COE 571 Digital System Testing

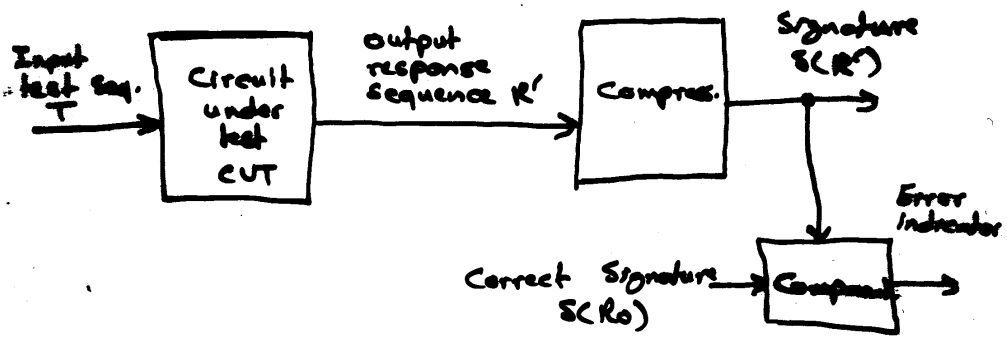
Dr. Aiman El-Maleh

Test Response Compaction

1. **Signature analysis**
2. **Linear feedback shift registers (LFSRs)**
3. **Types of LFSRs**
4. **Characteristic & reciprocal characteristic polynomials**
5. **Periodicity of LFSRs**
6. **Primitive ploynomials**
7. **Signature analyzers**
8. **Multiple input signature register (MISR)**

Testing using Test-Response Compression

- Observed test responses are saved in a compressed form, called **signature**
- A circuit is tested by comparing observed signature with correct signature
- Process of reducing test responses to a signature is called **response compacting or compressing.**



- A fault is detected if signature S(R') ≠ fault-free signature S(R0)
- Compression is important aspect of built-in self-test (BIST).

Signature Analysis

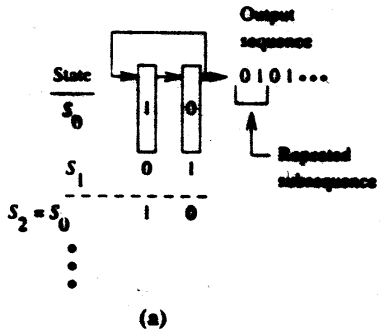
- Signature analysis is a compression technique based on cyclic Redundancy checking (CRC) and realized by linear feedback shift registers (LFSRs).
- LFSRs used as :
  - Source of pseudorandom binary test sequence
  - Carry out response compression
- A linear circuit is a logic network constructed from :
  - unit delays or D FFs
  - modulo-2 adders
  - modulo-2 scalar multipliers
- In the analysis of such circuits, all operations done are modulo-2
- Such a circuit is linear since it preserves principle of superposition :
  - its response to a linear combination of stimuli is linear combination of responses to individual stimuli

modulo-2 addition / subtraction

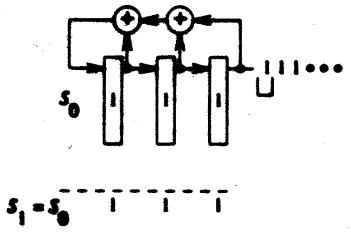
±	0	1
0	0	1
1	1	0

$X+X = -X-X = X-X = 0$

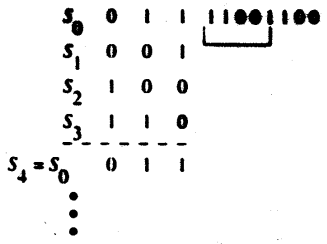
Feedback Shift Registers



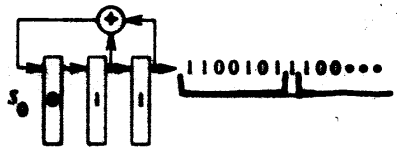
(a)

