E303: Communication Systems

Professor A. Manikas
Chair of Communications and Array Processing

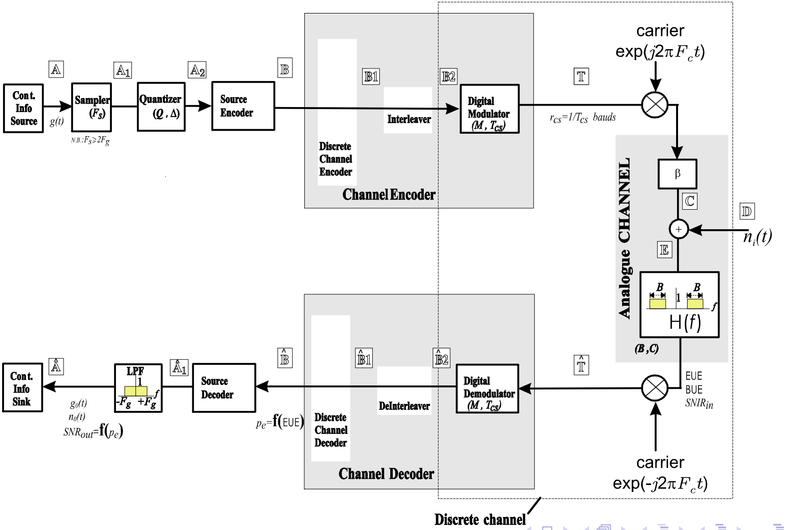
Imperial College London

An Overview of Fundamentals of Spread Spectrum: PN-codes and PN-signals

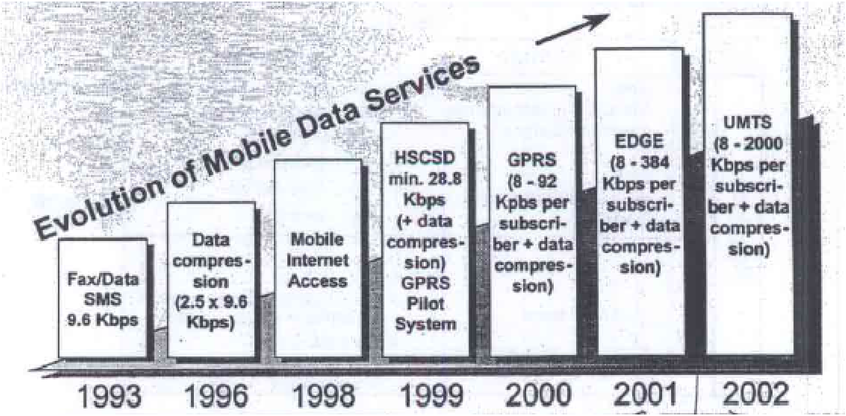
Table of Contents

Introduction

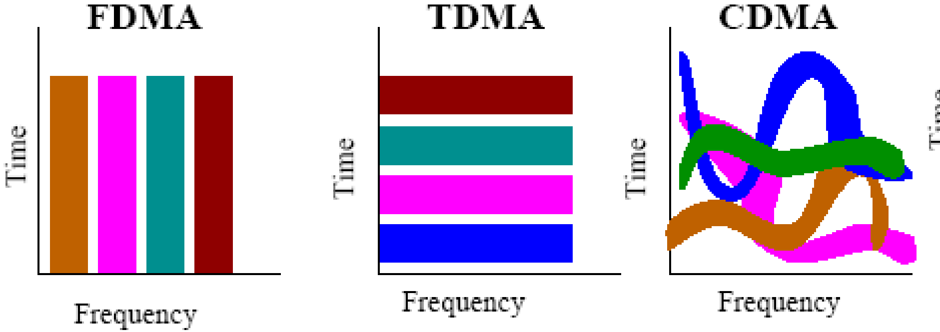
- General Block Diagram of a Digital Comm. System (DCS)



Pre-4G Evolution

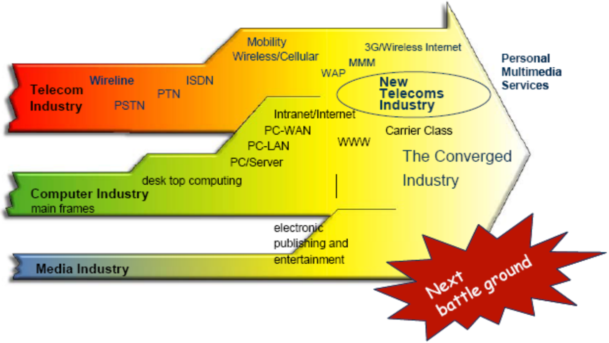


HSCDS: High Speed Circuit Switched Data
GPRS: General Packet Radio Systems (2+)
EDGE: Enhanced Data Rate GSM Evolution (2+)
UMTS:Universal Mobile Telecommunication Systems (3G)



Note: CDMA $\in$ Spread Spectrum Comms

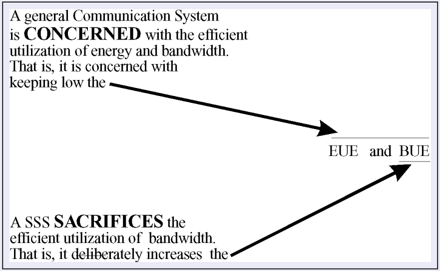
- Industry Transformation and Convergence [from Ericsson 2006, LZT 123 6208 R5B]



WCDMA (Wideband CDMA) is a 3G mobile comm system. It is a wireless system where the telecommunications, computing and **media** industry converge and is based on a Layered Architecture design. (Note: CDMA Systems $\in$ the class of SSS).

Definition (Spread Spectrum System (SSS))

When a DCS becomes a Spread Spectrum System (SSS)



Lemma (CS $\triangleq$ SSS)

$$CS \triangleq SSS \text{ iff} \begin{cases} \circ\ B_{ss} \gg \textit{message bandwidth (i.e. BUE=large)} \\ \circ\ B_{ss} \neq f\{\textit{message}\} \\ \circ\ \textit{spread is achieved by means of a code which is} \neq f\{\textit{message}\} \\ \textit{where } B_{ss} = \textit{transmitted SS signal bandwidth} \end{cases}$$

- our AIM: ways of accomplishing LEMMA-1.

N.B.:

- PCM, FM, etc spread the signal bandwidth but do not satisfy the conditions to be called SSS

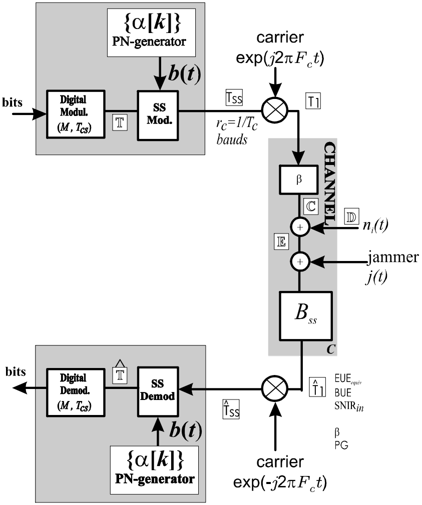
- $B_{\text{transmitted-signal}} \gg B_{\text{message}}$

  $\Rightarrow$SSS distributes the transmitted energy over a wide bandwidth

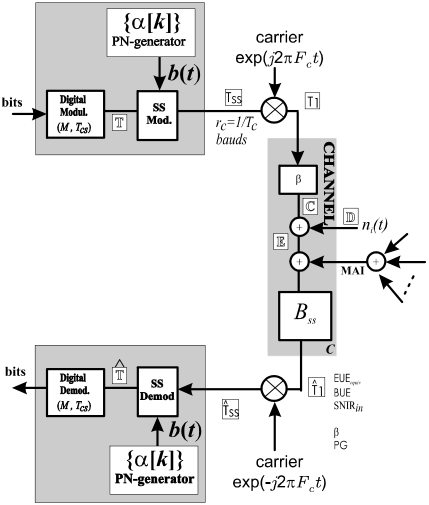
  $\Rightarrow$ SNIR at the receiver input is LOW.

  Nevertheless, the receiver is capable of operating successfully because the transmitted signal has distinct characteristics relative to the noise

(a) SSS:



(b) CDMA (K users):

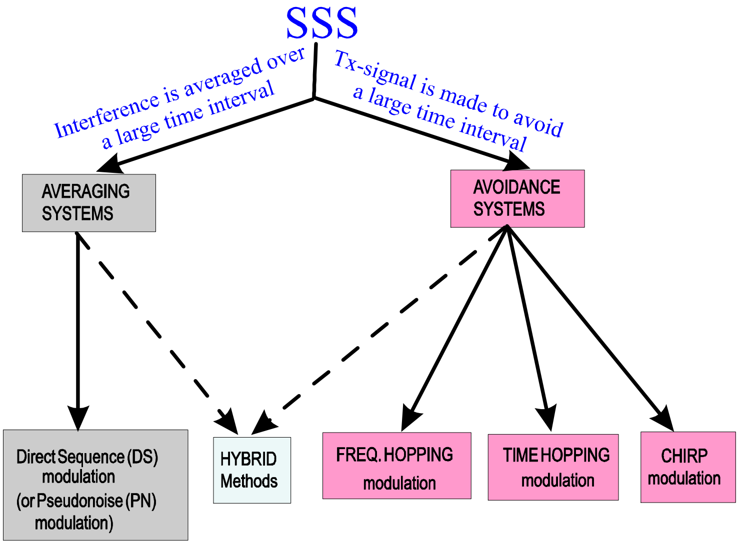


- The PN signal $b(t)$ is a function of a PN sequence of ±1's $\{\alpha[n]\}$
  - The sequences $\{\alpha[n]\}$ must agreed upon in advance by Tx and Rx and they have status of password.
  - This implies that :
    - ★ knowledge of $\{\alpha[n]\}\Rightarrow$demodulation$=$possible
    - ★ without knowledge of $\{\alpha[n]\}$ $\Rightarrow$demod.$=$very difficult
  - If $\{\alpha[n]\}$ (i.e. "password") is purely random, with no mathematical structure, then
    - ★ without knowledge of $\{\alpha[n]\}$ $\Rightarrow$demodulation$=$impossible
  - However all practical random sequences have some periodic structure. This means:

$$\alpha[n] = \alpha[n + N_c] \tag{1}$$

where N_c $=$period of sequence
i.e. pseudo-random sequence (PN-sequence)

Classification of SSS

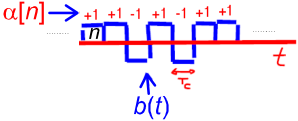


Modelling of b(t) in SSS

- DS-SSS (Examples: DS-BPSK, DS-QPSK):

$$b(t) = \sum_n \alpha[n].c(t - nT_c) \tag{2}$$

where $\{\alpha[n]\}$ is a sequence of ± 1's;
$c(t)$ is an energy signal of duration T_c =rect$\left\{\frac{t}{T_c}\right\}$



- FH-SSS (Examples: FH-FSK)

$$b(t) = \sum_n \exp\left\{j(2\pi \mathrm{k}[n]F_1 t + \phi[n])\right\}.c(t - nT_c) \tag{3}$$

where $\{\mathrm{k}[n]\}$ is a sequence of integers such that $\{\alpha[n]\} \mapsto \{\mathrm{k}[n]\}$
and $\{\alpha[n]\}$ is a sequence of ± 1's;
$c(t)$ is an energy signal of duration T_c
and with $\phi[n]$ = random: $\mathrm{pdf}_{\phi[n]} = \frac{1}{2\pi}\mathrm{rect}\left\{\frac{\varphi}{2\pi}\right\}$

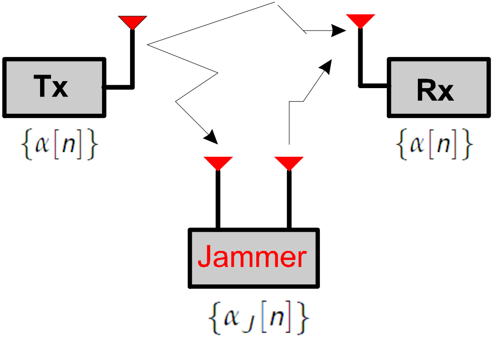
Applications of Spread Spectrum Techniques

1. Interference Rejection: to achieve interference rejection due to:
   - Jamming (hostile interference). N.B.: protection against cochannel interference is usually called anti-jamming (AJ)
   - Other users (Multiple Access Interefence - MAI): Spectrum shared by "coordinated " users.
   - Multipath: Self-Jamming by delayed signal
2. Energy Density Reduction (or Low Probability of Intercept LPI). LPI' main objectives:
   - to meet international allocations regulations
   - to reduce (minimize) the detectability of a transmitted signal by someone who uses **spectral analysis**
   - privacy in the presence of other listeners
3. Range or Time Delay Estimation

NB: interference rejection = most important application

- Jamming source, or, simply Jammer is defined as follows:

$$\boxed{\text{Jammer} \triangleq \text{intentional (hostile) interference}}$$

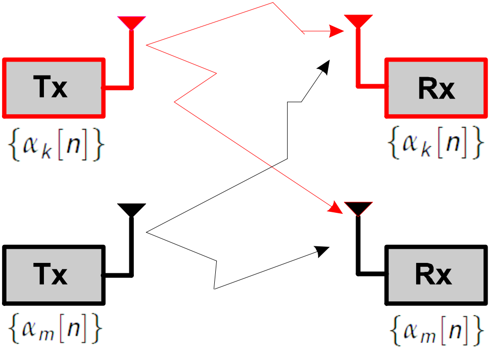


★ the jammer has full knowledge of SSS design except the jammer does not have the key to the PN-sequence generator,

★ i.e. the jammer may have full knowledge of the SSystem but it does **not** know the PN sequence used.

