Bounds on the Dimension of Codes and Subcodes with Prescribed Contraction Index

Alexander Vardy, Jakov Snyders, and Yair Be'ery
Tel Aviv University
Ramat Aviv 69978
Tel Aviv, Israel

Submitted by Vera S. Pless

ABSTRACT

Let $\mathscr{C}$ be a linear code over GF(q), spanned by the rows of a matrix $\mathbf{G}$ of rank k. A nonnegative integer λ is said to be the contraction index of $\mathscr{C}$ if a maximal set of pairwise linearly independent columns of $\mathbf{G}$ has $k + \lambda$ elements. We derive several upper and lower bounds on the dimension of a proper subcode of $\mathscr{C}$ with a prescribed contraction index $\nu < \lambda$. We also present an upper bound on the dimension of any linear code over GF(q) of length n, minimum Hamming distance d, and contraction index λ. For certain values of n and d the latter bound is shown to be tight for all q and λ. This substantially generalizes the results obtained by Delsarte and by Duc for $\lambda = 1$.

1. INTRODUCTION

Let $\mathscr{C}$ be an (n, k) *linear code* of length n and dimension k over GF(q), the finite field with q elements. Thus $\mathscr{C}$ is a k-dimensional linear subspace of the space of all the q-ary n-tuples. If $\{v_1, v_2, \ldots, v_k\}$ is a basis for $\mathscr{C}$, the matrix $\mathbf{G}$ having $\{v_1, v_2, \ldots, v_k\}$ as its rows is called a *generator matrix* of $\mathscr{C}$. Given a set of nonzero vectors with entries from GF(q), we say that these vectors are *pairwise linearly independent* over GF(q) if no vector in the set is a scalar multiple of some other vector in the set. The *contraction index* λ of the code $\mathscr{C}$ is defined as

$$\lambda = \max_{S} [\operatorname{card}(S) - k],$$

655 Avenue of the Americas, New York, NY 10010 0024-3795/90/$3.50

where the maximum is taken over the family of all sets S of pairwise linearly independent columns of $\boldsymbol{G}$. Obviously $0 \leqslant \lambda \leqslant n-k$. If the maximal set S contains all the n columns of $\boldsymbol{G}$, then $\lambda = n-k$ is the codimension of $\mathscr{C}$. In general, a code with contraction index λ is *contractible*, in the terminology of [8], to a code with codimension λ.

Our goal in this paper is to provide some answers to the following questions:

(1) Given a quadruple of nonnegative integers n, d, q, and λ, what is the dimension $J(n,d,q,\lambda)$ of the largest linear code over GF(q) of length n, minimum Hamming distance d, and contraction index λ?

(2) Given a linear code $\mathscr{C}$ with contraction index λ, what is the dimension $J(\nu)$ of the largest subcode of $\mathscr{C}$ with a prescribed contraction index $\nu < \lambda$?

In the sequel we determine $J(n,d,q,\lambda)$ exactly for all q and λ, provided that n and d assume certain values. We also present an upper bound on $J(n,d,q,\lambda)$ for other values of n and d and provide upper and lower bounds on $J(\nu)$. These results are derived by examination of the structure of certain matrices using linear algebra and combinatorial counting.

While the general problem of finding $J(n,d,q,\lambda)$ originates from recent research concerned with maximum-likelihood soft decision decoding (see [8, 9]), the special case $\lambda = 1$ had already been intensively studied in the context of majority logic decoding. Delsarte [3] and Duc [4] proved an upper bound on $J(n,d,q,1)$,[1] which is attainable over any finite field, provided d is even. For odd d a tighter, also attainable bound was reported in [9]. Hence, $J(n,d,q,1)$ is determined. In Section 2 we derive a bound on $J(n,d,q,2)$. The method employed can be, in principle, pursued further to the point where one might conjecture a general upper bound which pertains to all values of λ (Theorem 11). However, we postpone the proof of this conjecture until Section 4, as a direct proof is cumbersome for $\lambda \geqslant 3$. In Section 3 we derive bounds on $J(\nu)$ which enable us to provide an estimate of $J(\nu)$ for $0 \leqslant \nu \leqslant \lambda - 2$ and, in most cases, determine the value of $J(\nu)$ exactly for $\nu = \lambda - 1$. In Section 4 we employ some of the relations developed in Section 3 to prove the bound on $J(n,d,q,\lambda)$. Finally, in Section 5 we shall demonstrate that the results obtained herein suffice for determining the value of $J(\nu)$, $\nu = 0,1,2,3,4,5,8,10,11$, for the (24, 12) extended binary Golay code.

[1] This bound is frequently and somewhat inappropriately interpreted as a bound on $J(1)$.

2. PRELIMINARIES

In this section we introduce notation which is assumed in the remainder of the paper. We let $\mathscr{C}$ be an (n,k) linear code over GF(q) with minimum Hamming distance d and contraction index λ. In the sake of brevity, we shall often refer to $\mathscr{C}$ as an $\langle\langle n,k,\lambda\rangle\rangle$ code. For any matrix $\boldsymbol{P}$ we define a *contracted version* of $\boldsymbol{P}$, denoted by $\boldsymbol{P}^*$, as a matrix consisting of a maximal set of pairwise linearly independent columns of $\boldsymbol{P}$. Let $\boldsymbol{G}$ be a generator matrix of $\mathscr{C}$. The (n^*,k) code generated by $\boldsymbol{G}^*$ is denoted $\mathscr{C}^*$, and the dual code of $\mathscr{C}^*$ is denoted $(\mathscr{C}^*)^\perp$. Clearly, $n^* = k + \lambda$, and λ is also the contraction index of $\mathscr{C}^*$. Let g_i be the ith column of $\boldsymbol{G}$. If scalar multiples of a vector $\boldsymbol{b}$ appear as columns of $\boldsymbol{G}$ at l distinct positions $i_1, i_2, \ldots, i_l$, we say that the set $\{g_{i_1}, g_{i_2}, \ldots, g_{i_l}\}$ constitutes a *block of columns* (or in brief a *block*) of *multiplicity* l with *representative* $\boldsymbol{b}$. A block of columns whose representative has Hamming weight 1 will be called a *unit block*. A unit block and the row in which its representative is nonzero are said to be *associated*.

For $J(n,d,q,\lambda)$ to be well defined n, d, q, and λ must satisfy certain constraints. For instance, $J(n,d,q,1)$ is defined only if $n \geqslant \lceil 3d/2 \rceil$. Conditions of similar nature are stated in Theorems 3, 4, and 15. Trivially, $J(n,d,q,\lambda) \leqslant n - \lambda$. This bound is attainable for $\lambda \geqslant 1$ over any finite field, provided $d = 1$ or $d = 2$. Therefore in the sequel we assume that $d \geqslant 3$.

THEOREM 1. $J(n,d,q,0) = \lfloor n/d \rfloor$.

Proof. As $\lambda = 0$, $\mathscr{C}^*$ is a (k,k) code and the identity matrix may be taken for $\boldsymbol{G}^*$. Thus the multiplicity of each of the k unit blocks in $\boldsymbol{G}$ must be at least d. ∎

THEOREM 2 [4].

$$J(n,d,q,1) \leqslant \left\lfloor \frac{2n}{d} \right\rfloor - 1. \tag{1}$$

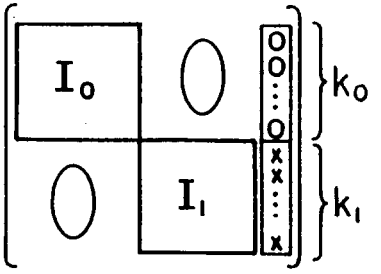
It is easily verified that (1) is actually an equality for an even d, provided that $n \geqslant 3d/2$. However, for an odd d, $J(n,d,q,1)$ is generally smaller. The proof presented here yields a much better insight than the proof of [9] and provides the ground for deriving additional results.

