

## - Pseudo-random sequences of length $2^n - 1$ generated by GF( $2^n$ ); $n \equiv 6$ in our example

### - Informal introduction

Pseudo-random (or PN, for pseudo-noise) sequences  $a = a_0, a_1, a_2, \dots$  are binary sequences of length  $m, m = 2^n - 1$  in our case, such that its autocorrelation function

$$\rho(\tau) = \frac{\sum_{j=0}^{m-1} s_j s_{j+\tau}}{m}, \text{ where } s_i = (-1)^{a_i},$$

satisfies the properties  $\rho(0) = 1$  [obvious],  $\rho(m) = 1$  [the series is periodic with period  $m$ ]

and  $\rho(\tau) = -\frac{1}{m}$  for  $1 \leq \tau < m$  [for  $m$  large the sequences are almost non-correlated with its

cyclic non-periodic shifts]. A physicist, by the way, might prefer to look at the periodic sequence  $s = s_0, s_1, s_2, \dots$  as a minimal energy cyclic arrangement of  $m$  spins. To determine *non-cyclic* minimal spin arrangements is generally a hard problem requiring brute force *branch and bound* techniques. A group-theorist likely thinks of almost orthogonal characters, while an engineer will see almost uncorrelated pulsed signals. There is a vast literature on the subject, but the classic book on coding theory by **N.J.A. Sloane** and **F.J. MacWilliams** is hard to beat as an introduction and reference work.

These sequences have been technically easy to generate ever since the past era of vacuum tubes and transistors by means of simple electronic circuits called *linear feedback registers*. They have been (and still are) frequently used in acoustics, satellite monitoring and for radar observations. I quote from p.394 of the third printing of modern Applied Algebra by *G. Birkhoff* and *Th. C. Bartee* (a book I used in class in the early seventies of the past century): "Satellite communication systems can be obtained which generate sequences transmitted at intervals of 0.000001 seconds, which repeat only once a year, using primitive polynomials of degree  $n = 50$ ".

### - Recurrent sequences over the rationals ( $n \equiv 6$ )

We shall consider the 6th order linear recurrence equation

$$b_{k+6} + b_{k+1} + b_k = 0,$$

whose characteristic polynomial is given by

$$m(X) = X^6 + X + 1$$

and whose familiar complex linearly independent set of 6 fundamental solutions is given by  $b_k = \lambda_i^k$ , for all integer  $k$ , where  $\lambda_i, i = 1, 2, 3, 4, 5, 6$  are the 6 distinct roots of  $m(X)$ . Let us first verify that  $m(X)$  is irreducible over the rational field and has distinct roots indeed.

```
> restart: with(linalg): m(X):=X^6+X+1;
'Dm(X)'=diff(m(X),X);
'irreduc(m(X))'=irreduc(m(X)); 'factor(m(X))'='
factor(m(X)); 'gcd(m(X),Dm(X))'=gcd(m(X),Dm(X));
```

Warning, the protected names norm and trace have been redefined and unprotected

```

m(X) := X^6 + X + 1
Dm(X) = 6 X^5 + 1
irreduc(m(X)) = true
factor(m(X)) = X^6 + X + 1
gcd(m(X), Dm(X)) = 1

```

We shall now determine floating point approximations of its real and complex factorizations and its characteristic roots  $\lambda_i$ .

```

> X^6+X+1=factor(X^6+X+1,real);
X^6+X+1=factor(X^6+X+1,complex);
X^6 + X + 1 = (X^2 + 1.581334378 X + 0.7154590126)
              (X^2 + 0.3094702890 X + 1.102177555) (X^2 - 1.890804667 X + 1.268129712)
X^6 + X + 1 = (X + 0.7906671888 + 0.3005069203 I)
              (X + 0.7906671888 - 0.3005069203 I) (X + 0.1547351445 + 1.038380754 I)
              (X + 0.1547351445 - 1.038380754 I) (X - 0.9454023333 + 0.6118366938 I)
              (X - 0.9454023333 - 0.6118366938 I)
> for i from 1 to 6 do lambda[i]:=RootOf(X^6+X+1,index=i)od:
> print(evalf(lambda[1]), evalf(lambda[2]),
        evalf(lambda[3])); print(evalf(lambda[4]),
        evalf(lambda[5]), evalf(lambda[6]));
0.9454023333 + 0.6118366938 I, -0.1547351445 + 1.038380754 I,
-0.7906671888 + 0.3005069203 I
-0.7906671888 - 0.3005069203 I, -0.1547351445 - 1.038380754 I,
0.9454023333 - 0.6118366938 I

