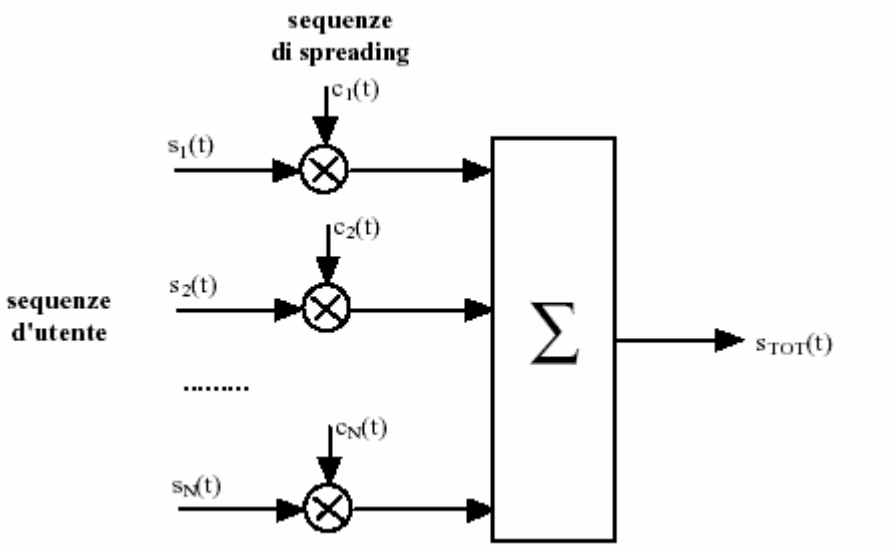
Nota sulle SEQUENZE PN
e CODICI di Gold.

G. Giunta

Nelle comunicazioni mobili, le proprietà di autocorrelazione e di intercorrelazione delle sequenze di spreading sono utilizzate per realizzare comunicazioni ad accesso multiplo (CDMA). Infatti, là dove si può realizzare un perfetto sincronismo, un insieme di codici ortogonali può essere utilizzato per realizzare una multiplazione a divisione di codice.

La tecnica CDMA (Code Division Multiple Access), utilizzata nei sistemi di terza generazione, permette a tutti gli utenti di trasmettere alla stessa frequenza, nello stesso istante.
Col CDMA ogni utente si vedrà assegnato tutto lo spettro per tutto il tempo della comunicazione. Per evitare che i segnali dei diversi comunicatori si sommino indistintamente, la separazione tra i vari utenti si ottiene assegnando a ciascuno un "codice di canalizzazione" .
Le sequenze sono usate per codificare in modo *univoco* l'informazione d'utente da trasmettere. Moltiplicando il segnale per la sequenza si ottiene una effetto di spreading del segnale in frequenza, cioè un allargamento della banda del segnale.
L'operazione consiste nell'associare a ciascun segnale da trasmettere un codice, tramite un'operazione di multlipazione, ossia ciascun segnale viene moltiplicato

con una sequenza binaria caratterizzata da una velocità di trasmissione (chip rate) maggiore della velocità dell'informazione da trasmettere. I bit ottenuti dopo quest'operazione sono detti chip. A questo punto le sequenze, così codificate, vengono sommate e trasmesse contemporaneamente sullo stesso canale.

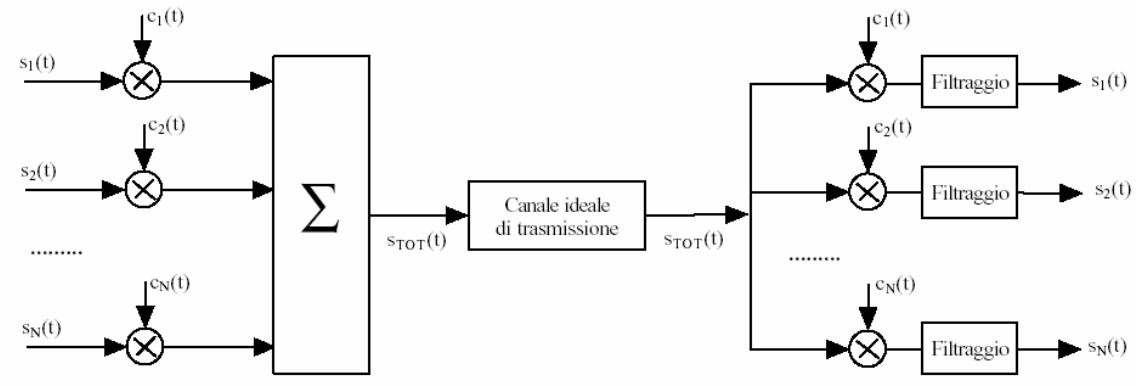


In Fig: Generazione di un segnale (sovrapposizione di segnali multipli ciascuno caratterizzato da una propria sequenza di spreading)

Essendo le sequenze diverse fra loro e scelte in modo che siano ortogonali (cross-correlazione nulla), in ricezione e sufficiente correlare il segnale ricevuto con la sequenza stessa; ciò fa sì che in condizioni ideali l'operazione opposta, DESPREADING, annulli l'effetto dell'interferenza mutua e permetta di estrarre il segnale desiderato.

Il codice da usare in ricezione sarà comunicato al terminale mobile (MS) tramite segnalazione in fase di negoziazione della connessione.

Ciò che accade è che la sequenza d'informazione "criptata" con il codice usato dal ricevitore viene recuperata, mentre le altre sequenze che usano codici diversi sono cancellate o fortemente attenuate; infatti, tramite poi, un filtro passa-basso si seleziona la componente utile del segnale.



In Fig: Intero sistema di trasmissione CDMA

In condizioni reali i disturbi e le distorsioni che subiscono i segnali lungo il canale degradano le condizioni di *ortogonalità,* perciò il numero di segnale che si possono sovrapporre sullo stesso canale è limitato.Quindi la capacità del sistema è limitata dal livello d'interferenza reciproca dopo l'operazione di despreading.

1.1 Codici OVSF

I codici OVSF (*Ortogonal Variable Spreading Factor)* sono sequenze ortogonali di lunghezze differenti adattabili a trasmissioni a pacchetto multirate. Infatti variare la velocità significa cambiare il numero di dati da trasmettere

all'interno del proprio slot, di durata fissa, e quindi si devono usare codici con un numero variabile di chips.

Supponendo di poter gestire flussi di dati con velocità variabile da R_{min} a $R_{max}=2^kR_{min}$, per poter allocare i vari flussi nella banda, che non varia, bisogna variare il numero di chip associati ad ogni singolo bit informativo aumentando (o diminuendo) la lunghezza delle sequenze di spreading.

Ciò permette di mantenere l'ortogonalità tra diversi canali fisici caratterizzati da differenti *bit rate* e fattori di spreading, così da garantire la condivisione delle risorse tra più utenti. L'uso di codici OVSF riduce in modo efficace l'interferenza dovuta ad accesso multiplo (*MAI, multiple access interference*).

