ALGORITMO PARA LA GENERACIÓN ALEATORIA DE MATRICES INVERTIBLES

P. Freyre*[1], N. Díaz* , E. R. Morgado**
*Facultad de Matemática y Computación, Universidad de La Habana, Cuba.
**Facultad de Matemática, Física y Computación, Universidad Central "Marta Abreu" de las Villas. Cuba.

RESUMEN
En el presente artículo se exponen cuatro algoritmos para matrices cuadradas nxn invertibles con sus elementos pertenecientes al campo primo Z_p. El primero permite la generación aleatoria de matrices, el segundo obtiene la inversa de una matriz seleccionada aleatoriamente por el algoritmo anterior. El tercero multiplica un vector fila por una matriz seleccionada aleatoriamente y el cuarto multiplica un vector fila por la matriz inversa de una matriz seleccionada aleatoriamente.

ABSTRACT
This work presents four new algorithms for square matrix of nxn defined in finite fields Z_p. The first one allows generate a random matrix, the second one calculates the inverse matrix of a randomly selected non-singular matrix by the previous algorithm; the third one multiplies a row vector by a randomly selected matrix and the fourth one multiplies a row vector by the inverse matrix of a randomly selected non-singular matrix.

MSC : 15A52

KEY WORDS: Vector – Random matrix products, Random matrix over finite fields.

1. INTRODUCCIÓN

El objetivo del presente trabajo es dar a conocer, programados en lenguaje Mathematica, cuatro nuevos algoritmos para matrices cuadradas nxn invertibles donde sus elementos pertenecen a un campo primo Z_p, ellos son:

1. Generación aleatoria de matrices.
2. Cálculo de la inversa de una matriz seleccionada aleatoriamente por el algoritmo anterior.
3. Multiplicación de un vector fila por una matriz seleccionada aleatoriamente.
4. Multiplicación de un vector fila por la matriz inversa de una matriz seleccionada aleatoriamente.

En Freyre P, Díaz N y Morgado E. R. (2009) se presentan en forma de pseudo código los cuatros algoritmos que se exponen en este trabajo para matrices cuadradas nxn con sus elementos pertenecientes a un campo finito arbitrario GF(q), q potencia de un primo p, bridándose además toda la fundamentación teórica y el análisis de la complejidad de los mismos. En Freyre P, Díaz N y Morgado E. R. (2010) se presentan programados, en

[1] For Contact: pfreyre@matcom.uh.cu

lenguaje Mathematica, para matrices booleanas el primero y los dos últimos de estos algoritmos.

Los algoritmos que se exponen en este trabajo para la multiplicación de un vector fila por una matriz seleccionada aleatoriamente y para la multiplicación de un vector fila por la matriz inversa de una seleccionada aleatoriamente mejoran en cuanto a complejidad a otros algoritmos conocidos (ver Knuth E. D. 1981 y Randal D. 1993).

En el trabajo se muestran 4 ejemplos de corrida de los programas. Los polinomios primitivos utilizados son tomados de Lidl R. y Niederreiter H. (1994).

2. GENERACIÓN ALEATORIA DE MATRICES.

En los programas tenemos que:

n – Es el tamaño de la matriz.

lpp – Es la lista de polinomios primitivos $g_i(x) \in Z_p[x]$, $i \in \{1\ldots n\}$, a utilizarse en el algoritmo, representados en forma descendente según su grado, y se calculan con anterioridad. Los mismos pueden ser seleccionados arbitrariamente.

vbc – Es un parámetro de entrada y no es más que la matriz $A=\{a_{i,j}\}_{nxn}$, donde $a_{i,j} \in Z_p$ y $i, j \in \{1\ldots n\}$, expresada en forma de filas comenzando por la n – ésima hasta la primera. Los componentes de la matriz A se seleccionan aleatoriamente y tienen como única restricción, que no exista $i \in \{1\ldots n\}$ tal que $a_{i,i} = a_{i,i+1} = \ldots a_{i,n} = 0$.

m – Es la matriz resultante.

v – Vector que se multiplica por la matriz.

vec – Vector resultante.

ALGORITMO PARA GENERAR DE FORMA ALEATORIA UNA MATRIZ BOOLEANA.

