On the admissible families of components of Hamming codes

Alexander M. Romanov
Sobolev Institute of Mathematics
630090 Novosibirsk, Russia
rom@math.nsc.ru

Abstract

In this paper, we describe the properties of the $i$-components of Hamming codes. We suggest constructions of the admissible families of components of Hamming codes. It is shown that every $q$-ary code of length $m$ and minimum distance 5 (for $q = 3$ the minimum distance is 3) can be embedded in a $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$. It is also shown that every binary code of length $m + k$ and minimum distance $3k + 3$ can be embedded in a binary 1-perfect code of length $n = 2^m - 1$.

Keywords: Hamming codes, 1-perfect codes, $q$-ary codes, binary codes, $i$-component.

1 Introduction

Let $\mathbb{F}_q^n$ be a vector space of dimension $n$ over the Galois field $\mathbb{F}_q$. The Hamming distance between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ is the number of coordinates in which they differ and it is denote by $d(\mathbf{x}, \mathbf{y})$. An arbitrary subset $C$ of $\mathbb{F}_q^n$ is called $q$-ary 1-perfect code of length $n$, if for every vector $\mathbf{x} \in \mathbb{F}_q^n$ there exists a unique vector $\mathbf{c} \in C$ such that $d(\mathbf{x}, \mathbf{c}) \leq 1$. It is known that $q$-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. We shall assume that the all-zero vector $\mathbf{0}$ is in code. A code is called linear if it is a linear space over $\mathbb{F}_q$. The linear 1-perfect codes are called Hamming codes. The $q$-ary Hamming code of length $n$ is denoted by $\mathbb{H}$.

The weight of a vector $\mathbf{x} \in \mathbb{F}_q^n$ is the number $d(\mathbf{x}, \mathbf{0})$. A vector of weight 3 of the code $\mathbb{H}$ is called triple. Consider the subspace $R_i$ spanned by the set of all triples of the code $\mathbb{H}$ having 1 in the $i$-th coordinate. All cosets $R_i + \mathbf{u}$ form the set of $i$-components of the $q$-ary Hamming code $\mathbb{H}$, where $i \in \{1, 2 \ldots n\}$, $\mathbf{u} \in \mathbb{H}$. A family of components
$R_{i_1} + \bar{u}_1, R_{i_2} + \bar{u}_2, \ldots, R_{i_t} + \bar{u}_t$ of the \textit{q}-ary Hamming code $H$ is called \textit{admissible} if for $r, s \in \{1, 2, \ldots, t\}$, $r \neq s$, we have $(R_{i_r} + \bar{u}_r) \cap (R_{i_s} + \bar{u}_s) = \emptyset$. See [5].

Let $n_1 \leq n_2$, $C_1 \subseteq F_q^{n_1}$, $C_2 \subseteq F_q^{n_2}$. We lengthen all the vectors of the code $C_1$ to the length of $n_2$ by appending a zero vector of length $n_2 - n_1$. They say that the code $C_1$ can \textit{be embedded} in the code $C_2$ if all the lengthened vectors of $C_1$ belong to $C_2$. We consider all the vectors of the code $C_2$ in which the last $n_2 - n_1$ coordinates are equal to zero. We delete the last $n_2 - n_1$ coordinate in all such vectors. If the resulting set of shortened vectors coincides with $C_1$, then we say that the code $C_1$ can be embedded in the code $C_2$ in the strong sense.

Avgustinovich and Krotov [2] showed that any binary code of length $m$ and minimum distance 3 can be embedded (in the strong sense) in a binary 1-perfect code of length $2^m - 1$.

In this paper, we describe properties of the $i$-components of Hamming codes. We suggest constructions of the admissible families of components of Hamming codes. It is shown that every $q$-ary code of length $m$ and minimum distance 5 (for $q = 3$ the minimum distance is 3) can be embedded in a $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$. It is also shown that every binary code of length $m + k$ and distance $3k + 3$ can be embedded in a binary 1-perfect code of length $n = 2^m - 1$.

