

# 文档说明

---

项目地址: <https://github.com/LvGitHub-9/SpreadSpectrumCommunication>

名称: 伪随机序列

说明: 扩频通信原理, 以及m序列、M序列、Gold序列、Kasami序列生成器和性质研究

版本: V1.0

作者: 小吕同学

修改记录:

版本号	日期	作者	说明
V1.0	2024-12-27	小吕同学	首次发布

FindMe: [https://space.bilibili.com/10179894?spm\\_id\\_from=333.1007.0.0](https://space.bilibili.com/10179894?spm_id_from=333.1007.0.0)

Copyright 2024 Lv. All Rights Reserved.

Distributed under MIT license.

See file LICENSE for detail or copy at <https://opensource.org/licenses/MIT>

# 扩频通信

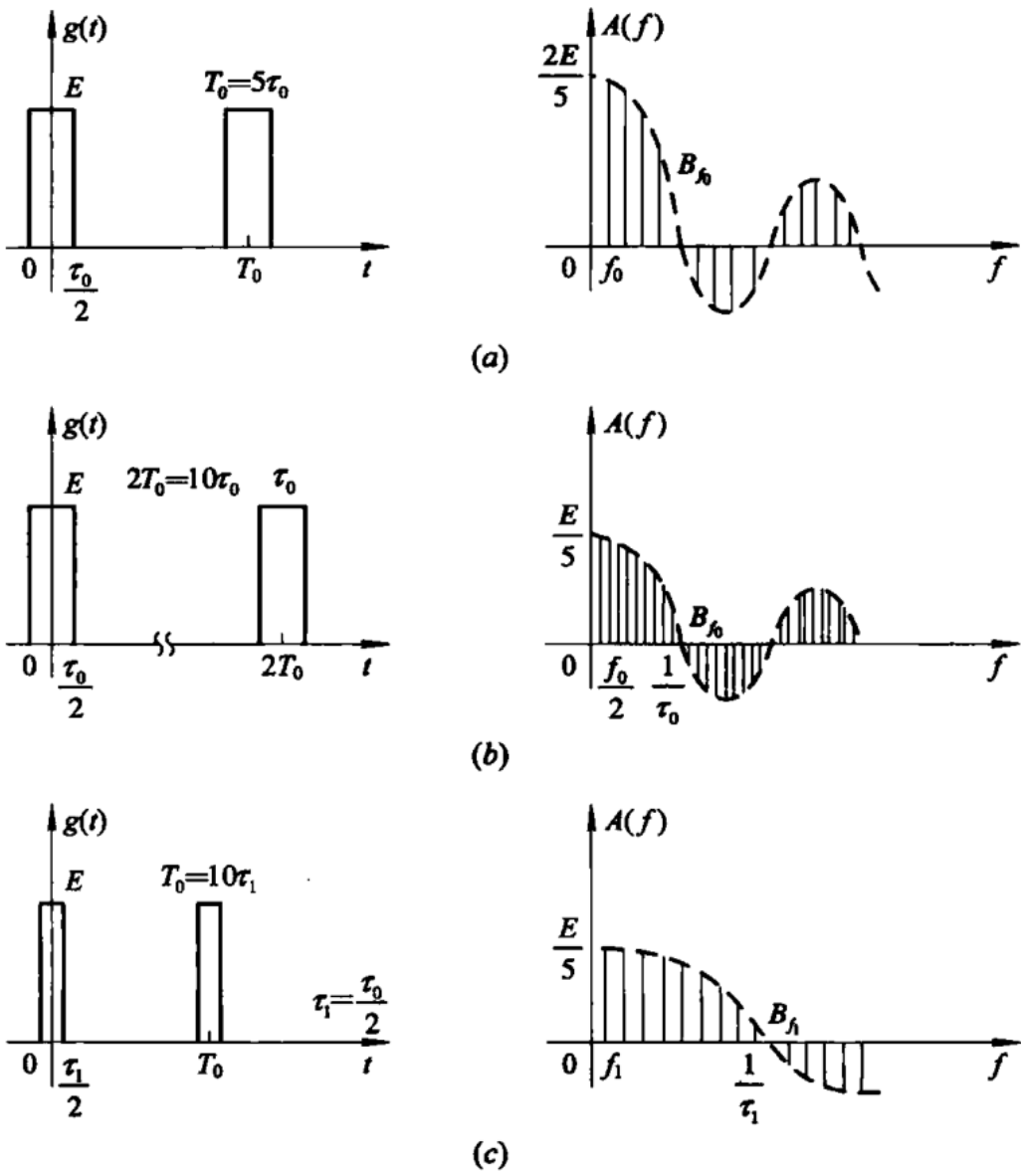
香农公式指出，在信息速率不超过信道容量情况下，带宽和信噪比可以互换

$$C = B \cdot \log_2(1 + \frac{S}{N})$$

扩频通信增大信号带宽，从而在极低信噪比下传输信息。甚至在信号被噪声淹没的情况下，也能进行可靠的通信。

## 扩频原理

周期门信号的傅里叶变换



可以看出

- 1) 用较窄的脉冲序列调制信号，可以将信号的频谱展宽；
- 2) 信号的总能量不变，在频谱被扩展的情况下，信号功率谱密度下降；

# 伪随机序列

---

扩展信号带宽并不是用随机的窄脉冲序列调制信号，考虑到接收端需要信号解调恢复原始信号，香农提出，用具有白噪声统计特性的信号来编码。白噪声的自相关函数是冲激函数，功率谱密度是常数。用具有白噪声统计特性的信号进行编码，会将信号隐藏在白噪声中。人类至今无法实现对白噪声的放大、调制、同步和检测等操作，如果没有伪随机序列，那么信号将很难被检测出来。密码学也会用到伪随机序列。

## 基本概念

---

最开始对伪随机序列提出的基本公设：

- 1) 平衡性：1比0最多多一个，最好相等；
- 2) 游程平衡性：相同长度的游程相等且对称；
- 3) 自相关函数为二值函数，近似冲激；

平衡性表示0和1出现的概率基本相同；游程平衡性表示0和1出现在序列每个位置上的概率相同；

自相关函数意为某一函数自己和自己的相似性，自相关函数是冲激函数意味着如果这个序列和自己不完全重合，那么输出是零；只有在完全重合的情况下，才会有输出，非常有利于检测和同步，自相关性反应了序列序元的均匀分布特性；

