GENERACIÓN ALEATORIA DE PERMUTACIONES DEL GRUPO SIMÉTRICO O DEL GRUPO ALTERNADO

P. Freyre[1]* y N. Díaz*
*Facultad de Matemática y Computación, Universidad de La Habana, Cuba.

ABSTRACT
In this paper three new algorithms for the random generation of permutations of degree n are shown, two of them for the Symmetric group S_n and one for the Alternating group A_n, in such a way, that they are mainly carried out by means of the operation of additions mod n o mod i, i = n..2.

MSC: 20B30

KEYWORDS: Random permutation, Symmetric group, Alternating group, S – boxes and Booleans functions.

RESUMEN
En este artículo se muestran tres nuevos algoritmos para la generación aleatoria de permutaciones de grado n, dos para el grupo Simétrico S_n y uno para el grupo Alternado A_n, las operaciones fundamentales que realizan los tres algoritmos son sumas mod n o mod i, i = n..2.

1. INTRODUCCIÓN

R. Sedgewick en [8] reporta que en los 20 años anteriores a la publicación de su trabajo se publicaron más de 30 algoritmos para la generación por computadoras de las n! permutaciones. Desde entonces son muchos los algoritmos para la generación aleatoria de permutaciones que se conocen [1], [3], [4], [5] y [10].

Un nuevo enfoque para la investigación del grupo Simétrico es el que se realiza desde la Teoría de Grupos Computacional cuando en 1971. C. Sims introduce los conceptos de base y conjunto generador fuerte lo que permite una representación e investigación efectiva de los grupos de permutaciones [2], [7], [9], [11] y [12].

El objetivo de este trabajo es la presentación de tres nuevos algoritmos para la generación aleatoria de permutaciones dos para el grupo Simétrico S_n y uno para grupo Alternado A_n. Los algoritmos y su fundamentación se alcanzan siguiendo el camino desarrollado en la Teoría de Grupos Computacional por C. Sims, en lo referente a la generación aleatoria de un elemento de un grupo finito [11] y [12].

A continuación se describen, a manera de ejemplo, tres algoritmos representativos para la generación aleatoria de permutaciones [8] y [6].

El primero parte de la generación aleatoria de una sucesión de signos enteros entre 1 y n, donde n es el grado de la permutación. La permutación aleatoria π se forma tomando, de la sucesión aleatoria de signos entre 1 y n, n signos sin repetición $\pi_1\ \pi_2\ \ldots\pi_n$ quedando conformada la permutación de la siguiente manera: $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi_1 & \pi_2 & \ldots & \pi_n \end{pmatrix}$

[1] pfreyre@matcom.uh.cu

El segundo algoritmo se basa en que todo entero x, que cumple que $0 \leq x < n!$, se puede escribir de manera única a través de la siguiente expresión:
$X = (n - l)!\, C_{n-1} + (n - 2)!\, C_{n-2} + \ldots + 2!\, C_2 + C_1$, donde los enteros C_j cumplen que $0 \leq C_j \leq j$, $1 \leq j < n$ y n es el grado de la permutación.
De esta manera la selección aleatoria de una permutación se alcanza generándose aleatoriamente los valores C_j, $1 \leq j < n$.
El tercer algoritmo es el conocido por Shuffling y por su simplicidad es muy utilizado, este algoritmo necesita tener almacenada una permutación inicial para su realización.
En el presente trabajo primero se exponen en forma de seudo código dos algoritmos para la generación aleatoria de permutaciones del grupo Simétrico y uno para el grupo Alternado, posteriormente se demuestran un lema y tres teoremas que constituyen el soporte teórico de los tres algoritmos, se finaliza el trabajo con las conclusiones.

2. DESARROLLO

2.1.- Descripción de los nuevos algoritmos

Los algoritmos 1 y 2 que se describen a continuación permiten la generación aleatoria de las permutaciones del grupo Simétrico y el algoritmo 3 la generación aleatoria de las permutaciones del grupo Alternado, este algoritmo en su estructura utiliza el algoritmo 1, pero puede ser construido también utilizando el algoritmo 2.

Algoritmo 1.-Generación aleatoria de permutaciones del grupo Simétrico S_n

Input: Sucesión Aleatoria γ_i, donde $\gamma_i \in \{i, i+1, \ldots, n\}$, i = 1, 2, …, n-1.

