

# Cascade Realizations of Two-valued Input Multiple-Valued Output Functions using Decomposition of Group Functions

Tsutomu Sasao

*Department of Computer Science and Electronics*

*Kyushu Institute of Technology,*

*Iizuka 820-8502, Japan*

## Abstract

*This paper considers a method to realize a two-valued input three-valued output function  $f : \{0, 1\}^n \rightarrow \{0, 1, 2\}$  by using a cascade of four-input cells. Decomposition of a group function is used to find a canonical form. We show that the Walsh spectrum specifies the canonical form, and the number of non-zero coefficients in the spectrum is proportional to the number of cells in the cascade. Finally, we show an extension to  $p$ -valued function  $f : \{0, 1\}^n \rightarrow \{0, 1, \dots, p-1\}$ . The designed cascades are reversible and conservative.*

## 1. Introduction

Recently, cascade realizations of logic functions receive attention for the following reasons:

The first reason is the DSM (Deep Sub-Micron) problems caused by lateral capacitance coupling between wires, inductance effect, and manufacturing variations. These make custom design of LSI very expensive and time consuming [3]. To solve these DSM problems, programmable cascade realizations have been developed [13].

The second one is the power dissipation problem. With the increase of the number of gates per chip, according to Moore's law, current standard CMOS technology will dissipate too much energy in a chip. Because of economic, ecological, and ethical reasons, we have to find a novel approach that dissipates drastically lower power than before. Reversible logic gives theoretical support to design circuits without loss of information, and consequently, without energy loss [1, 2, 5]. An  $n$ -input  $n$ -output circuit is *reversible* if there is a one-to-one correspondence between its input vectors and output vectors, that is, there is a distinct output vector for each input vector. An important restriction in the reversible logic circuits is that *each gate has exactly one fanout*. Thus, the design of cascades becomes very important [6, 8]. Conservative logic is another model for low power circuit [9, 5]. A circuit is *conservative* if the number of 1's in each input is equal to the number of 1's in the corresponding output [9].

Cascade can be classified into two classes: two-rail cascades, and multi-rail cascades [14]. Maitra [7] considered single-rail cascades of two-input cells. Unfortunately, single-rail cascades realize only a small fraction of two-valued logic functions. Short [15] showed that any logic function can be realized as a two-rail cascade of three-input cells. Yoeli-Turner [17] showed a design method for multi-rail cascades [4].

In this paper, we show a method to design two-valued input three-valued output functions by using a three-rail cascade of reversible and conservative logic elements. In the design of logic circuits, sum-of-products expressions (SOPs), exclusive-OR sum-of-products expression (ESOPs), and binary decision diagrams (BDDs) are extensively used. They are useful representations of logic functions [10, 11, 12]. In this paper, however, we will use *group function* as a basic tool to design cascades.

In Section 2, we survey the group theory. In Section 3, we introduce a group function, and its decomposition theory. We show that the canonical form of the cascade can be derived from the Walsh spectrum of the given function. In Section 4, we consider the complexity of the cascades and show some statistical data. In Section 5, we extend the theory to implement two-valued input  $p$ -valued output functions and show the sizes of cascades for an  $n$ -bit adder and an  $n$ -bit multiplier. In Section 6, we summarize the paper.

In this paper, we use the theory of finite groups and linear algebra in addition to Boolean algebra. The method is illustrated with numerous examples.

## 2. Group Theory

In this part, we will survey the group theory, which will be used in this paper.

**Definition 2.1** A group  $\langle G, \cdot, I \rangle$  is an algebraic system satisfying the following axioms:

*M0:* For any  $a, b \in G$ ,  $a \cdot b \in G$ .

*M1:* For any  $a, b, c \in G$ ,  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .

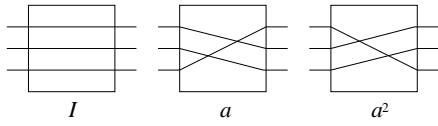


Figure 2.1. Elements of  $C_3$ .



Figure 2.2. Relations of elements.

M2: For any  $a \in G$ , a unique element  $I$  exists such that  $a \cdot I = I \cdot a = a$ .

M3: For any  $a \in G$ , an element  $b$  exists such that  $a \cdot b = b \cdot a = I$ .

The element  $b$  is the **inverse** of  $a$ , and denoted by  $a^{-1}$ .

A group is **Abelian** if it satisfies

M4: For any  $a, b \in G$ ,  $a \cdot b = b \cdot a$ .

We usually omit the operator “ $\cdot$ ”.

**Definition 2.2** A group is a **cyclic group** if every element in the group is a power of some fixed element  $a$  in  $G$ .

**Definition 2.3** A group that consists of all the permutations of  $n$  elements is a **symmetric group of degree  $n$** .

**Example 2.1** Fig. 2.1 shows  $C_3 = \{I, a, a^2\}$ , a set of three permutations, where  $I$  is the identity permutation,  $a$  is the single shifting permutation, and  $a^2$  is the double shifting permutation.  $C_3$  forms a **cyclic group of order three**. The product operation is the composition of the permutations.  $C_3$  is an **Abelian group**. Fig. 2.2(a) shows the relations of elements. Note that  $a^3 = I$ , and  $a^2 = a^{-1}$ . (End of Example)

**Example 2.2** Fig. 2.3 shows  $C_2 = \{I, g\}$ , a set of two permutations, where  $g$  swaps the lower two rails.  $C_2$  forms a **cyclic group of order two**.  $C_2$  forms an **Abelian group**. Fig. 2.2(b) shows the relations of elements. Note that  $g^2 = I$ , and  $g = g^{-1}$ . (End of Example)

**Example 2.3** Fig. 2.4 shows  $S_3 = \{I, a, a^2, g, ag, ga\}$ , which corresponds to all possible permutations of three rails.  $S_3$  has  $3! = 6$  elements, and forms the **symmetric group of degree three**. Note that  $S_3$  is a **non-Abelian group** since  $ag \neq ga$ .

