Computational Finite Fields

المجالات المنتهية الحسابية

أ.د قحطان حمزة الزبيدي. أستاذ بقسم الرياضيات. كلية العلوم . جامعة بنغازي
د. نبيلة مختار بالنور. أستاذ مساعد بقسم الرياضيات. كلية العلوم . جامعة بنغازي.

Prof. Kahtan H. Alzubaidy. Professor in Department of Mathematics. Faculty of Science. University of Benghazi

Email: kahtanalzubaidy@yahoo.com.
Dr: Nabila M. balnoor. Assistant Professor, Department of Mathematics. College of Science . Benghazi University.
Email: n.benour@yahoo.com

الملخص: تصميم برامج بلغة الميبل لإجراء حسابات في المجالات النهائية. تعتمد الطريقة على استخدام متعددات الحدود و المصفوفات.

الكلمات الداله: متعددات الحدود، المصفوفات، المجالات النهائية.

Abstract: We have created certain procedures in Maple language to do computations in finite fields. The method is based on using polynomials and matrices.
Keywords: polynomials, matrices, final fields.

Theoretical Background

A finite field is a field has a finite number of elements.

Assume that E is a field extension of F. E is a vector space over F, the vectors are the elements of E, the scalars are the elements of F, the product of a scalar $a \in F$ and a vector $b \in E$ is $ab \in E$. The dimension of this vector space is called the degree of E over F.

Theorem 1 [2]
Any finite field is an extension of the field $\mathbb{Z}_p$ where p is prime.

Theorem 2 [2]

1) If F is a finite field, then $|F| = p^n$ where p is prime and n is a positive integer.

2) If p prime and n positive integer then there is a field of order p^n.

3) Any two finite fields of the same order are isomorphic.

A finite field of order p^n is denoted by $GF(p^n)$.

Representations of Finite Fields

I) Polynomials

Theorem 3 [1]

Let p be a prime number and n a positive integer. A finite field of order p^n is given as follows:G $F(p^n) = {}^{\mathbb{Z}_P[x]}/_{m\langle X \rangle}$

, where $m(x)$ is an irreducible polynomial of degree n in $\mathbb{Z}_P[x]$.

Elements of $GF(p^n)$ are of the form $a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 + I$, where $I = \langle m(x) \rangle$ is the maximal ideal generated by $m(x)$.

The general element can be written briefly as follows:

$a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0$. Modulo p and modulo $m(x)$.

Clearly addition multiplication and quotient of polynomials modulo p and modulo $m(x)$

II) Cyclic groups

Theorem 4 [2]
Let $G^* = GF(p^n) - \{0\}$. Then G^* is a cyclic group of order $p^n - 1$.

The finite field of order p^n induced by the irreducible polynomial $m(x)$ is denoted by $GF(p^n, m(x))$.
An irreducible polynomial $m(x)$ is primitive if x is a primitive element in $GF(p^n, m(x))$.

Theorem 5 [2]
$G^* = C_{p^n-1} < x >$ iff $m(x)$ is a primitive polynomial.

III) Matrices

An associative algebra over a field F is a ring R such that:

i) R is a vector space over F with respect to addition and scalar multiplication by elements of F,

ii) $a(rs) = (ar)s = r(as)$ for all $r, s \in R$ and $a \in F$.

$GF(p^n)$ is an associative algebra over the field $\mathbb{Z}_p$. Its basis is $\{1, x, \dots, x^{n-1}\}$.

$M_n(F)$, the set of all n −square matrices over the field F is also an associative algebra.

