Construcción de Códigos de Control de Paridad a través de Códigos Geométricos de Goppa

W. Olaya

***Resumen*—Este trabajo establece una forma de obtener los códigos de control de paridad a través de códigos geométricos de Goppa. Se han considerado dos casos dependiendo de la característica del cuerpo tomado como alfabeto y la longitud del código; y se uso la técnica de restricción de un código lineal. Más precisamente, se demuestra que los códigos de control de paridad se obtienen como la restricción de un cierto código geométrico de Goppa racional.**

***Palabras claves*— Códigos correctores de errores, códigos geométricos de Goppa, cuerpos de funciones algebraicas.**

I. NOTACIÓN

Se usará la notación estándar de teoría de códigos algebraicos, ver [3] y [4]. Para códigos geométricos de Goppa, ver [5] y [7].

Fq	El cuerpo finito con q elementos, Fq:=Z/qZ
χ	La característica de un cuerpo
CPq(n)	El código de control de paridad q-ario de longitud n
C|Fq	La restricción del código C a Fq, $C\|Fq:=C\cap(Fq)^n$
F/Fq	El cuerpo de funciones algebraicas con cuerpo de constantes Fq
Fq(z)/Fq	El cuerpo de funciones racionales.
P_0	El lugar cero de z en Fq(z)/Fq
P_∞	El lugar infinito de z en Fq(z)/Fq
ν_P	La valuación de F en el lugar P de F/Fq
L(A)	El espacio vectorial asociado al divisor A
Sop(A)	El soporte del divisor A
a | b	"a divide a b", $a,b\in Z$

II. INTRODUCCIÓN

LOS códigos de control de paridad surgen a mediados del siglo pasado como ejemplo de una familia de códigos detectores de un error simple, su nombre proviene históricamente del primer código conocido, este era un código binario que agregaba un símbolo extra para hacer que el número de unos fuera par. Esta teoría de códigos detectores y correctores de errores tiene sus orígenes en el año de 1948 con los trabajos de C.E. Shannon, R. Hamming, M. Golay y otros. En principio estos códigos se crearon utilizando solo conceptos de algebra y teoría de números, razón por la cual se conocen como códigos algebraicos (ver [5] y [6]). Posteriormente, hacia el año 1977, V.D. Goppa introdujo una nueva forma de construir códigos lineales utilizando conceptos de la geometría algebraica, más precisamente, su construcción se hace utilizando cuerpos de funciones algebraicas (ver [1] y [2]). Estos códigos se conocen como códigos algebro-geométricos o códigos geométricos de Goppa. En este artículo utilizaremos las ideas de Goppa para construir los códigos de control de paridad, usando la técnica de restricción de un código lineal.

W. Olaya, está vinculado a la Escuela de Matemáticas (Facultad de Ciencias) de la Universidad Industrial de Santander (UIS), A.A. 678 Bucaramanga-Colombia (e-mail: wolaya@uis.edu.co).

III. PRELIMINARES

Para aquellos lectores que no estén muy familiarizados con la teoría de códigos detectores y correctores de errores, se recomienda ver [4]. Sobre códigos geométricos de Goppa ver [7].

A. El código de control de paridad CPq(n)

Consideremos Fq como alfabeto, el código de control de paridad CPq(n) es el subespacio vectorial $(Fq)^n$ obtenido al agregar a cada elemento de $(Fq)^{n-1}$ una última componente de tal forma que la suma de sus componentes sea cero en Fq. Más exactamente CPq(n) es un [n,n-1,2]-código q-ario definido como

$$CPq(n)=\left\{ (c_1,...,c_n) : (c_1,...,c_{n-1})\in (Fq)^{n-1},\ \sum_{i=1}^{n} c_i = 0 \right\}$$

Es decir, es un código lineal de longitud n, dimensión n-1 y distancia mínima 2, por lo tanto son códigos detectores de un error simple. Ver [5] pág. 13.

B. Códigos geométricos de Goppa

Sean F/Fq un cuerpo de funciones algebraicas, y $P_1,P_2,...,P_n$ distintos lugares de grado uno de F/Fq.

Consideremos el divisor $D=\sum_{i=1}^{n} P_i$ y sea G cualquier otro divisor de F/Fq tal que $P_i \notin Sop(G)$ para todo $i=1,...,n$.

El código geométrico de Goppa asociado a los divisores D y G se define como:

$$C_L(D,G) := \{(x(P_1), x(P_2),..., x(P_n)) : x \in L(G)\}.$$

Así, $C_L(D,G)$ puede interpretarse como la imagen del espacio vectorial L(G) bajo la función evaluación $ev_D : L(G) \to (Fq)^n$ dada por $x \to (x(P_1), x(P_2),..., x(P_n))$. En consecuencia, $C_L(D,G) = ev_D(L(G))$ y como ev_D es Fq-lineal tenemos que $C_L(D,G)$ es un código lineal q-ario.