Fig. 2.5 shows the relations of elements in  $S_3$ .  $S_3$  is a direct product of  $C_3$  and  $C_2$ :  $S_3 = C_3 \times C_2 = \{I, a, a^2\} \times \{I, g\} = \{I, a, a^2, g, ag, ga\}$ . Also, from Fig. 2.5, we see that  $gag = a^{-1}$ , and  $ga^{-1}g = a$  hold. (End of Example)

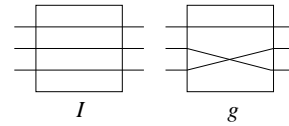


Figure 2.3. Elements of  $C_2$ .

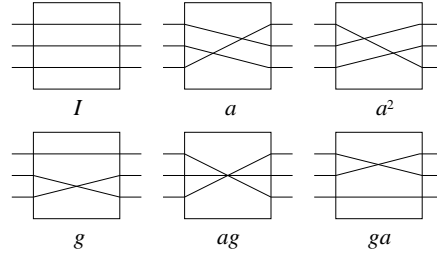


Figure 2.4. Elements of  $S_3$ .

### 3. Group Functions

In this part, we introduce a group function, which is an important tool to design multi-rail cascade.

#### 3.1. Group Functions

**Definition 3.1** Let  $G$  be a group, and  $B = \{0, 1\}$ .  $F : B^n \rightarrow G$ , is a **group function**.

**Example 3.1** Consider a group function  $F : B^n \rightarrow C_3$ , where  $C_3 = \{I, a, a^2\}$ . Note that the output of the group function  $F$  assumes the value equal to one of the three permutations in Fig. 2.1. (End of Example)

A group function can realize a three-valued function.

**Example 3.2** Consider a group function  $F : B^n \rightarrow C_3$ , and a three-valued function  $f : B^n \rightarrow \{0, 1, 2\}$ . By using a group function, we can realize a three-valued function as shown in Fig. 3.1. When the constants 0, 2, and 1 are connected to the left side of the permutation, the top output  $f_0$  realizes the following function:  $f_0 = 0$  when  $F = I$ ,  $f_0 = 1$  when  $F = a$ , and  $f_0 = 2$  when  $F = a^2$ . (End of Example)

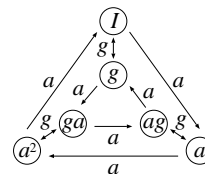
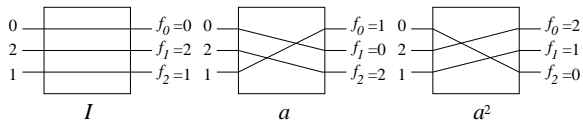
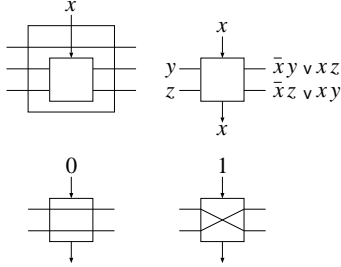


Figure 2.5. Relations of elements in  $S_3$ .



**Figure 3.1. Realization of three-valued function.**



**Figure 3.2. Hardware for  $g^x$ .**

### 3.2. Decomposition of Group Functions

**Theorem 3.1** A group function  $F(X) : B^n \rightarrow C_3$  is decomposable as follow:

$$F(\hat{X}, x_n) = F_a(\hat{X})g^{x_n} F_b(\hat{X})g^{x_n}, \quad (3.1)$$

where  $x_n$  denotes a variable, and  $F_a(\hat{X})$  and  $F_b(\hat{X})$  denote group functions that do not depend on  $x_n$ .

A proof can be found in [17].

The expansion (3.1) is essential in the design of cascades, and corresponds to the Shannon expansion in a logic function. Fig. 3.2 shows hardware to implement  $g^x$ . When  $x = 0$ ,  $g^x$  represents the identical permutation. When  $x = 1$ ,  $g^x$  swaps the two lower rails.

**Lemma 3.1** Let  $g \in C_2$ , and  $F$  be a group function  $B^n \rightarrow C_3$ . Then,  $gFg = F^{-1}$ .

From (3.1), we have

$$F(\hat{X}, 0) = F_a(\hat{X})g^0 F_b(\hat{X})g^0, \text{ and}$$

$$F(\hat{X}, 1) = F_a(\hat{X})g^1 F_b(\hat{X})g^1.$$

Let

$$F(\hat{X}, x_n) = \alpha^{f(\hat{X}, x_n)},$$

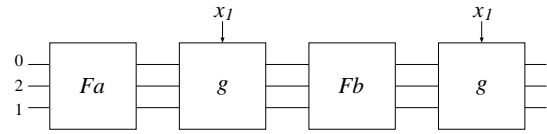
$$F_a(\hat{X}) = \alpha^{f_a(\hat{X})}, \text{ and}$$

