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 $\mathcal{M} = \{\pm 1, \ldots, \pm k\}$ 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 $\mathcal{M} = \{1, a, \ldots, a^r, b, \ldots, b^s\}$ and $\mathcal{M} = \{\pm 1, \pm a, \ldots, \pm a^r, \pm b, \ldots, \pm b^s\}$. 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 $m = 1, \ldots, k$ 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 $m \in \{1, \ldots, k\}$ 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

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

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 $\{\pm h, \pm 2h, \ldots, \pm kh\}$ 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

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

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 $i - j \equiv 0$ mod $(r + s + 1)$. 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

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