THEOREM 3. *If d is odd, then*

$$J(n,d,q,1) = \left\lfloor \frac{2(n+1)}{d+1} \right\rfloor - 1,$$

provided that $n+1 \geqslant 3(d+1)/2$.

Proof. As $\lambda = 1$, $\mathscr{C}^*$ is a $(k+1,k)$ code and $\boldsymbol{G}^*$ may be taken to be



where x stands for any nonzero element of GF(q), I_0 and I_1 are identity matrices, and $k_1 \geqslant 2$. Denote by $\tilde{l}$ the multiplicity of the block of columns whose representative is the rightmost column of $\boldsymbol{G}^*$, and let the numbers $m_1, m_2, \ldots, m_{k_0}$ and $l_1, l_2, \ldots, l_{k_1}$ be the multiplicities of the unit blocks associated with, respectively, zeros and nonzeros of the rightmost column of $\boldsymbol{G}^*$. Obviously, $m_i \geqslant d$ for all $i = 1,2,\ldots,k_0$. Also, $l_{i_1} + l_{i_2} \geqslant d$ whenever $i_1 \neq i_2$. Since d is odd, this implies that $l_i \geqslant (d+1)/2$ for $k_1 - 1$ values of i. For the remaining value, say $i = j$, we shall use $l_j + \tilde{l} \geqslant d$. Thus

$$n \geqslant \sum_{i=1}^{k_0} m_i + \sum_{\substack{i=1 \\ i \neq j}}^{k_1} l_i + \left(l_j + \tilde{l}\right) \geqslant k_0 d + (k_1 - 1)\frac{d+1}{2} + d$$

$$\geqslant (k-1)\frac{d+1}{2} + d.$$

This yields

$$J(n,d,q,1) \leqslant \left\lfloor \frac{2(n+1)}{d+1} \right\rfloor - 1. \tag{2}$$

By taking $k_0 = 0$, $l_1 = l_2 = \cdots = l_{k_1} = (d+1)/2$ and $\bar{l} = (d-1)/2 + \delta$, where $\delta \equiv n+1 \pmod{(d+1)/2}$, the upper bound is attained whenever $n+1 \geqslant 3(d+1)/2$. ■

THEOREM 4. *For even d*

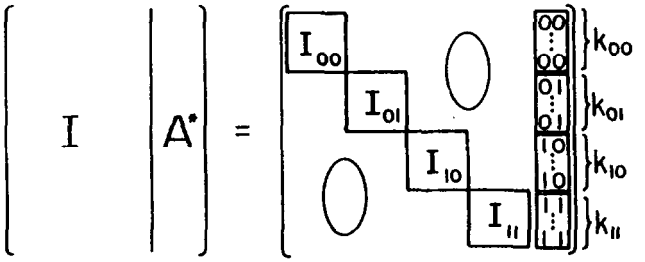
$$J(n,d,2,2) = \left\lfloor \frac{2(n-1)}{d} \right\rfloor - 1,$$

and for odd d

$$J(n,d,2,2) = \left\lfloor \frac{2(n+1)}{d+1} \right\rfloor - 1,$$

provided that $n \geqslant 2d+1$.

Proof. Since $\lambda = q = 2$, $\mathbf{G}^*$ may be assumed to have the following form:



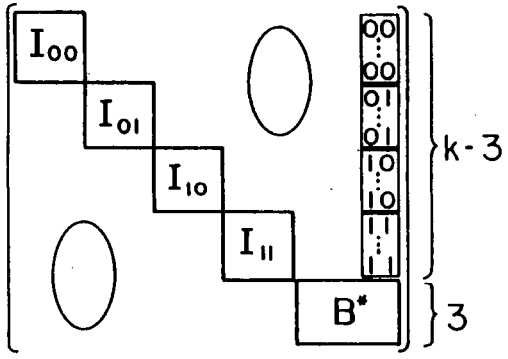
where $I_{00}, I_{01}, I_{10}, I_{11}$ are identity matrices and $k_{00} + k_{01} + k_{10} + k_{11} = k$. If two unit blocks of multiplicities (say) l_1 and l_2 are associated with identical rows of the matrix A^*, then evidently $l_1 + l_2 \geqslant d$. As $\lambda = 2$, the two columns of A^* are distinct, and the weight of each is at least 2. Hence, one of the following holds:

(a) $k_{11} = 0, \quad k_{01} \geqslant 2, \quad k_{10} \geqslant 2.$

(b) $k_{11} \geqslant 1, \quad k_{01} \geqslant 1, \quad k_{10} \geqslant 1.$

(c) $k_{11} \geqslant 2, \quad k_{01} \geqslant 1, \quad k_{10} = 0.$

Thus a row-permuted version of G^* is given by



where the multiplicity of each of the $k-3$ unit blocks is at least $\lceil d/2 \rceil$, and the matrix B^*, which includes the representatives of the three unit blocks whose multiplicities might be less than $\lceil d/2 \rceil$, is one of the following:

(a) $$B^* = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix},$$

(b) $$B^* = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix},$$

(c) $$B^* = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

In the three cases different sets of constraints are imposed on $l_1, l_2, \ldots, l_5$, the multiplicities of the five blocks of columns whose representatives constitute B^*. Yet they yield $l_1 + l_2 + l_3 + l_4 + l_5 \geq 2d + 1$ for each case. Hence,

$$n \geq (k-3)\frac{d}{2} + (2d+1) \qquad \text{if } d \text{ is even}$$

and

$$n + 1 \geq (k-3)\frac{d+1}{2} + (2d+2) \qquad \text{if } d \text{ is odd.}$$

Rearranging the above inequalities, we obtain

$$J(n,d,2,2) \leqslant \left\lfloor \frac{2(n-1)}{d} \right\rfloor - 1$$

and

$$J(n,d,2,2) \leqslant \left\lfloor \frac{2(n+1)}{d+1} \right\rfloor - 1,$$

respectively. Also it follows that $n \geqslant 2d+1$ for any $\langle\langle n,k,2\rangle\rangle$ binary code with minimum distance d. If this condition holds, the foregoing bounds are attainable as demonstrated, for instance, by the following matrices:

$$\begin{array}{cccccccc} d/2 & d/2 & d/2 & d/2 & d/2 & d/2 & d/2+\delta_1 & 1 \\ \left(\begin{array}{cccccccc} & & & 11\cdots1 & & & 11\cdots1 & 0 \\ & & & & 11\cdots1 & & 11\cdots1 & 1 \\ & & & & & 11\cdots1 & 11\cdots1 & 1 \\ 11\cdots1 & & & & & & 11\cdots1 & 1 \\ & 11\cdots1 & & & & & 11\cdots1 & 1 \\ & & \ddots & & & & \vdots & \vdots \\ & & 11\cdots1 & & & & 11\cdots1 & 1 \end{array}\right) \end{array}$$

and

$$\begin{array}{cccccccc} \frac{d+1}{2} & \frac{d+1}{2} & \frac{d+1}{2} & \frac{d-1}{2} & \frac{d-1}{2} & \frac{d+1}{2} & \frac{d+1}{2}+\delta_2 & 1 \\ \left(\begin{array}{cccccccc} & & & 11\cdots1 & & & 11\cdots1 & 0 \\ & & & & 11\cdots1 & & 11\cdots1 & 1 \\ & & & & & 11\cdots1 & 11\cdots1 & 1 \\ 11\cdots1 & & & & & & 11\cdots1 & 0 \\ & 11\cdots1 & & & & & 11\cdots1 & 0 \\ & & \ddots & & & & \vdots & \vdots \\ & & 11\cdots1 & & & & 11\cdots1 & 0 \end{array}\right), \end{array}$$

where blanks denote 0's, $\delta_1 \equiv n-1 \pmod{d/2}$, $\delta_2 \equiv n+1 \pmod{(d+1)/2}$, and the numbers above the matrices stand for the multiplicities of the corresponding blocks of columns. ■

