text{ mod } (r + s + 1) \tag{6}$$

Observe that condition (5) is a special case of (6). However, in the proof of Theorem 1, which will be carried out in Section II, we shall first derive (5). Further (5) is also important in order to find splittings by computer research (see Section III).

There have been derived necessary and sufficient conditions on the existence of splittings of Z_p (and derived from them also conditions for arbitrary finite Abelian groups) by $\mathcal{M}_1$ and $\mathcal{M}_2$ for the special cases $\mathcal{M} = \{1, a, b\}$ by Galovich and Stein [9], for $\mathcal{M} = \{1, 2, 3\}$ by Stein [10], and for $\mathcal{M} = \{\pm 1, \pm 2, \pm 3\}$ and $\mathcal{M} = \{\pm 1, \pm 2, \pm 3, \pm 4\}$ by Munemasa [6]. We shall discuss these conditions in Section II and compare them with those of Theorem 1.

Further in Section II, as a consequence of Theorem 1, it will be derived that if $r + s$ is an even number, then the set of prime numbers p, for which a splitting of Z_p by $\mathcal{M}_1$ exists, is the same as the set of prime numbers p for which a splitting of Z_p by $\mathcal{M}_2$ exists. Especially, this holds for the sets $\mathcal{M}_1 = \{1, 2, 3\}$ and $\mathcal{M}_2 = \{\pm 1, \pm 2, \pm 3\}$, which answers a general respective question by Galovich and Stein [9] for this special case. Hence it is possible to treat splittings by $\{1, 2, 3\}$ and $\{\pm 1, \pm 2, \pm 3\}$ simultaneously, to show the equivalence of several of the above – mentioned conditions, and to apply results on splittings by $\{1, 2, 3\}$ in the analysis of perfect 3 – shift codes (which are just splittings by $\{\pm 1, \pm 2, \pm 3\}$).

In principle, splittings by sets $\mathcal{M}_1$ and $\mathcal{M}_2$ are completely characterized by Theorem 1. However, in order to find such splittings, several conditions imposed on the orbit of the elements a and b by (5) and (6) have to be verified.

This will be done in Section III for sets of the form $\mathcal{M} = \{1, a, b\}$ and $\mathcal{M} = \{1, a, a^2, b\}$, from which the perfect 3– and 4–shift codes can be obtained by the special choice of the parameters $a = 2$ and $b = 3$.

In Section IV we shall discuss the relation between splittings by $F(k)$ and $S(k)$ and tiling of the Euclidean space R^n by certain star bodies, the cross and the semicross. Further, we shall present the above – mentioned results from [6] and [9] on splittings of groups of composite order.

Finally, in Section V, the application of shift codes in peak – shift correction of run – length limited codes is briefly discussed and further connections between splittings of groups and Coding Theory are pointed out. Especially, splittings by $F(k)$ correspond to single – error correcting codes in the Lee metric and related error measures.

II. Factorizations of Z_p^* and $Z_p^*/\{1, -1\}$ with the Set $\{1, a, \ldots, a^r, b, \ldots, b^s\}$

We mentioned already that $\mathcal{F}$ is generated by the elements a^{r+s+1}, b^{r+s+1}, and ab in $\mathcal{G} = Z_p^*$ or $\mathcal{G} = Z_p^*/\{1, -1\}$. The next lemma shows that with $x \in \mathcal{S}$ these three elements multiplied by x necessarily are also contained in $\mathcal{S}$.

Lemma 1: In a factorization $\mathcal{G} = \mathcal{M}_1 \cdot \mathcal{S})$ with every element $x \in \mathcal{S}$, also $(ab)x \in \mathcal{S}$ and $a^{r+s+1}x$ and $b^{r+s+1}x$ must be the next powers of a and b, respectively, which multiplied by x are contained in $\mathcal{S}$.

Proof: Let $x \in \mathcal{S}$ be an element of the splitting set $\mathcal{S}$. Then $(ab)x$ must also be contained in $\mathcal{S}$. If this would not be the case, then $(ab)x = a^k y$ for some $k \in \{1, \ldots, r\}$ and $y \in \mathcal{S}$ or $(ab)x = b^l y'$ for some $l \in \{1, \ldots, s\}$ and $y' \in \mathcal{S}$. If $(ab)x = a^k y$ then $x' = bx = a^{k-1}y$ and x' would have two different representations $mh, m'h'$ with $m, m' \in \mathcal{M}_1$ and $h, h' \in \mathcal{S}$, which contradicts the definition of a splitting. Analogously, if $(ab)x = b^l y'$ then $x' = ax = b^{l-1}y'$ would have two different representations, which is not possible.

Now let k^* be the minimum power k such that $a^k x \in \mathcal{S}$ for some $x \in \mathcal{S}$. We have to show that $k^* = r + s + 1$.

First observe that obviously $k^* \geq r+1$, since otherwise $x' = a^{k^*} (= 1 \cdot x')$ would occur in two different ways as product of elements of $\mathcal{M}_1$ and $\mathcal{S}$.
In order to see that $k^* \notin \{r+1, \ldots, r+s\}$, we shall prove by induction the stronger statement

$$\text{If } x \in \mathcal{S} \text{ then for all } i = 1, \ldots, s+1 \text{ it is } a^{r+i}x = b^{s+1-i}y_i \text{ with } y_i = (ab)^{i-1}y \text{ for some } y \in \mathcal{S} \tag{7}$$

