Two Decoding Algorithms in Group Codes

Fabián Ricardo Molina Gómez - Consuelo Martínez López
Universidad de Oviedo

RECSI 2022, Universidad de Cantabria

Octubre 19, 2022

Notation

We will to consider from now on...

- a finite field $\mathbb{K}$ of order $q = p^m$ where p is prime,
- a linear code $\mathfrak{C}$ over $\mathbb{K}$ with length n and dimension k,
- the minimal distance d and the correcting capability t of $\mathfrak{C}$,
- a codeword $\mathfrak{c} \in \mathfrak{C}$ affected by $\mathfrak{e} \in \mathbb{K}^n$ of weight w,
- the received word $\mathfrak{r} = \mathfrak{c} + \mathfrak{e}$,
- a finite group $G = \{g_1 = 1_G, \ldots, g_n\}$ of order n,
- and the group algebra $\mathbb{K}G$ whose elements are $\mathbb{K}-$linear combinations

$$x = \sum_{i=1}^{n} \alpha_i g_i$$

where $\alpha_i \in \mathbb{K}$ for all $i = 1, \ldots, n$.

Notation

We will to consider from now on...

- a finite field $\mathbb{K}$ of order $q = p^m$ where p is prime,
- a linear code $\mathfrak{C}$ over $\mathbb{K}$ with length n and dimension k,
- the minimal distance d and the correcting capability t of $\mathfrak{C}$,
- a codeword $\mathfrak{c} \in \mathfrak{C}$ affected by $\mathfrak{e} \in \mathbb{K}^n$ of weight w,
- the received word $\mathfrak{r} = \mathfrak{c} + \mathfrak{e}$,
- a finite group $G = \{g_1 = 1_G, \ldots, g_n\}$ of order n,
- and the group algebra $\mathbb{K}G$ whose elements are $\mathbb{K}-$linear combinations

$$x = \sum_{i=1}^{n} \alpha_i g_i$$

where $\alpha_i \in \mathbb{K}$ for all $i = 1, \ldots, n$.

From now on...

- we fix the order of the elements of G and we take $\mathfrak{B} = G$ the $\mathbb{K}-$basis of $\mathbb{K}G$.
- Hence, the elements of $\mathbb{K}^n$ can be written as elements of the group algebra $\mathbb{K}G$ and $\mathfrak{C}$ can be seen as a vector $\mathbb{K}-$subspace of $\mathbb{K}G$.

Definition

It is said that $\mathfrak{C}$ is a $G-$*code over* $\mathbb{K}$, if $\mathfrak{C}$ is a (two-sided) ideal of $\mathbb{K}G$. That is,

$$x\mathfrak{C}y = \mathfrak{C} \qquad \forall x, y \in \mathbb{K}G.$$

In this case, $\mathfrak{C}$ is called *group code*.

From now on...

- we fix the order of the elements of G and we take $\mathfrak{B} = G$ the $\mathbb{K}-$basis of $\mathbb{K}G$.
- Hence, the elements of $\mathbb{K}^n$ can be written as elements of the group algebra $\mathbb{K}G$ and $\mathfrak{C}$ can be seen as a vector $\mathbb{K}-$subspace of $\mathbb{K}G$.

Definition

It is said that $\mathfrak{C}$ is a $G-$*code over* $\mathbb{K}$, if $\mathfrak{C}$ is a (two-sided) ideal of $\mathbb{K}G$. That is,

$$x\mathfrak{C}y = \mathfrak{C} \qquad \forall x, y \in \mathbb{K}G.$$

In this case, $\mathfrak{C}$ is called *group code*.

- From now on, we consider G and $\mathbb{K}$ such that the group algebra $\mathbb{K}G$ is semisimple. That is, q does not divide to n.
- This is equivalent to
$$\mathbb{K}G = \langle e_1 \rangle \oplus \cdots \oplus \langle e_s \rangle$$
where $\langle e_i \rangle$ is a minimal ideal generated by a primitive central idempotent e_i, for all $i \in \{1, \ldots, s\}$.
- The ideals $\langle e_i \rangle$, for all $i \in \{1, \ldots, s\}$, are called the simple components of $\mathbb{K}G$.
- Every two-sided ideal of $\mathbb{K}G$ is generated by a central idempotent e_0 and is a direct sum of some simple components of $\mathbb{K}G$.