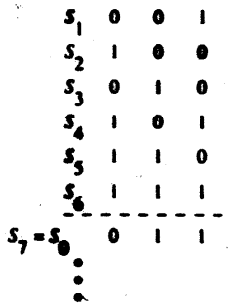


(b)



(c)





(d)

Types of LFSRs

- $c_i = 1$ ⇒ there is a connection, otherwise no connection

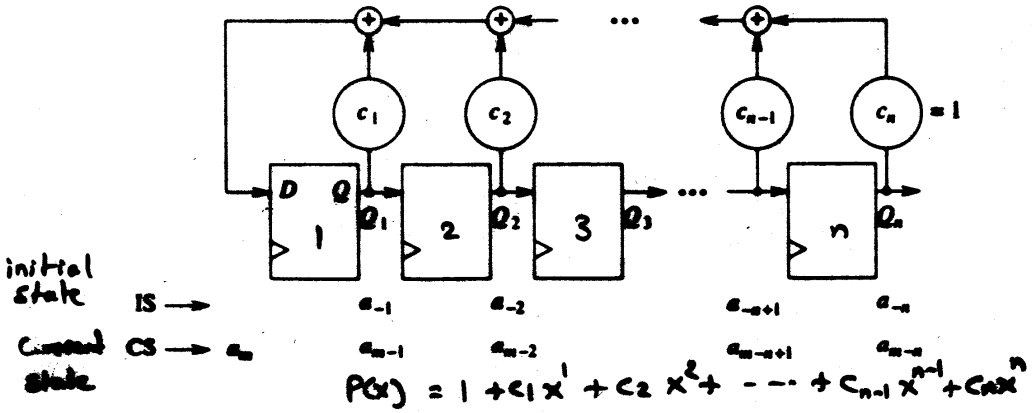


Figure 10.10 Type 1 (external-XOR) LFSR

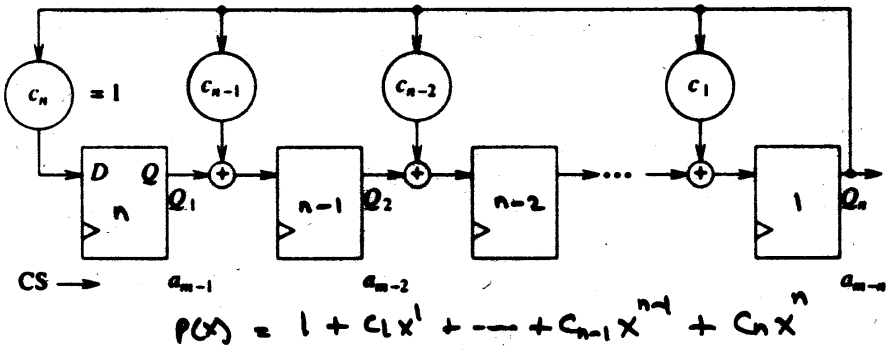


Figure 10.11 Type 2 (internal-XOR) LFSR

- A sequence of numbers $a_0, a_1, \cdots, a_m$ can be associated with a polynomial called a generating function $G(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m$

- Let $\{a_m\} = a_0, a_1, a_2, \cdots$ represent the output sequence generated by LFSR; $a_i = 0$ or 1

- This sequence can be expressed as:

$$G(x) = \sum_{m=0}^{\infty} a_m x^m$$

- From structure of typel LFSR, if current state of Q_i is a_{m-i} for $i = 1, 2, \cdots n$

$$a_m = \sum_{i=1}^{n} c_i a_{m-i}$$

- Thus, the operation of LFSR can be defined by a <u>recurrence relation</u>

- Let initial state of LFSR be $a_{-1}, a_{-2}, \cdots, a_{-n}$

$$G(x) = \sum_{m=0}^{\infty} a_m x^m = \sum_{m=0}^{\infty} \sum_{i=1}^{n} c_i a_{m-i} x^m$$

