Bounds for Binary Codes of Length Less Than 25

M. R. BEST, A. E. BROUWER, F. JESSIE MACWILLIAMS, ANDREW M. ODLYZKO, MEMBER, IEEE, AND NEIL J. A. SLOANE, FELLOW, IEEE

***Abstract*—Improved bounds for $A(n,d)$, the maximum number of codewords in a (linear or nonlinear) binary code of word length n and minimum distance d, and for $A(n,d,w)$, the maximum number of binary vectors of length n, distance d, and constant weight w in the range $n \leq 24$ and $d \leq 10$ are presented. Some of the new values are $A(9,4) = 20$ (which was previously believed to follow from the results of Wax), $A(13,6) = 32$ (which proves that the Nadler code is optimal), $A(17,8) = 36$ or 37, and $A(21,8) = 512$. The upper bounds on $A(n,d)$ are found with the help of linear programming, making use of the values of $A(n,d,w)$.**

I. INTRODUCTION

THE MAIN purpose of this paper is to present tables[1] of two of the most basic functions in coding theory, namely:

$A(n,d)$ = maximum number of codewords in any (linear or nonlinear) binary code of length n and minimum distance d between codewords (see Table I), and

$A(n,d,w)$ = maximum number of codewords in any binary code of length n, constant weight w and minimum distance d (see Table II),

in the range $n \leq 24$, $d \leq 10$. We also give a table of the function

$T(w_1,n_1,w_2,n_2,d)$ = maximum number of codewords in a binary code of length $n_1 + n_2$ and minimum distance d with exactly w_1 ones in the first n_1 coordinates and exactly w_2 ones in the last n_2 coordinates (see Table III),

for $n_1 + n_2 \leq 24$, $d = 10$.

All of the upper bounds on $A(n,d)$ outside the Plotkin range $n \leq 2d$ are obtained from modifications of Delsarte's linear programming method by making use of the values of $A(n,d,w)$. The tables of $A(n,d,w)$ are important both because they lead to bounds on $A(n,d)$, and because in their own right they give the size of the largest constant weight codes. They also give the solution to the following widely studied packing problem (see Erdös and Hanani [17], Kalbfleisch and Stanton [36], Schönheim [51], Stanton, Kalbfleisch and Mullin [59]): what is $D(t,k,v)$, the maximum number of k-subsets of a v-set S, such that every t-subset of S is contained in at most one k-set? The answer is $D(t,k,v) = A(v,2k - 2t + 2,k)$, so that Table II is also a table of values of $D(t,k,v)$.

TABLE I
VALUES OF $A(n,d)$

n	d=4	d=6	d=8	d=10
6	4	2	1	1
7	8	2	1	1
8	[a]16	2	2	1
9	[d]20[b]	4	2	1
10	[d]38 - 40	6	2	2
11	[d]72 - 80	12	2	2
12	[d]144 - 160	24	4	2
13	256	32[e]	4	2
14	512	64	8	2
15	1024	128	16	4
16	[a]2048	[f]256	32	4
17	[d]2560 - 3276	256 - 340	36 - 37[h]	6
18	[d]5120 - 6552	512 - 680	64 - 74	10
19	[d]9728 - 13104	1024 - 1288	128 - 144	20
20	[d]19456 - 26208	[g]2048 - 2372	256 - 279	40
21	[d]36864 - 43690	[g]2560 - 4096	512	40 - 55
22	[d]73728 - 87380	4096 - 6942	1024	[j]48 - 90
23	[d]147456 - 173784	8192 - 13774	2048	64 - 150
24	[d]294912 - 344636	[g]16384 - 24106	[i]4096	[k]128 - 280

[a] Hamming code [24].
[b] Theorem 6.
[d] Constructed in [21], [35], or [57].
[e] Theorem 4.
[f] Nordstrom–Robinson code [46].
[g] Constructed in [55].
[h] Theorem 9.
[i] Golay code [20].
[j] From a (24,48,12) Hadamard code.
[k] Constructed by [1].

Two recent papers which also use the linear programming approach are Best and Brouwer [3] and McEliece, Rodemich, Rumsey, and Welch [43].

Earlier tables of bounds on $A(n,d)$ were given in Johnson [33], McEliece *et al.* [42], and Sloane [53]. No table of $A(n,d,w)$ seems to have been published before, although unpublished tables of upper bounds exist (e.g., Delsarte *et al.* [12] and Johnson [32]). A table of $A(n,d,w)$ was promised in Stanton *et al.* [59] but has never appeared. A table of upper and lower bounds on linear codes appears in Helgert and Stinaff [29].

The following notation is used in this paper. All codes are binary. An (n,M,d) *code* consists of M (≥ 1) binary vectors (called *codewords*) of length n such that any two

Manuscript received September 9, 1976; revised April 5, 1977.
M. R. Best and A. E. Brouwer are with the Mathematical Centre, Amsterdam, The Netherlands.
F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane are with Bell Laboratories, Murray Hill, NJ 07974.
[1] We would appreciate hearing of any improvements to the tables. (Send them for example to N. J. A. Sloane, Mathematics and Statistics Research Center, Bell Laboratories, Murray Hill, NJ 07974, USA.)

TABLE IIA
DISTANCE 4: $A(n,d,w)$

n \ w	2	3[a]	4[a]	5	6	7	8	9	10	11	12
4	2	1	1								
5	2	2	1	1							
6	3	4	3	1	1						
7	3	7	7	3	1	1					
8	4	8	14	8	4	1	1				
9	4	12	18	18	12	4	1	1			
10	5	13	30	36	30	13	5	1	1		
11	5	17	[t]35	66	66	35	17	5	1	1	
12	6	20	51	[b]73-84	[e]132	73-84	51	20	6	1	1
13	6	26	65	[b]99-132	[d]143-182	143-182	99-132	65	26	6	1
14	7	28	91	[d]143-182	[d]210-308	[d]232-364	210-308	143-182	91	28	7
15	7	35	105	[d]213-271[f]	321-455	[d]435-660	435-660	321-455	213-271	105	35
16	8	37	140	[d]305-336	513-722	? -1040	[d]870-1320	? -1040	513-722	305-336	140
17	8	44	154-157	[d]424-476	792-952	? -1753	? -2210	? -2210	? -1753	792-952	424-476
18	9	48	[a]198	480-565	[d]1188-1428	? -2448	? -3944	? -4420	? -3944	? -2448	1188-1428
19	9	57	228	612-752	1428-1789	? -3876	? -5814	? -8326	? -8326	? -5814	? -3876
20	10	60	285	816-912	2040-2506	? -5111	? -9690	? -12920	? -16652	? -12920	? -9690
21	10	70	315	1071-1197	2856-3192	? -7518	? -13416	? -22610	? -27132	? -27132	? -22610
22	11	73	385	1386	3927-4389	? -10032	? -20674	? -32794	? -49742	? -54264	? -49742
23	11	83	416-419	1771	5313	? -14421	? -28842	? -52833	? -75426	? -104006	? -104006
24	12	88	498	[d]1859-2011	[e]7084	? -18216	? -43263	? -76912	? -126799	? -164565	? -208012

[a] Section IV-A.
[b] See [40].
[c] See [47].
[d] Miscellaneous constructions.
[e] From Theorem 9 and the Steiner systems $S(5,6,12)$, $S(3,5,17)$, $S(3,6,26)$, $S(5,6,24)$, $S(5,7,28)$, $S(5,8,24)$. ([13], [14], [66]).
[f] From Theorem 6 and the nonexistence of Steiner systems $S(4,5,15)$, $S(4,6,18)$. ([44], [66]).
[g] A cyclic code.
[h] From the 3-design with $t = 3$, $v = 16$, $k = 6$, $\lambda = 4$ obtained from the Nordstrom–Robinson code [46].
[i] From translates of the (16,256,6) Nordstrom–Robinson code, [46].
[j] From the (24,4096,8) Golay code, [20].
[k] From translates of the (16,32,8) Reed–Muller code.
[L] From linear programming.
[m] From a conference matrix, [56].
[n] A quasi-cyclic code.
[q] See [31], [34].
[r] See [62].
[s] See [60a].
[t] See Fig. 1.

codewords differ in at least d places, i.e., are at (*Hamming*) *distance* at least d apart. A code has *constant weight* w if each codeword contains w ones, i.e., has *weight* w. An *optimal* code is a code with the maximum number of codewords for the given n and d (and for the given w, in the case of a constant weight code).

Let $\mathcal{C}$ be an (n,M,d) code. The *weight distribution* of $\mathcal{C}$ with respect to a vector u is the $(n+1)$-tuple of integers $(A_i(u), i = 0, \cdots, n)$, where $A_i(u)$ is the number of codewords $v \in \mathcal{C}$ such that $\text{dist}(u,v) = i$. The *distance distribution* of $\mathcal{C}$ is the $(n+1)$-tuple of rational numbers $(A_0, A_1, \cdots, A_n)$ defined by

$$A_i = \frac{1}{M} \sum_{u \in \mathcal{C}} A_i(u), \qquad i = 0, \cdots, n.$$

Thus $A_0 = 1$, $A_i \geq 0$, and $\Sigma_i A_i = M \leq A(n,d)$.

II. BOUNDS ON $A(n,d)$

The first theorem is immediate, while the second gives $A(n,d)$ exactly if $n \leq 2d$.

Theorem 1:

$$A(n-1, 2\delta-1) = A(n, 2\delta),$$
$$A(n,d) \leq 2A(n-1,d).$$

Theorem 2: (Plotkin [48] and Levenshtein [39].) Provided certain Hadamard matrices of order n or less exist,[2]

$$A(n,2\delta) = 2\left[\frac{2\delta}{4\delta - n}\right], \qquad \text{if } 4\delta > n \geq 2\delta, \qquad (1)$$

[2] Hadamard matrices are known to exist for all orders congruent to 0(mod 4) and less than 268. In any case the right side is an upper bound on the left side in both (1) and (2).

```
11111111111100000000000000000000000
11100000000011111111100000000000000
00011100000011100000011111100000000
00010011000010011100011000011110000
00001000110011000001110011001111010000
10000100101000010010010101010010110
01000110000100001001001010110001110
00100001100101001000100011001010101
00100010011000100110010000101001101
10010000010101000101000100100110011
01001001001000110000101001000101011
```

Fig. 1. Columns form a constant weight code of length 11, weight 4, and distance 4, containing 35 codewords. Thus $A(11,4,4) = 35$.

