

PN-codes, PN-signals and Principles of Spread Spectrum Comms (Part-A)

Professor A. Manikas

Imperial College London

EE303 - Communication Systems
An Overview of Fundamentals

Table of Contents

1 Introduction

- 3GPP
- Definition of a SSS
- Classification of SSS
- Modelling of $b(t)$ in SSS
- Applications of Spread Spectrum Techniques
- Definition of a Jammer
- Definition of a MAI
- Processing Gain (PG)
- Equivalent EUE

2 Principles of PN-sequences

- Comments on PN-sequences Main Properties
- An Important "Trade-off"

3 m-sequences

- Shift Registers and Primitive Polynomials
- Implementation of an 'm-sequence'
- Auto-Correlation Properties
- Some Important Properties of m-sequences
- Cross-Correlation Properties and Preferred m-sequences
- A Note on m-sequences for CDMA

4 Gold Sequences

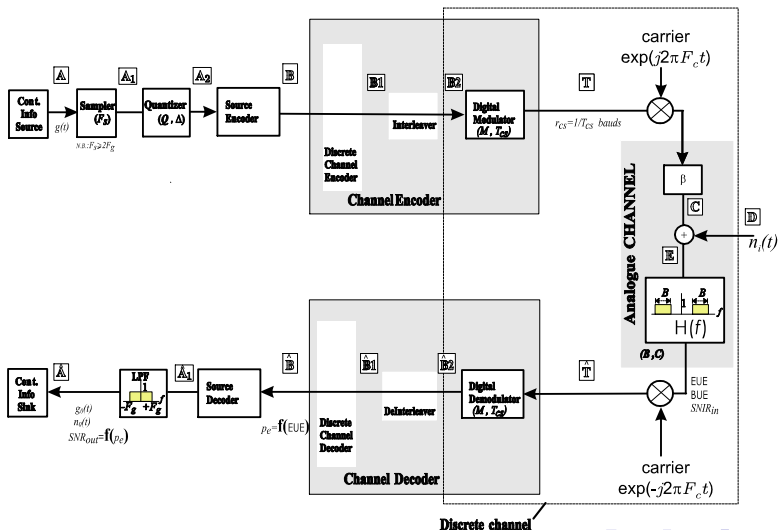
- Introductory Comments
- Auto-Correlation Properties
- Cross-Correlation Properties
- Balanced Gold Sequences

5 Appendices

- Appendix A: Properties of a Purely Random Sequence
- Appendix B: Auto and Cross Correlation functions of two PN-sequences
- Appendix C: The concept of a 'Primitive Polynomial' in GF(2)
- Appendix D: Finite Field - Basic Theory
- Appendix E: Table of Irreducible Polynomials over GF(2)

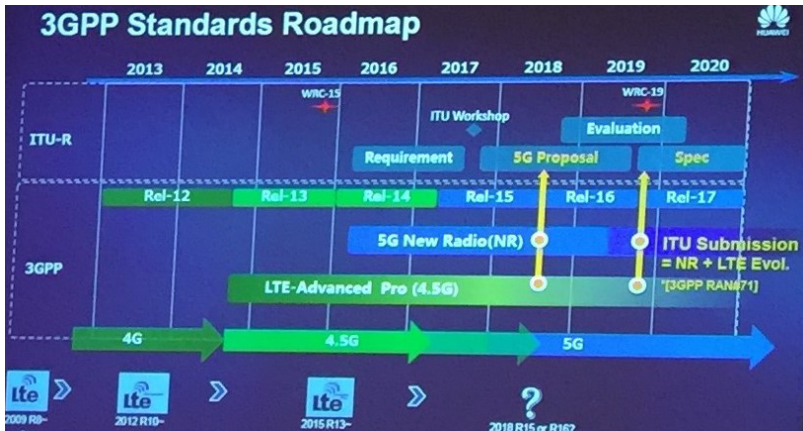
Introduction

- General Block Diagram of a Digital Comm. System (DCS)

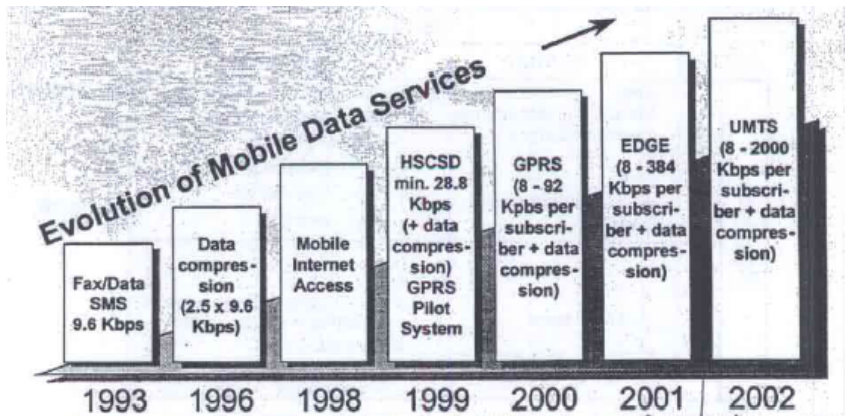


3GPP

- 3GPP is a cellular communication standard development body (3GPP \triangleq **3'd Generation Partnership Project**)
 - ▶ Found in 1998
 - ▶ Participated by over 100 companies and 1000s of communications experts
 - ▶ Globally dominant cellular standard
- 3GPP also
 - ▶ developed the 4G standards
 - ▶ is developing standards towards next generation (5G)