```

In infinite characteristic, that is, over the rationals, the  $\lambda_i$  satisfy an algebraic symmetry (given by Galois theory), but from the point of view of (asymptotic) analysis they act totally different. For large positive  $k$ , the behavior of  $\lambda_1^k$  and  $\lambda_6^k$  (of largest modulus) will be dominant in a generic solution  $b_k$ , whereas for negative  $k$ , the influence of  $\lambda_3$  and its conjugate  $\lambda_4$  (of least modulus) will be felt most. This aspect will disappear in characteristic 2, but will be fully compensated by a perfect cyclic symmetry. Let us check the moduli and the conjugacy of the pairs of equal modulus:

```

> for i from 1 to 3 do
  print(convert(evalf(lambda[i]),polar),convert(evalf(lambda
    [7-i]),polar)); od;
      polar(1.126112655, 0.5743836884), polar(1.126112655, -0.5743836884)
      polar(1.049846444, 1.718723598), polar(1.049846444, -1.718723598)
      polar(0.8458481026, 2.778386642), polar(0.8458481026, -2.778386642)
> (X-'lambda[1]')*(X-'lambda[6]')=expand(evalf((X-lambda[1])
  *(X-lambda[6])));
(X-'lambda[2]')*(X-'lambda[5]')=expand(evalf((X-lambda[2])
  *(X-lambda[5])));
(X-'lambda[3]')*(X-'lambda[4]')=expand(evalf((X-lambda[3])

```

```
*(X-lambda[4])));
```

$$(X - \lambda_1)(X - \lambda_6) = X^2 - 1.890804667 X + 1.268129712 + 0. I$$

$$(X - \lambda_2)(X - \lambda_5) = X^2 + 0.3094702890 X + 1.102177555 + 0. I$$

$$(X - \lambda_3)(X - \lambda_4) = X^2 + 1.581334378 X + 0.7154590126 + 0. I$$

Maple provides the method of generating functions (involving the reciprocal polynomial of  $m(X)$ ) to produce solutions to the given difference equation:

```
> alias(mu=RootOf(X^6+X^5+1=0));
```

```
'b(k) '=rsolve(b(n+6)+b(n+1)+b(n)=0,b(k));
```

```
'b(k) '=rsolve(b(n+6)+b(n+1)+b(n)=0,b(k),'genfunc'(z));
```

$\mu$

$$b(k) = \sum_{_R=\mu} \left( \frac{(b(3) \_R^3 + b(0) + b(1) \_R + b(2) \_R^2 + b(4) \_R^4 + b(5) \_R^5 + \_R^5 b(0)) \left(\frac{1}{\_R}\right)^k}{(5 \_R^4 + 6 \_R^5) \_R} \right)$$

$$b(k) = \frac{b(0) + b(1) z + b(2) z^2 + b(3) z^3 + b(4) z^4 + b(5) z^5 + z^5 b(0)}{1 + z^5 + z^6}$$

The linear independence of the set of 6 fundamental solutions may be verified explicitly as an illustration of the use of Vandermonde determinants and subsequently Cramer's rule might be applied to express a solution linearly in terms of its initial conditions and the fundamental set. But in practice no one will.

```
> i:='i': L:= [seq(a[i],i=1..6)];
```

$L := [a_1, a_2, a_3, a_4, a_5, a_6]$

```
> V:=vandermonde(L);
```

$$V := \begin{bmatrix} 1 & a_1 & a_1^2 & a_1^3 & a_1^4 & a_1^5 \\ 1 & a_2 & a_2^2 & a_2^3 & a_2^4 & a_2^5 \\ 1 & a_3 & a_3^2 & a_3^3 & a_3^4 & a_3^5 \\ 1 & a_4 & a_4^2 & a_4^3 & a_4^4 & a_4^5 \\ 1 & a_5 & a_5^2 & a_5^3 & a_5^4 & a_5^5 \\ 1 & a_6 & a_6^2 & a_6^3 & a_6^4 & a_6^5 \end{bmatrix}$$

```
> factor(det(V));
```

$$-(a_4 - a_5)(a_3 - a_4)(a_3 - a_5)(-a_6 + a_4)(-a_6 + a_5)(-a_6 + a_3)(a_2 - a_4)(a_2 - a_5)$$

$$(a_2 - a_3)(a_2 - a_6)(-a_4 + a_1)(a_1 - a_5)(a_1 - a_3)(a_1 - a_6)(-a_2 + a_1)$$

So this determinant is regular if and only if the  $a_i$  are distinct. In our case, where  $a_i = \lambda_i$ , they were.

