stichting
mathematisch
centrum

MC

AFDELING ZUIVERE WISKUNDE ZW 32/75 DECEMBER

M.R. BEST & A.E. BROUWER

THE TRIPLY SHORTENED BINARY HAMMING CODE IS OPTIMAL

Prepublication

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS(MOS) subject classification scheme (1970): 05Q05

The triply shortened binary Hamming code is optimal *)

by

M.R. Best & A.E. Brouwer

ABSTRACT

By explicit evaluation of the linear programming bound for the case $q = 2$, $d = 3$ (after adding one inequality when $n \equiv 0 \pmod 4$), we prove that $A[n,3] \le 2^{n-2}/\lfloor \frac{1}{4}n+1 \rfloor$. In particular the binary Hamming code is shown to remain optimal when it is shortened one, two or three times. Furthermore some general relations between solutions of the LP problem are derived.

KEY WORDS & PHRASES: *linear programming bound.*

*) This paper is not for review; it is meant to be published elsewhere.

1. INTRODUCTION

For any sequence $(A_i)_{i=0}^n$ we define the *dual sequence* $(B_k)_{k=0}^n$ by

$$B_k = \sum_{i=0}^{n} A_i K_k(i),$$

where

$$K_k(i) = \sum_j (-1)^j (q-1)^{k-j} \binom{i}{j} \binom{n-i}{k-j}$$

denotes a Kravčuk polynomial (cf. [1]).

An $[n,d]$-*code* is a code of length n and minimum (Hamming-) distance at least d over an alphabet Q of q elements. $A[n,d]$ is defined as the maximum cardinality of an $[n,d]$-code. An $[n,d]$-code for which this maximum is attained is called *optimal*.

Now let $(A_i)_{i=0}^n$ be the inner distribution of a code C of length n over Q, i.e.

$$A_i = |C|^{-1} \cdot |\{(x,y) \mid x,y \in C \text{ and } d(x,y) = i\}|$$

is the average number of codewords with Hamming distance i to a fixed codeword. P. DELSARTE proved that in this case the components B_k of the dual sequence of $(A_i)_i$ are nonnegative. Hence for any $[n,d]$-code its inner distribution $(A_i)_i$ must satisfy:

$$\begin{cases} A_i \geq 0 & \text{for} \quad 0 \leq i \leq n \\ B_k \geq 0 & \text{for} \quad 0 \leq k \leq n \\ A_0 = 1,\ A_i = 0 & \text{for} \quad 1 \leq i < d. \end{cases}$$

We shall denote this system by $LP[n,d]$. Since $B_0 = \Sigma A_i = |C|$ the *linear programming bound* can be formulated as

$$A[n,d] \leq \max\{B_0 \mid (A_i)_i \text{ is a solution of } LP[n,d]\}.$$

For $q = 2$, $d = 3$ (and for $d = 4$) we can solve the implied linear programming

problem explicitly. It turns out that the optimal solution is unique and specializes for $n = 2^m - 1$, $n = 2^m - 2$, $n = 2^m - 3$ to the weight enumerator of respectively the zero, one or two times shortened Hamming code.
For $n \equiv 0 \pmod 4$ however the (unique) optimal solution satisfies $A_{n-1} = 2n/(n+2) > 1$ which is clearly impossible for a single-error-correcting code. Therefore we added the inequality

$$A_{n-1} + A_n \le 1$$

to the system LP[n,3], and solved the resulting LP problem. This time there is an optimal solution which specializes for $n = 2^m - 4$ to the weight enumerator of the triply shortened Hamming code.

REMARK. The general idea of adding extra inequalities to LP[n,d] has proved to be very fruitful. For instance, we showed in that way that the [12,5]-Nadler code with 32 codewords is optimal, a result found independently and almost simultaneously by F.J. MacWilliams, A.M. Odlyzko and N.J.A. Sloane (private communication, sept 1975).

