

# Unid.1 - Seqüências de Espalhamento para Sistemas DS/CDMA

4ELE012 - Comunicações Móveis II  
(CDMA)

Dr. Taufik Abrão  
Prof. Adjunto do D<sup>pto</sup> Eng. Elétrica,  
CTU, UEL - 2001

## ***Seqüências de Espalhamento***

- **Objetivo:** obtenção de boas propriedades de AC e CC, balanceamento e  $\uparrow$ Equiv. Linear (EL)\*
- **Lineares ( $\downarrow$ EL)**
  - Seqs de Máximo Comprimento, SMC
  - Gold
  - Kasami Small, Large, Very Large
- **Não Lineares** – geração mais complexa ( $\uparrow$ EL)
  - Bent
  - GMW (Gordon, Mills e Welch)
  - Kronecker

\* Menor número de stgs lineares (Reg.Desloc)  
necessários à reprodução da seqüência

# Sequências de Espalhamento Lineares

- Definição matemática – Função geradora
- Construção a partir de Registradores Deslocamento
- Propriedades Seqs. Lineares
- Conjuntos de Seqs Lineares mais utilizados
- Geração dos Conjuntos
- Correlações Periódicas e Parciais

## Sequências Lineares - Definição

- Função geradora

Sequência :  $\{a_m\} = \{a_0; a_1; a_2; \dots; a_k \dots\}$  c/  $a_0 = 1^a$  saída

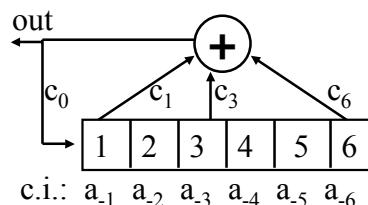
Função Geradora :  $G(x) = \sum_{k=0}^{\infty} a_k x^k$ , com  $x \in \mathbb{R}$

- Com um registrador deslocamento (SR) de  $n$  stgs:
  - estado inicial:  $\{a_i\}$ ,  $i = -n, \dots, -1$
  - realimentações do SR:  $\{c_i\}$ ,  $i = 1, \dots, n$

- Polinômio Característico:

$$f(\lambda) = \sum_{k=0}^n c_k \lambda^k = 1 + \sum_{k=1}^n c_k \lambda^k$$

$$f(\lambda) = 1 + \lambda + \lambda^3 + \lambda^6 \text{ exemplo} \rightarrow$$



c.i.:  $a_{-1} \ a_{-2} \ a_{-3} \ a_{-4} \ a_{-5} \ a_{-6}$

## Sequências Lineares - Definição

- Função geradora

$$G(x) = a_0 + a_1x + a_2x^2 + \dots = \sum_{k=0}^{\infty} a_k x^k$$

- Estado inicial do SR (**n** stgs.)

$$a_{-1}, a_{-2}, \dots, a_{-n+1}, a_{-n}$$

- Equação de Recorrência: obtenção de **a<sub>0</sub>** a **a<sub>n</sub>**

$$a_k = \sum_{i=1}^n c_i a_{k-i} \rightarrow \begin{array}{l} a_0 = c_1 a_{-1} \oplus c_2 a_{-2} \oplus \dots \oplus c_n a_{-n} \\ a_1 = c_1 a_0 \oplus c_2 a_{-1} \oplus \dots \oplus c_n a_{1-n} \\ \vdots = \vdots \qquad \qquad \qquad \vdots \qquad \qquad \qquad \vdots \\ a_n = c_1 a_{n-1} \oplus c_2 a_{n-2} \oplus \dots \oplus c_n a_0 \end{array}$$

## Sequências Lineares - Definição

- Substituindo a Eq. de Recorrência na Função Geradora, pode-se mostrar que (hipótese de  $c_0=1$ ):

$$G(x) = \frac{g(x)}{f(x)} = \frac{\sum_{i=1}^n c_i x^i (a_{-i} x^{-i} \oplus a_{-i+1} x^{-i+1} \oplus \dots \oplus a_{-1} x^{-1})}{\sum_{i=0}^n c_i x^i}$$

- **G(x)** está definido por:

- estado inicial:  $\{a_{-1}, a_{-2}, a_{-3}, \dots, a_{-n}\}$
- realimentações do SR:  $\{c_i\}, i = 1, \dots, n$
- Denominador é polinômio característico
- Caso particular: c.i.

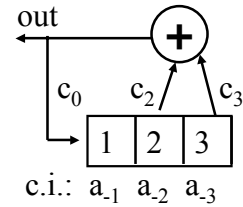
$$a_{-1} = a_{-2} = \dots = a_{-n+1} = \mathbf{0} \text{ e } a_{-n} = \mathbf{1} \Rightarrow G(x) = \frac{1}{f(x)}$$

## Sequências Lineares - Definição

- **Exemplo**

– Carga inicial: [ 0 0 1 ]

$$\Rightarrow G(x) = \frac{1}{f(x)}$$



$$f(x) = 1 + x^2 + x^3$$

- Fazendo-se **divisão longa**

$$\begin{array}{r}
 1 \\
 1 + x^2 + x^3 \\
 \hline
 x^2 + x^3 \\
 x^2 + x^4 + x^5 \\
 \hline
 x^3 + x^4 + x^5 \\
 x^3 + x^5 + x^6 \\
 \hline
 x^4 + x^6 \\
 x^4 + x^6 + x^7 \\
 \hline
 \end{array}
 \quad
 \begin{array}{r}
 1 + x^2 + x^3 \\
 \hline
 1 + x^2 + x^3 + x^4 + x^7 + x^9 + \dots \\
 G(x) = 1011100101\dots \\
 x^7 \\
 \hline
 x^7 + x^9 + x^{10} \\
 \hline
 x^9 + x^{10}
 \end{array}$$

## Sequências Lineares PROPRIEDADES

- SMC: número de taps de realimentação deve ser par
- Soma **mod2** de uma seq com qualquer defasagem da própria seq é uma outra defasagem da mesma seq.
- SMC são balanceadas:

$$\text{em um período: } \begin{cases} 2^{n-1} & \text{''uns''} \\ 2^{n-1} - 1 & \text{''zeros''} \end{cases}$$

# Sequências Lineares

## PROPRIEDADES

- SMC: há exatamente  $2^{n-(k+2)}$  bits consecutivos iguais (**blocos**) de comprimento **k**, exceto que:
  - há apenas 1 bloco contendo **n** “uns” e **n-1** “zeros”
  - Não há blocos de “zeros” de comprimento **n** ou de “uns” de comprimento **n-1**
- Usando a fórmula recursiva: 
$$a_k = \sum_{i=1}^n c_i a_{k-i}$$
  - e observando-se **apenas 2n-1** bits consecutivos da seq  $a_k \rightarrow$  RECONSTRUIR a Seq: realimentação e condições iniciais dos registradores