TABLE IIB
DISTANCE 6: $A(n,6,w)$*

n\w	3	4	5	6	7	8	9	10	11	12
6	2	1	1	1						
7	2	2	1	1	1					
8	2	2	2	1	1	1				
9	3	3	3	3	1	1	1			
10	3	5	6	5	3	1	1	1		
11	3	6	11	11	6	3	1	1	1	
12	4	9	$h_{12}{}^{q}$	22	12	9	4	1	1	1
13	4	13^{g}	$h_{18}{}^{q}$	g_{26}	26	18	13	4	1	1
14	4	14	h_{28}	h_{42}	$d_{42-51}{}^{r}$	42	28	14	4	1
15	5	15	h_{42}	h_{70}	$i_{60-88}{}^{L}$	60-88	70	42	15	5
16	5	20	48	h_{112}	i_{90-156}	$i_{120-150}{}^{L}$	90-156	112	48	20
17	5	20^{d}	e_{68}	112-136	112-244^{L}	125-283	125-283	112-244	112-136	68
18	6	b_{22}	68-72	$d_{144-202}{}^{f}$	$i_{160-349}$	$i_{232-428}{}^{L}$	$249-425^{L}$	232-428	160-349	144-202
19	6	$c_{25}{}^{s}$	i_{72-83}	$i_{172-228}$	$i_{228-520}{}^{L}$	$i_{332-739}$	$d_{472-789}{}^{L}$	472-789	332-739	228-520
20	6	a_{30}	i_{81-100}	$i_{232-276}$	310-651	$i_{492-1199}{}^{L}$	$d_{672-1363}{}^{L}$	$d_{944-1421}{}^{L}$	672-1363	492-1199
21	7	a_{31}	$d_{102-126}$	$i_{253-350}$	465-828	$d_{668-1708}$	$d_{1068-2364}{}^{L}$	$d_{1286-2702}{}^{L}$	1286-2702	1068-2364
22	7	a_{37}	$d_{132-136}$	294-462	675-1100	$d_{708-2277}$	$d_{1288-3775}{}^{t}$	$d_{1450-4416}{}^{L}$	$d_{1574-5064}{}^{L}$	1450-4416
23	7	a_{40}	$d_{147-170}$	399-521	969-1518	708-3162	$d_{1428-5819}$	$d_{1570-7521}{}^{L}$	$d_{1718-7953}{}^{L}$	1718-7953
24	8	e_{42}	$e_{168-192}$	$e_{532-680}$	$e_{1368-1786}$	708-4554	$d_{1458-8432}$	1570-12418^{L}	2576-14682	2576-15906^{L}

* See footnotes to Table IIA.

and

$$A(4\delta,2\delta) = 8\delta,\ A(n,2\delta) = 1, \qquad \text{if } n < 2\delta, \tag{2}$$

where here and hereafter $[\cdot]$ denotes the largest integer not exceeding the enclosed number.

The linear programming approach is based on the following theorem.

Theorem 3: (Delsarte [8]–[10]) Let $\mathcal{C}$ be an (n,M,d) code with distance distribution $(A_0, \cdots, A_n)$. Then the quantities $B_0, \cdots, B_n$ are nonnegative, where

$$B_k = M^{-1} \sum_{i=0}^{n} A_i K_k(i), \qquad k = 0,1,\cdots,n, \tag{2a}$$

and K_k is a Krawtchouk polynomial, defined by

$$K_k(t) = \sum_{j=0}^{k} (-1)^j \binom{n-t}{k-j}\binom{t}{j}, \qquad k = 0,1,\cdots,n.$$

For later reference we give a short proof.

Proof: Let w be a word in $\{0,1\}^n$ of weight i. Then it is easily checked that, with $\langle w,x\rangle \triangleq \Sigma w_i x_i \bmod 2$,

$$\sum_{\substack{x\in\{0,1\}^n \\ wt(x)=k}} (-1)^{\langle w,x\rangle} = K_k(i).$$

Consequently, by the definition of A_i,

$$\begin{aligned} B_k &= M^{-1} \sum_{i=0}^{n} A_i K_k(i) \\ &= M^{-2} \sum_{i=0}^{n} \sum_{\substack{u,v\in\mathcal{C} \\ wt(u-v)=i}} \sum_{\substack{x\in\{0,1\}^n \\ wt(x)=k}} (-1)^{\langle u-v,x\rangle} \\ &= M^{-2} \sum_{\substack{x\in\{0,1\}^n \\ wt(x)=k}} b_x^2 \geq 0, \end{aligned} \tag{3a}$$

TABLE IIC
DISTANCE 8: $A(n,8,w)$*

n\w	4	5	6	7	8	9	10	11	12
8	2	1	1	1	1				
9	2	2	1	1	1	1			
10	2	2	2	1	1	1	1		
11	2	2	2	2	1	1	1	1	
12	3	3	4	3	3	1	1	1	1
13	3	3	4	4	3	3	1	1	1
14	3	4	7	8	7	4	3	1	1
15	3	6	k_{10}	15	15	10	6	3	1
16	4	6	k_{16}	16-22	30	16-22	16	6	4
17	4	7	b_{17}	$j_{21-31}{}^{L}$	m_{34-35}	34-35	21-31	17	7
18	4	j_9	j_{20-21}	$j_{33-41}{}^{L}$	j_{46-63}	j_{48-70}	46-63	33-41	20-21
19	4	j_{12}	j_{28}	j_{52-57}	j_{78-97}	$j_{88-122}{}^{L}$	88-122	78-97	52-57
20	5	j_{16}	j_{40}	j_{80}	$j_{130-142}$	$j_{160-215}$	$j_{176-244}{}^{L}$	160-215	130-142
21	5	j_{21}	j_{56}	j_{120}	j_{210}	$j_{280-331}$	$j_{336-399}{}^{L}$	336-399	280-331
22	5	21^{b}	j_{77}	j_{176}	j_{330}	280-497^{L}	$j_{616-728}$	$j_{672-798}$	616-728
23	5	g_{23}	77-80	j_{253}	j_{506}	$j_{400-816}$	616-1111^{L}	$j_{1288-1417}{}^{L}$	1288-1417
24	6	e_{24}	77-92	253-274	j_{759}	$j_{640-1160}{}^{L}$	$j_{960-1639}{}^{L}$	1288-2305^{L}	j_{2576}

* See footnotes to Table IIA.

TABLE IID
DISTANCE 10: $A(n,10,w)$*

n\w	5	6	7	8	9	10	11	12
10	2	1	1	1	1	1		
11	2	2	1	1	1	1	1	
12	2	2	2	1	1	1	1	1
13	2	2	2	2	1	1	1	1
14	2	2	2	2	2	1	1	1
15	3	3	3	3	3	3	1	1
16	3	3	3	4	3	3	3	1
17	3	3	5	6	6	5	3	3
18	3	4	6	9	10	9	6	4
19	3	4	8	12[b]	19	19	12	8
20	4	5	[n]10	[b]17-18	[g]20-24	38	20-24	17-18
21	4	7	13[b]	[g]21-26	[g]21-41[L]	38-49[L]	38-49	21-41
22	4	7	15-19	[g]22-35	[g]22-57[L]	?-74[L]	?-82[L]	?-74
23	4	8	[b]16-23	[g]23-50[L]	[g]23-87[L]	?-117[L]	?-135[L]	?-135
24	4	9	[g]24-27	[g]24-69	?-119[L]	?-171[L]	?-223[L]	?-247[L]

* See footnotes to Table IIA.

where

$$b_x = \sum_{u \in \mathcal{C}} (-1)^{\langle u,x \rangle}. \qquad \text{Q.E.D.} \quad (3b)$$

Note: If $\mathcal{C}$ is a linear code, then b_x equals M or O depending on whether x belongs to the dual code or not, and $B_0, \cdots, B_n$ is the weight distribution of the dual code.

To apply Theorem 3, let $\mathcal{C}$ be an optimal code of length n and minimum distance d. Then

$$M = A(n,d) = 1 + A_d + A_{d+1} + \cdots + A_n.$$

Suppose $L^*(n,d)$ is the optimal solution to the following linear programming problem: choose real variables $A_d, A_{d+1}, \cdots, A_n$ so as to maximize

$$L = A_d + A_{d+1} + \cdots + A_n$$

subject to the constraints

$$A_i \geq 0, \qquad i = d, \cdots, n,$$

$$B_k \geq 0, \qquad k = 0, \cdots, n,$$

where

$$B_k = M^{-1} \left(K_k(0) + \sum_{i=d}^{n} A_i K_k(i) \right).$$

TABLE IIIA
UPPER BOUNDS FOR $T(w_1,n_1,w_2,n_2,10)$*

w_1	n_1 \ w_2 n_2	5 10	5 11	5 12	5 13	5 14	5 15	5 16	5 17	5 18	5 19	5 20	5 21	5 22	6 12	6 13	6 14	6 15	6 16	6 17	6 18	6 19	6 20	6 21	6 22	7 14	7 15	7 16	7 17	7 18	7 19	7 20	7 21	7 22
1	2	2*	2*	2*	3*	3*	3*	4*	4*	4*	5*	5*	6*	6*	2*	3*	4*	5*	6	6	8	8	10	14	14	4*	6	6	10	12	16	20	26	38
1	3	2*	2*	3*	3*	3*	4*	4*	5*	6*	7*	7*	9*		3*	4*	5*	6	8	9	12	12	15	21		6*	7	9	15	18	24	30	39		
1	4	2*	2*	3*	3*	4*	4*	5*	6*	7*	8*	9*			4*	4*	5*	7	9	12	16	16	20			6*	9	12	20	24	32	40			
1	5	2*	2*	3*	3*	4*	5*	6*	7*	7*	8*				4*	4*	5*	7	10	15	20	20				6*	10	15	24	30	40				
1	6	2*	2*	3*	3*	4*	6*	6*	7*	8*					4*	4*	6*	8	11	17	21					6*	11	18	26	36					
1	7	2*	2*	3*	3*	4*	6*	6*	7*						4*	4*	7*	8*	11	17						7*	11	18	26						
1	8	2*	2*	3*	3*	4*	6*	6*							4*	4*	7*	8*	12							8*	11	18							
1	9	2*	2*	3*	3*	4*	6*								4*	4*	7*	9*								8*	12								
1	10	2*	2*	3*	3*	4*									4*	4*	7*									8*									
1	11	2*	2*	3*	3*										4*	4*																		
1	12	2*	2*	3*											4*																			
1	13	2*	2*																															
1	14	2*																																

* Bound is exact.

