Pseudo-Noise Sequences

- Noise-like wideband spread-spectrum signals are generated using PN sequence.

  - In DS/SS(direct-sequence spread-spectrum) , a PN spreading waveform is a time function of a PN sequence.
  - In FH/SS(frequency-hopping spread-spectrum), frequency-hopping patterns can be generated from a PN code.
  - PN sequences are deterministically generated, however they almost like random sequences to an observer.
  - The time waveform generated from the PN sequences also seem like random noise.

M-sequences (1)

- M-sequence (binary maximal length shift-register sequence)

  - Generated using linear feedback shift-register and exclusive OR-gate circuits.

- Linear generator polynomial g(x) of degree m>0

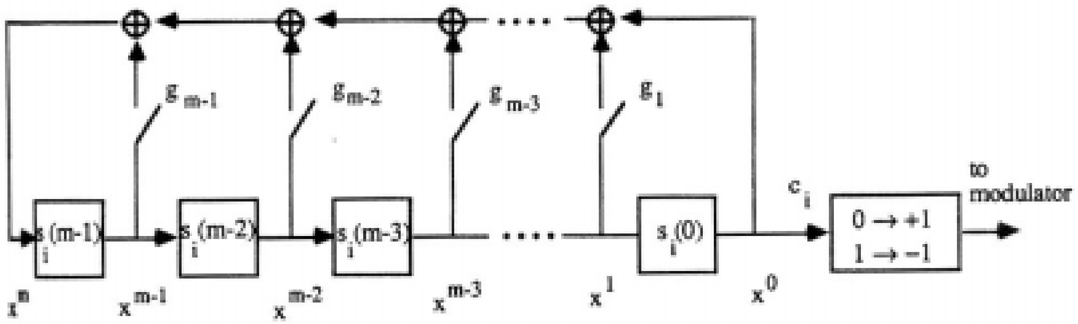
$$g(x) = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_1 x + g_0$$

  - Recurrence Equation ($g_m = g_0 = 1$)

$$x^m = g_{m-1} x^{m-1} + g_{m-2} x^{m-2} + \cdots + g_1 x + g_0 \qquad \text{(mod 2)}$$

  - If $g_i = 1$, the corresponding circuit switch is closed, otherwise $g_i \neq 1$, it is open.

  - Output of the shift-register circuit is transformed to 1 if it is 0, and –1 if it is 1.



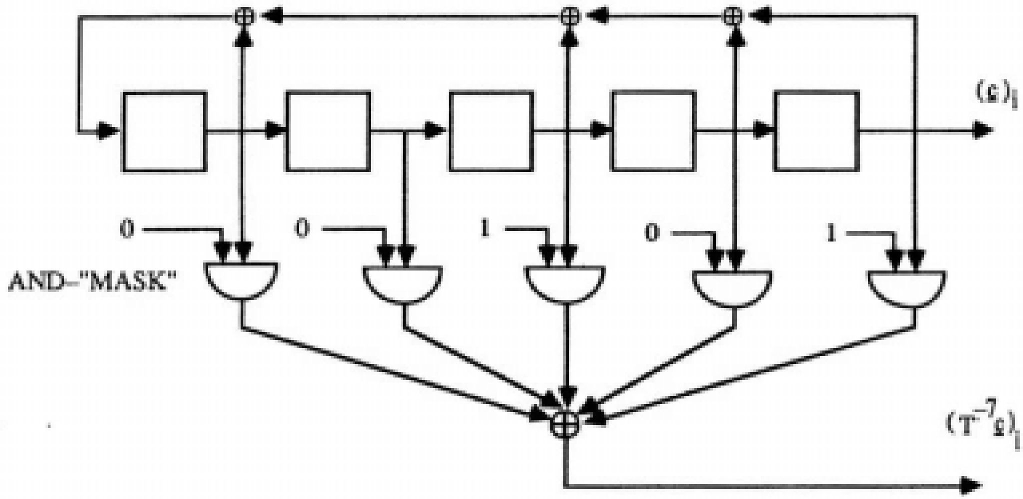
M-sequences (2)

