# Boolean Complementary Pairs

by

Jared Gobin

A thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfillment of the requirements of the degree of

Master of Science

Department of Mathematics

University of Manitoba

Winnipeg

**Abstract**

Golay pairs ($GP$s) are pairs of ($\pm 1$)-sequences with zero autocorrelation. $GP$s have numerous applications in engineering and mathematics such as in device synchronization, spectroscopy, and in the construction of Hadamard matrices. As a result, there is significant interest in understanding their mathematical structure. However, the structure of $GP$s appears to be very mysterious. Ternary complementary pairs ($TCP$s)—a generalization of $GP$s—are pairs of $(0, \pm 1)$-sequences with zero autocorrelation. Similar to $GP$s, the structure of $TCP$s appears to be quite challenging. In order to gain insight into $TCP$s and $GP$s, Craigen introduced Boolean complementary pairs ($BCP$s), which are pairs of $\mathbb{Z}_2$-sequences with zero autocorrelation. Craigen solved the structure of even-weight $BCP$s and with Woodford discovered a factorization involving $2 \times 2$ matrices in the odd-weight case. A review of Golay pairs, ternary complementary pairs, and Boolean complementary pairs is given. The odd-weight $BCP$ factorization is extended to all pairs of $\mathbb{Z}_2$-sequences with zero autocorrelation. Consequences of this extension are then established, including a connection to affixes.

# Acknowledgements

I am extremely grateful to David Gunderson for providing funding for this thesis and being a member of my examining committee. Thank you Robert Craigen for being my supervisor as well as on my examining committee. Thank you to Ben Li and Andriy Prymak for forming the rest of my examining committee. Lastly, I am very thankful to the Faculty of Graduate Studies, as this thesis was also graciously funded by a University of Manitoba Graduate Fellowship.

# Contents

# List of Symbols

| | |
|---|---|
| $\mathbb{Z}$ | the set of all integers. |
| $\mathbb{Z}^+$ | the set of all positive integers. |
| $\mathbb{N}$ | the set of all nonnegative integers. |
| $\mathbb{Z}_n$ | the ring of integers modulo $n$. |
| $I_n$ | the identity matrix of order $n$. |
| $0_n$ | the zero matrix of order $n$. |
| $M^\top$ | the transpose of the matrix $M$. |
| $\varnothing$ | the empty set. |
| $\subseteq$ | a subset. |
| $\subsetneq$ | a proper subset. |
| $\lvert S\rvert$ | the cardinality of the set $S$. |
| $R$ | an arbitrary integral domain, unless specified otherwise. |
| $-$ | represents "$-1$" in $(0, \pm 1)$-sequences and matrices. |

# 1

# Introduction

Complementary pairs have been widely used in engineering and mathematics since their inception in 1949 by Golay [14]. However, their mathematical structure remains largely mysterious.

Let $R$ be an integral domain, let $S \subseteq R$, let $n, w \in \mathbb{Z}^+$, and let $A = (a_i)_{i=0}^{n-1}$ be a sequence of length $n$ with entries in $S$. Define the **autocorrelation function** of $A$ to be a map $AF_A : \mathbb{N} \to R$, where

$$AF_A(j) := \begin{cases} \sum_{i=0}^{n-1-j} a_i a_{i+j} & j < n, \\ 0 & j \geqslant n. \end{cases}$$

In other words, $AF_A(j)$ is the sum of the product of all elements that are $j$ indices apart in the sequence $A$.

**Example 1.0.1.** Let $A = (a_i)_{i=0}^{2} = (a_0, a_1, a_2) = (1,5,2)$. Then

$$\begin{aligned} AF_A(0) &= a_0^2 + a_1^2 + a_2^2 = 1^2 + 5^2 + 2^2 = 30, \\ AF_A(1) &= a_0 a_1 + a_1 a_2 = 1 \times 5 + 5 \times 2 = 15, \text{ and} \\ AF_A(2) &= a_0 a_2 = 1 \times 2 = 2. \end{aligned}$$

□

A pair of sequences $(F, G)$ over $S$ is a **complementary pair of length** $n$ **and weight** $w$ if and only if both sequences are of length $n$, the number of nonzero entries in $F$ plus the number of nonzero entries in $G$ equals $w$, and for all integers $j > 0$, the pair satisfies

$$AF_F(j) + AF_G(j) = 0. \tag{1.0.1}$$

Complementary pairs are also said to have **zero autocorrelation**, and are abbreviated to $CP(n, w, S, R)$. If it is clear which ring $R$ the set $S$ belongs to, or if the ring $R$ does not matter, then $CP(n, w, S, R)$ may be shortened to $CP(n, w, S)$. Subsets of integral domains shall be called **coefficient sets**.

**Example 1.0.2.** Let $R = \mathbb{Z}$, $S = \{\pm 1\} \subset R$, $F = (f_i)_{i=0}^{3} =$ `(1,1,1,-1)`, and $G = (g_i)_{i=0}^{3} =$ `(1,1,-1,1)`. A useful convention will be to let "$-$" denote "$-1$" in sequences and matrices whose entries are a subset of $\{0, \pm 1\}$, where no confusion about the meaning of "$-$" can arise. This is for visual appeal and also eliminates the need for commas to separate entries of the sequences. Thus $F$ and $G$ become $F =$ `(111-)` and $G =$ `(11-1)`.

$R$ is an integral domain, $S$ is a subset of $R$, the pair $(F, G)$ has length 4, weight 8, and satisfies

$$\begin{aligned} AF_F(1) + AF_G(1) &= (1 + 1 - 1) + (1 - 1 - 1) = 0, \\ AF_F(2) + AF_G(2) &= (1 - 1) + (-1 + 1) = 0, \text{ and} \\ AF_F(3) + AF_G(3) &= (-1) + (1) = 0. \end{aligned}$$

Therefore, $(F, G)$ is a $CP(4, 8, \{\pm 1\}, \mathbb{Z})$. □

**Example 1.0.3.** Let $R = S = \mathbb{Z}_5$, $s \in S$, $F = (f_i)_{i=0}^{2} =$ `(1,0,4)`, and $G = (g_i)_{i=0}^{2} =$ `(3,s,-3)`. $R$ is an integral domain, $S$ is a subset of $R$, and the pair $(F, G)$

has length 3. The pair $(F, G)$ has weight 5 if $s \neq 0$ and weight 4 if $s = 0$. Checking autocorrelation coefficients shows

$$AF_F(1) + AF_G(1) = (1 \times 0 + 0 \times 4) + (3s - 3s) = 0, \text{ and}$$
$$AF_F(2) + AF_G(2) = (4) + (-9) = -5 = 0.$$

Therefore, $(F, G)$ is a $CP(3, 5, \mathbb{Z}_5)$ if $s \neq 0$ and is a $CP(3, 4, \mathbb{Z}_5)$ otherwise. □

A useful convention will be to denote sequences by uppercase letters and their entries by the lowercase equivalent. Indexing shall also begin with 0 unless specified otherwise. Thus for $n \in \mathbb{Z}^+$, a sequence $F$ of length $n$ with no specified index shall be written as $F = (f_i)_{i=0}^{n-1}$.

For a given coefficient set $S$, which positive integers $n$ and $w$ are the length and weight of a complementary pair over $S$? This is the driving question for complementary pairs, whose answer is often impenetrable to attack. It is this author's opinion/hope that the reason for this absence of results is that complementary pairs have not been studied from the correct perspective. Craigen and Woodford [8] established a new perspective to investigate Boolean complementary pairs, but did not publish their results. This thesis re-derives their results and begins the investigation of Boolean complementary pairs through this new perspective—a perspective that might harbour significant consequences.

Complementary pairs originated in a 1949 paper by Marcel Golay [14] (more famously known for Golay codes, a kind of error-correcting code), who sought to improve the single-slit optical spectrometer. Optical spectrometers are apparatus used to measure properties of specific wavelengths of light, such as their chemical composition. The single-slit spectrometer has a single entry and a single exit slit with an adjustable diffractor on the inside positioned to correspond to a specific

wavelength. Light is shone in the entrance slit of the spectrometer then separated into its composite wavelengths by the diffractor. Only light of the specified wavelength escapes through the exit slit, which allows one to record properties of that particular wavelength. Single-slit spectrometers are quite large relative to their slits. Therefore, Golay wanted to design a multi-slit spectrometer which would use many entrance slits, allowing for more light to pass through and therefore get a stronger reading. However, if one only wanted light of the desired wavelength to escape, the diffractor design within the multi-slit spectrometer would need to be extremely complicated. Golay's innovation was that one did not need to have only the specified wavelength of light escape; one only needs complementary pairs.

Golay gave his complementary pairs the name **complementary series**, and defined them to be a pair of equal length sequences with two kinds of elements with the property that the number of like elements for a given nonzero shift in one sequence is equal to the number of unlike elements of the same shift in the other. These pairs of sequences are now referred to as **Golay pairs**, and are equivalent to complementary pairs over the set $\{\pm 1\} \subset \mathbb{Z}$. To see this, let $n \in \mathbb{Z}^+$, and $F = (f_i)_{i=0}^{n-1}$ and $G = (g_i)_{i=0}^{n-1}$ be a pair of $(\pm 1)$-sequences. For any natural number $j$ less than $n$, one obtains

$$AF_F(j) + AF_G(j) = \sum_{i=0}^{n-1-j} f_i f_{i+j} + \sum_{i=0}^{n-1-j} g_i g_{i+j}. \tag{1.0.2}$$

Let

$$\begin{aligned} l_F &= \left|\{i \in \mathbb{Z} : 0 \leqslant i \leqslant n-1-j \text{ and } f_i = f_{i+j}\}\right|, \\ l_G &= \left|\{i \in \mathbb{Z} : 0 \leqslant i \leqslant n-1-j \text{ and } g_i = g_{i+j}\}\right|, \\ u_F &= \left|\{i \in \mathbb{Z} : 0 \leqslant i \leqslant n-1-j \text{ and } f_i \neq f_{i+j}\}\right|, \text{ and} \\ u_G &= \left|\{i \in \mathbb{Z} : 0 \leqslant i \leqslant n-1-j \text{ and } g_i \neq g_{i+j}\}\right|. \end{aligned}$$

That is, $l_F$ is the number of like elements of distance $j$ in $F$, $u_F$ is the number of unlike elements of distance $j$ in $F$, and similarly for $l_G$ and $u_G$ in $G$.

For any integer $i$ such that $0 \leqslant i \leqslant n-1$, note that

$$f_i f_{i+j} = \begin{cases} 1 & f_i = f_{i+j}, \\ -1 & f_i \neq f_{i+j}. \end{cases}$$

Therefore, equation (1.0.2) becomes

$$AF_F(j) + AF_G(j) = l_F - u_F + l_G - u_G. \tag{1.0.3}$$

Suppose $j > 0$. If $(F, G)$ is a complementary series, then $l_F = u_G$ and $l_G = u_F$, so equation (1.0.3) becomes $l_F - u_F + l_G - u_G = 0$, which implies that $(F, G)$ is a Golay pair.

If $(F, G)$ is a Golay pair, then equation (1.0.3) is zero, so $l_F - u_F + l_G - u_G = 0$. Notice that there are $n - j$ terms in $AF_F(j)$ and $AF_G(j)$, and all are $\pm 1$. Therefore, $l_F + u_F = l_G + u_G = n - j$. Then

$$\begin{aligned} 2l_F - 2u_G &= (l_F - u_F + l_G - u_G) + (l_F + u_F) - (l_G + u_G) \\ &= 0 + (n-j) - (n-j) \\ &= 0, \end{aligned}$$

which implies $l_F = u_G$. One similarly obtains $l_G = u_F$, and it follows that $(F, G)$ is a complementary series of length $n$ if and only if $(F, G)$ is a Golay pair of length $n$ (abbreviated to $GP(n)$). As there are no nonzero entries in a Golay pair, every $GP(n)$ is a $CP(n, 2n, \{\pm 1\}, \mathbb{Z})$.

Golay's diffraction design in the multi-slit spectrometer, which can be found in his first paper [14], is quite intricate. However, how Golay pairs are used is simple to describe. Let $n \in \mathbb{Z}^+$, and suppose $\mathbf{a} = (a_i)_{i=0}^{n-1}$ , $\mathbf{b} = (b_i)_{i=0}^{n-1}$ form a Golay pair (lowercase letters for the sequences following Golay [16]). Let $\mathbf{a}' = (-a_i)_{i=0}^{n-1}$ and $\mathbf{b}' = (-b_i)_{i=0}^{n-1}$. Divide the spectrometer into four components as shown in Figure 1.1 (this figure is only used to show how Golay pairs are used, not how the mechanism works). Each component is a sequence of $n$ equally-spaced slits, and slit $i$ is open or closed depending on whether the corresponding sequence term is 1 or $-1$. For instance, a quadrant indexed by $\mathbf{a}$ will have slit $i$ open if and only if $a_i = 1$, and is closed if and only if $a_i = -1$. The exit sequences are inverted to correspond with the inversion of the radiation upon hitting the diffractor. For instance, the exit $\mathbf{a}$ is actually $(a_{n-i})_{i=1}^{n}$. Two recording devices $D_1$ and $D_2$ are placed at the exits of the slits as shown in Figure 1.1.

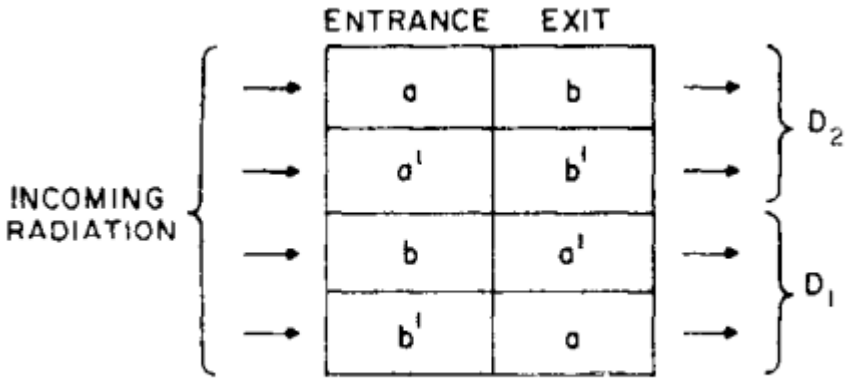


Figure 1.1: Golay's design for the multi-slit spectrometer (Golay, 1961 [16]).