- Multiple Access Interference (MAI) is defined as follows:

$$\boxed{\text{MAI} \triangleq \text{unintentional interference}}$$

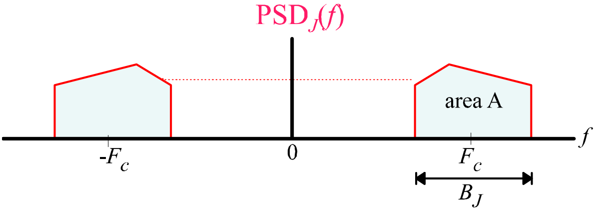


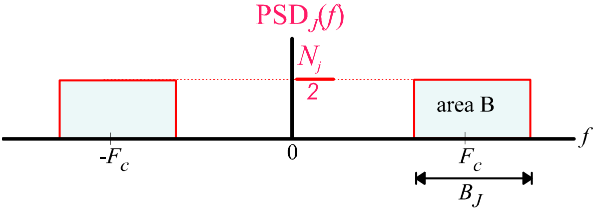
- PG: is a measure of the interference rejection capabilities
- definition:

$$\text{PG} \triangleq \frac{B_{ss}}{B} = \frac{1/T_c}{1/T_{cs}} = \frac{T_{cs}}{T_c} \tag{4}$$

  where B=bandwidth of the conventional system
- PG is also known as "spreading factor" (SF)
- PG = very important in DS-SSS
- PG $\neq$ very important in FH-SSS

- Remember:
  - ★ Jamming source, or, simply Jammer = intentional interference
  - ★ Interfering source = unintentional interference





- ★ With $\boxed{\text{area-B} = \text{area-A}}$ we can find N_j
- ★ $P_j = 2\times\ \underline{\text{area}\mathbf{A}} = 2\times\ \underline{\text{area}\mathbf{B}} = N_j B_j \Rightarrow N_j = \frac{P_j}{B_j}$

- if

$$B_J = qB_{ss};\ 0 < q \leq 1 \tag{5}$$

then

$$\text{EUE}_J = \frac{E_b}{N_J} = \frac{P_s.B_J}{P_J.r_b} = \frac{P_s.q.B_{ss}}{P_J.B} = \text{PG} \times \text{SJR}_{in} \times q \tag{6}$$

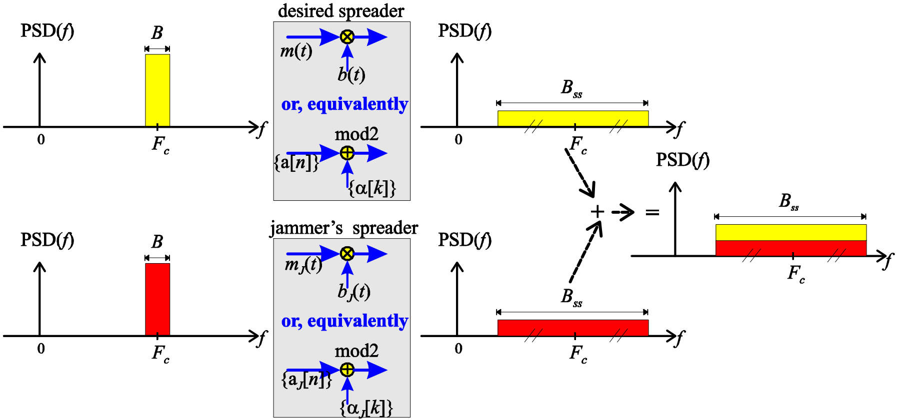
$$\text{EUE}_{equ} = \frac{E_b}{N_0 + N_J} \tag{7}$$

$$= \text{PG} \times \text{SJR}_{in} \times q \times \left(\frac{N_0}{N_j} + 1\right)^{-1} \tag{8}$$

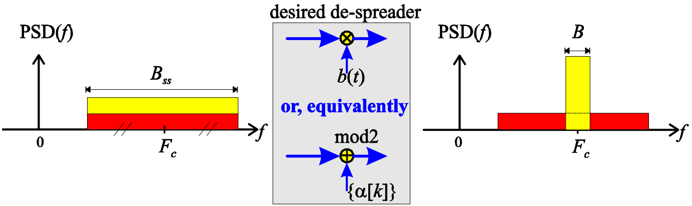
where

$$\text{SJR}_{in} \triangleq \frac{P_s}{P_J} \tag{9}$$

- SS Transmission in the presence of a Jammer (or MAI)



- SS Reception in the presence of a Jammer (or MAI)



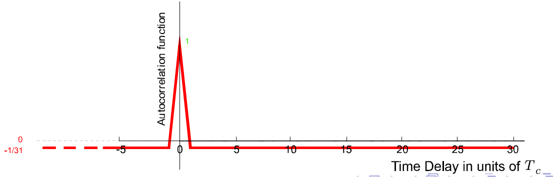
- PN-codes (or PN-sequences, or spreading codes) are sequences of +1s and -1s (or 1s and 0s) having special correlation properties which are used to distinguish a number of signals occupying the same bandwidth.
- Five Properties of Good PN-sequences:

Property-1	easy to generate
Property-2	randomness
Property-3	long periods
Property-4	impulse-like auto-correlation functions
Property-5	low cross-correlation

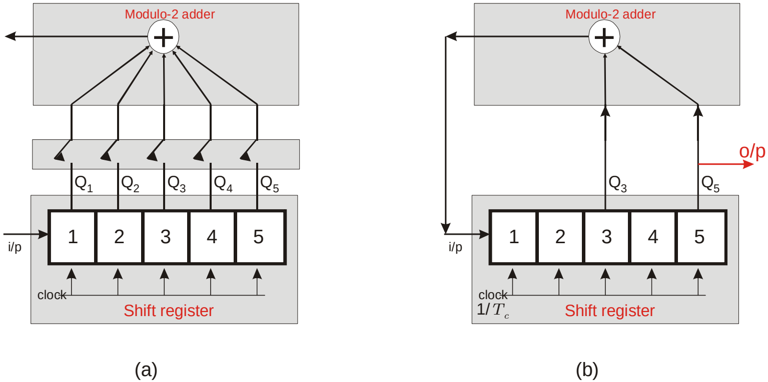
Comments on PN-sequences Main Properties

- Comments on Properties 1, 2 & 3
  - Property-1 is easily achieved with the generation of PN sequences by means of shift registers,
    while
  - Property-2 & Property-3 are achieved by appropriately selecting the feedback connections of the shift registers.

- Comments on Property-4
  - to combat multipath, consecutive bits of the code sequences should be uncorrelated.
    i.e. code sequences should have impulse-like autocorrelation functions. Therefore it is desired that the auto-correlation of a PN-sequence is made as small as possible.
  - The success of any spread spectrum system relies on certain requirements for PN-codes. Two of these requirements are:
    1. the autocorrelation peak must be sharp and large (maximal) upon synchronisation (i.e. for time shift equal to zero)
    2. the autocorrelation must be minimal (very close to zero) for any time shift different than zero.
  - A code that meets the requirements (1) and (2) above is the m-sequence which is ideal for handling multipath channels.



- The figure below shows a shift register of 5 stages together with a modulo-2 adder. By connecting the stages according to the coefficients of the polynomial $D^5 + D^2 + 1$ an m-sequence of length 31 is generated (output from Q5).
  The autocorrelation function of this m-sequence signal is shown in the previous page



- Comments on Property-5
  - If there are a number of PN-sequences

$$\{\alpha_1[k]\}, \{\alpha_2[k]\}, ..., \{\alpha_K[k]\} \tag{10}$$

    then if these code sequences are not totally uncorrelated, there is always an interference component at the output of the receiver which is proportional to the cross-correlation between different code sequences.
  - Therefore it is desired that this cross-correlation is made as small as possible.

An Important "Trade-off"

- There is a trade-off between Properties-4 and 5.
- In a CDMA communication environment there are a number of PN-sequences

$$\{\alpha_1[k]\}, \{\alpha_2[k]\}, ..., \{\alpha_K[k]\}$$

  of period N_c which are used to distinguish a number of signals occupying the same bandwidth.
- Therefore, based on these sequences, we should be able to
  - ★ combat multipath
    (which implies that the auto-correlation of a PN-sequence $\{\alpha_i[k]\}$ should be made as small as possible)
  - ★ remove interference from other users/signals,
    (which implies that the cross-correlation should be made as small as possible).

Corollary

The following inequality is always valid:

$$\boxed{R_{auto}^2 + R_{cross}^2 > \text{a constant which is a function of period } N_c} \qquad (11)$$

i.e. there is a trade-off between the peak autocorrelation and cross-correlation parameters.

- Thus, the autocorrelation and cross-correlation functions cannot be both made small simultaneously.
- The design of the code sequences should be therefore very careful.

N.B.:

- A code with excellent autocorrelation is the m-sequence.
- A code that provides a trade-off between auto and cross correlation is the gold-sequence.

m-sequences

- m-seq.: widely used in SSS because of their very good autocorrelation properties.
- PN code generator: is periodic
  - i.e. the sequence that is produced repeats itself after some period of time

Definition (m-sequence)

A sequence generated by a linear m-stages Feedback shift register is called a maximal length, a maximal sequence, or simply m-sequence, if its period is

$$N_c = 2^m - 1 \tag{12}$$

(which is the maximum period for the above shift register generator)

- The initial contents of the shift register are called initial conditions.

Shift Registers and Primitive Polynomials

- The period N_c depends on the feedback connections (i.e. coefficients c_i) and $N_c = max$, i.e. $N_c = 2^m - 1$, when the characteristic polynomial

$$c(D) = c_m D^m + c_{m-1} D^{m-1} + ... + c_1 D + c_0 \quad \text{with} \quad c_0 = 1 \qquad (13)$$

is a primitive polynomial of degree m.

$$\boxed{\text{rule: if } c_i = \begin{cases} 0 \Longrightarrow & \text{no connection} \\ 1 \Longrightarrow & \text{there is connection} \end{cases}} \qquad (14)$$

- Definition of PRIMITIVE polynomial = very important (see Appendix C)

Examples (Some Primitive Polynomials)

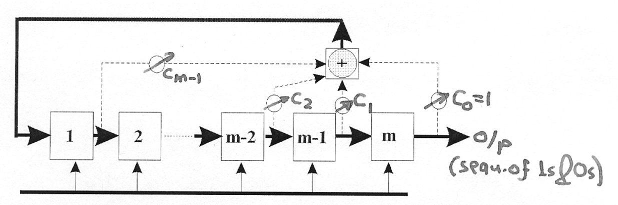
degree-m	polynomial
3	$D^3 + D + 1$
4	$D^4 + D + 1$
5	$D^5 + D^2 + 1$
6	$D^6 + D + 1$
7	$D^7 + D + 1$

- Please see Appendix E for some tables of irreducible & primitive polynomial over GF(2).

