Convolutional Encoding of Some Binary Quadratic Residue Codes

Chong-Dao Lee, Trieu-Kien Truong, Yan-Haw Chen *

Abstract—**In this paper, the optimal convolutional encoding for the five quadratic residue (QR) codes are investigated. Simulation results show that the smallest constraint length $K = 4$ (respectively, $K = 4$, 8, 11, 14) is convolutionally encoded for the QR code with length 24 (respectively, 32, 48, 72, 80).**

Keywords: convolutional encoding, quadratic residue codes

1 Introduction

Let n be a prime number of the form $n \equiv \pm 1 \pmod 8$. A binary QR code of length n is an $(n, (n+1)/2, d)$ cyclic code with the minimum distance d and the generator polynomial $g(x) = \prod_{i \in Q}(x - \beta^i)$, where $Q = \{i | i \equiv j^2 \bmod n \text{ for } 1 \le j \le n-1\}$ is the collection of all nonzero quadratic residues modulo n and β is a primitive nth root of unity in $GF(2^m)$ satisfying $n \mid 2^m - 1$. A codeword of the QR code of length n is a binary vector $\mathbf{c} = (c_0,\ c_1, \ldots,\ c_{n-1})$ so that its associated polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ is a multiple of $g(x)$. The extended QR code is defined to be the extended code of the QR code whose codewords are obtained by adjoining a parity-check bit to every codeword $\mathbf{c}$ of the QR code. For convenience, the parity-check bit with c_∞ is added to the right of the last entry of $\mathbf{c}$; that is, $\bar{\mathbf{c}} = c_0 c_1 \cdots c_{n-1} c_\infty$ with $c_\infty \equiv c_0 + c_1 + \cdots + c_{n-1} \pmod 2$. It is readily seen that the length of an extended QR code is $n + 1$.

It is well known that QR codes were good cyclic codes with high error-correcting capacity. In the past decades, many excellent studies concerning the algebraic methods to decode binary QR codes were presented in [1]-[3]. These decoding methods requires a vast calculation over the large finite field. This fact makes it difficult for software and hardware implementations. To solve them, the convolutional techniques of commonly used convolutional codes are considered for binary extended QR codes. In the late 1970s, Solomon and van Tilborg [4] developed that the binary (24, 12, 8) perfect Golay, (32, 16, 8), and (48, 24, 12) extended QR codes were shown to be convolutionally encoded with the small constraint lengths $K = 4,\ 4,\ 9$, respectively. Solomon in [5] has improved on the constraint length $K = 8$ for the extended QR code of length 48; moreover, Solomon and Jin [6] discovered the constraint lengths $K = 14$ and $K = 21$ for the (80, 40, 16) and (104, 52, 20) extended QR codes, respectively. Unfortunately, no satisfactory searching algorithm has been provided to confirm whether such a constraint length is the smallest value and the convolutional encoding way is unique for an extended QR code.

In this paper, programs written in C++ language is used to calculate the possible convolutional encoding of the five binary extended QR codes with lengths up to 80. It is shown in a simulation that the encoding of the extended QR code with length 24 (resp, 32, 48, 80) has the smallest constraint length $K = 4$ (resp., $K = 4$, 8, 14), which are the same results as given in [4]-[6]. The new convolutional encoding constructed for $K = 11$ is proposed for binary extended QR code with code length 72, which has not been investigated before. The convolutional encoding of the extended QR codes mentioned above with the smallest constraint length is listed in Section 3.

The remainder of this paper is organized as follows: Section 2 briefly reviews the convolutional encoding of binary extended QR codes of length 24 developed in [4]. In Section 3, the encoding techniques of some binary extended QR codes, which have not been encoded previously, are individually constructed by the smallest constraint length.

