A Note on Nonlinear Xing Codes

Yaron Shany and Yair Be'ery, *Senior Member, IEEE*

***Abstract*—Nonlinear Xing codes are considered. It is shown that Xing codes of length $p-1$ (where p is a prime) are subcodes of cosets of Reed–Solomon codes whose minimum distance equals Xing's lower bound on the minimum distance. This provides a straightforward proof for the lower bound on the minimum distance of the codes. The alphabet size of Xing codes is restricted not to be larger than the characteristic of the relevant finite field $\mathbb{F}_r$. It is shown that codes with the same length and the same lower bounds on the size and minimum distance as Xing codes exist for any alphabet size not exceeding the size r of the relevant finite field, thus extending Xing's results.**

***Index Terms*—Reed–Solomon codes, Xing codes.**

I. Introduction

In a recent paper [1], a new class of nonlinear codes with good parameters was presented. To find a lower bound on the minimum distance of the new codes, Xing used the deep Hurwitz genus formula from the theory of algebraic function fields. In Section II of this note, we show that Xing codes of length $p-1$ are subcodes of cosets of Reed–Solomon codes whose minimum distance is exactly the lower bound found by Xing. This gives a more straightforward proof for the lower bound on the minimum distance of these codes, and may hint on encoding and decoding techniques.

The alphabet size of Xing codes is restricted not to be larger than the characteristic p of the relevant finite field $\mathbb{F}_r$. In Section III of this note, we prove the existence of codes with the same length and the same lower bounds on the size and minimum distance as Xing codes for any alphabet size not exceeding r, thus generalizing Xing's results. Moreover, our proof, which is based only on elementary coding theory, is almost trivial.

II. Xing Codes and Reed–Solomon Codes

We begin by briefly describing Xing codes. Let $r=p^m$ for some prime p and some positive integer m. For a commutative ring R with identity, we write $R^\times$ for the multiplicative group consisting of all elements of R with a multiplicative inverse. Write

$$\mathbb{F}_r^\times=\{\alpha_1,\alpha_2,\ldots,\alpha_{r-1}\}.$$

Let $q\le p$ be a positive integer. Let d, $1\le d\le r-1$, be an integer and define a map

$$\sigma_q\colon\begin{cases}\mathbb{Z}_q^{r-1}\to(\mathbb{F}_r[x]/(x^d))^\times/\mathbb{F}_r^\times\\ (c_1,c_2,\ldots,c_{r-1})\mapsto\overline{\prod_{i=1}^{r-1}(x-\alpha_i)^{c_i}},\end{cases}$$

where here $\mathbb{Z}_p$ is the ring (field) $\{0,1,\ldots,p-1\}$ with addition and multiplication modulo p, and if $q<p$, $\mathbb{Z}_q$ stands for the subset $\{0,1,\ldots,q-1\}$ of $\mathbb{Z}_p$ without any associated algebraic structure. For $z\in\mathrm{im}(\sigma_q)$, we set $C_q(z,r,d):=\sigma_q^{-1}(z)$. Let $z_0\in\mathrm{im}(\sigma_q)$ be such that $|\sigma_q^{-1}(z_0)|$ attains the maximum of $\{|\sigma_q^{-1}(z)||z\in\mathrm{im}(\sigma_q)|\}$, and define $C_q(r,d):=\sigma_q^{-1}(z_0)$. Since $|(\mathbb{F}_r[x]/(x^d))^\times/\mathbb{F}_r^\times|=r^{d-1}$ and $|\mathbb{Z}_q^{r-1}|=q^{r-1}$, it follows that $|C_q(r,d)|\ge q^{r-1}/r^{d-1}$. Using the Hurwitz genus formula, Xing also showed that the minimum distance[1] of $C_q(z,r,d)$ is not less than d for any $z\in\mathrm{im}(\sigma_q)$, and hence also the minimum distance of $C_q(r,d)$ is not less then d. This establishes the existence of an $(r-1,\ge q^{r-1}/r^{d-1},\ge d)$ code over $\mathbb{Z}_q$, where the notation (n,M,d) code stands for a code of length n, size M, and minimum distance d.