Suppose electromagnetic radiation is uniformly radiated across the entrance of the spectrometer. For a nonnegative integer $i < n$, light through the entrance slit corresponding to $a_i$ is diffracted to hit the exit slits corresponding to $a_i, a_{i+1}, \ldots, a_{n-1}$. Similarly, light coming from $a_i'$ hits the slits corresponding to $a_i', a_{i+1}', \ldots, a_{n-1}'$, light

from $b_i$ hits the slits corresponding to $b'_i, b'_{i+1}, \ldots, b'_{n-1}$, and light from $b'_i$ hits the slits corresponding to $b_i, b_{i+1}, \ldots, b_{n-1}$. The light with the desired wavelength corresponds to light that enters from $a_i, a'_i, b_i, b'_i$ and hits the exit slits $a_i, a'_i, b'_i$, and $b_i$, respectively. By construction, the light from $b_i$ to $b'_i$ and from $b'_i$ to $b_i$ is blocked, and thus by examining Figure 1.1, one sees that light with the proper wavelength is only read by device $D_1$. Light corresponding to different wavelengths correspond to a nonzero shift in the slits. Say this shift is in $j$ slits. Then the number of exit slits in $\mathbf{a}$ where light escapes is equal to the number of pairs $(a_i, a_{i+j})$ where both are 1. The number of exit slits in $\mathbf{a}'$ where light escapes is equal to the number of pairs $(a'_i, a'_{i+j})$ where both are 1, that is, the number of pairs $(a_i, a_{i+j})$ where both are $-1$. Thus the total number of slits where light exits and is picked up only by $D_1$ is equal to the number of like elements in $\mathbf{a}$ of shift $j$. Similarly, this fixed wavelength will also correspond to the number of open slits from $\mathbf{b}$ to $\mathbf{b}'$ and $\mathbf{b}'$ to $\mathbf{b}$ of shift $j$, which is equal to the number of unlike elements of shift $j$ in $\mathbf{b}$. This radiation is picked up only by $D_2$. As light is uniformly radiated across the slits and the number of like elements of shift $j$ in $\mathbf{a}$ is equal to the number of unlike elements of shift $j$ in $\mathbf{b}$, the measurement $D_1 - D_2$ is only that of the desired wavelength.

The multi-slit spectrometer was the first of many applications of complementary pairs to engineering. Golay foretold of these numerous applications, but continued investigating Golay pairs for a different reason. In his 1961 paper [16], Golay stated

"Regardless of past or possible future applications, the writer has found these complementary series mathematically appealing, first because of the deep seated symmetries which characterize them, even though no sign of order may be obvious at first glance, and second because of the challenge offered by the problem of synthesizing them for $n = 26, 34$, etc,".

This is indeed the case with complementary pairs: interest is generated not only from the many applications to engineering, but also from the mysterious nature of their mathematical structure. Complementary pairs are strikingly similar in this respect to another object in mathematics: for $n, w \in \mathbb{Z}^+$, a **weighing matrix** of order $n$ and weight $w$ is an $n \times n$ matrix $W$ with entries $\{0, \pm 1\}$ such that $WW^\top = wI$. Weighing matrices have many applications such as in experimental designs in statistics and optical multiplexing in engineering [22]. The question of which positive integers $n, w$ are the order and weight of a weighing matrix is one that has drawn significant interest. In particular, the question of which integers are the orders of **Hadamard matrices** (weighing matrices with $n = w$) has received much attention since its posing in 1893 by Hadamard [20]. In the same paper, Hadamard showed that if Hadamard matrix of order $n$ exists, then $n$ is 1, 2, or a multiple of 4. It has been conjectured that for every integer $n$ that is a multiple of 4, a Hadamard matrix of order $n$ exists. Complementary pairs can be used to construct weighing matrices, as is shown later in this chapter and described in detail in Section 2.6.

Golay wrote three more papers on Golay pairs [15], [16], [17], each paper focusing on their mathematical structure. Golay found pairs of lengths $10, 26$, and all non-negative powers of 2, and showed that for $n, m \in \mathbb{Z}^+$, if one has a pair of length $n$ and $m$ then one can construct a pair of length $2nm$. Turyn [27] improved this result by demonstrating how to construct a pair of length $nm$ from pairs of length $n$ and $m$, thus proving the set of lengths of Golay pairs is closed under multiplication. Combining this result with the lengths Golay found shows that for every $a, b, c \in \mathbb{N}$, a Golay pair of length $2^a 10^b 26^c$ exists. So far, no Golay pair of any other length has been found. Indeed, it has been verified by Borwein and Ferguson [1] that every Golay pair of length up to 100 has length of the form $2^a 10^b 26^c$. Borwein and Ferguson also showed that all pairs of length up to 100 are constructible from five starting pairs of lengths $1, 10, 20$ and 26, and no starting pair is constructible from

any of the others. Only two other restrictions on the lengths of Golay pairs have been found: Golay [16] showed that the lengths of pairs are either 1 or even, and Eliahou, Kervaire, and Saffari [9] showed that the length of a Golay pair can not have a factor congruent to 3 (mod 4).

Most engineering applications of Golay pairs involve transforming one or both sequences in the pair to a signal through their discrete Fourier transforms. These signals have desirable properties, such as guaranteeing some power-efficiency in a transmitter. For instance, Golay pairs are used to construct power-efficient **multi-tone signals**, which are signals that are made up of multiple equal amplitude, equally spaced tones. Multi-tone signals are used to determine characteristics of an object, such as determining acoustic measurements of auditoriums [24]. The **crest factor** of a multitone signal is the ratio of the highest peak to the average, and a high crest factor results in a weaker transmission of a signal [25]. A multi-tone signal constructed from the discrete Fourier transform of a sequence in a Golay pair has an upper bound of 6 decibels on its crest factor [25], which guarantees some power-efficiency.

Golay pairs are also used in device synchronization. To show how this is done, a few more definitions and observations need to be made. Let $R$ be an integral domain, let $S \subseteq R$, let $n \in \mathbb{Z}^+$, and let $F = (f_i)_{i=0}^{n-1}$ and $G = (g_i)_{i=0}^{n-1}$ be two sequences with entries in $S$. For an arbitrary sequence $A$, the **periodic autocorrelation function** of $A$ is $PAF_A : \mathbb{N} \to R$, where for all $j \in \mathbb{N}$, one obtains

$$PAF_A(j) := AF_A(j) + AF_A(n-j)$$

The **cross-correlation function** of $(F, G)$ is $CCF_{F,G} : \mathbb{N} \to R$, where

$$CCF_{F,G}(j) := \begin{cases} \sum_{i=0}^{n-1-j} (f_i g_{i+j} + g_i f_{i+j}) & 0 \leqslant j \leqslant n-1, \\ 0 & j \geqslant n. \end{cases}$$

Lastly, suppose $(F, G)$ is a Golay pair. Then

$$\begin{aligned} AF_F(0) + AF_G(0) &= \sum_{i=0}^{n-1} f_i^2 + \sum_{i=0}^{n-1} g_i^2 \\ &= 2 \sum_{i=0}^{n-1} 1 \\ &= 2n. \end{aligned}$$

Therefore, 0 is the only $j \in \mathbb{N}$ such that $AF_F(j) + AF_G(j) \neq 0$.

Next, for signal transmission, the transmitter and receiver agree upon a time period $P$ in seconds which corresponds to how long the sequence will be sent for. Now suppose $A = (a_0, a_1, \ldots, a_{n-1})$ is a $(\pm 1)$-sequence and suppose $u(t)$ is its discrete Fourier transform with period $P$. The function $u(t)$ is a sum of sines and cosines that represents the amplitude of the signal at time $t$. For $j = 1, 2, \ldots, n$, the value $u(jP/n)$ is the amplitude corresponding uniquely to $a_{j-1}$. The signal is sent, and the receiver measures the amplitude of the signal at every $(P/n)$ seconds for a total of $n$ times. As each amplitude corresponds to a unique element, the signal can be decoded back into a sequence.

Now suppose one wants two devices to communicate, say someone wants to connect their phone to a router for WiFi. The phone sends its requests to the network by taking a sequence which corresponds to a command, transforming it into a signal using its Fourier transform, then sending it to the router. The router then converts the signal back into a sequence, but due to temporal offset this received sequence may be

a shifted version of the original. For example, the phone could send $(1, 2, 3, \ldots, 10)$ and the router might receive $(4, 5, \ldots, 10, 1, 2, 3)$. Without any correction, this temporal offset would cause the router to misinterpret the phone's request. Therefore, the router needs to know how to shift received sequences back into their intended form for proper communication. To this end, a Golay pair is used.

Let $n \in \mathbb{Z}^+$, let $(F, G)$ be a $GP(n)$, and let $A = (f_0, f_1, \cdots, f_{n-1}, g_0, g_1, \cdots, g_{n-1})$. To correct for temporal offset, the phone converts $A$ to a signal through its Fourier transform, which it then sends to the router. The router decodes the signal into a sequence $A'$ and computes $CCF_{A,A'}(0)$. It can be shown that there exists an integer $j < n$ corresponding to the temporal offset in the signal transmission such that $CCF_{A,A'}(0) = 2PAF_A(j)$. One can also show that $PAF_A(j)$ can be rewritten as $PAF_A(j) = AF_F(j) + AF_G(j) + CCF_{F,G}(n-j)$. If there is no temporal offset, that is, if $A' = A$, then $j = 0$ and one obtains

$$\begin{aligned} CCF_{A,A'}(0) &= 2PAF_A(0) \\ &= 2\left(AF_F(0) + AF_G(0) + CCF_{F,G}(n)\right) \\ &= 4n. \end{aligned}$$

If there is a temporal offset, then $0 < j < n$ and one obtains $AF_F(j) + AF_G(j) = 0$. It can be shown that $CCF_{F,G}(n-j)$ is small relative to $2n$ [21], resulting in

$$\begin{aligned} CCF_{A,A'}(0) &= 2PAF_A(j) \\ &= 2\left(AF_F(j) + AF_G(j) + CCF_{F,G}(n-j)\right) \\ &= 2CCF_{F,G}(n-j) \end{aligned}$$

being small relative to $4n$. Therefore, the router can tell if there is a temporal offset by checking if $CCF_{A,A'}(0)$ is near $4n$ (there can be minor errors in the process, hence the calculated values may be slightly off from their theoretical ones). If there is a

temporal offset, the router shifts the received sequence $A'$ until the cross-correlation function of $A$ with this shifted sequence evaluated at zero is near $4n$. The router then records this shift and applies it to received signals from the phone to properly interpret them, thus synchronizing the devices.

As previously mentioned, Golay pairs can also be used to construct Hadamard matrices. Let $n \in \mathbb{Z}^+$ and $M = (m_{i,j})_{i,j=0}^{n-1}$. The matrix $M$ is **circulant** if and only if for all integers $i, j$ such that $0 \leqslant i, j \leqslant n-1$, the equality $m_{i,j} = m_{i+1,j+1}$ holds (where indices are reduced modulo $n$). Observe that any row of a circulant matrix defines the entire matrix. Now suppose $F = (f_i)_{i=0}^{n-1}$ and $G = (g_i)_{i=0}^{n-1}$ form a $GP(n)$. Construct circulant matrices $A$ and $B$ by letting their first rows be $F$ and $G$, respectively. Let

$$H = \begin{pmatrix} A & B \\ -B^\top & A^\top \end{pmatrix},$$

and consider

$$\begin{aligned} HH^\top &= \begin{pmatrix} A & B \\ -B^\top & A^\top \end{pmatrix} \begin{pmatrix} A^\top & -B \\ B^\top & A \end{pmatrix} \\ &= \begin{pmatrix} AA^\top + BB^\top & BA - AB \\ A^\top B^\top - B^\top A^\top & AA^\top + BB^\top \end{pmatrix}. \end{aligned}$$

It will be shown in Lemma 2.6.3 that all circulant matrices commute and that the transpose of a circulant matrix is also circulant. Thus, $BA - AB = AB - AB = 0$ and $A^\top B^\top - B^\top A^\top = A^\top B^\top - A^\top B^\top = 0$. Therefore,

$$HH^\top = \begin{pmatrix} AA^\top + BB^\top & 0 \\ 0 & AA^\top + BB^\top \end{pmatrix}.$$

For integers $i$ and $j$ such that $0 \leqslant i, j \leqslant n-1$, the $(i,j)$-entry of $AA^\top + BB^\top$ is

$$\sum_{k=0}^{n-1-j+i} (f_k f_{k+j-i} + g_k g_{k+j-i}) + \sum_{k=0}^{j-i} (f_k f_{k+j-i} + g_k g_{k+j-i})$$
$$= AF_F(j-i) + AF_G(j-i) + AF_F(n-j+i) + AF_G(n-j+i).$$

Therefore, when $i \neq j$ the $(i,j)$-entry of $AA^\top + BB^\top$ is zero and the $(i,i)$-entry of $AA^\top + BB^\top$ is $2n$; hence $HH^\top = 2nI$. Therefore, as each entry of $H$ is $\pm 1$, $H$ is a Hadamard matrix of order $2n$. This construction can be applied for all $a, b, c \in \mathbb{N}$ to construct a Hadamard matrix of order $2^{a+1}10^b26^c$.

**Ternary complementary pairs** ($TCP$s) are complementary pairs over the set $\{0, \pm 1\} \subsetneq \mathbb{Z}$. The total number of zeros in the two sequences is called their **deficiency**, hence every Golay pair is a deficiency zero ternary complementary pair. $TCP$s have been studied for their connections to $GP$s, though the interest in $TCP$s also comes from connections to other areas such as orthogonal designs [12]. Gavish and Lempel [11], who coined the term "$TCP$", found lower bounds on the deficiency of $TCP$s for every possible length, found extra conditions on the lengths of certain small-deficiency pairs, and provided a construction of $TCP$s different from known constructions of $GP$s.

Gysin and Seberry published two papers on $TCP$s [18], [19], finding new restrictions on lengths and deficiencies and settling all cases of existence/nonexistence for lengths less than or equal to 20 and weights less than or equal to 40. The authors also gave many constructions for new $TCP$s from old, but it was later shown by Craigen [3] that their constructions were equivalent to Gavish and Lempel's standard construction [11]. Craigen provided a proper generalization of the standard construction in the same paper.

In 2001, Craigen and Koukouvinos [7] developed a theory of $TCP$s from a "weight-first" perspective. At that time, most of the work done on $TCP$s was to classify pairs by length first, then by deficiency. They argued that a weight-first perspective is more natural, citing that many equivalent $TCP$s have different lengths, but weight is always constant. Furthermore, the result by Eliahou, Kervaire, and Saffari [9] also applied in the $TCP$ case, and was actually a theorem about weight rather than length—it just happens that the length of a Golay pair is half its weight. From this perspective, the authors introduced **primitive pairs**, which are pairs that cannot be obtained from others by the standard multiplication outlined in the later Theorem 4.2.4. As such, primitive pairs are in essence the primes of the $TCP$ world.

Craigen and Koukouvinos continued their investigation into $TCP$s in 2006, this time with Georgiou and Gibson [5]. The authors developed a new computational strategy for finding $TCP$s: let $S$ be a coefficient set, $t \in \mathbb{Z}^+$, $A, B, C, D$ be sequences of length $t$ over $S$, and let $\#$ be an arbitrary symbol. Then $F = (A, \#, B)$ and $G = (C, \#, D)$ form an **affix** of length $t$ over $S$ if and only if for all $i \leqslant t$, one obtains

$$AF_F(2t + 1 - i) + AF_G(2t + 1 - i) = 0. \tag{1.0.4}$$

In other words, the autocorrelation coefficients that do not involve "#" are zero.