Pre-4G Evolution

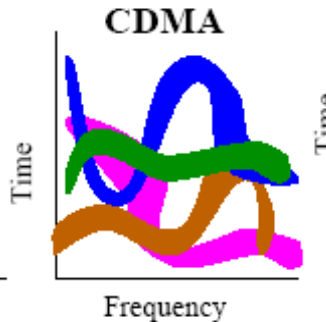
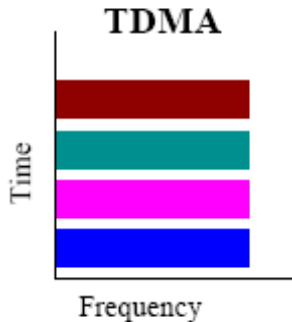
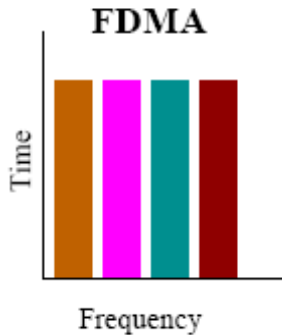


HSCDS: High Speed Circuit Switched Data

GPRS: General Packet Radio Systems (2+)

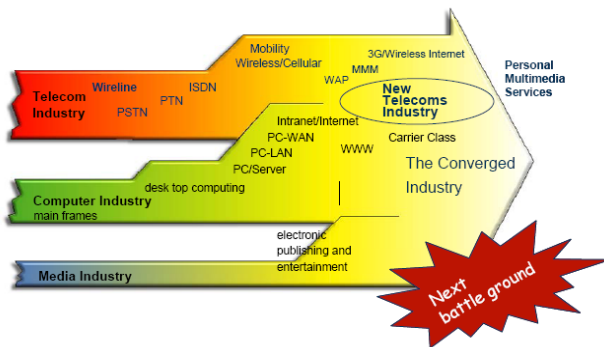
EDGE: Enhanced Data Rate GSM Evolution (2+)

UMTS: Universal Mobile Telecommunication Systems (3G)



Note: CDMA \in Spread Spectrum Comms

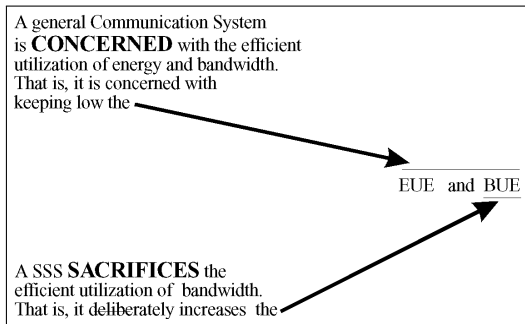
- Industry Transformation and Convergence [from Ericsson 2006, LZT 123 6208 R5B]



WCDMA (Wideband CDMA) is a 3G mobile comm system. It is a wireless system where the telecommunications, computing and **media** industry converge and is based on a Layered Architecture design. (Note: CDMA Systems \in the class of SSS).

Definition of a SSS

- When a DCS becomes a Spread Spectrum System (SSS)



- LEMMA-1: $CS \triangleq SSS$
 - $B_{SS} \gg \text{message bandwidth (i.e. BUE=large)}$
- iff $\left\{ \begin{array}{l} \circ B_{SS} \neq f\{\text{message}\} \\ \circ \text{spread is achieved by means of a code which is } \neq f\{\text{message}\} \end{array} \right.$
 - where B_{SS} =transmitted SS signal bandwidth
- our AIM: ways of accomplishing LEMMA-1.

- NB:

- ▶ PCM, FM, etc spread the signal bandwidth but do not satisfy the conditions to be called SSS

- ▶ $B_{\text{transmitted-signal}} \gg B_{\text{message}}$

⇒ SSS distributes the transmitted energy over a wide bandwidth

⇒ SNIR at the receiver input is LOW.

