

E303: Communication Systems

Professor A. Manikas Chair of Communications and Array Processing

Imperial College London

An Overview of Fundamentals: PN-codes/signals & Spread Spectrum

ロト 4 를 ト 4 를 ト · 트 · · 의 Q @

Prof. A. Manikas (Imperial College)

EE303: PN-codes & Spread Spectrum

v.16

1 / 47

Table of Contents

Introduction

- 3GPP
- Definition of a SSS
- Classification of SSS
- Modelling of b(t) in SSS
- Applications of Spread Spectrum Techniques
- Definition of a Jammer
- Definition of a MAI
- Processing Gain (PG)
- Equivalent EUE
- Principles of PN-sequences
 - Comments on PN-sequences Main Properties
 - An Important "Trade-off"
- 3 m-sequences
 - Shift Registers and Primitive Polynomials
 - Implementation of an 'm-sequence'
 - Auto-Correlation Properties
 - Some Important Properties of m-sequences
 - Cross-Correlation Properties and Preferred m-sequences
 - A Note on m-sequences for CDMA
- Gold Sequences
 - Introductory Comments
 - Auto-Correlation Properties
 - Cross-Correlation Properties
 - Balanced Gold Sequences
- Appendices
 - Appendix A: Properties of a Purely Random Sequence
 - Appendix B: Auto and Cross Correlation functions of two PN-sequences
 - Appendix C: The concept of a 'Primitive Polynomial' in GF(2)
 - Appendix D: Finite Field Basic Theory
 - Appendix E: Table of Irreducible Polynomials over GF(2)

Appendices

Appendix A: Properties of a purely random sequence

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

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

with

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

$$Var\{\alpha[n]\} = 1 \qquad (= 1^2 \times 0.5 + (-1)^2 \times 0.5 = 1)$$
(39)

$$Var\{\alpha[n]\} = 1 \quad (=1^2 \times 0.5 + (-1)^2 \times 0.5 = 1)$$
(30)

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

$$R_{\alpha\alpha}^{M}[k] \equiv \sum_{n=1}^{M} \alpha[n]\alpha[n+k] = \begin{cases} \sum_{n=1}^{M} \alpha[n]^{2} = \sum_{n=1}^{M} 1 = M & k = 0\\ \text{random} & k \neq 0 \end{cases}$$
(31)

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

$$\mathcal{E}\left\{R_{\alpha\alpha}^{M}[k]\right\} = \sum_{n=1}^{M} \mathcal{E}\{\alpha[n]\alpha[n+k]\} = \begin{cases} \sum_{n=1}^{M} \mathcal{E}\{\alpha[n]^{2}\} = \sum_{n=1}^{M} 1 = M & \text{if } k = 0\\ \sum_{n=1}^{M} \mathcal{E}\{\alpha[n]\}\mathcal{E}\{\alpha[n+k]\} = 0 & \text{if } k \neq 0 \end{cases}$$
(32)

– 47 – Dr A. Manikas Spread Spectrum

$$Var\{R_{\alpha\alpha}^{M}[k]\} = \mathcal{E}\{R_{\alpha\alpha}^{M}[k]^{2}\} - \mathcal{E}\{R_{\alpha\alpha}^{M}[k]\}^{2} =$$

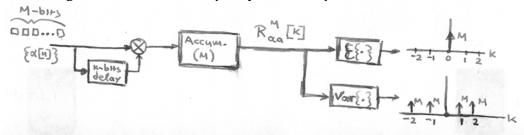
$$= \sum_{n=1}^{M} \sum_{m=1}^{M} \mathcal{E}\{\alpha[n]\alpha[n+k]\alpha[m]\alpha[m+k]\} - \mathcal{E}\{R_{\alpha\alpha}^{M}[k]\}^{2} =$$

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

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

$$R_{\alpha_1 \alpha_2}^M[k] = \sum_{n=1}^M \alpha_1[n] \alpha_2[n+k]$$
 (34)

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 $\{\alpha_i[n]\}$

• Consider the ∞ -sequences of ± 1 s 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

$$\diamond$$
 periodic cross-correlation: $R_{\alpha_i \alpha_j}[k] \equiv \sum_{n=1}^{N} \alpha_i[n] \alpha_j[n+k]$ (36)

$$\diamond \text{ odd cross-correlation function: } \widetilde{R}_{\alpha_i \alpha_j}[k] = C_{\alpha_i \alpha_j}[k] - C_{\alpha_i \alpha_j}[k-N] \tag{37}$$

Spread Spectrum - 49 - Dr A. Manikas

Compact Lecture Notes

- Note that:
 - ♦ it is easy to see that

$$R_{\alpha_i \alpha_j}[k] = C_{\alpha_i \alpha_j}[k] + C_{\alpha_i \alpha_j}[k - N]$$
(38)

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

$$R_{\alpha_i \alpha_i}[k] = R_{\alpha_i \alpha_i}[N - k] \tag{39}$$

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

$$\tilde{R}_{\alpha_i \alpha_i}[k] = -\tilde{R}_{\alpha_i \alpha_i}[N-k] \tag{40}$$

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

• For best CDMA system performance, all $C_{\alpha_i\alpha_j}[k]$, $R_{\alpha_i\alpha_j}[k]$, $R_{\alpha_i\alpha_j}[k]$ 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

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

$$(41)$$

Similarly we define the peak autocorrelation parameters

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

$$(42)$$

Spread Spectrum -51 - Dr A. Manikas

Compact Lecture Notes

• Finally we define

$$\begin{cases} R_{\text{peak}} = \max\{R_{\text{auto}}, R_{\text{cross}}\} \\ \widetilde{R}_{\text{peak}} = \max\{\widetilde{R}_{\text{auto}}, \widetilde{R}_{\text{cross}}\} \end{cases}$$

$$C_{\text{peak}} = \max\{C_{\text{auto}}, C_{\text{cross}}\}$$
(43)

• With the above definitions we can see that the smaller the peak correlation parameters $R_{\rm peak}$, $\widetilde{R}_{\rm peak}$ and $C_{\rm peak}$, 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,

$$R_{\text{peak}} \ge N \sqrt{\frac{K-1}{NK-1}} \qquad C_{\text{peak}} \ge N \sqrt{\frac{K-1}{2NK-K-1}}$$
 (44)

