GENERATION AND PROPERTIES OF PSEUDO-NOISE SEQUENCES

THE CODES THAT FORM THE SPREADING FUNCTION ACT AS NOISE-LIKE BUT DETERMINISTIC CARRIERS FOR THE INFORMATION BEING TRANSMITTED.

TO FULLY UNDERSTAND AND DESIGN GOOD NOISE-LIKE CODES WE WOULD NEED TO UNDERSTAND FINITE FIELD ARITHMETIC

- THIS IS BEYOND THE SCOPE OF THIS COURSE, SO WE CONSIDER ONLY THE FUNDAMENTAL PRINCIPLES

- AN ITRODUCTION TO FINITE FIELD ARITHMETIC CAN BE FOUND IN:

"INTRODUCTION TO SPREAD SPECTRUM COMMUNICATIONS" PUB PRENTICE-HALL, 1995 PETERSON, ZIEMER AND BORTH

WE WILL CONSIDER PN CODES;

* MAXIMAL LENGTH SEQUENCES
* GOLD CODES
* NASA JPL RANGING CODE

MAXIMAL LENGTH CODES

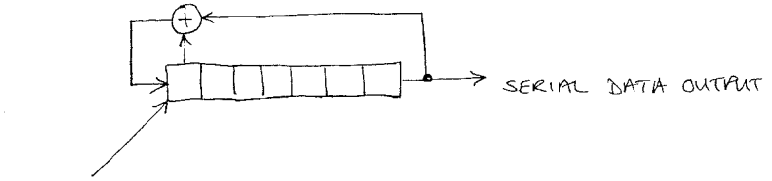
WE HAVE ALREADY ENCOUNTERED THESE BRIEFLY WHEN WE LOOKED AT CYCLIC CODES.

WE SAID THAT A MAXIMAL LENGTH CODE WAS CHARACTERIZED BY

$$(n,k) = (2^m-1, m) \qquad m \in Z^+$$

THE USUAL WAY OF GENERATING A MAXIMAL LENGTH CODE IS WITH A LINEAR FEEDBACK SHIFT REGISTER CIRCUIT

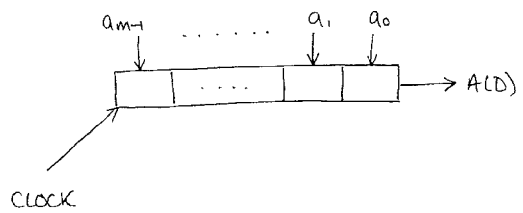
FOR EXAMPLE; THE FOLLOWING CIRCUIT GENERATES A SEQUENCE THAT IS MAXIMAL



$m=7$ (NUMBER OF STAGES)

$2^m-1 = 127$ (LENGTH OF SEQUENCE)

CONSIDER THE FOLLOWING DIAGRAM;

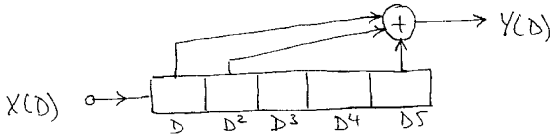


WE CAN PARALLEL LOAD THE SHIFT REGISTER AND CLOCK OUT THE BITSTREAM DEFINED BY;

$$A(D) = a_0 + a_1 D + a_2 D^2 + \ldots a_{m-1} D^{m-1}$$

WE CAN GENERATE A CONTINUOUS SEQUENCE BY FEED BACK.

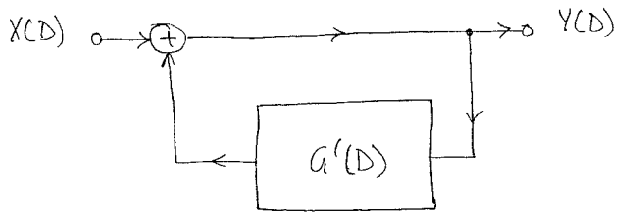
THE TRANSFER FUNCTION OF A SHIFT REGISTER STAGE CAN BE FOUND AS FOLLOWS;