Nevertheless, the receiver is capable of operating successfully because the transmitted signal has distinct characteristics relative to the noise

The diagram illustrates a SSMA-SSB communication system. The transmitter (top) takes 'bits' as input, processes them through a 'Digital Mod. (M, T_{CD})' block, and then an 'SS Mod.' block. A 'PN-generator' block provides a sequence $\{\alpha[k]\}$ to the 'SS Mod.' block, which outputs $b(t)$. The signal $b(t)$ is multiplied by a carrier $\exp(j2\pi F_c t)$ to produce $r_c = 1/T_c$ bauds. The signal then passes through a 'CHANNEL' block containing a β block, a C block, and an addition node. The channel also adds noise $n(t)$ and a jammer $j(t)$. The signal then passes through a B_{ss} block. The receiver (bottom) takes the signal from the channel, multiplies it by a carrier $\exp(-j2\pi F_c t)$, and then passes it through an 'SS Demod' block. A 'PN-generator' block provides a sequence $\{\alpha[k]\}$ to the 'SS Demod' block, which outputs $b(t)$. The signal $b(t)$ is then processed by a 'Digital Demod. (M, T_{CD})' block to produce the final 'bits'.

The diagram illustrates a multi-carrier communication system. The transmitter (top) takes 'bits' as input and processes them through a 'Digital Modul. (M, T_{cs})' block, followed by a delay block T and an 'SS Mod.' block. A 'PN-generator' block provides a sequence $\{\alpha[k]\}$ to the 'SS Mod.' block, which outputs $b(t)$. This signal is then multiplied by a carrier $\exp(j2\pi F_c t)$ in a multiplier block. The resulting signal passes through a delay block T and is transmitted over a channel with rate $r_c = 1/T_c$ bauds. The channel is represented by a block β and a delay block C . The received signal is then processed by a multiplier block with a carrier $\exp(-j2\pi F_c t)$. The output passes through a delay block T and is then processed by an 'SS Demod' block, which also receives $b(t)$ from a 'PN-generator' block. The final output is 'bits'.

Key components and labels include:

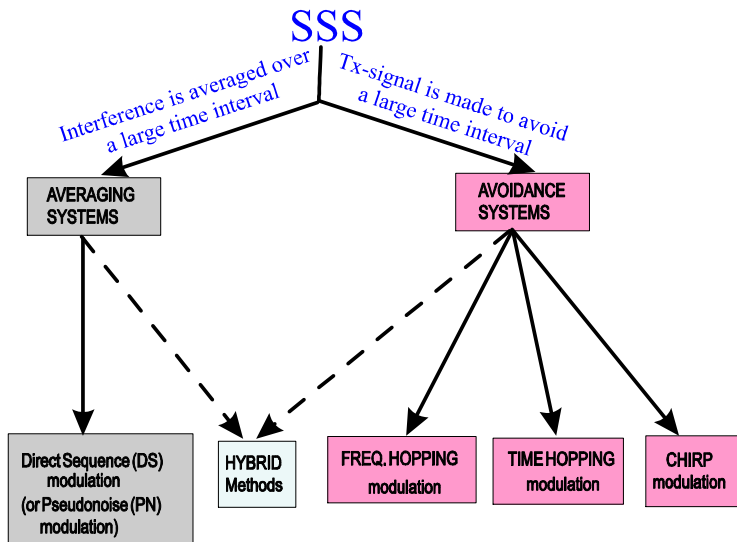
- Transmitter:** Digital Modul. (M, T_{cs}), SS Mod., PN-generator ($\{\alpha[k]\}$), carrier $\exp(j2\pi F_c t)$.
- Channel:** Block β , delay block C , noise $n_i(t)$, MAI (Multiple Access Interference).
- Receiver:** SS Demod, PN-generator ($\{\alpha[k]\}$), carrier $\exp(-j2\pi F_c t)$.
- Parameters:** $r_c = 1/T_c$ bauds, β PG, EUE $_{\text{opt}}$, BUE, SNIR $_{\text{in}}$.

- The PN signal $b(t)$ is a function of a PN sequence of ± 1 's $\{\alpha[n]\}$
 - ▶ The sequences $\{\alpha[n]\}$ must be agreed upon in advance by Tx and Rx and they have status of password.
 - ▶ This implies that :
 - ★ knowledge of $\{\alpha[n]\} \Rightarrow$ demodulation = possible
 - ★ without knowledge of $\{\alpha[n]\} \Rightarrow$ demod. = very difficult
 - ▶ If $\{\alpha[n]\}$ (i.e. “password”) is purely random, with no mathematical structure, then
 - ★ without knowledge of $\{\alpha[n]\} \Rightarrow$ demodulation = impossible
 - ▶ However all practical random sequences have some periodic structure.
This means:

$$\alpha[n] = \alpha[n + N_c] \quad (1)$$

where N_c = period of sequence
i.e. pseudo-random sequence (PN-sequence)

Classification of SSS



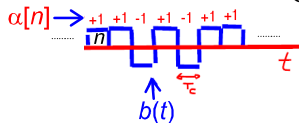
Modelling of $b(t)$ in SSS

- DS-SSS (Examples: DS-BPSK, DS-QPSK):

$$b(t) = \sum_n \alpha[n] \cdot c(t - nT_c) \quad (2)$$

where $\{\alpha[n]\}$ is a sequence of ± 1 's;

$c(t)$ is an energy signal of duration $T_c = \text{rect}\left\{\frac{t}{T_c}\right\}$