We present three examples of the admissible families of components of Hamming codes. In Example 1, for an arbitrary $q$-ary code $(A \cup \{0\}) \subseteq F_q^m$ with minimum distance 5 we construct an admissible family of components of $q$-ary Hamming code of length $n = (q^m - 1)/(q - 1)$. The admissible family of component is constructed so that switching the components of this family, we obtain a $q$-ary 1-perfect code $T$ of length $n$ in which can be embedded the $q$-ary code $A \cup \{0\}$ of length $m$. In Example 2, for an arbitrary ternary code of length $m$ and distance 3 in exactly the same method as in Example 1 we constructing an admissible family of components of the ternary Hamming code of length $n = (3^m - 1)/2$. In Example 3 for an arbitrary binary code of length $m + k$ and distance $3k + 3$ we constructing an admissible family of component of the binary Hamming code of length $n = 2^m - 1$. The admissible families of components from Examples 2 and 3 have the same properties as the admissible family of components from Example 1 and allow us, by switching the components, to construct the 1-perfect codes in which can be embedded codes of smaller length.

In Section 2 we present theorems describing the properties of the $i$-components of code $H$. In Section 3 we describe the constructions of admissible families of components of code $H$. In Section 4 we give Examples 2 and 3. In Section 5 we prove a theorem on the embeddability.

The parity-check matrix $H$ of the code $H$ of length $n = (q^m - 1)/(q - 1)$ consists of $n$ pairwise linearly independent column vectors $\vec{h}_i$. The transposed column vector $\vec{h}_i$ belongs to $F_q^n$, $i \in \{1, \ldots, n\}$. We assume that the columns of the parity-check matrix $H$
are arranged in some fixed order. The set \( \mathbb{F}_q^m \setminus \{ \vec{0} \} \) generates a projective space \( PG_{m-1}(q) \) of dimension \( m-1 \) over the Galois field \( \mathbb{F}_q \). In this space, points correspond to the columns of the parity-check matrix \( H \) and the three points \( i, j, k \) lie on the same line if the corresponding columns \( \vec{h}_i, \vec{h}_j, \vec{h}_k \) are linearly dependent. We denote by \( l_{xy} \) the line passing through the points \( x \) and \( y \), and we denote by \( P_{xyz} \) the plane spanned by three non-collinear points \( x, y, z \). Let \( \vec{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n \). Then, the support of the vector \( \vec{x} \) is the set \( \text{supp}(\vec{x}) = \{ i : x_i \neq 0 \} \). A triple belongs to the line if the support of this triple belongs to the line. The triples intersect at the point \( i \) if their supports intersect at the point \( i \).

2 Properties of \( i \)-components

Next, we present theorems describing the properties of the \( i \)-components of code \( \mathbb{H} \). Let the subcode \( \mathbb{H}_l \) of code \( \mathbb{H} \) be defined by the line \( l \). We consider the pencil of lines \( l_1, l_2, \ldots, l_{(n-1)/q} \) through a point \( i \). It is known [1] that

\[
R_i = \mathbb{H}_{l_1} + \mathbb{H}_{l_2} + \cdots + \mathbb{H}_{l_{(n-1)/q}}. \tag{1}
\]

**Theorem 1.** Let a vector \( \vec{u} = (u_1, u_2, \ldots, u_n) \in R_i \) and a component \( u_x \) of the vector \( \vec{u} \) be nonzero, \( x \neq i \). Then on the line \( l_{ix} \) there exists a point \( y \) distinct from the points \( i, x \) and such that component \( u_y \) of the vector \( \vec{u} \) is nonzero.

**Proof.** The basis of the subspace \( R_i \) is formed by all linearly independent triples of the code \( \mathbb{H} \) having 1 in the \( i \)-th coordinate. Consider representation of the vector \( \vec{u} \) with respect to the basis. From the conditions of the theorem, it follows that in this representation is a triple whose support contains points \( i, x \) and a point which is on the line \( l_{ix} \) and is distinct from the points \( i, x \). From formula (1) it follows that the basis triples belonging to the line \( l_{ix} \) form a subspace \( \mathbb{H}_{l_{ix}} \). The basis triples, that belong to other lines from the pencil of lines containing the point \( i \), intersect with the basis triples, that lie on the line \( l_{ix} \), only at one point \( i \). The theorem is proved.

**Theorem 2.** Let \( i \neq j \), a vector \( \vec{u} = (u_1, u_2, \ldots, u_n) \in R_i + R_j \), a component \( u_x \) of the vector \( \vec{u} \) be nonzero and the point \( x \) does not lie on \( l_{ij} \). Then on the plane \( P_{ijx} \) there exists a point \( y \) distinct from the points \( i, j, x \) and such that component \( u_y \) of the vector \( \vec{u} \) is nonzero.

