A connection between block and convolutional codes

SIAM J. APPL. MATH.
Vol. 37, No. 2, October 1979

0036-1399/79/3702-0014 $01.00/0

A CONNECTION BETWEEN BLOCK AND CONVOLUTIONAL CODES*

G. SOLOMON† AND H. C. A. VAN TILBORG‡

Abstract. Convolutional codes of any rate and any constraint length give rise to a sequence of quasi-cyclic codes. Conversely, any quasi-cyclic code may be convolutionally encoded. Among the quasi-cyclic codes are the quadratic residue codes, Reed–Solomon codes and optimal BCH codes. The constraint length K for the convolutional encoding of many of these codes (Golay, (48, 24) QR, etc.) turns out to be surprisingly small. Thus using the soft decoding techniques for convolutional decoding we now have a new maximum likelihood decoding algorithm for many block codes. Conversely an optimal quasi-cyclic code will yield a convolutional encoding with optimal local properties and therefore with good infinite convolutional coding properties.

Introduction. This paper is divided into 3 sections. In the first section we establish a relation between quasi-cyclic codes and convolutional codes. Let $i_0, i_1, \cdots, i_{n-1}$ be the first n information symbols of a rate $\frac{1}{2}$ convolutional code with constraint length K. If we stipulate that the next $(K-1)$ information symbols coincide with the first $(K-1)$ information symbols (i.e. $i_0, \cdots, i_{K-2}$), then the resulting $2n$ output symbols form a quasi-cyclic code. Conversely a quasi-cyclic code is shown to be convolutionally encodable. Our main thrust here is to minimize the constraint length K. We end the section by observing that the preceding results apply to any rate k/n convolutional (resp. quasi-cyclic) code.

In § 2 we extend the notion of quasi-cyclic codes and obtain a modified convolutional encoding, allowing us to include a larger class of codes. It also allows us to obtain a small constraint length K. Among the codes in this category are the quadratic residue codes, the Reed–Solomon codes, optimal BCH codes and many extended cyclic codes. One obvious advantage of this is a new maximum likelihood (soft and hard decision) decoding of these codes using convolutional decoding techniques. We illustrate the above by giving various examples, most notably a 4-stage convolutional encoding of the binary Golay (24, 12) code.

Finally in § 3, we present tables of rate $\frac{1}{2}, \frac{1}{3}$ and $\frac{2}{3}$ block codes and their convolutional encoding.

One can use § 6 in Chap. 16 of [4] as a starting reference to quasi-cyclic codes and references [3] and [6] to convolutional codes and their decoding.

1. From convolutional to quasi-cyclic codes and back. Let us consider a convolutional code (binary or nonbinary) of rate $\frac{1}{2}$ with constraint length K. The taps are described by the polynomials

$$p(x) = \sum_{i=0}^{K-1} p_i x^i \quad \text{and} \quad q(x) = \sum_{i=0}^{K-1} q_i x^i,$$

where $(p_0, q_0) \neq (0, 0)$ and $(p_{K-1}, q_{K-1}) \neq (0, 0)$. (See Fig. 1.) Let n be an integer. We shall only consider input sequences of the form $i_{-K+1}, \cdots, i_{-1}, i_0, i_1, \cdots, i_{n-1}$, where $i_{-j} = i_{n-j}$, for $1 \leqq j \leqq K-1$, i.e., sequences of length $n+K-1$, in which the first $K-1$ symbols are repeated at the end.

* Received by the editors August 2, 1977 and in final revised form October 24, 1978. This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, supported by the National Aeronautics and Space Administration under Contract NAS 7-100.

† Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91125.

‡ Department of Mathematics, Technological University of Eindhoven, Eindhoven, the Netherlands.

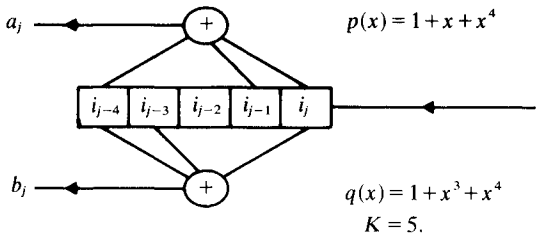

FIG. 1. *Binary convolutional code with* $K = 5$.

The two output sequences depend on the input sequence in the following way:

$$a_j = \sum_{l=0}^{K-1} p_l i_{j-l}, \qquad 0 \leqq j \leqq n-1,$$

$$b_j = \sum_{l=0}^{K-1} q_l i_{j-l}, \qquad 0 \leqq j \leqq n-1.$$

This is a trellis code with the same initial and final encoder states taking on any possible value (as opposed to the all zero state)! This fact is used to great effect in decoding (see the end of this section). Turning back to our notations we see that in terms of polynomials, we have, writing

$$i(x) = \sum_{l=0}^{n-1} i_l x^l, \quad a(x) = \sum_{l=0}^{n-1} a_l x^l \quad \text{and} \quad b(x) = \sum_{l=0}^{n-1} b_l x^l,$$

the relations

$$\begin{aligned} a(x) &\equiv i(x)p(x) \pmod{x^n - 1}, \\ b(x) &\equiv i(x)q(x) \pmod{x^n - 1}. \end{aligned} \tag{1.1}$$

In vector notation, this comes down to

$$(i_0, i_1, \cdots, i_{n-1})(P \mid Q) = (a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{n-1}),$$

where P and Q are $n \times n$ circulants with top row $(p_0, p_1, \cdots, p_{k-1}, 0, \cdots, 0)$, respectively $(q_0, q_1, \cdots, q_{k-1}, 0, \cdots, 0)$.

From the observations above it follows that the codewords from our convolutional code are the codewords in the linear code generated by the matrix

$$G = (P \mid Q).$$

Codes of this form are called *quasi-cyclic* codes. The rank of this matrix is easily determined by the following theorem, well known from the theory of algebra.