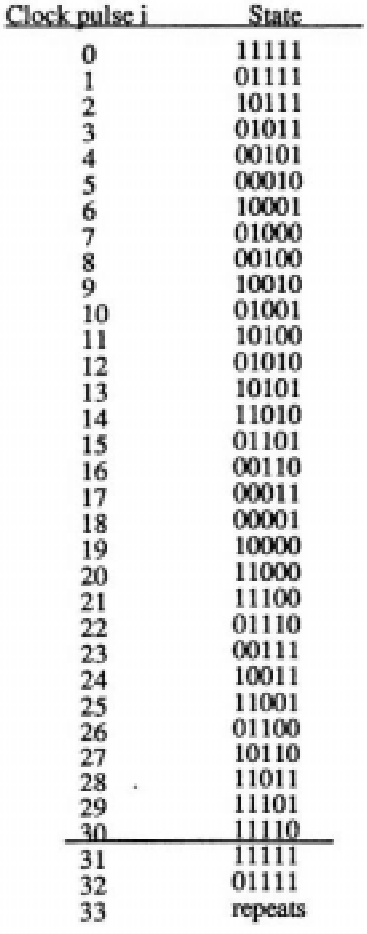
- The maximum number of non-zero state is $2^m - 1$, which is the maximum period of output sequence $\underline{c} = (c_0, c_1, c_2, \cdots\cdots)$
- The state of the shift-register at clock pulse i is the finite length vector $\underline{s}_i = (s_i(m-1), s_i(m-2), \ldots, s_i(0))$ and the output at clock pulse i is $c_i = s_i(0)$.
- Output sequence recurrence condition according to g(x)

$$c_{i+m} = g_{m-1}c_{i+m-1} + g_{m-2}c_{i+m-2} + \cdots + g_1 c_{i+1} + c_i \qquad \text{(mod 2)}$$

- Example of a shift-register sequence
  - For any nonzero starting state($\underline{s}_0 \neq (0,0,0,0,0)$), the state of shift-register varies according to the recurrence condition.
  - Other g(x) may yield a sequence of shorter period than $2^m - 1$.
  - For different initial loading, output sequences become a shift of the sequence $\underline{c}, T^{\mp j}\underline{c}$ (shift $\underline{c}$ to the left(right) by j units).
  - A linear combinations of $T^{-4}\underline{c}, T^{-3}\underline{c}, T^{-2}\underline{c}, T^{-1}\underline{c}, \underline{c}$, yields all the other shift of $\underline{c}$.
  - For example, $T^{-2}\underline{c} + \underline{c}$ yields $T^{-7}\underline{c} = T^{24}\underline{c}$

Example of M-sequence





Clock pulse i	State
0	11111
1	01111
2	10111
3	01011
4	00101
5	00010
6	10001
7	01000
8	00100
9	10010
10	01001
11	10100
12	01010
13	10101
14	11010
15	01101
16	00110
17	00011
18	00001
19	10000
20	11000
21	11100
22	01110
23	00111
24	10011
25	11001
26	01100
27	10110
28	11011
29	11101
30	11110
31	11111
32	01111
33	repeats

Shift-register sequence with $g(x) = x^5 + x^4 + x^2 + x + 1$

Primitive Polynomial (1)

- M-sequence

- A binary linear shift-register sequence that has a period N=2^m-1, where m is the degree of the generator polynomial

- Primitive Polynomial

- the generator polynomial of m-sequence is primitive polynomial.

- g(x) is a primitive polynomial of degree m if the smallest integer n for which g(x) divides x^n+1 is $n=2^m-1$.

- $g(x)=x^5+x^4+x^2+x+1$ is a primitive. On the other hand, $g(x)=x^5+x^4+x^3+x^2+x+1$ is not primitive since $x^6+1=(x+1)(x^5+x^4+x^3+x^2+x+1)$, so the smallest n is 6.

