On non-full-rank perfect codes over finite fields

Alexander M. Romanov

Received: 14 November 2017 / Revised: 31 May 2018 / Accepted: 2 June 2018 / Published online: 7 June 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract The paper deals with perfect 1-error correcting codes over a finite field with \( q \) elements (briefly \( q \)-ary 1-perfect codes). We show that the orthogonal code to a \( q \)-ary non-full-rank 1-perfect code of length \( n = (q^m - 1)/(q - 1) \) is a \( q \)-ary constant-weight code with Hamming weight equal to \( q^{m-1} \), where \( m \) is any natural number not less than two. Necessary and sufficient conditions for \( q \)-ary codes to be \( q \)-ary non-full-rank 1-perfect codes are obtained. We suggest a generalization of the concatenation construction to the \( q \)-ary case and construct a ternary 1-perfect code of length 13 and rank 12.

Keywords Hamming code · Perfect code · MDS code · Rank · Concatenation

Mathematics Subject Classification 94B05 · 94B25 · 11T71

1 Introduction

Let \( \mathbb{F}^n_q \) be a vector space of dimension \( n \) over the finite field \( \mathbb{F}_q \), where \( q = p^r \), \( p \) is a prime number, \( r \) is a positive integer. The Hamming distance between two vectors \( \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n \) is the number of coordinates in which they differ, denoted by \( d(\mathbf{x}, \mathbf{y}) \). The Hamming weight of a vector \( \mathbf{x} \in \mathbb{F}_q^n \) is equal to the Hamming distance between \( \mathbf{x} \) and the all-zero vector \( \mathbf{0} \), denoted by \( wt(\mathbf{x}) \). An arbitrary subset \( C \) of \( \mathbb{F}_q^n \) is called a \( q \)-ary code of length \( n \). The vectors in \( C \) are called codewords. A \( q \)-ary code \( C \) of length \( n \) is called a \( q \)-ary 1-perfect code of length \( n \) if for every vector \( \mathbf{x} \in \mathbb{F}_q^n \) there exists a unique codeword \( \mathbf{c} \in C \) such that \( d(\mathbf{x}, \mathbf{c}) \leq 1 \). Non-trivial \( q \)-ary 1-perfect codes of length \( n \) exist only if \( n = (q^m - 1)/(q - 1) \), where \( m \) is a natural number not less than two. Two codes \( C_1, C_2 \subseteq \mathbb{F}_q^n \) are said to be equivalent if there exists a vector \( \mathbf{v} \in \mathbb{F}_q^m \) and an \( n \times n \) monomial matrix \( \mathbf{M} \) over \( \mathbb{F}_q \) such that...
$C_2 = \{(v + cM) \mid c \in C_1\}$. We assume that the all-zero vector $0$ is in code unless otherwise stated. A code is called linear if it is a linear space over $\mathbb{F}_q$. Linear $q$-ary 1-perfect codes of length $n$ exist for all $n = (q^n - 1)/(q - 1)$, $m \geq 2$. For each $n = (q^n - 1)/(q - 1)$, $m \geq 2$, a linear $q$-ary 1-perfect code of length $n$ is unique up to equivalence and is called $q$-ary Hamming code.

Extended 1-perfect codes are formed from 1-perfect codes by adding an overall parity check bit.

Non-linear $q$-ary 1-perfect codes of length $n = (q^n - 1)/(q - 1)$ exist for $q = 2$, $m \geq 4$, and for $q \geq 3$, $m \geq 3$, see [9,23,25]; $q \geq 5$, $m = 2$, see [6,9,18,20]. Non-linear $q$-ary 1-perfect codes of length $n = (q^n - 1)/(q - 1)$ do not exist for $q = 2$, $m \leq 3$, and for $q = 3$, $m = 2$, see [1].

The rank of a code $C$ is the maximum number of linearly independent codewords of $C$. A code of length $n$ that has rank $n$ is said to have full-rank; otherwise, the code is non-full-rank. The rank of the $q$-ary Hamming code of length $n$ is $n - m$, where $n = (q^n - 1)/(q - 1)$, $m \geq 2$.