By a similar argument one may show that

$$J(n,d,q,2) \leqslant \left\lfloor \frac{2n}{d} + \frac{q}{2} \right\rfloor - 2, \tag{3}$$

and if d is odd,

$$J(n,d,q,2) \leqslant \left\lfloor \frac{2(n+1)}{d+1} + \frac{q}{2} \right\rfloor - 2. \tag{4}$$

Yet the proof involves many different cases and is rather cumbersome. Instead, we shall establish (3) and (4) as a special case of a substantially more general result of Theorem 11.

3. BOUNDS ON THE DIMENSION OF A SUBCODE

LEMMA 5. *Let $(\mathscr{C}^*)^\perp$ contain a codeword of Hamming weight w. Then there exists an $\langle\langle n,k',\lambda'\rangle\rangle$ subcode $\mathscr{C}' \subset \mathscr{C}$ such that*

$$k' \geqslant k - \left\lfloor \frac{w-1}{2} \right\rfloor \quad \textit{and} \quad \lambda' \leqslant \lambda - 1.$$

Furthermore, if w is odd, then any generator matrix of $\mathscr{C}'$ contains a block of zero columns.

Proof. As $\boldsymbol{G}^*$ is a parity-check matrix of $(\mathscr{C}^*)^\perp$, a codeword of weight w in $(\mathscr{C}^*)^\perp$ corresponds to a set of w blocks of columns of $\boldsymbol{G}$ with representatives $\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_w$ satisfying

$$\alpha_1 \boldsymbol{b}_1 + \alpha_2 \boldsymbol{b}_2 + \cdots + \alpha_w \boldsymbol{b}_w = \boldsymbol{0} \tag{5}$$

for some nonzero $\alpha_1, \alpha_2, \ldots, \alpha_w \in \mathrm{GF}(q)$. Assume that w is even. Then by row operations followed by deletion of at most $w/2-1$ rows of $\boldsymbol{G}$ we may obtain a matrix $\boldsymbol{G}'$ such that

$$\alpha_i \boldsymbol{b}'_i + \alpha_{i+1} \boldsymbol{b}'_{i+1} = \boldsymbol{0} \qquad \text{for} \quad i = 1,3,\ldots,w-3,$$

where $\boldsymbol{b}'_j$ is the representative of the block of columns of $\boldsymbol{G}'$, which

originates from the block of $\mathbf{G}$ with representative $\boldsymbol{b}_j$. Hence by (5) we also have $\alpha_{w-1}\boldsymbol{b}'_{w-1} + \alpha_w \boldsymbol{b}'_w = \mathbf{0}$. Let $\mathscr{C}'$ be the subcode of $\mathscr{C}$ generated by $\mathbf{G}'$. Then $\mathscr{C}'$ has dimension $k' \geqslant k - (w/2 - 1)$ and contraction index $\lambda' \leqslant (n^* - w/2) - k' \leqslant \lambda - 1$. Now let w be odd. Then a similar argument demonstrates the existence of a matrix $\mathbf{G}'$ of rank $k' \geqslant k - (w-1)/2$ such that

$$\alpha_i \boldsymbol{b}'_i + \alpha_{i+1}\boldsymbol{b}'_{i+1} = \mathbf{0} \qquad \text{for} \quad i = 1, 3, \ldots w-2,$$

and $\boldsymbol{b}'_w = \mathbf{0}$. ∎

Let $D(n, k, q)$ be the largest *minimum distance* of a linear code of length n and dimension k over GF(q). The function $D(n, k, q)$ has been intensively studied (see in particular [5, 10, 11]) and is tabulated for $q = 2$ and $1 \leqslant k \leqslant n \leqslant 127$ in [12]. For some ν, $0 \leqslant \nu \leqslant \lambda - 1$, assume that $J_0, J_1, \ldots, J_{\nu-1}$ are *a priori* known upper bounds on $J(0), J(1), \ldots, J(\nu-1)$, respectively. Then the following theorem provides an upper bound on $J(\nu)$.

THEOREM 6. *Let J be the largest integer that satisfies either of the following two conditions*

(i) $$J \leqslant J_\mu + (q-1) \qquad \textit{for some} \quad \mu \leqslant \nu - 1,$$

and

(ii) $$J - \left\lfloor \frac{D(J+\nu, \nu, q) - 1}{2} \right\rfloor \leqslant J_{\nu-1}.$$

Then $J(\nu) \leqslant J$.

Proof. Let $\mathscr{V}$ be an $\langle\langle n, J(\nu), \nu \rangle\rangle$ subcode of $\mathscr{C}$. Then $\mathscr{V}^*$ is a $(J(\nu)+\nu, J(\nu))$ code and $(\mathscr{V}^*)^\perp$ is a $(J(\nu)+\nu, \nu)$ code. Denote by s the minimum distance of $(\mathscr{V}^*)^\perp$. By Lemma 5 there exists a subcode $\mathscr{V}' \subset \mathscr{V}$ with contraction index $\mu \leqslant \nu - 1$ and dimension J' such that

$$J' \geqslant J(\nu) - \left\lfloor \frac{s-1}{2} \right\rfloor. \tag{6}$$

If $s \leqslant 2q$ then

$$J' \geqslant J(\nu) - (q-1).$$

If $s \geqslant 2q+1$, then, in view of (6) and Theorem 9, we may set $\mu = \nu - 1$, and therefore

$$J_{\nu-1} \geqslant J' \geqslant J(\nu) - \left\lfloor \frac{D(J(\nu)+\nu, \nu, q) - 1}{2} \right\rfloor.$$

Hence, $J(\nu)$ satisfies either (i) or (ii). ■

A different upper bound on $J(\nu)$ will be derived using the following well-known result due to Griesmer [5] and Solomon and Stiffler [10].

THEOREM 7 (*The Griesmer bound*). *For any* (n,k) *code over* GF(q) *with minimum distance* d,

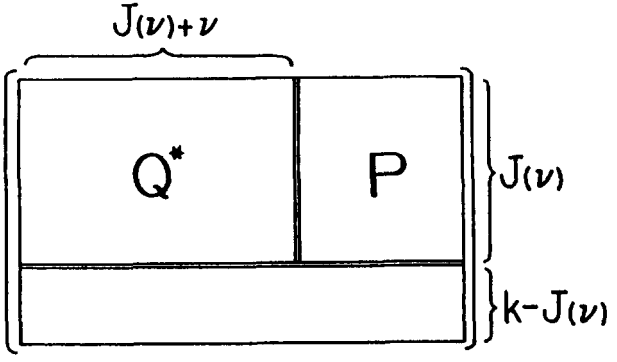
$$n \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil.$$

In the sequel $d^\perp$ denotes the minimum Hamming distance of $(\mathscr{C}^*)^\perp$.