- The number of primitive polynomial of degree m is equal to $\frac{1}{m}\phi(2^m-1)$, where $\phi(n)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$

- $p|n$ denotes “all distinct prime divisors of n”

- $\phi(n)$ is the number of positive integer less than n that are relatively prime to n.

Primitive Polynomial (2)

- Example

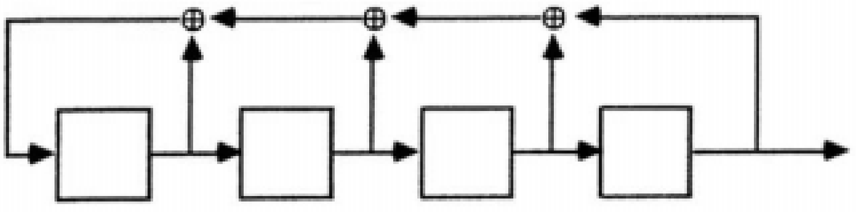
- for m=4, $\frac{1}{4}\phi(2^4-1)=\frac{1}{4}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=2$

- Above 2 polynomial is 100011 and 11001

- One may search for primitive polynomial by trial and error.

- for extensive tables of primitive polynomials, refer to materials on linear algebra and coding theory

- Example of non-primitive generator polynomial



Clock Pulse i	State
0	1111
1	0111
2	1011
3	1101
4	1110
5	1111
6	repeats

- $g(x)=x^5+x^4+x^3+x^2+x+1$ is not primitive , since it yields period 5 instead of 15.

Property of m-sequences (1)

- Property I – The Shift Property

  A cyclic shift(left-cyclic or right-cyclic) of an m-sequence is also an m-sequence

- Property II – The Recurrence Property

  Any m-sequence in S_m satisfies the recurrence condition $c_{i+m} = g_{m-1}c_{i+m-1} + g_{m-2}c_{i+m-2} + \cdots + g_1 c_{i+1} + c_i$ (mod2) for i=0,1,2,…..

- Property III – The window Property

  If a window of width m is slid along an m-sequence in S_m, each of $2^m - 1$ nonzero binary m-tuples is seen exactly once

- Property IV – One more 1 than 0's

  Any m-sequence in S_m contains 2^{m-1} 1's and $2^{m-1} - 1$ 0's

- Property V – The addition Property

  The sum of two m-sequence in S_m(mod2, term by term) is another in S_m

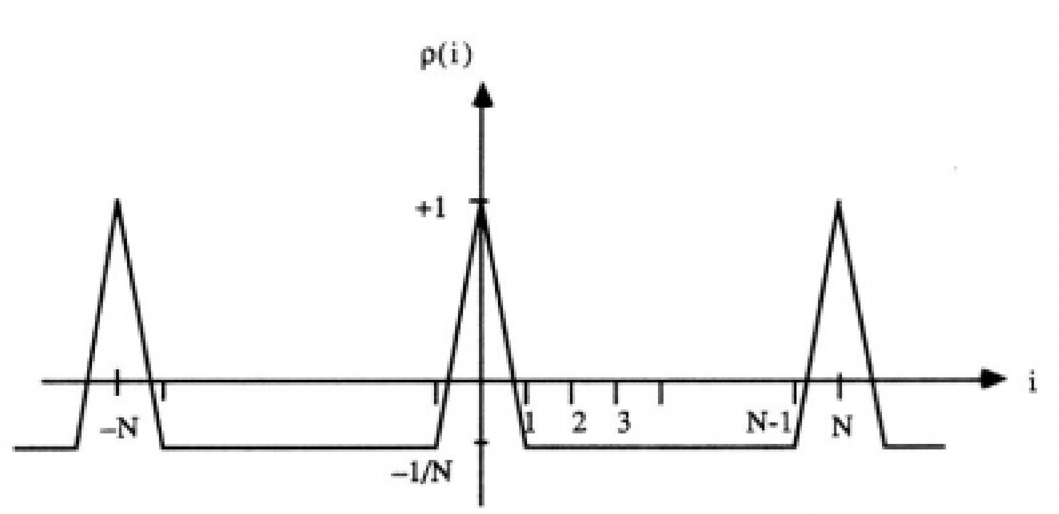
Property of m-sequences (2)

