ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO
DEPARTAMENTO DE ENGENHARIA ELETRÔNICA
ÁREA DE COMUNICAÇÕES E SINAIS

PEE 5710-COMUNICAÇÃO POR ESPALHAMENTO ESPECTRAL (NOTAS DE AULAS SOBRE SEQÜÊNCIAS DE CÓDIGOS)

DR. PAUL JEAN ETIENNE JESZENSKY

PROFESSOR ASSOCIADO

3/94

Introdução

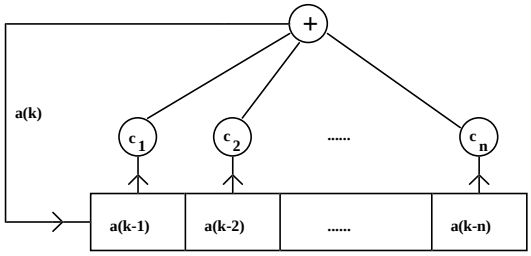
Na ref. [11] tem-se uma introdução à Técnica de Comunicação por Espalhamento Espectral, onde são apenas citadas algumas formas de geração e propriedades das seqüências de códigos mais usuais. Na ref. [4] faz-se uma revisão sobre os principais resultados conhecidos sobre seqüências de códigos. Como se trata de um paper de revisão, não há preocupações quanto ao formalismo, ou encadeamento lógico, na apresentação dos resultados. Já a ref. [8], e o presente trabalho, constituem um detalhamento de [4]. Em [8] as funções de correlação são exploradas em detalhes e a sua influência no desempemho de sistemas CDMA é avaliada. O presente trabalho, que deve preceder a ref. [8] numa primeira leitura, trata de maneira mais formal dos aspectos básicos das seqüências de códigos, utilizadas na área de Comunicação por Espalhamento Espectral. Num trabalho futuro serão detalhadas as famílias de seqüências de códigos mais usuais, como por exemplo as seqüências de máximo comprimento, Gold, Kasami, GMW, Bent, etc.

Função geradora de uma seqüência

Seja uma seqüência genérica representada por $\{a_m\}=\{a_0,a_1,a_2,...,a_k,...\}$ onde o índice denota o tempo, isto é, a primeira saída é a_0, a próxima é a_1, e assim por diante. Esta seqüência será representada por meio de uma função G(x), denominada de função geradora da seqüência, na forma: $G(x)=a_0+a_1x+a_2x^2+...+a_kx^k+....=\sum_{k=0}^{\infty} a_kx^k$; onde x é uma variável real auxiliar.

Seqüências geradas por registradores de deslocamento

Seja um registrador de deslocamentos na representação abaixo indicada.



O sinal realimentado escreve-se a partir da fórmula de recorrência $a(k)=\sum_{i=1}^{n} c_i a(k-i)$ com $k \geq n$ e $c_n=1$ sempre (caso contrário o grau não seria n). Define-se como polinômio característico para este tipo de montagem à $f(\lambda)=\sum_{k=0}^{n} c_k\lambda^k$ com $c_o=1$. Observe-se então que o polinômio característico descreve a implementação física do gerador (suas realimentações) e não o seu estado. O estado inicial é definido pelo conteúdo dos RD's para k=0: $a_{-1},a_{-2},...,a_{-n+1},a_{-n}$.

Escrevendo a_0 até a_n pela fórmula de recorrência, tem-se um sistema de equações seqüenciais que permite determinar estes estados futuros a partir da condição inicial.

$$\begin{aligned} a_0 &= c_1 a_{-1} + c_2 a_{-2} + \ldots\ldots + c_n a_{-n} \\ a_1 &= c_1 a_0 + c_2 a_{-1} + \ldots\ldots + c_n a_{-n+1} \\ &\vdots \\ a_n &= c_1 a_{n-1} + c_2 a_{n-2} + \ldots\ldots + c_n a_0 \end{aligned}$$

A expressão da função geradora, por sua vez, é calculável por:

$$G(x) = \sum_{k=0}^{\infty} a_k x^k = \sum_{k=0}^{\infty} \sum_{i=1}^{n} c_i a_{k-i} x^k = \sum_{i=1}^{n} c_i x^i \sum_{k=0}^{\infty} a_{k-i} x^{k-i}$$

$$= \sum_{i=1}^{n} c_i x^i (a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \ldots + a_{-1} x^{-1} + \sum_{k=i}^{\infty} a_{k-i} x^{k-i})$$

$$= \sum_{i=1}^{n} c_i x^i (a_{-i} x^{-i} + a_{-i+1} x^{-i+1} + \ldots + a_{-1} x^{-1} + G(x)); \text{ e isolando } G(x)$$

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

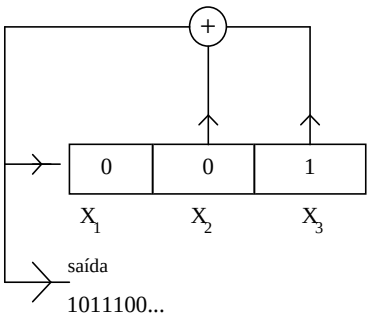
O numerador g(x) da função geradora é assim determinado pelas realimentações (c_i) e pelo estado inicial $a_{-1}, a_{-2}, \ldots, a_{-n+1}, a_{-n}$, enquanto o denominador é o próprio polinômio característico. No caso particular das condições iniciais serem $a_{-1}=a_{-2}=\ldots=a_{-n+1}=0$ e $a_{-n}=1$, lembrando que $c_n=1$ sempre, resulta $G(x)=\frac{1}{f(x)}$.

Seja um exemplo nestas condições:

$n=3; c_1=0$ e $c_2=c_3=1$ e $\therefore f(x)=1+x^2+x^3$; carga inicial [001]. A divisão longa fornece:

$G(x)=1+x^2+x^3+x^4+x^7+x^9+\cdots$ (verifique); e assim a seqüência é dada por [1011100⋯]

e tem período $2^n-1=2^3-1=7$.



X_1	X_2	X_3	t
0	0	1	-1
1	0	0	0
0	1	0	1
1	0	1	2
1	1	0	3
1	1	1	4
0	1	1	5
0	0	1	6

Teorema 1

A sucessão de estados em um registrador de deslocamentos é periódica com período $p \le 2^n - 1$, onde n é o número de estágios do registrador. A verificação é imediata.

Teorema 2

Se a seqüência $A = \{a_n\}$, gerada por um registrador de deslocamentos (RD), obedece a condição inicial: $a_{-1} = a_{-2} = ... = a_{1-n} = 0$ e $a_{-n} = 1$, então o período de A é o menor inteiro positivo p para o qual o polinômio característico f(x) divide $(1+x^p) \bmod 2$.

