S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 17, стр. 1165–1182 (2020) УДК 519.72
DOI 10.33048/semi.2020.17.088 MSC 94B60

LINEAR PERFECT CODES OF INFINITE LENGTH OVER INFINITE FIELDS

S.A.MALYUGIN

Abstract. Let F be a countable infinite field. Consider the space $F^{\mathbb{N}_0}$ of all sequences $u=(u_1,u_2,\dots)$, where $u_i\in F$ and $u_i=0$ except a finite set of indices $i\in\mathbb{N}$. A perfect F-valued code $C\subset F^{\mathbb{N}_0}$ of infinite length with Hamming distance 3 can be defined in a standard way. For each $m\in\mathbb{N}$ ($m\geqslant 2$), we define a Hamming code $H_F^{(m)}$ using a checking matrix with m rows. Also, we define one more Hamming code $H_F^{(\omega)}$ using a checking matrix with countable rows. Then we prove (Theorem 1) that all these Hamming codes are nonequivalent. In spite of this fact, Theorem 2 asserts that any perfect linear code $C\subset F^{\mathbb{N}_0}$ is affinely equivalent to one of the Hamming codes $H_F^{(m)}$, $m=2,3,\dots,\omega$. For the code $H_F^{(\omega)}$, we construct a continuum of nonequivalent checking matrices having countable rows (Theorem 4). Also, for this code, a countable family of nonequivalent checking matrices with columns having finite supports is constructed. Further, Theorem 8 asserts that a checking matrix with countable rows and columns with finite supports has a minimal checking submatrix.

Keywords: perfect F-valued code, code of infinite length, checking matrix, complete system of triples

1. The Main Definitions

Consider an arbitrary infinite countable field F. In contrast to finite fields, we have unlimited possibilities for choosing the base field F. For example, as such a field, we can consider the field of rationals, the field of algebraic numbers, the algebraic closure of a finite field, etc.

Malyugin, S.A., Linear perfect codes of infinite length over infinite fields.

The work of the author was carried out in the framework of the State Contract of the Sobolev (Project 0314-2019-0017).

Recevied December, 11, 2019, published August, 24, 2020.

Denote by $F^{\mathbb{N}_0}$ the set whose elements are all possible infinite sequences $u=(u_1,u_2,\dots)$, where $u_i{\in}F$ and all $u_i=0$ but a finite set of indices $i\in\mathbb{N}$ (the index 0 after $\mathbb{N}$ means that we consider only vectors from $F^{\mathbb{N}}$ having finite supports). The set $F^{\mathbb{N}_0}$ is an infinite-dimensional vector space over F. The standard basis of this space is formed by the vectors with the ith coordinate 1, $e_i=(0,\dots,0,\underset{i}{1},0,\dots)$. The set of the indices i for which $u_i{\neq}0$ is called the *support* of the vector $u\in F_q^{\mathbb{N}_0}$ and denoted by $[u]$. The number of nonzero coordinates of u is called its *weight* and denoted by $|u|$. The *Hamming distance* between vectors $u,v\in F^{\mathbb{N}_0}$ is defined as $|u-v|$.

Fix a natural number $r\in\mathbb{N}$.

Definition 1. *A subset C in $F^{\mathbb{N}_0}$ is called an r-perfect F-valued code* (*with distance $d=2r{+}1$*) *if all balls of radius r* (*in the Hamming metric*) *centered at C are pairwise disjoint and their union covers the space $F^{\mathbb{N}_0}$.*

A perfect code is called *linear* if it is a linear subspace in $F^{\mathbb{N}_0}$.

For any perfect code $C\subset F^{\mathbb{N}_0}$, denote by $L_d(C)$ the set of all vectors in C with weight d.

Lemma 1. *Every linear perfect code $C\subset F^{\mathbb{N}_0}$ is the linear span of $L_d(C)$.*

The proof of this lemma is omitted since it is differs insignificantly from the proof of Lemma 1 in [4].

Let H be any proper linear subspace in $F^{\mathbb{N}_0}$. Consider the matrix $B=(b_{i,j})_{i=1}^{n}{}_{j=1}^{\infty}$ consisting of n rows and infinitely many columns (the case $n=\infty$ is not excluded).

Definition 2. *We say that a matrix B is a checking matrix for a proper subspace $H\subset F^{\mathbb{N}_0}$ if $u=(u_1,u_2,\dots)\in H$ if and only if $\sum\limits_{j\in\mathbb{N}} b_{i,j}u_j=0$ for all $i=1,\dots,n$.*

Denote by $(F^{\mathbb{N}_0})^*$ the space of all linear functionals on $F^{\mathbb{N}_0}$. For every linear functional $f^*\in(F^{\mathbb{N}_0})^*$, there exists a unique vector $f=(f_1,f_2,\dots)\in F^{\mathbb{N}}$ such that, for every $u=(u_1,u_2,\dots)\in F^{\mathbb{N}_0}$, we have $f^*(u)=\langle f,u\rangle=\sum\limits_{k\in\mathbb{N}} f_ku_k$ (the sum contains only finitely many nonzero summands); moreover, $f_k=f^*(e_k)$ $(k\in\mathbb{N})$ (this fact is called the Riesz representation theorem in functional analysis). The kernel of the linear functional f^* will be denoted by $\ker f^*=\{u\in F^{\mathbb{N}_0}:f^*(u)=0\}$.

Lemma 2. (about separability). *Let H be a proper subspace in $F^{\mathbb{N}_0}$ and let $v_0\in F^{\mathbb{N}_0}\setminus H$. There exists a linear functional $f^*\in(F^{\mathbb{N}_0})^*$ such that $f(v_0)=1$ and $H\subseteq\ker f^*$.*

Proof. Let $v_1,v_2,\dots$ be a finite or countable basis of H. Since $v_0\notin H$, all the vectors $v_0,v_1,\dots$ are linearly independent. Complement the family $\{v_0,v_1,\dots\}$ to a basis of the whole space $F^{\mathbb{N}_0}$[1] by adding to it a finite or countable set of vectors $\{w_1,w_2,\dots\}$. Put $f^*(v_0)=1$ and $f^*(v_k)=0=f^*(w_k)$ $(k\in\mathbb{N})$. Any vector $u\in F^{\mathbb{N}_0}$ decomposes in this basis, i.e.,

$$u=u_0v_0+u_1v_1+\dots+u_1'w_1+u_2'w_2+\dots. \tag{1}$$

[1] Henceforth, by a basis we mean a Hamel basis, i.e., it consists of linearly independent vectors and its linear span coincides with the whole space

By the definition of a basis, this decomposition contains only finitely many nonzero coordinates $u_0, u_1, \dots, u_1', u_2' \dots$. By definition, we put $f^*(u) = u_0 f^*(v_0) + u_1 f^*(v_1) + \dots = u_0$. If $u = v_0$ then in (1) $u_0 = 1$ and all the remaining coordinates are zero i.e., $f^*(v_0) = 1$. If $u \in H$ then all the coordinates u_0, u_1', $u_2', \dots$ are zero in (1); therefore, $f^*(u) = 0$. That is, $H \subseteq \ker f^*$. □

Lemma 3. *Any proper linear subspace $H \subset F^{\mathbb{N}_0}$ has a checking matrix B consisting of finitely or countably many independent rows.*

Proof. Since the whole space $F^{\mathbb{N}_0}$ is countable, we can enumerate all vectors not lying in H into one sequence; i.e., $F^{\mathbb{N}_0} \setminus H = \{w_1, w_2, \dots\}$. For each w_i, choose a linear functional f_i^* such that $f_i^*(w_i) = 1$ and $H \subset \ker f_i^*$. For each functional f_i^*, there exists a vector $f_i \in F^{\mathbb{N}}$ representing it; namely, $f_i^*(u) = \langle f_i, u \rangle$ $(u \in F^{\mathbb{N}_0})$. For every $w_i \notin H$, we have $w_i \notin \ker f_i^*$; therefore, $\bigcap\limits_{i \in \mathbb{N}} \ker f_i^* = H$. This means that $u \in H$ if and only if $\langle f_i, u \rangle = 0$ for all $i \in \mathbb{N}$. Writing down each vector f_i by a row $f_i = (a_{i,1}, a_{i,2}, \dots)$ and collecting the rows into a matrix $B' = (a_{i,j})_{i=1}^{\infty}{}_{j=1}^{\infty}$, we obtain a checking matrix for H consisting of infinitely many rows. It only remains to separate a maximal collection of linearly independent rows in the set of all rows of B' and remove all rows depending linearly on this basis from B'. The so-obtained shortened matrix B is a desired one. □

Thus, we have proved in particular that any linear r-perfect code $C \subset F^{\mathbb{N}_0}$ has at least one checking matrix. Let us now formulate the condition that C is an r-perfect code in terms of checking matrices. Denote by $\vec{b}_j = \{b_{i,j}\}_{i=1}^{n}$ the jth column of the matrix $B = (b_{i,j})_{i=1}^{n}{}_{j=1}^{\infty}$.