Full-rank $q$-ary 1-perfect codes have been proposed for all $n = (q^n - 1)/(q - 1)$, $m \geq 4$ by using the switching constructions [3,19,21]. For $m = 3$ and for $q = p^r$, $r > 1$, the existence of full-rank $q$-ary 1-perfect codes is proved in [18]. The question of the existence of full-rank $q$-ary 1-perfect codes of length $n = (q^n - 1)/(q - 1)$ still remains open if $m = 3$, $q \geq 3$, $q$ is a prime number, and if $m = 2$, $q \geq 5$, see [6,18].

The switching constructions is closely related to the question of the minimum and maximum possible cardinality of the intersection of two distinct 1-perfect codes of the same length. In the $q$-ary case, this question still remains open. In the binary case, this question was answered in [3,4].

It is established that there exist at least $q^n$ nonequivalent $q$-ary 1-perfect codes of length $n$, where $c = \frac{1}{q} - \varepsilon$ ($\varepsilon \to 0$ as $n \to \infty$) [9,23,25].

The minimum distance of a code $C$ is the smallest Hamming distance between two distinct codewords in $C$, denoted by $d(C)$. A $q$-ary linear code of length $n$, dimension $k$, and minimum distance $d$ is called an $[n,k,d]_q$ code or an $[n,k,d]$ for $q = 2$. A $q$-ary non-linear code of length $n$ with $M$ codewords and minimum distance $d$ is called an $(n,M,d)_q$ code or an $(n,M,d)$ code for $q = 2$.

Consider a $q$-ary code with parameters $(n,M,d)_q$. Then the following inequality holds:

$$M \leq q^{n-d+1}.$$  \hspace{1cm} (1)

The inequality (1) is called the Singleton bound. The codes that achieve the Singleton bound are called maximum distance separable codes or briefly MDS. The MDS codes with parameters $[n,1,1]_q$, $[n,n-1,2]_q$, $[n,n,1]_q$ are called trivial MDS codes [10, pp. 33, 318]. It is widely known that MDS codes are the same as orthogonal arrays of index unity. In this paper, MDS codes will be considered only with minimum distance 2.

We give a description of the concatenation construction of binary 1-perfect codes. Let $m$ be any natural number not less than two and $n = 2^m - 1$. Moreover, let $C_1^0, C_1^1, \ldots, C_1^n$ be a partition of the vector space $\mathbb{F}_2^n$ into binary 1-perfect codes of length $n$ and let $C_0^1, C_0^2, \ldots, C_0^n$ be a partition of the binary MDS code with parameters $(n+1,n,2)$ into binary extended 1-perfect codes with parameters $(n+1,2^{n-m},4)$. (The binary MDS code with parameters $(n+1,n,2)$ consists of all binary vectors of length $n+1$ of even weight.) Then the given partitions $C_0^1, C_0^2, \ldots, C_0^n$, $C_1^0, C_1^2, \ldots, C_1^n$ and a permutation $\alpha$ acting on the index set $I = \{0,1,\ldots,n\}$ form the binary 1-perfect code

$$C_\alpha = \left\{(u|v) \mid u \in C_1^i, v \in C_2^{\alpha(i)}\right\}.$$
of length $2n + 1$, where $(\cdot | \cdot )$ denotes concatenation. It is known that the binary extended Hamming codes can be constructed by using the well-known $(u | u + v)$ construction [10, p. 76]. The concatenation construction of binary 1-perfect codes can be viewed as a combinatorial generalization of the $(u | u + v)$ construction.

In the binary case, the concatenation construction is based on partitions of two types – partitions of the space $F_2^n$ into 1-perfect codes and partitions of the binary MDS code into extended 1-perfect codes. For many decades, the question of the parameters of codes to which codes to the answer to this question and generalize the concatenation construction of binary 1-perfect codes to the $q$-ary case.

For $m \geq 4$, $q$-ary 1-perfect codes of length $n = (q^m - 1)/(q - 1)$ and rank $n - m + s$ exist for all $s \in \{0, 1, \ldots, m\}$, see [3, 19].

For $m = 3$, $q = p^r$, $r > 1$, the existence of $q$-ary 1-perfect codes of length $n = (q^3 - 1)/(q - 1)$ and rank $n - 3 + s$, $s \in \{2, 3\}$ is proved in [18]. For $m = 3$, $q \geq 3$, Lindström–Schönheim codes are codes of length $n = (q^3 - 1)/(q - 1)$ and rank $n - 2$, see [9, 19, 23]. For $m = 3$, $q \geq 3, q$ is a prime number, the question of the existence of $q$-ary 1-perfect codes of length $n = (q^3 - 1)/(q - 1)$ and rank $n - 3 + s, s \in \{2, 3\}$ still remains open [18, 19].

