11-1991

A Note on Repeated-Root Cyclic Codes

Robert H. Morelos-Zaragoza
University of Hawaii at Manoa, robert.morelos-zaragoza@sjsu.edu

$A=\{1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{m-1}\}$. Since A and B are dual bases, there exist unique indices k, j such that $B=A\cup\{\alpha^j+\alpha^k\}\backslash\{\alpha^k\}$. There are then unique indices k_1 and j_1 such that $\mathrm{tr}((\alpha^j+\alpha^k)\alpha^{k_1})=1$ and $\mathrm{tr}(\alpha^j\alpha^{j_1})=1$. Then, since the bases are duals, $\mathrm{tr}((\alpha^j+\alpha^k)\alpha^{j_1})=0$ and $\mathrm{tr}(\alpha^j\alpha^{k_1})=0$. It follows that $\mathrm{tr}(\alpha^k\alpha^{k_1})=\mathrm{tr}(\alpha^k\alpha^{j_1})=1$. Since $\alpha^k\in A$, the only way this can happen is if $k\in\{k_1,j_1\}$.

First, suppose that $k=k_1$. Then $\mathrm{tr}(\alpha^k\alpha^{j_1})=\mathrm{tr}((\alpha^j+\alpha^k)\alpha^k)=1$. Since $\alpha^k\in A$, it follows that $k=j_1$, whence $k_1=j_1$, a contradiction. Hence, we must have $k=j_1$. Then, $1=\mathrm{tr}(\alpha^k\alpha^{j_1})=\mathrm{tr}(\alpha^{2k})=\mathrm{tr}(\alpha^k)$. Also, $1=\mathrm{tr}(\alpha^j\alpha^{j_1})=\mathrm{tr}(\alpha^k\alpha^j)$. Since $\alpha^k\in A$, we must have $j=0$. Now, we have $\mathrm{tr}(\alpha^{k_1})=0$ and $\mathrm{tr}((1+\alpha^k)\alpha^{k_1})=1$, so $\mathrm{tr}(\alpha^k\alpha^{k_1})=1$. Since $\mathrm{tr}(\alpha^k)=1$ as well, we must have $k_1=0$ since $\alpha^k\in A$. That is, $\mathrm{tr}(1)=0$, which implies that m is even.

It is now easy to see that $\mathrm{tr}(\alpha^k)=\mathrm{tr}(\alpha^{m+k})=1$ and $\mathrm{tr}(\alpha^i)=0$ if $0\le i\le 2m-2$, $i\notin\{k,m+k\}$. The dual basis to $(1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{m-1})$ is

$$(\alpha^k+\alpha^0,\alpha^{k-1},\alpha^{k-2},\cdots,\alpha^0,\alpha^{m-1},\alpha^{m-2},\cdots,\alpha^{k+1}).$$

By Lemma 1, $f'(\alpha)=1/(\alpha^{k+1}+\alpha)$ since $g_0=\alpha^{-1}$. Now, the coefficient of x^1 in $f(x)$ is

$$\alpha g_1+g_0=\frac{1}{\alpha^{k+1}+\alpha}(\alpha^k+\alpha^k+1)=\frac{1}{\alpha^{k+1}+\alpha}.$$

This quantity is nonzero, so it must equal 1. Hence, $\alpha^{k+1}+\alpha+1=0$. Since α satisfies an irreducible polynomial $f(x)$ of degree m, it must be the case that $k=m-1$ and hence, $f(x)=x^m+x+1$ (where m is even). This completes the proof. □

We note that x^m+x+1 is usually reducible over GF(2). It is shown in [9], [10] that the only values of $m<1000$ for which x^m+x+1 is irreducible over GF(2) are the following: $m=2$, 3, 4, 6, 7, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900.

III. Summary

We have examined the question of choosing a polynomial basis of GF(2^m), say $\{1,\alpha,\alpha^2,\alpha^3,\cdots,\alpha^{m-1}\}$, in such a way that (generalized) bit-serial multiplication can be implemented efficiently. What is required is a polynomial basis such that the change of basis matrix from the dual basis to a scalar multiple of the original basis has as few "1" entries as possible. The best possible situation occurs when the minimal polynomial of α is an irreducible trinomial of degree m; then an appropriate scalar multiple, β, yields a change of basis matrix that is a permutation matrix. If no irreducible trinomial of degree m exists, then we have presented a construction which often yields bases where the change of basis matrix has low weight. A simple formula can be used to compute β and the weight of the change of basis matrix, given the minimal polynomial of α.

The results previously mentioned pertain to generalized bit-serial multiplication. In the original version of bit-serial multiplication due to Berlekamp (i.e., when $\beta=1$), the change of basis matrix is a permutation matrix, if and only if m is odd and the minimal polynomial of α is x^m+x+1. Further, the change of basis matrix has weight $m+1$, if and only if m is even and the minimal polynomial of α is x^m+x+1.

References

[1] E. R. Berlekamp, "Bit-serial Reed-Solomon encoders," *IEEE Trans. Inform. Theory*, vol. 28, pp. 869–874, 1982.