2. GENERATING FUNCTIONS

For theoretical purposes the definition of $(B_k)_k$ can be transformed into a much more convenient form by using generating functions. First of all we have

$$\sum_k K_k(i)\, w^{n-k}x^k = (w+(q-1)x)^{n-i}(w-x)^i.$$

Defining for any sequence $(S_i)_{i=0}^n$

$$S(w,x) = \sum_i S_i w^{n-i}x^i,$$

the definition of $(B_k)_k$ is reflected in $B(w,x) = A(w+(q-1)x,\ w-x)$.
If $F \gg 0$ denotes that F is a polynomial in w and x with positive coefficients, LP[n,d] can be reformulated as

$$\begin{cases} A(w,x) \gg 0 \\ B(w,x) \gg 0 \\ A_0 = 1,\ A_i = 0 \text{ for } 1 \le i < d. \end{cases}$$

(note that $A_0 = A(1,0)$ and $B_0 = B(1,0) = A(1,1)$.)

In the sequel we shall apply several times the coordinate transformation

$$\begin{cases} s = w + (q-1)\,x \\ t = w - x \end{cases} \quad \text{i.e.} \quad \begin{cases} w = (s+(q-1)t)/q \\ x = (s-t)/q \end{cases}$$

Observe that

$$\frac{\partial}{\partial s} + \frac{\partial}{\partial t} = \frac{\partial}{\partial w}$$

$$\frac{\partial}{\partial w} + \frac{\partial}{\partial x} = q\frac{\partial}{\partial s}$$

$$B(w,x) = A(s,t),$$

and

$$q^n A(w,x) = B(s,t).$$

3. SOME RESULTS ON KRAVČUK POLYNOMIALS.

We mention some results which we need in the sequel. For $q = 2$ we explicitate K_0, K_1, K_2 and K_n:

$$K_0(i) = 1$$

$$K_1(i) = n-2i$$

$$K_2(i) = \frac{1}{2}(n-2i)^2 - \frac{1}{2}n$$

$$K_n(i) = (-1)^i$$

as is easily verified from the definition. Moreover we remark that $q^n A_k = \Sigma B_i K_k(i)$, that is, the dual of the dual of a sequence is a constant factor (q^n) times the original sequence. [This follows at once from the bottom line of section 2.]

Next we need a result about certain submatrices of the Kravčuk matrix $(K_k(i))^n_{k,i=0}$. From the equation

$$K_k(i) = \sum_j (-q)^j (q-1)^{k-j} \binom{n-j}{k-j} \binom{i}{j}$$

(cf.[1]) one immediately sees that $K_k(i)$ is a polynomial in i of degree k: $K_k(i) = \Sigma_{t=0}^n a_{kt} i^t$ with leading coefficient $a_{kk} = (-q)^k/k!$. Now let $I \subseteq \{0,1,\ldots,n\}$ with $|I| = \ell$ and let $(K_k(i))_{k<\ell,\ i\in I}$ be the square submatrix of the first ℓ rows and ℓ different columns. Then

$$(K_k(i))_{k<\ell,\ i\in I} = (a_{kt})_{k,t<\ell} \cdot (i^t)_{t<\ell,\ i\in I}$$

Since $(a_{kt})_{k,t<\ell}$ is a lower triangular matrix with nonvanishing diagonal elements and $(i^t)_{t<\ell,\ i\in I}$ is a Vandermonde matrix, both matrices are regular and so is $(K_k(i))_{k<\ell,\ i\in I}$. Hence

THEOREM 1. *Let* $I \subseteq \{0,1,\ldots,n\}$ *with* $|I| = \ell$. *Then the matrix* $(K_k(i))_{k<\ell,\ i\in I}$ *is regular.*
(In fact its determinant equals $\prod_{k<\ell} \frac{(-q)^k}{k!} \cdot \prod_{\substack{i>i' \\ i,i'\in I}} (i-i')$ *.)* □

A consequence of this theorem is

COROLLARY. *Let* $I \subseteq \{1,\ldots,n\}$ *with* $|I| = d$. *If each optimal solution of* LP[n,d] *(or an extension of it) has* $B_i = 0$ *for* $i \in \{1,\ldots,n\}\setminus I$, *then there is exactly one optimal solution of the* LP *problem under consideration.*