In particular, the question of the existence of ternary 1-perfect codes of length 13 and rank 12 remained open. In this paper we have an answer to this question. We construct the ternary 1-perfect code of length 13 and rank 12 by using the $q$-ary concatenation construction proposed in this paper.

For $m = 2$, $q$-ary 1-perfect codes of length $n = (q^2 - 1)/(q - 1)$ and rank $n - 1$ exist for all $q \geq 5$, see [6, 18]. For $m = 2, q \geq 5$, the question of the existence of $q$-ary 1-perfect codes of length $n = (q^2 - 1)/(q - 1)$ and rank $n$ still remains open [6, 18].

In Sect. 2, we show that the code orthogonal to a non-full-rank $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$ is a $q$-ary constant-weight code with Hamming weight equal to $q^{m-1}$, where $m$ is any natural number not less than two. In Sect. 3, we present necessary and sufficient conditions conditions for $q$-ary codes to be $q$-ary non-full-rank 1-perfect codes. In Sect. 4, we suggest a generalization of the concatenation construction to the $q$-ary case. In Sect. 5, we present a ternary 1-perfect code of length 13 and rank 12 by using this generalization of the concatenation construction.

## 2 Orthogonal codes

Let $u, v \in F_q^n$. Then the **scalar product** of $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ is the mapping

$$u \cdot v = \sum_{i=1}^{n} u_i v_i.$$ 

Let $C \subset F_q^n$. Then the code

$$C^\perp = \{ u \mid u \in F_q^n \text{ and } u \cdot v = 0 \text{ for all } v \in C \}$$

is called the orthogonal or dual of the code $C$. The dual code of the Hamming code is the **simplex code**. The dual code of the Hamming code has parameters $[n, m, q^{m-1}]_q$, where $n = (q^m - 1)/(q - 1)$.

All codewords of a simplex code of length $n = (q^m - 1)/(q - 1)$, with the exception of the all-zero codeword, have the same weight equal to $q^{m-1}$, see [10, pp. 30, 31].
Following [3] we will use the methods described in [10, p. 132]. We shall represent sets of vectors from the space $F^n_q$ by formal polynomials in variables $z_1, z_2, \ldots, z_n$. The vector $v = (v_1, v_2, \ldots, v_n) \in F^n_q$ corresponds to the monomial $z^v = z_1^{v_1}z_2^{v_2} \ldots z_n^{v_n}$. The set of all monomials in the variables $z_1, z_2, \ldots, z_n$ forms a multiplicative group $G$ whose multiplication corresponds to the addition in $F^n_q$. Next, we define the group algebra $QG$ of the group $G$ over the field of rational numbers $Q$, which consists of all formal sums

$$
\sum_{v \in F^n_q} a_v z^v, \quad a_v \in Q, \quad z^v \in G.
$$

For each $u \in F^n_q$, we define the character of the group $G$. Let $\chi_u(z^v) = \zeta^{uv}$, where $\zeta$ is a primitive $q$th root of unity. The character $\chi_u$ is extended on $QG$ by linearity. Then

$$
\chi_u(C) = \chi_u \left( \sum_{v \in C} z^v \right) = \sum_{v \in C} \chi_u(z^v) = \sum_{v \in C} \zeta^{uv}.
$$

and, therefore, $\chi_u(C) = |C|$ for $u \in C^\perp$, where $C$ is a code (linear or non-linear).

Obviously that

$$
\chi_u(v + v') = \chi_u(v)\chi_u(v'),
$$

where $u, v, v' \in F^n_q$, and

$$
\chi_u(A + B) = \chi_u(A)\chi_u(B),
$$

where $A, B \subseteq F^n_q$.

It is known [10, p. 134] that if a code $C$ is linear, then

$$
\chi_u(C) = \begin{cases} 
|C| & \text{if } u \in C^\perp, \\
0 & \text{if } u \notin C^\perp.
\end{cases}
$$

Therefore, $\chi_u(F^n_q) = 0$ for any $u \in F^n_q \setminus \{0\}$.