Nota: Para un lugar de grado uno y un elemento $x \in F$ con $\nu_P(x) \geq 0$, x(P) es el valor de x en P. (i.e. $x(P) \in Fq$ y $\nu_P(x - x(P)) > 0$) Ver [7] pág. 5.

Un código geométrico de Goppa asociado a los divisores del cuerpo de funciones racionales Fq(z)/Fq se conoce como código geométrico de Goppa racional.

IV. Resultado principal

Se construirá el código CPq(n) como la restricción de un código geométrico de Goppa racional. Se consideraron dos casos dependiendo de la divisibilidad de la longitud n del código a construir entre la característica del cuerpo tomado como alfabeto.

Caso 1. Si $\neg(\chi(Fq) \mid n)$.

Supongamos que m es un entero tal que $n \mid q^{m-1}$ y $\beta \in F q^m$ es una raíz n-ésima primitiva de la unidad. Consideremos el cuerpo de funciones racionales $F q^m(z)/F q^m$ y denotemos por P_i el cero de $z-\beta^{i-1}$, para i=1,..,n.

Sean $D=\sum_{i=1}^{n} P_i$ y $G=(n-1)P_\infty - P_0$ divisores de $F q^m(z)/F q^m$. Puesto que $grad(G) = n-2$, el teorema de Riemann-Roch implica que $dim(G) = n-1$, ver [7] pág. 22. Así, el conjunto $\{z, z^2, ..., z^{n-1}\}$ es una base para L(G).

Ahora, $ev_D(z^j) = (1, \beta^j, ..., (\beta^{n-1})^j)$ y puesto que β es una raíz n-ésima primitiva de la unidad, tenemos que $\sum_{i=0}^{n-1} (\beta^i)^j = 0$. Es decir, la suma de las componentes de $ev_D(z^i)$ es cero en Fq, para j=1,2,...,n-1.

Luego, si $x \in L(G)$ entonces $x=\sum_{k=1}^{n-1} a_k z^k$ donde $a_k \in F q^m$ para k=1,...,n-1. Por lo tanto,

$$\begin{aligned} ev_D(x) &= (x(P_1), x(P_2),..., x(P_n)) \\ &= \left(\sum_{k=1}^{n} a_k z^k(P_1), \sum_{k=1}^{n} a_k z^k(P_2),..., \sum_{k=1}^{n} a_k z^k(P_n) \right) \\ &= \left(\sum_{k=1}^{n} a_k, \sum_{k=1}^{n} a_k \beta^k, ..., \sum_{k=1}^{n} a_k (\beta^{n-1})^k \right). \end{aligned}$$

En consecuencia, $C_L(D,G) = CPq^m(n)$. Ya que por un lado $\sum_{k=1}^{n} a_k \sum_{i=0}^{n-1} (\beta^i)^k = 0$, es decir, la suma de las componentes de las palabras del código es igual a cero en $F q^m$ y por otro lado $(1, \beta^j, ..., (\beta^{n-2})^j)$ para j=1,2,…,n conforman una base para $(F q^m)^{n-1}$.

De esta manera, tenemos que $C_L(D,G) | Fq = CPq(n)$.

Caso 2. Si $\chi(Fq) \mid n$.

De manera similar, Supongamos que m es un entero tal que $n-1 \mid q^{m-1}$ y $\beta \in F q^m$ es una raíz (n-1)-ésima primitiva de la unidad. Consideremos el cuerpo de funciones racionales $F q^m(z)/F q^m$ y denotemos por P_i el cero de $z-\beta^{i-1}$, para i=1,..,n-1.

Sean $D=\sum_{i=1}^{n-1} P_i$ y $G=(n-2)P_\infty$ divisores de $F q^m(z)/F q^m$. Entonces $grad(G) = n-2$ y $dim(G) = n-1$. Así, el conjunto $\{1, z, z^2, ..., z^{n-2}\}$ es una base para L(G). Además, $ev_D(1) = (1,1,...,1)$ y $ev_D(z^j) = (1, \beta^j, ..., (\beta^{n-2})^j, 0)$. Es claro que la suma de las componentes de $ev_D(1)$ y $ev_D(z^j)$ para j=1,2,…,n-2 es igual a cero.

Por consiguiente, de la misma forma que en caso anterior, tenemos que $C_L(D,G) | Fq = CPq(n)$.