$$R_{xx}(\tau) \stackrel{\text{def}}{=} \lim_{T \rightarrow \infty} \int_{-\frac{T}{2}}^{\frac{T}{2}} x(t)x(t-\tau)dt$$

在码分多址系统里，不仅需要伪随机序列自相关性好，还需要不同扩频码之间的互相关性处处为0，防止在信号接收端扩频码的相互干扰，因此伪随机序列的理想特性：

- 1) 尖锐的自相关特性；
- 2) 处处为零的互相关特性；
- 3) 足够长的码长；
- 4) 足够多的数量；
- 5) 工程上易于生产加工；

# m序列

最长线性移位寄存器序列，系统由反馈系数Ci和状态寄存器Di组成。C0和Cn的系数为1，表示反馈连接。

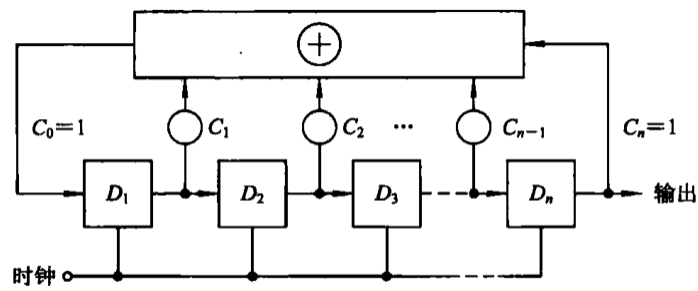


图 2-3 由 n 级简单型移位寄存器构成的码序列发生器

由反馈系数构成的特征多项式表示为

$$G(x) = C_0 + C_1x^1 + C_2x^2 + \cdots + C_nx^n = \sum_{i=0}^n C_i x^i$$

其中x的幂次表示位置。由特征多项式生成m序列的必要条件是，特征多项式必须是本原多项式，需要满足以下条件：

- 1) G(x)不可约；
- 2) n阶反馈系数下，G(x)必须可整除  $(x^{2^n-1}+1)$  ；
- 3) G(x)不能成为比2) 更低阶的因式；

满足以上条件后，通过穷举法可以得到以下反馈系数表，用于生成m序列。

表 2-1 部分 m 序列反馈系数表

级数 n	周期 P	反馈系数 Ci(八进制)
3	7	13
4	15	23
5	31	45, 67, 75
6	63	103, 147, 155
7	127	203, 211, 217, 235, 277, 313, 325, 345, 367
8	255	435, 453, 537, 543, 545, 551, 703, 747
9	511	1021, 1055, 1131, 1157, 1167, 1175
10	1023	2011, 2033, 2157, 2443, 2745, 3471
11	2047	4005, 4445, 5023, 5263, 6211, 7363
12	4095	10 123, 11 417, 12 515, 13 505, 14 127, 15 053
13	8191	20 033, 23 261, 24 633, 30 741, 32 535, 37 505
14	16383	42 103, 51 761, 55 753, 60 153, 71 147, 67 401
15	32765	100 003, 110 013, 120 265, 133 663, 142 305
16	65531	210 013, 233 303, 307 572, 311 405, 347 433
17	131061	400 011, 411 335, 444 257, 527 427, 646 775