Given a $q$-ary code with parameters $(n, M, d)_q$, let $B_i$ be the number of codewords of weight $i$, where $0 \leq i \leq n$. We assume that the all-zero vector $0$ is in code thus $B_0 = 1$. The ordered set $\{B_0, B_1, \ldots, B_n\}$ is called the weight distribution of the code.

**Theorem 1** Let $C$ be a $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$ and rank $k$. Let $\{B_0, B_1, \ldots, B_n\}$ be the weight distribution of the code $C^\perp$. Then

$$
B_i = \begin{cases} 
1 & \text{if } i = 0, \\
0 & \text{if } 1 \leq i \leq q^{m-1} - 1, \\
q^{n-k} - 1 & \text{if } i = q^{m-1}, \\
0 & \text{if } q^{m-1} + 1 \leq i \leq n.
\end{cases}
$$

**Proof** Let $V \subseteq F^n_q$ be a Hamming sphere of radius 1 centred in the all-zero vector 0. Since the code $C$ is $q$-ary 1-perfect, $F^n_q = C + V$ and $\chi_u(F^n_q) = \chi_u(C)\chi_u(V) = 0$ for any $u \in F^n_q \setminus \{0\}$. Thus $\chi_u(V) = 0$ if $\chi_u(C) \neq 0$. The number of vectors in $V$ is $1 + n(q - 1) = q^m$. Since $\chi_u(V) = 0$ for any nonzero $u \in F_q$, $\chi_u(V) = q^m - q\cdot wt(u) = 0$ for $wt(u) = q^{m-1}$. Since $C$ is a $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$ and rank $k$, the rank of $C^\perp$ is $n - k$.

\[ \square \]
3 Necessary and sufficient conditions

We denote by $M_{q,n}$ the $q$-ary MDS code with parameters $[n, n - 1, 2]_q$, i.e.

$$M_{q,n} = \left\{ (x_1, x_2, \ldots, x_{n-1}, -\sum_{i=1}^{n-1} x_i) \mid (x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_q^{n-1} \right\}.$$

Consider a non-full-rank code $C$ of length $n = (q^m - 1)/(q - 1)$ over the field $\mathbb{F}_q$. Let $w \in C^\perp \setminus \{0\}$. If $wt(w) \neq q^{m-1}$, by Theorem 1 the code $C$ is not 1-perfect. Assume that $wt(w) = q^{m-1}$. Moreover, assume that the first $n - q^{m-1}$ components of the vector $w$ are 0, and the remaining components of this vector are 1. Let a vector $(u|v) \in C$. We assume that $u$ has length equal to $n - q^{m-1}$. For each vector $v \in M_{q,q^{m-1}}$, we define a $q$-ary code $C'(v)$ of length $n - q^{m-1}$. Let

$$C'(v) = \left\{ u \in \mathbb{F}_q^{n-q^{m-1}} \mid (u|v) \in C \right\}.$$

For each vector $u \in \mathbb{F}_q^{n-q^{m-1}}$, we define a $q$-ary code $C''(u)$ of length $q^{m-1}$. Let

$$C''(u) = \left\{ v \in M_{q,q^{m-1}} \mid (u|v) \in C \right\}.$$

**Theorem 2** The code $C$ of length $n = (q^m - 1)/(q - 1)$ over the field $\mathbb{F}_q$ is a $q$-ary non-full-rank 1-perfect code if and only if the code $C'(v)$ is a $q$-ary 1-perfect code of length $n - q^{m-1}$ for any $v \in M_{q,q^{m-1}}$ and the code $C''(u) \subseteq M_{q,q^{m-1}}$ is a $q$-ary code with parameters $(q^{m-1}, q^{m-1}-m, d)_q$ for any $u \in \mathbb{F}_q^{n-q^{m-1}}$, where $d = 3$ for $q > 2$ and $d = 4$ for $q = 2$.

