reference [1]. Further, this code is the "best" (58,29) self-dual code [5]. In this code too, the number of codewords of weight i is usually a multiple of 29. By computer search we find the following weight distribution for B (with B_i denoting the number of codewords with weight i).

i	B_i
0 & 58	1
12 & 46	$4060 = 2^2 \cdot 5 \cdot 7 \cdot 29$
14 & 44	$35119 = 7 \cdot 173 \cdot 29$
16 & 42	$306791 = 71 \cdot 149 \cdot 29$
18 & 40	$1668051 = 3^2 \cdot 7 \cdot 11 \cdot 83 \cdot 29$
20 & 38	$6857949 = 3 \cdot 7 \cdot 11261 \cdot 29$
22 & 36	$20988199 = 397 \cdot 1823 \cdot 29$
24 & 34	$47840401 = 7 \cdot 463 \cdot 509 \cdot 29$
26 & 32	$82361972 = 2^2 \cdot 7 \cdot 11 \cdot 9221 \cdot 29$
28 & 30	$108372913 = 11 \cdot 339727 \cdot 29$

REFERENCES

- [1] M. Karlin, V. K. Bhargava, and S. E. Tavares, "A note on extended quaternary quadratic residue codes and their binary images," *Inform. Contr.*, vol. 38, pp. 148-153, Aug. 1978.
- [2] V. K. Bhargava, G. E. Séguin, and J. M. Stein, "Some (mk, k) cyclic codes in quasi-cyclic forms," *IEEE Trans. Inform. Theory*, vol. IT-24, pp. 630-632, Sept. 1978.
- [3] M. Karlin, "New binary coding results by circulants," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 81-92, Jan. 1969.
- [4] F. J. MacWilliams, "Decomposition of cyclic codes of block length $3p, 5p, 7p$," *IEEE Trans. Inform. Theory*, vol. IT-25, pp. 112-118, Jan. 1979.
- [5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam: North-Holland and New York: Elsevier/North-Holland, 1977.

Some New Constant Weight Codes

ROBERT E. KIBLER

Abstract—Nonlinear cyclic codes are constructed which improve on published lower bounds for the number $A(n, d, w)$ of codewords in a binary code of length n , constant weight w , and minimum distance d .

Let $A(n, d, w)$ be the maximum number of codewords in any binary code of length n , constant weight w , and minimum distance d . Tables of bounds for $A(n, d, w)$ in the range $n < 24$, $d < 10$ appeared in [1]. In this correspondence we construct a number of nonlinear cyclic codes and thus improve some of the lower bounds on $A(n, d, w)$. Revised tables, incorporating the results given here, may be found in [2].

A code C is *cyclic* if whenever $(v_0, v_1, \dots, v_{n-1})$ is in C , so also is $(v_1, v_2, \dots, v_{n-1}, v_0)$. The codes of our examples are cyclic; we shall describe them by listing a set of generators such that any codeword is a cyclic shift of one of the generators.

Manuscript received May 3, 1979.

The author is with the Department of Defense. His address is 12610 Iyvestone Lane, Laurel, MD 20811.

A code C is said to be *closed under decimation* if whenever $(v_0, v_1, v_2, \dots, v_{n-1})$ is in C , so too is $(v_0, v_1, v_2, \dots, v_{(n-1)t})$ for every t , $0 < t < n$, which is relatively prime to n ; subscripts are considered modulo n . It may well happen that some decimation of a codeword v will be equal to a cyclic shift of v ; that is, the (t, n) decimations of v may not yield $(t, n)n$ distinct codewords. When a code is closed under decimation we may shorten still further the list of codewords required to describe the code. Any code may be decimated at interval t , where $(t, n) = 1$; the decimated code is equivalent to the original.

For each codeword v of C , let $B_i(v)$ denote the number of codewords which are at distance i from v . If $B_i(v)$ is independent of v , we say the code is *distance-invariant*. We write B_i for the average number of codewords at distance i from a fixed codeword. Thus $B_0 = 1$ and $B_i = 0$ if $0 < i < d$. For constant weight codes, $B_i = 0$ when i is odd.

$A(13, 4, 5) > 117$: This code is closed under decimation and is generated as a cyclic code by the six distinct decimations of 1111000010000 and the three distinct decimations of 1110001001000. This code is distance-invariant with $B_4 = 32$, $B_6 = 44$, $B_8 = 36$, and $B_{10} = 4$ and is the unique maximal binary cyclic code with these parameters.

$A(14, 4, 5) > 154$: There are many inequivalent cyclic codes satisfying the bound. An example of a set of generators is

```
11110100000000
11001001000010
11000100001010
11000100010100
11100001000100
11100000010010
10101001001000
11010010100000
11011000010000
11100000101000
11001100100000
```

$A(13, 4, 6) > 156$: There are two inequivalent cyclic codes satisfying the bound. One is closed under decimation and is generated as a cyclic code by the six distinct decimations of 11110100000010, the two distinct decimations of 1111001000100, and the four distinct decimations of 1110110010000. This code has $B_4 = 36$, $B_6 = 55$, $B_8 = 54$, $B_{10} = 9$, and $B_{12} = 1$; it is not distance-invariant.