## Recurrent sequences over $\text{GF}(2)$ ( $n \equiv 6, m(X) \equiv X^6 + X + 1$ )

We introduce the usual notation.  $M = \text{GF}(2)(\alpha)$ , where  $\alpha$  is a root of the primitive irreducible polynomial  $m(X)$  over  $\text{GF}(2)$ . In this case, the Vandermonde determinant is necessarily equal to 1, the only nonzero element of  $\text{GF}(2)$ . In odd prime characteristic  $p$ , the Vandermonde determinant would be a square root  $r$  of an element of  $\text{GF}(p)$  outside  $\text{GF}(p)$  and any odd permutation of the roots would map  $r$  onto  $-r$ . Let us start Maple anew:

```
> restart:with(linalg):m(X):=X^6+X+1:alias(alpha=RootOf(X^6+
X+1)):
i:='i': for i from 1 to 6 do a[i]:=alpha^(2^(i-1)) od:
i:='i': L:=[seq(a[i],i=1..6)]: print(L);
V:=transpose(vandermonde(L)); T:=map(x->Normal(x) mod
2,V);
```

Warning, the protected names norm and trace have been redefined and unprotected

$$V := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} \\ \alpha^2 & \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} \\ \alpha^3 & \alpha^6 & \alpha^{12} & \alpha^{24} & \alpha^{48} & \alpha^{96} \\ \alpha^4 & \alpha^8 & \alpha^{16} & \alpha^{32} & \alpha^{64} & \alpha^{128} \\ \alpha^5 & \alpha^{10} & \alpha^{20} & \alpha^{40} & \alpha^{80} & \alpha^{160} \end{bmatrix}$$

$T :=$

$$T := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^4 & \alpha^3 + \alpha^2 & \alpha^4 + \alpha + 1 & \alpha^3 + 1 \\ \alpha^2 & \alpha^4 & \alpha^3 + \alpha^2 & \alpha^4 + \alpha + 1 & \alpha^3 + 1 & \alpha \\ \alpha^3 & \alpha + 1 & \alpha^2 + 1 & \alpha^4 + 1 & \alpha^3 + \alpha^2 + 1 & \alpha^4 + \alpha \\ \alpha^4 & \alpha^3 + \alpha^2 & \alpha^4 + \alpha + 1 & \alpha^3 + 1 & \alpha & \alpha^2 \\ \alpha^5 & \alpha^5 + \alpha^4 & \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 & \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1 & \alpha^5 + \alpha^2 + \alpha & \alpha^5 + \alpha^2 \end{bmatrix}$$

```
> det(T) mod 2;
```

1

There is however no need for this result. Let  $\theta$  be any nonlinear functional on  $M$ , that is  $\theta$  is any  $K$ -linear mapping from  $M$  onto the prime field  $K = \{0, 1\}$ . Since

$$\alpha^{(k+6)} + \alpha^{(k+1)} + \alpha^k = \alpha^k (\alpha^6 + \alpha + 1) = \alpha^k \cdot 0 = 0, \text{ putting } b_k = \theta(\alpha^k) \text{ gives a solution to}$$

the recurrence. But, the number of nonzero linear functionals is  $2^6 - 1 = 63$  [for each of 6 basisvectors of  $M$  over  $K$  we have 2 independent possibilities to assign to under  $\theta$ , viz. 0 or 1, and the all-zero choice is excluded] and this coincides with the number of not identically zero sets of 6 initial conditions for the recurrence. It follows that *all* nonzero solutions of the

recurrence are of this form. Clearly, since  $\alpha^{63} = 1$ , all this sequences are periodic with period 63, or a divisor of 63. Let  $d$  be any period of  $b_k = \theta(\alpha^k)$ . Then by linearity