2 Preliminaries

In the (24, 12, 8) extended Golay code, a code polynomial $\bar{c}(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} + x^{23}$ is of weight 8 and is expressed as a sum of the generator polynomial $g(x)$ and the parity-check polynomial x^{23}, where $g(x) = \prod_{i \in Q}(x - \beta^i) = 1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$ is a code polynomial in the (23, 12, 7) Golay code and $Q = \{1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 9,\ 12,\ 13,\ 16,\ 18\}$. It is noticed that in the polynomial $g(x)$ except for $x^0 = 1$ term, the sets $S_Q = \{2,\ 4,\ 6\}$ and $S_N = \{5,\ 10,\ 11\}$ imply that $|S_Q| = |S_N| = 3$. Then, the code polynomial $g(x)$ can be constructed below. The polynomial $p(x) = 1 + x^2 + x^3$ is mapped into $x^{\phi(0)} + x^{\phi(2)} + x^{\phi(3)} = x^2 + x^4 + x^6$ through the mapping $\phi(i) = 2 \cdot 16^i \pmod{23}$; similarly, the polynomial $q(x) = 1 + x + x^3$, which is the reciprocal polynomial of $p(x)$, becomes $x^{\varphi(0)} + x^{\varphi(1)} + x^{\varphi(3)} = x^5 + x^{10} + x^{11}$ by $\varphi(i) =$

*Departments of Communication Engineering and Information Engineering, I-Shou University, Taiwan, R.O.C. Tel/Fax: 886-7-6577711 Email: {chongdao, truong, chenyan}@isu.edu.tw

$5 \cdot 16^i \pmod{23}$. Obviously, the constructed polynomial $c(x) = 1 + (x^2 + x^4 + x^6) + (x^5 + x^{10} + x^{11}) = g(x)$ is a code polynomial for the Golay code. As a consequence of the polynomials $p(x)$ and $q(x)$, the extended Golay code with its constraint length $K = 4$ is thus obtained.

It is a simulation on a computer that used the C++ language has been executed to search the possible convolutional encoding of 5 extended QR codes mentioned in this paper. The convolutional encoding of each extended QR code with the smallest constraint length is illustrated in the next section.

3 New Convolutional Encoding

This section illustrates the convolutional encoding techniques of binary extended QR codes for $23 \leq n \leq 80$, which are not published before. In each of the following codes, the code polynomial is constructed by using a technique similar to that given in the previous section.

3.1 (48, 24, 12) extended QR code

The convolutional encoding of this code with the smallest constraint length $K = 8$ having $p(x) = 1 + x^2 + x^5 + x^6 + x^7$ and $q(x) = 1 + x + x^2 + x^5 + x^7$ was found in [5]. In this code, however, another method is provided below. Let $p(x) = 1 + x^3 + x^4 + x^5 + x^7$ and $q(x) = 1 + x^2 + x^3 + x^4 + x^7$. The primitive polynomial $p(x)$ is mapped into $x^6 + x^9 + x^{12} + x^{16} + x^{18}$ by $\phi(i) \equiv 6 \cdot 17^i \pmod{47}$. The polynomial $x^{22} + x^{40} + x^{44} + x^{45} + x^{46}$ is obtained from $q(x)$ through $\varphi(i) \equiv 46 \cdot 17^i \pmod{47}$. As a result, the polynomial $1 + x^6 + x^9 + x^{12} + x^{16} + x^{18} + x^{22} + x^{40} + x^{44} + x^{45} + x^{46}$ is a code polynomial for the (47, 24, 11) QR code with generator polynomial $g(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^9 + x^{10} + x^{12} + x^{13} + x^{14} + x^{18} + x^{19} + x^{23}$.

3.2 (72, 36, 12) extended QR code

A full computer search shows in this code that there exists two ways to be convolutionally encoded for the constraint length $K = 11$.

Case 1: Let $p(x) = 1 + x + x^2 + x^4 + x^7 + x^8 + x^{10}$ and $q(x) = 1 + x^2 + x^3 + x^6 + x^8 + x^9 + x^{10}$ be the primitive polynomials. These two polynomials can be mapped into $c_1(x) = x^6 + x^8 + x^{10} + x^{16} + x^{20} + x^{25} + x^{45}$ and $c_2(x) = x^7 + x^{13} + x^{14} + x^{23} + x^{34} + x^{66} + x^{68}$ via $\phi(i) \equiv 16 \cdot 27^i \pmod{71}$ and $\varphi(i) \equiv 68 \cdot 27^i \pmod{71}$, respectively. The code polynomial $c(x) = 1 + c_1(x) + c_2(x)$ is of weight 15.

