MATHEMATICAL COMMUNICATIONS
Math. Commun. **20**(2015), 23–35

On perfect 1-$\mathcal{E}$-error-correcting codes*

Olof Heden[1,†] and Murat Güzeltepe[2]

[1] *Department of Mathematics, KTH, S-10 044 Stockholm, Sweden*
[2] *Department of Mathematics, Sakarya University, TR–54 187 Sakarya, Turkey*

Received June 19, 2014; accepted October 29, 2014

Abstract. We generalize the concept of perfect Lee-error-correcting codes, and present constructions of this new class of perfect codes that are called perfect 1-$\mathcal{E}$-error-correcting codes. We also show that in some cases such codes contain quite a few perfect 1-error-correcting q-ary Hamming codes as subsets.
AMS subject classifications: 94B60
Key words: perfect codes

1. Introduction

The first perfect 1-error-correcting codes were constructed by Hamming [8]. They were binary and, as being null-spaces of matrices $\mathbf{H}$, subspaces of vector spaces Z_2^n of dimension n over the finite field with two elements. Hamming's construction was generalized to perfect codes over alphabets of any size equal to a power of a prime number (see Section 6). In that case, the errors also appear in coordinate positions, and any word can be uniquely corrected to a word in the perfect code C by changing at most one coordinate position. More precisely: *Let $S = \mathrm{GF}(q)^n$ be the direct product of n copies of the finite field $\mathrm{GF}(q)$ with q elements. A subset C of S is a perfect 1-error-correcting code in the Hamming metric if to every word $\bar{x} = (x_1, \ldots, x_n)$ in S there is a unique word $\bar{e} = (0, \ldots, 0, \epsilon_i, 0, \ldots, 0)$ of weight one and with $\epsilon_i \in \mathrm{GF}(q)$ such that*

$$\bar{x} + \bar{e} \in C.$$

There are important, useful, and well-known generalizations of the error-correcting model introduced by Hamming to the cases when the error e_i belongs to a subset $\mathcal{E}$ of the alphabet used to form the codewords. A well-studied example is when the alphabet is the ring $\mathbb{Z}_n$ and $\mathcal{E} = \{1, -1\}$. Such codes are recognized as *perfect 1-error-correcting codes in the Lee metric* [17]. They are important for many reasons, such as serving as models for codes correcting synchronization errors, to use phaseshift keying (PSK) modulation, see e.g. [23, pp. 298 – 333] or [20], and getting nice so called tilings of the real n-dimensional space R^n, see e.g. [6]. In the most general case, when $\mathcal{E}$ can be any given subset of the alphabet in use, we call this kind of codes *perfect 1-$\mathcal{E}$-error-correcting codes*. Fan and Gao gave a construction

*The work of the second author was supported by Sakarya University Research funds as a Research Project with project number 2013-02-00-002.
†Corresponding author. *Email addresses:* olohed@math.kth.se (O. Heden), mguzeltepe@sakarya.edu.tr (M. Güzeltepe)

of a certain class of perfect 1-$\mathcal{E}$-error-correcting codes. They proved the following theorem in Section D of [5].

Theorem 1. *To every subgroup $\mathcal{E}$ of the multiplicative group $\mathrm{GF}(q)^\star$ of a finite field $\mathrm{GF}(q)$ with q elements, there is a perfect 1-$\mathcal{E}$-error-correcting code C over the alphabet $\mathrm{GF}(q)$. The code C has length $n = (q-1)/|\mathcal{E}|$ and is linear of dimension $n-1$ over $\mathrm{GF}(q)$.*

Simply, Fan and Gao define the code C to be the null-space of a matrix

$$\mathbf{H} = \left(d_1 \; d_2 \; \cdots \; d_t \right), \tag{1}$$

where d_1, d_2, ..., d_t are coset representatives to $\mathcal{E}$ in the multiplicative group of $\mathrm{GF}(q)$.

In Section 2, we present a general result, which gives necessary and sufficient conditions for a construction similar to that of Fan and Gao, to result in a perfect code. In that section, we also present perfect codes, such that both the error set $\mathcal{E}$ and the alphabets can differ in distinct coordinate positions. We call these codes *perfect 1-$\overline{\mathcal{E}}$-error correcting codes.*

In Section 3, we show how perfect 1-$\mathcal{E}$-error-correcting codes can be combined to obtain new 1-$\mathcal{E}$-error-correcting codes, both linear and non-linear. Thereby, perfect codes in the Hamming metric are used to describe the combining process. In Section 4, we generalize Theorem 1 by showing how to construct 1-$\mathcal{E}$-error-correcting codes of length $n(k)$ and dimension $n(k)-k$, for any positive integer k. Finally, in Section 5, we show that if $t = \log_p(|\mathcal{E}|+1)$ divides $\log_p(q)$, then there are linear 1-$\mathcal{E}$-error-correcting codes C of length n and dimension $n-1$ that contain $n!$ distinct Hamming codes of length n over $\mathrm{GF}(p^t)$.

2. Basic definitions and results

The original purpose of this study was to investigate how far the construction of Fan and Gao could be strengthened. Therefore, let us begin with the following observation:

Assume that we consider words in some kind of algebraic context, and assume that the error-correcting code C is the null-space of a matrix $\mathbf{H}$ on the form (1). For using the technique with syndromes when correcting errors occurring during transmissions of codewords, it is necessary that the distributive rule holds. That is,

$$\mathbf{H}\bar{x}^T = \mathbf{H}(\bar{c}^T + \bar{\epsilon}^T) = \mathbf{H}\bar{c}^T + \mathbf{H}\bar{\epsilon}^T = \mathbf{H}\bar{\epsilon}^T \,. \tag{2}$$

Here, $\bar{c}$ is the codeword, $\bar{\epsilon}$ is an error vector, $\bar{x}$ is the received word, and $\mathbf{H}\bar{x}^T$ is the *syndrome* of the word $\bar{x}$. The received word $\bar{x} = \bar{c} + \bar{\epsilon}$ is corrected to the sent codeword $\bar{x} - \bar{\epsilon}$.