Implementation of an m-sequence

- use a maximal length shift register
  i.e. in order to construct a shift register generator for sequences of any permissible length, it is only necessary to know the coefficients of the primitive polynomial for the corresponding value of m

$$f_c = \frac{1}{T_c} = \text{chip-rate} = \text{clock-rate} \tag{15}$$

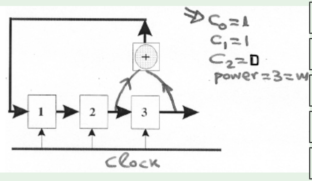


$$c(D) = c_m D^m + c_{m-1} D^{m-1} + \dots + c_1 D + c_0 \tag{16}$$

$$\text{with} \quad c_0 = 1 \tag{17}$$

Example ($c(D) = D^3 + D + 1$ = primitive $\Longrightarrow$ power $= m = 3$)

- coefficients$=(1,0,1,1) \Rightarrow N_c = 7 = 2^m - 1$ i.e.period$= 7T_c$



	1st	2nd	o/p 3rd
initial condition	1	1	1
clock pulse No.**1**	0	1	1
clock pulse No.**2**	0	0	1
clock pulse No.**3**	1	0	0
clock pulse No.**4**	0	1	0
clock pulse No.**5**	1	0	1
clock pulse No.**6**	1	1	0
clock pulse No.**7**	1	1	1

- Note that the sequence of 0's and 1's is transformed to a sequence of ± 1s by using the following function

$$\text{o/p} = 1 - 2 \times \text{i/p} \tag{18}$$

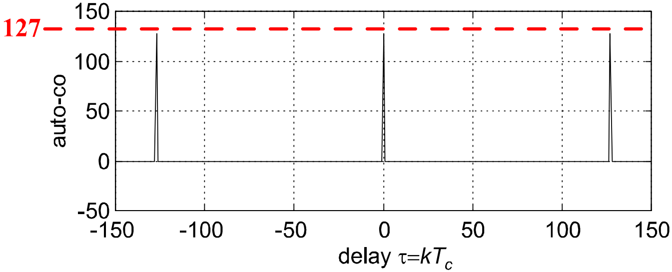
Auto-Correlation Properties

- An m-sequ. $\{\alpha[n]\}$ has a two valued auto-correlation function:

$$R_{\alpha\alpha}[k] = \sum_{n=1}^{N_c} \alpha[n]\alpha[n+k] = \begin{cases} N_c & k = 0 \bmod N_c \\ -1 & k \neq 0 \bmod N_c \end{cases} \tag{19}$$

- This implies that $R_{bb}(\tau)$ is also a "two-valued"

$R_{bb}(\tau)$:



- Remember that a sequence $\{\alpha[n]\}$ of period $N_c = 2^m - 1$, generated by a linear FB shift register, is called a maximal length sequence.

Some Properties of m-sequences

- There is an appropriate balance of -1s and +1s
  - In any period there are $\left\{ \begin{array}{lll} N_{c-} &= 2^{m-1} & \text{No. of -1s} \\ N_{c+} &= 2^{m-1}-1 & \text{No. of +1s} \end{array} \right\}$

    i.e.

$$\Pr(+1) \simeq \Pr(-1) \tag{20}$$

- shift-property of m-sequences:
  - if $\{\alpha[n]\}$ is an m-sequence then

$$\{\alpha[n]\} + \underbrace{\{\alpha[n+m]\}}_{\text{shift by } m} = \underbrace{\{\alpha[n+k]\}}_{\text{shift by } k \neq m} \tag{21}$$

- In a complete SSS we use more than one different m-sequences
  - Thus the number of m-sequs of a given length is an IMPORTANT property
    - ★ because in a CDMA system several users communicate over a common channel so that different -sequences are necessary to distinguish their signals
  - Number of m-sequs of length N_c :

$$\text{No. of m-sequs of length } N_c \triangleq \frac{1}{m}\Phi\left\{N_c\right\} \tag{22}$$

where

$$\begin{aligned} \Phi\left\{N_c\right\} &\triangleq \text{Euler totient function} &(23)\\ &= \text{No of } (+)\text{ve integers} < N_c \text{ and relative prime to } N_c \end{aligned}$$

  - Note: if $N_c = p.q$ where p, q are prime numbers then

$$\Phi\left\{N_c\right\} = (p-1).(q-1) \tag{24}$$

Cross-Correlation Properties and Preferred m-sequences

- sequences of period N_c are used to distinguish two signals occupying the same bandwidth.
- A measure of interaction between these signals is their cross-correlation:

$$R_{\alpha_i \alpha_j}[k] = \sum_{n=1}^{N_c} \alpha_i[n] \alpha_j[n+k]$$

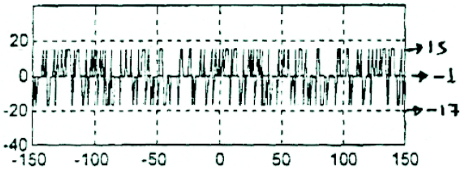
- However,
  - there exist **certain pairs of sequences** that have large peaks and noise-like behaviour in their cross-correlation
  - while others exhibit a rather smooth three valued cross-correlation.
- The latter are called **preferred sequences**.

- It can be shown that the cross-correlation of **preferred sequences** takes on values from the set

$$\{-1, -R_{cross}, R_{cross}-2\} \quad (25)$$

where
$$R_{cross} = \begin{cases} 2^{\frac{m+1}{2}}+1 & m = odd \\ 2^{\frac{m+2}{2}}+1 & m = even \end{cases} \quad (26)$$

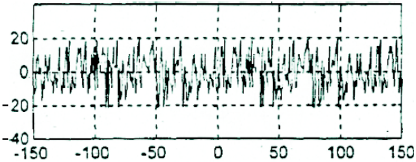
$R_{b_i b_j}(\tau) =$preferred:



delay $\tau = kT_c$

m

$R_{b_i b_j}(\tau) =$ *non*-preferred:



m

A Note on m-sequences for CDMA

- Because of the high cross-correlation between m-sequences, the interference between different users in a CDMA environment will be large.
  - Therefore, m-sequences are not suitable for CDMA applications.
- However, in a complete synchronised CDMA system, different offsets of the same m-sequence can be used by different users.
  - In this case the excellent autocorrelation properties (rather than the poor cross-correlation) are employed.
  - Unfortunately this approach cannot operate in an asynchronous environment.

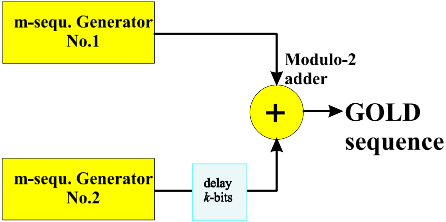
Gold Sequences

- Although m-sequences possess excellent randomness (and especially autocorrelation) properties, they are not generally used for CDMA purposes as it is difficult to find a set of m-sequences with low cross-correlation for all possible pairs of sequences within the set.

- However, by slightly relaxing the conditions on the autocorrelation function, we can obtain a family of code sequences with lower cross-correlation.

- Such an encoding family can be achieved by Gold sequences or Gold codes which are generated by the modulo-2 sum of two m-sequences of equal period.

- The Gold sequence is actually obtained by the modulo-2 sum of two *m*-sequences with different phase shifts for the first *m*-sequence relative to the second.
- Since there are $N_c = 2^m - 1$ different relative phase shifts, and since we can also have the two *m*-sequences alone, the actual number of different Gold-sequences that can be generated by this procedure is $2^m + 1$.



Auto-Correlation Properties

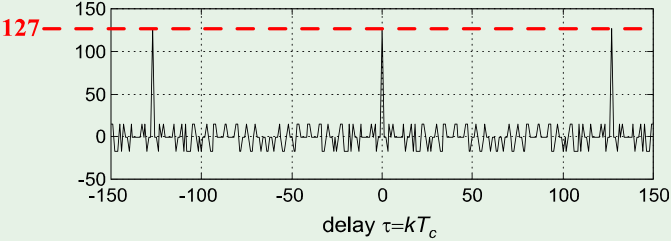
- Gold sequences, however, are not maximal length sequences.
- Therefore, their auto-correlation function **is not** the two valued one given by Equ. (19), i.e.

$$\{N_c, -1\} \tag{27}$$

- The auto-correlation still has the periodic peaks, but between the peaks the auto-correlation is no longer flat.

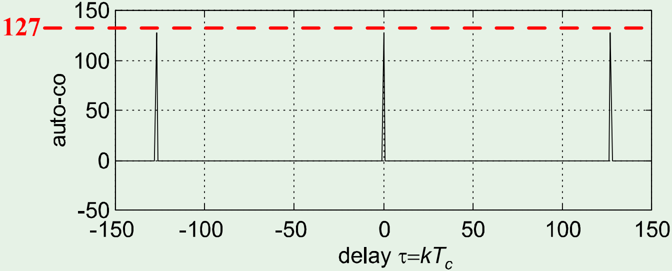
Example (Gold Sequence of $N_c = 127 = 2^7 - 1$)

$R_{bb}(\tau)$:



Example (m-sequence of $N_c = 127 = 2^7 - 1$)

$R_{bb}(\tau)$:



Cross-Correlation Properties

- Gold-sequences have the same cross-correlation characteristics as preferred m-sequences,
  i.e. their cross-correlation is three valued.
- Gold sequences have higher R_{auto} and lower R_{cross} than m-sequences, and the trade-off (see Equ. 11) between these parameters is thus verified.

Balanced Gold codes.

- Balanced Gold Sequence: The number of "-1s" in a code period exceed the number of "1s" by one as is the case for m-sequences.
- We should note that not all Gold codes (generated by modulo-2 addition of 2 m-sequences) are balanced, i.e. the number of "-1s" in a code period does not always exceed the number of "1s" by one.
- For example, for $m = odd$ only $2^{m-1} + 1$ code sequences of the total $2^m + 1$ are balanced, while the rest code $2^{m-1} - 1$ sequences have an excess or a deficiency of -1s.
- For $m = 7$, for instance, only 65 **balanced** Gold codes can be produced, out of a total possible of 129. Of these, 63 are non-maximal and two are maximal length sequences.
- Balanced Gold codes have more desirable spectral characteristics than non-balanced.
- Balanced Gold codes are generated by appropriately selecting the relative phases of the two original m-sequences.
- SUMMARY: By selecting any preferred pair of primitive polynomials it is easy to construct a very large set of PN-sequences (Gold-sequences). Thus, by assigning to each user one sequence from this set, the interference from other users is minimised.

Appendices

1. Appendix A:
   Properties of a purely random sequence
2. Appendix B:
   Auto and Cross Correlation functions of two PN-sequences
3. Appendix C:
   The concept of a 'Primitive Polynomial' in GF($2^\subset$)
4. Appendix D:
   Finite Field - Basic Theory
5. Appendix E:
   Table of Irreducible Polynomials over GF(2)

Appendices

Appendix A: Properties of $\{\alpha[n]\}$ if it is a purely random sequence

Let the sequence $\{\alpha[n]\}$ be the output of a discrete, memoryless source

INFORMATION SOURCE of $\pm$ 1s
$\begin{cases} P(\alpha[n]=1)=0.5 \\ P(\alpha[n]=-1)=0.5 \end{cases}$

$\longrightarrow \{\alpha[n]\}$

with

$$\mathcal{E}\{\alpha[n]\}=0 \qquad (=1\times 0.5+(-1)\times 0.5=0) \tag{2}$$
$$Var\{\alpha[n]\}=1 \qquad (=1^2\times 0.5+(-1)^2\times 0.5=1) \tag{3}$$

The auto-correlation of the sequence $\{\alpha[n]\}$ over M symbols is defined as follows

$$R_{\alpha\alpha}^{M}[k] \equiv \sum_{n=1}^{M}\alpha[n]\alpha[n+k]=\begin{cases}\sum_{n=1}^{M}\alpha[n]^2=\sum_{n=1}^{M}1=M & k=0\\ \text{random} & k\neq 0\end{cases} \tag{4}$$

Therefore the mean and the variance of the autocorrelation function $R_{\alpha\alpha}^{M}[k]$ are as follows

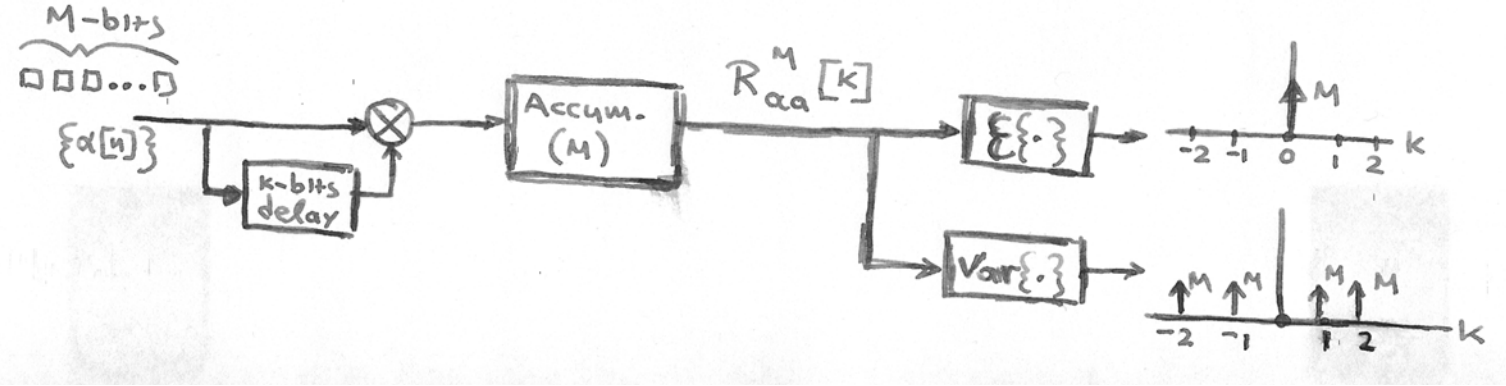
$$\mathcal{E}\{R_{\alpha\alpha}^{M}[k]\}=\sum_{n=1}^{M}\mathcal{E}\{\alpha[n]\alpha[n+k]\}=\begin{cases}\sum_{n=1}^{M}\mathcal{E}\{\alpha[n]^2\}=\sum_{n=1}^{M}1=M & \text{if } k=0\\ \sum_{n=1}^{M}\mathcal{E}\{\alpha[n]\}\mathcal{E}\{\alpha[n+k]\}=0 & \text{if } k\neq 0\end{cases} \tag{5}$$

$$
\begin{aligned}
Var\left\{R_{\alpha\alpha}^{M}[k]\right\} &= \mathcal{E}\left\{R_{\alpha\alpha}^{M}[k]^2\right\} - \mathcal{E}\left\{R_{\alpha\alpha}^{M}[k]\right\}^2 = \\
&= \sum_{n=1}^{M}\sum_{m=1}^{M}\mathcal{E}\{\alpha[n]\alpha[n+k]\alpha[m]\alpha[m+k]\} - \mathcal{E}\left\{R_{\alpha\alpha}^{M}[k]\right\}^2 = \\
&= \begin{cases} \sum_{n=1}^{M}\sum_{m=1}^{M}\mathcal{E}\left\{\alpha^2[n]\right\}.\mathcal{E}\left\{\alpha^2[m]\right\} - \mathcal{E}\left\{R_{\alpha\alpha}^{M}[0]\right\}^2 = M^2 - M^2 = 0 & \text{if } k=0 \\ \sum_{n=1}^{M}\mathcal{E}\left\{\alpha^2[n]\right\}.\mathcal{E}\left\{\alpha^2[n+k]\right\} - \mathcal{E}\left\{R_{\alpha\alpha}^{M}[k]\right\}^2 = M - 0 = M & \text{if } k\neq 0 \end{cases}
\end{aligned} \tag{6}
$$

