# CONSTRUCCIONES MINIMALES ASOCIADAS A CÓDIGOS CONCATENADOS GENERALIZADOS

I. MÁRQUEZ-CORBELLA, E. MARTÍNEZ-MORO, AND E. SUÁREZ-CANEDO

Abstract. In order to obtain the set of codewords of minimal support of codes defined over $\mathbb{F}_q$ we must compute a Graver basis of the ideal associated to such codes, see [8]. The main aim of this article is to reduce the complexity of the previous algorithm for a well known class of codes, namely generalized concatenated codes. The ideas behind this paper are useful both in iterated secret sharing schemes as well as in the design of general error correcting algorithms for this family of codes.

## Introducción

Un código lineal $\mathcal{C}$ con parámetros $[n, k]$ es simplemente un $k$-subespacio vectorial de $\mathbb{F}_q^n$. Se define el peso de Hamming para un vector $\mathbf{c} \in \mathbb{F}_q^n$ como el número de coordenadas no nulas de $\mathbf{c}$. Una *matriz generatriz* de $\mathcal{C}$ es una matriz $G$ de tamaño $k \times n$ cuyas filas generan $\mathcal{C}$, y una *matriz de paridad* para $\mathcal{C}$ es una matriz $H$ de tamaño $(n-k) \times n$ cuyas columnas generan el complemento ortogonal de $\mathcal{C}$ con respecto al producto $\cdot$ usual.

La distancia de Hamming entre dos vectores es simplemente el peso de Hamming de su diferencia. El soporte de una palabra no nula del código $\mathcal{C}$ (es decir, de un vector no nulo en $\mathcal{C}$) es simplemente el conjunto de índices correspondientes a coordenadas no nulas de la palabra. El cálculo de los soportes minimales con respecto a la inclusión es clave en la descodificación por gradiente de códigos lineales [1, 6, 2, 4] así como en la determinación de esquemas para compartir secretos basados en dichos códigos [11].

Llamaremos *test-set* a un conjunto de palabras minimales capaz de descodificar por gradiente (ver [1]). Ikegami y Kaji [7] proporcionaron un método para calcular un test-set para el código $\mathcal{C}$ en el caso binario. En [8] se considera una base de Graver asociada a un problema de programación modular capaz de proporcionar un *test-set* universal que, mediante el levantamiento de Lawrence, proporciona todos los soportes minimales asociados al código.

Desafortunadamente debemos calcular una base Gröbner reducida de cierto ideal asociado al código que, a pesar de utilizar los artificios de tipo FGLM creados *ad hoc* en [3], tiene una complejidad $\mathcal{O}\left(n^2 q^{n-k}\right)$ [3, 2]. Una de las principales ideas para disminuir su complejidad es reducir la longitud $n$ del código (por lo tanto el número de variables involucradas en el cálculo de la base de Gröbner) utilizando códigos más pequeños para la construcción de otros, controlando sus parámetros, la combinatoria de los test-sets y el conjunto de soportes minimales. En esta contribución estudiaremos los soportes minimales y test-sets de una familia de códigos concatenados generalizados [5] asociados con construcciones iteradas para compartir secretos [10, 9].

## 1. Construcción de códigos concatenados generalizados

Consideremos los siguientes códigos en $\mathbb{F}_q$:

- Una familia de códigos $\{\mathcal{C}_i\}_{i=1}^r$ de parámetros $[n_i, k_i]$ con matriz de paridad $H_{\mathcal{C}_i}$ y matriz generatriz $G_{\mathcal{C}_i}$, tal que toda palabra $\mathbf{c}^i = (c_1, \dots, c_{n_i}) \in \mathcal{C}_i$ verifica que $\sum_{j=1}^{n_i} c_j \neq 0$ para todo $i = 1, \dots, r$.
- $\mathcal{C}_0$ código de parámetros $[r, k]$ (no imponemos ninguna condición sobre la dimensión) con matriz de paridad: $H_{\mathcal{C}_0} = \begin{pmatrix} \mathbf{h}_1 & \dots & \mathbf{h}_r \end{pmatrix}$.

