5. L. A. Sholomov, "On realization of partially defined Boolean functions using circuits of functional elements," Probl. Kibern., Nauka, Moscow, No. 21, 215-226 (1969).
6. K. Prachar, Distribution of Primes [Russian translation], Mir, Moscow (1967).
7. P. Busschbach, "Constructive methods to solve problems of s-surjectivity, conflict resolution, coding in defective memories," Rapport Interne ENST 84 D005 (Dec. 1984).
8. I. I. Dumer, "On correcting defects of fixed multiplicity," Proc. 1988 Int. Workshop on Algebraic and Combinatorial Coding Theory, Sofia (1988), pp. 49-53.
9. I. I. Dumer, "On correcting defects by linear codes," Proc. 3rd Int. Seminar on Information Theory 'Convolutional Codes and Multiuser Communication', Abstracts of Papers [in Russian], Sochi (1987), pp. 76-79.

QUASIPERFECT LINEAR BINARY CODES WITH DISTANCE 4 AND COMPLETE CAPS IN PROJECTIVE GEOMETRY

A. A. Davydov and L. M. Tombak

UDC 621.391.15

We prove that if a linear binary code with distance $d = 4$ is quasiperfect (i.e., has a covering radius 2) and the code length is $N \geq 2^{r-2} + 2$, where r is the number of check symbols, then the check matrix is symmetric in the following sense: the matrix columns may be partitioned into $N/2$ pairs so that the sum of the columns in each pair is constant. As a corollary, we derive all possible values of the length N of a binary linear quasiperfect code with $d = 4$ for $N \geq 2^{r-2} + 1$ and construct all such nonequivalent codes for $N > 2^{r-2} + 2^{r-6}$. The results are extended to complete caps in the projective geometry $PG(r - 1, 2)$.

1. INTRODUCTION. THE MAIN RESULTS

All codes considered in this paper are linear binary block codes. A code with minimum distance $d = 4$ is quasiperfect [1, 2] if the covering radius of the code is 2. The covering radius is understood in the sense of [1, Sec. 6.6, p. 174].

In this paper, we investigate the structure of the check matrix and the possible lengths of quasiperfect codes with $d = 4$. We consider "long" codes of length greater than $N_{max}/2$, where N_{max} is the maximum length of a code with $d = 4$ for given redundancy. As the main result, we show that check matrices of all these codes are symmetric (in the sense defined below). This has enabled us to identify all the possible lengths of such codes and to construct their check matrices from matrices of codes of length $N_{max}/2 + 1$.

All nonequivalent check matrices are listed for codes of length greater than $N_{max}/2 + N_{max}/32$. (We also give without proof all the nonequivalent check matrices for codes of length $N_{max}/2 + N_{max}/32$.) The results are extended to complete caps in projective geometry utilizing the one-to-one correspondence between complete caps and the check matrices considered.

We introduce some notation: $[n, n - r, d]\rho$ code is a code of length n with r check symbols, minimum distance d, covering radius ρ, and cardinality 2^{n-r} (this notation is close to that used in [3]); N is the length of a quasiperfect code with $d = 4$; $[N, N - r, 4]2$ code is a quasiperfect code with $d = 4$.

Proposition 1 [4, 5]. A code has covering radius 2 if and only if any nonzero column not included in the check matrix is representable as the sum of two columns of the matrix.

Conversely, in a code with $d = 4$, no column of the check matrix is a sum of two other matrix columns [1, 2]. Therefore, quasiperfect codes with $d = 4$ are "non-lengthening" in the sense that no column can be added to the check matrix

Translated from Problemy Peredachi Informatsii, Vol. 25, No. 4, pp. 11-23, October-December, 1989. Original article submitted October 26, 1987.

0032-9460/89/2504-0265$12.50

without reducing the code distance. Any linear code with d = 4 is either a quasiperfect code or a shortening of some quasiperfect code with d = 4.

A *cap* in projective geometry is the collection of points no two of which lie on the same line [6-12]. A *complete cap* is a cap to which no point may be added so that the resulting set remains a cap.

If a column of length r is considered as a point in the projective geometry PG(r — 1, 2), then a straight line corresponds to any three columns, one of which is the sum of the other two; an N-point complete cap corresponds to the check matrix of a quasiperfect [N, N — r, 4]2 code [9, 11] (see Proposition 4, Sec. 6).

In general, the following questions remain open:

I. What is the structure of the check matrices of [N, N − r, 4]2 codes and the corresponding complete caps?

II. What are the possible values of N, the length of a [N, N − r, 4]2 code? What is the possible number of points N in a complete cap?

The following results are currently known.

In [6] and [10, Lemma VII, p. 167] it is shown that

$$N \leqslant 2^{r-1} = N_{\max}. \tag{1}$$

For $N = 2^{r-1}$ we have the extended Hamming code. Following [12], let $m_2'(r - 1, 2)$ be the number of points in the complete cap of maximum cardinality among all the complete caps with strictly fewer than N_{max} points. In [10, p. 168] it is shown that

$$\text{If } N < 2^{r-1}, \text{ then } N \leqslant m_2'(r-1, 2) \leqslant (2^r - 1)/3. \tag{2}$$

In this paper, we consider the range of code lengths

$$N \geqslant 2^{r-2} + 1.$$

A somewhat unexpected answer (in our view) is obtained to question I, which is stated below in the form of Theorem 1, the main result of this paper.

Definition 1. The check matrix H of a [n, n − r, 4]ρ code is called symmetric if it is representable in the form

$$H = \left\| \begin{array}{c|c} 0 \ldots 0 & 1 \ldots 1 \\ \hline H_1 & H_1 \end{array} \right\|, \tag{3}$$

where H_1 is the check matrix of the [n/2, n/2 − (r − 1), d_1]ρ_1 code.

The construction (3) is usually called the *Plotkin construction* (see [13-16]). Define the matrices P_4 and $H_r(n)$:

$$P_4 = \begin{Vmatrix} 10001 \\ 01001 \\ 00101 \\ 00011 \end{Vmatrix} \tag{4}$$

is the check matrix of the [5, 5 − 4, 5]2 code;

$$H_r(n) = \begin{cases} \text{the check matrix of a quasiperfect } [N = n,\ N - R,\ 4]2 \text{ code,} \\ \quad \text{if } n \neq 2 \text{ and } n \neq 5, \\ P_4, \text{ if } n = 5 \text{ and } r = 4, \\ \left\| \begin{matrix} 01 \\ 11 \end{matrix} \right\|, \text{ if } n = 2 \text{ and } r = 2. \end{cases} \tag{5}$$

THEOREM 1. For $N \geq 2^{r-2} + 2$ the check matrix H of a quasiperfect [N, N − r, 4]2 code is necessarily symmetric, i.e., representable in the form (3). Here H_1 is the matrix $H_{r-1}(N/2)$.

Complete caps have similar symmetry.

Proof of Theorem 1 utilizes the results of [17] from abelian group theory.

Corollary 1 for $N \geq 2^{r-2} + 1$ provides an exhaustive answer to question II (improving bound (2) in the process).

