ELSEVIER

Discrete Mathematics 147 (1995) 57–72

DISCRETE MATHEMATICS

# Codes with a poset metric

Richard A. Brualdi*, Janine Smolin Graves, K. Mark Lawrence

*Department of Mathematics, University of Wisconsin-Madison, 480 Lincoln Drive, Madison, WI53706, USA*

Received 27 October 1993

**Abstract**

Niederreiter generalized the following classical problem of coding theory: given a finite field $F_q$ and integers $n > k \geqslant 1$, find the largest minimum distance achievable by a linear code over $F_q$ of length $n$ and dimension $k$. In this paper we place this problem in the more general setting of a partially ordered set and define what we call poset-codes. In this context, Niederreiter's setting may be viewed as the disjoint union of chains. We extend some of Niederreiter's bounds and also obtain bounds for posets which are the product of two chains.

## 1. Introduction

Let $F_q$ be a finite field and $F_q^m$ the vector space of $m$-tuples over $F_q$. Let $n$ be a positive integer. One of the basic problems of coding theory [1,5] is to determine the largest integer $d$ such that there exist $n$ vectors $h_1, h_2, \ldots, h_n$ in $F_q^m$ every $d-1$ of which are linearly independent. Let $H$ be the $m$ by $n$ matrix over $F_q$ whose columns are the vectors $h_1, h_2, \ldots, h_n$. Then $H$ is the parity check matrix of a linear code of length $n$ and dimension $n-m$ with minimum distance $d$. The problem of determining $d$ was generalized by Niederreiter [2–4] as follows.

Let $n_1, n_2, \ldots, n_s$ be positive integers and let

$$H = \{h_{(i,j)}\colon 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant n_i\} \tag{1}$$

be a system of $n_1 + n_2 + \cdots + n_s$ vectors in $F_q^m$ partitioned into $s$ ordered sets of vectors of cardinalities $n_1, n_2, \ldots, n_s$, respectively. Define

$$d(H) = \min \sum_{i=1}^{s} d_i,$$

where the minimum is extended over all integers $d_1, d_2, \ldots, d_s$ such that $0 \leqslant d_i \leqslant n_i$ $(1 \leqslant i \leqslant s)$ and $\sum_{i=1}^{s} d_i$ is positive, for which the set of vectors

$$\{h_{(i,j)}\colon 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant d_i\}$$

* Corresponding author.

0012-365X/95/$09.50 
SSDI 0012-365X(94)00228-2

is linearly dependent. If there are no such integers $d_1, d_2, \ldots, d_s$ (implying that $n_1 + n_2 + \cdots + n_s \leqslant m$), then $d(H)$ is defined to be $n_1 + n_2 + \cdots + n_s + 1$.[1] Equivalently, $d(H)$ equals 1 plus the maximum integer $t$ such that for all partitions of $t$ into nonnegative parts $t_1, t_2, \ldots, t_s$ with $t_i \leqslant n_i$ $(1 \leqslant i \leqslant s)$, the vectors $\{h_{(i,j)}\colon 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant t_i\}$ are linearly independent. The problem raised and studied by Niederreiter is to find, or at least study, the number

$$d_q(n_1, n_2, \ldots, n_s; m) = \max d(H),$$

where the maximum is taken over all systems $H$ of the form (1). If $n_1 = n_2 = \cdots = n_s = 1$, then we have the fundamental problem of coding theory described above.

One can view Niederreiter's problem in the setting of a partially ordered set, henceforth abbreviated *poset*, in the following way. We are given a poset

$$P(n_1, n_2, \ldots, n_s) = \{(i,j)\colon 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant n_i\}$$

consisting of $s$ disjoint chains $N_1, N_2, \ldots, N_s$ of sizes $n_1, n_2, \ldots, n_s$, respectively. Recall that an *ideal* $I$ of a poset is a subset of its elements with the property that $x \in I$ and $y < x$ imply that $y \in I$. An ideal of $P(n_1, n_2, \ldots, n_s)$ is obtained by choosing for each $i$, all elements of $N_i$ at or below a specified element $x_i$ of $N_i$. Thus the ideals of size $t$ of $P(n_1, n_2, \ldots, n_s)$ are in one-to-one correspondence with partitions $t_1, t_2, \ldots, t_s$ of $t$ for which $0 \leqslant t_i \leqslant n_i$ for each $i = 1, 2, \ldots, s$. We are asked to assign vectors of $F_q^m$ to the elements of the poset $P(n_1, n_2, \ldots, n_s)$ in such a way that the vectors assigned to each ideal of size $t$ form a linearly independent set and $t$ is maximum (the number $d_q(n_1, n_2, \ldots, n_s; m)$ is then one more than this maximum value). If we take $n_i = 1$ for each $i$, then $N_i$ is a chain with only one element and $P(1, 1, \ldots, 1)$ is a trivial poset in which no two elements are comparable, that is, $P(1, 1, \ldots, 1)$ is an *antichain*. The above viewpoint suggests the possibility of extending Niederreiter's problem, and thus the fundamental problem of coding theory, to an arbitrary (finite) poset. We first introduce the idea of a poset metric.

Let $P$ be an arbitrary poset of cardinality $n$ whose partial order relation is denoted as usual by $\leqslant$. If $A \subseteq P$, then $\langle A \rangle$ denotes the smallest ideal of $P$ which contains $A$ (since the intersection of ideals is an ideal, $\langle A \rangle$ is the intersection of all ideals of $P$ containing $A$). Consider the vector space $F_q^n$ of $n$-tuples over $F_q$. Without loss of generality, we assume that $P = \{1, 2, \ldots, n\}$ and thus the coordinate positions of vectors in $F_q^n$ are in one-to-one correspondence with the elements of $P$. Let $x = (x_1, x_2, \ldots, x_n)$ be a vector in $F_q^n$. We define the *P-weight* of $x$ to be the cardinality

$$w_P(x) = |\langle \mathrm{supp}(x) \rangle|$$

of the smallest ideal of $P$ containing the *support* of $x$ where $\mathrm{supp}(x) = \{i\colon x_i \neq 0\}$. Note that if $x'$ is obtained from $x$ by changing one or more nonzero coordinates to zero,

[1] In this case Niederreiter defines $d(H)$ to be $m + 1$.

then it is possible that $w_P(x') = w_P(x)$. If $x$ and $y$ are two vectors in $F_q^n$, then their *P-distance* is

$$d_P(x, y) = w_P(x - y).$$

If $P$ is an antichain, then $P$-weight and $P$-distance are, respectively, Hamming weight and Hamming distance of classical coding theory.