Lemma 4. *Let $B = (b_{i,j})_{i=1}^{n}{}_{j=1}^{\infty}$ be a checking matrix for a proper subspace $C \subset F^{\mathbb{N}_0}$. Then C is an r-perfect code for some $r \in \mathbb{N}$ if and only if*

(1) *any $2r$ columns $\vec{b}_{j_1}, \dots, \vec{b}_{j_{2r}}$ in B are linearly independent;*

(2) *for any $r+1$ different columns $\vec{b}_{j_1}, \dots, \vec{b}_{j_{r+1}}$ and any numbers $u_1, \dots, u_{r+1} \in F \setminus \{0\}$, there exists a (unique) collection of columns $\vec{b}_{k_1}, \dots, \vec{b}_{k_r}$ and numbers $v_1, \dots, v_r \in F \setminus \{0\}$ such that*

$$\sum_{m=1}^{r+1} u_m \vec{b}_{j_m} + \sum_{m=1}^{r} v_m \vec{b}_{k_m} = \vec{0}.$$

Proof. The necessity of conditions (1) and (2) is obvious. Prove sufficiency. Condition (1) is equivalent to the assertion that the weight of the nonzero vectors of an r-perfect code C cannot be less than $d = 2r + 1$. Condition (2) means that every vector $\sum\limits_{m=1}^{r+1} u_m e_{j_m}$ of weight $r+1$ is at the Hamming distance r from the (unique) nonzero vector $\sum\limits_{m=1}^{r+1} u_m e_{j_m} + \sum\limits_{m=1}^{r} v_m e_{k_m}$ in C. Starting from this, we prove that any vector $w \in F^{\mathbb{N}_0}$ is at the Hamming distance at most r from some vector in C. This is proved by induction on the weight $|w|$. If $|w| \leqslant r$ then w is at distance at most r from the zero vector $0 \in C$. Assume that $|w| = n > r$ and $w = \sum\limits_{m=1}^{n} w_m e_{j_m}$. It follows from (2) that the vector $\sum\limits_{m=1}^{r+1} w_m e_{j_m}$ from $F^{\mathbb{N}_0}$ is at distance r from some vector $v = \sum\limits_{m=1}^{r+1} u_m e_{j_m} + \sum\limits_{m=1}^{r} v_m e_{k_m}$ in C. By the induction assumption, the vector $w_1 = -\sum\limits_{m=1}^{r} v_m e_{k_m} + \sum\limits_{m=r+2}^{n} w_m e_{j_m}$ of weight $< n$ is at distance at most r from some vector $v_1 \in C$. Then the vector $w = v + w_1$ is at distance at most r from the vector $v + v_1 \in C$. □

Consider two infinite countable sets M_1 and M_2 and two infinite countable fields F_1 and F_2. Refer as an *isometry* of the spaces $F_1^{M_{1,0}}$ and $F_2^{M_{2,0}}$ to a one-to-one mapping $A : F_1^{M_{1,0}} \to F_2^{M_{2,0}}$ preserving the Hamming distance. In the case $F_1 = F_2 = F$, the isometry A that is an affine mapping is called an *affine isometry.*

Definition 3. *Two r-perfect codes $C_1 \subset F_1^{M_{1,0}}$, $C_2 \subset F_2^{M_{2,0}}$ are called equivalent if there exists an isometry A of $F_1^{M_{1,0}}$ onto $F_2^{M_{2,0}}$ such that $A(C_1) = C_2$. Two r-perfect codes $C_1 \subset F^{M_{1,0}}$, $C_2 \subset F^{M_{2,0}}$ are called affinely equivalent if there exists an affine isometry A of $F^{M_{1,0}}$ onto $F^{M_{2,0}}$ such that $A(C_1) = C_2$.*

Consider any isometry $A : F_1^{M_{1,0}} \to F_2^{M_{2,0}}$. The image of zero $A(0) = v$ is a finite vector in $F_2^{M_{2,0}}$. Consider the isometry $A_0(u) = A(u) - v$ ($u \in F_1^{M_{1,0}}$). This isometry takes 0 to 0; therefore, it preserves the weights of all vectors. In particular, for every index $\alpha \in M_1$, $A_0(xe_\alpha) = a_\alpha(x)e_{\pi(\alpha)}$. If $x' \neq x$, $x, x' \in F_1 \setminus \{0\}$ then $A_0(x'e_\alpha) = a_\alpha(x')e_{\pi'(\alpha)}$. Obviously, $\pi(\alpha) = \pi'(\alpha)$; otherwise, A_0 is not an isometry. Moreover, $a_\alpha(x) \neq a_\alpha(x')$ for the same reason. Since the inverse mapping A_0^{-1} is also an isometry, a_α maps the field F_1 onto F_2 and $a_\alpha(0) = 0$. In all other respects, a_α can be an absolutely arbitrary bijective mappings of $F_1 \setminus \{0\}$ onto $F_2 \setminus \{0\}$. Returning to the initial isometry $A(u) = A_0(u) + v$, we obtain its general form

$$A\left(\sum_{\alpha\in M_1} u_\alpha e_\alpha\right) = \sum_{\alpha\in M_1} b_\alpha(u_\alpha)e_{\pi(\alpha)} = \left(\sum_{\beta\in M_2} b_{\pi^{-1}(\beta)}(u_{\pi^{-1}(\beta)})e_\beta\right) + v, \qquad (2)$$

where $\pi : M_1 \to M_2$ is any bijective mapping from M_1 onto M_2, and, for every $\alpha \in M_1$, b_α, is an arbitrary bijective mapping of F_1 onto F_2; moreover, $b_\alpha(0) = 0$ for all $\alpha \in M_1$ but some finitely many elements in $\pi^{-1}([v])$. Since we consider only finite vectors, all sums in (2) are finite.

Any affine isomorphism $A : F^{M_{1,0}} \to F^{M_{2,0}}$ has the form $A(u) = A_0(u) + v$ ($u \in F^{M_{1,0}}$), where $v \in F^{M_{2,0}}$ and A_0 is a linear isomorphism of $F^{M_{1,0}}$ onto $F^{M_{2,0}}$ preserving the Hamming distance. Since A_0 preserves the weights of vectors, for any basis vector e_α, we have $A_0(e_\alpha) = y_\alpha e_{\pi(\alpha)}$, where $y_\alpha \in F \setminus \{0\}$ and $\pi : M_1 \to M_2$ is a bijective mapping from M_1 onto M_2. The general form of this mapping is as follows:

$$A\left(\sum_{\alpha\in M_1} x_\alpha e_\alpha\right) = \sum_{\alpha\in M_1} (x_\alpha y_\alpha + a_{\pi(\alpha)})e_{\pi(\alpha)} = \sum_{\beta\in M_2} (x_{\pi^{-1}(\beta)}y_{\pi^{-1}(\beta)} + v_\beta)e_\beta. \quad (3)$$

In the present article, we will not study r-perfect codes for $r > 1$. Therefore, henceforth, we assume that $r = 1$.

2. The Construction of Linear 1-Perfect Codes of Infinite Length

Before starting to construct linear 1-perfect codes, we must choose the index set. The most convenient index set for codes over infinite fields is the set of transfinite numbers (ordinals). All necessary information from the theory of ordinals can be found in [2]. The symbol ω traditionally designates the first infinite transfinite number. Denote by N_1 the set of all transfinite numbers less than ω, i.e., $N_1 = \{\alpha : \alpha < \omega\} = \{0, 1, 2, \dots\} = \mathbb{N} \cup \{0\}$. In fact, N_1 is the set of all naturals including 0. We will be interested only in transfinite numbers $\alpha < \omega^2 = \omega \cdot \omega$. Each such number α is uniquely representable as $\alpha = m\omega + n$ $(m, n \in \mathbb{N} \cup \{0\})$. Moreover, $\alpha < \alpha' = m'\omega + n'$ if and only if either $m < m'$ or $m = m'$ and $n < n'$. Consequently, the totally ordered set $N_\omega = \{\alpha : \alpha < \omega^2\}$ is order isomorphic to the set of all pairs $(m, n) \in (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$ with lexicographic order.