$\theta(\alpha^k (\alpha^d - 1)) = 0$ , whereas  $\theta$  is nonzero. So, since  $M$  is generated by  $\alpha$ , as a field,

necessarily  $\alpha^d - 1 = 0$ . Hence, since  $\alpha$  is even primitive,  $d$  must be a multiple of 63, which settles the converse. The important thing to realize now is that the successive strings of length 6 in any binary sequence of period 63 must be distinct until after 63 steps they start to repeat. But there exist exactly 63 binary strings of length 6 in all. We conclude that *all* 63 nonzero strings of 6 initial conditions occur somewhere (as a consecutive string) in the sequence. **Moreover, all nonzero solutions of the recurrence are cyclic shifts from one another**, and hence *all* have the same weight 32, for symmetry reasons. As an application we shall prove the formula  $\rho(\tau) = -\frac{1}{m}$ . Since  $(-1)^{a_j} (-1)^{a_{j+\tau}} = (-1)^{(a_j+a_{j+\tau})}$  and  $a_j + a_{j+\tau}$  provides a solution of the *linear* recurrence as well, we get 32 times a  $-1$  and 31 times a  $(-1)^0 = 1$  in the numerator for  $\rho(\tau)$  etc. We return to practice.

If we use the remember option, Maple can generate the solution sequences easily. Below is a list  $l$  of initial conditions, which may be made up of symbols or integers (mod 2).

```
> l:= [seq(c[i], i=0..5)]:
b:=proc(n::nonnegint) Rec(n,l) end:
Rec:=proc(n,l::list)
option remember;
if n>=0 and n<=5 then l[n+1]
else Rec(n-5,l)+Rec(n-6,l) mod 2
fi
end;
```

```
Rec := proc(n, l::list)
```

```
option remember;
```

```
if 0 ≤ n and n ≤ 5 then l[n + 1]
```

```
else (Rec(n - 5, l) + Rec(n - 6, l)) mod 2
```

```
end if
```

```
end proc
```

```
> for k from 0 to 68 do b(k) od:
```

```
> print(seq(b(m), m=0..62));
```

```
c0, c1, c2, c3, c4, c5, c1 + c0, c2 + c1, c3 + c2, c4 + c3, c5 + c4, c1 + c0 + c5, c2 + c0, c3 + c1,
c4 + c2, c5 + c3, c1 + c0 + c4, c2 + c1 + c5, c3 + c1 + c2 + c0, c4 + c2 + c3 + c1,
c5 + c3 + c4 + c2, c1 + c0 + c4 + c5 + c3, c2 + c5 + c0 + c4, c3 + c0 + c5, c4 + c0, c5 + c1,
c1 + c0 + c2, c2 + c1 + c3, c3 + c2 + c4, c4 + c3 + c5, c5 + c1 + c4 + c0, c0 + c2 + c5, c3 + c0,
c4 + c1, c5 + c2, c1 + c0 + c3, c2 + c1 + c4, c3 + c2 + c5, c4 + c1 + c3 + c0, c5 + c2 + c4 + c1,
c1 + c0 + c3 + c5 + c2, c2 + c4 + c0 + c3, c3 + c5 + c1 + c4, c4 + c1 + c0 + c2 + c5,
c5 + c2 + c3 + c0, c0 + c3 + c4, c4 + c1 + c5, c5 + c1 + c2 + c0, c0 + c2 + c3, c3 + c4 + c1,
c4 + c5 + c2, c1 + c5 + c0 + c3, c2 + c0 + c4, c3 + c5 + c1, c4 + c1 + c0 + c2,
c5 + c2 + c3 + c1, c1 + c0 + c3 + c4 + c2, c2 + c4 + c1 + c5 + c3, c3 + c5 + c1 + c2 + c0 + c4,
c4 + c0 + c2 + c3 + c5, c5 + c3 + c4 + c0, c0 + c4 + c5, c5 + c0
```

We verify the announced periodicity of period 63:

```
> print(seq(b(m),m=63..68));
```

$c_0, c_1, c_2, c_3, c_4, c_5$

In particular we may generate the Galois sequence  $g$  of period 63 depicted in a circular array around the stamp of Galois on the main page [in  $g$  the first 5 entries are repeated at the end, for later use].

```
> l:=[1,0,0,0,0,0]: g:=[seq(b(m),m=0..67)];
```

```
g := [1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1,
      1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0,
      0, 0]
```