- Property VI – The Shift and Add Property

  The sum of an m-sequence and a cyclic shift of itself(mod2, term by term) is another m-sequence

- Property VII – Thumb-Tack Autocorrelation

  The normalized periodic autocorrelation function of an m-sequence, defined as $\rho(i) = \frac{1}{N}\sum_{j=0}^{N-1}(-1)^{c_j \oplus c_{i+j}}$ is equal to for $i = 0$(mod N) and –1/N for $i \neq 0$(mod N)



- $\rho(i) = \frac{1}{N}$(# of 0's in $\underline{c} \oplus T^{i}\underline{c}$ - # of 1's in $\underline{c} \oplus T^{i}\underline{c}$)

- proved easily by shift and add property

Property of m-sequences (3)

- Property VIII – Runs

A run is string of consecutive 1's or a string of consecutive 0's. In any m-sequence, one-half of the runs have length 1, one-quarter have length 2, one-eighth have length 3, and so on. In particular, there is one run of length m of 1's , one run of length m-1 of 0's.

- Property IX – Characteristic Phase

There is exactly one m-sequence $\underline{\tilde{c}}$ in the set S_m that satisfies $\underline{\tilde{c}} = \tilde{c}_{2i}$ The m-sequence $\underline{\tilde{c}}$ is called the characteristic m-sequence or characteristic phase of the m-sequence in S_m

