DESCODIFICACIÓN POR GRADIENTE COMO REDUCCIÓN

M. BORGES-QUINTANA, M.A. BORGES-TRENARD, I. MÁRQUEZ-CORBELLÁ, AND E. MARTÍNEZ-MORO

Abstract. We show an unified algebraic structure related to two gradient descent decoding procedures for binary codes proposed independently by Liebler and by Ashikhmin and Barg showing their link and relationship. The main tool used is the Gröbner representation of the monoid associated to the linear code.

Introducción

El *problema de la descodificación completa* (PDC) en la teoría de códigos consiste en recibida una palabra (vector) $\mathbf{y}$ de $\mathbb{F}_2^n$ calcular la palabra perteneciente a $\mathcal{C} \lhd \mathbb{F}_2^n$ (subespacio lineal de $\mathbb{F}_2^n$) que difiera menos posiciones (distancia de Hamming) de la palabra recibida. Si fijamos una cota t para los errores que podemos corregir el problema se transforma en (t-PDC) determinar un elemento de $\mathcal{C}$ (si existe) tal que difiera en menos de t posiciones de $\mathbf{y}$. Nótese que aquellos errores que se pueden corregir son los líderes (vectores de menor peso de Hamming $\mathrm{wt}(\cdot)$, i.e. con menor número de coordenadas no nulas) de las clases de equivalencia $\mathbb{F}_2^n/\mathcal{C}$. Cuando existe más de un líder existe más de una elección para el error. Denotaremos por $\overline{\mathbf{y}}$ a la clase de equivalencia que contiene a $\mathbf{y}$ y por $\mathrm{wt}(\overline{\mathbf{y}})$ al peso de Hamming de cualquiera de sus líderes. Por lo tanto el siguiente problema surge de una forma natural:

> *Problema del cálculo del líder* (PCL):
> **Input:** Dada una matriz $r \times n$ binaria H, $\mathbf{s} \in \mathbb{F}_2^r$ y un entero no negativo t.
> **Problema:** ¿Existe un vector $\mathbf{e} \in \mathbb{F}_2^r$ de peso de Hamming a lo más t tal que $H\mathbf{e} = s$?

Todos estos problemas son NP-completos (véase [2, 3]) incluso si se permite realizar preproceso en los datos [11].

Recientemente se ha mostrado interés, relacionado con el estudio de la descodificación de los códigos LDPC, en la siguiente cuestión para la que aún no existe una clara respuesta: *¿Qué parámetros o atributos de un código contribuyen a reconocer e implementar una función de descodificación por gradiente que proporcione los líderes de las clases de equivalencia?* Los lectores interesados pueden consultar [12] para una descripción más detallada del problema. En el mismo artículo Liebler define *la descodificación por gradiente (líder)* como aquella que recibida la palabra $\mathbf{y}$ se reemplaza el *vecino* $\mathbf{y}'$ a distancia de Hamming 1 tal que $\mathrm{wt}(\overline{\mathbf{y}}) \geq \mathrm{wt}(\overline{\mathbf{y}'})$ y reemplazar $\mathbf{y}$ por $\mathbf{y}'$ hasta que lleguemos a $\mathrm{wt}(\overline{\mathbf{y}}) = 0$.

Descodificación por gradiente (líder)
Input: $\mathbf{y}$ palabra recibida.
Repite hasta que $\mathrm{wt}(\overline{\mathbf{y}}) = \mathbf{0}$
Calcula $\mathbf{y}'$ tal que $\mathrm{wt}(\mathbf{y} - \mathbf{y}') = 1$ y $\mathrm{wt}(\overline{\mathbf{y}}) \geq \mathrm{wt}(\overline{\mathbf{y}'})$, $\mathbf{y} \leftarrow \mathbf{y}'$
Return: $\mathbf{y}$.