On the index set N_1, we will construct the first linear perfect code. Enumerate all elements of the field F into one sequence $F = \{a_1, a_2, a_3, \dots\}$, $a_1 = 0$, $a_2 = 1$. Consider the following checking matrix

$$D_1 = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & \cdot \end{pmatrix}. \tag{4}$$

The column of the checking matrix (4) with number $i > 0$ has the form $\begin{pmatrix} a_i \\ 1 \end{pmatrix}$, and for $i = 0$ it has the form $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Henceforth, we denote the ith column of the checking matrix by $\vec{i}$. In fact, D_1 contains all two-dimensional columns for which the last nonzero element is equal to 1.

Analogously, for each $m \in \mathbb{N}$, $m\omega = \underbrace{\omega + \dots + \omega}_{m}$ and $N_m = \{\alpha : \alpha < m\omega\}$, define the checking matrix

$$D_m = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & 0 & 1 & 0 & 1 & a_3 & \cdot & \cdot & 0 & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & 0 & 0 & 1 & 1 & 0 & \cdot & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & \cdot & 0 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 1 & \cdot \end{pmatrix}, \tag{5}$$

consisting of all $(m + 1)$-dimensional columns $\vec{\alpha}$ in $F^{m+1} \setminus \{0\}$ whose last nonzero coordinate is equal to 1.

For the set of indices $N_\omega = \{\alpha : \alpha < \omega^2\}$, define the last checking matrix

$$D_\omega = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & 0 & 1 & 0 & 1 & a_3 & \cdot & 0 & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & 0 & 0 & 1 & 1 & 0 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & 1 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \tag{6}$$

where the columns $\vec{\alpha}$ of the matrix D_ω range over all nonzero infinite columns in $F^{\mathbb{N}_0}$ whose last nonzero coordinate is equal to 1.

For each $m = 1, \dots, m, \dots, \omega$, define the linear code $H_F^{(m)}$ as the set of all finite vectors $u = (u_\alpha)_{\alpha \in N_m} \in F^{N_m}$, for which

$$\sum_{\alpha \in N_m} u_\alpha \vec{\alpha} = 0, \tag{7}$$

For $r = 1$, item (1) of Lemma 4 states that any two columns of a checking matrix of a 1-perfect code must be linearly independent, and item (2) means that, for any two columns $\vec{\alpha}$ and $\vec{\beta}$ of a checking matrix of a 1-perfect code and any two numbers $s, t \in F \setminus \{0\}$, there exists a column $\vec{\gamma}$ and a number $u \in F \setminus \{0\}$ such that $u\vec{\gamma} = s\vec{\alpha} + t\vec{\beta}$. This immediately implies matrices (4),(5),(6) are checking matrices for linear 1-perfect codes $H_F^{(1)}$,..., $H_F^{(m)}$,...,$H_F^{(\omega)}$ respectively.

Following a tradition, refer to the codes $H_F^{(1)}$,...,$H_F^{(m)}$,..., $H_F^{(\omega)}$ as the *Hamming codes of infinite length over the infinite field F*. The matrices $D_1, \dots, D_m, \dots, D_\omega$ will be called the *canonical* checking matrices for the codes $H_F^{(1)}$,..., $H_F^{(m)}$,..., $H_F^{(\omega)}$ respectively. Further we will prove that all these codes are not equivalent to each other.

Theorem 1. *For any two infinite countable fields F_1, F_2, the Hamming codes $H_{F_1}^{(m)}$, $H_{F_2}^{(m')}$ are not equivalent to each other for $m' \neq m$.*

Proof. Suppose that two codes $H_{F_1}^{(m)}$ and $H_{F_2}^{(m')}$ are equivalent and an isometry $A : F_1^{N_{m,0}} \to F_2^{N_{m',0}}$ is an equivalence mapping, that is, $A(H_{F_1}^{(m)}) = H_{F_2}^{(m')}$. Since $A(0) = v \in H_{F_2}^{(m')}$, the linearity of the code $H_{F_2}^{(m')}$ implies that $A_0(u) = A(u) - v$ ($u \in F_1^{N_{m,0}}$) is also an equivalence mapping for the codes $H_{F_1}^{(m)}$ and $H_{F_2}^{(m')}$; moreover, $A_0(0) = 0$. Let $m = 1$, $m' > 1$. The columns of the checking matrix (4) are two-dimensional; therefore, any three columns are linearly dependent. Hence, for any three indices $\alpha_1, \alpha_2, \alpha_3 \in N_1$, there exists a vector $u \in H_{F_1}^{(1)}$ with support $[u] = \{\alpha_1, \alpha_2, \alpha_3\}$. In other words, the linear code $H_{F_1}^{(1)}$ has a *complete system of triples*. No other code $H_{F_2}^{(m')}$ for $m' > 1$ has a complete system of triples (the checking matrices (5) and (6) contain three linearly independent columns). Since, in Definition 3 and formula (2), the mapping π maps N_1 onto the whole set $N_{m'}$ bijectively, the image $A_0(H_{F_1}^{(1)})$ must also be a code with a complete system of triples. This contradiction shows that the code $H_{F_1}^{(1)}$ is equivalent for no code $H_{F_2}^{(m')}$ for $m' > 1$ (including $m' = \omega$)

Now, examine the case $1 < m < m'$. Consider any collection of $m + 1$ indices $\alpha_1, \dots, \alpha_{m+1} \in N_m$. The corresponding columns $\vec{\alpha}_1, \dots, \vec{\alpha}_m$ of the checking matrix (6) are linearly dependent. Hence, there exists a nonzero vector $u \in H_{F_1}^{(m)}$ with support $[u] \subset \{\alpha_1, \dots, \alpha_{m+1}\}$. This property fails for the code $H_{F_2}^{(m')}$ because there exist $m + 1$ indices $\alpha'_1, \dots, \alpha'_{m+1} \in N_{m'}$ for which the columns $\vec{\alpha}'_1, \dots, \vec{\alpha}'_{m+1}$ of the checking matrix for $H_{F_2}^{(m')}$ are linearly independent. Therefore, for no code vector $u' \in H_{F_2}^{(m')}$, its support $[u']$ does not belong to the set of indices $\{\alpha'_1, \dots, \alpha'_{m+1}\}$. This property of the code $H_{F_2}^{(m')}$ says that it is not equivalent to the code $H_{F_1}^{(m)}$ (the case $m' = \omega$ is not excluded). □

Remark 1. It is not known whether the codes $H_{F_1}^{(m)}$ and $H_{F_2}^{(m)}$ are equivalent for nonisomorphic infinite countable fields F_1 and F_2.

3. A Classification of Nonequivalent Linear Codes

Theorem 2. *Every linear perfect code $C \subset F^{\mathbb{N}_0}$ is affinely equivalent to one of the codes $H_F^{(1)}$,..., $H_F^{(m)}$,...,$H_F^{(\omega)}$.*

Proof. Let $B = (b_{i,j})_{i=1}^{n}{}_{j=1}^{\infty}$ be a checking matrix for the linear space C. Consider two variants separately:

(1) B consists of finitely many linearly independent rows. Suppose that $n = 1$, i.e., A consists of a single row. If $b_{1,i} = 0$ for some $i \in \mathbb{N}$ then this would imply that the vector e_i of weight 1 belongs to C. Therefore, all elements $b_{1,i} \neq 0$ ($i \in \mathbb{N}$). Then, for $i_1 \neq i_2$, the vector $u = b_{1,i_2}e_{i_1} - b_{1,i_1}e_{i_2}$ of weight 2 must belong to C. That is, the checking matrix B consists of at least two rows. If B contains two linearly dependent columns then C contains a vector of weight 2. Hence, all columns in B are proportional to each other. The linear independence of the rows implies that B contains a nonzero minor

$$\Delta_n = \begin{vmatrix} b_{1,i_1} & \dots & b_{1,i_n} \\ \vdots & \vdots & \vdots \\ b_{n,i_1} & \dots & b_{n,i_n} \end{vmatrix} \neq 0$$

Denote the columns of this minor by $\vec{i_1}, \dots, \vec{i_n}$. Consider an arbitrary nonzero combination of these rows $\alpha = x_1\vec{i_1} + \dots + x_n\vec{i_n}$ in which at least two numbers of $x_1, \dots, x_n$ are nonzero. From $\Delta_n \neq 0$ it follows that the vector $v = x_1e_{i_1} + \dots + x_ne_{i_n}$ does not belong to the code C. There exist $j \in \mathbb{N}$ and $y \in F \setminus \{0\}$ such that the vector $u = x_1e_{i_1} + \dots + x_ne_{i_n} + ye_j \in C$. Assume that $j \in \{i_1, \dots, i_n\}$. Assume without loss of generality that $j = i_1$. Then the nonzero vector $w = (x_1 + y)e_{i_1} + \dots + x_ne_{i_n}$, belonging to C, must be orthogonal to all rows of the checking matrix A; a contradiction to $\Delta_n \neq 0$. Hence, $j \notin \{i_1, \dots, i_n\}$, and the definition of a checking matrix implies that $y\vec{j} + x_1\vec{i_1} + \dots + x_n\vec{i_n} = 0$. Therefore, the column $\vec{j}$ of the checking matrix differs only by a constant factor from an arbitrary linear combination of fixed linearly independent columns $\vec{i_1}, \dots, \vec{i_n}$. We have proved that any nonzero n-dimensional column is proportional to some column in the checking matrix B. If we replace each column in B by the proportional column in which the last nonzero coordinate is 1 then we obtain a new matrix which differs from (5) only be a renumbering of the columns. Consequently, if we multiply the ith coordinate of all the vectors in C by a suitable factor y_i and renumber all coordinates $i \in \mathbb{N}$ with the use of a suitable mapping $\pi : \mathbb{N} \to N_{n-1}$ then, as a result, we obtain the code $H_F^{(n-1)}$. This completely proves the affine equivalence of C and $H_F^{(n-1)}$.

