Hindawi Publishing Corporation
Research Letters in Communications
Volume 2009, Article ID 107432, 3 pages
doi:10.1155/2009/107432

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.

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 $\mathbb{F}_3 = \mathrm{GF}(3)$ containing α, a primitive twenty-third root of unity, is $\mathbb{F}_{3^{11}} = \mathrm{GF}(3^{11})$. Denote the set $\{0\} \cup \mathcal{Q}$ by $\mathcal{Z}$ and define $g(x) \in \mathbb{F}_3[x]$ as

$$g(x) = \prod_{i\in\mathcal{Z}} (x - \alpha^i) = x^{12} + x^9 + x^7 + x^6 + 2x^5 + x^4 + 2x^3 + 2x + 1. \quad (1)$$

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 $k \in \mathcal{Z}$, $g(\alpha^k) = 0$, whence $s_k = r(\alpha^k)$. For this reason, the s_ℓ with $\ell \bmod 23 \in \mathcal{Z}$ are called *known* syndromes. The other s_ℓ are called *unknown* syndromes.

The set of indices j for which $e_j \neq 0$ is $L = \{i_1, \ldots, i_\nu\}$. We have $0 \leq i_1 < i_2 < \cdots < i_\nu \leq 22$. 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:

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

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]:

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

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

$$X_I = \begin{bmatrix} z_1^{i_1} & z_2^{i_1} & \cdots & z_\nu^{i_1} \\ z_1^{i_2} & z_2^{i_2} & \cdots & z_\nu^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{i_{\nu+1}} & z_2^{i_{\nu+1}} & \cdots & z_\nu^{i_{\nu+1}} \end{bmatrix},$$

$$X_J = \begin{bmatrix} z_1^{j_1} & z_2^{j_1} & \cdots & z_\nu^{j_1} \\ z_1^{j_2} & z_2^{j_2} & \cdots & z_\nu^{j_2} \\ \vdots & \vdots & \ddots & \vdots \\ z_1^{j_{\nu+1}} & z_2^{j_{\nu+1}} & \cdots & z_\nu^{j_{\nu+1}} \end{bmatrix}, \tag{4}$$

$$Y_I = \begin{bmatrix} e_{i_1} & 0 & \cdots & 0 \\ 0 & e_{i_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e_{i_\nu} \end{bmatrix}.$$

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

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

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 $k \in \mathcal{Z}$ can be readily computed by the decoder as $r(\alpha^k)$. Since $5 \notin \mathcal{Z}$, 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),

$$S(I_1, J_1) = \begin{bmatrix} s_4 & \underline{s_5} & s_8 & s_{12} & s_0 \\ \underline{s_5} & s_6 & s_9 & s_{13} & s_1 \\ s_8 & s_9 & s_{12} & s_{16} & s_4 \\ s_{12} & s_{13} & s_{16} & \underline{s_{20}} & s_8 \\ s_1 & s_2 & \underline{s_5} & s_9 & \underline{s_{20}} \end{bmatrix},$$
$$S(I_2, J_2) = \begin{bmatrix} s_4 & \underline{s_5} & s_8 & s_{12} & s_{16} \\ s_8 & s_9 & s_{12} & s_{16} & \underline{s_{20}} \\ s_{12} & s_{13} & s_{16} & \underline{s_{20}} & s_1 \\ s_0 & s_1 & s_4 & s_8 & s_{12} \\ s_1 & s_2 & \underline{s_5} & s_9 & s_{13} \end{bmatrix}. \tag{6}$$

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 $f_2 = \det\ S(I_1, J_1)$ 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:

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

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

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

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

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:

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

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.

EURASIP Journal on Wireless Communications and Networking

Special Issue on Optical Wireless Communications and Networking

Call for Papers

Optical wireless systems play an increasingly important role in our communication infrastructure, and new systems for very high-data-rate secure communications are under development. From space-based systems to terrestrial long-distance and indoor systems, they are being investigated for fixed, portable, and mobile communication applications. Current research activities in the design and performance of transceivers, pointing, acquisition, and tracking (PAT), modulation and diversity techniques, modeling and analysis of indoor wireless, and developments in hybrid systems, which use RF links together with optical links, are some examples that demonstrate current intense interests in optical wireless.

This issue aims at providing a venue for recent developments in optical wireless systems and networks. New experimental indoor and outdoor results are of particular interest. Original theoretical results, including modeling and simulation, are also welcome. Integration of optical wireless with other personal area networks is another area of interest. The contributions for this special issue should address one of the following topic areas:

- Technologies: channel modeling, modulation and coding for improved outdoor and indoor communication, statistics in reliability and availability, MIMO systems, Gbit/s technology, networking of directional wireless systems, interplay between PAT and network topology, emerging concepts and technologies, new hybrid optical/RF transceiver designs, applications of modulating retroreflectors, cross-layer issues in optical wireless sensor networks, link layer, network and transport protocols, and modeling
- Short-range systems: sensor networks, indoor systems, and IrDA personal device technologies
- Medium-range systems: special modulation and coding schemes, hybrid systems, and switchover technologies
- Long-range systems: HAPs and intersatellite communications

Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://www.hindawi.com/journals/wcn/guidelines.html. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	December 1, 2009
First Round of Reviews	March 1, 2009
Publication Date	June 1, 2010

Lead Guest Editor

Deva K. Borah, Klipsch School of Electrical & Computer Engineering, New Mexico State University, Las Cruces, NM 88003, USA; dborah@nmsu.edu

Guest Editors

Anthony C. Boucouvalas, Telecommunication Science and Technology Department, University of Peloponnese, Terma Karaiskaki, 22100 Tripoli, Greece; acb@uop.gr