The statement (7) holds for $i = 1$, since $a^{r+1}x = b^j y$ for some $y \in \mathcal{S}$ and $j \in \{0, \ldots, s-1\}$ is not possible. Otherwise, $a^{r+1}bx = a^r(abx) = b^{j+1}y$ could be written in two different ways as product of members of the splitting set (abx and y) and elements of $\mathcal{M}_1$ (a^r and b^{j+1}).
So we proved that for $x \in \mathcal{S}$ it is $a^{r+1}x = b^s y$ for some $y \in \mathcal{S}$. Hence $a^{r+2}x = b^{s-1} \cdot aby = b^{s-1}y_2$ with $y_2 = aby \in \mathcal{S}$ and further $a^{r+3}x = b^{s-2}y_3$ with $y_3 = (ab)^2 y \in \mathcal{S}$, $\ldots$, $a^{r+s}x = b^y_s$ with $y_s = (ab)^{s-1}y \in \mathcal{S}$, and $a^{r+s+1}x = (ab)^s y \in \mathcal{S}$.
So $a^{r+s+1}x \in \mathcal{S}$ and $a^{r+i}x \notin \mathcal{S}$ for $i \in \{1, \ldots, s\}$, since otherwise the element $a^{r+i+1}b^{i+1}x = a^r((ab)^{i+1}x) = b^s y_i$ could be represented in two different ways as a product of a member of the splitting set ($(ab)^{i+1}x$ or y_i) and an element of $\mathcal{M}_1$ (a^r or b^s).
Analogously, it can be shown that $r+s+1$ is also the minimum power l^* such that $b^{l^*}x \in \mathcal{S}$ when $x \in \mathcal{S}$ (obviously $l^* > s$ and $l^* \notin \{s+1, \ldots, s+r\}$ by an argument as (7)).

Proof of Theorem 1:

First we shall demonstrate that a set $\mathcal{S}$ with the properties (4), (5), and (6) from Theorem 1 is a splitting set as required. It suffices to show that every element $z = a^i b^j$ of the subgroup $< a, b >$ can uniquely be obtained from one element $a^{i'} b^{j'}, i' - j' \equiv 0 \bmod (r+s+1)$ in $\mathcal{F}$ by multiplication with a power of a or b from the set $\mathcal{M}_1 = \{1, a, a^2, \ldots a^r, b, b^2, \ldots b^s\}$.
To see this let $z = a^i b^j$ with $i - j \equiv k \bmod (r+s+1)$. If $k = 0$, then by (5) and (6) z must be contained in $\mathcal{S}$. If $k \in \{1, \ldots, r\}$, then $z = a^k h = a^k(a^{i-k}b^j)$ is the only possibility to write z as a product of an element (namely a^k) from $\mathcal{M}_1$ and a member h of $\mathcal{S}$. Finally, if $k \in \{r+1, \ldots, r+s\}$, then again by (5) and (6) $z = b^k h' = b^k(a^i b^{j-k})$ is the unique way of representing z as product of an element (b^k) of $\mathcal{M}_1$ and one (h') of $\mathcal{S}$.

In order to show that a splitting set $\mathcal{S}$ must have a structure as in (4), let now $x \in \mathcal{S}$. Lemma 1 then implies that all powers of a^{r+s+1}, b^{r+s+1} and ab and all combinations of them, i. e., all elements of the form

$$h = (a^{r+s+1})^{k_1}(b^{r+s+1})^{k_2}(ab)^{k_3} = a^{(r+s+1)\cdot k_1 + k_3} b^{(r+s+1)\cdot k_2 + k_3} \tag{8}$$

multiplied by x must also be contained in $\mathcal{S}$, which just yields that $hx \in \mathcal{S}$ for all

$$h = a^i \cdot b^j \text{ with } i - j \equiv 0 \bmod r+s+1 \tag{9}$$

It is also clear that every element of this form (9) can occur as a combination (8). So all elements of $\mathcal{F}$ as defined under (3) multiplied by x must be contained in $\mathcal{S}$, if $x \in \mathcal{S}$.
Further observe that with $x \in \mathcal{S}$ an element of the form $a^i b^j x$ with $i-j$ not divisible by $r+s+1$ cannot be contained in a splitting set $\mathcal{S}$, since in this case the unique representability would be violated (see above).
Since the elements of a proper coset $\mathcal{N}$ in $\mathcal{G}$ of $< a, b >$ cannot be obtained from elements of another such coset by multiplication with powers of a or b, for every such coset $\mathcal{N}$ we can choose a representative $x_{\mathcal{N}}$ and the elements $x_{\mathcal{N}} \cdot \mathcal{F}$ can be included in the splitting set in order to assure that every element from $\mathcal{N}$ can be uniquely written as a product $m \cdot h, m \in \mathcal{M}_1, h \in \mathcal{S}$.

The conditions (5) and (6) are necessary conditions on the orbits of a and b that must be fulfilled if a perfect shift code should exist in $\mathcal{G}$.
It is easy to verify that the elements a and b each must have an order divisible by $r+s+1$ in order to assure the existence of a factorization $\mathcal{G} = \mathcal{M}_1 \cdot \mathcal{S}$, $\mathcal{G} = Z_p^*, Z_p^*/\{1, -1\}$. Assume that this would not be the case, e. g.,

$$\text{ord}(a) = k_1 \cdot (r+s+1) + k_2, 0 < k_2 < r+s+1.$$

By Lemma 1 with $x \in \mathcal{S}$ all elements $(a^{r+s+1})^k x$ must also be contained in the set $\mathcal{S}$. However, for $k = k_1 + 1$ this yields

$$\mathcal{S} \ni (a^{r+s+1})^{k_1+1} x = a^{(r+s+1)k_1 + k_2 + ((r+s+1)-k_2)} x = a^{r+s+1-k_2} x$$

which is not possible by Lemma 1.
Further, from Lemma 1 we can conclude that with $x \in \mathcal{S}$ also $(ab)^{l_1} x$ and $(ab)^{l_2} x$ for all l_1 and l_2 are contained in the splitting set $\mathcal{S}$. Now if $a^{l_1} = b^{l_2}$ then $(ab)^{l_1} = a^{l_1} b^{l_1} = b^{l_1+l_2}$, $(ab)^{l_2} = a^{l_2} b^{l_2} = a^{l_1+l_2}$ and with Lemma 1 and the preceding considerations $l_1 + l_2$ must be divisible by $r+s+1$.

REMARKS:

1) Observe that (for a and b fulfilling (5) and (6)) all the sets $\mathcal{M}_1 = \{1, a, \ldots, a^r, b, \ldots, b^s\}$ ($\mathcal{M}_2 = \{\pm 1, \pm a, \ldots, \pm a^r, \pm b, \ldots, \pm b^s\}$) with the same sum $r+s$ yield the same splitting set.

2) Obviously, the group $\mathcal{F}$ fulfilling conditions (5) and (6) also is defined for $i - j \equiv 0 \bmod 2$, although this case for our considerations is not of importance since then $r = 0$ or $s = 0$ and one of the parameters a or b will not occur.