$$= \sum_{i=1}^{n} c_i x^i \sum_{m=0}^{\infty} a_{m-i} x^{m-i}$$

Let $j = m - i$

$$\Rightarrow \sum_{m=0}^{\infty} a_{m-i} x^{m-i} = \sum_{j=-i}^{\infty} a_j x^j$$

$$= a_{-i} x^{-i} + \cdots + a_{-1} x^{-1} + \sum_{j=0}^{\infty} a_j x^j$$

$$\Rightarrow G(x) = \sum_{i=1}^{n} c_i x^i \left[a_{-i} x^i + \cdots + a_{-1} x^{-1} + G(x) \right]$$

$$\Rightarrow G(x) = \sum_{i=1}^{n} c_i x^i G(x) + \sum_{i=1}^{n} c_i x^i \left(a_{-i} x^{-i} + \cdots + a_{-1} x^{-1} \right)$$

$$\text{or} \quad G(x) = \frac{\sum_{i=1}^{n} c_i x^i \left(a_{-i} x^{-i} + \cdots + a_{-1} x^{-1} \right)}{1 + \sum_{i=1}^{n} c_i x^i}$$

- Thus, $G(x)$ is a function of the initial state $a_{-1}, a_{-2}, \cdots, a_{-n}$ of the LFSR and feedback coefficients
- The denominator denoted by
  $$P(x) = 1 + c_1 x + c_2 x^2 + \cdots + c_n x^n$$
  is the <u>characteristic polynomial</u> of the sequence $\{a_m\}$ and the LFSR
- For an n-stage LFSR, $c_n = 1$.
- If we set $a_{-1} = a_{-2} = a_{1-n} = 0$ and $a_{-n} = 1$
  $$G(x) = \frac{1}{P(x)} = \sum_{m=0}^{\infty} a_m x^m$$

- Since the sequence $\{a_m\}$ is cyclic with period P

$$\frac{1}{P(x)} = (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) + x^p (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) + x^{2p} (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}) + \cdots$$

$$= (a_0 + a_1 x + \cdots + a_{p-1} x^{p-1})(1 + x^p + x^{2p} + \cdots$$

$$= \frac{a_0 + a_1 x + \cdots + a_{p-1} x^{p-1}}{1 - x^p}$$

- Thus, $P(x)$ evenly divides into $1 - x^p$

- For type 1 LFSR $a_m(t) = \sum_{i=1}^{n} c_i a_{m-i}(t)$

- Note that $a_i(t) = a_{i+1}(t-1)$

- Let x be a shift operator such that

$$x^k a_i(t) = a_i(t-k)$$

$$\Rightarrow a_m(t) = \sum_{i=1}^{n} c_i a_{m-i}(t) = \sum_{i=1}^{n} c_i x^i a_m(t)$$

- Note that $x a_m(t) = a_m(t-1) = a_{m-1}(t)$

$$\Rightarrow a_m + c_1 x\, a_m + c_2 x^2 a_m + \cdots + c_n x^n a_m = 0$$

$$\text{or} \quad \underbrace{[\,1 + c_1 x + c_2 x^2 + \cdots + c_n x^n\,]}_{\text{characteristic polynomial}} a_m = 0$$

- Let $y^{-k} a_l(t) = a_l(t-k) = x^k a_l(t)$

$$\Rightarrow [\,1 + c_1 y^{-1} + c_2 y^{-2} + \cdots + c_n y^{-n}\,] a_m = 0$$

$$\Rightarrow [\,y^n + c_1 y^{n-1} + c_2 y^{n-2} + \cdots + c_n\,] a_m y^{-n}$$

- Replacing y by x

$$\Rightarrow p^*(x) = c_n + c_{n-1} x + c_{n-2} x^2 + \cdots + c_1 x^{n-1} +$$

- $p^*(x)$ is said to be <u>reciprocal polynom</u> of $p(x)$ since $p^*(x) = x^n p(1/x)$