**Proof.** This theorem is proved similarly to the previous one. The basis triples of \( R_i + R_j \) that lie on the plane \( P_{ijx} \) form a subspace. The lines from the pencil of lines containing the point \( i \) either lie on the plane \( P_{ijx} \) or intersect with this plane at only one point \( i \). The lines of the pencil of lines through the point \( j \) have the same property. The theorem is proved.
3 Example 1

Next, we describe the constructions of admissible families of components of code $\mathbb{H}$.

**Example 1.**

In the parity-check matrix $H$ of the Hamming code $\mathbb{H}$ of length $n = (q^m - 1)/(q - 1)$, we choose $m$ linearly independent columns. We assume that we have chosen the columns $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$. Let $(\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_q^m$ be a code containing $t$ nonzero vectors $\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t$, the weight of each of them be greater than or equal to three. Let the distance between any two distinct vectors from the set $\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}$ be greater than or equal to five. With each vector $\vec{\lambda}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm})$ of length $m$ we associate a vector $\vec{u}_s$ of length $n$, where $s \in \{1, \ldots, t\}$. Let

$$\mu_s \vec{h}_i = \lambda_{s1} \vec{h}_1 + \lambda_{s2} \vec{h}_2 + \cdots + \lambda_{sm} \vec{h}_m,$$

where $\mu_s \in \mathbb{F}_q$, $i_s \in \{1, 2, \ldots, n\}$. Then we put

$$\vec{u}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm}, 0, \ldots, 0, -\mu_s, 0, \ldots, 0).$$

The support of the vector $\vec{u}_s$ belongs to $\{1, 2, \ldots, m\} \cup \{i_s\}$. Since the Hamming code $\mathbb{H}$ forms a null space of parity check matrix $H$, we have $\vec{u}_s \in \mathbb{H}$. Thus, based on vectors of length $m$ from the set $\Lambda$, we constructed a family of components $R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \ldots, R_{i_t} + \vec{u}_t$ of the $q$-ary Hamming code $\mathbb{H}$ of length $n = (q^m - 1)/(q - 1)$.

Etzion and Vardy [3] used a set of linearly independent columns of the parity-check matrix of the Hamming code for constructing the full-rank binary 1-perfect codes.

Next, we show that the family of components from Example 1 is admissible.

**Proposition 1.**

Let $s \in \{1, 2, \ldots, t\}$. Then, $\vec{u}_s \notin R_{i_s}$.

**Proof.** From the construction it follows that the support of the vector $\vec{u}_s = (u_1, u_2, \ldots, u_n)$ belongs to $\{1, 2, \ldots, m\} \cup \{i_s\}$ and column $\vec{h}_{i_s}$ is a linear combination of three or more columns from the set $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}$. Since the columns $\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m$ are linearly independent, it follows that for $x \in \{1, 2, \ldots, m\}$ no linear combination of columns $\vec{h}_{i_s}$ and $\vec{h}_x$ does not belong to $\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\} \setminus \{\vec{h}_x\}$. Thus from Theorem 1 we have that $\vec{u}_s \notin R_{i_s}$. The proposition is proved.

**Theorem 3.**

The family of the component $R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \ldots, R_{i_t} + \vec{u}_t$ of the $q$-ary Hamming code $\mathbb{H}$ of length $n$ is admissible.

**Proof.** Let $r, s \in \{1, 2, \ldots, t\}$, $r \neq s$. Then, we show that

$$(R_{i_r} + \vec{u}_r) \cap (R_{i_s} + \vec{u}_s) = \emptyset. \quad (2)$$

In order to satisfy the equality [2] it suffices to show that $\vec{u}_r - \vec{u}_s \notin R_{i_r} + R_{i_s}$. We consider several cases.
1. Let \( i_r = i_s \).

Then, the vectors \( \vec{u}_r \) and \( \vec{u}_s \) are linearly dependent. From the construction of vectors \( \vec{u}_r \) and \( \vec{u}_s \), we obtain that the weight of vector \( \vec{u}_r - \vec{u}_s \) is greater than or equal to six. Hence, arguing as in the proof of Proposition 1, we obtain that \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} \).

2. Let \( i_r \neq i_s \).

Then, we show that \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} + \mathbb{R}_{i_s} \). By Theorem 2, it suffices to show that the support of vector \( \vec{u}_r - \vec{u}_s \) contains a point \( x \) not lying on the line \( l_{i_r i_s} \) and such that no other point (distinct from the points \( i_r, i_s, x \)) of the support does not belong to the plane \( P_{i_r i_s x} \).

2.1. Let the columns \( \vec{h}_{i_r} \) and \( \vec{h}_{i_s} \) be such that as a result of any linear combination of these columns, one obtains a column, which can be represented linear combination of three or more columns from the set \( \{ \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \} \).

