Six New Constant Weight Binary Codes.

Article *in* Ars Combinatoria -Waterloo then Winnipeg- · April 2003

Source: DBLP

Six New Constant Weight Binary Codes

Hui Kheng Aw
Kimberly-Clark Corporation
2100 Winchester Road
Neenah, Wisconsin 54956
USA

Yeow Meng Chee
12 Jambol Place
Singapore 119339
ym@ymchee.com

Alan C. H. Ling
Department of Computer Science
University of Vermont
Burlington, Vermont 05405
USA

Abstract

We give six improved bounds on $A(n, d, w)$, the maximum cardinality of a binary code of length n with minimum distance d and constant weight w.

1 Introduction

A *binary code* of *length* n is any set $\mathcal{C} \subseteq \{0, 1\}^n$. The elements of $\mathcal{C}$ are called *codewords*. $\mathcal{C}$ is said to have *minimum distance* d and *constant weight* w if the Hamming distance between any two distinct codewords is at least d and $\|\mathbf{u}\|^2 = w$ for all $\mathbf{u} \in \mathcal{C}$. For simplicity, we refer to a binary code of length n, minimum distance d, and constant weight w as an (n, d, w)-*code*. We also assume without loss of generality that d is even. Define $A(n, d, w)$ to be the maximum cardinality of an (n, d, w)-code, that is,

$$A(n, d, w) = \max\{|\mathcal{C}| : \mathcal{C} \text{ is an } (n, d, w){-}\text{code}\}.$$

The function $A(n, d, w)$ is fundamental in the theory of error-correcting codes [2]. Unfortunately, the exact determination of $A(n, d, w)$ is difficult. Most efforts have therefore focused on establishing good bounds for $A(n, d, w)$. The function $A(n, d, w)$ is also widely studied in combinatorial design theory, under the guise of packing designs [3].

In this paper, we give some improved lower bounds on $A(n, d, w)$.

2 Results

2.1 A Cyclic $(30, 8, 5)$-Code

The set of all distinct cyclic shifts of the two vectors

$$100000100000100000100000100000$$

$$110100000001000100000000000000$$

is a $(30, 8, 5)$-code with 36 codewords.

2.2 Length-Reduction Heuristic

We represent a binary code $\mathcal{C}$ by a $\{0, 1\}$-matrix $M(\mathcal{C})$ whose columns are the codewords of $\mathcal{C}$. Let $\mathcal{M}_{n,m}(d, w)$ be the set of all $n \times m$ $\{0, 1\}$-matrices M with constant column sum w, such that the Hamming distance between any two distinct columns $\mathbf{u}$ and $\mathbf{v}$ of M is at least d. So for an (n, d, w)-code $\mathcal{C}$, we have $M(\mathcal{C}) \in \mathcal{M}_{n,|\mathcal{C}|}(d, w)$. For a positive integer i, $M \in \{0, 1\}^{n\times m}$, and $\mathbf{u} \in \{0, 1\}^n$, we denote by $M_i(\mathbf{u})$ the matrix obtained by replacing the ith column of M by $\mathbf{u}$. We also denote by $\tilde{M}$ the matrix obtained from M by deleting its last row.

The `length-reduction` heuristic works as follows. The inputs are n, m, d, and w, where $n \geq w \geq d/2$. We begin with $M \in \mathcal{M}_{N,m}(d, w)$, for some N. At each stage of the heuristic, we generate a random integer i and a random element $\mathbf{u} \in \{0, 1\}^n$ whose last component is zero. If $M_i(\mathbf{u}) \in \mathcal{M}_{n,m}(d, w)$, then we replace M by $M_i(\mathbf{u})$. It could happen at this point that the last row of M is a zero vector. If this is the case, we replace M by $\tilde{M}$, and repeat the process. We stop when M has only n rows.

Let

$$I_{m,w} = \begin{bmatrix} \mathbf{1}_w & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \mathbf{1}_w & \cdots & \mathbf{0} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & \mathbf{1}_w \end{bmatrix},$$

where $\mathbf{1}_w$ is the w-dimensional column vector of all ones. Clearly, $I_{m,w} \in \mathcal{M}_{mw,m}(d,w)$ for any $d \leq 2w$. For our experiments, the initial choice of M is $I_{m,w}$.

`length-reduction` **heuristic**(n, m, d, w)

Step 1: $M = I_{m,w}$ and $N = mw$.