- FH-SSS (Examples: FH-FSK)

$$b(t) = \sum_n \exp \{j(2\pi k[n] F_1 t + \phi[n])\} \cdot c(t - nT_c) \quad (3)$$

where $\{k[n]\}$ is a sequence of integers such that $\{\alpha[n]\} \mapsto \{k[n]\}$
and $\{\alpha[n]\}$ is a sequence of ± 1 's;

$c(t)$ is an energy signal of duration T_c

and with $\phi[n] = \text{random}$: $\text{pdf}_{\phi[n]} = \frac{1}{2\pi} \text{rect}\left\{\frac{\phi}{2\pi}\right\}$

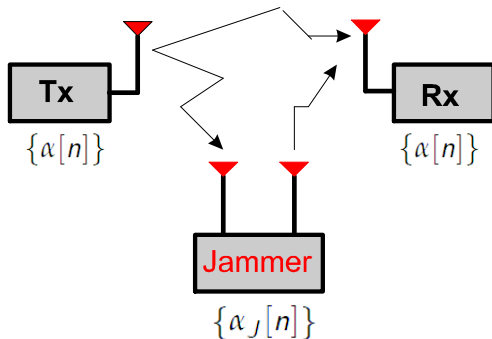
Applications of Spread Spectrum Techniques

- ① Interference Rejection: to achieve interference rejection due to:
 - ▶ Jamming (hostile interference). N.B.: protection against cochannel interference is usually called anti-jamming (AJ)
 - ▶ Other users (Multiple Access Interference - MAI): Spectrum shared by “coordinated “ users.
 - ▶ Multipath: Self-Jamming by delayed signal
- ② Energy Density Reduction (or Low Probability of Intercept LPI). LPI' main objectives:
 - ▶ to meet international allocations regulations
 - ▶ to reduce (minimize) the detectability of a transmitted signal by someone who uses **spectral analysis**
 - ▶ privacy in the presence of other listeners
- ③ Range or Time Delay Estimation

NB: interference rejection = most important application

- Jamming source, or, simply Jammer is defined as follows:

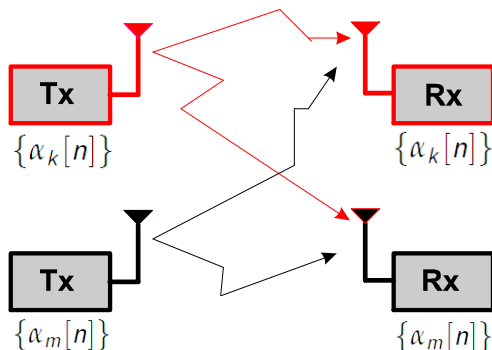
Jammer \triangleq intentional (hostile) interference



- ★ the jammer has full knowledge of SSS design except the jammer does not have the key to the PN-sequence generator,
- ★ i.e. the jammer may have full knowledge of the SSSystem but it does know the PN sequence used.

- Multiple Access Interference (MAI) is defined as follows:

$$\text{MAI} \triangleq \text{unintentional interference}$$



- PG: is a measure of the interference rejection capabilities
- definition:

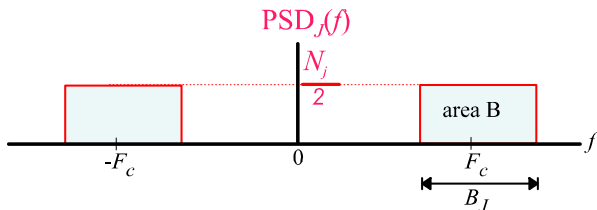
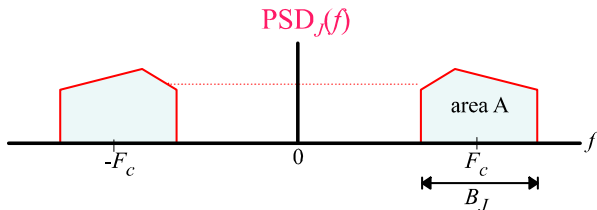
$$\text{PG} \triangleq \frac{B_{ss}}{B} = \frac{1/T_c}{1/T_{cs}} = \frac{T_{cs}}{T_c} \quad (4)$$

where B =bandwidth of the conventional system

- PG is also known as "spreading factor" (SF)
- PG = very important in DS-SSS
- PG \neq very important in FH-SSS

- Remember:

- ★ Jamming source, or, simply Jammer = intentional interference
- ★ Interfering source = unintentional interference



- ★ With $\boxed{\text{area-B} = \text{area-A}}$ we can find N_j
- ★ $P_j = 2 \times \text{area A} = 2 \times \text{area B} = N_j B_J \Rightarrow N_j = \frac{P_j}{B_J}$

- if

$$B_J = qB_{ss}; \quad 0 < q \leq 1 \quad (5)$$

then

$$\text{EUE}_J = \frac{E_b}{N_J} = \frac{P_s \cdot B_J}{P_J \cdot r_b} = \frac{P_s \cdot q \cdot B_{ss}}{P_J \cdot B} = \text{PG} \times \text{SJR}_{in} \times q \quad (6)$$