通过确定的反馈系数生成的m序列是一个周期序列，长度为 $2^n-1$ 。在初始状态非全零的情况下，对于同一个反馈系数，任何初始状态生成的m序列的差别仅在于周期的起始点不同。

# m序列生成器

```
%% m/M序列发生器
% initial: 系统初始状态（非全零，阶数符合即可）
% feedback: 反馈系数（查表，八进制）
% mode: 为0时生成m序列，长度 $2^n-1$ ；
%       为1时生成M序列，长度 $2^n$ ；
% m: 生成的m/M二值序列，没有进行逻辑映射；
function [m]=mseq(initial,feedback,mode)

n=length(initial);           % 阶数
temp=de2bi(oct2dec(feedback)); % 反馈系数8转10进制转2进制
temp=flip1r(temp);           % 翻转
final=temp(2:length(temp));   % 舍去首位

output=[];
comp=[zeros(1,n-1) 1];       % 生成M序列时使用
for ii=1:2^n-1
    output=[output initial(n)];
    if(mode & initial==comp) % 生成M序列时使用
        output=[output 0];
    end
    temp=mod(sum(final.*initial),2);
    initial=[temp initial(1:n-1)];
end

m=output;                     % 没有进行逻辑映射
```

## m序列的性质

- 1) 平衡性：1的个数比0多一个；
- 2) 游程平衡性：相邻码元长度成为游程，0和1的游程具有对称性，k阶游程占游程的 $1/2^k$ ；
- 3) 移位相加性：m序列移位后逐位模2加，得到的是移位后的m序列；
- 4) 周期性：周期序列长度 $2^n-1$ ；
- 5) 自相关与互相关性：首先进行逻辑映射， $1 \rightarrow +1$ ， $0 \rightarrow -1$ ；（负逻辑映射也行， $1 \rightarrow -1$ ， $0 \rightarrow +1$ ）

```
%% m序列相关性
close all; clear; clc;
initial=[1 0 1 1 0 0];      % 6阶
feedback=103;
m1 = mseq(initial,feedback,0);
m1 = 2*m1 - 1;

initial=[1 0 1 1 0 0];      % 6阶
feedback=147;
m2 = mseq(initial,feedback,0);
m2 = 2*m2 - 1;

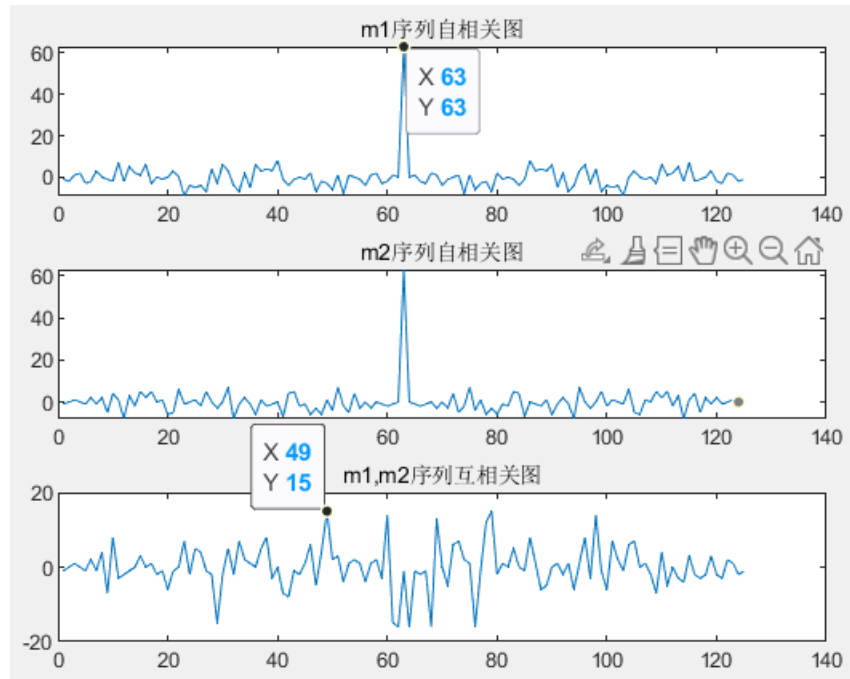
subplot(3,1,1)
plot(xcorr(m1))               % 自相关图
title('m1序列自相关图')
```

```

subplot(3,1,2)
plot(xcorr(m2))           % 自相关图
title('m2序列自相关图')
subplot(3,1,3)
plot(xcorr(m1,m2))       % 互相关图
title('m1,m2序列互相关图')