**Example 1.0.4.** Let $F =$ (`1,1,#,1,-1`) and $G =$ (`1,1,#,-1,1`). The sequences (`1,1`), (`1,-1`), and (`-1,1`) all have length 2, and $(F, G)$ is a pair of sequences of length $2 \times 2 + 1 = 5$. One can verify that

$$AF_F(4) + AF_G(4) = (-1) + (1) = 0, \text{ and}$$
$$AF_F(3) + AF_G(3) = (1 - 1) + (-1 + 1) = 0.$$

Therefore, $(F, G)$ is an affix of length 2 over $\{\pm 1\}$. □

Now let $n \in \mathbb{Z}^+$, let $A, B, C$, and $D$ be length $n$ sequences with entries in $\{0, \pm 1\}$, and suppose $F = (A, B)$ and $G = (C, D)$ form a $TCP$ of length $2n$. One can verify that $\widetilde{F} = (A, \#, B)$ and $\widetilde{G} = (C, \#, D)$ form an affix of length $n$. Thus every even-length $TCP$ corresponds to a unique affix of half its length (similarly with the odd-length case, except one replaces the middle entry with "#"). Thus when one wishes to construct a $TCP$ of length $2n$, one can begin with the affixes of length $n$, remove the "#" symbol (replace "#" with $0, 1$, or $-1$ in the odd-length case), then check the remaining autocorrelation coefficients to see if they are zero.

When building an affix of a specified length, one begins with the set of all affixes of length one less than that and sees if any of these smaller affixes can be "completed" to the larger size. For instance, to build an affix of length $n+1$ from $\widetilde{F} = (A, \#, B)$ and $\widetilde{G} = (C, \#, D)$, one finds which $x, y, u, v \in \{0, \pm 1\}$ make $H = (A, x, \#, y, B)$ and $K = (C, u, \#, v, D)$ an affix. Since $(\widetilde{F}, \widetilde{G})$ is an affix, one only needs to check that $AF_H(n+2) + AF_K(n+2) = 0$ as the other autocorrelation coefficients are automatically zero. Thus one has a systematic method for generating affixes of larger sizes, which also yields a systematic approach to constructing $TCP$s of a given length. This method vastly outperforms the naive approach of trying all possible permutations of $0, 1$, and $-1$ to construct a $TCP$ of a given length, which is computationally costly.

Despite gaining some insight into ternary complementary pairs, just like the $GP$ case, their structure appeared to be very mysterious. If one examines the results about these complementary pairs, one sees that they fall into one of two categories: they are either a nonexistence result, or a method of constructing a new pair from old pairs. There is no theory about why a $TCP$ or $GP$ should exist, only theory about why one should not. All known $TCP$s and $GP$s have either been constructed from other pairs or have been found by computer or by hand.

In 2003, Craigen [2] introduced **Boolean complementary pairs** ($BCP$s), which are complementary pairs over $\mathbb{Z}_2$, to try to gain insight into $TCP$s. Each $TCP$ corresponds to a $BCP$ by mapping the entries in the sequences from $\mathbb{Z}$ into $\mathbb{Z}_2$. The idea behind $BCP$s was that if one could classify all complementary pairs over $\mathbb{Z}_2$, then one has obtained all possible "zero patterns" within $TCP$s. One could then attempt to construct all $TCP$s by placing minus signs in the correct places of $BCP$s. Craigen completely classified even-weight $BCP$s and certain types of odd-weight $BCP$s. Later, Craigen and Woodford [8] provided an algebraic factorization for the odd-weight pairs that was markedly different than the even-weight pairs. This factorization involves $2 \times 2$ matrices defined by certain properties of the odd-weight pair under investigation. This factorization has a much higher degree of complexity than the even-weight case.

The purpose of this thesis is to not only use Craigen and Woodford's factorizations to gain insight into $BCP$s, but to also show that these factorizations themselves are intriguing and worthy of study. Chapters 2 to 5 are an overview of what is known about $GP$s, $TCP$s, and $BCP$s. The point of this is to not only familiarize the reader with what is known in the literature, but also to contrast the known results with the original results in this thesis. Chapter 6 develops and extends the factorizations of odd-weight $BCP$s found by Craigen and Woodford to all pairs of sequences with entries in $\mathbb{Z}_2$. Chapter 7 investigates these factorizations and Chapter 8 concludes the thesis by considering possible continuations of this work.

# 2

# General Concepts, Properties, and Constructions of Complementary Pairs

Examining the literature on complementary pairs reveals common concepts, properties, and constructions. This chapter unifies these results and ideas by proving and discussing them in their general cases. Consequentially, many results in Chapters 3, 4, and 5 follow immediately from the work in this chapter. As this chapter is a simple generalization of others' work, each citation will indicate whose result is being generalized. Constructions of orthogonal matrices using complementary pairs are included in the final section.

## 2.1 The Laurent polynomial form of complementary pairs

**Definition 2.1.1.** Let $x$ be an indeterminate and let $S$ be a set. The set of all **Laurent polynomials** in $x$ over $S$ is

$$S[x, x^{-1}] = \left\{ \sum_{i=m}^{m+n} s_i x^i : m \in \mathbb{Z}, n \in \mathbb{N}, s_m, s_{m+1}, \ldots, s_{m+n} \in S \right\}.$$

Complementary pairs have an equivalent Laurent polynomial form that is structurally revealing and is easier to work with than their sequence form. For these reasons, the Laurent polynomial form shall be used primarily throughout this thesis.

The degree of Laurent polynomials shall be important in the discussion of lengths of complementary pairs. However, Laurent polynomials have a slightly different definition of degree than standard polynomials.

**Definition 2.1.2.** The **degree** of a nonzero Laurent polynomial $f(x)$ (written $\deg(f(x))$) is the difference between its highest and lowest powers of $x$ with nonzero coefficients. Suppose $f(x)$ and $g(x)$ have equal degree. The **degree of the pair** $(f(x), g(x))$ is the degree of the two polynomials. If $f(x)$ has degree zero, the pair $(f(x), 0)$ shall be considered a degree zero pair.

**Example 2.1.1.** The polynomial $f(x) = 2x^{-4}+x^{-1}+7+x^2$ is a Laurent polynomial over the set $\{0, 1, 2, 7\}$ and has degree $6 = 2 - (-4)$. Note that $f(x)$ is not a Laurent polynomial over the set $\{1, 2, 7\}$. This is because the definition of Laurent polynomials requires that every coefficient from the least power of $x$ in $f(x)$ to the greatest is in $\{1, 2, 7\}$. The coefficients of $x^{-3}, x^{-2}$, and $x$ in $f(x)$ are all zero, which lies outside the set $\{1, 2, 7\}$. □

The only notion of degree used in this thesis is Laurent polynomial degree. Therefore, any mention of degree is to be interpreted as the Laurent polynomial degree. Similarly, the only polynomials of interest are Laurent polynomials, hence any mention of polynomials shall be interpreted as Laurent polynomials.

Notice that the definition of the autocorrelation function of a sequence found on page 1 relied on the index of the sequences starting at $i = 0$. This was done out of simplicity for the reader and is not necessary. The Laurent polynomial representation of complementary pairs requires an arbitrary starting index, hence autocorrelation shall now be redefined.

**Definition 2.1.3.** Let $S$ be a coefficient set, $t \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, and $A = (a_i)_{i=t}^{n-1+t}$. The **autocorrelation function** of $A$ is $AF_A : \mathbb{N} \to R$, where

$$AF_A(j) := \begin{cases} \sum_{i=t}^{n-1+t-j} a_i a_{i+j} & j < n, \\ 0 & j \geqslant n. \end{cases}$$

That is, the autocorrelation function of a sequence evaluated at $j$ is the sum of all terms indexed $j$ apart.

**Definition 2.1.4.** Let $S$ be a coefficient set, $t \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, and $A = (a_i)_{i=t}^{n-1+t}$ be a sequence of length $n$ over $S$. The **Laurent polynomial form** of $A$ is the polynomial

$$a(x) = \sum_{i=t}^{n-1+t} a_i x^i.$$

If an index is not specified in a sequence, the index is assumed to begin at 0. For convention, a sequence denoted with an uppercase letter shall have its Laurent polynomial denoted by the lowercase version of the letter. For example, a sequence $F$ would have Laurent polynomial form $f(x)$. Furthermore, for all $j \in \mathbb{Z}$, the coefficient of $x^j$ in $f(x)$ shall be written as $f_j$ unless explicitly stated otherwise. Thus for

$m, n \in \mathbb{Z}$, if the least and highest powers of $x$ in $f(x)$ are $m$ and $n$, respectively, then $f(x)$ is assumed to be written as $f(x) = \sum_{i=m}^{n} f_i x^i$.

**Example 2.1.2.** Consider $F = (\texttt{111-})$ and $G = (\texttt{11-1})$, which form a $GP(4)$. No index is given for either $F$ nor $G$, hence it is assumed that their indices start at zero. Therefore, their polynomial forms are $f(x) = 1 + x + x^2 - x^3$ and $g(x) = 1 + x - x^2 + x^3$. If instead $F$ is indexed starting at $-7$, then $F$'s polynomial form is $f(x) = x^{-7} + x^{-6} + x^{-5} - x^{-4} = x^{-7}(1 + x + x^2 - x^3)$. □

Knowing the degree of a polynomial is not enough to know the length of the original sequence. For instance, the sequences $F = (\texttt{111-})$ and $\widetilde{F} = (\texttt{111-000})$ have the same associated polynomial but have different lengths. However, it is straightforward to see that for $n \in \mathbb{Z}^+$, any sequence of length $n$ that does not start or end with a zero has a degree $n-1$ associated polynomial. Moreover, one also sees that two sequences with the same index have the same associated polynomial if and only if zeros can be appended to the end of one sequence to obtain the other. For example, $\widetilde{F}$ only differs from $F$ by the three appended zeros at the end of $\widetilde{F}$. Appending zeros to the end (or the start) of a sequence does not change the sequence's autocorrelation function. For example, for all $j \in \mathbb{N}$, one has $AF_F(j) = AF_{\widetilde{F}}(j)$. Therefore, from the point of view of complementarity, two sequences who differ solely by some zeros at the starts or ends of the sequences are the "same". Therefore, the following definition from Craigen and Koukouvinos [7] is made.

**Definition 2.1.5.** A sequence is **reduced** if and only if its first and last terms are nonzero.

**Example 2.1.3.** The sequence $F = (\texttt{111-})$ is reduced but $\widetilde{F} = (\texttt{111-000})$ is not. □

**Definition 2.1.6.** For a polynomial $f(x)$, define the **conjugate** of $f(x)$ to be $f^*(x) = f(x^{-1})$.

**Theorem 2.1.7** (Folklore)**.** Let $R$ be an integral domain, let $S \subseteq R$ be a coefficient set, let $n, w \in \mathbb{Z}^+$, let $\lambda = AF_F(0) + AF_G(0)$, and let $(F, G)$ be a pair of reduced sequences of length $n$ over $S$. Then $(F, G)$ is a $CP(n, w, S, R)$ if and only if their associated polynomials $f(x)$ and $g(x)$ have degree $n-1$, have a total of $w$ nonzero coefficients, and satisfy

$$f(x)f^*(x) + g(x)g^*(x) = \lambda. \tag{2.1.1}$$

*Proof.* As $F$ and $G$ are reduced, it follows that $f(x)$ and $g(x)$ both have degree $n-1$. It is easy to see that $(F, G)$ has weight $w$ if and only if $f(x)$ and $g(x)$ have $w$ total nonzero coefficients. For all $j \in \mathbb{Z}$, the coefficient of $x^j$ and $x^{-j}$ in equation (2.1.1) is

$$\sum_{i=0}^{n-1-j} (f_i f_{i+j}) + \sum_{i=0}^{n-1-j} (g_i g_{i+j}) = AF_F(j) + AF_G(j).$$

When $j = 0$, one has $\lambda = AF_F(0) + AF_G(0)$. The result follows. □

The polynomial $(ff^* + gg^*)(x)$ shall be interpreted as $f(x)f^*(x) + g(x)g^*(x)$, and equation (2.1.1) shall be written as $(ff^* + gg^*)(x) = \lambda$ for visual appeal.

**Example 2.1.4.** Let $F = (\texttt{11})$ and $G = (\texttt{1-})$, which form a $GP(2)$. For $f(x) = 1 + x$ and $g(x) = 1 - x$,

$$\begin{aligned}(ff^* + gg^*)(x) &= (1 + x)(1 + x^{-1}) + (1 - x)(1 - x^{-1}) \\ &= (1 + x^{-1} + x + 1) + (1 - x^{-1} - x + 1) \\ &= 4.\end{aligned}$$

□

Note any sequence of zeros cannot be reduced. However, a sequence of zeros can still be represented by the zero polynomial. Complementary pairs where both sequences are zero are not of any concern in this thesis, but pairs where exactly one sequence is zero, such as the sequences (1) and (0), are of interest and shall be considered degree zero complementary pairs.

Theorem 2.1.7 allows one to discuss complementary pairs solely through the use of Laurent polynomials with the underlying assumption that the polynomials correspond to a pair of sequences. Therefore, for an integral domain $R$, a coefficient set $S \subseteq R$, and $n, w \in \mathbb{Z}^+$, a pair of degree $n-1$ polynomials $(f(x), g(x))$ with $w$ total nonzero coefficients with some $\lambda \in R$ such that $(ff^* + gg^*)(x) = \lambda$ shall also be referred to as a $CP(n, w, S, R)$.

When the coefficient set of a complementary pair is a subset of $\{0, \pm 1\}$, as in the case of all complementary pairs beyond this chapter, then one can say more about the $\lambda$ in Theorem 2.1.7.

**Lemma 2.1.8.** Suppose $n, w \in \mathbb{Z}^+$, $S \subseteq \{0, \pm 1\}$ is a coefficient set, and $(f(x), g(x))$ is a $CP(n, w, S)$. Then $(ff^* + gg^*)(x) = w$.

*Proof.* The $\lambda$ in Theorem 2.1.7 satisfies $\lambda = \sum_{i=0}^{n-1} f_i^2 + \sum_{i=0}^{n-1} g_i^2$, which is the weight of $(f(x), g(x))$ as every nonzero element of $S$ squares to 1. □

As previously mentioned, the polynomial representation of complementary pairs is more algebraically revealing than the sequence representation. This is exemplified in the following lemma.

**Lemma 2.1.9** (Folklore)**.** Let $S$ be a coefficient set in a unique factorization domain $R$, let $\lambda \in R$ be nonzero, and let $(f(x), g(x))$ be complementary over $S$ such that $(ff^* + gg^*)(x) = \lambda$. Then $f(x)$ and $g(x)$ are relatively prime.