THEOREM 1.1. *Let* $p(x)$ *and* $q(x)$ *be two polynomials of degree at most* $n-1$ *and* P *and* Q *the associated circulants. Then*

$$\text{rank } (P \mid Q) = n - \textit{degree of } \text{g.c.d. } (p(x), q(x), x^n - 1).$$

Proof. Let $f(x) = \text{g.c.d. } (p(x), q(x), x^n - 1)$. Moreover let $i(x) = \sum_{l=0}^{n-1} i_l x^l$. Then

$$(i_0, \cdots, i_{n-1})(P \mid Q) = (0, \cdots, 0 \mid 0, \cdots, 0) \tag{1.2}$$

iff $i(x)p(x) \equiv i(x)q(x) \equiv O(\text{mod } x^n - 1)$, i.e., iff $i(x)$ is divisible by $(x^n - 1)/f(x)$. So the dimension of the subspace of vectors $(i_0, \cdots, i_{n-1})$ satisfying (1.2) equals the degree of f. Therefore, the rank of $(P \mid Q)$ is n-degree f. □

Example 1.2. The binary code with $n=7$, $p(x)=1+x+x^3$, $q(x)=1+x^2+x^3$. Single g.c.d. $(p(x), q(x), x^7-1)=1$, one has

$$\text{rank } (P|Q)=7.$$

Of specific interest are quasi-cyclic codes with generator matrix

$$(I|F),$$

where I is the $n\times n$ identity matrix and F a circulant with top row $(f_0, \cdots, f_{n-1})$ (associated with the polynomial $f(x)=\sum_{i=0}^{n-1} f_i x^i$). Obviously such a code is systematic on the first n positions.

THEOREM 1.3. *Let $p(x)$ and $q(x)$ be two polynomials of degree at most $n-1$ and let P and Q be the associated circulants. Then the code C generated by $(P|Q)$ can also be generated by $(I|F)$, where F is a circulant, iff $(p(x), x^n-1)=1$. In this case $q(x)\equiv f(x)p(x) \pmod{x^n-1}$.*

Proof. $(1|f(x))$ is in the code iff there is a polynomial $i(x)$ such that $(i(x)p(x), i(x)q(x))\equiv(1, f(x))(\text{mod } x^n-1)$, i.e., iff $p(x)$ has an inverse $(\text{mod } x^n-1)$, i.e., iff g.c.d. $(p(x), x^n-1)=1$. Clearly in this case $i(x)=(p(x))^{-1}$ and $q(x)\equiv p(x)f(x) \pmod{x^n-1}$. □

Remark. From $q(x)\equiv f(x)p(x)(\text{mod } x^n-1)$ and (1.1) it follows that $b(x)\equiv f(x)a(x)(\text{mod } x^n-1)$.

Example 1.4. $p(x)=1+x+x^2$, $q(x)=1+x^2$, $n=7$. In this case $(p(x), x^7-1)=1$. One can find $f(x)$ by the Euclidean algorithm. It turns out that $f(x)=x+x^3+x^4+x^6$.

From a convolutional coding point of view one wants the encoding register to have few stages. In other words, the maximum degree of $p(x)$ and $q(x)$ should be small. So we now look at the reverse problem. Given a code C generated by $(I|F)$ where F is a circulant associated with a polynomial $f(x)$, find polynomials $p(x)=\sum_{i=0}^{K-1} p_i x^i$, $q(x)=\sum_{i=0}^{K-1} q_i x^i$, $(p_0, q_0)\neq(0, 0)$, $(p_{K-1}, q_{K-1})\neq(0, 0)$ such that $(P|Q)$ generates the same code C (where P and Q are the circulants associated with $p(x)$ and $q(x)$). For this we rephrase a theorem that can be found in J. J. Bussgang [2].

THEOREM 1.5. *For every integer n and polynomial $f(x)=\sum_{i=0}^{n-1} f_i x^i$, there exist polynomials $p(x)=\sum_{i=0}^{K-1} p_i x^i$, $q(x)=\sum_{i=0}^{K-1} q_i x^i$ such that $q(x)\equiv f(x)p(x) \pmod{(x^n-1)}$, $K\leqq\lceil(n+1)/2\rceil$, $(p_0, q_0)\neq(0, 0)$ and $(p_{K-1}, q_{K-1})\neq(0, 0)$.*

Proof. Look at the coefficients p_i as variables. Since we want the coefficient of x^l in $q(x)\equiv f(x)p(x)(\text{mod } x^n-1)$ to be zero for $l\geqq K$, we need a nontrivial solution of the equations

$$\begin{aligned}
&x^{n-1}\colon\ p_0 f_{n-1}+p_1 f_{n-2}+\cdots+p_{K-1} f_{n-K} &&=0\\
&x^{n-2}\colon\ p_0 f_{n-2}+p_1 f_{n-3}+\cdots+p_{K-1} f_{n-K-1} &&=0\\
&\quad\vdots\\
&x^{K}\colon\ \ p_0 f_K+p_1 f_{K-1}+\cdots+p_{K-1} f_1 &&=0.
\end{aligned}\tag{1.2}$$

For $K=\lceil(n+1)/2\rceil$ one has more unknowns than relations, which guarantees a nontrivial solution $p(x)$. One computes $q(x)$ from $q(x)\equiv f(x)p(x)(\text{mod } x^n-1)$. The condition $(p_0, q_0)\neq(0, 0)$ can be met by repeatedly dividing $p(x)$ and $q(x)$ by x if necessary. If $(p_{K'+1}, q_{K'-1})=\cdots=(p_K, q_K)=(0, 0)$ for some $K'<K$ in this solution and $(p_{K'}, q_{K'})\neq(0, 0)$, then we have to replace K by K'. □

One should realize however that the polynomials $p(x)$ and $q(x)$ obtained from Theorem 1.5 do not necessarily have the property g.c.d. $(p(x), q(x), x^n-1)=1$. On the other hand each solution $(p(x), q(x))$ with max degree $(p(x), q(x))\leqq\lceil(n-1)/2\rceil$ is a solution of (1.2) and can be obtained from Theorem 1.5.