Let $\mathrm{RS}_r(d)$ be the $[r-1,r-d,d]$ Reed–Solomon code over $\mathbb{F}_r$, where the notation $[n,k,d]$ code stands for a linear code of length n, dimension k, and minimum distance d. For the rest of this section, we shall focus on the case where $r=p$. Note that [1, Corollary 2.4] and all of the examples in Xing's paper correspond to this case. Our main result in this section is the following theorem.

Theorem 1: The code $C_q(p,d)$ is contained in a coset of $\mathrm{RS}_p(d)$ for some coordinate ordering of $\mathrm{RS}_p(d)$.

Before proving this theorem, we need the following technical lemma.

Lemma 1: Let

$$P(x):=\prod_{i=1}^{p-1}(x-\alpha_i)^{c_i}\in\mathbb{F}_p[x]$$

(for $c_1,c_2,\ldots,c_{p-1}\in\mathbb{Z}_p=\mathbb{F}_p$), and let D be the formal derivative. Then for any positive integer $j\le p-1$

$$(D^jP)(0)=k\sum_{i=1}^{p-1}c_i\beta_i^j+Q_j\left(\sum_{i=1}^{p-1}c_i\beta_i,\sum_{i=1}^{p-1}c_i\beta_i^2,\ldots,\sum_{i=1}^{p-1}c_i\beta_i^{j-1}\right)$$

where $0\ne k\in\mathbb{F}_p$, $\beta_i=-\alpha_i^{-1}$ for $i\in\{1,2,\ldots,p-1\}$, and $Q_j\in\mathbb{F}_p[x_1,x_2,\ldots,x_{j-1}]$ is such that $Q_j(0,0,\ldots,0)=0$.

Proof: Write $n:=p-1$. For a vector $d\in\mathbb{F}_p^n$ and for $i\in\{1,2,\ldots,n\}$, we write d_i for the ith component of d. In addition, for $l\in\{1,2,\ldots,n\}$, we let $c^{(l)}$ be the vector $d\in\mathbb{F}_p^n$ with

$$d_l=\begin{cases}c_l-1, & \text{if } c_l\ne 0\\ 0, & \text{if } c_l=0\end{cases}$$

and $d_i=c_i$ for $i\in\{1,2,\ldots,n\}$, $i\ne l$. As

$$\left(c^{(l_1)}\right)^{(l_2)}=\left(c^{(l_2)}\right)^{(l_1)}$$

for any $l_1,l_2\in\{1,2,\ldots,n\}$, we shall simply write $c^{(l_1,l_2)}$ for either of these (identical) vectors. The vector $c^{(l_1,l_2,\ldots,l_m)}$ is defined in a similar way for any positive integer $m\le n$ and any $l_1,l_2,\ldots,l_m\in\{1,2,\ldots,n\}$. Now, it can be verified by induction that

$$D^jP=\sum_{(i_1,i_2,\ldots,i_j)\in\{1,2,\ldots,p-1\}^j}c_{i_1}c_{i_2}^{(i_1)}c_{i_3}^{(i_1,i_2)}\cdots c_{i_j}^{(i_1,i_2,\ldots,i_{j-1})}\times\prod_{m=1}^{p-1}(x-\alpha_m)^{c_m^{(i_1,i_2,\ldots,i_j)}}$$

and hence, we get (1) at the top of the following page. For $l\in\{2,3,\ldots,j\}$, each expression of the form $c_{i_l}^{(i_1,i_2,\ldots,i_{l-1})}$ in (1) can be replaced by[2] $c_{i_l}-\delta_{i_1,i_l}-\delta_{i_2,i_l}-\cdots-\delta_{i_{l-1},i_l}$, where for integers u, v, $\delta_{u,v}$ equals 1 if $u=v$ and 0 otherwise. Since the coefficient of $\delta_{i_1,i_2,\ldots,i_j}$ (which, by definition, equals 1 if all the

Manuscript received January 27, 2003; revised November 25, 2003.

