SOBRE LA GENERACION DE NUMEROS PSEUDOALEATORIOS UNIFORMES

L. A. ROMERO*

RESUMEN

En este trabajo se presenta sistemáticamente la fundamentación de los métodos para la generación de números pseudoaleatorios uniformes basados en propiedades de polinomios primitivos sobre un campo de Galois módulo q. El desarrollo algébrico formal de dichas propiedades nos permite sugerir alternativas a su implementación a los usuarios de las CID.

INTRODUCCION

La generación de números pseudoaleatorios uniformes es el peso inicial para la obtención de valores variables que obedezcan a diversas distribuciones según las necesidades de las simulaciones o estrategias experimentales a efectuar.

*Dpto. de Neurofisiología, CNIC.

1 Inicialmente fueron los métodos congruenciales multiplicativos [2], pero esos métodos poseen la limitante de que el tamaño del período queda acotado por el largo de palabra del equipo digital que se utilice, lo que repercute además en la imposibilidad de su uso para la generación de un número arbitrario de variables aleatorias independientes [3], pues ello queda condicionado por el largo de palabra de que se disponga.

He aquí que se dispone de un método para la generación de números pseudoaleatorios uniformes basado en propiedades de polinomios primitivos cuyo período se puede hacer arbitrariamente largo, pues sólo está en función del grado del polinomio primitivo escogido y no de la máquina empleada; además de que la velocidad de generación en algunas de sus alternativas es varias veces superior a cualquier método congruencial multiplicativo.

Fundamentos del Método

En esta parte expondremos las definiciones y propiedades que nos hacen fácilmente comprensibles los fundamentos del método en su aspecto formal algébrico con todos sus alcances.

Llamaremos código por diferencias al código cuya función de codificación convierte un bloque inicial a de m-dígitos.

$$a = (a_0, a_1 \ldots\ldots, a_{m-1})$$

en una sucesión infinita $S = \{s_0, s_1, \ldots\ldots, s_n, \ldots\ldots\}$ definida por medio de una ecuación lineal en diferencias ΔE de la forma

$$C_0 s_i = C_1 s_{(i-1)} + \ldots + C_m s_{(i-m)} = 0 \quad \Delta E, \qquad (1)$$

donde $i = m, m-1, \ldots$ y C_i, s_i, pertenecen a un campo de Galois módulo q que denotamos GF(q). La secuencia código S comienza con el bloque

$$s_0 = A_0, \; s_1 = A_1, \; \ldots, \; s_{m-1} = A_{m-1}$$

Como primera propiedad se nos presenta que toda sucesión S asociada a una ecuación lineal en diferencias como (1) es periódica.

Como prueba de lo anterior tenemos que dada la sucesión S generada por la ecuación ΔE de (1), podemos ver que la función codificadora que está dada por ΔE y que expresamos

$$f: (s_0, s_1, \ldots, s_{m-1}) \rightarrow (s_1, s_2, \ldots, s_{m-1}, -C_0^{-1} (\sum_{i=1}^{m} C_i s_{m-1}))$$

es lineal y por tanto un morfismo del grupo aditivo de todos los m-plos sobre el campo GF(q). Ocurre que f toma el vector nulo sólo sobre el vector nulo. En efecto, si $f(s_0, s_1, \ldots, s_{m-1}) = \bar{0}$ entonces $s_1 = s_2 = \ldots = s_{m-1} = 0$ y $-C_m s_0 = 0$ luego $s_0 = 0$,

puesto que es uno-a-uno, es una permutación sobre el conjunto de las m-plos sobre GF(q), por tanto existirá r tal que $f^{r-1} = f$ y f^r será pues la transformación identidad.

Ahora vemos que $f^k(s_0, \ldots, s_{m-1}) = (s_k, \ldots, s_{m-k-1})$ en la secuencia iniciada por $(s_0, \ldots, s_{m-1})$ y continuada por uso de ΔE, quedando demostrada la propiedad.

Con el propósito de comodidad notacional introducimos los operadores de "desplazamiento" X definidos sobre F^W espacio de todas las sucesiones infinitas $S = \{s_i\}$ $i \in \mathbb{N}$ de elementos de GF(q) de la forma

$$X: (s_0, s_1, \ldots, s_i, \ldots) \rightarrow (0, s_0, s_1, \ldots, s_{i-1}, \ldots),$$

"desplazamiento a la derecha"

quedando según esta notación las ecuaciones en diferencias ΔE en la forma

$$\left[C_0 I + C_1 X^{-1} + \ldots + C_m X^{-m}\right] S = \bar{0}$$

donde $C_o \neq 0$, $C_m = 1$

y al polinomio

$$C(X) = C_o + C_1X + \ldots + C_mX^m$$

le llamamos polinomio característico a la izquierda, y al polinomio recíproco (con raíces recíprocas)

$$\overline{C}(X) = C_oX^m + C_1X^{m-1} + \ldots + C_m$$

polinomio característico (a la derecha)