COROLLARY 1. In the range $N \geq 2^{r-2} + 1$ with $r \geq 5$, the length N of a quasiperfect [N, N − r, 4]2 code may take any value from the series

$$N = 2^{r-2} + 2^{r-2-g} \text{ for } g = 0, 2, 3, 4, 5, \ldots, r-2. \tag{6}$$

The length N may not take any value other than those listed in (6).

From (6) we obtain an exact value of $m_2'(r-1, 2)$:

$$m_2'(r-1,2)=2^{r-2}+2^{r-4}.$$

Corollaries 2 and 3 refine the answer to question I.

Let $M_r(v, i)$ be the matrix locator [18], i.e., the matrix consisting of i identical columns of length r where each column is a binary representation of the number v.

COROLLARY 2. In the range $N \geq 2^{r-2}+2$ with $r \geq 5$, the check matrix of any $[N, N-r, 4]2$ code is representable in the form

$$H_r(2^{r-2}+2^{r-g-2})=\left\|\begin{array}{c|c|c|c} M_{r-g-2}(0, 2^g+1) & M_{r-g-2}(1, 2^g+1) & \cdots & M_{r-g-2}(D, 2^g+1) \\ \hline H_{g+2}(2^g+1) & H_{g+2}(2^g+1) & & H_{g+2}(2^g+1) \end{array}\right\|, \tag{7}$$

where $D = 2^{r-g-2}-1$, $g = 0,2,3,4,5, \ldots, r-2-1$, and the lower $g+2$ rows are the 2^{r-g-2}-fold repetition of the same matrix.

Matrix (7) is obtained by $(r-g-2)$-application of construction (3).

By Corollary 2, the structure of the check matrices of $[N=(2^g+1)2^{r-g-2}, N-r, 4]2$ codes in the range $N \geq 2^{r-2}+2$ is completely determined by the structure of the matrices $H_{g+2}(2^g+1)$. The answer to question I thus reduces to an answer to an essentially more restricted question:

Ia. What is the structure of the matrices $H_{g+2}(2^g+1)$?

In this paper, we compute all the matrices $H_{g+2}(2^g+1)$ for $g = 0,2,3$, which in turn makes it possible to enumerate for $N > 2^{r-2}+2^{r-6}$ all the nonequivalent $[N, N-r, 4]2$ codes (and the corresponding complete caps) and thus to obtain an exhaustive answer to question I for this range. Corollary 3 provides the sought answer.

Let X_r, P_r, and L_r be the matrices obtained from (7) for $g = 0$, 2, and 3, respectively. The matrix X_r is the check matrix of the extended Hamming code and it contains 2^{r-1} distinct columns of length $r-1$ and a column of ones. The matrix P_r was proposed by Panchenko [15]:

$$X_r=H_r(2^{r-1})=\left\|\begin{array}{c|c|c|c} M_{r-2}(0,2) & M_{r-2}(1,2) & \cdots & M_{r-2}(2^{r-2}-1,2) \\ \hline 01 & 01 & & 01 \\ 11 & 11 & \cdots & 11 \end{array}\right\|, \tag{8}$$

$$P_r=H_r(5\cdot 2^{r-4})=\left\|\begin{array}{c|c|c|c} M_{r-4}(0,5) & M_{r-4}(1,5) & \cdots & M_{r-4}(2^{r-4}-1,5) \\ \hline 10001 & 10001 & & 10001 \\ 01001 & 01001 & & 01001 \\ 00101 & 00101 & \cdots & 00101 \\ 00011 & 00011 & & 00011 \end{array}\right\|, \tag{9}$$

$$L_r=H_r(9\cdot 2^{r-5})=\left\|\begin{array}{c|c|c} M_{r-5}(0,9) & \cdots & M_{r-5}(2^{r-5}-1,9) \\ \hline H_5(9) & \cdots & H_5(9) \end{array}\right\|, \tag{10}$$

where

$$H_5(9)=\left\|\begin{array}{cc} 00000 & 1111 \\ \hline 10001 & 0000 \\ 01001 & 1001 \\ 00101 & 0101 \\ 00011 & 0011 \end{array}\right\|.$$

Denote by Π_r the code defined by the check matrix P_r of the form (4) or (9).

COROLLARY 3. For $N > 2^{r-2}+2^{r-6}$, $r \geq 6$, there exist precisely three nonequivalent quasiperfect $[N, N-r, 4]2$ codes: $[N=2^{r-1}, N-r, 4]2$ Hamming code with check matrix X_r; $[N=2^{r-2}+2^{r-4}, N-r, 4]2$ code Π_r with check matrix P_r; and $[N=2^{r-2}+2^{r-5}, N-r, 4]2$ code Ω_r with check matrix L_r.

Remark 1. Equivalent codes, in the usual way, are codes whose check matrices can be transformed into one another by interchanging columns and performing elementary operations on rows [2, Sec. 2.6]: interchanging any two rows and adding one row to another. In the same sense we understand the expressions "up to equivalence" and "matrix is reducible to the form".

Remark 2. We will list without proof all the nonequivalent matrices $H_{4+2}(2^4+1)$, thus providing an exhaustive answer to question I for the range $N > 2^{r-2}+2^{r-7}$ (see Sec. 5).

Remark 3. Enumeration of all $[N > 2^{r-2} + \beta, N - r, 4]2$ codes is of interest in providing an answer to question I, but it also may be used for other purposes, such as solving the extremal problems of [15, 19-21] in the class of linear codes (minimization of the number of minimum-weight words).

This enumeration also may be useful for studying codes with $d \geq 5$, given the results of [8], say.

The results of this paper may be used for construction and analysis of covering codes with $\rho = 2$ [3-5]. Quasiperfect codes with $d = 4$ are examples of codes for which $\rho = t[n, k]$, where $t[n, k]$ is the minimum covering radius of $[n, k]$ linear binary code [3, 5].

Remark 4. The methods of this paper may be applied to show that quasiperfect $[N = 2^{r-2}, N - r, 4]2$ codes do not exist.

The paper is organized as follows. Section 2 introduces the necessary notation. Section 4 provides sufficient conditions of symmetry. One of the lemmas is proved in the Appendix. Section 5 proves the main results: Theorem 1 and Corollaries 1-3. Section 6 extends the results to caps in the projective geometry $PG(r - 1, 2)$.

2. NOTATION

All symbols, vectors, columns, and matrices in this paper are binary. A matrix (depending on context) may be treated as a set whose elements are the matrix columns.

We use the following notation: $[n, n - r, d]$ code is a code of length n with r check symbols and distance d; $\rho(V)$ is the covering radius of the code V; E^r is the space of r-dimensional column vectors; $E_0{}^r$ is the space E^r with the zero vector removed; H is the check matrix of the $[n, n - r, d]$ code; $H = \|h_1 h_2 \ldots h_n\|$, where h_i is a matrix column, $h_i \in E_0{}^r$; $V^\perp$ is the $[n, r, d^\perp]$ code dual to the $[n, n - r, 4]$ code V; $d^\perp$ is the minimum distance of the code $V^\perp$; T denotes the transpose; $h^{(i)}$ or $h^{(ij)}$ is column h with the symbol i or the column $(i, j)^T$ adjoined at the top (if column h is of length r, then columns $h^{(i)}$ and $h^{(ij)}$ are respectively of length $r + 1$ and $r + 2$); $\{B\}^{(i)}$ or $\{B\}^{(ij)}$ is the matrix B (a collection of columns of B) with symbol i or column $(i, j)^T$ respectively adjoined at the top of each column; $|F|$ is the cardinality of the set F (in particular, the number of columns in the matrix F considered as a collection of columns); $\lfloor x \rfloor$ is the whole part of x; $\lceil x \rceil$ is the smallest integer not less than x.