$\gamma_n = n$;
For j = 1 to n do
Begin
Per [j] = j;
For i = j down to 1 do
Begin
Per[j] = (Per[j] + $\gamma_i - i$ *)*
If Per [j] > n then Per [j] = (Per [j] + i -1) mod n;
end;
end;

Ouput: $Per = \begin{pmatrix} 1 & 2 & \ldots & n \\ Per[1] & Per[2] & \ldots & Per[n] \end{pmatrix}$

Algoritmo 2.-Generación aleatoria de permutaciones del grupo Simétrico S_n

Input: Sucesión Aleatoria γ_i, donde $\gamma_i \in \{i, i-1, \ldots, 1\}$, i = n, n-1, …, 2.

$\gamma_1 = 0$;
For j = n down to 1 do
Begin
Per [j] = j;
For i = j to n do
Begin
Per[j] = (Per[j] + γ_i *) mod i;*
If Per [j] = 0 then Per [j] = i;
end;
end;

Ouput: $Per = \begin{pmatrix} 1 & 2 & \ldots & n \\ Per[1] & Per[2] & \ldots & Per[n] \end{pmatrix}$

Algoritmo 3.- Generación aleatoria de permutaciones del grupo Alternado A_n para n par.

Input: Sucesión Aleatoria γ_i, donde $\gamma_i \in \{i, i+1, \ldots, n\}$, $T^{(i)} = (i, i+1, i+2) \in A_n$

y i = 1, 2, ..., n – 2.
$\gamma_{n-1} = n - 1; \gamma_n = n$;
For j = 1 to n do
Begin
Per[j] = j;
For i = j downto 1 do
If I par then
Begin
Per[j] = (Per[j] + γ_i– 1);
If Per[j] > n then (Per[j] + i– 1) mod n;
end;
Else
Begin
If γ_i–i> 0 then
Begin
Per[j] = ($T^{(i)}$(Per[j]));
If Per[j] >i then (Per[j] + γ_i–i– 1);
If Per[j] > n then (Per[j] + i) mod n;
end;
end;
end;

Output: $Per = \begin{pmatrix} 1 & 2 & \dots & n \\ Per[1] & Per[2] & \dots & Per[n] \end{pmatrix}$

Para n impar el algoritmo es similar.

2.2.- Soporte teórico de los algoritmos.

En este epígrafe los autores enuncian y demuestran un lema y tres teoremas que constituyen el soporte teórico de los tres algoritmos del epígrafe anterior.
En los enunciados y demostraciones de los teoremas y lemas se asume que:

1. Una base para el grupo Simétrico S_n tiene n-1 elementos de Ω = {1, 2, ...,n} y para el grupo Alternado A_n tiene n – 2 [7] y [12].
2. El símbolo ⌊⌋ denota a la función parte entera.
3. Para x mod s = y si y = 0 entonces se toma y = s, esto hace que la representación de las permutaciones sea de la siguiente manera: $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi_1 & \pi_2 & \dots & \pi_n \end{pmatrix} \in S_n$.

Tenemos que G es el grupo Simétrico o el Alternado y Ω es el conjunto {1, 2, ...,n}. La acción de g ∈G sobre β∈Ω se denotará por $\beta^g \in \Omega$. El estabilizador en G de los puntos $\beta_1, \beta_2, \dots, \beta_i \in \Omega$ se denotará como $G_{\beta_1,\dots\beta_i}$. Una base para G es una secuencia finita de puntos B = ($\beta_1, \beta_2, \dots, \beta_k$) tal que $G_{\beta_1,\dots\beta_k} = \{I_n\}$, donde I_n denota la permutación identidad. La base B determina una cadena descendente de estabilizadores $G = G^{(1)} \supseteq G^{(2)} \supseteq G^{(3)} \dots \supseteq G^{(k+1)} = \{I_n\}$, donde $G^{(i)} = G_{\beta_1,\dots\beta_{i-1}}$ [2], [7], [9], [11] y [12].

La órbita de β∈Ω bajo la acción de G es $\beta^G = \{\beta^g / g \in G\}$. Dado la base B = ($\beta_1, \beta_2, \dots, \beta_k$), las órbitas básicas, que se denotan como $\Delta^{(i)}$, son conjuntos de puntos $\beta_i^{G^{(i)}} \in \Omega$, para i =1, 2, …, k. [2], [7], [9], [11] y [12].

