

## Symmetric polynomials and some good codes

Ling, San; Niederreiter, Harald; Xing, Chaoping

2000

Ling, S., Niederreiter, H., & Xing, C. (2000). Symmetric Polynomials and Some Good Codes. *Finite Fields and Their Applications*, 7(1), 142-148.

<https://hdl.handle.net/10356/96319>

<https://doi.org/10.1006/ffta.2000.0305>

---

© 2000 Academic Press. This is the author created version of a work that has been peer reviewed and accepted for publication by *Finite Fields and Their Applications*, Academic Press. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [<http://dx.doi.org/10.1006/ffta.2000.0305>].

*Downloaded on 23 Mar 2023 23:36:34 SGT*

# Symmetric Polynomials and Some Good Codes

San Ling

*Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543,  
Republic of Singapore*  
E-mail: lings@math.nus.edu.sg

Harald Niederreiter

*Institute of Discrete Mathematics, Austrian Academy of Sciences, Sonnenfelsgasse 19,  
A-1010 Vienna, Austria*  
E-mail: niederreiter@oeaw.ac.at

and

Chaoping Xing

*Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543,  
Republic of Singapore*  
E-mail: xingcp@math.nus.edu.sg

Elements from extensions of  $\mathbf{F}_q$  are employed to construct a class of linear codes over  $\mathbf{F}_q$  with good parameters through symmetric polynomials over  $\mathbf{F}_q$ .

## 1. INTRODUCTION

Constructions of generalized Reed–Solomon codes over  $\mathbf{F}_q$  (see [3, Chap. 10]) only employ elements of  $\mathbf{F}_q$ ; hence their lengths are at most  $q$ . In order to make use of elements of  $\mathbf{F}_{q^2}$ , we modified the constructions of generalized Reed–Solomon codes in [4]. It turns out that the modified constructions yield many good codes and many improvements on Brouwer’s table [1] are achieved. In this paper we develop the idea of constructing linear codes using

elements from any finite extension of  $\mathbf{F}_q$ . It seems more natural to describe our constructions through elementary symmetric polynomials. Our results show that codes from our constructions have good parameters and the length of codes constructed in this way could be arbitrarily large.

This paper is arranged as follows. In Section 2 we discuss some basic results on certain linear spaces and present our constructions of linear codes. We list examples of good codes from our constructions in Section 3.

## 2. CONSTRUCTION OF CODES

Let  $q$  be a prime power and let  $s$  be a positive integer. Consider the polynomial in  $\mathbf{F}_q[X, Y]$  given by

$$\prod_{i=0}^{s-1} (Y - X^{q^i}) = Y^s - \sigma_1 Y^{s-1} + \sigma_2 Y^{s-2} + \cdots + (-1)^{s-1} \sigma_{s-1} Y + (-1)^s \sigma_s. \quad (1)$$

It is clear that  $\sigma_i$  is a polynomial in  $\mathbf{F}_q[X]$  for all  $1 \leq i \leq s$ . In fact,  $\sigma_i$  is the  $i$ th elementary symmetric polynomial in the  $s$  symbols  $X, X^q, X^{q^2}, \dots, X^{q^{s-1}}$ .

**LEMMA 2.1.** *For any  $\alpha \in \mathbf{F}_{q^s}$  and  $1 \leq i \leq s$ , we have  $\sigma_i(\alpha) \in \mathbf{F}_q$ .*

*Proof.* From (1) it is obvious that

$$\sigma_i(\alpha) = \sigma_i(\alpha^q) = \cdots = \sigma_i(\alpha^{q^{s-1}}).$$

It follows therefore that  $\sigma_i(\alpha) = \sigma_i(\alpha)^q$ , which is equivalent to  $\sigma_i(\alpha) \in \mathbf{F}_q$ . ■

**LEMMA 2.2.** *Let  $f \in \mathbf{F}_q[X]$  and let  $\beta \in \mathbf{F}_{q^s}$ . Then  $f(\beta) = 0$  if and only if  $f(\beta^{q^i}) = 0$  for all  $0 \leq i \leq s-1$ .*

*Proof.* Since the coefficients of  $f$  are in  $\mathbf{F}_q$ , it follows that  $f(\beta^{q^i}) = (f(\beta))^{q^i}$  for all  $0 \leq i \leq s-1$ . The lemma follows immediately from this equality. ■

Let  $(j_1, j_2, \dots, j_s)$  be an  $s$ -tuple of non-negative integers. We define the polynomial  $e_{j_1 j_2 \dots j_s} \in \mathbf{F}_q[X]$  as follows:

$$e_{j_1 j_2 \dots j_s} := \sigma_1^{j_1} \sigma_2^{j_2} \cdots \sigma_s^{j_s} \in \mathbf{F}_q[X].$$