Let H be the check matrix of the $[n, n - r, 4]$ code V and respectively the generating matrix of the $[n, r, d^\perp]$ code $V^\perp$. If the code $V^\perp$ contains a word of weight w, then the matrix H is representable in the form

$$H = \left\| \begin{array}{c|c} \overbrace{0 \ldots 0}^{n_0 = n - w} & \overbrace{1 \ldots 1}^{w} \\ \hline B(w) & A \end{array} \right\|, \tag{11}$$

where $B(w)$ and A are $(r - 1) \times (n - w)$ and $(r - 1) \times w$ matrices, respectively. The matrix $B(w)$ is called the residual matrix. $B(w)$ is the generating matrix of the $[n_0 = n - w, r - 1, d_0{}^\perp]$ code $V_0{}^\perp$, which is called the residual code [22]. We know (see [1, Sec. 17.5] and [22]) that

$$d_0{}^\perp \geq \lceil d^\perp / 2 \rceil, \quad \text{if} \quad w = d^\perp \tag{12}$$

3. SYMMETRIC CHECK MATRICES OF BINARY CODES WITH d = 4

Definition 2. The check matrix $H = \|h_1 h_2 \ldots h_n\|$ of the $[n, n - r, 4]$ code V is called symmetric relative to the column s from $E_0{}^r$ not included in the matrix if the matrix columns can be partitioned into $n/2$ pairs so that the sum of the columns in each pair equals s, i.e., up to column numbering we have the relationship

$$h_1 + h_2 = h_3 + h_4 = \ldots = h_{n-1} + h_n = s, \; s \in \{E_0{}^r \backslash H\}. \tag{13}$$

From (13) it follows that the sum of column s with any column h_i is also a column of the matrix H, i.e.,

$$s + h_i = h_j, \; s \in \{E_0{}^r \backslash H\}, \; h_i, \; h_j \in H, \; i = \overline{1, n}. \tag{14}$$

Denote by $S(H)$ the collection of columns relative to which the matrix H is symmetric.

Definition 3. The check matrix H of the code V is called symmetric if the set $S(H)$ is nonempty.

LEMMA 1. Definitions 1 and 3 are equivalent.

Proof. If the matrix H is of the form (3), then it is symmetric relative to the column $(10\ldots0)^T$. Let the matrix H be symmetric relative to the column s. Then, simultaneously applying the elementary operations of [2, Sec. 2.6] (addition and transposition) to the rows of the matrix and to the corresponding coordinates of the column s, we can reduce s to the form $(10\ldots0)^T$. As a result (see (13)) the matrix H is transformed to a matrix (3) up to the order of columns.

LEMMA 2. For $r = 4$ there exist two codes with $d \geq 4$, $\rho = 2$: the $[5, 5-4, 5]2$ code with check matrix (4) and the $[8, 8-4, 4]2$ code — extended Hamming code with check matrix X_4.

The proof is straightforward. For complete caps, the corresponding facts are presented in [10, pp. 167, 169].

LEMMA 3. In the construction (3) with $r \geq 5$, the matrix H is the check matrix of a quasiperfect $[N, N-r, 4]2$ code if and only if H_1 is the matrix $H_{r-1}(N/2)$.

Proof. Let H be the check matrix of the $[N, N-r, 4]2$ code V. Then $H_1 = \|h_{11}\ldots h_{1N_1}\|$ is the check matrix of the $[N_1, N_1 - r + 1, d_1]\rho_1$ code V_1 with $N_1 = N/2$. If the column $s \in \{E_0^{r-1}\backslash H_1\}$, then $s^{(0)} \in \{E_0^r\backslash H\}$. Since $\rho(V) = 2$, then by Proposition 1 there are two columns h_i, h_j in H such that $h_i + h_j = s^{(0)}$. This means (see (3)) that $h_{1m}^{(0)} + h_{1k}^{(0)} = h_{1m}^{(1)} + h_{1k}^{(1)} = s^{(0)}$, where h_{1m}, h_{1k} are some columns from H_1. Therefore $h_{1m} + h_{1k} = s$ and, by Proposition 1, $\rho_1 = 2$. Since the code V has $d = 4$, then $d_1 \geq 4$. Thus, either $d_1 = 5$ or $d_1 = 4$. If $d_1 = 5$, then V_1 is the $[5, 5-4, 5]2$ code Π_4. If $d_1 = 4$, then V_1 is a $[N_1, N_1 - (r-1), 4]2$ code of length $N_1 > 5$ (by Lemma 2 and an obvious argument, $N_1 \geq r$). This proves the lemma in one direction.

The proof in the other direction relies on the same ideas.

4. SUFFICIENT CONDITIONS OF SYMMETRY OF THE CHECK MATRIX OF A CODE WITH d = 4

LEMMA 4. If the check matrix H of the $[N, N-r, 4]2$ code V is represented in the form (11) and the residual matrix B(w) is symmetric, then the matrix H is also symmetric, and $S(H) \supseteq \{S(B(w))\}^{(0)}$.

Proof. Consider the columns from E_0^{r-1}: $b_i \in B(w)$, $a_i \in A$, $s \in S(B(w))$. Assume that $s^{(0)} \notin S(H)$. Then (see (14)) there is a column a_1 such that $a_1^{(1)} + s^{(0)} \notin H$. Since $\rho(V) = 2$, then by Proposition 1 there exist columns b_1 and a_2 such that $b_1^{(0)} + a_2^{(1)} = a_1^{(1)} + s^{(0)}$. Hence $b_1 + s = a_1 + a_2$, where $b_1 + s \in B(w)$ but $a_1 + a_2 \notin B(w)$. A contradiction. Therefore, $s^{(0)} \in S(H)$.

LEMMA 5. If a symmetric submatrix Q has been identified in the matrix X_r, then the matrix $X_r\backslash Q$ is also symmetric, and $S(X_r\backslash Q) = S(Q)$.

The proof follows from (13), (14) and the fact that $S(X_r) = \{E_0^r\backslash X_r\} \supset S(Q)$.

The following facts from the theory of abelian groups (Definition 4 and Proposition 2 from [17]) are needed for the proof of Lemma 6.