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

$$R_{\mathrm{peak}} \ge \sqrt{N}$$
 $C_{\mathrm{peak}} \ge \sqrt{\frac{N}{2}}$ (45)

Moreover, it can show that

$$R_{\text{auto}}^2 + R_{\text{cross}}^2 > N \qquad \qquad C_{\text{auto}}^2 + C_{\text{cross}}^2 > \frac{N}{2} \tag{46}$$

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): $f(D) = f_n D^n + f_{n-1}D^{n-1} + \dots + f_1D + f_0$ $\downarrow f(D) = f_n D^n + f_{n-1}D^{n-1} + \dots + f_1D + f_0$

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

$$\bullet \text{ if } f(D), g(D) \in \mathrm{GF}(2) \quad \text{then} \quad \left\{ \begin{array}{ll} f(D) + g(D) & \in \mathrm{GF}(2) \\ f(D) \cdot g(D) & \in \mathrm{GF}(2) \end{array} \right.$$

divisible polynomial:

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

irreducible polynomial:

A polynomial $f(D) \in GF(2)$ 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))

Spread Spectrum -53 - Dr A. Manikas

Compact Lecture Notes

Dr A. Manikas

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

primitive polynomial:

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

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 3.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 5 \ \pm 5 \ = 5 \ \pm 5 \$
- 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 <u>multiplicative identity</u> element which will always be denoted by 1.

$$s_{i}.1 = s_{i}$$

6. The set S must contain a <u>multiplicative inverse</u> element s_i^{-1} for every element s_i (excluding the additive identity 0)

$$s_i.s_i^{-1} = 1$$

- 7. Multiplication must be <u>distributive</u> over addition. $\rightarrow s_{\ell} + (s_{\ell} + s_{k}) = (s_{\ell} + s_{k}) + s_{k}$
- 8. Both addition and multiplication must be Associative. $\rightarrow (s_1 + s_1) \cdot s_k = s_L s_k + s_l s_k$

Spread Spectrum - 55 - Dr A. Manikas

Compact Lecture Notes

•EXAMPLE

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

modulo-3 +	0	1	2	modulo-3 ×	0	1	2
0	0	1	2	0	0	0	0
1	1	2	0	1	0	1	2
2	2	0	1	2	0	2	1

is a field of 3 elements

e.g.

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

$$-1=2$$

$$-2=1$$

• 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 ×	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 $S = \{0, 1, 2, \dots, M-1\}$, 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 prime fields.

• 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, $1 \div 2 = 1 \cdot (2^{-1}) = 1.2 = 2$.

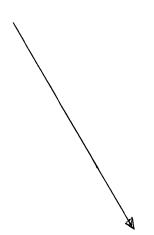
- ullet Note that nonprime fields do not necessarily employ modulo-M arithmetic.
- Fields can be constructed having any prime number of elements p or p^m . A field having p^m elements is called an extension field of the field having p elements.
- Finite fields are often referred to as Galois fields, 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 $GF(2^m)$

Spread Spectrum - 57 - Dr A. Manikas

Compact Lecture Notes

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

(from "Error-Correcting Codes" by Peterson & Weldom 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:

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 0.1110101010101, 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.

472

Spread Spectrum

– 59 –

APPENDIX C 473

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
- 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

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 $p_{13}(X) = X^6 + X^4 + X^3 + X + 1$:

Compact Lecture Notes

Dr A. Manikas

474 APPENDIX C

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

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

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

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

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.

$2^{3} - 1 = 7$ $2^{4} - 1 = 3 \times 5$ $2^{5} - 1 = 31$ $2^{6} - 1 = 3 \times 3 \times 7$ $2^{7} - 1 = 127$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
$2^{8} - 1 = 3 \times 5 \times 17$ $2^{9} - 1 = 7 \times 73$ $2^{10} - 1 = 3 \times 11 \times 31$ $2^{11} - 1 = 23 \times 89$ $2^{12} - 1 = 3 \times 3 \times 5 \times 7 \times 13$	$2^{24} - 1 = 3 \times 3 \times 5 \times 7 \times 13 \times 17 \times 241$ $2^{25} - 1 = 31 \times 601 \times 1801$ $2^{26} - 1 = 3 \times 2731 \times 8191$ $2^{27} - 1 = 7 \times 73 \times 262657$ $2^{28} - 1 = 3 \times 5 \times 29 \times 43 \times 113 \times 127$
$\begin{array}{lll} 2^{13} & -1 & = 8191 \\ 2^{14} & -1 & = 3 \times 43 \times 127 \\ & & \\ 2^{15} & -1 & = 7 \times 31 \times 151 \\ & & \\ 2^{16} & -1 & = 3 \times 5 \times 17 \times 257 \\ & & \\ 2^{17} & -1 & = 131071 \\ & & \\ 2^{18} & -1 & = 3 \times 3 \times 3 \times 7 \times 19 \times 73 \end{array}$	

APPENDIX C 475

- 1. The residues of 1, X, X^2 , X^4 , ..., $X^{2^{m-1}}$ are formed modulo f(X).
- These are multiplied and reduced modulo f(X) to form the residue of X^{2m}-1. If the result is not 1, the polynomial is rejected. If the result is 1, the test is continued.
- For each factor r of 2^m 1, the residue of X' 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.