Definimos la matriz:

$$H = \left(\begin{array}{c|c|c|c} \overbrace{\mathbf{h}_1 \dots \mathbf{h}_1}^{n_1} & \overbrace{\mathbf{h}_2 \dots \mathbf{h}_2}^{n_2} & \dots & \overbrace{\mathbf{h}_r \dots \mathbf{h}_r}^{n_r} \\ \hline H_{\mathcal{C}_1} & \mathbf{0} & \dots & \mathbf{0} \\ \hline \mathbf{0} & H_{\mathcal{C}_2} & \dots & \mathbf{0} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & \dots & H_{\mathcal{C}_r} \end{array}\right) \in \mathbb{F}_q^{(r-k)+\sum_{i=1}^r (n_i - k_i) \times \sum_{i=1}^r n_i}.$$

Llamaremos al código $\mathcal{C} = \mathcal{C}_0[\mathcal{C}_1, \dots, \mathcal{C}_r]$ que tiene a $H$ como matriz de paridad *código concatenado generalizado* (nótese que, si $\mathcal{C}_0$ es todo $\mathbb{F}_q^r$, el código resultante es simplemente la concatenación de los $r$ códigos $C_i$ con $i = 1, \dots, r$).

Los objetivos del trabajo son los siguientes:

(1) Si conocemos los soportes minimales de los códigos $\{\mathcal{C}_i\}_{i=1,\dots,r}$ y del código $\mathcal{C}_0$ es posible conocer los soportes minimales de $\mathcal{C}$.
(2) Podemos deducir un test-set de $\mathcal{C}$ a partir de los test-sets de los códigos $\{\mathcal{C}_i\}_{i=1}^r$ y del test-set de $\mathcal{C}_0$.
(3) Como consecuencia del apartado anterior resulta factible obtener un algoritmo de descodificación por gradiente para $\mathcal{C}$.

Observemos que las palabras del código $\mathcal{C}$ están definidas de la siguiente forma:

- Para toda palabra de $\mathcal{C}_0$ definida como $\mathbf{c} = (c_1^0, \dots, c_r^0)$.
- Buscamos en cada código $\mathcal{C}_i$ con $i = 1, \dots, r$ una palabra cuyas componentes sumen $c_i^0$.
- Finalmente concatenamos todas estas palabras.

### 1.1. Parámetros y propiedades de $\mathcal{C} = \mathcal{C}_0[\mathcal{C}_1, \dots, \mathcal{C}_r]$.

(1) Los parámetros de $\mathcal{C} = \mathcal{C}_0[\mathcal{C}_1, \dots, \mathcal{C}_r]$ son los siguientes:
   - **Longitud:** $N = \sum_{i=1}^r n_i$.
   - **Dimensión:** $K \leq \sum_{i=1}^r k_i$.
     En efecto observamos que:

$$N - K \geq \sum_{i=1}^r (n_i - k_i) = \sum_{i=1}^r n_i - \sum_{i=1}^r k_i = N - \sum_{i=1}^r k_i \Rightarrow -K \geq -\sum_{i=1}^r k_i \Rightarrow K \leq \sum_{i=1}^r k_i.$$

   - **Distancia mínima:**

$$D = \min\left\{\sum_I d_i \ : \ I \text{ soporte minimal de } \mathcal{C}_0\right\} \leq d_0 \min\{d_i\}_{i=1,\dots,r}.$$