One may also define the cross-correlation of two sequences $\{\alpha_1[n]\}$ and $\{\alpha_2[n]\}$

$$R_{\alpha_1\alpha_2}^{M}[k] = \sum_{n=1}^{M}\alpha_1[n]\alpha_2[n+k] \tag{7}$$

Since $\{\alpha_1[n]\}$ and $\{\alpha_2[n]\}$ are independent the results are essentially the same as for the auto-correlation of $\{\alpha_1[n]\}$ with non-zero lag k. This shows that completely random sequences have nice auto- and cross-correlation properties.



Note that pure random sequences could be used as code sequences, but since the receiver needs a replica of the desired code sequence in order to despread the signal, PN sequences are used instead in practice.

Appendix B: Auto and Cross Correlation functions of two PN-sequences $\{\alpha_i[n]\}$ and $\{\alpha_j[n]\}$

- Consider the ∞-sequences of ± 1s of period N:

$$\{\alpha_i[n]\} = ..., \alpha_i[N-1], \alpha_i[N], \alpha_i[1], \alpha_i[2], ..., \alpha_i[N-1], \alpha_i[N], \alpha_i[1], ...$$

$$\{\alpha_j[n]\} = ..., \alpha_j[N-1], \alpha_j[N], \alpha_j[1], \alpha_j[2], ..., \alpha_j[N-1], \alpha_j[N], \alpha_j[1], ...$$

- Then, there are three different cross-correlation functions

$\diamond$ aperiodic cross-correlation:
$$C_{\alpha_i\alpha_j}[k] \equiv \begin{cases} \sum_{n=1}^{N-k} \alpha_i[n]\alpha_j[n+k] & 0 \leq k \leq N-1 \\ \sum_{n=1}^{N+k} \alpha_i[n-k]\alpha_j[n] & 1-N \leq k \leq 0 \\ 0 & \|k\| \geq N \end{cases} \quad (8)$$

$\diamond$ periodic cross-correlation:
$$R_{\alpha_i\alpha_j}[k] \equiv \sum_{n=1}^{N} \alpha_i[n]\alpha_j[n+k] \quad (9)$$

$\diamond$ odd cross-correlation function:
$$\widetilde{R}_{\alpha_i\alpha_j}[k] = C_{\alpha_i\alpha_j}[k] - C_{\alpha_i\alpha_j}[k-N] \quad (10)$$

- Note that:

  ◇ it is easy to see that

$$R_{\alpha_i\alpha_j}[k] = C_{\alpha_i\alpha_j}[k] + C_{\alpha_i\alpha_j}[k-N] \tag{11}$$

  ◇ the periodic (or even) cross-correlation function has the property

$$R_{\alpha_i\alpha_j}[k] = R_{\alpha_i\alpha_j}[N-k] \tag{12}$$

  ◇ the name of "odd cross-correlation" function follows from the property

$$\widetilde{R}_{\alpha_i\alpha_j}[k] = -\widetilde{R}_{\alpha_i\alpha_j}[N-k] \tag{13}$$

- For a single code sequence, the corresponding autocorrelation functions have similar properties.

- For best CDMA system performance, all $C_{\alpha_i\alpha_j}[k]$, $R_{\alpha_i\alpha_j}[k]$, $\widetilde{R}_{\alpha_i\alpha_j}[k]$ should be as small as possible, since they are proportional to the interference from other users.

  The out-of-phase (i.e. for lag not equal to zero) autocorrelation functions should also be made as small as possible, since these affect the multipath suppression capabilities and the acquisition and tracking performance of the receivers.

  We thus define the peak cross-correlation parameters

$$\begin{cases} R_{\text{cross}} = \max\left\{ \left\| R_{\alpha_i\alpha_j}[k] \right\|, \forall (i,j,k;\ i<j) \right\} \\ \widetilde{R}_{\text{cross}} = \max\left\{ \left\| \widetilde{R}_{\alpha_i\alpha_j}[k] \right\|, \forall (i,j,k;\ i<j) \right\}, \\ C_{\text{cross}} = \max\left\{ \left\| C_{\alpha_i\alpha_j}[k] \right\|, \forall (i,j,k;\ i<j) \right\} \end{cases} \tag{14}$$

- Similarly we define the peak autocorrelation parameters

$$\begin{cases} R_{\text{auto}} = \max\left\{ \left\| R^N_{\alpha_i\alpha_i}[k] \right\|, \forall i;\ \forall k \neq 0 (\text{mod } N) \right\}, \\ \widetilde{R}_{\text{auto}} = \max\left\{ \left\| \widetilde{R}^N_{\alpha_i\alpha_i}[k] \right\|, \forall i;\ \forall k \neq 0 (\text{mod } N) \right\}, \\ C_{\text{auto}} = \max\left\{ \left\| C^N_{\alpha_i\alpha_i}[k] \right\|, \forall i;\ \forall k \neq 0 (\text{mod } N) \right\} \end{cases} \tag{15}$$

- Finally we define

$$\begin{cases} R_{\text{peak}} = \max\{R_{\text{auto}}, R_{\text{cross}}\} \\ \widetilde{R}_{\text{peak}} = \max\left\{\widetilde{R}_{\text{auto}}, \widetilde{R}_{\text{cross}}\right\} \\ C_{\text{peak}} = \max\{C_{\text{auto}}, C_{\text{cross}}\} \end{cases} \tag{16}$$

- With the above definitions we can see that the smaller the peak correlation parameters R_{peak}, $\widetilde{R}_{\text{peak}}$ and C_{peak}, the better the performance of a system. These parameters, however, cannot be made as small as we wish. For example, for a set of K sequences of period N, according to the Welch lower bound ,

$$R_{\text{peak}} \geq N\sqrt{\frac{K-1}{NK-1}} \qquad C_{\text{peak}} \geq N\sqrt{\frac{K-1}{2NK-K-1}} \tag{17}$$

Therefore for large values of K and N the lower bounds on R_{peak} and C_{peak} are approximately

$$R_{\text{peak}} \geq \sqrt{N} \qquad C_{\text{peak}} \geq \sqrt{\frac{N}{2}} \tag{18}$$

Moreover, it can show that

$$R_{\text{auto}}^2 + R_{cross}^2 > N \qquad C_{\text{auto}}^2 + C_{\text{cross}}^2 > \frac{N}{2} \tag{19}$$

The above shows that not only is there a lower bound on the maximum correlation parameters, but also a trade-off between the peak autocorrelation and cross-correlation parameters. Thus the autocorrelation and cross-correlation functions cannot be both made small simultaneously. The design of the code sequences should be therefore very careful so that all the of above quantities of interest remain as small as possible.

Appendix C: The concept of a 'Primitive Polynomial' in GF(2) (see Appendix 4E for 'finite field' basic theory).

- Consider a polynomial $f(D)$ over the binary field GF(2): $f(D) = \underset{\neq 0}{\underset{\uparrow}{f_n}}\, D^n + f_{n-1}D^{n-1} + \ldots + f_1 D + f_0$

  The largest power of D with non-zero coef. is called ***degree*** of $f(D)$ over GF(2)

- if $\underset{m}{\underset{\uparrow}{f(D)}}, \underset{n}{\underset{\uparrow}{g(D)}} \in \mathrm{GF}(2)$ then $\begin{cases} f(D)+g(D) & \in \mathrm{GF}(2) \\ f(D)\,.\,g(D) & \in \mathrm{GF}(2) \end{cases}$

- ***divisible polynomial*:**

  A polynomial $g(D) \in \mathrm{GF}(2)$ is said to divide $f(D) \in \mathrm{GF}(2)$ if $\exists\, h(D)$: $f(D)=h(D).g(D)$.
  Then the polynomial $f(D)$ is called divisible

- ***irreducible polynomial:***

  A polynomial $f(D) \in \mathrm{GF}(2)$ of degree m is called irreducible if $f(D)$ is not divisible by any polynomial over GF(2) of degree less than m but greater than zero.
  (or equivalently if it cannot factored into polynomials of smaller degree whose coefs are also 0 and 1 – i.e the polynomials belong to GF(2))

- two important properties of irreducible polynomials: if $f(D)$=*irreducible* $\Rightarrow \begin{cases} f(0) \neq 0 \\ f(D) \text{ has odd number of terms} \end{cases}$

- ***primitive polynomial:***

  if $\begin{cases} f(D) = \text{irreducible (of degree } m\text{) polynomial, and} \\ f(D) \nmid (D^k - 1) \quad \text{i.e. } f(D) \text{ does not divide } D^k - 1 \text{ for any } k < 2^m - 1 \\ \neq 0 \end{cases}$

  then $f(D) \equiv$ *primitive polynomial*

e.g. $D^3 + D^2 + 1$; $D^4 + D + 1$

- only a small number of polynomials are *primitive*, **but** $\forall m \; \exists$ at least one *primitive* polynomial.

- examples: $f(D) = D^3 + D^2 + 1$ = *primitive*
  $f(D) = D^4 + D^2 + 1$ = *irreducible but not primitive*

Appendix D: FINITE FIELD -BASIC THEORY

- Consider a set $S = \{s_1, s_2, ..., s_M\}$ having M elements.
  A finite field is constructed by defining two binary operations on the set called addition & multiplication such that certain conditions are satisfied. Addition and multiplication of two elements s_i and s_j are denoted $s_i + s_j$ and $s_i + s_j$ respectively.

- The conditions that must be satisfied for S and the two operations to be a finite field are:

1. The addition or multiplication of any two elements of S must yield an element of S.
   That is, the set is closed under both addition and multiplication.

2. Both addition and multiplication must be commutative $\rightarrow s_i \underset{\cdot}{+} s_j = s_j \underset{\cdot}{+} s_i$

3. The set S must contain an **additive identity** element which will always be denoted by 0.
   $$s_i + 0 = s_i$$
4. The set S must contain an **additive inverse** element $-s_i$ for every element s_i
   $$s_i + (-s_i) = 0$$
5. The set S must contain a **multiplicative identity** element which will always be denoted by 1.
   $$s_i.1 = s_i$$
6. The set S must contain a **multiplicative inverse** element s_i^{-1} for every element s_i (excluding the additive identity 0)
   $$s_i.s_i^{-1} = 1$$
7. Multiplication must be **distributive** over addition. $\rightarrow s_i \underset{\cdot}{+} (s_j \underset{\cdot}{+} s_k) = (s_i \underset{\cdot}{+} s_j) \underset{\cdot}{+} s_k$
8. Both addition and multiplication must be **Associative**. $\rightarrow (s_i + s_j) \cdot s_k = s_i s_k + s_j s_k$

• **EXAMPLE**

It is easy to verify that $S = \{0, 1, 2\}$ with addition and multiplication defined as follows

modulo-3 $+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

modulo-3 $\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

is a field of 3 elements

e.g.

additive inverse $-0 = 0$ multiplicative inverse $1^{-1} = 1$

$-1 = 2$ $2^{-1} = 2$

$-2 = 1$

• **EXAMPLE**

It is easy also to verify that $S = \{0, 1\}$, with addition and multiplication defined as follows:

modulo-2 $+$	0	1
0	0	1
1	1	0

modulo-2 $\times$	0	1
0	0	0
1	0	1

is a field of 2 elements

e.g.

additive inverse $-0 = 0$ multiplicative inverse $1^{-1} = 1$

$-1 = 1$

• Note that $S = \{0, 1\}$ field above is the binary number field. Furthermore that addition can be performed electronically using EXCLUSIVE-OR gate and multiplication can be performed using an AND-gate.

