Decoding the Golay Code with Venn Diagrams

MARIO BLAUM AND JEHOSHUA BRUCK

***Abstract*—A decoding algorithm based on Venn diagrams to decode the [23, 12, 7] Golay code is presented. The decoding algorithm is based on the "design" properties of the parity sets of the code. As for other decoding algorithms for the Golay code, decoding can be easily done by hand.**

I. Introduction

Let C be a binary linear $[n,k,d]$ error-correcting code [4] defined by the parity-check matrix H. Let

$$H=\begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_{n-k} \end{pmatrix},$$

where each $\boldsymbol{h}_j$ is a binary vector of length n. We associate to each $\boldsymbol{h}_j$ its support A_j, where the support of a vector is the set of coordinates corresponding to nonzero elements. For example, the support of $v=(10101\cdots)$ is $\{1,3,5,\cdots\}$. The sets A_j are called parity sets of C. Let $\boldsymbol{v}$ be a codeword transmitted through a noisy channel, and $\boldsymbol{r}$ be the received vector, i.e., $\boldsymbol{r}=\boldsymbol{v}\oplus\boldsymbol{e}$, where $\boldsymbol{e}$ is the error vector ("$\oplus$" denotes exclusive OR). There is a one-to-one correspondence between error patterns of weight $\le\lfloor(d-1)/2\rfloor$ and syndromes [4], where the syndrome of $\boldsymbol{e}$ is the vector of length $n-k$ defined as

$$\boldsymbol{s}=(s_1,s_2,\cdots,s_{n-k})=\boldsymbol{e}H^T=\boldsymbol{r}H^T$$

where H^T denotes the transpose of H.

We denote by E the support of the error vector $\boldsymbol{e}$. We call the set E the error set. The goal of the decoder is to determine the error set E from the syndrome $\boldsymbol{s}$. Notice that

$$\boldsymbol{s}=\boldsymbol{e}H^T=(\boldsymbol{e}\cdot\boldsymbol{h}_1,\boldsymbol{e}\cdot\boldsymbol{h}_2,\cdots,\boldsymbol{e}\cdot\boldsymbol{h}_{n-k}) \tag{1}$$

where the single center dot denotes inner product. The inner product between two binary vectors is equal to the parity of the intersection of their supports, i.e.,

$$\boldsymbol{s}=\boldsymbol{e}H^T$$
$$=(|E\cap A_1|\bmod 2,|E\cap A_2|\bmod 2,\cdots,|E\cap A_{n-k}|\bmod 2). \tag{2}$$

From (2), we see that the parity set A_j contains an odd number of locations in error if and only if $s_j=1$ $(1\le j\le n-k)$. If $s_j=1$, we say that A_j is flagged; otherwise, A_j is unflagged. If set A_j is flagged then it contains at least one location in error. Using this observation, we can easily see that the following decoding algorithm corrects one error (a nice description of the algorithm using Venn diagrams is presented in [5]).

Decoding Algorithm 1.1 (for 1-Error Correcting Codes)

Let C be a binary $[n,k,d]$ 1-error-correcting code (i.e., $d\ge 3$) defined by the parity sets $A_1,A_2,\cdots,A_{n-k}$. Using the previous notation, assume that no more than one error has occurred during transmission. Denote the flagged sets by $F_1,F_2,\cdots,F_w$ and the unflagged sets by $U_1,U_2,\cdots,U_{n-k-w}$. Then

$$E=F_1F_2\cdots F_w\bar{U}_1\bar{U}_2\cdots\bar{U}_{n-k-w},$$

where $E=\emptyset$ if $w=0$, AB denotes $A\cap B$ and $\bar{A}$ is the complement of A with respect to $\{1,2,\cdots,n\}$.

Example 1.1: Consider the [7,4] Hamming code [4] in which the parity-check matrix is

$$H=\begin{pmatrix} 1&1&0&1&1&0&0\\ 1&0&1&1&0&1&0\\ 0&1&1&1&0&0&1 \end{pmatrix}.$$

The parity-check sets are $A_1=\{1,2,4,5\}$, $A_2=\{1,3,4,6\}$ and $A_3=\{2,3,4,7\}$. Assume we receive $\boldsymbol{r}=(1001\ 010)$. Since H is in systematic form [4], the first four bits are the information bits. The syndrome is $\boldsymbol{s}=\boldsymbol{r}H^T=(011)$. So, set A_1 is unflagged and sets A_2 and A_3 are flagged. Applying algorithm 1.1, $E=\bar{A}_1A_2A_3=\{3\}$. So, bit 3 is in error and $\boldsymbol{r}$ is decoded as $\boldsymbol{v}=(1011\ 010)$. If we are only interested in the information symbols, we decode $\boldsymbol{r}$ as (1011).

