Research Letter

Decoding the Ternary (23, 11, 9) Quadratic Residue Code

J. Carmelo Interlando

Department of Mathematics and Statistics, San Diego State University, San Diego, CA 92182-7720, USA

Correspondence should be addressed to J. Carmelo Interlando, interlan@mail.sdsu.edu

Received 11 January 2009; Accepted 10 April 2009

Recommended by Guosen Yue

The algebraic decoding of binary quadratic residue codes can be performed using the Peterson or the Berlekamp-Massey algorithm once certain unknown syndromes are determined or eliminated. The technique of determining unknown syndromes is applied to the nonbinary case to decode the expurgated ternary quadratic residue code of length 23.

Copyright © 2009 J. Carmelo Interlando. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Quadratic residue (QR) codes are cyclic, nominally half-rate codes, that are powerful with respect to their error-correction capabilities. Decoding QR codes is in general a difficult task, but great progress has been made in the binary case since the work of Elia [1] and He *et al.* [2]. Decoding algorithms for certain nonbinary QR codes were proposed by Higgs and Humphreys in [3] and [4]. In [5], decoding of QR codes is performed by embedding them in codes over cyclotomic number fields.

This paper shows that one technique used to decode binary QR codes can be applied successfully to decode nonbinary QR codes. The main idea is to determine certain unknown syndromes in order to restore linearity to Newton's identities. Once this is done, either the Peterson or the Berlekamp-Massey algorithm can be used to solve the identities. The method of determining unknown syndromes was first presented by He *et al.* in [2] to decode the binary QR code of length 47 and subsequently to decode several other binary QR codes; see [6] and references therein.

Section 2 reviews the necessary background and the latter method, with the objective of establishing notation. In Section 3, the method is illustrated on the decoding of the expurgated ternary QR code of length 23. The focus is solely on the calculation of the error-location polynomial. Error values can be found from the evaluator polynomial [7, p. 246] once the error locations are determined.

2. Background and Terminology

Let $\mathcal{Q} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$ be the set of quadratic residues of 23 and $\mathcal{N}$ the set of quadratic nonresidues of 23. The smallest extension of $\mathbb{F}_3 = \text{GF}(3)$ containing α , a primitive twenty-third root of unity, is $\mathbb{F}_{3^{11}} = \text{GF}(3^{11})$. Denote the set $\{0\} \cup \mathcal{Q}$ by $\mathcal{Z}$ and define $g(x) \in \mathbb{F}_3[x]$ as

$$g(x) = \prod_{i \in \mathcal{Z}} (x - \alpha^i) \quad (1)$$

$$= x^{12} + x^9 + x^7 + x^6 + 2x^5 + x^4 + 2x^3 + 2x + 1.$$

The cyclic code generated by $g(x)$ is the expurgated ternary QR of length 23; see [7]. Its minimum Hamming distance is equal to 9, which can be verified by direct inspection.

Let $c(x) = \sum_{i=0}^{22} c_i x^i \in \mathbb{F}_3[x]$ be the sent code polynomial, that is, a multiple of $g(x)$. The received polynomial, denoted by $r(x) = \sum_{i=0}^{22} r_i x^i$, satisfies $r(x) = c(x) + e(x)$ where $e(x) = \sum_{i=0}^{22} e_i x^i \in \mathbb{F}_3[x]$ is the error pattern. Let ν denote the Hamming weight of $e(x)$. Observe that $e(x)$ can be correctly determined provided $\nu \leq 4$. Only $g(x)$ and $r(x)$ are known to the receiver, which seeks to determine the most probable $e(x)$. For any $k \in \mathbb{Z}$, the syndrome s_k is defined as $s_k = e(\alpha^k)$. It follows that $s_{3k} = s_k^3$, for all $k \in \mathbb{Z}$. Observe that for all $k, \ell \in \mathbb{Z}$, $s_k = s_\ell$ whenever $k \equiv \ell \pmod{23}$. For any $k \in \mathbb{Z}$, $g(\alpha^k) = 0$, whence $s_k = r(\alpha^k)$. For this reason, the s_ℓ with $\ell \pmod{23} \in \mathcal{Z}$ are called *known* syndromes. The other s_ℓ are called *unknown* syndromes.

The set of indices j for which $e_j \neq 0$ is $L = \{i_1, \dots, i_\nu\}$. We have $0 \leq i_1 < i_2 < \dots < i_\nu \leq 22$. The elements of L are called the error locations, and the $z_j = \alpha^{i_j} \in \mathbb{F}_{3^{11}}$ are the error-location numbers. These are the roots of the error-location polynomial:

$$\sigma(x) = x^\nu + \sum_{j=0}^{\nu-1} \sigma_{\nu-j} x^j = \prod_{j=1}^{\nu} (x - z_j), \quad (2)$$

where the σ_i are the elementary symmetric functions that in turn are related to the syndromes via Newton's identities [7, pp. 244–245]:

$$s_k + \sum_{j=1}^{\nu} \sigma_j s_{k-j} = 0 \quad \text{for } k \in \mathbb{Z}. \quad (3)$$

The equations in (3) can be solved efficiently when there are a sufficient number of consecutive known syndromes. However, when decoding QR codes, typically this is not the case. Such difficulty can be overcome by calculating one or more unknown syndromes with the aid of the following result from [2, p. 1182], applied to the nonbinary case [8] (recall that $s_k = \sum_{j=1}^{\nu} e_{i_j} z_j^k$, for all $k \in \mathbb{Z}$).