PROOF. We know that $q^n A_k = \sum_i K_k(i) B_i$. Since all A_k for $k < d$ and all B_i for $i \notin I$ are known, this yields (using $k<d$) a system of d equations in the unknowns $B_i (i\in I)$ with nonvanishing determinant. □

4. MODIFICATIONS OF CODES AND SEQUENCES.

A. Shortening.

Let C be an [n,d]-code over Q. A *shortened code* $C^{p,j}$ of it consists of all words with the symbol $j \in Q$ at a fixed position p, where the symbol itself is deleted. Obviously each $C^{p,j}$ is an [n-1,d]-code, and there exists one for which $|C^{p,j}| \geq q^{-1} |C|$. In general the inner distribution $(A_i^{p,j})_{i=0}^{n-1}$ of $C^{p,j}$ cannot be determined from the inner distribution $(A_i)_i$

of C. But if all shortened codes $C^{p,j}$ (p any position, $j \in Q$) have the same inner distribution (and in particular if C is invariant under an automorphism group which acts transitively on bitpositions as well as on the symbols of the alphabet Q) then $A_i^{p,j} = \frac{n-i}{n} A_i$.
In fact we have in general

$$\sum_{p,j} |C^{p,j}| A_i^{p,j} = \sum_p |\{(x,y) \mid x,y \in C,\ d(x,y) = i \text{ and } x_p = y_p\}| = (n-i) \cdot |C| \cdot A_i$$

and

$$\sum_{p,j} |C^{p,j}| = n \cdot |C|$$

hence the sequence $(\frac{n-i}{n} A_i)_i$ is a convex combination of the sequences $(A_i^{p,j})_i$.
Thus motivated we define for each sequence $(A_i)_{i=0}^n$ the *shortened sequence* $(A_i^0)_{i=0}^{n-1}$ by $A_i^0 = \frac{n-i}{n} A_i$.
In the language of generating functions this means

$$A^0(w,x) = \frac{1}{n} \frac{\partial}{\partial w} A(w,x).$$

B. Puncturing.
Let C be an [n,d]-code over Q with $d \geq 2$. A *punctured code* $C^{p,-}$ of it consists of all words of C with the symbol at position p deleted. Obviously $C^{p,-}$ is an [n-1, d-1]-code with $|C^{p,-}| = |C|$. In general the inner distribution $(A_i^{p,-})_i$ of $C^{p,-}$ cannot be obtained from the inner distribution $(A_i)_i$ of C. But if all punctured codes $C^{p,-}$ (p any position) have the same inner distribution (and in particular if C is invariant under an automorphism group which acts transitively on the bit positions), then $A_i^{p,-} = \frac{n-i}{n} A_i + \frac{i+1}{n} A_{i+1}$.
In fact we have

$$\begin{aligned}\sum_p |C^{p,-}| A_i^{p,-} &= \sum_p |\{(x,y) \mid x,y \in C \text{ and } ((d(x,y)=i \text{ and } x_p=y_p) \text{ or} \\ &\qquad (d(x,y)=i+1 \text{ and } x_p \neq y_p))\}| \\ &= ((n-i)A_i + (i+1)A_{i+1}) \cdot |C|\end{aligned}$$

and

$\sum_{p} |C^{p,-}| = n \cdot |C|$

hence the sequence $\left(\frac{n-i}{n} A_i + \frac{i+1}{n} A_{i+1}\right)_i$ is a convex combination of the sequences $(A_i^{p,-})_i$. Therefore we define for each sequence $(A_i)_{i=0}^n$ the *punctured sequence* $(A_i^-)_{i=0}^{n-1}$ by $A_i^- = \frac{n-i}{n} A_i + \frac{i+1}{n} A_{i+1}$.
In the language of generating functions this means

$$A^-(w,x) = \frac{1}{n}\left(\frac{\partial}{\partial w} + \frac{\partial}{\partial x}\right) A(w,x).$$