Definition 4 [17]. The subset Y of an additive abelian group G is called periodic if there exists a nonzero element g in G such that its sum with any element y_i of Y is again an element of Y (compare with (14)):

$$\exists g \in G,\ g \neq 0 : \forall y_i \in Y,\ g + y_i \in Y. \tag{15}$$

Proposition 2 [17, Theorem 3.1]. Let F and E be subsets of the additive abelian group G and $F + E$ the sum of the subsets F and E that consists of all the elements of the form $f + e$, where $f \in F$ and $e \in E$. We have the following proposition:

$$\text{if } |F + E| \leq |F| + |E| - 2, \text{ then } F + E \text{ is a periodic subset.} \tag{16}$$

LEMMA 6. Assume that the check matrix H of the $[N \geq 2^{r-2} + 2, N-r, 4]2$ code V is representable in the form (11), where the residual matrix B(w) is a submatrix of X_{r-1} i.e.,

$$H = \left\| \begin{array}{c|c} 0\ldots0 & \overbrace{1\ldots1}^{w} \\ \hline B(w) & A \end{array} \right\| = \left\| \begin{array}{c|c|c} 0\ldots0 & \overbrace{1\ldots1}^{w} & 1\ldots1 \\ \hline 1\ldots1 & 0\ldots0 & 1\ldots1 \\ \hline B_1 & F & E \end{array} \right\|. \tag{17}$$

B_1, F, E are some matrices with $(r-2)$ rows. Then the matrix H is symmetric.

Proof. Define the matrix $B_2 = E^{r-2}\backslash B_1$. Since $\rho(V) = 2$, then using Proposition 1 and treating the sum of matrices as the sum of two sets whose elements are columns (see Proposition 2), we obtain from (17) $\{F\}^{(10)} + \{E\}^{(11)} = \{B_2\}^{(01)}$,

whence it follows that $\{F\}^{(0)} + \{E\}^{(1)} = \{B_2\}^{(1)}$ and $F + E = B_2$. Consider F, E, and B_2 as subsets of the abelian group E^{r-2}. Since $N=|X_{r-1}|-|B_2|+|F|+|E|$, $N\geq 2^{r-2}+2$ and $|X_{r-1}| = 2^{r-2}$, we have $|B_2| = |F + E| \leq |F| + |E| - 2$, and from Proposition 2 it follows that B_2 is a periodic subset, or equivalently (see (14) and (15)) the matrix B_2 is symmetric. But then the matrix $\{B_2\}^{(1)}$ is also symmetric and therefore, by Lemma 5, the matrix $\{B_1\}^{(1)} = B(w)$ is symmetric and, by Lemma 4, the matrix H is symmetric.

Definition 5. The code V has property Z if the dual code $V^{\perp}$ contains at least one pair of words in which zeros do not occur in identical positions (i.e., a pair of words whose bitwise disjunction gives an all-one word).

Property Z is clearly sufficient for the check matrix H of the code V to be representable in the form (17).

Define a $r \times (2^{r-2} + 1)$ matrix

$$H_r(a_1, \ldots, a_v; x) = \left\| \begin{array}{c|c|c|c|c} 0 & \ldots & 0 & 1 & 1 \ldots 1 \\ \hline X_{r-1} \setminus \{a_1, \ldots, a_v\} & x & x + a_1 & \ldots & x + a_v \end{array} \right\|, \tag{18}$$

where $a_1, \ldots, a_v, x$ are some columns of the matrix X_{r-1}.

The following lemma is used in the proof of Lemma 8 and Corollary 3.

LEMMA 7. For $r = 5$, the matrix $H_5(2^3 + 1) = H_5(a_1; x)$ is the only (up to equivalence) matrix $H_5(9)$ and it is reducible to the form (10).

Proof. Represent the matrix $H_5(9)$ in the form (11), where $w = d^{\perp} \geq 1$. In this case, $V^{\perp}$ is the $[9, 9 - 4, d^{\perp}]$ code. With four check symbols, $N_{max} = 8$ (see (1)). Therefore, $d^{\perp} \leq 3$. Hence, $8 \geq n_0 = 9 - d^{\perp} \geq 6$. In view of the above, $B(d^{\perp})$ is the check matrix of some $[8 \geq n_0 \geq 6, n_0 - 4, 4]$ code. By Lemma 2, this is either an extended Hamming code or its shortening, i.e., $B(d^{\perp}) \subseteq X_4$. The equality $B(d^{\perp}) = X_4$ (when $n_0 = 8$) contradicts Lemma 4. Assume that $n_0 = 6$, i.e., $B(d^{\perp}) = X_4\{a_1, a_2\}$, where a_1, a_2 are columns from X_4. Since X_{r-1} contains an all-one row (see (8)), the sum of two columns from $E^{r-1}\setminus X_{r-1}$ again produces a column that does not belong to X_{r-1}. Therefore, by Proposition 1, in the case $B(d^{\perp}) \subset X_{r-1}$, the matrix A in (11) should include columns that belong to X_{r-1} and at the same time columns that do not belong to this matrix. Therefore, for $n_0 = 6$, the matrix $H_5(9)$ is reducible to the form $H_5(a_1, a_2; x)$. But the column $(1, x + a_1 + a_2)^T$ is not the sum of two columns of the matrix $H_5(a_1, a_2; x)$. Thus, the case $n_0 = 6$ is ruled out.

It remains to consider $n_0 = 7$, i.e., $B(d^{\perp}) = X_4\setminus a_1$. It is clear from the previous argument that the only possibility is $H_5(9) = H_5(a_1; x)$. It is easy to see that all the matrices $H_5(a_1; x)$ are equivalent and any of them can be reduced to the form (10) by elementary row operations.

LEMMA 8. Let the check matrix H of the $[N \geq 2^{r-2} + 2, N - r, 4]2$ code V be representable in the form (11) so that the residual matrix $B(d^{\perp})$ is a submatrix of the matrix P_{r-1} of the form (4) or (9). Then the code V has property Z and the matrix H is symmetric.

Lemma 8 is proved in the Appendix.

5. PROOF OF THE MAIN RESULTS

We will first prove Corollaries 1-3 on the assumption that Theorem 1 holds. Corollaries 1-3 are proved before Theorem 1, because the theorem is proved by induction on r. In making the inductive hypothesis that Theorem 1 holds for $r - 1$, it is useful to have the corollaries of the theorem that are true for $r - 1$.

LEMMA 9. If $r \geq 5$, then a $[N = 2^{r-2} + 1, N - r, 4]2$ code exists.

Proof. It is easy to verify that the matrix $H_r(a_1; x)$ (see (18)) is the check matrix of the sought code for $r \geq 5$.

LEMMA 10. The $[2^{r-2} + 1, r \geq 5, d]$ codes have $d \leq 2^{r-3} - 1$.

The lemma follows from the result of [23] on the nonexistence of codes on the Griesmer bound [1, Sec. 17.5] for $3 \leq d \leq 2^{r-2} - 2$.

Proposition 3 (see [1, 2] and [10, Lemma VII, p. 167]). The extended Hamming code is the only $[2^{r-1}, 2^{r-1} - r, 4]2$ code.