476 APPEND	IX C					APPENDIX C 417	
Table C.2. Irred	lucible Polyno	mials of Degre	ee ≤34 over G	F(2).		Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.	
DEGREE 2	1 7H					DEGREE 12CONTINUED 167 16115G 169 16547C 171 10213B 173 12247E 175 16757D 177 16017	c
DEGREE 3	1 13F					179 17675E 181 10151E 183 14111A 185 14037A 187 14613H 189 13535. 195 00165 197 11441E 199 10321E 201 14067D 203 13157B 205 14513	D
DEGREE 4	1 23F	3 370	5 07			207 10603A 209 11067F 211 14439F 213 164570 215 10653B 217 13563I 219 11657B 221 17513C 227 12753F 229 13431E 231 10167B 233 11313 235 11411A 237 13737B 239 13425E 273 00023 275 14601C 277 16021	F
DEGREE 5	1 45E	3 75G	5 67H			279 16137D 281 170256 283 15723F 285 17141A 291 15775A 293 11477 295 11463B 297 17073C 299 16401C 301 12315A 307 14221E 309 11763	F
DEGREE 6 11 155E	1 103F 21 007	3 1278	5 147H	7 111A	9 015	311 12705E 313 14357F 315 17777D 325 00163 327 17233D 329 11637 331 16407F 333 11703A 339 16003C 341 11561E 343 12673B 345 14537 347 17711G 349 13701E 355 10467B 357 15347C 359 11075E 361 16363	D
DEGREE 7 11 325G	1 211E 13 203F	3 217E 19 313H	5 235E 21 345G	7 367H	9 277E	363 11045A 365 11265A 371 14043D 397 12727F 403 14373D 405 13003 407 17057G 409 10437F 411 10077B 421 14271G 423 14313D 425 14155	8 C
DEGREE 8 11 747H	1 435E 13 453F	3 567B 15 7270	5 763D 17 023	7 551E 19 545E	9 675C 21 613D	427 10245A 429 11073B 435 10743B 437 12623F 439 12007F 441 15353I 455 00111 585 00013 587 14545G 589 16311G 595 13413A 597 12265.	A
23 543F 51 037	25 433B 85 007	27 4778	37 537F	43 703H	45 471A	603 14411C 613 15413H 619 17147F 661 10605E 683 10737F 685 16355 691 15701G 693 12345A 715 00133 717 16571C 819 00037 1365 00007	
DEGREE 9	1 1021E 13 1167F	3 1131E 15 1541E	5 1461G 17 1333F	7 1231A 19 1605G	9 1423G 21 1027A	DEGREE 13 1 20033F 3 23261E 5 24623F 7 23517F 9 30741 11 21643F 13 30171G 15 21277F 17 27777F 19 35051G 21 34723	н
11 1055E 23 1751E	25 1743H	27 1617H	29 1553H 45 1175E	35 1401C 51 1725G	37 1157F 53 1225E	23 34047H 25 32535G 27 31425G 29 37505G 31 36515G 33 26077H 35 35673H 37 20635E 39 33763H 41 25745E 43 36575G 45 26653H	F
39 1715E 55 1275E	41 1563H 73 0013	43 1713H 75 1773G	77 1511C	83 1425G	85 1267E	47 21133F 49 22441E 51 30417H 53 32517H 55 37335G 57 25327I 59 23231E 61 25511E 63 26533F 65 33343H 67 33727H 69 2727II	Ε
DEGREE 10	1 2011E	3 20178	5 2415E	7 3771G	9 2257B	71 25017F 73 26041E 75 21103F 77 27263F 79 24513F 81 32311 83 31743H 85 24037F 87 30711G 89 32641G 91 24657F 93 32437I	н
11 2065A 23 2033F	13 2157F 25 2443F	15 2653B 27 3573D	17 3515G 29 2461E	19 2773F 31 3043D	21 3753D 33 0075C	95 20213F 97 25633F 99 31303H 101 22525E 103 34627H 105 25775 107 21607F 109 25363F 111 27217F 113 33741G 115 37611G 117 23077	E
35 3023H	37 3543F	39 2107B 51 2547B	41 2745E 53 2617F	43 2431E 55 3453D	45 3061C 57 3121C	119 21263F 121 31011G 123 27051E 125 35477H 131 34151G 133 27405	Ε
47 3177H 59 3471G	49 3525G 69 2701A	71 3323H	73 3507H	75 24378	77 2413B	135 346416 137 324456 139 363756 141 22675E 143 36073H 145 35121 147 365016 149 33057H 151 36403H 153 35567H 155 23167F 157 36217H	
83 3623H 99 0067	85 2707E 101 2055E	87 2311A 103 3575G	89 2327F 105 3607C	91 3265G 107 3171G	93 37770 109 2047F	159 22233F 161 32333H 163 24703F 165 33163H 167 32757H 169 23761F	E
147 2355A	149 3025G	155 2251A	165 0051	171 3315C	173 3337H	171 24031E 173 30025G 175 37145G 177 31327H 179 27221E 181 255771 183 22203F 185 37437H 187 27537F 189 31035G 195 24763F 197 202451	
179 32116	341 0007					199 20503F 201 20761E 203 25555E 205 30357H 207 33037H 209 34401	G
