stichting
mathematisch
centrum

MC

DEPARTMENT OF PURE MATHEMATICS ZW 71/76 FEBRUARY

W.G. VALIANT

$A(14,6,7) < 52$ OR THE NONEXISTENCE OF A CERTAIN CONSTANT WEIGHT CODE

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): 05B05, 05B40

A(14,6,7) < 52

or

the nonexistence of a certain constant weight code *)

by

W.G. Valiant

ABSTRACT

We show that a binary constant weight code with word length $n = 14$, minimum distance $d = 6$ and constant weight $w = 7$ cannot have 52 code words (while 52 is the value both of the Johnson bound and of Delsarte's linear programming bound). This means that in any block design with parameters $b = 52$, $v = 14$, $r = 26$, $k = 7$, $\lambda = 12$, there are two blocks that intersect in at least 5 points.

KEY WORDS & PHRASES: *3-design, constant weight code, linear programming bound.*

---

*) This paper is not for review; it is meant for publication elsewhere.

1. THE JOHNSON BOUND

Let $A(n,d,w)$ be the maximum cardinality of a binary constant weight code with word length n, minimum distance d, and constant weight w. Then JOHNSON [2] showed that

$$A(n,d,w) \le \frac{n}{w} A(n-1,d,w-1) \qquad (w > 0),$$

and from the proof it is immediately clear that if equality holds, then the code is a 1-design. More generally

$$A(n,d,w) \le \frac{n}{w} \cdot \frac{n-1}{w-1} \cdot \ldots \cdot \frac{n-t+1}{w-t+1} \cdot A(n-t,d,w-t) \qquad (w \ge t),$$

and if equality holds, then the code is a t-design.

Since $A(12,6,5) = 12$ (cf. [2]) it follows that $A(14,6,7) \le \frac{14}{7} \cdot \frac{13}{6} \cdot 12 = 52$, and if equality holds, then we have a block design with parameters $b = 52$, $v = 14$, $r = 26$, $k = 9$, $\lambda = 12$. Such block designs exist in abundance, but here we have the restriction that the Hamming distance between two blocks must be at least 6, i.e. two blocks may intersect in at most 4 points. We shall see that this is impossible.

2. THE LINEAR PROGRAMMING BOUND

Another upper bound for the cardinality of constant weight codes has been derived by DELSARTE [1]. We copy his formulas: Let

$$v_i = \binom{w}{i}\binom{n-w}{i},$$

$$\mu_i = \binom{n}{i} - \binom{n}{i-1},$$

$$E_k(u) = \sum_{j=0}^{k} (-1)^j \binom{u}{j}\binom{w-u}{k-j}\binom{n-w-u}{k-j},$$

$$Q_i(k) = \mu_i v_k^{-1} E_k(i),$$

and let (a_i) be the inner distribution of a binary constant weight code C with word length n and constant weight w, i.e.

$a_i = |C|^{-1} \cdot |\{(x,y) \in C^2 \mid d_H(x,y) = 2i\}|$.

Then $$\sum_{k=0}^{w} a_k Q_i(k) \geq 0 \qquad \text{for } i = 0,1,\ldots,w \qquad (w \leq \tfrac{1}{2}n).$$

Since $|C| = \sum_{k=0}^{w} a_k$ we have the linear programming bound:

$$|C| \leq \max\{\sum_{k=0}^{w} a_k \mid a_k \geq 0 \ (k=0,\ldots,w),\ a_0 = 1,\ \sum_{k=0}^{w} a_k Q_i(k) \geq 0,$$
$$a_1 = \ldots = a_{\frac{d}{2}-1} = 0\}.$$

In our case ($n = 14$, $w = 7$) the matrix $(Q_i(k))$ is found to be

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
13 & 65/7 & 39/7 & 13/7 & -13/7 & -39/7 & -65/7 & -13 \\
77 & 253/7 & 187/21 & -33/7 & -33/7 & 187/21 & 253/7 & 77 \\
273 & 507/7 & -39/7 & -351/35 & 351/35 & 39/7 & -507/7 & -273 \\
637 & 65 & -91/3 & 39/5 & 39/5 & -91/3 & 65 & 637 \\
1001 & -143/7 & -143/7 & 143/7 & -143/7 & 143/7 & 143/7 & -1001 \\
1001 & -715/7 & 143/7 & -143/35 & -143/35 & 143/7 & -715/7 & 1001 \\
429 & -429/7 & 143/7 & -429/35 & 429/35 & -143/7 & 429/7 & -429
\end{pmatrix}$$

By computer it was found that the unique optimal solution of the linear programming problem is: $\underline{a} = (1\ 0\ 0\ 33\ 8\ 9\ 1\ 0)$, which yields $|C| = 52$. [Note that this solution corresponds to a code which could be a 3-design: 3 -(14,7,5), in a sense the nicest solution possible. Again a 3-design 3 -(14,7,5) does exist, but it contains blocks with too small a distance.]