Theorem 6 [3]
Any associative algebra over a field F of dimension n is isomorphic to a subalgebra of $M_n(F)$.
To find the corresponding matrix of a polynomial $f(x)$ in $GF(p^n, m(x))$.
Take the polynomials $f(x), xf(x), \dots, x^{n-1}f(x)$ modulo $m(x)$ modulo p.
The required matrix is formed by taking the coefficients of these polynomials as columns

Computations [4]

```
> restart;
> with(PolynomialTools) :
> with(linalg) : with(LinearAlgebra) : with(ListTools) : with(combinat) :
```

I) Polynomial Representations

Cartesian Products
Cartesian product of two lists

```
> cp2:=proc(K,L)
> [seq(seq([x,y],y in L),x in K)];
> end proc;
                cp2 := proc(K, L) [seq(seq([x, y], in(y, L)), in(x, K))] end proc
> L4 := cp2([0, 1], [0, 1]);
                L4 := [[0, 0], [0, 1], [1, 0], [1, 1]]
> nops(%);
                4
> L9 := cp2([0, 1, 2], [0, 1, 2]);
                L9 := [[0, 0], [0, 1], [0, 2], [1, 0], [1, 1], [1, 2], [2, 0], [2, 1], [2, 2]]
> nops(%);
                9
```

Cartesian product of three lists

```
> cp3:=proc(K,L,M)
> local G;
> G:=cp2(cp2(K, L), M);
> [seq(Flatten(J), `in`(J, G))];
> end proc;
```

cp3 := **proc**(*K*, *L*, *M*)
local *G*;
G := *cp2*(*cp2*(*K*, *L*), *M*); [*seq*(*ListTools*:-*Flatten*(*J*), *in*(*J*, *G*))]
end proc

> *L8* := *cp3*([0, 1], [0, 1], [0, 1]);

L8 := [[0, 0, 0], [0, 0, 1], [0, 1, 0], [0, 1, 1], [1, 0, 0], [1, 0, 1], [1, 1, 0], [1, 1, 1]]

> *nops*(%);

8

> *L27* := *cp3*([0, 1, 2], [0, 1, 2], [0, 1, 2]);

L27 := [[0, 0, 0], [0, 0, 1], [0, 0, 2], [0, 1, 0], [0, 1, 1], [0, 1, 2], [0, 2, 0], [0, 2, 1], [0, 2, 2], [1, 0, 0], [1, 0, 1], [1, 0, 2], [1, 1, 0], [1, 1, 1], [1, 1, 2], [1, 2, 0], [1, 2, 1], [1, 2, 2], [2, 0, 0], [2, 0, 1], [2, 0, 2], [2, 1, 0], [2, 1, 1], [2, 1, 2], [2, 2, 0], [2, 2, 1], [2, 2, 2]]

> *nops*(%);

27

Cartesian product of four lists

```
> cp4:=proc(K,L,M,N)
> local G;
> G:=cp2(cp3(K, L, M),N);
> [seq(Flatten(J), `in`(J, G))];
> end proc;
```

cp4 := **proc**(*K*, *L*, *M*, *N*)
local *G*;
G := *cp2*(*cp3*(*K*, *L*, *M*), *N*); [*seq*(*ListTools*:-*Flatten*(*J*), *in*(*J*, *G*))]
end proc

> *L16* := *cp4*([0, 1], [0, 1], [0, 1], [0, 1]);

L16 := [[0, 0, 0, 0], [0, 0, 0, 1], [0, 0, 1, 0], [0, 0, 1, 1], [0, 1, 0, 0], [0, 1, 0, 1], [0, 1, 1, 0], [0, 1, 1, 1], [1, 0, 0, 0], [1, 0, 0, 1], [1, 0, 1, 0], [1, 0, 1, 1], [1, 1, 0, 0], [1, 1, 0, 1], [1, 1, 1, 0], [1, 1, 1, 1]]

> nops(%);

16

Cartesian product of five lists

```
> cp5:=proc(K,L,M,N,O)
> local G;
> G:=cp2(cp4(K, L,M,N), O);
> [seq(Flatten(J), `in`(J, G))];
> end proc;
```

```
cp5 := proc(K, L, M, N, O)
    local G;
    G := cp2(cp4(K, L, M, N), O); [seq(ListTools:-Flatten(J), in(J, G))]
end proc
```