## Seq Lineares – PROPRIEDADES

- $\therefore$  Códigos lineares  $\rightarrow$  pouca Segurança
- Para c.i. tudo “zero”, exceto  $a_{-n}=1$ ,  $G(x) = 1/f(x)$
- Se  $\{a_m\}$  for periódica com período  $p \Rightarrow (1+x^p)$  será divisível por  $f(x)$ , c.i. = (0, 0, ..., 0, 1)
- Se  $\{a_m\}$  é de máximo comprimento  $\Rightarrow$  polinômio é irredutível (não pode ser fatorado)
- Se o polinômio característico é irredutível e de grau  $n \Rightarrow$  período da seq é fator de  $2^n-1$  e independe de  $g(x)$ , exceto no caso  $g(x)=0$ .
  - Caso  $2^n-1$  for primo  $\Rightarrow$  todo pol. irredutível de grau **n** gerará uma SMC

## Seq Lineares – PROPRIEDADES

- Para gerar SMC para todo  $n \Rightarrow$  polinômio característico deve ser **primitivo**
  - Um pol. Irreduzível de grau  $n$  é dito primitivo se e somente se o menor  $p$  para o qual  $f(x)$  divide  $(1+x^p)$  é  $p=N=2^n-1$
- se  $f_1(x)$  e  $f_2(x)$  são pol. característicos  $\Rightarrow$  qualquer seq obtida por soma mod2 das anteriores pode ser gerada por um RegDesl de pol. Caract.  $f(x) = f_1(x) \cdot f_2(x)$  com número de estágios igual à soma dos de  $f_1(x)$  e  $f_2(x)$ .
- se  $G(x) = g(x)/f(x)$  é a função geradora de uma seq  $\Rightarrow G^2(x)$  representa a seq anterior intercalada de zeros

## Seq Lineares – PROPRIEDADES

- se  $G_a(x)$  e  $G_b(x)$  representam duas seqs  $\Rightarrow$  a seq intercalada de **a** e **b** é dada por:

$$G_{a,b}(x) = \frac{f_b^2(x) g_a^2(x) + x f_a^2(x) g_b^2(x)}{f_a^2(x) f_b^2(x)}$$

- núm. de pol. primitivos, (= núm. de SMC) de grau  $n$ :

$$\lambda(n) = \frac{\varphi(2^n - 1)}{n} = \text{função de Euler}$$

$\lambda(n)$  = núm. de positivos inteiros menores que  $n$  e primos como o mesmo, calculável por:

## Seq Lineares – PROPRIEDADES

se  $m = \prod_{i=1}^k p_i^{\alpha_i}$  onde  $p_i$  é primo e  $\alpha_i$  inteiro,  $\implies$

$$\varphi(m) = \begin{cases} 1 & \text{se } m = 1 \\ \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1) & \text{se } m > 1 \end{cases}$$

- Ex.  $m=6 \implies 2^6-1 = 63 = 3^2 \cdot 7^1$  (fatores primos)
  - $\implies \varphi(63) = 2 \cdot 3^1 \cdot 6 \cdot 7^0 = 36$
  - $\therefore \lambda(6) = \varphi(63) / n = 36/6 = \mathbf{6 \text{ SMC}}$

## Seq Lineares – PROPRIEDADES

- De forma análoga ( a partir da função de Möbius) pode-se calcular o número de pol. **irredutíveis** de grau  $n$  ( $\geq$  núm pol. primitivos)
- Consultando tabela polinômios binários. Para  $n = 6$ , na notação octal:
  - [103]: 001 000 011  $\rightarrow x^6 + \quad \quad \quad + x + 1$
  - [147]: 001 100 111  $\rightarrow x^6 + x^5 + \quad \quad \quad + x^2 + x + 1$
  - [155]: 001 101 101  $\rightarrow x^6 + x^5 + \quad + x^3 + x^2 + \quad + 1$
  - [127]: 001 010 111  $\rightarrow x^6 + \quad + x^4 \quad + x^2 + x + 1$
  - [111]: 001 001 001  $\rightarrow x^6 + \quad \quad \quad + x^3 \quad \quad + 1$
  - Os 3 primeiros pol constam das tabelas de primitivos (geram SMC), os 2 últimos são irredutíveis, mas não primitivos ([127] e [111] não geram SMC.
  - Para completar a lista (9 pol. Irredutíveis)  $\implies$  pol. **Recíprocos**.

## Seq Lineares – PROPRIEDADES

- pol. **recíproco** de  $f(x)$  : gera a seq inversa da seq gerada por  $f(x)$ , dado por:

$$f^R(x) = x^n f\left(\frac{1}{x}\right)$$

- o polinômio recíproco de primitivo (irredutível) é também primitivo (irredutível)

– do ex. anterior:

$$f_{[103]}^R(x) = x^6 \left( \frac{1}{x^6} + \frac{1}{x} + 1 \right) = x^6 + x^5 + 1 \rightarrow [141]$$

– analogamente:  $[147]^R = [163]$ ;  $[155]^R = [133]$ , completando os 6 pol. Primitivos.

– completar os 9 Irredutíveis:  $[127]^R = [165]$  e  $[111]^R = [111]$ .

## Seq Lineares – PROPRIEDADES

- **Decimação k** da seq.  $\{a_m\}$  de comprimento  $p$   
 = seq  $\{c_m\}$  tal que  $c_m = a_{km}$ , para todo  $m$ 
  - Período da nova seq é dada por:  $p/\text{mdc}(p,k)$
  - escrito ainda como:  $c = a[k]$  : seq  $c$  é obtida por decimação  $k$  da seq  $a$ , com  $k$  inteiro
- Caso  $\{a_m\}$  seja SMC com  $p = 2^n - 1 \Rightarrow \{a_{km}\}$  será SMC se e somente se  $k$  e  $p$  primos entre si.
  - Todas as SMC de período  $p = 2^n - 1$  podem ser construídas por decimação de  $\{a_m\}$
- Deslocamento da seq de  $m$  posições à direita  
 $\Rightarrow x^m G(x)$  e reduzir o resultado  $\text{mod}(f(x))$ , se o grau do numerador for maior ou igual a  $n$

## Seq Lineares – PROPRIEDADES

- Deslocamento da seq de  $m$  posições à direita
  - Ex: seja função geradora:  $G(x)=1 / (1+x^4+x^5)$ , cuja seq gerada tem  $p=21$ , e dada por: **1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0** .... (repete)
  - Deslocar  $m=11$ :
    - $\Rightarrow x^{11}G(x) = x^{11} / (1+x^4+x^5)$ ,
    - reduzir o resultado  $\text{mod}(f(x)) \Rightarrow$  grau do numerador  $> n$ :

$$\begin{array}{r}
 x^{11} \\
 \hline
 x^{11} + x^{10} + x^6 \\
 \hline
 x^{10} + x^6 \\
 \hline
 x^3 + x^2 + 1
 \end{array}
 \qquad
 \begin{array}{r}
 x^5 + x^4 + 1 \\
 \hline
 x^6 + x^5 + x^4 + x^3 + x^2 + 1 \\
 \hline
 \end{array}$$

$\therefore x^{11}G(x) \text{ mod}(f(x)) = \frac{x^3 + x^2 + 1}{x^5 + x^4 + 1}$

## Seq Lineares – PROPRIEDADES

- Deslocamento da seq de  $m$  posições à direita
  - Realizando a divisão longa

$$\begin{array}{r}
 x^3 + x^2 + 1 \\
 \vdots \\
 \hline
 \end{array}
 \qquad
 \begin{array}{r}
 x^5 + x^4 + 1 \\
 \hline
 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1 \\
 \uparrow \\
 \text{Período } p = 21;
 \end{array}$$