Considerando:

$R_c = 2^nR_{min}$ banda a disposizione

SF = *spreading factor* = $R_c/R_b = (2^n\ R_{min})/R_{min} = 2^n$ Massimo fattore di espansione utilizzabile

Se la velocità dei bit informativi aumenti di un fattore 2^k, affinché la banda rimanga invariata bisognerà ridurre il fattore di espansione della stessa quantità, ottenendo il suo valore minimo $SF = (2^n\ R_{min}/2^k\ R_{min}) = 2^{n-k}$

Tali sequenze binarie, con valori nell'alfabeto [-1,1], si possono ricavare in modo semplice dalle funzioni di Walsh, ottenute a partire dalle matrici di Hadamard. Le matrici di Hadamard della lunghezza desiderata possono essere generate attraverso la procedura ricorsiva:

$$\mathbf{H}_1 = [0]\ ,\ \mathbf{H_2} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix},\ \mathbf{H}_4 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix},\ \mathbf{H}_{2N} = \begin{bmatrix} \mathbf{H}_N & \mathbf{H}_N \\ \mathbf{H}_N & \overline{\mathbf{H}}_N \end{bmatrix}$$

dove N, lunghezza delle righe. Come si può facilmente notare, queste matrici contengono una riga di tutti ‘0’ mentre le rimanenti righe hanno ognuna un numero uguale di ‘1’ e ‘0’.

Un codice di Walsh di lunghezza $N = 2^n$ è formato dalle righe (o colonne) della matrice di Hadamard H_N in cui ‘0’ e ‘1’ sono codificati rispettivamente come ‘1’ e ‘-1’. Dal modo in cui sono state costruite le matrici si può immediatamente vedere che due parole del codice di Walsh sono ortogonali: ogni coppia di codici contiene infatti N/2 bit uguali e altrettanti diversi.

Per due parole di codice distinte $c_{N,i}, c_{N,j}$ di lunghezza *N* vale la relazione

$$\sum_{t=0}^{N-1} c_{N,i}(t) c_{N,j}(t) = 0 \qquad \text{con } i \neq j$$

può essere vista come la correlazione mutua delle due sequenze, valutata in $\tau = 0$

In trasmissione ogni bit è moltiplicato per una funzione di Walsh e lo *spreading factor* (SF) risulta pari ad *N*. I codici di spreading ortogonali possono essere usati se tutti gli utenti che condividono lo stesso canale sono sincronizzati nel tempo con un’accuratezza della frazione del chip in quanto la correlazione mutua tra versioni traslate di due funzioni di Walsh non è nulla. Alcune funzioni sono infatti la versione traslata di altre.

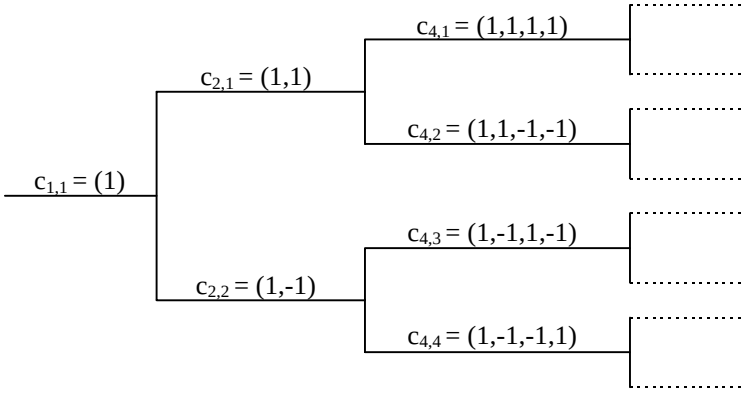
1.1.1 Variable Length Ortogonal Codes

Dal momento che la banda del segnale espanso è la stessa per tutti gli utenti è necessario usare numerosi fattori di spreading nei canali fisici per supportare trasmissioni multi rate.

Un metodo per ottenere codici ortogonali di varia lunghezza che mantengano l'ortogonalità tra differenti rate e fattori di spreading si basa sulla trasformazione modificata di Hadamard.

Questi codici ortogonali di lunghezza variabile possono essere generati ricorsivamente usando la struttura ad albero, dove ad ogni livello corrisponde uno specifico fattore di spreading SF.

Sono riportate due possibili rappresentazioni dei codici OSVF: la struttura ad albero e la forma matriciale



$$C_{1,1} = 1\begin{bmatrix} C_{2,1} \\ C_{2,2} \end{bmatrix} = \begin{bmatrix} C_{1,1} & C_{1,1} \\ C_{1,1} & \overline{C_{1,1}} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} C_{4,1} \\ C_{4,2} \\ C_{4,3} \\ C_{4,4} \end{bmatrix} = \begin{bmatrix} C_{2,1} & C_{2,1} \\ C_{2,1} & \overline{C_{2,1}} \\ C_{2,2} & C_{2,2} \\ C_{2,2} & \overline{C_{2,2}} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} C_{2^{n+1},1} \\ C_{2^{n+1},2} \\ C_{2^{n+1},3} \\ C_{2^{n+1},4} \\ \vdots \\ C_{2^{n+1},2^{n+1}-1} \\ C_{2^{n+1},2^{n+1}} \end{bmatrix} = \begin{bmatrix} C_{2^n,1} & C_{2^n,1} \\ C_{2^n,1} & \overline{C_{2^n,1}} \\ C_{2^n,2} & C_{2^n,2} \\ C_{2^n,2} & \overline{C_{2^n,2}} \\ \vdots & \vdots \\ C_{2^n,2^n} & C_{2^n,2^n} \\ C_{2^n,2^n} & \overline{C_{2^n,2^n}} \end{bmatrix}$$

Figura Descrizione matriciale (con metodo di generazione) dei codici OSVF.

La matrice N-ma è quadrata di ordine NxN con $N = 2^n$, le cui righe rappresentano il livello dell'albero corrispondente al fattore di espansione SF = N, C_N (1, 2,..., N) rappresenta una sequenza di lunghezza N, ottenuta in modo ricorsivo moltiplicando le sequenze dei livelli precedenti, tra loro e con il loro complemento a due.

Alcune proprietà:

- I codici dello stesso livello sono codici di Walsh-Hadamard e quindi ortogonali.
- Due codici qualsiasi, appartenenti a livelli diversi, sono ortogonali se quello di livello superiore non `e stato ricavato a partire da quello di livello inferiore. In altre parole un codice può essere usato in una cella se e solo se nessun altro codice `e presente sul percorso dal codice considerato alla radice dell'albero, o nel sottoalbero che ha origine dal codice. In questo modo il numero di codici disponibili non `e fissato ma dipende dal rate e quindi dal fattore di spreading di ognuno dei canali fisici.

1.2 Rumore pseudo casuale

Una sequenza di codice pseudo noise (PN) è usata come mezzo per l'allargamento dell'ampiezza di banda per segnali di energia.
La scelta di un buon codice è importante, perché il tipo e la lunghezza del codice limita le capacità del sistema.
La sequenza di codice Pn è una sequenza, periodica di 0 e 1.