It can be shown (following the considerations in [5] about 2–shift codes) that a splitting by $\{1, a, \ldots, a^r\}$ ($\{\pm 1, \pm a, \ldots, \pm a^r\}$) in Z_p exists exactly if the order of a in Z_p^* ($Z_p^*/\{1, -1\}$) is divisble by $r+1$. This is clear, since with $x \in \mathcal{S}$ also $a^{r+1}x$ must be a member of the splitting set $\mathcal{S}$ in this case.

Galovich and Stein [9] already considered splittings of Abelian groups by the set $\{1, a, b\}$. They could derive necessary and sufficient conditions on the existence of splittings. Especially for $a = 2, b = 3$, they found for cyclic groups of prime order $p \equiv 1 \bmod 3$:

(i) Let g be a generator of $< 2, 3 >$ and let $2 = g^u, 3 = g^v, d = \gcd(u, v), u' = \frac{u}{d}, v' = \frac{v}{d}$, and $d_1 = \gcd(d, p-1)$. Then $\{1, 2, 3\}$ splits Z_p if and only if 3 divides $\frac{p-1}{d_1}$ and $u' \cdot v' \equiv 2 \bmod 3$.

Later Stein [10] obtained further necessary and sufficient conditions for splittings by $\{1, 2, 3\}$ using number theoretic methods involving Newton sums (see also Section IV).

(ii) The set $\{1, 2, 3\}$ splits Z_p if and only if for some positive integer u it is $1^{(p-1)/3u} + 2^{(p-1)/3u} + 3^{(p-1)/3u} \equiv 0 \bmod p$ and $(1^{(p-1)/3u})^2 + (2^{(p-1)/3u})^2 + (3^{(p-1)/3u})^2 \equiv 0 \bmod p$.

Munemasa considered splittings by $\{\pm 1, \pm 2, \pm 3\}$ and by $\{\pm 1, \pm 2, \pm 3, \pm 4\}$. He found necessary and sufficient conditions based on the behaviour of the subgroups $< -1, 2, 3 >$ and $< -1, 6 >$ of Z_p^* generated by the elements $-1, 2, 3$ and $-1, 6$ respectively.

(iii) A splitting of Z_p, where p is aprime number, by $\{\pm 1, \pm 2, \pm 3\}$ exists if and only if

$| < -1, 2, 3 > : < -1, 6 > | \equiv 0 \bmod 3.$

(iv) A splitting of Z_p, where p is a prime number, by $\{\pm 1, \pm 2, \pm 3, \pm 4\}$ exists if and only if $| < -1, 2, 3 > : < -1, 6 > | \equiv 0 \bmod 4.$

Whereas in order to check condition (i) one has to find a generator of the subgroup $< 2, 3 >$, the approach in [6] is very similar to the one in this paper.

Munemasa [6] proved (for $a = 2, b = 3, r = 1, 2, s = 1$) that with $a, b \in \mathcal{S}$ also the elements ab and a^{r+s+1} must be contained in the splitting set $\mathcal{S}$. His proof then follows a different line compared to the proof of Theorem 1, where it is shown next that also b^{r+s+1} must be a member of $\mathcal{S}$. Theorem 1 describes the structure of the splitting set such that only the conditions (5) and (6) have to be checked, which can be done faster than checking (iii) or (iv). However, the aim in [6] and [9] was to characterize splittings of arbitrary Abelian groups and not only of Z_p. In order to do so, a general approach does not work. Such conditions have to be verified for each set $\mathcal{M}$ individually, if the group orders are composite numbers.

Further, Saidi [11] obtained necessary conditions on the existence of splittings by $\{1, 2, 3\}$ and by $\{\pm 1, \pm 2, \pm 3\}$ based on cubic residues.

(v) Assume that 2 and 3 are cubic nonresidues mod p and $L \equiv \pm M \bmod 12$, where $4p = L^2 + 27M^2, L \equiv 1 \bmod 3$. Then $\{1, 2, 3\}$ splits Z_p.

The primes fulfilling the above conditions are also characterized in [11], they are of the form $p = 7M^2 \pm 6MN + 36N^2$, where $L = M \pm 12N$. Since any primitive quadratic form represents infinitely many primes [12], Saidi further concludes that the set $\{1, 2, 3\}$ splits Z_p for infinitely many primes p. It can be shown that this last condition (v) is not sufficient, since there is a splitting in Z_p for $p = 919$ but 919 is not of the form as required in (v) (cf. also Section III). In [11] similar conditions (with $L \equiv \pm M \bmod 24$) as in (v) are derived for the set $\{\pm 1, \pm 2, \pm 3\}$, from which by the same argumentation as above follows that there are infinitely many primes p for which a splitting of Z_p by $\{\pm 1, \pm 2, \pm 3\}$ and hence a perfect 3–shift code exists.

Observe, that in [11] splittings by the sets $\{1, 2, 3\}$ and $\{\pm 1, \pm 2, \pm 3\}$ are treated separately. As a consequence of Theorem 1, we shall now show that they can be analyzed simultaneously. This follows from a more general result.

THEOREM 2: Let r, s be positive integers such that $r + s$ is an even number. Then a splitting of the group Z_p, p prime, by the set $\mathcal{M}_1 = \{1, a, \dots, a^r, b, \dots, b^s\}$ exists if and only if there also is a splitting of Z_p by the set $\mathcal{M}_2 = \{\pm 1, \pm a, \dots, \pm a^r, \pm b, \dots, \pm b^s\}$

PROOF: It is easy to see that from every splitting $(\mathcal{S}, \mathcal{M}_2)$ of Z_p by the set $\mathcal{M}_2$ we obtain a splitting $(\mathcal{S} \cup -\mathcal{S}, \mathcal{M}_1)$ of Z_p by the set $\mathcal{M}_1$. This holds because for every $h \in \mathcal{S}$ by definition of a splitting the sphere $\{\pm h, \pm ha, \dots, \pm ha^r, \pm hb, \dots, \pm hb^s\} = \{h, ha, \dots, ha^r, hb, \dots, hb^s\} \cup \{-h, -ha, \dots, -ha^r, -hb, \dots, -hb^s\}$ and hence h and $-h$ can be chosen as members of the splitting set in a splitting of Z_p by $\mathcal{M}_1$.