- Property X – Decimation

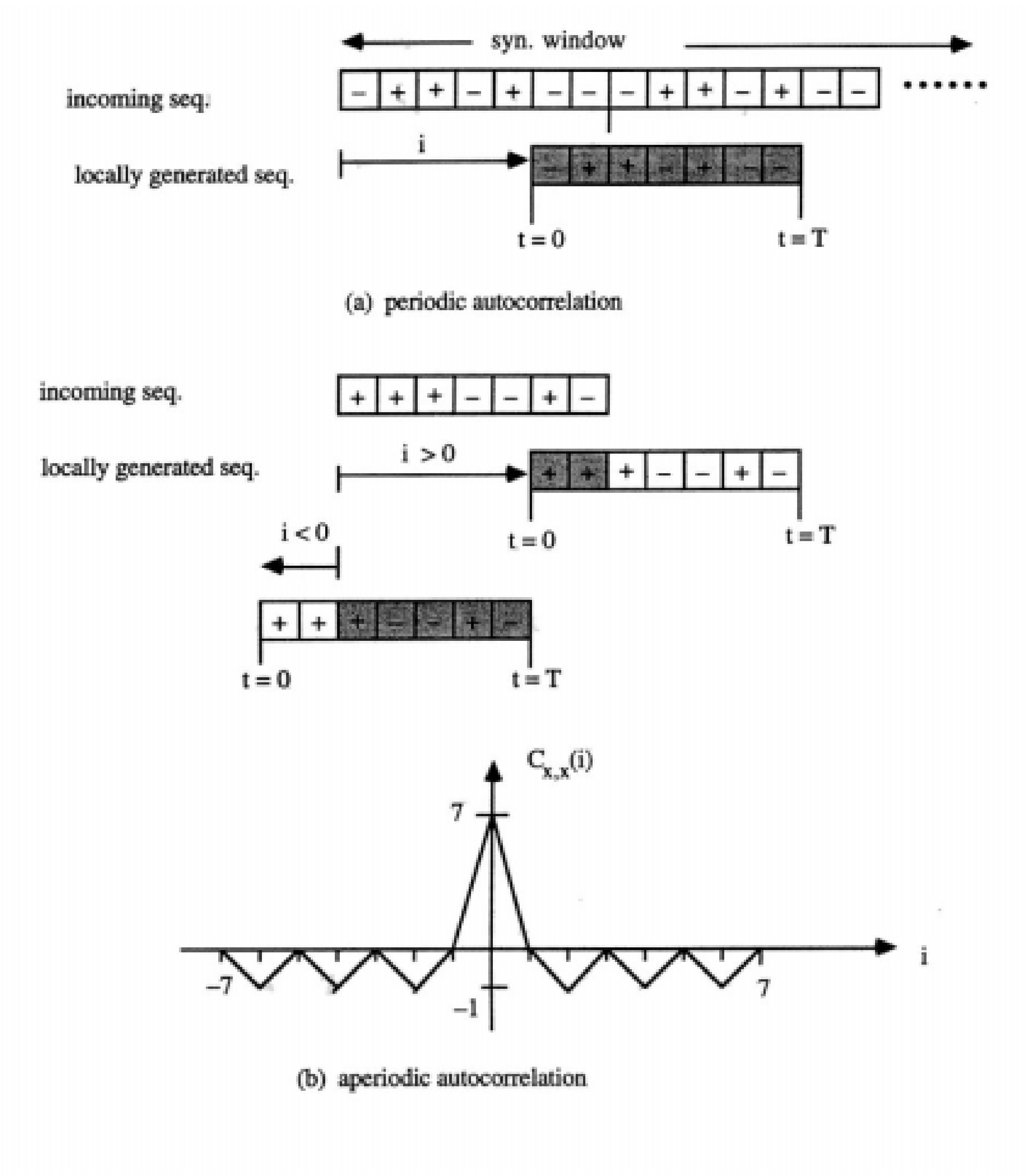
The decimation by n>0 of a m-sequence $\underline{c}$, denoted as $\underline{c}[n]$, has a period equal to N/gcd(N,n), if it is not the all-zero sequence, its generator polynomial $\hat{g}(x)$ has roots that are n-th powers of the roots of g(x)

Autocorrelation of m-sequences (1)

- Periodic autocorrelation
  - -The m-sequence have the best periodic autocorrelation in terms of minimizing the maximum value of the out-of-phase autocorrelation
  - Best utilized if the synchronization window is longer than on period
- Aperiodic autocorrelation
  - If the synchronization window is only one period long or less, then the correlation is aperiodic
  - Barker sequences are sequences that have out-of phase aperiodic autocorrelation magnitude bounded by 1.
  - A formal definition of the aperiodic cross-correlation of $\underline{x}=(x_0,x_1,\ldots,x_{N-1})$ and $\underline{y}=(y_0,y_1,\ldots,y_{N-1})$ is given by

$$C_{x,y}(i)=\begin{cases}\sum_{j=0}^{N-1-i} x_j y_{j+i}^{*} & 0\le i\le N-1\\ \sum_{j=0}^{N-1+i} x_{j-i} y_j^{*} & -(N-1)\le i<0\end{cases}$$

Autocorrelation of m-sequences (2)



(a) periodic autocorrelation

(b) aperiodic autocorrelation

M-sequences summary

- Have a thumb-tack autocorrelation function.
- Best possible periodic autocorrelation (Minimizing out of phase autocorrelation).
- Excellent for the code synchronization operation.
- The number of m-sequences is small ($\frac{1}{m}\phi(N)$).
- Some m-sequence pairs have large crosscorrelation values.
- M-sequences are not suitable for use in the same SSMA sequence set.
- Definition of periodic crosscorrelation for two sequences $u = u_0 u_1 \cdots u_{N-1}$ and $v = v_0 v_1 \cdots v_{N-1}$

$$\theta_{u,v}(n) = \sum_{i=0}^{N-1} u_i v_{n+1}^{*}, \quad n \in \mathrm{Z}$$

Preferred Pair

- Any pair of m-sequences having the same period N can be related by $\underline{y} = \underline{x}[q]$, for some q.