Consequently, if we consider words in a direct product $S = G_1 \times G_2 \times \cdots \times G_n$ of alphabets G_i, for $i \in [n]$, and codes as null-spaces of a matrix $\mathbf{H}$ on the form (1), and an error-correcting procedure using syndromes, then, presuming some algebraic structure, it is necessary that the following two conditions are satisfied:

(i) the alphabets G_i, for $i \in [n]$, are subgroups of an Abelian group G,

(ii) for each $i \in [n]$, the subgroup G_i is a left module over a ring R_i such that the matrix entry d_i of $\mathbf{H}$ belongs to R_i.

Thus, in this note, we will always assume that a *code* is a subset C of a direct product $S = G_1 \times \cdots \times G_n$ of a family of n finite left modules G_i, for $i \in [n]$, over rings R_i. We also assume that these modules G_i are subgroups of the same Abelian group G.

By $\bar{e}_{i,\epsilon}$ we denote the word that has weight one with its only non-zero entry $\epsilon_i \in G_i$ in position i. If, for $i \in [n]$ $\mathcal{E}_i$, is a subset of the module G_i, then by $\overline{\mathcal{E}}$ we denote the set

$$\overline{\mathcal{E}} = \{\bar{e}_{i,\epsilon} \mid i \in [n], \ \ \epsilon \in \mathcal{E}_i\}. \tag{3}$$

A code C is a *perfect 1-$\overline{\mathcal{E}}$-error-correcting code in S* if to every word $\bar{x} \in S \setminus C$ there is a unique codeword $\bar{c} \in C$ such that

$$\bar{x} = \bar{c} + \bar{e}_{i,\epsilon}\,,$$

for a unique coordinate position $i \in [n]$ and a unique $\epsilon \in \mathcal{E}_i$. We denote and define an *$\overline{\mathcal{E}}$-sphere* centered at a word $\bar{c}$ by

$$\mathrm{S}_{\overline{\mathcal{E}}}(\bar{c}) = \{\bar{c} + \bar{e}_{i,\epsilon} \mid i \in [n], \ \epsilon \in \mathcal{E}_i\}.$$

The next proposition is an immediate consequence of the definitions above.

Proposition 1. *If C is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code in the direct product $G_1 \times \cdots \times G_n$ of Abelian groups, then every code in the family of codes*

$$\mathcal{F} = \{C + \bar{e}_{i,\epsilon} \mid i \in [n], \ \epsilon \in \mathcal{E}_i\} \cup \{C\}$$

is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code. The codes in $\mathcal{F}$ are pairwise disjoint and

$$\bigcup_{C \in \mathcal{F}} C = G_1 \times \cdots \times G_n.$$

We say that the codes in $\mathcal{F}$ constitute *a perfect partition or a tiling of $G_1 \times \cdots \times G_n$ into 1-$\overline{\mathcal{E}}$-error-correcting codes*. Such partitions are one of the main ingredients in the combining construction of perfect 1-$\overline{\mathcal{E}}$-error-correcting codes given in the next section.

The *sum* of a family of subgroups G_i, $i \in [n]$, of an Abelian group G is defined here and denoted as follows:

$$G_1 + G_2 + \cdots + G_n = \{g_1 + g_2 + \cdots + g_n \in G \mid g_i \in G_i, \ i \in [n]\}.$$

Now we are ready to state the main theorem of this section the proof of which consists of trivial verifications.

Theorem 2. *Assume that the groups G_i, for $i \in [n]$, are subgroups of the same Abelian group G. For $i \in [n]$, let $\mathcal{E}_i$ be any subset of G_i and let φ_i be any automorphism of G_i. Define the code C in the direct product $S = G_1 \times G_2 \times \cdots \times G_n$ to be the set*

$$C = \{(x_1, \ldots, x_n) \in S \mid \varphi_1(x_1) + \cdots + \varphi_n(x_n) = 0\}.$$

Then C is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code in S if and only if the following two conditions are satisfied:

$$\{0\} \cup \varphi_1(\mathcal{E}_1) \cup \ldots \cup \varphi_n(\mathcal{E}_n) = G_1 + G_2 + \cdots + G_n, \tag{4}$$

$$i \neq j \quad \Longrightarrow \quad \varphi_i(\mathcal{E}_i) \cap \varphi_j(\mathcal{E}_j) = \emptyset. \tag{5}$$

The code C is a subgroup of S.

The theorem above generalizes a construction of perfect codes given by Herzog and Schönheim [15]. They considered partitions of the set of non-zero elements of Abelian groups G into the set of non-zero elements of a family of subgroups G_i, $i \in [n]$, of G:

$$G = G_1 \cup G_2 \cup \ldots \cup G_n, \quad \text{with} \quad G_i \cap G_j = \{0\} \quad \text{if} \quad i \neq j.$$

Simply, if in Theorem 2, for $i \in [n]$, we let φ_i be the identity map and $\mathcal{E}_i = G_i \setminus \{0\}$, then we get the construction of Herzog and Schönheim. Their construction is a generalization of the construction of Hamming [8]. For details, see Section 2.1.