Esternamente sembra una sequenza random ma per chi conosce il codice non lo è. Si hanno due tipi di sequenze: le sequenze corte caratterizzate dal fatto che si ha una stessa sequenza PN per ciascun simbolo; le sequenze lunghe, la sequenza periodica PN è di molto più lunga rispetto al simbolo, cosicché a ciascun simbolo è associato un differente modello.

- I Long code sono costituiti da sequenze periodiche di periodo 2^{42}-1 generate da registri LFSR e sono usate per effettuare lo spreading nel *uplink*. Stazioni base differenti non sono distinte da codici differenti ma dalle relative fasi. La somma tra i long ed entrambi gli shorth code (I e Q) assicura che la cross-correlazione tra i segnali provenienti da diverse stazioni sia bassa.

  L' espressione polinomiale di un long code è la seguente

$$G(X) = X^{42} + X^{35} + X^{33} + X^{31} + X^{27} + X^{26} + X^{25} + X^{22} + X^{21} + X^{19} + X^{18} + X^{17} + X^{16} + X^{10} + X^{7} + X^{6} + X^{5} + X^{3} + X^{2} + X^{1} + 1$$

- Uno short code è dato da una coppia di sequenze di periodo 2^{15}. le quali derivano da sequenze di periodo 2^{15}-1 prodotte da un registro LFSR aumentate con un bit, pari a zero, per portarne la lunghezza fino ad essere pari ad una potenza di due.

  Per la sequenza I si ha

$$P_I(X) = X^{15} + X^{13} + X^9 + X^8 + X^7 + X^5 + 1$$

  e per la sequenza Q

$$P_Q(X) = X^{15} + X^{12} + X^{11} + X^{10} + X^6 + X^5 + X^4 + X^3 + 1$$

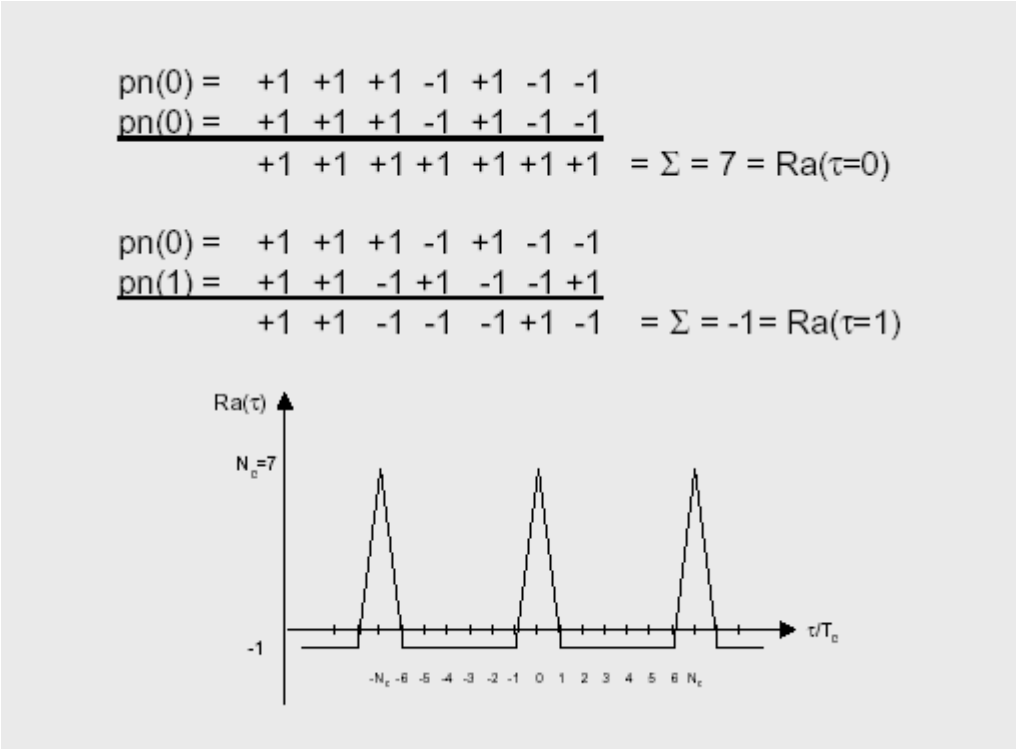
Il bit extra è inserito, in ogni sequenza, immediatamente dopo la comparsa di 14 zeri consecutivi dal registro generatore che accade una volta ogni periodo. Per rate di spreading pari a 1.2288 MHz il periodo degli short code è di 80/3 = 26.666...ms

L'origine del nome pseudo noise risiede nel fatto che il segnale digitale ha una funzione di autocorrelazione molto simile a quella di un segnale a rumore bianco.
La funzione di *autocorrelazione* per la sequenza periodica PN è definita come il numero di concordanze meno il numero di differenze in una parola, col termine di paragone di un periodo intero della sequenza con uno shift ciclico della sequenza stessa.

$$Ra(\tau) = \int_{-N_C T_C/2}^{N_C T_C/2} pn(t)\, pn(t+\tau) dt$$

La funzione di l'autocorrelazione per una sequenze PN, nel caso di sincronizzazione perfetta di due sequenze uguali, ha un largo picco massimo mentre vale –1 nel caso in cui i segnali non siano sincronizzati.

In figura è possibile vedere un esempio di autocorrelazione nel caso in cui i due segnali siano sincronizzati e non.



In Figura: Esempio di autocorrelazione di un segnale PN

La *cross-correlazione* descrive l'interferenza tra codici pn_i e pn_j:

$$Ra(\tau) = \int_{-N_C T_C/2}^{N_C T_C/2} pn_i(t)\, pn_j(t+\tau)\, dt$$

è la misura di concordanza tra due diversi codici pn_i e pn_j.

Quando la cross-correlazione è zero per tutti i τ, i codici sono chiamati *ortogonali*.

Nella CDMA molti utenti utilizzano la stessa banda e trasmettono contemporaneamente. Quando i codici tra gli utenti sono ortogonali non c'è