We end this section by presenting a simplified version of the decoding algorithm 1.1 for the [7,4] Hamming code. The idea is to use at most one parity set at a time for decoding. A similar principle will be used later to decode the Golay code. Given the parity sets A_1, A_2, and A_3 of Example 1.1 we eliminate from them the locations corresponding to the redundancy (5, 6, and 7) as well as location 4. With this new definition, the parity sets are $A_1=\{1,2\}$, $A_2=\{1,3\}$ and $A_3=\{2,3\}$.

The error set E will contain elements from $\{1,2,3,4\}$ only, since we are not interested in errors in the redundant bits. Complements are now taken with respect to the generic set $\{1,2,3\}$. Let w be the weight of the syndrome. The algorithm makes a decision based on w.

Decoding Algorithm 1.2 (for the [7, 4] Hamming Code)

Given a syndrome $\boldsymbol{s}$ of weight w, the error set E is obtained as follows.

1) $w\le 1\Rightarrow E=\emptyset$.
2) $w=2\Rightarrow E=$ complement of the unflagged set.
3) $w=3\Rightarrow E=\{4\}$.

For instance, applying Algorithm 1.2 to the syndrome in Example 1.1, since the unflagged set is A_1 then $E=\bar{A}_1=\{3\}$. The main contribution of this correspondence is a decoding algorithm for the [23,12,7] Golay code. The algorithm finds the error set E using set operations on the parity sets similar to Algorithm 1.2. It is not a surprise that the Golay code is more complicated to handle. We need to study the relations between subsets of size 1, 2, or 3 (since the Golay code is 3-error-correcting) with respect to the parity sets of the code. This will be done in the next section. The actual decoding algorithm is stated and proved in Section III.

II. Partial Descriptions and Configurations of Sets

In this section, we consider subsets of a generic set $\{1,2,\cdots,u\}$. Given two subsets A and B, we denote by AB their intersection $A\cap B$ and by $\bar{A}$ the complement of A with respect to $\{1,2,\cdots,u\}$.

Manuscript received July 21, 1988; revised November 15, 1989. This work was presented in part at the Advanced International Workshop on Sequences, Positano, Italy, June 1988.

The authors are with IBM Research, Almaden Research Center, San Jose, CA 95120.

IEEE Log Number 9034944.

Definition 2.1: Let A be a subset of $\{1,2,\cdots,u\}$. We say that $\langle a_1,a_2,\cdots,a_t\rangle b_1,b_2,\cdots,b_w$ is a partial description of A if and only if $\{a_1,a_2,\cdots,a_t\}\subseteq A$ and $\{b_1,b_2,\cdots,b_w\}\subseteq \bar{A}$. We use the notation $A\approx\langle a_1,a_2,\cdots,a_t\rangle b_1,b_2,\cdots,b_w$. Of course, in general, a partial description of a set is not unique. The following lemma is clear.

Lemma 2.1: Let A be a set having two partial descriptions, $A\approx\langle a_1,a_2,\cdots,a_t\rangle b_1,b_2,\cdots,b_w$ and

$$A\approx\langle a_1',a_2',\cdots,a_{t'}'\rangle b_1',b_2',\cdots,b_{w'}',$$

then A has the partial description

$$A\approx\langle\{a_1,a_2,\cdots,a_t\}\cup\{a_1',a_2',\cdots,a_{t'}'\}\rangle\{b_1,b_2,\cdots,b_w\}\cdot\cup\{b_1',b_2',\cdots,b_{w'}'\}.$$

For example, if $A\approx\langle 1,2\rangle 3,4$ and $A\approx\langle 1,5,6\rangle 4,7$, then $A\approx\langle 1,2,5,6\rangle 3,4,7$. The next concept we want to convey is the one of configuration.

Definition 2.2: Given a family of subsets $A_1,A_2,\cdots,A_m$ and a fixed subset $C=\{c_1,c_2,\cdots,c_t\}$ of $\{1,2,\cdots,u\}$, the configuration determined by C with respect to $A_1,A_2,\cdots,A_m$ is the family of partial descriptions of $A_1,A_2,\cdots,A_m$ given by using only the elements of C.

Example 2.1: Let the generic set be $\{1,2,3\}$ and $A_1=\{1,2\}$, $A_2=\{1,3\}$, $A_3=\{2,3\}$ (these sets were defined in the previous section as modified parity sets of the [7,4] Hamming code). Let $C=\{1\}$. Then a configuration of C with respect to A_1,A_2,A_3 is $A_1\approx\langle 1\rangle$, $A_2\approx\langle 1\rangle$, $A_3\approx\langle\ \rangle 1$.