Demonstração: nas condições indicadas tem-se $G(x) = \frac{1}{f(x)} = \sum_{n=0}^{\infty} a_n x^n$

- se A tem período p então:

$$\frac{1}{f(x)} = (a_0 + a_1 x + ... + a_{p-1}x^{p-1}) + x^p(a_0 + a_1 x + ... + a_{p-1}x^{p-1}) + x^{2p}(a_0 + a_1 x + ... + a_{p-1}x^{p-1}) + ...$$

$$= (a_0 + a_1 x + ... + a_{p-1}x^{p-1})(1 + x^p + x^{2p} + ...) = \frac{a_0 + a_1 x + ... + a_{p-1}x^{p-1}}{(1 + x^p)}$$

$$\Rightarrow \frac{(1 + x^p)}{f(x)} = a_0 + a_1 x + ... + a_{p-1}x^{p-1} \text{ indicando que } f(x) \text{ divide } (1 + x^p)$$

- inversamente se f(x) divide $(1 + x^p)$ seja este quociente indicado por:

$\frac{(1 + x^p)}{f(x)} = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_{p-1}x^{p-1}$. Nestas condições tem-se:

$$\frac{1}{f(x)} = (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_{p-1}x^{p-1}) + x^p(\alpha_0 + \alpha_1 x + \alpha_2 x^2 + ... + \alpha_{p-1}x^{p-1}) + ...$$

$= G(x) = \sum_{n=0}^{\infty} a_n x^n$; e igualando as potências idênticas de $x \Rightarrow \{a_n\} = \{\alpha_n\}$. Assim o período de A é p, ou um fator deste. Ou, de outra forma, o período de A é o menor p positivo para o qual f(x) divide $(1 + x^p)$.

Corolário

Seja a função geradora $G(x) = \frac{g(x)}{f(x)}$, onde o numerador g(x) tem grau menor do que o de f(x) (na expressão geral de G(x) verifica-se que o grau de f(x) é n e o de g(x) é ≤n-1). Se g(x) não tem fatores em comum com f(x) o teorema anterior continua válido, e o menor p tal que f(x) divide $(1+x^p)$, denominado de expoente de f(x), é o período da seqüência correspondente. O caso g(x)=1 corresponde ao teorema demonstrado. Outro caso importante é quando f(x) é irredutível, caso em que não há fatores em comum com g(x), exceto quando g(x)=0, que corresponde ao caso de condições iniciais nulas. Assim quando f(x) é irredutível o período da seqüência gerada pelos RD's não depende das condições iniciais, exceto na condição inicial identicamente nula (caso trivial em que permanece no mesmo estado indefinidamente).

Por definição uma seqüência é dita de máximo comprimento (SMC), na forma gerada por n RD's, quando seu período for $p=2^n-1$.

Notas sobre a extensão do corpo binário GF(2) para um corpo GF(2^n), com n>1; ref. [1], [6] e [9]

- o corpo GF(2^n) tem 2^n elementos;

- considere-se todos os polinômios de grau (n-1) sobre GF(2). Existem 2^n destes polinômios, de forma que cada um deles pode ser usado para representar um elemento simples do corpo de extensão GF(2^n). Por exemplo, para n=2 o corpo de extensão tem 4 elementos, e existem 4 polinômios de grau (n-1)=1, que são: 0; 1; D; D+1. Escritos numa forma genérica: $\alpha_1 D + \alpha_2$ com $\alpha_i \in GF(2) = \{0;1\}$;

- a adição é na forma usual (a operação é mod2, é fechada,..., etc);

- a multiplicação é definida usando-se polinômios especiais de grau n, denominados de polinômios primitivos. Um polinômio h(D) de grau n é dito primitivo se o menor inteiro p para o qual h(D) divide (D^p+1) é $p=2^n-1$. Polinômios primitivos são irredutíveis, isto é, não podem ser fatorados. O produto de dois elementos de GF(2^n) é definido como o resto da divisão do produto convencional pelo polinômio primitivo escolhido para definir a multiplicação. A multiplicação é referida como multiplicação módulo h(D) e escreve-se modh(D).
Observação: o produto convencional é de grau ≤(2n-2); quando dividido por um polinômio de grau n, o resto será de grau ≤ (n-1) e assim será um elemento de GF(2^n) ⇒o produto é uma operação fechada.

Seja uma tabela construida a partir do elemento 1, em que cada elemento sucessivo é obtido multiplicando o anterior por Dmodh(D).

$1; D; D^2; \ldots.$ quando se chegar a D^{n-1} o próximo será D^n e este é calculável por :

resto da divisao de D^n por $h(D) = D^n + h_{n-1}D^{n-1} + h_{n-2}D^{n-2} + \ldots + h_1 D + 1.$ É fácil

verificar que o quociente é 1 e o resto é dado por $(h_{n-1}D^{n-1} + h_{n-2}D^{n-2} + \ldots + h_1 D + 1)$

e assim pode-se escrever : $D^n = (h_{n-1}D^{n-1} + h_{n-2}D^{n-2} + \ldots + h_1 D + 1) \bmod h(D)$

Assim, seja um exemplo com $h(D)=D^4+D+1 \Rightarrow D^4=(D+1) \bmod h(D)$

D^i	$D^i \bmod h(D) = \alpha_1 D^3+\alpha_2 D^2+\alpha_3 D+\alpha_4$; c / $\alpha_i \in GF(2)$	α_i
D^0	1	0001
D^1	D	0010
D^2	D^2	0100
D^3	D^3	1000
D^4	$D^4 = D+1$	0011
D^5	D^2+D	0110
D^6	D^3+D^2	1100
D^7	$D^4+D^3=D^3+D+1$	1011
D^8	$D^4+D^2+D=D^2+D+D+1=D^2+1$	0101
D^9	D^3+D	1010
D^{10}	$D^4+D^2=D^2+D+1$	0111
D^{11}	D^3+D^2+D	1110
D^{12}	$D^4+D^3+D^2=D^3+D^2+D+1$	1111
D^{13}	$D^4+D^3+D^2+D=D^3+D^2+D+D+1=D^3+D^2+1$	1101
D^{14}	$D^4+D^3+D=D^3+D+D+1=D^3+1$	1001
D^{15}	$D^4+D=D+D+1=1$	0001 (igual à D^0)

- Os 15 polinômios anteriores mais 0000 constituem os elementos de GF(16)=GF(2^4);

- Como, por definição, um polinômio primitivo divide ($D^{2^n-1}+1$), pode-se escrever: $D^{2^n-1}+1 = q(D)h(D) \Rightarrow D^{2^n-1} = q(D)h(D)+1$ e portanto o resto da divisão de D^{2^n-1} por h(D) é 1. Assim de uma forma geral pode-se escrever que: $D^{2^n-1} = 1 \bmod h(D)$, conforme já foi verificado na tabela anterior;

- O inverso de um elemento D^j é $(D^j)^{-1}=D^{2^n-1-j}$ pois $D^{2^n-1-j}D^j=D^{2^n-1}=1$;

- Se α é raiz de h(D), primitivo com coeficientes em GF(2), então o conjunto de raizes de h(D) é $\{\alpha^{2^i}\}$ i= 0;1;2;...;n−1. Isto é, as n raízes são dadas por $\{\alpha;\alpha^2;\alpha^4;....\alpha^{2^{n-1}}\}$.
De fato, se α é raíz de h(D) $\Rightarrow \alpha^n+h_{n-1}\alpha^{n-1}+.....+h_1\alpha+1=0$; elevando ao quadrado:
$\alpha^{2n}+h_{n-1}\alpha^{2(n-1)}+.....+h_1\alpha^2+1=h(\alpha^2)=0$ e assim sucessivamente até $\alpha^{2^{n-1}}$, pois para o próximo $\alpha^{2^n} = \alpha \bmod h(D)$.

