The [32,10,12] TFCI code

A. E. Brouwer

January 19, 2012

Earlier, a $[32, 6, 16]$ 1st order Reed-Muller code R was used to encode the TFCI (Transport Format Combination Indicator) in mobile communication systems. When it became desirable to encode 10 data bits (instead of 6), a $[32, 10, 12]$ subcode C_0 of the 2nd order Reed-Muller code was chosen that contains the code R used earlier. The question arises how precisely C_0 was constructed. A basis of C_0 is given below.

1	11111111111111111111111111111111
v_1	01010101010101010101010101010101
v_2	00110011001100110011001100110011
v_3	00001111000011110000111100001111
v_4	00000000111111110000000011111111
v_5	00000000000000001111111111111111
m_1	00101000011000111111000001110111
m_2	00000001110011010110110111000111
m_3	00001010111110010001101100101011
m_4	00011100001101110010111101010001

The vectors 1, v_i $(i = 1, 2, 3, 4, 5)$ form a basis of R. The new vectors m_j $(j = 1, 2, 3, 4)$ were added.

The r-th order Reed-Muller code of length 2^m consists of the evaluations of polynomials of degree at most r on $\mathbb{F}_2^m$. Clearly, this code contains the t-th order Reed-Muller code for $t < r$. In particular, the 2nd order Reed-Muller code contains the 1st order Reed-Muller code.

The weight enumerator of C_0 is $1 + 240x^{12} + 542x^{16} + 240x^{20} + x^{32}$, the same as one would expect for a subcode of the 2nd order Reed-Muller code. (The 1st order RM code has $1 + 62x^{16} + x^{32}$, and each of the 15 cosets adds $16x^{12} + 32x^{16} + 16x^{20}$.)

Code words in the 1st order Reed-Muller code R are linear functions in the v_i, i.e., are of the form $a_0 + a_1v_1 + a_2v_2 + a_3v_3 + a_4v_4 + a_5v_5$ for a total of $2^6 = 64$ code words. Code words in the corresponding 2nd order Reed-Muller code are quadratic functions in the v_i. Here the m_j are not quadratic in the v_i, so this is not a subcode of the 2nd order Reed-Muller code that is coordinatized with the v_i.

In fact, here $m_1 = v_2 + v_1v_2 + v_3 + v_1v_3 + v_1v_4 + v_1v_2v_4 + v_3v_4 + v_5 + v_2v_5 + v_1v_2v_5 + v_1v_3v_5 + v_4v_5 + v_2v_4v_5$, $m_2 = v_1v_2v_3 + v_4 + v_2v_4 + v_1v_5 + v_2v_5 + v_3v_5 + v_1v_3v_5 + v_1v_4v_5 + v_2v_4v_5$, $m_3 = v_3 + v_1v_3 + v_4 + v_3v_4 + v_2v_3v_4 + v_1v_2v_5 + v_4v_5 +$

$v_2v_4v_5 + v_3v_4v_5$, $m_4 = v_1v_2 + v_3 + v_2v_3 + v_1v_2v_3 + v_2v_4 + v_1v_2v_4 + v_3v_4 + v_1v_3v_4 + v_2v_3v_4 + v_2v_5 + v_1v_4v_5$.

There exists a file `03134r0P802-15_TG3a-Samsung-CFP-document-1.doc` where the use of a $[32, 11, 12]$ subcode of the 2nd order Reed-Muller code is proposed, and the five additional 'mask' vectors there are actually quadratic functions in the v_i.