$$Y(D) = X(D)(D + D^2 + D^5)$$

$$G'(D) = Y(D)/X(D) = D + D^2 + D^5$$

THE MAXIMAL LENGTH SEQUENCE GENERATOR IS BASED ON THE CONFIGURATION SHOWN BELOW

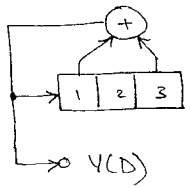


HENCE THE TRANSFER FUNCTION OF THE COMPLETE GENERATOR

$$\frac{Y(D)}{X(D)} = \frac{1}{1 + G'(D)} = \frac{1}{G(D)}$$

CONSIDER A SIMPLE EXAMPLE;

$2^m - 1 = 7$



$G(D) = 1 + G'(D)$
$G(D) = 1 + [D + D^3]$

SO LONG AS THE SHIFT REGISTER IS NOT LOADED WITH THE ALL-ZERO STATE A SEQUENCE OF SOME KIND IS OUTPUT AS Y(D) AND FED-BACK TO THE INPUT

IN ORDER THAT THE SEQUENCE BE MAXIMAL LENGTH, IT IS NECESSARY FOR THE TRANSFER FUNCTION $G(D)$ TO BE OF A PARTICULAR FORM.

IF THE SHIFT REGISTER FEEDBACK CONNECTIONS DO NOT CORRESPOND TO THESE ALLOWED FORMS, A SEQUENCE WILL STILL BE PRODUCED, BUT IT WILL NOT BE MAXIMAL, AND IT WILL NOT HAVE THE SPECIAL AUTO-CORRELATION PROPERTIES THAT MAXIMAL LENGTH SEQUENCES HAVE.

TO PRODUCE A MAXIMAL LENGTH SEQUENCE IT IS NECESSARY THAT $G(D) = 1 + G'(D)$ (WHICH DESCRIBES THE FEEDBACK TAP POINTS) BE IRREDUCIBLE

A POLYNOMIAL THAT IS IRREDUCIBLE CANNOT BE FACTORED INTO POLYNOMIALS OF SMALLER DEGREE WHOSE COEFFICIENTS ARE ONLY PERMITTED TO BE 0 OR 1

FOR EXAMPLE $G(D) = 1 + G'(D) = 1 + D + D^3$

IS AN IRREDUCIBLE POLYNOMIAL.

HENCE THE GENERATOR SHOWN ON PAGE 4 WILL PRODUCE A MAXIMAL LENGTH SEQUENCE

TO SHOW THIS CONSIDER PRE-LOADING THE SHIFT-REGISTERS WITH THE BINARY WORD 111, FOR EACH CLOCK PULSE THE RESULTING WORDS ARE:

	CLOCK PULSE	STAGE 1	STAGE 2	STAGE 3
INITIAL CONTENTS →	0	1	1	1
	1	0	1	1
	2	1	0	1
	3	0	1	0
	4	0	0	1
	5	1	0	0
	6	1	1	0
REPEAT OF SEQUENCE →	7	1	1	1

$G(D) = 1 + D + D^3$ IS NOT THE ONLY IRREDUCIBLE POLYNOMIAL OF DEGREE 3, WE COULD HAVE CHOSEN $G(D) = 1 + D^2 + D^3$ WHICH PRODUCES A COMPLETELY DIFFERENT SEQUENCE OF LENGTH 7

THE IRREDUCIBLE POLYNOMIALS ARE ALSO CALLED PRIMITIVE POLYNOMIALS

THE NUMBER OF DIFFERENT MAXIMAL LENGTH SEQUENCES OF A GIVEN LENGTH, $(L = 2^m - 1)$ TENDS TO INCREASE AS m INCREASES.

THE NUMBER OF DIFFERENT PSEUDO-NOISE SEQUENCES IS PARTICULARLY IMPORTANT WHEN THE SPREAD SPECTRUM IS BEING USED AS A CODE-DIVISION MULTIPLE ACCESS SCHEME, WHERE EACH USER HAS A DIFF-ERENT SPREADING SEQUENCE OF THE SAME LENGTH, L.