However if one accepts equivalent codes, one may possibly find small degree polynomials $p(x)$ and $q(x)$, with g.c.d. $(p(x), q(x), x^n - 1) = 1$, by applying Theorem 1.5 to the codes obtained from the following theorem.

THEOREM 1.6. *Let C_1 and C_2 be two quasi-cyclic codes of length $2n$, generated by $(1, f_1(x))$, respectively $(1, f_2(x))$. Then C_1 and C_2 have the same weight enumerator if any of the following relations holds*:

(i) $f_2(x) \equiv x^l f_1(x) \pmod{(x^n - 1)}$, $0 \leqq l \leqq n-1$,

(ii) $f_2(x) \equiv f_1^{-1}(x)$, *where* $(f_1(x), x^n - 1) = 1$,

(iii) $f_2(x) = f_1(x^l) \pmod{x^n - 1}$, *where* $(l, n) = 1$.

Proof. Let $w(a(x), b(x))$ denote the sum of the weights of the vectors $(a_0, \cdots, a_{n-1})$ and $(b_0, \cdots, b_{n-1})$ associated with $a(x)$ and $b(x)$.

(i) $w(i(x), i(x)f_2(x)) = w(i(x), i(x)x^l f_1(x)) = w(i(x), i(x)f_1(x))$.

(ii) Since $(1, f_1) = f_1(f_2, 1)$ and $(f_2, 1) = f_2(1, f_1)$ the codes generated by $(1, f_1)$ and $(f_2, 1)$ are the same. So (ii) follows from the obvious equivalence of the codes generated by $(1, f_2)$ and $(f_2, 1)$.

(iii) Since $(l, n) = 1$, for each $i(x)$ there exists a polynomial $j(x)$ such that $j(x^l) \equiv i(x) \pmod{x^n - 1}$.

Moreover multiplying by l mod n gives a permutation of the integers $0, 1, \cdots, n-1$. So

$$w(i(x), i(x)f_2(x)) = w(i(x), i(x)f_1(x^l)) = w(j(x^l), j(x^l)f_1(x^l))$$
$$= w(j(x), j(x)f_1(x)). \qquad \square$$

By means of Theorems 1.5 and 1.6 one can try in individual cases to find code generators with small constraint length. In general we cannot say anything about the minimum value of K, but for certain classes of codes we can and shall do this (in § 2).

Table 1 (see § 3) gives a list of code generators $p(x)$ and $q(x)$ (and $f(x)$) for $n \leqq 21$. The number d stands for the minimum distance and K for the constraint length. Of course there is no reason to restrict ourself to $(2n, n)$ quasi-cyclic codes. A rate k/n convolutional encoder with input sequences $(\mathbf{i}_1, \cdots, \mathbf{i}_k)$, where $\mathbf{i}_j = (i_{j,-K+1}, \cdots, i_{j,-1}, i_{j,0}, i_{j,1}, \cdots, i_{j,n-1})$, $1 \leqq j \leqq k$, corresponds to a linear code (nm, km) code with constraint length K and generator matrix:

$$G = \begin{pmatrix} P_{11} & P_{12} & \cdots & P_{1n} \\ P_{k1} & P_{k2} & \cdots & P_{k,n} \end{pmatrix},$$

where P_{ij} is a $m \times m$ circulant.

In general it remains a problem to go beyond the existing bounds on the minimum distance of such a code. Tables 2 and 3 list some rate $\frac{1}{3}$ and $\frac{2}{3}$ codes, by the polynomials $p_{ij}(x)$ associated with P_{ij}.

Decoding. A quasi-cyclic code may be encoded convolutionally. Consequently it may be decoded by convolutional decoding techniques. The usual convolutional code is a trellis code with zeros in the first and last $(K-1)$ positions of the encoder.

The trellis codes here begin and end with the same binary $(K-1)$ tuple which is not necessarily zero. Thus any hard or soft decoding algorithm, e.g., Viterbi, Fano sequential, etc., may be adapted to decode the block codes here. In particular if one knew the initial $(K-1)$ entries, then the technique would be identical in complexity. For each possible $(K-1)$ tuple, one can perform a decoding, and then choose the most likely candidate under the decoding criterion used.

A Viterbi decoding for constraint length 4 was applied 8 times in the maximum likelihood decoding of the Golay (24, 12; 8) code by Booth, Herro and Solomon [1]. The Golay code (as seen in the next section) can be made to exhibit a quasi-cyclic

structure. Now 2^{K-1} decodings for large K is prohibitive. Possible research areas for soft decoding would be in the sequential decoding techniques tailored for the finite lengths considered.

Another technique would be to continuously recycle the received word and decode it as a long convolutional codeword. When the decoded word exhibits the correct periodicity (say, over length $3K$ or $4K$) we accept the decoding.

The way is open for simplified maximum likelihood decoding of many block codes.

2. Cyclic codes through convolution. In § 1 we related convolutional codes to quasi-cyclic codes and demonstrated the inherent duality between them. A quasi-cyclic code may be encoded and consequently *decoded* convolutionally. In this section, we treat several families of cyclic codes and look for a quasi-cyclic structure. We first extend our concept of quasi-cyclic codes.

DEFINITION 2.1. (I) The pure quasi-cyclic codes of the form $(P \mid Q)$ will be called of type A_0.

(ii) If one adjoins an overall parity bit on P and/or Q the code will be of type A_1.

(iii) If one increases the dimension of a type A_1 code by adjoining one row to its generator matrix we will call it a code of type A_2.

We find that many important codes fit neatly into this "messy" characterization. The results are as follows:

I. All extended quadratic residue codes are of type A_2 (as well as A_1). The binary Golay code is encodable by a convolutional encoder with constraint length 4.