- Na demonstração anterior utilizou-se o fato de que se f(D) é um polinômio sobre GF(2) então $(f(D))^2 = f(D^2)$. De fato seja $f(D)=D^n+f_{n-1}D^{n-1}+.....+f_1D+1$; elevando ao quadrado (isto é, fazendo-se o produto f(D).f(D)) tem-se, observando que $f_k=f_k^2$ e que todos os duplos produtos cancelam-se ($f_if_jD^{i+j}$ cancela com $f_jf_iD^{j+i}$), o resultado:
$f^2(D)=D^{2n}+f_{n-1}D^{2(n-1)}+.....+f_1D^2+1$. Assim tem-se a afirmação inicial verificada, e mais genericamente $f(D^{2^i}) = (f(D))^{2^i}$, pois $(a+b)^{2^i}=(a^{2^i}+b^{2^i})$ com coeficientes em GF(2).

<u>Teorema 3</u>

Se a seqüência A é de máximo comprimento (SMC) seu polinômio característico é irredutível (é de fato uma condição necessária para que um polinômio característico gere uma SMC).
Como A é uma SMC o conteúdo dos RD's passa por todos os estados, exceto tudo zero. Seja então (000..01) a sua condição inicial; nestas condições o teorema 2 é válido e diz-se que o expoente de f(x) é p. Seja então f(x)=s(x)t(x), isto é vamos supor f(x) redutível; tem-se: $\frac{1}{f(x)} = \frac{\alpha(x)}{s(x)} + \frac{\beta(x)}{t(x)}$, por decomposição em frações parciais. Sejam r1 e r2 os graus de s(x) e t(x), com r1>0, r2>0, inteiros e tais que r1+r2=n. Assim $\frac{\alpha(x)}{s(x)}$ é uma série de potências cujos coeficientes são periódicos com período no máximo (2^{r1}-1), e analogamente para $\frac{\beta(x)}{t(x)}$ o período máximo é de (2^{r2}-1). Assim a soma das duas representa uma série de potências cujos coeficientes tem um período no máximo o m.m.c. dos períodos individuais, que não pode exceder o produto dos períodos.
Então: $2^n-1 \le (2^{r1}-1)(2^{r2}-1)=2^{r1+r2}-2^{r1}-2^{r2}+1 \le 2^n-2-2+1=2^n-3$
Esta contradição mostra que a hipótese de f(x) possuir fatores é falsa. A demonstração assume que s(x) e t(x) são fatores distintos. Para completar a demonstração seja $f(x)=s^2(x)$. Nestas condições o período de f(x) é o dobro do de s(x) e assim: $2(2^{n/2}-1)<2^n-1$, recaindo-se nas argumentações anteriores.

A recíproca do teorema não é válida: existem polinômios irredutíveis que não geram SMC's. Por exemplo: $f(x)=x^4+x^3+x^2+x+1$ é irredutível, mas como é divisor de $(1+x^5)$ seu período é 5 (e não $2^n-1=15$, como seria se fosse uma SMC). Outro exemplo: $f(x)=x^6+x^3+1$ é irredutível, mas seu expoente é 9 ao invés de 63.

Teorema 4

Todo polinômio irredutível, módulo2, de grau n é divisor de $(x^{2^n-1}+1)$.

Teorema 5

Se uma seqüência tem polinômio característico irredutível de grau n, o período da seqüência é fator de (2^n-1).

Corolário

Se (2^n-1) é primo, todo polinômio irredutível de grau n corresponde a uma SMC.

Seqüência inversa

Denomina-se de seqüência inversa de uma dada a_i, de período p, àquela em que seus elementos são tais que $b_i=a_{p-i}$.

É fácil verificar que neste caso os polinômios característicos das duas seqüências relacionam-se por: $f_I(x)=x^n f(x^{-1})$. Por exemplo, a seqüência inversa da gerada por $f(x)=x^6+x+1$ é dada por $f_I(x)=x^6+x^5+1$. Na consulta de tabelas de polinômios primitivos, ver ref. [10] por exemplo, é usual encontrar-se a notação dos mesmos na forma octal. Assim para o exemplo acima $f(x)=[103]_8=[001000011]_2$ e $f_I(x)=[141]_8=[001100001]_2$, onde cada dígito na notação binária, indica o coeficiente correspondente de x no polinômio característico.

Número de polinômios primitivos e de irredutíveis; ref. [1] e [3]

O número de polinômios primitivos de grau n é dado por: $\lambda(n)=\frac{\varphi(2^n-1)}{n}$, onde $\varphi(.)$ é a função de Euler que representa o número de positivos inteiros menores do que n e primos com o mesmo. Este número é calculável por:

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

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

Exemplo : $n=6 \Rightarrow m=2^6-1=63=3^2\times 7^1 \Rightarrow \varphi(63)=2\times 3^1\times 6\times 7^0=36$ e assim $\lambda(6)=36/6=6$

Os polinômios primitivos de grau 6 são, na notação octal, [103], [147], [155] e seus inversos, ou recíprocos, [141], [163] e [133], respectivamente. Assim existem apenas 6 SMC's de grau 6, dados pelos polinômios primitivos acima listados. A demonstração, que pode ser vista na ref. [1], baseia-se em alguns conceitos da Teoria de Números e é omitida aqui.
O número de polinômios irredutíveis de grau n é dado por $N_I=\frac{1}{n}\sum_{\frac{d}{n}} 2^d \mu(\frac{n}{d})$; onde a somatória se estende para todos os divisores de n (inclusive 1) e $\mu(.)$ é a função de Möbius, definida por:

$$\mu(m)=\begin{cases}1 & m=1\\ 0 & \prod_{i=1}^{k}\alpha_i>1\\ (-1)^k & m \text{ é o produto de } k \text{ primos distintos}\end{cases}$$

Retomando o exemplo anterior com n=6, como os divisores de 6 são 1; 2; 3 e 6, tem-se:

$$N_I=\frac{1}{6}\left\{2^1\mu(6)+2^2\mu(3)+2^3\mu(2)+2^6\mu(1)\right\}=\frac{1}{6}\left\{2\times1+4\times(-1)+8\times(-1)+64\times1\right\}=9\,.$$

E assim o número de polinômios irredutíveis de grau 6 é 9. Além dos 6 primitivos, anteriormente citados, tem-se ainda [127], [111] e seus recíprocos [165] e [111], totalizando os 9 polinômios antecipados. Os polinômios [127] e [111] não geram SMC's e como $2^n-1=63=3^2\times7$ o seu período poderá ser 3; 7; 9 ou 21 (63 não, pois não é primitivo!). Que o polinômio irredutível [111], por exemplo, não é primitivo é fácil verificar pois é um fator de (x^9+1), isto é, é fator de (x^m+1) com m=9, que é menor do $2^6-1=63$. Observação:

$[111]_8=[001\quad 001001]_2\Rightarrow f(x)=x^6+x^3+1=f_I(x)\,e\,(x^9+1)=(x^6+x^3+1)(x^3+1)$