In order to show the converse direction, we shall prove that whenever there exists a splitting of Z_p by $\mathcal{M}_1$, it is also possible to find a splitting $(\mathcal{S}, \mathcal{M}_1)$ of Z_p such that with every element $h \in \mathcal{S}$ also its additive inverse $-h$ is contained in the splitting set. in this case the two spheres $\{h, ha, \dots, ha^r, hb, \dots, hb^s\}$ and $\{-h, -ha, \dots, -ha^r, -hb, \dots, -hb^s\}$ are disjoint by definition of a splitting such that their union $\{\pm h, \pm ha, \dots, \pm ha^r, \pm hb, \dots, \pm hb^s\}$ is a sphere in a splitting by $\mathcal{M}_2$.

By Theorem 1 the splitting set $\mathcal{S}$ is essentially determined by the subgroup $\mathcal{F} = \{a^i b^j : i - j \equiv 0 \bmod (r + s + 1) \subset < a, b >$ (with the conditions (5) and (6) fulfilled). Obviously, the element $1 \in \mathcal{F}$. Now there are two possible structures of $\mathcal{F}$ depending on the behaviour of -1:

1) $-1 \in < a, b >$: Then also $-1 \in \mathcal{F}$, since otherwise $-1 = a^i b^j$ for some $i - j \not\equiv 0 \bmod (r + s + 1)$ and hence $1 = (-1)^2 = a^{2i} b^{2j} \notin \mathcal{F}$ (since $2(i - j) \not\equiv 0 \bmod (r + s + 1)$) which is not possible. Since $\mathcal{F}$ is a group, with every element $h \in \mathcal{F}$ hence also $-h \in \mathcal{F}$. Also, for every coset $x_i < a, b >, i = 0, \dots, \rho - 1$, obviously, with $x_i h, h \in \mathcal{F}$ also $-x_i h$ must be contained in the splitting set $\mathcal{S}$.

2) $-1 \notin < a, b >$: Then -1 must be contained in the coset $- < a, b >$ and one can choose $x_1 = -x_0$ as representative of this coset and include $x_1 \mathcal{F} = -x_0 \mathcal{F}$ in the splitting set $\mathcal{S}$, if x_0 is the representative from $< a, b >$ such that $x_0 \mathcal{F} \in \mathcal{S}$.

From the next coset (if there are still some cosets left not used so far for the splitting set) we include some representative x_2 and hence also $x_2\mathcal{F}$ into the splitting set. Now the element $-x_2$ cannot be contained in any coset from which already elements are included into the splitting set so far. Obviously $-x_2$ is not contained in $x_2 < a, b >$ (since $-1 \notin < a, b >$) and if it were contained in $< a, b >$, then x_2 would be an element of $- < a, b >$ and vice versa, which is not possible by construction.
In the same way we can continue to include pairs $h, -h$ from the cosets of $< a, b >$ not used so far and with them the sets $h\mathcal{F}$ and $-h\mathcal{F}$ into the splitting set $\mathcal{S}$ until there is no further coset left.

REMARKS:

1) For $r + s$ odd a similar result does not hold, since then it is possible that $-1 \in < a, b >$ but $-1 \notin \mathcal{F}$, since now $2(i - j)$ may be divisible by $r + s + 1$ although $i - j \not\equiv 0 \bmod (r + s + 1)$. For instance, there exist splittings of Z_p by $\mathcal{M}_1 = \{1, 2, 3, 4\}$ for $p = 409, 1201, 2617, 3433$, but there do not exist splittings by $\{\pm 1, \pm 2, \pm 3, \pm 4\}$ in the same groups.

2) For $r + s$ even there are two possible structures for a splitting set $\mathcal{S}$. Either $-1 \in < a, b >$, then automatically $-1 \in \mathcal{F}$ and hence with every element $h \in \mathcal{S}$ also $-h$ is forced to be in the splitting set $\mathcal{S}$. If $-1 \notin < a, b >$, then there also exist splittings for which there are elements h in the splitting set $\mathcal{S}$ such that $-h \notin \mathcal{S}$ – depending on the choice of the representatives of the cosets.

By the special choice of the parameters $a = 2, b = 3, r = s = 1$ the following corollary is immediate.

COROLLARY 1: A splitting of the group Z_p, p prime, by the set $\{1, 2, 3\}$ exists if and only if there also is a splitting of Z_p by the set $\{\pm 1, \pm 2, \pm 3\}$.

Obviously, by the first argument in the proof of Theorem 2 (derive a splitting $(\mathcal{S} \cup -\mathcal{S}, \mathcal{M}_1)$ from a splitting $(\mathcal{S}, \mathcal{M}_2)$) it holds that for every positive integer k the group Z_p is split by $S(k) = \{1, \dots, k\}$ if it is split by $F(k) = \{\pm 1, \dots, \pm k\}$. In [9] it is asked for which parameters k the converse holds (for arbitrary finite Abelian groups). Hickerson ([4], p. 168) demonstrated by the example $p = 281$ that the converse does not hold for $k = 2$. Corollary 1 now demonstrates that it holds for $k = 3$ and with Remark 1 it is clear that the converse does not hold for $k = 4$. However, for arbitrary Abelian groups splittings by $\{1, 2, 3\}$ and $\{\pm 1, \pm 2, \pm 3\}$ are not equivalent, since there is the trivial splitting $(\{1, 2, 3\}, \{1\})$ in Z_4 and obviously in Z_4 a splitting by $\{\pm 1, \pm 2, \pm 3\}$ does not exist. In Section IV we shall see that this is essentially the only exception. Further from Corollary 1, it is immediate that the conditions (i), (ii), and also (iii) now characterize splittings of Z_p by $\{1, 2, 3\}$ as well as by $\{\pm 1, \pm 2, \pm 3\}$.