```

程序输出



## 6) 功率谱密度

```

%% m序列功率谱密度
close all; clear; clc;
T=0.005;           % 码片周期5ms
fs=126e3;          % 采样频率126kHz
ts=1/fs;           % 采样间隔
t=0:ts:T-ts;       % 时间轴
df=fs/length(t);   % 频率间隔
f=-fs/2:df:fs/2-df; % 频率点

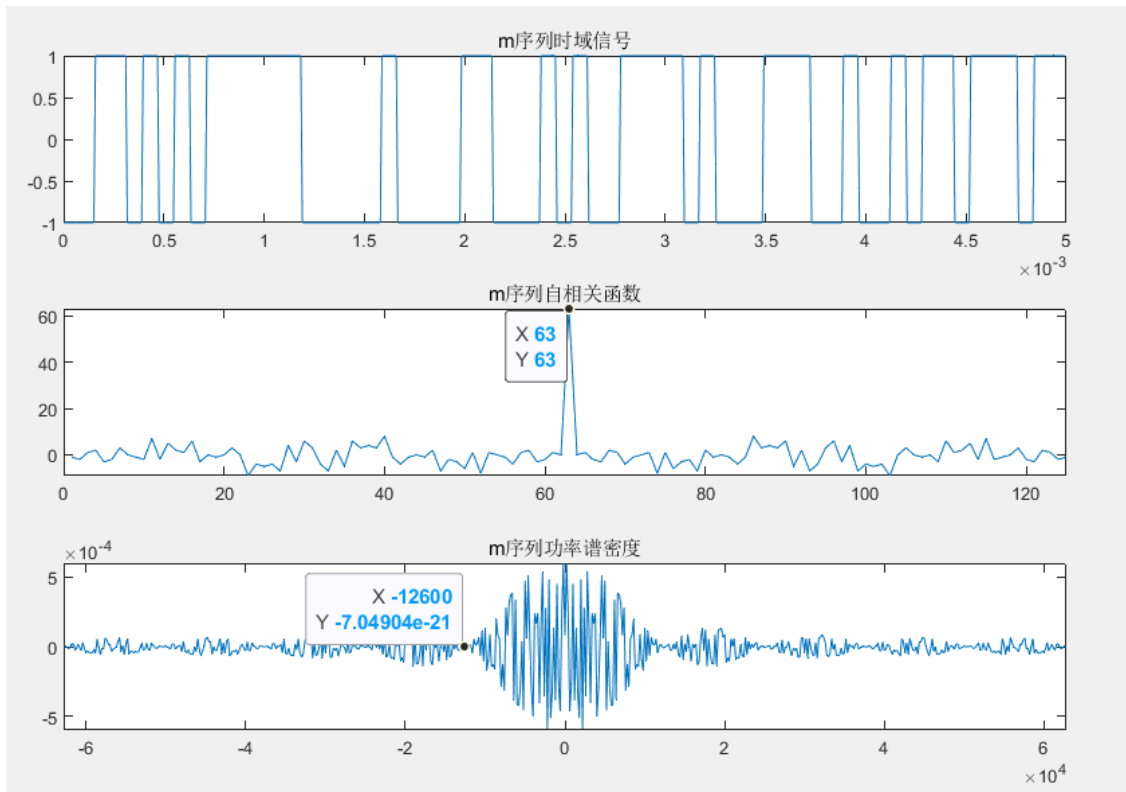
initial=[1 0 1 1 0 0]; % 6阶
feedback=103;
m = mseq(initial,feedback,0);
m = 2*m - 1;

x=rectpulse(m,length(t)/length(m)); % 脉冲成型
mft=fft(x)/fs; % fft

subplot(3,1,1)
plot(t,x)
title('m序列时域信号')
subplot(3,1,2)
plot(xcorr(m))
title('m序列自相关函数')
axis([0 125 -9 length(m)])

```

```
subplot(3,1,3)
plot(f,fftshift(mft))
title('m序列功率谱密度')
axis([-62800 62800 -0.0006 0.0006])
% 如何计算带宽：先求门信号的FT，找出第一过零点带宽f=1/门信号宽度，
% 门信号宽度为5ms（总时间）/63（扩频码长）/10（脉冲成型）
```