$$F_b(\hat{X}) = \alpha^{f_b(\hat{X})}.$$

From these relations, we have

$$\alpha^{f(\hat{X}, 0)} = \alpha^{f_a(\hat{X}) + f_b(\hat{X})}, \text{ and}$$

$$\alpha^{f(\hat{X}, 1)} = \alpha^{f_a(\hat{X}) - f_b(\hat{X})}.$$



**Figure 3.3. Canonical Cascade for one-variable function.**

Therefore, we have

$$f(\hat{X}, 0) = f_a(\hat{X}) + f_b(\hat{X}) \pmod{3}, \text{ and}$$

$$f(\hat{X}, 1) = f_a(\hat{X}) - f_b(\hat{X}) \pmod{3}.$$

By using a matrix notation, we have

$$\begin{bmatrix} f(\hat{X}, 0) \\ f(\hat{X}, 1) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f_a(\hat{X}) \\ f_b(\hat{X}) \end{bmatrix} \pmod{3}.$$

Note that

$$W_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \pmod{3}$$

is the **Walsh matrix** of one variable. Since,

$$W_1^2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = 2 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = -I_1 \pmod{3},$$

we have  $W_1^{-1} \equiv -W_1 \pmod{3}$ .

### 3.3. One-Variable Case

For a one-variable function, the canonical form for the group function is written as  $\alpha^{f(x_1)} = \alpha^{w_a} g^{x_1} \alpha^{w_b} g^{x_1}$ . Fig. 3.3 shows the canonical cascade of one-variable function. It consists of four cells. By setting  $x$  to 0 and 1, we have  $\alpha^{f(0)} = \alpha^{w_a} g^0 \alpha^{w_b} g^0 = \alpha^{w_a + w_b}$ , and  $\alpha^{f(1)} = \alpha^{w_a} g^1 \alpha^{w_b} g^1 = \alpha^{w_a - w_b}$ . Thus, we have

$$\begin{bmatrix} f(0) \\ f(1) \end{bmatrix} = \begin{bmatrix} f_0 \\ f_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} w_a \\ w_b \end{bmatrix} \pmod{3}.$$

Since  $W_1^{-1} \equiv -W_1 \pmod{3}$ , we have

$$\begin{bmatrix} w_a \\ w_b \end{bmatrix} = - \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f_0 \\ f_1 \end{bmatrix}.$$

$\vec{w} = (w_a, w_b)^t$  is the vector representing the canonical form of the cascade.

**Example 3.3** Consider the one-variable function  $f(x_1) = x_1$ . In this case,  $f_0 = 0$  and  $f_1 = 1$ , thus, we have  $w_a = -1$  and  $w_b = 1$ . So,  $F(x)$  is written as  $F(x) = \alpha^{-1} g^{x_1} \alpha g^{x_1}$ . Fig. 3.4 shows the canonical cascade. Since the last cell is not utilized to the function, the cascade can be simplified to Fig. 3.5. (End of Example)

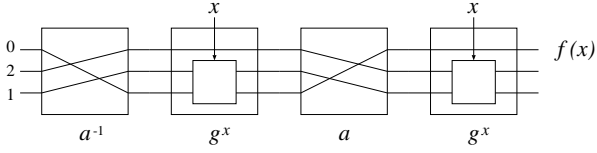


Figure 3.4. Canonical cascade for  $f(x) = x$ .

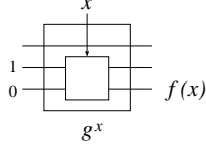


Figure 3.5. Simplified cascade for  $f(x) = x$ .

### 3.4. Two-Variable Case

In this part, we will derive the canonical form for two-variable functions. From (3.1), we have  $F(x_1, x_2) = F_a(x_2)g^{x_1}F_b(x_2)g^{x_1}$ . Thus,  $F(x_1, x_2)$  can be realized by a cascade shown in Fig. 3.6. Since  $F_a$  and  $F_b$  are group functions of one variable, we have the canonical cascade shown in Fig. 3.7. Note that it consists of 10 cells. The canonical form of two-variable function is written as

$$\begin{aligned} a^{f(x_1, x_2)} &= a^{w_a}g^{x_2}a^{w_b}g^{x_2}g^{x_1}a^{w_c}g^{x_2}a^{w_d}g^{x_2}g^{x_1} \\ &= a^{w_a}g^{x_2}a^{w_b}g^{x_1 \oplus x_2}a^{w_c}g^{x_2}a^{w_d}g^{x_1 \oplus x_2}. \end{aligned}$$

By assigning 0 and 1 to  $x_1$  and  $x_2$ , we have the following four equations:

$$\begin{aligned} f(0, 0) &= f_0 = w_a + w_b + w_c + w_d \\ f(0, 1) &= f_1 = w_a - w_b + w_c - w_d \pmod{3} \\ f(1, 0) &= f_2 = w_a + w_b - w_c - w_d \\ f(1, 1) &= f_3 = w_a - w_b - w_c + w_d \end{aligned}$$

In the matrix form, they are represented as

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} w_a \\ w_b \\ w_c \\ w_d \end{bmatrix} \pmod{3}.$$

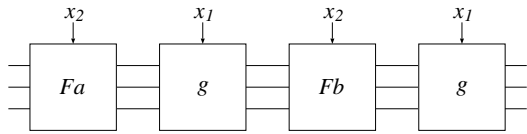


Figure 3.6. Cascade realization of two-variable function.

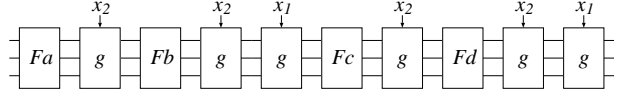


Figure 3.7. Canonical cascade for two-variable function.

