



Digitaltechnik EITF65

Lecture 13: Linear Sequential Circuits, Part 1

Linear Boolean functions

Definition (Linearity)

A function f is said to be linear if

$$f(\mathbf{x} \oplus \mathbf{y}) = f(\mathbf{x}) \oplus f(\mathbf{y}) \quad (\text{L}_1)$$

$$f(\alpha \mathbf{x}) = \alpha f(\mathbf{x}) \quad (\text{L}_2)$$

In other words

- ▶ The sum of the arguments gives the same as the sum of the functions.
- ▶ Multiplying the argument with a scalar is the same as multiplying the function.

Theorem

A Boolean function is linear if and only if it can be written as

$$\begin{aligned} f(\mathbf{x}) &= a_1x_1 \oplus \cdots \oplus a_nx_n \\ &= (a_1 \dots a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{ax} \quad a_i \in \{0, 1\} \end{aligned}$$

- *Any linear Boolean function can be realized with an n -input modulo 2 adder.*

Realisation of linear Boolean functions

- ▶ A combinational circuit containing only modulo 2 adders realizes a linear Boolean function.
- ▶ A linear Boolean function can be implemented with modulo 2 adders.

Linearity test

With the **ring sum expansion (RSE)** all Boolean functions can (uniquely) be written with Boolean ring operations (\oplus, \otimes) instead of Boolean algebra operations ($\vee, \wedge, '$).

$$f(\mathbf{x}) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n \\ \oplus a_{n+1} x_1 x_2 \oplus \cdots \oplus a_{2^n-1} x_1 \dots x_n$$

In a **linear Boolean function** $a_i = 0$, $i = 0$ and $i > n$,

$$f_a(\mathbf{x}) = a_1 x_1 \oplus \cdots \oplus a_n x_n$$

Theorem (4.6)

All Boolean functions $f(\mathbf{x}) \in B_n$ can be written with the (ring) operations \oplus and \otimes , by the *ring sum expansion (RSE/RMF)*,

$$f(\mathbf{x}) = \bigoplus_{j=0}^{2^n-1} a_j \bigotimes_{i \in I_n(j)} x_i$$

where $a_j \in B$ and $I_n(j)$ is an index function.

The RSE/RMF expression is unique for the function.

Remark: Often the name Reed-Muller form is used.

Derivation of RSE/RMF

Four ways to derive the RSE/RMF from a Boolean expression:

- Use the definition of the Boolean operations:

$$a \wedge b = a \cdot b$$

$$a \vee b = a \oplus b \oplus ab$$

$$a' = 1 \oplus a$$

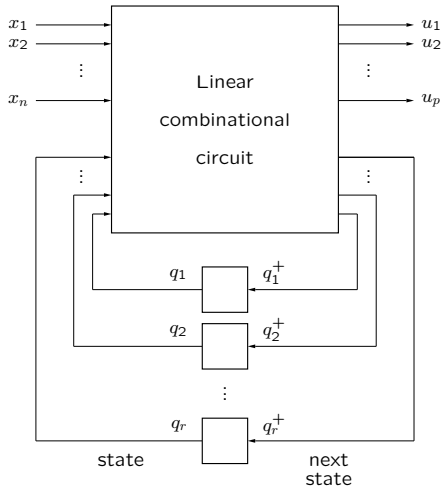
- Use deMorgan's law to get rid of \vee , then use $a' = 1 \oplus a$.
- Write the function in DNF. Then use that

$$m_i \vee m_j = m_i \oplus m_j \oplus \underbrace{m_i \cdot m_j}_{=0, i \neq j} = m_i \oplus m_j$$

and $a' = 1 \oplus a$.

- Reed-Muller transform

Linear sequential circuit



Linear sequential circuit

Linear sequential circuit

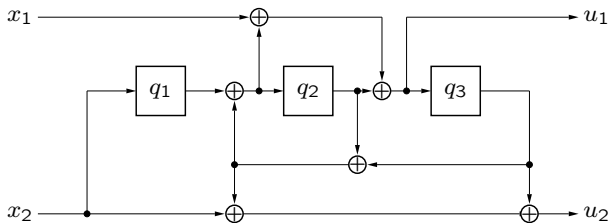
A **linear sequential circuit** is a sequential circuit with only modulo 2 adders and delay elements.

Theorem

A linear sequential circuit can be described by

$$\begin{cases} \mathbf{q}^+ = A\mathbf{q} \oplus B\mathbf{x} \\ \mathbf{u} = C\mathbf{q} \oplus H\mathbf{x} \end{cases}$$

A linear sequential circuit



An example

Example

The equations can be expressed in matrix form as

$$\begin{pmatrix} q_1^+ \\ q_2^+ \\ q_3^+ \end{pmatrix} = \begin{pmatrix} x_2 \\ q_1 \oplus q_2 \oplus q_3 \\ x_1 \oplus q_1 \oplus q_3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} \oplus \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \begin{pmatrix} x_1 \oplus q_1 \oplus q_3 \\ x_2 \oplus q_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \\ q_3 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Hence,

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Rank

Definition (Matrix Rank)

The **rank** of a matrix A is the maximum number of linearly independent rows (or columns) in A .

