Gold Codes

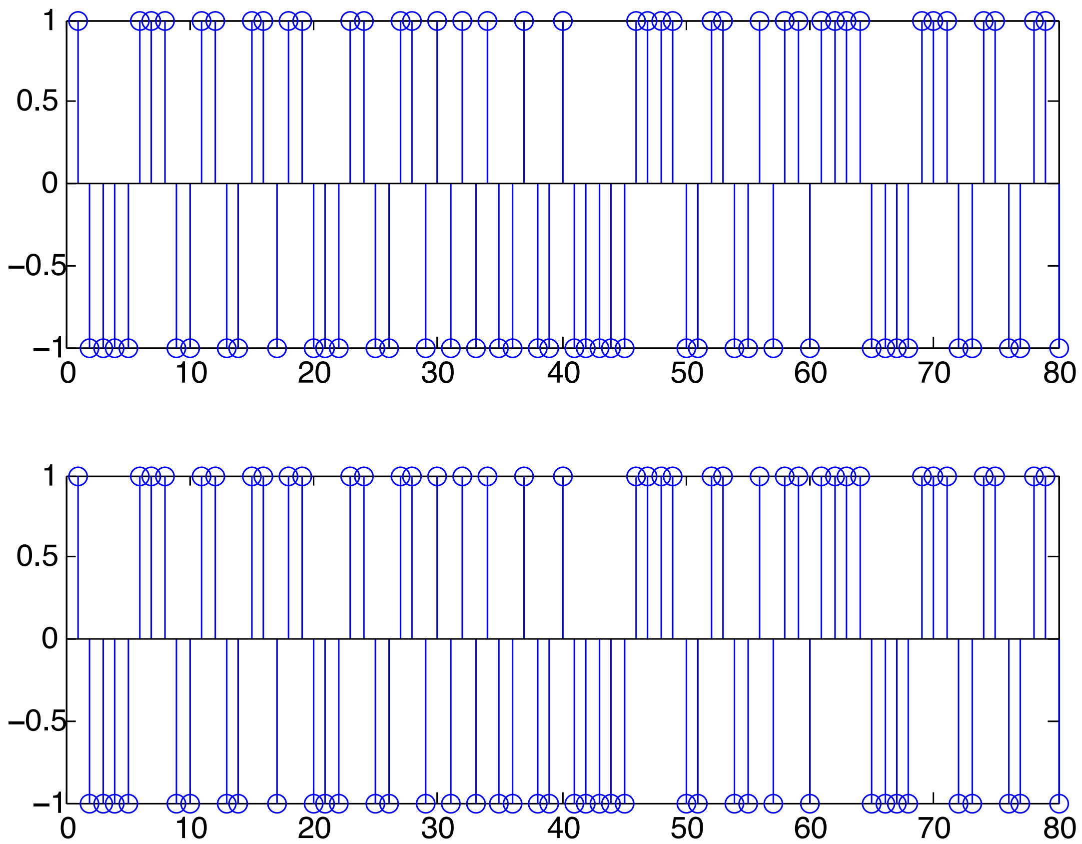


Figure: From the top, Gold code generated with two SSRSG and one SSRSG implementation, respectively

Balanced Gold Codes

- In most cases, we prefer spreading codes that have a balanced number of zeros and ones as with the ML SSRS
- Family of Gold codes can be classified into tree sets when r is odd

Set	Number of Ones	Number of Codes
1	2^{r-1}	$2^{r-1}+1$
2	$2^{r-1}+2^{\frac{r-1}{2}}$	$2^{r-2}-2^{\frac{r-3}{2}}$
3	$2^{r-1}-2^{\frac{r-1}{2}}$	$2^{r-2}+2^{\frac{r-3}{2}}$

- It is clear that codes in Set 1 are the balanced codes
- Portion of balanced codes in a family of Gold codes

$$\eta = \frac{2^{r-1}+1}{2^r+1} \approx 0.5 \text{ for large } r$$

- We may claim that approximately half of Gold codes of a given order are balanced

Balanced Gold Codes

- In order to isolate the balanced Gold codes, we need to introduce the concept of characteristic phase of an ML SSRS

Definition 7.4

The characteristic phase of an ML SSRS is the phase such that sampling the sequence at every other symbol (decimated by a factor of 2) at the phase results in the original sequence

Theorem 7.5

The initial load $a^c(D)$ given in below results in the characteristic phase for a given ML SSRSG with generator $g(D)$

$$a^c(D) = \begin{cases} \frac{d\{Dg(D)\}}{dD}, & r = \text{odd} \\ g(D) + \frac{d\{Dg(D)\}}{dD}, & r = \text{even} \end{cases}$$

Balanced Gold Codes

Example 7.6

Consider the primitive polynomial $g(D) = D^4 + D + 1$

- Characteristic phase

$$\begin{aligned} a^c(D) &= g(D) + \frac{d\{Dg(D)\}}{dD} \\ &= D^4 + D + 1 + 5D^4 + 2D + 1 \\ &= D^4 + D + 1 + D^4 + 1 = D \end{aligned}$$