(2) Si $K = \sum_{i=1}^{n} k_i$ entonces $\mathcal{C}$ es la suma directa o la concatenación de los códigos $\{\mathcal{C}_i\}_{i=1,\dots,r}$. Por lo tanto, una matriz generatriz de $\mathcal{C}$ es:

$$G = \left(\begin{array}{c|c|c|c} G_{\mathcal{C}_1} & \mathbf{0} & \dots & \mathbf{0} \\ \hline \mathbf{0} & G_{\mathcal{C}_2} & \dots & \mathbf{0} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & \dots & G_{\mathcal{C}_r} \end{array}\right) \in \mathbb{F}_q^{\sum_{i=1}^{r} k_i \times \sum_{i=1}^{r} n_i} = \mathbb{F}_q^{K \times N}.$$

(3) Supongamos que los códigos $\{\mathcal{C}_i\}_{i=1,\dots,r}$ tienen todos la misma dimensión, i.e. $S = k_1 = \dots = k_r$ y admitamos que las siguientes matrices se corresponden con matrices generatrices de los códigos $\mathcal{C}_0$ y $\{\mathcal{C}_i\}_{i=1,\dots,r}$ respectivamente:

$$G_{\mathcal{C}_0} = \begin{pmatrix} g_{11}^0 & \dots & g_{1r}^0 \\ \vdots & \ddots & \vdots \\ g_{k1}^0 & \dots & g_{kr}^0 \end{pmatrix} \in \mathbb{F}_q^{k \times r} \quad \text{y} \quad G_{\mathcal{C}_i} = \left(g_{lj}^i\right) \in \mathbb{F}_q^{S \times n_i} \ i = 1, \dots, r \ .$$

Sin pérdida de generalidad, siempre podemos presumir que las filas de cada matriz $G_{\mathcal{C}_i}$ con $i = 1, \dots, r$ suman 1, i.e. $\sum_{l=1}^{n_i} g_{jl}^i = 1$ con $j = 1, \dots, S$. Entonces el código $\hat{\mathcal{C}}$ generado por las filas de la siguiente matriz

$$\hat{G} = \begin{pmatrix} g_{11}^0 G_{\mathcal{C}_1} & \dots & g_{1r}^0 G_{\mathcal{C}_r} \\ \vdots & \ddots & \vdots \\ g_{k1}^0 G_{\mathcal{C}_1} & \dots & g_{kr}^0 G_{\mathcal{C}_r} \end{pmatrix}$$

verifica que $\hat{\mathcal{C}} \subseteq \mathcal{C}$ (se dará la igualdad si las dimensiones de $\hat{\mathcal{C}}$ coinciden con las dimensiones de $\mathcal{C}$).

(4) Si $\mathcal{C}_1 = \dots = \mathcal{C}_r$ entonces $\mathcal{C}$ se corresponde con el código $\mathcal{C}_1 \otimes \mathcal{C}_0$, en este caso $D = d_0 d_1$.

Finalmente nótese que la condición de que la suma de las componentes de cada palabra distinta del cero de los códigos $\mathcal{C}_i$ sea no nula no es una restricción gracias al siguiente lema:

**Lema 1.1.** *Sea $\mathcal{C}$ un código lineal de parámetros $[n, k, d]$ en $\mathbb{F}_q$ con $q = p^r$ ($p$ primo), podemos encontrar un entero entero $s \geq r$ y un código $\mathcal{C}'$ de parámetros $[n, k, d]$ en $\mathbb{F}_{p^s}$ tal que el soporte de toda palabra $\mathbf{c} = (c_1, \dots, c_n) \in \mathcal{C}'$ se corresponde con el soporte de una palabra de $\mathcal{C}$ y se verifica que $\sum_{i=1}^{n} c_i \neq 0$ en $\mathbb{F}_{p^s}$.*

La demostración es una consecuencia directa del lema y del teorema principal en [9]. Es más, claramente los códigos $\mathcal{C}$ y $\mathcal{C}'$ del lema anterior tienen la misma capacidad correctora y los mismos soportes minimales, lo que nos va a permitir un algoritmo de descodificación por gradiente equivalente.