III. COMPUTATIONAL RESULTS ON SPLITTINGS AND PERFECT 3– AND 4–SHIFT CODES

Theorem 1 in principle completely characterizes splittings of Z_p by $\mathcal{M}_1 = \{1, a, \dots, a^r, b, \dots, b^s\}$ and $\mathcal{M}_2 = \{\pm 1, \pm a, \dots, \pm a^r, \pm b, \dots, \pm b^s\}$. The conditions on the existence of such splittings, however, have to be verified for each Z_p^* or $Z_p^*/\{1, -1\}$ individually. Especially, condition (6) requires that many products $a^i b^j$ have to be calculated. Often it is enough to check the orbits of the elements a and b, since a splitting cannot exist if (5) is violated. The complexity can also be reduced when a generator of the subgroup $< a, b >$ is known (cf. the Galovich/Stein condition (i) from the previous section). A good candidate is the element ba^{-1}, since if a is contained on its orbit, so is $b = a(ba^{-1})$ and hence all products $a^i b^j$.

COROLLARY 2: If a is on the orbit of ba^{-1} in $\mathcal{G} = Z_p^*$ or $\mathcal{G} = Z_p^*/\{1, -1\}$, i. e., $a = (ba^{-1})^l$ for some l, then (with $\mathcal{F}$ fulfilling the conditions (5) and (6))

i) $< a, b >= \{(ba^{-1})^m : m = 0, \dots, \operatorname{ord}(ba^{-1}) - 1\}$ is generated by the element ba^{-1},

ii) For $r = s = 1$, i. e., $r + s + 1 = 3$, $\mathcal{F}$ is generated by $(ba^{-1})^3$, hence

$$\mathcal{F} = \{(ba^{-1})^{3m} : m = 0, \ldots, \frac{1}{3}\text{ord}(ba^{-1}) - 1\},$$

iii) A factorization $\mathcal{G} = \{1, a, b\} \cdot \mathcal{F}$ exists, exactly if

$$l \equiv 1 \bmod 3$$

Proof: i) is clear from the preceding discussion. In order to prove (ii) and (iii), observe that obviously by (6) the order of ba^{-1} must be divisible by 3. Hence, $(ba^{-1})^m = b^m a^{-m} \in \mathcal{F}$ exactly if m is divisible by 3. Further observe that $\mathcal{F}$ is generated by $a^3 = (ba^{-1})^{3l} \in \mathcal{F}, b^3 = (ba^{-1})^{3(l+1)} \in \mathcal{F}$ and $ab = (ba^{-1})^{2l+1}$ which is contained in $\mathcal{F}$ exactly if $l \equiv 1 \bmod 3$.

For $\mathcal{G} = Z_p^*$ the results in Corollary 2 already can be derived from the considerations in [9]. Following the same line of proof, Corollary 2 can be extended to the case $r + s + 1$ odd, where then (iii) reads $l \equiv \frac{r+s}{2} \bmod (r + s + 1)$.

With the set $\mathcal{M}_1 = \{1, a, b\}$ the perfect 3–shift codes (splittings by $\{\pm 1, \pm 2, \pm 3\}$ or with Corollary 1 even by $\{1, 2, 3\}$ of Z_p) arise for the special choice of the parameters $a = 2$ and $b = 3$. It is possible to formulate necessary and sufficient conditions on the existence of perfect 3–shift codes depending only on the behaviour of the element $3 \cdot 2^{-1}$, even if this does not generate the subgroup $< 2, 3 >$[13].

As mentioned before, perfect shift codes are much faster to find if the subgroup $\mathcal{F}$ is generated by one element and one might first check the orbit of 2, 3, or $3 \cdot 2^{-1}$ by Theorem 1 and Corollary 2. This way, it was calculated that the first perfect 3–shift codes for primes up to 1000 exist in Z_p for $p =$ 7, 37, 139, 163, 181, 241, 313, 337, 349, 379, 409, 421, 541, 571, 607, 631, 751, 859, 877, 919, 937.

Saidi [11] computed a list of all primes $p < 1000$ such that a splitting of Z_p by $\{1, 2, 3\}$ fulfilling condition (v) of the previous section exists. It was mentioned before that condition (v) is not sufficient, since $p = 919$ is not of the required form. However, for all other primes, the list of [11] coincides with our list above.

4–shift codes are just splitting sets obtained from splittings of Z_p by the set $\{\pm 1, \pm a, \pm a^2, \pm b\}$ for the special choice of the parameters $a = 2$ and $b = 3$. Again it might be useful to consider the orbit of further elements besides a and b to speed up the computation of an algorithm which finds perfect shift codes. However, the element ba^{-1} now does not generate $< a, b >$, but also the orbit of the element ba^{-2} may be checked now.

Corollary 3: If a splitting $(\{1, a, a^2, b\}, \mathcal{S})$ of a group $\mathcal{G} = Z_p^*$ or $\mathcal{G} = Z_p^*/\{1, -1\}$ exists, then

i) ba^{-1} has even order in $\mathcal{G}$,

ii) a is not on the orbit of ba^{-1},

iii) if $a^{4l_1} = (ba^{-1})^{l_2}$ for some positive integers l_1 and l_2, then $l_2 \equiv 0 \bmod 2$.

iv) $\mathcal{F}$ is the union of the cosets of the subgroup $< (ba^{-2})^4 >$ generated by the element $(ba^{-2})^4$.

Proof:

i) is immediate from conditions (5) and (6), since if $1 = (ba^{-1})^m = (ba)^m \cdot a^{-2m}$ then $2m$ must be divisible by 4.

ii) If $(ba^{-1})^m = a$ for some m, then $b^m = a^{m+1}$, which cannot occur since $2m + 1$ is not divisible by 4 (condition (6)).

iii) follows from condition (6).

iv) If a splitting by $\{\pm 1, \pm a, \pm a^2, \pm b\}$ exists, then for some t it is $(ba^{-2})^t = 1 \in \mathcal{F}$. Hence $b^t = a^{2t}$ and by (6) the order t of ba^{-2} must be divisible by 4. Now by conditions (5) and (6) $(ba^{-2})^m$

can be contained in $\mathcal{F}$ if and only if m is divisible by 4, since $(ba^{-2})^m = b^m a^{-2m} = b^m a^{t-2m}$ and $3m - t$ and hence also m must be divisible by 4.