[2] T. Beth, "On the arithmetics of Galoisfields and the like," in *Proc. 3rd Int. Conf. AAECC, Lecture Notes in Comput. Sci.*, vol. 229, 1986, pp. 2–16.

[3] K. Imamura, "On self-complimentary bases of GF(q^n) over GF(q)", *Trans. IECE Jap.*, vol. 12, pp. 717–721, 1983.

[4] R. Lidl and H. Niederreiter, *Finite Fields*. Cambridge: Cambridge Univ. Press, 1987.

[5] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers*. Boston, MA: Kluwer Academic Publishers, 1987.

[6] M. Morii, M. Kasahara, and D. L. Whiting, "Efficient bit serial multiplication and the discrete-time Wierner–Hopf equation over finite fields," *IEEE Trans. Inform. Theory*, vol. 35, pp. 1177–1183, Sept. 1989.

[7] W. W. Peterson and E. J. Weldon, Jr., *Error Correcting Codes*. Cambridge, MA: M.I.T. Press, 1972.

[8] M. Wang and I. F. Blake, "Bit-serial multiplication in finite fields," *SIAM J. Discrete Math.*, vol. 3, pp. 140–148, 1990.

[9] N. Zierler and J. Brillhart, "On primitive trinomials (mod2)," *Inform. Contr.*, vol. 13, pp. 541–554, 1968.

[10] N. Zierler and J. Brillhart, "On primitive trinomials (mod2), II," *Inform. Contr.*, vol. 14, pp. 566–569, 1969.

A Note on Repeated-Root Cyclic Codes

Robert Morelos-Zaragoza, *Member*, *IEEE*

***Abstract*—In papers by Castagnoli *et al.* and Van Lint, cyclic codes with repeated roots are analyzed. Both papers fail to acknowledge a previous work by Chen, dating back to 1969, which includes an analysis of even, length binary cyclic codes. Results from Chen's study are presented.**

***Index Terms*—Binary cyclic codes of even length.**

In [1] and [2], the so called repeated-root cyclic codes have been analyzed. However, both papers have failed to mention C. L. Chen's doctoral thesis [3]. In Section 3.6 of [3],[1] entitled "Some Remarks on Cyclic Codes of Even Length," binary cyclic codes of length $2n$ are analyzed. Specifically, the following theorem is proven.

Theorem 1: Let $g_2(x)$ be a factor of the polynomial $g_1(x)$, both over GF(2). For $i=1,2$, let $g_i(x)$ generate an (n,k_i,d_i) cyclic code. Then the minimum distance, d, of the cyclic $(2n,k)$ code generated by $g(x)=g_1(x)g_2(x)$ is given by

$$d=2d_2, \quad \text{if } d_1\ge 2d_2$$

$$d=d_1, \quad \text{if } d_1\le 2d_2.$$

In the proof of Theorem 1, Chen indicates that the following matrix has a row space equivalent to that of the parity-check

Manuscript received May 12, 1991. This work was supported by NSF Grant NCR-8813480.

The author is with the Department of Electrical Engineering, University of Hawaii, Holmes Hall 483, 2540 Dole Street, Honolulu, HI 96822.

IEEE Log Number 9102266.

[1] Interested readers may obtain a copy from the author.

matrix of an even-length cyclic code,

$$\left(\begin{array}{ccccc|ccccc} 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} & 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} & 1 & \beta_2 & \beta_2^2 & \cdots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \beta_s & \beta_s^2 & \cdots & \beta_s^{n-1} & 1 & \beta_s & \beta_s^2 & \cdots & \beta_s^{n-1} \\ \hline 0 & 0 & 0 & \cdots & 0 & \beta_1^{n-1} & 1 & \beta_1 & \cdots & \beta_1^{n-2} \\ 0 & 0 & 0 & \cdots & 0 & \beta_2^{n-1} & 1 & \beta_2 & \cdots & \beta_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \beta_{s'}^{n-1} & 1 & \beta_{s'} & \cdots & \beta_{s'}^{n-2} \end{array}\right),$$

where $\beta_1, \beta_2, \cdots, \beta_s$ are all the roots of $g_1(x)$ and $\beta_1, \beta_2, \cdots, \beta_{s'}$ are the roots of $g_2(x)$, $s' \le s$. It follows that even length cyclic codes are equivalent to codes with the $|\bar{u}|\bar{u}+\bar{v}|$ structure, as indicated in [2].

References

[1] G. Castagnoli, J. L. Massey, P. A. Shoeller, and N. von Seeman, "On repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 337–342, Mar. 1991.

[2] J. H. van Lint, "Repeated-root cyclic codes," *IEEE Trans. Inform. Theory*, vol. 37, no. 2, pp. 343–345, Mar. 1991.

[3] C. L. Chen, "Some Results on Algebraically Structured Error-Correcting Codes," Ph.D. dissert., Univ. of Hawaii, Honolulu, HI, 1969.