*Proof.* As $f(x)$ and $g(x)$ are polynomials over a subset of a unique factorization domain, greatest common divisors are well-defined. Let $h(x) = \gcd(f(x), g(x))$ and $k(x), r(x)$ be such that $f(x) = h(x)k(x)$ and $g(x) = h(x)r(x)$. Then

$$\begin{aligned}(ff^* + gg^*)(x) &= (hh^*kk^* + hh^*rr^*)(x) \\ &= hh^*(x)(kk^* + rr^*)(x).\end{aligned}$$

As $(ff^* + gg^*)(x) = \lambda \neq 0$, one obtains $hh^*(x)(kk^* + rr^*)(x) = \lambda \neq 0$. Let $m \in \mathbb{Z}$ be the greatest power of $x$ in $(kk^* + rr^*)(x)$. To see that $m \geqslant 0$, suppose that $m < 0$. Then since $(kk^* + rr^*)^*(x) = (kk^* + rr^*)(x)$, one obtains $-m$ as a positive power of $x$ in $(kk^* + rr^*)(x)$, contradicting $m < 0$ being the greatest power of $x$. Now, if $h(x)$ is not a unit, then one can see that the greatest power of $x$ in $h(x)h^*(x)$ is greater than zero. Therefore, the greatest power of $x$ in $hh^*(x)(kk^* + rr^*)(x)$ is greater than zero, which is a contradiction since $hh^*(x)(kk^* + rr^*)(x) = \lambda$. Therefore, $h(x)$ is a unit and $f(x)$ and $g(x)$ are relatively prime. □

**Definition 2.1.10.** For a pair of polynomials $f(x)$ and $g(x)$, the sum $(ff^* + gg^*)(x)$ is referred to as their **Gram-sum**.

**Definition 2.1.11.** Let $M$ be a complex matrix, and $*$ its conjugate transpose. The **Gram matrix** of $M$ is the matrix $MM^*$ .

Gram matrices are used in many areas, including control theory where it is used to determine properties of a linear system. Gram matrices were first studied by the mathematician Jørgen Pedersen Gram (of Gram-Schmidt process fame), and the term Gram-sum is to reflect the connection that complementary pairs have to matrices, as is explored in more detail in Section 2.6.

The definition of complementary pairs assumes the sequences in the pair have the same length. However, reduced complementary pairs cannot be of different lengths, as is shown in the following lemma.

**Lemma 2.1.12.** Let $(F, G)$ be a reduced complementary pair, $n, m \in \mathbb{Z}^+$, and suppose $F$ and $G$ have lengths $n$ and $m$, respectively. Then $n = m$.

*Proof.* For sake of contradiction, assume $n > m$. Write $F = (f_i)_{i=0}^{n-1}$. Since $F$ is reduced, $f_0$ and $f_{n-1}$ are nonzero and thus $f_0 f_{n-1} \equiv 1 \pmod 2$. Since $n > m$, one obtains $AF_G(n-1) = 0$. Therefore, $AF_F(n-1) + AF_G(n-1) = f_0 f_{n-1} +$

$0 \equiv 1 \pmod 2$, hence $(F, G)$ is not complementary, a contradiction. Therefore, $n = m$. □

## 2.2 Symmetry

**Definition 2.2.1.** A polynomial $f(x)$ is **symmetric** if and only if $f(x) = f^*(x)$. A polynomial is **symmetric-equivalent** if and only if there exists $k \in \mathbb{Z}$ such that $f(x) = x^k f^*(x)$.

**Definition 2.2.2.** A polynomial $f(x)$ is **skew** if and only if $f(x) = -f^*(x)$. A polynomial is **skew-equivalent** if and only if there exists $k \in \mathbb{Z}$ such that $f(x) = -x^k f^*(x)$.

**Example 2.2.1.** The polynomial $f(x) = x^{-2}+1+x^2$ is symmetric as $f^*(x) = f(x)$, and the polynomial $g(x) = 1 - x$ is skew-equivalent as $-xg^*(x) = -x(1 - x^{-1}) = 1 - x = g(x)$. □

Note that any symmetric or skew polynomial has even degree. To see this, suppose $f(x)$ is symmetric or skew, and $n \in \mathbb{Z}^+$ is the highest power of $x$ in $f(x)$. Then as $f^*(x) \in \{f(x), -f(x)\}$, the highest power of $x$ in $f^*(x)$ is also $n$. It is seen that the lowest power of $x$ in $f(x)$ is the negative of the highest in $f^*(x)$, hence $\deg(f(x)) = n - (-n) = 2n$.

The preceding definitions can be misleading. By symmetric-equivalent and skew-equivalent, it is not meant that the polynomials can be multiplied by $x$ to some power to obtain a symmetric or skew polynomial. It is only meant that the conjugate can be multiplied by $x$ to some power to obtain the original polynomial or the negative thereof. For instance, the polynomial $g(x)$ in the previous example is skew-equivalent, but $g(x)$ cannot be multiplied by some power of $x$ to obtain a skew polynomial because $g(x)$ has odd degree.

When a polynomial in a complementary pair is symmetric-equivalent or skew-equivalent, further structure is often obtained.

**Lemma 2.2.3.** Let $S$ be a coefficient set and let $(f(x), g(x))$ be complementary over $S$ with $f(x)$ skew-equivalent such that $(ff^* + gg^*)(x) = \lambda$. Then $g(1)^2 = \lambda$.

*Proof.* Suppose $n \in \mathbb{Z}^+$ is such that $f(x) = \sum_{i=0}^{n-1} f_i x^i$. If $f(x)$ is skew-equivalent, then for each integer $i = 0, 1, \ldots, n-1$, one obtains $f_i = -f_{n-1-i}$. The term $f(1)$ is the sum of the coefficients of $f(x)$, so $f(1) = 0$. As $g^*(1) = g(1)$,

$$\begin{aligned}(ff^* + gg^*)(1) &= (gg^*)(1) \\ &= g(1)^2 \\ &= \lambda.\end{aligned}$$

□

## 2.3 Equivalence

Two complementary pairs can differ by some properties irrelevant to orthogonality and so are nevertheless similar pairs. These pairs are called equivalent (Definition 2.3.2) and the equivalence operations defining them are given in the following theorem.

**Theorem 2.3.1** (Based on [7])**.** Let $S$ be a coefficient set and $(f(x), g(x))$ be a complementary pair over $S$. Let $j \in \mathbb{Z}$ and $s \in S$ be nonzero. If the pairs obtained under the following operations have coefficients in $S$, then they are complementary over $S$:

1. Exchanging: exchanging the polynomials for each other;
2. Shifting: multiplying either polynomial by $x^j$;
3. Conjugating: replacing either polynomial with its conjugate;
4. Expanding: evaluating both polynomials at $x^j$;

5. Outer-scaling: multiplying both polynomials by $s$, or if $s^2 = 1$, then multiplying either polynomial by $s$;

6. Inner-scaling: evaluating both polynomials at $sx$.

7. Inverting any of the above operations, if possible.

*Proof.* Note that the right-hand side of equation (2.1.1) does not depend on $x$ and hence evaluating the left-hand side at any nonzero $x$ does not change the right-hand side.

1. Addition is commutative, so the order of the polynomials does not matter in equation (2.1.1).

2. Note that $(x^j f(x))^* = x^{-j} f^*(x)$ and hence $(x^j f(x))(x^j f(x))^* = f(x)f^*(x)$.

3. Follows from the fact that $(f^*(x))^* = f(x)$.

4. Follows by considering $(ff^* + gg^*)(x^j)$.

5. Follows from

$$(sf(x))(sf^*(x)) + (sg(x))(sg^*(x)) = s^2(ff^* + gg^*)(x)$$

and if $s^2 = 1$, then $(sf(x))(sf^*(x)) = f(x)f^*(x)$.

6. Follows by considering $(ff^* + gg^*)(sx)$. □

Note that the operations in Theorem 2.3.1 do not necessarily produce an equivalent complementary pair since the resultant pair can have coefficients outside the coefficient set. For example, consider the pair $(f(x), g(x)) = (1 + x, 1 - x)$, which is complementary over $\{\pm 1\}$. One can expand the pair to get $(f(x^2), g(x^2)) = (1+x^2, 1-x^2)$, whose coefficients fall outside of $\{\pm 1\}$. However, the pairs $(f(x), g(x))$ and $(f(x^2), g(x^2))$ are equivalent over $\{0, \pm 1\}$.

**Definition 2.3.2.** Let $S$ be a coefficient set and let $(f(x), g(x))$ and $(h(x), k(x))$ be two complementary pairs over $S$. The pairs $(f(x), g(x))$ and $(h(x), k(x))$ are **equivalent** relative to $S$ if and only if one can be obtained from the other by performing any number of operations in Theorem 2.3.1. Equivalence between pairs shall be denoted by "$\cong$".

**Example 2.3.1.** Consider the set $S = \{0, \pm 1\}$ and $f(x) = x^8 + x^9 - x^{10}, g(x) = -x^{-17} - x^{-15}$, which form a $TCP(3, 5)$. By Theorem 2.3.1, one can multiply $f(x)$ by $x^{-8}$ and $g(x)$ by $-x^{17}$ to get $(f(x), g(x)) \cong (1 + x - x^2, 1 + x^2)$. □

## 2.4 Constructions of complementary pairs

Different constructions exist for different kinds of complementary pairs. However, these constructions only differ because one desires the resultant pair to stay within the same coefficient set. The fact that the constructed pair is complementary comes from Theorem 2.4.1, which is essentially due to Turyn [27]. Methods of constructing new complementary pairs from old ones are also referred to as products.

**Theorem 2.4.1** (Turyn, 1974 [27])**.** Let $S$ be a coefficient set and let $(f(x), g(x))$ and $(h(x), k(x))$ be complementary pairs over $S$. Then

$$r(x) = f(x)h(x) + g(x)k(x),$$

$$s(x) = f(x)k^*(x) - g(x)h^*(x)$$

is a complementary pair (not necessarily over $S$).

*Proof.*

$$\begin{aligned}(rr^* + ss^*)(x) &= (f(x)h(x) + g(x)k(x))(f(x)h(x) + g(x)k(x))^* \\ &\quad + (f(x)k(x)^* - g(x)h^*(x))(f(x)k^*(x) - g(x)h^*(x))^* \\ &= f(x)f^*(x)h(x)h^*(x) + f(x)g^*(x)h(x)k^*(x) \\ &\quad + f^*(x)g(x)h^*(x)k(x) + g(x)g^*(x)k(x)k^*(x) \\ &\quad + f(x)f^*(x)k(x)k^*(x) - f(x)g^*(x)h(x)k^*(x) \\ &\quad - f^*(x)g(x)h^*(x)k(x) + g(x)g^*(x)h(x)h^*(x) \\ &= f(x)f^*(x)h(x)h^*(x) + g(x)g^*(x)k(x)k^*(x) \\ &\quad + f(x)f^*(x)k(x)k^*(x) + g(x)g^*(x)h(x)h^*(x) \\ &= (ff^* + gg^*)(x)(hh^* + kk^*)(x),\end{aligned}$$

and the result follows. □

**Example 2.4.1.** Consider $(f(x), g(x)) = (x^{-1} + 1 + x, x^{-1} + x)$ and $(h(x), k(x)) = (x^{-2} + 1 + x^2, x^{-2} + x^2)$, which are a $CP(3, 5, \mathbb{Z}_2)$ and a $CP(5, 5, \mathbb{Z}_2)$, respectively. Then by Theorem 2.4.1,

$$\begin{aligned}r(x) &= (x^{-1} + 1 + x)(x^{-2} + 1 + x^2) + (x^{-1} + x)(x^{-2} + x^2) \\ &= x^{-2} + x^{-1} + 1 + x + x^2, \text{ and} \\ s(x) &= (x^{-1} + 1 + x)(x^{-2} + x^2) + (x^{-1} + x)(x^{-2} + 1 + x^2) \\ &= x^{-2} + x^{-1} + x + x^2\end{aligned}$$

are complementary over $\mathbb{Z}_2$. It can be verified that $(r(x), s(x))$ is a $CP(5, 9, \mathbb{Z}_2)$. □

## 2.5 Restrictions on weight

As previously mentioned, the driving question for the study of complementary pairs is "for a given coefficient set $S$, which integers are the lengths and weights of complementary pairs over $S$?". There have only been two main results about the weights of complementary pairs, though one is trivial.

**Lemma 2.5.1.** Let $S$ be a coefficient set, $n, w \in \mathbb{Z}^+$, and $(f(x), g(x))$ be a $CP(n, w, S)$. Then $w \leqslant 2n$.

*Proof.* There are only $2n$ possible coefficients to be nonzero, so $w \leqslant 2n$. □

**Theorem 2.5.2** (Eliahou, Kervaire, and Saffari, 1990 [9])**.** Let $S \subseteq \mathbb{Z}$, let $n, w \in \mathbb{Z}^+$, let $p$ be a prime factor of $w$, and let $(f(x), g(x))$ be a $CP(n, w, S, \mathbb{Z})$ such that $(ff^* + gg^*)(x) = w$. If at least one coefficient of $f(x)$ or $g(x)$ is not divisible by $p$, then $p \not\equiv 3 \pmod 4$ and there exist $h(x), k(x) \in \mathbb{Z}_p[x, x^{-1}]$, a scalar $c \in \mathbb{Z}_p$ such that $c^2 = -1$, and $i \in \mathbb{Z}$ such that $f(x) = h(x)k(x)$ and $g(x) = cx^i h(x)k^*(x)$.

*Proof.* As $\mathbb{Z}_p[x, x^{-1}]$ is a principal ideal domain, greatest common divisors are well-defined. As at least one coefficient of $x$ in $f(x)$ or $g(x)$ is not divisible by $p$, at least one of the polynomials is nonzero and so the pair $(f(x), g(x))$ has a greatest common divisor in $\mathbb{Z}_p[x, x^{-1}]$. Let $h(x) = \gcd(f(x), g(x))$ and $k(x), r(x) \in \mathbb{Z}_p[x, x^{-1}]$ be such that $f(x) = h(x)k(x)$ and $g(x) = h(x)r(x)$. Then $(ff^* + gg^*)(x) = w = 0 \in \mathbb{Z}_p[x, x^{-1}]$, so

$$\begin{aligned}(ff^* + gg^*)(x) &= (hh^*kk^* + hh^*rr^*)(x) \\ &= h(x)h^*(x)(kk^* + rr^*)(x) \\ &= 0.\end{aligned}$$

Since $h(x) \neq 0$, one has $h^*(x) \neq 0$ and $h(x)h^*(x) \neq 0$. Therefore, as $\mathbb{Z}_p[x, x^{-1}]$ is an integral domain, one obtains $(kk^* + rr^*)(x) = 0$, that is, $k(x)k^*(x) = -r(x)r^*(x)$.

As $\gcd(k(x), r(x)) = 1$, there exist $c \in \mathbb{Z}_p$ and $i \in \mathbb{Z}$ such that $r(x) = cx^i k^*(x)$. Therefore, $f(x) = h(x)k(x)$ and $g(x) = cx^i h(x)k^*(x)$. Furthermore,

$$\begin{aligned}(kk^* + rr^*)(x) &= (kk^* + c^2 kk^*)(x) \\ &= (1 + c^2)kk^*(x) \\ &= 0.\end{aligned}$$

The polynomials $k(x)$ and $k^*(x)$ are nonzero in $\mathbb{Z}_p[x, x^{-1}]$ as otherwise both $f(x)$ and $g(x)$ would be zero. Therefore, the product $k(x)k^*(x)$ is nonzero and so $c^2 = -1$. It is well-known that $-1$ is a quadratic residue modulo $p$ if and only if $p \not\equiv 3 \pmod 4$ [23]. □

Eliahou, Kervaire, and Saffari originally proved Theorem 2.5.2 by using the sequence form of complementary pairs. Their proof takes up much of their eleven page paper. The authors [10] later used the polynomial form to prove the result, which significantly reduced their proof length.