- Definition :
  - $m \neq 0$ (mod 4) : that is, m=odd or m=2(mod 4)
  - $\underline{y} = \underline{x}[q]$, where q is odd and either $q = 2^k + 1$ or $q = 2^{2k} - 2^k + 1$
  - $\gcd(m,k) = \begin{cases} 1 & for\, m\, odd \\ 2 & for\, m = 2(\mathrm{mod}\, 4) \end{cases}$

    gcd : the greatest common divisor

- It is known that preferred-pairs of m-sequences do not exist for m=4,8,12,16, and it was conjectured that no solutions exist for all m=0 (mod 4).

Gold sequences

- Gold sequences of length N can be constructed from a preferred-pair of m-sequences.
- A preferred-pair of m-sequences , say $\underline{x}$ and $\underline{y}$, has a three-valued correlation function :

$$\theta_{\underline{x},\underline{y}}(n) = -1,\ -t(m),\ \ or\ \ t(m)-2 \text{ for all n,}$$

$$\text{where } t(m) = 1 + 2^{\lfloor (m+2)/2 \rfloor}$$

- The set of Gold sequences includes the preferred-pair of m-sequences $\underline{x}$ and $\underline{y}$, and the mod 2 sums of $\underline{x}$ and cyclic shifts of $\underline{y}$.

$$S_{Gold} = \{\underline{x}, \underline{y}, \underline{x} \oplus \underline{y}, \underline{x} \oplus T^{-1}\underline{y}, \underline{x} \oplus T^{-2}\underline{y}, \cdots\cdots, \underline{x} \oplus T^{-(N-1)}\underline{y}\}$$

$$T^{-1}\underline{y} = (y_1, y_2, y_3, \cdots\cdots, y_{N-1}, y_0) \text{ is a left cyclic shift of } \underline{y}.$$

- The maximum correlation magnitude for any two Gold sequences in the same set is equal to the constant $t(m)$.

Example of Gold sequences for m=3

- Number of m-sequences : $\frac{1}{3}\phi(7)=2$
- Length of m-sequences : $N=2^3-1=7$
- Primitive polynomials of degree m=3 (initial loading : 001)