In our constructions of perfect codes below, we mainly use the following corollary of Theorem 2.

Theorem 3. *Assume that, for $i \in [n]$, each of the subgroups G_i of the Abelian group G is a left module over a ring R_i. Let $\mathbf{H} = \begin{pmatrix} d_1 & \cdots & d_n \end{pmatrix}$, where the entries d_i, for $i \in [n]$, belong to R_i. Let C consist of the elements $\bar{x} = (x_1, \ldots, x_n)$ in the direct product $S = G_1 \times \cdots \times G_n$ such that*

$$\mathbf{H}\bar{x}^T = \bar{0}^T,$$

that is, C is the null-space in S of $\mathbf{H}$. Let $\overline{\mathcal{E}}$ be defined as in (3).

Then, C is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code if and only if the following three conditions are satisfied:

$$\{0\} \cup d_1\mathcal{E}_1 \cup \ldots \cup d_n\mathcal{E}_n = \{\mathbf{H}\bar{x}^T \mid \bar{x} \in S\}, \tag{6}$$

$$i \neq j \quad \Longrightarrow \quad d_i\mathcal{E}_i \cap d_j\mathcal{E}_j = \emptyset, \tag{7}$$

$$|d_i\mathcal{E}_i| = |\mathcal{E}_i| \qquad i = 1, 2, \ldots, n. \tag{8}$$

The size of C is

$$|C| = \frac{|G_1| \cdot \cdots \cdot |G_n|}{1 + |\mathcal{E}_1| + \cdots + |\mathcal{E}_n|}.$$

The code C is a subgroup of the group S. If the rings R_i, for $i \in [n]$, are the same commutative ring R, then C is also a left module over R.

The theorem above follows from Theorem 2, as for each d_i, $i \in [n]$, the map

$$\varphi_i : x_i \quad \mapsto \quad d_i x_i, \qquad i = 1, 2, \ldots, n,$$

is a homomorphism of the left module G_i over the ring R_i.

The next example shows how we can use Theorem 3 to construct perfect 1-$\mathcal{E}$-error-correcting codes over mixed alphabets and with mixed error sets.

Example 1. *Let F be any finite field and let F_1 and F_2 be two distinct non-trivial subfields of F. Assume that $F_2 \subseteq F_1$, and let $\mathcal{E}_2$ denote the multiplicative group of F_2. Let $\mathcal{E}_1$ be any subgroup of the multiplicative group of F_1 such that $\mathcal{E}_1$ contains $\mathcal{E}_2$. Let $\mathcal{E}_3$ be any subgroup of $\mathcal{E}_2$.*

Then

$$F = \{0\} \cup d_1\mathcal{E}_1 \cup \ldots \cup d_t\mathcal{E}_1, \qquad \mathcal{E}_1 = f_1\mathcal{E}_2 \cup \ldots \cup f_s\mathcal{E}_2, \qquad \mathcal{E}_2 = g_1\mathcal{E}_3 \cup \ldots \cup g_r\mathcal{E}_3$$

for families of coset representatives $d_i \in F$, for $i \in [t]$, $f_i \in F_1$, for $i \in [s]$, and $g_i \in F_2$, for $i \in [r]$, where $t = (|F| - 1)/|\mathcal{E}_1|$, $s = |\mathcal{E}_1|/|\mathcal{E}_2|$ and $r = |\mathcal{E}_2|/|\mathcal{E}_3|$. We can split each coset $d_i\mathcal{E}_1$ into cosets of $\mathcal{E}_2$ and each coset $f_i\mathcal{E}_2$ into cosets of $\mathcal{E}_3$. For example: if $d_1\mathcal{E}_1 = \mathcal{E}_1$ and $f_1\mathcal{E}_2 = \mathcal{E}_2$, then we get the following partition of the non-zero elements of F:

$$F \setminus \{0\} = g_1\mathcal{E}_3 \cup \ldots \cup g_r\mathcal{E}_3 \cup f_2\mathcal{E}_2 \cup \ldots \cup f_s\mathcal{E}_2 \cup d_2\mathcal{E}_1 \cup \ldots \cup d_t\mathcal{E}_1. \tag{9}$$

Thus we have many possibilities to construct perfect 1-$\overline{\mathcal{E}}$-error-correcting codes. For example, using the split of $F \setminus \{0\}$ in (9) we get a perfect 1-$\overline{\mathcal{E}}$-error-correcting code C in the direct product $S = F_2^r \times F_1^{s-1} \times F^{t-1}$, by letting C be the null-space of the matrix

$$\mathbf{H} = \begin{pmatrix} g_1 & \cdots & g_r & f_2 & \cdots & f_s & d_2 & \cdots & d_t \end{pmatrix}.$$

As F, F_1 and F_2 are fields, the necessary conditions of Theorem 3 are satisfied. Hence, C is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code.

In most cases of applications, in Theorem 3 we can assume that $R_i = R$, for $i \in [n]$. For the reader's convenience and for the future need of references we state the theorem in that case:

Theorem 4. *Let R be a finite ring. Assume that $\mathcal{E}$ is a subset of R and that d_1, d_2, ..., d_n are elements in R such that*

$$R = \{0\} \cup d_1\mathcal{E} \cup \ldots \cup d_n\mathcal{E}, \tag{10}$$

$$i \neq j \qquad \Longrightarrow \qquad d_i\mathcal{E} \cap d_j\mathcal{E} = \emptyset, \tag{11}$$

and

$$|\mathcal{E}| = |d_2\mathcal{E}| = |d_3\mathcal{E}| = \cdots = |d_n\mathcal{E}|. \tag{12}$$

Then the null-space C of the $1 \times n$-matrix

$$\mathbf{H} = \begin{pmatrix} d_1 & d_2 & \cdots & d_n \end{pmatrix}, \tag{13}$$

is a perfect 1-$\mathcal{E}$-error-correcting code in the direct product R^n. The size of C is $|C| = |R|^{n-1}$.