- Thus, every LFSR can be associated with two characteristic polynomials

- Note that $p^*(x)$ produces the reverse of what $p(x)$ produces

Reciprocal Characteristic Polynomials

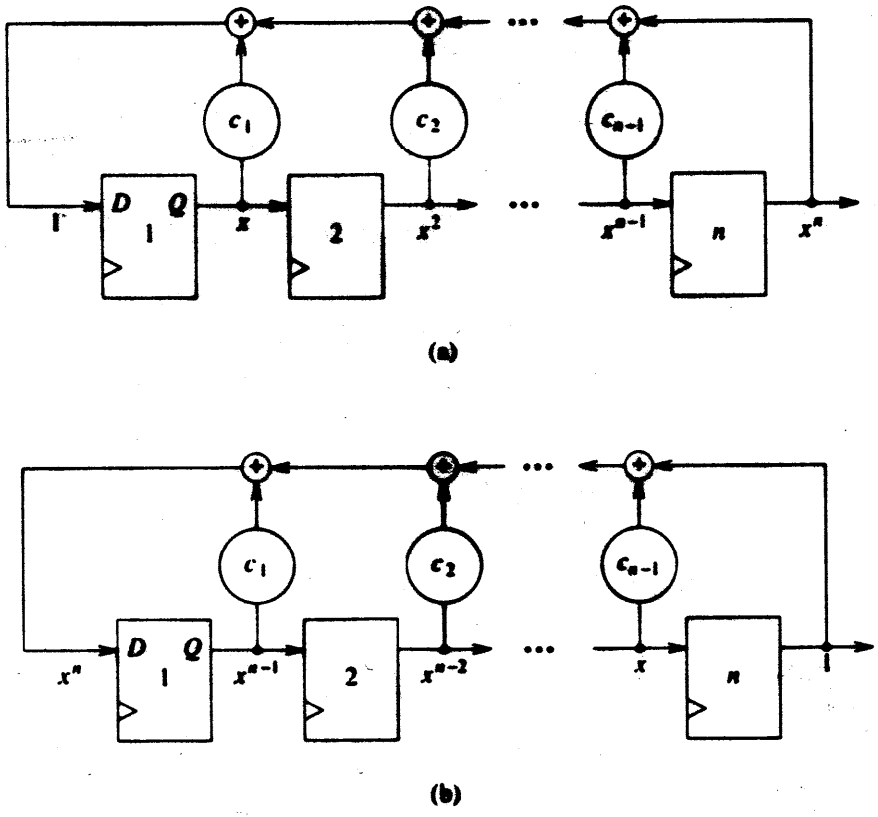


Figure 10.12 Reciprocal characteristic polynomials
(a) $P(x) = 1 + c_1 x + c_2 x^2 + \ldots + c_{n-1}x^{n-1} + x^n$
(b) $P^*(x) = 1 + c_{n-1} x + c_{n-2} x^2 + \ldots + c_1 x^{n-1} + x^n$

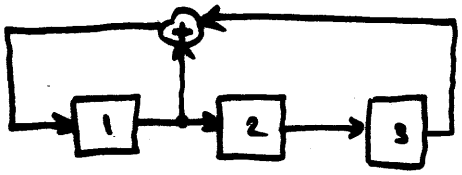
Reciprocal Polynomials

Example

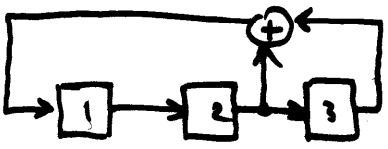
- Let $P(x) = 1 + x + x^3$
- Its reciprocal polynomial $P^*(x)$