TABLE IIIB
UPPER BOUNDS FOR $T(w_1,n_1,w_2,n_2,10)$*

w_1	n_1 \ w_2 n_2	4 8	4 9	4 10	4 11	4 12	4 13	4 14	4 15	4 16	4 17	4 18	4 19	4 20	5 10	5 11	5 12	5 13	5 14	5 15	5 16	5 17	5 18	5 19	5 20	6 12	6 13	6 14	6 15	6 16	6 17	6 18	6 19	6 20
2	4	2*	2*	2*	3*	3*	3*	4*	4*	4*	4*	5*	5*	5*	2*	3*	4*	5*	6	6	8	10	12	14	14	4*	6	8	12	16	18	24	24	30
2	5	2*	2*	3*	3*	3*	4*	4*	5*	5*	5*	6*	6*		3*	4*	5*	6	8	10	12	15	17	20		6	8	12	17	22	30	40	40		
2	6	2*	3*	3*	3*	4*	4*	5*	6*	6*	7*	9			4*	4*	6	8	10	15	18	20	21			6	11	15	21	30	45	60			
2	7	2*	3*	3*	4*	4*	5*	7*	7*	8	9				4*	5*	7*	9	12	18	21	24				8	14	21	28	38	58				
2	8	2*	3*	4*	4*	5*	6*	7*	8	9					4*	5*	8	11	16	21	24					9	16	25	32	44					
2	9	2*	3*	4*	5*	6*	6*	7*	9						4*	6	9	13	16	21						10	18	30	36						
2	10	2*	3*	5*	5*	6*	7*	8							5*	6	10	15	19							12	20	35							
2	11	2*	3*	5*	5*	6*	7*								5*	7	10	15								12	21								
2	12	2*	3*	5*	6*	6*									6*	7	12									14									
2	13	2*	3*	5*	6*										6*	7																		
2	14	2*	3*	5*											6*																			
2	15	2*	3*																															
2	16	2*																																

* Bound is exact.

TABLE IIIC
UPPER BOUNDS FOR $T(w_1,n_1,w_2,n_2,10)$*

w_1	n_1	w_2=3, n_2=6	3, 7	3, 8	3, 9	3, 10	3, 11	3, 12	3, 13	3, 14	3, 15	3, 16	3, 17	3, 18	4, 8	4, 9	4, 10	4, 11	4, 12	4, 13	4, 14	4, 15	4, 16	4, 17	4, 18	5, 10	5, 11	5, 12	5, 13	5, 14	5, 15	5, 16	5, 17	5, 18
3	6	2*	2*	2*	3*	3*	3*	4*	4*	4*	4*	4*	4*	4*	2*	3*	4*	4*	6	6	7	8	9	10	12	4*	6	8	11	16	20	24	30	34
3	7	2*	2*	3*	3*	3*	4*	4*	4*	5*	5*	5*	5*		3*	4*	5*	6	7	9	11	13	14	16		6	8	12	18	23	33	41	46		
3	8	2*	2*	3*	3*	4*	4*	5*	5*	5*	6*	6*			4*	5*	6	8	10	13	17	18	21			8*	11	18	24	32	48	56			
3	9	3*	3*	3*	4*	4*	5*	6*	6*	6*	7*				4*	6*	7	10	15	18	21	22				9	15	24	33	48	63				
3	10	3*	3*	4*	4*	5*	6	7	7	8					4*	7	10	13	18	20	23					12	20	30	43	53					
3	11	3*	4*	4*	5*	6	7*	8	9						5*	7	11	16	21	25						14	22	36	54						
3	12	4*	4*	5*	6*	7	8	9							6*	9	13	19	24							18	28	40							
3	13	4*	4*	5*	6*	7	9								6*	9	15	19								18	30								
3	14	4*	5*	5*	6*	8									6*	10	15									20									
3	15	4*	5*	6*	7*										7	12																		
3	16	4*	5*	6*											8																			

* Bound is exact.

TABLE IIID
UPPER BOUNDS FOR $T(w_1,n_1,w_2,n_2,10)$

w_1	n_1	w_2=8, n_2=16	8, 17	8, 18	8, 19	8, 20	8, 21	8, 22	9, 18	9, 19	9, 20	9, 21	9, 22
1	2	8	12	18	24	40	52	70	20	38	52	82	114
1	3	12	18	27	36	60	78		30	57	78	123	
1	4	16	24	36	48	80			40	76	104		
1	5	20	30	**45**	60				50	95			
1	6	22	36	54					60				
1	7	22	38										
1	8	22											

w_1	n_1	w_2=6, n_2=12	6, 13	6, 14	6, 15	6, 16	6, 17	6, 18	7, 14	7, 15	7, 16	7, 17	7, 18
3	6	10	16	24	34	44	60	80	30	44	60	100	120
3	7	14	25	35	49	70	104		42	70	**105**	**153**	
3	8	21	37	56	74	101			56	100	148		
3	9	27	48	75	96				84	129			
3	10	33	60	94					104				
3	11	44	73										
3	12	48											

w_1	n_1	w_2=7, n_2=14	7, 15	7, 16	7, 17	7, 18	7, 19	7, 20	8, 16	8, 17	8, 18	8, 19	8, 20
2	4	10	14	18	30	36	48	60	24	36	54	72	120
2	5	15	22	30	50	60	80		40	60	90	120	
2	6	18	30	45	72	90			60	90	135		
2	7	21	38	63	91				76	115			
2	8	28	44	72					88				
2	9	36	49										
2	10	40											

TABLE IIIE
UPPER BOUNDS FOR $T(w_1,n_1,w_2,n_2,10)$*

w_1	n_1	w_2=4, n_2=8	4, 9	4, 10	4, 11	4, 12	4, 13	4, 14	4, 15	4, 16	5, 10	5, 11	5, 12	5, 13	5, 14	5, 15	5, 16	6, 12	6, 13	6, 14	6, 15	6, 16
4	8	4*	6*	8	10	14	18	21	22	28	10*	16	24	36	46	63	70	28	50	70	98	132
4	9	6*	9*	12	18	21	29	31	37		18*	24	40	54	72	93		47	76	107	151	
4	10	8	12	17	25	33	42	51			22	37	60	82	107			67	104	153		
4	11	10	18	25	35	48	55				33	55	81	108				90	139			
4	12	14	21	33	48	63					42	66	102					116				
4	13	18	29	42	55						58	89										
4	14	21	31	51							62											
5	10										36*	48	73	96	125							
5	11										48	77	106	146								
5	12										73	106	154									

* Bound is exact.

Then plainly

$$A(n,d) \leq 1 + L^*(n,d).$$

This is the simplest version of the *linear programming bound* for binary codes (Delsarte [8]).

Often it is possible to impose additional constraints on the B_i. Certainly

$$B_i \leq A(n,d,i), \tag{4}$$

so bounds on $A(n,d,w)$ can be used (see Table II). Sometimes several such bounds can be combined, as the following example illustrates.

Theorem 4: $A(13,6) = 32$, and so the Nadler code is optimal.

Proof: In 1959, Stevens and Bouricius [60] found (13,32,6) and (14,64,6) codes, showing that $A(13,6) \geq 32$.

The former code was rediscovered by Nadler [45], and is usually referred to as the Nadler code. (See also Van Lint [41].)

To prove $A(13,6) \leq 32$, we proceed as follows. First observe that, if we shorten a $(13,M,6)$ code and then add an overall parity check, we get a $(13,M,6)$ code $\mathcal{C}$ in which all distances are even.