Nótese que en este algoritmo en cada iteración se cambia de clase de equivalencia hasta alcanzar la clase correspondiente al $\mathbf{0}$, esto es, el código. Existe otro algoritmo de descodificación por gradiente de Ashikhmin y Barg [1] en que cada paso el representante elegido permanece en la misma clase de equivalencia hasta que se alcanza el líder (mostraremos una definición rigurosa en la sección 2). Liebler menciona en [12] que dichos algoritmos, a pesar de compartir la filosofía de la descodificación por gradiente, son diferentes. El propósito de nuestra contribución es mostrar que estos dos algoritmos son *duales* en el sentido que son dos formas de entender la representación de Gröbner de un código.

1. Representación de Gröbner de un código

Definición 1.1. Una *representación de Gröbner* de $\mathbb{F}_2^n/\mathcal{C}$ [5, 6] es un par N, ϕ donde N es un sistema de representantes de la clases de equivalencia $\mathbb{F}_2^n/\mathcal{C}$ tal que $\mathbf{0} \in N$ y para cada $\mathbf{n} \in \mathrm{N}\backslash\{\mathbf{0}\}$ existe $\mathbf{e}_i$, $i \in 1, \ldots, n$, tal que $\mathbf{n} = \mathbf{n'} + \mathbf{e}_i$ y $\mathbf{n'} \in \mathrm{N}$. Además $\phi : \mathrm{N} \times \{\mathbf{e}_i\}_{i=1}^n \to \mathrm{N}$ es una función que envía cada par $(\mathbf{n}, \mathbf{e}_i)$ al elemento N que pertenece a la clase de equivalencia del elemento $\mathbf{n} + \mathbf{e}_i$.

El nombre de representación de Gröbner no es casual. Fijamos un orden compatible con el grado y consideramos el ideal binomial

$$\mathcal{I}_\mathcal{C} = \{\mathbf{x}^{\mathbf{w}_1} - \mathbf{x}^{\mathbf{w}_2} \mid \mathbf{w}_1 - \mathbf{w}_2 \in \mathcal{C}\} \subseteq \mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n] \tag{1}$$

donde $\mathbb{K}$ es un cuerpo cualquiera y si $\mathbf{w} = (w_1, \ldots, w_n)$ entonces, abusando la notación y considerando $\mathbf{w}$ en $\mathbb{Z}^n$, se tiene que $\mathbf{x}^\mathbf{w} = \prod x_i^{w_i}$. La representación de Gröbner del código corresponde con la representación del ideal $\mathcal{I}_\mathcal{C}$ utilizando el algoritmo FGLM (véase [14] capítulo 29 para una referencia completa) donde N son las formas normales y ϕ representa las "tablas de multiplicación" correspondientes a la multiplicación de una forma normal por una variable. Además, puesto que el orden es compatible con el grado total los elementos de N son mínimos respecto al mismo en cada clase de equivalencia, es decir, corresponden a líderes de la misma. La representación de Gröbner de un código puede ser calculada mediante una modificación del algoritmo FGLM (véase [5]), una implementación del algoritmo en GAP [10] se puede encontrar en [7]. El ideal binomial $\mathcal{I}_\mathcal{C}$ también puede ser visto como el núcleo de un problema de programación lineal modular, véase [13].

Asociada a una representación de Gröbner podemos definir el borde de un código [9] como

Definición 1.2. Sea $\mathcal{C}$ un código y H su matriz de paridad y N, ϕ su representación de Gröbner, el *borde de* $\mathcal{C}$ es el conjunto

$$\begin{aligned} B(\mathcal{C}) = \quad & \{(\mathbf{n}_1 + \mathbf{e}_i, \mathbf{n}_2) \mid i \in [1, n], \mathbf{n}_1 + \mathbf{e}_i \neq \mathbf{n}_2, \\ & \mathbf{n}_1, \mathbf{n}_2 \in N \text{ and } H \cdot (\mathbf{n}_1 + \mathbf{e}_i) = H \cdot \mathbf{n}_2\}, \end{aligned} \tag{2}$$

Nótese que las dos componentes del borde se encuentran en la misma clase de equivalencia, es decir, su suma pertenece al código. Podemos expresar el conjunto en (2) en términos de