Programación del algoritmo.

```
Clear[Lbi]
Lbi[n_,i_,v_,vbc_,lpp_]:=
 Block[{x,t},
  x=lpp[[1]][Take[v,{1,i-1}]] +
    lpp[[1]][Take[vbc[[i]],{1,i-1}]]*lpp[[1]][Take[v,{i,i}]];
  If[TrueQ[x==0],x=lpp[[1]][PadLeft[{},n]]];
  t=lpp[[i]][Take[v,{i,n}]]*lpp[[i]][Take[vbc[[i]],{i,n}]];
  If[TrueQ[t==0],t=lpp[[i]][PadLeft[{},n+1-i]]];
  Return[Join[Take[x[[1]],{1,i-1}],t[[1]]]];
 ]
```

```
Clear[Genmatriz]
Genmatriz[n_,vbc_,lpp_]:=
  Block[{m={},v=IdentityMatrix[n],i,j,vec},
    For[j=1, j<=n,j++,
      i=j+1;vec=v[[j]];While[(i=i-1)>0,vec=Lbi[n,i,vec,vbc,lpp]];
      AppendTo[m,vec]
    ];
   Return[m];
 ]
```

ALGORITMO PARA LA MULTIPLICACIÓN DE UN VECTOR X POR UNA MATRIZ SELECCIONADA ALEATORIAMENTE.

Programación del algoritmo.

```
Clear[Lbi]
Lbi[n_,i_,v_,vbc_,lpp_]:=
  Block[{x,t},
    x=lpp[[1]][Take[v,{1,i-1}]] +
       lpp[[1]][Take[vbc[[i]],{1,i-1}]]*lpp[[1]][Take[v,{i,i}]];
    If[TrueQ[x==0],x=lpp[[1]][PadLeft[{},n]]];
    t=lpp[[i]][Take[v,{i,n}]]*lpp[[i]][Take[vbc[[i]],{i,n}]];
    If[TrueQ[t==0],t=lpp[[i]][PadLeft[{},n+1-i]]];
    Return[Join[Take[x[[1]],{1,i-1}],t[[1]]]];
    ]
Clear[Mulvec]
Mulvec[n_,v_,vbc_,lpp_]:=
  Block[{vec},
    vec=v;Do[vec=Lbi[n,n - i,vec,vbc,lpp],{i,0,n-1}];
    Return[vec];
    ]
```

ALGORITMO PARA LA MULTIPLICACIÓN DE UN VECTOR BINARIO X POR LA INVERSA DE UNA MATRIZ SELECCIONADA ALEATORIAMENTE.

Programación del algoritmo.

```
Clear[ILb]
ILb[n_,i_,v_,vbc_,lpp_]:=
  Block[{x,t},
    t=lpp[[i]][Take[v,{i,n}]]*(lpp[[i]][Take[vbc[[i]],{i,n}]]^-1);
```

```
    If[TrueQ[t==0],t=lpp[[i]][PadLeft[{},n+1-i]]];
    x=lpp[[1]][Take[v,{1,i-1}]] -
       lpp[[1]][Take[vbc[[i]],{1,i-1}]]*lpp[[1]][t[[1]][[{1}]]];
    If[TrueQ[x==0],x=lpp[[1]][PadLeft[{},n]]];
    Return[Join[Take[x[[1]],{1,i-1}],t[[1]]]];
    ]
 Clear[IMulvec]
IMulvec[n_,v_,vbc_,lpp_]:=
  Block[{i,vec},
    i=0;vec=v;While[(i=i+1)<n+1,vec=ILb[n,i,vec,vbc,lpp]];
    Return[vec];
    ]
```

Ejemplo 1. Dados los polinomios primitivos: $1 + x + x^6$; $1 + x^2 + x^5$; $1 + x + x^4$; $1 + x^2 + x^3$; $1 + x + x^2$; $1 + x$, y los vbc = {{1,0,0,0,0,0},{0,1,1,0,0,1},{0,0,0,1,0,1}, {0,1,0,0,1,0},{0,1,1,0,1,1},{1,0,1,0,1,1}} que han sido seleccionados aleatoriamente.

Generación de la matriz aleatoria.

```
<<Algebra`FiniteFields`
lpp = {GF[2, {1, 1, 0, 0, 0, 0, 1}], GF[2, {1, 0, 1, 0, 0, 1}], GF[2, {1, 1, 0, 0, 1}],
        GF[2, {1, 0, 1, 1}], GF[2, {1, 1, 1}], GF[2, {1, 1}]}
vbc = {{1,0,0,0,0,0},{0,1,1,0,0,1},{0,0,0,1,0,1},{0,1,0,0,1,0},{0,1,1,0,1,1},
         {1,0,1, 0,1,1}}
m = Genmatriz[6,vbc,lpp]
MatrixForm[%]
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Multiplicación de un vector por la matriz.