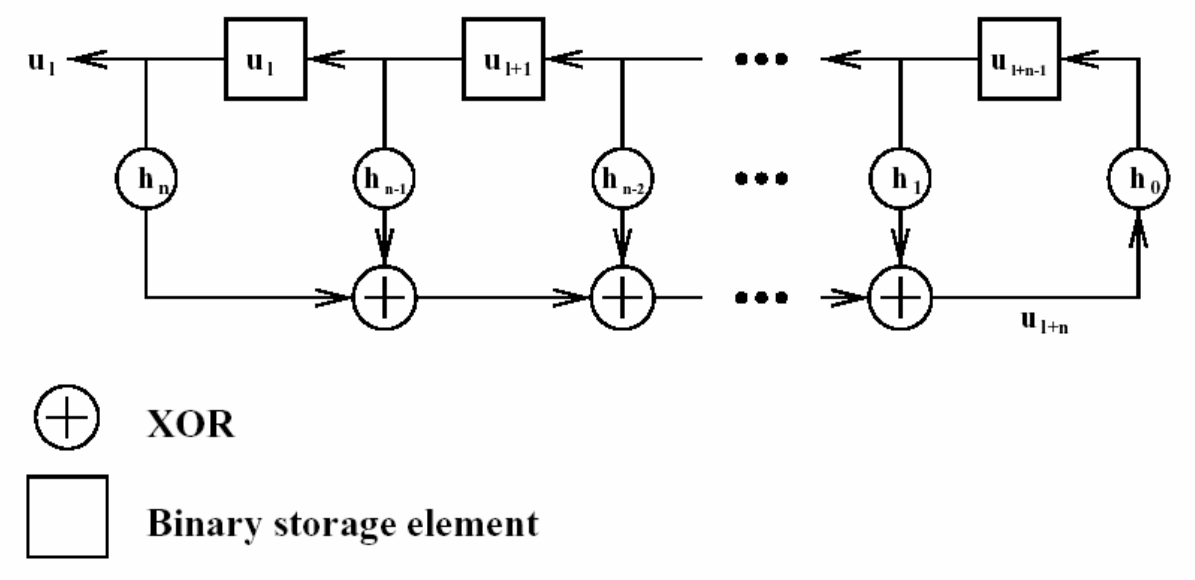
interferenza tra gli utenti dopo l'operazione di despreading e la privacy della comunicazione di ciascun utente è protetta.
Nella realtà i codici non sono perfettamente ortogonali, da ciò ne deriva che la cross-correlazione tra i codici utente introduce una diminuzione delle prestazioni, aumenta il rumore dopo il despreading, cosa che limita il massimo numero di utenti contemporaneamente.

1.3 LFSR: linear feedback shift register

Il progetto di una sequenza è uno dei problemi più importanti nei sistemi ad spread spectrum (SS).
Prima di affrontare questo problema, ricordiamo alcune aspetti importanti delle sequenze di spreading.
Gli elementi della sequenza dovrebbero comportarsi come variabili random, e la sequenze dovrebbe essere pseudo-random: quando si calcola lo spettro di potenza di un segnale a SS, si modellano gli elementi della sequenza come delle variabili casuali. Basandosi su questo modello, è possibile ottenere effetti dell'allargamento dello spettro.
Dovrebbe essere facile, per un trasmettitore e il ricevitore predefinito, generare una sequenza di spreading
Dovrebbe essere difficile per qualunque involontario ricevitore acquisire e rigenerare la sequenza di spreadin.

Le sequenze di spreading sono generalmente generate da feedback shift registers, dal momento che i registri sono facili da costruire. Gli shift register, generano codici che sono periodici e pseudo casuali.

Nella figura è illustrato una possibile rappresentazione di un registro comunemente utilizzato.



In figura: Registro a scorrimento

La sequenza binaria $u = \{u_l\}$ è generata da n-stati dello shift register e pesata con $h_0, h_1, ..., h_{n-1}, h_n$ che assumono valori nell'insieme $\{0,1\}$.

Per ottenere la sequenza di spreading dalla sequenza binaria *u* si definisce una mappa dallo spazio delle sequenze binarie allo spazio delle sequenze bipolari, quindi lo 0 è progettato +1, e 1 sostituito con –1.[4]

Bisogna notare che h_0 deve essere 1, altrimenti l'uscita della sequenza u sarà identicamente nulla, dopo n traslazioni; similmente anche h_n deve essere 1 altrimenti potremmo rimuovere l'ultimo livello di sinistra per ottenere un più corto shift register senza incidere sulla sequenza di uscita.

Dalla figura si vede che la sequenza di uscita soddisfa:

$$u_{l+n} = h_n u_l \oplus h_{n-1} u_{l+1} \oplus ... \oplus h_1 u_{l+n}$$

dove $\oplus$ rappresenta addizione modulo due, ossia l'operazione di x-or.
In genere si rappresentano i pesi (tappi) dello shift register $h_0, h_1, ..., h_{n-1}, h_n$, con un polinomio binario h(x):

$$h(x) = h_0 x^n + h_1 x^{n-1} + ... + h_{n-1} x + h_n$$

Al contrario, possiamo dire che una sequenza binaria u è generata da h(x) se gli elementi della sequenza soddisfano la formula sopra.

I coefficienti di h(x) sono dati spesso in notazione ottale.
Un esempio di polinomio è $x^4 + x + 1$, rappresentato da <23> in notazione ottale.
Uno shif register h(x) può generare differenti sequenze in funzione del contenuto iniziale degli elementi memorizzati nel registro stesso: quando tutti gli elementi inseriti contengono 0 inizialmente, la sequenza generata è una sequenza di tutti zero.Questa sequenza è di poco interesse pratico.
Lo shift register può essere anche visto come una macchina a stati, con $2^n - 1$stati.
E' da notare che lo stato con tutti zero è escluso.
Il primo stato determina la sequenza generata dallo shift register.

Prima di fare un esempio è necessario riportare alcune proprietà delle sequenze a shift register.

- Ciascuna sequenza "u" è periodica, il periodo è al massimo $2^n - 1$, dove n è il grado del polinomio che genera "u"
- Se u e v sono generate da h(x), allora u $\oplus$ v è una sequenza generata da h(x);

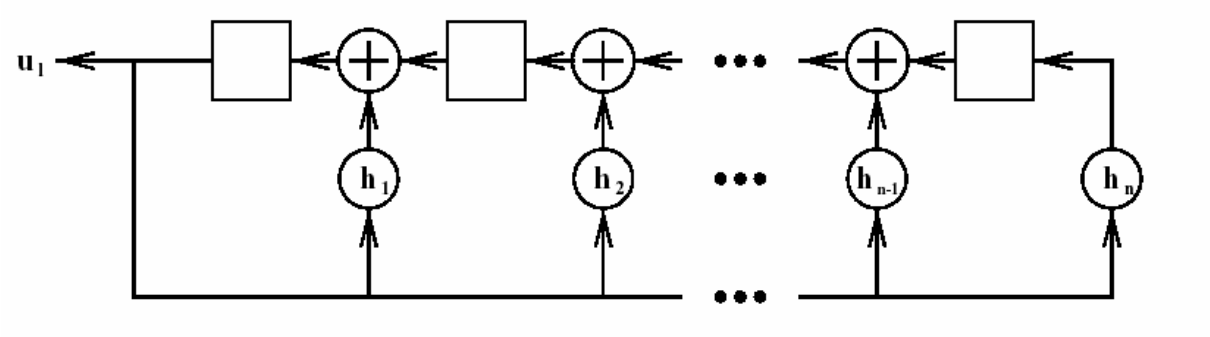
Qui sotto è possibile vedere le 15 possibili sequenze non nulle generate da un polinomio di grado 4: $h(x) = x^4 + x + 1$ in funzione dei diversi stati iniziali del registro a scorrimento

Sequence	Initial state	First period
$u^{(1)}$	0001	000100110101111
$u^{(2)}$	0010	001001101011110
$u^{(3)}$	0011	001101011110001
$u^{(4)}$	0100	010011010111100
$u^{(5)}$	0101	010111100010011
$u^{(6)}$	0110	011010111100010
$u^{(7)}$	0111	011110001001101
$u^{(8)}$	1000	100010011010111
$u^{(9)}$	1001	100110101111000
$u^{(10)}$	1010	101011110001001
$u^{(11)}$	1011	101111000100110
$u^{(12)}$	1100	110001001101011
$u^{(13)}$	1101	110101111000100
$u^{(14)}$	1110	111000100110101
$u^{(15)}$	1111	111100010011010

In questo caso le sequenze generate dal polinomio hanno periodo di $2^4 - 1 = 15$.

