Remark 4: The author is unable to deal analytically with the general case of $p \neq 1/2$ where one does not have the property of symmetry. However, the case that p is close to $1/2$ may be tractable and interesting.

References

[1] R. S. Liptser and A. N. Shiryayev, *Statistics of Random Processes, Vol. 1: General Theory*. New York: Springer-Verlag, 1977.

[2] R. K. Mehra and A. E. Bryson, "Linear smoothing using measurements containing correlated noise with an application to inertial navigation," *IEEE Trans. Automat. Contr.*, vol. AC-13, pp. 496–503, Oct. 1968.

[3] H. E. Rauch, F. Tung, and C. T. Striebel, "Maximum likelihood estimates of linear dynamic systems," *AIAA J.*, vol. 3, pp. 1445–1450, Aug. 1965.

[4] J. E. Wall, A. S. Willsky, and N. R. Sandell, "On the fixed-interval smoothing problem," *Stochastics*, vol. 5, pp. 1–41, 1981.

[5] W. M. Wonham, "Some applications of stochastic differential equations to optimal nonlinear filtering," *J. SIAM Contr., Ser. A*, Vol. 2, pp. 347–369, 1965.

[6] Y. C. Yao, "Estimation of noisy telegraph processes: Nonlinear filtering vs. nonlinear smoothing," Tech. rep. ONR29, Statistics Center, Mass. Inst. Tech., Cambridge, MA, Feb. 1983.

The Covering Radius of Cyclic Codes of Length up to 31

DIANE E. DOWNIE AND N. J. A. SLOANE, FELLOW, IEEE

***Abstract*—The covering radius is given for all binary cyclic codes of length less than or equal to 31. Many of these codes are optimal in the sense of having the smallest possible covering radius of any linear code of that length and dimension.**

There has been considerable interest recently in the covering radius of codes (see [1], [3]–[5]), but many open questions remain concerning the covering radius of particular families of codes. In this correspondence we give the covering radius R for all cyclic codes of length $n \leq 31$. As our source for these codes we used C. L. Chen's table in Peterson and Weldon [6, App. D] with four omissions corrected.

Several methods were used to compute R. Most codes were handled by computer. Let C be an $[n, k]$ code.

Method 1: By definition, $R \leq R_0$ if and only if every vector of weight $R_0 + 1$ is within distance R_0 of some codeword. This method may be implemented by first making a list of the codewords, and then testing each n-tuple of weight $R_0 + 1$ to see if it is within distance R_0 of some codeword. The number of steps is proportional to

$$\binom{n}{R_0 + 1} 2^k$$

and 2^k words are needed to store the code.

Method 2: Let H be a parity check matrix for C. Then C has $R \leq R_0$ if and only if every $(n - k)$-tuple is the sum of at most R_0 columns of H [3, Sec. I-A]. This may be implemented by initially setting $\text{hit}(u) = 0$ for all $(n - k)$-tuples u, then finding all sums of R_0 or fewer columns of H, and for each sum s, setting $\text{hit}(s) = 1$. At the end, if $\text{hit}(u) = 1$ for all u, we conclude that $R \leq R_0$. The number of steps is roughly proportional to

$$\binom{n}{R_0} R_0$$

and 2^{n-k} words of storage are needed.

TABLE I
COVERING RADIUS R AND NORM N OF CYCLIC CODES OF LENGTH ≤ 31

n	k	d	roots	R	N
7	4	3	1	1*	3
7	3	4	0,1	3	6
9	3	3	1	3*	7
9	2	6	0,1	4*	8
15	11	3	1	1*	3
15	10	4	0,1	3	6
15	9	3	1,5	3	6
15	9	4	3,5	3	6
15	8	4	0,1,5	4	8
15	8	4	0,3,5	5	10
15	7	3	1,7	3*	7
15	7	5	1,3	3*	7
15	6	6	0,1,3	5	10
15	6	6	0,1,7	4	8
15	5	3	1,5,7	5*	11
15	5	7	1,3,5	5*	10
15	4	6	0,1,5,7	6	12
15	4	8	0,1,3,5	7	14
15	3	5	1,3,7	6*	13
15	2	10	0,1,3,7	7*	14
17	9	5	1	3*	7
17	8	6	0,1	5	10
21	16	3	3,7	2*	5
21	15	3	1	2*	5
21	15	4	0,3,7	3	6
21	14	4	0,1	3	6
21	13	3	1,7	3*	7
21	13	4	3,7,9	3*	7
21	12	3	1,9	3*	7
21	12	4	0,3,7,9	7	14
21	12	4	0,1,7	4	8
21	12	5	1,3	3*	7
21	11	4	0,1,9	4	8
21	11	6	0,1,3	5	10
21	10	4	1,7,9	4*	9
21	10	5	1,3,7	6	12
21	9	3	1,5	5	11
21	9	4	0,1,7,9	9	18
21	9	6	1,3,9	5	11
21	9	8	0,1,3,7	7	14
21	8	6	0,1,3,9	7	14
21	8	6	0,1,5	6	12

*Optimal.

Manuscript received October 26, 1984.