$= x^3 P(\frac{1}{x}) = x^3 [1 + x^{-1} + x^{-3}]$

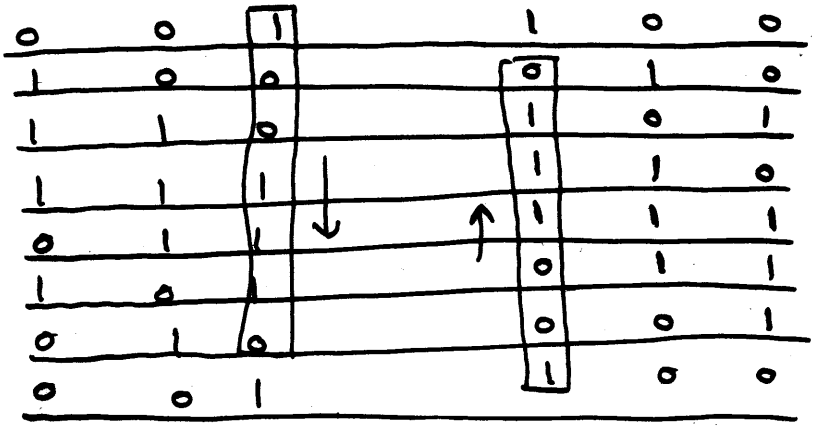
$= x^3 + x^2 + 1$



$P(x) = 1 + x + x^3$



$P(x) = 1 + x^2 + x^3$



Generated sequence:

1 0 0 1 1 1 0, 1 0 0 —

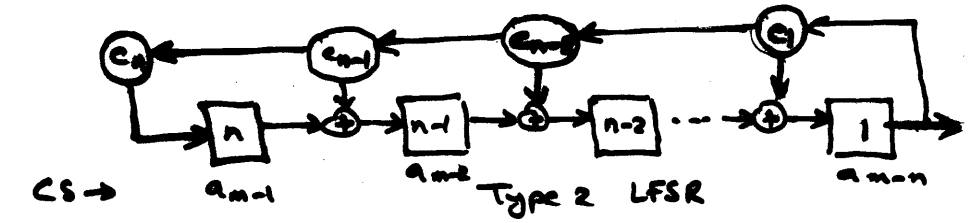
Generated sequence:

1, 0 1 1 1 0 0 1, 0 1 —

Type 2 LFSR

Characteristic Polynomial

- A given characteristic polynomial can be realized by two different LFSRs.



- For $i = 2, 3, \cdots, n$

$$a_{m-i}(t+1) = a_{m-i+1}(t) + c_{n-i+1}\, a_{m-n}(t)$$

If we define $a_m(t) = 0$, the equation also holds for $i = 1$

- Let X be a shift operator such that

$$X^k a_i(t) = a_i(t-k)$$

$$\Rightarrow X^{-1} a_{m-i}(t) = a_{m-i+1}(t) + c_{n-i+1}\, a_{m-n}$$

for $i = 1, 2, \cdots, n$

- Multiplying the ith equation by X^{-i+1} we get:

$$\begin{aligned}
X^{-1} a_{m-1} &= c_n a_{m-n} \\
X^{-2} a_{m-2} &= X^{-1} a_{m-1} + c_{n-1} X^{-1} a_{m-n} \\
X^{-3} a_{m-3} &= X^{-2} a_{m-2} + c_{n-2} X^{-2} a_{m-n} \\
&\vdots \\
X^{-n} a_{m-n} &= X^{-n+1} a_{m-n+1} + c_1 X^{-n+1} a_{m-n}
\end{aligned}$$

- Summing these equations & canceling terms appearing on both sides:

$$\Rightarrow X^{-n} a_{m-n} = [c_1 X^{-n+1} + \cdots + c_{n-2} X^{-2} + c_{n-1} X^{-1} + c_n] a_{m-}$$

$$\text{or } [X^{-n} + c_1 X^{-n+1} + \cdots + c_{n-2} X^{-2} + c_{n-1} X^{-1} + c_n] a_{m-n} =$$

Multiplying by X^n we get:

$$[\underbrace{1 + c_1 X + \cdots + c_{n-2} X^{n-2} + c_{n-1} X^{-1} + c_n X^n}] a_{m-n}$$

Characteristic polynomial for type 2 LFSR

- A type 2 LFSR can be associated with two characteristic polynomials reciprocal of each other