$$x^3+x+1 \quad : \quad \underline{x}=1001011$$

$$x^3+x^2+1 \quad : \quad \underline{y}=1001110$$

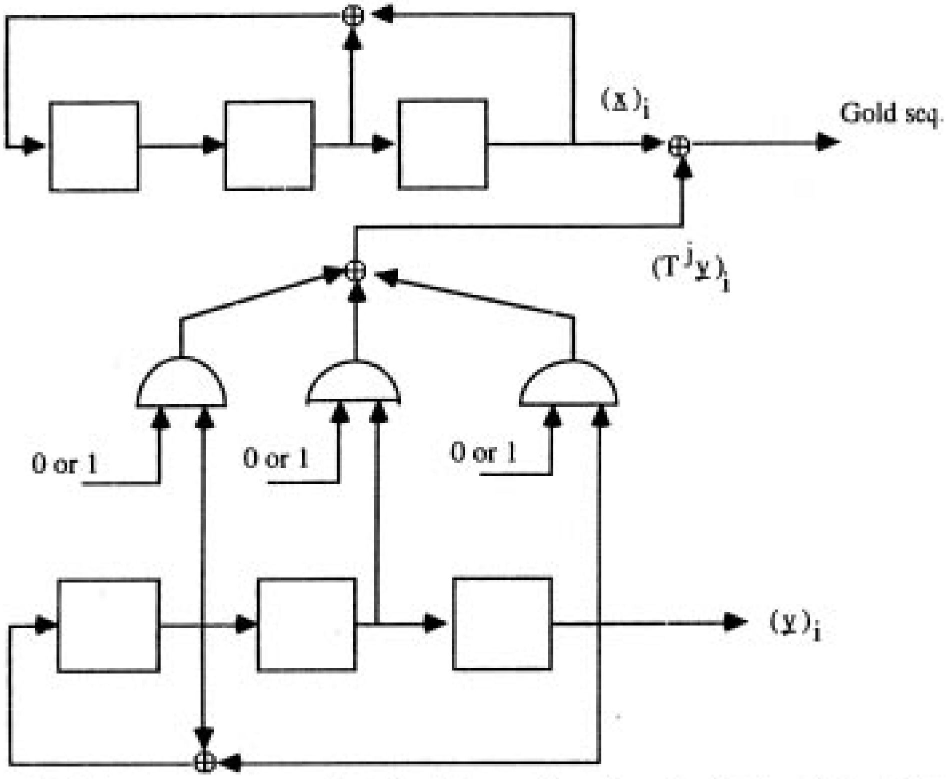


Figure 7.1: Gold sequence generator for the preferred-pair $g_1(x)=x^3+x+1$ and $g_2(x)=x^3+x^2+1$.

- The corresponding set of 9 Gold sequences of period 7 is given by:

1001011	1001110	0000101
1010110	1110001	0111111
01000010	0011000	1101100

- Autocorrelation function for both m-sequences : thumb-tack shaped
- $t(m) = 1 + 2^{\lfloor (m+2)/2 \rfloor}$=5
- Crosscorrelation function are three-valued : -1, -5, or 3

  $(\theta_{\underline{x},\underline{y}}(n) = -1,\ -t(m) = -5,\ \ or\ \ t(m) - 2 = 3)$

- $t(m)/N \approx 2^{-m/2}$ goes to 0 exponentially as m goes to infinity.
- This suggests that longer Gold sequences will perform better as SSMA sequences.

Kasami Sequences

- Kasami sequences are obtained by decimating the m-sequence $\underline{x}$ and performing mod2 addition on cyclically shifted sequences.

Small set of Kasami sequences

- Decimation sequence $\underline{y} = \underline{x}[s(m)]$, where $s(m) = 2^{m/2} + 1$
- $\underline{y}$ is also a periodic m-sequence, with a smaller period equal to $(2^m - 1)/s(m) = 2^{m/2} - 1$
- The small set of Kasami sequences is given by :

$$S_{Kasami} = \{\underline{x}, \underline{x} \oplus \underline{y}, \underline{x} \oplus T^{-1}\underline{y}, \underline{x} \oplus T^{-2}\underline{y}, \cdots\cdot, \underline{x} \oplus T^{-(2^{m/2}-2)}\underline{y}\}$$

$T^{-1}\underline{y} = (y_1, y_2, y_3, \cdots\cdot, y_{N-1}, y_0)$ is a left cyclic shift of $\underline{y}$.

- The crosscorrelation function for two Kasami sequences takes on values in the set

$$\{\theta_{x,y}(n) = -1, -s(m), or\; s(m) - 2\}$$

- The total number of sequences in the set is $2^{m/2}$.

Large set of Kasami sequences

- Consists of sequences of period $2^m - 1$, and contains both the Gold sequences and the small set of Kasami sequences as subsets.

- Let m-sequences $\underline{y}$ and $\underline{z}$ formed by the decimation of $\underline{x}$ by $2^{m/2}+1$ and $2^{(m+2)/2}+1$, and take all sequences formed by adding $\underline{x}$, $\underline{y}$, and $\underline{z}$ with different shifts of $\underline{y}$ and $\underline{z}$.

- All the values of auto-correlation and cross-correlation from members of this set are limited to five values

  $\{-1, -1 \pm 2^{n/2}, -1 \pm 2^{n/2}+1\}$

- These sequences are one of the candidates for the scrambling code in W-CDMA systems.