(2) B consists of countably many linearly independent rows. Further we will carry out the following elementary transformations of the matrix B:
(a) a permutation of rows in B;
(b) the replacement of a row $(b_{i_1,j})_{j=1}^{\infty}$ by a linear combination $(x_1b_{i_1,j} + x_2b_{i_2,j})$ ($x_1 \neq 0$);
After applying such operations, the new checking matrix will generate the same code C;
(c) the multiplication of a column by a nonzero element of F;
(d) a renumbering of the columns of the matrix in another order (a renumbering corresponding to some countable transfinite number $\alpha < \omega^2$ is possible);
obviously, after applying operations (c) and (d), the new checking matrix generates another code C', which is affinely equivalent to C.

The matrix B will be transformed by means of induction.

The induction base. Since $e_1 \notin C$, there exists a number $i \in \mathbb{N}$ for which $b_{i,1} \neq 0$. Permuting the rows of the matrix B, we may assume that $b_{1,1} \neq 0$. If

$b_{i,1} \neq 0$ for some row with number $i > 1$ we have then replace it by the row $(b_{i,j} - (b_{i,1}/b_{1,1})b_{1,j})_{j=1}^{\infty}$. After that, divide the first row by $b_{1,1}$. The obtained matrix B_0 generates another code C_0 affinely equivalent to C. If $b_{1,2} = 0$ for all $i > 1$ then the vector $b_{1,2}e_1 - e_2$ of weight 2c must belong to C_0. Therefore, there exists a number $i_1 > 1$ for which $b_{i_1,2} \neq 0$. Moving this row to the second position, we get $a_{2,2} \neq 0$. After that, replace all rows with numbers $i_2 \neq 2$ by the rows $(b_{i_2,j} - (b_{i_2,2}/b_{2,2})b_{2,j})_{j=1}^{\infty}$. After this operation, divide the second row by $b_{2,2}$. As a result, we obtain the following checking matrix B_1:

$$B_1 = \begin{pmatrix} 1 & 0 & b_{1,3} & \cdot & \cdot \\ 0 & 1 & b_{2,3} & \cdot & \cdot \\ 0 & 0 & b_{3,3} & \cdot & \cdot \\ 0 & 0 & b_{4,3} & \cdot & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

It generates another perfect code C_1, which is also affinely equivalent to C. Now, for every $x \in F \setminus \{0\}$, consider the vector $v(x) = xe_1 + e_2$. It must be at Hamming distance 1 from some code vector $xe_1 + e_2 + y(x)e_j$ $j > 2$. Therefore, the column $\vec{j}$ of checking matrix B_1 is a linear combination of the first two columns; namely, $-y(x)\vec{j} = x\vec{1} + \vec{2}$. Multiply the jth column by $-y$, and if $x = 1$ then move it to the third position in B_1. Further, exhausting all possible $x \neq 0, 1$ and moving the corresponding columns of B_1 multiplied by the corresponding numbers $-y(x)$ to the first place, we after countably many such operations, transform B_1 into the following checking matrix:

$$B_\omega = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & b_{1,i_1} & b_{1,i_2} & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & b_{2,i_1} & b_{2,i_2} & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & b_{3,i_1} & b_{3,i_2} & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \tag{8}$$

whose right-hand side lists all columns with numbers $i_1, i_2, \dots$ that have not yet taken part in the processes of the permutation of columns. In this matrix, $a_1 = 0$, $a_2 = 1$, $a_3, \dots$ enumerate all the elements of F. For finishing the base step, from correctness considerations, it is necessary to introduce a numbering of columns such that their numbers form a monotone increasing sequence. As above, enumerate the left-hand block of the checking matrix (8) (which contains only columns with nonzero first two coordinates) by $0, 1, 2, \dots$. The numbers of the right-hand block (with the columns not yet involved in the process of transforming the checking matrix) will now be numbered by transfinite numbers; the columns with old numbers i_k will be given by new transfinite numbers $\omega + i_k$.

The induction step. Suppose that we have already transformed the initial checking matrixc into an $(m+1)$-block matrix of the following form:

$$B_{m\omega} = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & \cdot & 0 & 1 & 0 & 1 & x_3 & \cdot & b_{1,m\omega+i_1} & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & \cdot & 0 & 0 & 1 & 1 & 0 & \cdot & b_{2,m\omega+i_1} & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & b_{3,m\omega+i_1} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & b_{m+1,m\omega+1} & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & b_{m+2,m\omega+1} & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}, \tag{9}$$

generating the code $C_{m\omega}$ affinely equivalent to C. The last block of the matrix (9) contains the columns that are not yet involved in the transformation process. The column with number $\beta = m\omega + i_1$ contains an element $b_{i,\beta} \neq 0$ for some $i > m+1$. Otherwise, this column is proportional to some column from the previous blocks. Permuting the rows of $B_{m\omega}$, we may assume that $i = m+2$. Next, for each number $i_1 \neq i$, subtract from the row with number i_1 the row with number i multiplied by a suitable factor y such that, in the new i_1th row, the coordinate with number $m\omega + i_1$ vanishes. After dividing the column with number $m\omega + i_1$ by $b_{m+2,m\omega+i_1}$, we obtain the matrix

$$B'_{m\omega} = \begin{pmatrix} 1 & 0 & 1 & a_3 & a_4 & \cdot & \cdot & 0 & 1 & 0 & 1 & a_3 & \cdot & 0 & \cdot \\ 0 & 1 & 1 & 1 & 1 & \cdot & \cdot & 0 & 0 & 1 & 1 & 0 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 1 & 1 & 1 & 1 & 1 & \cdot & 0 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & 1 & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 & 0 & 0 & 0 & \cdot & 0 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Assign the new number $m\omega$ to the column in $B'_{m\omega}$ with number $m\omega + i_1$. Now, the columns with numbers $0, 1, \omega, 2\omega, \dots, m\omega$ are basis columns, i.e., the column $\overrightarrow{k\omega}$ has only one nonzero coordinate at the $(k+2)$th position, equal to 1 $(k = 1, \dots, m)$. The obtained matrix $B'_{m\omega}$ is a checking matrix for some code $C'_{m\omega}$ affinely equivalent to C. For any $x_0, x_1, \dots, x_m$, consider the vector $v = x_0 e_0 + x_1 e_1 + x_2 e_\omega + \cdots + x_m e_{(m-1)\omega} + e_{m\omega}$, where at least one number x_i is nonzero. It does not belong to the code $C'_{m\omega}$ since the columns $\vec{0}$,$\vec{1}$, $\vec{\omega}$,…,$\overrightarrow{m\omega}$ are linearly independent. Therefore, there exists a column $\vec{\beta}$ (with number $\beta = \beta(x_0, x_1, \dots, x_m) > m\omega$) and there is a number $y \in F \setminus \{0\}$ such that $v + ye_\beta \in C'_{m\omega}$. Consequently, $-y\vec{\beta} = x_0\vec{0} + x_1\vec{1} + \cdots + x_m\ \overrightarrow{(m-1)\omega} + \overrightarrow{m\omega}$, and hence the column $\vec{\beta}$ is proportional to the column

$$\begin{pmatrix} x_0 \\ x_1 \\ \cdot \\ x_m \\ 1 \end{pmatrix}. \tag{10}$$

Exhausting different collections $x = (x_0, x_1, \dots, x_m)$, we will find all columns proportional to all possible columns of the form (10) in the last block of $B'_{m\omega}$. Move all these columns in turn to the positions after the vector $\overrightarrow{m\omega}$ and assign the new transfinite numbers $m\omega + 1$, $m\omega + 2$,… to them. Moreover, assign the new transfinite numbers $(m+1)\omega + i'_1$, $(m+1)\omega + i'_2$,…, to the remaining unused columns in the rightmost last block, where i'_1, i'_2,… are the old numbers of the unused columns of the initial checking matrix B. As a result of all this, we obtain the matrix $B_{(m+1)\omega}$ differing from matrix (9) only by the fact that we must replace m by $m+1$ everywhere and eliminate from the last block some countably many vectors that were moved to the previous block. Denote the code generated by the checking matrix $B_{(m+1)\omega}$ by $C_{(m+1)\omega}$. It is also affinely equivalent to C. This finishes the induction step.

