Pseudo Noise(PN) Sequence

Contents

- Desired properties
- Linear feedback shift register, m-sequence
- Gold Sequences
- Reference

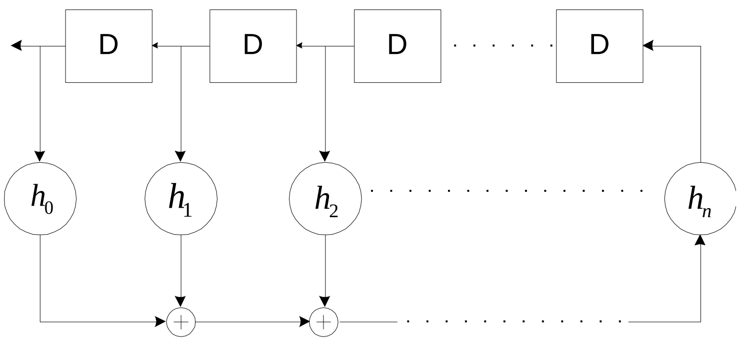
  D. V. Sarwate & M. B. Pursley,
  "Crosscorrelation properties of pseudorandom and related sequences,"
  IEEE Proc, vol.68, pp.593~619, May 1980

Desired properties

- Random property
  (Autocorrelation, Crosscorrelation)
- Easy to generate
- Long Period
- Difficult to reconstruct

* Random code

Linear feedback shift register



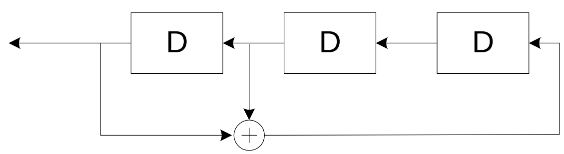
$h_0 \ldots h_n$ *is* 0 *or* 1

$h(x) = h_0 + h_1 x + h_2 x^2 \ldots h_n x^n$

$h_o = h_n = 1$

$h_i = \{0,1\}$ i=1, ⋯ , n-1

Example) $h(x) = 1 + x + x^3$



0	1	1
1	1	1
1	1	0
1	0	0
0	0	1
0	1	0
1	0	1
0	1	1

- A sequence is periodic
- possible max seq lenghth

- Periodic autocorrelation

$$\theta_c(m) \equiv \frac{1}{N}\sum_{n=0}^{N-1} c_n c_{n+m} = \frac{1}{N}\sum_{n=0}^{N=1}(-1)^{b_n}(-1)^{b_{n+m}}$$

$$= \frac{1}{N}\sum_{n=0}^{N=1}(-1)^{b_n \oplus b_{n+m}}$$

($\oplus$:modulo-2 addition)

- If $\{b_n\}$ is a binary sequence, $b_n \in \{0,1\}$
  its Hamming weight is

  $W_H\{b_n\}$ = number of 1's in $\{b_n\}$.

- If $\{a_n\}\neq\{b_n\}$ are 2 binary sequences, their Hamming distance is

$$d_H(\{a_n\}, \{b_n\}) = W_H(\{a_n\}\oplus\{b_n\})$$

- T is the cyclic shift (left) operator. If $b=\{b_0, b_1, \cdots b_n\}$, then

$$T\mathbf{b}=\{b_1, b_2, \cdots b_n, b_0\}$$

Periodic autocorrelation:

$$\theta_b(m) = \frac{1}{N}\sum_{n=0}^{N-1}(-1)^{b_n \oplus T^m b_n}$$

$$= \left(\frac{1}{N}\{\text{No. of same chips} - \text{No. of diffrent chips}\}\right)$$