$A(19, 6, 5) > 76$: The maximal cyclic code, unique up to decimation, is generated by

```
111001010000000000
110100000100001000
110000001010100000
1001001000100001000
```

For this code $B_6 = 35$, $B_8 = 25$, $B_{10} = 15$; it is not distance-invariant.

$A(20, 6, 5) > 84$: There are two maximal inequivalent cyclic codes. One may be generated by

```
1110100000000000100
11000010000011000000
10100100000000101000
11000001000100000010
10001000100010001000
```

$A(21, 6, 5) > 105$: Again the maximal cyclic code is essentially unique. A set of generators is

```
11101000000010000000
110001000010000000100
100100100000100001000
110000101100000000000
110000010000000101000
```

$A(17,6,7) \geq 119$: There are many cyclic codes meeting this bound. One set of generators is

11111010010000000
11100010000101010
11110000001001100
11100001110000100
11011001000101000
11000101001001010
11001100010010010.

Our remaining examples are codes which are closed under decimation but which may not be maximal among cyclic codes with these parameters. We describe the code by giving the generators together with the number of their distinct decimations.

$A((14,4,6) \geq 273$:

11111000010000 (3)
11110100000010 (3)
11110011000000 (6)
11101000100010 (3)
11011000101000 (3)
11100001110000 (3).

$A(15,4,6) \geq 325$:

111100010001000 (2)
111100001010000 (4)
111010000100100 (8)
110110010100000 (2)
110100010010010 (4)
110100000101100 (1)
110001100011000 (2).

$A(19,4,6) \geq 1482$:

1111010001000000000 (18)
1110110000010000000 (18)
1111001000000000100 (9)
1111000100000001000 (9)
1110011100000000000 (9)
1110000111000000000 (9)
1110100100001000000 (6).

$A(14,4,7) \geq 254$:

11111010100000 (6)
11110110010000 (6)
11111001000100 (3)
11101100000110 (3)
10101010101010 (1).

This code, which is closed under the taking of complements, has $B_4 = B_{10} = 40$, $B_6 = B_8 = 86$.

$A(17,4,7) \geq 1224$:

11111000110000000 (16)
11110100100001000 (16)
11110010100100000 (16)
11111001000000100 (8)
11110000101010000 (8)
11111010000000010 (8) or 11111100000100000 (8).

The two codes are inequivalent.

$A(19,4,7) \geq 2679$:

1111100101000000000 (18)
1111011000000100000 (18)
1111010100100000000 (18)
1111010001010000000 (18)
1111001100001000000 (18)
1111001000000011000 (18)
1111101000000000010 (9)
1111100010000001000 (9)
1111100000100100000 (9)
1110010000001101000 (6).

$A(17,4,8) \geq 1496$:

11111100101000000 (16)
11111011000100000 (16)
11111010110000000 (16)
11111001001010000 (16)
11110110010000010 (16)
11111101000000010 (8).

$A(17,6,8) \geq 136$:

11111100100000100 (8).

Finally, we make some remarks concerning $A(24,10,8)$. The lower bound can be improved to 27, for example by the cyclic code with generators

111101001000100010000000
100100100100100100100100.

By linear programming [1] the upper bound is 69. In fact this cannot be attained, and thus $27 \leq A(24,10,8) \leq 68$.

Here is a sketch of the proof. The Delsarte inequalities [1, eq. (13)] imply that if C is a code attaining $A(24,10,8) = 69$, then the distance distribution of C is given by $B_{10} = 56$, $B_{12} = 0$, $B_{14} = 8$, and $B_{16} = 4$. Hence $B_{12}(u) = 0$ and $B_{16}(u) = 4$ for all $u \in C$. It is easy to see that if v and w are any two of the four vectors at distance 16 from u , then v and w must have exactly three ones in common. Furthermore there is an essentially unique way of constructing four vectors of length 16, weight 8, and with any pair overlapping in exactly three places, namely

1111100111000000
1110011000111000
1001111000000111
0100000110110111.

We now have five codewords: $u_1 = 0^{16}1^8$, and u_2, u_3, u_4, u_5 obtained by appending eight zeros to the above vectors. Next we construct codewords u_6, u_7 , and u_8 which, together with u_1 , form the system of four vectors disjoint from u_2 . Again there is essentially only one way of doing this. The final step is to show that it is impossible to find four codewords which are disjoint from u_3 and have the proper overlaps with the other codewords. Hence $A(24,10,8) \neq 69$.

Postscript

A. E. Brouwer [3] has pointed out that the codes constructed here are invariant under the affine group consisting of all permutations on n letters of the form $x \rightarrow ax + b$, where a is relatively prime to n . By considering other groups he obtained further improvements to some values of $A(n,d,w)$.

REFERENCES

- [1] 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.
- [2] R. L. Graham and N. J. A. Sloane, "Lower bounds for constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 37-43, Jan. 1980.
- [3] A. E. Brouwer, "A few new constant weight codes," *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 366-367, May 1980.