D. E. Downie is with Smith College, Northampton, MA 01063, USA.
N. J. A. Sloane is with AT&T Bell Laboratories, Murray Hill, NJ 07974, USA.

0018-9448/85/0500-0446$01.00

TABLE I (*Continued*)

n	k	d	roots	R	N
21	7	3	1,5,7	7	15
21	7	8	1,3,7,9	6	13
21	6	6	0,1,5,7	8	16
21	6	7	1,3,5	6*	13
21	6	8	0,1,3,7,9	9	18
21	5	10	0,1,3,5	8*	16
21	4	9	1,3,5,7	8*	17
21	3	7	1,3,5,9	9*	19
21	3	12	0,1,3,5,7	10	20
21	2	14	0,1,3,5,9	10*	20
23	12	7	1	3*	7
23	11	8	0,1	7	14
25	5	5	1	10*	21
25	4	10	0,1	11	22
27	9	3	1	9	
27	8	6	0,1	10	
27	7	6	1,9	10	
27	6	6	0,1,9	12	24
27	3	9	1,3	12*	25
27	2	18	0,1,3	13*	26
31	26	3	1	1*	3
31	25	4	0,1	3	
31	21	5	1,3	3*	
31	21	5	1,5	3*	
31	21	5	1,15	3*	
31	20	6	0,1,3	5	
31	20	6	0,1,5	5	
31	20	6	0,1,15	5	
31	16	5	1,5,11	5	11
31	16	6	1,3,7	5	11
31	16	7	1,3,5	5	11
31	16	7	1,5,7	5	11
31	15	6	0,1,3,7	9	18
31	15	8	0,1,3,5	7	14
31	15	8	0,1,5,7	7	14
31	15	8	0,1,5,11	6	12
31	11	11	1,3,5,7	7*	
31	11	11	1,3,5,11	7*	
31	11	10	1,3,7,15	8	
31	10	12	0,1,3,5,7	11	
31	10	12	0,1,3,5,11	11	
31	10	10	0,1,3,7,15	11	
31	6	15	1,3,5,7,11	11	
31	5	16	0,1,3,5,7,11	15	

A few codes were handled analytically. For example, the even subcode of a Hamming code has $R = 3$ ($R \geq 3$ follows from the supercode lemma [3, Prop. 1] and $R \leq 3$ from Delsarte's bound [3, Th. 1]). Secondly, if an $[n, k, d]$ code C can be obtained from an $[n' = n + 1,\ k' = k,\ d' = d + 1]$ even weight code with known covering radius R' by deleting a coordinate, then C has covering radius $R' - 1$ [3, Corr. 1]. We applied this to the $[32, 6, 16]R = 12$ Reed–Muller code [2] and to the $[32, 16, 9]$ $R = 6$ quadratic residue code [1].

The table gives n, k, d and the roots of the generator polynomial, as in [6] (and, as in [6], codes with $k = 1$ or $d \leq 2$ are excluded). Then we give the covering radius R and in many cases the *norm* N, as defined in [4]. (For reasons of economy we did not compute N in every case. In each case when we did compute N, the condition $2R \leq N \leq 2R + 1$ was satisfied, showing that the code was normal. The existence of an abnormal code is still an open question [4].)

Entries marked with an asterisk are optimal in the sense of having the smallest possible covering radius of any linear code of that length and dimension (see the table in [4]). Some unstarred entries may also be optimal. For example at the time of writing it is only known that the smallest covering radius of a $[15, 6]$ code is either 3 or 4.

The table in [6] contains the following errors (on page 495). The fifth code of length 31 should have roots 1, 15 (not 1, 7) and $d = 5$; the eighth code of length 31 should have roots 0, 1, 15 (not 0, 1, 7) and $d = 6$; the nineteenth code should have roots 1, 3, 7, 15 (not 1, 3, 7, 11) and $d = 10$ (not 11); and the twenty-second code should have roots 0, 1, 3, 7, 15 (not 0, 1, 3, 7, 11) and $d = 10$ (not 12).

Acknowledgment

H. F. Mattson Jr. had already computed some of these covering radii (cf. [5]), and we thank him for confirming our results, as well as for some helpful discussions. D. E. Downie wishes to thank Bell Laboratories for its support and hospitality under the 1984 Summer Research Program. The computations were performed on the Bell Laboratories Cray-1 computer.

References

[1] E. F. Assmus, Jr. and V. Pless, "On the covering radius of extremal self-dual codes," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 359–363, May 1983.

[2] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32, 6) Reed–Muller code," *IEEE Trans. Inform. Theory*, vol. IT-18, pp. 203–207, Jan. 1972.

[3] G. D. Cohen, M. R. Karpovsky, H. F. Mattson, Jr., and J. R. Schatz, "Covering radius-survey and recent results," *IEEE Trans. Inform. Theory*, this issue.

[4] R. L. Graham and N. J. A. Sloane, "On the covering radius of codes, *IEEE Trans. Inform. Theory*, this issue.

[5] H. F. Mattson, Jr., "Another upper bound on covering radius," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 356–359, May 1983.

[6] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge, MA: Mass. Inst. Tech., 1972.