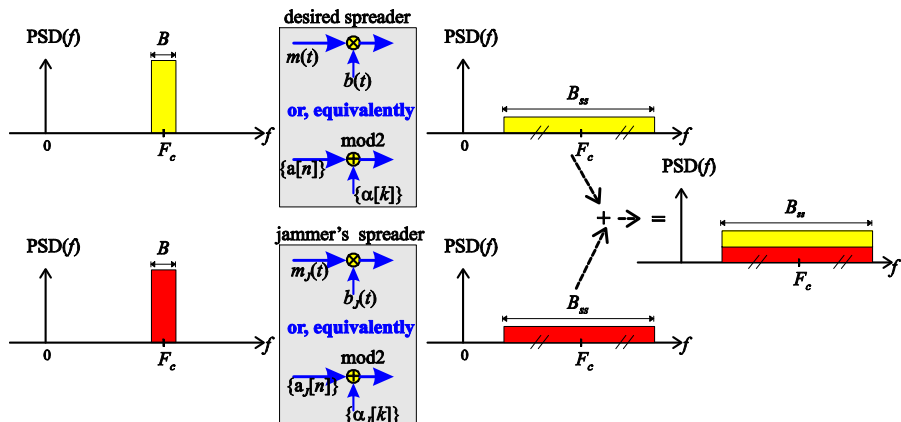
$$\text{EUE}_{equ} = \frac{E_b}{N_0 + N_J} \quad (7)$$

$$= \text{PG} \times \text{SJR}_{in} \times q \times \left(\frac{N_0}{N_J} + 1 \right)^{-1} \quad (8)$$

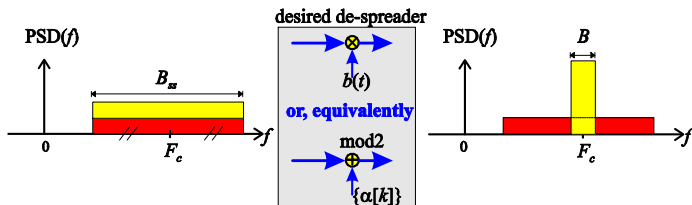
where

$$\text{SJR}_{in} \triangleq \frac{P_s}{P_J} \quad (9)$$

- SS Transmission in the presence of a Jammer (or MAI)



- SS Reception in the presence of a Jammer (or MAI)



- PN-codes (or PN-sequences, or spreading codes) are sequences of +1s and -1s (or 1s and 0s) having special correlation properties which are used to distinguish a number of signals occupying the same bandwidth.
- Five Properties of Good PN-sequences:

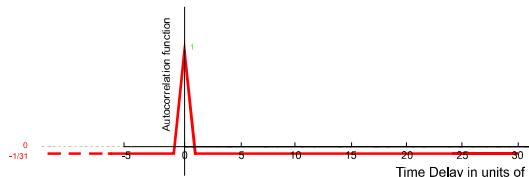
Property-1	easy to generate
Property-2	randomness
Property-3	long periods
Property-4	impulse-like auto-correlation functions
Property-5	low cross-correlation

Comments on PN-sequences Main Properties

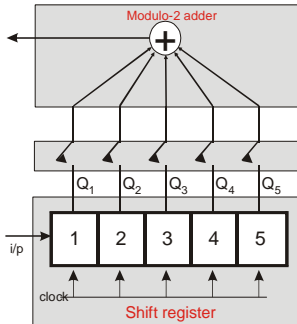
- Comments on Properties 1, 2 & 3
 - ▶ Property-1 is easily achieved with the generation of PN sequences by means of shift registers, while
 - ▶ Property-2 & Property-3 are achieved by appropriately selecting the feedback connections of the shift registers.

• Comments on Property-4

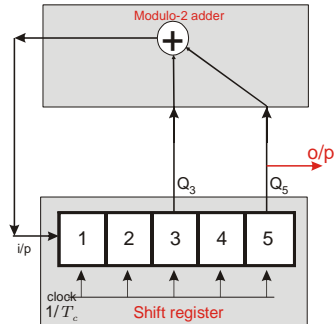
- ▶ to combat multipath, consecutive bits of the code sequences should be uncorrelated.
i.e. code sequences should have impulse-like autocorrelation functions.
Therefore it is desired that the auto-correlation of a PN-sequence is made as small as possible.
- ▶ The success of any spread spectrum system relies on certain requirements for PN-codes. Two of these requirements are:
 - 1 the autocorrelation peak must be sharp and large (maximal) upon synchronisation (i.e. for time shift equal to zero)
 - 2 the autocorrelation must be minimal (very close to zero) for any time shift different than zero.
- ▶ A code that meets the requirements (1) and (2) above is the m-sequence which is ideal for handling multipath channels.