Proof of Corollaries 1 and 2. Let $N \geq 2^{r-2} + 2$. Then the check matrix $H_r(N)$ of a quasiperfect $[N, N - r, 4]2$ code can be constructed, by Theorem 1 and Lemma 3, in the form (3) from the matrix $H_{r-1}(N_1)$, where $N_1 = N/2$. The matrix $H_{r-1}(N_1)$ in turn can be constructed in the form (3) from the matrix $H_{r-2}(N_2)$, where $N_2 = N/2^2$, and so on. The process stops with the matrix $U = H_{r-x}(N_x)$, where $N_x = N/2^x = 2^g + 1$, $x = r - 2 - g$, $g \in \{2,3,4, \ldots, r - 2 - 1\}$. By Lemma 9, the matrix $U = H_{g+2}(2^g + 1)$ exists. The matrix locators $M_{r-g-2}(i, 2^g + 1)$ in (7) are obtained by construction. The code length is $N=2^x N_x=2^{r-g-2}(2^g+1)$, $g=2, 3, 4, \ldots$. For $g = 0$ we obtain the $[2^{r-1}, 2^{r-1} - r, 4]2$ Hamming code (see (5)-(8)).

Corollary 1 for $N = 2^{r-2}+1$ follows from Lemma 9.

Proof of Corollary 3. Consider the matrix (7) for g = 0, 2, 3, using respectively Proposition 3, Lemma 2, and Lemma 7.

Proof of Theorem 1. From (1) and Proposition 3 (see also (8)) it follows that the theorem is true for $N = 2^{r-1}$ and we need to consider the case $2^{r-1} > N \geq 2^{r-2} + 2$. The proof in this case is by induction on the number of check symbols r. If $2^{r-1} > 2^{r-2} + 2$, then $r \geq 4$. The theorem is true for r = 4 (see Lemma 2). Assume that Theorem 1, and hence also Corollaries 1-3, hold for r − 1 check symbols and prove that the theorem holds for r check symbols.

Represent the check matrix H in the form (11) so that $w = d^{\perp}$. By Griesmer's bound, seeing that $2^{r-1} > N$, we have $d^{\perp} < N/2$. Hence $n_0 = N - d^{\perp} > N/2 \geq 2^{r-3} + 1$, i.e., $n_0 = 2^{r-3} + \alpha$, where $\alpha \geq 2$. The matrix $B(d^{\perp})$ is the check matrix of the $[n_0, n_0 - (r-1), d_0 = 4]$ code V_0, which is either quasiperfect or is obtained by shortening of some quasiperfect $[N_Q, N_Q - (r-1), 4]2$ code Q. (The inequality $d_0 < 5$ follows from the sphere packing bound [1, Sec. 1.5].)

In the first case, by the inductive hypothesis, the matrix $B(d^{\perp})$ is symmetric and therefore, by Lemma 4, the matrix H is symmetric.

In the second case, by the inductive hypothesis, $N_Q = 2^{r-3} + 2^{r-3-g}$, where g = 0,2,3,4,... .

Let g = 0. Then (see (5), (7), (8)), the code Q is the extended Hamming code, $B(d^{\perp})$ is a submatrix of the matrix X_{r-1}, and by Lemma 6 the matrix H is symmetric.

For $g \geq 2$, the code Q is obtained by (r − 3 − g)-fold application of the construction (3) to the $[2^g + 1, 2^g + 1 - (g+2), d \geq 4]2$ code Q_2. Clearly, $d_Q{}^{\perp} = 2^{r-3-g} d_g{}^{\perp}$, where $d_Q{}^{\perp}$ and $d_g{}^{\perp}$ are the distances of the codes $Q^{\perp}$ and $Q_g{}^{\perp}$, respectively.

Let $g \geq 3$. Then $r > 6$ and by Lemma 10, $d_g{}^{\perp} \leq 2^{g-1} - 1$. Therefore $d_Q{}^{\perp} \leqslant 2^{r-3-g}(2^{g-1}-1) = 2^{r-4} - 2^{r-3-g}$. Hence, for the given code with the check matrix H, using (12), we obtain $d^{\perp} \leqslant 2d_0{}^{\perp} \leqslant 2d_Q{}^{\perp} \leqslant 2^{r-3} - 2^{r-2-g}$. Thus, $n_0 = N - d^{\perp} > 2^{r-3} + 2^{r-2-g} > N_Q$. A contradiction. The case $g \geq 3$ is ruled out.

Let g = 2. Then $N_Q = 2^{r-3} + 2^{r-5}$, the code Q is Π_{r-1}, $B(d^{\perp})$ is a submatrix of the matrix P_{r-1}, and by Lemma 8 the matrix H is symmetric. Q.E.D.

Remark 5. It can be shown that there exist precisely five nonequivalent matrices $H_6(17)$, which all have the structure (see (18), (8))

$$H_6(a_1, a_2, \ldots, a_v; x) \quad \text{for} \quad v = 1, 3, 4, 5, 6. \tag{19}$$

Here the columns a_1, a_2, a_3, a_4, a_5 are linearly independent in all the matrices.

A specific choice of the columns a_i and x does not produce new nonequivalent matrices. Using the matrices (19) in construction (7), we obtain five nonequivalent $[N = 2^{r-2} + 2^{r-6}, N - r, 4]2$ codes. Together with Corollary 3, this provides an exhaustive answer to question I (Sec. 1) for $N > 2^{r-2} + 2^{r-7}$.

Remark 6. The following extremal problem is considered in [15, 19-21]: minimize A_d (the number of minimum-weight words) in a code with given parameters — length, distance, and cardinality. Our results simplify the solution of this extremal problem in the class of linear codes with d = 4. For instance, using the results of [15], we can show that of the three codes in Corollary 3, it is the code Π_r that ensures the least A_4 for a given length n. Therefore, in the range $2^{r-2} + 2^{r-4} \geq n > 2^{r-2} + 2^{r-6}$, the absolute minimum of A_4 among linear codes for given n and r is attained on the shortened codes Π_r. The $[n = 2^{r-2} + r, n - r, 4]$ codes widely used in memories [18] fall in this range for r = 7-9. The codes Π_r therefore provide a reasonable alternative to the extended Hamming code while ensuring reliable storage of information [15, 24].

6. COMPLETE CAPS IN THE GEOMETRY PG(r − 1, 2): SYMMETRY OF STRUCTURE AND NUMBER OF POINTS

A column from $E_0{}^r$ is associated to a point in the projective geometry PG(r − 1, 2). Then [1, 6-12] a *line* is three linearly dependent columns (i.e., three columns one of which is the sum of the other two); a *cap* is a collection of columns no three of which are linearly dependent; a *complete cap* is a cap to which no column may be added; an *exterior point* is a column from $E_0{}^r$ not contained in the cap; a *chord* is a line containing two points from a cap and an exterior point; a *tangent* is a line containing a column from a cap and two exterior points.

Any exterior point lies at least on one chord of a complete cap (compare with Proposition 1). Proposition 1, Lemma 2, and the results of [7], [9], [10, pp. 167, 169], and [11] lead to

Proposition 4. Let a column of length r be considered as a point in the projective geometry PG(r − 1, 2). Then there is a one-to-one correspondence between complete caps of N points and the matrices $H_r(N)$ (see (5)).

For N = 5, r = 4, we have the dual case of Qwist's cap [7]; for N = 2, r = 2 the geometry is a straight line with two points belonging to the cap.

We preserve the same notation for caps and points as for matrices and columns. $H_r(N)$ is a complete cap of N points in the geometry PG(r − 1, 2). Equivalence of caps is understood in the sense of Remark 1.

Definition 6. The cap H containing n points is symmetric relative to the exterior point s if this point lies on n/2 chords. The point s is called a symmetry point of the cap H.

