Convolutional Encoding of Self-Dual Block Codes (II)

G. Solomon[1]

Y. Jin[2]

Solomon and van Tilborg [2] have developed convolutional encoding algorithms for quadratic residue (QR) codes of lengths 48 and beyond. For these codes and reasonable constraint lengths, there are sequential decodings for both hard and soft decisions. There are also Viterbi type decodings that may be simple, as in a convolutional encoding/decoding of the extended Golay Code. In addition, the previously found constraint length K = *9 for the (48, 24; 12) QR code was lowered to* K = *8 by Solomon [1]. In our search for the smallest possible constraint lengths* K *for (80, 40; 16) self-dual quadratic residue and nonquadratic residue codes, we have found the constraint lengths* K = *14 and* K = *13, respectively. We have discovered a* K = *21 convolutional encoding for the (104, 52; 20) QR code; there may be a smaller* K *for a (104, 52; 20) self-dual code that is not a quadratic residue code. The smaller the* K*, the less complex the sequential or Viterbi decoder.*

I. (80, 40; 16) QR Code

The vector $(\mathbf{c_i})$ is a codeword of the $(79, 40; 15)$ QR code generated by check polynomial $g(x) = x^{40}+x^{39}+x^{37}+x^{35}+x^{32}+x^{29}+x^{28}+x^{24}+x^{22}+x^{18}+x^{17}+x^{16}+x^{15}+x^{13}+x^{12}+x^{11}+x^{6}+x^{4}+x^{3}+1$, where

$$\mathbf{c_i} = 1 \quad \text{for } i = 0, 1, 14, 15, 24, 30, 34, 35, 37, 39, 41,$$

$$43, 47, 53, 57, 58, 61, 66, 68, 69, 70, 71, 74$$

$$\mathbf{c_i} = 0 \quad \text{otherwise}$$

Let

[1] Independent consultant to the Communications Systems Research Section.

[2] Student at the California Institute of Technology, Pasadena, California.

$$f_i^{(1)} = c_{1\times 44^i}$$

$$f_i^{(2)} = c_{3\times 44^i} \quad \text{for } i = 0, 1, \cdots, 38$$

Then

$$f^{(1)}(x) = 1$$

$$\begin{aligned} f^{(2)}(x) = {} & x + x^2 + x^3 + x^6 + x^8 + x^{10} + x^{11} + x^{14} \\ & + x^{15} + x^{17} + x^{19} + x^{21} + x^{22} + x^{23} + x^{25} + x^{26} \\ & + x^{27} + x^{28} + x^{30} + x^{32} + x^{33} \end{aligned}$$

Since

$$f^{(2)}(x) = \frac{x^d q(x)}{p(x)} \pmod{x^{39} + 1}$$

where

$$q(x) = 1 + x^2 + x^4 + x^5 + x^{11} + x^{12} + x^{13}$$

$$p(x) = 1 + x + x^2 + x^8 + x^9 + x^{11} + x^{13}$$

$$d = 27$$

$$\gcd(p(x), x^{39} + 1) = 1$$

$$K = 14$$

By previous results in Solomon and van Tilborg [2], we can use $p(x)$ and $q(x)$ as taps in the convolutional encoder with the tail biting sequence of information of length 39. Appending the overall parity checks to the length 39 parity sequences and then adding the 40th information bit to the $p(x)$ sequence gives us the appropriate QR code. We have thus found an encoding with constraint length $K = 14$.

II. (80, 40; 16) Non-QR Code

On the other hand, let us use as the encoding taps the following polynomials in the convolutional encoder:

$$p(x) = 1 + x + x^2 + x^4 + x^5 + x^{10} + x^{12}$$

$$q(x) = 1 + x^2 + x^7 + x^8 + x^{10} + x^{11} + x^{12}$$

$$K = 13$$

Adjoining the parity checks to the parity sequences and then adding the 40th information bit to the $p(x)$ sequence as in Solomon [1], we construct a self-dual (80, 40; 16) block code. The minimum distance is verified by computer simulation. This code may not be the QR code.

