HIGH-RATE BINOMIAL CONVOLUTIONAL CODES

by Ph. PIRET

Abstract
A construction is described of high-rate RS-like convolutional codes, and a lower bound is given on their free distance. These codes can be used to construct asymptotically good binary convolutional codes.

1. Introduction

In a preceding report 4), a class of RS-like convolutional codes was introduced. These codes were obtained only for length $n$, rate $R = k/n$ and constraint length $\nu$ related by the inequality

$$R n \nu \leq n + 1,$$

and their free distance was lower-bounded as follows:

$$d_f \geq \nu (n - k + 1).$$

Our aim in this paper will be to obtain codes with a slightly weaker bound on $d_f$, but for which $n$, $k$ and $\nu$ would no more be so drastically bounded as in (1).

After recalling the formalism used to represent the RS-like codes, and some useful arguments for computing $d_f$, we shall present in sec. 3 a construction of high-rate RS-like convolutional codes, and a lower bound on their free distance. These codes are then used to obtain long, asymptotically good, binary convolutional codes, of arbitrary rate, by use of some arguments developed by Justesen 3).

2. Representation of the RS-like codes

Let $q$ be a power of 2, and consider a linear convolutional code of length $n$, rate $k/n$ and constraint length $\nu$ on $GF(q)$. Its generator matrix can be given the form

$$G = [G_0, G_1, \ldots, G_j, \ldots, G_{\nu - 1}],$$

where we suppose that all $G_j$ generate cyclic RS block codes 2). We shall consider an $n$-tuple with polynomial representation

$$g_r(X) = \frac{X^n - 1}{X - \alpha^r}, \quad r = 0, 1, \ldots, n - 1,$$

where $\alpha$, primitive of order $n$, is in $GF(q)$ but in no proper subfield. The $k$
n-tuples of each $G_j$ are chosen in this set so that each $G_j$ can be represented by a column of $k$ integers referring to the indices of the chosen $n$-tuples. Using this convention, we represent the generator matrix $G$ by a rectangular array of integers $g_{ij}$ $(0 \leq i \leq k - 1$, $0 \leq j \leq v - 1)$. The space of the admitted sequences is then generated by the rows of a matrix $\Gamma$ that we now describe. Consider therefore the matrix $G$, represented by $v$ columns of $g_{ij}$, and the operator $T^s$ that shifts $G$, $s$ columns to the right. The matrix $\Gamma_s$ is then given by

$$\Gamma_s = \begin{bmatrix} G \\ T \times G \\ \vdots \\ T^s \times G \end{bmatrix}$$

and all semi-infinite sequences of the code are in the “row space” of $\Gamma_s$. Each row of $T^s \times G$ contains $v$ significative numbers, in $v$ consecutive columns. The first of these is the $(s + 1)$th and the empty places, in $\Gamma_s$ or $\Gamma_s$, correspond to the zero word.

As described elsewhere \(^4\) this representation is well suited to check whether a sufficient condition is satisfied that guarantees the non-catastrophic character of the generator matrix.

Denote now by $\nu$ some $n$-tuple in a sequence of the code. Each generator $g_r(X)$ is used $t_r$ times with a non-zero coefficient in the sum that defines $\nu$.

The following property was precedingly noticed \(^4\).

**Property 2.1.** The $n$-tuple $\nu$ is not zero if it is defined by a sum for which at least one of the corresponding $t_r$ is equal to 1.

This property follows from the fact that the complete space of $n$-tuples is the direct sum of its $n$ irreducible ideals.

3. The binomial RS-like convolutional codes

As in sec. 2, we wish to specify a code by an array of $g_{ij}$ $(0 \leq i \leq k - 1$, $0 \leq j \leq v - 1)$, and thus by a function $\psi(i, j)$ that applies the pairs of indices $(i, j)$ into $Z_n$, that is the set of integers modulo $n$. Precedingly \(^4\), the function $\psi(i, j)$ has been defined as follows:

$$\psi(i, j) = i + j \times k \mod n,$$

but restriction (1) is then necessary to keep a bound such as (2), if $v \geq 3$ \(^4\). For high-rate codes ($R > 1/2$), defined by (6), the lower bound obtained on $d_f$ is only of the order of $2(n - k + 1) + (v - 2)$ which is disappointing for large $v$.
In the following, a construction of RS-like codes is given that is effective for any rate. The constraint length \( v \) is upper-bounded by

\[
\binom{a}{2} \leq n - k,
\]

with \( 0 \leq a \leq 1 \), so that \( v \) is no more fixed by \( R \), but can be increased as much as desired by taking \( n \) sufficiently large.