Comparando com a anterior:

$$\begin{array}{r}
 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ \dots \text{ (repete)} \\
 \hline
 \text{10 chips} \\
 \uparrow
 \end{array}$$

## SMC, Gold e Kasami

- Construção
- Propriedades de Correlação
- Comparação

### SMC - Construção

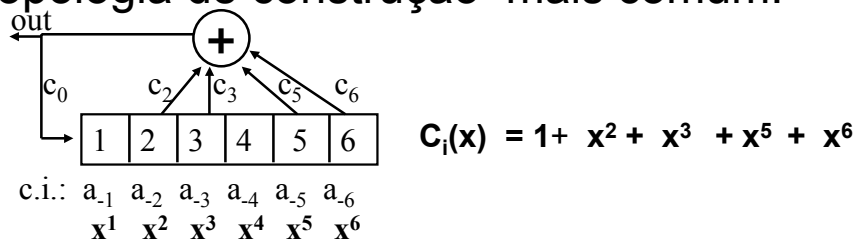
- a partir de um polinômio gerador cujos coeficientes estão restritos aos valores 0 e 1
- operações aritméticas são do tipo mod(2).
- Polinômio binário de grau  $n$  é denotado por:  $C(x) = c_n x^n + c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \dots + c_0$ , onde  $c_n = c_0 = 1$ .
  - Ex:  $x^5 + x^4 + x^2 + x + 1$  e  $x^6 + x^5 + x^3 + x^2 + 1$ ,  
 $\Rightarrow \{1,1,0,1,1,1\} = [67]_8$  e  $\{1,1,0,1,1,0,1\} = [155]_8$

## SMC - Construção (cont)

- uma seq  $\{a_i\}$  qualquer é dita gerada pelo polinômio  $C_i(x)$  se tomado qualquer segmento de tamanho  $n$  de  $\{a_i\}$  e substituído em  $C_i(x)$  resultar em zero:

$$C_i(x) = c_n x^n + c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \dots + c_0 = 0$$

- topologia de construção mais comum:



## SMC - Construção (cont)

- processo de geração
  - vantagem: muito simples
  - desvantagem: existem poucos polinômios primitivos de grau  $n$  (veja tab.)
- Tabela polinom primitivos: [Peterson, 85]
- Propriedades Adicionais para as SMC:
  - existem  $N=2^n-1$  seqs não nulas geradas por  $C(x)$ , **ciclicamente equivalentes**
  - $T^i \mathbf{b} \oplus T^j \mathbf{b} = T^k \mathbf{b}$  com  $1 \leq i, j, k \leq N$  e  $i \neq j \neq k$  inteiros (*gera a mesma seq  $\mathbf{b}$  com fase distinta*)

## Conjuntos SMC de grau n

n	$N=2^n-1$	tamanho conjunto	$ \theta_c _{\max}$	$M_n$	t(n)
3	7	2 seqs	5	2	5
4	15	2	9	0	9
5	31	6	11	3	9
6	63	6	23	2	17
7	127	18	41	6	17
8	255	16	95	0	33
9	511	48	113	2	33
10	1023	60	383	3	65
11	2047	176	267	4	65
12	4095	144	1407	0	129
13	8191	630	$\geq 703$	4	129
14	16383	756	$\geq 5631$	3	257
15	32767	1800	$\geq 2047$	2	257
16	65535	2048	$\geq 4095$	0	513

## Correlação Cruzada (CC) Periódica

$$\theta_{a,b}(\ell) = \sum_{i=0}^{N-1} a_i b_{i+\ell}, \quad \ell \in Z; \quad b_{i+\ell} \triangleq b_{[i+\ell] \bmod N}$$

- $a=b \Rightarrow$  Auto Correlação (AC) Periódica

## CC Parcial ou Aperiódica

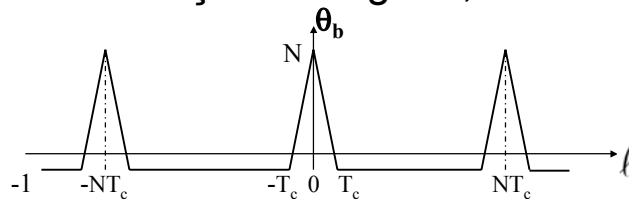
$$C_{a,b}(\ell) = \begin{cases} \sum_{i=0}^{N-1-\ell} a_i b_{i+\ell} & 0 \leq \ell < N \\ \sum_{i=-\ell}^{N-1} a_i b_{i+\ell+N} & -N \leq \ell < 0 \\ 0 & |\ell| \geq N \end{cases}$$

## SMC - Propriedades de Correlação

- Espectro de Auto-Correlação (AC)
  - para SMC polarizadas existem apenas 2 valores para a função AC Periódica:

$$\theta_b(\ell) = \begin{cases} N & \ell = 0 \\ -1 & \ell \neq 0 \end{cases}$$

- com formatação retangular, a AC será:



## SMC - Propriedades de Correlação

- Correlação Cruzada (CC) de duas SMCs distintas a e b de período  $N=2^n - 1$  assume apenas 3 valores q<sup>do</sup>:
  - $\mathbf{b = a[q]}$
  - n não é potência de 2
  - decimação  $\mathbf{q}$  admite um dos valores:  $2^{k+1}$  ou  $2^{2k} - 2^k - 1$ , sendo que:
  - $e = \text{mdc}(n,k)$  tal que  $n/e$  é ímpar
 resultando em ....

$$\theta(a, b)(\ell) = \begin{cases} -1 + 2^{\frac{n+\epsilon}{2}} & \text{ocorrendo } 2^{n-1-\epsilon} + 2^{\frac{n-2-\epsilon}{2}} \text{ vezes} \\ -1 & \text{ocorrendo } 2^n - 2^{n-\epsilon} - 1 \text{ vezes} \\ -1 - 2^{\frac{n+\epsilon}{2}} & \text{ocorrendo } 2^{n-1-\epsilon} - 2^{\frac{n-2-\epsilon}{2}} \text{ vezes} \end{cases}$$

– se  $\epsilon \uparrow \Rightarrow \theta_{a,b} \uparrow$ , porém com  $\downarrow$  freq

– se  $\epsilon \downarrow \Rightarrow \theta_{a,b} \downarrow$ , porém com  $\uparrow$  freq

• **Par Preferencial:**

– SMC a e b de mesmo grau n, não múltiplo de 4 que possuam CC com apenas os valores -1, -t(n), t(n)-2, **com**

$$t(n) = 1 + 2 \lfloor \frac{n+2}{2} \rfloor$$

• **Correlação Cruzada (CC) de duas SMCs distintas a e b de período  $N=2^n - 1$  assume apenas 4 valores  $q^{\text{do}}$  :**

–  $b = a[-1 + 2^{(2n+2)/2}] = a[-t(n)-2]$

– mesmo grau **n** e múltiplo de 4

$$\theta_{a,b}(\ell) = \begin{cases} -1 + 2^{\frac{n+2}{2}} & \text{ocorrência: } \frac{2^{n-1} + 2^{\frac{n-2}{2}}}{3} \text{ vezes} \\ -1 + 2^{\frac{n}{2}} & \text{ocorrência: } 2^{\frac{n}{2}} \text{ vezes} \\ -1 & \text{ocorrência: } 2^{n-1} + 2^{\frac{n-2}{2}} - 1 \text{ vezes} \\ -1 - 2^{\frac{n}{2}} & \text{ocorrência: } \frac{2^n + 2^{\frac{n}{2}}}{3} \text{ vezes} \end{cases}$$

se  $\epsilon > 3 \Rightarrow$  estes valores de  $\theta_{a,b}$  resultam menores que os anteriores (3 valores)

- **Polinômio Primitivo de grau 5: [45] =**  $1 \ 0 \ 1 \ 0 \ 0 \ 1$   
 $1 \ x \ x^2 \ x^3 \ x^4 \ x^5$
- Além deste, tem-se [75] e [67] e seus respectivos polinômios inversos, gerando ao todo 6 SMC.

