JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Transformación de Gray en anillos de Galois

Guillermo Morales-Luna

Departamento de Computación, Cinvestav-IPN, México, gmorales@cs.cinvestav.mx

Formulamos diversas presentaciones de la transformación de Gray, la cual permite identificar anillos de Galois con subconjuntos de espacios vectoriales sobre cuerpos finitos, por lo que es posible construir códigos sistemáticos de autenticación sobre anillos de Galois. Presentamos las nociones básicas involucradas, la generalización debida a Carlet y una generalización nuestra sobre anillos de Galois de cualquier característica.

Inicialmente recordamos hechos básicos de los anillos de Galois, particularmente los realizados mediante anillos de residuos, después la transformación básica de Gray, la generalización de Carlet, su versión en anillos de Galois de característica potencia de dos, y posteriormente nuestra propia generalización a cualquier característica.

Un *anillo de Galois* es uno finito R, con unidad, tal que su conjunto de divisores de cero,

$$Z(R) = \{r \in R - \{0\} \mid \exists s \in R : \ rs = 0\},$$

junto con el cero, es un ideal principal de R, es decir,

$$Z(R) \cup \{0\} = \langle p\,1 \rangle = \langle \underbrace{1 + \cdots + 1}_{p \text{ veces}} \rangle$$

para algún primo $p \in \mathbb{Z}^+$, $1 \in R$.

Ejemplo 1 (Aritmética modular) *Para un entero primo p y $s \in \mathbb{Z}^+$, el anillo de residuos $\mathbb{Z}_{p^s}$ posee una unidad, a saber el elemento $1 \in \mathbb{Z}^+$, y $\langle p \rangle$ es el único ideal maximal, el cual además coincide con $Z(\mathbb{Z}_{p^s}) \cup \{0\}$. En consecuencia, $\mathbb{Z}_{p^s}$ es un anillo de Galois. Se tiene, $\mathbb{Z}_{p^s}/\langle p \rangle = \mathbb{F}_p$, el cuerpo primitivo de característica p.*

Naturalmente, $\bmod p : a = \sum_{j=0}^{s-1} a_j p^j \mapsto a \bmod p = a_0$ es un homomorfismo de anillos $\mathbb{Z}_{p^s} \to \mathbb{F}_p$ con núcleo $\langle p \rangle$. Se extiende naturalmente a un homomorfismo $\bmod p : \mathbb{Z}_{p^s}[X] \to \mathbb{F}_p[X]$, $g(X) = \sum_{j=0}^{m-1} a_j X^j \mapsto g(X) \bmod p = \sum_{j=0}^{m-1} (a_j \bmod p) X^j$.

De manera general, si R es un anillo de Galois, el ideal $\langle p\,1 \rangle$ que coincide con el conjunto de los divisores de cero y de cero mismo en R, es el único ideal maximal (pues todo elemento fuera de él es una unidad) y, en consecuencia $R/\langle p\,1 \rangle$ es un cuerpo finito, es decir, es de la forma $\mathbb{F}_{p^m}$, y la característica de R es p^s, para alguna $s \in \mathbb{N}$. El anillo $\mathbb{Z}_{p^s}$ se identifica naturalmente con un subanillo de R, mediante el monomorfismo $r \mapsto r\,1$.

El ideal $\langle p\,1 \rangle$ consta de los divisores de cero. Cada ideal principal $\langle p^i\,1 \rangle$ tiene cardinal $p^{(s-i)m}$. En particular, $\operatorname{card}(\langle p\,1 \rangle) = p^{(s-1)m}$ y $\operatorname{card}(R) = p^{sm}$.

Sea $\pi : R \to R/\langle p\,1 \rangle$ la proyección canónica, la cual es un homomorfismo de anillos. Este se extiende a uno $\pi : R[X] \to (R/\langle p\,1 \rangle)[X]$.

Proposición 1 *Sea R un anillo de Galois de característica p^s y cardinal p^{sm}. Entonces R ha de ser isomorfo a $\mathbb{Z}_{p^s}[X]/\langle h(X) \rangle$, donde $h(X) \in \mathbb{Z}_{p^s}[X]$ es irreducible de grado m.*

Corolario 1 *Cualesquiera dos anillos de Galois de iguales características y de iguales cardinales han de ser isomorfos.*

En este caso, se escribe $R = \mathrm{GR}(p^s, m)$.