There are only 21 prime numbers $p = 8N + 1 < 25000$ for which a perfect 4–shift code exists in Z_p, namely $p = 97$, 1873, 2161, 3457, 6577, 6673, 6961, 7297, 7873, 10273, 12721, 13537, 13681, 13729, 15601, 15649, 16033, 16561, 16657, 21121, 22129.
Observe that $p = 2161$ is the first number for which as well a perfect 3–shift as a perfect 4–shift code in Z_p exists.

For $q = r + s + 1 > 3$ it is not known if there are infinitely many primes for which a splitting by the sets $\mathcal{M}_1$ or $\mathcal{M}_2$ in Z_p exists. For $q = 3$ this follows from Saidi's investigations (cf. the considerations after condition (v) in Section II).
Stein [8] could demonstrate that the set of positive integers N for which a splitting by $\{\pm 1, \pm 2, \pm 3\}$ exists in Z_N has density 0.
The distribution of 3– and 4– shift codes among the first 500 primes of the required form $p = 2qN + 1$ can be seen in the table below. Here are listed the numbers of primes $p = 2 \cdot |\mathcal{M}| \cdot N + 1$, $N = 1, \ldots, 500$, for which a factorization $< a, b >= \mathcal{M} \cdot \mathcal{F}$ in $Z_p^*/\{1, -1\}$ with $\mathcal{F} = \{a^i b^j : i - j \equiv 0 \bmod q\}$ exists. Here for $q = r + s + 1 \geq 3$ just the splittings of Z_p by $\mathcal{M} = \{\pm 1, \pm a, \ldots, \pm a^r, \pm b \ldots, \pm b^s\}$ (and especially for $(a, b) = (2, 3)$, $q = 3$ and 4 the perfect 3– and 4–shift codes) are counted.

$\frac{q}{(a,b)}$	2	3	4	5	6	7	8	9	10
(2,3)	48	46	4	23	6	12	1	13	8
(2,5)	50	48	5	22	17	18	1	13	1
(2,7)	46	48	5	23	9	21	1	17	1
(3,4)	3	50	1	28	2	19	1	17	1
(3,5)	41	51	19	32	2	18	11	15	2
(3,7)	44	46	20	29	3	24	9	16	7
(4,5)	4	50	2	31	0	17	0	17	1
(4,7)	3	51	0	28	0	13	0	14	0
(5,7)	43	49	18	19	15	18	9	15	1

Observe that there are usually more splittings when q is odd. However in this case by Theorem 2 splittings by $\mathcal{M}_1$ and $\mathcal{M}_2$ are equivalent. For even q this is not the case and there may also exist primes of the form $p = qn + 1$ yielding a splitting in Z_p by $\mathcal{M}_1$. The following table contains the number of such primes $p = |\mathcal{M}| \cdot N + 1$, $N = 1, \ldots, 1000$, for which a factorization $< a, b >= \mathcal{M} \cdot \mathcal{F}$ in Z_p^* exists. Observe that for $q = r + s + 1 \geq 3$ just the splittings of Z_p by $\mathcal{M} = \{1, a, \ldots, a^r, b \ldots, b^s\}$ are counted. These numbers have been obtained by checking the conditions in Theorem 1 or Corollaries 2 and 3, respectively, for each group Z_p.

$\frac{q}{(a,b)}$	2	3	4	5	6	7	8	9	10
(2,3)	85	46	41	23	35	12	4	13	11
(2,5)	88	48	43	22	28	18	2	13	1
(2,7)	82	48	40	23	18	21	2	17	16
(3,4)	23	50	1	28	17	19	3	17	6
(3,5)	84	51	40	32	34	18	17	15	5
(3,7)	86	46	35	29	31	24	17	16	11
(4,5)	26	50	5	31	8	17	1	17	8
(4,7)	25	51	2	28	6	13	1	14	4
(5,7)	88	49	33	19	27	18	16	15	3

IV. Tilings by the Cross and Semicross and Splittings of Groups of Composite Order

We considered splittings of Abelian groups by the sets $S(k)$ and $F(k)$ in order to analyze perfect shift codes. Such splittings have been studied in literature for another reason. They are closely related to tilings (partitioning into translates of a certain cluster) of the n–dimensional Euclidean space R^n by the (k,n)–cross and the (k,n)–semicross, respectively. A (k,n)–*semicross* is a translate of the cluster consisting of the $kn+1$ unit n – dimensional cubes whose edges are parallel to the coordinate axes and whose centers are the $kn+1$ points specified by the n – tuples

$$(0,0,\ldots,0),(j,0,\ldots,0),(0,j,\ldots,0),\ldots(0,0,\ldots,j)$$

$j=1,2\ldots,k$. Accordingly, a (k,n)–*cross* (or *full cross*) is a translate of the cluster consisting of the $2kn+1$ unit n – dimensional cubes whose edges are parallel to the coordinate axes and whose centers are the $2kn+1$ points specified by the n – tuples (for $j=1,2\ldots,k$)

$$(0,0,\ldots,0),(\pm j,0,\ldots,0),(0,\pm j,\ldots,0),\ldots(0,0,\ldots,\pm j).$$

the $(3,2)$ – semicross the $(1,3)$ – cross

The following results concerning lattice tilings are proved, for instance, in [2]. A lattice tiling is a tiling, where the translates of any fixed point of a cluster (e.g. the center of the cross) form a lattice. A lattice tiling by the cross (semicross) corresponds to a splitting of some Abelian group by the set $F(k)$ ($S(k)$). The analysis can further be reduced to cyclic groups $Z_N = Z/Z_N$.

Fact 1 ([8]): A lattice tiling of the n – dimensional Euclidean space R^n by the (k,n) – semicross (by the (k,n) – cross) exists, if and only if the set $\{1,2,\ldots,k\}$ (the set $\{\pm 1,\pm 2,\ldots,\pm k\}$) splits an Abelian group of order $kn+1$ ($2kn+1$).

Fact 2 ([4]): If $S(k)$ ($F(k)$) splits an Abelian group of order N, then it also splits the cyclic group Z_N of the same order.