Reciprocity laws relate the primes $p$ where a polynomial splits into linear factors in $\mathbb{Z}_p[x, x^{-1}]$. If $p$ divides the weight of a $TCP$, then the two polynomials in the $TCP$ split into the same number of factors over $\mathbb{Z}_p[x, x^{-1}]$. Theorem 2.5.2 establishes a connection between complementary pairs and polynomial splitting, though this is not mentioned by Eliahou, Kervaire, and Saffari:

**Corollary 2.5.3.** Let $n, w \in \mathbb{Z}^+$ and $(f(x), g(x))$ be a $CP(n, w, \mathbb{Z})$ such that $(ff^* + gg^*)(x) = w$. Then for all primes $p \mid w$, the two polynomials $f(x)$ and $g(x)$ split into the same number of irreducible factors over $\mathbb{Z}_p[x, x^{-1}]$.

*Proof.* By the proof of Theorem 2.5.2, there exist $h(x), k(x) \in \mathbb{Z}_p[x, x^{-1}]$, $c \in \mathbb{Z}_p$ such that $c^2 = -1$ and $i \in \mathbb{Z}$ such that $f(x) = h(x)k(x)$ and $g = cx^i h(x)k^*(x)$. By taking

the conjugate upon splitting, one sees that $k(x)$ splits into $m$ irreducible factors if and only if $k(x^{-1})$ does. The result follows. □

## 2.6 Orthogonal matrices

Complementary pairs can be used to construct orthogonal matrices. In particular, Golay pairs and ternary complementary pairs can be used to construct Hadamard and weighing matrices. Hadamard matrices are the most famous orthogonal matrices, and as previously mentioned, it is still an open question as to whether one exists in every order that is a multiple of 4. The most prominent constructions of orthogonal matrices using complementary pairs are covered in this section.

### 2.6.1 Orthogonal and circulant matrices

**Definition 2.6.1.** Let $S$ be a coefficient set, $n \in \mathbb{Z}^+$ and $M$ be an $n \times n$ matrix. Then $M$ is **orthogonal** of order $n$ if and only if there exists some scalar $\lambda$ such that $MM^\top = \lambda I$. If there are $w \in \mathbb{Z}^+$ nonzero entries in every row of $M$, then $M$ is said to have **weight** $w$.

**Example 2.6.1.** Consider the matrix $H = \begin{pmatrix} 1 & 1 \\ 1 & - \end{pmatrix}$. Then $HH^\top = 2I$, hence $H$ is orthogonal and is in fact a Hadamard matrix of order 2. □

Circulant matrices, like complementary pairs, have an equivalent polynomial expression.

**Definition 2.6.2.** For $n \in \mathbb{Z}^+$, let $X_n = \mathrm{circ}(0, 1, 0, \ldots, 0)$ be an $n \times n$ circulant matrix. If it is clear which $n$ is being used, "$X_n$" may be written simply as "$X$".

**Lemma 2.6.3.** Let $n \in \mathbb{Z}^+$ and $X = X_n$. Then

1. For all $k \in \mathbb{Z}$, $X^k = \mathrm{circ}(m_0, m_1, \ldots, m_{n-1})$, where $m_{k \pmod n} = 1$ and $m_i = 0$ for all $i \neq k \pmod n$;

2. $X^{-1} = X^{n-1} = X^\top$;

3. An $n \times n$ matrix is circulant if and only if it is a polynomial in $X$;

4. The transpose of a circulant matrix is circulant;

5. All $n \times n$ circulant matrices commute;

6. The product of circulant matrices is also circulant.

*Proof.*

1. If the rows of an $n \times n$ matrix $M$ are $r_0, r_1, \ldots, r_{n-1}$ in order, then it is easy to see that the rows of $XM$ are $r_1, r_2, \ldots, r_{n-1}, r_0$ in order. Thus $X^2 = \mathrm{circ}(0, 0, 1, 0, \ldots, 0)$, $X^3 = \mathrm{circ}(0, 0, 0, 1, 0, \ldots, 0)$, $\ldots$, $X^{n-1} = \mathrm{circ}(0, 0, \ldots, 0, 1)$, and $X^n = \mathrm{circ}(1, 0, 0, \ldots, 0) = I$. Let $q, r \in \mathbb{N}$ be such that $k = qn + r$ with $0 \leqslant r < n$. Then

$$X^k = X^{qn+r} = X^{q^n} X^r = X^r,$$

and the claim follows.

2. By part 1 one sees that $X^n = XX^{n-1} = X^{n-1}X = I$. One can verify directly that $X^\top = X^{n-1}$, so the claim follows.

3. Let $M = \mathrm{circ}(m_0, m_1, \ldots, m_{n-1})$. Then

$$M = M(X) = m_0 I + m_1 X + m_2 X^2 + \cdots + m_{n-1} X^{n-1}.$$

For the converse, one sees that if

$$M = M(X) = m_0 I + m_1 X + m_2 X^2 + \cdots + m_{n-1} X^{n-1}$$

then $M = \text{circ}(m_0, m_1, \ldots, m_{n-1})$.

4. For any circulant matrix $M(X)$, it is seen that $M(X)^\top = M(X^\top)$. By part 2, one obtains $M(X^\top) = M(X^{n-1})$, which is a polynomial in $X$. The result follows from part 3.

5. By part 3, all circulant matrices are polynomials in $X$. $X$ commutes with itself, so the result follows.

6. A product of polynomials in $X$ is another polynomial in $X$ and is thus a circulant matrix. □

**Example 2.6.2.** Consider the circulant matrix

$$M = \text{circ}(1, 2, 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}.$$

By letting $X = X_3 = \text{circ}(0, 1, 0)$, one sees that $M = M(X) = I + 2X + 3X^2$. □

Note that by part 3 of Lemma 2.6.3, $n \times n$ circulant matrix arithmetic is equivalent to polynomial arithmetic in $\dfrac{R[x, x^{-1}]}{x^n - 1}$.

**Lemma 2.6.4.** Fix $n \in \mathbb{Z}^+$ and an integral domain $R$. Let $\lambda \in R$ and suppose $f_1(x), f_2(x), \ldots, f_n(x) \in R[x, x^{-1}]$ satisfy

$$f_1(x) f_1(x^{-1}) + f_2(x) f_2(x^{-1}) + \cdots f_n(x) f_n(x^{-1}) = \lambda.$$

Then the circulant matrices $f_1(X), f_2(X), \ldots, f_n(X)$ satisfy

$$f_1(X)f_1(X^{-1}) + f_2(X)f_2(X^{-1}) + \cdots f_n(X)f_n(X^{-1}) = \lambda I.$$

*Proof.* As

$$f_1(x)f_1(x^{-1}) + f_2(x)f_2(x^{-1}) + \cdots f_n(x)f_n(x^{-1}) = \lambda, \text{ one obtains}$$
$$f_1(x)f_1(x^{-1}) + f_2(x)f_2(x^{-1}) + \cdots f_n(x)f_n(x^{-1}) \equiv \lambda \pmod{x^n - 1},$$

and the result follows. □

### 2.6.2 Basic construction

**Lemma 2.6.5** (Folklore)**.** Let $S$ be a coefficient set, $n, w \in \mathbb{Z}^+$, and $(F, G)$ be a $CP(n, w, S)$. Let $f(X) = \text{circ}(f_0, f_1, \ldots, f_{n-1})$ and $g(X) = \text{circ}(g_0, g_1, \ldots, g_{n-1})$. Then $M = \begin{pmatrix} f(X) & g(X) \\ -g(X^{-1}) & f(X^{-1}) \end{pmatrix}$ is an orthogonal matrix of order $2n$ and weight $w$.

*Proof.* As $f(X)$ and $g(X)$ have length $n$ and weight $w$, the matrix $M$ is a $2n \times 2n$ matrix that has $w$ nonzero entries in each row. One can see by inspection and by using part 2 of Lemma 2.6.3 that $f(X)^\top = f(X^\top) = f(X^{-1})$ and $g(X)^\top = g(X^\top) =$

$g(X^{-1})$. Now,

$$\begin{aligned}
MM^\top &= \begin{pmatrix} f(X) & g(X) \\ -g(X^{-1}) & f(X^{-1}) \end{pmatrix} \begin{pmatrix} f(X)^\top & -g(X^{-1})^\top \\ g(X)^\top & f(X^{-1})^\top \end{pmatrix} \\
&= \begin{pmatrix} f(X) & g(X) \\ -g(X^{-1}) & f(X^{-1}) \end{pmatrix} \begin{pmatrix} f(X^{-1}) & -g(X) \\ g(X^{-1}) & f(X) \end{pmatrix} \\
&= \begin{pmatrix} f(X)f(X^{-1}) + g(X)g(X^{-1}) & -f(X)g(X) + g(X)f(X) \\ -g(X^{-1})f(X^{-1}) + f(X^{-1})g(X^{-1}) & f(X)f(X^{-1}) + g(X)g(X^{-1}) \end{pmatrix} \\
&= \begin{pmatrix} wI_n & 0_n \\ 0_n & wI_n \end{pmatrix} \\
&= wI_{2n},
\end{aligned}$$

proving the claim. □

**Example 2.6.3.** Consider $F = (111-)$ and $G = (11-1)$, a $GP(4)$. The circulant matrices with first rows $F$ and $G$ are

$$f(X) = I + X + X^2 - X^3 = \mathrm{circ}(111-) = \begin{pmatrix} 1 & 1 & 1 & - \\ - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \\ 1 & 1 & - & 1 \end{pmatrix} \text{ and}$$

$$g(X) = I + X - X^2 + X^3 = \mathrm{circ}(11-1) = \begin{pmatrix} 1 & 1 & - & 1 \\ 1 & 1 & 1 & - \\ - & 1 & 1 & 1 \\ 1 & - & 1 & 1 \end{pmatrix},$$

respectively.

By Lemma 2.6.5, the matrix

$$H = \begin{pmatrix} f(X) & g(X) \\ -g(X)^\top & f(X)^\top \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & - & 1 & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - & 1 & 1 & - \\ - & 1 & 1 & 1 & 1 & - & 1 & 1 \\ 1 & - & 1 & 1 & 1 & 1 & - & 1 \\ 1 & 1 & - & 1 & 1 & 1 & 1 & - \\ - & 1 & 1 & - & 1 & 1 & 1 & 1 \\ 1 & - & 1 & 1 & - & 1 & 1 & 1 \\ 1 & 1 & - & 1 & 1 & - & 1 & 1 \end{pmatrix}$$

is a Hadamard matrix of order 8. □

### 2.6.3 Williamson array

**Theorem 2.6.6** (Williamson, 1944 [28])**.** Let $m \in \mathbb{Z}^+$, $\lambda$ be a scalar, and $a(X)$, $b(X)$, $c(X)$, and $d(X)$ be $m \times m$ symmetric circulant matrices such that any two matrices commute and such that $a(X)^2 + b(X)^2 + c(X)^2 + d(X)^2 = \lambda I$. Then the **Williamson array**

$$W = \begin{pmatrix} a(X) & b(X) & c(X) & d(X) \\ -b(X) & a(X) & -d(X) & c(X) \\ -c(X) & d(X) & a(X) & -b(X) \\ -d(X) & -c(X) & b(X) & a(X) \end{pmatrix}$$

is an orthogonal matrix.

*Proof.* First, let $I = I_m$ and $0 = 0_m$. By Lemma 2.6.3, one has that $a(X), b(X), c(X)$, and $d(X)$ commute. Furthermore, as $a(X), b(X), c(X)$, and $d(X)$ are symmetric,

they are equal to their transposes. Using this information, one calculates

$$
\begin{aligned}
WW^\top &= \begin{pmatrix} a(X) & b(X) & c(X) & d(X) \\ -b(X) & a(X) & -d(X) & c(X) \\ -c(X) & d(X) & a(X) & -b(X) \\ -d(X) & -c(X) & b(X) & a(X) \end{pmatrix} \begin{pmatrix} a(X) & -b(X) & -c(X) & -d(X) \\ -b(X) & a(X) & d(X) & c(X) \\ c(X) & -d(X) & a(X) & b(X) \\ d(X) & c(X) & -b(X) & a(X) \end{pmatrix} \\
&= \begin{pmatrix} \lambda I & 0 & 0 & 0 \\ 0 & \lambda I & 0 & 0 \\ 0 & 0 & \lambda I & 0 \\ 0 & 0 & 0 & \lambda I \end{pmatrix} \\
&= \lambda I_{4m}.
\end{aligned}
$$

□

One can construct orthogonal matrices by using complementary pairs and a Williamson array as follows: take two complementary pairs of the same order, say $(f(x), g(x))$ and $(g(x), k(x))$. Form the four circulant matrices $f(X), g(X), h(X)$, and $k(X)$. If these circulant matrices are symmetric, then by Lemma 2.6.4, the Williamson array of those matrices is orthogonal.

### 2.6.4 Goethals—Seidel construction

The next construction was given by Goethals and Seidel [13] in 1970, and is a generalization of the Williamson construction.

**Theorem 2.6.7** (Goethals and Seidel, 1970 [13])**.** Let $m \in \mathbb{Z}^+$, $\lambda$ a scalar, $R$ be the $m \times m$ matrix whose back-diagonal is all 1s and every other entry is 0, and let $a(X), b(X), c(X)$, and $d(X)$ be circulant matrices of order $m$ such that

$$a(X)a(X)^\top + b(X)b(X)^\top + c(X)c(X)^\top + d(X)d(X)^\top = \lambda I_m.$$

The **Goethals—Seidel array** for $a(X)$, $b(X)$, $c(X)$, and $d(X)$ is

$$M = \begin{pmatrix} a(X) & b(X)R & c(X)R & d(X)R \\ -b(X)R & a(X) & -d(X)^\top R & c(X)^\top R \\ -c(X)R & d(X)^\top R & a(X) & -b(X)^\top R \\ -d(X)R & -c(X)^\top R & b(X)^\top R & a(X) \end{pmatrix},$$

and satisfies $MM^\top = \lambda I_{4m}$.

*Proof.* For any circulant $m \times m$ matrix $p(X)$, the matrix $p(X)R$ is symmetric. To see this, note that post-multiplying a matrix by $R$ reverses the entries in the rows of said matrix. Thus if $p(X) = \mathrm{circ}(p_0, p_1, \ldots, p_{n-1})$, the first row of $p(X)R$ is $(p_{n-1}, p_{n-2}, \ldots, p_0)$. Now let $Q = p(X)R$ and for $i, j \in \mathbb{Z}$ denote the $(i, j)$-entry of $Q$ by $q_{i,j}$. Since each row in $p(X)$ was a right-cyclic shift of the row above, each row of $Q$ is a left-cyclic shift of the row above. Thus $q_{i,j} = q_{i+1,j-1}$ (where indices are taken modulo $n$). Therefore, for all $k \in \mathbb{Z}$, one obtains $q_{i,j} = q_{i+k,j-k}$. Taking $k = j - i$ shows that $q_{i,j} = q_{j,i}$ and thus $p(X)R = (p(X)R)^\top = R^\top p(X)^\top$. Therefore, $p(X)R$ is symmetric.

