1 `restart;maple_mode(1);cas_setup(0,0,0,1,0,1e-10,10,[1,50,0,25],0,0,0); #radians,pas de cmplx, pas de  Sqrt`

// Warning: some commands like subs might change arguments order

2 `Factor(x^23-1) mod 2;`

$$(1\cdot x+1)\cdot(1\cdot x^{11}+1\cdot x^{10}+1\cdot x^{6}+1\cdot x^{5}+1\cdot x^{4}+1\cdot x^{2}+1)\cdot(1\cdot x^{11}+1\cdot x^{9}+1\cdot x^{7}+1\cdot x^{6}+1\cdot x^{5}+1\cdot x+1$$

3 Astuce: pour recuperer directement le second facteur, on utilise factors, mais
il en faut la forme inerte pour travailler sur Z/2Z, d'ou les guillemets

4 `'factors(x^23-1)' mod 2)`

$$\left[\begin{array}{cc} 1 & \left[\begin{array}{cc} 1\cdot x+1 & 1 \\ 1\cdot x^{11}+1\cdot x^{10}+1\cdot x^{6}+1\cdot x^{5}+1\cdot x^{4}+1\cdot x^{2}+1 & 1 \\ 1\cdot x^{11}+1\cdot x^{9}+1\cdot x^{7}+1\cdot x^{6}+1\cdot x^{5}+1\cdot x+1 & 1 \end{array}\right] \end{array}\right]$$

5 `g:=('factors(x^23-1)' mod 2)[2][2,1];`

$$1\cdot x^{11}+1\cdot x^{10}+1\cdot x^{6}+1\cdot x^{5}+1\cdot x^{4}+1\cdot x^{2}+1$$

6 On ne peut pas creer F2[x]/g avec GF car les racines de g ne sont pas
primitives dans (F_2^11) puisqu'elles sont d'ordre 23, et la commande GF veut
un polynome irreductible dont les racines engendre le groupe multiplicatif du
corps voulu.

7 `FF:=GF(2,11,['a','FF']);`

$$\mathrm{GF}(2,a^{11}+a^{9}+1,[a \quad FF],\mathrm{undef})$$

8 `factor(g,FF(a));`

Evaluation time: 0.65625

$$(x+FF(a^{4}+a^{2}+a+1))\cdot(x+FF(a^{6}+a^{5}+a^{2}+a+1))\cdot(x+FF(a^{8}+a^{4}+a^{2}+1))\cdot(x+FF(a^{8}+a^{7}+a^{6}+a^{5}+a^{3}+a+1))\cdot$$
$$(x+FF(a^{10}+a^{9}+a^{5}+a^{4}+a+1))\cdot(x+FF(a^{10}+a^{9}+a^{5}+a^{4}+a^{3}+a+1))\cdot(x+FF(a^{10}+a^{9}+a^{8}+a^{2}+1))\cdot(x+FF(a^{10}$$

9 On note t la premiere racine de g trouvee dans F2048

10 `t:=subs(x=0,factors(factor(g,FF(a)))[2][1,1]);`

Evaluation time: 1.29688

$$0+FF(a^{4}+a^{2}+a+1)$$

11 On va maintenant comparer les racines de g avec les puissances de l'une d'entre
elles: t. On va illustrer que ce sont les t^i ou i est un carre modulo
23. On cree la liste des carres avec la fonction ensembles pour simplifier les
doublons.

12 `carres:={seq(i^2 mod 23 ,i=1..22)};`

$$[1 \quad 4 \quad 9 \quad 16 \quad 2 \quad 13 \quad 3 \quad 18 \quad 12 \quad 8 \quad 6]$$

13 `P:=1;for i in carres do P:=P*(x-t^i) od;`

$$(FF(a^{4}+a^{2}+a+1)+x)\cdot(FF(a^{10}+a^{8}+a^{5}+a^{4}+a^{3}+a+1)+x)\cdot$$
$$(FF(a^{10}+a^{9}+a^{8}+a^{2}+1)+x)\cdot(FF(a^{10}+a^{9}+a^{5}+a^{4}+a+1)+x)\cdot(FF(a^{8}+a^{4}+a^{2}+1)+x)\cdot$$
$$(FF(a^{10}+a^{9}+a^{8}+a^{6}+a^{2}+1)+x)\cdot(FF(a^{9}+a^{5}+a^{4}+a^{3}+1)+x)\cdot$$
$$(FF(a^{10}+a^{9}+a^{5}+a^{4}+a^{3}+a+1)+x)\cdot(FF(a^{6}+a^{5}+a^{2}+a+1)+x)\cdot$$
$$(1,\ (FF(a^{10}+a^{9}+a^{8}+a^{7}+a^{6}+a^{2}+1)+x)\cdot(FF(a^{8}+a^{7}+a^{6}+a^{5}+a^{3}+a+1)+x)\ )$$

14 `normal(P);#On retrouve bien g`

$$x^{11}+x^{10}+x^{6}+x^{5}+x^{4}+x^{2}+FF(1)$$

15 `g;`

$$x^{11}+x^{10}+x^{6}+x^{5}+x^{4}+x^{2}+1$$

16 G23 a 2^{23-deg(g)} elements. Le cardinal d'une boule de rayon 3 est la somme
de C_23^i pour i allant de 0 'a 3. L'annnulation du terme suivant signifie que
G23 a les invriants numeriques d'un code binaire 3 correcteur parfait de
dimension 12 dans un espace vectoriel de dimension 23.