A way to denote the configuration in Example 2.1 is as follows:

$$\begin{array}{ll}\langle 1\rangle & \langle\ \rangle 1\\ \langle 1\rangle & \end{array}.$$

In other words, we have two columns: in the first column, we write the sets that contain one element of C, while in the second column we write the sets that contain no elements of C. The next example deals with the parity sets of the [23,12,7] Golay code.

Example 2.2: The [23,12,7] Golay code can be defined as the code in which the parity-check matrix in systematic form is [4] $H=(P|I_{11})$, where I_{11} is the 11×11 identity matrix and P is the 11×12 matrix

$$P=\begin{pmatrix}1&0&1&0&0&0&1&1&1&0&1&1\\1&1&0&1&0&0&0&1&1&1&0&1\\0&1&1&0&1&0&0&0&1&1&1&1\\1&0&1&1&0&1&0&0&0&1&1&1\\1&1&0&1&1&0&1&0&0&0&1&1\\1&1&1&0&1&1&0&1&0&0&0&1\\0&1&1&1&0&1&1&0&1&0&0&1\\0&0&1&1&1&0&1&1&0&1&0&1\\0&0&0&1&1&1&0&1&1&0&1&1\\1&0&0&0&1&1&1&0&1&1&0&1\\0&1&0&0&0&1&1&1&0&1&1&1\end{pmatrix}. \quad (3)$$

Using the notation of Section I, the sets A_j, $1\le j\le 11$, have eight elements each. Observe that element 12 appears in all of the sets and element $12+j$ appears exactly once in set A_j. We redefine the parity sets in such a way that elements 12 and $12+j$ are excluded and the generic set is $\{1,2,\cdots,11\}$. Thus, we have

$$\begin{aligned}A_1&=\{1,3,7,8,9,11\}\\A_2&=\{1,2,4,8,9,10\}\\A_3&=\{2,3,5,9,10,11\}\\A_4&=\{1,3,4,6,10,11\}\\A_5&=\{1,2,4,5,7,11\}\\A_6&=\{1,2,3,5,6,8\}\\A_7&=\{2,3,4,6,7,9\}\\A_8&=\{3,4,5,7,8,10\}\\A_9&=\{4,5,6,8,9,11\}\\A_{10}&=\{1,5,6,7,9,10\}\\A_{11}&=\{2,6,7,8,10,11\}.\end{aligned}$$

For example, the configuration determined by $C=\{1,2\}$ is

$$\begin{array}{lll}\langle 1,2\rangle & \langle 1\rangle 2 & \langle\ \rangle 1,2\\ \langle 1,2\rangle & \langle 1\rangle 2 & \langle\ \rangle 1,2\\ \langle 1,2\rangle & \langle 1\rangle 2 & \\ & \langle 2\rangle 1 & \\ & \langle 2\rangle 1 & \\ & \langle 2\rangle 1 & \end{array}.$$

As we can see, we denote the configuration of a subset C with respect to sets $A_1,A_2,\cdots,A_m$ with $|C|+1$ columns: in the first column, we write all the partial descriptions containing the $|C|$ elements of C; in the second column, we write all the partial descriptions containing $|C|-1$ elements of C; and so on. Eventually, in the last column, we write all the partial descriptions containing no elements of C. From now on, we concentrate on the configurations associated with the Golay code. We are interested in configurations of sets of size up to 3, for reasons that will become clear in the next section.

Consider the sets $A_1,A_2,\cdots,A_{11}$ defined in Example 2.2. The following two lemmas describe the basic properties of the sets.

Lemma 2.2: Let a,b,c be elements of $\{1,2,\cdots,11\}$. We then have the following.

1) $\{a\}$ is contained in exactly six sets.
2) $\{a,b\}$ is contained in exactly three sets.
3) $\{a,b\}$ is disjoint with exactly two sets.
4) $\{a,b,c\}$ is contained in either one or two sets.
5) $\{a,b,c\}$ is disjoint with at most one set.

The next lemma is the dual of the previous one.

Lemma 2.3: Let A_i,A_j,A_k be any three of the sets in Example 2.2. We then have the following.

1) A_i contains exactly six elements.
2) A_iA_j contains exactly three elements.
3) $\bar{A}_i\bar{A}_j$ contains exactly two elements.
4) $A_iA_jA_k$ contains either one or two elements.
5) $\bar{A}_i\bar{A}_j\bar{A}_k$ contains at most one element.

The next step is to find the configuration of sets of size up to 3 with respect to the 11 sets. As we can see from Lemma 2.2, there are two possibilities for a subset of size 3. We say that $\{a,b,c\}$ is of class 1 if it is contained in exactly one set A_j, $1\le j\le 11$. Otherwise we say that $\{a,b,c\}$ is of class 2.