It should be mentioned that Fact 2 does not hold for arbitrary sets $\mathcal{M}$. For small parameters $k=3,4$ one can concentrate on cyclic groups Z_p of prime order p. It was shown by Galovich and Stein [9] for $S(3)$ and $S(4)$ and by Munemasa [6] for $F(3)$ and $F(4)$, respectively, that there exists a splitting of Z_N, where N is a composite number, by the set $S(k)$ ($F(k)$) if and only if there exists a splitting of Z_p by $S(k)$ (or $F(k)$, respectively) for every prime factor p of N (with the exception of the primes 2 and 3, which can easily be handled separately). Hence the analysis of splittings by those sets for Abelian groups $\mathcal{G}$, where $|\mathcal{G}|$ is a composite number, can easily be done with the following results.

Fact 3 ([9]): The set $\{1,2,3\}$ splits the finite Abelian group $\mathcal{G}$ if and only if it splits Z_p for every odd prime p dividing $|\mathcal{G}|$ and the 2– Sylow subgroup of $\mathcal{G}$ is either trivial or isomorphic to Z_4.

The set $\{1,2,3,4\}$ splits the finite Abelian group $\mathcal{G}$ if and only if it splits Z_p for every odd prime $p\neq 3$ dividing $|\mathcal{G}|$ and the 3– Sylow subgroup of $\mathcal{G}$ is either trivial or isomorphic to Z_9.

Fact 4 ([6]): For $k = 1, 2$, and 3 the set $F(k) = \{\pm 1, \pm 2, \dots, \pm k\}$ splits the finite Abelian group $\mathcal{G}$ if and only if it splits Z_p for every prime p dividing $|\mathcal{G}|$.
The set $\{\pm 1, \pm 2, \pm 3, \pm 4\}$ splits the finite Abelian group $\mathcal{G}$ if and only if it splits Z_p for every odd prime $p \neq 3$ dividing $|\mathcal{G}|$ and the 3– Sylow subgroup of $\mathcal{G}$ is either trivial or isomorphic to Z_9.
The trivial splittings $(\{1, 2, 3\}, \{1\})$ in Z_4 and $(\{1, 2, 3, 4\}, \{1, -1\})$ and $(\{\pm 1, \pm 2, \pm 3, \pm 4\}, \{1\})$ are responsible for the exceptional behaviour of the primes 2 and 3.
Results similar to Facts 3 and 4 are derived for $S(5)$ and $S(6)$ in [1]. More results on splitting of Abelian groups and further conditions under which a splitting by $S(k)$ or $F(k)$ exists are presented e. g. in [1] or [2].

V. Concluding Remarks

Stein in [10] used results on Newton sums (for the set $\mathcal{M}$ the j–th Newton sum is $\sum_{m \in \mathcal{M}} m^j$) in order to compute all splittings of Z_p, p prime, by sets $S(k)$ for $k = 5, \dots, 12$ up to quite large prime numbers. The smallest primes p for which a splitting of Z_p by $S(k)$ (besides the trivial splittings with splitting set $\{1\}$ or $\{1, -1\}$) exists are

k	5	6	7	8	9	10	11	12
p	421	103	659	3617	27127	3181	56431	21061

It is easy to see that, if there is no splitting by $S(k)$, then there also does not exist a splitting by $F(k)$ and hence no perfect k – shift code. Hence Stein's results also suggest that perfect shift codes seem to be quite sparsely distributed for $k > 3$ (for $k = 4$ cf. Section III). Especially, for the application in run–length limited coding, groups of small order, in which a perfect shift code exists, are of interest. The reason is that simultaneously $|\mathcal{G}|$ perfect run – length limited codes correcting single peak shifts are obtained (one for each $g \in \mathcal{G}$) by the construction

$$\mathcal{C}(g) = \{(x_1, \dots, x_n) : \sum_{i=1}^{n} f(i) \cdot x_i = g\}, \tag{10}$$

where x_i is the length of the i–th run (the number of consecutive 0's between the $(i-1)$–th and the i–th 1) and the $f(i)$'s are obtained from the members of a perfect shift code $\mathcal{S} = \{h_1, \dots, h_n\}$ by $f(n) = h_n$, $f(i) - f(i+1) = h_i$ for $i = 1, \dots, n-1$. Observe that the same shift code may yield several perfect run – length limited codes depending on the order of the h_i's. This is intensively discussed in [5].
So the size of the best such code will be about $\frac{1}{|\mathcal{G}|}$ times the number of all possible codes $(x_1, \dots, x_n)$ with n peaks (= ones). The above table suggests that for $k \geq 4$ groups in which a splitting by $F(k)$ exists are hard to find. One might relax the conditions and no longer require perfectness but a good packing, cf. also [5]. Packings of R^n by the cross or the semicross have been considered e.g in [14], [15], [16], and [17].

Tilings of metric spaces are intimately related to perfect codes. For recent results on binary perfect codes and tilings of binary spaces see e.g. [18], [19], and [20]. From tilings of the Euclidean space R^n by the $(1, n)$–cross one can obtain perfect nonbinary single – error correcting codes in the Lee - metric, since the sphere around the codeword of such a code in the Lee metric corresponds to a full $(1, n)$–cross. Whereas Fact 1 just guarantees the existence of a tiling, Golomb and Welch [21] could demonstrate by the construction (10) (where now the x_i's are the components of a codeword $(x_1, \dots, x_n)$ and $f(i) = i$ for all $i = 1, \dots n$) that the $(1, n)$–cross always tiles R^n, from which they could derive perfect single–error correcting codes in the Lee metric.
The Lee metric is a special case of an error measure for codes over an alphabet $\{0, \dots, q-1\}, q \geq 3$ for which a single error distorting cordinate x_i in a codeword $(x_1, \dots, x_n)$ results in one of the

letters $x_i + j \bmod q, j \in \{1, \ldots, k\}$ (the Lee metric arises for $k = 1$). Relations between such nonbinary single–error correcting codes and splittings of groups can already be found in [22] (cf. also [2], p. 80).

Martirosyan [23] considers the case $k = 2$, which is closely related to perfect 2–shift codes. Again in [23] the construction (10) is used by choosing the $f(i)$'s appropriately. Construction (10) had been introduced by Varshamov/Tenengolts [24] for $\mathcal{G} = Z_n$ and extended by Levenshtein [25] (in a more general setting) and Constantin/Rao [26] for arbitrary Abelian groups (cf. also [27]). Martirosyan [23] also derives a formula for the size of the set $\mathcal{C}(g)$.