The final step. In the code $H_F^{(\omega)}$, consider the subcode $\widetilde{H}_F^{(m)}$ consisting of all vectors $u \in H_F^{(\omega)}$ whose supports $[u] \subset N_{m\omega}$. This subcode is obviously affinely equivalent to the Hamming code $H_F^{(m)}$, and also $\widetilde{H}_F^{(m)} \subset \widetilde{H}_F^{(m+1)}$ and $H_F^{(\omega)} = \bigcup\limits_{m\in\mathbb{N}} \widetilde{H}_F^{(m)}$. The previous inductive construction also implies that $\widetilde{H}_F^{(m)} \subset C_{m\omega}$. Denote by N'_m the index set for the code $C_{m\omega}$ constructed in the previous item. Let $A'_{m\omega} : F^{N'_{m,0}} \to F^{\mathbb{N}_0}$ be a linear isometry taking the code $C_{m\omega}$ to C. Denote by $A_{m\omega}$ the restriction of this isometry to the subspace $\widetilde{F}^{N_m} = \{u \in F^{N'_{m,0}} : [u] \subset N_m \subset N'_m\}$. Since, in the previous induction step, only the columns of the checking matrix (30) are rearranged that are located in the rightmost block and the columns of the previous blocks remain unchanged, it follows the mapping $A_{(m+1)\omega}$ is an extension of $A_{m\omega}$. Suppose that A is the union of all the mappings $A_{m\omega}$ ($A = \bigcup\limits_{m\in\mathbb{N}} A_{m\omega}$ in the sense that the union of the graphs of the mappings $A_{m\omega}$ is the graph of A). Note that, at each induction step, the leftmost column is eliminated from the rightmost block (this column has the minimal number, it is then transformed into a column having only one nonzero coordinate, equal to 1, and the new number $m\omega$ is assigned to it). Therefore, each column in the initial checking matrix B will be eliminated at some induction step m. This and the fact that $N_\omega = \bigcup\limits_{m\in\mathbb{N}} N_m$ implies that A is a linear isometry of $F^{N_{\omega,0}}$ onto the whole space $F^{\mathbb{N}_0}$. Since $A_m(\widetilde{H}_F^{(m)}) \subset C$, we have $A(H_F^{(\omega)}) \subseteq C$. Show that the previous inclusion is an equality. Let $v \in C$. The support of $[v]$ is finite; therefore, for sufficiently large m, all columns in the rightmost block of the checking matrix (9) will have numbers in the initial checking matrix B not belonging to the support $[v]$. Therefore, the support of the vector $u = A^{-1}(v) = A_m^{-1}(v)$ must be a subset in N_m. But $A_m^{-1}(v) = A'^{-1}_{m\omega}(v) \in C_{m\omega}$. Consequently, the vector u is orthogonal to the checking matrix $B_{m\omega}$, and hence it must belong to the code $\widetilde{H}_F^{(m)}$. Therefore, $A(u) = v$. The equality $A(H_F^{(\omega)}) = C$ is completely proved. $\square$

Remark 2. For any $m < m'$, consider the subcode $\widetilde{H}_F^{(m)}$ in $H_F^{(m')}$ consisting of all vectors $u \in H_F^{(m')}$ for which the support $[u] \subset N_m \subset N_{m'}$. This subcode is affinely (linearly) equivalent to the code $H_F^{(m)}$, and the proof of Theorem 2 implies that all these codes are embedded into each other so that the following "tower" is formed:

$$\widetilde{H}_F^{(1)} \subset \cdots \subset \widetilde{H}_F^{(m)} \subset \cdots \subset H_F^{(\omega)};$$

moreover, $H_F^{(\omega)} = \bigcup\limits_{m=1}^{\infty} \widetilde{H}_F^{(m)}$.

Remark 3. The structure of the checking matrices (4),(5),(6) shows that the index set N_m of the code $H_F^{(m)}$ can be endowed with the structure of a projective geometry of dimension m. The straight line in this geometry passing through points $\alpha_1, \alpha_2 \in N_m$ is defined as the union of the supports of all vectors u of weight 3 in $H_F^{(m)}$ whose supports $[u]$ contain both points α_1 and α_2. Denote this geometry by $PG_F(m)$. Using these straight lines, we can define projective subspaces of any lesser dimensions in $PG_F(m)$. In particular, in the geometry $PG_F(\omega)$ generated by the code $H_F^{(\omega)}$, one can find finite-dimensional spaces embedded into one another

$$\widetilde{PG}_F(1) \subset \dots \subset \widetilde{PG}_F(m) \subset \dots \subset PG_F(\omega),$$

generated by the subcodes $\widetilde{H}_F^{(m)}$; moreover, $PG_F(\omega) = \bigcup\limits_{m=1}^{\infty} \widetilde{PG}_F(m)$.

4. Some Unusual Properties of the Constructed Codes

The first code $H_F^{(1)}$ possesses a previously unencountered property. As was established in the previous section, it has a complete system of triples, i.e., for any three different indices i_1, i_2, i_3, there exists a vector of weight 3 $u \in H_F^{(1)}$ such that $[u] = \{i_1, i_2, i_3\}$. In the previous works [1, 5, 6], it was proved that the codes over finite fields with a complete system of triples are nonsystematic. But the code $H_F^{(1)}$, being linear, is systematic. The point is that its checking set consists only of the two indices corresponding to the first two columns of the checking matrix (4).

The second unusual property is possessed by the code $H_F^{(\omega)}$ (and also the Hamming code H_q^{∞} over the finite field F_q of [5]).

Theorem 3. *There exists a continual family of linearly independent vectors in F^{N_ω} whose orthogonal complement is the code $H_F^{(\omega)}$.*

Proof. Lemma 3 and the proof of Theorem 2 imply that the dimension of the quotient space $G_\omega = F^{N_{\omega,0}}/H_F^{(\omega)}$ is infinite. Since the number of elements in G_ω (as well as in $H_F^{(\omega)}$) is countable, G_ω has a countable basis $(h_k)_{k\in\mathbb{N}}$. Every linear functional $g^* \in G_\omega^*$ is uniquely defined by its values on this basis, i.e., there exists a one-to-one correspondence between the functionals f^* and the vectors $(f^*(h_1), f^*(h_2), \dots) \in F^{N_\omega}$. The cardinality of F^{N_ω} coincides with the cardinality of the set $\mathbb{N}^{\mathbb{N}}$, which, as is well known is, the continuum (for the finite field F_q consisting of $q \geqslant 2$ elements, this cardinality is also the continuum $q^{\mathbb{N}}$). Therefore, the cardinality of the basis of the space G_ω^*, which is linearly isomorphic to $F^{\mathbb{N}}$, is also the continuum (equal to the cardinality of the set of all real numbers $\mathbb{R}$) (Proving the existence of a basis requires applying the axiom of choice). Fix a basis $\{g_t^*\}_{t\in\mathbb{R}}$ in G_ω. Denote by $P : F^{N_{\omega,0}} \to G_\omega$ the factorization mapping, i.e., for every $u \in F^{N_{\omega,0}}$, $P(u)$ is the coset modulo $H_F^{(\omega)}$ containing u. Consider the family of linear functionals $f_t^* = g_t^* \circ P$. This definition implies that $H_F^{(\omega)} \subset \ker f_t^*$ for every $t \in \mathbb{R}$. Hence, $H_F^{(\omega)} \subseteq \bigcap\limits_{t\in\mathbb{R}} \ker f_t^*$. Lemma 2 (on separability) implies that in fact $H_F^{(\omega)} = \bigcap\limits_{t\in\mathbb{R}} \ker f_t^*$. Now, for every $t \in \mathbb{R}$ consider the vector $f_t = (f_t^*(e_\alpha))_{\alpha\in N_\omega}$ in F^{N_ω} representing the functional f_t^*, i.e., $f_t^*(u) = \langle f_t, u\rangle$ $(u \in F^{N_{\omega,0}})$. Then the matrix whose rows are f_t, where t ranges over $\mathbb{R}$, is a desired family whose orthogonal complement is the code $H_F^{(\omega)}$. □

Of course, Lemma 3 implies that applying such "checking matrices" with continually many rows is superfluous. The point is that Lemma 2 (on separability) immediately implies that any such "checking matrix" of continually many linearly independent rows contains a checking submatrix consisting of countably many linearly independent rows. In this connection, introduce the following definition:

Definition 4. *Two checking matrices B_1 and B_2 of a linear code C are called strongly equivalent if B_2 can be obtained from B_1 by a consecutive application of the following operations:*
(a) *a permutation of the rows of B;*
(b$'$) *the multiplication of a row by a nonzero element of F;*
(c) *the multiplication of a column by a nonzero element of F;*
(d) *a renumbering of the columns of a matrix in another order.*

We excluded the following operation from Definition 4 (see the proof of Theorem 2):

(b) the replacemenent of a row $(b_{i_1,j})_{j=1}^{\infty}$ by a linear combination $(x_1b_{i_1,j}+x_2b_{i_2,j})$ $(x_1\neq 0)$

and replaced it by operation (b$'$). The main motivation for this is that then the permitted operations with the columns coincide with the permitted operations with the rows. Moreover, the proof of Theorem 2 implies that an application of operation (b) gives a chance to reduce any checking matrix of the code $H_F^{(\omega)}$ to the canonical form (6).