Osserviamo che

- Differenti stati iniziali del registro, danno differenti sequenze.
- Tutte le sequenze sono versioni ciclicamente shiftate di $u^{(1)}$ e tutte le fasi di $u^{(1)}$ sono generate dal polinomio, infatti:
- La sequenza $u^{(1)} \oplus u^{(2)} = u^{(3)}$ è generata dallo stesso polinomio.

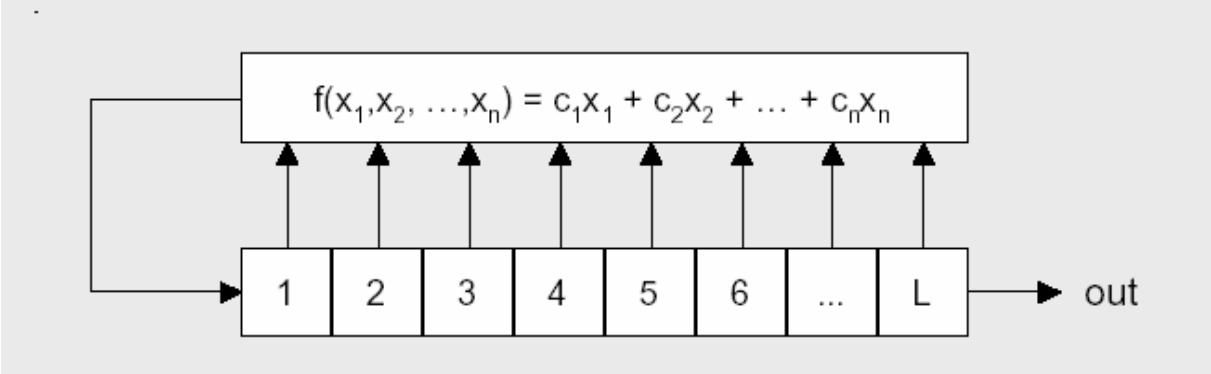


In figura: Configurazione di un registro a scorrimento ad alta velocità

Si può notare che la configurazione dello shift register qui riportata
può essere impiegata per ottenere la sequenza generata dallo shift register precedentemente visto, con il vantaggio che la nuova configurazione è più adatta per implementazioni ad alta velocità, dal momento che c'è un minore propagazione del ritardo nel percorso di reazione.
Sebbene le due configurazioni diano le stesse sequenze di uscita, esse hanno differenti traiettorie a livello di stati; da qui si deduce che per generare le stesse sequenze dobbiamo cominciare con differenti stati iniziali.

1.4 Sequenze a massima lunghezza: m-sequenze

Le sequenze *maximal-length*, chiamate anche *m-sequences* sono sequenze binarie generate in modo ricorsivo attraverso un registro a scorrimento o un elemento di ritardo di lunghezza fissata.
Abbiamo visto che un registro a scorrimento riporta tutti i segnali di retroazione come singolo input al registro stesso. Qui sotto è riportata un'altra figura che illustra chiaramente uno LFSR.



Funzionamento di uno Shift register Generator (LFSR) a L stadi

La funzione di reazione $f(x_1, x_2, .., x_n)$, ossia la somma modulo 2 di variabili x_i, contenute nelle celle del registro e con c_i i coefficienti di reazione (c_i=0 se aperto, c_i=1 se chiuso).

Tali sequenze soddisfano alle seguenti proprietà

- Un LFSR con L flip-flop produce sequenze che dipendono dalla lunghezza del registro L, dai collegamenti di reazione (retroazione) e dalle condizioni iniziali. E' proprio quando il periodo (cioè la lunghezza) della sequenza è esattamente

$$N_c = 2^L - 1, \quad dove\, L \geq 1\ grado\ della\ ricorsione$$

  che la sequenza (PN) è chiamata sequenza a massima lunghezza.

- In ogni periodo appaiono tutte le possibili sequenze binarie di L bit ad esclusione di quella completamente nulla.

- Una m-sequenza generata da un LFSR possiede un numero pari di tappi (sono cioè gli stadi dai quali si prelevano i valori e si sommano in xor prima di inviarli in retroazione e inserirli nuovamente come input).

- In un intero periodo della m-sequenza c'è un maggior numero di "1" che di "0". Nel momento in cui tutte le condizioni sono verificate, eccetto quella tutti zero, in una m-sequenza, allora devono esserci $2^{L-1} = \frac{1}{2}(N_c + 1)$ "1" e $2^{L-1} - 1$ "0".

- Risulta che tutte le m-sequenze con periodo *Nc* sono generate da *polinomi primitivi* di grado L. Al contrario, ogni sequenza generata da un polinomio primitivo è una m-sequenza.

Un esempio di lista di polinomi primitivi di grado non superiore ad 8

Degree	Primitive polynomials
2	⟨7⟩
3	⟨13⟩
4	⟨23⟩
5	⟨45⟩, ⟨75⟩, ⟨67⟩
6	⟨103⟩, ⟨147⟩, ⟨155⟩
7	⟨211⟩, ⟨217⟩, ⟨235⟩, ⟨367⟩, ⟨277⟩, ⟨325⟩, ⟨203⟩, ⟨313⟩, ⟨345⟩
8	⟨435⟩, ⟨551⟩, ⟨747⟩, ⟨453⟩, ⟨545⟩, ⟨537⟩, ⟨703⟩, ⟨543⟩

Polinomi primitivi

Il polinomio di quarto grado: $x^4 + x + 1$ (<23>) già citato è un polinomio primitivo che, dal registro a L=4 stadi, genera 15 differenti sequenze di periodo 15.

E' da notare che il reciproco di un polinomio primitivo (x^n h(1/x) è ancora un polinomio primitivo che genera m-sequenze: il polinomio reciproco di

$$x^4 + x + 1 \longrightarrow x^4 + x^3 + 1,$$

in genere i polinomi reciproci si ottengono da quelli primitivi.

Sono richiesti quei registri che sono in grado con il minimo numero di stadi di generare le m-sequenze.

Una proprietà importante è che ci sono esattamente *Nc* non zero sequenze generate da un polinomio primitivo.

- L'autocorrelazione (periodica di periodo N_c) di una *m*-sequence, dove lo '0' è codificato come '1' e '1' come '-1' assume due valori:

$$Ra(\tau) = \sum_{n=0}^{N_c-1} u_n u_{n+\tau}^* = \begin{cases} N_c \, quando \, \tau \bmod N_c = 0 \\ -1 quando \, \tau \bmod N_c \neq 0 \end{cases}$$

  Ossia –1 per tutti i valori della fase schiftati di τ, eccetto per l'intervallo [-1, +1], nel quale la correlazione varia linearmente dal valore –1 a $N_c = 2^L - 1$(la lunghezza della sequenza).