A manera de ejemplos se tiene a los siguientes:

- $\mathrm{GR}(p,m) = \mathbb{F}_{p^m}$
- $\mathrm{GR}(p^n,1) = \mathbb{Z}_{p^n}$.
- $\mathrm{GR}(2^2,3) = \mathbb{Z}_4[X]/(f(X))$ con $f(X) = X^3 + X + 1$.
- $\mathrm{GR}(2^2,3) = \mathbb{Z}_4[X]/(g(X))$ con $g(X) = X^3 + 2X^2 + X - 1$.
- $\mathrm{GR}(3^2,2) = \mathbb{Z}_9[X]/(h(X))$ con $h(X) = X^2 + 4X - 1$.

Proposición 2 (Representación p-ádica) *Existen un polinomio básico primitivo $h(X) \in \mathbb{Z}_{p^s}[X]$ de grado m, divisor de $X^{p^m-1} - 1$, y una raíz $\xi \in \mathrm{GR}(p^s, sm)$ de $h(X)$, de orden $p^m - 1$, tales que*

$$\mathrm{GR}(p^s, sm) = \mathbb{Z}_{p^s}[\xi] = \{ \sum_{j=0}^{m-1} a_j \xi^j |\ (a_j)_{j=0}^{m-1} \subset \mathbb{Z}_{p^s} \}.$$

Se tiene incluso que $h(X)$ es el único polinomio mónico de grado a lo sumo m que anula a ξ.

Sea $\Xi = \left(\xi^i\right)_{i=0}^{p^m-2}$. Entonces se tiene la representación p-ádica*:*

$$\forall c \in \mathrm{GR}(p^s, sm)\ \exists!\, (c_k)_{k=0}^{s-1} \subset \{0\} \cup \Xi :\ c = \sum_{k=0}^{s-1} c_k p^k.$$

Se tendrá además: [*c es una unidad* $\iff$ $c_0 \neq 0$.]

Ξ se dice ser un *conjunto de representantes de Teichmüller* en $\mathrm{GR}(p^s, sm)$.

Recordamos aquí la construcción básica de la transformación de Gray y la generalización hecha por Carlet [1].

El *alfabeto de bits* puede verse como cualquiera de las estructuras $(0+1) \approx \mathbb{Z}_2 \approx \mathbb{F}_2$ y el de *bigramas* como cualquiera de

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \approx \mathbb{Z}_4 \approx \mathbb{F}_2^{\mathbb{F}_2} \approx \mathbb{F}_2^2 \approx \mathbb{F}_{2^2},$$

de hecho una identificación entre ellas la da la *transformación de Gray*:

$$\Gamma : \mathbb{Z}_4 \to \mathbb{F}_2^2\ , \quad \begin{array}{ccc} 0 & \mapsto & 00 \\ 1 & \mapsto & 01 \\ 2 & \mapsto & 11 \\ 3 & \mapsto & 10 \end{array}$$

Actuando por componentes, ésta se extiende a una transformación $\Gamma : \mathbb{Z}_4^m \to \mathbb{F}_2^{2m}$, con $m \geq 1$. Para cada $r \in \mathbb{Z}_4$ se define $\nu(r) = w_H(\Gamma(r))$, donde w_H es el *peso de Hamming*, y para $\mathbf{r} = (r_i)_{i=0}^{m-1} \in \mathbb{Z}_4^m$ se define $\nu(\mathbf{r}) = \sum_{i=0}^{m-1} \nu(r_i)$. Se tiene entonces una métrica $\delta : \mathbb{Z}_4^m \times \mathbb{Z}_4^m \to \mathbb{N}$, $(\mathbf{r}, \mathbf{s}) \mapsto \delta(\mathbf{r}, \mathbf{s}) = \nu(\mathbf{s} - \mathbf{r})$, y ésta es tal que Γ es una isometría.

Alternativamente, al escribir en binario a cada $r \in \mathbb{Z}_4$ se tiene $r = r_0 + 2r_1$, con $r = (r_1 r_0)_2$, $r_0, r_1 \in \mathbb{F}_2$. Se define la *transformación de Gray*, en este caso, como $\Gamma : \mathbb{Z}_4 \to \mathbb{F}_2^{\mathbb{F}_2}$, $r \mapsto \Gamma(r)$, con

$$\Gamma(r) : \mathbb{F}_2 \to \mathbb{F}_2\ ,\ x \mapsto r_0 + x r_1$$

(aquí, las operaciones son las de $\mathbb{F}_2$).