Definición 2.2.1.- Estructura de Schreier. Se define la estructura de Schreier para una base B como el arreglo $L = [L_{\beta_1}, \dots, L_{\beta_k}]$ en el cuál $L_{\beta_i} = \begin{bmatrix} \beta_i, \alpha_1, \alpha_2, \dots \alpha_{s_i} \\ I_n, g_1^{(i)}, g_2^{(i)}, \dots g_{s_i}^{(i)} \end{bmatrix}$, $\Delta^{(i)} = (\beta_i, \alpha_1, \alpha_2, \dots, \alpha_{s_i})$, $g_1^{(i)}, g_2^{(i)}, \dots, g_{s_i}^{(i)} \in G^{(i)}$, $\beta_i^{g_1^{(i)} g_2^{(i)} \dots g_j^{(i)}} = \alpha_j$, i = 1, 2,…, k y j = 1, 2,…, s_i

Definición 2.2.2.- Transversal derecho. Llamamos transversal derecho de $G^{(i+1)}$ en $G^{(i)}$ al conjunto $U_i=\{x_0 , x_1 , x_2 ,\ldots, x_{t_i}\}$ de representantes de los cosetos derechos de $G^{(i+1)}$ en $G^{(i)}$, siendo x_0 =Id y t_i+1 el índice de $G^{(i+1)}$ en $G^{(i)}$.

Todo elemento $g \in G$ se puede expresar de manera única como un producto $g = u_k u_{k-1}\ldots u_1$ con $u_i \in U_i$ = $\left\{\prod_{j=0}^{l} g_j^{(i)} / g_0^{(i)} = I_n, l = 0,1,\ldots, s_i\right\}$ y i = 1, 2,…, k, donde U_i es el transversal derecho de $G^{(i+1)}$ en $G^{(i)}$.

Una selección aleatoria de los elementos de G se alcanza mediante una selección aleatoria de los elementos de U_i, i = 1, 2,…, k, [2], [7], [9], [11] y [12].

Lema: 2.2.1.- Sea $g^{(i)} = (i, i + 1, ..., n) \in G^{(i)}$, $\alpha = i, i + 1, ..., n$, $\gamma_i \in \{1, 2, ..., n - i\}$ y i = 1, 2, ..., n – 1.

Entonces $\left(g^{(i)}\right)^{\gamma_i}(\alpha) = (\alpha + \gamma_i + (\lfloor(\alpha + \gamma_i)/(n + 1)\rfloor)(i - 1)) \bmod n$.

Demostración

Si $\alpha + \gamma_i \le n$, entonces $\left(g^{(i)}\right)^{\gamma_i}(\alpha) = (\alpha + \gamma_i)$, i = 1, 2, … ,n – 1, porque cuando la permutación $g^{(i)} = (i, i + 1, \ldots, n)$ actúa γ_i veces sobre α el valor resultante no es mayor que la longitud del ciclo de la permutación.

Si $\alpha + \gamma_i > n$, entonces $\left(g^{(i)}\right)^{\gamma_i}(\alpha) = (\alpha + \gamma_i + (\lfloor(\alpha + \gamma_i)/(n + 1)\rfloor)(i - 1)) \bmod n$, i = 1, 2, …, n – 1, porque cuando la permutación $g^{(i)} = (i, i + 1, \ldots, n)$ actúa γ_i veces sobre α el valor resultante es mayor que la longitud del ciclo de la permutación. Por tanto es necesario realizar un desplazamiento de i – 1 pasos.

□.

Teorema 2.2.1.- Sea B = (1, 2, …,n – 1) una base para el grupo Simétrico S_n, entonces $\alpha^{u_i} = (\alpha + \gamma_i - i + (\lfloor(\alpha + \gamma_i - i)/(n + 1)\rfloor)(i - 1)) \bmod n$, donde: $\alpha \in \Omega$, $u_i = \left(g^{(i)}\right)^{\gamma_i - i} \in U_i$, U_i es el tranversal derecho de $G^{(i+1)}$ en $G^{(i)}$, $g^{(i)} = (i, i+1, \ldots, n) \in G^{(i)}$, $\gamma_i \in \{ i, i+1, \ldots, n\}$ y i = 1, 2, ..., n – 1.