  Il picco di autocorrelazione aumenta con l'aumentare della lunghezza N_c della m-sequenza e approssima la funzione di autocorrelazione del rumore bianco.

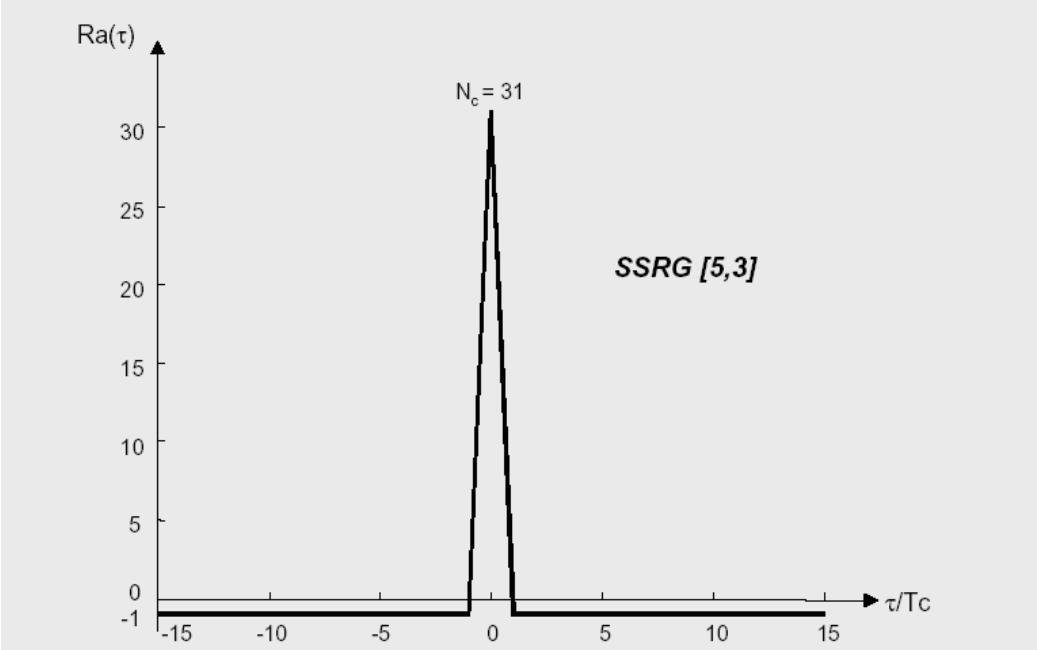


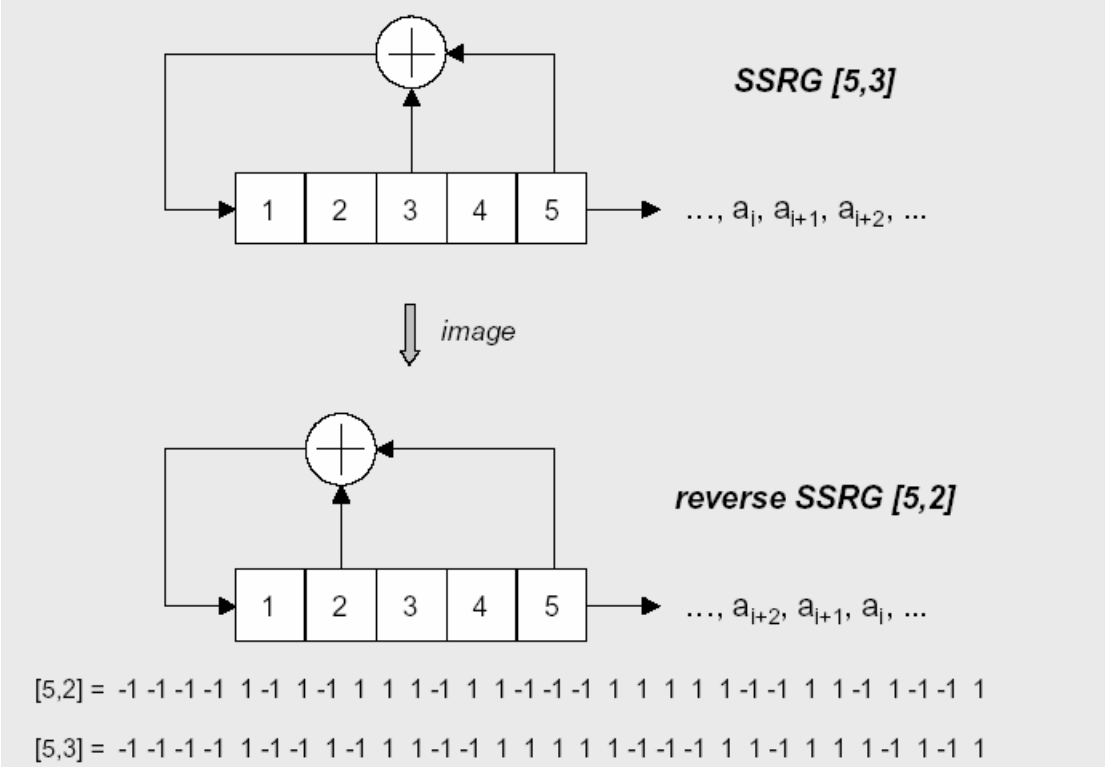
Grafico della una funzione di autocorrelazione di una sequenza generata da uno LFSR a 5 stadi

- In ogni periodo di lunghezza N_c ogni sotto sequenza $s \le L$ bit, non nulli, è presente 2^{L-s} volte, mentre una sottosequenza di $s \le L$ tutti nulli è presente $2^{L-s} - 1$ volte.

- Se un LFSR ad L stadi ha tappi di reazione sui livelli L, k, m ed ha sequenza $\ldots\ldots, a_l, a_{l+1}, a_{l+2}, \ldots$ allora l'opposto LFSR ha tappi di reazione su L, L-K, L- m e sequenza $\ldots. a_{l+2}, a_{l+1}, a_l, \ldots$

Un esempio di registro diretto ed inverso è sotto riportato.
Nel primo caso abbiamo un registro [5,3], cioè un registro a 5 stadi, le cui funzioni di reazione sono il terzo e il quinto elemento che si sommeranno in xor; quindi tale somma sarà inserita all'ingresso del registro facendo scorrere gli elementi di un posto.

La stessa cosa avviene nel registro inverso che presenterà, come detto, tappi di reazione su livelli diversi, generando così la sequenza immagine.



In figura: Immagine di uno LFSR e del suo inverso

Nella seguente tabella sono riportate le connessioni di reazione (in numero pari), per m-sequenze generate con un LFSR; bisogna ricordare che per ogni insieme $[l, k, ..., p]$ esiste un'insieme immagine inverso [L, L-k,…,L-p]

era una identica sequenza invertita nel tempo.