DEGREE 11	1 4005E	3 4445E	5 4215E	7 4055E	9 6015G	223 32347H 225 20677F 227 22307F 229 33441G 231 33643H 233 24165	
11 7413H 23 4757B	13 4143F 25 4577F	15 4563F 27 6233H	17 4053F 29 6673H	19 5023F 31 7237H	21 5623F 33 7335G	235 27427F 237 24601E 239 36721G 241 34363H 243 21673F 245 321671 247 21661E 265 33357H 267 26341E 269 31653H 271 37511G 273 23003I	
35 4505E	37 5337F	39 5263F	41 5361E	43 5171E	45 6637H	275 22657F 277 25035E 279 23267F 281 34005G 283 34555G 285 24205	
47 7173H 59 4533F	49 5711E 61 4341E	51 5221E 67 6711G	53 6307H 69 6777D	55 6211G 71 7715G	57 5747F 73 6343H	291 26611E 293 32671G 295 25245E 297 31407H 299 33471G 301 226131 303 35645G 305 32371G 307 34517H 309 26225E 311 35561G 313 256631	
75 6227H	77 6263H	79 5235E	81 7431G	83 6455G	85 5247F	315 24043F 317 30643H 323 20157F 325 37151G 327 24667F 329 33325	G
87 5265E 103 7107H	89 5343B 105 7041G	91 4767F 107 4251E	93 5607F 109 5675E	99 4603F 111 4173F	101 6561G 113 4707F	331 32467H 333 30667H 335 22631E 337 26617F 339 20275E 341 366259 343 20341E 345 37527H 347 31333H 349 31071G 355 23353F 357 262431	
115 7311C	117 5463F	119 5755E	137 6675G	139 7655G	141 5531E	359 21453F 361 36015G 363 36667H 365 34767H 367 34341G 369 34547I	н
147 7243H 163 7745G	149 7621G 165 7317H	151 7161G 167 5205E	153 4731E 169 4565E	155 4451E 171 6765G	157 6557H 173 7535G	371 354656 373 24421E 375 23563F 377 36037H 391 31267H 393 27133I 395 307056 397 304656 399 35315G 401 32231G 403 32207H 405 26101I	
179 4653F	181 5411E	183 5545E	185 7565G	199 6543H	201 5613F	407 22567F 409 21755E 411 22455E 413 33705G 419 37621G 421 21405E	Ε
203 6013H 219 7273H	205 7647H 29 3 7723H	211 6507H 299 4303B	213 6037H 301 5007F	215 7363H 307 7555G	217 7201G 309 4261E	423 30117H 425 23021E 427 21525E 429 36465G 431 33013H 433 27531E 435 24675E 437 33133H 439 34261G 441 33405G 443 34655G 453 32173E	
331 6447H	333 5141E	339 7461G	341 5253F			455 33455G 457 35165G 459 22705E 461 37123H 463 27111E 465 35455G	G
DEGREE 12	1 10123F	3 12133B	5 10115A	7 121538	9 11765A	467 31457H 469 23055E 471 30777H 473 37653H 475 24325E 477 312510 547 35163H 549 33433H 551 37243H 553 27515E 555 32137H 557 26743F	
11 15647E	13 125138	15 130778	17 16533H	19 16047H	21 10065A	563 30277H 565 20627F 567 35057H 569 24315E 571 24727F 581 303310	G
23 11015E 35 10377B	25 13377B 37 13565E	27 14405A 39 13321A	29 14127H 41 15341G	31 17673H 43 15053H	33 13311A 45 15173C	583 34273H 585 23207F 587 31113H 589 36023H 595 27373F 597 20737F 599 36235G 601 21575E 603 26215E 605 21211E 611 20311E 613 34003F	
47 15621E	49 17703C	51 10355A	53 15321G	55 10201A	57 12331A	615 34027H 617 20065E 619 22051E 621 22127F 627 23621E 629 24465E	Ε
59 11417E 71 11471E	61 13505E 73 16237E	63 10761A 75 16267D	65 00141 77 15115C	67 13275E 79 12515E	69 16663C 81 17545C	651 26457F 653 31201G 659 34035G 661 27227F 663 22561E 665 21615E 667 22013F 669 23365E 675 26213F 677 26775E 679 32635G 681 33631G	
83 12255E	85 11673B	87 17361A	89 11271E	91 10011A	93 14755C 105 13617A	683 32743H 685 31767H 691 34413H 693 22037F 695 30651G 697 26565E	
95 17705A 107 14135G	97 17121G 109 14711G	99 173230 111 15415C	101 14227H 113 13131E	103 12117E 115 13223A	117 16475C	711 22141E 713 22471E 715 35271G 717 37445G 723 22717F 725 26505E 727 24411E 729 24575E 731 23707F 733 25173F 739 21367F 741 25161E	
119 14315C	121 16521E 141 13571A	123 13475A 143 12111A	133 11433B 145 16535C	135 10571A 147 17657D	137 15437G 149 12147F	743 24147F 793 36307H 795 24417F 805 20237F 807 36771G 809 37327H	1
			157 14675G		165 10621A	811 27735E 813 31223H 819 36373H 821 33121G 823 32751G 825 33523H	