Note that

$$W_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

is the Walsh matrix of two variables. Since,

$$W_2^2 = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix} = 4 \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \equiv I_2 \pmod{3}.$$

We have  $W_2 \equiv W_2^{-1} \pmod{3}$ . Thus,  $W_2$  is a *self-inverse matrix*. The vector representing the canonical form is  $\vec{w} = (w_a, w_b, w_c, w_d)^t \equiv W_2 \cdot \vec{F} \pmod{3}$ , where  $\vec{F} = (f_0, f_1, f_2, f_3)^t$ . In this case,  $\vec{w}$  is equal to the Walsh spectrum of  $\vec{F}$ .

**Example 3.4** Consider the two-variable function  $f(x_1, x_2) = x_1 \oplus x_2$ . In this case,  $\vec{F} = (f_0, f_1, f_2, f_3)^t = (0, 1, 1, 0)^t$ . Since,

$$W_2 \cdot \vec{F} = \begin{bmatrix} 2 \\ 0 \\ 0 \\ -2 \end{bmatrix} \equiv \begin{bmatrix} -1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} w_a \\ w_b \\ w_c \\ w_d \end{bmatrix} \pmod{3},$$

we have

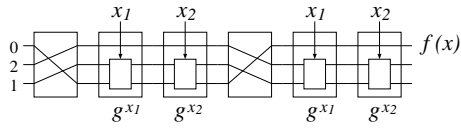
$$\begin{aligned} F &= a^{-1}g^{x_2}a^0g^{x_1 \oplus x_2}a^0g^{x_2}a^1g^{x_1 \oplus x_2} \\ &= a^{-1}g^{x_2 \oplus x_1 \oplus x_2 \oplus x_2}a^1g^{x_1 \oplus x_2} \\ &= a^{-1}g^{x_1 \oplus x_2}a^1g^{x_1 \oplus x_2}. \end{aligned}$$

Fig. 3.8(a) shows the cascade for  $f(x_1, x_2) = x_1 \oplus x_2$ , and Fig. 3.8(b) shows the simplified one. (End of Example)

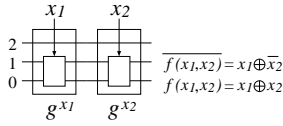
**Example 3.5** Consider the two-variable function  $f(x_1, x_2) = x_1x_2$ . In this case,  $\vec{F} = (f_0, f_1, f_2, f_3)^t = (0, 0, 0, 1)^t$ . Similarly, we have  $\vec{w} = (w_a, w_b, w_c, w_d)^t = (1, -1, -1, 1)^t$ . The canonical form is

$$F = ag^{x_2}a^{-1}g^{x_1 \oplus x_2}a^{-1}g^{x_1}ag^{x_1 \oplus x_2}.$$

Fig. 3.9(a) shows the simplified cascade for  $f(x_1, x_2) = x_1x_2$ . Since the function takes only two values, the constant 2 can be replaced by the constant 0. In this case, the left most cell can be removed, and we have Fig. 3.9(b), which has only three cells. (End of Example)

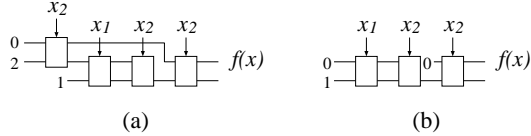


(a) Cascade for  $f(x_1, x_2) = x_1 \oplus x_2$ .



(b) Simplified cascade for  $f(x_1, x_2) = x_1 \oplus x_2$ .

**Figure 3.8.**



**Figure 3.9.** Cascades for  $f(x_1, x_2) = x_1x_2$ .

### 3.5. Three-Variable Cases

The canonical form for a three-variable function  $f(x_1, x_2, x_3)$  is given by

$$a^f(x_1, x_2, x_3) = a^{w_a} g^{x_3} a^{w_b} g^{x_2 \oplus x_3} a^{w_c} g^{x_3} a^{w_d} g^{x_1 \oplus x_2 \oplus x_3} a^{w_e} g^{x_3} a^{w_f} g^{x_2 \oplus x_3} a^{w_g} g^{x_3} a^{w_h} g^{x_1 \oplus x_2 \oplus x_3}.$$

From this, we have  $\vec{F} = W_3 \vec{w}$ , where  $\vec{F} = (f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)^t$ ,  $\vec{w} = (w_a, w_b, w_c, w_d, w_e, w_f, w_g, w_h)^t$ , and

$$W_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

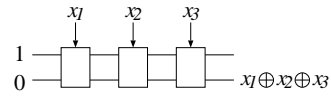
$W_3$  is the Walsh matrix of three variables. Since  $W_3^2 = 2^3 I_3 \equiv -I_3 \pmod{3}$ , we have  $W_3^{-1} \equiv -W_3 \pmod{3}$ . Thus,  $\vec{w} = -W_3 \cdot \vec{F}$ .