- ▶ The figure below shows a shift register of 5 stages together with a modulo-2 adder. By connecting the stages according to the coefficients of the polynomial $D^5 + D^2 + 1$ an m-sequence of length 31 is generated (output from Q5). The autocorrelation function of this m-sequence signal is shown in the previous page



(a)



(b)

- Comments on Property-5

- ▶ If there are a number of PN-sequences

$$\{\alpha_1[k]\}, \{\alpha_2[k]\}, \dots, \{\alpha_K[k]\} \quad (10)$$

then if these code sequences are not totally uncorrelated, there is always an interference component at the output of the receiver which is proportional to the cross-correlation between different code sequences.

- ▶ Therefore it is desired that this cross-correlation is made as small as possible.

An Important "Trade-off"

- There is a trade-off between Properties-4 and 5.
- In a CDMA communication environment there are a number of PN-sequences

$$\{\alpha_1[k]\}, \{\alpha_2[k]\}, \dots, \{\alpha_K[k]\}$$

of period N_c which are used to distinguish a number of signals occupying the same bandwidth.

- Therefore, based on these sequences, we should be able to
 - ★ combat multipath
(which implies that the auto-correlation of a PN-sequence $\{\alpha_i[k]\}$ should be made as small as possible)
 - ★ remove interference from other users/signals,
(which implies that the cross-correlation should be made as small as possible).

- However

$$R_{auto}^2 + R_{cross}^2 > \text{a constant which is a function of period } N_c \quad (11)$$

i.e. there is a trade-off between the peak autocorrelation and cross-correlation parameters.

Thus, the autocorrelation and cross-correlation functions cannot be both made small simultaneously.

- The design of the code sequences should be therefore very careful.
- N.B.:
 - ▶ A code with excellent autocorrelation is the m-sequence.
 - ▶ A code that provides a trade-off between auto and cross correlation is the gold-sequence.

m-sequences - definition

- m-seq.: widely used in SSS because of their very good autocorrelation properties.
- PN code generator: is periodic
 - ▶ i.e. the sequence that is produced repeats itself after some period of time
- **Definition** : A sequence generated by a linear m -stages Feedback shift register is called a maximal length, a maximal sequence, or simply m-sequence, if its period is

$$N_c = 2^m - 1 \quad (12)$$

(which is the maximum period for the above shift register generator)

- The initial contents of the shift register are called initial conditions.

Shift Registers and Primitive Polynomials

- The period N_c depends on the feedback connections (i.e. coefficients c_i) and $N_c = \max$, i.e. $N_c = 2^m - 1$, when the characteristic polynomial

$$c(D) = c_m D^m + c_{m-1} D^{m-1} + \dots + c_1 D + c_0 \quad \text{with } c_0 = 1 \quad (13)$$

is a primitive polynomial of degree m .

$$\text{rule: if } c_i = \begin{cases} 0 \implies \text{no connection} \\ 1 \implies \text{there is connection} \end{cases} \quad (14)$$

- Definition of PRIMITIVE polynomial = very important (see Appendix C)

- Some Examples of Primitive Polynomials

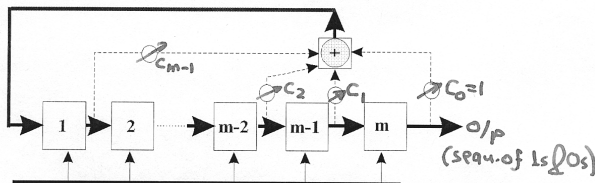
degree- m	polynomial
3	$D^3 + D + 1$
4	$D^4 + D + 1$
5	$D^5 + D^2 + 1$
6	$D^6 + D + 1$
7	$D^7 + D + 1$

- Please see Comm Systems LNs (Spread Spectrum Topic) for some tables of irreducible & primitive polynomial over GF(2).

Implementation of an m-sequence

- use a maximal length shift register
i.e. in order to construct a shift register generator for sequences of any permissible length, it is only necessary to know the coefficients of the primitive polynomial for the corresponding value of m

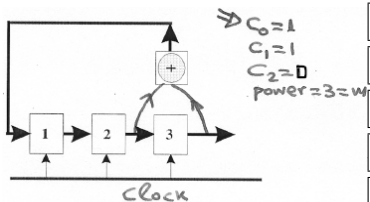
$$f_c = \frac{1}{T_c} = \text{chip-rate} = \text{clock-rate} \quad (15)$$



$$c(D) = c_m D^m + c_{m-1} D^{m-1} + \dots + c_1 D + c_0 \quad (16)$$

$$\text{with } c_0 = 1 \quad (17)$$

- Example: $c(D) = D^3 + D + 1 = \text{primitive} \implies \text{power} = m = 3$
 - coefficients = (1, 0, 1, 1) $\Rightarrow N_c = 7 = 2^m - 1$ i.e. period = $7T_c$



	1st	2nd	o/p 3rd
initial condition	1	1	1
clock pulse No.1	0	1	1
clock pulse No.2	0	0	1
clock pulse No.3	1	0	0
clock pulse No.4	0	1	0
clock pulse No.5	1	0	1
clock pulse No.6	1	1	0
clock pulse No.7	1	1	1