The next lemma is an easy corollary of Lemma 2.2. It describes the complete configurations of subsets with one, two, and three elements.

Lemma 2.4: Let $\{a,b,c\}\subset\{1,2,\cdots,11\}$. Then we have the following.

1) $\{a\}$ has the following configuration:

$$\begin{array}{l}\langle a\rangle \quad \langle\ \rangle a\\ \langle a\rangle \quad \langle\ \rangle a\\ \langle a\rangle \quad \langle\ \rangle a\\ \langle a\rangle \quad \langle\ \rangle a\\ \langle a\rangle \quad \langle\ \rangle a\\ \langle a\rangle\end{array}.$$

2) $\{a,b\}$ has the following configuration:

$$\begin{array}{lll}\langle a,b\rangle & \langle a\rangle b & \langle\ \rangle a,b\\ \langle a,b\rangle & \langle a\rangle b & \langle\ \rangle a,b\\ \langle a,b\rangle & \langle a\rangle b & \\ & \langle b\rangle a & \\ & \langle b\rangle a & \\ & \langle b\rangle a & \end{array}.$$

3) $\{a,b,c\}$ has only two possible configurations.
   a) If $\{a,b,c\}$ is of class 1, then it has the following configuration:

$$\begin{array}{llll}\langle a,b,c\rangle & \langle a,b\rangle c & \langle a\rangle b,c & \langle\ \rangle a,b,c\\ & \langle a,b\rangle c & \langle b\rangle a,c & \\ & \langle a,c\rangle b & \langle c\rangle a,b & \\ & \langle a,c\rangle b & & \\ & \langle b,c\rangle a & & \\ & \langle b,c\rangle a & & \end{array}.$$

   b) If $\{a,b,c\}$ is of class 2, then it has the following configuration:

$$\begin{array}{lll}\langle a,b,c\rangle & \langle a,b\rangle c & \langle a\rangle b,c\\ \langle a,b,c\rangle & \langle a,c\rangle b & \langle a\rangle b,c\\ & \langle b,c\rangle a & \langle b\rangle a,c\\ & & \langle b\rangle a,c\\ & & \langle c\rangle a,b\\ & & \langle c\rangle a,b\end{array}.$$

The proofs of the previous three lemmas follow from observing the structure of the sets $A_1,A_2,\cdots,A_{11}$. It is also possible to prove the lemmas by using the theory of t-designs [4]: the 11 sets correspond to a Hadamard two-design and the statement about three-sets can be obtained using the concept of block intersection numbers.

The next results are concerned with some particular intersections of the sets $A_1,A_2,\cdots,A_{11}$. They will be used in the next section. We prove only one of them, the others are proved similarly. In all cases $\{a,b,c\}\subset\{1,2,\cdots,11\}$.

Lemma 2.5: Consider the configuration of $\{a,b\}$ in Lemma 2.4. Let $A_{i_1}\approx\langle a,b\rangle$, $A_{i_2}\approx\langle a,b\rangle$, $A_{i_3}\approx\langle a,b\rangle$, $A_{i_4}\approx\langle\ \rangle a,b$, and $A_{i_5}\approx\langle\ \rangle a,b$. Then

1) $A_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}\bar{A}_{i_5}=\{a,b\}$;
2) $A_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}A_{i_5}=\varnothing$;
3) $A_{i_1}\bar{A}_{i_2}A_{i_3}A_{i_4}A_{i_5}=\varnothing$.

Proof:

1) Clearly, $\{a,b\}\subset A_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}\bar{A}_{i_5}$. By Lemma 2.2, a subset of three elements cannot be contained in more than two sets A_j, so we have equality.
2) Assume $c\in A_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}\bar{A}_{i_5}$, $c\notin\{a,b\}$. Then, $A_{i_1}\approx\langle a,b,c\rangle$, $A_{i_2}\approx\langle a,b,c\rangle$, $A_{i_3}\approx\langle a,b\rangle c$, $A_{i_4}\approx\langle c\rangle a,b$, and $A_{i_5}\approx\langle\ \rangle a,b,c$. Since $\{a,b,c\}$ appears in two sets, it is of class 2. By Lemma 2.4, there is no set in the configuration of $\{a,b,c\}$ in which the partial description is $\langle\ \rangle a,b,c$. But $A_{i_5}\approx\langle\ \rangle a,b,c$, which is a contradiction.
3) Assume $c\in A_{i_1}\bar{A}_{i_2}\bar{A}_{i_3}A_{i_4}A_{i_5}$. Then, $A_{i_1}\approx\langle a,b,c\rangle$, $A_{i_2}\approx\langle a,b\rangle c$, $A_{i_3}\approx\langle a,b\rangle c$, $A_{i_4}\approx\langle c\rangle a,b$, and $A_{i_5}\approx\langle c\rangle a,b$. Since both A_{i_2} and A_{i_3} have the partial description $\langle a,b\rangle c$, by Lemma 2.4 we conclude that $\{a,b,c\}$ is of class 1. Also by Lemma 2.4, since both A_{i_4} and A_{i_5} have the partial description $\langle c\rangle a,b$, $\{a,b,c\}$ is of class 2. This is a contradiction. □