We note that if each of the elements d_i, for $i \in [n]$, commutes with every element in R, then the code C in the theorem is a left ideal in the ring R^n. The code C is always a right ideal in R^n.

In a special case, the construction above coincides with the construction provided by Fan and Gao, see the next example.

Example 2 (Fan and Gao, [5]). *Let $\mathcal{E}$ be any subgroup of the multiplicative group G of the finite field $\mathrm{GF}(q)$, and let d_1, d_2,..., d_n, where $n = |G|/|\mathcal{E}|$, be any family of coset representatives to $\mathcal{E}$ in G. Then we can apply Theorem 4, as (10), (11) and (12) hold.*

The multiplicative group of a finite field with q elements is cyclic, and, for every divisor h of $q-1$, it has a unique subgroup H of size h, see e.g. [16]. Every such subgroup H is also cyclic. Thus we may use Theorem 4 to construct many perfect 1-$\mathcal{E}$-error-correcting codes. They are linear codes of dimension $n-1$ and length n, where $n = (q-1)/h$.

If $h = 2$, then the subgroup $\mathcal{E}$ consists of the elements $\{1, -1\}$, and the code constructed in this way is a perfect 1-error-correcting code in the Lee metric.

Note that we can change the roles of the error set $\mathcal{E}$ and its coset representatives, as shown in the next example.

Example 3. *The multiplicative group of the finite field $\mathbb{Z}_{13}$ has the non-trivial subgroups $H_2 = \{1, -1\}$, $H_3 = \{1, 3, 9\}$, $H_4 = \{1, 5, 8, -1\}$ and $H_6 = \{1, 4, 3, -1, 9, 10\}$. As for instance,*

$$\mathbb{Z}_{13} \setminus \{0\} = H_6 \cup 2H_6, \qquad \text{and} \qquad H_6 \cap 2H_6 = \emptyset,$$

we get that with $\mathcal{E} = \{1, 2\}$ and $\{d_i \mid i \in [6]\} = H_6$, the conditions in (10), (11) and (12) are fulfilled. Hence, by Theorem 4 there is a perfect 1-$\{1, 2\}$-error-correcting code in $\mathbb{Z}_{13}^6$.

If we use H_2 instead, we get a perfect 1-$\{1, 2, 3, 4, 5, 6\}$-error-correcting code in $\mathbb{Z}_{13}^2$ consisting of the words (a, a), for $a \in \mathbb{Z}_{13}$.

2.1. Mixed perfect codes and vector space partitions

A *subspace partition* of the finite vector space $V(n, q)$ of dimension n over the finite field $\mathrm{GF}(q)$ is a collection of subspaces U_1, U_2, ..., U_t satisfying the two conditions

$$V(n, q) = \bigcup_{i=1}^{t} U_i \qquad \text{and} \qquad U_i \cap U_j = \{\bar{0}\}, \quad \text{if } i \neq j. \tag{14}$$

Herzog and Schönheim [15] observed that the kernel of the map f

$$f : (u_1, u_2, \ldots, u_t) \quad \mapsto \quad u_1 + u_2 + \cdots + u_t \tag{15}$$

from the direct product $S = U_1 \times U_2 \times \cdots \times U_t$ to $V(n, q)$, is a perfect 1-error-correcting code in S equipped with the Hamming metric. If the dimensions of the subspaces U_i, $i \in [n]$, are not equal, then this kind of codes is called *mixed*

perfect 1-error-correcting codes. Such codes are used in some of the examples below in order to demonstrate the combining construction of perfect 1-$\mathcal{E}$-error-correcting codes described in the next section.

In just a very limited number of vector spaces $V = V(n,q)$, it is completely clarified which possibilities there are for the dimensions that appear in a subspace partition of V. For a survey of the known results in this area, see [13].

3. Combining codes

We consider a direct product $S = S_1 \times \cdots \times S_t$ of direct products $S_i = R_{i,1} \times \cdots \times R_{i,t_i}$, where $R_{i,j}$, for $j \in [t_i]$ and $i \in [t]$, are Abelian groups. We assume that the error sets $\mathcal{E}_i$, for $i \in [t]$, are subsets of R_{i_j}, for $j \in [t_i]$.

The construction below has been presented for special cases partly independently by several authors, like Zinoviev [30], Solov'eva [27] and Etzion [4].[§]

There are two fundamental ingredients in this construction of perfect 1-$\overline{\mathcal{E}}$-error-correcting codes. One is a family of partitions of the direct products S_i, for each $i \in [t]$, into perfect 1-$\mathcal{E}_i$-error-correcting codes $C(i,\mu)$, for $\mu = 0, 1, \ldots, p_i - 1$, where

$$p_i = \frac{|S_i|}{|C(i,\mu)|} = 1 + t_i|\mathcal{E}_i|.$$

As the other ingredient we can take any (mixed) perfect 1-error-correcting code M in the direct product

$$\mathcal{A}_1 \times \cdots \times \mathcal{A}_t$$

equipped with the Hamming metric, where $|\mathcal{A}_i| = p_i$, for $i \in [t]$.