1.  $\begin{matrix} -1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$
2.  $\begin{matrix} -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 \\ -1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{matrix}$
3.  $\begin{matrix} -1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \end{matrix}$
4.  $\begin{matrix} -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 \end{matrix}$
5.  $\begin{matrix} -1 & 1 & 1 & -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 & 1 \end{matrix}$
6.  $\begin{matrix} -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{matrix}$

- **Polinômio Primitivo de grau 5: [45] =**  $1 \ 0 \ 1 \ 0 \ 0 \ 1$   
 $1 \ x \ x^2 \ x^3 \ x^4 \ x^5$

• **Correlações Cruzadas**

- $\theta_{12} =$   $\begin{matrix} -1 & 7 & 7 & -9 & 7 & -9 & -1 & -1 & -1 & 7 & 7 & -1 & 7 & -9 & -9 & -1 \\ 7 & -1 & -9 & -1 & -1 & -1 & -1 & -9 & -1 & -1 & 7 & -1 & 7 & 7 & 7 & 7 \end{matrix}$
- $\theta_{13} =$   $\begin{matrix} -1 & -1 & -1 & -9 & -1 & -1 & -9 & -1 & 7 & -9 & -1 & -1 & 7 & 7 & 7 & -9 \\ 7 & -1 & -1 & -1 & -9 & 7 & -1 & 7 & 7 & 7 & -1 & -9 & -1 & 7 & 7 & 7 \end{matrix}$
- $\theta_{14} =$   $\begin{matrix} -1 & -1 & 7 & -1 & 7 & -1 & -9 & 7 & -1 & 7 & -1 & -1 & -1 & -1 & 7 & 7 \\ -1 & -1 & 7 & -1 & -1 & -9 & -9 & -9 & 7 & -9 & -1 & 7 & 7 & -9 & 7 & 7 \end{matrix}$
- $\theta_{15} =$   $\begin{matrix} -1 & -1 & 7 & 7 & -9 & -1 & -1 & 7 & -9 & -1 & -9 & -9 & -9 & 7 & 7 & -1 \\ 7 & -1 & -1 & -1 & 7 & -1 & -1 & 7 & -1 & 7 & -1 & -9 & 7 & -1 & 7 & 7 \end{matrix}$
- $\theta_{16} =$   $\begin{matrix} 3 & -5 & -9 & -5 & 3 & 3 & 7 & 3 & -9 & 3 & 7 & -9 & 7 & 7 & 11 & -1 \\ -1 & 3 & -1 & -5 & 3 & -9 & -1 & -5 & -5 & 3 & 3 & 3 & -9 & 7 & 7 & 7 \end{matrix}$

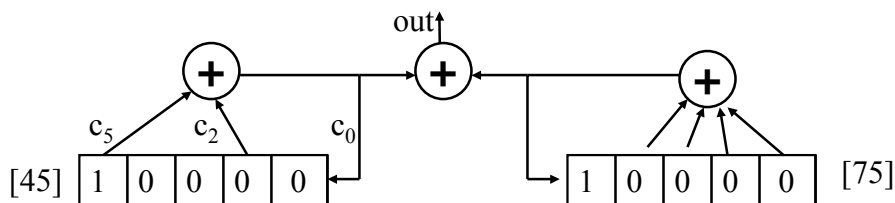
Portanto:  $\theta_{12}$  ;  $\theta_{13}$  ;  $\theta_{14}$  e  $\theta_{15}$  possuem correlações = -1, 7, -9 = -1 mod(8)

$\theta_{16}$  possui correlações = 3, -5; -9, 7; 11 = -1 mod(4)

→ pol1 e 6 são inversos

## Gold - Construção

- comprimento  $N = 2^n - 1$
- Conjunto:  $N+2$  seqs
- Construção:
  - 2 RD em paralelo, gerando SMCs, **a** e **b**
$$G(a,b) = \{a, b, a \oplus b, a \oplus T^1 b, a \oplus T^2 b, a \oplus T^3 b, \dots, a \oplus T^{N-1} b\}$$



## Gold - Propriedades

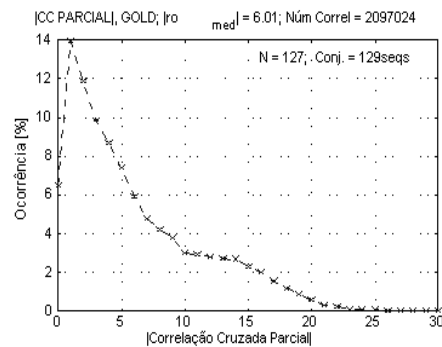
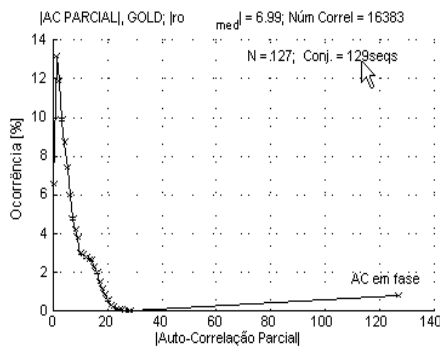
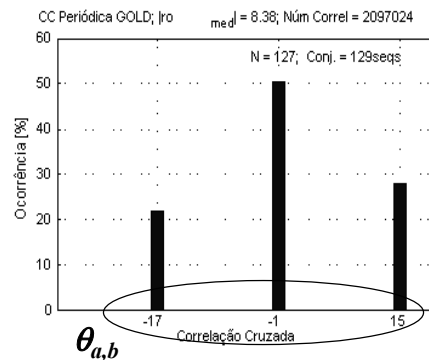
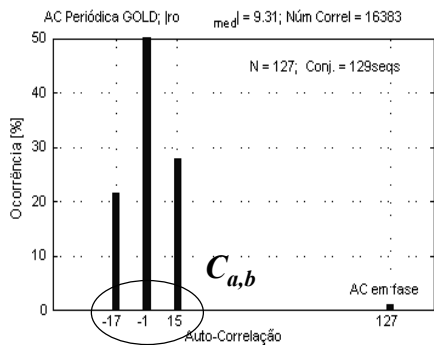
- **a** e **b** devem constituir par preferencial de SMCs
  - seqs do conjunto de Gold  $G(a,b)$  apresentam 3 valores (relativos aos pares pref.) com pico igual a  $t(n)$
- para qualquer par da família  $\Rightarrow$  picos CC e CA periódicas estão limitados aos máximos valores obtidos para  $\theta_{a,b}$ : prop. de correlação do conjunto dependem de **a** e **b**
  - $\Rightarrow$  pior caso: valores de pico semelhantes aos das SMC's