For an $m \times n$ matrix the rank is bounded by $\text{Rank}(A) \leq \min\{m, n\}$

Inverse matrix

- ▶ if $m = n$ then $\text{Rank}(A) = m \Leftrightarrow A^{-1}$ exists,
 $AA^{-1} = A^{-1}A = I$.
- ▶ if $m < n$ then $\text{Rank}(A) = m \Leftrightarrow A_R^{-1}$ exists,
 $AA_R^{-1} = I$.
- ▶ if $m > n$ then $\text{Rank}(A) = n \Leftrightarrow A_L^{-1}$ exists,
 $A_L^{-1}A = I$.

Derivation of rank

The rank of a matrix A can be derived by Gauss elimination. After elimination the number of **pivot elements** is the rank.

Consider the matrix (over the binary Boolean ring)

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Gauss elimination

$$\rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 & 0 \\ 0 & \textcircled{1} & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} \textcircled{1} & 0 & 1 & 0 \\ 0 & \textcircled{1} & 1 & 0 \\ 0 & 0 & \textcircled{1} & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

The rank is 3.

Remark: The same derivation over the real numbers will give rank 4.

Diagnostic Matrix

Diagnostic Matrix

The **diagnostic matrix** is the $pr \times r$ matrix

$$K = \begin{pmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{r-1} \end{pmatrix}$$

with maximum rank, $\text{Rank}(K) = r$.

If $\text{Rank}(K) < r$, then there are equivalent states.

Theorem (7.4)

Let A , B , C , and H determine a linear sequential circuit where $\text{Rank}(K) = k$. Then, the reduced form is given by

$$A_{\text{red}} = TAR$$

$$B_{\text{red}} = TB$$

$$C_{\text{red}} = CR$$

$$H_{\text{red}} = H$$

where T consists of the first k linearly independent rows of the diagnostic matrix K , and R is a right inverse of T .

The example continued (I)

The diagnostic matrix:

$$K = \begin{pmatrix} C \\ CA \\ CA^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

The rank: $\text{Rank}(K) = 2$. Thus,

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad R = T_R^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

where R is a right inverse of T .

The example continued (II)

How to find the right inverse of T ?

Since the first 2 columns of T are linearly independent we write T as

$$T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = (M \quad N)$$

where M is the first 2 (linearly independent) columns of T , and N is the rest. An inverse of M can be found in

$$M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Since

$$(M \quad N) \begin{pmatrix} M^{-1} \\ 0 \end{pmatrix} = MM^{-1} = I$$

we have found a right inverse in

$$R = \begin{pmatrix} M^{-1} \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

The example continued (III)

The matrices are

$$A_{\text{red}} = TAR = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$B_{\text{red}} = TB = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$$C_{\text{red}} = CR = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

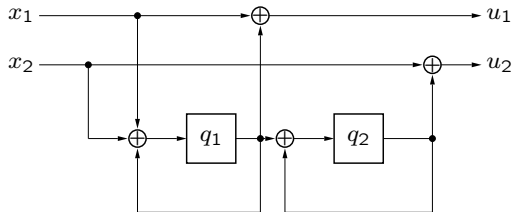
$$H_{\text{red}} = H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hence,

$$\begin{pmatrix} q_1^+ \\ q_2^+ \end{pmatrix} = A_{\text{red}}\mathbf{q} \oplus B_{\text{red}}\mathbf{x} = \begin{pmatrix} q_1 \oplus x_1 \oplus x_2 \\ q_1 \oplus q_2 \end{pmatrix}$$

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = C_{\text{red}}\mathbf{q} \oplus H_{\text{red}}\mathbf{x} = \begin{pmatrix} q_1 \oplus x_1 \\ q_2 \oplus x_2 \end{pmatrix}$$

Reduced form



Definition

The sequence

$$\mathbf{x} = \dots x_{-1} x_0 x_1 x_2 \dots$$

can be represented by

$$x(D) = \dots \oplus x_{-1} D^{-1} \oplus x_0 \oplus x_1 D \oplus x_2 D^2 \oplus \dots = \sum_i x_i D^i$$

where D is a delay operator.