IF THE NUMBER AVAILABLE CODES IS SMALL THIS PLACES AN IMMEDIATE RESTRICTION ON THE NUMBER OF USERS. IT CAN BE SHOWN THAT THE NUMBER OF MAXIMAL SEQUENCES FOR AN m STAGE SHIFT REGISTER IS;

$$N = \frac{\phi(2^m - 1)}{m}$$

$\phi(I)$ IS THE EULER NUMBER

FORTUNATELY ALL OF THE IRREDUCIBLE POLYNOMIALS HAVE BEEN FOUND UPTO QUITE LARGE DEGREES - THESE HAVE BEEN TABULATED IN MANY BOOKS

TABLE 3-6. Number of Primitive Polynomials N_p of Degree r

r	N_p	r	N_p
2	1	16	2,048
3	2	17	7,710
4	2	18	8,064
5	6	19	27,594
6	6	20	24,000
7	18	21	84,672
8	16	22	120,032
9	48	23	356,960
10	60	24	276,480
11	176	25	1,296,000
12	144	26	1,719,900
13	630	27	4,202,496
14	756	28	4,741,632
15	1,800	29	18,407,808

Source: Ref. 22.

TABLE 3-5. Primitive Polynomials Having Degree $r \le 34$ (continued)

Degree	Octal Representation of Generator Polynomial (g_0 on right to g_r on left)
6	[103]*, [147], [155]
7	[211]*, [217], [235], [367], [277], [325], [203]*, [313], [345]
8	[435], [551], [747], [453], [545], [537], [703], [543]
9	[1021]*, [1131], [1461], [1423], [1055], [1167], [1541], [1333], [1605], [1751], [1743], [1617], [1553], [1157]
10	[2011]*, [2415], [3771], [2157], [3515], [2773], [2033], [2443], [2461], [3023], [3543], [2745], [2431], [3177]
11	[4005]*, [4445], [4215], [4055], [6015], [7413], [4143], [4563], [5023], [5623], [4577], [6233], [6673]
12	[10123], [15647], [16533], [16047], [11015], [14127], [17673], [13565], [15341], [15053], [15621], [15321], [11417], [13505]
13	[20033], [23261], [24623], [23517], [30741], [21643], [30171], [21277], [27777], [35051], [34723], [34071], [32535], [31425]
14	[42103], [43333], [51761], [40503], [77141], [62677], [44103], [45145], [76303], [64457], [57231], [64167], [60153], [53753]
15	[100003]*, [102043], [110013], [102067], [104307], [100317], [117775]*, [103451], [110073], [102061], [114725], [103251], [100021]*, [100201]*
16	[210013]*, [234313], [233303], [307107], [307527], [306357], [201737], [272201], [242413], [270155], [302157], [210205], [305667], [236107]
17	[400011]*, [400017], [400431], [525251], [410117], [407131], [411335], [444257], [600013], [403555], [525327], [411077], [400041]*, [400101]*
18	[1000201]*, [1000247], [1002411], [1062441], [1100045], [1000407], [1003011], [1020121], [1101005], [1000077], [1001361], [1001567], [1001727], [1002777]
19	[2000047], [2000641], [2001441], [2000107], [2000077], [2000157], [2000175], [2000257], [2000677], [2000737], [2001557], [2001637], [2005775], [2006677]
20	[4000011]*, [4001051], [4004515], [6000031], [4442235]
21	[10000005]*, [10040205], [10020045], [10040315], [10000635], [10000725], [10005235], [10000135], [12000025]

TABLE 3-5. Primitive Polynomials Having Degree $r \le 34$ (continued)