L	$N_c=2^L-1$	Feedback Taps for m-sequences	# m-sequences
2	3	[2,1]	2
3	7	[3,1]	2
4	15	[4,1]	2
5	31	[5,3] [5,4,3,2] [5,4,2,1]	6
6	63	[6,1] [6,5,2,1] [6,5,3,2]	6
7	127	[7,1] [7,3] [7,3,2,1] [7,4,3,2] [7,6,4,2] [7,6,3,1] [7,6,5,2] [7,6,5,4,2,1] [7,5,4,3,2,1]	18
8	255	[8,4,3,2] [8,6,5,3] [8,6,5,2] [8,5,3,1] [8,6,5,1] [8,7,6,1] [8,7,6,5,2,1] [8,6,4,3,2,1]	16
9	511	[9,4] [9,6,4,3] [9,8,5,4] [9,8,4,1] [9,5,3,2] [9,8,6,5] [9,8,7,2] [9,6,5,4,2,1] [9,7,6,4,3,1] [9,8,7,6,5,3]	48
10	1023	[10,3] [10,8,3,2] [10,4,3,1] [10,8,5,1] [10,8,5,4] [10,9,4,1] [10,8,4,3] [10,5,3,2] [10,5,2,1] [10,9,4,2] [10,6,5,3,2,1] [10,9,8,6,3,2] [10,9,7,6,4,1] [10,7,6,4,2,1] [10,9,8,7,6,5,4,3] [10,8,7,6,5,4,3,1]	60
11	2047	[11,2] [11,8,5,2] [11,7,3,2] [11,5,3,2] [11,10,3,2] [11,6,5,1] [11,5,3,1] [11,9,4,1,] [11,8,6,2,] [11,9,8,3] [11,10,9,8,3,1]	176

In Figura: Grafico della una funzione di autocorrelazione di una sequenza generata da uno LFSR a 5 stadi

I codici lineari sono facilmente decifrabili una volta che una breve serie sequenziale di chips della sequenza è nota. Le m-sequenze essendo codici lineari non sono utilizzabili per assicurare un sistema di trasmissione.
(Il sistema complessivo potrebbe essere ancora sicuro se l'informazione stessa fosse codificata, con una sicura tecnica di crittografica).

Le proprietà che abbiamo visto fanno sì che le sequenze maximum-length, anche se deterministiche e periodiche, appaiano aleatorie sia dal punto di vista della frequenza relativa di sottosequenze di bit, sia dal punto di vista della funzione di

autocorrelazione. A parte il valore nell'origine, la densità spettrale delle sequenze è uniforme.

1.5 Codici di Gold

Le m-sequenze sono comunemente impiegate quando è richiesta una buona funzione di autocorrelazione. Sfortunatamente, la cross-correlazione (la misura della concordanza tra due diversi codici) non si comporta tanto bene come l'autocorrelazione

Quando in un ambiente multi utente, come lo è CDMA, un ampio numero di trasmittenti deve dividere una comune banda di frequenza (ambiente multi utente), si necessita di una serie di codici, scelti con attenzione e con buone proprietà di cross-correlazione per evitare interferenze tra gli utenti.

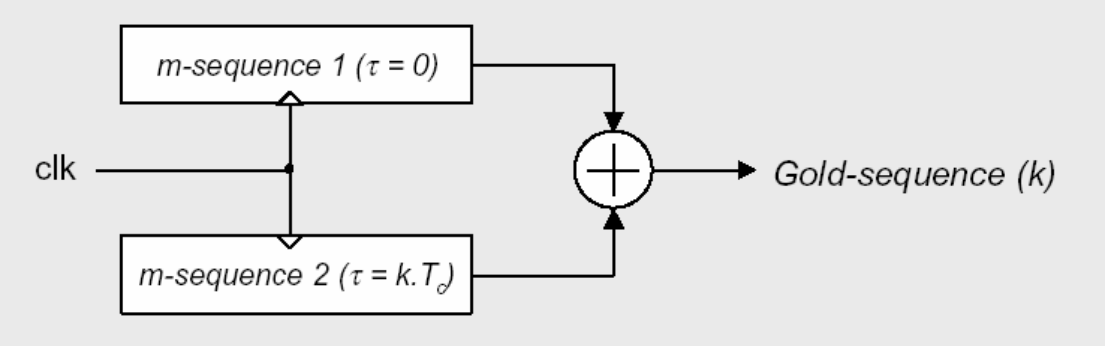
In genere in molte applicazioni sono richieste più di due sequenze: è necessario trovare, quindi, un più largo insieme di codici che abbiano buone proprietà di cross-correlazione. Se vi è questa necessità, dobbiamo allora considerare un'altra classe di sequenze di spreading, che abbiano buone proprietà di cross-correlazione.

Le sequenze di Gold sono una delle più comuni alternative.

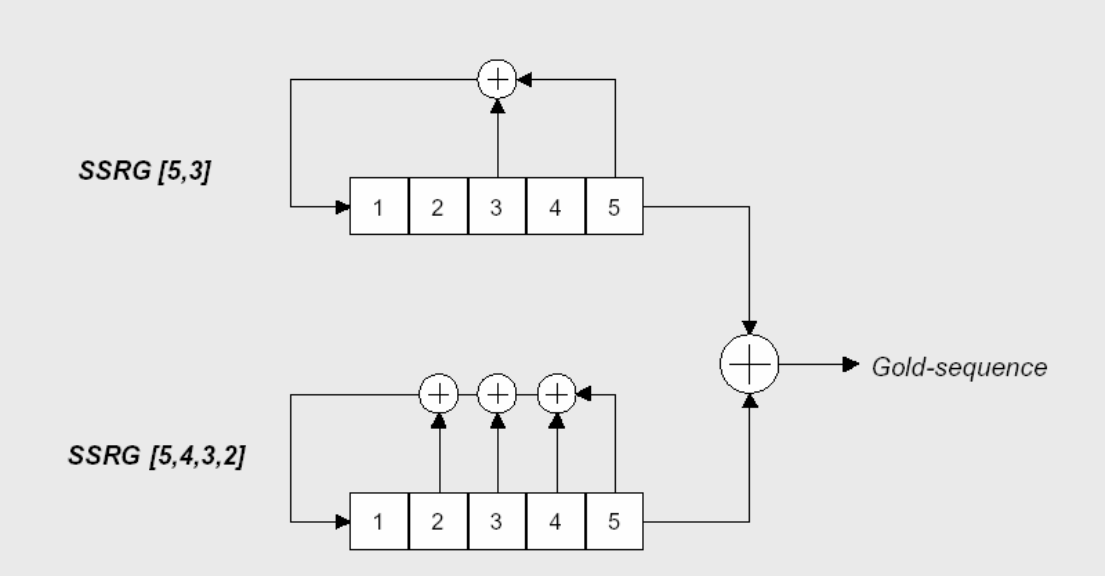
Le m-sequenze hanno un'eccellente proprietà di autocorrelazione e sono impiegate in molte applicazioni, mentre l'intercorrelazione è relativamente povera confrontata con i codici di Gold, cosicché la stessa sequenza con differente offset sono spesso utilizzate per differenti usi.

In questo modo la proprietà fondamentale di discriminazione fra i differenti codici di spreading dipende dalla proprietà di autocorrelazione.