\mathcal{D} -transform (Ex)

Example

Examples of \mathcal{D} -transform

$$\begin{array}{l} \text{▶ } \underset{\substack{\uparrow \\ t=0}}{\mathbf{1}}011010111\dots \xrightarrow{\mathcal{D}} 1 \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^7 \oplus D^8 \oplus D^9 \oplus \dots \end{array}$$

$$\begin{array}{l} \text{▶ } 110\underset{\substack{\uparrow \\ t=0}}{\mathbf{1}}101\dots \xrightarrow{\mathcal{D}} D^{-3} \oplus D^{-2} \oplus 1 \oplus D \oplus D^3 \oplus \dots \\ \qquad \qquad \qquad = D^{-3}(1 \oplus D \oplus D^3 \oplus D^4 \oplus D^6 \oplus \dots) \end{array}$$

$$\text{▶ } D^2 \oplus D^6 \oplus D^7 \oplus D^8 \oplus \dots \xrightarrow{\mathcal{D}^{-1}} \underset{\substack{\uparrow \\ t=0}}{\mathbf{0}}01000111\dots$$

$$D^2(1 \oplus D^4 \oplus D^5 \oplus D^6 \oplus \dots) \xrightarrow{\mathcal{D}^{-1}} \underset{\substack{\uparrow \\ t=2}}{\mathbf{1}}000111\dots$$

\mathcal{D} -transform of periodic sequences

Theorem

The (infinite) periodic sequence

$$\mathbf{s} = [s_0 s_1 \dots s_{T-1}]^\infty = s_0 \dots s_{T-1} s_0 \dots s_{T-1} \dots$$

has the \mathcal{D} -transform

$$s(D) = \frac{P(D)}{1 \oplus D^T}$$

where $P(D)$ is the \mathcal{D} -transform of one period,

$$P(D) = \mathcal{D}(s_0 s_1 \dots s_{T-1})$$

and T the period.

\mathcal{D} -transform of periodic sequences

Proof.

\mathcal{D} -transform of $[s_0 \dots s_{T-1}]^\infty$:

- ▶ 1st position

$$[10 \dots 0]^\infty \xrightarrow{\mathcal{D}} 1 \oplus D^T \oplus D^{2T} \oplus \dots = \frac{1}{1 \oplus D^T}$$

- ▶ $i + 1$ st position

$$[0 \dots 1 \dots 0]^\infty \xrightarrow{\mathcal{D}} D^i \oplus D^{T+i} \oplus D^{2T+i} \oplus \dots = \frac{D^i}{1 \oplus D^T}$$

Super positioning gives

$$\begin{aligned} [s_0 s_1 \dots s_{T-1}]^\infty &\xrightarrow{\mathcal{D}} s_0 \frac{1}{1 \oplus D^T} \oplus \dots \oplus s_{T-1} \frac{D^{T-1}}{1 \oplus D^T} \\ &= \frac{s_0 \oplus s_1 D \oplus \dots \oplus s_{T-1} D^{T-1}}{1 \oplus D^T} \\ &= \frac{\mathcal{D}(s_0 s_1 \dots s_{T-1})}{1 \oplus D^T} \end{aligned}$$



\mathcal{D} -transform of periodic sequences

Example

$$\blacktriangleright [01]^\infty \xrightarrow{\mathcal{D}} \frac{D}{1 \oplus D^2}$$

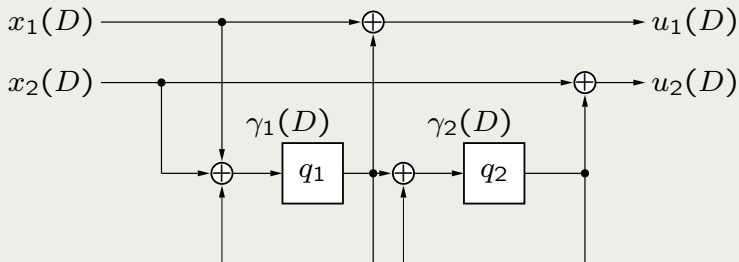
$$\blacktriangleright [110]^\infty \xrightarrow{\mathcal{D}} \frac{1 \oplus D}{1 \oplus D^3} = \frac{1 \oplus D}{(1 \oplus D)(1 \oplus D \oplus D^2)} = \frac{1}{1 \oplus D \oplus D^2}$$

\blacktriangleright

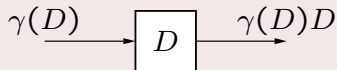
$$\begin{aligned} \overset{\substack{\text{red } 1 \\ \uparrow \\ t=0}}{1} [110]^\infty &\xrightarrow{\mathcal{D}} 1 \oplus D \oplus D^2 \frac{1 \oplus D}{1 \oplus D^3} = \frac{(1 \oplus D)(1 \oplus D^3)}{1 \oplus D^3} \oplus \frac{1 \oplus D}{1 \oplus D^3} \\ &= \frac{1 \oplus D \oplus D^3 \oplus D^4 \oplus D^2 \oplus D^3}{1 \oplus D^3} = \frac{1 \oplus D \oplus D^2 \oplus D^4}{1 \oplus D^3} \\ &= \frac{1 \oplus D^2 \oplus D^3}{1 \oplus D \oplus D^2} \end{aligned}$$