7) m序列个数

### 2.2.4 m序列的个数

理论分析给出  $n$  级线性移位寄存器能够生成的 m 序列的个数为

$$N_m = \frac{\Phi(2^n - 1)}{n}$$

其中，欧拉函数定义为

$$\Phi(n) = \begin{cases} 1, & n = 1 \\ \prod_{i=1}^k p_i^{a_i-1} (p_i - 1), & n = \prod_{i=1}^k p_i^{a_i} \text{ (素数分解)} \\ p - 1, & n = p \text{ 为素数} \end{cases} \quad (2-19)$$

式中， $p$ 、 $p_i (i=1, 2, \dots, k)$  为素数。

例如  $n=6$  时，可得

$$N_m = \frac{\Phi(2^6 - 1)}{6} = \frac{\Phi(63)}{6} = \frac{\Phi(7 \times 3^2)}{6} = \frac{36}{6} = 6$$

再如  $n=9$  时，可得

$$N_m = \frac{\Phi(2^9 - 1)}{9} = \frac{\Phi(511)}{9} = \frac{\Phi(73 \times 7)}{9} = \frac{72 \times 6}{9} = 48$$

# Gold序列

Gold序列是由m序列优选对模2加得来;

m序列优选对: 反馈系数不同的同阶m序列, 互相关值小于一定数值的情况下就是m序列优选对;

设序列 $\{a\}$ 是对应 $n$ 阶本原多项式 $f(x)$ 产生的 $m$ 序列, 序列 $\{b\}$ 是对应 $n$ 阶本原多项式 $g(x)$ 产生的 $m$ 序列; 若它们的互相关函数值 $R_{ab}(\tau)$ 满足不等式

$$|R_{ab}(k)| \leq \begin{cases} 2^{\frac{n+1}{2}} + 1, & n \text{ 为奇数} \\ 2^{\frac{n+2}{2}} + 1, & n \text{ 为偶数, } n \text{ 不是 } 4 \text{ 的整数倍} \end{cases} \quad (2-20)$$

则 $f(x)$ 和 $g(x)$ 产生的 $m$ 序列 $\{a\}$ 和 $\{b\}$ 就构成一优选对。

当 $n$ 等于6时,  $2^{((n+2)/2)+1}=17$ , 满足优选对条件

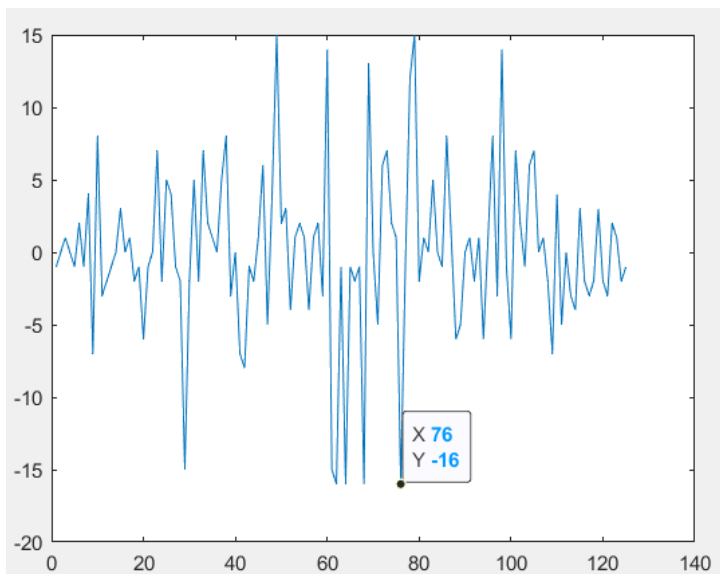
```
% m序列优选对
% 两个反馈系数生成的m序列互相关函数小于一定值, 称为m序列优选对
close all; clear; clc;
initial=[1 0 1 1 0 0];          % 6阶
feedback=103;
m1 = mseq(initial,feedback);
m1 = 2*m1 - 1;

initial=[1 0 1 1 0 0];          % 6阶
feedback=147;
m2 = mseq(initial,feedback);
m2 = 2*m2 - 1;

% 互相关
a=xcorr(m1,m2);
disp(['最大值:', num2str(max(abs(a)))])
plot(a)
```

程序输出

> 最大值:16





下图给出部分m序列优选对的本原多项式

表 2-8 部分优选对码表

级数	基准本原多项式	配对本原多项式
7	211	217, 235, 277, 325, 203, 357, 301, 323
	217	211, 235, 277, 325, 213, 271, 357, 323
	235	211, 217, 277, 325, 313, 221, 361, 357
	236	217, 203, 313, 345, 221, 361, 271, 375
9	1021	1131, 1333
	1131	1021, 1055, 1225, 1725
	1461	1743, 1541, 1853
10	2415	2011, 3515, 3177
	2641	2517, 2218, 3045
11	4445	4005, 5205, 5337, 5263
	4215	4577, 5747, 6765, 4563