But if it is not a subcode of the 2nd order Reed-Muller code coordinatized by the v_i, then how was this code C_0 constructed? The automorphism group of C_0 has size 10 only, it is an ugly code. However, it has a unique extension to a $[32, 11, 12]$ code C. The lexicographically smallest additional basis vector is $z =$ `00000000001011010010111001101010`. This code C has a group $2^5 : 31 : 5$ of size $32 * 31 * 5 = 4960$, acting primitively on the 32 positions, necessarily $A\Gamma L(1, 32)$. The twice derived group is the elementary abelian 2^5 that is the additive group of the field. We find the six basis vectors

```
11111111111111111111111111111111
00001010111110010001101100101011
01110000011110100111110010001001
01101101100000000011111000011111
01001110110101111011100010000100
00101000011000111111000001110111
```

that span a 1st order RM code R' inside C. Note that only three of these six vectors are in C_0. In other words, C_0 does not contain the 1st order RM code R'.

If we call these six coordinates 1, x_1, x_2, x_3, x_4, x_5, then the given ten basis vectors and the additional vector z are 1, and

v_1	$x_1 + x_2 + x_3 + x_2x_3 + x_4 + x_3x_4 + x_5 + x_2x_5 + x_3x_5$
v_2	$x_1 + x_2 + x_3 + x_1x_3 + x_2x_4 + x_3x_4 + x_2x_5$
v_3	$x_1 + x_3 + x_1x_3 + x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_1x_5 + x_3x_5 + x_4x_5$
v_4	$x_1x_2 + x_4 + x_1x_4 + x_3x_4 + x_5 + x_2x_5$
v_5	$x_1 + x_1x_2 + x_2x_3 + x_1x_4 + x_2x_4 + x_5 + x_1x_5$
m_1	x_5
m_2	$x_1 + x_3 + x_4 + x_5$
m_3	x_1
m_4	$x_1 + x_2 + x_4 + x_5$
z	$x_1x_2 + x_1x_3 + x_2x_3 + x_4 + x_1x_4 + x_2x_4 + x_3x_4 + x_5 + x_2x_5 + x_3x_5$

all at most quadratic in the x_i, as desired.

Extended BCH code

The extended cyclic code C' of length 32 with generator polynomial $1+x^2+x^4+x^6+x^7+x^9+x^{10}+x^{13}+x^{17}+x^{18}+x^{20}$ (and final parity check) is isomorphic to the code C.

This polynomial has roots α^i where α is a primitive element of $\mathbb{F}_{32}$ and $i \in \{1, 2, 4, 8, 16\} \cup \{3, 6, 12, 24, 17\} \cup \{5, 10, 20, 9, 18\} \cup \{7, 14, 28, 25, 19\}$. It follows that C' is the parity check extension of the (narrow-sense) primitive BCH code of length 31 and designed distance 11.

An explicit generator matrix:

```
00000000001011000100110110101011
10000000000101100010011011010101
01000000000010110001001101101011
10100000000001011000100110110101
01010000000000101100010011011011
10101000000000010110001001101101
01010100000000001011000100110111
10101010000000000101100010011011
11010101000000000010110001001101
01101010100000000001011000100111
10110101010000000000101100010011
```

Deleting the last row from this generator matrix yields a 10-dimensional code C'' with weight enumerator $1 + 310x^{12} + 527x^{16} + 186x^{20}$, that no longer contains the all-1 vector, and has many low weight vectors.

MacWilliams & Sloane p. 455

It has been suggested that the code C_0 is related in a certain way to the code one gets from MacWilliams & Sloane [4] p. 455, Corollary 17, equation (30), for $m = 5$, $t = 2$, $d = 2$. However, the suggested construction ($1 + 5 + 5$ basis vectors, derived from the circulants θ_0, θ_1^*, θ_5^*) is based on a misreading of [4]. In that corollary the code is generated by a single circulant. (Namely, by $\theta_0 + \theta_1^* + \theta_5^* =$ `1000000100010110000101100110100`, extended by a parity check, so that one gets `10000001000101100001011001101001`.

In other words, the generator matrix one gets out of Corollary 17, formula (30) is

```
10000001000101100001011001101001
01000000100010110000101100110101
00100000010001011000010110011011
10010000001000101100001011001101
01001000000100010110000101100111
10100100000010001011000010110011
11010010000001000101100001011001
01101001000000100010110000101101
00110100100000010001011000010111
10011010010000001000101100001011
11001101001000000100010110000101
```

Deleting the last row from this generator matrix yields a 10-dimensional code C'' with weight enumerator $1 + 246x^{12} + 527x^{16} + 250x^{20}$, that no longer contains the all-1 vector, rather different from C_0.