17 `normal(2^23-add(seq(binomial(23,i),i=0..3))*2^12);`

$$0$$

18 il y a 4 entiers consecutifs donc la distance est au moins 5

19 sort(op(carres));

(1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18)

Menu

20 G:=matrix(12,23,(i,j)->(coeff(Rem(x^(i-1)*g,x^23-1,x) mod 2,x,j-1)));

// Warning: g x declared as global variable(s)

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

Menu

21 GE:=augment(G,transpose(G*[1$23]) mod 2); #le code etendu

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

Menu

22 VE:=Nullspace(GE) mod 2;

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

23 Pour montrer que les espaces vectoriels engendr'es par les lignes de GE et
celles de VE sont les memes, on cree la matrice M suivante et l'on doit montrer
qu'elle est de rang 12. On ne dispose pas d'une instruction de rang modulaire,
on utilise donc Nullspace mod 2

24 M:=[op(GE),op(VE)];

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

25 dim(Nullspace(M) mod 2);#c'est bien de rang 12

$$[12 \quad 24]$$

26 puisque le code etendu est egal a son dual, on a:
m.m'=0[2], et donc (m+m').(m+m')=m.m+m'.m' [4]
Donc si les poids de m et m' sont multiples de 4, celui de m+m' aussi
On en deduit que le code etendu a une distance multiple de 4, et comme elle
vaut au moins 5, et qu'il y a des mots de poids 8, c'est 8. Donc celle de G23
est 7 ou 8, et comme il y a des lignes de poids 7 dans G cette distance vaut 7

27

undef

28 ---

29

30
```
MU:=proc(U,n)
local PU;
PU:=[seq(coeff(convert(series(U,x=0,2*n),polynom),x,i),i=0..2*n+1)];
matrix(n+1,n+1,(i,j)->PU[i+j-1]);
end;
```
// Warning: PU declared as global variable(s)
// Warning: i x j declared as global variable(s)
// End defining MU

```
proc(U,n)
  local PU;
  PU:=[seq(coeff(convert(series(U,x=0,2*n),polynom),x,i),i=(0 .. (2*n+1)))];
  matrix(n+1,n+1, (i,j)->PU[i+j-1]);

end;
```
Menu

31
```
scalU:=proc(p,q,n)
local PU;
([seq(coeff(p,x,i),i=0..n)]*MU(U,n)*transpose([seq(coeff(q,x,i),i=0..n)]))[1];
end;
```
// Warning: MU U i x declared as global variable(s)
// End defining scalU

```
proc(p,q,n)
  local PU;
  ([seq(coeff(p,x,i),i=(0 .. n))]*MU(U,n)*transpose(seq(coeff(q,x,i),i=(0 .. n))))[1];

end;
```
Menu

32
```
purge(u):U:=add(u[i]*x^i,i=0..6);
```
$$(\text{Done},\ u[0]+(u[1])\cdot x+(u[2])\cdot x^2+(u[3])\cdot x^3+(u[4])\cdot x^4+(u[5])\cdot x^5+(u[6])\cdot x^6)$$
Menu

33
```
scalU(1,x,3);scalU(x^2,x^2,3);
```
$$(u[1],\ u[4])$$
Menu

34
```
U:=1/(x+1/(x^2+1/(x^3+x+1+1/(x+2+1/x))));
```
$$\cfrac{1}{x+\cfrac{1}{x^2+\cfrac{1}{x^3+x+1+\cfrac{1}{x+2+\frac{1}{x}}}}}$$
Menu

35
```
factor(gramschmidt([1,x,x^2,x^3,x^4],(p,q)->scalU(p,q,4)));
```
// Success
$$[1\quad \sqrt{3}\cdot(x+3)\quad \sqrt{3}\cdot(x^2+3\cdot x-3)\quad \sqrt{273}\cdot(-3\cdot x^3-20\cdot x^2-21\cdot x+42)\quad \sqrt{32214}\cdot(-273\cdot x^4-1194\cdot$$
Menu

36
```
S:=[seq(pade(U,x,2*i-1,i),i=1..4)]
```
$$\left[\frac{1}{3\cdot x+1}\quad \frac{1}{-3\cdot x^2-(-3)\cdot x+1}\quad \frac{3\cdot x^2+(-11)\cdot x-3}{42\cdot x^3+(-21)\cdot x^2+(-20)\cdot x-3}\quad \frac{626\cdot x^3+192\cdot x^2+375\cdot x+273}{483\cdot x^4+77\cdot x^3+498\cdot x^2+1194\cdot x+27} \right]$$
Menu

37 On constate bien que les denominateurs des approximants de pade coincident a facteur
pres avec les polyn^omes reciproques des orthonormalises de schmidt
(NB le polynome reciproque d'une polynome est le polynome cree a
partir de la suite des coefficients pris dans l'ordre inverse. (Le
facteur vient de la norme 1)

38
```
recip:=proc(P)
normal(x^degree(P)*subs(x=1/x,P))
end;
```
// Warning: x declared as global variable(s)
// End defining recip

```
proc(P)
  normal(x^(degree(P))*subs(x=(1/x),P));

end;
```
Menu

39
```
seq(recip(denom(i)),i=S); #donne bien les polyn^omes obtenus par gramschmidt
```
$$(x+3,\ -x^2-3\cdot x+3,\ -3\cdot x^3-20\cdot x^2-21\cdot x+42,\ 273\cdot x^4+1194\cdot x^3+498\cdot x^2+77\cdot x+483)$$
Menu

40