Next, note that $R^\top = R$ and $R^2 = I_m$, hence for any circulant matrix $p(X)$, one obtains $p(X)R = Rp(X)^\top$. This property, along with parts 4 and 5 of Lemma 2.6.3, are used to show that $M$ satisfies $MM^\top = \lambda I_{4m}$: one simply computes $MM^\top$ in polynomial form. For instance, the $(1, 2)$-entry of $MM^\top$ (in polynomial form) is

$$\begin{aligned} &- a(X)Rb(X)^\top + b(X)Ra(X)^\top - c(X)RRd(X) + d(X)RRc(X) \\ &= -a(X)b(X)R + b(X)a(X)R - c(X)d(X) + d(X)c(X) \\ &= (a(X)b(X)R - a(X)b(X)R) + (c(X)d(X) - c(X)d(X)) \\ &= 0_m + 0_m \\ &= 0_m. \end{aligned}$$

One can similarly show that the other non-diagonal elements are 0. The diagonal elements of $MM^\top$ in polynomial form are seen to be

$$\begin{aligned}
&a(X)a(X)^\top + b(X)RRb(X)^\top c(X)RRc(X)^\top + d(X)RRd(X)^\top \\
&= a(X)a(X)^\top + b(X)b(X)^\top c(X)c(X)^\top + d(X)d(X)^\top \\
&= \lambda I_m.
\end{aligned}$$

Therefore, $MM^\top = \lambda I_m$. □

**Corollary 2.6.8.** Let $S$ be a coefficient set in an integral domain $R$, $n, u, w \in \mathbb{Z}^+$, and suppose $(f(x), g(x))$ and $(h(x), k(x))$ are a $CP(n, w, S)$ and $CP(n, u, S)$, respectively. Then the Goethals—Seidel array of $f(X), g(X), h(X), k(X)$ is orthogonal of order $4n$ and weight $u + w$.

*Proof.* Since $(f(x), g(x))$ and $(h(x), k(x))$ are a $CP(n, w, S)$ and $CP(n, u, S)$, respectively, there exists a $\lambda \in R$ such that

$$f(x)f(x^{-1}) + g(x)g(x^{-1}) + h(x)h(x^{-1}) + k(x)k(x^{-1}) = \lambda.$$

Therefore,

$$f(X)f(X)^\top + g(X)g(X)^\top + h(X)h(X)^\top + k(X)k(X)^\top = \lambda I_n$$

and the result follows from Theorem 2.6.7. □

# 3

# Golay Pairs

Golay pairs were the first complementary pairs to appear in the literature and it is their mysterious structure and numerous applications to engineering that have inspired research into complementary pairs. The most basic question about their structure—for which lengths do they exist—remains open. This chapter examines the known structure of Golay pairs, including basic properties, constructions of new Golay pairs from old, and restrictions on lengths.

For economy, a polynomial $f(x)$ shall be written simply as $f$ when no confusion can arise.

## 3.1 Preliminaries

Like all complementary pairs, there are several equivalence operations one can perform on a Golay pair. However, the operation of expanding in Theorem 2.3.1 is not an equivalence operation of $GP$s. This is because if $(f(x), g(x))$ is a $GP$, then for any $j \in \mathbb{Z}$ with $|j| > 1$, the polynomials $f(x^j)$ and $g(x^j)$ are polynomials over $\{0, \pm 1\}$, not $\{\pm 1\}$.

**Theorem 3.1.1.** Let $n \in \mathbb{Z}^+$ and $(f, g)$ be a Golay pair of length $n$. The pairs obtained under the following operations are also Golay pairs of length $n$:

1. Exchanging: exchanging the two polynomials for each other;
2. Shifting: for $j \in \mathbb{Z}$, multiplying either polynomial by $x^j$;
3. Conjugating: replacing either polynomial with its conjugate;
4. Negating: multiplying either polynomial by $-1$;
5. Alternating: negating every second coefficient of both polynomials.

*Proof.* Note that none of the above operations change a coefficient of either polynomial to be something other than $\pm 1$, hence the result follows from Theorem 2.3.1. □

**Definition 3.1.2.** Two Golay pairs are **equivalent** if and only if one can be obtained from the other through any of the operations in Theorem 3.1.1.

**Corollary 3.1.3.** Let $n \in \mathbb{Z}^+$. Every Golay pair of length $n$ is equivalent to a length $n$ pair $(f, g) = \left(\sum_{i=0}^{n-1} f_i x^i, \sum_{i=0}^{n-1} g_i x^i\right)$ where $f_0 = f_{n-1} = g_0 = 1$ and $g_{n-1} = -1$.

*Proof.* Let $\alpha, \beta \in \mathbb{Z}$ and $(h, k) = (x^\alpha \sum_{i=0}^{n-1} h_i x^i, x^\beta \sum_{i=0}^{n-1} k_i x^i)$ be a $GP(n)$. By Theorem 3.1.1, $(h, k)$ can be shifted so that $(h, k) \cong (\sum_{i=0}^{n-1} h_i x^i, \sum_{i=0}^{n-1} k_i x^i)$. Examining autocorrelation coefficients yields

$$AF_H(n-1) + AF_K(n-1) = h_0 h_{n-1} + k_0 k_{n-1} = 0.$$

Therefore, either $h_0 = h_{n-1}$ and $k_0 \neq k_{n-1}$ or vice versa. By possibly exchanging the two polynomials, one can assume without loss of generality that $h_0 = h_{n-1}$ and $k_0 \neq k_{n-1}$. By possibly negating, one can assume without loss of generality that $h_0 = h_{n-1} = k_0 = 1$ and $k_{n-1} = -1$. □

**Definition 3.1.4.** A polynomial is said to be **normalized** if and only if the least power of $x$ in the polynomial is zero.

**Example 3.1.1.** Consider the polynomials $f = -x^{-2} - x^{-1}$ and $g = x^8 - x^9$. One can multiply $f$ and $g$ by $x^2$ and $x^{-8}$, respectively, to obtain the (normalized) equivalent pair $(-1-x, 1-x)$. Multiplying $-1-x$ by $-1$ yields the equivalent pair $(1+x, 1-x)$, which has a nicer representation than the pair $(f, g)$. □

## 3.2 Constructions

Golay found Golay pairs of lengths $10, 26$, and all nonnegative powers of 2 [14], [15], [16], [17]. An example of a Golay pair for each length $\leqslant 26$ is included in Table 3.1.

| Length | $F$ | $G$ |
|---|---|---|
| 1 | (1) | (1) |
| 2 | (11) | (1-) |
| 4 | (111-) | (11-1) |
| 8 | (111-11-1) | (111---1-) |
| 10 | (11-1-1--11) | (11-11111--) |
| 16 | (111-11-1111---1-) | (111-11-1---111-1) |
| 20 | (11-1-1--1111-11111--) | (11-1-1--11--1-----11) |
| 26 | (1111-11-1-1-1-1-111-111) | (1111-11-1-11111-1--11--) |

Table 3.1: Golay pairs of all possible lengths $\leqslant 26$, from Borwein and Ferguson [1].

**Corollary 3.2.1** (Golay, 1961 [16])**.** Let $n \in \mathbb{Z}^+$ and $(f, g)$ be a normalized $GP(n)$. Then $(f(x)+x^n g(x), f(x)-x^n g(x))$ and $(f(x^2)+xg(x^2), f(x^2)-xg(x^2))$ are $GP(2n)$s.

*Proof.* By Theorem 3.1.1, the pair $(f(x), x^n g(x))$ is complementary. Take $(f(x), x^n g(x))$ along with $(h, k) = (1, 1)$ in Theorem 2.4.1 to see that $(f(x) + x^n g(x), f(x) - x^n g(x))$ is a complementary pair.

By Theorem 3.1.1, the pair $(f(x^2), xg(x^2))$ is complementary. Again by taking $(f(x^2), xg(x^2))$ along with $(h, k) = (1, 1)$ in Theorem 2.4.1 one sees that $(f(x^2) + xg(x^2), f(x^2) - xg(x^2))$ is complementary.

To see that the resultant pairs are polynomials over $\{\pm 1\}$, let $f(x) = \sum_{i=0}^{n-1} f_i x^i$ and $g(x) = \sum_{i=0}^{n-1} g_i x^i$. Then

$$f(x) \pm x^n g(x) = f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \pm (g_0 x^n + g_1 x^{n+1} + \cdots + g_{n-1}x^{2n-1}),$$

and

$$f(x^2) \pm xg(x^2) = f_0 \pm g_0 x + f_1 x^2 \pm g_1 x^3 + \cdots + f_{n-1}x^{2n-2} \pm g_{n-1}x^{2n-1}.$$

Therefore, all polynomials are over $\{\pm 1\}$. □

**Example 3.2.1.** To illustrate Corollary 3.2.1, consider the problem of constructing Golay pairs for all lengths that are powers of 2. Beginning with the pair $(1, 1)$, one can double this pair using the first construction in Corollary 3.2.1 to get $(1+x, 1-x)$, a $GP(2)$. One can then double this new pair to get $(1 + x + x^2 - x^3, 1 + x - x^2 + x^3)$, a $GP(4)$. This process can be repeated to obtain a Golay pair of every length that is a power of 2. □

**Theorem 3.2.2** (Golay, 1961 [16])**.** Let $n, m \in \mathbb{Z}^+$ and $(f, g), (h, k)$ be a normalized $GP(n)$ and $GP(m)$, respectively. Then

$$r(x) = f(x)h(x^n) + x^{nm}g(x)k(x^n),$$

$$s(x) = f(x)k^*(x^n) - x^{nm}g(x)h^*(x^n)$$

is a $GP(2nm)$.

*Proof.* By Theorem 3.1.1, the pairs $(f(x), x^{nm}g(x))$ and $(h(x^n), k(x^n))$ are complementary. The fact that $(rr^* + ss^*)(x) = 4nm$ now follows from Theorem 2.4.1. To

see that $r(x)$ and $s(x)$ have coefficients $\pm 1$, observe that

$$\begin{aligned} r(x) = h_0 &\left(f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}\right) \\ &+ h_1 \left(f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}\right) x^n \\ &\vdots \\ &+ h_{m-1} \left(f_0 + f_1 x + \cdots + f_{n-1}x^{n-1}\right) x^{nm-n} \\ &+ k_0 \left(g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}\right) x^{nm} \\ &+ k_1 \left(g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}\right) x^{nm+n} \\ &\vdots \\ &+ k_{m-1} \left(g_0 + g_1 x + \cdots + g_{n-1}x^{n-1}\right) x^{2nm-n}, \end{aligned}$$

which is $r(x)$ written with powers of $x$ in increasing order. For every integer $b$, one sees that there exist $i, j \in \mathbb{Z}$ such that the coefficient of $x^b$ in $r(x)$ is $h_i f_j$ or $k_i g_j$. Since $f(x), g(x), h(x)$, and $k(x)$ are polynomials over $\{0, \pm 1\}$, so is $r(x)$. One can apply similar logic to show that $s(x)$ is a polynomial over $\{0, \pm 1\}$. □

**Definition 3.2.3.** The **support** of a polynomial $f(x) = \sum_{i \in \mathbb{Z}} f_i x^i$ is $S := \{j \in \mathbb{Z} : f_j \neq 0\}$.

**Definition 3.2.4.** A pair of polynomials is **disjoint** if and only if they have disjoint support.

**Example 3.2.2.** The polynomials $f(x) = 1 + x - x^6$ and $g(x) = x^2 + x^8$ have supports $\{0, 1, 6\}$ and $\{2, 8\}$, respectively, and are thus disjoint. □

Turyn was able to generalize Theorem 3.2.2 by observing that if $(f, g)$ is a normalized $GP(n)$, then $(f(x) + g(x), f(x) - g(x))$ is a disjoint complementary pair. Taking $(h, k) = (1, 1)$ in Theorem 2.4.1 shows that the pair $(f(x) + g(x), f(x) - g(x))$ is complementary. To see that the pair is disjoint, fix any integer $j$ such that $0 \leqslant j \leqslant n$ and compare $f_j + g_j$ to $f_j - g_j$. Since $f_j, g_j \in \{\pm 1\}$, if $f_j = g_j$ then

$f_j + g_j \in \{\pm 2\}$ and $f_j - g_j = 0$. If $f_j \neq g_j$ then $f_j + g_j = 0$ and $f_j - g_j \in \{\pm 2\}$. Therefore, $(f(x) + g(x), f(x) - g(x))$ is a disjoint complementary pair with coefficients $\{0, \pm 2\}$. Moreover, by outer-scaling both polynomials by $\frac{1}{2}$, it is seen that the pair $\left(\frac{1}{2}(f+g), \frac{1}{2}(f-g)\right)$ is a disjoint $TCP$.

**Theorem 3.2.5** (Turyn, 1974 [27])**.** Let $n, m \in \mathbb{Z}^+$ and $(f, g), (h, k)$ be a normalized $GP(n)$ and $GP(m)$, respectively. Then

$$r(x) = \frac{1}{2}(f(x) + g(x))h(x^n) + \frac{1}{2}(f(x) - g(x))k(x^n),$$

$$s(x) = \frac{1}{2}(f(x) + g(x))k^*(x^n) - \frac{1}{2}(f(x) - g(x))h^*(x^n)$$

is a $GP(nm)$.