**Lemma 1.1.** *If $P$ is a poset of $n$ elements, then $P$-distance $d_P(\cdot,\cdot)$ is a metric on $F_q^n$.*

**Proof.** Clearly, $P$-distance is symmetric and positive definite. To prove that $d_P(x,y) \leqslant d_P(x,z) + d_P(z,y)$ for all $x$, $y$ and $z$ it suffices to show that $P$-weight satisfies the triangle inequality $w_P(x + y) \leqslant w_P(x) + w_P(y)$. Since $\operatorname{supp}(x + y) \subseteq \operatorname{supp}(x) \cup \operatorname{supp}(y)$ and since the union of two ideals is also an ideal, we have

$$\begin{aligned} w_P(x + y) &\leqslant |\langle \operatorname{supp}(x)\rangle \cup \langle \operatorname{supp}(y)\rangle| \\ &\leqslant |\langle \operatorname{supp}(x)\rangle + \langle \operatorname{supp}(y)\rangle| \\ &= w_P(x) + w_P(y). \qquad \square \end{aligned}$$

We call the metric $d_P(\cdot,\cdot)$ on $F_q^n$ a *poset-metric*. If $F_q^n$ is endowed with a poset-metric, then we call a subset $C$ of $F_q^n$ a *poset-code*. If the poset-metric corresponds to a poset $P$, then $C$ is a *P-code*. We follow the usual notation of coding theory. Thus if $C$ is linear, that is, $C$ is a subspace of $F_q^n$ of dimension $k$, then $C$ is an $[n, k]$ poset-code. If $d_P$ is the minimum $P$-distance between distinct codewords of $C$ (if $C$ is linear, this is the same as the minimum $P$-weight of a nonzero codeword), then $C$ is an $[n, k, d_P]$ poset-code. Let $x$ be a vector in $F_q^n$ and let $r$ be a nonnegative integer. The *P-sphere* with *center* $x$ and *radius* $r$ is the set

$$S_P(x; r) = \{y \in F_q^n\colon d_P(x, y) \leqslant r\}$$

of all vectors in $F_q^n$ whose $P$-distance to $x$ is at most equal to $r$. The number of vectors in $F_q^n$ whose distance to the zero vector is exactly $i$ equals

$$\begin{cases} 1 & \text{if } i = 0, \\ \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i) & \text{if } i > 0, \end{cases} \tag{2}$$

where $\Omega_j(i)$ equals the number of ideals of $P$ with cardinality $i$ having exactly $j$ maximal elements. Since $d_P(x, y) = d_P(0, y - x)$, it follows that the number of vectors in a sphere of radius $r$ does not depend on its center and equals

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} (q-1)^j q^{i-j} \Omega_j(i). \tag{3}$$

In particular, if $q = 2$ the number of vectors in a sphere of radius $r$ equals

$$1 + \sum_{i=1}^{r} \sum_{j=1}^{i} 2^{i-j} \Omega_j(i).$$

**Example.** Let $q = 2$ and $n = 8$, and consider the poset $P$ with elements $\{1,2,3,4,5,6,7,8\}$ in which $1 < i$ for each $i = 2,3,\dots,8$ and these are the only strict comparabilities. Let $C$ be the $[8,4,4]$ binary code contained in $F_2^8$ obtained by adding an overall parity check to the $[7,4,3]$ binary Hamming code. Then a parity check matrix for $C$ is

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

The code $C$ has weight distribution $A_0 = 1$, $A_4 = 14$, $A_8 = 1$, where $A_i$ is the number of codewords with Hamming weight $i$.[2]

We now consider $C$ to be a $P$-code. Since $1 < i$ in $P$ for each $i = 2,3,\dots,n$, the only vector in $F_2^8$ with $P$-weight equal to 1, is the vector $(1,0,0,0,0,0,0,0)$. Every other vector in $F_2^8$ with Hamming weight equal to 1 has $P$-weight equal to 2. Of the 14 codewords of $C$ with Hamming weight equal to 4, exactly 7 have a 1 in position 1. Hence the $P$-weight distribution of $C$ is $A(P)_0 = 1$, $A(P)_4 = 7$, $A(P)_5 = 7$, $A(P)_8 = 1$. In particular, the minimum $P$-distance of $C$ equals 4. The number of vectors in a sphere of radius 2 equals $1 + 1 + 2(7) = 16 = 2^4$. We claim that the $P$-spheres of radius 2 about distinct codewords $c'$ and $c$ are pairwise disjoint. To show this it suffices to assume that $c' = 0$. Thus $c \neq 0$ and $c$ has $P$-weight at least 4. Suppose that there exists a vector $x \in F_2^8$ such that $d_P(0,x) \leqslant 2$ and $d_P(c,x) \leqslant 2$. Thus $w_P(x) \leqslant 2$ and, without loss of generality, $x = (a,b,0,0,0,0,0,0)$, where $a$ and $b$ are 0 or 1. Then $w_P(c) \geqslant 4$ implies that $c$ has 1's in at least two of the positions $3,4,\dots,8$. But then $d_P(c,x) \geqslant 3$, a contradiction. Thus the $P$-spheres about distinct codewords are disjoint and each contains $2^4$ vectors. Since there are $2^4$ codewords, the $P$-spheres of radius 2 about codewords perfectly cover $F_2^8$. We conclude that $C$ is a perfect code in the $P$-metric![3]

We now generalize Niederreiter's problem. Let $P$ be a poset with elements $\{1,2,\dots,n\}$. Let

$$H = \{h_i \colon 1 \leqslant i \leqslant n\} \tag{4}$$

be a system of vectors in $F_q^m$ indexed by the elements of $P$. Define $d_P(H)$ to be the minimum positive integer $d$ such that there exists an ideal $I$ of $P$ of size $d$ such that the vectors $\{h_i \colon i \in I\}$ are linearly dependent. If there is no such ideal (implying that $n \leqslant m$), then $d_P(H)$ is defined to be $n + 1$. Since every set of $m + 1$ vectors in $F_q^m$ is

[2] We follow the usual practice in coding theory of not listing the $A_i$ which equal 0.

[3] This is in contrast to the classical situation in which the $[7,4,3]$ Hamming code is perfect but the extended code $C$ is not.

linearly dependent, we have $d_P(H) \leqslant m + 1$. Viewing $H$ as a parity check matrix of an $[n, n - m]$ linear code $C$, we see that $d_P(H)$ is the minimum $P$-weight of a nonzero codeword of $C$ (equivalently, the minimum $P$-distance distinct between codewords). Let

$$d_q(P; m) = \max d_P(H),$$

where the maximum is taken over all systems (4). Thus $d_p(P; m)$ is the largest minimum $P$-distance attainable by an $[n, n - m]$ $P$-code over $F_q$. Clearly, $d_q(P; m) \leqslant m + 1$; furthermore, by choosing a system $H$ of nonzero vectors we see that $d_q(P; m) \geqslant d_p(H) \geqslant 2$. Hence

$$2 \leqslant d_q(P; m) \leqslant m + 1.$$

**Problem.** Determine $d_q(P; m)$ for different posets $P$.

In the next section we discuss perfect codes in certain $P$-metrics, and in particular we show that the extended binary Hamming codes and the extended binary Golay code are perfect codes in the $P$-metric where $P$ is a poset generalizing the poset in the preceding example. In the last section we first review the bounds on $d_q(n_1, n_2, \ldots, n_s; m) = d_q(P(n_1, n_2, \ldots, n_s); m)$ obtained by Niederreiter and then extend some of these bounds. We also discuss bounds on $d_2(P; m)$ for another natural poset $P$.