Theorem 4. (1) *Any two checking matrices of the code $H_F^{(m)}$ for $m\in\mathbb{N}$ are strongly equivalent to each other.* (2) *The code $H_F^{(\omega)}$ has a continuum of strongly nonequivalent checking matrices consisting of countably many linearly independent rows.*

Proof. Let $m\in\mathbb{N}$. The proof of Theorem 2 implies that every checking matrix of the code $H_F^{(m)}$ must consist of all possible nonzero $(m+1)$-dimensional columns such that no two columns are proportional to each other. Obviously, any two such checking matrices are obtained from each other by some permutation of the rows and their multiplication by nonzero scalars from F (application of operations (a), (b$'$) is not required in this case).

For the code $H_F^{(\omega)}$, consider the canonical checking matrix (6). Consider the binary representation of a real number $t\in(0,1)$, i.e., $t=\sum\limits_{i=1}^{\infty}2^{-k_i}$ $(0<k_1<k_2<\dots)$. Denote these numbers by $k_i=k_i(t)$ $(i\in\mathbb{N})$. Transform matrix (6) as follows: (1) replace the row $(d_{1,j})_{j<\omega^2}$ of the matrix D_ω by the row $(d_{1,j}+d_{2,j})_{j<\omega^2}$; (2) let $F=\{a_0,a_1,a_2,\dots\}$ be an enumeration of the elements of the field F, $a_0=0$, $a_1=1$, furthermore, replace the first k_1 even rows with numbers $i=4,6,\dots,2k_1{+}2$ by the rows $(d_{i,j}+a_3d_{2,j})_{j<\omega^2}$; then replace the next even k_2 rows with numbers $i=2(k_1+2),\dots,2(k_1+k_2)+2$ by the rows $(d_{i,j}+a_4d_{2,j})$,..., replace k_m even rows with numbers $i=2(k_1+\dots+k_{m-1}+2),\dots,2(k_1+\dots+k_m)+2$ by $(d_{i,j}+a_{m+2}d_{2,j})_{j<\omega^2}$; (3) for each $i>1$, replace the ith row $(d_{i,j})_{j<\omega^2}$ of the obtained matrix D'_ω by the row $(d_{i,j}-a_2d_{1,j})_{j<\omega^2}$. After these transformations, the ith column of the new matrix $D_\omega(t)$ looks as follows: $d_{1,j}(t)=d_{1,j}+d_{2,j}$, $d_{2,j}(t)=(1-a_2)d_{2,j}-a_2d_{1,j}$, $d_{i,j}(t)=d_{i,j}+(a_{m+2}-a_2)d_{2,j}-a_2d_{1,j}$, for even $2(k_1+\dots+k_{m-1}+2)\leqslant i\leqslant 2(k_1+\dots+k_m)+2$, $d_{i,j}(t)=d_{i,j}-a_2(d_{1,j}+d_{2,j})$ for all odd $i>1$. Obviously, for every $t\in(0,1)$, the matrix $D_\omega(t)$ consists of linearly independent rows and generates the same code $H_F^{(\omega)}$. Since all columns of the matrix D_ω are finite, for sufficiently large i, we obtain

(1) $d_{i,j}(t)=0$ if $d_{1,j}=d_{2,j}=0$;

(2) $d_{i,j}(t)=-a_2d_{1,j}$ if $d_{2,j}=0$;

(3) $d_{i,j}(t) = (a_{m+2} - a_2)d_{2,j} - a_2 d_{1,j}$, for even $2(k_1 + \cdots + k_{m-1} + 2) \leqslant i \leqslant 2(k_1 + \cdots + k_m) + 2$ and $d_{i,j}(t) = -a_2(d_{1,j} + d_{2,j})$ for odd i.

Further we will be interested only in the columns of the matrix $D_\omega(t)$ for which all coordinates are nonzero. Such are, for example, the first two columns ($j = 1, 2$). Therefore, case (1) is excluded from consideration.

Introduce the following equivalence relation for numbers $t \in (0, 1)$: $t \sim t'$ if and only if $t - t'$ is a binary rational number (i.e., is representable as the sum $\sum_{i=1}^{n} 2^{-k_i}$). We will now prove that if $t \not\sim t'$ then the checking matrices $D_\omega(t)$ and $D_\omega(t')$ are not equivalent. Assume that they are equivalent. Consider the first two columns of $D_\omega(t')$. They possess the following property:

(A) for an infinite set of coordinates i, the parts of the first and second columns with these coordinates are proportional to each other (in this case, for odd i and the proportionality coefficient $(d'_{1,2} + d'_{2,2})/d'_{1,1}$); moreover, the complement to this set of coordinates is also infinite (in this case, this is the set of even i).

Under the equivalence mapping, to these two columns there correspond two columns of $D_\omega(t)$ with numbers j_1, j_2. After multiplying them by nonzero numbers x_1, x_2, some permutation of the coordinates (rows) with their subsequent multiplication by numbers $y_i \neq 0$, we must get the first two columns of the matrix $D_\omega(t')$. Under such transformations, Property (A) is preserved. Therefore, these columns cannot be of type (2) both (they are completely proportional starting from some sufficiently large i). For the same reason, they cannot be of type (3) both if $(d_{1,j_1}/d_{1,j_2}) = (d_{2,j_1}/d_{2,j_2})$. The following variants are left:

(2), (3). The j_1th column has type (2), and the j_2th column has type (3). If π is a permutation of the rows under the action of the supposed equivalence then the $\pi(i)$th position of the first column contains the element $-x_1 y_{\pi(i)} a_2 d_{1,j_1}$. The $\pi(i)$th position of the second column contains the element $-x_2 y_{\pi(i)} a_2(d_{1,j_2} + d_{2,j_2})$ if i was odd and $x_2 y_{\pi(i)}[(a_{m+2} - a_2)d_{2,j_2} - a_2 d_{1,j_2}]$ if i was even (the numbers i are still assumed sufficiently large). We have the proportionality of the large subcolumns with numbers $\pi(i)$, where the i's are odd (with the proportionality coefficient $x_1 d_{1,j_1}/[x_2(d_{1,j_2} + d_{2,j_2})]$). Multiply the second column by $x_1 d_{1,j_1}/[x_2(d_{1,j_2} + d_{2,j_2})]$ and subtract from it the first column. As a result, we obtain the element $x_1 y_{\pi(i)} a_{m+2} d_{1,j_1}/(d_{1,j_2} + d_{2,j_2})$ at position $\pi(i)$ if i was even and zero if i was odd. After that divide the obtained result by the $\pi(i)$th element of the first column; as a result we obtain either zero or $-a_{m+2}/(d_{1,j_2} + d_{2,j_2})$. For different m, all these numbers are distinct, and for each m, this number occurs exactly k_m times (for sufficiently large m). In this way, we can "read" all the k_m's and reconstruct the fractional part of the number $2^{k_m} t$ for sufficiently large m. Since, under the equivalence transformation, the j_1th and j_2th columns of the matrix $D_\omega(t)$ coincide with the first and second rows of $D'_\omega(t)$, we will in fact also "read" the fractional part of the number $2^{k_m} t'$, which must thus coincide with the fractional part of $2^{k_m} t$, which contradicts the fact that $t \not\sim t'$. If we divide $x_1 y_{\pi(i)} a_{m+2} d_{1,j_1}/(d_{1,j_2} + d_{2,j_2})$ by the $\pi(i)$th entry of the second row then, for sufficiently large even i, we also obtain the numbers $x_1 x_2^{-1} d_{1,j_1} a_{m+2}/[a_{m+2}(d_{1,j_2} + d_{2,j_2})d_{2,j_2} - a_2(d_{1,j_2} + d_{2,j_2})^2]$, which are distinct for sufficiently large m. Therefore, also in this case, we can uniquely "read" the factional part of $2^{k_m} t$. We have examined two variants of our actions because it is impossible to determine from the original form of the columns which of them has type (2).