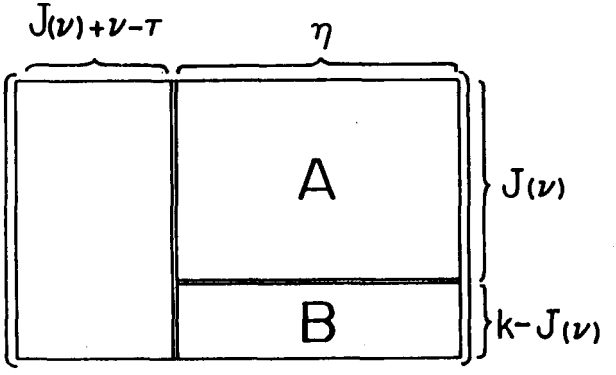
THEOREM 8. *For any pair of integers* ν *and* μ *such that* $0 \leqslant \nu \leqslant \mu \leqslant \lambda - 1$,

$$J(\nu) \leqslant n^* - \mu - \frac{1}{2} \sum_{i=0}^{\lambda-\mu-1} \left\lceil \frac{d^\perp}{q^i} \right\rceil. \tag{7}$$

Proof. Consider the case $\nu = \mu$. Let $\mathscr{Y}$ be an $\langle\langle n, J(\nu), \nu \rangle\rangle$ subcode of $\mathscr{C}$ generated by a matrix $\boldsymbol{Q}$. Then $\boldsymbol{G}^*$ is given by



where P has $n^* - [J(\nu) + \nu]$ columns. Denote by τ the number of columns of P^*, a contracted version of P. Let A be the matrix consisting of all the columns of P and those columns of Q^* that are scalar multiples of some column of P. Evidently, A has exactly $\eta = n^* - [J(\nu) + \nu] + \tau$ columns. Now write G^* as follows:



and define $\mathscr{D}$ to be the (η, κ) code obtained from $\mathscr{C}^*$ by deleting (puncturing out) the first $n^* - \eta$ coordinates. Let $\mathscr{D}^\perp$ be the dual code of $\mathscr{D}$. The minimum distance of $\mathscr{D}^\perp$ is at least $d^\perp$ (cf. [1, Lemma 1]). Hence, applying the Griesmer bound to $\mathscr{D}^\perp$, we have

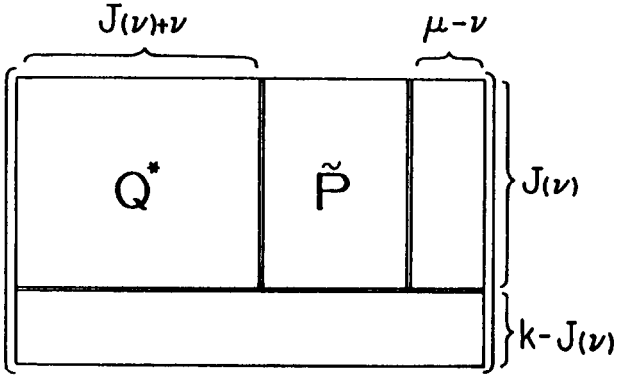
$$\eta \geqslant \sum_{i=0}^{\eta-\kappa-1} \left\lceil \frac{d^\perp}{q^i} \right\rceil.$$

Now $\kappa \leqslant \operatorname{rank}(A) + \operatorname{rank}(B) \leqslant \tau + [k - J(\nu)]$. Consequently $\eta - \kappa \geqslant \lambda - \nu$ and

$$n^* - [J(\nu) + \nu] + \tau \geqslant \sum_{i=0}^{\lambda-\nu-1} \left\lceil \frac{d^\perp}{q^i} \right\rceil.$$

In view of $\tau \leqslant n^* - [J(\nu) + \nu]$, the proof for $\nu = \mu$ is completed. To prove (7)

for $\nu < \mu$ write $\mathbf{G}^*$ in the following form:



where the matrix $\tilde{\boldsymbol{P}}$ has $n^* - [J(\nu) + \mu]$ columns. The result readily follows by substituting $\tilde{\boldsymbol{P}}$ for $\boldsymbol{P}$ in the foregoing argument. ■

To clarify our interest in the case $\nu < \mu$, consider the function

$$f(\nu) = n^* - \nu - \frac{1}{2} \sum_{i=0}^{\lambda-\nu-1} \left\lceil \frac{d^\perp}{q^i} \right\rceil$$

with n^*, $d^\perp$, q, and λ fixed. It has a global minimum at $\nu_0 = \lambda - \lceil \log_q d^\perp \rceil$. In fact, for $\nu < \nu_0$ we have $f(\nu) = f(\nu_0) + (\nu_0 - \nu)/2 > f(\nu_0)$. However, (7) implies an upper bound which is a monotonically nondecreasing function of ν.

We now show that (7) holds with equality for $\nu = \lambda - 1$, provided that $d^\perp \geqslant 2q + 1$.

THEOREM 9. *If* $d^\perp \geqslant 2q + 1$ *then*

$$J(\lambda - 1) = n^* - (\lambda - 1) - \left\lceil \frac{d^\perp}{2} \right\rceil.$$

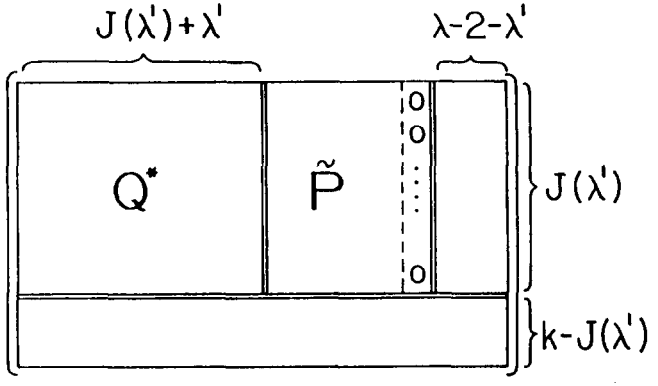
Proof. It follows from (7) that for $0 \leqslant \nu \leqslant \lambda - 2$ and $d^\perp \geqslant 2q + 1$,

$$J(\nu) \leqslant n^* - (\lambda - 2) - \frac{1}{2} \sum_{i=0}^{1} \left\lceil \frac{d^\perp}{q^i} \right\rceil \leqslant k - \frac{d^\perp - 1}{2}. \tag{8}$$

By Lemma 5, $J(\lambda') \geqslant k - \lfloor (d^{\perp} - 1)/2 \rfloor$ for some $\lambda' \leqslant \lambda - 1$. Assume that $0 \leqslant \lambda' \leqslant \lambda - 2$. Then using (8) we conclude that $d^{\perp}$ is odd and

$$J(\lambda') = k - \frac{d^{\perp} - 1}{2}. \tag{9}$$

Let $\mathscr{Y}$ be an $\langle\langle n, J(\lambda'), \lambda' \rangle\rangle$ subcode of $\mathscr{C}$ generated by a matrix $\boldsymbol{Q}$ which, according to Lemma 5, has at least one zero column. Then $\boldsymbol{G}^*$ may be written as follows:



and $\tilde{\tau}$, the number of columns of $\tilde{\boldsymbol{P}}^*$, is at most $n^* - [J(\lambda') + \lambda - 2] - 1$. Going through the proof of Theorem 8 again, with $\boldsymbol{P}$ replaced by $\tilde{\boldsymbol{P}}$, we obtain

$$n^* - [J(\lambda') + \lambda - 2] + \tilde{\tau} \geqslant \sum_{i=0}^{1} \left\lceil \frac{d^{\perp}}{q^i} \right\rceil.$$