## 2. Perfect *P*-codes

Let $P$ be a poset with elements $\{1, 2, \ldots, n\}$, and let $C$ be a code in $F_q^n$ whose coordinate positions are indexed by the elements of $P$. Then $C$ is a *perfect P-code* provided there exists an integer $r$ such that the $P$-spheres of radius $r$ with centers at the codewords of $C$ are pairwise disjoint and their union is $F_q^n$.

We first characterize perfect $P$-codes in the case that $P$ is a chain.

**Theorem 2.1.** *Let $P$ be the poset with elements $\{1, 2, \ldots, n\}$ where $1 < 2 < \cdots < n$, and let $C$ be a code in $F_q^n$. Then $C$ is a perfect $P$-code if and only if there exists an integer $k$ with $0 \leqslant k \leqslant n$ such that $|C| = q^k$ and the set of all vectors $(x_{n-k+1}, \ldots, x_n)$ such that $(x_1, \ldots, x_{n-k}, x_{n-k+1}, \ldots, x_n) \in C$ for some $(x_1, \ldots, x_{n-k}) \in F_q^{n-k}$ equals $F_q^k$. In particular, the linear code $C_k$ of dimension $k$ consisting of all vectors $(0, \ldots, 0, a_{n-k+1}, \ldots, a_n)$ in $F_q^n$ whose first $n - k$ coordinates equal 0 is a perfect $P$-code with minimum $P$-distance equal to $n - k + 1$.*

**Proof.** We first show that the codes specified in the theorem are perfect. It follows from their defining properties that these codes have cardinality $q^k$ and minimum $P$-distance $n - k + 1$ and that there is a unique codeword with any prescribed last $k$ coordinates. Thus each vector $(y_1, \ldots, y_n)$ in $F_q^n$ is contained in the $P$-sphere of radius $n - k$ about some codeword of the form $(x_1, \ldots, x_{n-k}, y_{n-k+1}, \ldots, y_n)$, but is not contained in the $P$-sphere of radius $n-k+1$ about any other codeword. Hence $C_k$ is a perfect $P$-code.

Conversely, assume that $C$ is perfect $P$-code. Let $r$ be an integer such that the $P$-spheres of radius $r$ about the codewords of $C$ are pairwise disjoint and their union is $F_q^n$. The $P$-spheres of radius $r$ have cardinality $q^r$, and hence $|C| = q^{n-r}$. Let $y = (y_1, y_2, \ldots, y_n)$ be a vector in $F_q^n$. Then there exists a codeword $c$ such that $y$ is in $S_P(c; r)$ and hence a codeword $c$ of the form $c = (c_1, \ldots, c_r, y_{r+1}, \ldots, y_n)$. Hence $C$ has the form given in the theorem with $r = n-k$. $\square$

In contrast to the previous theorem, we now show that there are no nontrivial perfect $P$-codes if $P$ is a union of two disjoint chains of equal size.

**Theorem 2.2.** *Let $n = 2\ell$ be an even positive integer. Let $P$ be the poset consisting of two disjoint chains $N$ and $N'$ of the same size $\ell$. Then the only perfect $P$-codes $C$ in $F_q^n$ are $C = F_q^n$ and $C = \{x\}$ for each vector $x$ in $F_q^n$.*

**Proof.** Clearly the codes $C = F_q^{2\ell}$ and $C = \{x\}$ are perfect $P$-codes. We now show that there are no other perfect $P$-codes. Let the elements of $N$ be $\{1, 2, \ldots, \ell\}$, where $1 < 2 < \cdots < \ell$, and let the elements of $N'$ be $\{1', 2', \ldots, \ell'\}$, where $1' < 2' < \cdots < \ell'$. Suppose to the contrary that $C$ is a perfect $P$-code where $1 < |C| < q^{2\ell}$. Let $r$ be the integer such that the $P$-spheres of radius $r$ with centers at the codewords of $C$ are pairwise disjoint and cover $F_q^{2\ell}$. Then $1 \leqslant r \leqslant 2\ell - 1$.

First assume that $r \geqslant \ell$. Let $x = (x_1, \ldots, x_\ell, x_{1'}, \ldots, x_{\ell'})$ and $y = (y_1, \ldots, y_\ell, y_{1'}, \ldots, y_{\ell'})$ be any two vectors in $F_q^{2\ell}$. Then the vector $(x_1, \ldots, x_\ell, y_{1'}, \ldots, y_{\ell'})$ is contained in $S_P(x; r) \cap S_P(y; r)$. In particular, the $P$-spheres of radius $r$ about any two codewords overlap. Since $|C| \geqslant 2$, this contradicts the assumption that $C$ is perfect.

Now assume that $1 \leqslant r < \ell$. We first compute the cardinalities of $P$-spheres of radius $r$. Let $i$ be an integer with $1 \leqslant i \leqslant \ell$. It follows from (2) that the number of vectors whose distance to a given vector $x$ in $F_q^n$ equals $i$ is

$$\alpha_i = 2(q-1)q^{i-1} + (i-1)(q-1)^2 q^{i-2} = (q-1)q^{i-2}[(i+1)q - i + 1].$$

Hence for each vector $x$ we have

$$|S_P(x; r)| = 1 + \sum_{i=1}^{r} \alpha_i.$$

It follows by induction that

$$|S_P(x; r)| = q^{r-1}[r(q-1) + q]. \tag{5}$$

Since $C$ is perfect, $q^{2\ell} = |C|\,|S_P(x; r)|$. Hence there exists a positive integer $j$ such that $r(q-1) + q = q^j$. Thus $|S_P(x; r)| = q^{r+j-1}$. Moreover,

$$r = \frac{q^j - q}{q-1},$$

and since $r \geqslant 1$, we have $j \geqslant 2$. Thus $r = q(1 + q + \cdots + q^{j-2}) \geqslant 2(j-1) \geqslant j$. We have

$$|C| = q^{2\ell - r - j + 1} = q^{2(\ell - r) + r - (j-1)},$$

and since $r > j - 1$, it follows that $|C| > q^{2(\ell - r)}$. By the pigeon-hole principle, there exist distinct codewords $x = (x_1, \ldots, x_\ell, x_{1'}, \ldots, x_{\ell'})$ and $y = (y_1, \ldots, y_\ell, y_{1'}, \ldots, y_{\ell'})$ such that $x_i = y_i$ and $x_{i'} = y_{i'}$ for $i = r+1, \ldots, \ell$. Since the vector $(x_1, \ldots, x_\ell, y_{1'}, \ldots, y_{\ell'})$ is contained in $S_P(x; r) \cap S_P(y; r)$, the $P$-spheres of radius $r$ about the codewords $x$ and $y$ overlap, again contradicting the assumption that $C$ is perfect. □

We now generalize the example in Section 1 and show that there are simple posets $P$ such that the extended binary Hamming codes and extended Golay codes are perfect $P$-codes.