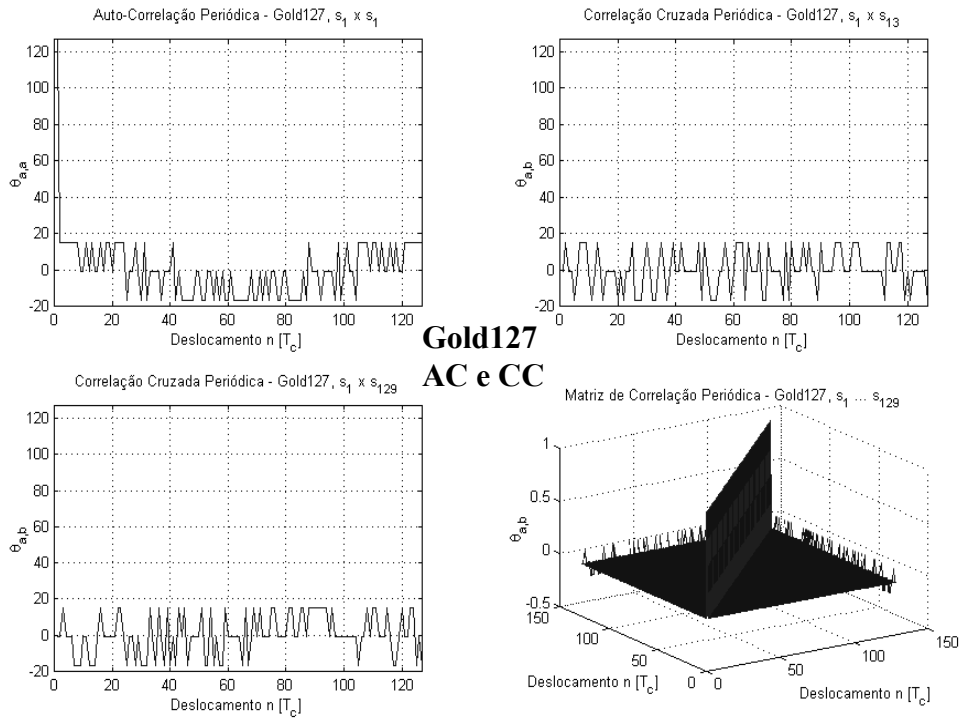
# Gold - Propriedades de Correlação

- Auto-Correlação periódica fora de fase ou Correlação Cruzada periódica:

$$\theta_{a,b}(\ell) = \begin{cases} -1 + 2^{\frac{n+1}{2}} & \text{ocorrência: 25\%} \\ 1 - 2^{\frac{n+1}{2}} & \text{ocorrência: 25\%} \\ -1 & \text{ocorrência: 50\%} \end{cases} \quad n = \text{ímpar}$$

$$\theta_{a,b}(\ell) = \begin{cases} -1 + 2^{\frac{n+2}{2}} & \text{ocorrência: 12,5\%} \\ 1 - 2^{\frac{n+2}{2}} & \text{ocorrência: 12,5\%} \\ -1 & \text{ocorrência: 75\%} \end{cases} \quad n = \text{par}$$





## *Gold – Ocorrência para CC*

Família GOLD	$m$	$Trial$	Ocorrência para os 3 valores de $\theta$ normaliz.		
(Período, $N = 2^m - 1$ ) Núm. Seqs, $K = N + 2$	ímpar	$todos \tau = KN(K - 1)$	$\left  -2^{\frac{m+1}{2}} - 1 \right  / N$ 25%	$\left  2^{\frac{m+1}{2}} - 1 \right  / N$ 25%	$ -1  / N$ 50%
Gold31	5	$todos \tau$	0,2903 18,14%	0,2258 30,24	0,0323 51,61
Gold127	7	200	0,1339 21,75%	0,1181 27,87%	0,0079 50,38%
Gold511	9	5	0,0646 23,30%	0,0607 26,54%	0,0020 50,16%
		15	0,0646 23,42%	0,0607 26,51%	0,0020 50,07%
Gold63	6 (par)	$todos \tau$	0,2698 9,23%	0,2381 15,38%	0,0159 75,40%

Tabela 4.3. Percentagens de ocorrências das correlações cruzadas para algumas famílias de Gold.

## Kasami

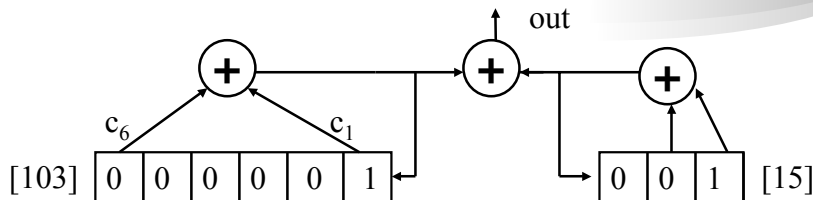
- Construção
- Propriedades de Correlação
- Comparação

### Conjunto Kasami Small

- Tamanho do Conjunto:  $m = 2^{n/2}$  seqs
  - Só existe para  $n$  par
- comprimento  $N = 2^n - 1$
- AC fora de fase ou CC periód.:  $-1; -1 \pm 2^{n/2}$
- Construção:
  - Geração a partir de uma SMC,  $\mathbf{a}$  de grau  $n$  par sobre a qual realiza-se uma decimação de ordem  $s(n) = 2^{n/2} + 1$ , resultando uma nova seq  $\mathbf{b} = \mathbf{a}[s(n)]$
  - seq  $\mathbf{b}$  é uma SMC de grau  $n/2$  e  $N = 2^{n/2} - 1$

- XOR bit a bit de a com b, para todos os deslocamentos possíveis entre as mesmas

$$K_{\text{small}}(a) = \{a, a \oplus b, a \oplus T^1 b, a \oplus T^2 b, a \oplus T^3 b, \dots, a \oplus T^{m-2} b\}$$



Vantagem  $K_{\text{small}}$ :  $|\Theta|_{\text{max}} = 2^{n/2} + 1$

- próx limite Welch =  $2^{n/2} - 1$  (valor ótimo)
- $\approx$  metade de  $|\Theta|_{\text{max}}$  para Gold