We do not need the computer result but shall only use the last row of this matrix, which gives the inequality

$$21 - \frac{3}{5}a_3 + \frac{3}{5}a_4 - a_5 + 3a_6 - 21a_7 \geq 0$$

for the inner distribution of any code with $n = 14$, $w = 7$, $d = 6$.

3. BLOCK INTERSECTION NUMBERS

Let C be a constant weight code with $|C| = 52$, $n = 14$, $d = 6$, $w = 7$, and fix a word (block) $x \in C$. Let n_i be the number of blocks $y \in C$ that intersect x in exactly i points.

Since $d = 6$ we have $n_5 = n_6 = 0$, $n_7 = 1$.

Since C is a 2-design we have

$$n_0 + n_1 + n_2 + n_3 + n_4 = b - 1 = 51,$$

$$n_1 + 2n_2 + 3n_3 + 4n_4 = k(r-1) = 175,$$

$$n_2 + 3n_3 + 6n_4 = \binom{k}{2}(\lambda-1) = 231,$$

which yields

$$n_2 = 12 - 6n_0 - 3n_1,$$

$$n_3 = 5 + 8n_0 + 3n_1,$$

$$n_4 = 34 - 3n_0 - n_1.$$

If $n_0 \geq 2$, then there are two blocks y_1 and y_2 disjoint from x; but then $y_1 = y_2$ and $d_H(y_1,y_2) = 0$, which is impossible.

If $n_0 = 1$, then C contains the block y complementary to x; since any block z that intersects x in i points intersects y in $(7-i)$ points, it follows that $n_1 = n_2 = 0$. But this contradicts the equation $n_2 = 12 - 6n_0 - 3n_1$.

Therefore n_0 has to be zero, and we are left with the following five possibilities:

n_0	0	0	0	0	0
n_1	0	1	2	3	4
n_2	12	9	6	3	0
n_3	5	8	11	14	17
n_4	34	33	32	31	30

If $n_1 \geq 2$, then there are two blocks y_1 and y_2 wich both intersect x

in a single point; but then $d_H(y_1,y_2) \le 4$, which is impossible.

If $n_1 = 1$, then there is a block y which intersects x in a single point $p := x \cdot y$; let q be the point not in the union of x and y: $q := := j - x - y + p$, where j is the all-one vector. There are 9 blocks $u_i (1 \le i \le 9)$ intersecting x in two points. Each of them intersects y in four points and contains q but not p.

If n_i' are the block intersection numbers of C defined with y as fixed block, then $n_1' \ge 1$ since $|x \cap y| = 1$; therefore $(n_1',n_2',n_3',n_4') = (1,9,8,33)$, and in particular we find 9 blocks $v_i (1 \le i \le 9)$ intersecting y in two points, x in four points, each containing q but not p.

Next we remember that C is a 2-design with $\lambda = 12$, so the pair $\{p,q\}$ must be contained in 12 blocks $w_i (1 \le i \le 12)$ which have to be different from the blocks x,y,u_i,v_i encountered thus far. But now we have already found $9 + 9 + 12 = 30$ ones at position q, while r is only 26. This gives a contradiction.

Consequently $n_1 = 0$ and the only possibility remaining is given by the first column of the above table. In particular, the n_i are independent of the block x chosen and therefore the inner distribution equals $\underline{a} = (1\ 0\ 0\ 34\ 5\ 12\ 0\ 0)$. But this $\underline{a}$ does not satisfy the inequality given at the end of the previous section. Therefore the assumption that C exists leads to a contradiction, and we have $A(14,6,7) < 52$.

REFERENCES

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

[2] JOHNSON, S.M., *A new upper bound for error-correcting codes*, IRE Trans. Information Theory IT-8 (1962) 203-207.

ADDED IN PROOF

Let $T(n_1,w_1,n_2,w_2,d)$ be the maximum number of code words possible in a binary code of word length $n_1 + n_2$ with minimum distance d, and such that any code word has w_1 ones in its first n_1 positions, and w_2 ones in the remaining n_2 positions. Then (using some obvious inequalities from [3]) we have

$$T(7,2,7,5,6) = T(7,2,7,2,6) \leq \left\lfloor \frac{7}{2} \cdot T(6,1,7,2,6) \right\rfloor = \left\lfloor \frac{7 \cdot 3}{2} \right\rfloor = 10.$$

[In fact one can show that $T(7,2,7,5,6) = 10$.]

This means that for any constant weight code C with $n = 14$, $d = 16$, $w = 7$, the number of blocks (code words) intersecting a given $x \in C$ in exactly two points is at most 10, i.e. $n_2 \leq 10$. This is another way of showing the impossibility of the first column in the table of Section 3.

[3] JOHNSON, S.M., *Upper bounds for constant weight error correcting codes*, Discrete Math. 3 (1972) 109-124.