The support of vector \( \vec{u}_r - \vec{u}_s \) belongs to \( \{ 1, 2, \ldots, m \} \cup \{ i_r \} \cup \{ i_s \} \). Consequently, the point \( x \) belong to \( \{ 1, 2, \ldots, m \} \). Since the columns \( \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \) are linearly independent, it is obvious that none of the columns of the set \( \{ \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \} \setminus \{ \vec{h}_x \} \) is not a linear combination of the columns \( \vec{h}_{i_r}, \vec{h}_{i_s}, \vec{h}_x \). Consequently, \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} + \mathbb{R}_{i_s} \).

2.2. Let the columns \( \vec{h}_{i_r} \) and \( \vec{h}_{i_s} \) be such that as a result of linear combination of these columns, one obtains the column \( \vec{h} \) which can be represented linear combination of two columns \( \vec{h}_{y'}, \vec{h}_{y''} \) from the set \( \{ \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \} \).

2.2.1. If at least one of the points \( y', y'' \) do not belong to the support of vector \( \vec{u}_r - \vec{u}_s \), then \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} + \mathbb{R}_{i_s} \).

2.2.2. Let \( y', y'' \) be the points belonging to the support of vector \( \vec{u}_r - \vec{u}_s \). Then, we choose a point in the support of the vector \( \vec{u}_r - \vec{u}_s \) which is distinct from the points \( i_r, i_s, y', y'' \). Such a choice is possible by the construction of vectors \( \vec{u}_r, \vec{u}_s \). The support of the vector \( \vec{u}_r - \vec{u}_s \) belongs to \( \{ 1, 2, \ldots, m \} \cup \{ i_r \} \cup \{ i_s \} \). Hence, the points \( x, y', y'' \) belong to \( \{ 1, 2, \ldots, m \} \) and are not collinear. Consider any other linear combination of columns \( \vec{h}_{i_r}, \vec{h}_{i_s} \) as a result of which, we obtain a column that is linearly independent from the column \( \vec{h} \). Since the distance between the vectors \( \vec{h}_r \) and \( \vec{h}_s \) greater than or equal to five and columns \( \vec{h}_r, \vec{h}_2, \ldots, \vec{h}_m \) are linearly independent, it follows that the distance between the columns \( \vec{h}_s \) and \( \vec{h}_s \) is also greater than or equal to five. Consequently, as a result of the linear combination, we obtain a column which is a linear combination of three or more columns from the set \( \{ \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \} \). Thus, \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} + \mathbb{R}_{i_s} \).

2.3. Let the columns \( \vec{h}_{i_r} \) and \( \vec{h}_{i_s} \) be such that as a result of a linear combination of these columns, we obtain the column from the set \( \{ \vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m \} \). Then the same arguments as in the previous case, we obtain that \( \vec{u}_r - \vec{u}_s \notin \mathbb{R}_{i_r} + \mathbb{R}_{i_s} \). The theorem is proved.
4 Examples 2 and 3

Next, we give Examples 2 and 3. The family of components in these examples are constructed in exactly the same way as in Example 1.

Example 2.

Let \((\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_3^m\) bet a code containing \(t\) nonzero vectors \(\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\), the weight of each of them be greater than or equal to three. Let also the distance between any two distinct vectors in \(\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}\) be greater than or equal to three. Then, the set \(\Lambda\) corresponds to admissible family of component of the ternary Hamming code of length \(n = (3^m - 1)/2\).

Example 3.

In the parity-check matrix \(H\) of the binary Hamming code \(H\) of length \(n = 2^m - 1\), we choose \(m\) linearly independent columns. We assume that we have chosen the columns \(\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\). In the parity-check matrix \(H\), we also choose \(k\) columns which are linear combination of two columns from \(\{\vec{h}_1, \vec{h}_2, \ldots, \vec{h}_m\}\). We assume that these columns are the columns \(\vec{h}_{m+1}, \vec{h}_{m+2}, \ldots, \vec{h}_{m+k}\). Let \((\Lambda \cup \{\vec{0}\}) \subset \mathbb{F}_3^{m+k}\) be a code contains \(t\) nonzero vectors \(\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\), the weight of each of them be greater than or equal to \(3k + 3\). Let the distance between any two distinct vectors in \(\Lambda = \{\vec{\lambda}_1, \vec{\lambda}_2, \ldots, \vec{\lambda}_t\}\) be greater than or equal to \(3k + 3\). With each vector \(\vec{\lambda}_s = (\lambda_{s1}, \lambda_{s2}, \ldots, \lambda_{sm+k})\) of length \(m + k\) same way as in Example 1 we associate a vector \(\vec{u}_s\) of length \(n = 2^m - 1\), where \(s \in \{1, \ldots, t\}\). Then, the set \(\Lambda\) corresponds to admissible family of components of the binary Hamming code of length \(n = 2^m - 1\).