As  $\deg(\sigma_i) = q^{s-1} + q^{s-2} + \cdots + q^{s-i}$ , we have

$$\deg(e_{j_1 j_2 \dots j_s}) = \sum_{i=1}^s (q^{s-1} + q^{s-2} + \cdots + q^{s-i}) j_i.$$

**LEMMA 2.3.** *The  $q^s$  polynomials  $e_{j_1 j_2 \dots j_s}$ ,  $0 \leq j_1, j_2, \dots, j_s \leq q-1$ , are linearly independent over  $\mathbf{F}_q$ .*

*Proof.* It suffices to show that, for any two different  $s$ -tuples  $(j_1, j_2, \dots, j_s)$  and  $(k_1, k_2, \dots, k_s)$  with  $0 \leq j_1, j_2, \dots, j_s \leq q-1$  and  $0 \leq k_1, k_2, \dots, k_s \leq q-1$ , the polynomials  $e_{j_1 j_2 \dots j_s}$  and  $e_{k_1 k_2 \dots k_s}$  have different degrees.

We suppose that for some  $0 \leq j_1, j_2, \dots, j_s \leq q-1$  and  $0 \leq k_1, k_2, \dots, k_s \leq q-1$ , we have

$$\deg(e_{j_1 j_2 \dots j_s}) = \deg(e_{k_1 k_2 \dots k_s}).$$

In other words,

$$\sum_{i=1}^s (q^{s-1} + \dots + q^{s-i}) j_i = \sum_{i=1}^s (q^{s-1} + \dots + q^{s-i}) k_i,$$

or equivalently,

$$\sum_{i=1}^s (q^{s-1} + \dots + q^{s-i}) (j_i - k_i) = 0.$$

It follows that  $j_s - k_s \equiv 0 \pmod{q}$ , hence  $j_s = k_s$ . This implies

$$\sum_{i=1}^{s-1} (q^{s-1} + \dots + q^{s-i}) (j_i - k_i) = 0,$$

from which it follows that  $j_{s-1} - k_{s-1} \equiv 0 \pmod{q}$ , and hence  $j_{s-1} = k_{s-1}$ . Continuing the same argument, we obtain  $j_i = k_i$  for all  $1 \leq i \leq s$ . ■

For  $1 \leq m \leq q$ , let  $V_{s,m}$  be the  $\mathbf{F}_q$ -vector space spanned by the set  $\{e_{j_1 j_2 \dots j_s} : \sum_{i=1}^s j_i \leq m-1, j_i \geq 0\}$ . Clearly, for  $1 \leq m \leq q$  and  $s \geq 1$ ,

$$\begin{aligned} \dim_{\mathbf{F}_q} V_{s,m} &= |\{e_{j_1 j_2 \dots j_s} : \sum_{i=1}^s j_i \leq m-1, j_i \geq 0\}| \\ &= |\{(j_1, j_2, \dots, j_s) : \sum_{i=1}^s j_i \leq m-1, j_i \geq 0\}|. \end{aligned}$$

LEMMA 2.4. *We have  $\dim_{\mathbf{F}_q} V_{s,m} = \binom{m+s-1}{s}$ .*

*Proof.* Let  $n(s, m)$  denote the dimension of  $V_{s,m}$ . Then  $n(s, m)$  is equal to the coefficient of  $x^{m-1}$  in the formal power series

$$G(x) := (1 + x + x^2 + \dots)^{s+1} = (1-x)^{-s-1}$$

over the reals. By evaluating this coefficient as a Taylor coefficient, we get

$$n(s, m) = \frac{G^{(m-1)}(0)}{(m-1)!} = \binom{m+s-1}{s}. \quad \blacksquare$$

For  $m \geq 2$  and  $s \geq 2$ , let  $\mathbf{l} = (\ell_1, \ell_2, \dots, \ell_{s-1}) \in \mathbf{Z}^{s-1}$  with  $0 \leq \ell_{s-1} \leq \ell_{s-2} \leq \dots \leq \ell_1 \leq m-1$  and let

$$\begin{aligned} A(s, m, \mathbf{l}) &= |\{(j_1, j_2, \dots, j_s) : \sum_{i=1}^s j_i = m-1, j_i \geq 0, j_s \leq \ell_{s-1}, j_s + j_{s-1} \\ &\leq \ell_{s-2}, \dots, \sum_{i=2}^s j_i \leq \ell_1\}|. \end{aligned}$$

For example, when  $s = 2$ ,  $\mathbf{l} = \ell$  for  $0 \leq \ell \leq m - 1$ , so  $A(2, m, \ell) = \ell + 1$ . When  $s = 3$  and  $\mathbf{l} = (\ell_1, \ell_2)$ , we have  $A(3, m, \mathbf{l}) = \frac{1}{2}(\ell_1 + 1)(\ell_1 + 2) - \frac{1}{2}(\ell_1 - \ell_2)(\ell_1 - \ell_2 + 1)$ .

