Lower Bounds for Constant Weight Codes

R. L. GRAHAM AND N. J. A. SLOANE, FELLOW, IEEE

Abstract—Let $A(n,2\delta,w)$ denote the maximum number of codewords in any binary code of length n, constant weight w, and Hamming distance 2δ. Several lower bounds for $A(n,2\delta,w)$ are given. For w and δ fixed, $A(n,2\delta,w) \gtrsim n^{w-\delta+1}/w!$ and $A(n,4,w) \sim n^{w-1}/w!$ as $n \to \infty$. In most cases these are better than the "Gilbert bound." Revised tables of $A(n,2\delta,w)$ are given in the range $n<24$ and $\delta<5$.

I. Lower Bounds for $A(n,4,w)$

Theorem 1:

$$A(n,4,w) \geq \frac{1}{n}\binom{n}{w}.$$

Proof: Let $\mathbb{F}_w^n$ denote the set of $\binom{n}{w}$ binary vectors of length n and weight w, and let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ denote the residue classes modulo n. Consider the map

$$T\colon \mathbb{F}_w^n \to \mathbb{Z}_n$$

Manuscript received February 20, 1979; revised August 22, 1979.
The authors are with Bell Laboratories, Inc., Murray Hill, NJ 07974.

whose value at $\boldsymbol{a} = (a_0, \cdots, a_{n-1}) \in \mathbb{F}_w^n$ is

$$T(\boldsymbol{a}) = \sum_{a_i=1} i \pmod n$$
$$= \sum_{i=0}^{n-1} i a_i \pmod n. \tag{1}$$

For $0 \leq i \leq n-1$ let C_i be the constant weight code $T^{-1}(i)$. We claim that the Hamming distance between any two distinct codewords of C_i, say $\boldsymbol{a}$ and $\boldsymbol{b}$, is at least four. For suppose it is two. Since $\boldsymbol{a}$ and $\boldsymbol{b}$ have weight w this means that $\boldsymbol{a}$ and $\boldsymbol{b}$ agree everywhere except for two positions, one (say the rth) where $\boldsymbol{a}$ is one and $\boldsymbol{b}$ is zero and another (say the sth) where $\boldsymbol{a}$ is zero and $\boldsymbol{b}$ is one. But $T(\boldsymbol{a}) = T(\boldsymbol{b}) = i$, so from (1)

$$T(\boldsymbol{a}) = x + r = i \pmod n,$$
$$T(\boldsymbol{b}) = x + s = i \pmod n$$

for some $x \in \mathbb{Z}_n$. This implies $r \equiv s \pmod n$, which is impossible. Thus C_i has a Hamming distance of at least four between its codewords. Also

$$|C_0|+|C_1|+\cdots+|C_{n-1}|=\binom{n}{w},$$

so, for at least one j,

$$|C_j|\geq\frac{1}{n}\binom{n}{w}.$$

This completes the proof of Theorem 1.

Corollary 2: Let C_i be as defined in the proof of Theorem 1. Then

$$A(n,4,w)\geq\max_{0\leq i\leq n-1}|C_i|.$$

This is stronger (though less informative). For example, Theorem 1 gives $A(14,4,6)\geq 215$ while Corollary 2 gives $A(14,4,6)\geq 217$ (see Table I).

Remarks

1) This paper was prompted by our seeing B. Bose and T. R. N. Rao's report [1] on unidirectional codes, where (among other things) it is proved that $A(n,4,w)\geq(n+1)^{-1}\binom{n}{w}$. Our proof of Theorem 1 is almost identical to their proof.

2) Other bounds on $A(n,2\delta,w)$ may be found in S. M. Johnson [2] and in [3] and in the references given in these papers. In particular Johnson showed that

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

which implies

$$A(n,2\delta,w)\lesssim\frac{(\delta-1)!\,n^{w-\delta+1}}{w!}\qquad(2)$$

as $n\to\infty$. For $\delta=2$ this reads

$$A(n,4,w)\lesssim\frac{n^{w-1}}{w!}.$$

Combining this with Theorem 1 we have Theorem 3.

Theorem 3:

$$A(n,4,w)\sim\frac{n^{w-1}}{w!}$$

for w fixed, as $n\to\infty$.