Demostración

Sea B = (1, 2, …,n – 1) una base para el grupo Simétrico S_n [7]. Por la transitividad de los subgrupos en la cadena de estabilizadores, tenemos que en la estructura de Schreier L_{β_i} puede ser descrita de la siguiente manera:

$L_{\beta_i} = \begin{bmatrix} i\ ,\ i+1\ ,i+2\ ,\ldots,n \\ I_n,\ g^{(i)},\ g^{(i)},\ldots,\ g^{(i)} \end{bmatrix}$, $\Delta^{(i)} = (i\ ,\ i+1,\ldots,n)$, $g^{(i)} = (i, i+1,\ldots,\ n) \in G^{(i)}$ y i = 1, 2, ..., n – 1. Entonces, U_i = $\{ \left(g^{(i)}\right)^{s_i}$, s_i = 0, 1, ..., n – i, i = 1, 2, ..., n -1 y $\left(g^{(i)}\right)^0 = I_n\}$.Tomando en cuenta la estructura cíclica de la permutación $g^{(i)}$, i = 1, 2, …, n -1 y que $\alpha \le n$. Entonces, por el lema II.2.1 tenemos que: $\alpha^{u_i} = \left(g^{(i)}\right)^{\gamma_i - i}(\alpha) = (\alpha + \gamma_i - i + (\lfloor(\alpha + \gamma_i - i)/(n + 1)\rfloor)(i - 1)) \bmod n$, donde $\gamma_i \in \{ i, i+1, \ldots, n\}$ y , i = 1, 2, ...,n– 1.

□.

Teorema 2.2.2.- Sea B = (n, n-1, …,2) una base para el grupo Simétrico S_n, [7] entonces $\alpha^{u_i} = (\alpha + \gamma_i) \bmod n-i+1$, donde: $\alpha \in \Omega$, $u_i = \left(g^{(i)}\right)^{\gamma_i} \in U_i$, U_i es el tranversal derecho de $G^{(i+1)}$ en $G^{(i)}$, $g^{(i)} = (n-i+1, 1, \ldots, n-i) \in G^{(i)}$, $\gamma_i \in \{ n-i+1, 1, ..., n-i \}$ y i = 1, 2, ..., n-1.

Demostración

La demostración es similar a la del teorema anterior asumiendo que:

La estructura de Schreier L_{β_i} puede ser descrita de la siguiente manera:

$L_{\beta_i} = \begin{bmatrix} n-i+1\ ,\ 1\ ,\ \ 2\ ,\ldots,\ n-i \\ I_n,\qquad g^{(i)},\ g^{(i)},\ldots,\ g^{(i)} \end{bmatrix}$, $\Delta^{(i)} = (n-i+1,1,\ldots,n-i)$, $g^{(i)} = (n-i+1,\ 1,\ldots,\ n-i) \in G^{(i)}$ y i = 1, 2, ..., n – 1.

□.

Teorema 2.2.3.- Sea B = (1, 2, …,n – 2) una base para el grupo Alternado A_n. Entonces:
Para n par:
Si i es impar

$$\alpha^{u_i} = \left\{ \begin{array}{c} \alpha \text{ if } \gamma_i = i \\ else \\ T^{(i)}(\alpha) + \gamma_i - i - 1 + (\lfloor (T^{(i)}(\alpha) + \gamma_i - i - 1)/(n+1) \rfloor)(i) \mod n \end{array} \right\}$$

Si i es par

$$\alpha^{u_i} = (\alpha + \gamma_i - i + (\lfloor (\alpha + \gamma_i - i)/(n+1) \rfloor)(i - 1)) \bmod n$$

Para n impar

Si i es par

$$\alpha^{u_i} = \left\{ \begin{array}{c} \alpha \text{ if } \gamma_i = i \\ else \\ T^{(i)}(\alpha) + \gamma_i - i - 1 + (\lfloor (T^{(i)}(\alpha) + \gamma_i - i - 1)/(n+1) \rfloor)(i) \mod n \end{array} \right\}$$

Si i es impar

$$\alpha^{u_i} = (\alpha + \gamma_i - i + (\lfloor (\alpha + \gamma_i - i)/(n+1) \rfloor)(i - 1)) \bmod n$$

Donde: $\alpha \in \Omega$, $u_i \in U_i$, U_i es el tranversal derecho de $G^{(i+1)}$ en $G^{(i)}$, $g^{(i)} = (i, i+1, \ldots, n) \in G^{(i)}$, $\gamma_i \in \{ i, i+1, \ldots, n\}$, $T^{(i)} = (i, i+1, i+2) \in A_n$ y i = 1, 2, ..., n –2.