## Gold序列生成器

```
%% Gold序列发生器
% initial: 系统初始状态（非全零，阶数符合即可）
% feedback1: 反馈系数（查表，八进制）
% feedback2: 反馈系数（查表，八进制）
% shift: 用于移位模2加
% gold1,gold2: 生成的两个gold序列
function [gold1,gold2]=goldseq(initial,feedback1,feedback2,shift)

n = length(initial); % 阶数
m1 = mseq(initial,feedback1,0); % 生成两个m序列
m2 = mseq(initial,feedback2,0);

% 生成两个gold序列
gold1=mod(m1+m2,2); % 模2加
gold2=mod(m1+circshift(m2,shift),2); % 移位模2加

% 以下程序判断是否为m序列优选对
m1=2*m1-1; % 逻辑映射
m2=2*m2-1;
res=max(abs(xcorr(m1,m2))); % 求互相换函数

if(rem(n,2)==0) % 判断是否为m序列优选对
    if(max(res)>2^(n/2+1)+1)
        disp('非m序列优选对')
    end
end
if(rem(n,2)~=0)
    if(max(res)>2^(n/2+1/2)+1)
        disp('非m序列优选对')
    end
end
end
```

# Gold序列性质

1) 不再具有m序列性质，但是任意互相关函数都满足

$$|R_{\omega}(k)| = \begin{cases} 2^{\frac{n+1}{2}} + 1, & n \text{ 为奇数} \\ 2^{\frac{n+2}{2}} + 1, & n \text{ 为偶数, } n \text{ 不是 } 4 \text{ 的整数倍} \end{cases}$$

2) Gold序列数量远远大于m序列，都可以做地址码；

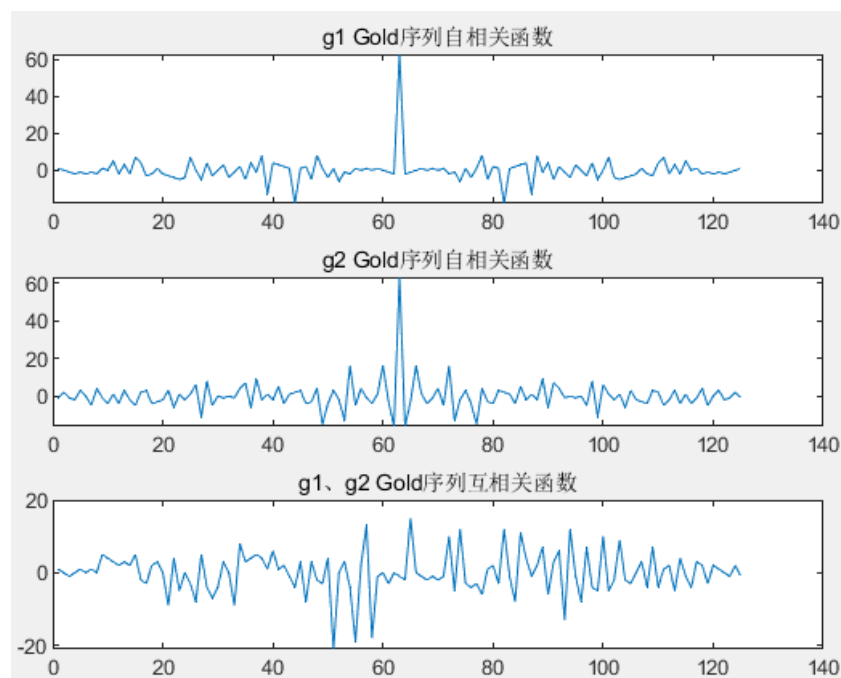
3) n为奇数时，50%的互相关值为-1；n为偶数时（不被4整除），75%的互相关值为-1；

4) 自相关和互相关性

```
%% Gold序列相关函数
close all; clear; clc;
initial=[1 0 1 1 0 0];          % 6阶
feedback1=103;
feedback2=147;
[g1,g2]=goldseq(initial,feedback1,feedback2,20);
g1 = 2*g1 - 1;                  % 逻辑映射
g2 = 2*g2 - 1;

subplot(3,1,1)
plot(xcorr(g1))
title('g1 Gold序列自相关函数')
subplot(3,1,2)
plot(xcorr(g2))
title('g2 Gold序列自相关函数')
subplot(3,1,3)
plot(xcorr(g1,g2))
title('g1、g2 Gold序列互相关函数')
```