Finally the free distance of the codes will be shown to satisfy

\[
\frac{d_f}{vn} \geq (1 - R) - \phi(v, n).
\]

It is then possible to define an increasing function \( \nu(n) \) with the following properties:

\[
\lim_{n \to \infty} \nu(n) = \infty,
\]

\[
\lim_{n \to \infty} \phi[n, \nu(n)] = 0.
\]

The announced construction is as follows. For any integer \( \mu \), with \( 1 \leq \mu \leq v \), a binomial RS-like code is specified by the function \( \psi_\mu(i, j) \):

\[
g_{0j} = \psi_\mu(0, j) = \binom{a - j}{2} \mod n, \quad 0 \leq j \leq \mu - 1,
\]

\[
g_{0j} = \psi_\mu(0, j) = \binom{\mu - j + 2}{2} \mod n, \quad \mu - 1 \leq j \leq v - 1,
\]

\[
g_{ij} = \psi_\mu(i, j) = i + \psi_\mu(0, j) \mod n, \quad 0 \leq i \leq k - 1.
\]

Some comments can be given on this definition of the \( g_{ij} \). Let first \( \lambda \) be the maximum of \( \mu \) and \( v - \mu + 1 \). We then suppose that (7) is valuable with \( a \nu = \lambda \). In this case the non-catastrophic character of \( G \) is easily checked by use of precedingly developed arguments. Moreover, the definition of the \( g_{ij} \) as given by (11), is natural since \( \psi(i, j) \) satisfy well enough the following requirements:

1. to be non-linear in \( j \);
2. to be slowly increasing or decreasing with \( j \);
3. to map pairs of integers into \( \mathbb{Z}_n \).

Since a lower bound on \( d_f \), similar to (8), will be given for these codes, the construction (11) seems to be a useful one.
4. The free distance of the binomial codes

We first note that an infinite sequence of a binomial code has an infinite weight since the code is not catastrophic. Only finite sequences must be investigated to lower-bound the free distance. Consider now \( s \) consecutive information \( k \)-tuples, where at least the first and the last are not zero, so that the resulting encoded sequence contains \( v + s - 1 \) consecutive \( n \)-tuples. Such a sequence can be represented by a subset \( \gamma_s \) of the rows of \( \Gamma_s \), so that there is a one-to-one correspondence between the non-zero information symbols and the rows of \( \gamma_s \). The \( h \)th column of \( \gamma_s \), \( 1 \leq h \leq v + s - 1 \), then is a representation of the \( h \)th encoded word and, as was noticed in sec. 2, an \( n \)-tuple of numbers \( t_v \), \( 0 \leq v \leq n - 1 \), can be associated to it. If at least one of the associated \( t_v \) is equal to 1, the corresponding word is surely non-zero, and a lower bound can be obtained on its weight as follows. If \( v_M \) and \( v_m \) are respectively the largest and the smallest indices \( v \) for which \( t_v \) is non-zero, then the corresponding non-zero word has a weight \( w \) that is lower-bounded \(^2\) by

\[
w \geq n - v_M + v_m. \tag{12}\]

A row of \( \gamma_s \) contains \( v \) significative numbers \( g_{ij} \), \( 0 \leq j \leq v - 1 \), that appear respectively in \( v \) consecutive columns from the \( x \)th up to the \( (x + v - 1) \)th, \( 1 \leq x \leq s \). The other places in such a row are empty. If \( g_{ij} \) is the \((j + 1)\)th significative number of such a row, it appears in the \((x + j)\)th column of \( \gamma_s \). In the following a number \( g_{ij} \) will frequently be denoted by the triple \((x, i, j)\); \( i \) and \( j \) refer to the value of this number and \( x \) and \( j \) to the column of \( \gamma_s \) where it appears. Both notations will be indifferently used. We now define \( m(h) \) as being the minimum of all numbers \( g_{ij} \) that appear in the \( h \)th column of \( \gamma_s \):

\[
m(h) = \min_{(x, i, j) \in \gamma_s} (x, i, j). \tag{13}\]

The complete set of the \( m(h) \) associated with \( \gamma_s \) is denoted by \( M(\gamma_s) \), and the subset of these \( m(h) \) for which \( t_m(h) = 1 \), is denoted by \( U(\gamma_s) \). We shall now obtain a bound on \( d_f \) by showing that \( |U(\gamma_s)| \geq v \).

Consider now \( r_1 \) and \( r_2 \), which are two rows of \( \gamma_s \), and \( K(r_1, r_2) \), which is the subset of the columns of \( \gamma_s \) where \( r_1 \) and \( r_2 \) simultaneously have significative numbers.