**Proof** We prove Theorem 2 for $q > 2$. For $q = 2$ see [3]. Let us prove the sufficiency of the conditions of Theorem 2. For this it is necessary to show that the number of codewords in the code $C$ is correct and the minimum distance $d(C)$ of the code $C$ is 3. Let us show that the number of code codewords in the code $C$ is correct. By the definition of the code $C'$, we have

$$|C| = \sum_{v \in M_{q,q^{m-1}}} |C'(v)| = q^{m-1} \cdot q^{n-q^{m-1}-(m-1)} = q^n - m.$$

By the definition of the code $C''$, we have

$$|C| = \sum_{u \in \mathbb{F}_q^{n-q^{m-1}}} |C''(u)| = q^{n-q^{m-1}} \cdot q^{m-1} - m = q^n - m.$$

Now we show that the minimum distance $d(C) = 3$. Let the vectors $(u|v)$ and $(u'|v')$ belong to the code $C$. Assume that $u = u'$, then $v, v' \in C''(u)$ and $d((u|v), (u'|v')) \geq 3$. Assume that $v = v'$, then $u, u' \in C'(v)$ and $d((u|v), (u'|v')) \geq 3$. Assume that $u \neq u'$ and $v \neq v'$, then $d((u|v), (u'|v')) \geq 3$. Since $v, v' \in M_{q,q^{m-1}}$, then $d(v, v') \geq 2$ and, therefore, $d((u|v), (u'|v')) \geq 3$.

Consider a vector $w \in \mathbb{F}_q^n$. Suppose that the first $n - q^{m-1}$ components of the vector $w$ are equal to 0, and the remaining components of this vector are equal to 1. Then it is obvious that $w \in C^\perp$ and, therefore, the code $C$ is a $q$-ary 1-perfect code of non-full-rank.

Next we prove the necessity of the conditions of Theorem 2. By the conditions of Theorem 2, the code $C$ is a $q$-ary 1-perfect code of non-full-rank and, consequently, there exists a nonzero vector $w \in C^\perp$. Then it follows from Theorem 1 that $wt(w) = q^{m-1}$. Suppose that
the first \( n - q^m \) components of the vector \( w \) are equal to 0, and the remaining components of this vector are equal to 1. Consider a vector \((u|v) \in C\). Assume that \( u \) has length equal to \( n - q^m \). Since the first \( n - q^m \) components of the vector \( w \) are equal to 0, we have \( v \in M_{q,q^m} \).

Since \( d(C) \geq 3 \), then \( d(C' (v)) \geq 3 \). Since the length of \( C' (v) \) is \( n - q^m \), it follows from the sphere-packing bound that \( |C' (v)| \leq q^n - q^m - (m-1) \). Let \( |C' (v')| < q^n - q^m - (m-1) \) for some \( v' \).

\[
|C| = \sum_{v \in M_{q,q^m}} |C' (v)| = \left(q^m - 1\right)q^n - q^m - (m-1) + |C' (v')| < q^n - m,
\]

which contradicts the condition of Theorem 2 on the perfectness of the code \( C \).

Since \( d(C) \geq 3 \), then \( d(C'' (u)) \geq 3 \). Since the code \( C \) is a \( q \)-ary 1-perfect code of length \( n \) and the length of the code \( C'' (u) \) is equal to \( q^m \), it is known that \( |C'' (u)| \leq q^{m-1} \) see [2, 10, p. 537].

Let \( |C'' (u')| < q^m - m \) for some \( u' \). Then

\[
|C| = \sum_{u \in F_q^n} |C'' (u)| = \left(q^m - q^m - 1\right)q^m - m + |C'' (u')| < q^n - m.
\]

\[\square\]

For \( q = 2 \), the code \( C'' (u) \) has the parameters \( (2^m - 1, 2^{m-1} - m, 4) \), see [3].

From Theorem 2.1 of the paper [7] it follows, in particular, that for any \( q \)-ary 1-perfect code \( C \) of non-full-rank and length \( n = (q^m - 1)/(q-1) \) there exists a monomial transformation \( \psi \) of the space \( F_q^n \) such that

\[\psi(C) = \{(u|v) \mid u \in C' (v), v \in M_{q,q^m}\},\]

where \( C' (v) \) is a \( q \)-ary 1-perfect code of length \( n - q^m \).

It follows from Theorem 2 that any vector \( w \in C_{\frac{1}{n}} \setminus \{0\} \) forms a representation of the code \( C \) in the form (2).