With the notation as above, we have the following theorem:

Theorem 5. *The following union of codes*

$$C = \bigcup_{(d_1 \ldots, d_t) \in M} \{(\bar{c}_1|\bar{c}_2|\ldots|\bar{c}_t) \mid \bar{c}_i \in C(i,d_i) \ \textit{for} \ i \in [t]\},$$

is a perfect 1-$\overline{\mathcal{E}}$-error-correcting code in the direct product S.

Proof. Consider any word $\bar{x} = (\bar{x}_1|\bar{x}_2|\ldots|\bar{x}_t)$ of S. Then there are elements $d_i \in \mathcal{A}_i$, for $i \in [t]$, such that

$$\bar{x}_i \in C(i,d_i).$$

If $\bar{d} = (d_1, d_2, \ldots, d_t)$ belongs to M, then $\bar{x}$ belongs to C. Else, $\bar{d}$ differs in a unique coordinate position from one and only one word in M. Let i denote that position, and assume that $(d_1, \ldots, d_{i-1}, d_i', d_{i+1} \ldots, d_t)$ belongs to M. Then for a unique word $\bar{x}_i' \in C(i,d_i')$,

$$\bar{x}_i = \bar{x}_i' + \bar{e}_{j,\epsilon}\,,$$

where $j \in [t_i]$ and $\epsilon \in \mathcal{E}_i$, and where $\bar{e}_{j,\epsilon}$ is defined as in the previous section. Hence, every word in $S \setminus C$ belongs to at least one $\overline{\mathcal{E}}$-sphere centered at a word of C.

[§]The authors rediscovered this construction inspired by the construction in [10]. There, the first known variant of this construction appears, although in a very special case.

Simple counting arguments show that

$$|C| + \sum_{\bar{c} \in C} |S_{\overline{\mathcal{E}}}(\bar{c})| = |S|.$$

Hence, two $\overline{\mathcal{E}}$-spheres centered at codewords cannot intersect, as otherwise there would exist a word of $S \setminus C$ not belonging to an $\overline{\mathcal{E}}$-sphere centered at a word of C.

The conclusion is that C must be a perfect 1-$\overline{\mathcal{E}}$-error-correcting code. □

The construction described above is called the *combining construction*. The perfect code M is said to be the *outer code* in this construction.

3.1. Non-linear perfect 1-$\mathcal{E}$-error-correcting codes

Shapiro and Slotnic [25] conjectured that every perfect code in the Hamming metric is linear. A few years later, the first non-linear perfect code in the Hamming metric was found by Vasil'ev [29]. By using the combining construction, we are now able to construct non-linear perfect 1-$\mathcal{E}$-error-correcting codes. In fact, the original purpose of the combining construction was to produce non-linear perfect 1-error-correcting codes in the Hamming metric.

By taking a non-linear perfect 1-error-correcting code in the Hamming metric as the outer code M, we almost always get a non-linear perfect 1-$\mathcal{E}$-error-correcting code. (There are quite a few non-linear perfect 1-error-correcting codes in the Hamming metric, see the references in Section 6.)

Now consider the situation when all rings $R_{i,j}$ are equal to the same ring R, the error sets $\mathcal{E}_i$ can be distinct in distinct coordinate positions. Then $p_{i,j} = q = |R|$, for all $i \in [t]$ and $j \in [t_i]$. For $i \in [t]$, the components $C(i, \mu)$ in the partition of S_i are the sets

$$C(i, \mu) = \{\bar{x} \in R^{t_i} \mid \mathbf{H}\bar{x}^T = \mu\},$$

for $\mu \in R$ and some $1 \times t_i$-matrix $\mathbf{H} = \begin{pmatrix} d_{i_1} & \cdots & d_{i_{t_i}} \end{pmatrix}$. Then

$$C(i, \mu) + C(i, \mu') = C(i, \mu + \mu').$$

Consequently, if the outer code M is linear, the obtained code is linear.

There are many ways to destroy this linearity. For instance, we can choose the outer code M to be non-linear. Another possibility is to make some permutation of the components $C(i, \mu)$. The easiest way to obtain a non-linear code might be to switch in S_1 to a "new" partition into perfect 1-$\mathcal{E}$-error-correcting codes:

$$\mathcal{F}' = \{C(1, \mu)' \mid \mu \in R\},$$

where, for $\mu \in R$,

$$C(1, \mu)' = C(1, \pi(\mu)),$$

for some permutation π of the elements of R such that $\pi(0) = 0$.

3.2. Some examples

We give three examples that show the applicability of the combining construction.

Example 4. *(Mixed perfect 1-error-correcting codes in the Lee-metric) Let* $\mathcal{E} = \{1, -1\}$*, and let* $R = \mathbb{Z}_{25}$*. Then the conditions of Theorem 4 are satisfied with* $d_i = i$*, for* $i \in [12]$*, as well as in the case* $R = \mathbb{Z}_5$ *with* $d_1 = 1$ *and* $d_2 = 2$*. Thus there are perfect 1-error-correcting codes in* $\mathbb{Z}_{25}^{12}$ *and* $\mathbb{Z}_5^2$*, respectively, equipped with the Lee metric.*

From a construction of Herzog and Schönheim [15], and independently Beutelspacher [2] and Bu [3], we know that the vector space $V(3, 5)$ *of dimension 3 over the finite field with five elements admits a subspace partition into one subspace of dimension 2 and 25 subspaces of dimension 1. From Section 2.1, we thus get that there is a mixed perfect 1-error-correcting code* M *in the direct product* $\mathrm{GF}(25) \times \mathrm{GF}(5)^{25}$*.*

By combining Proposition 1 and Theorem 5, whereby we use the code M *as the outer code, we obtain a perfect 1-error-correcting mixed code* C *in the direct product*

$$\mathbb{Z}_{25}^{12} \times \mathbb{Z}_5^{50}$$

equipped with the Lee metric. Note that this code C *is not linear, as the additive groups of* $\mathrm{GF}(25)$ *and* $\mathbb{Z}_{25}$ *are not isomorphic.*

Observe that linear perfect 1-error-correcting mixed codes in the Lee metric are considered by AIBdaiwi et al. in [1]. However, they do not mention the word "mixed".