> $L32 := cp5([0,1],[0,1],[0,1],[0,1],[0,1]);$

$L32 := [[0,0,0,0,0],[0,0,0,0,1],[0,0,0,1,0],[0,0,0,1,1],[0,0,1,0,0],[0,0,1,0,1],[0,0,1,1,0],[0,0,1,1,1],[0,1,0,0,0],[0,1,0,0,1],[0,1,0,1,0],[0,1,0,1,1],[0,1,1,0,0],[0,1,1,0,1],[0,1,1,1,0],[0,1,1,1,1],[1,0,0,0,0],[1,0,0,0,1],[1,0,0,1,0],[1,0,0,1,1],[1,0,1,0,0],[1,0,1,0,1],[1,0,1,1,0],[1,0,1,1,1],[1,1,0,0,0],[1,1,0,0,1],[1,1,0,1,0],[1,1,0,1,1],[1,1,1,0,0],[1,1,1,0,1],[1,1,1,1,0],[1,1,1,1,1]]$

> $nops(\%);$

$$32$$

Listing of the field elements

> $\mathbf{GF}(2^2) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L4})], x);$

$$GF(4) := [0, 1, x, 1+x]$$

> $\mathbf{GF}(2^3) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L8})], \mathrm{x});$

$$GF(8) := [0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2]$$

> $\mathbf{GF}(2^4) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L16})], \mathrm{x});$

$$GF(16) := [0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2, x^3, 1+x^3, x+x^3, x^2+x^3, 1+x+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3]$$

> $\mathbf{GF}(3^2) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L9})], \mathrm{x});$

$$GF(9) := [0, 1, 2, x, 2x, 1+x, 2+x, 2+2x, 1+2x]$$

> $\mathbf{GF}(3^3) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L27})], \mathrm{x});$

$$GF(27) := [0, 1, 2, x, 2x, 1+x, 2+x, 2+2x, 1+2x, x^2, 2x^2, 2+x^2, 1+x^2, 2x+x^2, x+x^2, 2+2x^2, 1+2x^2, 2x+2x^2, x+2x^2, 2+2x+x^2, 2+x+x^2, 1+2x+x^2, 1+x+x^2, 2+2x+2x^2, 2+x+2x^2, 1+2x+2x^2, 1+x+2x^2]$$

> $\mathbf{GF}(2^5) := Sort([seq(FromCoefficientList(J,x), \mathrm{J}\ \mathbf{in}\ \mathrm{L32})], \mathrm{x});$

$$GF(32) := [0, 1, x, 1+x, x^2, 1+x^2, x+x^2, 1+x+x^2, x^3, 1+x^3, x+x^3, x^2+x^3, 1+x+x^3, 1+x^2+x^3, x+x^2+x^3, 1+x+x^2+x^3, x^4, 1+x^4, x+x^4, x^2+x^4, x^3+x^4, 1+x+x^4, 1+x^2+x^4, x+x^2+x^4, 1+x^3+x^4, x+x^3+x^4, x^2+x^3+x^4, 1+x+x^2+x^4, 1+x+x^3+x^4, 1+x^2+x^3+x^4, x+x^2+x^3+x^4, 1+x+x^2+x^3+x^4]$$

Field Operations

Algebraic operations can be performed by using maple command modpol.

> $modpol\left(\frac{x}{1+x}, x^2+x+1, x, 2\right);$

$$1+x$$

> $modpol\left((x+1)^{-1}, x^3+x+1, x, 2\right);$

$$x+x^2$$

> $modpol\left((x+1)\cdot(x^2+x), x^3+x^2+1, x, 2\right);$

$$1+x+x^2$$

Inverse element

```
> inv:=proc(f,g,x,p);
> modpol(1/f ,g,x,p);
> end proc;
```

$$inv := \textbf{proc}(f, g, x, p)\ \ modpol(1/f, g, x, p)\ \ \textbf{end proc}$$

> $inv\left(x, x^2+x+1, x, 2\right);$

$$1+x$$

II) Cyclic Representation

Cyclic representation of $GF(p^n)$ induced by a primitive polynomial of degree n over $\mathbb{Z}_p$.