Denote by S(H) the collection of symmetry points of the cap H.

Definition 7. The cap H is symmetric if the set S(H) is nonempty.

The Plotkin construction (3) corresponds in projective geometry to the following method of construction of the cap H in PG(r − 1, 2) from the cap H_1 in PG(r − 2, 2). In the section of the geometry PG(r − 1, 2) by the hyperplane PG(r − 2, 2) construct a cap H_1 containing n/2 points. Through an exterior point s, not in PG(r — 2, 2), draw n/2 tangents to the cap H_1. All the points of these tangents, except the point s, jointly form a symmetric cap H containing n points. The point s ∈ S(H).

Applying Proposition 4 and noting that for N = 5, r = 4 and N = 2, r = 2 complete caps exist although the corresponding [N, N − r, 4]2 codes do not exist, we can extend the results of this paper to complete caps in the following way.

THEOREM 2. In the projective geometry PG(r − 1, 2), any complete cap containing $N \geq 2^{r-2} + 2$ points is symmetric, i.e., has an exterior point that lies on N/2 chords.

COROLLARY 4. In the geometry PG(r − 1, 2), r ≥ 2, in the range $N \geq 2^{r-2} + 1$, the number of points N contained in a complete cap may take any value from the series (6) and no other value.

COROLLARY 5. In the geometry PG(r − 1, 2), r ≥ 3, any complete cap $H_r(N)$ with $N \geq 2^{r-2} + 2$ may be represented as the result of (r − 2 − g)-fold application of the Plotkin construction to the complete cap $H_{g+2}(2^g + 1)$ from the geometry PG(g + 1, 2), where g =0,2,3,4, ..., r − 2 − 1.

COROLLARY 6. In the geometry PG(r − 1, 2) for r ≥ 6, $N > 2^{r-2} + 2^{r-6}$, there exist precisely three nonequivalent complete caps $H_r(N)$ corresponding to the check matrices X_r, P_r, and L_r (see (8)-(10)).

APPENDIX

Proof of Lemma 8. By the condition of the lemma, the matrix H is representable in the form

$$H = \left\| \begin{array}{c|c} \overbrace{0\ldots0}^{n_0} & \overbrace{1\ldots1}^{d^\perp} \\ \hline B(d^\perp) & A \end{array} \right\| = \left\| \begin{array}{c|c} \overbrace{0\ldots0}^{n_0=5\cdot 2^{r-5}-\Delta} & 1\ldots1 \\ \hline F_0 & F_1 \\ \hline L_0 & L_1 \end{array} \right\| = \left\| \begin{array}{c} \overbrace{0\ldots01\ldots1}^{N=2^{r-2}+\beta} \\ \hline F \\ \hline L \end{array} \right\|. \tag{A.1}$$

where $B(d^\perp)$ is a submatrix of the matrix P_{r-1}; L_0, L_1, and L are 4 × n_0, 4 × $d^\perp$, and 4 × N matrices, respectively; F_0, F_1, and F are (r − 5) × n_0, (r − 5) × $d^\perp$, and (r − 5) × N matrices, respectively; $n_0+d^\perp=N$; $N=2^{r-2}+\beta$, $\beta\geq 2$; $n_0=5\cdot 2^{r-5}-\Delta$, $\Delta>0$.

1. A pair of words in the code $V^\perp$ without zeros in the corresponding positions will be sought in the linear hull U of the four bottom rows of the matrix H, denoted by L in (A.1). The existence of such a pair depends on the type of the columns in L, but not on the number of columns of each type. If L only contains columns from P_4 (see (4)) of the type $(1000)^T$, $(0100)^T$, $(0010)^T$, $(0001)^T$, and $(1111)^T$ (these columns are of weight 1 or 4), then we can easily count that U contains 30 pairs of words ensuring property Z. Now assume that the submatrix L_0 contains only columns from P_4 (this is possible by the condition of the lemma), and the submatrix L_1 contains (in addition to columns from P_4) m_i varieties of columns of weight i, where i = 0, 2, 3. It can be directly verified that for $m_2 + m_3 \leq 2$ and $m_0 = 0$, pairs of words ensuring property Z are preserved in U. For example, if $m_2 = 2$, $m_3 = m_0 = 0$, and L_1 contains two columns of the type $(1100)^T$ and $(0011)^T$, then 12 pairs of words with the required properties are preserved in U.

Thus, in proving the lemma, it suffices to show that

$$m_2+m_3\leqslant 2, \quad m_0=0. \tag{A.2}$$

(If property Z holds, symmetry of the matrix H follows from Lemma 6.)

2. $B(d^\perp)$ is the generating matrix of the $[n_0, r - 1, d_{r-1}^\perp(\Delta)]$ code dual to the code Π_{r-1} shortened by Δ symbols. Using (9), we transform the matrix $B(d^\perp)$ by interchanging columns to the form

$$B(d^\perp) = \left\| \begin{array}{c} F_0 \\ \hline \\ L_0 \\ \\ \end{array} \right\| = \left\| \begin{array}{c|c|c|c|c} W_1 & W_2 & W_3 & W_4 & W_5 \\ \hline 1\ 1\ldots1 & 0\ 0\ldots0 & 0\ 0\ldots0 & 0\ 0\ldots0 & 1\ 1\ldots1 \\ 0\ 0\ldots0 & 1\ 1\ldots1 & 0\ 0\ldots0 & 0\ 0\ldots0 & 1\ 1\ldots1 \\ 0\ 0\ldots0 & 0\ 0\ldots0 & 1\ 1\ldots1 & 0\ 0\ldots0 & 1\ 1\ldots1 \\ 0\ 0\ldots0 & 0\ 0\ldots0 & 0\ 0\ldots0 & 1\ 1\ldots1 & 1\ 1\ldots1 \end{array} \right\|, \tag{A.3}$$

where W_i is the matrix consisting of $2^{r-5} - \Delta_i$ distinct symbols of length $r - 5$, $i = 1, ..., 5$; $\Delta_1+\Delta_2+\Delta_3+\Delta_4+\Delta_5=\Delta=5\cdot 2^{r-5}-n_0$. Considering the linear hull of the submatrix L_0, we note that $d^{\perp}_{r-1}(\Delta)\leqslant 2^{r-4} - \max\limits_{i,j}\{\Delta_i+\Delta_j\}\leqslant 2^{r-4}-2\Delta/5$, where the maximum is over *a pair* of indices. On the other hand, $n_0 = 5\cdot 2^{r-5} - \Delta$. Using (12), we obtain $d^{\perp}_{r-1}(\Delta) \geqslant d^{\perp}/2 = (N-n_0)/2 = (3\cdot 2^{r-5}+\beta+\Delta)/2$. Combined with the previous inequality, this gives

$$\Delta\leqslant 2^{r-3}-\beta-2\max_{i,j}\{\Delta_i+\Delta_j\}, \quad \Delta\leqslant 5(2^{r-5}-\beta)/9. \tag{A.4}$$

Let Ψ be a submatrix of the matrix H; $Y(\Psi)$ a collection of columns with top coordinate 1 which cannot be included in the matrix H without reducing the distance if it contains the submatrix Ψ. Then (see (A.1)) we have

$$|Y(\Psi)|\leqslant 2^{r-1}-d^{\perp}=2^{r-1}-(N-n_0)=13\cdot 2^{r-5}-\Delta-\beta. \tag{A.5}$$

The proof of (A.2) is by contradiction. We will assume that (A.2) does not hold and show that this violates (A.5).