II. There exist a class of Reed–Solomon and optimal[1] nonbinary BCH codes of type A_0. The $p(x)$, $q(x)$, and K developed when used for pure convolutional coding guarantee optimality for K and the field used, $K = d/2$ for rate $\frac{1}{2}$.

III. Almost all good binary codes of small length, with various rates are seen to be of one of the types above. See Tables 1, 2 and 3.

2.1. Quadratic residue codes.

THEOREM 2.2. *Let U be the extension by an overall parity bit of the $(2n+1, n+1)$ binary quadratic residue code generated by $f_{QR}(x) = \prod_{i \in QR}(x + \alpha^i)$, where $QR = \{j^2 \pmod{2n+1} \mid 1 \leqq j \leqq 2n\}$ and $2n+1$ is a prime of the form $8l \pm 1$. Then U is of type A_2. Furthermore the $(2n+1, n)$ code generated by $f_{QR}(x)(x+1)$ is of type A_1 and the shortened $(2n, n)$ code obtained by eliminating the first digit is of type A_0.*

Remark. In fact, by choosing the proper $(2n+1, n)$ subcode or U, one can sometimes find a type A_0 code with smaller K (e.g., Golay (24, 12), QR(32, 16), QR(48, 24) code). This technique of construction may be applied to other cyclic codes to see if they are of any of the types A_i, and thus amenable to maximum likelihood convolutional decoding techniques.

Note. In the book by F. J. MacWilliams and N. J. A. Sloane [4, Chap. 16, § 6] it is shown that all $(2n+2, n+1)$ extended quadratic residue codes are of type A_0. So by our earlier results they have a convolutional encoding. However, the convolution found with our methods gives rise to a smaller K and uniform degrees of $p(x)$ and $q(x)$, making these codes suitable for standard convolutional encoding and decoding. Thus the maximum likelihood decoding properties are predictable by analogy with the simulated results of convolutional codes with these constraints.

Proof of Theorem 2.2. Consider the $(2n+1, n+1)$ extended quadratic residue code U. We have

$$x^{2n+1} + 1 = (x+1) f_{QR}(x) f_{NQR}(x)$$

[1] An (n, k, d) code with $d = n - k + 1$.

where

$$f_{\mathrm{NQR}}(x)=\prod_{i\in \mathrm{NQR}}(x+\alpha^i), \qquad \mathrm{NQR}=\{1\leqq j\leqq 2n \mid j\notin \mathrm{QR}\}.$$

Let α be a primitive $(2n+1)$th root of unity. The codeword $\mathbf{u}\in U$, corresponding to $u(x)=\sum_{i=0}^{2n} u_i x^i$ where $u(x)$ is divisible by $f_{\mathrm{QR}}(x)$, can also be described in terms of Mattson–Solomon polynomials [5]

$$g_{\mathbf{u}}(z)=c_0+\sum_{i\in \mathrm{QR}} c_i z^i,$$

where

$$c_0\in \mathrm{GF}(2), \qquad c_i\in \mathrm{GF}(2^m) \quad \text{for } i\in \mathrm{QR}$$

and for all i

$$c_{2i}=c_i^2, \quad \text{here } 2i \text{ is taken (mod } 2n+1),$$

and m is the multiplicative order of 2(mod $2n+1$).

Now $\mathbf{u}=(u_i)$, $i=0, 1, \cdots, 2n, \infty$, is given by

$$u_i=g_{\mathbf{u}}(\alpha^i), \qquad i=0, 1, \cdots, 2n,$$
$$u_\infty=g_{\mathbf{u}}(0).$$

We can also choose NQR as the index set for i and obtain an equivalent code. Let the integer j be a multiplicative generator of the quadratic residues of $(2n+1)$, i.e., $j^n\equiv 1(\mathrm{mod}\ 2n+1)$ and $\{j^i\}$ runs through QR. Clearly, $n=me$ for some e. if $e=1$, then 2 can be chosen for j and $f_{\mathrm{QR}}(x)$ is irreducible. One may also write

$$g_{\mathbf{u}}(z)=c_0+\sum_{i=0}^{e-1} \mathrm{Tr}\, c_i z^{j^i}.$$

Here the trace Tr is defined by $\mathrm{Tr}\, y=\sum_{i=0}^{m-1} y^{2^i}$. This corresponds to the factorization of

$$f_{\mathrm{QR}}(x)=\prod_{i=0}^{e-1} f_{j^i}(x)$$

where $f_{j^i}(x)$ is the irreducible polynomial of degree m with α^{j^i} as a root. By the normal base theorem (see [4, Chap. 4, § 9]) we can choose $c\in \mathrm{GF}(2^m)$, such that the set $\{c, c^2, c^4, \cdots, c^{2^{m-1}}\}$ is a basis for $\mathrm{GF}(2^m)$. Then $\mathrm{Tr}\, c=1$. Let $\mathbf{v}=(\mathrm{Tr}\, cz: z=\alpha^i, 0\leqq i\leqq 2n)$. Recall that α is a primitive $(2n+1)$th root of unity. For convenience we choose α such that $\mathrm{Tr}\, \alpha=1$. Let r be in NQR; we may write $\mathrm{NQR}=\{rj(\mathrm{mod}\ 2n+1)\mid j\in \mathrm{QR}\}$. Define the digits (p_i) and (q_i) by

$$p_i=\mathrm{Tr}\, c\alpha^{j^i}, \qquad i=0, 1, \cdots, n-1,$$
$$q_i=\mathrm{Tr}\, c\alpha^{rj^i}, \qquad i=0, 1, \cdots, n-1,$$
$$p_\infty=\sum_{i=0}^{n-1} p_i=\sum \mathrm{Tr}\, c\alpha^{j^i},$$
$$q_\infty=\sum_{i=0}^{n-1} q_i=\sum \mathrm{Tr}\, c\alpha^{rj^i}.$$

Clearly if $\sum_{i=0}^{n-1}\alpha^{j^i}=1$, then $p_\infty=v_0=1$; $q_\infty=v_\infty=0$, otherwise $p_\infty=v_\infty$, $q_\infty=v_0$.