As $d^{\perp} \geqslant 2q + 1$ and $\tilde{\tau} \leqslant n^* - [J(\lambda') + \lambda - 2] - 1$, this yields

$$J(\lambda') \leqslant n^* - (\lambda - 2) - \frac{1}{2}\left(d^{\perp} + \left\lceil 2 + \frac{1}{q} \right\rceil + 1 \right) = k - \frac{d^{\perp}}{2},$$

a contradiction to (9). Hence, $\lambda' = \lambda - 1$ and

$$J(\lambda - 1) = k - \left\lfloor \frac{d^{\perp} - 1}{2} \right\rfloor = n^* - (\lambda - 1) - \left\lceil \frac{d^{\perp}}{2} \right\rceil. \qquad \blacksquare$$

Clearly, there always exists some value of ν for which (7) holds with equality. However, this value of ν might be less than $\lambda-1$ if $d^{\perp} \leqslant 2q$. Finally, it is noteworthy that there exist codes for which the bound of Theorem 8 yields the value of $J(\nu)$ exactly for all $1 \leqslant \nu \leqslant \lambda-1$. For instance, let $\mathscr{C}$ be the q-ary Hamming code, defined by the parity-check matrix $\boldsymbol{H}$, whose columns are all the q-ary λ-tuples with first nonzero entry equal to 1. It may be shown that if q is even, then for $\nu = 1, 2, \ldots, \lambda-1$

$$J(\nu) \geqslant \frac{q^{\nu}(q^{\lambda-\nu}+1)-2}{2(q-1)} - \nu. \tag{10}$$

As the Hamming codes have the parameters [6] $n^* = n = (q^{\lambda}-1)/(q-1)$, $k = n-\lambda$, $d = 3$, and $d^{\perp} = q^{\lambda-1}$, substitution into (7) yields

$$J(\nu) \leqslant \frac{q^{\lambda}-1}{q-1} - \nu - \frac{1}{2}\sum_{i=0}^{\lambda-\nu-1} q^{\lambda-1-i} = \frac{q^{\nu}(q^{\lambda-\nu}+1)-2}{2(q-1)} - \nu.$$

Hence, (10) holds with equality and the bound of Theorem 8 is tight for $1 \leqslant \nu \leqslant \lambda-1$.

4. A BOUND ON $J(n, d, q, \lambda)$

In this section we present an upper bound on $J(n, d, q, \lambda)$ which includes all of (1)–(4) as special cases. Without loss of generality we assume throughout that $\boldsymbol{G}$, a generator matrix of $\mathscr{C}$, has the form $[\boldsymbol{U} \mid \boldsymbol{A}]$, where $\boldsymbol{U}$ consists of all the unit blocks of $\boldsymbol{G}$. Then $\boldsymbol{G}^* = [\boldsymbol{I} \mid \boldsymbol{A}^*]$. If $\boldsymbol{A}$ satisfies $(\boldsymbol{A}^{\mathrm{t}})^* = \boldsymbol{A}^{\mathrm{t}}$, where the superscript $^{\mathrm{t}}$ denotes transposition, we say that $\mathscr{C}$ is *row contracted*. The dimension of any row contracted code is obviously upper-bounded by $(q^{\lambda}-1)/(q-1)$. For $\lambda \geqslant 2$, let $\boldsymbol{M}$ be the matrix having as its rows some $(q^{\lambda}-1)/(q-1)$ pairwise linearly independent q-ary λ-tuples. Denote by $\boldsymbol{M}_0$ the submatrix of $\boldsymbol{M}$ consisting of all the rows with Hamming weight at least 2.

LEMMA 10. *Let $\boldsymbol{M}[i]$ be a matrix obtained by deleting some i rows from $\boldsymbol{M}$. If $i \geqslant \lambda+1$, then $\boldsymbol{M}[i]$ has a column of weight at most $q^{\lambda-1}-2$. Furthermore, $\boldsymbol{M}[\lambda]$ does not contain a column of weight less than $q^{\lambda-1}-1$ iff $\boldsymbol{M}[\lambda] = \boldsymbol{M}_0$.*

Proof. Each column of $\boldsymbol{M}$ contains $q^{\lambda-1}$ nonzero entries. The result thus follows by counting the total number of nonzeros in $\boldsymbol{M}[i]$ by rows and then by columns. ■

THEOREM 11. *For* $\lambda \geqslant 1$,

$$J(n,d,q,\lambda) \leqslant \left\lfloor \frac{2n}{d} + \frac{q^{\lambda}-q}{2(q-1)} \right\rfloor - \lambda,$$

and if d *is odd*,

$$J(n,d,q,\lambda) \leqslant \left\lfloor \frac{2(n+1)}{d+1} + \frac{q^{\lambda}-q}{2(q-1)} \right\rfloor - \lambda.$$

Proof. We shall proceed by induction on λ. The inequalities (1) and (2) are regarded as induction base. The induction hypothesis is that for all $\nu = 1,2,\ldots,\lambda-1$,

$$J(n,d,q,\nu) \leqslant \left\lfloor \frac{2n}{d} + \frac{q^{\nu}-q}{2(q-1)} \right\rfloor - \nu,$$

and if d is odd,

$$J(n,d,q,\nu) \leqslant \left\lfloor \frac{2(n+1)}{d+1} + \frac{q^{\nu}-q}{2(q-1)} \right\rfloor - \nu.$$

It has to be shown that

$$n \geqslant \left(k - \frac{q^{\lambda}-q}{2(q-1)} + \lambda\right)\frac{d}{2} \tag{11}$$

and if d is odd,

$$n+1 \geqslant \left(k - \frac{q^{\lambda}-q}{2(q-1)} + \lambda\right)\frac{d+1}{2}. \tag{12}$$

We assume that

$$k > \frac{q^\lambda - q}{2(q-1)} - \lambda,$$

as otherwise (11) and (12) trivially hold.

LEMMA 12. *The inequalities* (11) *and* (12) *hold, provided* $\mathscr{C}$ *is row contracted.*

Proof. We distinguish three cases. Since the proof employs Lemma 5, which discriminates between odd and even weight codewords, we also have to distinguish between odd and even values of q in cases 2 and 3.

Case 1: $\boldsymbol{A}^* = \boldsymbol{M}[i]$, $\lambda + 1 \leqslant i \leqslant \lambda + \lfloor (q^\lambda - 1)/2(q-1) \rfloor$. By Lemma 10 $\boldsymbol{A}^*$ contains a column of Hamming weight at most $q^{\lambda-1} - 2$. Such a column of $\boldsymbol{A}^*$ corresponds to a codeword of $(\mathscr{C}^*)^\perp$ of weight $w \leqslant q^{\lambda-1} - 1$. Hence by Lemma 5 $\mathscr{C}$ contains an $\langle\langle n, k', \lambda' \rangle\rangle$ subcode $\mathscr{C}'$, where

$$\lambda' \leqslant \lambda - 1 \quad \text{and} \quad k' \geqslant k - \left\lfloor \frac{w-1}{2} \right\rfloor \geqslant k - \left\lfloor \frac{q^{\lambda-1} - 2}{2} \right\rfloor.$$

Let $d' = d + \delta$, $\delta \geqslant 0$, denote the minimum distance of $\mathscr{C}'$. If δ is even, then by the induction hypothesis

$$n \geqslant \left(k' - \frac{q^{\lambda-1} - q}{2(q-1)} + \lambda - 1 \right) \frac{d'}{2}, \tag{13}$$

and if d is odd,

$$n + 1 \geqslant \left(k' - \frac{q^{\lambda-1} - q}{2(q-1)} + \lambda - 1 \right) \frac{d'+1}{2} \tag{14}$$

In view of $k' \geqslant k - q^{\lambda-1}/2 + 1$, (13) and (14) yield respectively (11) and (12). Finally, if δ is odd, then $d' \geqslant d + 1$ and (12) follows from (13).