- We will assume that e_0 is sum of some $e_i's$ and $\mathfrak{C} = \langle e_0 \rangle$.
- Also, we consider $\mathfrak{C}^+ = \langle e_0^+ \rangle$ where $e_0^+ = 1 - e_0$.
- Hence, $\mathfrak{c} \in \mathbb{K}G$ is a codeword, if and only if, $\mathfrak{c}e_0^+ = 0$.
- The *syndrome of* $\mathfrak{r}$ is defined as $S(\mathfrak{r}) = \mathfrak{r}e_0^+$ and therefore,

$$S(\mathfrak{r}) = (\mathfrak{c} + \mathfrak{e})e_0^+ = \mathfrak{e}e_0^+.$$

- Decoding by minimal distance is equivalent to find the solution $\mathfrak{e} \in \mathbb{K}G$ of *the key equation* $Xe_0^+ = S(\mathfrak{r})$ and whose weight $w \leq t$.

Theorem 1.

Let $\mathfrak{C}$ be a group code that corrects up to t errors and $\mathfrak{r}$ a received word with syndrome $S(\mathfrak{r}) = \mathfrak{r}e_0^+$. If there exists one element that of weight $w \leq t$ and that is a solution of the key equation $Xe_0^+ = S(\mathfrak{r})$, then it is unique.

Syndrome Decoding

- Previously decoding, we compute $g_i e_0^+$, $i = 1, \ldots, n$ and define the column vector C_{g_i} of its coefficients.

Theorem 2.

Suppose that $\mathfrak{C}$ is a $G-$code with minimal distance d. If $b < d$ and $g_{i_1}, \ldots, g_{i_b}$ are distinct elements of G, then

$$\mathcal{C}(g_{i_1}, \ldots, g_{i_b}) = \begin{pmatrix} C_{g_{i_1}} & \cdots & C_{g_{i_b}} \end{pmatrix} \in M_{n \times b}(\mathbb{K}),$$

has rank b.

- Once the word $\mathfrak{r}$ is received, we compute $S = S(\mathfrak{r})$ and consider the column vector S^T of its coefficients.
- The goal is to find $\mathfrak{e} = \alpha_1 g_{i_1} + \cdots + \alpha_q g_{i_w}$ of weight $w \leq t$ such that $\mathfrak{e} e_0^+ = S(\mathfrak{r})$.

- There are no errors ($\mathfrak{e} = 0$), if and only if, $S(\mathfrak{r}) = 0$.
- If the number of errors is $w \leq t$, then $\mathfrak{e} = \alpha_1 g_{i_1} + \cdots + \alpha_t g_{i_t}$ is the unique solution of $Xe_0^+ = S(\mathfrak{r})$, satisfying this property.
- The above occurs, if and only if,

$$X_1 C_{g_{i_1}} + \cdots + X_t C_{g_{i_t}} = S^T,$$

  has unique solution $X_i = \alpha_i$, $i = 1, \ldots, t$.
- This is equivalent to the matrices $\mathcal{C}(g_{i_1}, \ldots, g_{i_t})$ y

$$\mathcal{M}(g_{i_1}, \ldots, g_{i_t}) = \left(\begin{array}{ccc|c} C_{g_{i_1}} & \ldots & C_{g_{i_t}} & S^T \end{array} \right),$$

  have both rank t.

Step 1.

Compute the syndrome $S(\mathfrak{r})$ of $\mathfrak{r}$. If $S(\mathfrak{r}) = 0$, then there are no errors. Otherwise, continue to

Step 2.

Take a $t-$set $\{g_{i_1}, \ldots, g_{i_t}\}$ of G. Consider the matrix $\mathcal{M}(g_{i_1}, \ldots, g_{i_t})$ and compute its rank.

a. If the rank is equal to t, then solve the system

$$X_1 C_{g_{i_1}} + \cdots + X_t C_{g_{i_t}} = S^T.$$

If $\alpha_{j_1}, \ldots, \alpha_{j_w} \neq 0$, then the error is $\mathfrak{e} = \alpha_{j_1} g_{i_{j_1}} + \cdots + \alpha_{j_w} g_{i_{j_w}}$.

b. Otherwise, take another $t-$set of G and repeat step 2.

The algorithm ends when a $t-$set $\{g_{i_1}, \ldots, g_{i_t}\}$ of G is found such that

$$\text{Rank}(\mathcal{M}(g_{i_1}, \ldots, g_{i_t})) = t \qquad \text{(P1)}$$

or when all $t-$sets of G have been evaluated and none satisfies (P1). In the last case, the algorithm concludes that more than t errors have occurred and $\mathfrak{r}$ cannot be decoded.