By setting $p_i' = p_{i-1}$, $q_i' = q_{i-1}$, $p_\infty' = p_\infty$, $q_\infty' = q_\infty$, we generate a new sequence which is a cyclic shift to the right of the (p_i), (q_i) sequences. This corresponds to

$$p_i' = \operatorname{Tr} c(\alpha^{ji})^{j^{-1}}, \qquad q_i' = \operatorname{Tr} c(\alpha^{ri^i})^{j^{-1}}$$

or having taken

$$\mathbf{v}' = (\operatorname{Tr} cz^{j^{-1}} \mid z = 0, z = \alpha^i, 0 \leqq i \leqq 2n).$$

The permutation of the coordinates $z \to z^{j^{-1}}$, with orbits $\{\infty\}$, $\{0\}$, QR and NQR, takes the vector $(\operatorname{Tr} cz)$ into $(\operatorname{Tr} cz^j)$, which is also a codeword of the QR code as can be seen from the expression for $g_{\mathbf{u}}(z)$. We label the code automorphism induced by the coordinate permutation above T.

Similarly T^k is the code automorphism corresponding to the kth cyclic shift to the right of the (p_i), (q_i) sequences. The corresponding coordinate permutation is $z \to z^{j^{-k}}$.

We now show that every codeword of the QR code with $c_0 = 0$ is obtainable by linear combinations of the cyclic shifts of the (p_i), (q_i) sequences. Let $c' \in \mathrm{GF}(2^m)$. Since both j^e and 2 have multiplicative order $m \pmod{2n+1}$ it follows that the map T^e takes $\operatorname{Tr} cz$ into $\operatorname{Tr} cz^{2^s}$ for some s. Similarly T^{2e} takes $\operatorname{Tr} cz$ into $\operatorname{Tr} cz^{2^s}$, etc. Since

$$\{c^{2^{i \cdot s}} \mid 0 \leqq i \leqq m-1\} = \{c^{2^i} \mid 0 \leqq i \leqq m-1\}$$

and the latter forms a basis of $\mathrm{GF}(2^m)$, we can write $c' = \sum_{i=0}^{m-1} h_i c^{2^{i-s}}$, $h_i \in \mathrm{GF}(2)$.

Define the operator

$$\tilde{T} = \sum_{i=0}^{m-1} h_i T^{i \cdot e}.$$

Then $\tilde{T}\mathbf{v}$ is a linear combination of shifts of the (p_i), (q_i) sequences. We see that $\tilde{T}\mathbf{v} = \{\operatorname{Tr} c'z\}$. Similarly $\tilde{T}T^i\mathbf{v} = \operatorname{Tr} c'z^{j^{-1}}$ for any i. Thus the quasi-cyclic code (p_i, q_i) is of type A_0 and $(p_i, q_i, p_\infty, q_\infty)$ is of type A_1. Adjoining the all-one vector corresponding to $c_0 = 1$ gives the entire QR code.

An alternate choice for the $(2n+1, n)$ subcode is effected by choosing a different $\mathbf{u}$ to generate the initial (p_i), (q_i) sequences. Choose $c \neq 0$ such that $\operatorname{Tr} c = 0$ and define $\mathbf{u} = (u_i)$ by the rule

$$u_i = 1 + \operatorname{Tr} c\alpha^i, \qquad 0 \leqq i \leqq 2n,$$

$$u_\infty = 1.$$

Let $d, d^2, d^4, \cdots, d^{2^{m-1}}$ span the $(m-1)$-dimensional subspace consiststing of the trace zero elements of $\mathrm{GF}(2^m)$ (take for example $d = c + c^2$, where $\{c^{2^i}, 0 \leqq i \leqq m-1\}$ spans $\mathrm{GF}(2^m)$). With the map T defined as before, one can easily show that the operator $\tilde{T} = \sum_{i=0}^{n-1} e_i T^i$, with $e_i \in \mathrm{GF}(2)$, yielding a linear combination of the permutated vectors, gives rise to all vectors of the form

$$c_0 + \sum_{i=0}^{e-1} \operatorname{Tr} c_i z^{ji},$$

where $\operatorname{Tr} \sum_{i=0}^{e-1} c_i = 0$ and $c_0 \in \mathrm{GF}(2)$.

Adjoining a vector $\sum_{i=0}^{e-1} \operatorname{Tr} f_i x^{ji}$, where $\operatorname{Tr} f_i = 1$ for each i, will give us any vector of the QR code. It is this alternate construction we use to obtain a constraint length of $K = 4$ for the (24, 12; 8) and (32, 18; 8) quadratic residue codes.

We now give a convolutional encoding of these two codes and follow with an immediate justification.

(24, 12; 8) *Golay code.*

Encoding. Information $i_0, i_1, i_2, \cdots, i_{11}$.

Consider i_0, and $i_1, i_2, \cdots, i_{11}$ separately, where $i_{-j} = i_{11-j}$ for $1 \leqq j \leqq 3$. (See Fig. 2.)

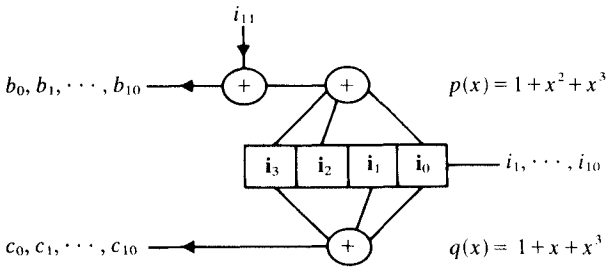

FIG. 2

Then $a_\infty = i_0 + i_1 + \cdots + i_{11} = \sum a_i$; $b_\infty = i_1 + i_2 + \cdots + i_{11} = \sum b_i$. We obtain $a_0, b_0, a_1, b_1, \cdots, a_{10}, b_{10}, a_\infty, b_\infty$.