Case 2: $\boldsymbol{A}^* = \boldsymbol{M}[\lambda]$. We may assume that $\boldsymbol{A}^* = \boldsymbol{M}_0$ and $q \neq 2^m$, since otherwise the proof of case 1 applies. Note that $\boldsymbol{G}^* = [\boldsymbol{I} \mid \boldsymbol{M}_0]$ contains rows of weight 3. This implies the existence of three blocks of columns of $\boldsymbol{G}$, so that one of them (consisting of, say, the first l columns) has multiplicity at

least $d/3$. Consider the $\langle\langle n-l, k-1, \lambda\rangle\rangle$ code $\mathscr{Y}$ obtained from $\mathscr{C}$ by *shortening* [6], that is, by taking all the codewords that have 0's in the first l coordinates and then deleting those 0's. A generator matrix of $\mathscr{Y}^*$ may be written as $[\boldsymbol{I} \mid \boldsymbol{M}[\lambda+1]]$. Using Lemmas 5 and 10, we conclude that $\mathscr{Y}$ contains a subcode $\mathscr{Y}'$ with parameters

$$n' = n - l, \qquad k' \geqslant (k-1) - \left\lfloor \frac{q^{\lambda-1}-2}{2} \right\rfloor = k - \frac{q^{\lambda-1}-1}{2},$$

$$d' \geqslant d, \qquad \lambda' \leqslant \lambda - 1.$$

By applying the induction hypothesis to $\mathscr{Y}'$, in view of $l \geqslant d/3$, we obtain (11) and (12).

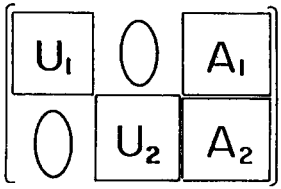
Case 3: $\boldsymbol{A}^* = \boldsymbol{M}[i]$, $0 \leqslant i \leqslant \lambda - 1$. At least one row of $\boldsymbol{A}^*$ has weight 1. Hence assume that the bottom row of $\boldsymbol{G}^*$ has weight 2, and let l_1, l_2 denote the multiplicities of the two blocks whose representatives, $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ respectively, have nonzero entries in the bottom row of $\boldsymbol{G}$. Since $l_1 + l_2 \geqslant d$, we may further assume that $l_1 \geqslant \lceil d/2 \rceil$, where l_1 is the multiplicity of the block consisting of the first l_1 columns of $\boldsymbol{G}$. Let $\mathscr{Y}$ be the $\langle\langle n - l_1, k-1, \lambda\rangle\rangle$ code obtained from $\mathscr{C}$ by shortening the first l_1 coordinates. Then a generator matrix of $\mathscr{Y}$ contains a block of columns with representative of weight at most $q^{\lambda-1}-1$, which results by deleting the last coordinate of $\boldsymbol{b}_2$. This implies the existence of a codeword $\boldsymbol{u} \in (\mathscr{Y}^*)^{\perp}$ of weight $w \leqslant q^{\lambda-1}$. Hence, using Lemma 5, $\mathscr{Y}$ contains an $\langle\langle n - l_1, k', \lambda'\rangle\rangle$ subcode $\mathscr{Y}'$ with minimum distance $d' \geqslant d$, where $\lambda' \leqslant \lambda - 1$ and $k' \geqslant (k-1) - \lfloor (w-1)/2 \rfloor$. Now if either $q = 2^m$ or $w < q^{\lambda-1}$, then $k' \geqslant k - q^{\lambda-1}/2$ and the inequalities (11) and (12) follow by applying the induction hypothesis to $\mathscr{Y}'$. Hence we assume that $q \neq 2^m$ and $w = q^{\lambda-1}$. Yet in this case w is odd, and since one of the nonzero entries of $\boldsymbol{u}$ corresponds to a block of multiplicity l_2, Lemma 5 implies that any generator matrix of $\mathscr{Y}'$ contains a block of l_2 zero columns. Puncturing these zero columns out, we obtain a code $\mathscr{Y}''$ with parameters

$$n'' = (n - l_1) - l_2 \leqslant n - d, \qquad k'' = k', \qquad d'' = d' \geqslant d, \qquad \lambda'' = \lambda' \leqslant \lambda - 1.$$

Substitution of these parameters into the induction hypothesis yields (11) and (12). ■

The foregoing lemma proves the induction step for a row contracted code. Yet if $\mathscr{C}$ is not row contracted, then $\boldsymbol{G}$ may be assumed to have the following

form:



where U_1 and U_2 consist of the unit blocks of G, $(A_1^t)^* = A_1^t$, and all the nonzero rows of A_2 are scalar multiples of some row of A_1. Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be the (n_1, k_1) and (n_2, k_2) codes generated by, respectively, $G_1 = [U_1 \mid A_1]$ and $G_2 = [U_2 \mid A_2]$. We claim the following:

LEMMA 13. *The code $\mathscr{C}_1$ is a row contracted code with contraction index at most λ, minimum distance at least d. Furthermore the following properties hold:*

(i) $k = k_1 + k_2$.
(ii) $n \geqslant n_1 + k_2\lceil d/2 \rceil$.

Proof. We prove only (ii), as the rest is obvious. If two unit blocks of G of multiplicities l_1 and l_2 are associated with rows of A that are linearly dependent, then $l_1 + l_2 \geqslant d$. Thus G_2 may be chosen so that the multiplicity of each unit block of U_2 is at least $\lceil d/2 \rceil$, and property (ii) follows. ■

Using Lemmas 12 and 13, we have

$$n_1 \geqslant \left(k_1 - \frac{q^\lambda - q}{2(q-1)} + \lambda \right) \frac{d}{2},$$

and if d is odd,

$$n_1 + 1 \geqslant \left(k_1 - \frac{q^\lambda - q}{2(q-1)} + \lambda \right) \frac{d+1}{2}.$$

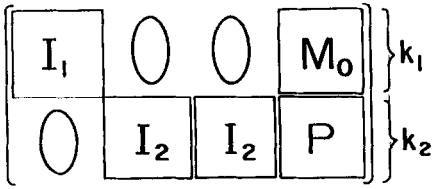
The above inequalities together with properties (i) and (ii) establish the induction step for any linear code $\mathscr{C}$, which completes the proof of Theorem 11. ■

In the sequel we present several explicit constructions that attain the bound of Theorem 11 for various values of n, d, q, and λ.

