Convolutional Encoding of Self-Dual Codes

G . Solomon [1]

Beverly Hills, CA

Abstract

Self-dual block codes of rate 1/2 are constructed here. The codes are of length $8m$ with weights w, $w =$ O mod 4. The codes have a convolutional portion of length $8m - 2$ and non-systematic. information length $4m - 1$. The last two bits arc parity checks on the two $(4m - 1)$ length parity sequences. The final information bit complements onc of the extended parity sequences of length $4m$. Solomon and Van Tilborg [I] have developed algortihms to generate these for the quadratic residue codes of lengths 24 and beyond. For reasonable constraint lengths, there arc Viterbi type decodings possible that may be simple as in the convolutional encoding/decoding of the extended Golay Code [2]. In addition, the $K = 9$ constraint length for the QR (48, 24;12) code found in [I] is lowered here to K = 8.

I. THEOREM

Let $n = 4m - 1$. We may construct a block code of rate 1/2 of length $2(n + 1)$ with weights multiples of 4 as follows.

1. The portion of length 2n is convolutionally generated by a K stage register $p(x)$ and $q(x)$ of degree K-1 whose entries are n +- K-1 bits long with the first and last (K-1) bits identical. Two parity sequences, each of length 12 arc non-systematically generated, onc for each polynomial.

2. An additional 2 bits arc adjoined as overall parity checks 011 the n bit parity sequences. The $(n + 1)^{th}$ information bit is added to each bit of the $p(x)$ parity sequence.

3. The encoder polynomials $p(x)$ and $q(x)$ of degree 1{-1. arc related thusly: $q(x) = x^{K-1}p(x^{-1})$

Proof

The proof uses the Solomon-McEliece Γ_2 Formula [3] 011 the Mattson-Solomon (MS) representation of the even weight parity sequences of lengths n = 4111-1 generated by $p(x)$ and $q(x)$. Using the relationship of $p(x)$ to $q(x)$, one obtains equality of Γ_2 for the two sequences. Treating odd weight parity sequences as complements of the all-one parity sequence, one sees that extending the lengths by even parity again gives even weights $w, w = 0$ mod 4. Note too that the complementing of onc extended sequence preserves the weight property.

11. NEW CONSTRUCTION OF A QR (48, 24;] 2) CODE

In this section wc introduce an improved construction of the (48,24;1 2) Quadratic Residue Code that requires a convolutional encoding of Ii' = 8 stages instead of $K = 9$ as in Solonlol~-vail Tilborg, [1].

Let n = 23, K = 8, $p(x) = x^7 + x^6 + x^5$ +- x^2 +- 1 and *q(r)* $= x^7 + x^5 + x^2 + x + 1$. Apply the construction in the theorem above to obtain a self-dual (48,24 ;12) code. J'his is the (48,24 ;12) Quadratic Residue code.

For, if the check polynomial for the QR code in powers of x is 0,1,4,6,9,12,13,15,16,19, 20, 24, one may generate a codeword at coordinates 0,2,5,6,7,13,15,22,23,28,37, (in powers of say /3 so that $Tr\beta = 1$, a 47^{th} root of unity). The overall parity check bit is given by $x =$ O. The coordinates 2,6,7,28,37 may be identified with the quadratic residue points with $x = 1$, the 0^{th} power coordinate the overall parity check on the trace one or QR points. elements the trace zero elements, excepting $x = 0$, The coordinates 5,13,15,22,23 then arc non QR points with $x =$ O as parity. In powers of 4 starting with 37 onc gets (37 728 18256242 . . . . onc gets O 1 257 as an ordering. Similarly the non quadratic residues in powers of 4, starting with 22 are (22 41 23 45 39 15 13 5 . . ., one gets 0 2 5 6 7 as an ordering. Thus if wc choose $p(x) = x^7 + x^5 + x^2 + x + 1$ and $q(x) = x^7 + x^6 + x^5 + x^2 + 1$, this will generate a convolutional portion of length 46. Adding the overall parity checks yields the QR code. Thus K = 8.

III. VITERBI DECODING

This requires two decodings as in [2]. Assume the received $p(x)$ sequence has not been complemented. i.e., the 24th information bit is zero. As onc dots not know the initial 7 bits, onc may take the received encoded sequences, repeat 3 or 4 times and attach then) cad to end. Now Viterbi decode as if wc started in tbc middle. Use the parity information to Lake advantage of Hamming distance 12. Alternately assume that the $p(x)$ sequence has been complemented, and do the obvious decoding.

REFERENCES

[1] G. Solomon and H.C.A. van Tilborg, "A Connection Between Block and Convolutional Codes" SIAM J. APPL. MATH Vol. 37 No. 2 Oct. 1979 pp 358-369.

[2] R.W.D. Booth, M. A. Herro and G. Solomon, "Convolutional coding techniques for certain quadratic residue codes" International Telemetering Conferen ccc, (XI) Proceedings (Silver Springs, Maryland 1975

[3] G. Solomon and J{. J. McEliece, "Weights of Cyclic Codes," Journal of Combinatorial Theory, vol. 1, no. 4, pp. 459-475, December 1966

[1] This work was performed by the author while acting as a consultant to the Jet l’repulsion Laboratory, California Institute of Technology, under contract to the National Aeronautics and Space Administration