The authors are with the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel (e-mail: shany@eng.tau.ac.il; ybeery@eng.tau.ac.il).

Communicated by J. Justesen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.825038

[1]Here, the term "minimum distance" stands for minimum Hamming distance.

[2]Note that the alternative expression is not necessary equal to the original expression, but the replacement is still legal.

$$(D^j P)(0) = \left(\prod_{m=1}^{p-1} (-\alpha_m)^{c_m}\right) \sum_{(i_1,i_2,\ldots,i_j)\in\{1,2,\ldots,p-1\}^j} c_{i_1} c_{i_2}^{(i_1)} c_{i_3}^{(i_1,i_2)} \cdots c_{i_j}^{(i_1,i_2,\ldots,i_{j-1})} \beta_{i_1}\beta_{i_2}\cdots\beta i_j. \quad (1)$$

arguments are identical and 0 otherwise) in (1) is $(j-1)! \neq 0$, the assertion follows. □

Proof of Theorem 1: Observe first that for positive integers $q_1 < q_2 \leq p$, and for a fixed $z \in \mathrm{im}(\sigma_{q_1})$, $C_{q_1}(z,p,d) \subseteq C_{q_2}(z,p,d)$ (this follows immediately from the definition of these codes). Therefore, to prove the assertion, it is sufficient to show that $C_p(z,p,d)$ is a coset of $\mathrm{RS}_p(d)$ for every $z \in \mathrm{im}(\sigma_p)$. To this end, observe that σ_p is a homomorphism from the additive group $\mathbb{Z}_p^{r-1} = \mathbb{F}_p^{r-1}$ to the multiplicative group $(\mathbb{F}_p[x]/(x^d))^\times/\mathbb{F}_p^\times$. To see this, note that since $d < p$, it follows that in $(\mathbb{F}_p[x]/(x^d))^\times/\mathbb{F}_p^\times$

$$\overline{(x+\alpha)^p} = \overline{x^p + \alpha^p} = 1$$

for any $\alpha \in \mathbb{F}_p^\times$. So, in order to establish the theorem, it is sufficient to show that $C_p(1,p,d)$ is equal to $\mathrm{RS}_p(d)$ up to a permutation. As before, let us write $n = p-1$. A vector $c \in \mathbb{F}_p^n$ is in $C_p(1,p,d)$ iff the coefficients of $x, x^2, \ldots, x^{d-1}$ in

$$P(x) = \prod_{i=1}^{p-1} (x-\alpha_i)^{c_i} \in \mathbb{F}_p[x]$$

are all zero. Since $j! \neq 0$ in $\mathbb{F}_p$ for any positive integer $j \leq p-1$, the above condition is equivalent to

$$(DP)(0) = 0, (D^2P)(0) = 0, \ldots, (D^{d-1}P)(0) = 0.$$

Therefore, it follows from Lemma 1 that $c \in C_p(1,p,d)$ iff

$$\sum_{i=1}^{n} c_i \beta_i^j = 0$$

for $j = 1, 2, \ldots, d-1$, which establishes the proof. □

Note that the last assertion of the proof resembles the proof of Proposition 1 in [2]. Note also that the case $d < p < r$ can be treated in a similar way, replacing $\mathrm{RS}_p(d)$ by the Bose–Chaudhuri–Hocquenghem (BCH) code $\mathrm{RS}_r(d) \cap \mathbb{F}_p^{r-1}$.

III. Extending Xing's Results

In the following theorem we show that Xing's existence results can be extended to comply with larger alphabet sizes. As before, the idea is to consider subcodes of Reed–Solomon codes.

Theorem 2: Let $A \subseteq \mathbb{F}_r$, set $q := |A|$, and let $d \leq r-1$ be a positive integer. Then there exists an $(r-1, M, d')$ code over A with $M \geq q^{r-1}/r^{d-1}$ and $d' \geq d$.