Como ilustración de la notación introducida exponemos el siguiente ejemplo:

Sea GF (q) Z_2 (Campo de Galois módulo 2)

y la ecuación en diferencias E dada por

$$S_i + S_{i-1} + S_{i-3} = 0 \ (\text{mod.}2)/$$

En este caso el polinomio característico (a la izquierda será

$$C(X) = 1 + X + X^3.$$

En efecto, si tenemos $S = \{S_o, S_1, S_2, \ldots, S_i, \ldots\}$ entonces

$$I(S) = S_o, S_i, \ldots S_i, \ldots$$

$$X(S) = 0, S_o, S_1, \ldots, S_{i-1}, \ldots$$

$$X^3(S) = 0, 0, 0, S_o, S_1, \ldots, S_{i-3}, \ldots,$$

sumando

$$(I + X + X^3)S = (S_o, S_1 + S_o, S_2 + S_1, S_3 + S_2 + S_o, S_4 + S_3 + S_1, \ldots) = \overline{0}$$

donde se aprecia que los términos de orden $i > 3$ cumplen

$$S_i + S_{i-1} + S_{i-3} = 0 \ (\text{mod. } 2).$$

Designaremos también por Función Generadora de una sucesión infinita $S = \{S_i\}$ $i \in \mathbb{N}$ a la que viene dada por la serie de potencias formales

$$S(X) = \sum_{i=0}^{\infty} S_iX^i$$

Tendremos, pues, si el conjunto de los coeficientes constituye un anillo conmutativo R entonces el conjunto R $[[X]]$ de todas las series formales de potencias con dichos coeficientes será un anillo conmutativo; y en él podremos llamar invertible al elemento $P(X) \in R$ $[[X]]$ tal que exista $q(X) \in R$ $[[X]]$ cumpliendo

$$P(X).q(X) = 1$$

y ocurriendo por tanto que los coeficientes de las series formales respectivas satisfarán las ecuaciones

$$P_oq_o = 1$$

$$P_oq_1 + P_1q_o = 0$$

$$P_oq_2 + P_1q_1 + P_2q_2 = 0$$

$$P_oq_n + P_1q_{n-1} + \ldots + P_nq_o = 0$$

quedando, pues, como una condición necesaria y suficiente para que $P(X) = \sum_{i=0}^{\infty} P_iX^i$ sea invertible en R $[[X]]$ el hecho de que p_o lo sea en el anillo R.

Tenemos ahora que una ecuación en diferencias ΔE generadora de códigos con $C_o = 1$ y $C_m \neq 0$ posee polinomio característico sobre el campo GF(q)

$$C(X) = C_o + C_1X + \ldots + C_mX^m + 0X^{m-1} + \ldots$$

invertible en GF $[[X]]$.

Lográndose con todo ello el siguiente resultado:

La secuencia S con función generadora

$$S(X) = S_o + S_1X + S_2X^2 + \ldots = \sum_{i=0}^{\infty} S_iX^i,$$

donde

$$S(X) = \frac{a(x)}{c(x)}$$

y a (x) es de longitud o grado $L < m$, satisface ΔE con polinomio característico $C(X)$.

Lo anterior se aprecia en el razonamiento siguiente; puesto que

$$C(X) \cdot S(X) = A_0 + A_1X + \ldots + A_{m-1}X^{m-1} + 0X^m + \ldots$$

en GF $[[X]]$, de la definición de producto,
en GF $[[X]]$ el coeficiente X^n es

$$CS_n + C_1S_{n-1} + \ldots + C_nS_0 = 0 \text{ para } n \geq m.$$

En el caso $C_0 =$, ello es idéntico a la ecuación (1), luego la secuencia S asociada a la serie formal satisface ΔE. Como corolarios de lo anterior apuntamos los siguientes. Cada solución $S = \{S_i\}$, $i \in \mathbb{N}$ de la ecuación Δ E tiene en R $[[X]]$ una función generadora

$$S(X) = \sum_{i=0}^{\infty} S_iX^i = \frac{a(X)}{c(X)}$$

donde $C(X)$ es el polinomio característico para Δ E.

Además, dada la ecuación E con polinomio característico $C(X)$ sobre GF(q), el conjunto $S(C(X))$ de todas las soluciones de Δ E es el mismo que el conjunto de todas las secuencias de coeficientes de series de potencias formales $S(X) = \frac{a(X)}{c(X)}$ para las cuales grado (a) < grado (c).

