On cyclic MDS codes of length q over GF(q)

*Ron M. Roth**

*and Gadiel Seroussi***

ABSTRACT

It is shown that a cyclic code C of length q over $GF(q)$ is MDS if and only if either i) q is a prime, in which case C is equivalent, up to a coordinate permutation, to an extended Reed-Solomon code, or ii) C is a trivial code of dimension $k \in \{1, q-1, q\}$. Hence, there exists a non-trivial cyclic extended Reed-Solomon code of length q over $GF(q)$ if and only if q is a prime.

* Department of Electrical Engineering, Technion, Israel Institute of Technology, Haifa 32000 - Israel.
** Department of Computer Science, Technion, Israel Institute of Technology, Haifa 32000 - Israel.

I. Statement of results

An (n,k,d) linear code C over a finite field $F=GF(q)$ is *maximum distance separable* (in short, MDS) if $d=n-k+1$. MDS codes are optimal in the sense that they achieve the maximum possible minimum distance for given length and dimension.

Let α be a primitive element of $GF(q)$. The $(q-1,k,q-k)$ *Reed-Solomon code* (in short, RS code) over $GF(q)$ is the cyclic code generated by $g(x)=\prod_{i=1}^{q-1-k}(x-\alpha^i)$.[1] The $(q,k,q-k+1)$ *extended RS code* is obtained from the RS code by adding an overall parity check digit. The generator matrix of the extended code is

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} & 0 \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{(q-2)\cdot 2} & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \cdots & \alpha^{(q-2)(k-1)} & 0 \end{bmatrix}.$$

RS codes and extended RS codes are well known to be MDS. An extensive treatment of RS codes, and of MDS codes in general, can be found in [1, chs. 10 and 11].

Two linear codes are said to be *equivalent* if one is obtained from the other by a permutation of coordinates. In this note, we characterize all cyclic MDS codes of length q over $GF(q)$. The results are summarized in the following theorem and corollary:

Theorem 1: Let C be a cyclic code of length q over $F=GF(q)$. Then,

(i) If q is a prime, then C is equivalent to an extended RS code, and hence, it is MDS.

(ii) If $q=p^m$ for some prime p and integer $m>1$, then C is MDS if and only if C is one of the following trivial codes: the $(q,1,q)$ repetition code, the $(q,q-1,2)$ single-parity-check code, or the $(q,q,1)$ entire vector space F^q.

---

[1] Actually, we are dealing with *narrow sense* RS codes, which are the most commonly studied. In general, the roots of the code are defined to be α^b, α^{b+1}, $\cdots$, $\alpha^{b+q-2-k}$, for some integer b. In our case, $b=1$.

Corollary 1: The extended Reed-Solomon code of length q and dimension $2 \le k \le q-2$ over $GF(q)$ is equivalent to a cyclic code if and only if q is prime.

The fact that all cyclic codes of prime length p over $GF(p)$ are MDS had already been established by Assmus and Mattson in [2]. Here we identify those codes with extended RS codes of prime length, and we show that no other non-trivial extended RS codes can be cyclic.

II. Proofs

Proof of Theorem 1: Let C be a cyclic (q,k,d) code over $GF(q)$. Then C has a generator polynomial $g(x)$ of degree $q-k$, which satisfies [1, ch. 7]

$$g(x) \mid x^q - 1.$$

Since raising to the q-th power is a linear operation in $GF(q)$, we have

$$x^q - 1 = (x-1)^q$$

Hence, we must have

$$g(x) = (x-1)^{q-k}.$$

Assume $q=p^m$ for some prime p and integer $m \ge 1$. We distinguish now between the cases $m=1$ and $m>1$, giving, repectively, parts (i) and (ii) of the theorem.

Part (i): $m=1$. Consider the polynomials

$$f_i(x) = \sum_{j=0}^{q-1} j^i x^j, \quad 0 \le i \le q-1.$$

(Arithmetic is carried out modulo the prime q, and we define $0^0 \equiv 1$). We claim that $f_i(x)$ is divisible by $(x-1)^{q-1-i}$, $0 \le i \le q-1$, and therefore, the vectors representing the polynomials $f_0(x), f_1(x), \cdots, f_{k-1}(x)$, are in C. We prove the claim by induction on i. For $i=0$, we have

$$f_0(x) = \sum_{j=0}^{q-1} x^j = \frac{x^q - 1}{x-1} = (x-1)^{q-1}.$$

For $1 \le i \le q-1$, assume $(x-1)^{q-i} \mid f_{i-1}(x)$. Then, the formal derivative ([1, p. 98]) $f'_{i-1}(x)$ of $f_{i-1}(x)$ satisfies $(x-1)^{q-1-i} \mid f'_{i-1}(x)$. However,

$$f'_{i-1}(x) = \Big(\sum_{j=0}^{q-1} j^{i-1} x^j \Big)' = \sum_{j=0}^{q-1} j^i x^{j-1}.$$