For classroom use I will add a Maple procedure to easily locate any nonzero string of 6 consecutive bits in  $g$ . The function  $s$  selects such a string.

```
> s:=k->[g[k],g[k+1],g[k+2],g[k+3],g[k+4],g[k+5]]:
```

```
> p:=proc(L::list)
```

```
    local i::nonnegint, j::posint:
```

```
        for i from 0 to 62 do if L=s(i+1) then RETURN([i,i+5]);
        fi od end;
```

```
p := proc(L::list)
```

```
    local i::nonnegint, j::posint;
```

```
        for i from 0 to 62 do if L = s(i + 1) then RETURN([i, i + 5]) end if end do
```

```
end proc
```

```
> print(p([1,0,0,0,0,0]),p([0,1,0,0,0,0]),p([0,0,1,0,0,0]),
      p([0,0,0,1,0,0]),p([0,0,0,0,1,0]),p([0,0,0,0,0,1]));
print(p([1,1,0,0,0,0]));
```

[0, 5], [5, 10], [4, 9], [3, 8], [2, 7], [1, 6]

[62, 67]

By  $G_6$  we denote the standard form of the generator matrix for the cyclic (63,6,32)-linear binary blockcode  $C$  whose first row  $w$  is given by the first 63 entries of  $g$ . The code  $C$  has length 63, dimension 6 and minimal (nonzero) weight 32. It is cyclic in a very strong sense, namely that all 63 nonzero code words are cyclic shifts of  $w$ , as we have seen before. By using the output above we immediately see that e.g. the second row of  $G_6$  is given by a cyclic shift of  $w$  over five positions to the right. The code can detect all error patterns of weight 31 and correct all error patterns of weight 15 (the integer part of  $31/2$ ).

An  $m \times n$  matrix is in standard form if its left  $m \times m$  part is an  $m \times m$  identity matrix. In the present case a code word starts accordingly with 6 information symbols followed by 57 check symbols, which are recursively constructed by means of the given difference equation.

```
> k:='k': w:=[seq(g[k],k=1..63)];
```

```
w := [1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1,
      1, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1]
```

The same procedure applied to the two subfields  $K = \text{GF}(4)$  and  $L = \text{GF}(8)$  gives us a generator matrix  $G_2$  corresponding to the primitive polynomial  $X^2 + X + 1$  and another generator matrix  $G_3$  corresponding to  $X^3 + X + 1$ :

```
> G2:=matrix(2,3,[[1,0,1],[0,1,1]]):
```

```
G3:=matrix(3,7,[[1,0,0,1,0,1,1],[0,1,0,1,1,1,0],[0,0,1,0,1,1,1]]);
print(G2=evalm(G2), G3=evalm(G3));
```

$$G_2 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, G_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Since both matrices are in standard form corresponding check matrices (which are generator polynomials for the dual codes, but also can be seen as coefficient matrices for a minimal system of linear equations determining the codes) can be written down by hand in no time. The standard trick, involving transposition of the non-identity part of the generator matrix, will be illustrated by Maple, for  $G_3$  only.

```
> Q:=matrix(4,3,[col(G3,4),col(G3,5),col(G3,6),col(G3,7)]);
```

$$Q := \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

```
> h3:=(i,j)->if j<4 then Q[i,j] elif i+3=j then 1 else 0
fi:H3:=matrix(4,7,h3):
H3new:=map(x-> x mod
2,addrow(addrow(addrow(H3,1,3,1),1,4,1),2,4,1)):
print(H3=evalm(matrix(4,7,h3)),H3new=evalm(map(x-> x mod
2,addrow(addrow(addrow(H3,1,3,1),1,4,1),2,4,1))));
```

$$H_3 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}, H_{3new} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

We have applied a few elementary row operations on the check matrix  $H_3$  to obtain a new (equivalent) one which nicely exhibits the defining linear equations  $b_k + b_{k+1} + b_{k+3} = 0$  (and the associated polynomial  $1 + X + X^3$ ) of the code.

A closer look at  $G_3$  shows that its 7 columns are *all* the nonzero columns of length 3 possible. In other words  $G_3$  itself is a check matrix of a 1-error correcting perfect (7,4,3)-code  $H$ . All of the cosetleaders of  $H$  have weight 1 and each of their 7 syndroms is contained in one of the 7 columns of  $G_3$ .  $H$  is a classical *Hamming* code, of course. Similarly for  $G_2$  and  $G_6$ . These dual codes of Hamming codes are called *simplex codes*. It easily follows from the cyclic structure of  $G_6$ , for instance, that no zero-column occurs, since no 6 consecutive bits in  $g$  are zero, and that no two columns are the same, since otherwise  $g$  would repeat itself too early.