- The generated sequence with $a^c(D)$

$$\begin{aligned} b^c(D) &= \frac{D}{D^4 + D + 1} \\ &= D + D^2 + D^3 + D^4 + D^6 + D^8 + D^9 + D^{12} + D^{16} + \cdots \end{aligned}$$

which gives

$$b_c = 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, \cdots$$

- Decimation on b_c by 2 gives $b_c' = 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, \cdots$

Balanced Gold Codes

Example 7.7

Consider the primitive polynomial $g(D) = D^5 + D^2 + 1$

- Characteristic phase

$$a^c(D) = \frac{d\{D^6 + D^3 + D\}}{dD} = D^2 + 1$$

- Note that, if r is odd, then $a^c(D)$ is of form $1 + a^*(D)$ where $a_0^* = 0$
- First symbol of an ML sequence whose order is odd in its characteristic phase will be a one

Theorem 7.8

- Let $g_1(D)$ and $g_2(D)$ be a preferred pair of primitive polynomials of an odd order
- The Gold code generated by $g_1(D)$ and $g_2(D)$ produces a balanced Gold code if the initial load corresponding to $g_2(D)$ is chosen so that the first '1' in the characteristic phase of the sequence lines up with a zero in the sequence generated by $g_1(D)$

Balanced Gold Codes

Example 7.9

- Consider the following preferred primitive polynomial pair

$$\begin{aligned} g_1(D) &= D^3 + D + 1 = (13)_8 \\ g_2(D) &= D^3 + D^2 + 1 = (15)_8 \end{aligned}$$

- Decimation by 3 of the sequence generated by $g_1(D)$ yields the sequence generated by $g_2(D)$ (Theorem 6.6)

$$\begin{aligned} g'(\alpha^3) &= \alpha^9 + \alpha^6 + 1 \\ &= (\alpha+1)^3 + (\alpha+1)^2 + 1 = (\alpha+1)^2\alpha + 1 \\ &= \alpha^3 + \alpha + 1 = 0 \leftarrow \alpha \text{ is the root of } g_1(D) \end{aligned}$$

- Initial load $a_2^c(D)$ that results in the characteristic phase is

$$a_2^c(D) = \frac{d\{D^4 + D^3 + D\}}{dD} = D^2 + 1$$

Balanced Gold Codes

- Let the initial load corresponding to $g_1(D)$ be $a_1(D) = 1$

$$\begin{aligned} b_1 &= 1,1,1,0,1,0,0,1,1,1,0,\cdots \\ b_2^c &= 1,0,0,1,0,1,1,1,0,0,1,\cdots \end{aligned}$$

- For $b_1 \oplus b_2^c$ to be a balanced Gold code, the '1' (noted by red color) should line up with a zero in b_1 before being added

$$\begin{aligned} b_1 &= 1,1,1,0,1,0,0|,1,1,1,0,\cdots \\ b_3 &= 0,1,1,1,0,0,1|,0,1,1,1,\cdots \leftarrow b_2^c \text{ delayed by three clocks} \\ b_1 \oplus b_3 &= 1,0,0,1,1,0,1|,1,0,0,1,\cdots \end{aligned}$$

Balanced Gold Codes

- Note that $b_1 \oplus b_3$ is balanced and there are two more balanced codes

Procedure for balanced Gold code generation

1. Select a preferred pair of ML SSRS $b_1(D)$ and $b_2(D)$
2. Implement the Gold code generator
3. Set the initial load of the lower ML SSRSG so that it is in its characteristic phase
4. Set the initial load of the upper ML SSRSG so that $a_0^1 = 0$

- This procedure will generate a family of 2^{r-1} balanced Gold codes

Balanced Gold Codes

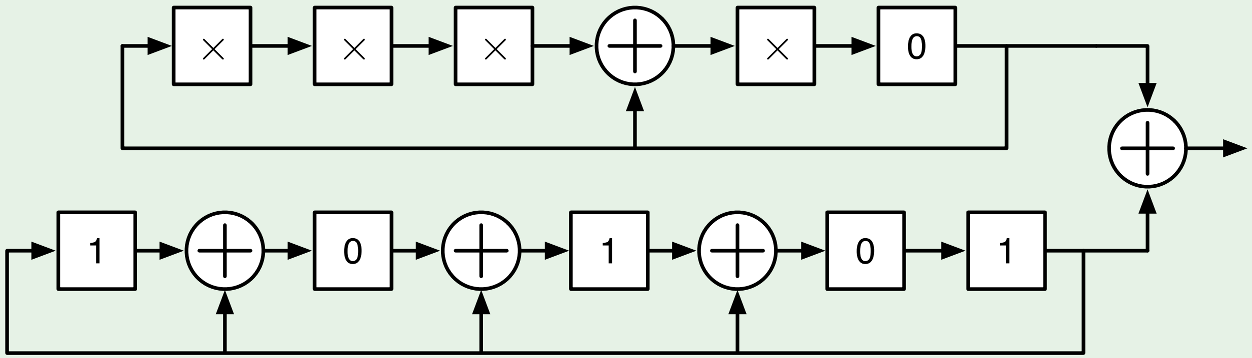
Example 7.10

- Let us generate a set of balanced Gold codes of length $2^5 - 1$

$$\begin{aligned} g_1(D) &= D^5 + D^2 + 1 \\ g_2(D) &= D^5 + D^4 + D^3 + D^2 + 1 \end{aligned}$$