We now denote by \( c \) the cardinality of \( K(r_1, r_2) \). We suppose that \( c \geq 2 \), and that the first significative columns of \( r_1 \) and \( r_2 \) are respectively the \( x_1 \)th and the \( x_2 \)th. The columns of \( K(r_1, r_2) \) are indexed by \( h \), from some \( h_0 \) that is the minimum of \( x_1 \) and \( x_2 \), up to \( h_0 + c - 1 \), and \( r_i(h) \) denotes the number of \( r_i \) that is in the \( h \)th column of \( \gamma_s \). We also define \( \Delta(h) \) as being \( r_1(h) - r_2(h) \).
With these hypotheses we emphasize the following property, which is evident, having in mind the construction of the numbers $g_{ij}$.

**Property 4.1.** If $c \geq 2$, and if $h$ is submitted to $h_0 \leq h \leq h_0 + c - 2$, then the two following properties are equivalent:

(1) \[ x_1 \leq x_2 - 1, \]

(2) \[ \Delta(h + 1) \geq \Delta(h) + 1. \]

This property is illustrated by the example of table I where $v = 8$ and $c = 6$.

**TABLE I**

<table>
<thead>
<tr>
<th></th>
<th>11</th>
<th>7</th>
<th>4</th>
<th>2</th>
<th>1</th>
<th>2</th>
<th>4</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r_1$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$r_2$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$h$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$\Delta(h)$</td>
<td>-6</td>
<td>-4</td>
<td>-2</td>
<td>-1</td>
<td>-4</td>
<td>-1</td>
<td>-4</td>
<td>-1</td>
</tr>
<tr>
<td>$\Delta(h + 1) - \Delta(h)$</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Definition 4.2.** The relative abscissa of $m(h)$ is the minimal value of $j$ for all numbers $(x, i, j)$ that are equal to $m(h)$, in the $h$th column of $\gamma_s$.

**Theorem 4.3.** If $j_1$ and $j_2$ are the relative abscissae of $m(h_a)$ and $m(h_a + 1)$, which are two consecutive numbers of $M(\gamma_s)$, then $j_2 \leq j_1 + 1$, with equality only if $m(h_a + 1) \in U(\gamma_s)$.

**Proof.** Suppose that $r_1$ and $r_2$ are the rows of $\gamma_s$ where $m(h_a)$ and $m(h_a + 1)$ have their relative abscissae $j_1$ and $j_2$. Suppose also that they have their first significative number respectively in the $(x_1)$th and the $(x_2)$th columns of $\gamma_s$.

We first consider the case where $r_2 = r_1$. The second statement of property 4.1 is satisfied by the hypotheses except if $j_2 = 0$. In both cases, $x_1$ must be $\leq x_2 - 1$ so that

\[ h_a - x_1 \geq h_a - x_2 + 1, \]

and this is just the same as

\[ j_1 \geq j_2. \]

We now suppose that $r_2 \neq r_1$. In this case, $j_1 + 1 = j_2$ and we show that $m(h_a + 1) \in U(\gamma_s)$.

Suppose there exists an other row $r$ that contains the number $(x, i, j)$, equal to $m(h_a + 1)$, in the $(h_a + 1)$th column of $\gamma_s$. The value of $x$ cannot be $\geq x_1 + 1$ since $j_1 + 1 = j_2$. It can neither be $\leq x_1 - 1$, since $m(h_a)$ would not be a number of the row $r_1$ and this is a contradiction. The number $m(h_a + 1)$ must thus appear only once in the $(h_a + 1)$th column of $\gamma_s$.

Q.E.D.
Let now $u(f)$ be the relative abscissa of the $f$th number of $U(y_s)$. We just proved that $u(f+1) \leq u(f) + 1$. Since $m(1)$ and $m(v + s - 1) \in U(y_s)$ with relative abscissae equal to 0 and $v - 1$, there is at least one $u(f)$ equal to $j$ for all $j$, $(0 \leq j \leq v - 1)$. The corresponding sequence of the code thus contains for all $j$, at least one non-zero word with $v_m \geq g_{0j}$.

The above considerations are illustrated by fig. 1. This figure gives a graphical representation of a sequence of a code with $v = 5$. The values of the numbers $g_{ij}$ are represented in ordinate.

