EVEN MORE EFFICIENT SOFT DECODING OF THE GOLAY CODES

Alexander Vardy and *Yair Be'ery* *

Department of Electrical Engineering – Systems
Tel–Aviv University, Ramat–Aviv 69978, Tel–Aviv, Israel
* also with the DSP Group Ltd., Givat Shmuel 51905, Israel

We present an algorithm for maximum–likelihood soft decision decoding of the binary (24,12,8) Golay code. The algorithm involves projecting the codewords of the binary Golay code onto the codewords of the (6,3,4) code over GF(4), – the hexacode. The complexity of the proposed algorithm is at most 651 real operations which is, to the best of our knowledge, less than the complexity of any algorithm ever published. Along similar lines the tetracode may be employed for decoding the ternary (12,6,6) Golay code with only 530 real operations. The proposed algorithm also implies a reduction in the number of computations required for decoding of the Leech lattice.

The (24,12,8) extended binary Golay code C is certainly one of the most interesting codes known. The problem of maximum–likelihood soft decision decoding of the binary Golay code was intensively investigated over the last few years. Conway and Sloane [3] published a decoding algorithm which requires 1614 operations, Be'ery and Snyders [1] have proposed an algorithm with a worst case complexity of 1551 operations while the recent decoding algorithm of Forney [4] requires only 1351 operations. Yet, using the terminology of Forney [6], the "world record" in the decoding of the binary Golay code belongs to Be'ery and Snyders [2,8] and it stands on 827 operations. In the paper we claim a more efficient algorithm which requires at most 651 operations. To be precise we note that, in compliance with the convention of [1–5,8], the complexity of decoding is measured in terms of the total number of real additions and comparisons. The figures cited above follow those of [8]. As Conway and Sloane [3] say use these figures for comparison only.

Our decoding algorithm involves projecting the codewords of C onto the codewords of the *hexacode* H, – the unique (6,3,4) linear code over $GF(4)$. The elements of $GF(4)$, – $0,1,\omega,\bar{\omega}$ will be hereafter called *characters*. We represent binary vectors of length 24 by 4×6 arrays with entries from $GF(2)$. A row or a column of such array is called *odd* or *even* according as it contains an odd or even number of nonzeros. Let now $\underline{u}$ be the 4–tuple $(0,1,\omega,\bar{\omega})$ over $GF(4)$. Any column 4–tuple $\underline{a} = (a_1,a_2,a_3,a_4)$ over $GF(2)$ satisfying $\underline{u}\cdot\underline{a} = \alpha$, where $\alpha \in GF(4)$, is said to be an *interpretation* the character α. Conversely, α is said to be a *projection* of $\underline{a}$. By taking the projection of each of the six columns of the 4×6 array we may project binary vectors of length 24 onto quaternary vectors of length 6.

DEFINITION [7]. *The code C is the set of all the 4×6 arrays with elements from $GF(2)$, which satisfy the following conditions:*

(i). *The parity of all the columns is the same, i.e. all the columns are either even or odd.*
(ii). *The parity of the columns equals the parity of the top row.*
(iii). *The projection is in the hexacode.*

Now assume that a codeword of C is transmitted through a binary channel with output alphabet $\mathbb{R}$, characterized by the transition probability densities $f_j(v) = f(v/j)$, where $j \in GF(2)$ and $v \in \mathbb{R}$. Let the vector $\underline{v} = (v_1,v_2,\ldots v_{24})$ be observed at the output. As shown in [1] maximum–likelihood soft–decision decoding consists of finding a codeword $\underline{c} = (c_1,c_2,\ldots c_{24}) \in C$ which maximizes the *metric* $M(\underline{c})$ given by

$$M(\underline{c}) = \sum_{i=1}^{24} (-1)^{c_i}\,\mu_i \qquad ,$$

where $\mu_i = \log\left[f_0(v_i)/f_1(v_i)\right]$ is the *confidence value* of the i–th bit. The 24 real values $\mu_1,\mu_2,\ldots\mu_{24}$ are the input to our decoder. The decoding algorithm is described in five steps:

1. For each of the six coordinates of H, i.e. $j = 1,2,3,4,5,6$ and for each character we compute the *confidence value of the even interpretation* $\mu_j^e(x)$ and the *confidence value of the odd interpretation* $\mu_j^o(x)$. The confidence values $\mu_1^e(x)$ and $\mu_1^o(x)$ are defined as follows

$$\mu_1^e(0) = |\mu_1+\mu_2+\mu_3+\mu_4| \qquad \mu_1^o(0) = |\mu_1-\mu_2-\mu_3-\mu_4|$$
$$\mu_1^e(1) = |\mu_1+\mu_2-\mu_3-\mu_4| \qquad \mu_1^o(1) = |\mu_1-\mu_2+\mu_3+\mu_4|$$
$$\mu_1^e(\omega) = |\mu_1-\mu_2+\mu_3-\mu_4| \qquad \mu_1^o(\omega) = |\mu_1+\mu_2-\mu_3+\mu_4|$$
$$\mu_1^e(\bar{\omega}) = |\mu_1-\mu_2-\mu_3+\mu_4| \qquad \mu_1^o(\bar{\omega}) = |\mu_1+\mu_2+\mu_3-\mu_4|$$

while the confidence values of the other coordinates are defined similarly. Note that using a Gray code this step may be performed with only 10 real additions per coordinate.