II. Lower Bounds on $A(n,2\delta,w)$ Based on $GF(q)^{\delta-1}$

Theorem 4: Let q be a prime power such that $q\geq n$. Then

$$A(n,2\delta,w)\geq\frac{1}{q^{\delta-1}}\binom{n}{w}.$$

Proof: Let $q\geq n$ be a prime power, and let the elements of GF(q) be labeled $\omega_0,\omega_1,\cdots,\omega_{q-1}$. Define a map

$$T:\ \mathbb{F}_w^n\to\mathrm{GF}(q)^{\delta-1}$$

by

$$T(\boldsymbol{a})=\begin{bmatrix}T_1(\boldsymbol{a})\\T_2(\boldsymbol{a})\\\vdots\\T_{\delta-1}(\boldsymbol{a})\end{bmatrix},$$

where

$$T_1(\boldsymbol{a})=\sum_{a_i=1}\omega_i,$$

$$T_2(\boldsymbol{a})=\sum_{\substack{i<j\\a_i=a_j=1}}\omega_i\omega_j,$$

$$T_3(\boldsymbol{a})=\sum_{\substack{i<j<k\\a_i=a_j=a_k=1}}\omega_i\omega_j\omega_k,$$

$$\cdots$$

For each $(\delta-1)$-tuple

$$\boldsymbol{v}=\begin{bmatrix}v_1\\v_2\\\vdots\\v_{\delta-1}\end{bmatrix}\in\mathrm{GF}(q)^{\delta-1},$$

let $C_{\boldsymbol{v}}=T^{-1}(\boldsymbol{v})$. Then for some $\boldsymbol{v}$

$$|C_{\boldsymbol{v}}|\geq\frac{1}{q^{\delta-1}}\binom{n}{w}.$$

It remains to show that $C_{\boldsymbol{v}}$ has a Hamming distance of 2δ. Suppose on the contrary that there are vectors $\boldsymbol{a},\boldsymbol{b}\in C_{\boldsymbol{v}}$ with distance $(\boldsymbol{a},\boldsymbol{b})=2\gamma\leq 2\delta-2$. This means that there are 2γ distinct coordinates $r_1,\cdots,r_\gamma,s_1,\cdots,s_\gamma$ such that

$$\begin{array}{rl} & \quad\ \ r_1\ r_2\ \ \ r_\gamma\qquad s_1\ s_2\ \ \ s_\gamma\\ \boldsymbol{a}= & \cdots\ 1\ 1\ 1\ 1\ \cdots\ 0\ 0\ 0\ 0\ \cdots,\\ \boldsymbol{b}= & \cdots\ 0\ 0\ 0\ 0\ \cdots\ 1\ 1\ 1\ 1\ \cdots,\end{array}$$

and $\boldsymbol{a}$ and $\boldsymbol{b}$ agree in all other coordinates. Write $\alpha_i=\omega_{r_i}$, $\beta_i=\omega_{s_i}$ $(1\leq i\leq\gamma)$. Since $T(\boldsymbol{a})=T(\boldsymbol{b})$ the elementary symmetric functions of the α_i and β_i agree:

$$\sigma_1=\sum_i\alpha_i=\sum_i\beta_i,$$

$$\sigma_2=\sum_{i<j}\alpha_i\alpha_j=\sum_{i<j}\beta_i\beta_j,$$

$$\cdots$$

$$\sigma_{\delta-1}=\sum_{i_1<\cdots<i_{\delta-1}}\alpha_{i_1}\cdots\alpha_{i_{\delta-1}}=\sum_{i_1<\cdots<i_{\delta-1}}\beta_{i_1}\cdots\beta_{i_{\delta-1}}.$$

Therefore $\alpha_1,\cdots,\alpha_\gamma,\beta_1,\cdots,\beta_\gamma$ are 2γ distinct zeros of the polynomial

$$x^\gamma-\sigma_1x^{\gamma-1}+\sigma_2x^{\gamma-2}-\cdots\pm\sigma_\gamma.$$

But a polynomial of degree γ over a field has at most γ zeros. This contradiction completes the proof of Theorem 4.

Again we can strengthen this result.

Corollary 5: Let q be a prime power such that $q\geq n$.

Then

$$A(n,2\delta,w) \geq \max_{v \in GF(q)^{\delta-1}} |C_v|.$$

Remarks

1) For any ϵ there is an $n_0(\epsilon)$ such that for all $n > n_0(\epsilon)$ there is a prime in the interval $(n,(1+\epsilon)n)$ [4, p. 88]. Thus in Theorem 4, q need never be much greater than n and combining this with (2) we have Theorem 6.

Theorem 6:

$$\frac{n^{w-\delta+1}}{w!} \lesssim A(n,2\delta,w) \lesssim \frac{(\delta-1)!\,n^{w-\delta+1}}{w!}$$

for w fixed, as $n \to \infty$.

2) As A. M. Odlyzko has observed, the standard argument used to prove the Gilbert bound for codes (see Berlekamp [5, Theorem 13.71]) when applied to constant weight codes yields Theorem 7.