• **An Important Result (presented without proof)**:
The set of integers $S = \{0, 1, 2, \ldots, M - 1\}$,

$$\text{where}\begin{cases} M \text{ is prime, and} \\ a\text{ddition and multiplication are carried out modulo-}M \end{cases}$$

is a field. These fields are called **<u>prime fields</u>**.

• **Subtraction and Division:**
The operations of subtraction and division are also easily defined for any field using the addition and multiplication tables, just as is done with the real-number field.
Subtraction is defined as the addition of the additive inverse and division is defined as multiplication by the multiplicative inverse.
For example for the field $S = \{0,1,2\}$ subtraction is defined by 1 + (− 2) = 1 + 1 = 2.
Similarly, $1 \div 2 = 1 \,.\, (2^{-1}) = 1.2 = 2$.

• Note that nonprime fields do not necessarily employ modulo-M arithmetic.

• Fields can be constructed having any prime number of elements p or p^m. A field having p^m elements is called an extension field of the field having p elements.

• Finite fields are often referred to as Galois fields, using the notation GF(M) for the field having M elements.

• The remainder of this discussion will be concerned exclusively with the binary number field GF(2) and its extensions GF(2^m). The reason for this is that the electronics used to implement the code generators is binary, and some of the shift register generators will be shown to generate the elements of GF(2^m)

Appendix E: Table of Irreducible Polynomials over GF(2)

(from "Error-Correcting Codes" by Peterson & Weldom MIT Press, 1972)

From : "Error-Correcting Codes"
by Peterson & Weldon
MIT PRESS , 1972.

Appendix C Tables of Irreducible Polynomials over $GF(2)$

From Table C.2 all irreducible polynomials of degree 16 or less over $GF(2)$ can be found, and certain of their properties and relations among them are given. A primitive polynomial with a minimum number of nonzero coefficients and polynomials belonging to all possible exponents are given for each degree 17 through 34.

Polynomials are given in an octal representation. Each digit in the table represents three binary digits according to the following code:

0	000	2	010	4	100	6	110
1	001	3	011	5	101	7	111

The binary digits then are the coefficients of the polynomial, with the high-order coefficients at the left. For example, 3525 is listed as a tenth-degree polynomial. The binary equivalent of 3525 is 011101010101, and the corresponding polynomial is $X^{10} + X^9 + X^8 + X^6 + X^4 + X^2 + 1$.

The reciprocal polynomial of an irreducible polynomial is also irreducible, and the reciprocal polynomial of a primitive polynomial is primitive. Of any pair consisting of a polynomial and its reciprocal polynomial, only one is listed in the table. Each entry that is followed by a letter in the table is an irreducible polynomial of the indicated degree. For degree 2 through 16, these polynomials along with their reciprocal polynomials comprise all irreducible polynomials of that degree.

The letters following the octal representation give the following information:

A, B, C, D	Not primitive.
E, F, G, H	Primitive.
A, B, E, F	The roots are linearly dependent.
C, D, G, H	The roots are linearly independent.
A, C, E, G	The roots of the reciprocal polynomial are linearly dependent.
B, D, F, H	The roots of the reciprocal polynomial are linearly independent.

The other numbers in the table tell the relation between the polynomials. For each degree, a primitive polynomial with a minimum number of nonzero coefficients was chosen, and this polynomial is the first in the table of polynomials of this degree. Let α denote one of its roots. Then the entry following j in the table is the minimum polynomial of α^j. The polynomials are included for each j unless for some $i < j$ either α^i and α^j are roots of the same irreducible polynomial or α^i and α^{-j} are roots of the same polynomial. The minimum polynomial of α^j is included even if it has smaller degree than is indicated for that section of the table; such polynomials are not followed by a letter in the table.

Examples. The primitive polynomial (103), or $X^6 + X + 1 = p(X)$ is the first entry in the table of sixth-degree irreducible polynomials. If α designates a root of $p(X)$, then α^3 is a root of (127) and α^5 is a root of (147). The minimum polynomial of α^9 is $(015) = X^3 + X^2 + 1$, and is of degree 3 rather than 6.

There is no entry corresponding to α^{17}. The other roots of the minimum polynomial of α^{17} are α^{34}, $\alpha^{68} = \alpha^5$, α^{10}, α^{20}, and α^{40}. Thus the minimum polynomial of α^{17} is the same as the minimum polynomial of α^5, or (147). There is no entry corresponding to α^{13}. The other roots of the minimum polynomial $p_{13}(X)$ of α^{13} are α^{26}, α^{52}, $\alpha^{104} = \alpha^{41}$, $\alpha^{82} = \alpha^{19}$, and α^{38}. None of these is listed. The roots of the reciprocal polynomial $p_{13}^*(X)$ of $p_{13}(X)$ are $\alpha^{-13} = \alpha^{50}$, $\alpha^{-26} = \alpha^{37}$, $\alpha^{-52} = \alpha^{11}$, $\alpha^{-41} = \alpha^{22}$, $\alpha^{-19} = \alpha^{44}$ and $\alpha^{-38} = \alpha^{25}$. The minimum polynomial of α^{11} is listed as (155) or $X^6 + X^5 + X^3 + X^2 + 1$. The minimum polynomial of α^{13} is the reciprocal polynomial of this, or $p_{13}(X) = X^6 + X^4 + X^3 + X + 1$:

The exponent to which a polynomial belongs can be found as follows: If α is a primitive element of $GF(2^m)$, then the order e of α^j is

$$e = \frac{(2^m - 1)}{\mathrm{GCD}(2^m - 1, j)}$$

and e is also the exponent to which the minimum function of α^j belongs. Thus, for example, in $GF(2^{10})$, α^{55} has order 93, since

$$93 = \frac{1023}{\mathrm{GCD}(1023, 55)} = \frac{1023}{11}$$

Thus the polynomial (3453) belongs to 93. In this regard Table C.1 is useful.

Marsh (1957) has published a table of all irreducible polynomials of degree 19 or less over $GF(2)$. In Table C.2 the polynomials are arranged in lexicographical order; this is the most convenient form for determining whether or not a given polynomial is irreducible.

For degree 19 or less, the minimum-weight polynomials given in this table were found in Marsh's tables. For degree 19 through 34, the minimum-weight polynomial was found by a trial-and-error process in which each polynomial of weight 3, then 5, was tested. The following procedure was used to test whether a polynomial $f(X)$ of degree m is primitive:

Table C.1. Factorization of $2^m - 1$ into Primes.

$2^3 - 1 = 7$	$2^{19} - 1 = 524287$
$2^4 - 1 = 3 \times 5$	$2^{20} - 1 = 3 \times 5 \times 5 \times 11 \times 31 \times 41$
$2^5 - 1 = 31$	$2^{21} - 1 = 7 \times 7 \times 127 \times 337$
$2^6 - 1 = 3 \times 3 \times 7$	$2^{22} - 1 = 3 \times 23 \times 89 \times 683$
$2^7 - 1 = 127$	$2^{23} - 1 = 47 \times 178481$
$2^8 - 1 = 3 \times 5 \times 17$	$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$
$2^9 - 1 = 7 \times 73$	$2^{25} - 1 = 31 \times 601 \times 1801$
$2^{10} - 1 = 3 \times 11 \times 31$	$2^{26} - 1 = 3 \times 2731 \times 8191$
$2^{11} - 1 = 23 \times 89$	$2^{27} - 1 = 7 \times 73 \times 262657$
$2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$	$2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$
$2^{13} - 1 = 8191$	$2^{29} - 1 = 233 \times 1103 \times 2089$
$2^{14} - 1 = 3 \times 43 \times 127$	$2^{30} - 1 = 3 \times 3 \times 7 \times 11 \times 31 \times 151 \times 331$
$2^{15} - 1 = 7 \times 31 \times 151$	$2^{31} - 1 = 2147483647$
$2^{16} - 1 = 3 \times 5 \times 17 \times 257$	$2^{32} - 1 = 3 \times 5 \times 17 \times 257 \times 65537$
$2^{17} - 1 = 131071$	$2^{33} - 1 = 7 \times 23 \times 89 \times 599479$
$2^{18} - 1 = 3 \times 3 \times 3 \times 7 \times 19 \times 73$	$2^{34} - 1 = 3 \times 43691 \times 131071$

1. The residues of $1, X, X^2, X^4, \ldots, X^{2^{m-1}}$ are formed modulo $f(X)$.
2. These are multiplied and reduced modulo $f(X)$ to form the residue of $X^{2^m} - 1$. If the result is not 1, the polynomial is rejected. If the result is 1, the test is continued.
3. For each factor r of $2^m - 1$, the residue of X^r is formed by multiplying together an appropriate combination of the residues formed in Step 1. If none of these is 1, the polynomial is primitive.

Each other polynomial in the table was found by solving for the dependence relations among its roots by the method illustrated at the end of Section 8.1.

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 2	1 7H				
DEGREE 3	1 13F				
DEGREE 4	1 23F	3 37D	5 07		
DEGREE 5	1 45E	3 75G	5 67H		
DEGREE 6	1 103F	3 127B	5 147H	7 111A	9 015
11 155E	21 007				
DEGREE 7	1 211E	3 217E	5 235E	7 367H	9 277E
11 325G	13 203F	19 313H	21 345G		
DEGREE 8	1 435E	3 567B	5 763D	7 551E	9 675C
11 747H	13 453F	15 727D	17 023	19 545E	21 613D
23 543F	25 433B	27 477B	37 537F	43 703H	45 471A
51 037	85 007				
DEGREE 9	1 1021E	3 1131E	5 1461G	7 1231A	9 1423G
11 1055E	13 1167F	15 1541E	17 1333F	19 1605G	21 1027A
23 1751E	25 1743H	27 1617H	29 1553H	35 1401C	37 1157F
39 1715E	41 1563H	43 1713H	45 1175E	51 1725G	53 1225E
55 1275E	73 0013	75 1773G	77 1511C	83 1425G	85 1267E
DEGREE 10	1 2011E	3 2017B	5 2415E	7 3771G	9 2257B
11 2065A	13 2157F	15 2653B	17 3515G	19 2773F	21 3753D
23 2033F	25 2443F	27 3573D	29 2461E	31 3043D	33 0075C
35 3023H	37 3543F	39 2107B	41 2745E	43 2431E	45 3061C
47 3177H	49 3525G	51 2547B	53 2617F	55 3453D	57 3121C
59 3471G	69 2701A	71 3323H	73 3507H	75 2437B	77 2413B
83 3623H	85 2707E	87 2311A	89 2327F	91 3265G	93 3777D
99 0067	101 2055E	103 3575G	105 3607C	107 3171G	109 2047F
147 2355A	149 3025G	155 2251A	165 0051	171 3315C	173 3337H
179 3211G	341 0007				
DEGREE 11	1 4005E	3 4445E	5 4215E	7 4055E	9 6015G
11 7413H	13 4143F	15 4563F	17 4053F	19 5023F	21 5623F
23 4757B	25 4577F	27 6233H	29 6673H	31 7237H	33 7335G
35 4505E	37 5337F	39 5263F	41 5361E	43 5171E	45 6637H
47 7173H	49 5711E	51 5221E	53 6307H	55 6211G	57 5747F
59 4533F	61 4341E	67 6711G	69 6777D	71 7715G	73 6343H
75 6227H	77 6263H	79 5235E	81 7431G	83 6455G	85 5247F
87 5265E	89 5343B	91 4767F	93 5607F	99 4603F	101 6561G
103 7107H	105 7041G	107 4251E	109 5675E	111 4173F	113 4707F
115 7311C	117 5463F	119 5755E	137 6675G	139 7655G	141 5531E
147 7243H	149 7621G	151 7161G	153 4731E	155 4451E	157 6557H
163 7745G	165 7317H	167 5205E	169 4565E	171 6765G	173 7535G
179 4653F	181 5411E	183 5545E	185 7565G	199 6543H	201 5613F
203 6013H	205 7647H	211 6507H	213 6037H	215 7363H	217 7201G
219 7273H	293 7723H	299 4303B	301 5007F	307 7555G	309 4261E
331 6447H	333 5141E	339 7461G	341 5253F		
DEGREE 12	1 10123F	3 12133B	5 10115A	7 12153B	9 11765A
11 15647E	13 12513B	15 13077B	17 16533H	19 16047H	21 10065A
23 11015E	25 13377B	27 14405A	29 14127H	31 17673H	33 13311A
35 10377B	37 13565E	39 13321A	41 15341G	43 15053H	45 15173C
47 15621E	49 17703C	51 10355A	53 15321G	55 10201A	57 12331A
59 11417E	61 13505E	63 10761A	65 00141	67 13275E	69 16663C
71 11471E	73 16237E	75 16267D	77 15115C	79 12515E	81 17545C
83 12255E	85 11673B	87 17361A	89 11271E	91 10011A	93 14755C
95 17705A	97 17121G	99 17323D	101 14227H	103 12117E	105 13617A
107 14135G	109 14711G	111 15415C	113 13131E	115 13223A	117 16475C
119 14315C	121 16521E	123 13475A	133 11433B	135 10571A	137 15437G
139 12067F	141 13571A	143 12111A	145 16535C	147 17657D	149 12147F
151 14717F	153 13517B	155 14241C	157 14675G	163 10663F	165 10621A