**Example 3.6** Consider the function  $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ . Note that  $\vec{F} = (0, 1, 1, 0, 1, 0, 0, 1)^t$ , and

$$\begin{aligned} W_3 \vec{F} &= (4, 0, 0, 0, 0, 0, 0, -4)^t \\ &\equiv (1, 0, 0, 0, 0, 0, 0, -1)^t \pmod{3}. \end{aligned}$$

The vector representing the canonical form is

$$\vec{w} = -W_3 \vec{F} = (-1, 0, 0, 0, 0, 0, 0, 1)^t \pmod{3}.$$



**Figure 3.10.** Simplified cascade for  $x_1 \oplus x_2 \oplus x_3$ .

**Table 3.1.**  $f = x_1 + x_2 + x_3 \pmod{3}$ .

$x_1$	$x_2$	$x_3$	$f$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	2
1	0	0	1
1	0	1	2
1	1	0	2
1	1	1	0

The group function is

$$\begin{aligned} F(x_1, x_2, x_3) &= a^{-1} g^{x_3} a^0 g^{x_2 \oplus x_3} a^0 g^{x_3} a^0 g^{x_1 \oplus x_2 \oplus x_3} \\ &= a^0 g^{x_3} a^0 g^{x_2 \oplus x_3} a^0 g^{x_3} a^1 g^{x_1 \oplus x_2 \oplus x_3} \\ &= a^{-1} g^{x_1 \oplus x_2 \oplus x_3} a g^{x_1 \oplus x_2 \oplus x_3}. \end{aligned}$$

Fig. 3.10 shows the simplified cascade for  $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$ . (End of Example)

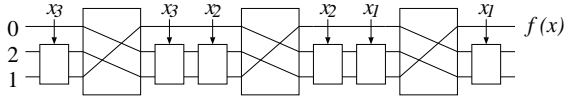
**Example 3.7** Consider the function  $f(x_1, x_2, x_3) = x_1 + x_2 + x_3 \pmod{3}$ . Table 3.1 shows the function table of the three-valued function, and the operator “+” denotes the integer addition of mod 3. Note that  $\vec{F} = (0, 1, 1, 2, 1, 2, 2, 0)^t$ .  $W_3 \vec{F} = (0, -1, -1, 0, -1, 0, 0, 0)^t$ , and the vector representing the canonical form is  $\vec{w} = (0, 1, 1, 0, 1, 0, 0, 0)^t$ . The group function is

$$\begin{aligned} F(x_1, x_2, x_3) &= a^0 g^{x_3} a^1 g^{x_2 \oplus x_3} a^1 g^{x_3} a^0 g^{x_1 \oplus x_2 \oplus x_3} \\ &= a^1 g^{x_3} a^0 g^{x_2 \oplus x_3} a^0 g^{x_3} a^0 g^{x_1 \oplus x_2 \oplus x_3} \\ &= g^{x_3} a g^{x_2 \oplus x_3} a g^{x_1 \oplus x_2} a g^{x_1}. \end{aligned}$$

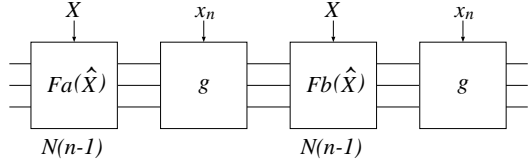
Fig. 3.11 shows the simplified cascade for  $f(x_1, x_2, x_3) = x_1 + x_2 + x_3 \pmod{3}$ . Note that the last two gates can also be removed. (End of Example)

### 3.6. n-Variable Case

**Theorem 3.2** Let  $\vec{F}$  be the truth vector for a function  $f : B^n \rightarrow \{0, 1, 2\}$ . The vector representing the canonical form of the cascade is  $\vec{w} = (-1)^n W_n \vec{F} \pmod{3}$ , where  $W_n$  is the Walsh matrix of  $n$  variables.



**Figure 3.11.** Simplified cascade for  $x_1 + x_2 + x_3 \pmod{3}$ .



**Figure 4.1.** Realization of  $n$ -variable function.

**(Proof)** Note that  $W_n^2 = 2^n I_n$ . When  $n$  is an odd number, i.e.,  $n = 2r + 1$ . We have  $2^n = 2^{2r+1} = 4^r \times 2$ . Since  $4^r = (3 + 1)^r \equiv 1 \pmod{3}$ , we have  $2^n \equiv 2 \equiv -1 \pmod{3}$ . Similarly, when  $n$  is an even number, i.e.,  $n = 2r$ , we have  $2^n = 2^{2r} = 4^r$ . Thus,  $2^n \equiv 1 \pmod{3}$ . (Q.E.D)

$W_n \vec{F}$  is the **Walsh spectrum** [16] of  $f$ . Thus, the canonical form of the cascade for  $f : B^n \rightarrow \{0, 1, 2\}$  can be obtained from the Walsh spectrum of  $f$ .

## 4. Complexity of Cascades

In this part, we will consider the number of cells to realize an  $n$ -variable function by a cascade.

### 4.1. Upper Bounds on the Number of Cells

**Theorem 4.1** Let  $N(n)$  be the number of cells in the canonical cascade for an  $n$ -variable function  $f : B^n \rightarrow \{0, 1, 2\}$ . Then,  $N(n) = 3 \cdot 2^n - 2$ .