(32, 16; 8) *quadratic residue code.*

Encoding. Information $i_0, i_1, \cdots, i_{15}$.

Consider i_{15}, and $i_0, i_1, \cdots, i_{14}$ separately.

Run $i_{12}, i_{13}, i_{14}, i_0, i_1, \cdots, i_{14}$ into same encoder (4-stage);
$p(x) = 1 + x^2 + x^3$;
$q(x) = 1 + x + x^3$;

as for the Golay code. Encode and decode exactly as in the Golay case. We shall now justify these assertions.

For the (24, 12; 8) *Golay code.* The vector $(10101110001100000000) = (c_i)$ is a codeword in the (23, 12; 7) Golay code with generator polynomial $x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$. Let

$$p_i = c_{2 \cdot 16^i}, \qquad q_i = c_{5 \cdot 16^i}$$

$$p_\infty = c_0; \qquad q_\infty = c_\infty.$$

Let $p(x) = \sum_{i=0}^{10} p_i x^i$, $q(x) = \sum_{i=0}^{10} q_i x^i$. This yields the $p(x)$ and $q(x)$ in the encoder. The vectors obtained by this encoding are of form

$$(d_0 + \operatorname{Tr} cz) \quad \text{where } \operatorname{Tr} c = 0, \quad d_0 \in \mathrm{GF}(2).$$

A cyclic shift of the p_i and q_i corresponds to the automorphism $T: z \to z^{16}$ of the code. $i_0 = 1$ gives us the Tr z vector to give the total dimension 12.

For the (32, 16; 8) QR *code.* Let

$$f(x) = (x+1) \prod_{i \in \mathrm{QR}} (x + \alpha^i) = (x+1) f_{\mathrm{QR}}(x).$$

Since QR = {1, 2, 4, 8, 16, 5, 10, 20, 9, 18, 7, 14, 28, 25, 19},

$$f_{\mathrm{QR}}(x) = (x+1)(x^5 + x^2 + 1)(x^5 + x^4 + x^2 + x + 1)(x^5 + x^3 + x^2 + x + 1)$$

with α a root of $x^5 + x^2 + 1$. $T: z \to z^7$ gives rise to a sequence in powers of α

$$1, 7, 18, 2, 14, 5, 4, 28, 10, 8, 25, 20, 16, 19, 9$$

and sends codewords

$$(d_0 + \operatorname{Tr}(cz + dz^5 + ez^7);\ z = \alpha^i,\ 0 \leqq i \leqq 30)$$

into

$$(d_0 + \mathrm{Tr}\,(d^8 z + cz^7 + e^2 z^5);\ z = \alpha^i,\ 0 \leqq i \leqq 30).$$

Set

$$p_i = c_{2\cdot 7^i}, \qquad i = 0, 1, \cdots, 14,$$
$$q_i = c_{-5\cdot 7^i}, \qquad i = 0, 1, \cdots, 14,$$
$$p_\infty = c_0, \qquad q_\infty = \sum c_i,$$

where $c_0 = c_1 = c_2 = c_{18} = c_{21} = c_{26} = c_{27} = c_\infty = 1$ and $c_i = 0$ for all other i. This is a cyclic shift of $x^{16} f(x^{-1})/(x+1)$ which is a word in the code. This leads to the same $p(x)$ and $q(x)$ as the binary Golay code and requires similarly one additional vector to get dimension 16. A soft- and hard-decision convolution encoding/decoding of these two block codes has been designed and simulated by Booth, Herro and Solomon [1]. Another example of this technique gives a convolutional encoding of the:

(48, 24, 12) QR *code.* A 9 stage convolutional encoder with $n = 23$ and

$$p(x) = 1 + x + x^3 + x^4 + x^8,$$
$$q(x) = 1 + x^4 + x^5 + x^7 + x^8,$$

gives a (46, 23; 10) code of type A_0. We adjoin p_∞ and q_∞ as before to obtain words of the form $c_0 + \mathrm{Tr}\, cz$, $\mathrm{Tr}\ c = 0$. To obtain full dimension we must add the all-one vector to the a_i-output (which corresponds to the $\mathrm{Tr}\, z$ vector). To verify this, take the identification rules

$$p_i = c_{21^i}, \quad q_i = c_{-2\cdot 21^i}, \qquad 0 \leqq i \leqq 22,$$

and the codeword (c_i) given by

$$c_i = 1 \quad \text{for } i = 0, 7, 8, 16, 22, 27, 31, 33, 36, 39, 44, \infty,$$
$$c_i = 0 \quad \text{otherwise.}$$

We will now apply these techniques to a rate $\frac{1}{3}$ code. The code chosen is the (30, 10; 11) shortened BCH code. This code will be shown to be of type A_2; i.e., it consists of a direct sum of a quasi-cyclic code plus a (30, 1) code. So far, the best type A_0 (30, 10) code has $d = 10$.

The extended (32, 10; 12) BCH *code* consists of codewords of form

$$(\mathrm{Tr}\,(cz + dz^5);\ z = \alpha^i,\ i = 0, 1, \cdots, 30 \text{ and } z = 0)$$

where $c, d \in \mathrm{GF}(2^5)$, and α is the 31st root of unity defined by $\alpha^5 = \alpha^2 + 1$. Let us consider the (32, 9; 12) subcode consisting of words of the above form with the added condition that $\mathrm{Tr}\,(c + d) = 0$. The map T: $z \to (z+1)^2$, takes $z = 0$ into $z = 1$ and vice versa and is a permutation of the remaining 30 positions.