程序输出



# 平衡Gold序列

在一个周期里，平衡Gold序列的1比0多一个

```
%% 平衡Gold序列
close all; clear; clc;
initial=[1 0 1 1 0 0];          % 6阶
feedback1=103;
feedback2=147;
[g1,g2]=goldseq(initial,feedback1,feedback2,20);
g1 = 2*g1 - 1;                  % 逻辑映射
g2 = 2*g2 - 1;

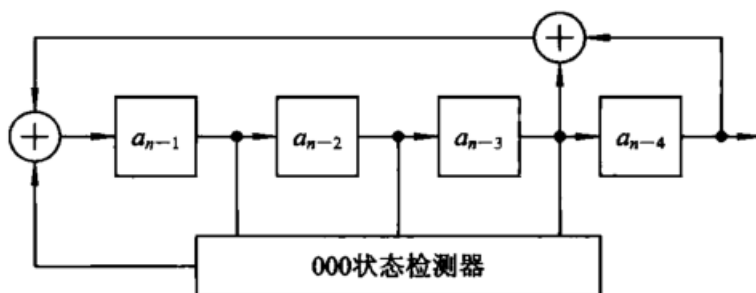
% 判断平衡Gold码
if(sum(g1)==1)
    if(sum(g2)==1)
        disp('是平衡Gold序列')
    end
end
end
```

程序输出

```
> 是平衡Gold序列
```

# M序列

m序列的长度为 $2^n-1$ ，1比0多一个。M序列只是在系统特定状态时补一个0，如下图所示



## M序列生成器

```
%% m/M序列发生器
% initial: 系统初始状态（非全零，阶数符合即可）
% feedback: 反馈系数（查表，八进制）
% mode: 为0时生成m序列，长度 $2^n-1$ ；
%       为1时生成M序列，长度 $2^n$ ；
% m: 生成的m/M二值序列，没有进行逻辑映射；
function [m]=mseq(initial,feedback,mode)

n=length(initial);           % 阶数
temp=de2bi(oct2dec(feedback)); % 反馈系数8转10进制转2进制
temp=flipr(temp);            % 翻转
final=temp(2:length(temp));  % 舍去首位

output=[];
comp=[zeros(1,n-1) 1];      % 生成M序列时使用
for ii=1:2^n-1
    output=[output initial(n)];
    if(mode & initial==comp) % 生成M序列时使用
        output=[output 0];
    end
    temp=mod(sum(final.*initial),2);
    initial=[temp initial(1:n-1)];
end

m=output;                    % 没有进行逻辑映射
```

## M序列性质

- 1) M序列长度为 $2^n$ ，一个周期中，0和1的个数各为 $2^{n-1}$ ；
- 2) 序列游程完全对称；
- 3) 不具有移位相加性；
- 4) 互相关函数的性能不如m序列；

```
%% m和M序列自相关函数特性
close all; clear; clc;
```

```

initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
m1 = mseq(initial,feedback,0);
m1 = 2*m1 - 1;

initial=[1 0 1 1 0 0];           % 6阶
feedback=147;
m2 = mseq(initial,feedback,0);
m2 = 2*m2 - 1;
disp(['m序列互相关最大值',num2str(max(abs(xcorr(m1,m2))))])

initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
m1 = mseq(initial,feedback,1);
m1 = 2*m1 - 1;

initial=[1 0 1 1 0 0];           % 6阶
feedback=147;
m2 = mseq(initial,feedback,1);
m2 = 2*m2 - 1;
disp(['M序列互相关最大值',num2str(max(abs(xcorr(m1,m2))))])

```

程序输出

```

m序列互相关最大值16
M序列互相关最大值19

```

初始状态改变时，互相关函数最大值也会改变

```

% 初始状态改变
initial=[1 0 0 0 0 0];

% 程序输出
> m序列互相关最大值17
> M序列互相关最大值17

```

5) M序列数量远大于m序列;

表 2-13 M 序列和 m 序列数量与  $n$  的关系

$n$	1	2	3	4	5	6
$\Phi(2^n - 1)/n$	1	1	2	2	6	6
$2^{2^{n-1}-n}$	1	1	2	16	2048	67 108 864

# Kasami序列

Kasami序列是由m序列之上构建而来;

选取长度为 $2^n-1$  ( $n$ 为偶数) 的m序列, 因式分解 $2^n-1=(2^{n/2}-1)(2^{n/2}+1)=p*q$ , 对m序列以 $q$ 为间隔进行抽样, 得到长度为 $p$ 的序列。可以证明该序列仍为m序列。将此序列重复 $q$ 次, 与原序列模2加, 即可得到小集合Kasami序列。当改变序列的相位时, 就可以得到一个新的Kasami序列;