Lemma 2.6: In the configuration of $\{a,b\}$, let $A_{i_1}\approx\langle a\rangle b$, $A_{i_2}\approx\langle a\rangle b$, $A_{i_3}\approx\langle a\rangle b$, $A_{i_4}\approx\langle b\rangle a$ and $A_{i_5}\approx\langle b\rangle a$. We then have the following.

1) $A_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}\bar{A}_{i_5}=\{a\}$ and $\bar{A}_{i_1}\bar{A}_{i_2}\bar{A}_{i_3}A_{i_4}A_{i_5}=\{b\}$.
2) $A_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}A_{i_5}=\varnothing$ or $\bar{A}_{i_1}\bar{A}_{i_2}A_{i_3}\bar{A}_{i_4}A_{i_5}=\varnothing$.
3) $A_{i_1}\bar{A}_{i_2}A_{i_3}A_{i_4}A_{i_5}=\varnothing$ or $\bar{A}_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}A_{i_5}=\varnothing$.

Lemma 2.7: In the configuration of $\{a,b\}$, let $A_{i_1}\approx\langle a,b\rangle$, $A_{i_2}\approx\langle a,b\rangle$, $A_{i_3}\approx\langle\ \rangle a,b$ and $A_{i_4}\approx\langle\ \rangle a,b$. Then we have the following.

1) $A_{i_1}A_{i_2}\bar{A}_{i_3}\bar{A}_{i_4}=\{a,b\}$.
2) $|A_{i_1}\bar{A}_{i_2}A_{i_3}\bar{A}_{i_4}|<2$.
3) $|\bar{A}_{i_1}\bar{A}_{i_2}A_{i_3}A_{i_4}|<2$.
4) $|A_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}|<2$.
5) $|A_{i_1}\bar{A}_{i_2}A_{i_3}A_{i_4}|<2$.

Lemma 2.8: In the configuration of $\{a,b\}$, let $A_{i_1}\approx\langle a,b\rangle$, $A_{i_2}\approx\langle a,b\rangle$, $A_{i_3}\approx\langle a,b\rangle$ and $A_{i_4}\approx\langle\ \rangle a,b$. Then we have the following.

1) $A_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}=\{a,b\}$.
2) $|A_{i_1}\bar{A}_{i_2}\bar{A}_{i_3}\bar{A}_{i_4}|<2$.
3) $|\bar{A}_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}|<2$.
4) $|A_{i_1}A_{i_2}\bar{A}_{i_3}A_{i_4}|<2$.

Lemma 2.9: Let $\{a,b,c\}$ be of class 1. In the configuration of $\{a,b,c\}$, let $A_{i_1}\approx\langle a,b,c\rangle$, $A_{i_2}\approx\langle a\rangle b,c$, $A_{i_3}\approx\langle b\rangle a,c$, $A_{i_4}\approx\langle c\rangle a,b$. We then have the following.

1) $A_{i_1}A_{i_2}\bar{A}_{i_3}\bar{A}_{i_4}=\{a\}$.
2) $A_{i_1}A_{i_2}A_{i_3}\bar{A}_{i_4}=\varnothing$.

Lemma 2.10: Let $\{a,b,c\}$ be of class 2. In the configuration of $\{a,b,c\}$, let $A_{i_1}\approx\langle b,c\rangle a$, $A_{i_2}\approx\langle a,c\rangle b$ and $A_{i_3}\approx\langle a,b\rangle c$. Then $A_{i_1}A_{i_2}\bar{A}_{i_3}=\{c\}$.

III. Decoding of the [23,12,7] Golay Code

In this section we state and prove the decoding algorithm for the [23,12,7] Golay code. The proof strongly relies on the results of the previous section. For several other methods to decode the Golay code the reader is referred to [1]–[4], [6], [7], [8]. Some of these other decoding algorithms can also be done by hand and have similar complexity. The algorithm performs set operations (union, intersection and complement) on either the flagged or unflagged parity sets, whichever is smaller. So, the algorithm works with at most five sets at a time. As with the [7,4] Hamming code, we restrict the set E to the information bits (i.e., $E\subset\{1,2,\cdots,12\}$).