Spread Spectrum - *61* -Dr A. Manikas

Compact Lecture Notes

478 APPENDIX C

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

APPENDIX C

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

480 APPENDIX C

APPENDIX C

Table C	.2. Irreduc	ible Polynomials	of Degree ≤34	over $GF(2)$.		Table C.2. Irreducible Polynomials of Degree ≤ 34 over $GF(2)$.
	15CONT I	NUED				DEGREE 15CONTINUED 929 160461E 931 117137B 933 134323F 935 123361E 937 105237F
	166775E	221 1531430	223 172213F	225 105213E	227 156053H	
	156745G	231 1706238	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 1201778	289 117547F	291 126051E	1057 000057 1059 104427F 1061 113075E 1063 162133H 1065 120717F
293	111335E	295 177101G	297 1437036	299 106047E	301 1374278	1067 144713F 1069 121605E 1071 122225A 1073 134657E 1075 130125E
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	
	136237F	335 132103F	337 171035G	339 132651E	341 134105A	
343	100261A	345 170227H	347 101233F	349 100445E	351 144707G	1125 133011E 1127 162337A 1129 105261E 1131 101427E 1133 156563F 1135 103663E 1137 146043H 1139 151403H 1141 100157A 1143 163653E
	165355E	355 150243H	357 163353C	359 114041E	361 113025E	1135 1036035 1137 1400431 1137 1374371 1141 100170 1145 1050350
	104447F	365 143301G	367 165011G	369 137361E	371 117201A	1163 176657H 1165 166425G 1167 103617E 1169 160021A 1171 161277H
	141655G	375 160113G	377 106715E	379 140575E	381 112123E	1173 1655656 1175 152153F 1177 111243E 1179 1656556 1181 134165E
387	140733F	389 124243E	391 116073E	393 147321E	395 123721E	1173 103300 1173 12731 1177 1173 12740 1177 1173 127403F 1195 170007H
	150225G	399 134741A	401 157111G	403 134411A	405 172317G	1197 167765C 1199 103415E 1201 137703E 1203 111563F 1205 147305G
	153327E	409 140573H	411 113625E	413 101673B	415 170543F	1207 156257F 1209 175177B 1211 141317B 1213 177467H 1219 140421G
	176735E	419 115307F	421 141635E	423 157241G	425 153005E	1221 127071E 1223 142457F 1225 122021A 1227 146771E 1229 110211E
	167051A	429 177175G	431 146331G	433 166541G	435 102513F	1231 134567F 1233 156321G 1235 114335E 1237 111603E 1239 121275A
	123121E	439 162463G	441 134037B	443 174571E	445 123433F	1241 110103E 1243 127161E 1245 163273H 1251 144533F 1253 173135C
	150167H	449 175465E	451 113255E	453 137325A	455 123045A	1255 155445E 1257 140441E 1259 103761E 1261 173523F 1263 167307F
457	133571E	459 135215E	461 110221E	463 157435E	465 121437A	1265 127457F 1267 102205A 1269 112251E 1291 106311E 1293 141633F
	177707G	469 143501C	471 161667F	473 157427G	475 150671G	1295 135151A 1297 106641E 1299 102265E 1301 164453G 1303 163071G
	112407F	479 165563E	481 112053E	483 1353638	485 130617F	1305 111641E 1307 134403E 1309 102667A 1315 177055E 1317 115373F
	125613F	489 114713F	491 165113G	493 143733G	495 162155E	1319 150231G 1321 175651G 1323 160377B 1325 136063E 1327 101073F
	135017B	499 126753F	501 137765E	503 106577E	521 112113F	1329 165303G 1331 116675E 1333 140221A 1335 100201E 1337 103223B
223	105555E	525 153425C	527 115313A	529 105761E	531 132165E	1339 105415E 1341 122445E 1347 143631E 1349 137441E 1351 104421A
	176147H	535 114621E	537 135751E	539 152763C	541 124757F	1353 154023H 1355 127225E 1357 176427H 1359 151265C 1361 150215E
543	112245E 156065C	545 123221E	547 141757G	549 160547F	551 101331E	1363 144225G 1365 115205A 1367 123307E 1369 133437E 1371 166653E
	141151G	555 156725G 565 126015E	557 113373E 567 171335C	559 137643F 569 146717H	561 156237G	1373 101515E 1379 126023B 1381 166553H 1383 172701E 1385 140271G
	121355E	579 166021G	581 145361C	583 134325E	571 130305E 585 157155E	1387 121143E 1389 111577E 1391 132747E 1393 143057C 1395 111137B
	124647E	589 163761C	591 114457E	593 155243G	595 153137D	1397 127401E 1399 150317E 1401 177731G 1415 155335G 1417 123057F
507	137253F	599 151551G	601 113645E	603 150305G	605 163745G	1419 117715E 1421 162657B 1423 171745G 1425 130527F 1427 144467G
	165473F	609 1130578	611 160173H	613 177663F	615 161117H	1429 115045E 1431 177115G 1433 155751G 1435 103767A 1437 115127E
617	144115E	619 156635G	621 150633H	623 115061A	625 143253H	1443 176741E 1445 141475G 1447 112553E 1449 154307D 1451 105621E
	165451G	629 160305E	631 146025E	633 106751E	635 132625E	1453 170051G 1455 147707F 1457 160445A 1459 161031E 1461 131405E
	160553D	643 123561E	645 116637F	647 111423E	649 117107E	1463 164121A 1465 111003F 1467 167331E 1469 165311G 1475 157405G
651	466761C	653 153555G	655 132127F	657 112333E	659 135267F	1477 140557A 1479 156655G 1481 164561G 1483 114231E 1485 106407F 1487 111033F 1489 172123G 1491 146667D 1493 143523G 1495 170765G
661	146727H	663 132753F	665 143343A	667 131705E	669 141005E	
	113147F	673 125323F	675 123235E	677 103653F	679 173025C	1497 105725E 1499 132155E 1501 150261G 1507 122517E 1509 107567E 1511 166267E 1561 153461C 1563 166011G 1565 133445E 1571 156365G
681	120661E	683 154545G	685 133553F	687 132001E	689 153773G	1573 176111G 1575 137331A 1577 165407G 1579 106445E 1581 145551C
691	1752416	693 160237B	695 171131E	697 172415E	699 1451116	1583 124341E 1585 127215E 1587 135005E 1589 117731A 1591 110141E
	122603F	707 170507C	709 160757G	711 171207G	713 147553B	1593 152345G 1595 164441G 1605 172621G 1607 143567G 1609 153443H
	112365E	717 146111E	719 122003F	721 1212738	723 122005E	1611 146203E 1613 120417F 1615 103553F 1617 110567A 1619 126067F
	135401E	727 102441E	729 175515G	731 132507E	733 130223F	1621 140747F 1623 107037F 1625 135503E 1627 126735E 1629 172445G
	142713C	737 102615E	739 105713F	741 134241E	743 173643F	1635 117131E 1637 105173F 1639 105071E 1641 174167G 1643 114745A
	163617G	747 175043E	749 132051A	751 104217F	753 115523F	1645 133407A 1647 136215E 1649 153113H 1651 141321E 1653 132523F
755	120247B	757 164447H	759 173667F	761 137051E	775 104073B	1655 136335E 1657 167255E 1671 146301G 1673 131265A 1675 120133F
	177065C	779 117071E	781 115537E	783 135201E	785 146643F	1677 157557E 1679 107711E 1681 174751E 1683 133257F 1685 151217G
787	113465E	789 152263G	791 1776170	793 104755E	795 147415G	1687 144653C 1689 176203H 1691 155213H 1693 135207F 1699 131367F
	126001E	799 170307F	801 174425E	803 112475E	805 173263C	1701 146543C 1703 130033F 1705 166311A 1707 150213G 1709 143227F
	176643H	809 130303F 819 116075A	811 125471E 821 150677G	813 173711G	815 165547E	1711 176013G 1713 147751G 1715 131543B 1717 131111E 1719 111267F
	163723G 152447H	819 116075A 829 126205E	835 120557E	823 175227G 837 160335A	825 166407H 839 125543E	1721 144151G 1723 110433F 1733 171173F 1735 116367F 1737 115421E
	152447H	843 100713E	845 121251E	847 141123D	849 174517F	1739 112223F 1741 111635E 1743 157165C 1745 135223F 1747 106143F
	106251E	853 116277F	855 106611E	857 174563H	859 140023H	1749 176015G 1751 142461G 1753 154233E 1755 114677F 1757 103363A
	132037A	863 147767G	865 164531G	867 155065E	869 146263F	1763 150327F 1765 126325E 1767 126105A 1769 111713F 1771 172303B
	1604016	873 102057F	875 146133C	877 117021E	879 147003F	1773 170763G 1775 124175E 1777 176357F 1807 164667E 1809 136611E
	127723F	883 120471E	885 162455G	887 130627F	889 152135C	1811 163123E 1813 151037D 1815 121431E 1817 110165E 1819 172005G
	157057H	901 162153F	903 151755C	905 170277H	907 165633H	1821 104265E 1827 154763A 1829 152703D 1831 163555G 1833 135021E
	173105E	911 102507F	913 176037H	915 171627G	917 162171C	1835 124071E 1837 164247H 1839 166113H 1841 101625A 1843 145427H
	130745E	921 177517H	923 114327F	925 127167F	927 133113E	1845 106633F 1847 155437E 1849 174633H 1851 161657H 1861 174605G