$$= \frac{1}{N}\left(N - 2W_H\left(b \oplus T^m b\right)\right)$$

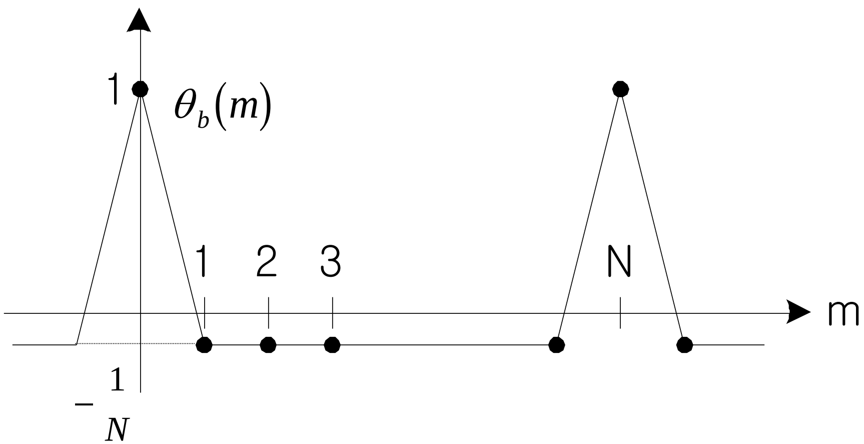
PN sequence

- Consider a sequence $\{b_n\}$ of period N(odd) such that

$$i)\quad W_H\left(\{b_n\}\right) = \frac{N+1}{2}$$

$$ii)\quad b \oplus T^m b = T^l b,\ \text{for}\ \ \forall m \bmod N \neq 0$$

$$
\begin{aligned}
\theta_b(m) &= \frac{N - 2W_H\left(b \oplus T^m b\right)}{N} \\
&= \frac{N - 2W_H\left(T^l b\right)}{N} \\
&= \frac{N - 2W_H(b)}{N} \\
&= \frac{N - (N+1)}{N} \\
&= -\frac{1}{N} \qquad \left(\text{for } \forall m \ \bmod N \neq 0\right)
\end{aligned}
$$



- n Shift registers: $N = 2^n - 1$

  -> Maximum length sequence

  (m-sequence)

- If $h(n)$ produces an m-seq.,

  $h(n)$ is called a primitive polynomial.

Degree	Polynomials(octal)
2	7
3	13
4	23
5	45, 75, 67

- If $h(x)$ is of degree of n which generates an m-seq., then its reciprocal $x^n h(1/x)$ also generates a m-seq.