Periodicity of LFSRs

- The LFSR goes through a cyclic or periodic sequence of states and the output produced is also periodic
- The maximum length of this period is $2^n - 1$ where n is the number of stages
- **Theorem:** If the initial state of an LFSR is $a_{-1} = a_{-2} = \dots = a_{1-n} = 0$, $a_{-n} = 1$, then the LFSR sequence $\{a_m\}$ is periodic with a period that is the smallest integer k for which $p(x)$ divides $(1 - x^k)$
- Example: $p(x) = 1 + x + x^3$

Dividing $1 - x^6$ by $1 + x + x^3$ (quotient $x^3 + x + 1$):

$$1 - x^6$$
$$x^3 + x^4 + x^6$$
$$1 + x^3 + x^4$$
$$x + x^2 + x^4$$
$$1 + x + x^2 + x^3$$
$$1 + x + x^3$$
$$x^2$$

So, $p(x)$ does not divide $(1 - x^6)$

Dividing $1 - x^7$ by $1 + x + x^3$ (quotient $x^4 + x^2 + x + 1$):

$$1 - x^7$$
$$x^4 + x^5 + x^7$$
$$1 + x^4 + x^5$$
$$x^2 + x^3 + x^5$$
$$1 + x^2 + x^3 + x^4$$
$$x + x^2 + x^4$$
$$1 + x + x^3$$
$$1 + x + x^3$$
$$0$$

$p(x)$ divides $(1 - x^7)$

$\Rightarrow$ period is **7**.

- **Definition:** If the sequence generated by an n-stage LFSR has period $2^n - 1$, then it is called *maximal-length sequence*.

- **Definition:** The characteristic polynomial associated with a maximal-length sequence is called a primitive polynomial.

- **Definition:** An irreducible polynomial is one that cannot be factored i.e., not divisible by any other polynomial other than 1 and itself.

- **Theorem:** An irreducible polynomial P(x) of degree n satisfies the conditions:
  1. For $n \geq 2$, P(x) has an odd number of terms including the 1 term
  2. For $n \geq 4$, P(x) must divide (evenly) into $1 + x^K$, where $K = 2^n - 1$

- **Theorem:** An irreducible polynomial is primitive if the smallest positive integer K that allows the polynomial to divide evenly into $1 + x^K$ occurs for $K = 2^n - 1$, where n is the degree of the polynomial.

Primitive Polynomials

Examples

n	$\lambda_2(n)$
1	1
2	1
4	2
8	16
16	2048
32	67108864

Figure 10.13 Number of primitive polynomials of degree n

1:	0				13:	4	3	1	0	25:	3	0		
2:	1	0			14:	12	11	1	0	26:	8	7	1	0
3:	1	0			15:	1	0			27:	8	7	1	0
4:	1	0			16:	5	3	2	0	28:	3	0		
5:	2	0			17:	3	0			29:	2	0		
6:	1	0			18:	7	0			30:	16	15	1	0
7:	1	0			19:	6	5	1	0	31:	3	0		
8:	6	5	1	0	20:	3	0			32:	28	27	1	0
9:	4	0			21:	2	0			33:	13	0		
10:	3	0			22:	1	0			34:	15	14	1	0
11:	2	0			23:	5	0			35:	2	0		
12:	7	4	3	0	24:	4	3	1	0	36:	11	0		