**(Proof)** As shown in Fig. 3.1, we can realize a constant function by using one cell, so  $N(0) = 1$ . As shown in Fig. 3.3, we can realize a one-variable function by using four cells, so  $N(1) = 4$ . As shown in Fig. 4.1, we can realize an  $n$ -variable function by using a pair of  $(n-1)$ -variable cascades and two  $g^x$  cells. Thus, we have the recurrence relation:  $N(n) = 2N(n-1) + 2$ . By solving this recurrence relation, we have  $N(n) = 3 \cdot 2^n - 2$ . (Q.E.D)

### 4.2. Actual Size of Cascades

As shown in Theorem 3.1, any function can be decomposed as  $F(\hat{X}, x_n) = F_a(\hat{X})g^{x_n}F_b(\hat{X})g^{x_n}$ . If  $F_b = a^0 = I$ , then  $F(\hat{X}, x_n) = F_a(\hat{X})g^{x_n}g^{x_n} = F_a(\hat{X})$ . Therefore, except for the first coefficient, a zero coefficient in the Walsh spectrum implies that three cells can be removed

**Table 4.1.** Average number of zero coefficients in the spectrum for  $n$ -variable functions.

$n$	Zeros coefficients		$2^n/3$
	Two-valued	Three-valued	
5	10.8	9.0	11
6	19.7	21.9	21
7	39.3	43.3	43
8	84.8	84.4	85
9	163.8	171.2	171
10	348.5	337.7	341
11	684.6	675.3	683
12	1369.4	1398.3	1365
13	2712.6	2722.9	2731
14	5460.8	5465.2	5461

from the canonical cascade. Thus, functions with fewer non-zero coefficients tend to have shorter cascades. Also,  $n$  rightmost cells are not used to realize the function (see, for example, Fig. 3.8(a)). Thus, at least  $n$  cells can be removed.

## 4.3. Experimental Results

We generated 10 random two-valued functions of  $n$  variables, where  $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$ . That is, functions produce value 0 for  $2^{n-1}$  combinations, and 1 for  $2^{n-1}$  combinations. Then, we obtained the Walsh spectrum for them. In Table 4.1, the column for *Two-valued* shows the average number of zero coefficients in the spectrum. From the table, we can see that the number of zero coefficients in the spectrum is near to  $2^n/3$ .

We did the similar experiments for three-valued output functions. In this case, we generated random functions such that  $|f^{-1}(0)| = |f^{-1}(1)| \simeq |f^{-1}(2)| \simeq 2^{n-1}/3$ . In Table 4.1, the column for *Three-valued* shows the average number of zero coefficients in the spectrum. The result is similar to the case of two-valued functions. That is, the average number of zero coefficients is near to  $2^n/3$ .

The number of cells in the canonical cascade is about  $3 \cdot 2^n$ , and there are about  $2^n/3$  zero-coefficients. Also, for each zero-coefficient, we can remove three cells. Thus, we have the following:

**Conjecture 4.1** The average number of cells in cascades for  $n$ -variable randomly generated functions is about  $2^{n+1}$ .

## 5. Extension to $p$ -valued Functions

In the previous sections, we showed a method to realize a three-valued function  $f : B^n \rightarrow \{0, 1, 2\}$ .

In this part, we will extend the method to realize a  $p$ -valued function, where  $p$  is a prime number. Let  $C_p = \{I, a, a^2, a^3, \dots, a^{p-1}\}$  be a cyclic group of order  $p$ , where

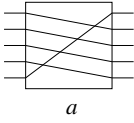


Figure 5.1.  $a$  in  $C_5$ .

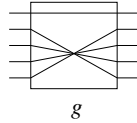


Figure 5.2.  $g$  in  $C_5$ .

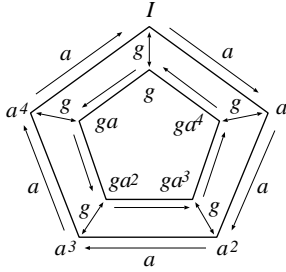


Figure 5.3. Relations of elements in  $D_5$ .

the element  $a$  permutes the  $i$ -th rail into  $(i+1)$ -th (mod  $p$ ) rail. Also, let  $C_2 = \{I, g\}$  be a cyclic group of order 2, where  $g$  swaps the  $i$ -th rail with the  $(p-i)$ -th rail when  $i \neq 0$ .

**Theorem 5.1** A group function  $F(x) : B^n \rightarrow C_p$  is decomposable as follows:

$$F(\hat{X}, x_n) = F_a(\hat{X})g^{x_n} F_b(\hat{X})g^{x_n}, \quad (5.1)$$

where  $x_n$  denotes a variable, and  $F_a(\hat{X})$  and  $F_b(\hat{X})$  denote group functions that do not depend on  $x_n$ .

**Example 5.1** When  $p = 5$ , let  $a$  and  $g$  be permutations shown in Fig. 5.1 and Fig. 5.2, respectively. Then,  $C_5 = \{I, a, a^2, a^3, a^4\}$  forms a cyclic group of order five, and  $C_2 = \{I, g\}$  forms a cyclic group of order two. Also,  $D_5 = C_5 \times C_2$  forms a dihedral group of order 10. Fig. 5.3 show the relations of elements in  $D_5$ . It is easy to verify that  $ga = a^{-1}$ . (End of Example)

Similarly to the case of  $p = 3$ , we have the following relation:

$$\begin{bmatrix} f(\hat{X}, 0) \\ f(\hat{X}, 1) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} f_a(\hat{X}) \\ f_b(\hat{X}) \end{bmatrix} \pmod{p},$$

where

$$F(\hat{X}, x_n) = a^{f(\hat{X}, x_n)}, \\ F_a(\hat{X}) = a^{f_a(\hat{X})}, \text{ and } F_b(\hat{X}) = a^{f_b(\hat{X})}.$$

**Theorem 5.2** Let  $\vec{F}$  be the function vector for  $f : B^n \rightarrow \{0, 1, 2, \dots, p-1\}$ , where  $p$  is a prime number. Then,  $f$  can be realized as a cascade of elements in  $C_p$  and  $g$ . The coefficients for the canonical form of the cascade are equal to the Walsh spectrum  $2^{-n} W_n \vec{F} \pmod{p}$ .