Fig. 1. Representation of the following matrix $y_3$:

$$
\begin{array}{cccccc}
6 & 4 & 3 & 4 & 6 \\
4 & 2 & 1 & 2 & 4 \\
3 & 1 & 0 & 1 & 3 \\
6 & 4 & 3 & 4 & 6 \\
\end{array}
$$

We now apply the above material to obtain a lower bound on $d_f$ by use of inequality (12). First, the weight of the first and the $(v + s - 1)$th word in a sequence represented by $y_s$ is at least $n - k + 1$. Second, $v_M$ is upper-bounded by $k - 1 + (\frac{v - 2}{2})$. As described above, we are permitted to write

$$
d_f \geq 2(n - k + 1) + \sum_{j=1}^{v-2} [n - k + 1 - (\frac{v - 2}{2}) + g_{0j}],
$$

(14)
and this bound can be transformed to obtain

\[ d_f \geq v(n - k + 1) - (v - 2) \left( \left( \frac{2}{3} \right) - \left( \frac{1}{3} \right)^- + 1 \right). \] (15)

The maximum of this bound is obtained for \( \mu = (v + 1)/2 \), if \( v \) is odd, and for \( \mu = v/2 \) or for \( \mu = (v + 2)/2 \), if \( v \) is even. We then obtain

\[
\begin{align*}
d_f & \geq v(n - k + 1) - (v^2 - 1)(2v - 3)/24 \quad \text{(odd \( v \))}, \\
d_f & \geq v(n - k + 1) - v(v - 2)(2v + 7)/24 \quad \text{(even \( v \))}.
\end{align*}
\] (16)

For large \( n \), we can write

\[
\frac{d_f}{vn} \geq (1 - R) - \frac{v^2}{12n} - O(v/n),
\] (17)

and if we increase \( n \) and \( v \) in such a way that \( \lim v^2/n \) is zero for \( n \to \infty \), we obtain the result announced by (8).

5. Asymptotically good convolutional codes

The preceding results can be used to construct long asymptotically good binary convolutional codes of any rate. Moreover the parameter \( v \) can be increased as much as desired, at least if \( \lim v^2/n \) is zero for increasing \( n \). The arguments used are similar to those of Justesen 3).

We consider the case where \( v \) is an odd integer \( (v = 2\mu - 1) \), but the case of an even \( v \) is very similar.

In the following the RS-like codes are on \( GF(2^m) \). Their words have a length \( n = 2^m - 1 \) and their rate \( k/n \) is denoted by \( R \). Each of the \( n \) symbols of \( GF(2^m) \) that constitute a word, is now binary-encoded by a shortened version of length \( 2m - s \), of a distinct code in the pseudo-random ensemble of Wozencraft's codes 1). The rate \( ml/(2m - s) \) of these codes is denoted by \( r_w \). The rate of the resulting binary code is denoted by \( r_b \) and is equal to \( R r_w \). The words of the binary code have a length \( n_b \) that is equal to \( (2^m - 1)(2m - s) \). From the paper of Justesen 3), and from the preceding sections, it follows that for each integer \( j \), \( 0 \leq j \leq v - 1 \), there is in each non-zero sequence of the binary code at least one non-zero word whose weight \( W(j) \) is lower-bounded by

\[
W(j) \geq \frac{n - k - \binom{\mu}{2} + g_{0,j}}{n} (2m - s)(2^m - 2^s) [H^{-1}(1 - r_w) - O(m)].
\] (18)
This implies that the free distance of this convolutional binary code satisfies the following inequality:

$$\lim_{n \to \infty} \left( \frac{d_f}{mn_b} \right) \geq \left[ 1 - \frac{r_b}{r_W} - \frac{(v^2 - 1)(2v - 3)}{24vn} \right] H^{-1}(1 - r_W).$$

(19)

If $v$ is also increased in such a way that $\lim \frac{v^2}{n}$ is $0$ for $n \to \infty$, we obtain

$$\lim_{n \to \infty} \left( \frac{d_f}{mn_b} \right) \geq \left( 1 - \frac{r_b}{r_W} \right) H^{-1}(1 - r_W).$$

(20)

The optimization of $r_W$ then follows just as in the paper of Justesen.

6. Conclusion

We have described a construction for RS-like convolutional codes that is effective for all rates and for a sufficiently large number of constraint lengths.

A lower bound on their free distance was obtained and asymptotically good binary convolutional codes were derived. We suggest here a possible refinement of the above construction. The value of $g_{ij}$ given by (11) should be taken modulo $v$. If each sequence of the resulting code would keep the property to have at least $v$ non-zero words, the function $\phi(v, n)$ would be quadratic (no more cubic) in the parameter $v$. We conjecture that it is effectively so at least when $v$ is a prime, but up to now, we have no proof of this conjecture.

MBLE Research Laboratory Brussels, June 1972

REFERENCES