Let $X \subseteq \mathbb{N}^2$ and for each $(n,d) \in X$ let $R[n,d]$ be a restriction laid upon sequences $(A_i)_{i=0}^n$ (with $A_1 = \ldots = A_{d-1} = 0$). We say the collection $\{R[n,d] \mid (n,d) \in X\}$ is *invariant under shortening (puncturing)* if for each $(n,d) \in X$ with $(n-1, d) \in X$ ($(n-1, d-1) \in X$) whenever a sequence satisfies $R[n,d]$ then the shortened (punctured) sequence satisfies $R[n-1,d]$ ($R[n-1,d-1]$).

THEOREM 2. *Let* $LI[n,d]$ *be the set of all linear inequalities with real coefficients and variables* A_i, *such that they are satisfied by each sequence* $(A_i)_i$ *which is the inner distribution of an* $[n,d]$*-code. Then* $\{LI[n,d] \mid (n,d) \in \mathbb{N}^2\}$ *is invariant under shortening and puncturing.*

PROOF. A convex combination of solutions to a linear inequality is again a solution. □

THEOREM 3. $\{LP[n,d] \mid (n,d) \in \mathbb{N}^2\}$ *is invariant under shortening and puncturing.*

PROOF. Suppose $(A_i)_{i=0}^n$ satisfies $LP[n,d]$. Then

$$B^0(w,x) = A^0(s,t) = \frac{1}{n}\frac{\partial}{\partial s} A(s,t) = \frac{1}{nq}\left(\frac{\partial}{\partial w} + \frac{\partial}{\partial x}\right) B(w,x) \gg 0$$

and

$$B^-(w,x) = A^-(s,t) = \frac{1}{n}\left(\frac{\partial}{\partial s} + \frac{\partial}{\partial t}\right) A(s,t) = \frac{1}{n}\frac{\partial}{\partial w} B(w,x) \gg 0.$$

The verification of the other conditions is left to the reader. □

THEOREM 4. *Let* $(A_i^0)_i$ *and* $(A_i^-)_i$ *be respectively the shortened and the punctured sequence of* $(A_i)_i$. *Then* $B_0^0 = q^{-1} \cdot B_0 + (nq)^{-1} B_1$ *and* $B_0^- = B_0$.

PROOF. From the proof of theorem 3 follows:

$$B_0^0 = B^0(1,0) = \frac{1}{nq}\left[\frac{\partial}{\partial w} B(w,0)\right]_{w=1} + \frac{1}{nq}\left[\frac{\partial}{\partial x} B(1,x)\right]_{x=0} = \frac{1}{q} B_0 + \frac{1}{nq} B_1$$

and

$$B_0^- = B^-(1,0) = \frac{1}{n}\left[\frac{\partial}{\partial w} B(w,0)\right]_{w=1} = B_0. \quad \square$$

Calling a sequence $(A_i)_i$ an *optimal* solution of a restriction when B_0 is maximal we have:

THEOREM 5. *Let* $\{R[n,d] \mid (n,d) \in X\}$ *be a collection of restrictions invariant under shortening and such that* $R[n,d]$ *implies* $LP[n,d]$ *for each* $(n,d) \in X$. *If* $(A_i)_i$ *is a solution of* $R[n,d]$ *and its shortened sequence* $(A_i^0)_i$ *is a (unique) optimal solution of* $R[n-1, d]$ *and* $B_0^0 = q^{-1} \cdot B_0$ *then the sequence* $(A_i)_i$ *itself is a (unique) optimal solution of* $R[n,d]$.