Christopher C. Davis, Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA; davis@umd.edu

Rittwik Jana, AT&T Labs Research, 180 Park Ave, Florham Park, NJ, USA; rjana@research.att.com

Steve Hranilovic, Department of Electrical and Computer Engineering, McMaster University, Hamilton, ON, Canada L8S 4K1; hranilovic@mcmaster.ca

EURASIP Journal on Wireless Communications and Networking

Special Issue on Interference Management in Wireless Communication Systems: Theory and Applications

Call for Papers

Interference is a fundamental nature of wireless communication systems, in which multiple transmissions often take place simultaneously over a common communication medium. In recent years, there has been a rapidly growing interest in developing reliable and spectral efficient wireless communication systems. One primary challenge in such a development is how to deal with the interference, which may substantially limit the reliability and the throughput of a wireless communication system. In most existing wireless communication systems, interference is dealt with by coordinating users to orthogonalize their transmissions in time or frequency, or by increasing transmission power and treating each other's interference as noise. Over the past twenty years, a number of sophisticated receiver designs, for example, multiuser detection, have been proposed for interference suppression under various settings. Recently, the paradigm has shifted to focus on how to intelligently exploit the knowledge and/or the structure of interference to achieve improved reliability and throughput of wireless communication systems.

This special issue aims to bring together state-of-the-art research contributions and practical implementations that effectively manage interference in wireless communication systems. Original contributions in all areas related to interference management for wireless communication systems are solicited for this special issue. We are particularly interested in manuscripts that report the latest development on interference channels or cognitive radio channels from the perspectives of information theory, signal processing, and coding theory. Topics of interest include, but are not limited to:

- Information theoretic study of interference channels or cognitive radio channels
- Game theoretical approach to interference management in wireless networks
- Cooperative wireless communication systems
- Relaying in interference networks
- Advanced coding schemes for interference/cognitive radio channels
- Interference channels with confidentiality requirement
- Femtocell networks
- Signal processing algorithms for interference mitigation
- Receiver designs for interference channels or cognitive radio channels
- MIMO interference channels or MIMO cognitive radio channels
- Base station cooperation for interference mitigation
- Network coding for interference channels or cognitive radio channels
- Resource allocation for interference management

Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://www.hindawi.com/journals/wcn/guidelines.html. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	November 1, 2009
First Round of Reviews	February 1, 2010
Publication Date	June 1, 2010

Lead Guest Editor

Yan Xin, NEC Laboratories America, Inc., Princeton, NJ 08540, USA; yanxin@nec-labs.com

Guest Editors

Xiaodong Wang, Electrical Engineering Department, Columbia University, New York, NY 10027, USA; wangx@ee.columbia.edu

Geert Leus, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands; g.j.t.leus@tudelft.nl

Guosen Yue, NEC Laboratories America, Inc., Princeton, NJ 08540, USA; yueg@nec-labs.com

Jinhua Jiang, Department of Electrical Engineering, Stanford University Stanford, CA 94305, USA; jhjiang@stanford.edu

EURASIP Journal on Wireless Communications and Networking

Special Issue on Network Coding for Wireless Networks

Call for Papers

The main idea in network coding was introduced in 2000 by Ahlswede et al. With network coding, an intermediate node in a network cannot only forward its incoming packets but also encode them. It has been shown that the use of network coding can enhance the performance of wired networks significantly. Recent work indicates that network coding can also offer significant benefits for wireless networks.

Communications over wireless channels are error-prone and unpredictable due to fading, mobility, and intermittent connectivity. Moreover, in wireless networks, transmissions are broadcast and can be overhead by neighbors, which is treated in current systems as interference. Finally, security poses new challenges in wireless networks, where both passive and active attacks have quite different premises than in wired networks. Ideas in network coding promise to help toward all these issues, allowing to gracefully add redundancy to combat errors, take advantage of the broadcast nature of the wireless medium and achieve opportunistic diversity, exploit interference rather than be limited by it, and provide secure network communication against adversarial attacks.

In this special issue, we are interested in original research articles which can carry the momentum further and take the wireless network coding research to the next level. The areas of interest include novel network code designs and algorithms, new applications of wireless network coding, network coding capacity, and performance analysis. In addition to original research articles, we are open to review articles. The following list indicates topics of interest which is by no means exhaustive:

- Network codes and algorithms for wireless networks
- Physical layer network coding
- Joint source coding and network coding
- Graph codes and network coding
- Reduced complexity decoding for network coding
- Secure network coding
- Capacity and fundamental bounds on network coding performance
- Cross-layer optimization and network coding
- Energy-efficient network coding
- TCP, routing, MAC, or scheduling algorithms for network codes
- Wireless network coding for multimedia application
- Wireless network coding for bio-medical application

Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://www.hindawi.com/journals/wcn/guidelines.html. Prospective authors should submit an electronic copy of their complete manuscript through the journal Manuscript Tracking System at http://mts.hindawi.com/ according to the following timetable:

Manuscript Due	October 1, 2009
First Round of Reviews	January 1, 2010
Publication Date	April 1, 2010

Lead Guest Editor

Heung-No Lee, Department of Information and Communications, Gwangju Institute of Science and Technology (GIST), Gwangju, South Korea; heungno@gist.ac.kr

Guest Editors

Sae-Young Chung, School of EECS, KAIST, Daejeon, South Korea; sychung@ee.kaist.ac.kr

Christina Fragouli, School of Computer and Communication Sciences, EPFL, Lausanne, Switzerland; christina.fragouli@epfl.ch

Zhi-Hong Mao, ECE/Bio-Medical Dept., the University of Pittsburgh, Pittsburgh, PA, USA; zhm4@pitt.edu