Spread Spectrum - 63 - Dr A. Manikas

Compact Lecture Notes

482 APPENDIX C

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

	15CONT								
	136701E	1865 144425E		126747F		157441C		167015E	
1873	142737H	1875 152301E	1877	131727E		120221E	1881		
1883	106457B	1885 152253H	1891	157645A	1893	141541G	1895	170325E	
1897	141677C	1899 102733E	1901	135443F	1903	124251E	1905	1507316	
1907	127137F	1909 100347F	1911	130415A	2185	1471616	2187	154247F	
2189	1612056	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	1445770	
2249	117027F	2251 106273F	2253	107217F	2259	146373F	2261	153445C	
2263	1457270	2265 121451A	2267	146607F	2269	113543F		161013A	
2277	177131G	2279 112633E	2281	137545E	2283	140227F	2285	112377F	
2323	123163F	2325 100725A	2327	162315G	2329	155027G	2331		
2333	132357F	7339 141231E	2341	117457F	2343	143403H	2345		
2347	137601E	2349 143271G	2355	143727F	2357	107447F		136401A	
	1577116	2363 170337E	2373	166257D	2375	131733E	2377	176453H	
2379	116057F	2381 156773H	2387	114371A		155505G	2391		
2303	151573E	2395 106713F	2397	177751G	2403	175601G	2405	177563G	
2407	155175G	2409 170367G	2411	132015E		126375E	2419		
2421	1517476	2443 1731538	2445	111505E	2451	127243F		107323F	
	106745E	2457 165327B		153577H		150341G		155737H	
2469	150005G	2471 146007A	2473	146155E		117655E		101023E	
2483	126227F	2485 1731638	2487	103175E		105143F	2491		
2501	101433F	2503 155757H	2505	121017F		100425E		126657E	
2515	172363H	2517 120463E		154561G		126771E		156161E	
2605	1477256	2611 1775270		121641E		111365E		125057E	
2631	1426116	2633 110435E	2635	104575A		164313G		126163E	
2645	112347F	2647 126155E		131667F		141365G		116307B	
	143531E	2661 141445E	2663	104141E		167001G		110343A	
2669	111047F	2675 107121E	2677	106125E		167203G		175337F	
2707	1652016	2709 106767B	2711	152351G		144731G		161043G	
2717	113171E	2723 133533A	2725	175405G		177231G		127653E	
	165535G	2733 114701E	2739	146177H		121327E		132277F	
	1531756	2759 155407A	2761	145433H		167463H		104763A	
	127437F	2773 176255E	2775	134435E		124335E		1433730	
2781	1705016	2787 126711E		103257E		120601E		155773B	
2839	134255E	2841 103737F	2843	164001G		161147F		135565E	
	110573E	2855 175711E		116631E		131623E	2861	155725G	
	154537F	2869 114347B		140755G		113515E		120155E	
	160137E	2891 163647B		121725E		157255G	2901		
	1411256	2905 107337A		117125E		144603H	2915		
2917	154331G	2919 115607A	2921	154411E		154155E		122275E	
2931	136457F	2957 126433F		154515E		150371G		173331E	
	146753E	2971 132741E		145477H		000073		174115E	
	127365E	3177 107645E		117443F		163335E		115675E	
	131651A	3219 170523H		167313H		137127F		140205E	
3227	102357B	3237 163365G		172027H		131165A		162241E	

APPENDIX C 483

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

DEGREE	15CONT	INUED							
5325	117243F		141707H		134205E		107417F 171027C	5421 5459	122401E 174707H
5427	170037E 145453E	5429	107127E	5451	161465E	5453	1710270	7479	1/4/0/8
5461	1454535								
DEGREE	16	1	210013F	3	215435A	5	227215A	7	234313F
9	2256578	11	233303F	13	307107H	15	3115130	17	336523D
19	307527H	21	363501C	23	306357H	25	3535730	27	3573330
29	201735E	31	272201E	33	310327D	35	304341C	37	242413F
39	327721C	41	270155E	43	302157H	45 55	374111C 212113B	47 57	210205E 314061C
49	305667H	51	2374038	53 63	236107F 333575C	65	2673138	67	311405G
59 69	271055E 323527D	61 71	313371G 346355G	73	350513H	75	237421A	77	
79	233503F	81	261105A	83	3062216	85	267075A	87	235063B
89	244461E	91	204015E	93	327421C	95	226455A	91	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 371771C
139	367737H	141	230535A	143 153	342567H 301663D	145 155	265157B 370565C	157	201045E
149 159	217137F 304731C	151 161	262367F 303657H	163	212653F	165	245351A	167	347433H
169	260237F	171	311651C	173	256005E	175	206353B	177	362053D
179	352603H	181	310017H	183	3330130	185	256415A	187	376175C
189	2435138	191	312301G	193	260475E	195	347211C	197	
199	201551E	201	362555C	203	333643H	205	304261C	207	230541A
209	250311E	211	333117H	213	274317B	215	301425C	217	247353F
219	254601A	221	2120638	223	207661E	225	3171710	227	214215E
229	322661G	231	274635A	233	326035G	235 245	200215A 242437B	237 247	324127D 363637H
239	230653F		342105G	243 253	305471C 266663F	255	3616170	257	000717
249 259	330561C 255517F	261	211473F 344733D	263	311155G	265	3402070	267	273211A
269	366421G		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	2320138	307	312405G
	233017B	311	266701E	313	262351E	315	3241410	317	365221G
319		321	200365A 302335G	323 333	215613B 251211A	325 335	207221A 262421A	327 337	360667H
329 339	274627F 223133B	331 341		343	337553H	345	215015A	347	221213F
349	276531E	351		353	362737H	355	240171A	357	241173B
359	274353F	361		363	231753B		227065A	367	217451E
369		371		373	235275E	375	372075C	377	357527H
379		381		383	311515G	385	202155A	387	
389		391		393	227157B	395	2377338	397	207717F
399		401		403		405	3246310		274621E
409		411		413 423	326261G 374163D	415 425	236555A 264255A	417 427	341343D 234015E
	220625E	421 431		423	243631E	435	325757D	437	
439	206635A 217473F	441		443	230355E	445	301653D	447	
449		451		453	344045C	455		457	
459		461		463	276645E	465	346725C	467	301535G
469		471	202265A	473	247617F	475	325475C	477	
479	237351E	481	341741G	483	3613530	485		487	
489		491		493	2520238	495	272423B	497	
499		501		503	351353H 356057H	505 523	377171C 217633F	507 525	317357D 277215A
517		519		521		533		535	
527	257643B 205003B	529 539		531 541	311661C 212115E	543		545	3543770
	236511E	549		551	241251E	553			2457338
557		559		561	3716430		340311G		200751A
567		569		571	374721G	573	310745C		227063B
577		579	322367D	581	375213H	583		585	
587		589		591	200451A	593		595	3452670
597		599		601	252623F	603		605	241175A 363211C
607	355507H	609	261177B	611	317203H	613	361541G	615	3032110