PROOF. If $(A_i^0)_i$ is an optimal solution of $R[n-1, d]$ and $(A_i^*)_i$ is any solution of $R[n,d]$ then $B_0^* \le q\, B_0^{*0} \le q\, B_0^0 = B_0$ hence $(A_i)_i$ is optimal. If $(A_i^0)_i$ is the unique optimal solution of $R[n-1, d]$ and $(A_i^*)_i$ is any optimal solution of $R[n,d]$ then $B_0^* \ge B_0$ hence $B_0^* = q\, B_0^{*0} = q\, B_0^0 = B_0$. By the uniqueness of $(A_i^0)_i$ it follows that $A_i^{*0} = A_i^0$ for $0 \le i \le n-1$ and hence $A_i^* = \frac{n}{n-i} A_i^{*0} = \frac{n}{n-i} A_i^0 = A_i$ for $0 \le i \le n-1$. But also $A_n^* = A_n$ since $\sum_i A_i^* = B_0^* = B_0 = \sum_i A_i$. Hence $(A_i)_i$ is unique. $\square$

REMARK. Of course the requirement $R[n,d] \Rightarrow LP[n,d]$ was needed only to ensure that $B_1 \ge 0$ hence $B_0 \le q\, B_0^0$ for any solution $(A_i)_i$ of $R[n,d]$.

THEOREM 6. *If* $\{R[n,d] \mid (n,d) \in X\}$ *is invariant under puncturing and such that* $R[n,d]$ *implies* $LP[n,d]$ *for each* $(n,d) \in X$ *and* $(A_i)_i$ *is a solution of* $R[n,d]$ *such that its punctured sequence* $(A_i^-)_i$ *is a (unique) optimal solution of* $R[n-1, d-1]$ *then the sequence* $(A_i)_i$ *itself is a (unique) optimal solution of* $R[n,d]$.

PROOF. If $(A_i^-)_i$ is an optimal solution of $R[n-1, d-1]$ and $(A_i^*)_i$ is any solution of $R[n,d]$ then $B_0^* = B_0^{*-} \le B_0^- = B_0$ hence $(A_i)_i$ is optimal. If $(A_i^-)_i$ is the unique optimal solution of $R[n-1, d-1]$ and $(A_i^*)_i$ is any optimal solution of $R[n,d]$ then $A^-(s,t) = A^{*-}(s,t)$ hence $\frac{\partial}{\partial w}(B^*(w,x)-B(w,x)) = 0$ and $B^*(w,x) = B(w,x) + cx^n$. Using $B(1,1) = q^n A_0 = q^n$ it follows that $c = 0$. $\square$

REMARK. Here $R[n,d] \Rightarrow LP[n,d]$ was needed only to ensure that $A_0 = 1$ for any solution $(A_i)_i$ of $R[n,d]$.

5. THE CASE $q = 2$, $d = 3$ or $d = 4$.

For the case $q = 2$, $d = 3$ or $d = 4$ we can give the solution of $LP[n,d]$ explicitly.

THEOREM 7. *Let* $q = 2$. *If* $d = 3$ *then let* $(A_i)_i$ *be defined by*

$$A(w,x)= \begin{cases} \frac{1}{n+2}(w+x)^n + \frac{1}{n+2}(w+x)^{\frac{1}{2}n-1}(w-x)^{\frac{1}{2}n}((n+1)w+x) & \text{if } n \equiv 0 \pmod 2 \\ \frac{1}{n+3}(w+x)^n + \frac{1}{n+3}(w+x)^{\frac{1}{2}(n-3)}(w-x)^{\frac{1}{2}(n-1)}((n+2)w^2+2wx-x^2) & \\ & \text{if } n \equiv 1 \pmod 4 \\ \frac{1}{n+1}((w+x)^n + \frac{n}{n+1}(w+x)^{\frac{1}{2}(n-1)}(w-x)^{\frac{1}{2}(n+1)} & \text{if } n \equiv 3 \pmod 4). \end{cases}$$

If $d = 4$ *then let* $(A_i)_i$ *be defined by*

$$A(w,x) = \begin{cases} \frac{1}{2(n+1)}((w+x)^n + (w-x)^n) + \frac{n}{n+1}w(w^2-x^2)^{\frac{1}{2}(n-1)} & \text{if } n \equiv 1 \pmod 2 \\ \frac{1}{2(n+2)}((w+x)^n + (w-x)^n) + \frac{1}{n+2}(w^2-x^2)^{\frac{1}{2}n-1}((n+1)w^2-x^2) & \\ & \text{if } n \equiv 2 \pmod 4 \\ \frac{1}{2n}((w+x)^n + (w-x)^n) + \frac{n-1}{n}(w^2-x^2)^{\frac{1}{2}n} & \text{if } n \equiv 0 \pmod 4). \end{cases}$$