(3), (2). The j_1th column has type (3), and the j_2th column has type (2). This case is analogous to the previous case.

(3), (3). The j_1th and j_2th columns have the same type (3). In this case, we realize the same strategy. For the completeness of the exposition, we give only the final part of the calculations. After multiplying the second column by the proportionality coefficient $x_1x_2^{-1}(d_{1,j_1}+d_{2,j_1})/(d_{1,j_2}+d_{2,j_2})$ and subtracting the first column form it, we obtain a column with zero $\pi(i)$th coordinate if i was odd and $x_1y_{\pi(i)}a_{m+2}(d_{1,j_1}d_{2,j_2}-d_{1,j_2}d_{2,j_1})/(d_{1,j_2}+d_{2,j_2})$ if i was even. Dividing this by the $\pi(i)$th coordinate of the first column, we obtain the numbers

$$a_{m+2}(d_{1,j_1}d_{2,j_2}-d_{1,j_2}d_{2,j_1})/(d_{1,j_2}+d_{2,j_2})[a_{m+2}d_{2,j_1}-a_2(d_{1,j_1}+d_{2,j_1})],$$

which are distinct for $(d_{1,j_1}/d_{1,j_2}) \neq (d_{2,j_1}/d_{2,j_2})$ and sufficiently large even numbers i. The multiplicity of the occurrence if each such number among the coordinates of the obtained column is again k_m, which also in this case makes it possible to "read" the fractional part of the number $2^{k_m}t$ in the obtained column (for sufficiently large m). If we divide the difference by the $\pi(i)$th coordinate of the second column then we obtain the numbers

$$x_1x_2^{-1}a_{m+2}(d_{1,j_1}d_{2,j_2}-d_{1,j_2}d_{2,j_1})/(d_{1,j_2}+d_{2,j_2})[a_{m+2}d_{2,j_2}-a_2(d_{1,j_2}+d_{2,j_2}],$$

which are also distinct for distinct sufficiently large m, which also in this case will lead to the "reading" of the fractional part of $2^{k_m}t$.

Since the cardinality of the set of the numbers equivalent to a given number $t \in (0,1)$ is countable, the cardinality of the equivalence classes in the quotient set $A = (0,1)/\sim$ is also the continuum. Consequently, if we choose one number t_α in each equivalence class $\alpha \in A$ (here we again need to apply the axiom of choice) then we obtain a family of nonequivalent checking matrices $(D_\omega(t_\alpha))_{\alpha\in A}$. □

We have been able to construct a continual family of strongly nonequivalent checking matrices using column with infinite supports. But all columns in the checking matrix (6) are finite. It turns out that if we consider only checking matrices with finite columns then the problem of the nonuniqueness of checking matrices for the code $H_F^{(\omega)}$ does not disappear.

Theorem 5. *There exist infinitely many strongly nonequivalent checking matrices for the code $H_F^{(\omega)}$ consisting of countably many linearly independent rows and column with finite supports.*

Proof. For each $m \in \mathbb{N}$, $m > 1$, construct a checking matrix $D_\omega(m)$ of finite columns whose minimal weight is equal to m. The first two columns of this matrix look as follows:

$$\begin{pmatrix} (1)_m & (0)_m \\ (0)_m & (1)_m \\ 0 & 0 \\ \vdots & \vdots \end{pmatrix}.$$

Here $(x)_m$ stands for the m-dimensional column whose all coordinates are equal to x. We add linear combinations of these two columns to the matrix from the right; as a result, we obtain the matrix

$$\begin{pmatrix} (1)_m & (0)_m & (1)_m & (a_3)_m & (a_4)_m & \cdot \\ (0)_m & (1)_m & (1)_m & (1)_m & (1)_m & \cdot \\ 0 & 0 & 0 & 0 & 0 & \cdot \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

Here $(a_k)_{k\in\mathbb{N}}$, $a_0 = 0$, $a_1 = 1$,. . . is an enumeration of all the elements of the field F. The sense of this construction is that we copy the first block of the checking matrix (6) m times. Obviously, the rank of the first $2m$ rows of this matrix is equal to 2. Extend this matrix adding to it from the right one more column

$$\begin{pmatrix} (1)_m & (0)_m & (1)_m & (a_3)_m & (a_4)_m & \cdot & 1 \\ (0)_m & (1)_m & (1)_m & (1)_m & (1)_m & \cdot & (0)_{2m-1} \\ (0)_m & (0)_m & (0)_m & (0)_m & (0)_m & \cdot & (1)_m \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}. \tag{11}$$

Owing to the unity in the first row and the last column, the rank of the first $2m$ rows has increased by 1 and become equal to 3. Furthermore, like in constructing the checking matrix (6), add linear combinations of the columns of (11) from the right. After that, add the following column from the right:

$$\begin{pmatrix} (1)_m & (0)_m & (1)_m & (a_3)_m & \cdot & 1 & \cdot & 0 \\ (0)_m & (1)_m & (1)_m & (1)_m & \cdot & (0)_{2m-1} & \cdot & 1 \\ (0)_m & (0)_m & (0)_m & (0)_m & \cdot & (1)_m & \cdot & (0)_{3m-2} \\ (0)_m & (0)_m & (0)_m & (0)_m & \cdot & (0)_m & \cdot & (1)_m \\ 0 & 0 & 0 & 0 & \cdot & 0 & \cdot & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

The second row and the last column of this matrix contains 1. The third and the remaining blocks are constructed in the same way, by adding linear combinations of the previously constructed columns from the right. The main principle is that we begin each new block by a column that increases the rank of the previously constructed rows by one. For this it suffices to begin the kth block from a column that contains one unity in the $(k-1)$th row and m more unities in the rows with numbers $km+1, \dots, (k+1)m$. Continuing this process by induction infinitely, construct a matrix $D'_\omega(m)$ with linearly independent rows. For proving this, consider the submatrix consisting of those columns that begin the construction of each block. It looks as follows:

$$\begin{pmatrix} 1 & 0 & 0 & \cdot \\ (0)_{2m-1} & 1 & 0 & \cdot \\ (1)_m & (0)_{3m-2} & 1 & \cdot \\ (0)_m & (1)_m & (0)_{4m-3} & \cdot \\ (0)_m & (0)_m & (1)_m & \cdot \\ \vdots & \vdots & \vdots & \vdots \end{pmatrix}.$$

This submatrix consists of linearly independent rows since all its main minors are equal to 1. Hence, the whole matrix $D'_\omega(m)$ consists of linearly independent rows. Moreover, it possesses the same properties as matrix (6), i.e., the orthogonal complement to it is a code affinely equivalent to $H_F^{(\omega)}$ (by Theorem 2). Permuting the columns of the matrix $D'_\omega(m)$ appropriately, we obtain a checking matrix $D_\omega(m)$ for the code $H_F^{(\omega)}$ for which the minimal weight of the column is equal to m. □

Remark 4. The proof of Theorem 5 shows that it remains valid also for codes of infinite length over finite fields. Consequently, the Hamming codes H_q^∞, $H_2^\infty = H^\infty$, defined in [3, 4, 5], also have infinitely many nonequivalent checking matrices with countably many linearly independent rows.

For establishing a uniqueness theorem for checking matrices of the Hamming code $H_F^{(\omega)}$, introduce the following definitiion:

Definition 5. *A checking matrix B for a linear code H is called minimal if a matrix B' obtained from B by removing one of its rows is already not a checking matrix for H. That is, there exists a finite vector $u \notin H$ orthogonal to all rows in B'.*

Obviously, a minimal checking matrix must have linearly independent rows. This definition and Theorem 4 also imply that the checking matrices with linearly independent rows for the codes $H_F^{(m)}$ $(m = 2, 3, \dots)$ are minimal (due to their uniqueness).

Theorem 6. *If a checking matrix $B = (b_{i,j})_{i,j=1}^\infty$ of the code $H_F^{(\omega)}$ having countably many rows satisfies the following two conditions:*
(A) B is minimal,
(B) all columns in B are finite,
then B is strongly equivalent to the canonical matrix (6).