Figure 10.14 Exponents of terms of primitive polynomials

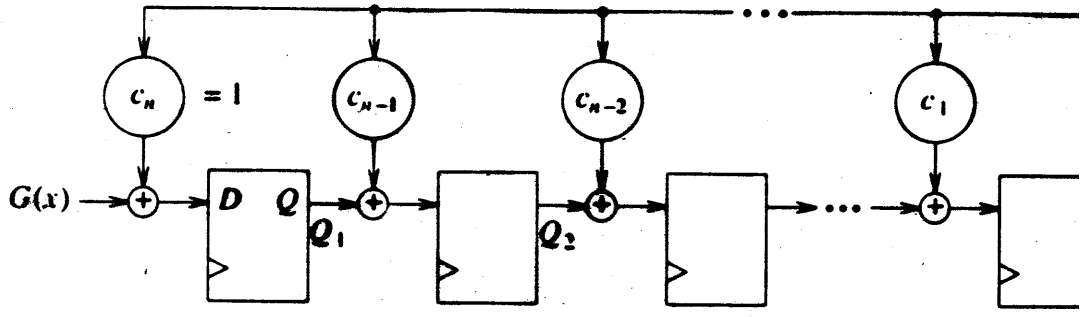
LFSRs as Signature Analyzers

- $P(x) = 1 + \sum_{i=1}^{n} c_i x^i$
- $P^*(x) = 1 + \sum_{i=1}^{n} c_i x^{n-i}$
- $\frac{G(x)}{P^*(x)} = Q(x) + \frac{R(x)}{P^*(x)}$

or $G(x) = Q(x)\,P^*(x) + R(x)$

- The input sequence $\{a_m\}$ is represented by $G(x)$ and output sequence by $Q(x)$
- Highest degree of $G(x)$ is first bit to enter LFSR
- Highest degree of $Q(x)$ is first output bit produced n clock cycles later

Type 2 LFSR

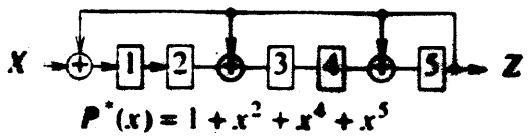


Initial State : $I(x) = 0$

Final State : $R(x)$

Shift Register Polynomial Division

- Type 1 LFSR performs polynomial division & produces correct quotient. However, contents of LFSR is not the remainder.



(a)

Input sequence: 1 1 1 1 0 1 0 1 (8 bi

$G(x) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$

(b)

Time	Input stream	Register contents	Output stream
		1 2 3 4 5	
0	1 0 1 0 1 1 1 1	0 0 0 0 0 ←	Initial state
1	1 0 1 0 1 1 1	1 0 0 0 0	
⋮	⋮	⋮	
5	1 0 1	0 1 1 1 1	
6	1 0	0 0 0 1 0	1
7	1	0 0 0 0 1	0 1
8	Remainder →	0 0 1 0 1	1 0 1
		1 x x^2 x^3 x^4	
		Remainder	Quotient
		$R(x) = x^2 + x^4$	$1 + x^2$

(c)

Figure 10.16 Polynomial division

Error Polynomial & Masking

- Let $E(x)$ be an <u>error polynomial</u> i.e. each non-0 coefficient represents an error in corresponding bit position

- Example:
  - Assume correct response $R_0 = 10111$
  - Let erroneous response be $R' = 11101$
  - Difference or error polynomial is 01010
  - Thus, $G_0(x) = x^4 + x^2 + x + 1$
  - $G'(x) = x^4 + x^3 + x^2 + 1$
  - $E(x) = x^3 + x$

- $G'(x) = G(x) + E(x)$ (modulo 2)

- Since $G(x) = Q(x)\, P^*(x) + R(x)$, an <u>undetectable</u> response sequence satisfies

  $G'(x) = G(x) + E(x) = Q'(x)\, P^*(x) + R(x)$

  $\Rightarrow$ $G(x)$ and $G'(x)$ produce same remainder

Theorem: Let $R(x)$ be generated signature for an input $Q(x)$ using LFSR with charact. polyn. $P(x)$. For an error polynomial $E(x)$, $Q(x)$ and $Q'(x) = Q(x) + E(x)$ have the same signature iff $E(x)$ is a multiple of $P(x)$.

- Both type 1 & type 2 LFSRs can be used to generate a signature $R(x)$.