Cyclic Representation of $GF(p^n)$ induced by q.

Cyclic elements

```
> G:=proc(p,n);
> [0,[seq(x^r, r = 0 .. p^n-2)][]];
> end proc;
```

$$G := \textbf{proc}(p, n)\ \ [0, [seq(x\verb|^|r, r=0\,..p\verb|^|n-2)][\,]]\ \ \textbf{end proc}$$

> $p := 2;$

$$p := 2$$

> $n := 3;$

$$n := 3$$

> $q := x^3+x+1;$

$$q := 1+x+x^3$$

> $Irreduc(q)$ **mod** $2;$

$$true$$

> $Primitive(q)$ **mod** $2;$

$$true$$

> $G(p, n);$

$$[0, 1, x, x^2, x^3, x^4, x^5, x^6]$$

Corresponding field elements

```
> F:=proc(p,n,q,x);
> [seq(modpol(G(p,n)[t], q, x, p), t = 1 .. p^n)];
> end proc;
```

$$F := \textbf{proc}(p, n, q, x)\ \ [seq(modpol(G(p, n)[t], q, x, p), t=1\,..p\verb|^|n)]\ \ \textbf{end proc}$$

> $F(p, n, q, x);$

$$[0, 1, x, x^2, 1+x, x+x^2, 1+x+x^2, 1+x^2]$$

Sum of cyclic elements

```
> su:=proc(A,B)local t;
> t := Search(modpol(A+B, q, x, p), F(p,n,q,x));
> if t=1 then 0 else x^(t-2) end if;
> end proc;
```

$su := \textbf{proc}(A, B)$
  local t;
  $t := ListTools:\text{-}Search(modpol(A + B, q, x, p), F(p, n, q, x))$;
  if $t = 1$ **then** 0 **else** $x\hat{}(t - 2)$ **end if**
end proc

> $su(x^2, x^5, \mathrm{n}, q, x, p)$;

$$x^3$$

Product of cyclic elements

```
> pr:=proc(A,B)local m;
> m := Search(modpol(A*B, q, x, p), F(p,n,q,x));
> if m=1 then 0 else x^(m-2) end if;
> end proc;
```

$pr := \textbf{proc}(A, B)$
  local m;
  $m := ListTools:\text{-}Search(modpol(A * B, q, x, p), F(p, n, q, x))$;
  if $m = 1$ **then** 0 **else** $x\hat{}(m - 2)$ **end if**
end proc

> $pr(x^4, x^5, n, q, x, p)$;

$$x^2$$

```
> CP:=proc(A,B)
> local M,P,CP;
> M := Matrix(nops(A),nops(B), proc (i, j) options operator, arrow; [A[i], B[j]] end proc);
> [seq(seq(M(i, j), i = 1 .. nops(A)), j = 1 .. nops(B))];
> end proc;
```

$CP := \textbf{proc}(A, B)$
  local M, P, CP;
  $M := Matrix(nops(A), nops(B), (i, j) \rightarrow [A[i], B[j]])$;
  $[seq(seq(M(i, j), i = 1 ..nops(A)), j = 1 ..nops(B))]$
end proc

Table of $C \times R$ of a binary operation f.
Sum Table

```
> ST:=proc(C,R,f)
```

```
> local m,n,M,RR,CC,U;
> n:=nops(R);m:=nops(C);M := Matrix(m,n, (x,y)->f(C[x],R[y]));
> RR := Matrix(1, n, [R]);
> CC:=Matrix(m,1,[seq([x],x=C)]);
> U := [sum];
> blockmatrix(2, 2, [U, RR, CC, M, U, CC, RR, M]);
> end proc;
```

$$
\begin{aligned}
&ST := \mathbf{proc}(C, R, f)\\
&\quad \mathbf{local}\ m, n, M, RR, CC, U;\\
&\quad n := nops(R);\\
&\quad m := nops(C);\\
&\quad M := Matrix(m, n, (x, y) \rightarrow f(C[x], R[y]));\\
&\quad RR := Matrix(1, n, [R]);\\
&\quad CC := Matrix(m, 1, [seq([x], x = C)]);\\
&\quad U := [sum];\\
&\quad linalg\text{:-}blockmatrix(2, 2, [U, RR, CC, M, U, CC, RR, M])\\
&\mathbf{end\ proc}
\end{aligned}
$$