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 12--CONTINUED					
167 16115G	169 16547C	171 10213B	173 12247E	175 16757D	177 16017C
179 17675E	181 10151E	183 14111A	185 14037A	187 14613H	189 13535A
195 00165	197 11441E	199 10321E	201 14067D	203 13157B	205 14513D
207 10603A	209 11067F	211 14433F	213 16457D	215 10653B	217 13563B
219 11657B	221 17513C	227 12753F	229 13431E	231 10167B	233 11313F
235 11411A	237 13737B	239 13425E	273 00023	275 14601C	277 16021G
279 16137D	281 17025G	283 15723F	285 17141A	291 15775A	293 11477F
295 11463B	297 17073C	299 16401C	301 12315A	307 14221E	309 11763B
311 12705E	313 14357F	315 17777D	325 00163	327 17233D	329 11637B
331 16407F	333 11703A	339 16003C	341 11561E	343 12673B	345 14537D
347 17711G	349 13701E	355 10467B	357 15347C	359 11075E	361 16363F
363 11045A	365 11265A	371 14043D	397 12727F	403 14373D	405 13003B
407 17057G	409 10437F	411 10077B	421 14271G	423 14313D	425 14155C
427 10245A	429 11073B	435 10743B	437 12623F	439 12007F	441 15353D
455 00111	585 00013	587 14545G	589 16311G	595 13413A	597 12265A
603 14411C	613 15413H	619 17147F	661 10605E	683 10737F	685 16355C
691 15701G	693 12345A	715 00133	717 16571C	819 00037	1365 00007
DEGREE 13	1 20033F	3 23261E	5 24623F	7 23517F	9 30741G
11 21643F	13 30171G	15 21277F	17 27777F	19 35051G	21 34723H
23 34047H	25 32535G	27 31425G	29 37505G	31 36515G	33 26077F
35 35673H	37 20635E	39 33763H	41 25745E	43 36575G	45 26653F
47 21133F	49 22441E	51 30417H	53 32517H	55 37335G	57 25327F
59 23231E	61 25511E	63 26533F	65 33343H	67 33727H	69 27271E
71 25017F	73 26041E	75 21103F	77 27263F	79 24513F	81 32311G
83 31743H	85 24037F	87 30711G	89 32641G	91 24657F	93 32437H
95 20213F	97 25633F	99 31303H	101 22525E	103 34627H	105 25775E
107 21607F	109 25363F	111 27217F	113 33741G	115 37611G	117 23077F
119 21263F	121 31011G	123 27051E	125 35477H	131 34151G	133 27405E
135 34641G	137 32445G	139 36375G	141 22675E	143 36073H	145 35121G
147 36501G	149 33057H	151 36403H	153 35567H	155 23167F	157 36217H
159 22233F	161 32333H	163 24703F	165 33163H	167 32757H	169 23761E
171 24031E	173 30025G	175 37145G	177 31327H	179 27221E	181 25577F
183 22203F	185 37437H	187 27537F	189 31035G	195 24763F	197 20245E
199 20503F	201 20761E	203 25555E	205 30357H	207 33037H	209 34401G
211 32715G	213 21447F	215 27421E	217 20363F	219 33501G	221 20425E
223 32347H	225 20677F	227 22307F	229 33441G	231 33643H	233 24165E
235 27427F	237 24601E	239 36721G	241 34363H	243 21673F	245 32167H
247 21661E	265 33357H	267 26341E	269 31653H	271 37511G	273 23003F
275 22657F	277 25035E	279 23267F	281 34005G	283 34555G	285 24205E
291 26611E	293 32671G	295 25245E	297 31407H	299 33471G	301 22613F
303 35645G	305 32371G	307 34517H	309 26225E	311 35561G	313 25663F
315 24043F	317 30643H	323 20157F	325 37151G	327 24667F	329 33325G
331 32467H	333 30667H	335 22631E	337 26617F	339 20275E	341 36625G
343 20341E	345 37527H	347 31333H	349 31071G	355 23353F	357 26243F
359 21453F	361 36015G	363 36667H	365 34767H	367 34341G	369 34547H
371 35465G	373 24421E	375 23563F	377 36037H	391 31267H	393 27133F
395 30705G	397 30465G	399 35315G	401 32231G	403 32207H	405 26101E
407 22567F	409 21755E	411 22455E	413 33705G	419 37621G	421 21405E
423 30117H	425 23021E	427 21525E	429 36465G	431 33013H	433 27531E
435 24675E	437 33133H	439 34261G	441 33405G	443 34655G	453 32173H
455 33455G	457 35165G	459 22705E	461 37123H	463 27111E	465 35455G
467 31457H	469 23055E	471 30777H	473 37653H	475 24325E	477 31251G
547 35163H	549 33433H	551 37243H	553 27515E	555 32137H	557 26743F
563 30277H	565 20627F	567 35057H	569 24315E	571 24727F	581 30331G
583 34273H	585 23207F	587 31113H	589 36023H	595 27373F	597 20737F
599 36235G	601 21575E	603 26215E	605 21211E	611 20311E	613 34003H
615 34027H	617 20065E	619 22051E	621 22127F	627 23621E	629 24465E
651 26457F	653 31201G	659 34035G	661 27227F	663 22561E	665 21615E
667 22013F	669 23365E	675 26213F	677 26775E	679 32635G	681 33631G
683 32743H	685 31767H	691 34413H	693 22037F	695 30651G	697 26565E
711 22141E	713 22471E	715 35271G	717 37445G	723 22717F	725 26505E
727 24411E	729 24575E	731 23707F	733 25173F	739 21367F	741 25161E
743 24147F	793 36307H	795 24417F	805 20237F	807 36771G	809 37327H
811 27735E	813 31223H	819 36373H	821 33121G	823 32751G	825 33523H

Table C.2. Irreducible Polynomials of Degree ≤34 over *GF*(2).

DEGREE 13--CONTINUED

839 26415E	841 23737F	843 25425E	845 34603H	851 31047H	853 37305G
855 21315E	857 35777H	859 32725G	869 20571E	871 30301G	873 34757H
875 21067F	877 25151E	1171 27513F	1173 33721G	1179 34775G	1189 23571E
1195 27411E	1197 20457F	1203 21557F	1205 30177H	1227 26347F	1229 27477F
1235 34243H	1237 27235E	1323 25175E	1325 31231G	1331 31131G	1333 25503F
1355 33045G	1357 24253F	1363 35351G	1365 26053F		

DEGREE 14

	1 42103F	3 40547B	5 43333E	7 51761E	9 54055A
11 40503F	13 77141G	15 47645A	17 62677G	19 44103F	21 46425A
23 45145E	25 76303G	27 62603D	29 64457G	31 57231E	33 52737B
35 64167F	37 60153F	39 62115C	41 55753F	43 72427D	45 64715A
47 70423H	49 47153F	51 67653D	53 53255E	55 41753F	57 74247D
59 40725E	61 42667F	63 65301A	65 67517H	67 45653F	69 72501C
71 67425G	73 42163F	75 73757D	77 45555E	79 74561G	81 60523B
83 53705E	85 40123E	87 41403B	89 56625E	91 70311E	93 75547C
95 45627F	97 67335G	99 56733A	101 53253F	103 66411E	105 57745A
107 65551G	109 43017F	111 62125A	113 71073E	115 67333H	117 70677C
119 52215E	121 44177F	123 70535C	125 46327F	127 71747D	129 00203
131 61335G	133 43161E	135 46047B	137 60645G	139 40317F	141 47727A
143 65001G	145 54335E	147 76175C	149 65153H	151 50351E	153 42711A
155 41625E	157 44435E	159 41163A	161 47667F	163 41441E	165 54175A
167 45713F	169 75267H	171 72051C	173 64223H	175 42337F	177 51275A
179 65155E	181 63015E	183 57521A	185 67173H	187 50661E	189 41735A
191 50645E	193 72433F	195 47043B	197 65133H	199 53543F	201 62431A
203 42777F	205 47203F	207 46605A	209 64377H	211 73725G	213 43611A
215 42301A	217 51145E	219 44307B	221 73647H	223 74427H	225 53747A
227 45511E	229 42637F	231 63117D	233 40363E	235 75201G	237 63155C
239 72717G	241 56557F	243 75363D	245 70553F	247 66675G	249 55501A
251 60263H	261 53043B	263 75303F	265 74315E	267 66031A	269 62505G
271 60057H	273 54473A	275 60253F	277 45671E	279 71525C	281 61443E
283 64635G	285 64475C	287 67401G	289 44203F	291 50343A	293 77747H
295 54101E	297 65645A	299 41177F	301 65661A	303 42361A	305 43047F
307 45563F	309 50717A	311 53233E	313 67101G	315 62251C	317 64251E
323 40635E	325 46113E	327 44367B	329 40665E	331 63331G	333 71545C
335 73107H	337 42727F	339 43775A	341 65667E	343 61677H	345 53525A
347 52723F	349 42323F	351 41433B	353 43173E	355 46305E	357 45663B
359 71315E	361 44031E	363 73457B	365 52577E	367 52621E	369 40063B
371 52027F	373 45201E	375 77001C	377 45737E	379 64035G	381 52225A
387 00253	389 60765G	391 66545G	393 71323A	395 62767G	397 73137H
399 40145A	401 63265G	403 47551E	405 71711C	407 40353F	409 76055G
411 70065C	413 73527F	415 67201G	417 43723B	419 61251E	421 47357F
423 62261C	425 50575E	427 61267H	429 40511A	431 71721G	433 65121G
435 61053D	437 45371E	439 54627E	441 77703A	443 65057H	445 76225E
451 73071G	453 52553B	455 60025E	457 60471G	459 53513B	461 67303H
463 42763F	465 52261A	467 53657F	469 75443F	471 67267D	473 53373B
475 65165E	477 44037B	479 54737F	481 61175E	483 65031A	485 51707E
487 57627F	489 57251A	491 44073F	493 45761E	495 63463C	529 65277F
531 55247B	533 56171E	535 63513H	537 43377B	539 45641E	541 63227H
547 54243F	549 62055C	551 53061E	553 46321E	555 51431A	557 71147H
559 64053D	561 41551A	563 75521E	565 46701E	567 53763B	569 56463F
571 77057G	573 41105A	579 41171A	581 41307F	583 70425E	585 74117D
587 50135E	589 67737H	591 47615A	593 53057F	595 55103F	597 54443B
599 53051E	601 61555G	603 64157D	605 57407F	611 64653F	613 65513H
615 73603D	617 47525E	619 55165E	621 64215C	623 76377H	625 57365E
627 50557B	629 45725E	631 71301G	633 56465A	635 51745A	645 00217
647 47233F	649 53015E	651 53361A	653 46215E	655 50613E	657 77211C
659 46565E	661 44141E	663 55771A	665 71263G	667 41315E	669 62225C
675 51565A	677 76267H	679 62467H	681 64003C	683 71645G	685 76223G
687 52627A	689 70665G	691 45773F	693 64033D	695 45533E	697 50007F
699 45257B	701 45311E	707 44023F	709 72153G	711 60117D	713 46617E
715 70461G	717 47513B	719 65575E	721 56435E	723 67157C	725 71403G
727 46107F	729 65007A	731 50667B	733 55331E	739 52017F	741 51317B
743 66163F	745 70767G	747 70215C	749 76401G	751 63043H	753 63753D
755 43317F	781 77031G	783 45617B	785 52603F	787 57503F	789 63667D
791 75761G	793 60075G	795 72307B	797 51633F	803 57475E	805 61533G

Table C.2. Irreducible Polynomials of Degree ≤34 over *GF*(2).