Proof: Put $n := r-1$ and $k := r-d$. Let H be a parity-check matrix for $\mathrm{RS}_r(d)$, and consider the map

$$\mu : \begin{cases} A^n \to \mathbb{F}_r^{n-k} \\ v \mapsto Hv^t \end{cases}$$

where v^t stands for v transposed. Since $|A^n| = q^n$ and $|\mathrm{im}(\mu)| \leq r^{n-k}$, it follows that there is an element $u \in \mathrm{im}(\mu)$ with

$$|\mu^{-1}(u)| \geq q^n/r^{n-k} = q^{r-1}/r^{d-1}.$$

Define $C := \mu^{-1}(u)$. Then C has the desired parameters, as C is contained in a single coset of $\mathrm{RS}_r(d)$ in $\mathbb{F}_r^n$. □

Remark 1: Note that Theorem 2 does not imply that Xing's codes are necessarily contained in a coset of a Reed–Solomon code when $d \geq p$. Note also that by replacing the Reed–Solomon code by a non-*maximum-distance separable (MDS)* code in the proof of Theorem 2, it is possible to obtain codes of lengths other than $r-1$ at the price of a reduced size.

Remark 2: If $q = p^{m_1}$, where $m_1 < m$ is an integer dividing m, and $A = \mathbb{F}_{p^{m_1}} \subset \mathbb{F}_r = \mathbb{F}_{p^m}$, then it is interesting to compare the lower bound on M from Theorem 2 to the known lower bound on the size of the BCH code $\mathrm{RS}_r(d) \cap A^{r-1}$ (which, in this case, equals the pre-image of 0 in Theorem 2). The dimension of the BCH code over $\mathbb{F}_{p^{m_1}}$ is not less than $(r-1) - (d-1)m/m_1$, since this dimension equals $(r-1) - \deg Q$, where Q is the least common multiplier (l.c.m.) of $d-1$ minimal polynomials of elements of $\mathbb{F}_r = \mathbb{F}_{p^m}$ over $\mathbb{F}_{p^{m_1}}$. This simple lower bound on the dimension of the BCH code gives the same lower bound as Theorem 2 on the size, i.e.,

$$M \geq p^{m_1((r-1)-(d-1)m/m_1)}.$$

Since by the definition of the code from Theorem 2 its size is not smaller than that of the BCH code,[3] this means that for the choice of $|A| = p^{m_1}$ the lower bound presented in the theorem is probably not tight (especially in the cases where the above bound on the dimension of the BCH code is not tight, see [3, Ch. 9]). However, as demonstrated by Xing [1], there exist cases where the lower bound of Theorem 2 is slightly larger than the size of any known linear code. In fact, it is also possible to find cases where $q > p$ and the bound of Theorem 2 is slightly larger than the size of any known linear code. For example, for $q = 9$ and $r = 7^2$, Theorem 2 implies the existence of a $(48, \approx 9^{32.0588}, 10)$ code over an alphabet of nine elements, while the largest known linear code over $\mathbb{F}_9$ of minimum distance 10 has dimension 32 [4].

Acknowledgment

The authors thank Dr. I. Reuven and Prof. C. P. Xing for carefully reading an earlier version of the manuscript.

References

[1] C. P. Xing, "Construction of codes from residue rings of polynomials," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2995–2997, Nov. 2002.
[2] I. M. Duursma, "Preparata codes through lattices," *IEEE Trans. Inform. Theory*, vol. 47, pp. 36–44, Jan. 2001.
[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[4] A. Brouwer. Bounds on the Minimum Distance of Linear Codes (Server). [Online]. Available: http://www.win.tue.nl/~aeb/voorlincod.html

[3] Actually, under the above assumptions the size of the code from Theorem 2 equals the size of the BCH code, because $\boldsymbol{\mu}$ is an $\mathbb{F}_{p^{m_1}}$-linear map.