Demostración

Sea B = (1, 2, …,n – 2) una base para el grupo Alternado A_n [7]. Por la transitividad de los subgrupos en la cadena de estabilizadores, tenemos que en la estructura de Schreier L_{β_i} puede ser descrita de la siguiente manera:

Para n par tenemos que si i es impar, entonces:

$$L_{\beta_i} = \begin{bmatrix} i, & i+1, & i+2, & \ldots, & n \\ I_n, & T^{(i)}, & g^{(i)}, & \ldots, & g^{(i)} \end{bmatrix}$$, $\Delta^{(i)} = (i, i+1, \ldots, n)$, $g^{(i)} = (i+1, i+2, \ldots, n)$ y $T^{(i)} = (i, i+1, i+2) \in G^{(i)}$ y i = 1, 2, ..., n – 3. Lo que nos lleva a que:

$U_i = \{ \left(g^{(i)}\right)^{s_i} \left(T^{(i)}\right)^{\lambda_i}$, $s_i = 0, 1, \ldots, n - i - 1$, i = 1, 2, ..., n -3, $\lambda_i = \left\{ \begin{array}{c} 0 \text{ ó } 1 \text{ si } s_i = 0 \\ 1 \text{ si } s_i \neq 0 \end{array} \right\}$ y $\left(T^{(i)}\right)^0 = \left(g^{(i)}\right)^0 =$ $I_n\}$.Tomando en cuenta la estructura cíclica de la permutación $g^{(i)}$ y que $\alpha \leq n$. Entonces, por el lema II.2.1 tenemos que:

$$\alpha^{u_i} = \left\{ \begin{array}{c} \alpha \text{ if } \gamma_i = i \\ else \\ T^{(i)}(\alpha) + \gamma_i - i - 1 + (\lfloor (T^{(i)}(\alpha) + \gamma_i - i - 1)/(n+1) \rfloor)(i) \mod n \end{array} \right\}$$

Si i es par, entonces la estructura de U_i, i = 2, 4, . . . , n – 2, se deduce por el teorema II.2.1.
La prueba para n impar se obtiene de manera similar.

□.

3. CONCLUSIONES

En este trabajo se exponen tres algoritmos para la generación aleatoria de permutaciones, dos para el grupo Simétrico y uno para el grupo Alternado que parten de prefijar las bases {1, 2,..., n-1}, {n, n-1,..., 2} y {1, 2,..., n-2} respectivamente [8] y de seleccionar adecuadamente los transversales derechos, [2], [7], [9], [11] y [12], lo que hace que la generación aleatoria de las permutaciones se realice a través de sumas módulo n para el primer y tercer algoritmo y sumas mod i, i = n..2 para el segundo. Hacemos

notar que el segundo algoritmo para la generación aleatoria del grupo Simétrico puede ser utilizado en la generación aleatoria de permutaciones del grupo Alternado de igual manera que el primero.

RECEIVED MARCH, 2014
REVISED OCTOBER , 2014

REFERENCIAS

[1] AKL, S. G. (1987): Adaptive and optimal parallel algorithms for enumerating permutations and combinations. **The Computer Journal,** 30, 433-436.

[2] BAARNHIELM, H. (2004): The Schreier-Sims algorithm for matrix groups. http://matrixss.sourceforge.net. **Consulted** 28-10, 2004.

[3] COSNARD, M. and FERREIRA, A. G. (1989): Generating permutations on VLSI suitable linear network. **The Computer Journal,** 32, 571-573.

[4] GUPTA, P. and BHATTACHARJEE, P. (1983): Parallel generation of permutations. **The Computer Journal,** 26, 97-105.

[5] HUSSAIN, S. M. and AJLOUNI, N. M. (2006): Key based random permutation (KBRP). **Journal of Computer Science**. 2, 419-421.

[6] KNUTH, E. D. (1981): **The art of computer programming**. 2da. Ed. 2. Addison Wesley. Reading. Massachusetts.

[7] MURRAY, H. S. (2003): The Schreier - Sims algorithm. Australian National University. http://www.maths.usyd.edu.au/u/murray/research/essay.pdf. **Consulted** 07 -11, 2013.

[8] SEDGEWICK, R. (1977): Permutation generation methods. **Computing Survey**. 9, 137-164.

[9] SERESS, A. (2003): Permutation groups algorithm. http://assets.cambridge.org/052166/103X/. **Consulted** 06 -11, 2013.

[10] SKIENA, S. (1990**): Permutations. §1.1 in Implementing Discrete Mathematics**: **Combinatory and graph theory with mathematic**. Reading, MA: Addison-Wesley. :3-16.

[11] SIMS, C. C. (1998): Computational group theory. http://www.math.rutgers.edu/sims/publication/survey.pdf. **Consulted** 17-10, 2013.

[12] SIMS, C. C. (2003): Computational group theory, Computer Algebra Handbook. Springer. http://www.math.rutgers.edu/~sims/publications/. **Consulted** 17-10, 2013.