Theorem 7 (The "Gilbert Bound"):

$$A(n,2\delta,w) \geq \frac{\binom{n}{w}}{\sum_{i=0}^{\delta-1} \binom{w}{i}\binom{n-w}{i}},$$

and so as $n \to \infty$

$$A(n,2\delta,w) \gtrsim \frac{(\delta-1)!\,n^{w-\delta+1}}{w!\binom{w}{\delta-1}}.$$

For small w this is sometimes better than the lower bounds of Theorems 4, 6, and 11. For example when n is large Theorem 7 is stronger than the lower bound of Theorem 6 if w is such that

$$\binom{w}{\delta-1} < (\delta-1)!,$$

but for larger values of w the new bounds are better than the "Gilbert bound."

3) For large n the best upper and lower bounds on $A(n,2\delta,w)$ differ by a factor of

$$\min\left\{(\delta-1)!,\binom{w}{\delta-1}\right\}.$$

In at least one case it is known that the upper bound is correct. From the work of H. Hanani, A. E. Brouwer, and A. Schrijver (the references are given in [3]) it follows that

$$A(n,6,4) \sim \frac{n^2}{12}.$$

III. Lower Bounds on $A(n,2\delta,w)$ Using Sets with Distinct Sums

A subset $S = \{s_1, \cdots, s_n\}$ of $\mathbb{Z}_m$ is called an *S_t-set of size n and modulus m* if all the sums

$$s_{i_1} + s_{i_2} + \cdots + s_{i_t} \tag{3}$$

for $i_1 < i_2 < \cdots < i_t$ are distinct in $\mathbb{Z}_m$.

Provided $t < (n+1)/2$, an S_t-set is automatically an S_u-set for $u < t$. Since there are $\binom{n}{t}$ sums (3), we must have

$$m \geq \binom{n}{t}. \tag{4}$$

The set $\{0,1,2,4\}$ is an example of an S_2-set of size 4 and modulus $m = 6 = \binom{4}{2}$. It can be shown that no S_2-set of size n and modulus $\binom{n}{2}$ exists for $n > 4$; this and other properties of S_2-sets will appear in a companion paper [6].

A perfect difference set is also an S_2-set, for if the *differences* $s_i - s_j$ are distinct then so are the *sums* $s_i + s_j$, but the converse is not true, as the above example shows. The following construction was given by R. C. Bose and S. Chowla [7] in 1962 and generalizes the construction of a Singer perfect difference set (see for example [4, p. 83]).

Theorem 8 (Bose and Chowla): For any prime power q there is an S_t-set of size $q+1$ and modulus $m = (q^{t+1}-1)/(q-1)$.

Proof: Let $\pi(x)$ be a primitive irreducible polynomial of degree $t+1$ over GF(q) and let ξ be a zero of $\pi(x)$. Then ξ is a primitive element of GF(q^{t+1}),

$$\xi^{q^{t+1}-1} = 1 \quad \text{and} \quad \xi^m = \alpha,$$

where α is a primitive element of GF(q). Also the elements of GF(q^{t+1}) may be written as

$$\xi^j = b_0^{(j)} + b_1^{(j)}\xi + \cdots + b_t^{(j)}\xi^t, \tag{5}$$

where $b_i^{(j)} \in GF(q)$, for $0 \leq j \leq q^{t+1}-2$ (see [8, ch. 4]). Let S consist of those values of j in the range $0 \leq j < m$ for which the coefficients $b_2^{(j)}, \cdots, b_t^{(j)}$ are zero. Then the products

$$\xi^{j_1}\xi^{j_2}\cdots\xi^{j_t}, \qquad j_1 < j_2 < \cdots < j_t,$$

are distinct elements of GF(q^{m+1}) (since these are the products of t linear factors, the representations of these products in the form (5) are all distinct). Therefore S is an S_t set.

Remark: The other construction of S_t-sets given by Bose and Chowla [7, Theorem 1], [4, p. 81, Theorem 3] leads to a bound on $A(n,2\delta,w)$ which is weaker than Theorem 4.

The connection between S_t-sets and $A(n,2\delta,w)$ is given by the following theorem.

Theorem 9: If there exists an $S_{\delta-1}$-set of size n and modulus m then

$$A(n,2\delta,w) \geq \frac{1}{m}\binom{n}{w}.$$

Proof: The proof is similar to that of Theorems 1 and 4, but using the map

$$T: \mathbb{F}_w^n \to \mathbb{Z}_m$$

given by

$$T(a) = \sum_{a_i=1} s_i \pmod m$$

and the codes $C_i = T^{-1}(i)$.