The proof of the fact that the families of components in Examples 2 and 3 are admissible is similar to the proof of Theorem 3. In the case of ternary codes, we should take in account the features of the Galois field \(\mathbb{F}_3\). Let \(\vec{x}, \vec{y} \in \mathbb{F}_3^m\). Then, it is obvious that if \(d(\vec{x}, \vec{y}) = m\) and vectors \(\vec{x}, \vec{y}\) does not contain zero components, then they are linearly dependent.

5 Embedding in perfect code

Next, we prove a theorem on the embeddability.

By \(\vec{e}_i\) we denote a vector of length \(n\), where \(i\)-th component is equal to 1 and other components are equal to 0.

Let
\[
\mathcal{T} = \left( \mathbb{H} \setminus \bigcup_{s=1}^{t} (R_{i_s} + \vec{u}_s) \right) \cup \left( \bigcup_{s=1}^{t} (R_{i_s} + \vec{u}_s + \mu_s \cdot \vec{e}_s) \right) .
\]

By Theorem 3 the family of component \(R_{i_1} + \vec{u}_1, R_{i_2} + \vec{u}_2, \ldots, R_{i_t} + \vec{u}_t\) of \(q\)-ary Hamming code \(\mathbb{H}\) is admissible (similar theorems on the admissibility of the family component are
valid for the codes from Examples 2 and 3). Consequently, the set $T$ is $q$-ary 1-perfect code of length $n$, see [3, 4]. By Proposition 1, the code $T$ contains the zero vector.

**Theorem 4.**

Every $q$-ary code of length $m$ and minimum distance 5 (for $q = 3$ the minimum distance is 3) can be embedded in a $q$-ary 1-perfect code of length $n = (q^m - 1)/(q - 1)$. Every binary code of length $m + k$ and minimum distance $3k + 3$ can be embedded in a binary 1-perfect code of length $n = 2^{m - 1}$.

**Proof.** From the construction of the admissible family of component of $q$-ary code $H$ in Example 1 and formula 3, it follows that every $q$-ary code $\Lambda \cup \{\vec{0}\}$ of length $m$ and minimum distance 5 can be embedded (in the strong sense) in the $q$-ary 1-perfect code $T$ of length $n = (q^m - 1)/(q - 1)$.

From the construction of the admissible family of component of ternary code $H$ in Example 2 and Formula 3 it follows that every ternary code $\Lambda \cup \{\vec{0}\}$ of length $m$ and minimum distance 3 can be embedded (in the strong sense) in a ternary 1-perfect code $T$ of length $n = (3^m - 1)/2$.

From the construction of admissible family of component of binary code $H$ in Example 3 and Formula 3 it follows that every binary code $\Lambda \cup \{\vec{0}\}$ of length $m + k$ and minimum distance $3k + 3$ can be embedded in a binary 1-perfect code $T$ of length $n = 2^{m - 1}$, $k \geq 0$. In the case of binary codes of Example 3 the embedding is not strong. The theorem is proved.

**References**

[1] **Romanov A. M.** On partitions of $q$-ary Hamming codes into disjoint components. // Discrete Analysis and Operations Research. — 2004. Ser. 1, — V. 11, N 3. — P. 80–87.

[2] **Avgustinovich S. V., Krotov D. S.** Embedding in a perfect code // Journal of Combinatorial Designs. — 2009. — V. 17, N 5. — P. 419-423.

[3] **Etzion T., Vardy A.** Perfect binary codes: Constructions, properties and enumeration // IEEE Trans. Inf. Theory. — 1994. — V. 40, N 3. — P. 754-763.

[4] **Phelps K. T., Villanueva M.** Ranks of $q$-ary 1-perfect codes // Designs, Codes and Cryptogr. — 2002. — V. 27, N 1–2. — P. 139–144.

[5] **Romanov A. M.** Survey of Methods for Construction of Nonlinear Perfect Binary Codes // Journal of Applied and Industrial Mathematics. — 2008. — V. 2, N 2. — P. 252 — 269.