<u>Decimação de seqüências; ref. [5], [6] e [7]</u>

Seja $\{a_n\}$ uma seqüência arbitrária de comprimento p. Denomina-se decimação k da seqüência original à seqüência $\{c_n\}$ tal que $c_n=a_{kn}$ para todo n. Por exemplo: 110110... é uma decimação 2 possível da seqüência 10100010100010....É evidente que se k dividir p então $\{c_n\}$ terá um período, no máximo, p/k (no exemplo anterior p=6, k=2 e o período da seqüência decimada é 3), e portanto se p e k são primos entre si o período resultante será p. Genericamente, o período da seqüência decimada é dada por p/mdc(p,k). Seja então $\{a_n\}$ uma SMC com $p=(2^n-1)$, nestas condições demonstra-se que:

- a decimação a_{kn} de a_n é uma SMC se, e somente se, k e p forem primos entre si;

- todas as SMC's de período $p=(2^n-1)$ podem ser construidas por decimação de $\{a_n\}$;

- o polinômio primitivo correspondente à seqüência obtida por decimação k é tal que suas raízes são a potência k-ésima das raízes do polinômio original. Os números que antecedem os polinômios na notação octal referem-se exatamente a esta propriedade. Assim se α é raíz de 1-[103] então α^5 será raíz de 5-[147], e desta forma a seqüência gerada pelo polinômio [147] pode ser obtida por uma decimação 5 da seqüência correspondente ao polinômio [103];

- duas seqüências produzidas por decimação, com j e k primos em relação a (2^n-1), são ciclicamente distintas se, e somente se, $j\neq2^i k \bmod(2^n-1)$ para todo inteiro i.

Por exemplo: n=4; $p=(2^n-1)=15=3\times5\Rightarrow\lambda(n)=2$ que é o número de SMC's que existem para este grau. Dada uma delas a outra pode ser obtida por uma decimação conveniente. As decimações possíveis são: 1; 2; ..... 14; 15. Destas devem ser descartadas todas as que tem fatores comuns com 15. Restam pois as alternativas 2; 4; 7; 8; 11; 13; 14. e para estas pode-se construir a tabela indicada a seguir.

		$k \times 2^i$	
k	i = 1	i = 2	i = 4
2	2	4	8
4	4	8	16
7	7	14	28≡13
8	8	16≡1	32≡2
11	11	22≡7	44≡14
13	13	26≡11	52≡7
14	14	28≡13	56≡11

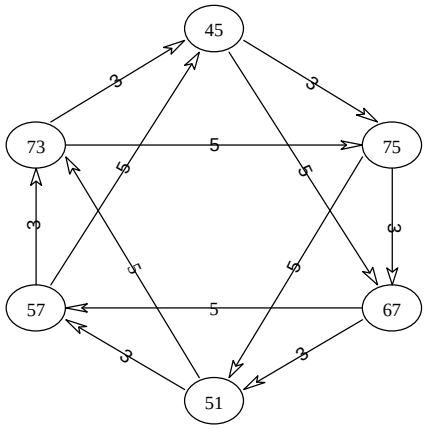
Observa-se então que as decimações 2; 4 e 8 são impróprias (conduzem a fases diferentes da mesma seqüência), enquanto as decimações 7; 11; 13 e 14 conduzem à outra seqüência procurada (conforme o valor ter-se-á fases distintas da mesma seqüência). Destes resultados pode-se ainda inferir:

- se k é uma decimação própria da seqüência, as decimações $2^i k \bmod(2^n - 1)$ levam a fases diferentes da mesma seqüência, para i=1; 2; ..; n-1;

- todas as decimações pares levam a fases diferentes da mesma seqüência;

- decimações próprias só são obtidas com k ímpar e obedecendo ao teorema enunciado.

Exemplo final: n=5; $p = (2^n - 1) = 31$ e $\lambda(5)=6$. Representando-os graficamente tem-se:



Os números nas interligações indicam as decimações, onde então de cada seqüência ilustra-se a construção de mais duas, com k=3 e 5. Observa-se que partindo da seqüência [73] pode-se obter a seqüência [57], por exemplo, por decimações sucessivas de 5; 5 e 3; e como 5×5×3=75=13mod31 o mesmo resultado é obtido com uma decimação 13. Observação: [51]; [57] e [73] são recíprocos de [45]; [75] e [67], respectivamente. Sistematizando o processo de decimação, seja para este último exemplo a tabela a seguir representada.

C_0	1^{*}_{**}	2	4	8	16^{*}
C_1	3^{*}_{***}	6	12	24	17
C_2	5_{**}	10	20	9^{*}	18
C_3	7	14	28	25_{**}	19^{*}
C_4	11	22	13_{***}	26^{*}	21
C_5	15_{***}	30	29	27^{*}	23

Os elementos desta tabela constituem-se dos números de 1 a 30 (2^n-2) e indicam as decimações possíveis de uma dada seqüência. Numa linha os números sucessivos são sempre o dobro do anterior mod31, de forma que todas as decimações desta linha são equivalentes, conforme teorema anterior (a menos da fase da seqüência resultante). A primeira linha desta tabela é constituida de potências sucessivas de 2, de 1 até 2^{n-1}. A próxima linha inicia-se com o menor número inteiro de 1 a 30, ainda não coberto pelas linhas anteriores, e assim sucessivamente. Desta forma, com esta tabela, tem-se uma construção sistemática para todas as SMC's de um determinado grau. Nesta tabela (ver também o diagrama anterior), a título de exemplo, indicam-se por:

N^{*} decimações sucessivas de 3, a partir do elemento 1. Na ordem percorrem-se os elementos 1; 3; 9; 27; 19; 26 e 16 (que corresponde a uma fase diferente da seqüência de partida);

N_{**} decimações sucessivas de 5, a partir do elemento 1. Na ordem percorrem-se os elementos 1; 5; 25 e retorna-se a 1.

N_{***} decimações sucessivas de 5, a partir do elemento 3. Na ordem percorrem-se os elementos 3; 15; 13 e retorna-se a 3.

Ao conjunto de conjuntos $C_0;C_1;\cdots$,acrescido de $\{0\}$, dá-se o nome de coconjunto ciclotômico de grau n (estudos nesta área remontam ao ano de 1800 com Gauss!).

A função traço; ref. [1], [6] e [7]

Uma ferramenta muito útil no cálculo de correlações é a denominada função traço (tradução livre para "trace function"), que pode ser definida como uma função linear de GF(2^n) em GF(2), dado por: $T_R(\beta)\triangleq\sum_{i=0}^{n-1}\beta^{2^i}=\beta+\beta^2+\beta^4+..+\beta^{2^{n-1}}$. A importância desta função no cálculo de correlações está no fato da seqüência $\{a_i\}$ poder ser escrita na forma $\{T_R(\alpha^i)\}$, onde α é a raiz do polinômio característico f(x) da seqüência $\{a_i\}$. Apresentam-se a seguir alguns detalhes e propriedades da função traço.