As this (32, 9; 12) subcode is always zero on the positions $z = 0$ and $z = 1$, we may consider the (30, 9; 12) code under this permutation T. T takes

$$\mathrm{Tr}\,(cz + dz^5) \quad \text{into} \quad \mathrm{Tr}\,(c^{16} + d^4 + d^{16})z + d^{16} z^5 + \mathrm{Tr}\,(c + d)$$
$$= \mathrm{Tr}\,((c^{16} + d^4 + d^{16})z + d^{16} z^5).$$

Now each orbit of T is of period 10, so we get three distinct orbits. Note $T^2 z = z^4$, so

$$T^4 z = z^{16}, \quad T^6 z = z^2, \quad T^8 z = z^8, \quad T^{10} z = z.$$

Thus we can find $(P|Q|R)$ for the (30, 9; 12) code (see Table 2) and one can encode convolutionally. To obtain the full (30, 10; 11) code we have to add the vector Tr z.

2.2. Cyclic codes of type A_0. There is a set of cyclic codes which by virtue of their dimension to length ratio are naturally quasi-cyclic. These include all Reed–Solomon codes, optimal BCH codes over nonbinary alphabets and other binary cyclic codes. From these codes, new quasi-cyclic codes result and new possible convolutional encodings. For example, if a cyclic code of distance d has an information rate k/n between $\frac{1}{2}$ and 1 we can find a set of quasi-cyclic codes of rate $i/(n-k+i)$ $1 \leqq i \leqq k$, with the same distance. Here k and n are relatively prime.

THEOREM 2.3. *Let C be a cyclic Reed–Solomon code over* GF (2^m) *of length* $ln = (2^m - 1)$ *and dimension lk. Then C is quasi-cyclic with constraint length K; more precisely C can be generated by a $k \times n$ matrix with $l \times l$ circulants p_{ij}, $i = 1, \cdots, k$, $j = 1, \cdots, n$, as entries, where $p_{ii} = 1$ for $i = 1, \cdots, k$ and*

$$p_{ij} = 0 \quad \text{for } i \neq j,\ j \leqq k.$$

Proof. There are n distinct orbits of length l under the permutation T, which is defined as a cyclic shift over n positions. We may write any RS word

$$a(x) = \sum_{i=0}^{ln-1} a_i x^i, \qquad a_i \in \text{GF}(2^m),$$

as a sum

$$a(x) = \sum_{i=0}^{l-1} a_{ni} x^{ni} + x \sum_{i=0}^{l-1} a_{ni+1} x^{ni} + \cdots + x^{n-1} \sum_{i=0}^{l-1} a_{ni+n-1} x^{ni},$$

i.e., $a(x) = p_1(x^n) + xp_2(x^n) + \cdots + x^{n-1}p_{n-1}(x^n)$, where $p_i(x)$ has degree at most $l-1$. Since the dimension of the RS code is kl we know that any kl coordinates are independent. So we may stipulate for any $1 \leqq i \leqq k$ that $p_j(x) = 0$ for all $1 \leqq j \leqq k$, $j \neq i$. This accounts for $(k-1)l$ zero coordinates. We may still stipulate $(l-1)$ coordinates to be zero, and a constant. So there is exactly one codeword

$$x^{i-1} + x^k p_{i,k+1}(x^n) + x^{k+1} p_{i,k+2}(x^n) + \cdots + x^{n-1} p_{i,n}(x^n).$$

Applying $T^0, T^1, \cdots, T^{l-1}$ to this codeword gives rise to the $l \times n$ matrix

$$(0|\cdots|0|I|0|\cdots|0|P_{i,k+1}|\cdots|P_{i,n}),$$

$$1, \cdots, i-1, i, i+1, \cdots, k, k+1, \cdots, n,$$

where P_{ij} is the $l \times l$ circulant corresponding to $p_{ij}(x)$, $k+1 \leqq j \leqq n$. Letting i run from 1 to k, one obtains the generator matrix as stated in the theorem. □

Instead of stipulating that $p_{ii}(x) = 1$ we may also stipulate that the highest $\lfloor (l-1)/(n-k+1) \rfloor$ powers of x in $p_{i,i}(x)$, $p_{i,k+1}(x), \cdots, p_{i,n}(x)$ be zero. This would lead to a convolutional encoding with constraint length $K = l - \lfloor (l-1)/(n-k+1) \rfloor = \lfloor d/(n-k+1) \rfloor$. For rate $(n-1)/n$ codes this gives $K = \lfloor d/2 \rfloor = (l+1)/2$. The question remains, however, is the dimension of the code generated this way. It is our conjecture that we do always obtain the full dimension kl. This conjecture is supported by examples below.

Example 2.4. Let α be a primitive element in GF (2^4) satisfying $\alpha^4 = 1 + \alpha$. Consider the (15, 10; 6) Reed–Solomon code generated by

$$g(x) = \prod_{i=-2}^{2} (x + \alpha^i) = x^5 + \alpha^4 x^4 + \alpha^{11} x^3 + \alpha^{11} x^2 + \alpha^4 x + 1.$$

The codeword

$$(1+\alpha^8 x+x^2)g(x)=1+\alpha^5 x+\alpha^{11}x^3+\alpha^{11}x^4+\alpha^5 x^6+x^7$$

can be written as $p(x^3)+xq(x^3)$ where $p(x)=1+\alpha^{11}x+\alpha^5 x^2$ and $q(x)=\alpha^5+\alpha^{11}x+x^2$. Since g.c.d. $(p(x), q(x), x^5-1)=1$, we find that the matrix $(P|Q)$, where P and Q are the circulants associated with $p(x)$ and $g(x)$, generates a $(10, 5; 6)$ quasi-cyclic code with constraint length 3.

Note. By a cyclic shift of the original code, $xp(x^3)+x^2q(x^3)$ is also in the code, thus leading to a rate $\frac{2}{3}$ quasi-cyclic code of length 15 and minimum distance 6. The generator matrix of this code is

$$\begin{pmatrix} P & Q & 0 \\ 0 & P & Q \end{pmatrix}.$$

Remark 2.5. For optimal BCH codes over GF (2^m) of length $n=(2^m+1)$ which have rates $(n-1)/n$ and generators $g(x)=(x-1)\sum_{i=1}^{(d-2)/2}(x+\alpha^i)(x+\alpha^{-i})$, d even, we have similar results.