ϕ como

$$B(\mathcal{C}) = \{(\mathbf{n} + \mathbf{e}_i, \phi(\mathbf{n}, \mathbf{e}_i)) \mid i \in [1, n], \mathbf{n} \in N\} \setminus \{(\mathbf{x}, \mathbf{x})\}.$$

2. Reducción

Conocido un código $\mathcal{C}$ y su correspondiente representación de Gröbner N, ϕ definimos la *reducción* de un elemento $\mathbf{n} \in N$ restpecto a $\mathbf{e}_i$ como el elemento canónico como $\mathbf{n}' = \phi(\mathbf{n}, \mathbf{e}_i)$ y lo denotamos por $\mathbf{n} \to_i \mathbf{n}'$. Para cada $\mathbf{x} \in \mathbb{F}_2^n$, $\mathbf{x} = \mathbf{0} + \sum_j \mathbf{e}_{i_j}$, por lo que podemos iterar un número finito de reducciones parea calcular el líder de la clase de equivalencia $\overline{\mathbf{x}}$, esto es obtenemos un procedimiento de descodificación por gradiente (líder) como sigue:

Descodificación por gradiente (líder)
Input: $\mathbf{y}$ palabra recibida.
Forward step
$\mathbf{y} = \sum_{j=1}^{s} \mathbf{e}_{i_j}$. Calcula $\mathbf{n} \in N$ correspondiente a la clase de $\mathbf{y}$, i.e.
(a) $\mathbf{n} = \mathbf{0}$.
(b) For $j = 1, ..., s$ do $\phi(\mathbf{n}, \mathbf{e}_{i_j}) = \mathbf{n}', \quad \mathbf{n} \leftarrow \mathbf{n}'$
Backward step
Mientras que $\mathbf{n} \neq \mathbf{0}$
(a) Calcula $\mathbf{y}'$ tal que $\mathbf{y}' = \mathbf{y} + \mathbf{e}_{i_j}$ y $\mathrm{wt}(\mathbf{n}) \geq \mathrm{wt}(\phi(\mathbf{n}, \mathbf{e}_{i_j}))$
(b) $\mathbf{y} \leftarrow \mathbf{y}', \quad \mathbf{n} \leftarrow \phi(\mathbf{n}, \mathbf{e}_{i_j})$.
Return: $\mathbf{y}$.

Nótese que la información de nuestra representación de Gröbner es excesiva para la reducción propuesta anteriormente, ya que una vez conocida la forma normal (i.e. el líder) $\mathbf{n}$ correspondiene al final del "Forward step" podemos descodificar $\mathbf{y}$. La información estrictamente necesaria para realizar la descodificación por gradiente (líder) es la función de asignación ϕ y sustituir los líderes en N por vectores del tipo (i, w_i) donde i es un ordinal de las clases de equivalencia y w_i el peso del líder de la clase i-ésima, es decir, se reduce considerablemente el tamaño respecto al par (N, ϕ) propuesto originalmente en [4].

Si tenemos ahora en cuenta la información en $B(\mathcal{C})$ podemos realizar la misma reducción sustituyendo en cada paso el primer término o head del correspondiente elemento del borde por su segunda componente o tail. Nótese que head + tail es una palabra del código, por lo tanto, la reducción se lleva a cabo sumando palabras adecuadas del código, es decir, sin moverse de la misma clase de equivalencia. Esta es la idea que subyace en la descodificación por conjuntos de comprobación ("Test sets") propuesta por Ashikhmin y A. Barg [1]. Un conjunto $\mathcal{T} \subseteq \mathcal{C}$ es de comprobación si para cada vector $\mathbf{y} \in \mathbb{F}_2^n$ o bien existe un $\mathbf{t} \in \mathcal{T}$ con $\mathrm{wt}(\mathbf{y} - \mathbf{t}) \leq \mathrm{wt}(\mathbf{y})$ o bien $\mathbf{y} \in \{\mathbf{x} \mid \mathrm{wt}(\mathbf{x}) \leq \mathrm{wt}(\mathbf{x} - \mathbf{c}), \mathbf{c} \in \mathcal{C}\}$. Claramente las palabras que se derivan del borde de un código constituyen un conjunto de comprobación. El algoritmo de descodificación es ahora