If (A_i) is the distance distribution of $\mathcal{C}$, then $A_0 = 1$ and the remaining A_i's are zero except (possibly) for A_6, A_8, A_{10}, and A_{12}. The inequalities $B_k \geq 0$ become

$$\begin{aligned}
&13 + A_6 - 3A_8 - 7A_{10} - 11A_{12} \geq 0,\\
&\binom{13}{2} - 6A_6 - 2A_8 + 18A_{10} + 54A_{12} \geq 0,\\
&\binom{13}{3} - 6A_6 + 14A_8 - 14A_{10} - 154A_{12} \geq 0,\\
&\binom{13}{4} + 15A_6 - 5A_8 - 25A_{10} + 275A_{12} \geq 0,\\
&\binom{13}{5} + 15A_6 - 25A_8 + 63A_{10} - 197A_{12} \geq 0,\\
&\binom{13}{6} - 20A_6 + 20A_8 - 36A_{10} + 132A_{12} \geq 0. \qquad (5)
\end{aligned}$$

Furthermore we have

$$A_{12}(u) \leq A(13,6,12) = A(13,6,1) = 1,$$

$$A_{10}(u) \leq A(13,6,10) = A(13,6,3) = 4.$$

However, these can be combined. For if $A_{12}(u) = 1$ then $A_{10}(u) = 0$. So

$$A_{10}(u) + 4A_{12}(u) \leq 4,$$

and averaging over u gives

$$A_{10} + 4A_{12} \leq 4. \qquad (6)$$

Actually (6) and the first two constraints of (5) turn out to be enough, and so we consider the problem: maximize

$$A_6 + A_8 + A_{10} + A_{12}$$

subject to

$$A_6 \geq 0, A_8 \geq 0, A_{10} \geq 0, A_{12} \geq 0$$

and

$$\begin{aligned}
13 + A_6 - 3A_8 - 7A_{10} - 11A_{12} &\geq 0,\\
78 - 6A_6 - 2A_8 + 18A_{10} + 54A_{12} &\geq 0,\\
4 - A_{10} - 4A_{12} &\geq 0. \qquad (7)
\end{aligned}$$

The dual problem is minimize

$$13u_1 + 78u_2 + 4u_3$$

subject to

$$u_1 \geq 0, u_2 \geq 0, u_3 \geq 0$$

and

$$\begin{aligned}
1 + u_1 - 6u_2 &\leq 0,\\
1 - 3u_1 - 2u_2 &\leq 0,\\
1 - 7u_1 + 18u_2 - u_3 &\leq 0,\\
1 - 11u_1 + 54u_2 - 4u_3 &\leq 0. \qquad (8)
\end{aligned}$$

Feasible solutions to these two problems are

$$A_6 = 24, A_8 = 3, A_{10} = 4, A_{12} = 0, \qquad (9)$$

$$u_1 = u_2 = \frac{1}{5}, u_3 = \frac{16}{5}. \qquad (10)$$

In fact, since the corresponding objective functions are equal, i.e., since

$$24 + 3 + 4 + 0 = 13 \cdot \frac{1}{5} + 78 \cdot \frac{1}{5} + 4 \cdot \frac{16}{5} = 31,$$

it follows that (9) and (10) are optimal solutions. (These solutions are easily obtained by hand using the simplex method—see [18] or [52].) It follows that $A(12,5) = A(13,6) \leq 32$. Q.E.D.

Remark: The following argument shows that (9) is the unique optimal solution. Let x_6, x_8, x_{10}, x_{12} be any optimal solution to the primal problem. The u_i of (10) are all positive and satisfy the first three constraints of (8) with equality, but not the fourth. Hence, from the theorem of complementary slackness (Simonnard [52]), the x_i must satisfy the primal constraints (7) with equality, and $x_{12} = 0$. These three equations have the unique solution

$$x_6 = 24, x_8 = 3, x_{10} = 4.$$

Thus (9) is the unique optimal solution. Therefore the distance distribution of a (13,32,6) code in which all distances are even is unique. This result has been used by Goethals [19] to show that the code itself is unique and that there are exactly two nonequivalent (12,32,5) codes (cf. Nadler [45], Van Lint [41]).

If $A(n,d) \not\equiv 0 \pmod 4$, the right side of the Delsarte inequalities $B_k \geq 0$ can sometimes be increased, as shown by Theorems 5 and 8.

Theorem 5: Let $\mathcal{C}$ be an (n,M,d) code with $M = A(n,d)$, and suppose that M is odd. Then

$$B_k \geq M^{-2}\binom{n}{k}, \qquad k = 0,1,\cdots,n. \qquad (10a)$$

Proof: If M is odd, then b_x (in (3b)) is odd, and hence nonzero. From (3a) we get

$$B_k \geq M^{-2} \sum_{\substack{x \in \{0,1\}^n \\ wt(x)=k}} b_x^2 \geq M^{-2}\binom{n}{k}. \qquad \text{Q.E.D.}$$

Remark: In the expression (2a) for B_k, the term corresponding to $i = 0$ (with $A_0 = 1$) is $M^{-1}K_k(0) = M^{-1}\binom{n}{k}$. Therefore the inequality (10a) enables us to rewrite (2a) as

$$\frac{M-1}{M^2}\binom{n}{k} + \frac{1}{M}\sum_{i=1}^{n} A_i K_k(i) \geq 0, \qquad 0 \leq k \leq n.$$

This means that if no extra inequalities have been added, the optimal solution is simply $(M-1)/M$ times the original one, and hence $\Sigma_{i=0}^{n} A_i \leq M - 1$, lowering the bound by exactly one. If extra inequalities are added, the gain is in general less.

As an application, we prove the following result.

Theorem 6: $A(9,4) = 20$.

Proof: Golay [21] found a (9,20,4) code, thus $A(9,4) \geq 20$. A cyclic (8,20,3) code is given in Sloane and Whitehead [57]. To prove $A(9,4) \leq 20$, as usual let $\mathcal{C}^-$ be an $(8,M,3)$ code with $M = A(8,3) = A(9,4)$; and let $\mathcal{C}$ be the $(9,M,4)$ extended even weight code, which has distance distribution $(A_0, \cdots, A_9)$ with $A_0 = 1$ and $A_1 = A_2 = A_3 = A_5 = A_7 = A_9 = 0$.

First, we maximize $A_4 + A_6 + A_8$ subject to $A_i \geq 0$, $B_k \geq 0$, and $A_8 \leq 1$. We obtain $A_4 + A_6 + A_8 \leq 20\frac{1}{3}$ and hence $M \leq 21$.

Suppose $M = 21$. Then, by Theorem 5, we can replace $B_k \geq 0$ by $B_k \geq (\frac{1}{441})\binom{9}{k}$. Since M is odd, it is obvious that $A_8 \leq \frac{20}{21}$. Hence in this case, in spite of the extra inequality, all constant terms occurring in the inequalities are multiplied by $\frac{20}{21}$, so

$$M \leq 1 + \frac{20}{21} \cdot 20\frac{1}{3} < 21.$$

Hence $A(9,4) = 20$. Q.E.D.

If $A(n,d) \equiv 2 \pmod 4$, then a positive lower bound for B_k can be obtained by noting that b_x cannot be zero too often. For example, if u_1, u_2, and $u_1 + u_2$ are distinct, then b_{u_1}, b_{u_2}, and $b_{u_1+u_2}$ cannot all be zero. The following linear inequality can be obtained in this way.

Theorem 7: Let $\mathcal{C}$ be an (n,M,d) code with $M = A(n,d)$, and suppose that $M \equiv 2 \pmod 4$. Then

$$B_k \geq \frac{4}{3M^2}\binom{n}{k},$$

if (i) k is even and $0 \leq k \leq \frac{2}{3}n$, or (ii) if d is even, $k \equiv n \pmod 2$, and $\frac{1}{3}n \leq k \leq n$.

A slightly stronger result is stated in the following theorem.

Theorem 8: Let $\mathcal{C}$ be an (n,M,d) code with $M = A(n,d)$, and suppose that $M \equiv 2 \pmod 4$. Then there exists an $l \in \{0,1, \cdots, n\}$ such that

$$B_k \geq 2M^{-2}\left(\binom{n}{k} + K_k(l)\right), \qquad k = 0,1, \cdots, n.$$

(Since $|K_k(l)| \leq \binom{n}{k}$, this also improves Theorem 3.)

Proof: Since M is even, b_u is even for each $u \in \{0,1\}^n$. Let e_j be the jth unit vector in $\{0,1\}^n$. Then

$$b_x - b_{x+e_j} = \sum_{u \in \mathcal{C}} (1 - (-1)^{\langle u, e_j \rangle})(-1)^{\langle u,x \rangle}.$$

Hence, for fixed j, the residue class of $b_x - b_{x+e_j} \pmod 4$ is even and independent of the choice of x.

Let J be the set of those $j \in \{1,2, \cdots, n\}$ for which $b_x - b_{x+e_j} \equiv 2 \pmod 4$, and let $l = |J|$ and $\xi = \Sigma_{j \in J} e_j$. Then

$$b_x - b_{x+e_j} \equiv 2\langle e_j, \xi \rangle \pmod 4.$$

By induction on the weight of x it follows that, since $b_0 = M \equiv 2 \pmod 4$,

$$b_x \equiv 2 + 2\langle x, \xi \rangle \pmod 4.$$

Now, for each $k \in \{0,1, \cdots, n\}$,

$$B_k = M^{-2} \sum_{\substack{x \in \{0,1\}^n \\ wt(x)=k}} b_x^2 \geq 2M^{-2} \sum_{\substack{x \in \{0,1\}^n \\ wt(x)=k}} (1 + (-1)^{\langle x, \xi \rangle})$$

$$= 2M^{-2}\left(\binom{n}{k} + K_k(l)\right). \quad \text{Q.E.D.}$$

We mention the following immediate consequence of Theorem 8, which is weaker but easier to apply.

Corollary: Let $\mathcal{C}$ be an (n,M,d) code with $M = A(n,d)$, and suppose that $M \equiv 2 \pmod 4$. Then

$$B_k \geq 2M^{-2}\left(\binom{n}{k} + \min_{l \in \{0,1, \cdots, n\}} K_k(l)\right),$$

e.g., $B_2 \geq (4/M^2)\left(\binom{n}{2} - [n^2/4]\right)$.

For example, this corollary can be used to prove the upper bound in Theorem 9; the lower bound comes from [56], [57].

Theorem 9: $A(17,8) = 36$ or 37.

Table I gives the bounds on $A(n,d)$. Many values come from Theorems 1 and 2. Otherwise the unmarked upper bounds are obtained by linear programming, as illustrated in Theorems 4 and 6. Other entries are explained by the key. The bounds $A(9,4) \leq 20$, $A(10,4) \leq 39$, $A(11,4) \leq 78$, and $A(12,4) \leq 154$ were claimed by Wax [63] in 1959. However, as we shall see in the next section, such bounds cannot be obtained by his method.

We conclude this section by repeating Elspas's question [16]: can $A(n,d)$ be odd and greater than one? From Theorem 2 and Table I we have the following theorem.