Example 2.6. The $(9, 6; 4)$ BCH code over GF (2^3) with

$$g(x)=(x+1)(x+\alpha)(x+\alpha^{-1}), \qquad \alpha^6+\alpha^3+1=0.$$

Now

$$p(x)=1+Ax,$$

$$q(x)=A+x,$$

correspond to the vector $(x+1)g(x)=p(x^3)+xq(x^3)$, where $A=\alpha+\alpha^{-1}\in$ GF (2^3), $A^3=A+1$. This encoder resembles the Viterbi dual code of rate $\frac{1}{2}$, over GF (2^3).

TABLE 1
Quasi-cyclic codes, rate $\frac{1}{2}$.

n	d	K	$p(x)$ $p_0p_1\cdots$	$q(x)$ $q_0q_1\cdots$	$f(x)$ $f_0f_1\cdots$
1	2	1	1	1	1
2	2	1	1	1	1
3	3	2	1	1 1	1 1
4	4	3	1	1 1 1	1 1 1
5	4	3	1	1 1 1	1 1 1
6	4	3	1	1 1 1	1 1 1
7	4	3	1	1 1 1	1 1 1
8	5	4	1 0 1 1	1 1	0 1 0 1 1 1
9	6	5	1 0 1 1	1 0 1 0 1	0 1 1 1 1 0 0 1
10	6	5	1 1 0 0 1	1 0 1 1	0 0 0 1 1 1 1 0 1
11	7	6	1 1 1	1 1 0 1 0 1	0 0 0 1 1 1 0 1 1 0 1
12	8	7	1 0 0 0 1 0 1	1 1 1 1 1	0 1 1 0 1 1 1 1 0 1
13	7	6	1 1 0 1 1 1	1 0 1 1 1	0 1 0 1 0 1 1 0 0 0 0 1 1
14	8	7	1 1 0 1 0 1 1	1 1 1 1 1	0 1 1 1 0 0 0 0 0 1 1 1 0 1
15	8	7	1 1 0 0 1 1 1	1 1 0 0 1	1 0 0 1 0 1 0 1 0 0 1 1 0 1
16	8	8	1 1 1 0 1 0 1	1 1 0 1 1 0 0 1	0 0 0 1 0 1 1 0 1 1 1 1
17	8	10	1	1 1 1 0 1 1 0 1 0 1	1 1 1 0 1 1 0 1 0 1
18	8	10	1	1 1 1 0 1 1 0 1 0 1	1 1 1 0 1 1 0 1 0 1
19	8	10	1	1 1 1 0 1 1 0 1 0 1	1 1 1 0 1 1 0 1 0 1
20	9	9	1 0 1 1 0 1 1 1 1	1 1 0 0 0 0 0 1 1	0 1 0 1 1 1 1 0 1 0 0 1 1
21	10	11	1 1 1 0 0 1 0 0 1 1 1	1 1 0 1 1 0 1	1 1 0 0 1 0 1 1 1 1 0 1 1

Remark 2.7. Other quasi-cyclic codes may be constructed from the BCH codes (33, 22; 12) over GF (2^5), (65, 52; 14) over GF (2^6), etc.

3. Tables. In the Tables 1, 2 and 3 the reader can find the polynomials $p_{ij}(x)$ for small, rate $\frac{1}{2}$, $\frac{1}{3}$, and $\frac{2}{3}$ block codes. Surprisingly many good block codes (in the sense of large minimum distance) turn out to have a quasi-cyclic structure and are hence encodable by convolutional techniques.

TABLE 2
Rate $\frac{1}{3}$, $p_1(x) = 1$.

n	d	K	$p_2(x)$	$p_3(x)$
1	3	1	1	1
2	4	2	1	1 1
3	4	2	1	1 1
4	6	3	1 1	1 1 1
5	7	4	1 1 1	1 1 1
6	8	5	1 1 1	1 1 1 0 1
7	8	5	1 0 1	1 1 1 1 1
8	8	6	1 1 0 1	1 1 0 1 0 1
9	10	6	1 1 1 0 0 1	1 0 1 1 1 1
10	10	8	1 1 0 0 1	1 0 1 1 1 1 1 1 1

TABLE 3
Rate $\frac{2}{3}$, $p_{11}(x) = p_{22}(x) = 1$, $p_{12}(x) = p_{21}(x) = 0$.

n	d	K	$p_{13}(x)$	$p_{23}(x)$
1	2	1	1	1
2	2	1	1	1
3	2	1	1	1
4	3	3	1 1	1 1 1
5	4	4	1 1 1	1 1 0 1
6	4	4	1 1 1	1 1 0 1
7	4	4	1 1 1	1 1 0 1
8	4	4	1 1 1	1 1 0 1
9	4	4	1 1 1	1 1 0 1
10	5	10	1 1 0 1 1	1 0 1 1 0 1
11	6	10	1 0 1 1 1 0 1	1 1 1 1 0 0 1 1

REFERENCES

[1] R. W. D. BOOTH, M. A. HERRO AND G. SOLOMON, *Convolutional coding techniques for certain quadratic residue codes*, International Telemetering Conference, (XI) Proceedings (Silver Springs, Maryland), 1975.

[2] J. J. BUSSGANG, *Some properties of binary convolutional code generators*, IEEE Trans. Inform. Theory, IT-11 (1965), pp. 90–100.

[3] G. D. FORNEY, JR., *Convolutional codes I: Algebraic structure*, Ibid., IT-16 (1970), pp. 720–738.

[4] F. J. MACWILLIAMS AND N. J. A. SLOANE, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam, 1977.

[5] H. F. MATTSON AND G. SOLOMON, *A new treatment of BCH codes*, J. Soc. Industr. Appl. Math., 9 (1961), pp. 654–669.

[6] A. J. VITERBI, *Convolutional codes and their performance in communication systems*, IEEE Trans. Inform. Theory, IT-13 (1967), pp. 260–269.