Step 2: Repeat Step 3 to Step 5 until $N = n$.

Step 3: Randomly choose $i \in \{1, 2, \ldots, m\}$ and $\mathbf{u} \in \{0,1\}^N$.

Step 4: If $M_i(\mathbf{u}) \in \mathcal{M}_{N,m}(d,w)$, then $M = M_i(\mathbf{u})$.

Step 5: If the last row of M is the zero vector, then $M = \tilde{M}$ and set $N = N - 1$.

It is easy to see that when the heuristic terminates, we have M as the matrix of an (n,d,w)-code of cardinality m.

Most algorithms and heuristics for constructing constant weight binary codes attempts to pack as many codewords into an (n,d,w)-code as possible, given n, d, and w. Here, the `length-reduction` heuristic takes the alternative approach of minimizing the length n of an (n,d,w)-code, given d, w, and its cardinality.

2.3 New Bounds

The `length-reduction` heuristic has been used to produce five new lower bounds on $A(n,d,w)$.

Theorem 1. $A(18,6,5) \geq 69$, $A(27,8,5) \geq 31$, $A(29,8,5) \geq 34$, $A(33,8,5) \geq 44$ and $A(34,8,5) \geq 47$.

Proof. The matrices in Appendix A represent the necessary (n,d,w)-codes for providing the lower bounds on $A(n,d,w)$. □

3 Conclusion

The following table summarizes the results obtained in this paper.

n	d	w	best lower bound on $A(n,d,w)$ previously known [1, 4, 5]	lower bound on $A(n,d,w)$ obtained in this paper
18	6	5	68	69
27	8	5	30	31
29	8	5	33	34
30	8	5	33	36
33	8	5	43	44
34	8	5	43	47

References

[1] A. E. Brouwer, J. B. Shearer, N. J. A. Sloane, and W. D. Smith, A new table of constant weight codes, *IEEE Trans. Inform. Theory* **36** (1990) 1334–1380.

[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.

[3] W. H. Mills and R. C. Mullin, Coverings and packings, in: *Contemporary Design Theory: A Collection of Surveys* (J. H. Dinitz, D. R. Stinson; eds.) John Wiley & Sons, New York, 1992, 371–399.

[4] E. M. Rains and N. J. A. Sloane, Table of constant weight binary codes, `URL=http://www.research.att.com/~njas/codes/Andw/`.

[5] J. Yin and A. M. Assaf, Constructions of optimal packing designs, *J. Combin. Designs* **6** (1998) 245–260.

Appendix

A Constant Weight Codes

The columns in the following matrices give the codewords for each code.

```
111111111111111111100000000000000000000000000000000000000000000000000
111110000000000000011111111111111000000000000000000000000000000000000
100001111000000000011110000000000111111111100000000000000000000000000
100000000010100000001000000101001001001010010100100000000100110000111 0
10000000000101100100000001001001001010010000101010001000001001100010 00
010001000111000000000100011100000000011100000000011111110000000000000000
010000100000000001010001000010000101001000100011000010000101010010000 1
010000000100001010001000100000101010100010100000010101000000100100110 01
00100100000000000110100010100001000100000100011010000111000100110000 10
00100010010011000000010000000111000000000111000000111000000111110000000000
00100001000100010010010000100000110010010000011000000100101010010000 11
00010100000001011000000100100000000000000000000011000100110001000011111 00000
00010001001001001000100000000001110000000001011000010110111001000010000
00010000110000000110001001001000010010100000010000001000010010101010 100
00001010001000010100000110001000100010000001100001000011001000000111010
00001001010000100001001000100110000100001010000000100010011000010101 01
00001000100110001000010001010001000001001001000011000000100000101001 11
0000000000000001000100000000000010000100010000000000000110100000010001011 00
```

(18, 6, 5)-code with 69 codewords

```
111111000000000000000000000
100000111110000000000000000
100000000001000010000000010110
100000000000100001000011100000
100000000000010000010100010000 1
010000100001111000000000000000
010000010000000000000001101010
010000000100000000010000100001 01
010000000001000010100010000100 00
001000100000000000011001000001 0
001000001000000001100000000000000
001000000100001000100000000001000
001000000010000100000001100000100
000100100000000000000001000110 01
000100010001000000111000000000000
000100000001000101000000010100000
000100000000001010000100010001 00
000010010000100000000110000000000
000010001000001000010000101000 0
000010000101000100000000100010 00
000010000001001000010001000000 10
000001100000000001010010010000 00
000001001001000000000101001000 00
000001000010100000001000000011 00
000001000000000110000000000000 11
000000000100100000100000001100 00
000000000100000001100100000000 01
```

