Digitalteknik EITF65

Lecture 13: Linear Sequential Circuits, Part 1

August 27, 2020

Linear Boolean functions

Definition (Linearity)

A function f is said to be linear if

$$f(\mathbf{x} \oplus \mathbf{y}) = f(\mathbf{x}) \oplus f(\mathbf{y}) \qquad (L_1)$$

$$f(\alpha \mathbf{x}) = \alpha f(\mathbf{x}) \qquad (L_2)$$

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.

Linear Boolean functions

Theorem

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

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

$$= \begin{pmatrix} a_1 \dots a_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \mathbf{ax} \qquad a_i \in \{0, 1\}$$

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

Linear Boolean functions

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.

RSE/RMF

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 $(\vee, \wedge, ')$.

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

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

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

RSE/RMF

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.

RSE/RMF

Derivation of RSE/RMF

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

- Use the definition of the Boolean operations:

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

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

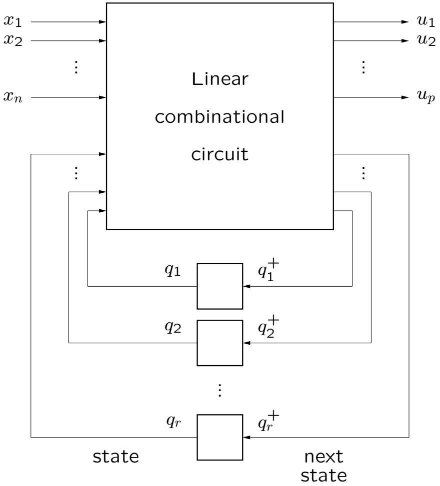
$$a' = 1 \oplus a$$

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

$$m_\mathbf{i} \vee m_\mathbf{j} = m_\mathbf{i} \oplus m_\mathbf{j} \oplus \underbrace{m_\mathbf{i} \cdot m_\mathbf{j}}_{=0,\ i \neq j} = m_\mathbf{i} \oplus m_\mathbf{j}$$

  and $a' = 1 \oplus a$.
- Reed-Muller transform

Linear sequential circuit



Linear sequential circuit

Linear sequential circuit

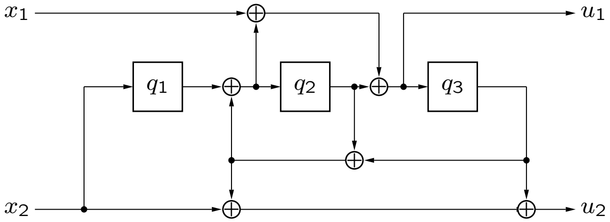
A linear sequential circuit is a sequential circuit with only modulo 2 adders and delay elements.

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 $\mathrm{Rank}(A) \leq \min\{m, n\}$

Inverse matrix

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

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

Reduced form

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: $\mathrm{Rank}(K) = 2$. 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

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

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

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

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)

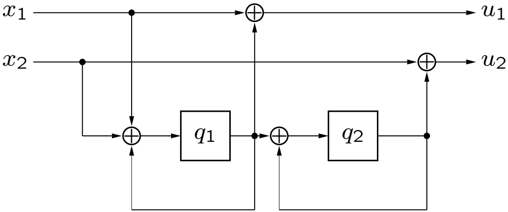
The matrices are

$$A_{\text{red}} = TAR = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
$$B_{\text{red}} = TB = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$
$$C_{\text{red}} = CR = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$H_{\text{red}} = H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

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



$\mathcal{D}$-transform

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

- $$\underset{\substack{\uparrow \\ t=0}}{1}011010111\ldots \xrightarrow{\mathcal{D}} 1 \oplus D^2 \oplus D^3 \oplus D^5 \oplus D^7 \oplus D^8 \oplus D^9 \oplus \cdots$$
- $$110\underset{\substack{\uparrow \\ t=0}}{1}101\ldots \xrightarrow{\mathcal{D}} D^{-3} \oplus D^{-2} \oplus 1 \oplus D \oplus D^3 \oplus \cdots$$
  $$= D^{-3}(1 \oplus D \oplus D^3 \oplus D^4 \oplus D^6 \oplus \cdots)$$
- $$D^2 \oplus D^6 \oplus D^7 \oplus D^8 \oplus \cdots \xrightarrow{\mathcal{D}^{-1}} \underset{\substack{\uparrow \\ t=0}}{0}01000111\cdots$$
  $$D^2(1 \oplus D^4 \oplus D^5 \oplus D^6 \oplus \cdots) \xrightarrow{\mathcal{D}^{-1}} \underset{\substack{\uparrow \\ t=2}}{1}000111\cdots$$

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

- 1st position

  $$[10\ldots0]^\infty \xrightarrow{\mathcal{D}} 1 \oplus D^T \oplus D^{2T} \oplus \cdots = \frac{1}{1 \oplus D^T}$$

- $i + 1$st position

  $$[0\ldots1\ldots0]^\infty \xrightarrow{\mathcal{D}} D^i \oplus D^{T+i} \oplus D^{2T+i} \oplus \cdots = \frac{D^i}{1 \oplus D^T}$$

Super positioning gives

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

□

$\mathcal{D}$-transform of periodic sequences

Example

- $[01]^\infty \xrightarrow{\mathcal{D}} \dfrac{D}{1 \oplus D^2}$
- $[110]^\infty \xrightarrow{\mathcal{D}} \dfrac{1 \oplus D}{1 \oplus D^3} = \dfrac{1 \oplus D}{(1 \oplus D)(1 \oplus D \oplus D^2)} = \dfrac{1}{1 \oplus D \oplus D^2}$
- $$\underset{\substack{\uparrow \\ t=0}}{1}1[110]^\infty \xrightarrow{\mathcal{D}} 1 \oplus D \oplus D^2 \frac{1 \oplus D}{1 \oplus D^3} = \frac{(1 \oplus D)(1 \oplus D^3)}{1 \oplus D^3} \oplus D^2 \frac{1 \oplus D}{1 \oplus D^3}$$
  $$= \frac{1 \oplus D \oplus D^3 \oplus D^4 \oplus D^2 \oplus D^3}{1 \oplus D^3} = \frac{1 \oplus D \oplus D^2 \oplus D^4}{1 \oplus D^3}$$
  $$= \frac{1 \oplus D^2 \oplus D^3}{1 \oplus D \oplus D^2}$$