Proof. Remove the ith row from B. Denote the obtained matrix by $B^{(i)}$. Condition (A) implies that there exists a finite vector $v \notin H_F^{(\omega)}$ orthogonal to the rows of the matrix $B^{(i)}$. The perfectness of the code $H_F^{(\omega)}$ implies the existence of a vector $u \in H_F^{(\omega)}$ such that the weight of the vector $w = u - v$ is equal to 1. It is also orthogonal to all rows in the matrix $B^{(i)}$. Let $w = xe_j$ $(x \in F \setminus \{0\})$. Orthogonality implies that the jth column of $B^{(i)}$ consists only of zeros. Therefore, the jth column of the initial checking matrix B, we have $b_{k,j} = 0$ for all $k \neq i$. That is, for each $i \in \mathbb{N}$, the column with number $j = j(i)$ is a basis column (equal to $b_{i,j}e_{j(i)}$). Since the columns have finite supports (by condition (B)), any other column is a linear combination of these basis columns. Now, using this information and permuting the columns of B appropriately and multiplying them by nonzero constants, we can easily reduce B to the canonical form (6). □

Theorem 5 implies that, after removing condition (A), Theorem 6 ceases to hold. Moreover, the proof of Theorem 4 implies that the nonequivalent checking matrices $D_\omega(t)$ $(t \in (0, 1))$ contain basis columns with the only nonzero entry at the ith coordinate for each $i \geqslant 2$, and they have no column having a unique first coordinate. Therefore, the matrices $D'_\omega(t)$ obtained from $D_\omega(t)$ by removing the first row are minimal, and they are still nonequivalent checking matrices of the code $H_F^{(\omega)}$. Consequently, Theorems 4 and 5 immediately give

Corollary 1. *Conditions (A) and (B) in Theorem* 6 *are independent, and Theorem* 6 *ceases to hold after removing one of these conditions.*

The checking matrices constructed in Theorems 4 and 5 possess the property that, after removing some rows, they become minimal checking matrices. This can create an illusion that this is always the case. The following theorem completely rejects this assumption.

Theorem 7. *There exists a checking matrix of the code $H_F^{(\omega)}$ consisting of countably many linearly independent rows and containing no minimal checking submatrix.*

Proof. Consider the set $\mathcal{P}_\omega$ of all nonzero polynomials with coefficients in F whose coefficient at the higher derivative is equal to 1. This countable set can be enumerated into one sequence $\mathcal{P}_\omega = \{p_j\}_{j=1}^\infty$. In the field F, consider any countable subset $G = \{b_1, b_2, \dots\}$. The matrix $B_G = (p_j(b_i))_{i,j=1}^\infty$ satisfies conditions (1), (2) of Lemma 4 for $r = 1$. Therefore, it is a checking matrix for some perfect linear code H_F^ω equivalent to $H_F^{(\omega)}$. Since every polynomial $p_j(x)$ can have only finitely many roots, all the columns of the matrix B_G are "finite", i.e., contain only finitely many zero coordinates. Every matrix B' obtained from B_G by removing some set of rows and containing infinitely many rows coincides with the matrix $B_{G'}$ for some infinite subset $G' \subset G$. Therefore, it is also a checking matrix for the same code H_F^ω, which proves the absence of a minimal checking submatrix for the matrix B_G. □

Remark 5. The proof of Theorem 7 shows that we can define the code $H_F^{(\omega)}$ differently, without explicitly using checking matrices. Enumerate the elements of the set $\mathcal{P}_\omega$ of all nonzero polynomials of one variable x with coefficients in F for which the coefficient at the higher degree is equal to 1 into one sequence $\mathcal{P}_\omega = \{p_j(x)\}_{j=1}^\infty$. We say that a vector $u = (u_1, u_2, \dots) \in F^{\mathbb{N}_0}$ belongs to the code H_F^ω (equivalent to the code $H_F^{(\omega)}$) if and only if

$$\sum_{j=1}^\infty u_j p_j(x) = 0. \tag{12}$$

(the finiteness of the vector u implies that this sum contains only finitely many nonzero summands). This remark is especially actual due to the fact that, as was shown in Theorems 4, 5, and 7, there appears a great arbitrariness in the definition of a checking matrix for $H_F^{(\omega)}$.

Note that the definition with the use of (12) remains valid also for the codes $H_F^{(m)}$ for any finite $m \in \mathbb{N}$. Instead of a checking matrix, we must consider the set $\mathcal{P}_m = \{p_j(x)\}_{j=1}^\infty$ of all nonzero polynomials of degree at most m (with the coefficient at the higher degree equal to 1).

The following theorem completes the study of the properties of checking matrices for codes of infinite length.

Theorem 8. *Let F be an at most countable field and let H_F be a linear perfect code of infinite length over F. If a checking matrix B for the code H_F consists of countably many linearly independent rows and all its columns are finite then it contains a minimal checking submatrix D of the same code H_F, which is obtained by removing some finite or infinite set of rows from B.*

Proof. Let i_1 be the least number of a row eliminating which from B gives a matrix B_1 containing no zero columns. The matrix B_1 is checking for some subspace L not containing vectors of weight 1. Since the perfect row H_F is a part of the subspace L, we have $L = H_F$ and the matrix B_1 is also checking for H_F. Then act by induction. Let i_1, $i_2, \dots,$ be an increasing sequence of the numbers of rows in B

such that, for each m, i_m is the least number of a row greater than all the previous numbers $i_1, \dots, i_{m-1}$ and such that eliminating all rows with numbers $i_1, \dots, i_m$ from B gives a matrix B_m containing no zero columns. Two variants are possible:

(1) The sequence $i_1, \dots, i_m$ is finite (we exclude the trivial case when the same matrix B is minimal). In this case, everything is proved since the last matrix B_m, obtained by eliminating the rows with numbers $i_1, \dots, i_m$ from B, is minimal.

(2) The sequence $i_1, i_2, \dots$ is infinite. In this case, consider the matrix B_∞ obtained by removing all rows with numbers $i_1, i_2, \dots$ from B.

Firstly, B_∞ consists of a nonempty set of rows. Prove this. Since the first column in B is finite, only finitely many rows in B have nonzero first coordinate. Let $i'_1, \dots, i'_k$ be the numbers of these rows. If $\{i'_1, \dots, i'_k\} \subset \{i_1, i_2, \dots\}$ then, for sufficiently large m, the matrix B_m has zero first column. We get a contradiction.

Secondly, B_∞ contains no zero columns. Suppose that the jth column consists only of zeros. Consider this column with number j in the original number B. Only finitely many rows of this matrix with numbers $i'_1, \dots, i'_k$ have nonzero jth coordinate. Hence, we must have $\{i'_1, \dots, i'_k\} \subset \{i_1, i_2, \dots\}$ and, for sufficiently large m, all rows with numbers $i'_1, \dots, i'_k$ are eliminated from B in constructing the matrix B_m. This makes the jth column of B_m zero. We again have a contradiction.

Thirdly, eliminating any row of the matrix B_∞ gives a matrix having a zero column. Consider the ith row of B_∞ (in the enumeration of the initial matrix B). Consider the least number $i_m > i$. But i_m is the first number for which the matrix B_m obtained from B by eliminating the rows with numbers $i_1, \dots, i_m$ not containing zero columns. This means that $i_m > i > i_{m-1}$ and eliminating the row with number i from B_{m-1} gives a matrix having a zero column with number j. The jth column will be zero all the more after eliminating the ith row from the "lesser" matrix B_∞.

As was shown above, the matrix B_∞ is checking for the initial code H_F, and Theorem 6 in particular implies that B_∞ is strongly equivalent to the canonical checking matrix (6). □

The author is grateful to the referee for a number of remarks concerning the exposition.

References

[1] S.V Avgustinovich, F.I. Solov'eva, *On the nonsystematic perfect binary codes*, Problems Inform. Transmission, **32**:3 (1996), 258–261. MR1441513

[2] A.N. Kolmogorov , S.V. Fomin, *Elements of function theory and functional analysis*, Nauka, Moscow, 1976. (in Russian)

[3] S.A. Malyugin, *Perfect binary codes of infinite length*, J. Appl. Indust. Math., **8**:4 (2017), 552–556. MR3665877

[4] S.A. Malyugin, *Perfect binary codes of infinite length with complete system of triples*, Sib. Elektron. Mat. Izv., **14** (2017), 877–888. MR3703590

[5] S.A. Malyugin, *Systemanic and nonsystematic perfect codes of infinite length over finite fields*, Sib. Elektron. Mat. Izv., **16** (2019), 1732–1751. Zbl 07143079

[6] K.T. Phelps , M.J. LeVan, *Nonsystematic perfect codes*, SIAM J. Discrete Math., **12**:1 (1999), 27–34. MR1666049

Sergey Artem'evich Malyugin
Sobolev Institute of Mathematics,
4, Koptyuga ave.,
Novosibirsk, 630090, Russia
Email address: mal@math.nsc.ru