Perfect 2–shift codes or splittings by the set $\{\pm 1, \pm 2\}$ have been studied e. g. in [5] and [8]. The (necessary and sufficient) conditions on the prime p for the existence of such a 2–shift code in the group Z_p is that the element 2 has order divisible by 4 in Z_p^*. In [23] it is further analyzed for which primes this condition is fulfilled. Especially, this holds for primes of the form $p \equiv 5 \bmod 8$, hence there are infinitely many perfect 2–shift codes.

The semicross and the cross are special polyominoes as studied by Golomb in [28], e. g., a right trominoe just corresponds to the $(1, 2)$ – semicross. As a further application in Information Theory, tilings of a bounded region by the cross and similar clusters have also been considered in [29] and [30] in the study of memory with defects.

Acknowledgments

The author wishes to thank Han Vinck for drawing his attention to [5], the anonymous referees for very helpful comments, and Torsten Sillke for pointing out [17].

References

[1] S. Stein, "Tiling, packing, and covering by clusters", *Rocky Mountain J. Math.*, vol. 16, 277 -321, 1986.

[2] S. Stein and S. Szabo, *Algebra and Tiling*, The Carus Mathematical Monographs 25, The Mathematical Association of America, 1994.

[3] S. Stein, "Algebraic tiling", *Amer. Math. Monthly*, vol. 81, pp. 445 – 462, 1974.

[4] D. Hickerson, "Splittings of finite groups", *Pacific J. Math.*, vol. 107, pp. 141 – 171, 1983.

[5] V. I. Levenshtein and A. J. Han Vinck, "Perfect (d,k)–codes capable of correcting single peak shifts", *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 656–662, 1993.

[6] A. Munemasa, "On perfect t–shift codes in Abelian groups", *Designs, Codes, and Cryptography*, vol. 5, pp. 253 – 259, 1995.

[7] S. Golomb, "A general formulation of error metrics", *IEEE Trans. Inform. Theory*, vol. 15, pp. 425 – 426, 1969.

[8] S. Stein, "Factoring by subsets", *Pacific J. Math.*, vol. 22, no. 3, pp. 523 – 541, 1967.

[9] S. Galovich and S. Stein, "Splittings of Abelian groups by integers", *Aequationes Mathematicae*, vol. 22, pp. 249 – 267, 1981.

[10] S. Stein, "Splitting groups of prime order", *Aequationes Mathematicae*, vol. 33, pp. 62 – 71, 1987.

[11] S. Saidi, "Semicrosses and quadratic forms", *European J. Combinatorics*, vol. 16, pp. 191 – 196, 1995.

[12] H. Weber, "Beweis des Satzes, daß jede eigentlich primitive quadratische Form unendlich viele prime Zahlen darzustellen fähig ist", *Math. Ann.*, vol. 20, 301 – 329, 1882.

[13] U. Tamm, "On perfect 3–shift N–designs", *Proceedings of 1997 IEEE Symposium on Information Theory*, Ulm, p. 454, 1997.

[14] S. Stein, "Packing of R^n by certain error spheres", *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 356 – 363, 1984.

[15] W. Hamaker and S. Stein, "Combinatorial packing of R^3 by certain error spheres", *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 364 – 368, 1984.

[16] D. Hickerson and S. Stein, "Abelian groups and packing by semicrosses", Pacific J. Math., vol 122, no. 1, pp. 95 – 109, 1986.

[17] S. Stein, "Packing tripods", *Math. Intelligencer*, vol. 17, no. 2, pp. 37 – 39, 1995.

[18] T. Etzion and A. Vardy, "Perfect codes: constructions, properties, and enumeration", *IEEE Trans. Inform. Theory*, vol. 40, no. 3, pp. 754–763, 1994.

[19] G. D. Cohen, S. Litsyn, A. Vardy, and G. Zemor, "Tilings of binary spaces", *SIAM J. Discrete Math.*, vol. 9, pp. 393–412, 1996.

[20] T. Etzion and A. Vardy, "On perfect codes and tilings: problems and solutions", *Proceedings of 1997 IEEE Symposium on Information Theory*, Ulm, p. 450, 1997.

[21] S. W. Golomb and L. R. Welch, "Algebraic coding and the Lee metric", *Error Correcting Codes (H. B. Mann ed.)*, pp. 175 – 194, 1968.

[22] W. Ulrich, "Non–binary error correction codes", *The Bell System Technical Journal*, pp. 1341 – 1388, 1957.

[23] S. Martirosyan, "Single – error correcting close packed and perfect codes", *Proceedings of 1st INTAS International Seminar on Coding Theory and Combinatorics*, Thahkadzor, Armenia, pp. 90 – 115, 1996.

[24] R. R. Varshamov and G. M. Tenengolts, "One asymmetric error correcting codes", (in Russian), *Avtomatika i Telemechanika*, vol. 26, no. 2, pp. 288 – 292, 1965.

[25] V. Levenshtein, "Binary codes with correction for deletions and insertions of the symbol 1", (in Russian), *Problemy Peredachi Informacii*, vol. 1, pp. 12 – 25, 1965.

[26] S. D. Constantin and T. R. N. Rao, "On the theory of binary asymmetric error correcting codes", *Information and Control*, vol. 40, pp. 20 – 26, 1979.

[27] K. A. S. Abdel Ghaffar and H. C. Ferreira, "On the maximum number of systematically – encoded information bits in the Varshamov – Tenengolts codes and the Constantin – Rao codes", *Proceedings of 1997 IEEE Symposium on Information Theory*, Ulm, p. 455, 1997.

[28] S. Golomb, *Polyominoes*, Princeton University Press, 2nd ed., 1994.

[29] E. E. Belitskaja, V. R. Sidorenko, and P. Stenström, "Testing of memory with defects of fixed configurations", *Proceedings of 2nd International Workshop on Algebraic and Combinatorial Coding Theory*, Leningrad, pp. 24 – 28, 1990.

[30] V. Sidorenko, "Tilings of the plane and codes for translational metrics", *Proceedings of 1994 IEEE Symposium on Information Theory*, Trondheim, p. 107, 1994.