Theorem: For an input data stream of length m, if all possible error patterns are equally likely, then the probability of masking in n-bit signature is:

$$P(M) = \frac{2^{m-n} - 1}{2^m - 1}$$

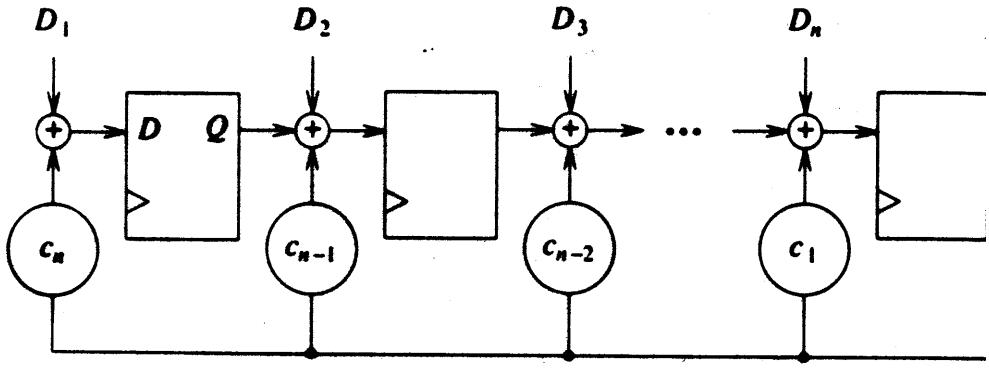
for $m \gg n$, $P(M) \approx 2^{-n}$

- Note that $P(x)$ has $2^{m-n} - 1$ non-0 multiples of degree less than m

Theorem An LFSR signature analyzer based on a polynomial with two or more non-0 coefficients detects all single-bit errors.

Multiple-Input Signature Register

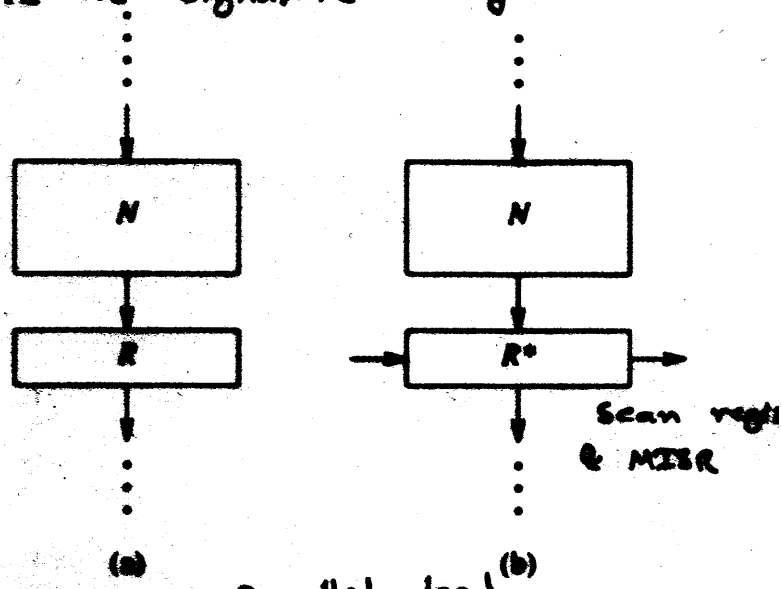
- Signature analysis can be extended to testing multiple-output circuits
- Operates as n single-input signature analyz



- Assuming all error patterns are equally likely, prob. of error masking is $\approx 2^{-n}$.
- Increasing effectiveness of signature analysi
  - increase MISR length
  - test can be repeated using different feedback polynomial
  - test can be repeated after changing test vectors order, thus producing differe error polynomial
  - periodically sampling signature analyzer output

Implementation Issues

- Often desirable to modify a functional reg to operate as signature analyzer



- clocking C & S ⇒ parallel load
- When S/T = 0, clocking A & B ⇒ Scan reg
- When S/T = 1, " " " ⇒ MISR

- LSSD double-latch SRL as a storage cell for signature analyzer based on typical LFSR