DEGREE 14--CONTINUED

807 60561C	809 53575E	811 62027H	813 64633C	815 67123F	817 43445A
819 73655C	821 54003F	823 62347F	825 63271C	827 71337F	837 57715A
839 54635E	841 46505E	843 64407C	845 57017E	847 54751E	849 42417A
851 57033F	853 54077F	855 42567B	857 50455E	859 62533H	861 42411A
867 74133D	869 72441G	871 43577F	873 52353B	875 55325E	877 67527G
879 75605C	881 52467F	883 61757F	885 66105C	887 51261E	889 62723D
903 00375	905 63537H	907 52457E	909 44735A	911 62413H	913 51671E
915 41001A	917 70773H	919 56031E	921 60227D	923 71345G	925 46125E
931 40655E	933 44221A	935 55323F	937 76005E	939 55435A	941 42531E
943 62671E	945 74277D	947 64617G	949 52137F	951 56637B	953 47753F
955 46773F	1093 72155G	1095 56067A	1097 63007E	1099 47111E	1101 54021A
1107 44523B	1109 54257F	1111 63567H	1113 43215A	1115 73665G	1117 45335E
1123 44147E	1125 62731C	1127 41657F	1129 77235G	1131 65643B	1133 51055E
1139 47637F	1141 40071E	1143 47771A	1161 00271	1163 57541E	1165 57107F
1171 61621G	1173 51511A	1175 57201E	1177 70251G	1179 43633B	1181 53315E
1187 44343F	1189 55705E	1191 40413B	1193 64641E	1195 44567E	1197 46451A
1203 60241C	1205 65705E	1207 71117H	1209 66703D	1211 53477F	1221 45355A
1223 74531G	1225 74607H	1227 71763C	1229 76707H	1235 60235G	1237 47673F
1239 54321A	1241 75571G	1243 77515G	1245 57611A	1251 55643B	1253 46175E
1255 74357H	1257 70267D	1259 46461E	1301 77345G	1303 51243F	1305 76151C
1307 56061E	1309 66427G	1315 54517F	1317 72465C	1319 50733F	1321 74045G
1323 71057D	1325 73143F	1331 51231E	1333 70201C	1335 77631C	1337 64021G
1351 72643H	1353 41777B	1355 71675G	1357 63073H	1363 47537E	1365 61261A
1367 65227H	1369 55073F	1371 77727B	1373 61363H	1379 43701E	1381 65147H
1383 52267B	1385 63153F	1387 72337G	1389 56607A	1395 40371A	1397 42721A
1419 00211	1421 75273F	1427 73555G	1429 67225G	1431 76617C	1433 74711E
1435 50325E	1437 70713C	1443 72513D	1445 57737F	1447 61333G	1449 40327A
1451 55111E	1453 40633F	1459 61641G	1461 65315C	1463 43647F	1465 67621G
1479 62745C	1481 41755E	1483 65727F	1485 74263D	1587 41573B	1589 55631E
1591 66405A	1593 60121C	1607 71615E	1609 77615G	1611 41447B	1613 46437F
1619 70633H	1621 65615G	1623 64605C	1625 55075E	1627 73151G	1637 75033H
1639 57327F	1641 66277D	1643 56007F	1645 55703F	1651 77277D	1677 00345
1683 57743A	1685 42645E	1687 50045E	1689 74255C	1691 53623E	1701 50477B
1703 52071E	1705 61237H	1707 67533B	1709 55417F	1715 45173E	1717 61461G
1719 43731A	1721 56717E	1735 54041E	1737 44613A	1739 70341G	1741 52065E
1747 56345E	1749 44441A	1751 76663H	1753 50777F	1755 70443D	2341 55471E
2347 53727F	2349 65637C	2355 57143B	2357 44741E	2379 67627D	2381 77177G
2387 51213E	2389 70273H	2395 62101G	2405 50241E	2411 65263H	2413 41241A
2451 00357	2453 76047H	2459 75723F	2469 73145C	2475 61377D	2477 41357F
2643 56421A	2645 76213H	2667 64213D	2709 00313	2731 41235E	2733 67605C
2739 44537B	2741 76505G	2763 65375C	2765 50721E	2771 75517H	2861 65357G
2867 47121E	5461 00007				

DEGREE 15

1 100003F	3 102043F	5 110013F	7 125253B	
9 102067F	11 104307F	13 100317F	15 177775E	17 103451E
19 110075E	21 127701A	23 102061E	25 114725E	27 103251E
29 163005G	31 103437A	33 112611E	35 137733B	37 120265E
39 117423F	41 106341E	43 161007H	45 174003E	47 113337E
49 125263B	51 126007E	53 105257E	55 114467E	57 177207G
59 147047F	61 111511E	63 127635A	65 114633E	67 133663F
69 102171E	71 170465G	73 131427E	75 161615E	77 136143A
79 115155E	81 123067F	83 102561E	85 170057H	87 125235E
89 173117E	91 125747B	93 124677B	95 134531E	97 125507F
99 171737G	101 152417F	103 142305G	105 146255C	107 120043F
109 136173F	111 122231E	113 164705G	115 177757F	117 146637E
119 177535C	121 102643F	123 103145E	125 112751E	127 151537G
129 115135E	131 137067E	133 122707A	135 174443E	137 100541E
139 112273F	141 145573F	143 114273F	145 124511E	147 122563B
149 140703F	151 101361A	153 103125E	155 150451C	157 147303G
159 123023F	161 103751A	163 154463H	165 177541G	167 101561E
169 144473G	171 162375G	173 131013F	175 117767A	177 160521G
179 164727G	181 102367E	183 147363F	185 132367E	187 172431E
189 133627B	191 156333E	193 114505E	195 176561G	197 152235G
199 127143F	201 176133E	203 123075A	205 173357G	207 117143E
209 144461E	211 151447G	213 173661E	215 151043F	217 142327B

Table C.2. Irreducible Polynomials of Degree ≤34 over $GF(2)$.

DEGREE 15--CONTINUED

219	166775E	221	153143G	223	172213F	225	105213E	227	156053H
229	156745G	231	170623B	233	140373G	235	152361G	237	142157H
239	117633F	241	103605E	243	116361E	245	137523A	247	101705E
249	116135E	251	102337E	253	173515G	259	136321A	261	120447F
263	117511E	265	115141E	267	173613F	269	131735E	271	114225E
273	121125A	275	136577F	277	113227E	279	114533B	281	166151E
283	112231E	285	165033E	287	120177B	289	117547F	291	126051E
293	111335E	295	177101G	297	143703G	299	106047E	301	137427B
303	110427F	305	131211E	307	110037F	309	160511G	311	153731G
313	144275G	315	151513C	317	133775E	319	134447E	321	127347E
323	163767H	325	110717E	327	175001E	329	100377A	331	125121E
333	136237F	335	132103F	337	171035G	339	132651E	341	134105A
343	100261A	345	170227H	347	101233F	349	100445E	351	144707G
353	165355E	355	150243H	357	163353C	359	114041E	361	113025E
363	104447F	365	143301G	367	165011G	369	137361E	371	117201A
373	141655G	375	160113G	377	106715E	379	140575E	381	112123E
387	140733F	389	124243E	391	116073E	393	147321E	395	123721E
397	150225G	399	134741A	401	157111G	403	134411A	405	172317G
407	153327E	409	140573H	411	113625E	413	101673B	415	170543F
417	176735E	419	115307F	421	141635E	423	157241G	425	153005E
427	167051A	429	177175G	431	146331G	433	166541G	435	102513F
437	123121E	439	162463G	441	134037B	443	174571E	445	123433F
447	150167H	449	175465E	451	113255E	453	137325A	455	123045A
457	133571E	459	135215E	461	110221E	463	157435E	465	121437A
467	177707G	469	143501C	471	161667F	473	157427G	475	150671G
477	112407F	479	165563E	481	112053E	483	135363B	485	130617F
487	125613F	489	114713F	491	165113G	493	143733G	495	162155E
497	135017B	499	126753F	501	137765E	503	106577E	521	112113F
523	105555E	525	153425C	527	115313A	529	105761E	531	132165E
533	176147H	535	114621E	537	135751E	539	152763C	541	124757F
543	112245E	545	123221E	547	141757G	549	160547F	551	101331E
553	156065C	555	156725G	557	113373E	559	137643F	561	156237G
563	141151G	565	126015E	567	171335C	569	146717H	571	130305E
573	121355E	579	166021G	581	145361C	583	134325E	585	157155E
587	124647E	589	163761C	591	114457E	593	155243G	595	153137D
597	137253F	599	151551G	601	113645E	603	150305G	605	163745G
607	165473F	609	113057B	611	160173H	613	177663F	615	161117H
617	144115E	619	156635G	621	150633H	623	115061A	625	143253H
627	165451G	629	160305E	631	146025E	633	106751E	635	132625E
637	160553D	643	123561E	645	116637F	647	111423E	649	117107E
651	166761C	653	153555G	655	132127F	657	112333E	659	135267F
661	146727H	663	132753F	665	143343A	667	131705E	669	141005E
671	113147F	673	125323F	675	123235E	677	103653F	679	173025C
681	120661E	683	154545G	685	133553F	687	132001E	689	153773G
691	175241G	693	160237B	695	171131E	697	172415E	699	145111G
701	122603F	707	170507C	709	160757G	711	171207G	713	147553B
715	112365E	717	146111E	719	122003F	721	121273B	723	122005E
725	135401E	727	102441E	729	175515G	731	132507E	733	130223F
735	142713C	737	102615E	739	105713F	741	134241E	743	173643F
745	163617G	747	175043E	749	132051A	751	104217F	753	115523F
755	120247B	757	164447H	759	173667F	761	137051E	775	104073B
777	177065C	779	117071E	781	115537E	783	135201E	785	146643F
787	113465E	789	152263G	791	177617D	793	104755E	795	147415G
797	126001E	799	170307F	801	174425E	803	112475E	805	173263C
807	176643H	809	130303F	811	125471E	813	173711G	815	165547E
817	163723G	819	116075A	821	150677G	823	175227G	825	166407H
827	152447H	829	126205E	835	120557E	837	160335A	839	125543E
841	144377H	843	100713E	845	121251E	847	141123D	849	174517F
851	106251E	853	116277F	855	106611E	857	174563H	859	140023H
861	132037A	863	147767G	865	164531G	867	155065E	869	146263F
871	160401G	873	102057F	875	146133C	877	117021E	879	147003F
881	127723F	883	120471E	885	162455G	887	130627F	889	152135C
891	157057H	901	162153F	903	151755C	905	170277H	907	165633H
909	173105E	911	102507F	913	176037H	915	171627G	917	162171C
919	130745E	921	177517H	923	114327F	925	127167F	927	133113E

Table C.2. Irreducible Polynomials of Degree ≤34 over $GF(2)$.

DEGREE 15--CONTINUED

929	160461E	931	117137B	933	134323F	935	123361E	937	105237F
939	166737F	941	147571G	943	127743F	945	116351A	947	157315E
949	162645G	951	162403G	953	105335E	955	124767E	957	175301E
963	134755E	965	116645E	967	143307G	969	124125E	971	155261G
973	104163A	975	167753F	977	127423F	979	115667F	981	140171E
983	133041E	985	156767H	987	116037A	989	142267G	991	130635E
1057	000057	1059	104427F	1061	113075E	1063	162133H	1065	120717F
1067	144713F	1069	121605E	1071	122225A	1073	134657E	1075	130125E
1077	177621G	1079	110741E	1081	136745E	1083	152531G	1085	115455A
1091	161235G	1093	144137G	1095	140675E	1097	145277G	1099	114303B
1101	101507E	1103	115271E	1105	151735E	1107	157205G	1109	114011E
1111	171125E	1113	147071A	1115	134721E	1117	122123F	1123	104735E
1125	133011E	1127	162337A	1129	105261E	1131	101427E	1133	156563F
1135	103663E	1137	146043H	1139	151403H	1141	100157A	1143	163653E
1145	105413F	1147	143651C	1157	156157E	1159	102463F	1161	151025G
1163	176657H	1165	166425G	1167	103617E	1169	160021A	1171	161277H
1173	165565G	1175	152153F	1177	111243E	1179	165655G	1181	134165E
1187	171467H	1189	150161E	1191	122011E	1193	125403F	1195	170007H
1197	167765C	1199	103415E	1201	137703E	1203	111563F	1205	147305G
1207	156257F	1209	175177B	1211	141317B	1213	177467H	1219	140421G
1221	127071E	1223	142457F	1225	122021A	1227	146771E	1229	110211E
1231	134567F	1233	156321G	1235	114335E	1237	111603E	1239	121275A
1241	110103E	1243	127161E	1245	163273H	1251	144533F	1253	173135C
1255	155445E	1257	140441E	1259	103761E	1261	173523F	1263	167307F
1265	127457F	1267	102205A	1269	112251E	1291	106311E	1293	141633F
1295	135151A	1297	106641E	1299	102265E	1301	164453G	1303	163071G
1305	111641E	1307	134403E	1309	102667A	1315	177055E	1317	115373F
1319	150231G	1321	175651G	1323	160377B	1325	136063E	1327	101073F
1329	165303G	1331	116675E	1333	140221A	1335	100201E	1337	103223B
1339	105415E	1341	122445E	1347	143631E	1349	137441E	1351	104421A
1353	154023H	1355	127225E	1357	176427H	1359	151265C	1361	150215E
1363	144225G	1365	115205A	1367	123307E	1369	133437E	1371	166653E
1373	101515E	1379	126023B	1381	166553H	1383	172701E	1385	140271G
1387	121143E	1389	111577E	1391	132747E	1393	143057C	1395	111137B
1397	127401E	1399	150317E	1401	177731G	1415	155335G	1417	123057F
1419	117715E	1421	162657B	1423	171745G	1425	130527F	1427	144467G
1429	115045E	1431	177115G	1433	155751G	1435	103767A	1437	115127E
1443	176741E	1445	141475G	1447	112553E	1449	154307D	1451	105621E
1453	170051G	1455	147707F	1457	160445A	1459	161031E	1461	131405E
1463	164121A	1465	111003F	1467	167331E	1469	165311G	1475	157405G
1477	140557A	1479	156655G	1481	164561G	1483	114231E	1485	106407F
1487	111033F	1489	172123G	1491	146667D	1493	143523G	1495	170765G
1497	105725E	1499	132155E	1501	150261G	1507	122517E	1509	107567E
1511	166267E	1561	153461C	1563	166011G	1565	133445E	1571	156365G
1573	176111G	1575	137331A	1577	165407G	1579	106445E	1581	145551C
1583	124341E	1585	127215E	1587	135005E	1589	117731A	1591	110141E
1593	152345G	1595	164441G	1605	172621G	1607	143567G	1609	153443H
1611	146203E	1613	120417F	1615	103553F	1617	110567A	1619	126067F
1621	140747F	1623	107037F	1625	135503E	1627	126735E	1629	172445G
1635	117131E	1637	105173F	1639	105071E	1641	174167G	1643	114745A
1645	133407A	1647	136215E	1649	153113H	1651	141321E	1653	132523F
1655	136335E	1657	167255E	1671	146301G	1673	131265A	1675	120133F
1677	157557E	1679	107711E	1681	174751E	1683	133257F	1685	151217G
1687	144653C	1689	176203H	1691	155213H	1693	135207F	1699	131367F
1701	146543C	1703	130033F	1705	166311A	1707	150213G	1709	143227F
1711	176013G	1713	147751G	1715	131543B	1717	131111E	1719	111267F
1721	144151G	1723	110433F	1733	171173F	1735	116367F	1737	115421E
1739	112223F	1741	111635E	1743	157165C	1745	135223F	1747	106143F
1749	176015G	1751	142461G	1753	154233E	1755	114677F	1757	103363A
1763	150327F	1765	126325E	1767	126105A	1769	111713F	1771	172303B
1773	170763G	1775	124175E	1777	176357F	1807	164667E	1809	136611E
1811	163123E	1813	151037D	1815	121431E	1817	110165E	1819	172005G
1821	104265E	1827	154763A	1829	152703D	1831	163555G	1833	135021E
1835	124071E	1837	164247H	1839	166113H	1841	101625A	1843	145427H
1845	106633F	1847	155437E	1849	174633H	1851	161657H	1861	174605G