For  $2 \leq m \leq q$  and  $\mathbf{l} = (\ell_1, \ell_2, \dots, \ell_{s-1}) \in \mathbf{Z}^{s-1}$  with  $0 \leq \ell_{s-1} \leq \ell_{s-2} \leq \dots \leq \ell_1 \leq m - 1$ , let  $V_{s, m, \mathbf{l}}$  be the  $\mathbf{F}_q$ -vector space spanned by the set

$$\begin{aligned} & \{e_{j_1 \dots j_s} : \sum_{i=1}^s j_i \leq m - 2, j_i \geq 0\} \\ & \cup \{e_{j_1 \dots j_s} : \sum_{i=1}^s j_i = m - 1, j_i \geq 0, j_s \leq \ell_{s-1}, \\ & j_s + j_{s-1} \leq \ell_{s-2}, \dots, \sum_{i=2}^s j_i \leq \ell_1\}. \end{aligned}$$

We see easily that the following statements are true:

1. We have  $\dim_{\mathbf{F}_q} V_{s, m, \mathbf{l}} = \binom{m+s-2}{s} + A(s, m, \mathbf{l})$ ; and
2. the highest degree of a polynomial in  $V_{s, m, \mathbf{l}}$  is

$$(m - 1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1}.$$

In particular, if  $\mathbf{l} = (m - 1, m - 1, \dots, m - 1)$ , then  $V_{s, m, \mathbf{l}} = V_{s, m}$ .

For every  $s \geq 1$ , let  $I_q(s)$  denote the number of monic irreducible polynomials in  $\mathbf{F}_q[X]$  of degree  $s$ . Then it is well known (see [2, Theorem 3.25]) that

$$I_q(s) = \frac{1}{s} \sum_{b|s} \mu\left(\frac{s}{b}\right) q^b,$$

where  $\mu$  is the Möbius function.

Let  $\beta_1, \beta_2, \dots, \beta_{I_q(s)} \in \mathbf{F}_{q^s}$  be roots of the distinct monic irreducible polynomials in  $\mathbf{F}_q[X]$  of degree  $s$  (one root for each such polynomial). Label also the elements of  $\mathbf{F}_q$  as  $\alpha_1, \alpha_2, \dots, \alpha_q$ .

For  $s \geq 2$ ,  $0 \leq t \leq q$ ,  $1 \leq r \leq I_q(s)$ ,  $2 \leq m \leq q$ , and  $\mathbf{l}$  as above, define the  $\mathbf{F}_q$ -linear code  $C_q(s, t, r, m, \mathbf{l})$  as

$$C_q(s, t, r, m, \mathbf{l}) = \{(f(\alpha_1), f(\alpha_2), \dots, f(\alpha_t), f(\beta_1), f(\beta_2), \dots, f(\beta_r)) : f \in V_{s, m, \mathbf{l}}\}.$$

**THEOREM 2.5.** *If  $s \geq 2$ ,  $0 \leq t \leq q$ ,  $2 \leq m \leq q$ ,  $\mathbf{l} = (\ell_1, \dots, \ell_{s-1}) \in \mathbf{Z}^{s-1}$  with  $0 \leq \ell_{s-1} \leq \dots \leq \ell_1 \leq m - 1$ , and  $I_q(s) \geq r > \frac{1}{s}((m - 1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t)$ , then the code  $C_q(s, t, r, m, \mathbf{l})$  has parameters  $[n, k, d]$ , where*

$$\begin{aligned} n &= t + r, \\ k &= \binom{m + s - 2}{s} + A(s, m, \mathbf{l}), \\ d &\geq r - \frac{1}{s} \left( (m - 1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t \right). \end{aligned}$$

*Proof.* Let  $f \in V_{s,m,\mathbf{l}}$ ,  $f \neq 0$ . Suppose that  $f$  has  $r_1$  roots among  $\{\alpha_1, \dots, \alpha_t\}$  and  $r_2$  roots among  $\{\beta_1, \dots, \beta_r\}$ . Then

$$r_1 \leq t \quad \text{and} \quad r_1 + sr_2 \leq \deg(f) \leq (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1}.$$