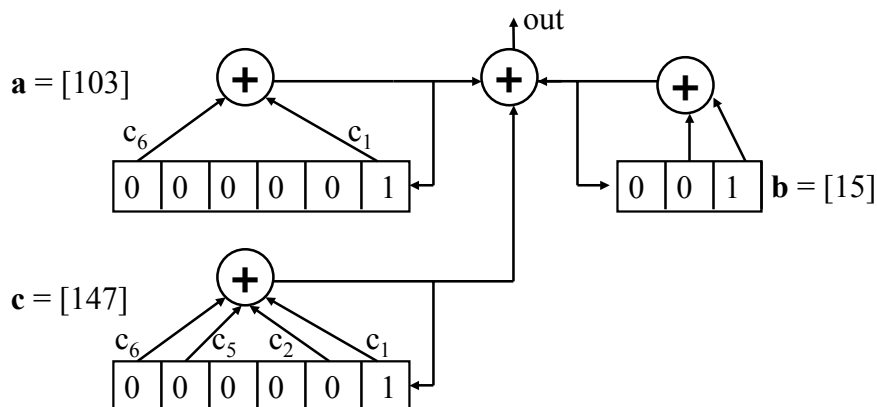
Desvantagem  $K_{\text{small}}$ : número limitado de seqs:

- bem inferior a de Gold

## Conjunto Kasami Large, $K_{\text{Large}}$

- Tamanho do Conjunto:
  - $m = 2^{n/2}(2^n + 1)$  seqs  $\rightarrow n = 2 \pmod{4}$
  - $m = 2^{n/2}(2^n + 1) - 1$  seqs  $\rightarrow n = 0 \pmod{4}$
- comprimento  $N = 2^n - 1$
- AC e CC period:  $-1$ ;  $-t(n)$ ;  $t(n) - 2$ ;  $-s(n)$ ;  $s(n) - 2$
- Construção:
  - Geração a partir de 3 seqs, **a**, **b**, **c**.
  - **a** é SMC de grau n par
  - **b** =  $a[s(n)]$ , de forma análoga ao  $K_{\text{small}}$
  - **c** =  $a[t(n)]$  : decimação  $t(n) = 1 + 2^{\lfloor \frac{n+2}{2} \rfloor}$

- $K_{\text{Large}}$  contém a família de Gold e a  $K_{\text{small}}$
- Mantém resultados similares para CC das famílias anteriores, porém com aumento significativo do número de seqs da família



## Códigos Lineares - Características

Família (Período, $N = 2^m - 1$ )	Tamanho	Valores de $\theta$	$ \theta_{Max} $	Limite $p/ \theta_{Max} $
SMC	$\ll 2^m - 1$	$\geq 3$ valores distintos	-	$N$
Gold, $m$ ímpar	$2^m + 1$	$-1; \pm 2^{\frac{m+1}{2}} - 1$	$\sqrt{2(N+1)} + 1$	$\sqrt{2N}$
Gold, $m$ par ( $\neq 0 \pmod{4}$ )	$2^m + 1$	$-1; \pm 2^{\frac{m+2}{2}} - 1$	$2\sqrt{N+1} + 1$	$2\sqrt{N}$
Kasami-S, $m$ par	$2^{\frac{m}{2}}$	$-1; \pm 2^{\frac{m}{2}} - 1$	$\sqrt{N+1} + 1$	$\sqrt{N}$ (Ótima)
Kasami-L, $m = 2 \pmod{4}$	$2^{\frac{3m}{2}} + 2^{\frac{m}{2}}$	$-1; \pm 2^{\frac{m}{2}} - 1;$	$2\sqrt{N+1} + 1$	$2\sqrt{N}$
Kasami-L, $m = 0 \pmod{4}$	$2^{\frac{3m}{2}} + 2^{\frac{m}{2}} - 1$	$\pm 2^{\lfloor \frac{m+2}{2} \rfloor} - 1$	$2\sqrt{N+1} + 1$	$2\sqrt{N}$
Kasami-VL	$2^{\frac{5m}{2}}$	-	$4\sqrt{N+1} + 1$	$4\sqrt{N}$
$S(0)$ (Quaternária)	$2^m + 1$	-	$\sqrt{N+1} + 1$	$\sqrt{N}$
$S(1)$ (Quaternária)	$\geq 2^{2m} + 2^m$	-	$2\sqrt{N+1} + 1$	$\sqrt{2, 62N}$
$S(2)$ (Quaternária)	$\geq 2^{3m} + 2^{2m}$	-	$4\sqrt{N+1} + 1$	$\sqrt{4, 35N}$

## Seqüências de BARKER

- Possíveis comprimentos:  $N=2, 3, 4, 5, 7, 11$  e  $13$ :

$$\mathbf{a} = (+1 - 1)$$

$$\mathbf{a} = (+1 + 1 - 1)$$

$$\mathbf{a} = (+1 + 1 - 1 + 1)$$

$$\mathbf{a} = (+1 + 1 + 1 - 1 + 1)$$

$$\mathbf{a} = (+1 + 1 + 1 - 1 - 1 + 1 - 1)$$

$$\mathbf{a} = (+1 + 1 + 1 - 1 - 1 - 1 + 1 - 1 - 1 + 1 - 1)$$

$$\mathbf{a} = (+1 + 1 + 1 + 1 + 1 - 1 - 1 + 1 + 1 - 1 + 1 - 1 + 1)$$

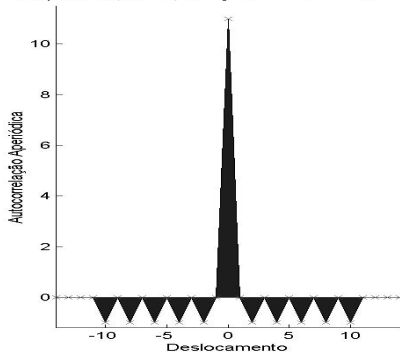
- Seqs espelhos (invertidas no tempo) também são seqs de Barker.

- Características:

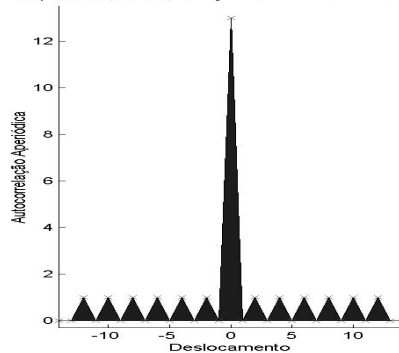
– funções de Autocorrelação Aperiódica **Quase ideais**:

$$\phi_k(n) = \begin{cases} 1 & , n = 0 \\ 0; \frac{1}{N}; -\frac{1}{N} & , 1 \leq |n| \leq N \end{cases}$$

Seq. Barker,  $N=11$ ,  $\mathbf{a} = [1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ -1 \ 1 \ -1]$



Seq. Barker,  $N=13$ ,  $\mathbf{a} = [1 \ 1 \ 1 \ 1 \ 1 \ -1 \ -1 \ 1 \ -1 \ -1 \ 1 \ -1 \ 1]$



- Seqs. Barker são mais robustas à interferência tonal (J) que as SMC → DEP mais bem distribuída no  $[-f/T_c; f/T_c]$

# Sequências de Espalhamento Ortogonais

- **Walsh-Hadamard**
- **OVSF**
- **Outros métodos de geração**
  - Silvester (utilizando W-H)
  - Gold estendida (adição 1 chip)