Degree	Octal Representation of Generator Polynomial (g_0 on right to g_r on left)
23	[4000004]*, [4040041], [4000063], [4001061], [5000241], [4022015], [4000634], [4040546], [4010327], [4123444], [4035561]
24	[10000207], [12524661], [11376306]
25	[2000001]*, [20000017], [20400051], [2000100], [2040020], [2520012], [2010141], [2042040], [2000055], [2001473]
26	[4000017], [4020164], [4023657], [4263256], [5106432], [4731675], [4133557]
27	[10000004], [1001007], [1020024], [1022061], [1257246], [1025605], [1122251], [1035302]
28	[2000001]*, [2104210], [2000025], [2020006], [2002502], [2001601]
29	[4000000]*, [4004004], [4000103], [4010000], [4000400], [4004043]
30	[10,040,000,007], [10,104,264,207], [10,115,131,333], [11,362,212,703], [10,343,244,533]
31	[20,000,000,011]*, [20,000,000,017], [20,000,020,411], [21,042, 104, 211], [20,010,010,017], [20,003,000,253], [20,004,100,071], [20,002,040,217], [20,000,200,435], [20,060,140,231], [21,042,107,357]
32	[40,020,000,007], [40,460,216,667], [40,035,352,525], [42,003,247,143], [41,760,427,607]
33	[100,000,020,001]*, [100,020,024,001], [104,000,420,001], [100,020,224,401], [111,100,021,111], [100,000,031,463], [104,020,466,001], [100,502,430,041], [100,601,431,001]
34	[201,000,000,007], [201,472,024,107], [377,000,007,527], [225,213,433,257], [227,712,240,037], [251,132,516,577], [211,636,220,473], [200,000,140,003]
35	[400,000,000,005]*
36	[1,000,000,004,001]*
37	[2,000,000,012,005]
38	[4,000,000,000,143]
39	[10,000,000,000,021]*

AN IMPORTANT PRACTICAL CONSIDERATION WHEN DESIGNING FEEDBACK CIRCUITS FOR SPREAD-SPECTRUM SYSTEMS IS THE MAXIMUM CLOCK RATE THAT THE CIRCUIT WILL OPERATE AT.

WHEN LARGE NUMBER OF MODULO-2 ADDITIONS ARE CARRIED OUT IN THE FEEDBACK PATH (FOR EXAMPLE WHEN $m=12$, OR 14) THE FEEDBACK PROPAGATION DELAY CAN BECOME EXCESSIVE AND THIS PLACES A LIMIT ON THE CLOCK RATE THAT CAN BE USED.

WE CAN IMPROVE THINGS BY DESIGNING OUR FEEDBACK CONNECTIONS CAREFULLY

FOR EXAMPLE;

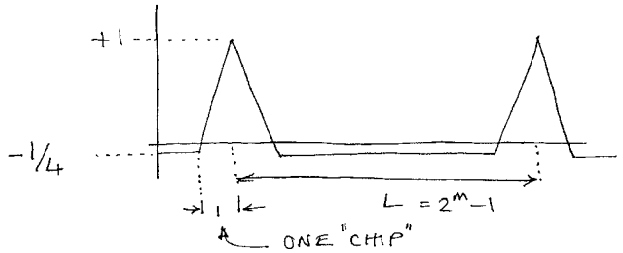
IS FASTER THAN;

THE RATE OF THE PN-SEQUENCE IS OFTEN CALLED THE "CHIP RATE"

AUTOCORRELATION FUNCTIONS

A PROPERTY OF ALL MAXIMAL LENGTH SEQUENCES IS THAT THEY HAVE A TRIANGULAR AUTO-CORRELATION FUNCTION WHICH, IN NORMALIZED FORM, HAS A PEAK AMPLITUDE OF +1, BEYOND THIS IT HAS A VALUE OF $-1/L$ WHERE L IS THE LENGTH OF THE SEQUENCE

FOR EXAMPLE;



THE NORMALIZED AUTO-CORRELATION FUNCTION $R(\tau)$ OF A PERIOD WAVEFORM $x(t)$ WITH PERIOD T_0 IS

$$R(\tau) = \frac{1}{N} \int_{-T_0/2}^{+T_0/2} x(t)\, x(t+\tau)\, dt \qquad -\infty < \tau < \infty$$