Theorem 10: If $A(n,d)$ is odd (and greater than one), then $A(n,d) \geq 37$. If Hadamard matrices exist of all orders congruent to 0(mod 4), then $A(n,d)$ is even whenever $n \leq 2d$.

III. The End of the Wax Bound

In 1959, Wax [63] computed a number of upper bounds for binary codes by a method used by Rankin [49] to obtain sphere packing bounds in Euclidean space (see also Rogers [50]). Most of the bounds obtained were rather weak, but there were three special cases in which his "soft sphere model" seemingly yielded astonishingly good results. These were

$A(8,3) \leq 20$,
$A(9,3) \leq 39$ (and hence $A(10,3) \leq 78$),
$A(11,3) \leq 154$.

The first bound is confirmed by Theorem 6, but no proof of the other bounds is known.

We were unable to duplicate Wax's calculations, and in fact in this section we shall establish a lower bound on the best upper bound that can be achieved with the soft sphere model, no matter which weight function is used. Since this lower bound is inconsistent with the data found by Wax, we may conclude that Wax's results are—at least in the interesting cases mentioned above—erroneous.

We are now left with the following bounds for $A(8,3)$, $A(9,3)$, $A(10,3)$, and $A(11,3)$:

$$A(8,3) = 20,$$
$$38 \le A(9,3) \le 40,$$
$$72 \le A(10,3) \le 80,$$
$$144 \le A(11,3) \le 160.$$

A. The Soft Sphere Model

Consider an (n,M,d) code as a subset of the vertices of the hypercube $[0,1]^n$ in Euclidean n-space $\mathbb{R}^n$. The Euclidean distance between two code points is at least $\sqrt{d}$. Therefore the spheres with centers at the code points and radii $R = \frac{1}{2}\sqrt{d}$ are disjoint. If V denotes the volume of the intersection of each sphere with the hypercube $[0,1]^n$ (by symmetry these volumes are all equal), then the number of code points evidently cannot exceed $1/V$. Hence $A(n,d) \le [1/V]$.

This method, called the "hard sphere model," yields very modest results, e.g., $A(9,3) \le 566$ (and not 56.7 as in Wax [63]) or $A(10,4) \le 401$.

In order to sharpen the bounds, the hard spheres are replaced by larger ones with variable mass density. As basic conditions, it is required that

(i) the density $\rho(x)$ associated with a single sphere is nonnegative and depends only on the distance to the center of that sphere, and
(ii) in any configuration of (partly overlapping) spheres with centers at least $2R$ apart, the total density at each point does not exceed unity.

If μ is the mass of the intersection of each sphere with the hypercube[3], we now obtain

$$A(n,d) \le [1/\mu].$$

The main problem is to determine a suitable density which satisfies the basic conditions (i) and (ii) and maximizes the mass μ. Rankin studied this problem in [49]. In order to simplify computations, he required in addition that

(iii) the spheres have radius $R\sqrt{2}$, i.e., $\rho(r) = 0$ if $r \ge R\sqrt{2}$.

The model described, with the conditions (i), (ii), and (iii), is called the "soft sphere model." We shall denote the least upper bound for $A(n,d)$ that can be achieved with this model by $A_w(n,d)$. Our aim is to give a lower bound for $A_w(n,d)$.

[3] In case $d \le 4$, one may instead define μ by 2^{-n} times the mass of the whole sphere, since the configuration may be continued with period 2 in all directions in $\mathbb{R}^n$. However, this extended model is also included in our analysis.

B. A Lower Bound for $A_w(n,d)$

First we derive an upper bound for ρ. We define, for each positive integer m,

$$y_m = \sqrt{2(m-1)/m}$$

(note: $y_1 = 0$, $y_2 = 1$), and the function σ: $[0,\infty] \to [0,1]$ by

$$\sigma(r) = \frac{1}{m}, \quad \text{if } Ry_m \le r < Ry_{m+1}, \quad m = 1,2,\cdots,n,$$
$$= \frac{1}{n+1}, \quad \text{if } Ry_{n+1} \le r < R\sqrt{2},$$
$$= 0, \quad \text{if } r \ge R\sqrt{2}.$$

Then we have the following lemma.

Lemma 11: $\rho \le \sigma$.

Proof: We have to prove that $\rho(r) \le 1/m$ if $r \ge Ry_m$ for $m = 1,2,\cdots,n+1$. Let $m \in \{1,2,\cdots,n+1\}$. Suppose m spheres with density function ρ are arranged so that their centers form the vertices of an $(m-1)$-dimensional regular simplex in $\mathbb{R}^n$ with edges of length $2R$. Then the distance from the center of gravity of the simplex to each of the vertices equals

$$R\sqrt{2(m-1)/m} = Ry_m.$$

(Proof by induction.)

The total density at the center of gravity equals $m\rho(Ry_m)$. Hence $\rho(Ry_m) \le 1/m$ and *a fortiori* $\rho(r) \le 1/m$ if $r \ge Ry_m$. Q.E.D.

This estimate for ρ immediately gives rise to an upper bound on the mass μ.

Lemma 12:

$$\mu \le \left(\frac{\pi e R^2}{n}\right)^{n/2} \frac{1}{\sqrt{\pi n}} \cdot \left(\sum_{m=1}^{n} \frac{1}{m(m+1)} \left(\frac{m}{m+1}\right)^{n/2} + \frac{1}{n+1}\right).$$

Proof: We denote the volume of the intersection of the n-dimensional hypersphere with radius r and center O in $\mathbb{R}^n$ and the n-dimensional hypercube $[0,1]^n$ by $B(r)$. The volume of the n-dimensional unit sphere will be denoted by J_n. It is well-known (see Sommerville [57a, p. 136], Feller [17a, p. 52]) that

$$J_n = \frac{\pi^{n/2}}{(n/2)!} \le \frac{\pi^{n/2} e^{n/2}}{(n/2)^{n/2}\sqrt{\pi n}} = \left(\frac{2\pi e}{n}\right)^{n/2} \frac{1}{\sqrt{\pi n}}.$$

Hence

$$\mu = \int_0^{R\sqrt{2}} \rho(r)\, dB(r) \le \int_0^{R\sqrt{2}} \sigma(r)\, dB(r)$$

$$= -\int_0^{R\sqrt{2}} B(r)\, d\sigma(r) \le -\int_0^{R\sqrt{2}} 2^{-n} J_n r^n\, d\sigma(r)$$

$$= 2^{-n} J_n \left(\sum_{m=2}^{n+1} \left(\frac{1}{m-1} - \frac{1}{m} \right) \cdot (Ry_m)^n + \frac{1}{n+1} (R\sqrt{2})^n \right)$$

$$\le \left(\frac{R}{2}\right)^n \left(\frac{2\pi e}{n}\right)^{n/2} \frac{1}{\sqrt{\pi n}} \left(\sum_{m=2}^{n+1} \frac{1}{(m-1)m} \cdot \left(\frac{2(m-1)}{m}\right)^{n/2} + \frac{2^{n/2}}{n+1} \right)$$

$$= \left(\frac{\pi e R^2}{n}\right)^{n/2} \frac{1}{\sqrt{\pi n}} \left(\sum_{m=1}^{n} \frac{1}{m(m+1)} \cdot \left(\frac{m}{m+1}\right)^{n/2} + \frac{1}{n+1} \right). \qquad \text{Q.E.D.}$$

This leads to the lower bound for $A_w(n,d)$.

Theorem 13:

$$A_w(n,d) \ge \left[\left(\frac{4n}{\pi e d}\right)^{n/2} \sqrt{\pi n} \left(\sum_{m=1}^{n} \frac{1}{m(m+1)} \cdot \left(\frac{m}{m+1}\right)^{n/2} + \frac{1}{n+1} \right)^{-1} \right].$$

Proof: $R = \frac{1}{2}\sqrt{d}$ and $A_w(n,d) = [1/\mu]$ for some density function ρ. Q.E.D.

Examples:

$$A_w(8,3) \ge 45, \quad A_w(9,4) \ge 27,$$
$$A_w(9,3) \ge 101, \quad A_w(10,4) \ge 56,$$
$$A_w(10,3) \ge 238, \quad A_w(11,4) \ge 119,$$
$$A_w(11,3) \ge 579, \quad A_w(12,4) \ge 259.$$

IV. Bounds on $A(n,d,w)$

The first two theorems are well-known (cf. Johnson [33]).

Theorem 14: Let d,w,n be integers, $d \neq 0$, $w \le n$. Then,

(i) $A(n,d-1,w) = A(n,d,w)$, if d is even,
(ii) $A(n,d,w) = A(n,d,n-w)$,
(iii) $A(n,d,w) = 1$, if $d > 2w$,
(iv) $A(n,d,w) = \left[\frac{n}{w}\right]$, if $d = 2w$.

Theorem 15: If a $2d \times 2d$ Hadamard matrix exists,

$$A(2d-2,d,d-1) = d,$$
$$A(2d-1,d,d-1) = 2d-1,$$
$$A(2d,d,d) = 4d-2.$$

Theorems 16–18 are due to Johnson [30], [31].

Theorem 16:

$$A(n,d,w) \le \left[\frac{dn}{dn - 2w(n-w)} \right]$$

provided the denominator is positive.

A slightly stronger result is given in the following theorem.

Theorem 17: Suppose $A(n,d,w) = M$, and define q and r by

$$wM = nq + r, \qquad 0 \le r < n.$$

Then

$$nq(q-1) + 2qr \le (w - d/2)M(M-1).$$

Theorem 18:

$$A(n,d,w) \le \left[\frac{n}{w} A(n-1,d,w-1) \right], \qquad (n \ge w \ge 1),$$

$$A(n,d,w) \le \left[\frac{n}{n-w} A(n-1,d,w) \right], \qquad (n > w \ge 0).$$

Theorem 19: If $n \ge w \ge t$, then

$$A(n,d,w) \le \frac{n}{w} \cdot \frac{n-1}{w-1} \cdot \cdots \cdot \frac{n-t+1}{w-t+1} \cdot A(n-t,d,w-t).$$

If equality holds, then any optimal constant weight code with parameters n,d,w is a t-design. In particular,

$$A(n,2\delta,w) = \frac{n(n-1)\cdots(n-w+\delta)}{w(w-1)\cdots\delta}$$

if and only if a Steiner system $S(w-\delta+1,w,n)$ exists. (For a bibliography of Steiner systems up to 1973, see Doyen and Rosa [14].)