- The initial load for $g_2(D)$

$$a_2^c(D) = \frac{d\{D^6 + D^5 + D^4 + D^3 + D\}}{dD} = D^4 + D^2 + 1$$



- The family of $2^{5-1} = 16$ balanced Gold codes

Welch's Lower Bound

- Welch's lower bound on the peak cross correlation value among a set of sequences of a given length

Theorem 8.1

The peak cross correlation $\theta_{\max}$ between any pair of sequences in a family of M binary SSRS of period N satisfy the following bound

$$\theta_{\max} \leq \sqrt{\frac{M-1}{NM-1}} \triangleq \theta^{\text{Welch}} \approx \frac{1}{\sqrt{N}} \text{ for large } M$$

- This lower bound on the maximum cross correlation is referred to as the Welch's bound

Welch's Lower Bound

- The peak correlation value of Gold codes

$$
\begin{aligned}
\theta_{\max}^{\text{Gold}} &= \begin{cases} \frac{1}{N}\left(1+2^{\frac{r+1}{2}}\right), & r = \text{odd} \\ \frac{1}{N}\left(1+2^{\frac{r+2}{2}}\right), & r = \text{even and not divisible by } 4 \end{cases} \\
&\approx \begin{cases} \sqrt{2}\cdot 2^{-\frac{r}{2}}, & r = \text{odd} \\ 2\cdot 2^{-\frac{r}{2}}, & r = \text{even and not divisible by } 4 \end{cases}
\end{aligned}
$$

- Gold cod possesses a peak cross correlation value that is $\sqrt{2}$ (r=odd) or 2 (r=even and not divisible by 4) times larger than that given by the Welch's bound

Kasami Codes

- We ask the question whether there exists a code whose peak cross correlation value actually achieves the Welch's lower bound
- The answer to this question is yes and a family of codes called the Kasami codes

Definition 8.2

- Start with an ML SSRS $\{b_n\}$ of an even order r
- Decimate the sequence by a factor of $2^{\frac{r}{2}} + 1$ to obtain a second sequence $\{b_n^d\}$
- The period of $\{b_n^d\}$ is $2^{\frac{r}{2}} - 1$
- By adding $\{b_n\}$ with $\{b_n^d\}$ and all $2^{\frac{r}{2}} - 1$ possible phase shifts of $\{b_n^d\}$ and including original sequence $\{b_n\}$, we obtain the family of $2^{\frac{r}{2}}$ Kasami codes of length $N = 2^r - 1$

Kasami Codes

Theorem 8.3

The side lobe of the auto correlation function and the cross correlation function between any pair of Kasami codes is three valued taking on values of

$$-\frac{1}{N}, -\frac{1}{N}\left[\eta(r)+1\right], \frac{1}{N}\left[\eta(r)-1\right]$$

where $\eta(r) = 2^{\frac{r}{2}}$

Kasami Codes

Lemma 8.4

The family of Kasami codes achieves the Welch's bound

- Proof
  - The peak cross correlation value between the Kasami codes $\theta_{\max}^{\text{Kasami}}$ satisfies

$$\theta_{\max}^{\text{Kasami}} = \frac{\eta(r)+1}{N} \rightarrow N\theta_{\max}^{\text{Kasami}} = \eta(r)+1$$
$$= 2^{\frac{r}{2}}+1 = M+1$$

where $M = \frac{r}{2}$ is the number of codes in the family of Kasami codes

Kasami Codes

- Welch's lower bound on the peak cross correlation values for the parameters of the Kasami codes is given by

$$
\begin{aligned}
N\theta^{\text{Welch}} &= \sqrt{\frac{N^2(M-1)}{NM-1}} \\
&= \sqrt{\frac{(M^2-1)^2(M-1)}{(M^2-1)M-1}} \\
&= \sqrt{\frac{M^5-M^4-2M^3+2M^2+M+1}{M^3-M+1}} \\
&= \sqrt{M^2-M-1+\frac{M}{M^3-M+1}} \\
&= \sqrt{M^2-M-1+\lambda}
\end{aligned}
$$

where

$$0 < \lambda = \frac{M}{M^3-M+1} < 1$$

Kasami Codes

- Hence,

$$
\begin{aligned}
N\theta^{\text{Welch}} &> \sqrt{M^2 - M - 1} \\
&\geq \sqrt{M^2 - 2M + 1} \\
&= M - 1
\end{aligned}
$$

- Note that $N\theta_{\max}^{\text{Kasami}} = M + 1$
- The last inequality follows from the fact that $M = 2^{\frac{r}{2}}$ for r even
- Since the value of the cross correlation times N must be an odd integer[1], $M + 1$ is the smallest possible peak cross correlation value predicted by the Welch's bound

[1] N and M are integer and N is odd