III. (104, 52; 20) QR Code

The vector $(\mathbf{c_i})$ is a codeword of the (103, 52; 19) QR code generated by check polynomial $g(x) = x^{52} + x^{51} + x^{50} + x^{48} + x^{45} + x^{42} + x^{38} + x^{37} + x^{36} + x^{35} + x^{33} + x^{28} + x^{27} + x^{26} + x^{21} + x^{17} + x^{16} + x^{12} + x^{10} + x^8 + x^4 + x^3 + x^2 + 1$, where

$$\mathbf{c_i} = 1 \quad \text{for } i = 0, 1, 6, 10, 11, 12, 31, 37, 39, 43, 45, 47, 48, 53, 54, 73, 75, 85, 87, 88, 89, 99, 101$$

$$\mathbf{c_i} = 0 \quad \text{otherwise}$$

Let

$$f_i^{(1)} = c_{1\times 2^i}$$

$$f_i^{(2)} = c_{3\times 2^i} \quad \text{for } i = 0, 1, \cdots, 50$$

Then

$$f^{(1)}(x) = 1$$

$$f^{(2)}(x) = x + x^2 + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{12} + x^{19} + x^{21} + x^{26}$$
$$+ x^{29} + x^{30} + x^{31} + x^{36} + x^{38} + x^{43} + x^{44} + x^{46} + x^{48} + x^{50}$$

Since

$$f^{(2)}(x) = \frac{x^d q(x)}{p(x)} \pmod{x^{51} + 1}$$

where

$$q(x) = 1 + x^4 + x^5 + x^9 + x^{10} + x^{12} + x^{15} + x^{16} + x^{17} + x^{19} + x^{20}$$

$$p(x) = 1 + x + x^3 + x^4 + x^5 + x^8 + x^{10} + x^{11} + x^{15} + x^{16} + x^{20}$$

$$d = 30$$

$$\gcd(p(x), x^{51} + 1) = 1$$

$$K = 21$$

By Solomon and van Tilborg [2], we can use $p(x)$ and $q(x)$ above in the convolutional encoder. We have thus found an encoding with constraint length $K = 21$.

IV. Further Problems

(1) For any $(2n + 2, n + 1)$ QR code, does there exist a polynomial $f(x)$ such that 1 and $f(x)$ can be used as taps in the encoder?

(2) If (1) is true, do there exist a polynomial $p(x)$ and integer d with $\gcd(p(x), x^n + 1) = 1$ such that $f(x) \equiv (x^d q(x)/p(x)) (\mathrm{mod}\ x^n + 1)$, where $q(x) = x^{deg(p(x))} p(1/x)$?

(3) If (2) is true, find the smallest K with $\deg(p(x)) = K - 1$.

(4) If (2) is done, is there any non-QR $(2n + 2, n + 1)$ code that can be generated by some $p'(x)$ and $q'(x)$ with $\gcd(p'(x), x^n + 1) = 1$ and $\deg(p'(x)) \leq K - 1$?

References

[1] G. Solomon, "Convolutional Encoding of Self-Dual Codes," *The Telecommunications and Data Acquisition Progress Report 42-116, vol. October–December 1993*, Jet Propulsion Laboratory, Pasadena, California, pp. 110–113, February 15, 1994.

[2] G. Solomon and H. C. A. van Tilborg, "A Connection Between Block and Convolutional Codes," *Siam. J. Appl. Math.*, vol. 37, no. 2, pp. 358–369, October 1979.

[3] R. W. D. Booth, M. A. Herro, and G. Solomon, "Convolutional Coding Techniques for Certain Quadratic Residue Codes," *Proceedings of the International Telemetering Conference (XI)*, Silver Springs, Maryland, 1975.