APPENDIX C

APPENDIX C 485

Table C.2.	Irreducible Polynomials of Degree \leq 34 over $GF(2)$.	
------------	--	--

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

DEGREE	16CON1	INUED						
617	366345G	619 33752	1G 621	362745C	623	366171G	625	204227B
627	222473B	629 23372	5A 631	346101G	633	2612538	635	
637	262073F	643 20660	3F 645	317531C	647	215343F	649	
651	221245A	653 32474	7H 655	301065C	657	223561A	659	232643F
661	3632716	663 25372			667	3370716	669	273361A
671	224611E	673 26761			677	316431G	679	237337F
681	214143B	683 27207			687	230371A	689	240675E
691	306643H	693 36653			697	3251730	699	
701	244333F	703 31173			707	234777F	709	
711 721	202141A 323175G	713 25646			717	341061C	719	375761G
731	231253B	723 23604 733 33023			727	222017F	729	352077D
741	316757D	743 30211			737	324073H	739	306015G
751	344623H	753 21112			747 757	226255A 302063H	749 759	3512256
761	303361G	763 31375			771	000573	773	375223D 326137H
775	256553B	777 22346			781	234667F	783	225405A
785	2017178	787 23025			791	367333H	793	346243H
795	272445A	797 32572			801	310267D	803	330177H
805	302635C	807 37230			811	264507F	813	341043D
815	275357B	817 30110			821	350403H	823	367033H
825	301347D	827 20160			831	212737B	833	232315A
835	201367B	837 22200	38 839	223121E	841	200475E	843	221151A
845	316261C	847 24526		2264478	851	234155E	853	305235G
855	2222678	857 33510			861	362577D	863	274671E
865	356471C	867 22325			871	321453H	873	341645C
875	3502770	877 24031			881	343503H	883	366673H
885	337063D	887 22573			891	3435470	893	231265E
899	315737H	901 30073			905	271347B	907	356741G
909	260775A	911 20434			915	332655C	917	276241E
919 929	244251E	921 31116			925	3052630	927	337547D
939	234545E 356233D	931 26114			935	335205C	937	303463H
949	256653F	941 25624 951 31067		373053H	945	204025A	947	346467H
959	332663H	961 36723		274757F 233035A	955 965	247275A 355155C	957 967	277047B
969	213625A	971 32022		323547H	975	276031A	977	352653H 213253F
979	226073F	981 20115			985	352123D	987	367065C
989	3014516	991 26223		373553D	995	270253B	997	263737F
999	214267B	1001 21723			1005	3655010	1007	205535E
1041	343055C	1043 34465		211245A	1047	306573D	1049	264001E
1051	343655G	1053 20151		370743D	1057	313415G	1059	307713D
1061	320445G	1063 22242		243043B	1067	214371E	1069	370321G
1071	265231A	1073 36540		305301C	1077	364355C	1079	312615G
1081	300155G	1083 33317	70 1085	341703D	1091	370275G	1093	267205E
1095	325731C	1097 37644	3H 1099	332033H	1101	266167B	1103	326461G
1105	244547B	1107 21264	78 1109	322171G	1111	206257F	1113	277641A
1115	310517D	1117 31224	7H 1119	365307D	1121	310437H	1123	344513H
1125	302167D	1127 33724		247743F	1131	275141A	1133	216607F
1135	3175670	1137 25535		353153D	1141	222633F	1143	254543B
1145	2113778	1147 24313		3771470	1155	253207B	1157	337311G
1159	272175E	1161 22254		226367F	1165	324433D	1167	360623D
1169	315713H	1171 33750		326065C	1175	2073078	1177	232045E
	337517D	1181 35373		372435G	1185	333515C	1187	213523F
1189	200535E	1191 26126		273073F	1195	264463B	1197	347463D
1199 1209	364201G	1201 24041		274167B	1205	3627150	1207	2536038
	262615A 301407H	1211 36014		315571G 215615A	1219	303045G	1221	362161C
	2143178	1235 37054		313437H	1239	316505G 275651A	1231	373237H
	214663F	1245 31340		216313F	1249	271655E	1241	361701C
	376415G	1255 213325		355771C	1259	306235G	1251	265663B 214157F
	256401A	1265 27262		216777F	1269	3136270	1271	214157F
	361521G	1275 333731		000433	1287	264637B	1289	326317H
1291	276441E	1293 27325		341037D	1297	326715G	1299	216007B
	217041E	1303 22223		2241078	1307	202277F	1309	256063B
	240323B	1313 260655		266671A	1317	273765A	1319	377755G
1321	264037F	1323 37061		300643D	1327	335675G		350057D

Spread Spectrum

- 65 -

Dr A. Manikas

Compact Lecture Notes

490 APPENDIX C

Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2). 1 1000201F 9 1200205A 17 1115701E 63 1313133B 57 1160435A 171 1626367D 309 15142455 657 1253607A 1071 1334325A 4599 1341035A 13797 1777777D 3 1010301A 11 1703601G 19 10231A1A 63 1313131A 57 1160435A 171 162365D 1197 1052465A 73 1642365C 219 1252555A 511 1231145A 1533 1055321A