**Theorem 2.3.** *For each positive integer $n$ let $P_n$ denote the poset with elements $\{1, 2, \ldots, n\}$ in which $1 < i$ for each $i = 2, 3, \ldots, n$ and these are the only strict comparabilities. Then for each positive integer $m$ the extended binary Hamming $\mathscr{H}(m)$ code with parameters $[n = 2^m, 2^m - m - 1, 4]$ is a perfect $P_n$-code. In addition, the extended binary Golay code $G_{24}$ with parameters $[24, 12, 8]$ is a perfect $P_{24}$-code, and the extended ternary Golay code $G_{12}$ with parameters $[12, 6, 6]$ is a perfect $P_{12}$-code.*

**Proof.** The proof that $\mathscr{H}(m)$ is a perfect $P_n$-code follows as in the example in Section 1. Indeed the spheres of radius 2 about the $2^{2^m - m - 1}$ codewords each contain $2^{m+1}$ vectors and are pairwise disjoint, and hence they perfectly cover $F_2^{2^m}$. The argument is similar for the extended Golay codes. We give the argument only for the ternary Golay code. The number of codewords of $G_{12}$ equals $3^6$. Each $P_{12}$-sphere of radius 3 contains

$$1 + 2 + 2(3)(11) + 2^2 3 \binom{11}{2} = 729 = 3^6$$

vectors. Let $x$ be a vector whose $P_{12}$-distance to 0 is at most 3. Then at most 2 of coordinates $2, 3, \ldots, 12$ of $x$ are nonzero. Let $c$ be a nonzero codeword. Since each nonzero codeword of $G_{12}$ has Hamming weight at least 6, $w_{P_{12}}(x) \geqslant 6$. Hence at least 5 of coordinates $2, 3, \ldots, 12$ of $c$ are nonzero. This implies that $d_{P_{12}}(c, x) \geqslant 4$. We conclude that the $P_{12}$-spheres of radius 3 about codewords are pairwise disjoint, and hence $G_{12}$ is a perfect $P_{12}$-code. □

## 3. Bounds for $d_q(P; m)$

Throughout this section we use the following notation. Let $m$ be a positive integer consider the vector space $F_q^m$ over the finite field $F_q$. Let $n_1, n_2, \ldots, n_s$ be positive integers such that $n_1 \geqslant n_2 \geqslant \cdots \geqslant n_s$. If $n_1 + n_2 + \cdots + n_s \leqslant m$, then clearly $d_q(n_1, n_2, \ldots, n_s; m) = n_1 + n_2 + \cdots + n_s + 1$. As a result we henceforth assume that

$$n_1 + n_2 + \cdots + n_s > m. \tag{6}$$

The following basic results are proved by Niederreiter [2]:

(N1) $2 \leqslant d_q(n_1, n_2, \ldots, n_s; m) \leqslant m + 1$;

(N2) $d_q(n'_1, n'_2, \ldots, n'_s; m) \leqslant d_q(n_1, n_2, \ldots, n_s; m)$ if $n_i \leqslant n'_i$ for $i = 1, 2, \ldots, s$;

(N3) Let $n'_i = \min\{n_i, m\}$ for $i = 1, 2, \ldots, s$. Then

$$d_q(n_1, n_2, \ldots, n_s; m) = d_q(n'_1, n'_2, \ldots, n'_s; m);$$

(N4) If $s \leqslant q + 1$, then $d_q(n_1, n_2, \ldots, n_s; m) = m + 1$;

(N5) Assume that $m \geqslant 2$. Let $\omega_m$ be the smallest integer such that $n_1 + \cdots + n_{\omega_m} \geqslant m$. If $s \geqslant q + \max\{\omega_m, 2\}$, then

$$d_q(n_1, n_2, \ldots, n_s; m) \leqslant m.$$

In addition, using constructions based on linear recurrence relations, Niederreiter [3] obtained lower bounds for $d_q(n_1, n_2, \ldots, n_s; m)$ and also obtained the following results:

(N6) If $m \geqslant 2$ and $s \leqslant (q^m - 1)/(q - 1)$, then $d_q(n_1, n_2, \ldots, n_s; m) \geqslant 3$, and if $s > (q^m - 1)/(q - 1)$, then $d_q(n_1, n_2, \ldots, n_s; m) = 2$;

(N7) Assume that $q + 2 \leqslant s \leqslant (q^m - 1)/(q - 1)$. If $n_1 \geqslant m + 2 - \lfloor \log_q((q-1)(s-1)+1) \rfloor$, then

$$d_q(n_1, n_2, \ldots, n_s; m) \leqslant m + 2 - \lfloor \log_q((q - 1)(s - 1) + 1) \rfloor.$$

If $n_1 \leqslant m + 1 - \lfloor \log_q((q - 1)(s - 1) + 1) \rfloor$, then

$$d_q(n_1, n_2, \ldots, n_s; m) \leqslant m + 2 - \lfloor \log_q((q - 1)(s - \omega_m + 1) + 1) \rfloor.$$

In this section we extend some of the bounds given above. In what follows, for each integer $j$ with $1 \leqslant j \leqslant n_1 + \cdots + n_s$, $\omega_j$ denotes the smallest integer $t$ such that $n_1 + \cdots + n_t \geqslant j$.

Let $H = \{h_{(i,j)}: 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant n_i\}$ be a system of vectors in $F_q^m$. The vector $h_{(i,j)}$ is assigned to the $j$th element of the $i$th chain of the poset $P(n_1, n_2, \ldots, n_s)$. If $I$ is an ideal $P(n_1, n_2, \ldots, n_s)$, then $H_I$ denotes the set of vectors from $H$ assigned to the elements of $I$.

**Lemma 3.1.** *Let $H = \{h_{(i,j)}: 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant n_i\}$ be a system of $n$ vectors in $F_q^m$. Let $r$ be an integer with $1 \leqslant r \leqslant m - 2$. Assume that $\omega_{m-r} \geqslant 2$ and that*

$$s \geqslant \omega_{m-r} + q^{r+1} - q^2 + q. \tag{7}$$

*Also assume that $H_I$ is linearly independent for every ideal $I$ of size $m - r$ of $P = P(n_1, n_2, \ldots, n_s)$. Then there exists an ideal $J$ of $P$ of size $m$ having exactly $\omega_{m-r} + r$ maximal elements such that $H_J$ is linearly independent.*

**Proof.** Let $u = (m - r) - \sum_{i=1}^{\omega_{m-r}-1} n_i$. The set

$$I = \{(i, j)\colon 1 \leqslant i < \omega_{m-r},\ 1 \leqslant j \leqslant n_i\} \cup \{(\omega_{m-r}, j)\colon 1 \leqslant j \leqslant u\}$$

is an ideal of $P$ of size $m - r$, and hence $H_I$ is linearly independent. Let $b_i = h_{(i,n_i)}$ for $1 \leqslant i < \omega_{m-r}$ and $b_{\omega_{m-r}} = h_{(\omega_{m-r},u)}$ be the vectors from $H$ assigned to the maximal elements of $I$. Let $c_i = h_{(i+\omega_{m-r},1)}$ $(1 \leqslant i \leqslant s - \omega_{m-r})$ be the vectors assigned to the minimal elements of the last $s - \omega_{m-r}$ chains of $P$. We extend $H_I$ to a basis $H_I \cup \{v_1, \ldots, v_r\}$ of $F_q^m$. Let $\hat{c}_i$ denote the projection of $c_i$ onto the subspace $V$ of $F_q^m$ spanned by $\{v_1, \ldots, v_r\}$.