### 4 Concatenation construction

Let \( m \) be any natural number not less than two, \( n = (q^m - 1)/(q-1) \). Let \( C_0^1, C_1^1, \ldots, C_{(q-1)m}^1 \) be a partition of the vector space \( F_q^n \) into \( q \)-ary 1-perfect codes of length \( n \). Moreover, let \( C_0^2, C_1^2, \ldots, C_{(q-1)m}^2 \) be a partition of an MDS code with parameters \((q - 1)n + 1, (q - 1)n, 2|q \) into \( q \)-ary codes with parameters \(((q - 1)n + 1, q^{(q-1)n-m}, 3)_q \) for \( q > 2 \). Such a partition exists by Theorem 2. For example, we can construct such a partition using a \( q \)-ary Hamming code (i.e. linear 1-perfect code). For \( q = 2 \), we consider binary extended 1-perfect codes, which are known to have parameters \((n + 1, 2^n - m, 4)\).

**Theorem 3** Given partitions \( C_0^1, C_1^1, \ldots, C_{(q-1)m}^1, C_0^2, C_1^2, \ldots, C_{(q-1)m}^2 \) and a permutation \( \alpha \) acting on the index set \( I = \{0, 1, \ldots, (q-1)n\} \). The \( q \)-ary code

\[C_\alpha = \{(u|v) \mid u \in C_i^1, v \in C_{\alpha(i)}^2\}\]

of length \( qn + 1 \) is 1-perfect.
Proof We need to show that the number of codewords in the code \( C_\alpha \) is correct and the minimum distance \( d(C_\alpha) \) of the code \( C_\alpha \) is 3. Since a \( q \)-ary 1-perfect code of length \( n \) contains \( q^{n-m} \) codewords, then

\[
|C_\alpha| = \sum_{v \in M_{q,(q-1)n+1}} |C'(v)| = q^{(q-1)n} q^{n-m} = q^{qn+1-(m+1)}.
\]

Next we show that the minimum distance \( d(C_\alpha) = 3 \). Let the vectors \((u|v)\) and \((u'|v')\) belong to the code \( C_\alpha \). Assume that \( v = v' \), then \( u, u' \in C^1_i \) for some \( i \in I \) and, consequently, \( d((u|v), (u'|v')) \geq 3 \). Assume that \( v = v' \), then \( u, u' \in C_\alpha(i) \) and \( d((u|v), (u'|v')) \geq 3 \). Further assume that \( u \neq u' \) and \( v \neq v' \), then \( d(u, u') \geq 1 \). Since \( v, v' \in M_{q,(q-1)n+1} \), then \( d(v, v') \geq 2 \) and, therefore, \( d((u|v), (u'|v')) \geq 3 \).

For \( q = 2, 3 \), the MDS codes with the minimum distance 2 are unique. It is obvious that \( q \)-ary 1-perfect codes can be constructed from any \( q \)-ary MDS code with minimum distance 2 by using the concatenation construction if there exists a partition of this MDS code into codes with parameters \(((q-1)n+1, q^{(q-1)n-m}, 3)_q \).

It was established in [3] that in the binary case, 1-perfect codes of full-rank can not be constructed by using the concatenation construction. Etzion and Vardy [3] suggested a construction of binary 1-perfect codes, which is based on the so-called perfect segmentations and they showed that their method allows obtaining codes not equivalent to any binary 1-perfect code constructed by the concatenation method.

Heden [5] constructed a binary 1-perfect code of length 15, which is not equivalent to any Vasil’ev code [25]. It is known that Heden’s construction can be considered as a concatenation construction, which is based on the partitions of the space \( \mathbb{F}_2^n \) into binary Hamming codes and partitions of the binary MDS code of length \( n+1 \) into binary extended Hamming codes. Solov’eva [24] investigated the properties of binary 1-perfect codes, which are constructed by the concatenation method from partitions of the space \( \mathbb{F}_2^n \) into Vasil’ev codes [25] and from the partition of the binary MDS codes into extended Vasil’ev codes. The concatenation construction is closely related to the problem of the partition of the space \( \mathbb{F}_q^n \) into 1-perfect codes. There are many papers in which various partitions of the space \( \mathbb{F}_q^n \) into 1-perfect codes are suggested (see, for example, [8]).

In [17], with the help of the concatenation construction, binary 1-perfect codes are constructed that belong to different switching classes.