WHERE $$N = \frac{1}{T_0} \int_{-T_0/2}^{+T_0/2} x^2(t)\, dt.$$

FOR OUR DISCRETE PN-SEQUENCE THIS CAN BE WRITTEN AS;

$$R(\tau) = \frac{1}{L} \times \left[\text{NUMBER OF AGREEMENTS LESS NUMBER OF DISAGREEMENTS FOR A CYCLIC SHIFT OF } \tau\right]$$

FOR EXAMPLE; CONSIDER THE SEQUENCE 1110010, $L = 7 = 2^3 - 1$

SHIFT	SEQUENCE	AGREE	DISAGREE	DIFF.
0	1110010	—	—	—
1	0111001	3	4	-1
2	1011100	3	4	-1
3	0101110	3	4	-1
4	0010111	3	4	-1
5	1001011	3	4	-1
6	1100101	3	4	-1
7	1110010	7	0	+7

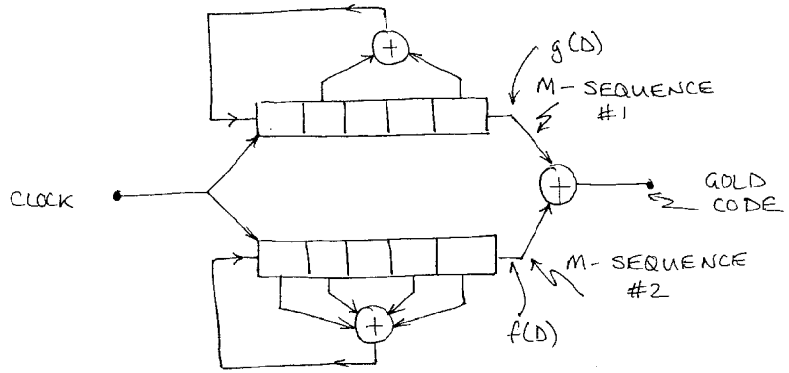
$\Rightarrow R(\tau) = -1/7, -1/7, -1/7, -1/7, -1/7, -1/7, +1.$

$\tau = 1, 2, 3, 4, 5, 6, 7.$

IF THE SEQUENCE IS NOT MAXIMAL, THERE ARE SIDELOBES TO THE AUTO-CORRELATION SEQUENCE.

GOLD CODES

GOLD CODES ARE GENERATED BY USING TWO MAXIMAL LENGTH SEQUENCES;



THE POLYNOMIALS FOR #1 AND #2 ARE

$$\#1 \quad g(D) = 1 + D^2 + D^5$$

$$\#2 \quad f(D) = 1 + D + D^2 + D^4 + D^5$$

THE GOLD CODE IS GENERATED BY TWO M-SEQUENCES OF LENGTH $L = 2^m - 1$, THE NUMBER OF GOLD CODES THAT CAN PRODUCED (OF LENGTH L) IS $2^m + 1 = L + 2$, OF WHICH TWO ARE MAXIMAL (THE BASE SEQUENCES). THE OTHERS ARE NON-MAXIMAL

THE MAIN USE OF GOLD CODES IS IN CDMA

ALTHOUGH THE GOLD CODE IS NON-MAXIMAL THERE ARE MORE GOLD CODES THAN THERE ARE MAXIMAL CODES FOR A GIVEN CODE SEQUENCE LENGTH.

IF WELL DESIGNED, NON-MAXIMAL CODES HAVE A PERFORMANCE IN CDMA NO WORSE THAN MAXIMAL CODES. THE ADDITIONAL SIDELOBES IN THE AUTO CORRELATION FUNCTION OF A NON-MAXIMAL CODE CAN COMPLICATE THE SYNCHRONIZATION PROCESS AT THE RECEIVER.

JPL RANGING CODE

UNTIL RECENT YEARS AND THE ADVENT OF CDMA THIS WAS THE LARGEST APPLICATION OF SPREAD-SPECTRUM METHODS

THE JPL CODES HAVE SPECIAL PROPERTIES WHICH MAKE THEM EASY TO SYNCHRONIZE AND ACQUIRE

THESE CODES FORMED THE BASIS OF RANGING FOR MOST SPACE EXPLORATION SINCE THE EARLY 1960'S.