3. Since $|W_i| = 2^{r-5} - \Delta_i$ and $\Delta_1 + ... + \Delta_5 = \Delta$, then from (A.4) it follows that there exists a column that occurs in all the five matrices W_i. Therefore elementary row operations in the matrix H will produce a new zero column in each submatrix W_i, without altering L_0. For example, by adding the bottom row of the submatrix L_0 to the corresponding rows of the submatrix F_0, we transform one of the columns of the matrix W_5 to zero column. Some column is still common to all the matrices W_i. Adding the sum of all rows of the submatrix L_0 to the corresponding rows of F_0, we transform this column to zero in the matrices W_1, ..., W_4 without altering the matrix W_5. These elementary operations are naturally performed at the same time on the rows of the matrix A in (A.1).

Since $d^{\perp} = 3\cdot 2^{r-5}+\beta+\Delta\geqslant 3\cdot 2^{r-5}+3$, then the matrix locator (Sec. 1) $M_{r-5}(v, i)$ with $i \geq 4$ can be identified in the $(r - 5) \times d^{\perp}$ submatrix F_1 containing at most 2^{r-5} distinct columns. By adding the top row of the matrix H, we can always make $v = 0$.

It follows from the above that a matrix G of the form

$$G=\left\|\begin{array}{c|c} \overbrace{00000}^{} & \overbrace{111\ldots1}^{i\geqslant 4} \\ \hline 00000 & 000\ldots0 \\ \ldots & \ldots \\ 00000 & 000\ldots0 \\ \hline 10001 & \\ 01001 & \\ 00101 & K_{ij} \\ 00011 & \end{array}\right\|, \tag{A.6}$$

can be identified in the matrix H (A.1), where K_{ij} is a $4 \times i$ matrix, $i \geq 4$; j is the index of the matrix K_{ij}; the number of zero rows is $r - 5$.

Consider the matrix φ consisting of the top and the four bottom rows of the matrix G. Here, φ is the check matrix of some $[n \geq 9, n - 5, 4]$ code R. The situation $\varphi \subseteq X_5$ is impossible, because an all-one row cannot be formed in φ. Therefore (see (2)), the code R is a $[9, 9 - 5, 4]2$ code, or a $[10, 10 - 5, 4]2$ code D, or a shortening of the code D by one symbol. In the first case, by Lemma 7, the matrix φ coincides with the matrix $H_5(9)$ in (10). For the second case, represent φ in the form (11) with $w = d^{\perp}$. By Griesmer's bound, $d^{\perp} \leq 4$. Therefore, $n_0 = 10 - d^{\perp} \geq 6$, and by Lemma 2, $B(d^{\perp}) \subset X_4$. Thus (by Lemma 6), the matrix φ is symmetric, and (by Lemma 2) the only possibility is $K_{ij} = P_4$, i.e., $\varphi = P_5$ and D is the code Π_5. In the third case, it is easy to verify that all shortenings of the code Π_5 by one symbol are equivalent to one another.

Thus, it suffices to consider three variants of the matrix K_{ij} in (A.6):

$$K_{41}=\left\|\begin{array}{c}0000\\1001\\0101\\0011\end{array}\right\|, \quad K_{52}=\left\|\begin{array}{c}10001\\01001\\00101\\00011\end{array}\right\|, \quad K_{43}=\left\|\begin{array}{c}1000\\0100\\0010\\0001\end{array}\right\|. \tag{A.7}$$

4. The submatrix Ψ of the matrix H from (A.1) is constructed in the form

$$\Psi=\left\|\begin{array}{c|c|c} \overbrace{0\ldots0}^{n_0} & \overbrace{1\ldots1}^{i=4 \text{ or } 5} & \overbrace{1\ldots1}^{v} \\ \hline & 0\ldots0 & \\ B(d^{\perp}) & \ldots & t_1\ldots t_v \\ & 0\ldots0 & \\ \hline & K_{ij} & f_1\ldots f_v \end{array}\right\|, \tag{A.8}$$

where t_s is a column of length $r - 5$ and f_s is a column of length 4, $s = 1, \ldots, \nu$, $\nu \geq 1$.

Let Y_v^* be the collection of columns from $Y(\Psi)$ for which the four bottom coordinates constitute the binary representation of the number v; Y_v the collection of columns of length $r - 5$ obtained from the columns of Y_v^* by eliminating the top and the four bottom coordinates ($|Y_v^*| = |Y_v|$);

$$\delta_v = 2^{r-5} - |Y_v|; \quad \Lambda_{i_1 i_2 \ldots i_k} = \{W_{i_1} \cup W_{i_2} \cup \ldots \cup W_{i_k}\},$$

where the matrices are treated as sets (Sec. 2). Clearly,

$$|Y(\Psi)| = 16 \cdot 2^{r-5} - \sum_{v=0}^{15} \delta_v. \tag{A.9}$$

If $Y_v \supseteq \Lambda_{i_1 i_2 \ldots i_k}$, then we have the inequalities

$$\delta_v \leq \Delta_{i_p} \quad \text{for} \quad p = \overline{1, k}; \quad \delta_v \leq \min\{\Delta_{i_1}, \Delta_{i_2}, \ldots, \Delta_{i_k}\}. \tag{A.10}$$

5. Now it suffices to show that (A.2) holds in each of the three alternative specifications of the submatrix K_{ij} in (A.8):

$$\text{a) } K_{ij} = K_{41}; \text{ b) } K_{ij} = K_{52}; \text{ c) } K_{ij} = K_{43}.$$

Consider variant a). In (A.8), let $\nu = 1$, $f_1 = (0000)^T$, i.e., $m_0 = 1$. Then (see (A.3), (A.7), (A.8)), $Y_v \supseteq \Lambda_{23i}$, $v = 0, 3, 5, 6$; $Y_1 \supseteq \Lambda_4$, $Y_2 \supseteq \Lambda_3$; $Y_4 \supseteq \Lambda_2$; $Y_j \supseteq \Lambda_{15}$, $j = 8, 15$; $Y_k \supseteq \Lambda_1$, $k = 9, 10, 12$; $Y_l \supseteq \Lambda_5$, $l = 11, 13, 14$. Using (A.10), let $\delta_v \leq \Delta_i$, $v = 1, 5, 6$; $\delta_k \leq \Delta_1$, $k = 8, 9, 10, 12$; $\delta_l \leq \Delta_5$, $l = 11, 13, 14, 15$; $\delta_p \leq \Delta_2$, $p = 0, 4$; $\delta_s \leq \Delta_3$, $s = 2, 3$; $\delta_7 \leq 2^{r-5}$. Now from (A.9), the second inequality in (A.4), and the equality $\Delta_1 + \ldots + \Delta_5 = \Delta$, we have $|Y(\Psi)| \geq 15 \cdot 2^{r-5} - (4\Delta_1 + 4\Delta_5 + 2\Delta_2 + 2\Delta_3 + 3\Delta_4) \geq 15 \cdot 2^{r-5} - 4\Delta \geq 15 \cdot 2^{r-5} - \Delta - 3(5 \cdot 2^{r-5}/9) > 13 \cdot 2^{r-5} - \Delta - \beta$. **This contradicts (A.5). Therefore, $m_0 \neq 1$. Thus, $m_0 = 0$, the second relationship in (A.2) holds, and we have $\delta_0 = 0$. We similarly show that for $\nu = 1$ we cannot take $f_1 \in \{(0011)^T, (0101)^T, (0110)^T\}$,** i.e., $\delta_3 = \delta_5 = \delta_6 = 0$.