Phelps [13] proposed a concatenation construction of binary extended 1-perfect codes of length \( 2n+2 \) starting from partitions of the binary MDS code with parameters \([n+1, n, 2] \) into binary extended 1-perfect codes of length \( n+1 \). Phelps [16] enumerated all nonequivalent binary extended 1-perfect codes of length 16, which can be constructed by the concatenation construction, and showed that this method allows to construct at least 963 such codes. As is known [12], there are 2165 nonequivalent binary extended 1-perfect codes of length 16. From [27] it is follows that there are 1990 nonequivalent binary extended 1-perfect codes of length 16 and and rank less than 15. Therefore, we can assume that by concatenation construction it is impossible to construct all binary extended 1-perfect codes of length 16 and rank less than 15.

Zinoviev suggested the generalized concatenated construction for the codes, which can be used, in particular, for 1-perfect codes [26]. Phelps [14] generalized the binary concatenation construction that doubled the length of the code, and instead of permutations Phelps suggested using quasigroups; herewith the length of the code began to increase many times. Some generalizations of the switching constructions and the Phelps’s construction [14] were proposed in [7, 11, 15]. Notice that the Heden and Krotov construction [7] is based on partitions of the
space \( \mathbb{F}_q^n \) into \( q \)-ary 1-perfect codes and codes with parameters \((q - 1)n + 1, q^{(q - 1)n - m}, 3)_q\) are not used in it.

5 Ternary codes

The ternary Hamming code of length 13 has rank 10. The ternary nonlinear 1-perfect Lindström–Schönheim codes of length 13 have a rank equal to 11, see [9, 19, 23]. In this section, using the concatenation method (Theorem 3), we construct a ternary 1-perfect code of length 13 and rank 12.

Let the matrix

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 \\
1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1
\end{bmatrix}
\]

be a parity-check matrix of the ternary Hamming code of length 13. We denote by \( H \) this Hamming code. Consider the vector \( 0000111111111 \in H^\perp \). According to Theorem 2, from this vector we consider a ternary linear code \( C'' \) with parameters \([9, 6, 3]_3\), whose codewords belong to the ternary MDS code \( M_{3, 9} \) with parameters \([9, 8, 2]_3\). Since the code \( C'' \) is linear and \( C'' \subset M_{3, 9} \), it forms a partition of \( M_{3, 9} \) into cosets \( C''_0, C''_1, \ldots, C''_8 \). A ternary Hamming code of length 4 forms a partition of the space \( \mathbb{F}_3^4 \) into cosets \( C'_0, C'_1, \ldots, C'_8 \). Consider the vectors:

- \( u_8 = 0 \ 0 \ 0 \ 1 \ v_8 = 1 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_7 = 0 \ 0 \ 0 \ 2 \ v_7 = 1 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_6 = 0 \ 0 \ 1 \ 0 \ v_6 = 1 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_5 = 0 \ 0 \ 2 \ 0 \ v_5 = 1 \ 0 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_4 = 0 \ 1 \ 0 \ 0 \ v_4 = 1 \ 0 \ 0 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_3 = 0 \ 2 \ 0 \ 0 \ v_3 = 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \ 0 \)
- \( u_2 = 1 \ 0 \ 0 \ 0 \ v_2 = 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \ 0 \)
- \( u_1 = 2 \ 0 \ 0 \ 0 \ v_1 = 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 2 \ 0 \ 0 \ 0 \)
- \( u_0 = 0 \ 0 \ 0 \ 0 \ v_0 = 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \)

Let \( u_i \in C'_i, v_i \in C''_i, i = 0, 1, \ldots, 8 \) and \( \alpha \) be the identity permutation acting on the index set \( I = \{0, 1, \ldots, 8\} \). We denote by \( C_\alpha \) the ternary 1-perfect code of length 13, constructed using the concatenation construction (Theorem 3).

Since \( 00000000111000, 0000001010100, 0000010010010, 0000000012021 \in H \), the vectors \( 0001111000, 001010100, 010010010, 00012021 \in C''_0 \).

The vectors:

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 2 & 1 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 2 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0
\end{bmatrix}
\]
belong to the code $C_\alpha$ and are linearly independent. Therefore, the code $C_\alpha$ has rank 12.

For ternary 1-perfect codes only one case still remains open, namely the existence of ternary 1-perfect codes of length 13 and rank 13.