DEGREE 19 7 2570103F 15 2331067F 1 2000047F 3 2020471E 11 2227023F 19 3610353H 15 2331067F

DEGREE 20
7 4001051E
15 4221037B
25 4307165A
165 5145217B
825 6044073D
465 5057137B
2325 4504261A
5115 5227265A
25575 66471330
615 7113055C
1353 76027770
6765 5521623B
19065 71645555
14943 4102041A 17 31464556 1 4000011E 9 4040217B 17 6000031G 75 4266075A 55 4346037B 31 4034755A 155 4367471A 341 4510031 1705 6406005C 41 4027577B 2755 5017111A 1271 70506570 6355 6130725C 19 3610353H
3 4000017R
11 4070071A
19 4442235E
33 40362678
165 5145217R
465 673 778
1023 75525570
123 47617578
615 7113055C
6765 55216238
18013 4365438
19065 7164555C 21 2766447F
5 420031A
13 4004515E
21 4103307B
55 4346037B
275 6077135C
155 4367471A
775 6505453D
1705 6406005C
8525 5746331A
205 55414277A
451 7544237D
2255 5017111A
6355 6130725C
13981 4100001A

DEGREE 21 7 11111115A 15 10050335E 49 11105347A 6223 17155161C 42799 10040001A DEGREE 22 7 2222223F 15 20110517B 23 20005611A 2047 22404051A 60787 34603145C 1 20000003F 9 20100453B 17 20430607F 69 20465307B 6141 36544657D 5 20001043F 13 20401207F 21 31400147D 267 24146477B 15709 217744138

DEGREE 23 1 40000041E 7 40010061E 9 50000241E 15 40405463F 17 40103271E 47 44636045A 178481 43073357B 3 40404041E 11 40220151E 19 41224445E

APPENDIX C 491 Table C.2. Irreducible Polynomials of Degree \leq 34 over GF(2).

1 200000011E 7 200010031E 13 201014171E 19 200014731E 601 353551603D 55831 253566335A 3 200000017F 9 200402017F 15 204204057F 21 201015517F 18631 277267355A DEGREE 25 5 204000051E 11 252001251E 17 200005535E 31 200523477B 1801 341573647D 1 400000107F 7 402365755E 13 510664323F 19 411335571E 8191 614326143D DEGREE 26 DEGREE 27 5 1020024171E 11 1250025757F 17 1112225171E 73 1215076703A 1 1000000047E 7 1004462703B 13 1257242631E 19 1037530241E 511 1745602367D 3 1001007071E 9 1102210617E 15 1020560103F 21 10065243478

DEGREE 28

1 4000000005E 7 4010000045E 13 4001040115E 19 404003075E 1103 4663771561A 486737 6276417701C

492 APPENDIX C

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

DEGREE 30		1	10040000007F	1	10045207405A
	10104264207F	÷			10466404155A
11	104211064678	13			12531150265A
17	11326212703F	19		21	
63	15671207425A	33			10617013661A
99	10231077101A	17		231	125515213538
231	12551521353B		12363365205A	31	10537567431A
	131042734078		13104273407B	279	17565561725C
	130637764438		14475010377C		14475010377C
	162177475170	341			
	13005472403B	3069		1023	
7161	17273014127A	7161			17327131755A
	11732145645A				15222475661C
	13137001367A		15642307235C		15642307235C
	14046056527C	1057	17576155211A 15362114071A	3171	
	11747625331A				16275156545A
	123051262538		11747625331A		14262504223C
			11274077671A	34881	11274077671A
	16671210137D		11346765601A		15727555211C
	15727555211C		11154174627A		14271111643D
	173137751570		17313775157D		17667776677D
	15116464137C		10170400463B		10170400463B
	13637044253B		13726766575A		14437537423D
	14437537423D		176575372770		13214207735A
	151007275038		15100727503B		11115104367B
	107373110478		12374572221A		.12374572221A
	11567732701A		14707036127B		16076273661C
10923	16076273661C	25487	10403615303A	76461	10221305567A
76461	10221305567A	10261	16150525151C	30783	10363607103A
30783	10363607103A	92349	12553152637A	71827	14221266525C
215481	17473760245C	215481	17473760245C	646443	17070134445A
	12527647623A	338613	12670030647A	338613	12670030647A
790097	12105065527A	2370291	10545323161A	2370291	10545323161A
	10400014607B	149943	10502035235A	149943	10502035235A
449829	12240170427B	349867	10101010111A	549791	11303560025A
1649373	15735076321C	1649373	15735076321C		11010100111A
1549411	121353566338		11274767701A		11274767701A
	16471647235C		11000100011A		
DEGREE 31		1	20000000011F	3	20000000017E
5	20000020411E	7	21042104211E	9	20010010017E
11	20005000251E	13	20004100071E		20202040217E
	20000200435E		20060140231E		21042107357E
• .		• •	200001702510		210.210.33.4
DEGREE 32		1	40020000007F	3	40001114005A
5	505210217478	î		á	
	40035532523F		42003247143F		42644424505A
	44165166133B		41760427607F		56032357221A
51	73274317525C		552550042278		60537314115C
257	522131425678		46633742135A		530461151238
	47254550703B		45052437233B		71265756301C
	65636126613D		57410204175A	15107	712077703010
21045	020301200130	0,,,,,	31410204113A		
DEGREE 33		1	100000020001E	1	100020024001E
5 1	04000420001E		1000000260001A		100020024001E
	11100021111E		100000020001A		104020466001E
	00502430041E		100601431001E		100034327001A
	00021260105A		107167672771A		100034327001A
	241553415678		142560223461C		150052442055C
	25725100311A		101534661265A		1077534752138
277419	E2.23100311A	13100017	101724001502W	22225031	1011734172130
DEGREE 34		1	201000000007F	3	201051003005A
	01472024107F		3770000007527H		201051003005A
	25213433257F		227712240037F		213753015051A
	51132516577F		211636220473F		377235535321C
	27304565547D		331706543633D		226405640551A
4,071	2.3043033410	131011	.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	373213	22040704077IM

Spread Spectrum - 67 - Dr A. Manikas