Sejam então as SMC's a_i e a_j, com j=qi, de período $p=2^n-1$ e $b_i=(-1)^{a_i}$. Como a_i pode ser representado por $a_i=T_R(\alpha^i)$, a correlação cruzada periódica de b_i e b_j escreve-se:

$$\theta_{i,j}(\ell)=\sum_{i=0}^{p-1} b_i b_{qi+\ell}=\sum_{i=0}^{p-1}(-1)^{T_R(\alpha^i)}(-1)^{T_R(\alpha^{qi+\ell})}=\sum_{x\in GF(2^n)}(-1)^{T_R(x+c_\ell x^q)}-(-1)^0=\sum_{x\in GF(2^n)}(-1)^{T_R(x+c_\ell x^q)}-1$$

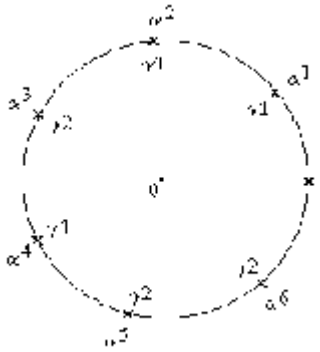
Assim à medida que x percorre GF(2^n), para um dado q e $c_\ell=\alpha^\ell$, pode-se determinar quão freqüentemente $T_R(x+c_\ell x^q)$ assume os valores 0 ou 1. Por exemplo, para valores de q tais que $q=2^k+1$ ou $q=2^{2k}-2^{k+1}$, se o mdc(n,k*)* for tal que $\frac{n}{mdc(n,k)}$ é ímpar, então a correlação cruzada periódica das seqüências assume apenas 3 valores (ver referência [1]).

Exemplo: sejam n=3 e $f(x)=1+x^2+x^3$ e portanto $p=2^n-1=7$, pois f(x) é primitivo.

- se α é raiz de $f(x)\Rightarrow 1+\alpha^2+\alpha^3=0$ e as outras raízes são $\left\{\alpha^2,\alpha^4,..,\alpha^{2^{n-1}}\right\}$; no caso

α^2 e $\alpha^4 \therefore f(\alpha^2)=1+\alpha^4+\alpha^6=(1+\alpha^2+\alpha^3)^2=0$ e $f(\alpha^4)=1+\alpha+\alpha^5=(1+\alpha^4+\alpha^6)^2=0$

e daí decorre ainda que $1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6=0\Rightarrow\alpha^7=1$



- a função traço é, neste exemplo, dada por $T_R(\beta)=\beta+\beta^2+\beta^4$ e com ela pode-se construir a tabela:

t	α^t	$T_R(\alpha^t)$	=	S_1	S_2
0	α^0	$\alpha^0+\alpha^0+\alpha^0$	γ_0	1	1
1	α^1	$\alpha+\alpha^2+\alpha^4$	γ_1	1	0
2	α^2	$\alpha^2+\alpha^4+\alpha$	γ_1	1	0
3	α^3	$\alpha^3+\alpha^6+\alpha^5$	γ_2	0	1
4	α^4	$\alpha^4+\alpha+\alpha^2$	γ_1	1	0
5	α^5	$\alpha^5+\alpha^3+\alpha^6$	γ_2	0	1
6	α^6	$\alpha^6+\alpha^5+\alpha^3$	γ_2	0	1

desta tabela sai que $\gamma_0=1$ e portanto $1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6=1+\gamma_1+\gamma_2$; e em virtude da relação anterior $1+\gamma_1+\gamma_2=0$; logo as seqüências (são apenas duas para este grau) são obtidas por:

$\gamma_1 = 1, \gamma_2 = 0 \rightarrow$ seqüência S_1 e

$\gamma_2 = 1, \gamma_1 = 0 \rightarrow$ seqüência S_2 (inversa da anterior)

- A forma usual de representação por RD's e correspondente tabela de estados é a já representada anteriormente na página 2 e a seqüência correspondente é $X_1 = \{1,0,1,1,1,0,0, \ldots\}$ com período p=7.

- a divisão longa $(1/f(x))=1+x^2+x^3+x^4+x^7+..$, corresponde à seqüência X_1.

<u>Propriedades da função traço; ref. [1] e [6]</u>

As principais propriedades da função $T_R(\beta)$ são a seguir relacionadas:

1) $T_R(\beta)=T_R(\beta^{2^i})$ para todo $\beta \in GF(2^m)$ e todo i; no exemplo anterior: $T_R(D)=T_R(D^2)=T_R(D^4)=..=1$.

2) $T_R(a\alpha+b\beta)=aT_R(\alpha)+bT_R(\beta)$ para todo $a,b \in GF(2)$ e $\alpha,\beta \in GF(2^m)$.

3) a equação $T_R(\beta)=b$ com $b \in GF(2)$ tem exatamente 2^{m-1} soluções β em $GF(2^m)$. De fato, se no exemplo anterior considerarmos ainda $\beta=0$, para o qual $T_R(0)=0$, verifica-se que a equação $T_R(\beta)=1$ tem 4 soluções $(2^{3-1}=4)$ que são $\beta=1; D; D^2$ e D^4 e $T_R(\beta)=0$ tem 4 soluções que são $\beta=0; D^3; D^5$ e D^6.

4) $\sum_{\beta \in GF(2^m)} (-1)^{T_R(\beta)}=0$ (resultado no campo real)

(observação : $(-1)^0=1$ e $(-1)^1=-1$, onde os expoentes 0 e $1 \in GF(2)$ e os resultados 1 e -1 $\in$ R).

É uma conseqüência da propriedade 3, levando em conta que para 2^{m-1} valores de β, $T_R(\beta)=1$ e para 2^{m-1} valores (os outros) de β, $T_R(\beta)=0 \Rightarrow$ para todo $\beta \in GF(2^m)$ tem-se $\sum (-1)^{T_R(\beta)}=0$

5) Levando em conta a notação $T_R(\beta)=T_{R_2}^{2^m}(\beta)$, se $GF(2) \subset GF(2^k) \subset GF(2^m) \Rightarrow T_{R_2}^{2^m}(\beta)=T_{R_2}^{2^k}(T_{R_{2^k}}^{2^m}(\beta))$ para todo $\beta \in GF(2^m)$. Observação: esta propriedade é importante na definição e análise das seqüências GMW.

Para esta generalização: $T_{R_{2^k}}^{2^m}(\beta)=\sum_{i=0}^{m/k-1} \beta^{2^{ki}}$; observe que para k=1 recai-se na definição anterior $T_{R_{2^k}}^{2^m}(\beta)=\sum_{i=0}^{m-1} \beta^{2^i}$.

O teorema será verificado com um exemplo apenas: seja $T_{R_2}^{2^4}(\beta)=T_{R_2}^{2^2}\left(T_{R_{2^2}}^{2^4}(\beta)\right)$. O primeiro membro vale

$T_{R_2}^{16}(\beta)=\beta+\beta^2+\beta^4+\beta^8$; o argumento do segundo membro é $T_{R_{2^2}}^{2^4}(\beta)=\beta+\beta^4$ e portanto seu valor é dado por

$T_{R_2}^{2^2}(\beta+\beta^4)=(\beta+\beta^4)+(\beta+\beta^4)^2=\beta+\beta^2+\beta^4+\beta^8$.

Segue-se um exemplo adicional de aplicação para o caso de p não primo. Sejam então:

$n=4, f(x)=x^4+x+1 \Rightarrow p=2^n-1=15$ (observação $15=5\times3$); assim $\frac{\varphi(2^n-1)}{n}=\frac{2\times4}{4}=2$ (número de seqüências de máximo comprimento de grau 4). Os elementos do coconjunto ciclotômico correspondente escrevem-se:

γ_1: 1 2 4 8 $\{1,2,4,8\}$

γ_2: 3 6 12 9 impróprio

γ_4: 5 10 5 10 impróprio

γ_3: 7 14 13 11 $\{7,11,13,14\}$

(as duas decimações denotadas como impróprias correspondem a decimações de 3 e 5 da SMC, e não levam pois à outra SMC, dado que o período da original é 15). As duas SMC's são dadas pois por: $f(x)$ e uma decimação q desta, onde q $\in \{7,11,13,14\}$.