Table 5.1. Table for two-bit adder.

$x_4$	$x_3$	$x_2$	$x_1$	$f$	$x_4$	$x_3$	$x_2$	$x_1$	$f$
0	0	0	0	0	1	0	0	0	2
0	0	0	1	1	1	0	0	1	3
0	0	1	0	2	1	0	1	0	4
0	0	1	1	3	1	0	1	1	5
0	1	0	0	1	1	1	0	0	3
0	1	0	1	2	1	1	0	1	4
0	1	1	0	3	1	1	1	0	5
0	1	1	1	4	1	1	1	1	6

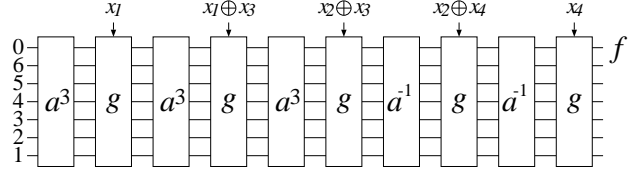


Figure 5.4. Cascade for a two-bit adder.

**Example 5.2** Consider a two-bit adder shown in Table 5.1. It has four inputs and one output, and computes  $f = 2(x_4 + x_2) + (x_3 + x_1)$ . Since,  $f$  is a seven-valued function, we realize  $f$  by using a group function  $B^4 \rightarrow C_7$ .

Note that  $W_7^2 = 2^7 I_7$ , and  $2^7 \equiv 2 \pmod{7}$ . We have  $W_7^{-1} \equiv \frac{1}{2} W_7 \pmod{7}$ .

The function vector is  $\vec{F} = (0, 1, 2, 3; 1, 2, 3, 4; 2, 3, 4, 5; 3, 4, 5, 6)^t$ , and the Walsh spectrum is  $(48, -8, -16, 0; -8, 0, 0, 0; -16, 0, 0, 0; 0, 0, 0, 0)^t$ . The vector representing the canonical form of the cascade is

$$\begin{aligned} \vec{w} &= \frac{1}{2}(48, -8, -16, 0; -8, 0, 0, 0; -16, 0, 0, 0; 0, 0, 0, 0)^t \\ &= (24, -4, -8, 0; -4, 0, 0, 0; -8, 0, 0, 0; 0, 0, 0, 0)^t \\ &\equiv (3, 3, -1, 0; 3, 0, 0, 0; -1, 0, 0, 0; 0, 0, 0, 0)^t \pmod{7}. \end{aligned}$$

The simplified group function is

$$\begin{aligned} F &= a^3 g^{x_1} a^3 g^{x_1 \oplus x_2} a^{-1} g^{x_2 \oplus x_3} a^3 g^{x_3 \oplus x_4} a^{-1} g^{x_4} \\ &= a^3 (g^{x_1} a^3 g^{x_1}) (g^{x_2} a^{-1} g^{x_2}) (g^{x_3} a^3 g^{x_3}) (g^{x_4} a^{-1} g^{x_4}) \\ &= a^3 (g^{x_1} a^3 g^{x_1}) (g^{x_3} a^3 g^{x_3}) (g^{x_2} a^{-1} g^{x_2}) (g^{x_4} a^{-1} g^{x_4}) \\ &= a^3 g^{x_1} a^3 g^{x_1 \oplus x_3} a^3 g^{x_2 \oplus x_3} a^{-1} g^{x_2 \oplus x_4} a^{-1} g^{x_4} \end{aligned}$$

Fig. 5.4 shows the cascade for  $F$ . (End of Example)

**Lemma 5.1** The number of non-zero coefficients in the Walsh spectrum for an  $n$ -bit adder is  $2n+1$ .

**(Proof)** The arithmetic expression [16] for the  $n$ -bit adder is  $D = \sum_{i=0}^{n-1} 2^i (x_i + y_i)$ . By using the relations  $\alpha_i = 1 - 2x_i$  and  $\beta_i = 1 - 2y_i$ , we have the relation  $x_i + y_i = 1 - \frac{1}{2}(\alpha_i + \beta_i)$ . Thus, the expression showing the Walsh

spectrum [16] is written as

$$\begin{aligned} D &= \sum_{i=0}^{n-1} 2^i [1 - \frac{1}{2}(\alpha_i + \beta_i)] \\ &= (2^n - 1) - \frac{1}{2} \sum_{i=0}^{n-1} 2^i (\alpha_i + \beta_i) \end{aligned}$$

So, the number of non-zero coefficients is  $2n + 1$ . (Q.E.D)

**Theorem 5.3** *An  $n$ -bit adder can be realized by the cascade with  $6n + 1$  cells.*

**(Proof)** The number of cells in the canonical cascade is  $3 \cdot 2^{2n} - 2$ . The total number of coefficients is  $2^{2n}$ , and the number of non-zero coefficients is  $2n + 1$ . Thus, the number of zero coefficients is  $2^{2n} - (2n + 1)$ . For each zero coefficient, we can remove three cells. Thus, the number of remaining cells is  $(3 \cdot 2^{2n} - 2) - 3[2^{2n} - (2n + 1)] = 6n + 1$ . Note that in Fig. 5.4, two  $g$  cells are necessary for  $x_1 \oplus x_3$ ,  $x_2 \oplus x_3$ , and  $x_2 \oplus x_4$ . Thus, Fig. 5.4 requires 13 cells. (Q.E.D)