THEOREM 14. *For* $\lambda \geq 2$ *and* $n \geq (q^\lambda - 1)/(q-1)$,

$$J(n,3,q,\lambda) = \left\lfloor \frac{q^\lambda + n(q-1) - 1}{2(q-1)} \right\rfloor - \lambda.$$

Proof. Consider the following construction:



(15)

where

$$k_1 = \frac{q^\lambda - 1}{q-1} - \lambda, \qquad k_2 = \left\lfloor \frac{n - k_1 - \lambda}{2} \right\rfloor,$$

$\boldsymbol{I}_1$ and $\boldsymbol{I}_2$ are identity matrices, $\boldsymbol{M}_0$ is as previously defined, and $\boldsymbol{P}$ is any matrix which does not contain zero rows. Assume that $n - k_1 - \lambda$ is even. Then the $\langle\langle n, k_1 + k_2, \lambda\rangle\rangle$ code generated by (15) attains the bound of Theorem 11. For the case of odd $n - k_1 - \lambda$, a bound meeting code is obtained by appending a column of weight 1 to (15). ■

Thus the upper bound of Theorem 11 is tight for any q and λ. Yet the above construction is not the only one that attains the bound of Theorem 11. For instance, several values of $J(n,d,q,2)$ for $q \neq 2$ and $d \neq 3$ are derived in the following theorem.

THEOREM 15.

(a) $J(n,4,3,2) = \frac{n}{2} - 1$ *for* $n = 2m, \quad m \geqslant 3.$

(b) $J(n,5,3,2) = \left\lfloor \frac{2n-1}{6} \right\rfloor$ *for* $n \geqslant 8.$

(c) $J(n,6,3,2) = \left\lfloor \frac{2n-3}{6} \right\rfloor$ *for* $n = 3m \text{ or } 3m+1, \quad m \geqslant 3.$

(d) $J(n,5,4,2) = \frac{n-1}{3}$ *for* $n = 3m+1, \quad m \geqslant 3.$

(e) $J(n,6,4,2) = \frac{n-2}{3}$ *for* $n = 3m+2, \quad m \geqslant 3.$

Proof. Consider the following constructions:

(a) $$\begin{pmatrix} 11 & 00 & 11 \\ 00 & 11 & 12 \end{pmatrix},$$

(b) $$\begin{pmatrix} 1 & 0 & 111 & 111 \\ 0 & 1 & 111 & 222 \end{pmatrix},$$

(c) $$\begin{pmatrix} 111 & 00 & 11 & 11 \\ 000 & 11 & 11 & 22 \end{pmatrix},$$

(d) $$\begin{pmatrix} 11 & 00 & 0 & 111 & 11 \\ 00 & 11 & 0 & 111 & \omega\,\omega \\ 00 & 00 & 1 & 111 & \bar{\omega}\,\bar{\omega} \end{pmatrix},$$

(e) $$\begin{pmatrix} 111 & 00 & 00 & 11 & 11 \\ 000 & 11 & 00 & 11 & \omega\,\omega \\ 000 & 00 & 11 & 11 & \bar{\omega}\,\bar{\omega} \end{pmatrix},$$

where ω and $\bar{\omega}$ are zeros of $x^2 + x + 1$ and $\bar{\omega}^2 = \omega$. These yield

(a) $$J(6,4,3,2) \geqslant 2,$$

(b) $$J(8,5,3,2) \geqslant 2,$$

(c) $$J(9,6,3,2) \geqslant 2,$$

(d) $$J(10,5,4,2) \geqslant 3,$$

(e) $$J(11,6,4,2) \geqslant 3.$$

For greater values of n we can easily extend the above constructions. Thus for instance the sequence

$$\begin{pmatrix} 00 & 11 & 00 & 11 \\ 00 & 00 & 11 & 12 \\ 11 & 00 & 00 & 11 \end{pmatrix}, \quad \begin{pmatrix} 00 & 00 & 11 & 00 & 11 \\ 00 & 00 & 00 & 11 & 12 \\ 00 & 11 & 00 & 00 & 11 \\ 11 & 00 & 00 & 00 & 11 \end{pmatrix},$$

$$\begin{pmatrix} 00 & 00 & 00 & 11 & 00 & 11 \\ 00 & 00 & 00 & 00 & 11 & 12 \\ 00 & 00 & 11 & 00 & 00 & 11 \\ 00 & 11 & 00 & 00 & 00 & 11 \\ 11 & 00 & 00 & 00 & 00 & 11 \end{pmatrix}, \cdots$$

yields

$$J(8,4,3,2) \geqslant 3, \qquad J(10,4,3,2) \geqslant 4, \qquad J(12,4,3,2) \geqslant 5, \ldots,$$

implying the lower bound on $J(n,4,3,2)$ for all $n = 2m$, $m \geqslant 3$. The other four constructions may be extended similarly. Theorem 11 provides the upper bounds in all the cases. ■

Another peculiar example of bound reaching codes is the family of $\langle\langle (q^\lambda - 1)/(q-1), J(\nu), \nu \rangle\rangle$ subcodes of a given q-ary Hamming code with codimension λ, where $\nu = 1, 2, \ldots, \lambda - 1$. Evidently, the minimum distance d of each of the $\lambda - 1$ subcodes is at least 3. Recall that if q is even then $J(\nu)$ is given by (10). Comparing the lower bound of (10) with the upper bound of Theorem 11, we conclude that d may not be greater than 3 and that (10) holds with equality. Hence these subcodes attain the bounds of Theorems 11 and 8, which, somewhat unexpectedly, coincide in this particular case.

We remark that the codes constructed in Theorems 14 and 15 are optimal in the sense discussed in this paper, i.e. for a fixed λ. Without fixing the contraction index one may possibly obtain codes of higher dimension for the same length and minimum distance. For instance, although $J(12,6,3,2) = 3$, there exists a (12,6) ternary code with minimum distance 6, namely the ternary Golay code. The motivation for restricting λ is that small contraction index implies low complexity of decoding (cf. [8, 9]).

5. AN EXAMPLE

A well-studied code (see for instance [7,2]) is the binary (24, 12) extended Golay code $\mathscr{G}$. It is an extremal doubly even self-dual code. Codewords of $\mathscr{G}$

of weight 8, called *octads*, hold the Steiner system $S(5,8,24)$. Evidently, the contraction index of $\mathscr{G}$ is 12. In this section we determine for $\mathscr{C} = \mathscr{G}$ the exact value of $J(\nu)$ for all $\nu = 0,1,2,3,4,5,8,10,11$.

PROPOSITION 16. *$J(0) \leqslant 3$, $J(1) \leqslant 5$, and $J(2) \leqslant 4$.*

Proof. We have $J(\nu) \leqslant J(24,8,2,\nu)$ for $0 \leqslant \nu \leqslant 2$. Hence,

$$J(0) \leqslant \lfloor 24/8 \rfloor,$$

$$J(1) \leqslant \lfloor 2\times 24/8 \rfloor - 1,$$

$$J(2) \leqslant \lfloor 2\times(24-1)/8 \rfloor - 1,$$

using Theorems 1, 2, and 4, respectively. ∎

It may be readily shown that the $\langle\langle 24,3,0\rangle\rangle$ and the $\langle\langle 24,5,1\rangle\rangle$ subcodes of $\mathscr{G}$ are unique up to a permutation of coordinates. The former is spanned by three disjoint octads, and the latter is spanned by five octads that share four common coordinates.