Hence, $f_i(x) = x f'_{i-1}(x)$, and thus, $(x-1)^{q-1-i} \mid f_i(x)$. This completes the proof of the claim. Let $\bar{G}$ denote the $k \times q$ matrix whose rows are the vector representations of the polynomials $f_0(x), f_1(x), \cdots, f_{k-1}(x)$. Then,

$$\bar{G} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & q-1 \\ 0 & 1^2 & 2^2 & \cdots & (q-1)^2 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 1^{k-1} & 2^{k-1} & \cdots & (q-1)^{k-1} \end{bmatrix}.$$

Since the first k columns of $\bar{G}$ form a Vandermonde matrix, $\bar{G}$ has dimension k, and, thus, it can be used as a generator matrix for C. Now, since α is a primitive element of $GF(q)$, the columns of $\bar{G}$ are the same, up to ordering, as the columns of the matrix G defined in Section I. Therefore, C is equivalent to the $(q, k, q-k+1)$ extended RS code generated by G.

Part (ii): $m>1$. Let $r=q-k$. Then, $g(x)=(x-1)^r$. If $r \le p^{m-1}$, then C includes the codeword (in polynomial representation)

$$c(x) = (x-1)^{p^{m-1}} = x^{p^{m-1}} - 1,$$

of weight 2. Hence, the minimum distance of the code satisfies $d \le 2$. If $d=2$, then to satisfy the MDS requirement we must have $k=q-1$, which implies that $g(x)=x-1$, and that C is the single-parity-check code. If $d=1$, then $k=q$, and C is the entire space F^q.

Consider now the case where $p^{m-1}<r\le p^m-1$. Clearly, a necessary condition for C to be MDS is that all $r+1$ coefficients of $g(x)=(x-1)^r$ be nonzero. Hence we require $\binom{r}{j} \not\equiv 0 \bmod p$, for all j, $0 \le j \le r$. By Lucas' theorem on binomial coefficients modulo p [3], [4, p. 68], these incongruences are simultaneously satisfied if and only if $r \equiv -1 \bmod p^{m-1}$. Hence $r = sp^{m-1} - 1$ for some integer s, $2 \le s \le p$. One of the codewords is $(x-1)^{r+1} = (x^{p^{m-1}} - 1)^s$, whose weight is at most $s+1$. Since $d = r+1 = sp^{m-1} > s+1$, this codeword must be the zero word. Hence $r+1=q$, or $r = q-1$, and, therefore, C is the code generated by

$$(x-1)^{q-1} = \frac{(x-1)^q}{x-1} = \frac{x^q-1}{x-1} = \sum_{j=0}^{q-1} x^j .$$

which is the $(q,1,q)$ repetition code.

Q.E.D.

Proof of Corollary 1: If q is prime, then, by part (i) of Theorem 1, the $(q,k,q-k+1)$ extended RS code is equivalent to the cyclic code generated by $(x-1)^{q-k}$. If q is not prime, then, by part (ii) of Theorem 1, there are no cyclic MDS codes of length q and dimension $2 \le k \le q-2$. Hence, since the extended RS code is always MDS, there are no cyclic extended RS codes with those parameters.

Q.E.D.

REFERENCES

[1] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam: North-Holland, 1983.

[2] E.F. Assmus, Jr., and H.F. Mattson, Jr., "New 5-designs", *J. Comb. Theory*, Vol. 6, pp. 122-151, 1969.

[3] M. E. Lucas, "Sur les congruences de nombres Euleriennes, et des coefficients différentials de functions trigonométriques, suivant un module premier," *Bull. Soc. Math. France,* vol. 6, pp. 49–54, 1878.

[4] D. E. Knuth, *The Art of Computer Programming, Vol. 1: Fundamental Algorithms.* Reading, MA: Addison-Wesley, 1969.