A função traço é neste caso $T_R(\beta)=\beta+\beta^2+\beta^4+\beta^8$ e pode-se pois construir a tabela abaixo (α é raíz de $f(x)=0$).

t	α^t	$T_R(\alpha^t)$	=	coconjunto
0	α^0	$\alpha^0+\alpha^0+\alpha^0+\alpha^0$	γ_0	$\{0\}$
1	α^1	$\alpha^1+\alpha^2+\alpha^4+\alpha^8$	γ_1	$\{1,2,4,8\}$
2	α^2	$\alpha^2+\alpha^4+\alpha^8+\alpha^1$	γ_1	
3	α^3	$\alpha^3+\alpha^6+\alpha^{12}+\alpha^9$	γ_2	$\{3,6,9,12\}$
4	α^4	$\alpha^4+\alpha^8+\alpha^1+\alpha^2$	γ_1	
5	α^5	$\alpha^5+\alpha^{10}+\alpha^5+\alpha^{10}$	γ_4	$\{5,10\}$
6	α^6	$\alpha^6+\alpha^{12}+\alpha^3+\alpha^9$	γ_2	
7	α^7	$\alpha^7+\alpha^{14}+\alpha^{13}+\alpha^{11}$	γ_3	
8	α^8	$\alpha^8+\alpha^1+\alpha^2+\alpha^4$	γ_1	
9	α^9	$\alpha^9+\alpha^3+\alpha^6+\alpha^{12}$	γ_2	
10	α^{10}	$\alpha^{10}+\alpha^5+\alpha^{10}+\alpha^5$	γ_4	
11	α^{11}	$\alpha^{11}+\alpha^7+\alpha^{14}+\alpha^{13}$	γ_3	
12	α^{12}	$\alpha^{12}+\alpha^9+\alpha^3+\alpha^6$	γ_2	
13	α^{13}	$\alpha^{13}+\alpha^{11}+\alpha^7+\alpha^{14}$	γ_3	
14	α^{14}	$\alpha^{14}+\alpha^{13}+\alpha^{11}+\alpha^7$	γ_3	
15	α^{15}	$\alpha^0+\alpha^0+\alpha^0+\alpha^0$	γ_0	

$\gamma_0=\gamma_4=0$ (óbvio), $\gamma_2=1$ (vide adiante) $\Rightarrow$ p/balancear $\bar{\gamma}_1=\gamma_3$

Em um período da seqüência temos:

$$\begin{aligned}\gamma_0 &= 0 \quad ... \quad 1\,\text{vez}\\ \gamma_1 &= x \quad ... \quad 4\,\text{vezes}\\ \gamma_2 &= 1 \quad ... \quad 4\,\text{vezes}\\ \gamma_3 &= \overline{x} \quad ... \quad 4\,\text{vezes}\\ \gamma_4 &= 0 \quad ... \quad 2\,\text{vezes}\end{aligned}$$

A seqüência, em sua forma genérica, é dada por:

$$\underbrace{\gamma_0\gamma_1\gamma_1\gamma_2\gamma_1\gamma_4\gamma_2\gamma_3\gamma_1\gamma_2\gamma_4\gamma_3\gamma_2\gamma_3\gamma_3}_{15\,\text{termos}}\gamma_0\cdots$$

$$\text{onde}\begin{cases}\gamma_1=\alpha+\alpha^2+\alpha^4+\alpha^8\\ \gamma_2=\alpha^3+\alpha^6+\alpha^9+\alpha^{12}\\ \gamma_3=\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14}\\ \gamma_4=\gamma_0=0\end{cases}\quad c/\ \gamma_i\in GF(2)=\{0,1\}$$

Particularizando para o polinômio $f(x)=x^4+x+1\Rightarrow D^4=(D+1)\bmod f(D)$ e construindo a tabela de caracterização de GF(16) tem-se:

$$\begin{aligned}D^0 &\quad 1\\ D^1 &\quad D\\ D^2 &\quad D^2\\ D^3 &\quad D^3\\ D^4 &\quad D+1\\ D^5 &\quad D^2+D\\ D^6 &\quad D^3+D^2\\ D^7 &\quad D^3+D+1\\ D^8 &\quad D^2+1\\ D^9 &\quad D^3+D\\ D^{10} &\quad D^2+D+1\\ D^{11} &\quad D^3+D^2+D\\ D^{12} &\quad D^3+D^2+D+1\\ D^{13} &\quad D^3+D^2+1\\ D^{14} &\quad D^3+1\\ D^{15} &\quad 1\end{aligned}$$

Desta tabela temos:

$$\gamma_1=\alpha+\alpha^2+\alpha+1+\alpha^2+1=0$$
$$\gamma_2=\alpha^3+\alpha^3+\alpha^2+\alpha^3+\alpha+\alpha^3+\alpha^2+\alpha+1=1$$
$$\gamma_3=\alpha^3+\alpha+1+\alpha^3+\alpha^2+\alpha+\alpha^3+\alpha^2+1+\alpha^3+1=1$$
e a seqüência correspondente é ... 0 0 0 1 0 0 1 1 0 1 0 1 1 1 1 ...

resultado que pode ser verificado por uma divisão longa ou com registradores de deslocamento realimentados segundo $f(x)$. A seqüência inversa da dada é caracterizada por:

$f_I(x)=x^4 f\left(\frac{1}{x}\right)=x^4+x^3+1 \Rightarrow D^4=(D^3+1) \bmod f_I(D)$ e portanto pode-se escrever:

D^0	1
D^1	D
D^2	D^2
D^3	D^3
D^4	D^3+1
D^5	D^3+D+1
D^6	D^3+D^2+D+1
D^7	D^2+D+1
D^8	D^3+D^2+D
D^9	D^2+1
D^{10}	D^3+D
D^{11}	D^3+D^2+1
D^{12}	D+1
D^{13}	D^2+D
D^{14}	D^3+D^2
D^{15}	1

Desta tabela temos:

$\gamma_1=\alpha+\alpha^2+\alpha^3+1+\alpha^3+\alpha^2+\alpha=1$

$\gamma_2=\alpha^3+\alpha^3+\alpha^2+\alpha+1+\alpha^2+1+\alpha+1=1$

$\gamma_3=\alpha^2+\alpha+1+\alpha^3+\alpha^2+1+\alpha^2+\alpha+\alpha^3+\alpha^2=0$

e a seqüência correspondente é ... 0 1 1 1 1 0 1 0 1 1 0 0 1 0 0 ...