Now in (A.8) let $\nu = 2$, $f_1 = (1100)^T$, $f_2 = (1110)^T$, i.e., $m_2 + m_3 = 3$. Reasoning as before, we have $Y_i \supseteq \Lambda_5$, $l = 1, 11$; $Y_3 \supseteq \Lambda_{2345}$; $Y_k \supseteq \Lambda_1$, $k = 4, 9$; $Y_8 \supseteq \Lambda_{25}$; $Y_{10} \supseteq \Lambda_{12}$; $Y_{12} \supseteq \Lambda_{13}$; $Y_{13} \supseteq \Lambda_{45}$; $Y_{14} \supseteq \Lambda_{35}$; $Y_{15} \supseteq \Lambda_{14}$. Let $\delta_v \leq \Delta_i$, $v = 4, 9$; $\delta_p \leq \Delta_2$, $p = 8, 10$; $\delta_s \leq \Delta_3$, $s = 12, 14$; $\delta_j \leq \Delta_4$, $j = 13, 15$; $\delta_l \leq \Delta_5$, $l = 1, 11$; $\delta_g \leq 2^{r-5}$, $g = 2, 7$. Using (A.4), (A.9), and the equalities $\Delta_1 + \ldots + \Delta_5 = \Delta$, $\delta_0 = \delta_3 = \delta_5 = \delta_6 = 0$, we obtain $|Y(\Psi)| \geq 14 \cdot 2^{r-5} - 2\Delta \geq 14 \cdot 2^{r-5} - \Delta - 5 \cdot 2^{r-5}/9$. Again (A.5) is violated. Thus, for the given f_1, f_2, the first relationship in (A.2) must hold.

Examining similarly the remaining pairs of columns f_1, f_2 of weight 2, 3, we conclude that $m_2 + m_3 \leq 2$ for $K_{ij} = K_{41}$, i.e., condition (A.2) holds and the matrix H has property Z.

Similar methods, using when necessary the first inequality in (A.4), will show that (A.2) also holds in cases b and c. Q.E.D.

We would like to acknowledge the valuable advice and comments of E. M. Gabidulin. We also acknowledge the useful and constructive discussion of the paper by P. Yu. Smelyanskii and the participants of the IPPI AN SSSR seminar on algebraic coding theory.

LITERATURE CITED

1. F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1977).
2. W. Peterson and E. Weldon, Error-Correcting Codes, MIT Press, Cambridge, Mass. (1972).
3. R. L. Graham and N. J. A. Sloane, "On the covering radius of codes," IEEE Trans. Inform. Theory, **31**, No. 3, 385-401 (1985).
4. T. Helleseth, "On the covering radius of cyclic linear codes and arithmetic codes," Discr. Appl. Math., **11**, No. 2, 157-173 (1985).
5. G. D. Cohen, M. G. Karpovsky, H. F. Mattson, and J. R. Shatz, "Covering radius — survey and recent results," IEEE Trans. Inform. Theory, **31**, No. 3, 328-343 (1985).
6. R. C. Bose, "Mathematical theory of the symmetrical factorial design," Sankhya, **8**, 107-166 (1947).
7. B. Qwist, "Some remarks concerning curves of the second degree in a finite plane," Ann. Acad. Sci. Fenn. Helsinki, Ser. A1, **134**, 1-27 (1952).
8. G. Tallini, "On caps of kinds in a Galois r-dimensional space," Acta Arithmet., **7**, No. 1, 19-28 (1961).

9. R. C. Bose and J. N. Srivastava, "On a bound useful in the theory of factorial designs and error correcting codes," Ann. Math. Stat., **35**, No. 1, 408-414 (1964).
10. B. Segre, "Introduction to Galois geometries," Atti. Accad. Naz. Lincei Memorie, **8**, 133-236 (1967).
11. R. Hill, "Caps and codes," Discr. Math., **22**, No. 2, 111-137 (1978).
12. J. W. P. Hirschfeld and J. A. Thas, "Linear independence in finite spaces," Geom. Dedicata, **23**, No. 1, 15-31 (1987).
13. M. Plotkin, "Binary codes with specified minimum distance," IEEE Trans. Inform. Theory, **6**, No. 4, 445-450 (1960).
14. N. J. A. SLoane and D. S. Whitehead, "A new family of single-error-correcting codes," IEEE Trans. Inform. Theory, **16**, No. 5, 717-719 (1970).
15. V. I. Panchenko, "On optimization of linear codes with distance 4," Proc. 8th All-Union Conf. on Coding Theory and Information Transmission, Abstracts of Papers [in Russian], part II, Moscow—Kuibyshev (1981), pp. 132-134.
16. É. É. Nemirovskii and S. L. Portnoi, "Matching block codes to a channel with phase jumps," Prob. Peredachi Inform., **23**, No. 3, 27-34 (1986).
17. J. H. B. Kemperman, "On small subsets in an abelian group," Acta Math. Stockholm, **103**, Nos. 1-2, 63-88 (1960).
18. I. M. Boyarinov, A. A. Davydov, and B. M. Shabanov, "Error correction in the main memory of a high-throughput computer," Avtomat. Telemekh., No. 7, 152-165 (1987).
19. S. Azumi and T. Kasami, "On optimal modified Hamming codes," Trans. Inst. Electr. Commun. Eng. Jpn., **A58**, No. 6, 325-330 (1975).
20. A. A. Davydov, L. N. Kaplan, Yu. B. Smerkis, and G. L. Tauglikh, "On optimization of shortened Hamming codes," Prob. Peredachi Inform., **17**, No. 4, 63-72 (1981).
21. A. A. Davydov and L. M. Tombak, "On the number of minimum weight words in block codes," Prob. Peredachi Inform., **24**, No. 1, 11-24 (1988).
22. H. C. A. van Tilborg, "The smallest length of binary 7-dimensional linear codes with prescribed minimum distance," Discr. Math., **33**, No. 2, 197-207 (1981).
23. V. N. Logachev, "Refining the Griesmer bound for small code distances," in: Optimization Methods and Their Applications [in Russian], Izd. Sib. Otd. AN SSSR, Irkutsk (1974), pp. 107-111.
24. A. A. Davydov and L. M. Tombak, "An alternative to Hamming codes for correcting single errors in supercomputer memories," Proc. 2nd All-Union Conf. on Topical Issues of Informatics and Computer Science, Abstracts of Papers [in Russian], Erevan (1987), pp. 23-25.