Ex) $n = 5$, $N = 2^5 - 1 = 31$

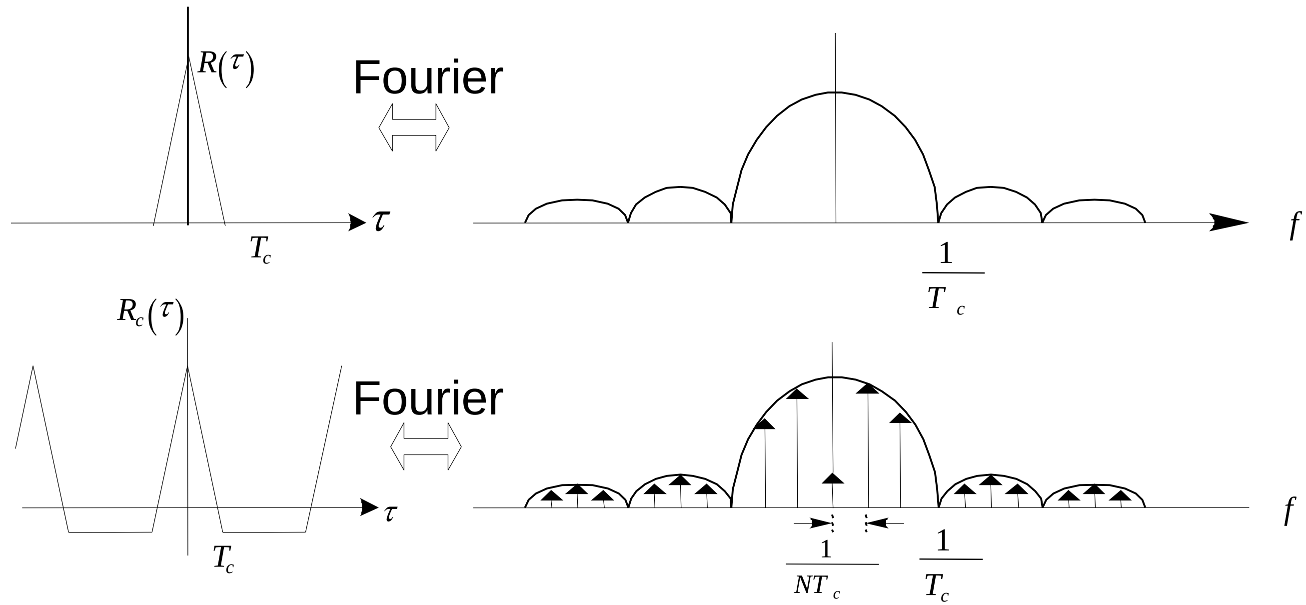
Primitive polynomials = 45, 75, 67

$$75:\ 111101 \rightarrow 1 + x^2 + x^3 + x^4 + x^5$$

$$x^n h(1/x) = x^5 \left(1 + \frac{1}{x^2} + \frac{1}{x^3} + \frac{1}{x^4} + \frac{1}{x^5}\right)$$

$$= x^5 + x^3 + x^2 + x + 1 \rightarrow 57$$

- Spectrum



$$R_c(\tau) \xrightarrow{Fourier} S(f) = \sum_{\substack{m=-\infty \\ m\neq 0}}^{\infty} \delta(f - mf_0) \frac{N+1}{N^2} \left(\frac{\sin(\pi f / f_c)}{\pi f / f_c} \right)^2 + \frac{1}{N^2}\delta(f),$$

$$\text{where } f_0 = \frac{1}{NT_c}$$

M-Seq properties

$$1)\ W_H(b) = \frac{N+1}{2}$$

$$2)\ b \oplus T^m b = T^l b \quad \text{(shiqt registers)}$$

$$3)\ \theta_b(m) = \begin{cases} -\frac{1}{N}, m \neq 0 \bmod N \\ 1, \quad m = 0 \bmod N \end{cases}$$

M-Seq properties(cont'd)

4) A run is defined as a string of consecutive 1's & 0's

i) 1/2 of the runs is length one

ii) 1/4 of the runs is length two

iii) 1/8 of the runs is length three

(example) 0111001

run length	no (tot no: 4)
1	2
2	1
3	1

Definition of Decimation

If $b = (b_0, b_1, \ldots b_{N-1})$, then the qth decimation of b is $b[q] = (b_0, b_q, b_{2q} \ldots b_{(N-1)q})$, where all subscripts are to be mod N

ex:

$$b = (1110010)$$

$$b[2] = (1100101) = \mathrm{T}b$$

$$b[3] = (1001110) = c$$

- $b[q]$ has a period $\dfrac{N}{g.c.d(N,q)}$

Crosscor. properties of m-seq

- Two sequences :

$$U = \left(u_0, u_1, \ldots u_{N-1}\right)$$

$$V = \left(v_0, v_1, \ldots v_{N-1}\right)$$

$$\theta_{UV}(l) = \frac{N - 2W_H\left(U \oplus T^l V\right)}{N}$$

– It is not important to know $\theta_{UV}(\ell)$ for all l.

- Crosscorrelation spectrum.

- Preferred pairs

  Let U, V be m-sequences of period $N=2^n-1$.

  If $V=U[q]$, where $q=2^k+1$, or $q=2^{2k}-2^k+1$, and e=g.c.d(n,k) is such that n/e is odd, then the spectrum of $\theta_{UV}(l)$ is 3-valued, and

$$N\theta_{UV}(l)=\begin{cases} -1+2^{(n+e)/2} & \text{occurs } 2^{n-e-1}+2^{(n-e-2)/2} \text{ times} \\ -1 & \text{occurs } 2^n-2^{n-e-1} \text{ times} \\ -1-2^{(n+e)/2} & \text{occurs } 2^{n-e-1}-2^{(n-e-2)/2} \text{ times} \end{cases}$$

Ex)

$$N = 63,\ n = 6,\ \ k = 2$$

$$\Rightarrow \ \ e = 2,\ q = 2^2 + 1 = 5$$

$$q = 2^4 - 2^2 + 1 = 13$$

$$V_1 = U\ 5,\ \text{or}\ \ V_2 = U\ 13$$

$$N\theta_{UV}(l) = \begin{cases} 15 & 10 \text{ times} \\ -1 & 47 \text{ times} \\ -17 & 6 \text{ times} \end{cases}$$

Crosscor. between preferred seq. pairs

n (Register length)	Code length	Crosscor. values	Freq. of occurrences
n odd	$N = 2^n - 1$	-1 $-2^{\frac{n+1}{2}} - 1$ $2^{\frac{n+1}{2}} - 1$	0.50 0.25 0.25
n even, not divisivle by 4	$N = 2^n - 1$	-1 $-2^{\frac{n+2}{2}} - 1$ $2^{\frac{n+2}{2}} - 1$	0.75 0.125 0.125

Gold Sequences

$g(x)$ & $h(x)$ are two different primitive binary polynomials. Let $g(x)$ generates an m-sequence of U of length N, $h(x)$ generates an m-sequence of V of length N. $g(x)h(x)$ generates the following sequences.