```
<<Algebra`FiniteFields`
x={0,1,1,0,1,1}
y=Mulvec[6,x,vbc,lpp]
IMulvec[6,y,vbc,lpp]
```

{0,1,1,0,1,1}
{1,0,1,0,0,0}
{0,1,1,0,1,1}

Multiplicación de un vector por la matriz inversa.

```
<<Algebra`FiniteFields`
x={0,1,1,0,1,1}
```

```
y=IMulvec[6,x,vbc,lpp]
Mulvec[6,y,vbc,lpp]
```

{0,1,1,0,1,1}
{0,0,1,1,1,0}
{0,1,1,0,1,1}

Ejemplo 2. Dados los polinomios primitivos: $2 + x^5 + x^6$; $1 + x^2 + x^4 + x^5$; $2 + x^3 + x^4$; $1 + 2x^2 + x^3$; $2 + x + x^2$; $1 + x$, y los vbc = {{2,0,0,2,1,1},{2,2,1,0,2,2},{0,2,1,1,0,1}, {0,1,2,2,0,2},{0,1,1,1,0,1},{2,1,1,1,1,2}} que han sido seleccionados aleatoriamente.

Generación de la matriz aleatoria.

```
<<Algebra`FiniteFields`
lpp = {GF[3, {2, 0, 0, 0, 0, 1, 1}], GF[3, {1, 0, 1, 0, 1, 1}], GF[3, {2, 0, 0, 1, 1}],
       GF[3, {1, 0, 2, 1}], GF[3, {2, 1, 1}],GF[3, {1, 1}]}
vbc = {{2,0,0,2,1,1},{2,2,1,0,2,2},{0,2,1,1,0,1},{0,1,2,2,0,2},{0,1,1,1,0,1},
       {2,1,1,1,1,2}}
m = Genmatriz[6,vbc,lpp]
MatrixForm[%]
```

$$\begin{pmatrix} 2 & 0 & 0 & 2 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 2 & 2 & 1 & 1 & 0 \\ 1 & 2 & 2 & 0 & 1 & 1 \\ 2 & 1 & 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 2 & 2 & 0 \end{pmatrix}$$

Multiplicación de un vector por la matriz.

```
<<Algebra`FiniteFields`
x={0,1,2,2,0,2}
y=Mulvec[6,x,vbc,lpp]
IMulvec[6,y,vbc,lpp]
```

{0,1,2,2,0,2}
{2,2,1,0,2,1}
{0,1,2,2,0,2}

Multiplicación de un vector por la matriz inversa.

```
<<Algebra`FiniteFields`
x={0,1,2,2,0,2}
y=IMulvec[6,x,vbc,lpp]
Mulvec[6,y,vbc,lpp]
```

{0,1,2,2,0,2}
{2,2,1,1,2,0}
{0,1,2,2,0,2}

Ejemplo 3. Dados los polinomios primitivos: $2 + x^5 + x^6$; $2 + x^2 + x^5$; $3 + x + x^3 + x^4$; $2 + x^2 + x^3$; $2 + x + x^2$; $2 + x$, y los vbc = {{1,2,0,0,4,4},{2,2,2,0,3,3},{4,1,2,3,1,1}, {1,2,3,4,1,0},{1,4,3,4,2,0},{2,1,3,0,3,1}} que han sido seleccionados aleatoriamente.

Generación de la matriz aleatoria.

```
<<Algebra`FiniteFields`
lpp = {GF[5, {2, 0, 0, 0, 0, 1, 1}], GF[5, {2, 0, 1, 0, 0, 1}], GF[5, {3, 1, 0, 1, 1}],
       GF[5, {2, 0, 1, 1}], GF[5, {2, 1, 1}],GF[5, {2, 1}]}
vbc = {{1,2,0,0,4,4},{2,2,2,0,3,3},{4,1,2,3,1,1},{1,2,3,4,1,0},{1,4,3,4,2,0},
       {2,1,3,0,3,1}}
m = Genmatriz[6,vbc,lpp]
MatrixForm[%]
```

$$\begin{pmatrix} 1 & 2 & 0 & 0 & 4 & 4 \\ 4 & 0 & 1 & 0 & 2 & 1 \\ 1 & 0 & 3 & 4 & 4 & 3 \\ 4 & 3 & 3 & 0 & 0 & 3 \\ 1 & 1 & 0 & 3 & 2 & 1 \\ 3 & 3 & 1 & 4 & 2 & 3 \end{pmatrix}$$

Multiplicación de un vector por la matriz.