Corollary 10:

$$A(n,2\delta,w) \geq \max_{0 \leq i \leq m-1} |C_i|.$$

From Theorems 8 and 9 we have Theorem 11.

Theorem 11: Let q be the smallest prime power such that $q+1 \geq n$. Then for $\delta \geq 3$

$$A(n,2\delta,w) \geq \frac{q-1}{q^{\delta}-1}\binom{n}{w}.$$

For some values of n this is stronger than Theorem 4, for others, weaker. Asymptotically they are the same.

IV. Tables

Tables of $A(n,2\delta,w)$ for $n \leq 24$ and $\delta \leq 5$ are given in [3] and [8]. A number of the lower bounds for $\delta=2$ and 3 can now be improved using the above results, and the revised tables are shown in Tables I–IV which appear on the following three pages. The tables for $\delta=4$ and 5 are included for completeness.

Key to Tables

Unmarked entries are copied from [3].

a) From Theorem 1.
b) From Corollary 2.
c) From Corollary 5.
d) From Corollary 10, using an S_2-set of size 24 and modulus 554 obtained from a perfect difference set [9].
e) From translates of the Nordstrom–Robinson code [10].
f) From the weight distribution of a certain code [10].
g) From a Hadamard matrix [10].
h) See Kibler [11].
i) These values were obtained by Colbourn ([12]; also written communication, August 1979) using the bound given by Johnson in [13, (29)]
j) A. E. Brouwer, [15].

We conclude with some addenda to [3]. Brouwer [10] has communicated to us the following improvements to [5, Table IIIA].

$$T(1,3,6,15,10)=6,$$
$$T(1,4,6,15,10)=7,$$
$$T(1,5,6,15,10)=7,$$
$$T(1,6,6,15,10)=7 \qquad \text{(not 8)}.$$

The results mentioned in the Note on page 92 of [3] have appeared in Best [14]. In the fifth line of eq. (5), change 197 to 297. On page 89, in line 2 of Section IVA the words "$D(t,k,v)$ where $v=$" are illegible.

Acknowledgment

The authors would like to thank B. Bose and T. R. N. Rao for sending us a copy of their report [1] and Andrew Odlyzko for some very helpful discussions. The authors also thank A. E. Brouwer, M. J. Colbourn, and R. E. Kibler for sending us improvements to the tables and the referees for their useful comments.

Note Added in Proof

A. E. Brouwer has recently shown that $A(24,10,11) \geq 52$, and P. Delsarte and P. Piret [16] have improved the lower bounds to several values of $A(23,6,w)$ and $A(24,6,w)$.

References

[1] B. Bose and T. R. N. Rao, "On the theory of unidirectional error correcting/detecting codes," Dept. Comp. Sci., Southern Methodist Univ., Dallas, TX, Tech. Rep. CS-7817, Sept. 1978.
[2] S. M. Johnson, "A new upper bound for error-correcting codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 203–207, 1962.
[3] M. R. Best, A. E. Brouwer, F. J. MacWilliams, A. M. Odlyzko and N. J. A. Sloane, "Bounds for binary codes of length less than 25," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 81–93, Jan. 1978.
[4] H. Halberstam and K. F. Roth, *Sequences*, vol. 1. Oxford: Oxford Univ., 1966.
[5] E. R. Berlekamp, *Algebraic Coding Theory*. New York: McGraw-Hill, 1968.
[6] R. L. Graham and N. J. A. Sloane, "On additive bases and harmonious graphs," to be published.
[7] R. C. Bose and S. Chowla, "Theorems in the additive theory of numbers," *Comment. Math. Helvet.* vol. 37, 141–147, 1962–1963.
[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: North-Holland, 1977.
[9] L. D. Baumert, *Cyclic Difference Sets, Lecture Notes in Math*, 182. New York: Springer-Verlag, 1971, p. 151.
[10] A. E. Brouwer, written communication.
[11] R. E. Kibler, "Some new constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, May 1980, to be published.
[12] M. J. Colbourn, "Analytic and computer techniques for set packings," M. S. thesis, Univ. Toronto, Toronto, ON, Canada, esp. p. 149, 1977.
[13] S. M. Johnson, "Upper bounds for constant weight error correcting codes," *Discrete Math.* vol. 3, pp. 109–124, 1972.
[14] M. R. Best, "Binary codes with minimum distance four," Mathematical Centre, Amsterdam, Rep. ZW 112/78, 1978.
[15] A. E. Brouwer, "A few new constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, May 1980, to be published.
[16] P. Delsarte and P. Piret, "On the (23,14,5) Wagner code," *IEEE Trans. Inform. Theory*, to be published.