(27, 8, 5)-code with 31 codewords

```
11111100000000000000000000000000
10000010000011110000000000000000
10000001000000000111100000000000
10000000001000000000001000100010010
10000000000010000000000100000001101
01000010000000000100000011100000 00
01000001000000000000011110000000000
01000000010010000010000000001001000
01000000000000010100000000000000100011
00100001000000100000000000001001010 00
00100000100010001000100010000000000
00100000001000000000100010000001000 1
001000000000100100000001000011000000
00010010000000000000010000000111000 0
000100010000100000000000000000100001 10
00010000100000001010001000000000000 1
00010000000010100001000011000000000 0
00001010000000000000100000000000010 10
000010001000000000000000101010001 00
00001000010000010000000101000100000 0
00001000000100000000101000000100000 01
00000100100000100010001000000010000
000001000100010010000100000000100
00000100001010000100000100001000000
00000100000100010001100001000000000
00000011111100000000000000000000000
00000000001000100001000010000000100
0000000000000100010000100001000010
0000000000000001100000000000100110 00
```

(29, 8, 5)-code with 34 codewords

```
11111110000000000000000000000000000000000000
10000001111110000000000000000000000000000000
10000000000000100000000000000000101000100010
10000000000000010001001000000010001100000000
10000000000000000000000010010000010000001110
01000001000000000010000000001000010100000001
01000000100000000000100010000010000001100000
01000000001000000001000000010101001000000000
01000000000001111100000000000000000000000000
00100000100000010000000100000001000000001001
00100000000010000100000011000000100010000000
00100000000001000011110000000000000000000000
00100000000000001000000000000100001010100000
00010001000000100000001110000000000000000000
00010000100000001010000000000000000010000110
00010000000010000000010000001010010000001000
00010000000000000101000000000000000000110001
00001001000001000000000000100000001010010000
00001000010000000010000001001100000000000000
00001000001000001000011000000000010000100000
00001000000100100000000000000100100000100010 0
00000101000000000000100001000010000000000010
00000100001000000110000000100000000001001000
00000100000100001000000100010010100000000000
00000100000011000000001000001000000000000101
00000010010000100000010000010000000010000001
00000010001000010000100000001000100000010000
00000010000101000000000001000000000100101000
00000010000010000001000100000000001000100010
00000000100000000000000100111000000000000000
00000000010000000100100100000000001100000100
00000000010000000000000000100001110000000000
00000000000100010000010010100100000000000010
```

(33, 8, 5)-code with 44 codewords

```
11111111000000000000000000000000000000000000000
10000000111111000000000000000000000000000000000
10000000000000010000000000100001000000010011000
10000000000000001000011000000000000100001000100
10000000000000000101000010001000000011000000000
01000000100000111100000000000000000000000000000
01000000010000000000000000000011000010000000101
01000000001000000001000001000000000100000101010
01000000000100000000100100000100100000000010000
00100000010000100011110000000000000000000000000
00100000001000010000001000011110000000000000000
00100000000010000000000010000000101000001100000
00100000000000001000000100000000000000010000011
00010000000010000100010000000010000000100010000
00010000000000100000000000000100000000010100100
00010000000000000001000111110000000000000000000
00010000000000000000100000010000011100000000000
00001000100000000001000000010001100000000000000
00001000001000100000000010000000010000000010001
00001000000010000000100001001000000000000000100
00001000000001010000000100000000000010100100000
00000100100000000000010000100100000010000000010
00000100001000000000100000000000000001111000000
00000100000100001010000000001001010000000100000
00000100000001000100001000000000100000000001001
00000010100000000000000100000010010001000001000
00000010010000000000000000101000100100100000000
00000010000100000000010001000000001000001000000
00000010000010000100000000010000000000001010010
00000001010000000100000001000100010000001000000
00000001000100000000000010010000000000100001100
00000001000010010010000000000000000101000000001
00000001000001001001000000100010010000000000000
00000000000000100000001000000001001001000000010
```

(34, 8, 5)-code with 47 codewords