$> f := (a, b) \rightarrow su(a, b);$

$$f := (a, b) \rightarrow su(a, b)$$

$> ST(G(p, n), G(p, n), f);$

$$
\begin{bmatrix}
sum & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6\\
0 & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6\\
1 & 1 & 0 & x^3 & x^6 & x & x^5 & x^4 & x^2\\
x & x & x^3 & 0 & x^4 & 1 & x^2 & x^6 & x^5\\
x^2 & x^2 & x^6 & x^4 & 0 & x^5 & x & x^3 & 1\\
x^3 & x^3 & x & 1 & x^5 & 0 & x^6 & x^2 & x^4\\
x^4 & x^4 & x^5 & x^2 & x & x^6 & 0 & 1 & x^3\\
x^5 & x^5 & x^4 & x^6 & x^3 & x^2 & 1 & 0 & x\\
x^6 & x^6 & x^2 & x^5 & 1 & x^4 & x^3 & x & 0
\end{bmatrix}
$$

Product Table

```
> PT:=proc(C,R,f)
> local m,n,M,RR,CC,U;
> n:=nops(R);m:=nops(C);M := Matrix(m,n, (x,y)->f(C[x],R[y]));
> RR := Matrix(1, n, [R]);
> CC:=Matrix(m,1,[seq([x],x=C)]);
> U := [pro];
> blockmatrix(2, 2, [U, RR, CC, M, U, CC, RR, M]);
> end proc;
```

$PT := \mathbf{proc}(C, R, f)$

$\quad \mathbf{local}\ m, n, M, RR, CC, U;$

$\quad n := nops(R);$

$\quad m := nops(C);$

$\quad M := Matrix(m, n, (x, y) \rightarrow f(C[x], R[y]));$

$\quad RR := Matrix(1, n, [R]);$

$\quad CC := Matrix(m, 1, [seq([x], x = C)]);$

$\quad U := [pro];$

$\quad linalg\text{:-}blockmatrix(2, 2, [U, RR, CC, M, U, CC, RR, M])$

$\mathbf{end\ proc}$

> $g := (c, d) \rightarrow pr(c, d);$

$$g := (c, d) \rightarrow pr(c, d)$$

> $PT(G(p, n), G(p, n), g);$

$$\begin{bmatrix} pro & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 \\ x & 0 & x & x^2 & x^3 & x^4 & x^5 & x^6 & 1 \\ x^2 & 0 & x^2 & x^3 & x^4 & x^5 & x^6 & 1 & x \\ x^3 & 0 & x^3 & x^4 & x^5 & x^6 & 1 & x & x^2 \\ x^4 & 0 & x^4 & x^5 & x^6 & 1 & x & x^2 & x^3 \\ x^5 & 0 & x^5 & x^6 & 1 & x & x^2 & x^3 & x^4 \\ x^6 & 0 & x^6 & 1 & x & x^2 & x^3 & x^4 & x^5 \end{bmatrix}$$

Inverse Table

```
> IT:=proc(n,a)
>  local L,H;
>  L:=[seq(a^i, i =0..n-1)];
>  H:=algsubs(a^(n)=1,[seq(a^(n-i),i=0..n-1)]);
>  Matrix(2,n,[L,H]);
> end proc;
```

$IT := \mathbf{proc}(n, a)$

$\quad \mathbf{local}\ L, H;$

$\quad L := [seq(a\text{^}i, i = 0..n-1)];$

$\quad H := algsubs(a\text{^}n = 1, [seq(a\text{^}(n-i), i = 0..n-1)]);$

$\quad Matrix(2, n, [L, H])$

$\mathbf{end\ proc}$

> $IT(8, x);$

$$\begin{bmatrix} 1 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 \\ 1 & x^7 & x^6 & x^5 & x^4 & x^3 & x^2 & x \end{bmatrix}$$