Then $(A_i)_i$ *is the unique optimal solution of* $LP[n,3]$ *and* $LP[n,4]$ *respectively. In particular we find the bounds*

$$A[n+1, 4] = A[n,3] \le \begin{cases} 2^n/(n+2) & \text{if } n \equiv 0 \pmod 2) \\ 2^n/(n+3) & \text{if } n \equiv 1 \pmod 4),\ n \neq 1 \\ 2^n/(n+1) & \text{if } n \equiv 3 \pmod 4). \end{cases}$$

COROLLARY. $A[2^m - j, 3] = 2^{2^m - m - j}$ *for* $j = 1, 2, 3$.

PROOF. (i) Observe that $(A_i)_i$ for $d = 3$ is obtained by puncturing the sequence for $d = 4$ and n increased by one. Also, for $d = 3$ and $n \equiv 1 \pmod 4$ or $n \equiv 2 \pmod 4$, $(A_i)_i$ is obtained by shortening the sequence for n one larger. The same holds for $d = 4$ and $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$.

(ii) In order to prove that $(A_i)_i$ satisfies LP[n,d] it suffices to consider the cases $d = 4$, $n \equiv 0 \pmod 4$ and $d = 4$, $n \equiv 1 \pmod 4$ by (i) and theorem 3.

If $d = 4$, $n \equiv 0 \pmod 4$ then

$$A(w,x) = \frac{1}{2n}\left((w+x)^n + (w-x)^n\right) + \frac{n-1}{n}(w^2-x^2)^{\frac{1}{2}n},$$

so

$$B(w,x) = A(w+x,\ w-x) = \frac{2^{n-1}}{n}(w^n+x^n) + \frac{n-1}{n}.\ (4wx)^{\frac{1}{2}n}.$$

Certainly $B(w,x) \gg 0$. Furthermore $A_{2i+1} = 0$ for each i and

$$A_{2i} = \frac{1}{n}\binom{n}{2i} + \frac{n-1}{n}\binom{\frac{1}{2}n}{i}(-1)^i \geq 0$$

since

$$\frac{\binom{n}{2i}}{\binom{\frac{1}{2}n}{i}} = \frac{(n-1)(n-3)\ldots(n-2i+1)}{(2i-1)(2i-3)\ldots3.1} \geq n-1$$

provided $1 \leq 2i \leq n-2$; but if $2i = n$ then i is even and $A_{2i} = \frac{1}{n} + \frac{n-1}{n} = 1$ is positive too. Finally $A_0 = 1$.

If $d = 4$, $n \equiv 1 \pmod 4$ then

$$A(w,x) = \frac{1}{2(n+1)}\left((w+x)^n + (w-x)^n\right) + \frac{n}{n+1}\, w\, (w^2-x^2)^{\frac{1}{2}(n-1)},$$

so

$$B(w,x) = A(w+x,\ w-x) = \frac{2^{n-1}}{n+1}(w^n+x^n) + \frac{n}{n+1}(w+x)\ (4wx)^{\frac{1}{2}(n-1)}.$$

Certainly $B(w,x) \gg 0$. Furthermore $A_{2i+1} = 0$ for each i and

$$A_{2i} = \frac{1}{n+1}\binom{n}{2i} + \frac{n}{n+1}\binom{\frac{1}{2}(n-1)}{i}(-1)^i \geq 0$$

since

$$\frac{\binom{n}{2i}}{\binom{\frac{1}{2}(n-1)}{i}} = \frac{n(n-2)\ldots(n-2i+2)}{(2i-1)(2i-3)\ldots3.1} \geq n$$

for $1 \leq 2i \leq n-1$. Also $A_0 = 1$.
In both cases one can check easily $A_1 = A_2 = A_3 = 0$ and hence $(A_i)_i$ is a solution of LP[n,d] in all cases.