Para $k \geq 2$, se define $\Gamma_k : \mathbb{Z}_{2^k} \to \mathbb{F}_2^{\mathbb{F}_2^{k-1}}$, como

$$\Gamma_k(r) : \mathbb{F}_2^{k-1} \to \mathbb{F}_2 \ , \ (x_0, \ldots, x_{k-2}) \mapsto r_0 + \sum_{\kappa=0}^{k-2} x_\kappa r_{\kappa+1} = r_0 + \langle \mathbf{r}_{-1} | \mathbf{x} \rangle$$

donde $r = \sum_{\kappa=0}^{k-1} r_\kappa 2^\kappa$, $r_\kappa \in \mathbb{F}_2$ y $\mathbf{r}_{-1} = (r_1 \ldots, r_{k-1}) \in \mathbb{F}_2^{k-1}$. Naturalmente, $\mathbb{F}_2^{\mathbb{F}_2^{k-1}} \approx \mathbb{F}_2^{2^{k-1}}$, por lo que la transformación de Gray puede verse como una aplicación $\Gamma_k : \mathbb{Z}_{2^k} \to \mathbb{F}_2^{2^{k-1}}$.

Para dos enteros $i, j \in \mathbb{Z}$ con $i \leq j$, escribiremos $[\![i, j]\!] = \{i, i+1, \ldots, j\}$.

Para un entero positivo $n \in \mathbb{Z}^+$ se define por coordenadas $\Gamma_{nk} : \mathbb{Z}_{2^k}^n \to \mathbb{F}_2^{2^{k-1}n}$, como

$$\Gamma_{nk}(\mathbf{r}) : [\![0, n-1]\!] \times \mathbb{F}_2^{k-1} \to \mathbb{F}_2 \ , \ (i; x_0, \ldots, x_{k-2}) \mapsto r_{i0} + \sum_{\kappa=0}^{k-2} x_\kappa r_{i,\kappa+1} = r_{i0} + \langle \mathbf{r}_{i,-1} | \mathbf{x} \rangle$$

donde $\forall i \in [\![0, n-1]\!]$, $r_i = \sum_{\kappa=0}^{k-1} r_{i,\kappa} 2^\kappa$, $r_{i,\kappa} \in \mathbb{F}_2$ y $\mathbf{r}_{i,-1} = (r_1 \ldots, r_{k-1}) \in \mathbb{F}_2^{k-1}$, $\mathbf{r} = (r_0, \ldots, r_{n-1})$.

Consideremos $s = 2$. Sea $\mathrm{GR}(p^2, m)^\star$ la colección de cadenas con elementos en el anillo de Galois $\mathrm{GR}(p^2, m)$. El *producto tensorial*, o *de Kroenecker*, usual se denota como

$$\otimes : \mathrm{GR}(p^2, m)^\star \times \mathrm{GR}(p^2, m)^\star \to \mathrm{GR}(p^2, m)^\star.$$

El *cuerpo residual* de $\mathrm{GR}(p^2, m)$ es $\mathrm{GR}(p^2, m)/\langle p\, 1 \rangle \approx \mathbb{F}_{p^m}$. La *proyección canónica* es

$$\pi : \mathrm{GR}(p^2, m) \to \mathbb{F}_{p^m}, \ z \mapsto z + \langle p\, 1 \rangle.$$

Sean $\mathbf{c} \in \mathbb{F}_{p^m}^{p^m}$ el vector en cuyas componentes aparecen todos los elementos de $\mathbb{F}_{p^m}$, y $\mathbf{u} \in \mathbb{F}_{p^m}^{p^m}$ el vector cuyas componentes son todas $1 \in \mathbb{F}_{p^m}$.