III) Matrix Representations

Standard polynomial form

```
> st:=proc(f,q);
> sort(rem(f,q,x),x,ascending);end proc;
```

$$st := \textbf{proc}(f, q)\ \ sort(rem(f, q, x), x, ascending)\ \ \textbf{end proc}$$

Matrix representation of $a + bx$ in $GF(2^2)$ induced by the polynomial q.

```
> mr22:=proc(a,b,x,q) local KK1,KK2;
> KK1 := [coeffs(st(a+b*x, q), x)];
> KK2 := [coeffs(st(x*(a+b*x), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2]))mod 2;
> end proc;
```

```
mr22 := proc(a, b, x, q)
    local KK1, KK2;
    KK1 := [coeffs(st(a + b*x, q), x)];
    KK2 := [coeffs(st(x*(a + b*x), q), x)];
    mod(LinearAlgebra[ListTools:-Transpose](Matrix([KK1, KK2])), 2)
end proc
```

$> Irreduc(x^2 + x + 1) \textbf{ mod } 2;$

$$true$$

$> mr22(a, b, x, x^2 + x + 1);$

$$\begin{bmatrix} a & b \\ b & a+b \end{bmatrix}$$

Matrix representation of $a + bx + cx^2$ in $GF(2^3)$ induced by the polynomial q.

```
> mr23:=proc(a,b,c,x,q) local KK1,KK2,KK3;
> KK1:=[coeffs(st(a+b*x+c*x^2, q), x)];
> KK2 := [coeffs(st(x*(a+b*x+c*x^2), q), x)];
> KK3 := [coeffs(st(x^2*(a+b*x+c*x^2), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2,KK3]))mod 2;
> end proc;
```

```
mr23 := proc(a, b, c, x, q)
    local KK1, KK2, KK3;
    KK1 := [coeffs(st(a + b*x + c*x^2, q), x)];
    KK2 := [coeffs(st(x*(a + b*x + c*x^2), q), x)];
    KK3 := [coeffs(st(x^2*(a + b*x + c*x^2), q), x)];
    mod(LinearAlgebra[ListTools:-Transpose](Matrix([KK1, KK2, KK3])), 2)
end proc
```

$> Irreduc(x^3 + x + 1) \textbf{ mod } 2;$

$$true$$

> $mr23(a,b,c,x,x^3+x+1);$

$$\begin{bmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{bmatrix}$$

> $Irreduc(x^3+x^2+1)$ **mod** 2;

true

> $mr23(a,b,c,x,x^3+x^2+1);$

$$\begin{bmatrix} a & c & b+c \\ b & a & c \\ c & b+c & a+b+c \end{bmatrix}$$

Matrix representation of $a+bx+cx^2+dx^3$ in $GF(2^4)$ induced by the polynomial q.

```
> mr24:=proc(a,b,c,d,x,q) local KK1,KK2,KK3,KK4;
> KK1:=[coeffs(st(a+b*x+c*x^2+d*x^3, q), x)];
> KK2 := [coeffs(st(x*(a+b*x+c*x^2+d*x^3), q), x)];
> KK3 := [coeffs(st(x^2*(a+b*x+c*x^2+d*x^3), q), x)];KK4 :=
[coeffs(st(x^3*(a+b*x+c*x^2+d*x^3), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2,KK3,KK4]))mod 2;
> end proc;
```

```
mr24 := proc(a, b, c, d, x, q)
    local KK1, KK2, KK3, KK4;
    KK1 := [coeffs(st(a + b*x + c*x^2 + d*x^3, q), x)];
    KK2 := [coeffs(st(x*(a + b*x + c*x^2 + d*x^3), q), x)];
    KK3 := [coeffs(st(x^2*(a + b*x + c*x^2 + d*x^3), q), x)];
    KK4 := [coeffs(st(x^3*(a + b*x + c*x^2 + d*x^3), q), x)];
    mod(LinearAlgebra[ListTools:-Transpose](Matrix([KK1, KK2, KK3, KK4])), 2)
end proc
```