Denotemos ahora por P_s el conjunto de todos los polinomios $p(X) = \sum_{i=0}^{r} P_iX^i$ tales que aplicando el "operador desplazamiento" (a la izquierda) tengamos

$$(P_0I + P_1X^{-1} + P_2X^{-2} + \ldots + P_rX^{-r})\, S = \bar{0}$$

para una sucesión S dada.

Tendremos que dicho conjunto P_s es un ideal del anillo de los polinomios GF $[[X]]$. Además, como GF $[X]$ es un anillo

euclideano y por tanto un anillo ideal principal (5), se desprende que dada S existe un polinomio característico (con coeficiente del término de mayor grado igual a la unidad) único C_s tal que

$$P(X^{-1}) = \bar{0} \text{ si y sólo si } C_s(X) \mid p(X)$$

A este polinomio C_s le llamamos polinomio minimal para la sucesión S.

De lo anterior se deriva el importante teorema que plantea que si el polinomio característico $C(X)$ de la ecuación ΔE es irreducible en el campo GF(q), entonces cada solución no trivial S satisface precisamente aquellas ΔE-ecuaciones con coeficientes constantes cuyo polinomio característico es un múltiplo de $C(X)$.

Con todo lo anterior se puede entonces entrar a abordar el cálculo de los períodos de las sucesiones asociadas a polinomios primos en GF(q).

Para ello primero observamos que si $f(X)$ y $g(X)$ son dos polinomios no nulos primos relativos sobre GF(q) y $h(X) = f(X).g(X)$ su producto, entonces

$$S(h(X) = S(f(X) + S(g(X)) \text{ donde}$$

$$S(f(X)) + S(g(X)) = \left\{ (S + S') \;\middle|\; S \in S\,(f(X)),\ S' \in S\,(g(X)) \right\}$$

Esta propiedad se puede ver al razonar que $S(f(X)) \cap S(g(X)) = \bar{0}$, ya que si $S \in S(f(X)) \cap S(g(X))$ entonces el polinomio minimal debe ser divisor común para f y g pero al ser f y g primos relativos ello implica que $C_s(X) = 1$ y $S = \bar{0}$.

Por otra parte, puesto que S(h) contiene a ambos S(f) y S(g) debe contener a la suma directa S(f) + S(g) cuya dimensión como espacio vectorial sobre GF(q) es (grado (f) + + grado (g)) igual a grado (h), luego el conjunto de sumas (s + s') agota S(h).

Definiciones de período de una sucesión y orden de un polinomio.

a) Período $\mathcal{T}(s)$ de una sucesión s es igual al menor entero positivo tal que

$$S_i = S_{i+r} \text{ para todo } i \in \mathbb{N}$$

b) Orden de un polinomio $f(X) = \sum_{i=0}^{m} f_i X^i$ con $f_o \cdot f_m \neq 0$ es el más pequeño $n \in \mathbb{N}$ tal que

$$f(X) \mid (X^n - 1)$$

denotaremos ord $f = n$.

Tendremos, pues, la siguiente propiedad: sean $S \in S(f(X))$ y $S' \in S(g(X))$ y sean $f(X)$ y $g(X)$ primos relativos, entonces el período $\mathcal{T}(S + S')$ es igual al mínimo común múltiplo (m.c.m.) de $\mathcal{T}(S)$ y $\mathcal{T}(S')$.

Justificaremos lo anterior razonando que si llamamos

$\mathcal{T}_1$ período de $S \in S(f(X))$, $\mathcal{T}_1 = \mathcal{T}(S)$

$\mathcal{T}_2$ período de $S' \in S(g(X))$, $\mathcal{T}_2 = \mathcal{T}(S')$

$\mathcal{T}_3$ período de $(S + S') \in S(f(X)) + S(g(X))$, $\mathcal{T}_3 = \mathcal{T}(S + S')$

tendremos

a) $S_i = S_{(i + \mathcal{T}_1)}$ para todo i

b) $S'_i = S'_{(i + \mathcal{T}_2)}$ para todo i

c) $S_i + S'_i = S_{(i + \mathcal{T}_3)} + S'_{(i + \mathcal{T}_3)}$ para todo i

si tomamos $k = $ m.c.m. $(\mathcal{T}_1, \mathcal{T}_2)$ sucederá al sumar que

$$S_i + S'_i = S_{i+k} + S'_{i+k},$$

luego por definición de $\mathcal{T}_3$ ocurre que $\mathcal{T}_3 \mid k$.