From [9] we know that if there is a mixed perfect 1-error-correcting code in a direct product $S_1 \times S_2 \times \cdots \times S_n$ equipped with the Hamming metric, and the prime number p divides one of the cardinalities of the sets S_i, then p divides the size of every S_i, $i \in [n]$. This fact limits the number of possibilities to use the combining construction in order to produce mixed perfect 1-error-correcting Lee codes.

Example 5. *(Lipschitz metric) The Lipschitz metric was introduced by Martinez et al. in [19]. In short: Consider the ring* $H(\mathbb{Z})$ *consisting of the "integer quaternions"*

$$H(\mathbb{Z}) = \{a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\},$$

where $e_i^2 = -1$*,* $e_1 e_2 = -e_2 e_1 = e_3$*,* $e_3 e_2 = -e_2 e_3 = -e_1$*,* $e_1 e_3 = -e_3 e_1 = -e_2$*. Let* π *be a Lipschitz prime, that is,*

$$\pi = a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3,$$

where $N(\pi) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ *is a prime number. The equivalence relation* $x \sim y$ *if* $x - y = \lambda\pi$*, for some* $\lambda \in H(\mathbb{Z})$*, gives rise to a set of* $N(\pi)^2$ *equivalence classes, that constitute an Abelian group* $H(\mathbb{Z})_\pi$*, see [19]. Let*

$$\mathcal{E} = \{\pm 1, \pm e_1, \pm e_2, \pm e_3\}.$$

In [7], constructions of many perfect 1-$\mathcal{E}$*-error-correcting codes in direct products of these Abelian groups* $H(\mathbb{Z})_\pi$ *are presented. For example, with* $\pi = 2 + e_1 + e_2 + e_3$*,*

an 1-$\mathcal{E}$-error-correcting code in the direct product $H(\mathbb{Z})^6_\pi$ is constructed. Now we can further construct such codes by combining Proposition 1 with Theorem 5, whereby we use any perfect 1-error-correcting code over an alphabet with 49 symbols as an outer code.

Example 6. *(Both Lipschitz and Hurwitz metrics.) The Hurwitz metric is introduced in [7]. In short, if we define an equivalence relation on the ring of Hurwitz integers $\mathcal{H} = H(\mathbb{Z}) \cup H(\frac{1}{2} + \mathbb{Z})$ similarly to the equivalence relation we defined in the previous example, then the number of equivalence classes will be the same as in $H(\mathbb{Z})$, see [7]. Let*

$$\mathcal{E}' = \{\pm 1, \pm e_1, \pm e_2, \pm e_3, \frac{1}{2}(\pm 1 \pm e_1 \pm e_2 \pm e_3)\}.$$

Let $\pi = 2 + e_1 + e_2 + e_3$, and let $\mathcal{H}_\pi$ denote the set of equivalence classes that occur under the equivalence relation induced by π. Then $|\mathcal{H}_\pi| = 49$. In [7], a perfect 1-$\mathcal{E}'$-error-correcting code in $\mathcal{H}^2_\pi$ is presented. If as an outer code we use any perfect 1-error-correcting code in the Hamming metric over an alphabet with 49 symbols, then we may construct perfect 1-$\{\mathcal{E}, \mathcal{E}'\}$-error-correcting codes. With such a code, in some coordinate positions we can correct errors belonging to the set $\mathcal{E}$, and, in other coordinate positions, correct errors belonging to the set $\mathcal{E}'$.

Indeed, the number of possibilities to construct codes by combining Proposition 1 and Theorem 5 is large. However, one restriction is the existence of perfect 1-error-correcting codes in the Hamming metric. For a survey of these codes see Section 6.

4. Linear perfect 1-$\mathcal{E}$error-correcting codes of length $n(k)$ and dimension $n(k) - k$

Let the $n' \times k$-matrix $\mathbf{H}'$ be a parity-check matrix to a perfect 1-error-correcting code $C_{H'}$ in the Hamming metric of length n' over the alphabet GF(q). Then $n' = (q^k - 1)/(q - 1)$ and

$$\mathbf{H}' = \begin{pmatrix} | & & | \\ \bar{k}_1 & \cdots & \bar{k}_{n'} \\ | & & | \end{pmatrix},$$

where $\bar{k}_1$, ..., $\bar{k}_{n'}$ are elements of the vector space $V = \mathrm{GF}(q)^k$ such that the 1-dimensional spaces $\bar{k}_i\mathrm{GF}(q)$, for $i \in [n']$, constitute a subspace partition of V. (Equivalently, the columns of $\mathbf{H}'$ represent the points in the finite $(k-1)$-dimensional projective geometry $\mathrm{PG}(k-1, q)$.)

The code $C_{H'}$ is the null-space of $\mathbf{H}'$, but $C_{H'}$ can also be defined as the kernel of the map f defined in (15) with the spaces $k_i\mathrm{GF}(q)$, for $i \in [n']$, forming the subspace partition of V. The dimension of C'_H is $n' - k$, as the rows of $\mathbf{H}'$ are linearly independent.