> $Irreduc(x^4+x+1)$ **mod** 2;

true

> $mr24(a,b,c,d,x,x^4+x+1);$

$$\begin{bmatrix} a & d & c & b \\ b & a+d & c+d & b+c \\ c & b & a+d & c+d \\ d & c & b & a+d \end{bmatrix}$$

Matrix representation of $a+bx+cx^2+dx^3+ex^4$ in $GF(2^5)$ induced by the polynomial q.

```
> mr25:=proc(a,b,c,d,e,x,q) local KK1,KK2,KK3,KK4,KK5;
> KK1:=[coeffs(st(a+b*x+c*x^2+d*x^3+e*x^4, q), x)];
> KK2 := [coeffs(st(x*(a+b*x+c*x^2+d*x^3+e*x^4), q), x)];
> KK3 := [coeffs(st(x^2*(a+b*x+c*x^2+d*x^3+e*x^4), q), x)];KK4 :=
[coeffs(st(x^3*(a+b*x+c*x^2+d*x^3+e*x^4), q), x)];KK5 :=
[coeffs(st(x^4*(a+b*x+c*x^2+d*x^3+e*x^4), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2,KK3,KK4,KK5]))mod 2;
```

```
> end proc;
```

$mr25 := \textbf{proc}(a, b, c, d, e, x, q)$
$\textbf{local}\ KK1, KK2, KK3, KK4, KK5;$
$KK1 := [coeffs(st(a + b*x + c*x\char`^2 + d*x\char`^3 + e*x\char`^4, q), x)];$
$KK2 := [coeffs(st(x*(a + b*x + c*x\char`^2 + d*x\char`^3 + e*x\char`^4), q), x)];$
$KK3 := [coeffs(st(x\char`^2*(a + b*x + c*x\char`^2 + d*x\char`^3 + e*x\char`^4), q), x)];$
$KK4 := [coeffs(st(x\char`^3*(a + b*x + c*x\char`^2 + d*x\char`^3 + e*x\char`^4), q), x)];$
$KK5 := [coeffs(st(x\char`^4*(a + b*x + c*x\char`^2 + d*x\char`^3 + e*x\char`^4), q), x)];$
$mod(LinearAlgebra[ListTools:\text{-}Transpose](Matrix([KK1, KK2, KK3, KK4, KK5])), 2)$
$\textbf{end proc}$

> $Irreduc(x^5 + x^2 + 1)\ \textbf{mod}\ 2;$

$$true$$

> $mr25(a, b, c, d, e, x, x^5 + x^2 + 1);$

$$\begin{bmatrix} a & e & d & c & b+e \\ b & a & e & d & c \\ c & b+e & a+d & c+e & d+b+e \\ d & c & b+e & a+d & c+e \\ e & d & c & b+e & a+d \end{bmatrix}$$

Matrix representation of $a + bx$ in $GF(3^2)$ induced by the polynomial q.

```
> mr32:=proc(a,b,x,q) local KK1,KK2;
>
> KK1 := [coeffs(st(a+b*x, q), x)];
> KK2 := [coeffs(st(x*(a+b*x), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2]))mod 3;
> end proc;
```

$mr32 := \textbf{proc}(a, b, x, q)$
$\textbf{local}\ KK1, KK2;$
$KK1 := [coeffs(st(a + b*x, q), x)];$
$KK2 := [coeffs(st(x*(a + b*x), q), x)];$
$mod(LinearAlgebra[ListTools:\text{-}Transpose](Matrix([KK1, KK2])), 3)$
$\textbf{end proc}$