Para una cadena $\mathbf{a} \in \mathrm{GR}(p^2, m)^\star$ se aplica en cada componente la representación p-ádica para escribir $\mathbf{a} = \rho_0(\mathbf{a}) + p\rho_1(\mathbf{a})$. La transformación de Gray es

$$\Gamma_{pmn} : \mathrm{GR}(p^2, m)^n \to \mathbb{F}_{p^m}^{p^{mn}} \ , \ \mathbf{a} \mapsto \Gamma_{pmn}(\mathbf{a}) = \mathbf{c} \otimes \rho_0(\mathbf{a}) + \mathbf{u} \otimes \rho_1(\mathbf{a}). \tag{1}$$

Se puede definir una distancia d_H en $\mathrm{GR}(p^2, m)^n$ de manera que Γ_{pmn} sea una isometría

$$(\mathrm{GR}(p^2, m)^n, d_H) \to (\mathbb{F}_{p^m}^{p^{mn}}, d_h),$$

donde d_h es la distancia de Hamming usual en $\mathbb{F}_{p^m}^{p^{mn}}$.

Proposición 3 *Las relaciones siguientes son verdaderas:*

$$\begin{aligned} \forall \mathbf{a} \in \mathrm{GR}(p^2, m)^n : \qquad \Gamma_{pmn}(p\mathbf{a}) &= \underbrace{(r_0(\mathbf{a}), \ldots, r_0(\mathbf{a}))}_{p \text{ veces}} \qquad \text{con } r_0 = \pi \circ \rho_0, \\ \forall \mathbf{a}_0, \mathbf{a}_1 \in \mathrm{GR}(p^2, m)^n : \ \Gamma_{pmn}(\mathbf{a}_0 + p\mathbf{a}_1) &= \Gamma_{pmn}(\mathbf{a}_0) + \Gamma_{pmn}(p\mathbf{a}_1). \end{aligned}$$

De manera general, en cualquier característica, la transformación de Gray permite identificar a anillos de Galois con subconjuntos de espacios vectoriales sobre cuerpos de Galois.

Sea $\mathbb{F}_q^q$ el espacio vectorial de dimensión q sobre el cuerpo de Galois $\mathbb{F}_q$, naturalmente $q = p^s$ para algún primo p y un entero $s \in \mathbb{Z}^+$. El producto de Kroenecker es, en este contexto

$$\mathbb{F}_q^m \times \mathbb{F}_q^n \to \mathbb{F}_q^{mn} \ , \ \left((u_i)_i, (v_j)_j \right) \mapsto (u_i)_i \otimes (v_j)_j = (w_{in+j} = u_i v_j)_{i,j},$$

y al "reiterarlo por la derecha"

$$\bigotimes_{k=0}^{n} v_k = \left(\bigotimes_{k=0}^{n-1} v_k\right) \otimes v_n$$

se tiene una aplicación $(\mathbb{F}_q^m)^{n+1} \to \mathbb{F}_q^{m^{n+1}}$. Sea $\mathbf{e}_j = (\delta_{ij})_{i=0}^{q-1}$ el j-ésimo vector en la base canónica de $\mathbb{F}_q^q$, donde δ_{ij} es la delta de Kroenecker. Sea $\mathbf{u}^{(q)} = (1,\ldots,1) = \sum_{j=0}^{q-1} \mathbf{e}_j \in \mathbb{F}_q^q$ el vector con componentes constantes de valor 1.

Sea $R = \mathrm{GR}(p^s, m)$ el anillo de Galois de característica p^s y grado m. Sea $\rho : R \to \mathbb{F}_p$ la reducción módulo p. Sea $T(R) = \{0\} \cup \left(\xi_R^j\right)_{j=0}^{q-2}$ un conjunto de representantes de Teichmüller en R y sea

$$\Xi = (0, \rho(\xi_R), \ldots, \rho(\xi_R^{q-2}), \rho(\xi_R^{q-1})) \in \mathbb{F}_q^q.$$

Para cada $i = 0,\ldots,s-2$ sea

$$\begin{aligned} \phi_i &= \bigotimes_{k=0}^{s-2} \left(\mathbf{u}^{(q)} + \delta_{ik}(\Xi - \mathbf{u}^{(q)})\right) \\ &= \left(\mathbf{u}^{(q)}\right)^{\otimes i} \otimes \Xi \otimes \left(\mathbf{u}^{(q)}\right)^{\otimes(s-2-i)} \in \mathbb{F}_q^{q^{s-1}} \end{aligned} \tag{2}$$

(aquí, para cada $\mathbf{v} \in \mathbb{F}_q^q$, $\mathbf{v}^{\otimes 0} = (1)$ y $\mathbf{v}^{\otimes(k+1)} = \mathbf{v}^{\otimes k} \otimes \mathbf{v}$). De (2) se tiene que ϕ_i es la concatenación de q^i segmentos, cada uno consistente a su vez de la concatenación de segmentos de la forma $\rho_j \mathbf{u}^{(q^{s-2-i})}$, siendo ρ_j la j-ésima componente de Ξ, para $j = 0,\ldots,q-1$.