Por otra parte, por definición de $\mathcal{T}_3$ se logran elementos tanto de $S(f(X))$ como de $S(g(X))$ con esa periodicidad ya que $S(f(X)) \cap S(g(X)) = \bar{0}$, por tanto $\mathcal{T}_3$ debe ser múltiplo de $\mathcal{T}_1$,

al propio tiempo que de $\mathcal{T}_2$, luego necesariamente $\mathcal{T}_3 = k$ por ser período para $S + S'$.

Pueden establecerse ahora los siguientes lemas:

Lema 1. Para cualquier $S \in S(f(X))$, $\mathcal{T}(S)$ divide ord. (f).

Prueba: Puesto que $f(X) \mid (X^{\text{ord. } f} - 1)$ tendremos que $(X^{\text{ord}(f)} - 1)\, S = \bar{0}$, entonces $S_i = S_{i + \text{ord. } f}$ luego $\mathcal{T}(S) \mid$ ord. (f) para cada $\mathcal{T}(S)$, $S \in S(f(S))$.

Lema 2. Si $f(X)$ es polinomio minimal para una sucesión S, entonces ord.$(f) = \mathcal{T}(S)$.

Prueba: puesto que $S \in S(X^{\mathcal{T}(S)} - 1)$ y $f(X) \mid (X^{\mathcal{T}(S)} - 1)$ entonces ord.$(f) \leq \mathcal{T}(S)$, pero por lema 1,

$\mathcal{T}(S) \mid$ ord.(f), quedando ord.$(f) = \mathcal{T}(S)$.

Como corolario importante de lo anterior nos queda que si $f(X)$ es irreducible sobre GF(q), entonces cada sucesión no nula $S \in S(f(X))$ tiene período $\mathcal{T}(S) =$ ord.(f). Y podemos ver con claridad el teorema que establece el período máximo para las sucesiones a generar:

Teorema. Sea $f(X)$ tal que divida a $(X^{(q^n - 1)} - 1)$, $f(X)$ sobre GF(q) y grado $f(X) = n$ y sea $f(X)$ de manera que no divida a polinomio de la forma $(X^t - 1)$ con $t < q^{n-1}$. ($f(X)$ polinomio primitivo). Entonces $\mathcal{T}(S) = q^{n-1}$ para toda sucesión no nula de $S(f(X))$.

Para demostrar esto podemos ver que si $f(X)$ divide a $(X^{(q^{n-1})} - 1)$ entonces $\mathcal{T}(s) \mid (q^{n-1})$ para toda $S \in S(f(X))$. Supongamos ahora que $\mathcal{T}(S) \mid t$ para algún $t < q^{n-1}$, entonces ello obliga a que $S \in S(X^t - 1)$ y por tanto $f(X) \mid (X^t - 1)$, contrario a lo supuesto en el enunciado; por consiguiente $\mathcal{T}(S) = q^n - 1$ para toda S no nula.

Estas son llamadas sucesiones de período maximal.

Es decir que disponemos de propiedades de polinomios primitivos que siendo característicos para una sucesión establecen el tamaño del período de la misma sólo en función del grado del mencionado polinomio.

Sobre la implementación de método en su aplicación para la generación de números aleatorios uniformes:

Para ello se desarrolló en nuestro departamento un programa en nemotécnico para trabajar sobre campos módulo dos. El analista Co. O. Báez implementó dicha fórmula de suma módulo 2, dejándola como una Function del Fortran de la CID 201 B del laboratorio.

Una implementación en campos módulo 2 aparece en (4). También podemos ver la siguiente alternativa: si se tiene en cuenta que el anillo Z_q (de los enteros módulo q) es un dominio de integridad si y sólo si q es primo (5) y que todo dominio de integridad finito es un campo, tenemos que con una aritmética módulo q primo puede desarrollarse directamente el método de obtención de la sucesión pseudoaleatoria S con la propia aritmética, con sólo la programación de las operaciones con el polinomio primitivo según el campo GF(q) que se escoja, teniendo, pues, como ventaja siempre que el ciclo a obtener estará sólo en función del grado de dicho polinomio.

BIBLIOGRAFIA

[1] A.C. Atkinson and M.C. Pearce: "The Computer Generation of Beta, Gamma and Normal Bandom Variables". J. Statist. Soc. A., Part 4, 1976.

[2] B. Soucek: "Minicomputers in Data Processing and Simulation". Wiley-Interscience, 1972.

[3] Coveyou et al.: "Fourier Analysis of Uniform Random Number Generation". J.A.C.M., 14 Jan. 1967.

[4] T.G. Lewis and W.H. Payne: "Generalized Feedback Shift Register Pseudorandom Number Algorithm". J.A.C.M., vol. 20 # 3, Jul. 1973.

[5] S. Lang: Algebra, Ed. Aguilar, 1971.