- Note that the sequence of 0's and 1's is transformed to a sequence of ± 1 s by using the following function

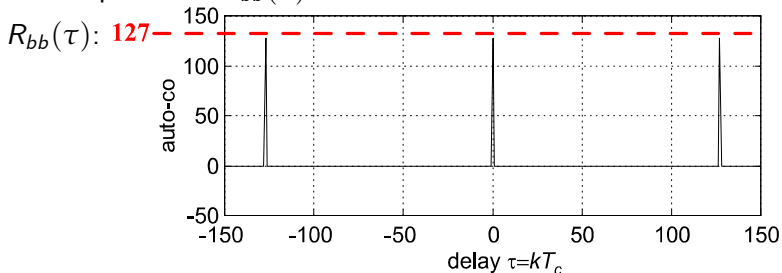
$$o/p = 1 - 2 \times i/p \quad (18)$$

Auto-Correlation Properties

- An m-seq. $\{\alpha[n]\}$ has a two valued auto-correlation function:

$$R_{\alpha\alpha}[k] = \sum_{n=1}^{N_c} \alpha[n]\alpha[n+k] = \begin{cases} N_c & k = 0 \bmod N_c \\ -1 & k \neq 0 \bmod N_c \end{cases} \quad (19)$$

- This implies that $R_{bb}(\tau)$ is also a "two-valued"



- Remember that a sequence $\{\alpha[n]\}$ of period $N_c = 2^m - 1$, generated by a linear FB shift register, is called a maximal length sequence.

Some Properties of m-sequences

- There is an appropriate balance of -1s and +1s

▶ In any period there are $\left\{ \begin{array}{ll} N_{c-} = 2^{m-1} & \text{No. of -1s} \\ N_{c+} = 2^{m-1} - 1 & \text{No. of +1s} \end{array} \right\}$
i.e.

$$\Pr(+1) \simeq \Pr(-1) \quad (20)$$

- shift-property of m-sequences:

- ▶ if $\{\alpha[n]\}$ is an m-sequence then

$$\{\alpha[n]\} + \underbrace{\{\alpha[n+m]\}}_{\text{shift by } m} = \underbrace{\{\alpha[n+k]\}}_{\text{shift by } k \neq m} \quad (21)$$

- In a complete SSS we use more than one different m-sequences
 - ▶ Thus the number of m-seq of a given length is an IMPORTANT property
 - ★ because in a CDMA system several users communicate over a common channel so that different -sequences are necessary to distinguish their signals
 - ▶ Number of m-seq of length N_c :

$$\text{No. of m-seq of length } N_c \triangleq \frac{1}{m} \Phi \{N_c\} \quad (22)$$

where

$$\begin{aligned} \Phi \{N_c\} &\triangleq \text{Euler totient function} \\ &= \text{No of (+)ve integers } < N_c \text{ and relative prime to } N_c \end{aligned} \quad (23)$$

- ▶ Note: if $N_c = p.q$ where p, q are prime numbers then

$$\Phi \{N_c\} = (p-1).(q-1) \quad (24)$$

Cross-Correlation Properties and Preferred m-sequences

- sequences of period N_c are used to distinguish two signals occupying the same bandwidth.
- A measure of interaction between these signals is their cross-correlation:

$$R_{\alpha_i \alpha_j}[k] = \sum_{n=1}^{N_c} \alpha_i[n] \alpha_j[n+k]$$

- However,
 - ▶ there exist **certain pairs of sequences** that have large peaks and noise-like behaviour in their cross-correlation
 - ▶ while others exhibit a rather smooth three valued cross-correlation.
- The latter are called **preferred sequences**.

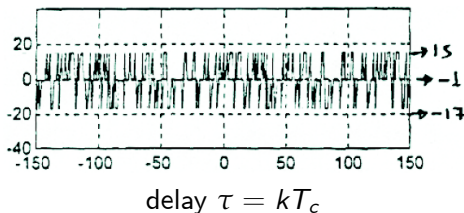
- It can be shown that the cross-correlation of **preferred sequences** takes on values from the set

$$\{-1, -R_{\text{cross}}, R_{\text{cross}} - 2\} \quad (25)$$

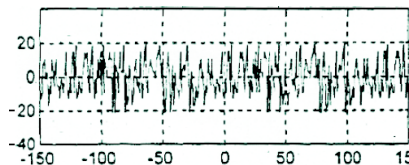
where

$$R_{\text{cross}} = \begin{cases} 2^{\frac{m+1}{2}} + 1 & m = \text{odd} \\ 2^{\frac{m+2}{2}} + 1 & m = \text{even} \end{cases} \quad (26)$$

$R_{b_i b_j}(\tau) = \text{preferred:}$



$R_{b_i b_j}(\tau) \overset{\text{non}}{\neq} \text{preferred:}$



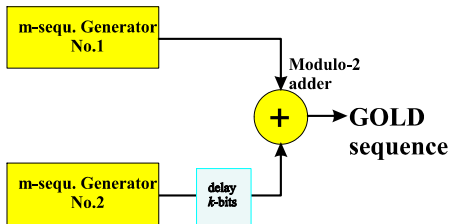
A Note on m-sequences for CDMA

- Because of the high cross-correlation between m-sequences, the interference between different users in a CDMA environment will be large.
 - ▶ Therefore, m-sequences are not suitable for CDMA applications.
- However, in a complete synchronised CDMA system, different offsets of the same m-sequence can be used by different users.
 - ▶ In this case the excellent autocorrelation properties (rather than the poor cross-correlation) are employed.
 - ▶ Unfortunately this approach cannot operate in an asynchronous environment.