que é inversa da seqüência anterior, obviamente. Observe-se ainda que de $\alpha^4+\alpha+1=0$, pode-se escrever:

$$\begin{array}{ll} \alpha^5+\alpha^2+\alpha^1=0 & \text{como } \alpha^4+\alpha+1=0 \\ \alpha^6+\alpha^3+\alpha^2=0 & \text{e } \alpha^6+\alpha^3+\alpha^2=0 \\ \quad . & \\ \quad . \quad \Rightarrow & 1+\alpha+\alpha^2+\alpha^3+\alpha^4=\alpha^6 \\ \quad . & \\ \alpha^{14}+\alpha^{11}+\alpha^{10}=0 & \end{array}$$

$$\overline{\alpha^5+\alpha^6+\ldots+\alpha^{14}+\alpha+\alpha^{11}=0}$$

e destas $1+\alpha+\alpha^2+\ldots+\alpha^{14}=\alpha+\alpha^6+\alpha^{11}$; basta agora verificar que o 2°membro é nulo. De fato

$\alpha+\alpha^6+\alpha^{11}=\alpha+\alpha^3+\alpha^2+\alpha+1+\alpha^3+\alpha^2+1=0$. E assim temos:

$1+\alpha+\ldots+\alpha^{14}=0 \Rightarrow (1+\alpha)(1+\alpha+\ldots+\alpha^{14})=0 \Rightarrow 1+\alpha^{15}=0 \therefore \alpha^{15}=1$

Esta relação é válida, obviamente, também para o polinômio da função inversa. Verificando com $f(x)=x^4+x^3+1$ temos:

$\rho^4+\rho^3+1=0$

$\rho^5+\rho^4+\rho=0$

.

.

$\rho^{13}+\rho^{12}+\rho^9=0$

$\rho^{14}+\rho^{13}+\rho^{10}=0$

$1+\rho+\ldots+\rho^{10}+\rho^3+\rho^{14}=0$

$\rho^{11}+\rho^{12}+\rho^{13}=\rho^9\left(\rho^4+\rho^3+1\right)+\rho^9+\rho^{11}=\rho^9+\rho^{11}$

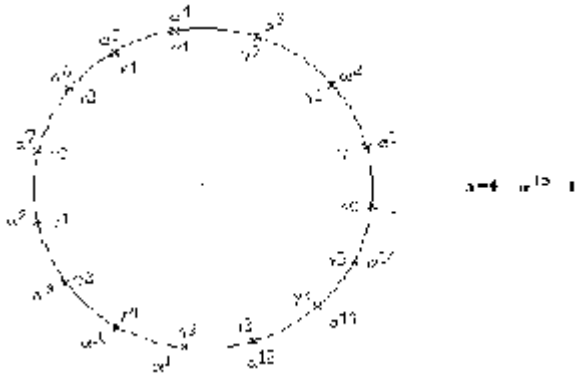
$=\rho^7\left(\rho^4+\rho^3+1\right)+\rho^{10}+\rho^9+\rho^7=\rho^{10}+\rho^9+\rho^7$

$=\rho^6\left(\rho^4+\rho^3+1\right)+\rho^6+\rho^7=\rho^7+\rho^6$

$=\rho^3\left(\rho^4+\rho^3+1\right)+\rho^3=\rho^3$(*)

$\therefore 1+\rho+\ldots+\rho^{14}=0\Rightarrow\rho^{15}=1$

Assim tem-se a representação:



(*) Obviamente o mesmo resultado é obtido usando-se a tabela:

$$\rho^{11}+\rho^{12}+\rho^{13}=\rho^3+\rho^2+1+\rho+1+\rho^2+\rho=\rho^3$$

Observe-se ainda que de:

$$\begin{cases}\gamma_1=\alpha+\alpha^2+\alpha^4+\alpha^8\\ \gamma_2=\alpha^3+\alpha^6+\alpha^9+\alpha^{12}=1 \quad \text{(ver adiante)}\\ \gamma_3=\alpha^7+\alpha^{11}+\alpha^{13}+\alpha^{14}\\ \quad 1+\alpha^5+\alpha^{10}=0 \quad \text{(ver adiante)}\end{cases}$$

obtém-se, levando em conta que $1+\rho+\ldots+\rho^{14}=0$, a relação entre os γ a determinar: $\gamma_1+\gamma_3=0$ (as soluções anteriores correspondem a $\gamma_1=1$ e $\gamma_3=0$; $\gamma_1=0$ e $\gamma_3=1$ e nos dois casos $\gamma_0=\gamma_4=0$ e $\gamma_2=1$).

Adendo : Qualquer que seja o polinômio primitivo adotado (com n=4) é válida a relação $\alpha^5+\alpha^{10}=1$, conforme se verifica a seguir.

se $\alpha^4+\alpha^3+1=0$

$$\alpha^5+\alpha^{10}=\alpha^6\left(\alpha^4+\alpha^3+1\right)+\alpha^9+\alpha^6+\alpha^5$$
$$=\alpha^5\left(\alpha^4+\alpha^3+1\right)+\alpha^8+\alpha^6$$
$$=\alpha^4\left(\alpha^4+\alpha^3+1\right)+\alpha^7+\alpha^6+\alpha^4$$
$$=\alpha^3\left(\alpha^4+\alpha^3+1\right)+\alpha^4+\alpha^3$$
$$=1 \text{ (ou c/ a tabela } (\alpha^3+\alpha+1+\alpha^3+\alpha=1))$$

se $\alpha^4+\alpha+1=0$

$$\alpha^5+\alpha^{10}=\alpha^6\left(\alpha^4+\alpha+1\right)+\alpha^5+\alpha^6+\alpha^7$$
$$=\alpha^3\left(\alpha^4+\alpha+1\right)+\alpha^3+\alpha^4+\alpha^5+\alpha^6$$
$$=\alpha^2\left(\alpha^4+\alpha+1\right)+\alpha^2+\alpha^4+\alpha^5$$
$$=\alpha\left(\alpha^4+\alpha+1\right)+\alpha+\alpha^4$$
$$=1 \text{ (ou c/ a tabela } (\alpha^2+\alpha+\alpha^2+\alpha+1=1))$$

E ainda, qualquer que seja o polinômio primitivo adotado (com n=4) é valida a relação: $\gamma_2=\alpha^3+\alpha^6+\alpha^9+\alpha^{12}=1$, conforme já verificado anteriormente nos dois casos.

Lista de Exercícios

1) Seja um registrador de deslocamentos de 24 estágios para a geração de SMC's.

- quantas SMC's distintas existem deste grau?
- ache o comprimento e período da seqüência, sabendo-se que a taxa de chips é de 2,0 Mbits/s;

2) Considere todas as realimentações possíveis de se realizar com um registrador de deslocamentos de n estágios, para a implementação de um gerador de seqüências. Quantas formas distintas existem no total? Destas, quantas são lineares? E destas últimas, quantas são de máximo comprimento? Faça um exemplo numérico para ilustrar o resultado.

3) Demonstre que a seqüência inversa da caracterizada por $f(x)$ é dada por $f_I(x)=x^n f(x^{-1})$. Observação: não use o resultado do exercício 5.

4) Seja uma seqüência caracterizada por uma função geradora $G(x)=g(x)/f(x)$. Considere agora a seqüência obtida da anterior por repetição de cada um dos seus elementos (.....10011.....1100001111....., por exemplo). Determine, em função da seqüência original, a função geradora da nova seqüência assim obtida.

5) Prove que se uma SMC é gerada por RD's com realimentação nos estágios L, m, n, p,...., a seqüência inversa será gerada com realimentação nos estágios L, L-m, L-n, L-p,.....Observação: não use o resultado do exercício 3.