2. For each of the six coordinates we sort the confidence values of even and odd interpretations in nondecreasing order.

3. If $\underline{x} = (x_1,x_2,x_3,x_4,x_5,x_6)$ is any vector in $GF(4)^6$ the sets $\{x_1,x_2\}$, $\{x_3,x_4\}$ and $\{x_5,x_6\}$ are said to be the *blocks* of $\underline{x}$. For each of the 4096 vectors $\underline{x} \in GF(4)^6$ we compute the *sums* $S_j^e(x_1,x_2)$, $S_j^o(x_1,x_2)$ and the *differences* $D_j^e(x_1,x_2)$, $D_j^o(x_1,x_2)$, where $j = 1,2,3$ runs through the blocks of $\underline{x}$. For the first block the sums and the differences are defined by:

$$S_1^e(x_1,x_2) = \mu_1^e(x_1) + \mu_2^e(x_2), \quad S_1^o(x_1,x_2) = \mu_1^o(x_1) + \mu_2^o(x_2)$$

$$D_1^e(x_1,x_2) = |\mu_1^e(x_1) - \mu_2^e(x_2)|, \quad D_1^o(x_1,x_2) = |\mu_1^o(x_1) - \mu_2^o(x_2)|$$

while for the other two blocks they are defined similarly.

4. In each of the 64 hexacodewords we locate the least reliable character in even interpretation and in odd interpretation, by means of an appropriate sorting of

$$\{\mu_1^e(0),\mu_1^e(1),\mu_1^e(\omega),\mu_1^e(\bar{\omega});\ \ldots\ ;\ \mu_6^e(0),\mu_6^e(1),\mu_6^e(\omega),\mu_6^e(\bar{\omega})\}$$

$$\{\mu_1^o(0),\mu_1^o(1),\mu_1^o(\omega),\mu_1^o(\bar{\omega});\ \ldots\ ;\ \mu_6^o(0),\mu_6^o(1),\mu_6^o(\omega),\mu_6^o(\bar{\omega})\}$$

5. For each of the 64 hexacodewords $\underline{x} = (x_1,x_2,x_3,x_4,x_5,x_6) \in H$ we compute the metric of $\underline{x}$ in even interpretation and in odd interpretation, according to

$$M^e(\underline{x}) = S_1^e(x_1,x_2)+S_2^e(x_3,x_4)+S_3^e(x_5,x_6)$$

$$M^o(\underline{x}) = S_1^o(x_1,x_2)+S_2^o(x_3,x_4)+S_3^o(x_5,x_6)$$

provided that the interpretations of the characters of $\underline{x}$ satisfy condition (ii) of the definition. If condition (ii) is violated and the least reliable character of $\underline{x}$ belongs to the j–th block, we replace $S_j^e(x_1,x_2)$ by $D_j^e(x_1,x_2)$ and/or $S_j^o(x_1,x_2)$ by $S_j^e(x_1,x_2)$. Among all the codewords of H we choose the codeword $\hat{\underline{x}}$ which has the highest metric in either interpretation, and decode to the codeword $\hat{\underline{c}} \in C$ whose projection is $\hat{\underline{x}}$. ∎

The complexity of the foregoing five steps is at most 60, 18, 192, 62, and 319 real operations, respectively. Thus the total number of real additions and comparisons required in our algorithm is 651 in the worst case, as compared to the best decoding algorithm presently known [8] which requires 827 such operations.

REFERENCES

[1] Y. Be'ery and J. Snyders, "Optimal soft decision block decoders based on Fast Hadamard Transform," *IEEE Trans. Inform. Theory*, vol.32, pp. 355–364, 1986.

[2] Y. Be'ery and J. Snyders, "New methods for soft decision decoding of the Golay (24,12) code," in *Proc. IEEE 15th Conf. Electr. Eng. in Israel*, Israel, 1987.

[3] J.H. Conway and N.J.A. Sloane, "Soft decoding techniques for codes and lattices, including the Golay code and the Leech lattice," *IEEE Trans. Inform. Theory*, vol.32, pp. 41–50, 1986.

[4] G.D. Forney, Jr., "Coset codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, vol.34, pp.1152–1187, 1988.

[5] G.D. Forney, Jr., "Coset codes III: Ternary codes, lattices and trellis codes," *IEEE Trans. Inform. Theory*, to appear.

[6] G.D. Forney, Jr., "A bounded distance decoding algorithm for the Leech lattice, with generalizations," *IEEE Trans. Inform. Theory*, vol.35. pp. 906–909, 1989.

[7] V.S. Pless, "Decoding the Golay Codes," *IEEE Trans. Inform. Theory*, vol.32, pp. 561–567, 1986.

[8] J. Snyders and Y. Be'ery, "Maximum likelihood soft decoding of binary block codes and decoders for the Golay codes," *IEEE Trans. Inform. Theory*, vol.35, pp. 963–975, 1989.