Theorem 1. Let $I = \{i_1, i_2, \dots, i_{\nu+1}\}$ and $J = \{j_1, j_2, \dots, j_{\nu+1}\}$ be two subsets of $\{0, \dots, 22\}$. They define two $(\nu + 1) \times \nu$ matrices and one $\nu \times \nu$ diagonal matrix given, respectively, by

$$\begin{aligned} X_I &= \begin{bmatrix} z_1^{i_1} & z_2^{i_1} & \dots & z_\nu^{i_1} \\ z_1^{i_2} & z_2^{i_2} & \dots & z_\nu^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{i_{\nu+1}} & z_2^{i_{\nu+1}} & \dots & z_\nu^{i_{\nu+1}} \end{bmatrix}, \\ X_J &= \begin{bmatrix} z_1^{j_1} & z_2^{j_1} & \dots & z_\nu^{j_1} \\ z_1^{j_2} & z_2^{j_2} & \dots & z_\nu^{j_2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{j_{\nu+1}} & z_2^{j_{\nu+1}} & \dots & z_\nu^{j_{\nu+1}} \end{bmatrix}, \\ Y_I &= \begin{bmatrix} e_{i_1} & 0 & \dots & 0 \\ 0 & e_{i_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & e_{i_\nu} \end{bmatrix}. \end{aligned} \quad (4)$$

Then the $(\nu + 1) \times (\nu + 1)$ matrix defined by $S(I, J) = X_I Y_I X_J^T$ is equal to

$$S(I, J) = \begin{bmatrix} s_{i_1+j_1} & s_{i_1+j_2} & \dots & s_{i_1+j_{\nu+1}} \\ s_{i_2+j_1} & s_{i_2+j_2} & \dots & s_{i_2+j_{\nu+1}} \\ \vdots & \vdots & \ddots & \vdots \\ s_{i_{\nu+1}+j_1} & s_{i_{\nu+1}+j_2} & \dots & s_{i_{\nu+1}+j_{\nu+1}} \end{bmatrix}. \quad (5)$$

Furthermore, $\det S(I, J) = 0$.

If $S(I, J)$ has entries that are unknown syndromes, then Theorem 1 can be used to determine them from the equation $\det S(I, J) = 0$.

3. Calculation of $\sigma(x)$ for the Ternary (23,11,9) QR Code

In this section the use of Theorem 1 for decoding nonbinary QR codes is illustrated. The focus is on the ternary QR code of length 23 generated by $g(x)$. The final result is an algorithm for finding $\sigma(x)$, the error-location polynomial, from $r(x)$. The decoder will determine the coefficients of $\sigma(x)$, namely, the σ_i , from (3). Knowledge of a sequence of consecutive syndromes is required. One choice is $s_{22} = s_{-1}, s_0, s_1, s_2, s_3, s_4, s_5, s_6$. Observe that any syndrome s_k where $k \in \mathbb{Z}$ can be readily computed by the decoder as $r(\alpha^k)$. Since $5 \notin \mathbb{Z}$, s_5 is the unknown syndrome to be determined during the decoding procedure described next. Since $5 \cdot 9 \equiv 22 \pmod{23}$, one has $s_{-1} = s_{22} = s_5^9$.

Let $I_1 = \{1, 2, 5, 9, 21\}$, $J_1 = \{3, 4, 7, 11, 22\}$, $I_2 = \{0, 4, 8, 19, 20\}$, and $J_2 = \{4, 5, 8, 12, 16\}$. Form the matrices $S(I_1, J_1)$ and $S(I_2, J_2)$ as in (5),

$$S(I_1, J_1) = \begin{bmatrix} s_4 & \underline{s_5} & s_8 & s_{12} & s_0 \\ \underline{s_5} & s_6 & s_9 & s_{13} & s_1 \\ s_8 & s_9 & s_{12} & s_{16} & s_4 \\ s_{12} & s_{13} & s_{16} & \underline{s_{20}} & s_8 \\ s_1 & s_2 & \underline{s_5} & s_9 & \underline{s_{20}} \end{bmatrix}, \quad (6)$$

$$S(I_2, J_2) = \begin{bmatrix} s_4 & \underline{s_5} & s_8 & s_{12} & s_{16} \\ s_8 & s_9 & s_{12} & s_{16} & \underline{s_{20}} \\ s_{12} & s_{13} & s_{16} & \underline{s_{20}} & s_1 \\ s_0 & s_1 & s_4 & s_8 & s_{12} \\ s_1 & s_2 & \underline{s_5} & s_9 & s_{13} \end{bmatrix}.$$

All the entries in $S(I_1, J_1)$ and $S(I_2, J_2)$ are known except for s_5 and s_{20} . However, $s_{20} = s_5^{27}$. Therefore, $f_1 = \det S(I_1, J_1)$ and $f_2 = \det S(I_2, J_2)$ are polynomials in a single variable, namely, s_5 . The next proposition was verified for each one of the 156906 error patterns of weights 1, 2, 3, and 4, using Magma [9].