A. Optimal Constant Weight Codes

As noted in the introduction, the determination of $A(n,d,w)$ is equivalent to determining I here $v = n$, $k = w$, and $t = k + 1 - \frac{1}{2}d$ (if d is even). However, this requires the construction of (maximal partial) Steiner t-designs, which is trivial for $t = 1$, while for $t = 2$ the recursive techniques of Hanani and Wilson are available (see, e.g., Wilson [64], [65]). For larger t, almost nothing is known (the best studied case being $t = 3$, $k = 4$). The known results are as follows.

1) *$t = 1$:* This is Theorem 14 (iv): $A(n,2w,w) = [n/w]$.

2) $t = 2$: In this case, we must look for a maximal collection of w-subsets of an n-set such that no 2-subset is covered twice (in other words, an edge-disjoint packing of w-cliques in the complete graph on n points). If a balanced incomplete block design exists with parameters $(b,v = n,r,k = w,\lambda = 1)$, that is, an $S(2,w,n)$, then obviously $A(n,d,w) = b = \binom{n}{2} / \binom{w}{2}$; otherwise we must look for the nearest approximation to this Steiner system.

a) $d = 4$, $w = 3$: It has been shown by Kirkman [38] in the cases $n \equiv 0, 1, 2$, or 3 (mod 6) and by Schönheim [51] in the remaining cases that

$$A(n,4,3) = \begin{cases} \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor, & \text{for } n \not\equiv 5 \pmod 6 \\ \left\lfloor \frac{n}{3} \left\lfloor \frac{n-1}{2} \right\rfloor \right\rfloor - 1, & \text{for } n \equiv 5 \pmod 6, \end{cases}$$

(see also Guy [22], Spencer [58] and Swift [61]). The cases $n \equiv 1$ or 3 (mod 6) correspond to Steiner triple systems.

b) $d = 6$, $w = 4$: As has been shown by Hanani [26], there exist Steiner systems $S(2,4,n)$ if and only if $n \equiv 1$ or 4 (mod 12). In Brouwer and Schrijver [7], group divisible designs GD(4,1,2;n) are constructed for each $n \equiv 2$ (mod 6), $n \neq 8$. In Brouwer [5], pairwise balanced designs PBD($\{4,7^*\};n$) are constructed for each $n \equiv 7$ or 10 (mod 12), $n \neq 10,19$. By using these and some similar constructions, it follows that if we define

$$\text{JB}(n,6,4) = \begin{cases} \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor - 1, & \text{for } n \equiv 7 \text{ or } 10 \pmod{12} \\ \left\lfloor \frac{n}{4} \left\lfloor \frac{n-1}{3} \right\rfloor \right\rfloor, & \text{otherwise,} \end{cases}$$

then $A(n,6,4) = \text{JB}(n,6,4)$ for all n with the exceptions of $n = 8$–11, 17, 19. The values of $A(n,6,4)$ for $n = 8$–11 are easily determined by hand, that of $A(17,6,4)$ was determined in Brouwer [4], and $A(19,6,4)$ was determined by Phinney [47] and Stinson [60a].

We conjecture that, for $t = 2$, w fixed and n sufficiently large (i.e., $n \geq n_0(w)$), $A(n,d,w)$ equals the Johnson bound (obtained by applying Theorems 14 and 18) (cf. Wilson [64]).

c) $d = 8$, $w = 5$: As shown by Hanani [26], [27], there exist Steiner systems $S(2,5,n)$ if and only if $n \equiv 1$ or 5 (mod 20). Shortening these gives optimal codes for $n \equiv 0$ or 4 (mod 20).

The values of $A(n,8,5)$ in Table II for $n \leq 15$ follow from the following observation.

Theorem 20: If d is even, $\lambda = w - d/2$ and $M \leq w/\lambda + 1$, then $A(n,d,w) \geq M$ if and only if $n \geq wM - \lambda\binom{w}{2}$.

Many more values of $A(n,8,5)$ are known, but most lie outside the range of the table.

3) $t = 3$, $d = 4$, $w = 4$: As shown by Hanani [25], Steiner quadruple systems exist for each $n \equiv 2$ or 4 (mod 6). Hence for these values of n we have $A(n,4,4) = \frac{1}{4}\binom{n}{3}$.

Shortening these codes once gives $A(n,4,4) = n(n-1)(n-3)/24$ for $n \equiv 1$ or 3 (mod 6). Upon using triplewise balanced designs TBD($\{4,6\};n$) in which the blocks of size 6 form a partition, it follows that $A(n,4,4) = n(n^2 - 3n - 6)/24$ for $n \equiv 0$ (mod 6) (cf. Brouwer [6]). Exact values for the case $n \equiv 5$ (mod 6) are not known.

B. The Linear Programming Bound for $A(n,d,w)$

This bound is based on the following theorem.

Theorem 21: (Delsarte [9], [10].) Let $\mathcal{C}$ be an $(n,M,2\delta)$ code of constant weight $w \leq n/2$, having distance distribution $(A_0, \cdots, A_{2w})$. Then the quantities $B_0, \cdots, B_{2w}$ are nonnegative, where now

$$B_{2k} = \frac{1}{M} \sum_{i=0}^{w} A_{2i} Q_k(i,n,w), \qquad k = 0, \cdots, w,$$

the coefficients $Q_k(i,n,w)$ are given by

$$Q_k(i,n,w) = \frac{n-2k+1}{n-k+1} E_i(k) \binom{n}{k} / \binom{w}{i} \binom{n-w}{i}, \tag{11}$$

and $E_i(x)$ is an Eberlein (or dual Hahn) polynomial defined by

$$E_i(x) = \sum_{j=0}^{i} (-1)^{i-j} \binom{w-j}{i-j} \binom{w-x}{j} \binom{n-w+j-x}{j}.$$

(See Delsarte [9], Eberlein [15], Hahn [23], and Karlin and McGregor [37] for these polynomials.)

As in the case of $A(n,d)$, we obtain a bound on $A(n,d,w)$ by maximizing $A_0 + A_2 + \cdots + A_{2w}$ subject to the constraints

$$A_{2i} \geq 0, \qquad i = \delta, \cdots, w,$$

$$A_0 = 1, A_2 = A_4 = \cdots = A_{2\delta-2} = 0, \tag{12}$$

and

$$B_{2k} \geq 0, \qquad k = 0, \cdots, w. \tag{13}$$

Additional constraints on the A_i can be expressed in terms of the function $T(w_1,n_1,w_2,n_2,2\delta)$ defined in Section I (see Table III). Let $u \in \mathcal{C}$ and consider the codewords $v \in \mathcal{C}$ such that $\text{dist}(u,v) = 2i$. By a suitable permutation of the coordinates, we may assume that

$$\begin{array}{lcccc} & \longleftarrow w \longrightarrow & & \longleftarrow n-w \longrightarrow & \\ u = (11\cdots1 & 11\cdots1 & 00\cdots0 & 00\cdots0), \\ v = (11\cdots1 & 00\cdots0 & 11\cdots1 & 00\cdots0). \\ & \leftarrow i \rightarrow & \leftarrow i \rightarrow & \end{array}$$

The number of such v's is $A_{2i}(u)$, and by definition of T we have

$$A_{2i}(u) \leq T(i,w,i,n-w,2\delta), \qquad i = \delta, \cdots, w,$$

so that

$$A_{2i} \leq T(i,w,i,n-w,2\delta), \qquad i = \delta, \cdots, w. \tag{14}$$

Sometimes it is possible to say more, as the following example illustrates.

Theorem 22:

$$A(17,8,7) \le 31.$$

Proof: Let $\mathcal{C}$ be a code of length 17, distance 8, and constant weight 7. Suppose $\mathcal{C}$ contains $M = A(17,8,7)$ codewords. For $u \in \mathcal{C}$, the only nonzero components of the weight distribution with respect to u are $A_0(u) = 1$, $A_8(u)$, $A_{10}(u)$, $A_{12}(u)$, $A_{14}(u)$, and then

$$A_i = \frac{1}{M}\sum_{u\in\mathcal{C}} A_i(u), \qquad i = 0, 8, 10, 12, 14.$$

We have

$$A_{14}(u) \le A(10,8,7) = A(10,8,1) = 1,$$

$$A_{12}(u) \le T(6,7,6,10,8) = T(1,7,4,10,8) = 5.$$

These imply $A_{12} \le 5$, $A_{14} \le 1$ as in (14). But we can say more. For if $A_{14}(u) = 1$, then $A_{12}(u) \le 2$. Therefore, for all $u \in \mathcal{C}$,

$$A_{12}(u) + 3A_{14}(u) \le 5 \text{ and } A_{14}(u) \le 1,$$

and so

$$A_{12} + 3A_{14} \le 5 \text{ and } A_{14} \le 1. \tag{15}$$

Linear programming with the constraints (12), (13), and (15) gives the stated result. Q.E.D.

Table II gives the bounds on $A(n,d,w)$. Upper bounds marked with an L are obtained by linear programming, as illustrated by Theorem 22. Unmarked lower and upper bounds are from Theorems 14–20. A useful technique for getting lower bounds is the following. Let $\mathcal{C}$ be an (n,M,d) code, and $\mathcal{C}^* = a + \mathcal{C} = \{a + u, u \in \mathcal{C}\}$ any translate of $\mathcal{C}$, with weight distribution $A_i(O)$. Then

$$A_i(O) \le A(n,d,i).$$

This technique works well for example with the (shortened) Nordstrom–Robinson and Golay codes. Other entries in the table are explained by the key. Letters on the left of an entry refer to lower bounds, on the right to upper bounds.