## Walsh-Hadamard (W-H)

- Características das seqs. W-H
  - Ortogonalidade na condição fase preferencial ( $\rho_{i,j}=0$ ),
  - Facilidade de construção.
- Construção:
  - Matrizes de Hadamard:  $\mathbf{H}_m$
  - Comprimento e Número das Seqs do conjunto W-H = número de linhas ou colunas da matriz:  $\mathbf{N} = 2^m$
  - Geração recursiva:

$$\mathbf{H}_{m+1} = \begin{bmatrix} \mathbf{H}_m & \mathbf{H}_m \\ \mathbf{H}_m & -\mathbf{H}_m \end{bmatrix},$$

onde  $\mathbf{H}_1 \in \{\pm D_1; \pm D_2; \pm D_3; \pm D_4\}$ , com

$$D_1 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix}; \quad D_2 = \begin{bmatrix} +1 & -1 \\ +1 & +1 \end{bmatrix}; \quad D_3 = \begin{bmatrix} -1 & +1 \\ +1 & +1 \end{bmatrix}; \quad D_4 = \begin{bmatrix} +1 & +1 \\ -1 & +1 \end{bmatrix};$$

- Exemplo W-H:

$$H_3 = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix}$$

- cada linha da matriz de Hadamard define um código de espalhamento ortogonal W-H.
- Desvantagem:
  - elevados valores de CC fora da fase preferencial.
  - elevados picos de AC fora da fase preferencial

### *Aplicações W-H*

- **CDMA Ortogonal** (como código de espalhamento ortogonal).
  - Cada usuário é identificado pelo código W-H;
  - Informação dos distintos usuários devem estar sincronizadas, com erro máximo de uma pequena fração de  $T_c$  (tipicamente, 10%  $T_c$ , **CDMA Quase-Síncrono**).
    - Por que (CC) ?
  - Canal com Multipercurso facilmente destrói a ortogonalidade das formas de ondas recebidas
    - Por que (AC) ?

## *Aplicações W-H*

- **Modulação Ortogonal**

- seqs W-H utilizadas para modulação da informação.
- Modul. Ortogonal  $M$ -ária, onde  $k = \log_2 M$  bits de info são utilizados na seleção de uma das  $M$  formas de onda ortogonais para a transmissão.
- Detecção do sinal: coerente ou não-coerente

- **Modulação Bi-Ortogonal**

- cada linha da matriz de Hadamard é modulada por um bit de informação; são enviados  $M$  bits simultaneamente
- requer detecção coerente.

## **OVSF**

*(Orthogonal Variable Spreading Factor)*

- Códigos ortogonais do tipo W-H estruturados em árvore;
- aplicações em multi-mídia (sistemas 3G): taxa de dados é variável (múltipla da taxa de dados básica)
  - Serviço de vídeo, com taxa de símbolos igual à máxima  $R_{\text{video}} = R_{\text{max}}$  será espalhada por uma seq. Ortogonal de comprimento  $N=2^m$ ;
  - serviço de voz com taxa  $R_{\text{voz}} = R_{\text{max}} / 2^k \Rightarrow$  espalhado por uma seq. Comprimento  $N=2^{m+k}$
  - **exemplo de geração recursiva de códigos ortogonais estruturados em árvore são os OVSF.**

# OVSF

## (Orthogonal Variable Spreading Factor)

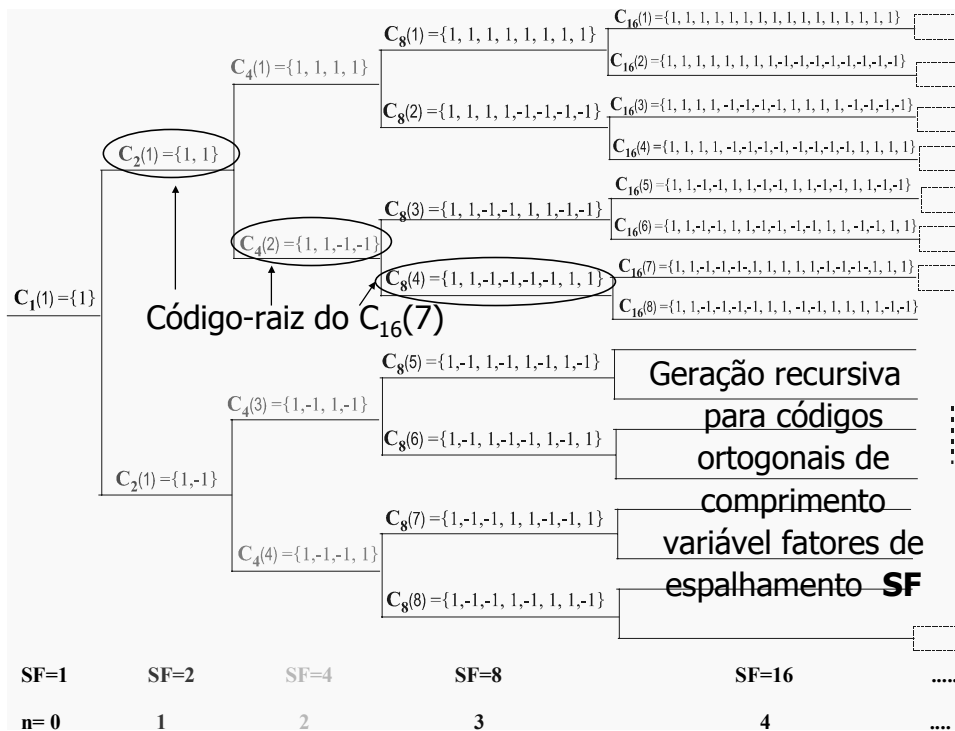
- geração recursiva de códigos OVSF:**

– Forma análoga à geração matrizes Hadamard

$$\{C_N(n)\}_{n=1,2,\dots,N}$$

$$C_N = \begin{bmatrix} C_N(1) \\ C_N(2) \\ C_N(3) \\ \vdots \\ C_N(N-1) \\ C_N(N) \end{bmatrix} = \begin{bmatrix} C_{\frac{N}{2}}(1) & \overline{C_{\frac{N}{2}}(1)} \\ C_{\frac{N}{2}}(1) & \overline{C_{\frac{N}{2}}(1)} \\ C_{\frac{N}{2}}(2) & \overline{C_{\frac{N}{2}}(2)} \\ C_{\frac{N}{2}}(2) & \overline{C_{\frac{N}{2}}(2)} \\ \vdots & \vdots \\ C_{\frac{N}{2}}(N/2) & \overline{C_{\frac{N}{2}}(N/2)} \\ C_{\frac{N}{2}}(N/2) & \overline{C_{\frac{N}{2}}(N/2)} \end{bmatrix}$$