$i)\quad y = T^i u$

$ii)\quad y = T^j v$

$iii)\quad y = T^i u \oplus T^j v$

$G(u,v) = \{u, v, \quad u \oplus T^o v, \cdots \quad u \oplus T^{N-1}\, v\}$

let $y, z \in G(u,v)$

$y \oplus T^d z \in G(u,v)$ ($\because$ y and z *are* generated by g(x) h(x))

$$W_H(y \oplus T^d z) = \begin{cases} \dfrac{N+1}{2} & \text{for } y \oplus T^d z = T^i u \quad \text{or} \quad T^j v \\ W_H(T^i u \oplus T^j v) & \text{for } y \oplus T^d z = T^i u \oplus T^j v \end{cases}$$

$$\theta_{yz}(d) = \frac{N - 2W_H(y \oplus T^d z)}{N}$$

$$= \begin{cases} -\dfrac{1}{N} & \text{for} \quad y \oplus T^d z = T^i u \quad \text{or} \quad T^j v \\ \dfrac{N - 2W_H(T^i u \oplus T^j v)}{N} = \theta_{uv}(i-j) & \text{for} \quad y \oplus T^{dz} = T^i u \oplus T^j v \end{cases}$$

(*It* $g(x)$ *and* $h(x)$ *are preferred pairs*)

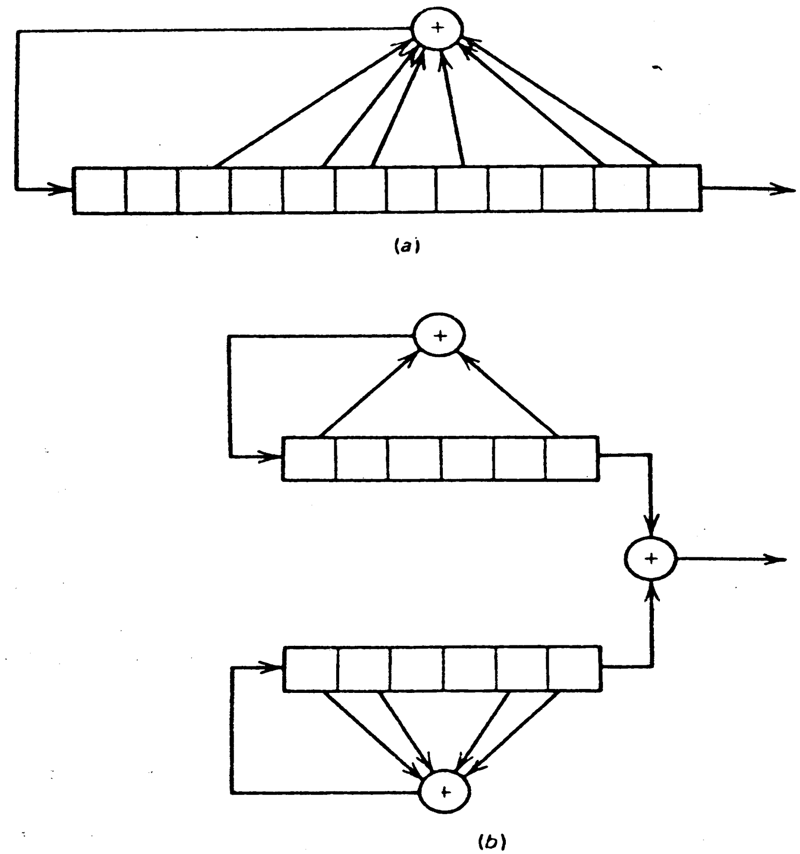


Figure 11.3 Gold code generator of length 63 symbols. (*a*) Single-shift register form ($n = 12$). (*b*) Double-shift register realization ($n = 6$).