We first show that the number $t$ of $c_i$ whose projection $\hat{c}_i$ is the zero vector is at most $q - 1$. Assume to the contrary that $t > q - 1$. Let $i$ be an integer with $1 \leqslant i \leqslant s - \omega_{m-r}$ and suppose that $\hat{c}_i = 0$. The set $(H_I \setminus \{b_j\}) \cup \{c_i\}$ is the set of vectors assigned to an ideal of size $m - r$ and hence is linearly independent for $j = 1, \ldots, \omega_{m-r}$. Since $\hat{c}_i = 0$, it follows that the projection $\beta_{ij}$ of $c_i$ onto $b_j$ is not zero for each $j$. Since $\omega_{m-r} \geqslant 2$, we may take $j$ equal to 1 and 2 in turn. Thus $\alpha_i = \beta_{i1}/\beta_{i2}$ is defined and nonzero. Since there are only $q - 1$ possible values for the $\alpha_i$, it follows that there exist $k$ and $l$ such that $\hat{c}_k = \hat{c}_l = 0$ and $\alpha_k = \alpha_l$. It follows that $\beta_{l2}c_k - \beta_{k2}c_l$ is a linear combination of the vectors in $H_I \setminus \{b_1, b_2\}$. Then $(H_I \setminus \{b_1, b_2\}) \cup (c_k, c_l\}$ is a linearly dependent set of vectors assigned to an ideal of size $m - r$, a contradiction. Hence $t \leqslant q - 1$.

We now claim that the set $S = \{\hat{c}_i\colon 1 \leqslant i \leqslant s - \omega_{m-r}\}$ spans $V$. Assume the claim is false. Since the dimension of $V$ is $r$, it follows that $S$ is contained in some $(r - 1)$-dimensional subspace of $V$ and hence that $|S| \leqslant q^{r-1}$. Consider the $c_i$ such that $\hat{c}_i \neq 0$. By (7), $s - \omega_{m-r} > q^{r+1} - q^2 + q - 1$ and since $t \leqslant q - 1$, it now follows that the number $s - \omega_{m-r} - t$ of these $c_i$ is greater than $q^{r+1} - q^2$. Let $U$ be the subspace of $F_q^m$ spanned by $V \cup \{b_1, b_2\}$. Since there are $q^2$ vectors in the subspace spanned by $\{b_1, b_2\}$ and at most $q^{r-1} - 1$ projections of these $c_i$ into $V$, it follows that there are at most $q^2(q^{r-1} - 1) = q^{r+1} - q^2$ possible projections of these $c_i$ into $U$. We conclude that not all of these $c_i$ have distinct projections into $U$. Hence there exist $c_k$ and $c_l$ with $k \neq l$ whose projections into $U$ are equal. It follows that $c_k - c_l$ is a linear combination of the vectors in $H_I \setminus \{b_1, b_2\}$. Then $(H_I \setminus \{b_1, b_2\}) \cup \{c_k, c_l\}$ is a linearly dependent set of vectors assigned to an ideal of size $m - r$, a contradiction. Hence $S$ spans $V$.

Let $S'$ be a basis of $V$ consisting of vectors in $S$. Then $H_J = H_I \cup \{c_i\colon \hat{c}_i \in S'\}$ is a set of linearly independent vectors corresponding to an ideal $J$ of size $m$ having exactly $\omega_{m-r} + r$ maximal elements. $\square$

We now extend Niederreiter's result (N5) above. We first consider the case $q = 2$.

**Theorem 3.2.** *Let $r$ and $m$ be integers with $0 \leqslant r \leqslant m - 2$. Assume that*

$$\omega_{m-r} \geqslant 2r + 2. \tag{8}$$

*Also assume that*

$$s \geqslant \begin{cases} \omega_m + 2 & \text{if } r = 0, \\ \omega_{m-1} + 3 & \text{if } r = 1, \\ \omega_{m-r} + 2^{r+1} - 2 & \text{if } r \geqslant 2. \end{cases} \tag{9}$$

*Then*

$$d_2(n_1, n_2, \ldots, n_s; m) \leqslant m - r. \tag{10}$$

**Proof.** If $r = 0$ the result is a consequence of (N5). Now assume that $r \geqslant 1$. Suppose to the contrary that $d_2(n_1, n_2, \ldots, n_s; m) > m - r$. Then there exists a system $H = \{h_{(i,j)}: 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n_i\}$ of vectors in $F_2^m$ such that $H_I$ is linearly independent for every ideal $I$ of size $m - r$ of the poset $P = P(n_1, n_2, \ldots, n_s)$. It follows from (9) that (7) holds for $q = 2$ and that

$$s - \omega_{m-r} - r \geqslant 2 \tag{11}$$

holds for all $r \geqslant 1$. By Lemma 3.1, there exists an ideal $J$ of $P$ of size $m$ having exactly $\omega_{m-r} + r$ maximal elements such that $H_J$ is linearly independent and thus is a basis of $F_2^m$. For ease of notation we denote these basis vectors by $b_1, b_2, \ldots, b_m$. Let

$$T = \{i: 1 \leqslant i \leqslant s \text{ and } (i, 1) \in J\}$$

be the set of indices of the chains which have a nonempty intersection with $J$ and let $\bar{T}$ be the set of indices of the remaining chains. Then $|T| = \omega_{m-r} + r$ and by (11), $|\bar{T}| = s - |T| \geqslant 2$. Let $J_{\max}$ be the set of the $\omega_{m-r} + r$ maximal elements of $J$. Let $a_i = (i, 1)$ be the minimal element of the $i$th chain of $P$ $(1 \leqslant i \leqslant s)$, and write

$$a_i = \sum_{l=1}^{m} \beta_{il} b_l \quad (i \in \bar{T}).$$

Let $M$ be any subset of $J_{\max}$ with $|M| = r + 1$. Let $i \in \bar{T}$ and consider the ideal $I = (J \setminus M) \cup \{a_i\}$ of size $m - r$. Thus $H_I$ is linearly independent, and it follows that $\beta_{il} \neq 0$ for at least one $l$ such that $b_l \in H_M$. Since $M$ was an arbitrary subset of $J_{\max}$ of cardinality $r + 1$, it follows that $\beta_{il} = 0$ for at most $r$ values of $l$ with $b_l \in H_{J_{\max}}$. Since $|\bar{T}| \geqslant 2$ there exist distinct elements $j$ and $k$ in $\bar{T}$, and for any such $j$ and $k$, there exist at least $|J_{\max}| - 2r = \omega_{m-r} - r \geqslant r + 2$ values of $l$ with $b_l \in H_{J_{\max}}$ such that both $\beta_{jl} \neq 0$ and $\beta_{kl} \neq 0$. Here the last inequality is a consequence of hypothesis (8). Since we are working over the binary field, it follows that $\beta_{jl} = \beta_{kl} = 1$ for at least $r + 2$ indices $l$ with $b_l \in H_{J_{\max}}$. Without loss of generality, $\beta_{jl} = \beta_{kl}$ for $l = 1, 2, \ldots, r + 2$. We then have

$$a_j - a_k = \sum_{l=r+3}^{m} (\beta_{jl} - \beta_{kl}) b_l.$$

It follows that $\{b_{r+3}, \ldots, b_m, a_j, a_k\}$ is a linearly dependent set of vectors corresponding to an ideal of $P$ of size $m - r$, a contradiction. Hence (10) holds. $\square$

We now obtain the conclusion of Theorem 3.2 for arbitrary $q$. Note that the assumptions of Theorem 3.3 when $q = 2$ are not identical to the assumptions of Theorem 3.2.