*Proof.* Theorem 2.4.1 shows that $(r, s)$ is a complementary pair. By expanding $r(x) = \frac{1}{2}(f(x)+g(x))h(x^n)+\frac{1}{2}(f(x)-g(x))k(x^n)$ and $s(x) = \frac{1}{2}(f(x)+g(x))k^*(x^n)-\frac{1}{2}(f(x)-g(x))h^*(x^n)$ similarly to what is done in Theorem 3.2.2, one sees that the coefficients of $r(x)$ and $k(x)$ are all $\pm 1$. Since $(h, k)$ is a normalized pair, the highest power of $x$ in both $h(x)$ and $k(x)$ is $m - 1$. Therefore, the highest power of $x$ in $h(x^n)$ and $k(x^n)$ is $nm - n$. Since $AF_F(n-1) + AF_G(n-1) = f_0 f_{n-1} + g_0 g_{n-1} = 0$, a quick proof by contradiction shows that one has either $f_0 = g_0$ and $f_{n-1} \neq g_{n-1}$ or vice versa. Therefore, exactly one of $\frac{1}{2}(f+g)$ and $\frac{1}{2}(f-g)$ has least power of $x$ as zero, and the other has highest power of $x$ as $n - 1$. Therefore, the degrees of $r(x)$ and $s(x)$ are seen to be $(nm - n) + (n - 1) = nm - 1$. Theorem 2.4.1 shows that

$$
\begin{aligned}
(rr^* + ss^*)(x) &= \left(\frac{1}{2}(f+g)\frac{1}{2}(f^*+g^*) + \frac{1}{2}(f-g)\frac{1}{2}(f^*-g^*)\right)(x)\,(hh^* + kk^*)\,(x^n) \\
&= \frac{2m}{4}\left((f+g)(f^*+g^*) + (f-g)(f^*-g^*)\right)(x) \\
&= \frac{2m}{4}\,(2ff^* + 2gg^*)\,(x) \\
&= 2nm.
\end{aligned}
$$

Which shows that $(r, s)$ is a $GP(nm)$. □

**Example 3.2.3.** From $f(x) = 1 + x - x^2 + x^3$ and $g(x) = 1 + x + x^2 - x^3$, and $h(x) = 1 + x - x^2 + x^3 - x^4 + x^5 - x^6 - x^7 + x^8 + x^9$ and $k(x) = 1 + x - x^2 + x^3 + x^4 + x^5 + x^6 + x^7 - x^8 - x^9$, a $GP(4)$ and a $GP(10)$, one constructs

$$
\begin{aligned}
r(x) =&(1+x)(1 + x^4 - x^8 + x^{12} - x^{16} + x^{20} - x^{24} - x^{28} + x^{32} + x^{36}) \\
&- (x^2 - x^3)(1 + x^4 - x^8 + x^{12} + x^{16} + x^{20} + x^{24} + x^{28} - x^{32} - x^{36}) \\
=& - x^{39} + x^{38} + x^{37} + x^{36} - x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{30} - x^{29} - x^{28} + x^{27} \\
&- x^{26} - x^{25} - x^{24} + x^{23} - x^{22} + x^{21} + x^{20} + x^{19} - x^{18} - x^{17} - x^{16} + x^{15} - x^{14} \\
&+ x^{13} + x^{12} - x^{11} + x^{10} - x^9 - x^8 + x^7 - x^6 + x^5 + x^4 + x^3 - x^2 + x + 1,
\end{aligned}
$$

and

$$
\begin{aligned}
s(x) =&(1+x)(1 + x^{-4} - x^{-8} + x^{-12} + x^{-16} + x^{-20} + x^{-24} + x^{-28} - x^{-32} - x^{-36}) \\
&+ (x^2 - x^3)(1 + x^{-4} - x^{-8} + x^{-12} - x^{-16} + x^{-20} - x^{-24} \\
&- x^{-28} + x^{-32} + x^{-36}) \\
=&x^{39} - x^{38} + x^{37} + x^{36} + x^{35} - x^{34} + x^{33} + x^{32} - x^{31} + x^{30} - x^{29} - x^{28} + x^{27} \\
&- x^{26} + x^{25} + x^{24} - x^{23} + x^{22} + x^{21} + x^{20} + x^{19} - x^{18} + x^{17} + x^{16} - x^{15} + x^{14} \\
&+ x^{13} + x^{12} - x^{11} + x^{10} + x^9 + x^8 + x^7 - x^6 - x^5 - x^4 + x^3 - x^2 - x - 1,
\end{aligned}
$$

which form a $GP(40)$. □

**Corollary 3.2.6** (Turyn, 1974 [27]). For $a, b, c \in \mathbb{N}$, a $GP(2^a 10^b 26^c)$ exists.

## 3.3 Restrictions on length

Theorem 2.5.2 shows that the lengths of Golay pairs have no factors congruent to 3 (mod 4). Golay [16] who showed that the length of a Golay pair is 1 or even. This follows from the fact that a Golay pair of length $n$ can be used to construct a Hadamard matrix of order $2n$, as shown in the introduction. It is well-known that the orders of a Hadamard matrix are $1, 2$, or multiples of 4, which implies the result. However, the result can also be proved in a different, more structurally revealing way:

**Lemma 3.3.1** (Sum-product rule). Let $m \in \mathbb{Z}^+$ and $x_1, x_2, \ldots, x_{2m} \in \{\pm 1\}$ such that $\sum_{i=1}^{2m} x_i = 0$. Then $\Pi_{i=1}^{2m} x_i = (-1)^m$.

*Proof.* As $\sum_{i=1}^{2m} x_i = 0$ and each $x_i \in \{\pm 1\}$, exactly half the $x_i$s equal 1 and the other half equal $-1$. The number of $x_i$s is $2m$, so the result follows. □

**Lemma 3.3.2** (Golay, 1961 [16]). Let $n > 1$ be a positive integer, and let $f = \sum_{i=0}^{n-1} f_i x^i$, and $g = \sum_{i=0}^{n-1} g_i x^i$ form a $GP(n)$. Then for all integers $i$ such that $0 \leqslant i \leqslant n-1$, one has

$$f_i g_i f_{n-1-i} g_{n-1-i} = -1.$$

*Proof.* (Induction on $i$.) For nonnegative integers $i$, let $P(i)$ denote the statement that

$$f_i g_i f_{n-1-i} g_{n-1-i} = -1.$$

**Base case:** $P(0)$ says

$$f_0 g_0 f_{n-1} g_{n-1} = -1.$$

Since $n > 1$, one has $AF_F(n-1) + AF_G(n-1) = f_0 f_{n-1} + g_0 g_{n-1} = 0$. As $f_0 f_{n-1}, g_0 g_{n-1} \in \{\pm 1\}$, the Sum-Product Rule shows that $f_0 g_0 f_{n-1} g_{n-1} = -1$, showing $P(0)$ is true.

**Inductive step:** Fix an integer $k$ such that $0 \leqslant k \leqslant n-2$ and assume for all $0 \leqslant i \leqslant k$ that $P(i)$ is true, that is,

$$f_i g_i f_{n-1-i} g_{n-1-i} = -1.$$

Then since

$$\begin{aligned} 0 &= AF_f(n-1-(k+1)) + AF_g(n-1-(k+1)) \\ &= \sum_{i=0}^{k+1} \left(f_i f_{i+n-1-(k+1)}\right) + \sum_{i=0}^{k+1} \left(g_i g_{i+n-1-(k+1)}\right), \end{aligned}$$

the sum-product rule shows that

$$\begin{aligned} &(f_0 g_0 f_{n-1} g_{n-1})(f_1 g_1 f_{n-2} g_{n-2}) \cdots (f_{k+1} g_{k+1} f_{n-1-(k+1)} g_{n-1-(k+1)}) \\ &= (-1)^k (f_{k+1} g_{k+1} f_{n-1-(k+1)} g_{n-1-(k+1)}) \\ &= (-1)^{k+1}. \end{aligned}$$

Therefore, $(f_{k+1} g_{k+1} f_{n-1-(k+1)} g_{n-1-(k+1)}) = -1$ and so $P(k+1)$ is true.

**Conclusion:** Therefore, by the Principle of Mathematical Induction, for all integers $i$ such that $0 \leqslant i \leqslant n-1$, the statement $P(i)$ is true.

□

**Corollary 3.3.3** (Golay, 1961 [16])**.** The lengths of Golay pairs are 1 or even.

*Proof.* Suppose $k \in \mathbb{Z}^+$ is such that $n = 2k+1$ is the length of a reduced Golay pair

$(f, g)$. Then by Lemma 3.3.2,

$$-1 = f_k g_k f_{2k+1-1-k} g_{2k+1-1-k} = f_k^2 g_k^2 = 1,$$

a contradiction. □

# 4

# Ternary Complementary Pairs

The two main perspectives which $TCP$s have been studied from are a "length-first" perspective and a "weight-first" perspective. The length-first perspective seeks to solve which integers are the lengths of $TCP$s, and typically then focuses on the possible deficiencies for $TCP$s of that length. The weight-first perspective seeks to solve which integers are the weights of $TCP$s. Craigen and Koukouvinos [7] argued that the weight-first approach is more natural since equivalent $TCP$s can have different lengths and deficiency by Theorem 2.3.1. Moreover, Theorem 2.5.2, arguably the most profound result for $TCP$s, is about the weight of the pair, not the pair's length. This chapter derives the most fundamental results known about $TCP$s.

## 4.1 Preliminaries

The length of a Golay pair is always even or one. This is not the case for $TCP$s, which is now shown:

**Example 4.1.1.** Let $f = 1 + x - x^2, g = 1 + x^2, h = 1 + x^4$, and $k = 1 - x^4$. Then

$$(ff^* + gg^*)(x) = (1 + x - x^2)(1 + x^{-1} - x^{-2}) + (1 + x^2)(1 - x^{-2}) = 5, \text{ and}$$
$$(hh^* + kk^*)(x) = (1 + x^4)(1 + x^{-4}) + (1 - x^4)(1 - x^{-4}) = 4.$$

Therefore, the pairs $(f, g)$ and $(h, k)$ are a $TCP(3, 5)$ and $TCP(5, 4)$, respectively. □

The $TCP$s $(0, 0)$ and $(1, 0)$ shall be considered a $TCP(1, 0)$ and $TCP(1, 1)$, respectively. Pairs equivalent to these shall be called **trivial pairs**. The degrees of $(0, 0)$ and $(1, 0)$ shall be considered to be negative infinity and zero, respectively.

The only restriction on the weights or lengths of $TCP$s is from Theorem 2.5.2, which shows that no $TCP$ has a weight with a factor congruent to 3 modulo 4.

## 4.2 Constructions

### 4.2.1 Disjoint and conjoint pairs

**Definition 4.2.1.** A pair of polynomials are **conjoint** if and only if they have equal supports.

Recall from Definition 3.2.4 that a pair is disjoint if and only if they have disjoint supports.

**Example 4.2.1.** Let $f = 1 + x - x^2 - x^3$ and $g = 1 - x + x^2 - x^3$. Then $f$ and $g$ both have support $\{0, 1, 2, 3\}$, and are hence conjoint. However, $x^4 g(x)$ has support $\{4, 5, 6, 7\}$, which is disjoint from $\{0, 1, 2, 3\}$, so $(f(x), x^4 g(x))$ is a disjoint pair. □

**Lemma 4.2.2** (Craigen and Koukouvinos, 2001 [7])**.** Let $w \in \mathbb{Z}^+$ and $(f, g)$ be a disjoint $TCP$ with weight $w$. Then $(f + g, f - g)$ is a conjoint $TCP$ of weight $2w$.

*Proof.* Conjointness follows from the fact that $f$ and $g$ are disjoint. Take $(h, k) = (1, 1)$ in Theorem 2.4.1 to get that $(f + g, f - g)$ is a conjoint $TCP$ of weight $2w$. □

**Lemma 4.2.3** (Craigen and Koukouvinos, 2001 [7])**.** Let $w \in \mathbb{Z}^+$ and $(f, g)$ be a conjoint $TCP$ with weight $2w$. Then $(\frac{1}{2}(f+g), \frac{1}{2}(f-g))$ is a disjoint $TCP$ of weight $w$.

*Proof.* Take $(h, k) = (1, 1)$ in Theorem 2.4.1 to get that $(f + g, f - g)$ is a complementary pair. Since $f$ and $g$ are conjoint and have coefficients $\{0, \pm 1\}$, it follows that $f+g$ and $f-g$ have coefficients $\{0, \pm 2\}$. By Theorem 2.3.1, outer-scaling $(f+g, f-g)$ by $\frac{1}{2}$ yields that $(\frac{1}{2}(f+g), \frac{1}{2}(f-g))$ is a complementary pair over $\{0, \pm 1\}$. A similar argument to the comment after Example 3.2.2 shows that $(\frac{1}{2}(f + g), \frac{1}{2}(f - g))$ is disjoint. □

Note that any conjoint pair necessarily has even weight. Thus the previous two lemmas show that any disjoint pair can be turned into a conjoint pair and vice versa. As any Golay pair can be turned into a reduced pair, Golay pairs are ideal for generating disjoint $TCP$s. Furthermore, finding disjoint $TCP$s can be conducive to constructing a Golay pair.

### 4.2.2 Standard multiplication

Standard multiplication is given in the following theorem, which uses the sequence form of $TCP$s. The application of disjoint and conjoint pairs to the theorem is immediate.

**Theorem 4.2.4** (Gavish and Lempel, 1994 [11])**.** Let $n, m, w, z \in \mathbb{Z}^+$, and suppose $(F, G)$ and $(H, K)$ are a $TCP(n, w)$ and a $TCP(m, z)$ (not necessarily reduced), respectively, with one of the pairs disjoint. In particular, there is no assumption

that either of the pairs are reduced. Then

$$r(x) = f(x)h(x^n) + g(x)k(x^n),$$

$$s(x) = f(x)k^*(x^n) - g(x)h^*(x^n)$$

is a $TCP$ with weight $wz$.

*Proof.* The fact that $(rr^* + ss^*)(x) = wz$ follows from Theorem 2.4.1. Suppose without loss of generality that $F = (f_0, f_1, \ldots, f_{n-1})$, $G = (g_0, g_1, \ldots, g_{n-1})$, $H = (h_0, h_1, \ldots, h_{m-1})$, and $K = (k_0, k_1, \ldots, k_{m-1})$. For a scalar $\lambda$, let $\lambda F$ and $\lambda G$ denote the sequences $(\lambda f_0, \lambda f_1, \ldots, \lambda f_{n-1})$ and $(\lambda g_0, \lambda g_1, \ldots, \lambda g_{n-1})$, respectively. Then in block form,

$$\begin{aligned} R &= (h_0F, h_1F, \cdots, h_{m-1}F) \\ &\quad + (k_0G, k_1G, \cdots, k_{m-1}G) \\ &= (h_0F + k_0G, h_1F + k_1G, \cdots, h_{m-1}F + k_{m-1}G) \end{aligned}$$

where sequence addition is the same as vector addition. Either $F$ and $G$ or $H$ and $K$ are disjoint, hence $R$ is ternary. The case for $S$ follows similarly. □

**Example 4.2.2.** Consider $F = (\texttt{11-}), G = (\texttt{000101})$, a disjoint $TCP(3, 5)$, and $H = (\texttt{100-00-1}), K = (\texttt{10100011-})$, a $TCP(9, 10)$. The sequence forms of $F, G, H$, and $K$ are $f = 1 + x - x^2, g = x^3 + x^5$, $h = 1 - x^3 - x^4 - x^7 + x^8$, and $k = 1 + x^2 + x^6 + x^7 - x^8$, respectively. By Theorem 4.2.4, the pair $(r, s)$ defined by

$$\begin{aligned} r(x) &= f(x)h(x^6) + g(x)k(x^6) \\ &= -x^{53} - x^{51} - x^{50} + x^{49} + x^{48} + x^{47} + x^{45} + x^{44} - x^{43} - x^{42} + x^{41} + x^{39} \\ &\quad + x^{26} - x^{25} - x^{24} + x^{20} - x^{19} - x^{18} + x^{17} + x^{15} + x^5 + x^3 - x^2 + x + 1, \text{ and} \end{aligned}$$

$$
\begin{aligned}
s(x) &= f(x)k(x^{-6}) - g(x)h(x^{-6}) \\
&= -x^{-48}(x^{53} + x^{51} + x^{50} - x^{49} - x^{48} + x^{38} - x^{37} - x^{36} - x^{35} - x^{33} - x^{29} \\
&\quad - x^{27} + x^{14} - x^{13} - x^{12} - x^{11} - x^{9} + x^{8} - x^{7} - x^{6} + x^{5} + x^{3} - x^{2} + x + 1)
\end{aligned}
$$

is a $TCP$ with weight 50. □

### 4.2.3 Generalized multiplication

The idea behind generalized multiplication is that requiring one of the pairs in Theorem 4.2.4 to be disjoint is a stronger condition than necessary.