TABLE I
$A(n,4,w)$

n\w	2	3	4	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	35	66	66	35	17	5	1	1	
12	6	20	51	[j]75-84	132	75-84	51	20	6	1	1
13	6	26	65	[h]118-132	[j]158-182	158-182	118-132	65	26	6	1
14	7	28	91	[j]169-182	[j]275-308	[j]316-364	275-308	169-182	91	28	7
15	7	35	105	[j]222-271	[j]370-455	[j]582-660	582-660	370-455	222-271	105	35
16	8	37	140	305-336	[j]592-722	[a]715-1040	[j]1164-1320	715-1040	592-722	305-336	140
17	8	44	154-157	424-476	[j]840-952	[h]1224-1753	[h]1496-2210	1496-2210	1224-1753	840-952	424-476
18	9	48	198	[j]504-565	[j]1260-1428	[a]1768-2448	[b]2438-3944	[b]2704-4420	2438-3944	1768-2448	1260-1428
19	9	57	228	612-752	[h]1482-1789	[h]2679-3876	[a]3978-5814	[a]4862-8326	4862-8326	3978-5814	2679-3876
20	10	60	285	816-912	2040-2506	[a]3876-5111	[b]6310-9690	[a]8398-12920	[b]9252-16652	8398-12920	6310-9690
21	10	70	315	1071-1197	2856-3192	[a]5538-7518	[a]9690-13416	[b]14000-22610	[a]16796-27132	16796-27132	14000-22610
22	11	73	385	1386	3927-4389	[a]7752-10032	[b]14550-20674	[a]22610-32794	[b]29414-49742	[a]32066-54264	29414-49742
23	11	83	416-419	1771	5313	[a]10659-14421	[a]21318-28842	[a]35530-52833	[a]49742-75426	[a]58786-104006	58786-104006
24	12	88	498	1859-2011	7084	[a]14421-18216	[b]30667-43263	[b]54484-76912	[b]81752-126799	[a]104006-164565	[b]112720-208012

TABLE II
$A(n,6,w)$

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	12	22	12	9	4	1	1	1
13	4	13	18	26	26	18	13	4	1	1
14	4	14	28	42	42-51	42	28	14	4	1
15	5	15	42	70	60-88	60-88	70	42	15	5
16	5	20	48	112	90-156	120-150	90-156	112	48	20
17	5	20	68	112-136	[h]119-240[i]	[h]136-283	136-283	119-240	119-240	68
18	6	22	68-72	144-202	160-349	232-428	249-425	232-428	160-349	144-202
19	6	25	[h]76-33	172-228	228-520	332-734[i]	472-789	472-789	332-734	228-520
20	6	30	[h]84-100	232-276	310-651	492-1107[i]	[e]736-1363	944-1421	736-1363	492-1107
21	7	31	[h]105-126	253-350	465-828	668-1695[i]	1068-2364	1286-2702	1286-2702	1068-2364
22	7	37	132-136	294-462	675-1100	708-2277	1288-3775	1450-4416	1574-5064	1450-4416
23	7	40	147-170	399-521	969-1518	[c]929-3162	[c]1551-5819	[c]2167-7521	[c]2576-7953	2576-7953
24	8	42	168-192	532-680	1368-1786	[d]1341-4554	[d]2379-8432	[d]3560-12186[i]	[d]4530-14682	[d]4903-15906

TABLE III
$A(n,8,w)$

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	10	15	15	10	6	3	1
16	4	6	16	16-22	30	16-22	16	6	4
17	4	7	17	21-31	34-35	34-35	21-31	17	7
18	4	9	20-21	33-41	46-63	48-70	46-63	33-41	20-21
19	4	12	28	52-57	78-97	88-122	88-122	78-97	52-57
20	5	16	40	80	130-142	160-215	176-244	160-215	130-142
21	5	21	56	120	210	280-331	336-399	336-399	280-331
22	5	21	77	176	330	280-493[1]	616-659[1]	672-785[1]	616-659
23	5	23	77-80	253	506	400-801[1]	616-1111	1288-1350[1]	1288-1350
24	6	24	77-92	253-274	759	640-1143[1]	960-1639	1288-2231[1]	2576

TABLE IV
$A(n,10,w)$

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	19	19	12	8
20	4	5	10	17-18	20-24	38	20-24	17-18
21	4	7	13	21-26	21-41	38-49	38-49	21-41
22	4	7	15-19	22-35	22-57	38-74	38-82	38-74
23	4	8	16-23	23-50	23-87	38-117	38-135	38-135
24	4	9	24-27	[h]27-68[h]	23-119	[f]54-171	38-223	[g]46-247