**Theorem 3.3.** *Let $r$ and $m$ be integers with $0 \leqslant r \leqslant m - 2$. Assume that*

$$\omega_{m-r} \geqslant r + 2. \tag{12}$$

*Also assume that* (7) *holds and that*

$$s \geqslant \omega_{m-r} + r + \binom{2r+2}{r+2}(q-1)^{r+1} + 1. \tag{13}$$

*Then*

$$d_q(n_1, n_2, \ldots, n_s; m) \leqslant m - r. \tag{14}$$

**Proof.** The first part of the proof follows closely the first part of the proof of the previous theorem. If $r = 0$ the result is a consequence of (N5). Now assume that $r \geqslant 1$. Suppose to the contrary that $d_q(n_1, n_2, \ldots, n_s; m) > m - r$. Then there exists a system $H = \{h_{(i,j)}: 1 \leqslant i \leqslant s, 1 \leqslant j \leqslant n_i\}$ of vectors in $F_q^m$ such that $H_I$ is linearly independent for every ideal $I$ of size $m - r$ of the poset $P = P(n_1, n_2, \ldots, n_s)$. It follows from (13) that

$$s - \omega_{m-r} - r > \binom{2r+2}{r+2}(q-1)^{r+1} \tag{15}$$

holds for all $r \geqslant 1$. By Lemma 3.1, there exists an ideal $J$ of $P$ of size $m$ having exactly $\omega_{m-r} + r$ maximal elements such that $H_J$ is linearly independent and thus is a basis of $F_q^m$. For ease of notation we denote these basis vectors by $b_1, b_2, \ldots, b_m$. Let

$$T = \{i: 1 \leqslant i \leqslant s \text{ and } (i, 1) \in J\}$$

be the set of indices of the chains which have a nonempty intersection with $J$ and let $\bar{T}$ be the set of indices of the remaining chains. Then $|T| = \omega_{m-r} + r$ and by (15),

$$|\bar{T}| = s - |T| > \binom{2r+2}{r+2}(q-1)^{r+1}.$$

Let $J_{\max}$ be the set of the $\omega_{m-r} + r$ maximal elements of $J$. By (12), $|J_{\max}| \geqslant 2r + 2$, and we fix a subset $K$ of $J_{\max}$ of cardinality $2r + 2$. Let $a_i = (i, 1)$ be the minimal element of the $i$th chain of $P$ $(1 \leqslant i \leqslant s)$, and write

$$a_i = \sum_{l=1}^{m} \beta_{il} b_l \quad (i \in \bar{T}).$$

Let $M$ be any subset of $J_{\max}$ with $|M| = r + 1$. Let $i \in \bar{T}$ and consider the ideal $I = (J \backslash M) \cup \{a_i\}$ of size $m - r$. Thus $H_I$ is linearly independent, and it follows that $\beta_{il} \neq 0$ for at least one $l$ such that $b_l \in H_M$. Since $M$ was an arbitrary subset of $J_{\max}$ of cardinality $r + 1$, it follows that $\beta_{il} = 0$ for at most $r$ values of $l$ with $b_l \in H_{J_{\max}}$ and hence for at most $r$ values of $l$ with $b_l \in H_K$. Thus $\beta_{il} \neq 0$ for at least $r+2$ values of $l$ with $b_l \in H_K$. For each $i \in \bar{T}$ we choose a set $C_i$ of any $r+2$ such $l$'s. It follows from (13) that

$$|\bar{T}| = s - \omega_{m-r} - r > \binom{2r+2}{r+2}(q-1)^{r+1}.$$

Hence there exists a subset $Z$ of $\bar{T}$ of cardinality strictly greater than $(q-1)^{r+1}$ such that $C_i = C_j = C$ for all $i$ and $j$ in $Z$. Without loss of generality, we may assume that $C = \{1, 2, \ldots, r+2\}$. Thus $\beta_{ij} \neq 0$ for $1 \leqslant j \leqslant r+2$ and $i \in Z$. Hence

$$\alpha_{ij} = \frac{\beta_{ij}}{\beta_{i,r+2}} \quad (1 \leqslant j \leqslant r+1)$$

is defined and nonzero for each $i$ in $Z$. Since $|Z| > (q-1)^{r+1}$, it follows that there exist distinct $i$ and $k$ in $Z$ such that

$$(\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{i,r+1}) = (\alpha_{k1}, \alpha_{k2}, \ldots, \alpha_{k,r+1}).$$

We then have

$$\beta_{k,r+2}a_i - \beta_{i,r+2}a_k = \sum_{l=r+3}^{m} (\beta_{k,r+2}\beta_{il} - \beta_{i,r+2}\beta_{kl})b_l.$$

It follows that $\{b_{r+3}, \ldots, b_m, a_i, a_k\}$ is a linearly dependent set of vectors corresponding to an ideal of $P$ of size $m-r$, a contradiction. Hence (14) holds. $\square$

We now consider $d_2(Q_k, m)$ for the poset $Q_k$ defined as follows. Let $k$ be a positive integer. Then $Q_k$ is the poset whose set of elements is

$$\{(i,j)\colon i \geqslant 0, j \geqslant 0, i+j \leqslant k-1\},$$

having the componentwise partial order given by

$$(i,j) \leqslant (i',j') \text{ if and only if } i \leqslant i' \text{ and } j \leqslant j'.$$

The set of elements of $Q_k$ is partitioned into $k$ *level sets* $L_0, L_1, \ldots, L_{k-1}$ where

$$L_t = \{(i,j)\colon i \geqslant 0, j \geqslant 0, i+j = t\} \quad (0 \leqslant t \leqslant k-1).$$

The number of elements of $Q_k$ is

$$n = \frac{k(k+1)}{2}.$$

Note that the smallest size of an ideal which contains the element $(i,j)$ is $(i+1)(j+1)$. The poset $Q_k$ is a subposet (the 'bottom half') of the product of a chain of size $k$ with itself.

If $n \leqslant m$, then $d_2(Q_k; m) = n+1$. We henceforth assume that $n > m$.