The algorithm searches for $t-$sets of G satisfying (P1). Thus,

- If $w = t$, the $t-$set that satisfies (P1) is unique.
- If $w < t$, all $t-$sets that satisfy (P1), allow to find the same error $\mathfrak{e}$.
- If $w > t$, no one $t-$set satisfies (P1).

The algorithm ends when a $t-$set $\{g_{i_1}, \ldots, g_{i_t}\}$ of G is found such that

$$\text{Rank}(\mathcal{M}(g_{i_1}, \ldots, g_{i_t})) = t \qquad \text{(P1)}$$

or when all $t-$sets of G have been evaluated and none satisfies (P1). In the last case, the algorithm concludes that more than t errors have occurred and $\mathfrak{r}$ cannot be decoded.

The algorithm searches for $t-$sets of G satisfying (P1). Thus,

- If $w = t$, the $t-$set that satisfies (P1) is unique.
- If $w < t$, all $t-$sets that satisfy (P1), allow to find the same error $\mathfrak{e}$.
- If $w > t$, no one $t-$set satisfies (P1).

Meggit's Generalization

- Group codes naturally generalize to cyclic codes.
- Then, some decoding algorithms in cyclic codes can be generalized to group codes.
- Note that, $g\mathfrak{e}e_0^+ = gS(\mathfrak{r})$ for all $g \in G$.
- Chosen a specific position $g_{i_0} \in G$, for any $\mathfrak{r} \in \mathbb{K}G$ we have $\mathfrak{r} = g'\mathfrak{r}'$ for some $g' \in G$ and $\mathfrak{r}' \in \mathbb{K}G$ such that $g_{i_0} \in \text{supp}(\mathfrak{r}')$.
- Therefore, we can consider the set $\mathcal{T}$ of elements (called *class leaders*) of $\mathbb{K}G$ having weight $\leq t$ and whose support contains $g_{i_0} \in G$.
- Previously to decoding, we make a list $\mathcal{L}$ of the syndrome of each class leader. This is called *syndrome reduced list*.

Step 1.

Compute the syndrome $S(\mathfrak{r})$ of $\mathfrak{r}$. If $S(\mathfrak{r}) = 0$, then there are no errors. Otherwise, continue to

Step 2.

Take $g \in G$ and compute $S_g(\mathfrak{r}) = gS(\mathfrak{r})$.

a. If $S_g(\mathfrak{r})$ is syndrome of some class leader $\mathfrak{e}' \in \mathcal{T}$ in $\mathcal{L}$, then the error is $\mathfrak{e} = g^{-1}\mathfrak{e}'$ and the algorithm ends.

b. Otherwise, the element g is discarded and another element of G is considered and Step 2 is repeated with it.

The algorithm ends when a element g satisfying (P2):

$S_g(\mathfrak{r})$ *is syndrome is in* $\mathcal{L}$ *for some element of* $\mathcal{T}$,

what it allows us to find the error or when all elements of G have been checked and none satisfies property (P2). In the last case, the algorithm concludes that more than t errors have occurred and $\mathfrak{r}$ cannot be decoded.

This algorithm is highly recommended for binary group codes because the complexity order of the decoding algorithms presented are

Algorithm	Precalculations	Decoding
Syndrome	$\mathcal{O}(n^2)$	$\mathcal{O}\left(n^3 \times \binom{n}{t}\right)$
Meggitt's Generalization in $\mathbb{F}_2$	$\mathcal{O}\left(nt \times \binom{n-1}{t-1}\right)$	$\mathcal{O}(n^3)$

The algorithm ends when a element g satisfying (P2):

$S_g(\mathfrak{r})$ *is syndrome is in* $\mathcal{L}$ *for some element of* $\mathcal{T}$,

what it allows us to find the error or when all elements of G have been checked and none satisfies property (P2). In the last case, the algorithm concludes that more than t errors have occurred and $\mathfrak{r}$ cannot be decoded.

This algorithm is highly recommended for binary group codes because the complexity order of the decoding algorithms presented are

Algorithm	Precalculations	Decoding
Syndrome	$\mathcal{O}(n^2)$	$\mathcal{O}\left(n^3 \times \binom{n}{t}\right)$
Meggitt's Generalization in $\mathbb{F}_2$	$\mathcal{O}\left(nt \times \binom{n-1}{t-1}\right)$	$\mathcal{O}(n^3)$

Thank you, so much!