Linear sequential circuit in D -domain

Example: Linear sequential circuit



D-element in D -domain



Relationship between x and u

The state sequences are (all (D) are omitted)

$$\begin{cases} \gamma_1 = x_1 \oplus x_2 \oplus \gamma_1 D \\ \gamma_2 = \gamma_1 D \oplus \gamma_2 D \end{cases} \Rightarrow \begin{cases} \gamma_1 = x_1 \frac{1}{1 \oplus D} \oplus x_2 \frac{1}{1 \oplus D} \\ \gamma_2 = x_1 \frac{D}{1 \oplus D^2} \oplus x_2 \frac{D}{1 \oplus D^2} \end{cases}$$

Insert into the output equations

$$\begin{cases} u_1 = x_1 \oplus \gamma_1 D \\ u_2 = x_2 \oplus \gamma_2 D \end{cases} \Rightarrow \begin{cases} u_1 = x_1 \frac{1}{1 \oplus D} \oplus x_2 \frac{D}{1 \oplus D} \\ u_2 = x_1 \frac{D^2}{1 \oplus D^2} \oplus x_2 \frac{1}{1 \oplus D^2} \end{cases}$$

In matrix form we write

$$\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} = \underbrace{\begin{pmatrix} \frac{1}{1 \oplus D} & \frac{D}{1 \oplus D} \\ \frac{D^2}{1 \oplus D^2} & \frac{1}{1 \oplus D^2} \end{pmatrix}}_{G(D)} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

$G(D)$ describes the relation between inputs and outputs.

Theorem

*The input-output relation in a linear sequential circuit is described by the **transfer function matrix** $G(D)$ as*

$$\mathbf{u}(D) = G(D)\mathbf{x}(D)$$

The transfer function matrix can be derived as

$$G(D) = C(I \oplus AD)^{-1}BD \oplus H$$

$$A, B, C, H \rightarrow G(D)$$

Proof.

A linear sequential circuit is described by

$$\begin{cases} \mathbf{q}^+ = A\mathbf{q} \oplus B\mathbf{x} \\ \mathbf{u} = C\mathbf{q} \oplus H\mathbf{x} \end{cases}$$

Since D is a delay operator we have

$$\mathbf{q} = \mathbf{q}^+ D$$

Hence, in the \mathcal{D} -domain we get

$$\begin{cases} \mathbf{q}^+ = A\mathbf{q}^+ D \oplus B\mathbf{x} \\ \mathbf{u} = C\mathbf{q}^+ D \oplus H\mathbf{x} \end{cases}$$

Rewrite the first equation as

$$(I \oplus AD)\mathbf{q}^+ = B\mathbf{x}$$

or, equivalently

$$\mathbf{q}^+ = (I \oplus AD)^{-1} B\mathbf{x}$$

Insert into the second equation

$$\begin{aligned} \mathbf{u} &= C(I \oplus AD)^{-1} B\mathbf{x} D \oplus H\mathbf{x} \\ &= \underbrace{(C(I \oplus AD)^{-1} BD \oplus H)}_{G(D)} \mathbf{x} \end{aligned}$$



$$A, B, C, H \rightarrow G(D)$$

Example

$$\begin{aligned}
 G(D) &= C (I \oplus AD)^{-1} BD \oplus H \\
 &= C_{\text{red}} (I \oplus A_{\text{red}} D)^{-1} B_{\text{red}} D \oplus H_{\text{red}} \\
 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \oplus \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} D \right)^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} D \oplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \frac{1}{1 \oplus D^2} \begin{pmatrix} 1 \oplus D & 0 \\ D & 1 \oplus D \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} D \oplus \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
 &= \begin{pmatrix} \frac{D(1 \oplus D)}{1 \oplus D^2} \oplus 1 & \frac{D(1 \oplus D)}{1 \oplus D^2} \\ \frac{D^2}{1 \oplus D^2} & \frac{D^2}{1 \oplus D^2} \oplus 1 \end{pmatrix} \\
 &= \begin{pmatrix} \frac{1 \oplus D}{1 \oplus D^2} & \frac{D \oplus D^2}{1 \oplus D^2} \\ \frac{D^2}{1 \oplus D^2} & \frac{1}{1 \oplus D^2} \end{pmatrix} = \begin{pmatrix} \frac{1}{1 \oplus D} & \frac{D}{1 \oplus D} \\ \frac{D^2}{1 \oplus D^2} & \frac{1}{1 \oplus D^2} \end{pmatrix}
 \end{aligned}$$