(iii) In order to prove that $(A_i)_i$ is the unique optimal solution of LP[n,d] it suffices by theorems 3, 5 and 6 to consider the cases $d = 3$, $n \equiv 0 \pmod 4$ and $d = 3$, $n \equiv 1 \pmod 4$. Let $n \equiv 0 \pmod 4$. Then since $(n-2i)(n-2i+2) = nK_0(i) + 2K_1(i) + 2K_2(i)$ we obtain

$$\sum_i (n-2i)(n-2i+2)\, B_i = (nA_0+2A_1+2A_2).\ 2^n = n.2^n$$

The coefficients $(n-2i)(n-2i+2)$ are non-negative and vanish only for $i = \frac{1}{2}n$ and $i = \frac{1}{2}n+1$. Therefore $B_0 \leq \frac{2^n}{n+2}$ and if $B_0 = \frac{2^n}{n+2}$ then $B_i = 0$ for $i \in \{1,2,\ldots,n\}\setminus\{\frac{1}{2}n, \frac{1}{2}n+1\}$. This proves optimality, and the uniqueness follows from the corollary to theorem 1.

Next let $n \equiv 1 \pmod 4$. Since

$$(n-2i)(n-2i+2) - 1 - 2(-1)^i = (n-1)K_0(i) + 2K_1(i) + 2K_2(i) - 2K_n(i)$$

we obtain

$$\sum_i ((n-2i)(n-2i+2) - 1 - 2(-1)^i)\, B_i = ((n-1)A_0 + 2A_1 + 2A_2 - 2A_n)\, 2^n \leq (n-1)2^n$$

The coefficients $(n-2i)(n-2i+2) - 1 - 2(-1)^i$ are non-negative and vanish only for $i \in \{\frac{1}{2}(n-1), \frac{1}{2}(n+1), \frac{1}{2}(n+3)\}$, as is easily verified.

Hence $B_0 \leq \frac{(n-1)2^n}{n^2+2n-3} = \frac{2^n}{n+3}$ and if $B_0 = \frac{2^n}{n+3}$ then $B_i = 0$ for

$i \in \{1,2,\ldots,n\}\setminus\{\frac{1}{2}(n-1), \frac{1}{2}(n+1), \frac{1}{2}(n+3)\}$. This again proves optimality and uniqueness. $\square$

<u>PROOF</u> of the corollary: shortening the appropriate Hamming code it is seen that the upper bound given in the theorem can be attained. □

6. AN ADDITIONAL INEQUALITY.

By adding the inequality $A_{n-1} + A_n \le 1$ (if $d=3$) or $2A_{n-2} + n(A_{n-1}+A_n) \le n$ (if $d=4$) to the system LP[n,d] we can improve the known bounds on A[n,3] for $n \equiv 0 \pmod 4$ and A[n,4] for $n \equiv 1 \pmod 4$, respectively. Denote the extended system by LPE[n,d].

<u>THEOREM 8</u>. *Let* $q = 2$. *If* $d = 3$ *then let* $(A_i)_i$ *be defined by*

$$A(w,x) = \frac{1}{n+4}(w+x)^n + \frac{1}{(n+1)(n+4)}(w+x)^{\frac{1}{2}n-2}(w-x)^{\frac{1}{2}n-1} \cdot$$

$$\cdot((n+1)(n+3)w^3 + 3(n+1)w^2x - 3(n+1)wx^2 - 3x^3) \quad \text{if } n \equiv 0 \pmod 4,$$

and by the expression given in theorem 7 otherwise.

If $d = 4$ *then let* $(A_i)_i$ *be defined by*

$$A(w,x) = \frac{1}{2(n+3)}((w+x)^n+(w-x)^n) + \frac{1}{n+3}\, w(w^2-x^2)^{\frac{1}{2}(n-3)}((n+2)w^2-3x^2)$$

$$\text{if } n \equiv 1 \pmod 4,$$

and by the expression given in theorem 7 otherwise.