> $Irreduc(x^2 + 1)\ \textbf{mod}\ 3$

$$true$$

> $mr32(a, b, x, x^2 + 1);$

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$$

Matrix representation of $a + bx + cx^2$ in $GF(3^3)$ induced by the polynomial q.

```
> mr33:=proc(a,b,c,x,q) local KK1,KK2,KK3;
> KK1:=[coeffs(st(a+b*x+c*x^2, q), x)];
> KK2 := [coeffs(st(x*(a+b*x+c*x^2), q), x)];
```

```
> KK3 := [coeffs(st(x^2*(a+b*x+c*x^2), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2,KK3]))mod 3;
> end proc;
```

$mr33 := \mathbf{proc}(a, b, c, x, q)$
local $KK1, KK2, KK3;$
$KK1 := [coeffs(st(a + b*x + c*x^\wedge 2, q), x)];$
$KK2 := [coeffs(st(x*(a + b*x + c*x^\wedge 2), q), x)];$
$KK3 := [coeffs(st(x^\wedge 2*(a + b*x + c*x^\wedge 2), q), x)];$
$mod(LinearAlgebra[ListTools{:}\text{-}Transpose](Matrix([KK1, KK2, KK3])), 3)$
end proc

> $Irreduc(x^3 + 2\cdot x + 2)$ **mod** 3;

$$true$$

> $mr33(a, b, c, x, x^3 + 2\cdot x + 2);$

$$\begin{bmatrix} a & c & b \\ b & a+c & b+c \\ c & b & a+c \end{bmatrix}$$

Matrix representation of $a + bx + cx^2 + dx^3$ in $GF(3^4)$ induced by the polynomial q.

```
> mr34:=proc(a,b,c,d,x,q) local KK1,KK2,KK3,KK4;
> KK1:=[coeffs(st(a+b*x+c*x^2+d*x^3, q), x)];
> KK2 := [coeffs(st(x*(a+b*x+c*x^2+d*x^3), q), x)];
> KK3 := [coeffs(st(x^2*(a+b*x+c*x^2+d*x^3), q), x)];KK4 :=
[coeffs(st(x^3*(a+b*x+c*x^2+d*x^3), q), x)];
> LinearAlgebra[Transpose](Matrix([KK1, KK2,KK3,KK4]))mod 3;
> end proc;
```

$mr34 := \mathbf{proc}(a, b, c, d, x, q)$
local $KK1, KK2, KK3, KK4;$
$KK1 := [coeffs(st(a + b*x + c*x^\wedge 2 + d*x^\wedge 3, q), x)];$
$KK2 := [coeffs(st(x*(a + b*x + c*x^\wedge 2 + d*x^\wedge 3), q), x)];$
$KK3 := [coeffs(st(x^\wedge 2*(a + b*x + c*x^\wedge 2 + d*x^\wedge 3), q), x)];$
$KK4 := [coeffs(st(x^\wedge 3*(a + b*x + c*x^\wedge 2 + d*x^\wedge 3), q), x)];$
$mod(LinearAlgebra[ListTools{:}\text{-}Transpose](Matrix([KK1, KK2, KK3, KK4])), 3)$
end proc

> $Irreduc(x^4 + x^3 + x^2 + x + 1)$ **mod** 3;

$$true$$

> $mr34(a, b, c, d, x, x^4 + x^3 + x^2 + x + 1);$

$$\begin{bmatrix} a & 2d & 2c+d & 2b+c \\ b & a+2d & 2c & d+2b \\ c & b+2d & a+2c & 2b \\ d & c+2d & b+2c & a+2b \end{bmatrix}$$

References

1) David S. Dummit, Richard M. Foote , Abstract Algebra ,$(2^{nd} ed)$, Prrentice Hall, USA, 1999,
2) Garrett Birkhoff & Thomas C. Bartee, Modern Applied Algebra, McGraw-Hill Book Company, 1970.
3) Nathan Jacobson, Basic Algebra I ,$(2^{nd} ed)$ FREEMAN, New York, 1985.
4) Maple User Manual, Version 15.01, 2011