Let $\mathcal{E}$ and d_1, ..., d_n be defined as in Example 2 and let $n(k) = nn'$. Now we can construct a perfect 1-$\mathcal{E}$-error-correcting code C of length $n(k)$.

The code C is the null-space of the $k \times n(k)$-matrix

$$\mathbf{H} = \left(d_1\mathbf{H}' \middle| d_2\mathbf{H}' \middle| \cdots \middle| d_n\mathbf{H}' \right),$$

which is the concatenation of the matrices $d_i\mathbf{H}'$. The rows of the matrix $\mathbf{H}$ are linearly independent, as the rows of the matrix $d_1\mathbf{H}'$ are linearly independent. Hence, the dimension of C is equal to $n(k) - k$.

For any $\bar{x} \in \mathrm{GF}(q)^{n(k)} \setminus C$, the syndrome $\mathbf{H}\bar{x}^T$ is an element in $\mathrm{GF}(q)^k$, and thus equal to $e_i\bar{k}_i$ for a unique column $\bar{k}_i$ of $\mathbf{H}'$ and a unique $e_i \in \mathrm{GF}(q) \setminus \{0\}$. As e_i is equal to $d_j\epsilon_i$ for a unique pair (d_j, ϵ_i), where $j \in [n]$ and $\epsilon_i \in \mathcal{E}$, we can find the "nearest" codeword simply by subtracting the word $\bar{x}$ with ϵ_i in the i-th coordinate position in the block of the vector $\bar{x}$ that corresponds to the block $d_j\mathbf{H}'$ in the matrix $\mathbf{H}$. Hence, C is a perfect 1-$\mathcal{E}$-error-correcting code.

5. Linear perfect 1-$\mathcal{E}$-error-correcting codes vs. Hamming codes

Assume that $q = p^m$, for some prime number p and some positive integer m. Let $\mathcal{E}$ be a subgroup of the multiplicative group of the finite field $\mathrm{GF}(q)$ such that $|\mathcal{E}| = p^t - 1$ for some integer t. Then t divides m and $\mathcal{E} \cup \{0\}$ is a subfield of $\mathrm{GF}(q)$ that we may identify with $\mathrm{GF}(p^t)$, see e.g. [16]. Thus we can regard $\mathrm{GF}(q)$ as a vector space over the finite field $\mathcal{E} \cup \{0\}$.

Let d_1, ..., d_n be as in Example 2, and let C be the perfect 1-$\mathcal{E}$-error-correcting code obtained in that example. The sets $U_i = d_i\mathcal{E} \cup \{0\}$, for $i \in [n]$, are vector spaces of dimension 1 over $\mathrm{GF}(p^t)$ constituting a subspace partition (14) of $\mathrm{GF}(q)$.

We can thus describe the direct product $S = \mathrm{GF}(q)^n$ as a direct product of unions of the 1-dimensional subspaces $d_i\mathcal{E} \cup \{0\}$:

$$S = \mathrm{GF}(q)^n = \begin{array}{c} \mathrm{GF}(q) \\ \times \\ \vdots \\ \times \\ \mathrm{GF}(q) \end{array} = \begin{array}{c} (\{0\} \cup d_1\mathcal{E} \cup d_2\mathcal{E} \cup \ldots \cup d_n\mathcal{E}) \\ \times \\ \vdots \\ \times \\ (\{0\} \cup d_1\mathcal{E} \cup d_2\mathcal{E} \cup \ldots \cup d_n\mathcal{E}) \end{array}$$

Let π be any permutation of the elements in the set $[n]$. Then, by Section 2.1, the set of words $(x_1, \ldots, x_n)$ in $\mathrm{GF}(p^t)^n$ such that

$$d_{\pi(1)}x_1 + \cdots + d_{\pi(n)}x_n = 0, \tag{16}$$

constitutes a perfect 1-error-correcting code C_π. Now, in each coordinate position in the direct product S, we perform the following linear map from $\mathrm{GF}(q)$ to $\mathrm{GF}(q)$:

$$\psi_i : \quad x_i \ \mapsto \ \frac{d_{\pi(i)}}{d_i}\, x_i, \qquad i \in [n].$$

Then the perfect 1-error-correcting code C_π is mapped to a perfect 1-error-correcting code $\psi(C_\pi)$ and

$$\psi(C_\pi) \subseteq \frac{d_{\pi(1)}}{d_1}\,(\mathcal{E} \cup \{0\}) \times \cdots \times \frac{d_{\pi(n)}}{d_n}\,(\mathcal{E} \cup \{0\}) \subseteq S. \tag{17}$$

Finally, for any element $(y_1, \ldots, y_n)$ of $\psi(C_\pi)$, from (16) we get that

$$d_1 y_1 + \cdots + d_n y_n = d_1 \frac{d_{\pi(1)}}{d_1} x_1 + \cdots + d_n \frac{d_{\pi(n)}}{d_n} x_n = 0.$$

Thus, the perfect 1-error-correcting code $\psi(C_\pi)$ is a subset of C. Distinct permutations give distinct direct products in (17). As there are $n!$ distinct permutations π of the set $[n]$, we can conclude that C contains at least $n!$ perfect 1-error-correcting codes.