6) Prove que para uma SMC, em um período inteiro, há exatamente $2^{n-(p+2)}$ bits consecutivos iguais (blocos) de comprimento p [exceto que há apenas um bloco contendo n "uns" e um contendo (n-1) "zeros"; não há blocos de "zeros" de comprimento n ou de "uns" de comprimento (n-1)].

7) Prove que se $G(x)=g(x)/f(x)$ representa a função geradora de uma seqüência, então $G^2(x)$ representa o da seqüência anterior intercalada de "zeros".

8) Sejam $G_a(x)=g_a(x)/f_a(x)$ e $G_b(x)=g_b(x)/f_b(x)$, conforme definição usual. Nestas condições, prove que a seqüência intercalada de a e b tem uma função geradora dada por:

$$G_{ab}(x)=[f_b^2(x)g_a^2(x)+xf_a^2(x)g_b^2(x)]/f_a^2(x)f_b^2(x)$$

9) Seja $f(x)=x^5+x^4+1$.

- verifique que $f(x)=(x^2+x+1)(x^3+x+1)$, indicando que o mesmo é redutível;
- por divisão longa, e condições iniciais 0..01, determine a seqüência assim gerada, verificando que seu período é p=21;
- justifique este valor de p;
- selecione condições iniciais adequadas para o conteúdo dos RD's, de forma que G(x) reduza-se à $G(x)=(x^3+x+1)^{-1}$;
- por divisão longa, e com as condições iniciais determinadas no item anterior, determine a seqüência assim gerada, verificando que seu período é p=7;
- justifique este valor de p.

10) Verifique através de um exemplo que, deslocar uma seqüência de m posições para a direita, implica em multiplicar sua função geradora por x^m e reduzir o resultado modf(x), caso o grau do resultado seja maior ou igual a n.

11) Demonstre os teoremas 4 e 5.

12) Prove que:
- para uma SMC gerada com RD's, o número de realimentações é necessariamente par;
- a soma mod2 de uma SMC com uma defasagem própria da mesma é outra defasagem da mesma seqüência;
- uma SMC é balanceada, isto é: o número de "uns" é 2^{n-1} e o de "zeros" é 2^{n-1}-1, num período completo da mesma.

13) Seja a função de autocorrelação da seqüência bipolarizada b_i definida, da forma usual, por $R(m)=p^{-1}\sum_{n=1}^{p} b_n b_{n+m}$, onde p é o período da seqüência. Prove que para uma SMC vale: $R(m)=\begin{cases}1 & m=0\\ -p^{-1} & 0<|m|<p\end{cases}$

14) Considere o exercício anterior. Mostre que estendendo a definição, e fazendo corresponder a cada chip um pulso retangular de largura T_c, tem-se:

$R_p(\tau)=-p^{-1}+(p+1)p^{-1}\sum_{-\infty}^{\infty}\Lambda[(\tau-ipT_c)T_c^{-1}]$; onde $\Lambda(\tau T_c^{-1})=\begin{cases}1-|\tau|T_c^{-1} & p/\ |\tau|<T_c\\ 0 & \text{c.c.}\end{cases}$

e, como conseqüência, a densidade espectral de potência (DEP) é dada por:

$$S_p(f)=p^{-2}\delta(f)+p^{-2}(p+1)\sum_{\substack{-\infty\\ i\neq 0}}^{+\infty}[\text{sinc}^2(ip^{-1})]\delta[f-i(pT_c)^{-1}]$$

15) Dado o segmento ....1111100100110....de uma SMC, gerada a partir de um RD de 5 estágios, determine a configuração de realimentação do RD e verifique sua resposta. Observação: este problema ilustra a vulnerabilidade das SMC's, quanto a possibilidade de quebra do código, a partir da observação de apenas um segmento, (2n-1) bits consecutivos, da mesma.

16) Considere o polinômio primitivo $f(x)=x^3+x+1$.
- determine a SMC correspondente por dois processos: por uma divisão longa e por meio de RD's realimentados;
- construa as seqüências obtidas a partir de decimações com k=2; 3; 4; 5 e 6; verifique para que valor(es) de k resulta em uma outra SMC;
- determine os elementos do coconjunto ciclotômico correspondente e confira sua resposta ao quesito anterior.

17) Prove que se $f_1(x)$ e $f_2(x)$ são dois polinômios característicos, então qualquer seqüência obtida por soma mod2 das anteriores, pode ser gerada por um RD de polinômio característico $f(x)=f_1(x)f_2(x)$, com um número de estágios igual à soma dos estágios de $f_1(x)$ e $f_2(x)$. Observação: esta propriedade é útil na geração dos códigos de Gold e Kasami.

18) Prove que $T_R(a\alpha+b\beta)=aT_R(\alpha)+bT_R(\beta)$ para todo $a,b\in GF(2)$ e $\alpha,\beta\in GF(2^m)$.

19) Construa o corpo GF(16) usando a base $\{1;\alpha;\alpha^2;\alpha^3\}$, onde α satisfaz à equação $\alpha^4+\alpha^3+1=0$. Determine o traço do elemento $\beta=b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3$.

20) Determine os elementos do coconjunto ciclotômico de grau 7. O resultado e mais detalhes podem ser vistos na ref. [7].

Referências Bibliográficas

[1] McEliece, R. J., Finite Fields for Computer Scientists and Engineers, Kluwer Academic Publishers, 1987.

[2] Golomb, S. W., Shift Register Sequences, Aegean Park Press, Laguna Hills-CA, 1982.

[3] Holmes, J. K., Coherent Spread Spectrum Systems, John Wiley & Sons, 1982.

[4] Jeszensky, P. J. E., Uma Revisão sobre Geradores Lineares de Seqüências para Comunicação por Espalhamento Espectral, 9º Simpósio Brasileiro de Telecomunicações, Anais pp 11.4.1/11.4.6, Setembro 1991.

[5] Sarwate, D. V. e M. B. Pursley, Crosscorrelation Properties of Pseudorandom and Related Sequences, Proceedings of the IEEE, vol. 68, no. 5, May 1980, pp 593/619.

[6] Simon, M. K., J. K. Omura, R. A. Scholtz e B. K. Levitt, Spread Spectrum Communications, vol. I, Rockville, MD, Computer Science Press, 1985.

[7] Golomb, S. W., Correlation Properties of Periodic and Aperiodic Sequences, and Applications to Multi-User Systems, parte de: New Concepts in Multi-User Communication, editado por J. K. Skwirzynski, NATO Advanced Study Institutes Series, Sijthoff Noordhoff International Publishers, 1981, pp 161/197.

[8] Jeszensky, P. J. E., Uma Motivação para o Estudo de Seqüências de Código, publicação do Departamento de Engenharia Eletrônica da EPUSP, pp 1/23, fevereiro 1992.

[9] Ziemer, R. E. e R. L. Peterson, Digital Communications and Spread Spectrum Systems, Macmillan Publishing Company, 1985.

[10] Peterson, W. W. e E. J. Weldon Jr., Error-Correcting Codes, 2nd Ed. Cambridge, Mass.: MIT Press, 1972.

[11] Jeszensky, P. J. E., Introdução à Técnica de Comunicação por Espalhamento Espectral, publicação para o Mini-Curso ministrado no 9º Simpósio Brasileiro de Telecomunicações, pp 1/61, Setembro 1991.