$C_N$  = vetor linha de N elementos

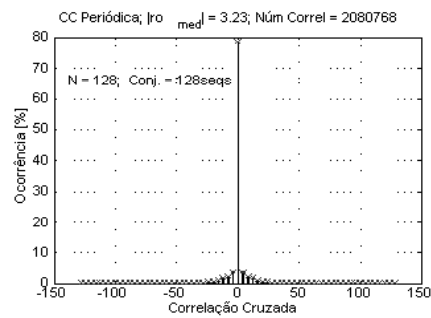
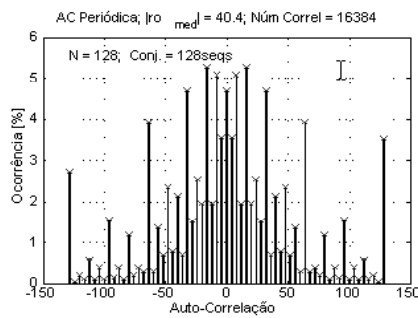
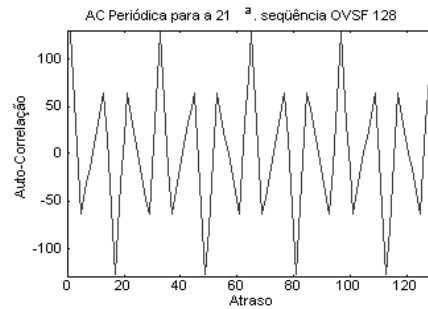
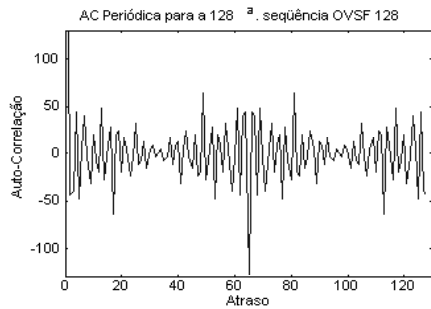


# OVSF

- Propriedades de correlação (e ortogonalidade) são similares às seqs. W-H
  - Todos os códigos OVSF gerados no **mesmo nível** = conj. W-H
    - os conj. OVSF e W-H são idênticos, diferindo apenas na ordem das seqs.
  - Quaisquer pares códigos OVSF gerados níveis distintos são ortogonais, desde que um deles não seja **código-raiz** do outro.
- Designação de códigos:
  - Um código pode ser designado se e somente se: **a)** nenhum outro pertencer ao caminho do específico código até a raiz; **b)** sub-árvore gerada por um específico código já tenha sido utilizada.
- Número total de códigos disponíveis não é fixo, depende:
  - da taxa de informação;
  - Fator de espalhamento de cada usuário físico.
- Em esquemas multitaxa (serviços multimídia):
  - Esquema MC: códigos OVSF de mesmo nível (mesmo PG)
  - Esquema MPG: OVSF de níveis distintos e inversamente proporcionais à taxa de dados.
- Utilização dos códigos ortogonais nos sistemas 2G e 3G na etapa de **canalização**:

Padrão	Canal	Canalização	Embaralhamento
IS-95	direto (sínc.)	Walsh ortogonal, $N^{chm} = 64$	<b>1º</b> espalhamento em quadratura (antes do Walsh): duas SMC de $N = 2^{15} - 1$ estendida de 1 chip, resultando em $N_{I,Q}^{scr\bar{b}} = 32.768$ chips (única seqüência para todos os usuários da mesma célula e distintos atrasos). <b>2º</b> espalhamento: seqüência SMC longa de $N_{longo}^{scr\bar{b}} = 2^{42} - 1$ chips e mascarada de forma distinta afim de identificar cada usuário.
	reverso (assínc.)	Walsh específico e de $N^{chm}$ variável.	<b>1º</b> espalhamento em quadratura: idem ao canal direto, duas PN em quadratura com $N_{I,Q}^{scr\bar{b}} = 32.768$ chips, seguido por espalhamento de um código de Walsh específico e variável. <b>2º</b> espalhamento: seqüência SMC longa mascarada de $N_{longo}^{scr\bar{b}} = 2^{42} - 1$ chips, resultando em distintos atrasos (sistema assíncrono) no receptor da ERB.
W-CDMA	direto (sínc.)	O V S F, $N^{chm} = 2^{9-k}$	seqüência Gold de $N^{scr\bar{b}} = 2^{18} - 1$ chips truncada em 10 ms, resultando única seq. PN para todos os usuários da mesma célula
	reverso (sínc./ assinc)	O V S F, $N^{chm} = 2^{8-k}$ , $k = 0, \dots, 6$	Conjunto de seqüências Kasami-VL Estendida de $N^{scr\bar{b}} = 256$ (código curto). Opcionalmente, uma seqüência Gold de $N^{scr\bar{b}} = 2^{41} - 1$ chips truncada em 10 ms, resultando única seq. PN para todos os usuários da mesma célula

## Auto-Correlação e Correlação Cruzada periódicas para duas seqüências OVSF com **SF=128**



## Conjuntos Seqüências

**NÃO-LINEARES**

## Conjuntos Seqüências NÃO-LINEARES

- Característica:
  - grande equivalente Linear (*linear span*)
  - Boas propriedades de correlação
- Famílias
  - **Bent**
    - ✓ reduzida interferência MAI (baixa CC)
    - ✓ balanceadas
  - **GMW** (Gordon, Mills e Welch):
    - ✓ Propriedades similares às SMC's
    - ✓ Definidas a partir função Traço

## Propriedade Correlação: Comparação

Parâmetro	GMW	Gold e Kasami
Auto Correlação Periódica, $\theta_a^{\theta_a}$	2 valores (idêntica à SMC)	3 valores
Correlação Cruzada Periódica, $\theta_{a,b}$	Não Uniforme Não Controlável	relativamente Uniforme e Controlável
Família de Códigos, <b>F</b>	Razoável (>>SMC)	<b>Grande</b>

## Referências Bibliográficas

1. Martinez, A. A. G. e Jeszenszky, P. J. E. **Geradores não lineares de seqüências para uso em sistemas spread spectrum**, SBT 1995.
2. Jeszenszky, P. J. E, **Teoria Básica e Aplicações das Seqüências de Códigos**. LCS, D<sup>pto</sup> Eng. Elétrica EPUSP, Out. 1998
3. Stüber, G. L. – **Principles of Mobile Communication**, 2<sup>nd</sup> Edition, Kluwer Academic Publishers, London, 2001.
4. Abrão, T. **Canceladores de Interferência Multiusuário Aplicados a Sistemas DS/CDMA de Múltipla Taxa**, Tese de Doutorado, EPUSP, São Paulo, Fev. 2001.

## Cronograma – Alterações 6 semanas (11 aulas x (3T+2P))

Unid. 1 – Seqs de Espalhamento para CDMA. **4 Fev**

Unid. 2 – Análise de MAI e Desempenho CDMA  
Convencional. **06, 08, 13 Fev**

Unid. 3 – Receptores Avançados: MuD. **15, 20, 22,**  
**27/Fev. e 01 Mar**

Unid. 4 – Esquemas Multitaxa para 3G. **06, 08, 13 Mar**

**Apresentação dos Temas: 13, 15 e/ou 20 Mar.**

## Cronograma - Alterações

- Proposta: **Desenvolvimento de um Tema** em CDMA envolvendo, necessariamente, a utilização de ferramentas matemáticas de simulação.
- Temas (possíveis)
  - Caracterização/simulação de Canal móvel
  - Aplicações com seqüências de espalhamento: ex: sistemas QS-CDMA etc.
  - Desempenho comparado de receptores CDMA.
  - Sistema OFDM (*Orthogonal Frequency Division Multiplexing*) ou CDMA Multicarrier
  - Aplicações Multimídia (Multitaxa) para 3G..... **Outros....**
- **Aulas de laboratório:** orientadas para a realização dos temas.