V. Bounds on $T(w_1,n_1,w_2,n_2,d)$

$T(w_1,n_1,w_2,n_2,d)$ is the maximum number of binary vectors of length $n_1 + n_2$, having mutual Hamming distance of at least d, where each vector has exactly w_1 ones in the first n_1 coordinates and exactly w_2 ones in the last n_2 coordinates. For example, we see that $T(1,3,2,4,6) = 2$, as illustrated by the vectors (1001100), (0100011). Properties of this function are given in the following theorems.

Theorem 23: (Johnson [34]).

(a) $T(w_1,n_1,w_2,n_2,d) = T(w_2,n_2,w_1,n_1,d)$,

(b) $T(w_1,n_1,w_2,n_2,d) = T(n_1 - w_1,n_1,w_2,n_2,d)$,

(c) $T(0,n_1,w_2,n_2,d) = A(n_2,d,w_2)$,

(d) $T(w_1,n_1,w_2,n_2,d) \le A(n_2,d - 2w_1,w_2)$,

(e) If $d = 2w_1 + 2w_2$, then

$$T(w_1,n_1,w_2,n_2,d) = \min\left\{\left[\frac{n_1}{w_1}\right], \left[\frac{n_2}{w_2}\right]\right\},$$

(f) $T(w_1,n_1,w_2,n_2,d)$

$$\le \left[\frac{n_1}{w_1} T(w_1 - 1,n_1 - 1,w_2,n_2,d)\right],$$

(g) $T(w_1,n_1,w_2,n_2,d)$

$$\le \left[\frac{n_1}{n_1 - w_1} T(w_1,n_1 - 1,w_2,n_2,d)\right],$$

(h) $T(w_1,n_1,w_2,n_2,2\delta) \le \left[\dfrac{\delta}{\dfrac{w_1^2}{n_1} + \dfrac{w_2^2}{n_2} + \delta - w_1 - w_2}\right]$,

provided the denominator is positive.

A slightly stronger result than Theorem 23(h) is the following.

Theorem 24: Suppose $T(w_1,n_1,w_2,n_2,2\delta) = M$, and define q_i,r_i $(i = 1,2)$ by

$$Mw_i = q_i n_i + r_i, \qquad 0 \le r_i < n_i.$$

Then

$$\sum_{i=1}^{2} \{n_i q_i(q_i - 1) + 2q_i r_i\} \le (w_1 + w_2 - \delta)M(M - 1),$$

with equality if and only if all distances are 2δ.

There is also a linear programming bound for $T(w_1,n_1,w_2,n_2,2\delta)$, based on Theorem 25. Define the *left* and *right weights* of a vector $u = (u_1, \cdots, u_{n_1+n_2})$ to be $w_L(u) = wt(u_1, \cdots, u_{n_1})$ and $w_R(u) = wt(u_{n_1+1}, \cdots, u_{n_2})$.

Theorem 25: Let $\mathcal{C}$ be an $(n_1 + n_2, M, 2\delta)$ code such that $w_L(u) = w_1$, $w_R(u) = w_2$ for all $u \in \mathcal{C}$, and let

$$A_{2i,2j}(u) = |\{v \in \mathcal{C}: w_L(u + v) = 2i, w_R(u + v) = 2j\}|,$$

$$A_{2i,2j} = \frac{1}{M}\sum_{u\in\mathcal{C}} A_{2i,2j}(u).$$

Then

$$B_{2k,2l} = \frac{1}{M}\sum_{i=0}^{w_1}\sum_{j=0}^{w_2} A_{2i,2j} Q_k(i,n_1,w_1) Q_l(j,n_2,w_2) \ge 0,$$

where $Q_k(i,n,w)$ is given in (11).

Proof: For $\nu = 1,2$, suppose $(X^{(\nu)}; R_0^{(\nu)}, \cdots, R_{n_\nu}^{(\nu)})$ is an association scheme with intersection numbers $p_{ijk}^{(\nu)}$, incidence matrices $D_i^{(\nu)}$, idempotents $J_i^{(\nu)}$, and eigenvalues $P_k^{(\nu)}(i)$, $Q_k^{(\nu)}(i)$ (cf. Delsarte [9], [10], Sloane [54]). Then $(X^{(1)} \times X^{(2)}; R_{ij} = R_1^{(1)} \times R_j^{(2)}, 0 \le i \le n_1, 0 \le j \le n_2)$ is an association scheme (the *product* scheme) with intersection numbers $p_{ikr}^{(1)} p_{jls}^{(2)}$, incidence matrices $D_i^{(1)} \otimes D_j^{(2)}$, idempotents $J_i^{(1)} \otimes J_j^{(2)}$, and eigenvalues $P_k^{(1)}(i)P_l^{(2)}(j)$, $Q_k^{(1)}(i)Q_l^{(2)}(j)$. Hence $\mathcal{C}$ is a code in the product of two

Johnson schemes. The result now follows from Theorem 3.3 of Delsarte [9] and Theorem 21 above. Q.E.D.

Table III gives upper bounds on $T(w_1,n_1,w_2,n_2,10)$. Entries marked with an asterisk (*) are exact.

Note Added in Proof: The first author has recently shown that $A(9,3) = 40$, $A(10,3) \leq 79$, $A(11,3) \leq 158$, $A(18,3) \geq 10\,240$, $A(19,3) \geq 20\,480$, $A(20,9) \leq 54$, and $A(21,9) \leq 89$.