This implies that, for  $\mathbf{c}_f = (f(\alpha_1), \dots, f(\alpha_t), f(\beta_1), \dots, f(\beta_r)) \in C_q(s, t, r, m, \mathbf{l})$ , its Hamming weight  $\text{wt}(\mathbf{c}_f)$  satisfies

$$\begin{aligned} & \text{wt}(\mathbf{c}_f) \\ & \geq n - (r_1 + r_2) \\ & \geq r + t - \frac{1}{s} \left( (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} + (s-1)t \right) \\ & = r - \frac{1}{s} \left( (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t \right) > 0. \end{aligned}$$

This in turn implies that the  $\mathbb{F}_q$ -linear map

$$\begin{aligned} V_{s,m,\mathbf{l}} & \rightarrow C_q(s, t, r, m, \mathbf{l}) \\ f & \mapsto (f(\alpha_1), \dots, f(\alpha_t), f(\beta_1), \dots, f(\beta_r)) \end{aligned}$$

is injective; hence

$$\dim_{\mathbb{F}_q} C_q(s, t, r, m, \mathbf{l}) = \dim_{\mathbb{F}_q} V_{s,m,\mathbf{l}} = \binom{m+s-2}{s} + A(s, m, \mathbf{l})$$

and

$$d \geq r - \frac{1}{s} \left( (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t \right). \quad \blacksquare$$

*Remark.* In the statement of Theorem 2.5, if  $m \leq q-1$  and  $r = I_q(s)$ , then the condition  $r > \frac{1}{s} \left( (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t \right)$  is automatically satisfied. To see this, we distinguish between two cases.

First, let  $s$  be a prime. In this case,  $t + rs = t + \sum_{b|s} \mu\left(\frac{s}{b}\right) q^b = t + q^s - q \geq q^s - q$ . Hence,

$$\begin{aligned} & r - \frac{1}{s} \left( (m-1)q^{s-1} + \sum_{i=1}^{s-1} \ell_i q^{s-i-1} - t \right) \\ & = \frac{1}{s} \left( rs + t - (m-1)q^{s-1} - \sum_{i=1}^{s-1} \ell_i q^{s-i-1} \right) \\ & \geq \frac{1}{s} \left( q^s - q - (q-2) \frac{q^s - 1}{q-1} \right) \\ & > 0. \end{aligned}$$

When  $s$  is composite, we need to show that

$$rs = \sum_{b|s} \mu\left(\frac{s}{b}\right) q^b > (q-2) \frac{q^s - 1}{q-1};$$

i.e.,

$$q^s + \left( \sum_{b|s, b \neq s} \mu\left(\frac{s}{b}\right) q^b \right) (q-1) + (q-2) > 0.$$

It is easy to see that  $|\sum_{b|s, b \neq s} \mu\left(\frac{s}{b}\right) q^b| \leq q^{s/2+1}$ , so

$$q^s + \left( \sum_{b|s, b \neq s} \mu\left(\frac{s}{b}\right) q^b \right) (q-1) + (q-2) \geq (q^s - q^{s/2+2}) + q^{s/2+1} + (q-2) > 0.$$

*Remark.* The construction of the code  $C_q(s, t, r, m, \mathbf{l})$  in this section can be extended by adding further coordinates  $f(\gamma)$  for roots  $\gamma$  of irreducible polynomials in  $\mathbf{F}_q[X]$  whose degrees are nontrivial divisors of  $s$ . However, so far our best examples stem from the case considered in Theorem 2.5.

### 3. EXAMPLES

A comparison of the codes obtained from the construction above and the codes from Brouwer's table [1] reveals that our construction yields a number of good codes. For  $s = 3$ ,  $q = 3, 4$ , or  $5$ , and  $r = I_q(3) = (q^3 - q)/3$ , a number of codes constructed with the method above have as good a lower bound on the minimum distance as the ones listed in [1]. We list some of them in the table below. The variables  $t, m, \ell_1, \ell_2, n, k$ , and  $d$  are the same as in Theorem 2.5.

$q$	$t$	$m$	$\ell_1$	$\ell_2$	$n$	$k$	$d$
5	0	2	1	1	40	4	30
5	1	2	1	1	41	4	30
5	2	2	1	1	42	4	31
5	3	3	2	2	43	10	21
4	0	2	1	1	20	4	13
4	1	2	1	1	21	4	14
3	0	2	1	1	8	4	4
3	1	2	0	0	9	2	6

## REFERENCES

1. A. Brouwer, "Bounds on the Minimum Distance of Linear Codes," *available at* <http://www.win.tue.nl/~aeb/voorlincod.html>.
2. R. Lidl and H. Niederreiter, "Finite Fields," Cambridge Univ. Press, Cambridge, UK, 1997.
3. F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes," North-Holland, Amsterdam, 1977.
4. C. Xing and S. Ling, A class of linear codes with good parameters, *IEEE Trans. Inform Theory* **46** (2000), to appear.