Indeed, the patent authors did not go this way but used mask sequences.

Mask sequences

The finite field $\mathbb{F}_{32}$ contains six cyclotomic classes of size 5. That is, there are six irreducible polynomials of degree 5 over $\mathbb{F}_2$. If α is root of one of these, then the 31 nonzero elements of $\mathbb{F}_{32}$ are $1, \alpha, \alpha^2, \ldots, \alpha^{30}$ and $\alpha^{31} = 1$.

The trace $\mathrm{tr}(x)$ of an element $x \in \mathbb{F}_{32}$ is defined as $x + x^2 + x^4 + x^8 + x^{16}$. It is an element of $\mathbb{F}_2$. The sequence of traces $\mathrm{tr}(\alpha^i)$, $0 \leq i \leq 30$, depends only on the minimal polynomial of α, so that there are six possible sequences of traces.

polynomial	trace sequence
$x^5 + x^2 + 1$	1001011001111100011011101010000
$x^5 + x^3 + 1$	1000010101110110001111100110100
$x^5 + x^3 + x^2 + x + 1$	1001001100001011010100011101111
$x^5 + x^4 + x^2 + x + 1$	1110100010010101100001110011011
$x^5 + x^4 + x^3 + x + 1$	1110110011100001101010010001011
$x^5 + x^4 + x^3 + x^2 + 1$	1111101110001010110100001100100

The cyclic shifts of a single trace sequence, with a trailing 0 added, together with their bitwise complements, form a code isomorphic to the 1st order Reed-Muller code. A generator matrix is given by the all-1 vector together with five cyclic shifts of this trace sequence. (That is, any further cyclic shift is a linear combination of these. The six choices of trace sequence give isomorphic codes.)

The code with generator matrix consisting of the all-1 vector and five cyclic shifts of each of two trace sequences, will have dimension 11. Up to isomorphism there are three choices, namely the first row above together with the second, third or last. The first possibility gives minimum distance 10. The other two possibilities are nonisomorphic, but both give minimum distance 12, with the same weight enumerator.

The patent description suggests that this, followed by a coordinate rearrangement, followed by the deletion of one generator, is the way the inventors followed.

Conclusion

The 10-dimensional code C_0 under investigation is a subcode of an 11-dimensional code C that is one of the two $[32, 11, 12]$ codes between the 1st order and the 2nd order Reed-Muller code (that have the weights of C, see [5]).

That 11-dimensional code C contains a copy R' (spanned by the x_i) of the 1st order Reed-Muller code, and using coordinates such that this code R' consists of the linear functions, the remaining code words of C are quadratic.

However, the 10-dimensional subcode C_0 does not contain R' (but only half of it). It does contain a different copy R (spanned by the v_i) of the 1st order Reed-Muller code, but using the v_i as coordinates, the remaining code words are not quadratic, and hence are not in the corresponding 2nd order Reed-Muller code.

In other words, C_0 can be obtained from a well-known code by throwing away half of its code words, and then rearranging the coordinate positions so as to make sure that the result contains R.

There are various other ways to obtain this code or similar codes. Whether this particular code has any advantages over other choices, I don't know.

References

[1] `r1-99913.pdf`

[2] `EP1188269B1.pdf`

[3] Y. Chen & A. J. H. Vinck, *The optimum distance profiles of the second order Reed-Muller codes*, ISIT 2009, Seoul, Korea.

[4] F. J. MacWilliams & N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland Publ. Co., 1981.

[5] J. Maks & J. Simonis, *Optimal subcodes of second order Reed-Muller codes and maximal linear spaces of bivectors of maximal rank*, Desigs, Codes and Cryptography **21** (2000) 165-180.