PROPOSITION 17. *$J(3) \leqslant 5$.*

Proof. By Theorem 11, $J(3) \leqslant \lfloor 2\times 24/8 \rfloor = 6$. The case $J(3) = 6$ is easily ruled out as follows. Let $\mathscr{V}$ be a $\langle\langle 24,6,3\rangle\rangle$ subcode of $\mathscr{G}$. Then since $D(6+3,3,2) = 4$, Lemma 5 implies the existence of a $(24,5)$ subcode $\mathscr{V}' \subset \mathscr{V}$ with contraction index at most 2. By the foregoing proposition the contraction index of $\mathscr{V}'$ must be 1, and since the $\langle\langle 24,5,1\rangle\rangle$ subcode of $\mathscr{G}$ is unique, we may assume that a generator matrix of $\mathscr{V}$ has the form

$$\begin{pmatrix} 1111 & 1111 & & & & & \\ 1111 & & 1111 & & & & \\ 1111 & & & 1111 & & & \\ 1111 & & & & 1111 & & \\ 1111 & & & & & 1111 & \\ \omega_1 & \omega_2 & \omega_3 & \omega_4 & \omega_5 & \omega_6 \end{pmatrix}, \tag{16}$$

where blanks denote 0's and $\omega_1, \omega_2, \ldots, \omega_6$ denote binary 4-tuples. If the Hamming weight of ω_1 is odd, then all the six 4-tuples must have odd weight, and the contraction index of $\mathscr{V}$ is 6. If ω_1 has even weight, then all the six 4-tuples must have even weight, and since the contraction index of $\mathscr{V}$ is 3, exactly three out of the six 4-tuples have weight 2. It follows that the weight of the bottom row of (16) is not divisible by 4, which is a contradiction. ∎

We note that the $\langle\langle 24,5,3\rangle\rangle$ subcode of $\mathscr{G}$ spanned by the five octads

$$\begin{pmatrix} 11111111000000000000000 \\ 00000000111111110000000 \\ 00000000000000001111111 \\ 11110000111100000000000 \\ 00000000110011000000111 \end{pmatrix}$$

is also unique up to a permutation of coordinates. The proof of the uniqueness of this subcode is rather long and is therefore omitted.

PROPOSITION 18. *$J(4) \leqslant 6$ and $J(5) \leqslant 7$.*

Proof. By Theorem 6, $J(4) \leqslant 7$. If $J(4) = 7$, then using Lemma 5 and $D(11,4,2) = 5$ we establish the existence of a $\langle\langle 24,5,\nu\rangle\rangle$ $(\nu \leqslant 3)$ subcode of $\mathscr{G}$, generated by a matrix having at least one zero column. Since both the $\langle\langle 24,5,1\rangle\rangle$ and the $\langle\langle 24,5,3\rangle\rangle$ subcodes of $\mathscr{G}$ are unique and both of them are generated by matrices with no column entirely zero, this leads to a contradiction. The fact that $J(5) \leqslant 7$ may be proved similarly. ■

PROPOSITION 19.

(i) *$J(\nu) \leqslant 8$ for $6 \leqslant \nu \leqslant 10$.*
(ii) *$J(11) = 9$.*

Proof. Evidently, $(\mathscr{G}^*)^{\perp} = \mathscr{G}^* = \mathscr{G}$. Hence $d^{\perp} = 8$ and (i), (ii) follow by applying Theorems 8 and 9, respectively. ■

The foregoing four propositions provide upper bounds on $J(\nu)$. Lower bounds may be obtained using the following generator matrix of $\mathscr{G}$:

$$\begin{pmatrix} 11111111 & 00000000 & 00000000 \\ 00000000 & 11111111 & 00000000 \\ 00000000 & 00000000 & 11111111 \\ 11110000 & 11110000 & 00000000 \\ 00000000 & 11110000 & 11110000 \\ 11001100 & 11001100 & 00000000 \\ 10101010 & 10101010 & 00000000 \\ 00000000 & 11001100 & 11001100 \\ 00000000 & 10101010 & 10101010 \\ 01111000 & 01111000 & 01111000 \\ 10011100 & 10011100 & 10011100 \\ 11111100 & 11111100 & 01010110 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \\ a_{10} \\ a_{11} \\ a_{12} \end{pmatrix}. \qquad (17)$$

For instance, rows $\{a_1, a_2, a_3, a_5, a_6\}$ span a subcode with contraction index 3, which is the unique $\langle\langle 24,5,3\rangle\rangle$ subcode of $\mathscr{G}$. Furthermore, consider the following sets of rows of (17):

$\nu = 0$: $\{a_1, a_2, a_3\}$,

$\nu = 1$: $\{a_1, a_2, a_3, a_4, a_5\}$,

$\nu = 2$: $\{a_1, a_2, a_3, a_{10}\}$,

$\nu = 3$: $\{a_1, a_2, a_3, a_5, a_6\}$,

$\nu = 4$: $\{a_1, a_2, a_3, a_4, a_5, a_6\}$,

$\nu = 5$: $\{a_1, a_2, a_3, a_4, a_5, a_6, a_8\}$,

$\nu = 6$: $\{a_1, a_2, a_3, a_4, a_5, a_{10}\}$,

$\nu = 7$: $\{a_1, a_2, a_3, a_{10}, a_{11}\}$,

$\nu = 8$: $\{a_1, a_2, a_3, a_4, a_5, a_6, a_8, a_{12}\}$,

$\nu = 9$: $\{a_1, a_2, a_3, a_4, a_5, a_6, a_9\}$,

$\nu = 10$: $\{a_1, a_2, a_3, a_4, a_5, a_6, a_8, a_{10}\}$,

$\nu = 11$: $\{a_1, a_2, a_3, a_4, a_5, a_6, a_8, a_{10}, a_{12}\}$.

Together with Propositions 16 through 19, this determines $J(\nu)$ for nine out of the twelve values of ν. These results are summarized in the following table:

ν	$J(\nu)$	ν	$J(\nu)$
0	3	6	6–8
1	5	7	5–8
2	4	8	8
3	5	9	7–8
4	6	10	8
5	7	11	9

Determination of the exact value of $J(\nu)$ for $\nu = 6, 7, 9$ is an open question.

Alexander Vardy wishes to thank Hagit Itzkowitz for her invaluable help.

REFERENCES

1 R. A. Brualdi, V. S. Pless, and J. S. Beissinger, On the MacWilliams identities for linear codes, *Linear Algebra Appl.* 107:181–189 (1988).

2 J. H. Conway, Three lectures on exceptional groups, in *Finite Simple Groups* (M. B. Powell and G. Higman, Eds.), Academic, New York, 1971, pp. 215–247.

3 P. Delsarte, A geometrical approach to a class of cyclic codes, *J. Combin. Theory* 6:340–358 (1969).

4 N. Q. Duc, On a necessary condition for L-step orthogonalization of linear codes and its applications, *Inform. and Control* 22:123–131 (1973).

5 J. H. Griesmer, A bound for error-correcting codes, *IBM J. Res. Develop.* 4:532–542 (1960).

6 F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, New York, 1977.

7 V. S. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* 5:215–228 (1968).

8 J. Snyders and Y. Be'ery, Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes, *IEEE Trans. Inform. Theory* 35:963–975 (1989).

9 J. Snyders and Y. Be'ery, An approach to maximum likelihood decoding of q-ary block codes, Proc. 1989 Conf. Inform. Sciences and Systems, Baltimore, Maryland, March 22–24, 1989, pp. 206–208.

10 G. Solomon and J. J. Stiffler, Algebraically punctured cyclic codes, *Inform. and Control* 8:170–179 (1965).

11 H. C. A. van Tilborg, The smallest lengths of binary 7-dimensional linear codes with prescribed minimum distance, *Discrete Math.* 33:197–207 (1981).

12 T. Verhoeff, An updated table of minimum-distance bounds for binary codes, *IEEE Trans. Inform. Theory* 33:665–680 (1987).

Received 1 October 1989; final manuscript accepted 23 December 1989