Let w be the weight of the syndrome and $m = \min\{w, 11-w\}$. So there are either m flagged or m unflagged sets. Denote those m flagged or unflagged sets by $B_1, B_2, \cdots, B_m$. The next decoding algorithm for the [23,12,7] Golay code is our main result.

Decoding Algorithm 3.1 for the [23, 12, 7] Golay Code

The error set E is found by one of the following set operations.

1) $w \le 3$ then $E = \emptyset$.
2) $w = 4$ then:
   a) $E = \{i\}$, where $\{i\} = B_1 B_2 B_3 B_4$; or
   b) $E = \{i, 12\}$, where $\{i\} = \bar{B}_1 \bar{B}_2 \bar{B}_3 \bar{B}_4$; or
   c) $E = \{i, j, k\}$, where $\{i, j, k\} = \cup B_a B_b \bar{B}_c \bar{B}_d$, the union running over the six partitions $\{a, b\} \cup \{c, d\} = \{1,2,3,4\}$.
3) $w = 5$ then:
   a) $E = \{i\}$, where $\{i\} = B_1 B_2 B_3 B_4 B_5$; or
   b) $E = \{i, 12\}$, where $\{i\} = \bar{B}_1 \bar{B}_2 \bar{B}_3 \bar{B}_4 \bar{B}_5$; or
   c) $E = \{i, j, 12\}$, where $\{i, j\} = B_a B_b B_c \bar{B}_d \bar{B}_e$ for one of the ten partitions $\{a,b,c\} \cup \{d,e\} = \{1,2,3,4,5\}$; or
   d) $E = \{i, j\}$, where $\{i\} = B_a B_b B_c \bar{B}_d \bar{B}_e$ and $\{j\} = \bar{B}_a \bar{B}_b \bar{B}_c B_d B_e$ for one of the ten partitions $\{a,b,c\} \cup \{d,e\} = \{1,2,3,4,5\}$.
4) $w = 6$ then:
   a) $E = \{i, 12\}$, where $\{i\} = B_1 B_2 B_3 B_4 B_5$; or
   b) $E = \{i\}$, where $\{i\} = \bar{B}_1 \bar{B}_2 \bar{B}_3 \bar{B}_4 \bar{B}_5$ or $\{i\} = B_a \bar{B}_b \bar{B}_c \bar{B}_d \bar{B}_e$ for one of the five partitions $\{a\} \cup \{b, c, d, e\} = \{1,2,3,4,5\}$; or
   c) $E = \{i, j\}$, where $\{i, j\} = B_a B_b B_c \bar{B}_d \bar{B}_e$, for one of the ten partitions $\{a,b,c\} \cup \{d,e\} = \{1,2,3,4,5\}$.
5) $w = 7$ then:
   a) $E = \{i\}$, where $\{i\} = \bar{B}_1 \bar{B}_2 \bar{B}_3 \bar{B}_4$; or
   b) $E = \{i, j\}$, where $\{i, j\} = B_a B_b \bar{B}_c \bar{B}_d$ for one of the six partitions $\{a, b\} \cup \{c, d\} = \{1, 2, 3, 4\}$, or $\{i, j\} = B_a B_b B_c \bar{B}_d$ for one of the four partitions $\{a,b,c\} \cup \{d\} = \{1,2,3,4\}$.
6) $w = 8$ then:
   a) $E = \{i\}$, where $\{i\} = \bar{B}_1 \bar{B}_2 \bar{B}_3$; or
   b) $E = \{i, j, k\}$, where $\{i, j, k\} = B_1 B_2 \bar{B}_3 \cup B_1 \bar{B}_2 B_3 \cup \bar{B}_1 B_2 B_3$.
7) $w \ge 9$, then $E = \{12\}$.

Proof: The proof considers all cases of a errors in the information bits and b errors in the redundant bits, $a + b \le 3$. Then we verify that each case of error is solved by a step in the decoding algorithm.