Gold Sequences

- Although m -sequences possess excellent randomness (and especially autocorrelation) properties, they are not generally used for CDMA purposes as it is difficult to find a set of m -sequences with low cross-correlation for all possible pairs of sequences within the set.
- However, by slightly relaxing the conditions on the autocorrelation function, we can obtain a family of code sequences with lower cross-correlation.
- Such an encoding family can be achieved by Gold sequences or Gold codes which are generated by the modulo-2 sum of two m -sequences of equal period.

- The Gold sequence is actually obtained by the modulo-2 sum of two m -sequences with different phase shifts for the first m -sequence relative to the second.
- Since there are $N_c = 2^m - 1$ different relative phase shifts, and since we can also have the two m -sequences alone, the actual number of different Gold-sequences that can be generated by this procedure is $2^m + 1$.



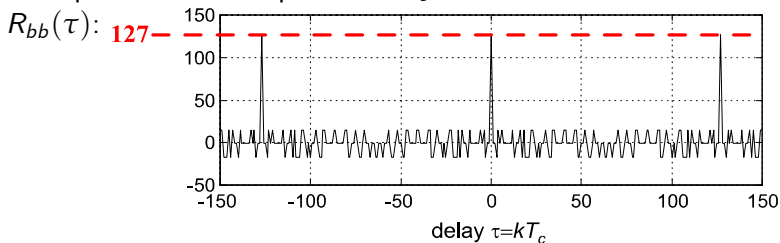
Auto-Correlation Properties

- Gold sequences, however, are not maximal length sequences.
- Therefore, their auto-correlation function **is not** the two valued one given by Equ. (19), i.e.

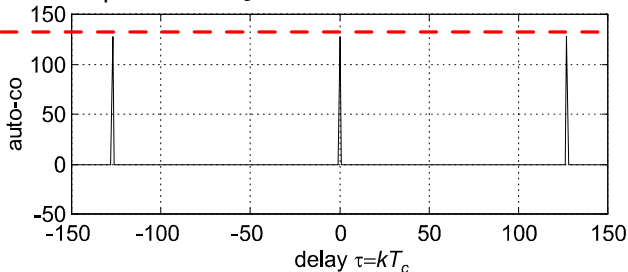
$$\{N_c, -1\} \quad (27)$$

- The auto-correlation still has the periodic peaks, but between the peaks the auto-correlation is no longer flat.

- Example of a Gold Sequence of $N_c = 127 = 2^7 - 1$



- Example of an m-sequence of $N_c = 127 = 2^7 - 1$



Cross-Correlation Properties

- Gold-sequences have the same cross-correlation characteristics as preferred m-sequences, i.e. their cross-correlation is three valued.
- Gold sequences have higher R_{auto} and lower R_{cross} than m-sequences, and the trade-off (see Equ. 11) between these parameters is thus verified.

Balanced Gold codes.

- Balanced Gold Sequence: The number of "-1s" in a code period exceed the number of "1s" by one as is the case for m-sequences.
- We should note that not all Gold codes (generated by modulo-2 addition of 2 m-sequences) are balanced, i.e. the number of "-1s" in a code period does not always exceed the number of "1s" by one.
- For example, for $m = \text{odd}$ only $2^{m-1} + 1$ code sequences of the total $2^m + 1$ are balanced, while the rest code $2^{m-1} - 1$ sequences have an excess or a deficiency of -1s.
- For $m = 7$, for instance, only 65 **balanced** Gold codes can be produced, out of a total possible of 129. Of these, 63 are non-maximal and two are maximal length sequences.
- Balanced Gold codes have more desirable spectral characteristics than non-balanced.
- Balanced Gold codes are generated by appropriately selecting the relative phases of the two original m-sequences.
- SUMMARY: By selecting any preferred pair of primitive polynomials it is easy to construct a very large set of PN-sequences (Gold-sequences). Thus, by assigning to each user one sequence from this set, the interference from other users is minimised.

Appendices

- ➊ Appendix A:
Properties of a purely random sequence
- ➋ Appendix B:
Auto and Cross Correlation functions of two PN-sequences
- ➌ Appendix C:
The concept of a 'Primitive Polynomial' in GF(2)
- ➍ Appendix D:
Finite Field - Basic Theory
- ➎ Appendix E:
Table of Irreducible Polynomials over GF(2)