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 15--CONTINUED

1863	136701E	1865	144425E	1867	126747F	1869	157441C	1871	167015E
1873	142737H	1875	152301E	1877	131727E	1879	120221E	1881	102147E
1883	106457B	1885	152253H	1891	157645A	1893	141541G	1895	170325E
1897	141677C	1899	102733E	1901	135443F	1903	124251E	1905	150731G
1907	127137F	1909	100347F	1911	130415A	2185	147161G	2187	154247F
2189	161205G	2195	101313E	2197	175203F	2199	154507G	2201	121055A
2203	113061E	2205	170211C	2211	102763E	2213	167367H	2215	106503F
2217	133641E	2219	160175C	2221	161061E	2227	103035E	2229	173037F
2231	130737F	2233	166137C	2235	130017F	2245	122213F	2247	144577D
2249	117027F	2251	106273F	2253	107217F	2259	146373F	2261	153445C
2263	145727D	2265	121451A	2267	146607F	2269	113543F	2275	161013A
2277	177131G	2279	112633E	2281	137545E	2283	140227F	2285	112377F
2323	123163F	2325	100725A	2327	162315G	2329	155027G	2331	173551C
2333	132357F	2339	141231E	2341	117457F	2343	143403H	2345	124005A
2347	137601E	2349	143271G	2355	143727F	2357	107447F	2359	136401A
2361	157711G	2363	170337E	2373	166257D	2375	131733E	2377	176453H
2379	116057F	2381	156773H	2387	114371A	2389	155505G	2391	100641F
2393	151573E	2395	106713F	2397	177751G	2403	175601G	2405	177563G
2407	155175G	2409	170367G	2411	132015E	2413	126375E	2419	170433F
2421	151747G	2443	173153B	2445	111505E	2451	127243F	2453	107323F
2455	106745E	2457	165327B	2459	153577H	2461	150341G	2467	155737H
2469	150005G	2471	146007A	2473	146155E	2475	117655E	2477	101023E
2483	126227F	2485	173163B	2487	103175E	2489	105143F	2491	174743G
2501	101433F	2503	155757H	2505	121017F	2507	100425E	2509	126657E
2515	172363H	2517	120463E	2519	154561G	2601	126771E	2603	156161E
2605	147725G	2611	177527D	2613	121641E	2615	111365E	2617	125057E
2631	142611G	2633	110435E	2635	104575A	2637	164313G	2643	126163E
2645	112347F	2647	126155E	2649	131667F	2651	141365G	2653	116307B
2659	143531E	2661	141445E	2663	104141E	2665	167001G	2667	110343A
2669	111047F	2675	107121E	2677	106125E	2699	167203G	2701	175337F
2707	165201G	2709	106767B	2711	152351G	2713	144731G	2715	161043G
2717	113171E	2723	133533A	2725	175405G	2727	177231G	2729	127653E
2731	165535G	2733	114701E	2739	146177H	2741	121327E	2743	132277F
2745	153175G	2759	155407A	2761	145433H	2763	167463H	2765	104263A
2771	127437F	2773	176255E	2775	134435E	2777	124335E	2779	143373D
2781	170501G	2787	126711E	2789	103257E	2791	120601E	2793	155773B
2839	134255E	2841	103737F	2843	164001G	2845	161147F	2851	135565E
2853	110573E	2855	175711E	2857	116631E	2859	131623E	2861	155725G
2867	154537F	2869	114347B	2871	140755G	2873	113515E	2887	120155E
2889	160137E	2891	163647B	2893	121725E	2899	157255G	2901	141401G
2903	141125G	2905	107337A	2907	117125E	2909	144603H	2915	147635E
2917	154331G	2919	115607A	2921	154411E	2923	154155E	2925	122275E
2931	136457F	2957	126433F	2963	154515E	2965	150371G	2967	173331E
2969	146753E	2971	132741E	2973	145477H	3171	000073	3173	124115E
3175	127365E	3177	107645E	3179	117443F	3181	163335E	3187	115675E
3213	131651A	3219	170523H	3221	167313H	3223	137127F	3225	140205E
3227	102357B	3237	163365G	3239	172027H	3241	131165A	3243	162241E
3245	142223G	3251	164155G	3253	176753H	3255	152433B	3257	125271E
3271	177377G	3273	100647E	3275	121101E	3277	142751E	3283	115721A
3285	144437G	3287	177443H	3289	101613F	3291	142633H	3301	156527H
3355	165725E	3365	110405E	3367	107675A	3369	115133E	3371	101551E
3373	133213E	3379	155621C	3381	114363A	3383	161253F	3385	160413F
3399	127077E	3401	136213E	3403	171115E	3405	121553E	3411	140007G
3413	116601E	3415	147437H	3417	100223E	3419	126643E	3429	133231E
3431	162037H	3433	141027E	3435	125255E	3437	166275A	3475	171621G
3477	107373E	3479	125337A	3481	110255E	3483	114611E	3493	114055A
3495	110501E	3497	104111E	3499	146375G	3501	126557F	3507	125361A
3509	121617F	3511	103333F	3513	103053E	3527	171371E	4681	000013
4683	133261A	4685	123735E	4691	142175G	4693	131645E	4699	167637G
4709	155303H	4715	160215G	4717	163275G	4755	124053F	4757	133201E
4763	141115G	4773	161105E	4779	100021E	4781	116567B	4787	145675G
4789	123471E	4811	137613F	4813	105701E	4819	121305E	4821	146705E
4907	124621A	4909	122443E	4915	123537E	4917	124317F	4939	106677E
4941	160723H	4947	131601E	4949	113405A	4955	155517G	5285	000045
5291	155707H	5293	134277F	5299	140513C	5301	111041A	5323	127273F

Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.

DEGREE 15--CONTINUED

5325	117243F	5331	141707H	5333	134205E	5419	107417F	5421	122401E
5427	170037E	5429	107127E	5451	161465E	5453	171027C	5459	174707H
5461	145453E								

DEGREE	16	1	210013F	3	215435A	5	227215A	7	234313F
9	225657B	11	233303F	13	307107H	15	311513D	17	336523D
19	307527H	21	363501C	23	306357H	25	353573D	27	357333D
29	201735E	31	272201E	33	310327D	35	304341C	37	242413F
39	327721C	41	270155E	43	302157H	45	374111C	47	210205E
49	305667H	51	237403B	53	236107F	55	212113B	57	314061C
59	271055E	61	313371G	63	333575C	65	267313B	67	311405G
69	323527D	71	346355G	73	350513H	75	237421A	77	203213F
79	233503F	81	261105A	83	306221G	85	267075A	87	235063B
89	244461E	91	204015E	93	327421C	95	226455A	97	202301E
99	351641C	101	376311G	103	201637F	105	365705C	107	352125G
109	273435E	111	202545A	113	243575E	115	251645A	117	277535A
119	327277D	121	250723F	123	340047D	125	274761A	127	226135E
129	357047D	131	214443F	133	277213F	135	315633D	137	300205G
139	367737H	141	230535A	143	342567H	145	265157B	147	371771C
149	217137F	151	262367F	153	301663D	155	370565C	157	201045E
159	304731C	161	303657H	163	212653F	165	245351A	167	347433H
169	260237F	171	311651C	173	256005E	175	206353B	177	362053D
179	352603H	181	310017H	183	333013D	185	256415A	187	376175C
189	243513B	191	312301G	193	260475E	195	347211C	197	215345E
199	201551E	201	362555C	203	333643H	205	304261C	207	230541A
209	250311E	211	333117H	213	274317B	215	301425C	217	247353F
219	254601A	221	212063B	223	207661E	225	317171C	227	214215E
229	322661G	231	274635A	233	326035G	235	200215A	237	324127D
239	230653F	241	342105G	243	305471C	245	242437B	247	363637H
249	330561C	251	211473F	253	266663F	255	361617D	257	000717
259	255517F	261	344733D	263	311155G	265	340207D	267	273211A
269	366421G	271	221257F	273	207753B	275	226315A	277	250017F
279	243111A	281	242225E	283	204703F	285	323563D	287	230451E
289	323341C	291	271725A	293	353263H	295	306575C	297	271251A
299	335227H	301	213375E	303	340333D	305	232013B	307	312405G
309	233017B	311	266701E	313	262351E	315	324141C	317	365221G
319	213651E	321	200365A	323	215613B	325	207221A	327	323077D
329	274627F	331	302335G	333	251211A	335	262421A	337	360667H
339	223133B	341	356255G	343	337553H	345	215015A	347	221213F
349	276531E	351	325413D	353	362737H	355	240171A	357	241173B
359	274353F	361	222563F	363	231753B	365	227065A	367	217451E
369	254471A	371	356221G	373	235275E	375	372075C	377	357527H
379	241341E	381	335263D	383	311515G	385	202155A	387	254241A
389	370137H	391	300405C	393	227157B	395	237733B	397	207717F
399	303375C	401	257051E	403	245367F	405	324631C	407	274621E
409	211101E	411	324755C	413	326261G	415	236555A	417	341343D
419	220625E	421	332745G	423	374163D	425	264255A	427	234015E
429	206635A	431	320731G	433	243631E	435	325757D	437	241677F
439	217473F	441	366373D	443	230355E	445	301653D	447	264433B
449	302321G	451	333323H	453	344045C	455	317163D	457	265401E
459	325033D	461	341667H	463	276645E	465	346725C	467	301535G
469	342325G	471	202265A	473	247617F	475	325475C	477	343213D
479	237351E	481	341741G	483	361353D	485	260665A	487	276727F
489	273141A	491	233743F	493	252023B	495	272423B	497	265617F
499	273015E	501	267421A	503	351353H	505	377171C	507	317357D
517	202703F	519	241245A	521	356057H	523	217633F	525	277215A
527	257643B	529	267507F	531	311661C	533	235145E	535	202411A
537	205003B	539	366155G	541	212115E	543	375437D	545	354377D
547	236511E	549	277745A	551	241251E	553	211571E	555	245733B
557	362633H	559	201031E	561	371643D	563	340311G	565	200751A
567	232211A	569	341345G	571	374721G	573	310745C	575	227063B
577	271161E	579	322367D	581	375213H	583	330073H	585	273007B
587	341147H	589	371427H	591	200451A	593	251741E	595	345267D
597	205143B	599	212355E	601	252623F	603	331627D	605	241175A
607	355507H	609	261177B	611	317203H	613	361541G	615	363211C