```
<<Algebra`FiniteFields`
x={4,1,2,3,1,1}
y=Mulvec[6,x,vbc,lpp]
IMulvec[6,y,vbc,lpp]
```

{4,1,2,3,1,1}
{1,1,2,0,0,1}
{4,1,2,3,1,1}

Multiplicación de un vector por la matriz inversa.

```
<<Algebra`FiniteFields`
x={4,1,2,3,1,1}
y=IMulvec[6,x,vbc,lpp]
Mulvec[6,y,vbc,lpp]
```

{4,1,2,3,1,1}
{4,0,4,3,1,1}
{4,1,2,3,1,1}

Ejemplo 4. Dados los polinomios primitivos: $3 + x^4 + x^5 + x^6$; $4 + x^4 + x^5$; $3 + x^2 + x^3 + x^4$; $2 + x + x^2 + x^3$; $3 + x + x^2$; $2 + x$, y los vbc = {{2,6,6,6,1,2},{5,1,6,0,6,6}, {2,1,2,5,3,6},{3,4,3,4,5,4},{0,0,5,3,3,5},{5,4,5,0,0,4}} que han sido seleccionados aleatoriamente.

Generación de la matriz aleatoria.

```
<<Algebra`FiniteFields`
lpp = {GF[7, {3, 0, 0, 0, 1, 1, 1}], GF[7, {4, 0, 0, 0, 1, 1}], GF[7, {3, 0, 1, 1, 1}],
       GF[7, {2, 1, 1, 1}], GF[7, {3, 1, 1}], GF[7, {2, 1}]}
vbc = {{2,6,6,6,1,2},{5,1,6,0,6,6},{2,1,2,5,3,6},{3,4,3,4,5,4},{0,0,5,3,3,5},
       {5,4,5,0,0,4}}
m = Genmatriz[6,vbc,lpp]
MatrixForm[%]
```

$$\begin{pmatrix} 2 & 6 & 6 & 6 & 1 & 2 \\ 4 & 3 & 4 & 5 & 0 & 4 \\ 0 & 0 & 2 & 0 & 2 & 5 \\ 5 & 2 & 2 & 1 & 1 & 2 \\ 1 & 3 & 4 & 6 & 4 & 3 \\ 5 & 5 & 4 & 1 & 1 & 4 \end{pmatrix}$$

Multiplicación de un vector por la matriz.

```
<<Algebra`FiniteFields`
x={3,4,3,4,5,4}
y=Mulvec[6,x,vbc,lpp]
IMulvec[6,y,vbc,lpp]
```

{3,4,3,4,5,4}
{4,3,0,6,2,6}
{3,4,3,4,5,4}

Multiplicación de un vector por la matriz inversa.

```
<<Algebra`FiniteFields`
x={3,4,3,4,5,4}
y=IMulvec[6,x,vbc,lpp]
Mulvec[6,y,vbc,lpp]
```

{3,4,3,4,5,4}
{0,1,6,6,3,3}
{3,4,3,4,5,4}

BIBLIOGRAFÍA

FREYRE P., DÍAZ N. Y MORGADO E. R. **(**2009**):** Fast algorithm for the multiplication of a row vector by a randomly selected matrix A. Journal of Discrete Mathematical Sciences & Cryptography**,** 12, 533–549.

FREYRE P, DÍAZ N Y MORGADO E. R. (2010) "Algoritmo para la generación aleatoria de matrices booleanas invertibles". Revista Investigación Operacional**.** Universidad de la Habana. Vol. 31, No.3, 258-263..

KNUTH E. D. (1981). The Art of Computer Programming. Vol 2. Addison – Wesley. 2da ed. , N. York.

LIDL R. y NIEDERREITER H. (1994). Introduction to Finite Fields and their Applications. Cambridge University. New York.

RANDAL D. (1993). Efficient Generation of Random Nonsingular Matrices. (http://citeseer.ist.psu.edu).