Descodificación por gradiente (test set)
Input: $\mathbf{y}$ palabra recibida y $\mathcal{T}$.
1.- $\mathbf{c} \leftarrow \mathbf{0}$.
2.- Buscar $\mathbf{t} \in \mathcal{T}$ tal que $\mathrm{wt}(\mathbf{y} - \mathbf{t}) \leq \mathrm{wt}(\mathbf{y})$. $\mathbf{c} \leftarrow \mathbf{c} + \mathbf{t}$. $\mathbf{y} \leftarrow \mathbf{y} + \mathbf{t}$.
3.- Repetir el paso anterior hasta que no exista dicho $\mathbf{t}$.
Return: $\mathbf{c}$.

La estructura dada por el borde es en cierta manera redundante y puede encontrarse una subestructura llamada borde reducido que realiza la misma reducción (el concepto es análogo al de base de Gröbner reducida). Una definición de borde reducido puede encontrarse en [9] y su relación con la minimalidad de las palabras representadas en el mismo en [8, 9]. Por último notar que el conjunto de comprobación $\mathcal{T}$ corresponde a un conjunto de comprobación de un problema de programación lineal modular, véase [13].

3. Conclusiones

Hemos mostrado como los dos algoritmos de descodificación por gradiente pueden derivarse de una misma estructura algebraica de un código binario dado por su representación de Gröbner como dos formas de interpretar la reducción dando así un tratamiento unificado a los dos algoritmos que Liebler [12] identificaba como distintos.

References

[1] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes* IEEE Trans. Inform. Theory **44** (1998), 2010–2017.

[2] A. Barg, *Complexity issues in coding theory*, In Handbook of Coding Theory, Elsevier Science, Vol. 1, (1998), 649–754

[3] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems* IEEE Trans. Inform. Theory, **IT-24**, no. 3, (1978), 384–386.

[4] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *n a Gröbner bases structure associated to linear codes*, J. Discrete Math. Sci. Cryptogr. **10** (2007), no. 2, 151–191.

[5] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *A general framework for applying FGLM techniques to linear codes*, AAECC 16, Lecture Notes in Comput. Sci., **3857**, (2006), 76–86.

[6] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *A Gröbner representation of linear codes*, In: T. Shaska, W.C. Huffman, D. Joyner, V. Ustimenko (eds.) Advances in Coding Theory and Cryptography, World Scientific (2007), 17–32.

[7] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *GBLA-LC: Gröbner Bases by Linear Algebra and Linear Codes*, In: ICM 2006. Mathematical Software, EMS, (2006), 604–605.

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

[9] M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbellá, E. Martínez-Moro, *On the Border of a Binary Code*. Submitted to Jour. Comp. Applied Maths.(2009).

[10] The GAP Group, GAP – Groups, Algorithms, and Programming.Version 4.12 (2009). `http://www.gap-system.org.`

[11] J. Bruck, M. Naor, *The Hardness of Decoding Linear Codes with Preprocessing*, IEEE Trans. Inform. Theory **36**, no. 2, (1990)

[12] R. Liebler,*Implementing gradient descent decoding*,Michigan Math. J. **58** , Issue 1 (2009), 285–291.

[13] I. Márquez-Corbella, E. Martínez Moro, *Combinatorics of minimal codewords of some linear codes*, Submitted to Advances in Mathematics of Communications (2010).

[14] T. Mora, *Solving polynomial equation systems. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia of Mathematics and its Applications, 99. Cambridge University Press, Cambridge, (2005).

Universidad de Oriente, Santiago de Cuba
E-mail address: `mijail@mbq.uo.edu.cu, mborges@mabt.uo.edu.cu`

Universidad de Valladolid
E-mail address: `imarquez@agt.uva.es, edgar@maf.uva.es`