Proposition 1. For $\nu = 1, 2, 3, 4$, $\gcd(f_1, f_2)$ is a first-degree polynomial in s_5 .

The above yields the following procedure for determining $\sigma(x)$.

Step 1. If $s_0 = s_1 = 0$, then declare that $\nu = 0$ and exit. Otherwise, proceed to Step 2.

Step 2. Let $f = \gcd(f_1, f_2)$. If $\deg f = 1$, solve $f = 0$ for s_5 and proceed to Step 3. Otherwise, declare that $\nu > 4$ and exit.

Step 3. Determine the coefficients of the error-location polynomial $\sigma(x)$ by solving the following linear system for the elementary symmetric functions:

$$s_k = - \sum_{j=k-4}^{k-1} s_j \sigma_{k-j} \quad \text{for } k = 3, 4, 5, 6. \quad (7)$$

If the linear system is nonsingular and $\sigma(x)$ has four roots $x_1, \dots, x_4 \in \mathbb{F}_{3^{11}}$ which satisfy $x_i^{23} = 1$ for $i = 1, \dots, 4$, then declare $\nu = 4$ and exit. Otherwise, proceed to Step 4.

Step 4. Solve the following linear system for the elementary symmetric functions:

$$s_k = - \sum_{j=k-3}^{k-1} s_j \sigma_{k-j} \quad \text{for } k = 4, 5, 6. \quad (8)$$

If the linear system is nonsingular and $\sigma(x)$ has three roots $x_1, x_2, x_3 \in \mathbb{F}_{3^{11}}$ which satisfy $x_i^{23} = 1$ for $i = 1, 2, 3$, then declare $\nu = 3$ and exit. Otherwise, proceed to Step 5.

Step 5. Solve the following linear system for the elementary symmetric functions:

$$s_k = - \sum_{j=k-2}^{k-1} s_j \sigma_{k-j} \quad \text{for } k = 5, 6. \quad (9)$$

If the linear system is nonsingular and $\sigma(x)$ has two roots $x_1, x_2 \in \mathbb{F}_{3^{11}}$ which satisfy $x_i^{23} = 1$ for $i = 1, 2$, then declare $\nu = 2$ and exit. Otherwise, proceed to Step 6.

Step 6. If we get to this point, then either $\nu = 1$ or $\nu > 4$. The coefficient σ_1 of $\sigma(x)$ is calculated as $\sigma_1 = -s_6/s_5$. If $\sigma_1 \in \mathbb{F}_{3^{11}}$ is such that $\sigma_1^{23} = 1$, then $\nu = 1$. Otherwise, declare that $\nu > 4$. Exit.

References

- [1] M. Elia, "Algebraic decoding of the (23, 12, 7) Golay code," *IEEE Transactions on Information Theory*, vol. 33, no. 1, pp. 150–151, 1987.
- [2] R. He, I. S. Reed, T.-K. Truong, and X. Chen, "Decoding the (47, 24, 11) quadratic residue code," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1181–1186, 2001.
- [3] R. J. Higgs and J. F. Humphreys, "Decoding the ternary Golay code," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 1043–1046, 1993.
- [4] R. J. Higgs and J. F. Humphreys, "Decoding the ternary (23, 12, 8) quadratic residue code," *IEE Proceedings: Communications*, vol. 142, no. 3, pp. 129–134, 1995.
- [5] M. Elia and J. C. Interlando, "Quadratic-residue codes and cyclotomic fields," *Acta Applicandae Mathematicae*, vol. 93, no. 1–3, pp. 237–251, 2006.
- [6] Y. Chang, T.-K. Truong, I. S. Reed, H. Y. Cheng, and C. D. Lee, "Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes," *IEEE Transactions on Communications*, vol. 51, no. 9, pp. 1463–1473, 2003.
- [7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, The Netherlands, 1977.
- [8] G.-L. Feng and K. K. Tzeng, "A new procedure for decoding cyclic and BCH codes up to actual minimum distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1364–1374, 1994.
- [9] J. J. Cannon and C. Playoust, *An Introduction to Algebraic Programming in Magma*, School of Mathematics and Statistics, University of Sydney, Sydney, Australia, 1996.