I codici di Gold sono generati dall'addizione, modulo 2, di due sequenze a massima lunghezza (m-sequenze), entrambe della stessa lunghezza.
Le sequenze di codice sono sommate chip a chip da un clock sincrono.
Visto che le m-sequenze sono della stessa lunghezza (i due generatori di codice mantengono la stessa relazione di fase) e i codici generati sono della stessa lunghezza dei due codici base i quali sono sommati insieme; la funzione di autocorrelazione sarà peggiorata rispetto a quella delle due m-sequenze.
Ogni cambiamento nella posizione di fase tra le due m-sequenze generate, genera una nuova sequenza.



In figura: Grafico illustrativo della generazione di sequenze di Gold



In figura: Altro esempio di grafico illustrativo per la generazione di una sequenza di Gold

Qualsiasi generatore di codice di Gold, a due registri, di lunghezza L può generare $2^L - 1$ sequenze (lunghezza $2^L - 1$) più le due m-sequenze di base, dando un totale di $2^L + 1$ sequenze.

L	N_c	normalized 3-value crosscorrelation	Frequency of occurence
Odd	$2^L - 1$	$-1/N_c$ $-(2^{(L+1)/2} + 1)/N_c$ $(2^{(L+1)/2} - 1)/N_c$	~ 0.50 ~ 0.25 ~ 0.25
Even (not k.4)	$2^L - 1$	$-1/N_c$ $-(2^{(L+2)/2} + 1)/N_c$ $(2^{(L+2)/2} - 1)/N_c$	~ 0.75 ~ 0.125 ~ 0.125

Non tutte le coppie di m-sequenze producono i codici di Gold, ma quelle che lo fanno sono chiamate *coppie preferite*.

Sia M un intero positivo e si consideri la sequenza maximal-length v ottenuta per campionamento di un fattore M della sequenza maximal-length u di periodo N_c

Le due sequenze sono chiamate *preferred m-sequences* se sono soddisfatte le seguenti proprietà:

1. $L \bmod 4 \neq 0$ cioè L deve essere multiplo dispari di 2, oppure dispari

2. Il fattore di campionamento M deve soddisfare una delle seguenti ipotesi

   - $M = 2^k + 1$

   oppure

   - $M = 2^{2k} - 2^k + 1$ con k intero

3. La correlazione mutua tra le due sequenze preferite u e v assume soltanto tre valori:

$$Ra_{u,v}(\tau) = \begin{cases} -1 + 2^{\frac{L+e}{2}}, valoreassunto 2^{L-e-1} + 2^{\frac{L-e-2}{2}} volte \\ -1, valore.assunto 2^{L} - 2^{L-e} - 1 volte \\ -1 - 2^{\frac{L+e}{2}}, valoreassunto 2^{L-e-1} - 2^{\frac{L-e-2}{2}} volte \end{cases}$$

$$\text{con } e = \begin{cases} -1, perLdispari \\ 2, perL \bmod 4 = 0 \end{cases}$$

Un insieme di sequenze *Gold* può essere costruito a partire da una qualsiasi coppia di *preferred m-sequences di periodo* N_c.

Per ogni coppia di sequenze di Gold x, y, valgono le seguenti proprietà:

- il *parametro di massima correlazione*, definito da

$$Ra_{\max} = \max\left\{\left|Ra_{x,y}(\tau)\right|\right\} \quad \text{dove} \begin{cases} 1 \le \tau \le N_c - 1 \\ 0 \le \tau \le N_c - 1 \end{cases} \text{ se } \begin{cases} x = y \\ x \ne y \end{cases}$$

  soddisfa la relazione

$$Ra_{\max} \le \sqrt{2^{L+1}} + 1$$

- sia la correlazione mutua che l'autocorrelazione per ritardo non nullo assumono solamente tre valori:

$$Ra_{x,y}(\tau) = \begin{cases} -1, -1 - 2^{\frac{L+1}{2}}, -1 + 2^{\frac{L+1}{2}} \\ -1, -1 - 2^{\frac{L+2}{2}}, -1 + 2^{\frac{L+2}{2}} \end{cases} \quad \text{per} \quad \begin{cases} Ldispari \\ altrove \end{cases}$$

Nella tabella riportata qui sotto, vediamo che per ogni lunghezza del registro vi sono le sequenze di reazione in grado di generare i Codici di Gold e i 3 rispettivi valori di crosscorrelazione:

L	$N_c=2^L-1$	preferred pairs of m-sequences	3-value crosscorrelations		
5	31	[5,3] [5,4,3,2]	7	-1	-9
6	63	[6,1] [6,5,2,1]	15	-1	-17
7	127	[7,3] [7,3,2,1] [7,3,2,1] [7,5,4,3,2,1]	15	-1	-17
8*	255	[8,7,6,5,2,1] [8,7,6,1]	31	-1	-17
9	511	[9,4] [9,6,4,3] [9,6,4,3] [9,8,4,1]	31	-1	-33
10	1023	[10,9,8,7,6,5,4,3] [10,9,7,6,4,1] [10,8,7,6,5,4,3,1] [10,9,7,6,4,1] [10,8,5,1] [10,7,6,4,2,1]	63	-1	-65
11	2047	[11,2] [11,8,5,2] [11,8,5,2] [11,10,3,2]	63	-1	-65

In figura: Tabella illustrativa delle proprietà di intercorrelazione di alcune sequenze di Gold

Solamente una parte dei codici di Gold generati sono bilanciati.

[5,4,3,2] = -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

[5,3] (0) = -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

Gold(0) = -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

Σ Gold(0) = -7 = not balanced

[5,4,3,2] = -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

[5,3] (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

Gold(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

Σ Gold(1) = 1 = balanced

In figura: Proprietà di bilanciamento di un Codice di Gold

E’ possibile trovare che molti valori di cross-correlazione dei codici di Gold siano “1”. Ciò suggerisce che potrebbe essere possibile ottenere valori di cross-correlazione a “0” riempiendo uno “0” nel codice originale di Gold. Infatti 2^n codici ortogonali, possono essere ottenuti da questa semplice sostituzione.
Questi codici sono chiamati Codici di Gold Ortogonali.

1.5.1 Partial-Period correlation

La correlazione *partial-period* tra le sequenze $\{u(t)\}$ e $\{v(t)\}$ è data da

$$\Delta_{u,v}(L,\tau,t_0) = \sum_{t=t_0}^{t=t_0-L-1} u(t+\tau)v^*(t)$$

Dove k è la lunghezza della sottosequenza con k tale che
$1 \le k \le N_c$, $0 \le \tau \le N_c - 1$, $1 \le t_0 \le N_c - 1$ e la somma $t+\tau$ è calcolata ancora modulo N_c.

Spesso nei sistemi *CDMA direct sequence* le sequenze pseudocasuali usate dai vari utenti sono molto lunghe. Per minimizzare la complessità hardware in ricezione si potrebbe calcolare, per demodulare i dati e acquisire la sincronizzazione, la correlazione solo su una parte del periodo della sequenza. In questo senso risulta di interesse questo tipo di correlazione.