## 2. Resultados

**Teorema 2.1.** *Los soportes minimales del código concatenado generalizado $\mathcal{C} = \mathcal{C}_0[\mathcal{C}_1, \dots, \mathcal{C}_r]$ se corresponden con los soportes de las palabras $(\mathbf{c}^1, \mathbf{c}^2, \dots, \mathbf{c}^r)$ donde $\mathbf{c}^i \in \mathcal{C}_i$ es la palabra nula o una palabra de soporte minimal en $\mathcal{C}_i$ para $i = 1, \dots, r$. Además el conjunto de índices correspondientes a palabras no nulas es un soporte minimal de $\mathcal{C}_0$.*

Teniendo en cuenta que los soportes minimales corresponden a una base de Graver asociada a un problema de programación modular en el código $\mathcal{C}$ (véase [8]) y que el test-set corresponde a una base de Gröbner del ideal asociado al problema se obtiene el siguiente resultado:

**Corolario 2.2.** *Se puede obtener un test-set del código $\mathcal{C}$ a partir de los test-set de los códigos componentes utilizando la estructura de los soportes minimales enunciada en el teorema anterior.*

## 3. Conclusiones

Hemos mostrado los principales parámetros y características de una clase de códigos concatenados generalizados. Estos códigos permiten la definición de estructuras iteradas para compartir secretos. Además sus soportes minimales y test-sets fácilmente pueden ser derivados de la estructura de sus componentes, lo que permite una descodificación por gradiente de los mismos. Nótese que cada componente puede ser tratada de forma independiente a la hora de realizar el cálculo, lo que admite una paralelización de los algoritmos propuestos en [8] y, por lo tanto, una reducción en los tiempos de ejecución de los mismos.

## References

[1] Alexander Barg. Complexity issues in coding theory. In *Handbook of coding theory, Vol. I, II*, pages 649–754. North-Holland, Amsterdam, 1998.

[2] M. Borges-Quintana, M. A. Borges-Trenard, P. Fitzpatrick, and E. Martínez-Moro. Gröbner bases and combinatorics for binary codes. *Appl. Algebra Engrg. Comm. Comput.*, 19(5):393–411, 2008.

[3] M. Borges-Quintana, M. A. Borges-Trenard, and E. Martínez-Moro. On a Gröbner bases structure associated to linear codes. *J. Discrete Math. Sci. Cryptogr.*, 10(2):151–191, 2007.

[4] M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella, and E. Martínez-Moro. An algebraic view to gradient descent decoding. *IEEE Information Theory Workshop (ITW)*, 2010.

[5] Ilya I. Dumer. Concatenated codes and their multilevel generalizations. In *Handbook of coding theory, Vol. I, II*, pages 1911–1988. North-Holland, Amsterdam, 1998.

[6] Tai Yang Hwang. Decoding linear block codes for minimizing word error rate. *IEEE Trans. Inform. Theory*, 25(6):733–737, 1979.

[7] Daisuke Ikegami and Yuichi Kaji. Maximum Likelihood Decoding for Linear Block Codes using Grobner Bases. *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, E86-A(3):643–651, 2003.

[8] Irene Márquez-Corbella and Edgar Martínez-Moro. Algebraic structure of the minimal support codewords set of some linear codes. *Adv. Math. Commun.*, 5(2):233–244, 2011.

[9] Irene Márquez-Corbella, Edgar Martínez-Moro, and Emilio Suárez-Canedo. On the composition of secret sharing schemes related to codes. *Quaderns CRM, "Workshop on Computational Security"*, pages 31–38, 2011.

[10] Edgar Martínez-Moro, Carlos Munuera, and Jorge Mozo. Compounding secret sharing schemes. *Australasian Journal of Combinatorics*, 30:277–290, 2004.

[11] James L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory*, pages 276–279, 1993.

Instituto de Matemáticas, Universidad de Valladolid
*E-mail address*: imarquez@agt.uva.es, edgar@maf.uva.es, esuarez@maf.uva.es