## 小集合Kasami序列生成器

```
function [kasami]=kasamiseq(initial,feedback,shift)

n=length(initial);           % 阶数
if(rem(n,2)~=0)
    disp('Kasami序列要求阶数为偶数!')
end

m = mseq(initial,feedback,0); % 生成m序列
ms=flipr(m);                 % 翻转
temp1 = 2^(n/2)+1;
temp2 = 2^(n/2)-1;

ka=[];
for i=1:temp2                 % m序列间隔temp1挑选
    ka=[ka ms(1+(i-1)*temp1)];
end

if(shift>temp2)
    disp('移位数大于阶数!')
end
ka=circshift(ka,shift);       % 循环移位

kas=[];
for i=1:temp1                 % 重复temp1次
    kas=[kas ka];
end

kasami=flipr(mod(ms+kas,2)); % 模2加
```

## 小集合Kasami序列性质

1) 平衡性: 小集合Kasami平衡性较差, 只有原m序列具有理想平衡性;

```

close all; clear; clc;
initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
k1 = kasamiseq(initial,feedback,0);
k1 = 2*k1-1;

initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
k2 = kasamiseq(initial,feedback,2);
k2 = 2*k2-1;

sum(k1)
sum(k2)

```

输出结果

```

> ans = -7
> ans = 9

```

修改初始状态，可以得到较为平衡的序列

```

% 修改初始状态
initial=[1 0 1 1 0 1];           % 6阶

% 输出结果
> ans = 1
> ans = 1

```

2) 小集合Kasami数量远远多于m序列，且Kasami 小集合序列的相关性优于 Kasami 大集合序列，因而在实际应用中多用 Kasami 小集合序列，此处不再研究大集合Kasami序列。

3) 自相关性和互相关性：

```

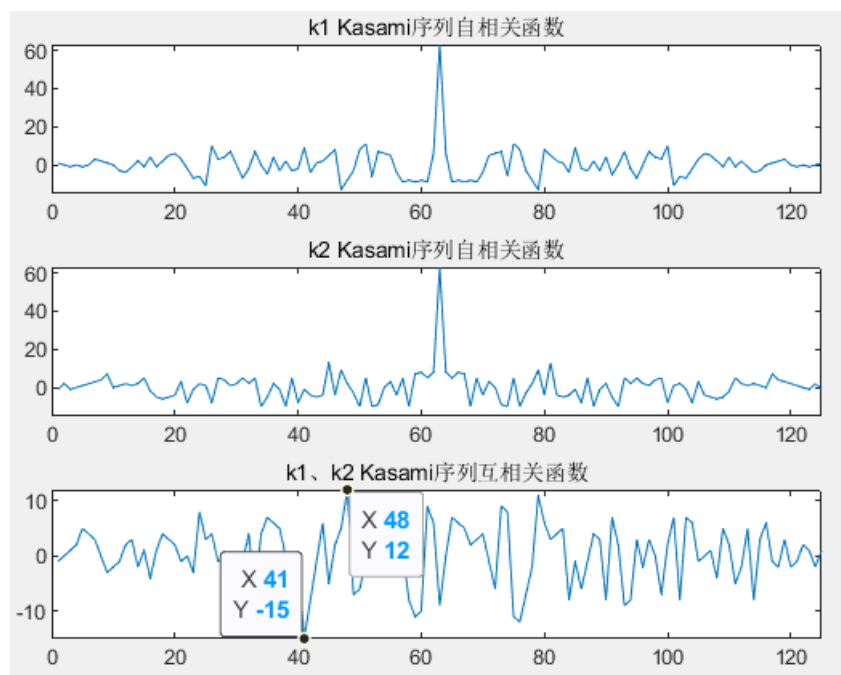
%% Kasami序列自相关性和互相关性
close all; clear; clc;
initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
k1 = kasamiseq(initial,feedback,0);
k1 = 2*k1-1;

initial=[1 0 1 1 0 0];           % 6阶
feedback=103;
k2 = kasamiseq(initial,feedback,2);
k2 = 2*k2-1;

subplot(3,1,1)
plot(xcorr(k1))
title('k1 Kasami序列自相关函数')
subplot(3,1,2)
plot(xcorr(k2))
title('k2 Kasami序列自相关函数')
subplot(3,1,3)
plot(xcorr(k1,k2))

```

```
title('k1、k2 Kasami序列互相关函数')
```





## 参考资料

---

[1] 暴宇, 李新民. 扩频通信技术及应用[M]. 西安电子科技大学出版社, 2011.

[2] 田日才, 迟永钢. 扩频通信[M]. 清华大学出版社, 2014.

[3] 李泽帅. 伪随机序列设计及其随机性分析[D]. 电子科技大学, 2019.