1) No errors in the information bits; then $w \le 3$ and Step 1 of the algorithm takes care of this case.
2) Exactly one error in bit i, $1 \le i \le 11$; there are three subcases.
   a) No errors in the redundancy; since i is contained in exactly six sets (Lemma 2.2), then $w = 6$. By Step 4b) of the algorithm, $\cap_{j=1}^{5} \bar{B}_j = \{i\}$, finding the error in i.
   b) One error in the redundancy; we have two possibilities.
      - $w = 5$. Since the error is in the five flagged sets, it is found by Step 3a) of the algorithm. The intersection of five sets cannot contain more than one element by Lemma 2.2.
      - $w = 7$. Since the error is in none of the four unflagged sets, it is found by Step 5a) of the algorithm. By Lemma 2.2, the intersection of the complements of four sets cannot contain more than one element.
   c) Two errors in the redundancy; we have three possibilities.
      - $w = 4$. The error is found by Step 2a) of the algorithm.
      - $w = 6$. The error will be in exactly one unflagged set and will not be in the other four unflagged sets, hence, it is found by Step 4b).
      - $w = 8$. The error is found by Step 6a).
3) One error in bit 12; we may have either no errors, one error or two errors in the redundancy. Any set such that only bit 12 is in error (and not its redundant bit) is flagged, hence $w = 11$, 10 or 9, and the error is determined by Step 7 of the algorithm.
4) Two errors in bits i and j, $1 \le i < j \le 11$; there are two subcases.
   a) No errors in the redundancy; by Lemma 2.4, subset $\{i, j\}$ is contained in exactly three sets and it is disjoint with exactly two sets. These five sets are unflagged, hence $w = 6$. The errors are then found by Step 4c) of the algorithm. Lemma 2.5 assures that we obtain the right solution, since all the intersections are empty except for one.
   b) One error in the redundancy; there are two possibilities.
      - $w = 5$; without loss of generality, we may assume that three of the flagged sets contain i and do not contain j, while the other two flagged sets contain j and do not contain i. So i is in one of the ten intersections $B_a B_b B_c \bar{B}_d \bar{B}_e$ of Step 3d), while j is in its "conjugate" $\bar{B}_a \bar{B}_b \bar{B}_c B_d B_e$. Lemma 2.6 assures that there is only one partition $\{a,b,c\} \cup \{d,e\}$ with this property.
      - $w = 7$; if the error in the redundancy corresponds to one of the three sets containing $\{i, j\}$, then two of the unflagged sets contain $\{i, j\}$ and two of them have empty intersection with $\{i, j\}$. If the error in the redundancy corresponds to one of the two sets in which the intersection with $\{i, j\}$ is empty, then three of the unflagged sets contain $\{i, j\}$ and only one has empty intersection with $\{i, j\}$. In any case, the errors are found by Step 5b). Lemmas 2.7 and 2.8 assure that only one of the ten intersections gives the two locations in error.
5) One error in bit i, $1 \le i \le 11$, and one error in bit 12; there are two subcases.
   a) No errors in the redundancy; in this case $w = 5$, since bit i is in six of the sets (Lemma 2.2), and these sets are unflagged because bit 12 is also in error. Since i is

in none of the five flagged sets, the errors are found by Step 3b).

b) One error in the redundancy; consider the two possibilities.

- $w = 4$; since i is in none of the flagged sets, E is found by Step 2b).
- $w = 6$; bit i is in the five unflagged sets, so E is found by Step 4a).

6) Three errors in bits i, j, and k, where $1 \le i < j < k \le 11$; we have two subcases (Lemma 2.2).

a) The three bits i, j, and k are contained in exactly one set (i.e., $\{i,j,k\}$ is of class 1). Then set $\{i,j,k\}$ has the configuration of Lemma 2.4. There are four flagged sets (i.e., $w = 4$) according to this configuration. Assume that $B_1 \approx \langle abc \rangle$, $B_2 \approx \langle a \rangle bc$, $B_3 \approx \langle b \rangle ac$, $B_4 \approx \langle c \rangle ab$. The errors are then found by Step 2(c). Lemma 2.9 assures that this is the right solution.

b) The three bits i, j, and k are contained in exactly two sets (i.e., $\{i,j,k\}$ is of class 2). Now set $\{i,j,k\}$ is of class 2 and its configuration is given by Lemma 2.4. According to this lemma, there are three unflagged sets. Assume that $B_1 \approx \langle ab \rangle c$, $B_2 \approx \langle ac \rangle b$, $B_3 \approx \langle bc \rangle a$. The errors are then found by Step 6(b). Lemma 2.10 assures that this is the right solution.

7) Two errors in bits i and j, $1 \le i < j \le 11$ and one error in bit 12; the pair $\{i,j\}$ is contained in exactly three sets (Lemma 2.2) and since bit 12 is also in error, these sets are flagged. The other flagged sets are those having empty intersection with $\{i,j\}$. There are two of them (Lemma 2.2), so $w = 5$; the errors are then found by Step 3c). The solution is the right one by Lemma 2.7.

Since the code has minimum distance 7 and we have exhausted all the possibilities, up to three errors will be corrected. □

Example 3.1: Let us look at several syndromes and apply decoding Algorithm 3.1 to them.