Case 2: Let the polynomials $p(x) = 1 + x^2 + x^3 + x^5 + x^6 + x^9 + x^{10}$ and $q(x) = 1 + x + x^4 + x^5 + x^7 + x^8 + x^{10}$. These two polynomials can be mapped into $c_1(x) = x^{20} + x^{24} + x^{25} + x^{29} + x^{30} + x^{45} + x^{49}$ and $c_2(x) = x^7 + x^{11} + x^{13} + x^{34} + x^{44} + x^{52} + x^{65}$ via $\phi(i) \equiv 45 \cdot 60^i \pmod{71}$ and $\varphi(i) \equiv 7 \cdot 60^i \pmod{71}$, respectively. The code polynomial $c(x) = 1 + c_1(x) + c_2(x)$ can thus be constructed.

The code polynomials $c(x)$ in both Case 1 and Case 2 are a multiple of the generator polynomial $g(x) = 1 + x + x^4 + x^5 + x^7 + x^8 + x^{13} + x^{17} + x^{24} + x^{25} + x^{26} + x^{27} + x^{28} + x^{33} + x^{35}$.

3.3 (80, 40, 16) extended QR code

The developed algorithm written in C++ language has been executed to determine that $K = 14$ is the smallest constraint length. There are two encoding ways. The first way is due to Solomon and Jin [6] that the polynomials $p(x) = 1 + x + x^2 + x^8 + x^9 + x^{11} + x^{13}$ and $q(x) = 1 + x^2 + x^4 + x^5 + x^{11} + x^{12} + x^{13}$ can construct the extended QR code with code length 80. The second way is to utilize the polynomials $p(x) = 1 + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 + x^{12} + x^{13}$ and $p(x) = 1 + x + x^5 + x^6 + x^7 + x^8 + x^9 + x^{11} + x^{13}$. The code polynomial $c(x) = 1 + (x^4 + x^8 + x^{11} + x^{18} + x^{19} + x^{25} + x^{36} + x^{49} + x^{67}) + (x^6 + x^{12} + x^{15} + x^{29} + x^{30} + x^{43} + x^{54} + x^{69} + x^{75})$ is constructed by using the mappings $\phi(i) \equiv 18 \cdot 32^i \pmod{79}$ and $\varphi(i) \equiv 15 \cdot 32^i \pmod{79}$, and $c(x)$ is a multiple of the generator polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^{11} + x^{13} + x^{14} + x^{16} + x^{18} + x^{19} + x^{20} + x^{21} + x^{24} + x^{25} + x^{26} + x^{27} + x^{29} + x^{30} + x^{31} + x^{35} + x^{36} + x^{39}$.

Acknowledgment

The work was supported by National Science Council, R.O.C., under Grants NSC97-2221-E-214-027-MY2.

References

[1] He R., Reed I.S., Truong T.K., Chen X., "Decoding the (47, 24, 11) quadratic residue code," *IEEE Trans on Inf. Theory*, V47, pp. 1181-1186, 3/01.

[2] Chang Y., Truong T.K., Reed I.S., Cheng H.Y., Lee C.D., "Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes," *IEEE Trans on Communs.*, V51, N9, pp. 1463-1473, 9/03.

[3] Elia M., Interlando J. C., "Quadratic residue codes and cyclotomic fields," *Acta Applied Math.*, V93, pp. 237-251, 06.

[4] Solomon G., van Tilborg H.C.A., "A connection between block and convolutional codes," *SIAM J. Applied Math.*, V37, N2, pp. 358-369, 10/79.

[5] Solomon G., "Convolutional encoding of self-dual codes," Jet Propulsion Laboratory, Pasadena, CA, *TDA Progress Report* 42-116, pp. 110-113, 2/94.

[6] Solomon G., Jin Y., "Convolutional encoding of self-dual block codes (II)," Jet Propulsion Laboratory, Pasadena, CA, *TDA Progress Report* 42-118, pp. 22-25, 8/94.