**Theorem 3.4.** *If $m \leqslant 7$, then $d_2(Q_k; m) = m+1$. If $m \geqslant 8$ and $k(k+1)/2 \geqslant m+2$, then $d_2(Q_k; m) \leqslant m$.*

**Proof.** It is not hard to show that $d_2(Q_k;m) = m+1$ if $m \leqslant 7$. For instance, suppose that $m=7$. If $k \geqslant 7$, then the union of the ideals of $Q_k$ of size 7 contains exactly 16 elements. Let $e_1, e_2, \ldots, e_7$ be a basis of $F_2^7$. Then the following assignment of vectors of $F_2^7$ to these 16 elements of $Q_k$ has the property that the vectors assigned to each ideal of size 7 are linearly independent and hence $d_2(Q_k;7) = 8$:

| | |
|---|---|
| $(0,0) \leftarrow e_1$ | $(2,1) \leftarrow e_4 + e_7$ |
| $(0,1) \leftarrow e_2$ | $(3,0) \leftarrow e_7$ |
| $(1,0) \leftarrow e_3$ | $(0,4) \leftarrow e_7$ |
| $(0,2) \leftarrow e_4$ | $(4,0) \leftarrow e_6$ |
| $(1,1) \leftarrow e_4 + e_5 + e_6 + e_7$ | $(0,5) \leftarrow e_5$ |
| $(2,0) \leftarrow e_5$ | $(5,0) \leftarrow e_4$ |
| $(0,3) \leftarrow e_6$ | $(0,6) \leftarrow e_3$ |
| $(1,2) \leftarrow e_5 + e_6$ | $(6,0) \leftarrow e_2$ |

Now assume that $m \geqslant 8$ and $k(k+1)/2 \geqslant m+2$. We show that it is impossible to find a system

$$H = \{h_{(i,j)}: i \geqslant 0, j \geqslant 0, i+j \leqslant k-1\}$$

of vectors of $F_2^m$ with the property that the set $H_I$ of vectors assigned to each ideal $I$ of size $m$ is linearly independent.

Assume to the contrary that we have such a system $H$. There exists integer $j \leqslant k-1$ and an ideal $J$ of size $m$ containing $L_0 \cup \cdots \cup L_{j-1}$ and contained in $L_0 \cup \cdots \cup L_{j-1} \cup L_j$. We may choose such a $J$ so that for some integer $t$, $\{(0,j),(1,j-1),\ldots,(t,j-t)\} = L_j \cap J$. We now distinguish two elements $c$ and $d$ of $J$. Let $d=(t,j-t)$, and let $c=(t-1,j-t+1)$ if $t>0$ and let $c=(j-1,0)$ if $t=0$. We also distinguish two elements $a$ and $b$ of $Q_k$ not in $J$. If $t \leqslant j-2$, let $a=(t+1,j-t-1)$ and $b=(t+2,j-t-2)$; if $t=j-1$, let $a=(j,0)$ and $b=(0,j+1)$; if $t=j$, let $a=(0,j+1)$ and $b=(1,j)$. Since $m \geqslant 8$, it follows that $J \cup \{a,b\}$ is an ideal of $Q_k$ of size $m+2$ in which each of $a,b,c$ and $d$ is a maximal element.

Since $J$ is an ideal of size $m$, $H_J$ is linearly independent and hence is a basis of $F_2^m$. Thus each vector in $F_2^m$ is a sum of a subset of the vectors in $H_J$. Let $u$ be the vector of $H_J$ assigned to $c$ and let $v$ be the vector of $H_J$ assigned to $d$. Let $x$ be the vector of $F_2^m$ assigned to $a$ and let $y$ be the vector assigned to $b$. Since $(J\setminus\{c\}) \cup \{a\}$ and $(J\setminus\{d\}) \cup \{a\}$ are both ideals of size $m$, both $u$ and $v$ occur in writing $x$ as a sum of vectors of $H_J$. Similarly, both $u$ and $v$ occur in writing $y$ as a sum of vectors of $H_J$. Therefore $x-y$ is a linear combination of the vectors $H_J\setminus\{u,v\}$, and hence $(H_J\setminus\{u,v\}) \cup \{x,y\}$ is a linearly dependent set of vectors assigned to the ideal $(J\setminus\{c,d\})\{a,b\}$ of size $m$, a contradiction. □

**Theorem 3.5.** *If* $m \geqslant 26$ *and* $k(k+1)/2 \geqslant m+2$, *then* $d_2(Q_k;m) \leqslant m-1$.

**Proof.** Assume that $m \geqslant 26$ and $k(k+1)/2 \geqslant m+2$. We show that it is impossible to find a system

$$H = \{h_{(i,j)}: i \geqslant 0, j \geqslant 0, i+j \leqslant k-1\}$$

of vectors of $F_2^m$ with the property that the set $H_I$ of vectors assigned to each ideal $I$ of size $m-1$ is linearly independent. Assume to the contrary that we have such a system.

Using a construction similar to that in the proof of Theorem 3.4 and the assumption that $m \geqslant 26$, we find an ideal $I$ of size $m-1$ containing four elements $c_1, c_2, c_3, c_4$ and an additional three elements $a_1, a_2, a_3$ not in $I$ such that $I' = I \cup \{a_1, a_2, a_3\}$ is an ideal of $Q_k$ of size $m+2$ in which each of of $c_1, c_2, c_3, c_4, a_1, a_2$, and $a_3$ is a maximal element (see Fig. 1 for the case $m = 26$). We first focus on two of the $c$'s, say $c_3$ and $c_4$, and two of the $a$'s, say $a_2$ and $a_3$ in order to produce an ideal $J$ of size $m$ contained in $I'$ such that $H_J$ is linearly independent and thus is a basis of $F_2^m$. Since $I$ is an ideal of size $m-1$, $H_I$ is linearly independent. Let $v_m$ be a vector such that $H_I \cup \{v_m\}$ is a basis of $F_2^m$. Let $u$, $v$, $y$ and $z$ be the vectors from $H$ assigned to $c_3, c_4, a_2$ and $a_3$, respectively. Each of the vectors $y$ and $z$ is a sum of a subset of the basis vectors. Since $(I \setminus \{c_3\}) \cup \{a_2\}$ is an ideal of size $m-1$, $H_{(I \setminus \{c_3\}) \cup \{a_2\}}$ is linearly independent and hence either $u$ or $v_m$ occurs in writing $y$ as a sum of the basis vectors. Since $(I \setminus \{c_4\}) \cup \{a_2\}$ is also an ideal of size $m-1$, either $v$ or $v_m$ also occurs in $y$. Hence if $v_m$ does not appear in $y$, then both $u$ and $v$ do. Similarly, if $v_m$ does not appear in $z$, then both $u$ and $v$ do. If $v_m$ appears in neither $y$ nor $z$, then $y - z$ is a linear combination of the vectors $H_{I \setminus \{c_3, c_4\}}$ assigned to the ideal $I \setminus \{c_3, c_4\}$ and hence $H_{(I \setminus \{c_3, c_4\}) \cup \{a_2, a_3\}}$ is a linearly dependent set of vectors assigned to the ideal $(I \setminus \{c_3, c_4\}) \cup \{a_2, a_3\}$ of size $m-1$. Therefore $v_m$ appears in at least one of $y$ and $z$, say $z$. Then $J = I \cup \{a_3\}$ is an ideal contained in $I'$ such that $H_J$ is a basis of $F_2^m$.