6. Remarks

The combining construction of 1-$\mathcal{E}$-error-correcting codes has some limitations. This is because perfect codes in the Hamming metric used as outer codes in the combining construction, have so far been constructed just over alphabets of a size equal to a power of a prime number. However, in that case there are several distinct constructions. A survey of perfect binary codes can be found in [11], or the book by Solov'eva [28]. Below we give references to some of the main results in this area:

The first construction of a perfect code was given by Hamming [8]. His codes were linear, binary and 1-error-correcting. The first non-linear perfect 1-error correcting binary code was found by Vasil'ev [29] in 1961. Almost a decade later, Vasil'ev's construction was generalized to the q-ary case by Lindström [18] and independently by Schönheim [24]. The first construction of mixed perfect codes not equivalent to any linear code was given by Heden [10]. The construction in Section 3 was inspired by Heden's construction. The construction of Heden was also the second found construction of non-linear perfect binary codes. Other nice and useful constructions have been given by Solov'eva [26] and Phelps [21], [22]. A kind of classification of perfect 1-error-correcting q-ary codes can be found in [14]. A very few known results on perfect 1-error-correcting codes over non-prime power alphabets are surveyed in [12].

In any way, it may be concluded that there indeed exist quite a few perfect 1-$\mathcal{E}$-error-correcting codes.

References

[1] B. AIBDAIWI, P. HORAK, L. MILAZZO, *Enumerating and decoding perfect linear Lee codes*, Des. Codes Cryptogr. **52**(2009), 155–162.

[2] A. BEUTELSPACHER, *Partial spreads in finite projective spaces and partial designs*, Math. Zeit. **145**(1975), 211–229.

[3] T. BU, *Partitions of a vector space*, Disc. Math. **31**(1980), 79–83.

[4] T. ETZION, *Product Constructions for Perfect Lee Codes*, IEEE Trans. Inform. Theory **57**(2011), 7473–7481.

[5] Y. FAN, Y. GAO, *Codes over algebraic integer rings of cyclotomic fields*, IEEE Trans. Inform. Theory **50**(2004), 194–200.

[6] S. W. GOLOMB, L. R. WELCH, *Perfect codes in the Lee metric and the packing of polyominoes*, SIAM J. Appl. Math. **18**(1970), 302–317.

[7] M. GÜZELTEPE, O. HEDEN, *Perfect Mannheim, Lipschitz and Hurwitz weight codes*, Math. Commun. **19**(2014), 253 – 276.

[8] R. W. Hamming, *Error Detecting and Error Correcting Codes*, Bell System Technical Journal **29**(1950), 147–160.
[9] O. Heden, *A generalized Lloyd theorem and mixed perfect codes*, Math. Scand. **37**(1975), 13–26.
[10] O. Heden, *A new construction of group and nongroup perfect codes*, Information and Control **34**(1977), 314–323.
[11] O. Heden, *A survey of perfect codes*, Adv. Math. Commun. **2**(2008), 223–247.
[12] O. Heden, *On Perfect codes over non prime power alphabets*, Contemp. Math. **523**(2010), 173–184.
[13] O. Heden, *A survey of the different types of vector space partitions*, Discrete Math. Algorithm. Appl. **4**(2012), 1–14.
[14] O. Heden, D. Krotov, *On the structure of non-full-rank perfect q-ary codes*, Adv. Math. Commun **5**(2011), 149–156.
[15] M. Herzog, J. Schöheim, *Group partition, factorization and the vector covering problem*, Canad. Math. Bull. **15**(1972), 207–214.
[16] S. Lang, *Algebra*, Addison Wesley, Reading, Massachusetts, London, Sidney and Manila, 1971.
[17] C. Y. Lee, *Some properties of non-binary error correcting codes*, IEEE Trans. Inform. Theory **4**(1958), 77–82.
[18] B. Lindström, *On group and non group perfect codes in q symbols*, Math. Scand. **25**(1969), 149–158.
[19] C. Martinez, R. Beivide, E. Gabidulin, *Perfect codes from Cayley graphs over Lipschitz integers*, IEEE Trans. Inform. Theory **55**(2009), 3552–3562.
[20] K. Nakamura, *A class of error-correcting codes for DPSK channels*, in: *Proceedings of the International Conference on Communications*, Boston, Massachusetts, 1979, 45.4.1–45.4.5.
[21] K. Phelps, *A combinatorial construction of perfect codes*, Siam Journal on Algebraic and Discrete Methods **4**(1983), 398–403.
[22] K. Phelps, *A general product construction for error correcting codes*, SIAM Journal of Algebra and Discrete Methods **5**(1984), 224–228.
[23] R. M. Roth, *Introduction to Coding Theory*, Cambridge University Press, Cambridge, 2006.
[24] J. Schönheim, *On linear and nonlinear, single-error-correcting q-nary perfect codes*, Information and Control **12**(1968), 23–26.
[25] H. S. Shapiro, D. L. Slotnick, *On the mathematical theory of error-correcting codes*, IBM J. Res. Develop. **3**(1959), 25–34.
[26] F. I. Solov'eva, *On binary nongroup codes*, Methody Discretnogo Analiza **37**(1981), 65–76,(in Russian).
[27] F. I. Solov'eva, *Class of closed-packed binary codes generated by q-ary codes*, Methody Discretnogo Analiza **48**(1989), 70–72 (in Russian).
[28] F. I. Solov'eva, *On Perfect Codes and Related Topics*, Com^{2}Mac Lecture Note Series 13, Pohang, 2004.
[29] Y. L. Vasil'ev, *On Nongroup close-packed codes*, Problemy Kibernetiki **8**(1962), 337–339.
[30] V. A. Zinoviev, *A combinatorial method for the construction and analysis of nonlinear error-correcting codes*, Doc. D. Thesis, Moscow, 1988.