REFERENCES

[1] W. O. Alltop, personal communication.
[2] M. R. Best, "The Wax bound for binary codes," Math. Centre Report ZW72, Amsterdam, 1976, (Preprint of Section III of this paper.)
[3] M. R. Best, and A. E. Brouwer, "The triply shortened binary Hamming code is optimal," *Discrete Math.*, vol. 17, pp. 235–245, 1977.
[4] A. E. Brouwer, "$A(17,6,4) = 20$, or the nonexistence of the scarce design SD(4,1;17,21)," Math. Centre Report ZW62, Amsterdam, 1975.
[5] ——, "Optimal packings of K_4's into a K_n—the case $n \not\equiv 2 \pmod 3$)," Math. Centre Report ZW76, Amsterdam, 1976.
[6] ——, "Some triplewise balanced designs," Math. Centre Report ZW77, Amsterdam, 1976.
[7] A. E. Brouwer and A. Schrijver, "A group-divisible design GD(4,1,2;n) exists if $n \equiv 2 \pmod 6$, $n \neq 8$ (or: 'The packing of cocktail party graphs with K_4's')," Math. Centre Report ZW64, Amsterdam, 1976.
[8] P. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Research Reports*, vol. 27, pp. 272–289, 1972.
[9] ——, "An algebraic approach to the association schemes of coding theory," *Philips Research Reports Supplements*, no. 10, 1973.
[10] ——, "The association schemes of coding theory," in *Combinatorics*, M. Hall, Jr., and J. H. van Lint, Eds. Amsterdam: Reidel, Dordrecht, and Mathematical Centre, 1975, pp. 143–161.
[11] ——, "Properties and applications of the recurrence $F(i+1,k+1,n+1) = q^{k+1}F(i,k+1,n) - q^kF(i,k,n)$," *SIAM J. Appl. Math.*, vol. 31, pp. 262–270, 1976.
[12] P. Delsarte, W. Haemers, and C. Weug, unpublished tables, 1974.
[13] R. H. F. Denniston, personal communication.
[14] J. Doyen and A. Rosa, "A bibliography and survey of Steiner systems," *Bolletino Unione Matematica Italiana*, vol. 7, pp. 392–419, 1973.
[15] P. J. Eberlein, "A two parameter test matrix," *Math. Comp.*, vol. 18, pp. 296–298, 1964.
[16] B. Elspas, "A conjecture on binary nongroup codes," *IEEE Trans. Inform. Theory*, vol. IT-11, pp. 599–600, Oct. 1965.
[17] P. Erdos, and H. Hanani, "On a limit theorem in combinatorical analysis," *Publ. Math. Debrecen*, vol. 10, pp. 10–13, 1963.
[17a] W. Feller, *An Introduction to Probability Theory and its Applications*, vol. 1, 2nd Ed. New York: Wiley, 1960.
[18] F. A. Ficken, *The Simplex Method of Linear Programming.* New York: Holt, Rinehart and Winston, 1961.
[19] J. M. Goethals, "The extended Nadler code is unique," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 132–135, Jan. 1977.
[20] M. J. E. Golay, "Notes on digital coding," *Proc. IRE*, vol. 37, p. 657, June 1949.
[21] ——, "Binary Coding," *IEEE Trans. Inform. Theory*, vol. IT-4, pp. 23–28, Sept. 1954.
[22] R. K. Guy, "A problem of Zarankiewicz," in *Theory of Graphs* (Proc. Colloq., Tihany). New York: Academic, 1968, pp. 119–150.
[23] W. Hahn, "Über Orthogonalpolynome, die q-Differenzengleichungen genügen," *Math. Nachr.*, vol. 2, pp. 4–34, 1949.
[24] R. W. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.*, vol. 29, pp. 147–160, Apr. 1950.
[25] H. Hanani, "On quadruple systems," *Canad. J. Math.*, vol. 12, pp. 145–157, 1960.
[26] ——, "The existence and construction of balanced incomplete block designs," *Annals Math. Stat.*, vol. 32, pp. 361–386, 1961.
[27] ——, "A balanced incomplete block design," *ibid.*, vol. 36, p. 711, 1965.
[28] ——, "Balanced incomplete block designs and related designs," *Discrete Math.*, vol. 11, pp. 255–369, 1975.
[29] H. J. Helgert, and R. D. Stinaff, "Minimum-distance bounds for binary linear codes," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 344–356, May 1973.
[30] S. M. Johnson, "A new upper bound for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, Apr. 1962.
[31] ——, "Improved asymptotic bounds for error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-9, pp. 198–205, July 1963.
[32] ——, unpublished tables, 1970.
[33] ——, "On upper bounds for unrestricted binary error-correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-17, pp. 466–478, July 1971.
[34] ——, "Upper bounds for constant weight error-correcting codes," *Discrete Math.*, vol. 3, pp. 109–124, 1972.
[35] D. Julin, "Two improved block codes," *IEEE Trans. Inform. Theory*, vol. IT-11, p. 459, July 1965.
[36] J. G. Kalbfleisch, and R. G. Stanton, "Maximal and minimal coverings of $(k-1)$-tuples by k-tuples," *Pacific J. Math.*, vol. 26, pp. 131–140, 1968.
[37] S. Karlin and J. L. McGregor, "The Hahn polynomials, formulas and an application," *Scripta Math.*, vol. 26, pp. 33–46, 1961.
[38] T. P. Kirkman, "On a problem in combinations," *Cambridge and Dublin Math. J.*, vol. 2, pp. 191–204, 1847.
[39] V. I. Levenshtein, "The application of Hadamard matrices to a problem in coding," *Problems of Cybernetics*, vol. 5, pp. 166–184, 1964.
[40] Shen Lin, personal communication.
[41] J. H. van Lint, "A new description of the Nadler code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 825–826, Nov. 1972.
[42] R. J. McEliece, E. R. Rodemich, H. C. Rumsey, Jr., and L. R. Welch, unpublished tables, 1972.
[43] ——, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 157–166, Mar. 1977.
[44] N. S. Mendelsohn and S. H. Y. Hung, "On the Steiner systems $S(3,4,14)$ and $S(4,5,15)$," *Notices Amer. Math. Soc.*, vol. 18, pp. 552–553, 1971; Abstract 71T-A78 and p. 792: erratum, and *Utilitas Math.*, vol. 1, pp. 5–95, 1972.
[45] M. Nadler, "A 32-point $n = 12$, $d = 5$ code," *IEEE Trans. Inform. Theory*, vol. IT-8, p. 58, Jan. 1962.
[46] A. W. Nordstrom and J. P. Robinson, "An optimum nonlinear code," *Info. Control*, vol. 11, pp. 613–616, 1967.
[47] H. R. Phinney, personal communication.
[48] M. Plotkin, "Binary codes with specified minimum distances," *IEEE Trans. Inform. Theory*, vol. IT-6, pp. 445–450, Sept. 1960.
[49] R. A. Rankin, "On the closest packing of spheres in n dimensions," *Annals of Math.*, vol. 48, pp. 1062–1081, 1947.
[50] C. A. Rogers, *Packing and Covering.* Cambridge: Cambridge University Press, 1964.
[51] J. Schönheim, "On maximal systems of k-tuples," *Stud. Sci. Math. Hungar.*, vol. 1, pp. 363–368, 1966.
[52] M. Simonnard, *Linear Programming.* Englewood Cliffs, NJ: Prentice-Hall, 1966.
[53] N. J. A. Sloane, "A survey of constructive coding theory, and a table of binary codes of highest known rate," *Discrete Math.*, vol. 3, pp. 265–294, 1972.
[54] ——, "An introduction to association schemes and coding theory," in *Theory and Application of Special Functions*, R. Askey, Ed. New York: Academic, 1975, pp. 225–260.
[55] N. J. A. Sloane, S. M. Reddy, and C. L. Chen, "New binary codes," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 503–510, July 1972.
[56] N. J. A. Sloane and J. J. Seidel, "A new family of nonlinear codes obtained from conference matrices," *Annals New York Acad. of Sciences*, vol. 175, pp. 363–365, 1970.
[57] N. J. A. Sloane and D. S. Whitehead, "A new family of single-error correcting codes," *IEEE Trans. Inform. Theory*, vol. IT-16, pp. 717–719, Nov. 1970.
[57a] D. M. Y. Sommerville, *An Introduction to the Geometry of N Dimensions.* New York: Dover, 1958.
[58] J. Spencer, "Maximal consistent families of triples," *J. Combinatorial Theory*, vol. 5, pp. 1–8, 1968.
[59] R. G. Stanton, J. G. Kalbfleisch, and R. C. Mullin, "Covering and packing designs," in *Proc. 2nd Chapel Hill Conf. Combinatorial Mathematics and its Applications*, R. C. Bose *et al.*, Eds., Chapel Hill, NC, 1970, pp. 428–450.

[60] R. F. Stevens and W. G. Bouricius, "The heuristic generation of large error-correcting codes," unpublished memorandum, IBM Research Center, Yorktown Heights, Aug. 1, 1959.
[60a] D. Stinson, "Determination of a Packing Number," preprint.
[61] J. C. Swift, "Quasi-Steiner systems," *Atti Acad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* (8), vol. 44, pp. 40–44, 1968.
[62] W. G. Valiant, "$A(14,6,7) < 52$ or the nonexistence of a certain constant weight code," Math. Centre Report ZW71, Amsterdam, 1976.
[63] N. Wax, "On upper bounds for error detecting and error-correcting codes of finite length," *IEEE Trans. Inform. Theory*, vol. IT-5, pp. 168–174, 1959.
[64] R. M. Wilson, "The construction of group-divisible designs and partial planes having the maximum number of lines of a given size," in *Proc. 2nd Chapel Hill Conf. Combinatorial Mathematics and its Applications*, R. C. Bose *et al.*, Eds., Chapel Hill, NC, 1970, pp. 488–497.
[65] ——, "An existence theory for pairwise balanced designs, I," *J. Combinatorial Theory* vol. 13A, pp. 220–245, 1972; "II," *ibid.*, vol. 13A, pp. 246–273, 1972; "III," *ibid.*, vol. 18A, pp. 71–79, 1975.
[66] E. Witt, "Über Steinersche Systeme," *Abh. Math. Sem. Univ. Hamburg*, vol. 12, pp. 265–275, 1938.

Some Results on Arithmetic Codes of Composite Length

TAI-YANG HWANG AND CARLOS R. P. HARTMANN, MEMBER, IEEE

***Abstract*—A new upper bound on the minimum distance of binary cyclic arithmetic codes of composite length is derived. New classes of binary cyclic arithmetic codes of composite length are introduced. The error correction capability of these codes is discussed, and in some cases the actual minimum distance is found. Decoding algorithms based on majority-logic decision are proposed for these codes.**

I. Introduction

ARITHMETIC CODES, first proposed by Diamond [1], are useful for error control in digital computation as well as in data transmission. They are particularly suitable for checking or correcting errors in arithmetic processors. Finding the minimum distance d of an arithmetic code is a major problem. Despite many similarities between cyclic arithmetic and cyclic block codes, no general lower bound analogous to the BCH bound for cyclic codes has been found for arithmetic codes. Thus in general, the determination of d still relies on a computer search. The search for a systematic way of constructing arithmetic codes is another major area of research. Three known classes of arithmetic codes are the high-rate perfect single-error correcting codes [2]–[4], the large-distance low-rate Mandelbaum–Barrows codes [5], [6], and the intermediate-rate intermediate-distance codes [7]. One of the interesting features of the codes introduced in [7] is that they can be decoded using majority-logic decisions.

In this paper, we present a new upper bound on d for binary cyclic arithmetic codes of composite length. This bound is quite tight and gives a rather good estimation of the actual minimum distance. We also construct new classes of binary cyclic arithmetic codes. Many of these codes have intermediate rate and intermediate distance, and they can be decoded by majority-logic decisions.

Manuscript received November 3, 1976; revised April 25, 1977. This work was supported by the National Science Foundation, under Grant ENG75-07709.

The authors are with School of Computer and Information Science, Syracuse University, Syracuse, NY 13210.

In Section II, we present the new upper bound on d. In Section III, we construct new classes of binary cyclic arithmetic codes. The decoding algorithms for these codes are given in Section IV. A discussion of the results is contained in Section V. Numerical examples are given in Appendix A. The conditions for the existence of codes in the classes constructed in Section III are given in Appendix B.

II. Bound on the Minimum Distance of Binary Cyclic Arithmetic Codes of Composite Length

A binary cyclic arithmetic code (or "AN code") of length n is of the set of integers of the form AN, where A is a fixed integer, called the generator of the code, and $N = 0,1,\cdots,B-1$. The integer B is chosen so that $AB = 2^n - 1$, where n is the multiplicative order of 2 modulo A. For a general background on binary cyclic AN code as well as for the definitions of arithmetic distance and arithmetic weight, the readers are referred to [8]–[10].

The following theorem, which is a generalization of [11, Theorem 1], gives an upper bound on d.

Theorem 1: Let A generate a binary arithmetic code of composite length $n = n_1 l_1$, $1 < l_1 < n$. If B is divisible by either $2^{n_1} + 1$ or by $2^{n_1} - 1$, then $d \le l_1$.

Proof: Let $B = B_1(2^{n_1} + 1)$. By [12, Lemma 6.3], l_1 is even. Thus

$$AB_1 = \frac{2^n - 1}{2^{n_1} + 1} = 2^{(l_1-1)n_1} - 2^{(l_1-2)n_1} + - \cdots + 2^{n_1} - 1$$

is a codeword of arithmetic weight l_1, $W(AB_1) = l_1$. Similarly, one can show that $d \le l_1$ when $B = B_2(2^{n_1} - 1)$. Q.E.D.

The following example will illustrate the application of Theorem 1.

Example 1: Let $AB = 2^{20} - 1$ with $A = 5 \cdot 31 \cdot 41$. Thus, $B = 3 \cdot 5 \cdot 11$ and $n = 20$. We note that $\mathrm{GCD}(A, 2^2 - 1) =$

0018-9448/78/0100-0093$00.75