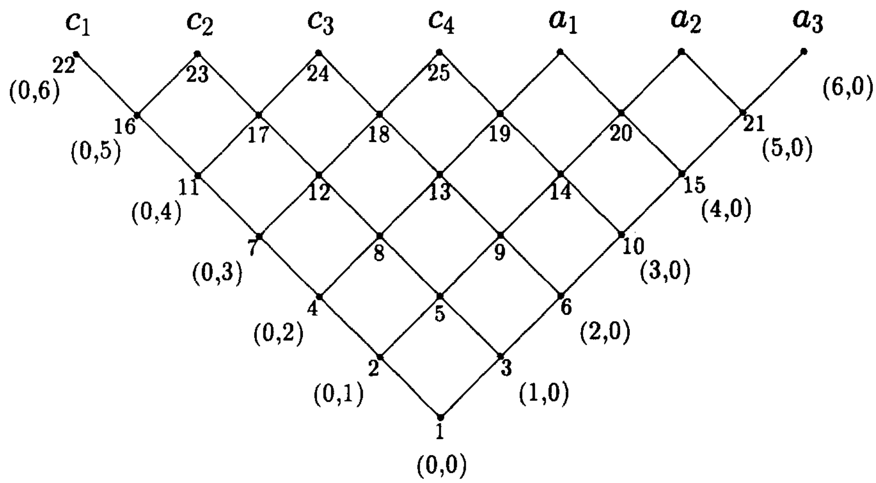


Fig. 1.

Each of the elements of $M = \{c_1, c_2, c_3, c_4, a_3\}$ is a maximal element of the ideal $J$ and for ease of notation, we relabel the vectors assigned to these elements as $u_1, u_2, u_3, u_4, u_5$, respectively. Let $x$ denote the vector assigned to $a_1$ and as above, let $y$ denote the vector assigned to $a_2$. Consider the ideals of size $m-1$ obtained from $J$ by removing any two elements of $M$ and adjoining $a_1$. Since the sets of vectors assigned to these ideals are linearly independent, we conclude that given any two of the vectors $u_1, \dots, u_5$, at least one appears in writing $x$ as a sum of the basis vectors. It follows that at least four of these vectors appear in $x$. Similarly, at least four occur in $y$. Hence at least three appear in both, say $u_1, u_2, u_3$. Then $x - y$ is a linear combination of the $m-3$ vectors in $H_{J \setminus \{c_1, c_2, c_3\}}$ and so $(J \setminus \{c_1, c_2, c_3\}) \cup \{a_1, a_2\}$ is an ideal of size $m-1$ whose assigned vectors are linearly dependent, a contradiction. □

We now obtain a more general bound for $d_2(Q_k; m)$.

**Theorem 3.6.** *Let $r$ be an integer with $r \geqslant 2$ and let $f(r) = 2^{2r+1} + r\,2^{r+2} - 2^r + 2r^2 + 2r + 2$. If $m \geqslant f(r)$ and $k \geqslant 2^{r+1} + 2r$, then $d_2(Q_k; m) \leqslant m - r$.*

**Proof.** Assume that $m \geqslant f(r)$ and $k \geqslant 2^{r+1} + 2r$. We show that it is impossible to find a system

$$H = \{h_{(i,j)} \colon i \geqslant 0, j \geqslant 0, i + j \leqslant k - 1\}$$

of vectors of $F_2^m$ with the property that the set $H_I$ of vectors assigned to each ideal $I$ of size $m - r$ is linearly independent. Assume to the contrary that we have such a system.

Since $k \geqslant 2^{r+1} + 2r$, the level set $L_{2^{r+1}+2r-1}$ contains exactly $2^{r+1} + 2r$ elements. We now use a construction similar to that in the proof of Theorem 3.4. Since

$$m - r \geqslant f(r) - r = \left( \sum_{i=1}^{2^{r+1}+2r-1} i \right) + 2r + 2 = \left( \sum_{i=1}^{2^{r+1}+2r-2} |L_i| \right) + 2r + 2,$$

we can find an ideal $I$ of size $m - r$ containing $2r + 2$ elements $c_1, c_2, \dots, c_{2r+2}$ and an additional $2^{r+1} - 2$ elements $a_1, a_2, \dots, a_{2^{r+1}-2}$ not in $I$ such that $I' = I \cup \{a_1, a_2, \dots, a_{2^{r+1}-2}\}$ is an ideal of $Q_k$ of size $m - r + 2^{r+1} - 2$ in which each of $c_1, c_2, \dots, c_{2^{r+1}+2}, a_1, a_2, \dots, a_{2^{r+1}-2}$ is a maximal element. This fact allows us to mimic the proof[4] of Lemma 3.1 and obtain an ideal $J$ of size $m$ containing $I$ and $r$ of the elements $a_1, a_2, \dots, a_{2^{r+1}-2}$, say $a_3, \dots, a_{r+2}$, such that $H_J$ is linearly independent and hence a basis of $F_2^m$. Note that since $J \subset I'$, each of the $3r + 2$ elements of $M = \{c_1, c_2, \dots, c_{2r+2}, a_3, \dots, a_{r+2}\}$ is a maximal element of $J$.

We now proceed as in the proof of Theorem 3.5. We label the vectors assigned to the elements of $M$ as $u_1, u_2, \dots, u_{3r+2}$, respectively. Let $x$ denote the vector assigned to

[4] The hypothesis in Lemma 3.1 that $\omega_{m-r} \geqslant 2$ ensured that $I$ had at least two maximal elements, and this conclusion holds in the current situation since $2r + 2 \geqslant 6$. The hypothesis (7) in Lemma 3.1 ensured the existence of at least $q^{r+1} - q^2 + q$ elements $(i + \omega_{m-r}, 1)$, $(1 \leqslant i \leqslant s - \omega_{m-r})$; in the current situation the role of these elements is played by $a_1, a_2, \dots, a_{2^{r+1}-2}$.

$a_1$ and let $y$ denote the vector assigned to $a_2$. Consider the ideals of size $m - r$ obtained from $J$ by removing any $r + 1$ elements of $M$ and adjoining $a_1$. The sets of vectors assigned to these ideals are linearly independent, and so given any $r + 1$ of the vectors $u_1, u_2, \ldots, u_{3r+2}$, at least one appears in writing $x$ as a sum of the basis vectors of $H_J$. Hence at least $2r + 2$ of these vectors appear in $x$ and similarly, at least $2r + 2$ occur in $y$. Hence at least $r + 2$ appear in both, say $u_1, u_2, \ldots, u_{r+2}$. Then $x - y$ is a linear combination of the $m - r - 2$ vectors in $H_{J \setminus \{c_1, c_2, \ldots, c_{r+2}\}}$ and therefore $(J \setminus \{c_1, c_2, \ldots, c_{r+2}\}) \cup \{a_1, a_2\}$ is an ideal of size $m - r$ whose assigned vectors are linearly dependent, a contradiction. $\square$

## References

[1] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Vols. I and II (North-Holland, Amsterdam, 1977).

[2] H. Niederreiter, Point sets and sequences with small discrepancy, Monatsh. Math. 104 (1987) 273–337.

[3] H. Niederreiter, A combinatorial problem for vector spaces over finite fields, Discrete Math. 96 (1991) 221–228.

[4] H. Niederreiter, Orthogonal arrays and other combinatorial aspects in the theory of uniform point distributions in unit cubes, Discrete Math. 106/107 (1992) 361–367.

[5] V. Pless, Introduction to the Theory of Error-Correcting Codes (Wiley, New York, 2nd ed., 1989).