V. Ejemplos

A. El código $CP_2(3)$

Como $\neg(2 \mid 3)$, sea $\beta \in F_4$ una raíz tercera primitiva de la unidad y consideremos el cuerpo de funciones racionales $F_4(z)/F_4$. Puesto que $F_4 = \{0, 1, \beta, \beta^2\}$ denotemos los lugares de grado uno de $F_4(z)/F_4$ como $P_0, P_1, P_\beta, P_{\beta^2}, P_\infty$. Sean $D = P_1 + P_\beta + P_{\beta^2}$ y $G = 2P_\infty - P_0$ divisores de $F_4(z)/F_4$. Así, $\{z, z^2\}$ es una base para L(G). Ahora, de los

16 elementos de L(G), los únicos cuya imagen bajo ev_D están en $(\mathrm{F}_2)^3$ son $\{0, z+z^2, \beta z+\beta^2 z^2, \beta^2 z+\beta z^2\}$, más exactamente, su imagen es $\{(0,0,0),(0,1,1\},(1,1,0),(1,0,1)\}$ respectivamente. Es decir, $C_L(D,G)|\mathrm{F}_2 = CP_2(3)$.

B. *El código* $CP_2(4)$

Como (2 | 4), sea $\beta \in \mathrm{F}_4$ y $\mathrm{F}_4(z)/\mathrm{F}_4$ como en el anterior. Sean $D = P_1 + P_\beta + P_{\beta^2} + P_0$ y $G = 2P_\infty$ divisores de $\mathrm{F}_4(z)/\mathrm{F}_4$. Entonces $\{1, z, z^2\}$ es una base para L(G). Y los únicos elementos cuya imagen bajo ev_D están en $(\mathrm{F}_2)^4$ y sus respectivas imágenes son:

$$
\begin{array}{ccc}
0 & \mapsto & (0,0,0,0) \\
1 & \mapsto & (1,1,1,1) \\
z+z^2 & \mapsto & (0,1,1,0) \\
\beta z+\beta^2 z^2 & \mapsto & (1,1,0,0) \\
\beta^2 z+\beta z^2 & \mapsto & (1,0,1,0) \\
z+z^2+1 & \mapsto & (1,0,0,1) \\
\beta z+\beta^2 z^2+1 & \mapsto & (0,0,1,1) \\
\beta^2 z+\beta z^2+1 & \mapsto & (0,1,0,1)
\end{array}
$$

Obteniendo así que $C_L(D,G)|\mathrm{F}_2 = CP_2(4)$.

VI. Comentario

Esta construcción de códigos de control de paridad, a través de códigos geométricos de Goppa, establece una inmersión de este importante código algebraico clásico en una teoría moderna de códigos, que ha demostrado ser más eficiente, pero que su implementación se ha demorado debido a la incertidumbre que genera un cambio sobre la actual forma algebraica de detectar y corregir errores de un mensaje transmitido a través de un canal ruidoso.

Aunque los códigos de control de paridad son ampliamente utilizados, ya que por su mínima redundancia presenta una reducción de costos de implementación y decodificación en sistemas actuales de error simple. Sabemos que no son objeto de investigación actualmente, puesto que la comunidad científica ha abordado el problema de la construcción de "buenos" códigos, garantizada por la teoría de Shannon, desde otras perspectivas (probabilísticas, algebro-geométricas, etc.). Sin lugar a dudas, esta alternativa de construcción permite comprender la implementación de los códigos geométricos de Goppa, generando códigos comúnmente utilizados y que se sabe con certeza que son confiables en comunicaciones a través de canales AWGN. Estos códigos han trazado una construcción práctica para familias de buenos códigos que sobrepasan las cotas asintóticas conocidas (ver [5]) y que a demostrado ser la mejor alternativa futurista en telecomunicaciones.

VII. Agradecimientos

Mis más sinceros agradecimientos a la Universidad del Valle por la asistencia de docencia otorgada para la realización de mis estudios de maestría.

VIII. Referencias

[1] V.D. GOPPA, "Codes on Algebraic Curves", Soviet math, vol 24, No 1, 170-172, 1981.
[2] V.D. GOPPA, *Geometry and Codes*, Kluwer Academic Plublisher, Boston 1988.
[3] R. HILL, *A First Course in Coding Theory*, Clarendan Press, Oxford 1986.
[4] J. VAN LINT, *Introduction to Coding Theory*, second edition, Springer-Verlag 1992.
[5] J. VAN LINT and G. VAN DER GEER, *Introduction to coding Theory and Algebraic Geometry*, Birkhauser, Verlag Basel, 1988.
[6] S. ROMAN, *Coding and Information Theory*, Springer-Verlag, N.Y. 1991.
[7] H. STICHTENOTH, *Algebraic Function Field and Codes*, Springer-Verlag, Berlin-Heidelberg, 1993.

IX. Biografía

Wilson Olaya León, nació el 13 de octubre de 1977 en Bucaramanga (Santander-Colombia), obtuvo su titulo de licenciado en matemáticas de la Universidad Industrial de Santander en mayo de 2001 y su titulo de magíster en ciencias matemáticas de la Universidad del Valle (Cali-Colombia) en noviembre de 2005. Actualmente es profesor de planta de la Escuela de Matemáticas de la Universidad Industrial de Santander (UIS).