Acknowledgements The author would like to thank the anonymous referees for their helpful comments and suggestions. The results of this paper were presented at the International Conference “Mathematics in the Modern World” [22].

References

1. Alderson T.L.: (6, 3)-MDS codes over an alphabet of size 4. Des. Codes Crypt. 38(1), 31–40 (2006).
2. Delsarte P.: Bounds for unrestricted codes, by linear programming. Philips Res. Rep. 27, 272–289 (1972).
3. Etzion T., Vardy A.: Perfect binary codes: constructions, properties, and enumeration. IEEE Trans. Inf. Theory 40(3), 754–763 (1994).
4. Etzion T., Vardy A.: On perfect codes and tilings: problems and solutions. SIAM J. Discrete Math. 11(2), 205–223 (1998).
5. Heden O.: A new construction of group and nongroup perfect codes. Inform. Control 34, 314–323 (1977).
6. Heden O.: On perfect p-ary codes of length $p + 1$. Des. Codes Cryptogr. 46(1), 45–56 (2008).
7. Heden O., Krotov D.S.: On the structure of non-full-rank perfect $q$-ary codes. Adv. Math. Commun. 5(2), 149–156 (2011).
8. Krotov D.S., Sotnikova E.V.: Embedding in $q$-ary 1-perfect codes and partitions. Discrete Math. 338(11), 1856–1859 (2015).
9. Lindström B.: On group and nongroup perfect codes in $q$ symbols. Math. Scand. 25, 149–158 (1969).
10. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland Publishing Co., Amsterdam (1977).
11. Mollard M.: A generalized parity function and its use in the construction of perfect codes. SIAM J. Algebr. Discrete Methods 7(1), 113–115 (1986).
12. Östergård P.R.J., Pottonen O., Phelps K.T.: The perfect binary one-error-correcting codes of length 15: part II-properties. IEEE Trans. Inform. Theory 56(6), 2571–2582 (2010).
13. Phelps K.T.: A combinatorial construction of perfect codes. SIAM J. Algebr. Discrete Methods 4, 398–403 (1983).
14. Phelps K.T.: A general product construction for error correcting codes. SIAM J. Algebr. Discrete Methods 5(2), 224–228 (1984).
15. Phelps K.T.: A product construction for perfect codes over arbitrary alphabets. IEEE Trans. Inf. Theory 30(5), 769–771 (1984).
16. Phelps K.T.: An enumeration of 1-perfect binary codes. Aust. J. Comb. 21, 287–298 (2000).
17. Phelps K.T., LeVan M.J.: Switching equivalence classes of perfect codes. Des. Codes Cryptogr. 16(2), 179–184 (1999).
18. Phelps K.T., Rifà J., Villanueva M.: Kernels and $p$-kernels of $p^r$-ary 1-perfect codes. Des. Codes Cryptogr. 37(2), 243–261 (2005).
19. Phelps K.T., Villanueva M.: Ranks of $q$-ary 1-perfect codes. Des. Codes Cryptogr. 27(1–2), 139–144 (2002).
20. Romanov A.M.: Hamiltonicity of minimum distance graphs of 1-perfect codes. Electron. J. Comb. 19(1), P65 (2012).
21. Romanov A.M.: On full-rank perfect codes over finite fields. J. Appl. Indus. Math. 10(3), 444–452 (2016).
22. Romanov A.M.: On non-full-rank perfect codes over finite fields. In: Proceedings of International Conference “Mathematics in the Modern World”, Novosibirsk, 14–19 August 2017, p. 473 (2017).
23. Schönheim J.: On linear and nonlinear single-error-correcting $q$-ary perfect codes. Inform. Control 12, 23–26 (1968).
24. Solov’eva F.I.: On binary nongroup codes. Methody Diskr. Anal. 37, 65–76 (1981).
25. Vasil’ev J.I.: On nongroup close-packed codes. Probl. Cybernet. 8, 375–378 (1962).
26. Zinoviev V.A.: Generalized concatenated codes. Probl. Inform. Transm. 12(1), 5–15 (1976).
27. Zinoviev V.A., Zinoviev D.V.: Binary perfect and extended perfect codes of lengths 15 and 16 with ranks 13 and 14. Probl. Inform. Transm. 46(1), 20–24 (2010).