Proposición 4 *Cada ϕ_i puede ser calculado efectiva y eficientemente.*

En efecto, dado k, con $0 \le k \le q^{s-1}-1$, sean $k_0 = k \bmod q^{s-1-i}$ y $k_1 = \lfloor \frac{k_0}{q^{s-2-i}} \rfloor$. Entonces la k-ésima $\phi_i(k)$ es la k_1-ésima coordenada de Ξ.

En resumen, si $T(R) = \{0\} \cup \left(\xi_R^j\right)_{j=0}^{q-2}$ es un conjunto de representantes de Teichmüller en R, entonces los arreglos ϕ_i definidos por (2) pueden ser escritos como $\forall i \in [\![0, s-2]\!]$:

$$\phi_i = \left[[0]_{q^{s-2-i}}, [\rho(\xi_R)]_{q^{s-2-i}}, \ldots, \left[\rho(\xi_R^{q-2})\right]_{q^{s-2-i}}, \left[\rho(\xi_R^{q-1})\right]_{q^{s-2-i}} \right]_{q^i}. \tag{3}$$

donde $[z]_\ell = z\mathbf{u}^{(\ell)}$. Como un último vector se define

$$\phi_{r-1} = [1]_{q^{s-1}} = \mathbf{u}^{(q^{s-1})}.$$

La *transformación de Gray* es, en este caso,

$$\begin{aligned} \Gamma : \mathrm{GR}(p^s, m) = R &\to \mathbb{F}_q^{q^{s-1}} \\ \sum_{i=0}^{s-1} r_i p^i &\mapsto \Gamma\left(\sum_{i=0}^{s-1} r_i p^i\right) = \sum_{i=0}^{s-1} \rho(r_i)\, \phi_i \end{aligned} \tag{4}$$

donde los elements de R aparecen en sus formas p-ádicas.

En particular, para $s = 2$, Γ definida por (4) coincidirá con Γ_{pmn} definida por (1) para $n = 1$.

El espacio vectorial $\mathbb{F}_q^{q^{s-1}}$ es uno métrico provisto de la distancia de Hamming: la distancia entre dos vectores es el número de coordenadas en las que difieren.

Proposición 5 *Las aseveraciones siguientes se cumplen*

- **Isometría** *[2] La transformación de Gray es una isometría entre el anillo de Galois R y el espacio vectorial* $\mathbb{F}_q^{q^{s-1}}$ *:*

$$\forall u, v \in R: \;\; d_h(u,v) = d_H(\Gamma(u), \Gamma(v)).$$

- *La transformación de Gray satisface [4]:*

$$\forall (u,v) \in R \times p^{s-1}R: \; \Gamma(u+v) = \Gamma(u) + \Gamma(v),$$

donde $p^{s-1}R$ *es el ideal de divisores de cero en R.*

Es precisamente debido a la isometría determinada por la transformación de Gray entre el anillo de Galois y el correspondiente espacio vectorial que se puede construir, digamos que de manera natural, códigos sistemáticos de autenticación [3].

Referencias

[1] Claude Carlet. $\mathbb{Z}_{2^k}$-linear codes. *IEEE Transactions on Information Theory*, 44(4):1543–1547, 1998.

[2] Marcus Greferath and Stefan E. Schmidt. Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Transactions on Information Theory*, 45(7):2522–2524, 1999.

[3] Juan Carlos Ku-Cauich and Guillermo Morales-Luna. Authentication schemes based on resilient maps. *IACR Cryptology ePrint Archive*, 2014:547, 2014.

[4] Juan Carlos Ku-Cauich and Horacio Tapia-Recillas. Systematic authentication codes based on a class of bent functions and the Gray map on a Galois ring. *SIAM J. Discrete Math.*, 27(2):1159–1170, 2013.