Then $(A_i)_i$ *is an optimal solution of* LPE[n,d].
In particular we find the bound

$$A[n+1,\ 4] = A[n,3] \le \frac{2^n}{n+4} \qquad \text{if } n \equiv 0 \pmod 4.$$

<u>COROLLARY</u>. $A[2^m-4,\ 3] = 2^{2^m-m-4}$.

<u>PROOF</u>. (i) Observe that $(A_i)_i$ for $d = 3$ is obtained by puncturing the sequence for $d = 4$ and n one larger. Also, for $d = 3$ and $n \equiv 0 \pmod 4$, $(A_i)_i$ is obtained by shortening the sequence for $n + 1$. The same holds for $d = 4$ and $n \equiv 1 \pmod 4$.

(ii) By theorems 3 and 7, $(A_i)_i$ satisfies LP[n,d]. Moreover, $\{LPE[n,d] \mid n \in \mathbb{N}, d \in \{3,4\}\}$ is invariant under puncturing:
If $(A_i)_i$ is a solution LPE[n,4] then $\bar{A}_{n-2} + \bar{A}_{n-1} = \frac{2}{n} A_{n-2} + A_{n-1} + A_n \leq 1$.
Therefore it is sufficient to show that (A_i) is a solution for d = 4 and that it is optimal for d = 3.
Compute A_{n-2}, A_{n-1} and A_n for d = 4:

If $n \equiv 0 \pmod 4$ then

$$A_{n-2} = 0,\ A_{n-1} = 0,\ A_n = 1.$$

If $n \equiv 1 \pmod 4$ then

$$A_{n-2} = 0,\ A_{n-1} = 1,\ A_n = 0.$$

If $n \equiv 2 \pmod 4$ then

$$A_{n-2} = \frac{n}{2},\ A_{n-1} = 0,\ A_n = 0.$$

If $n \equiv 3 \pmod 4$ then

$$A_{n-2} = 0,\ A_{n-1} = 0,\ A_n = 0.$$

Therefore in all cases $\frac{2}{n} A_{n-2} + A_{n-1} + A_n \leq 1$ is satisfied.

Since for $n \not\equiv 0 \pmod 4$ $(A_i)_i$ is the optimal solution of LP[n,3], it is a fortiori optimal for LPE[n,3]. Remains to show optimality for d = 3, $n \equiv 0 \pmod 4$.

Let $\alpha(i) = (n-2)\, K_0(i) + 2K_1(i) + 2K_2(i) + 2K_{n-1}(i) + 2K_n(i)$,
then if i is even

$$\alpha(i) = n + 4\,(n-2i) + (n-2i)^2 - n = (n-2i)(n-2i+4)$$

and if i is odd

$$\alpha(i) = n - 4 + (n-2i)^2 - n = (n-2i-2)(n-2i+2).$$

Since $n \equiv 0 \pmod 4$ this implies that $\alpha(i) \geq 0$, while $\alpha(i) = 0$ only for

$$i \in \{\tfrac{1}{2} n - 1,\ \tfrac{1}{2} n,\ \tfrac{1}{2} n + 1,\ \tfrac{1}{2} n + 2\}.$$

Now from

$$\sum_i \alpha(i)\, B_i = ((n-2)A_0+2A_1+2A_2+2A_{n-1}+2A_n) \cdot 2^n \leq n.2^n$$

and

$$\alpha(0) = n(n+4)$$

it follows that

$$B_0 \le 2^n/(n+4)$$

which proves optimality.

(iii) In order to conclude that $A[n,3] \le 2^n/(n+4)$ all we have to do is checking that the inequality $A_{n-1} + A_n \le 1$ is satisfied for the inner distribution of a code with $d = 3$. $\square$

REMARK. The solution of LPE[n,d] given in theorem 8 is not unique in general.

REFERENCES.

[1] P. DELSARTE, *An algebraic approach to the association schemes of coding theory*. Philips Res. Repts Suppl. 10 (1973)