1) Let $s = 01110010101$. Since $w = 6$, we go to Step 4 of the algorithm. The unflagged sets are $B_1 = A_1$, $B_2 = A_5$, $B_3 = A_6$, $B_4 = A_8$ and $B_5 = A_{10}$. In Step 4c), we obtain

$$A_1 \bar{A}_5 A_6 A_8 \bar{A}_{10} = \{3,8\} = E.$$

2) Let $s = 10110100101$. Again, we have $w = 6$. The unflagged sets are now $B_1 = A_2$, $B_2 = A_5$, $B_3 = A_7$, $B_4 = A_8$ and $B_5 = A_{10}$. Step 4b) gives

$$\bar{A}_2 A_5 \bar{A}_7 \bar{A}_8 \bar{A}_{10} = \{11\} = E.$$

3) Let $s = 00110111000$. Now we have $w = 5$. The five flagged sets are $B_1 = A_3$, $B_2 = A_4$, $B_3 = A_6$, $B_4 = A_7$ and $B_5 = A_8$. From Step 3a), we obtain that $A_3 A_4 A_6 A_7 A_8 = \{3\} = E$.

IV. Conclusion

We described a decoding algorithm for the [23,12,7] Golay code. The decoding algorithm is based on set operations over no more than five sets at a time. These sets are modified parity sets of the code, and they have six elements each. The regularity of the Golay code makes the algorithm simple enough to be implemented by hand. An interesting research problem is finding similar algorithms for other codes.

Regarding complexity, let us count the number of boolean operations (OR, exclusive OR, AND) needed to decode. The first step is finding the syndrome. This step requires 77 operations (each of the 11 rows in the parity check matrix has weight 8, so we need 7 exclusive-OR operations in each). Then we apply the algorithm itself. The worst case occurs when w, the weight of the syndrome, is 5 (Step 3 in Algorithm 3.1). Then, a) and b) take 44 boolean operations, c) takes 440 (there are 10 cases), and d) also takes 440 operations (half of the intersections were found in c)). This gives a total of 968 operations. If we add the complexity of the syndrome, we have a total of 1045 operations. As a comparison, the worst case of permutation decoding involves computing 14 times the syndrome [3,8]: this gives a total of $14 \times 77 = 1078$ operations.

Let us find average case complexity. We find the average for each step in Decoding Algorithm 3.1, then we add all those partial averages, obtaining the total average. In Step 2a), there are $11\binom{6}{2} = 165$ possible patterns (this case corresponds to one error in the information part and two errors of type $1 \to 0$ in the redundancy). Since each pattern requires 33 operations for decoding (we are multiplying 4 vectors of length 11), Step 2a) requires, on average, $(165 \times 33)/2048$ operations. In Step 2b), there are $11 \times 5 = 55$ possible patterns, since there is an error in one of the first 11 bits, an error in bit 12, and an error of type $1 \to 0$ in the redundancy. So, Step 2b) requires, on average, $(55 \times 66)/2048$ operations (each pattern takes 66 operations, since first it has to be verified that Step 2a) did not occur). As for Step 2c), there are $\binom{11}{4} - 165 - 55 = 110$ patterns. Since each pattern requires $66 + 6 \times 33 + 5 \times 11 = 319$ operations, the average of Step 2c) is $(110 \times 319)/2048$. Adding the average of Steps 2a), 2b), and 2c), the average of Step 2 is

$$\frac{165 \times 33 + 55 \times 66 + 110 \times 319}{2048} \approx 21.6. \tag{4}$$

Using an analogous procedure, we estimate the averages corresponding to Steps 3, 4, 5, and 6 of the algorithm. The average number of operations in Step 3 is ≈ 130.7, in Step 4 it is ≈ 48, in Step 5 it is ≈ 27.5 and in Step 6 it is ≈ 4.1. Adding all these averages together with the 77 operations necessary to find the syndrome, the average number of operations in Decoding Algorithm 3.1 is approximately 279. As a comparison, permutation decoding involves finding the syndrome 7 times on average, giving $77 \times 7 = 539$ operations.

References

[1] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*. New York: Springer-Verlag, 1988.

[2] M. Elia, "Algebraic decoding of the (23,12,7) Golay code," *IEEE Trans. Inform. Theory*, vol. IT-33, no. 1, pp. 150–151, Jan. 1987.

[3] D. M. Gordon, "Minimal permutation sets for decoding the binary Golay codes," *IEEE Trans. Inform. Theory*, vol. IT-28, no. 3, pp. 541–543, May 1982.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[5] R. J. McEliece, "The reliability of computer memories," *Sci. Amer.*, vol. 252, pp. 88–95, Jan. 1985.

[6] V. Pless, "Decoding the Golay codes," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 4, pp. 561–567, July 1986.

[7] G. Solomon and M. M. Sweet, "A Golay puzzle," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 174–175, Jan. 1983.

[8] J. Wolfman, "A permutation decoding of the (24,12,8) Golay code," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 5, pp. 748–750, Sept. 1983.