Example of Kasami sequences for m=4 (Small Set)

- Primitive polynomials $x^4 + x + 1$: $\underline{x} = 100010011010111$
- $s(m) = 2^2 + 1 = 5$
- Decimating $\underline{x}$ by $s(m)$, we get $\underline{y} = x[5] = 101101101101101$
- The period of $\underline{y} = 2^{m/2} - 1 = 3$
- The number of Kasami sequences $2^{m/2} = 4$
- Kasami sequences of length $2^m - 1 = 15$ are given by

100010011010111

001111110111010

111001000001100

010100101100001

- The crosscorrelation function for two Kasami sequences takes on values in the set

$$\{\theta_{x,y}(n) = -1, -s(m) = -(2^{m/2} + 1) = -5, or\ s(m) - 2 = 3\}$$

Orthogonal Codes

- Orthogonal functions are employed to improve the bandwidth efficiency of spread spectrum systems.
- The Walsh and Hadamard sequences make useful sets for CDMA.
- The orthogonal functions have the following characteristic :

$$\sum_{k=0}^{M-1} \phi_i(k\tau)\phi_j(k\tau) = 0\,, \quad i \neq j\,.$$

  - $\phi_i(k\tau)$, $\phi_j(k\tau)$: ith and jth orthogonal members of an orthogonal set.
  - τ : symbol duration
- Walsh functions are generated by mapping codeword rows of special square matrices called Hadamard matrices.

$$H_1 = [0], \quad H_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad H_2 = \left[\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right]\begin{array}{l} -W_0 \\ -W_1 \\ -W_2 \\ -W_3 \end{array},$$

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & \overline{H_N} \end{bmatrix}$$

- These functions have zero correlation between each other.
- Orthogonal spreading codes can be used if all the users of the same channel are synchronized in time to the accuracy of a small fraction of one chip, because the cross-correlation between different shifts of Walsh functions is not zero. (Forward channel)
- Another method can be used to modulate the orthogonal functions into the information stream of the CDMA signal. (Reverse channel)

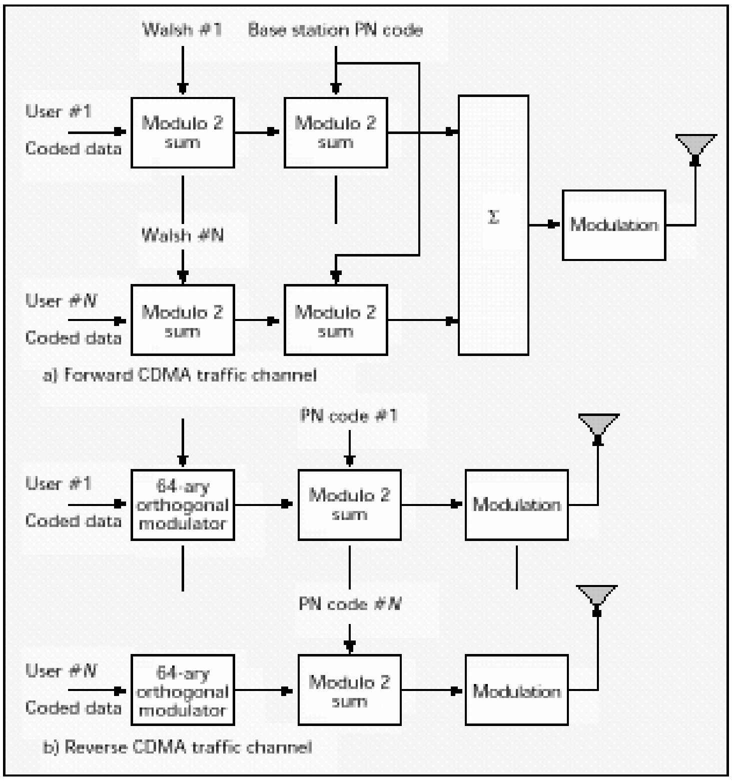


Fig. Application of Walsh functions and PN codes in the forward and reverse links of cellular CDMA