**Lemma 5.2** *The number of non-zero coefficients in the Walsh spectrum for an  $n$ -bit multiplier is  $(n + 1)^2$ .*

**(Proof)** The arithmetic expression for the  $n$ -bit multiplier is  $D = (\sum_{i=0}^{n-1} 2^i x_i)(\sum_{j=0}^{n-1} 2^j y_j)$ . By using the relations  $\alpha_i = 1 - 2x_i$  and  $\beta_j = 1 - 2y_j$ , we have the expression showing the Walsh spectrum:

$$D = \frac{1}{4} \left[ \sum_{i=0}^{n-1} 2^i (1 - \alpha_i) \right] \left[ \sum_{j=0}^{n-1} 2^j (1 - \beta_j) \right].$$

So, the number of non-zero coefficients is  $(n+1)^2$ . (Q.E.D)

Similarly to the proof of Theorem 5.3, we have

**Theorem 5.4** *An  $n$ -bit multiplier can be realized by the cascade with  $3(n + 1)^2 - 2$  cells.*

## 6. Conclusion and Comments

In this paper, we have shown a design method for cascades which implement two-valued input three-valued output functions. We used  $C_3$  (the cyclic group of order three) and  $S_3$  (the symmetric group of degree three) to decompose  $C_3$ . The designed cascades are reversible and conservative. The Walsh spectrum specifies the canonical cascade, and the number of non-zero coefficients in the spectrum is related to the number of the cells.

We have shown that an arbitrary  $n$ -variable function is realized with at most  $3 \cdot 2^n - 2$  cells. Also, by experiments, we have shown that a random function of  $n$  variables can be realized with about  $2^{n+1}$  cells. We also derived the numbers of cells to realize an  $n$ -bit adder and an  $n$ -bit multiplier.

Note that Yoeli-Turner [17] designed two-rail cascades. They used  $K$  (the Klein 4-group, that is isomorphic to  $C_2^2$ ), and  $A_4$  (the alternating group on four objects) to decompose  $K$ .

## Acknowledgments

This research is partly supported by the Grant in Aid for Scientific Research of The Japan Society for the Promotion of Science (JSPS), and Takeda Foundation. Discussion with Profs. Marek Perkowski, Alan Mishchenko, and Radomir Stanković motivated to write the paper. Dr. Pawel Kerntopf provided me related papers.

## References

- [1] C. Benett, "Logical reversibility of computation," *IBM Journal of Research and Development*, Vol. 17, 1973, pp. 525-532.
- [2] C. Benett, "Notes on the history of reversible computation," *IBM Journal of Research and Development*, Vol. 32, 1988, pp. 16-23.
- [3] R. K. Brayton, "Future of logic synthesis and Verification," in S. Hassoun and T. Sasao(e.d.), *Logic Synthesis and Verification*, Kluwer Publishers, (2001-11).
- [4] B. Elspas, "The theory of multi-rail cascades," in A. Mukhopadhyay (e.d.), *Recent Developments in Switching Theory*, Academic Press, New York, 1971.
- [5] E. Fredkin, and T. Toffoli, "Conservative Logic," *Int. Journal of Theoretical Physics*, Vol. 21, 1982, pp. 219-253.
- [6] P. Kerntopf, "On universality of binary reversible logic gates," *5th International Workshop on Boolean Problems*, Freiberg, Germany, Sept. 19-20, 2002, pp. 47-52.
- [7] K. K. Maitra, "Cascade switching networks of two-input flexible cells," *IRE Trans. Electron. Comput.*, EC-11, pp. 136-143, 1962.
- [8] M. Lukac, M. Pivtoraiko, A. Mishchenko, and M. Perkowski, "Automated synthesis of generalized reversible cascade using genetic algorithm," *5th International Workshop on Boolean Problems*, Freiberg, Germany, Sept. 19-20, 2002, pp. 33-45.
- [9] T. Sasao and K. Kinoshita, "Conservative logic elements and their universality," *IEEE Trans. on Comput.*, Vol. C-28, No. 9, pp. 682-685, Sept. 1979.
- [10] T. Sasao (ed.), *Logic Synthesis and Optimization*, Kluwer Academic Publishers (1993-01).
- [11] T. Sasao and M. Fujita (ed.), *Representation of Discrete Functions*, Kluwer Academic Publishers (1996-04).
- [12] T. Sasao, *Switching Theory for Logic Synthesis*, Kluwer Academic Publishers, (1999-02).
- [13] T. Sasao, M. Matsuura, and Y. Iguchi, "A cascade realization of multiple-output function for reconfigurable hardware," *International Workshop on Logic and Synthesis (IWLS01)*, Lake Tahoe, CA, June 12-15, 2001, pp. 225-230.
- [14] T. Sasao, "Design methods for multi-rail cascades," (invited paper) *5th International Workshop on Boolean Problems (IWBP2002)*, Freiberg, Germany, Sept. 19-20, 2002, pp. 123-132.
- [15] R. A. Short, "Two-rail cellular cascade," *AFIP Cont. Proc.*, Washington D.C., Vol. 27, Part I, pp. 355-369.
- [16] R. Stanković, T. Sasao, and C. Moraga, "Spectral transform decision diagrams," in [11].
- [17] M. Yoeli and Turner, "Decompositions of group functions with applications to two-rail cascades," *Information and Control*, Vol. 10, No. 6, pp. 565-571, 1967.