**Theorem 4.2.5** (Craigen, 2006 [3])**.** Let $w, z \in \mathbb{Z}^+$ and $(f, g), (h, k)$ be $TCP$s of weight $w$ and $z$, respectively. For all integers $i, j, n, m$, if

1. $i - j = n - m$ implies $f_i g_j k_n h_m = 0$, and
2. when $i \neq j$ and $n \neq m$, one obtains for all

$$(a, b, c, d) \in \{(f, f, h, h), (f, f, k, k), (g, g, h, h), (g, g, k, k)\}$$

that the equality $i - j = n - m$ implies $a_i b_j c_n d_m = 0$,

then

$$r = fh + gk,$$

$$s = fk^* - gh^*$$

is a $TCP$ of weight $wz$.

*Proof.* The fact that $(rr^* + ss^*)(x) = wz$ follows from Theorem 2.4.1.

In order to show $r$ and $s$ are ternary, it will be shown that every nonzero power of $x$ in $r(x)$ has at most one nonzero term total from $fh$ or $gk$, and similarly for $s(x)$. Fix an integer $p \neq 0$. The coefficient of $x^p$ in $f(x)h(x)$ is the sum of all terms of the

form $f_i h_m$ where $i + m = p$. Similarly, the coefficient of $x^p$ in $g(x)k(x)$ is the sum of all terms of the form $g_j h_n$ where $j + n = p$.

Now suppose $i + m = j + n = p$ with $i \neq j$ and $n \neq m$, and suppose $f_i h_m \neq 0$. To show that $f_j h_n = 0$, note that $i - j = n - m$ and take $(a, b, c, d) = (f, f, h, h)$ in Condition 2 to get $f_i f_j h_n h_m = (f_i h_m)(f_j h_n) = \pm f_j h_n = 0$, so one of $f_j$ and $h_n$ is zero. Thus in this case $fh$ only contributes one nonzero term to $x^p$. Now remove the assumptions that $i \neq j$ and $n \neq m$ and consider $g_j h_n$. By taking $(a, b, c, d) = (f, g, k, h)$, one sees that $f_i g_j k_n h_m = (f_i h_m)(g_j k_n) = \pm g_j k_n = 0$, so no term from $gk$ can contribute a nonzero term to $x^p$. One can repeat this procedure in the case that $g_i k_m \neq 0$ to show that $r(x)$ is a $(0, \pm 1)$-polynomial.

Fix an integer $p \neq 0$. The coefficient of $x^p$ in $fk^*$ is the sum of all terms of the form $f_i k_n$ where $i - n = p$. Similarly, the coefficient of $x^p$ in $-gh^*$ is the sum of all terms of the form $g_j h_m$ where $j - m = p$.

Now suppose $i - n = j - m = p$, with $i \neq j$ and $n \neq m$, and suppose $f_i k_n \neq 0$. To show that $f_j k_m = 0$, note that $i - j = n - m$ and take $(a, b, c, d) = (f, f, k, k)$ in Condition 2 to get $f_i f_j k_n k_m = (f_i k_n)(f_j k_m) = \pm f_j k_m = 0$. Thus $fk^*$ can contribute at most one nonzero term to $x^p$. Now remove the assumptions that $i \neq j$ and $n \neq m$ and consider the term $g_j h_m$. Note that again $i - j = n - m$ and take $(a, b, c, d) = (f, g, k, h)$ in Condition 1 to get that $f_i g_j k_n h_m = \pm g_j h_m = 0$. Therefore, no term from $gh^*$ can contribute a nonzero element to $x^p$. One can repeat this procedure when $g_j h_m \neq 0$ to show that $s(x)$ is a $(0, \pm 1)$-polynomial. □

One can verify that if one takes two ternary complementary pairs where one is disjoint, then the conditions of Theorem 4.2.5 are satisfied. What remains to show is that this new multiplication is indeed a proper generalization of the standard one. To this end, the following example is given.

**Example 4.2.3** (Craigen, 2006 [3])**.** Take $f(x) = 1 + x^2 - x^4$, $g(x) = 1 + x^4$ (a $TCP(5,5)$) and $h(x) = 1 + x^6 - x^{12}$, $k(x) = x^3 + x^{15}$ (a $TCP(13,5)$). By Theorem 4.2.5,

$$\begin{aligned} r &= fh + gk \\ &= (1 + x^2 - x^4)(1 + x^6 - x^{12}) + (1 + x^4)(x^3 + x^{15}) \\ &= 1 + x^2 + x^3 - x^4 + x^6 + x^7 + x^8 - x^{10} - x^{12} - x^{14} + x^{15} + x^{16} + x^{19}, \end{aligned}$$

and

$$\begin{aligned} s &= fk^* - gh^* \\ &= (1 + x^2 - x^4)(x^{-3} + x^{-15}) - (1 + x^4)(1 + x^{-6} - x^{-12}) \\ &= x^{-15}(1 + x^2 + x^3 - x^4 + x^7 - x^9 + x^{12} + x^{14} - x^{15} - x^{16} - x^{19}) \end{aligned}$$

is a $TCP(20,25)$ which can be verified to be unconstructable by smaller pairs through the standard multiplication. □

Craigen [3] showed a friendlier way of checking the conditions of Theorem 4.2.5.

**Definition 4.2.6.** For polynomials $f = \sum_{i\in\mathbb{Z}} f_i x^i$ and $g = \sum_{i\in\mathbb{Z}} g_i x^i$, define

$$D(f,g) := \{d \in \mathbb{Z} : \exists\, i,j \in \mathbb{Z} \text{ such that } d = j - i, \text{ and } g_j f_i \neq 0\}$$

and

$$A(f,g) := \{a \in \mathbb{Z}\backslash\{0\} : \exists\, i,j \in \mathbb{Z} \text{ such that } a = j - i, \text{ and either} f_i f_j \neq 0 \text{ or } g_i g_j \neq 0\}.$$

Then the conditions of the conditions of Theorem 4.2.5 are equivalent to $D(f,g) \cap D(k,h) = A(f,g) \cap A(k,h) = \varnothing$. To see this, suppose $D(f,g) \cap D(k,h) = A(f,g) \cap A(k,h) = \varnothing$ and $j - i = m - n$. Then either $f_i g_j = 0$ or $k_n h_m = 0$ and hence

$f_i g_j k_n h_m = 0$. Conversely, if $f_i g_j k_n h_m = 0$, then $j - i$ is not in one of $D(f, g)$ or $D(k, h)$. The other cases follow similarly.

## 4.3 Primitive pairs

With generalized multiplication established, it is natural to ask which $TCP$s cannot be constructed from other pairs. Such pairs are in a sense the "primes" of the $TCP$ world, and perhaps patterns within them will reveal general structure of $TCP$s.

**Definition 4.3.1.** A $TCP$ is **primitive** if and only if it can not be constructed using nontrivial pairs by the multiplication in Theorem 4.2.5. $TCP$s that are not primitive are called **imprimitive**.

The weight-first perspective focuses on the structure of primitive pairs. This is because if one has an imprimitive pair, then its weight is a product of the two primitive pairs constructing it. Therefore, the set of all weights of $TCP$s is the multiplicative closure of the set of all weights of primitive $TCP$s. Therefore, it is sufficient to solve for the weights of primitive pairs if one is looking to solve for the weights of all $TCP$s.

As general multiplication had not been discovered yet, Craigen, Georgiou, Gibson, and Koukouvinos [5] listed $TCP$s of weight $\leqslant 26$ that could not be constructed with nontrivial pairs under the standard multiplication. Craigen [3] later eliminated the pairs which were constructible under generalized multiplication. If a $TCP$ has prime weight, it is necessarily primitive as otherwise its weight would be the product of its factors' weights. However, a primitive $TCP(9, 8)$ exists, hence a primitive $TCP$ can have composite weight. From Craigen and Koukouvinos' table of primitive $TCP$s [5], it appears likely that every prime not congruent to 3 (mod 4) is the weight of

some primitive $TCP$. The authors notice this and conjecture it to always be the case:

**Conjecture 4.3.2.** Every prime not congruent to 3 modulo 4 is the weight of a primitive $TCP$.

If Conjecture 4.3.2 is true, then Theorem 2.5.2 would capture the structure of the weights of $TCP$s entirely because one could multiply primitive pairs together to achieve any weight that has no factors congruent to 3 modulo 4. Due to the computational complexity of generating $TCP$s, only primitive pairs up to length 21 have been fully classified and thus the validity of the conjecture is hard to test.

## 4.4 Symmetry and skewness

As noted in Chapter 2, symmetry and skewness are important concepts in complementary pairs. In the case of $TCP$s where one polynomial is skew, a simple construction for a new pair is obtained.

**Lemma 4.4.1.** Let $k, w \in \mathbb{Z}^+$, $n = 2k+1$, and $(f(x), g(x))$ be a pair of degree $n-1$ normalized $(0, \pm 1)$-polynomials with $w$ nonzero entries and $f(x)$ skew-equivalent. Then $(f(x), g(x))$ is a $TCP(n, w)$ if and only if $(f(x)+x^k, g(x))$ is a $TCP(n, w+1)$.

*Proof.* As $f(x)$ is skew-equivalent with odd-degree, the coefficient of $x^k$ in $f(x)$ is zero and thus $f(x)+x^k$ is a $(0, \pm 1)$-polynomial. As $x^k f^*(x) = -x^{-k} f(x)$, one obtains

$$\begin{aligned}(f(x)+x^k)(f(x)+x^k)^* + g(x)g^*(x) &= f(x)f^*(x) + x^{-k}f(x) + x^k f^*(x) \\ &\quad + 1 + g(x)g^*(x) \\ &= f(x)f^*(x) + x^{-k}f(x) - x^{-k}f(x) \\ &\quad + 1 + g(x)g^*(x) \\ &= w + 1. \end{aligned}$$

□

Let $n \in \mathbb{Z}^+$ and $(f(x), g(x))$ be a $TCP$ of length $n$. Examining $AF_F(n-1) + AF_G(n-1)$ will show that no two symmetric-equivalent or skew-equivalent polynomials can form a nontrivial $TCP$. However, a nontrivial pair where one is skew and the other is symmetric is possible, but only one such pair exists up to equivalence, as is now shown.

**Lemma 4.4.2** (Craigen and Koukouvinos, 2001 [7]). Let $n, w \in \mathbb{Z}^+$ and $(f, g)$ be a $TCP(n, w)$ with $f$ symmetric-equivalent and $g$ skew-equivalent. Then $w \in \{0, 1, 4\}$.

*Proof.* Suppose $n$ is even, say with $k \in \mathbb{Z}^+$ such that $n = 2k$. Without loss of generality, assume the least power of $x$ (should it exist) in $f$ and $g$ is 0. As $f$ is symmetric-equivalent and $g$ is skew-equivalent, there exist normalized $(0, \pm 1)$-polynomials $r(x) = \sum_{i=0}^{k-1} r_i x^i$ and $s(x) = \sum_{i=0}^{k-1} s_i x^i$ of degree $k-1$ such that $f = r + x^{2k-1} r^*$ and $g = s - x^{2k-1} s^*$. By Theorem 2.4.1, the polynomials

$$\begin{aligned} f + g &= r + x^{2k-1} r^* + s - x^{2k-1} s^*, \text{ and} \\ f - g &= r + x^{2k-1} r^* - s + x^{2k-1} s^* \\ &= x^{2k-1} \left( r^* + x^{-2k+1} r + s^* - x^{-2k+1} s \right) \\ &= x^{2k-1} \left( r + x^{2k-1} r^* + s - x^{2k-1} s^* \right)^* \\ &= x^{2k-1} (f + g)^* \end{aligned}$$

form a complementary pair over $\mathbb{Z}$. By Theorem 2.3.1, shifting $f - g$ yields that $(f + g, f - g) \cong (f + g, f + g)$ and so $(f + g, f + g)$ is a complementary pair as well. Therefore,

$$(f + g)(f + g)^* + (f + g)(f + g)^* = 2(f + g)(f + g)^* \in \mathbb{Z}.$$

If $f = -g$, then $f$ and $g$ have weight 0 as $f$ is symmetric-equivalent and $g$ is skew-equivalent. If $f \neq -g$, then $2(f + g)(f + g)^*$ has zero as its highest power of $x$ if and

only if $f+g$ has exactly one nonzero coefficient of $x$. Now

$$\begin{aligned} f+g &= \sum_{i=0}^{k-1}(r_i+s_i)x^i + x^{2k-1}\sum_{i=0}^{k-1}(r_i-s_i)x^{-i} \\ &= \sum_{i=0}^{k-1}(r_i+s_i)x^i + x^{k}\sum_{i=0}^{k-1}(r_{k-1-i}-s_{k-1-i})x^{i}. \end{aligned}$$

As $f+g$ has exactly one nonzero coefficient of $x$, then there is exactly one integer $i$ with $0 \leqslant i \leqslant k-1$ such that $r_i$ or $s_i$ is nonzero. Therefore, $f$ and $g$ have at most two nonzero coefficients each, hence when $n$ is even $w$ is either 0 or 4. The odd-length case follows similarly by considering the pairs $(f,g) = (r + x^k + x^{2k}r^*, s - x^{2k}s^*)$ and $(f,g) = (r + x^{2k}r^*, s - x^{2k}s^*)$. □

The $TCP$s with one polynomial symmetric-equivalent and the other skew-equivalent are all equivalent to $(0,0), (1,0)$, or $(11, 1-)$.

## 4.5 Small-deficiency pairs

The position of the zeros in $TCP$s with deficiency less than or equal to 3 can be completely classified. Furthermore, a complete classification of all $TCP$s with deficiency 1 can be obtained.

**Lemma 4.5.1** (Gavish and Lempel, 1994 [11])**.** The only integers $n$ such that a $TCP(n, 2n-1)$ exists are $n = 1$ and $n = 3$.

*Proof.* Let $(f,g)$ be a normalized $TCP(n, 2n-1)$ and $k \in \mathbb{Z}$ be such that $0 \leqslant k \leqslant n-1$ and $f_k = 0$. Without loss of generality, assume $k \leqslant \frac{n-1}{2}$ (otherwise take $f^*$). If $k < \frac{n-1}{2}$, then the coefficient of $x^{n-1-k}$ in $(ff^* + gg^*)(x)$ is odd and hence nonzero, since there is one zero coming from $f_k f_{n-1}$ and all of the other $2(k+1)-1$ terms are $\pm 1$. Therefore, $n = 2k+1$. Without loss of generality, assume $g_k = 1$ (otherwise take $-g$).

Now it will be shown that $f$ is symmetric-equivalent and $g - x^k$ is skew-equivalent. Note that from the proof of Lemma 3.3.2, for all $i < k$, one has $f_i + g_i + f_{n-1-i} + g_{n-1-i} \equiv 2 \pmod 4$ since no zeros have appeared in the two polynomials yet. Therefore, one obtains $f_i g_i f_{n-1-i} g_{n-1-i} = -1$. The coefficient of $x^{n-1-k}$ in $(ff^* + gg^*)(x)$ is

$$\begin{aligned}\sum_{i=0}^{k} f_i f_{n-1-k+i} + \sum_{i=0}^{k} g_i g_{n-1-k+i} &= f_{n-1-k} + f_k + \sum_{i=1}^{k-1} f_i f_{n-1-k+i} + \sum_{i=0}^{k} g_i g_{n-1-k+i} \\ &= 2f_k + \sum_{i=1}^{k-1} f_i f_{n-1-k+i} + \sum_{i=0}^{k} g_i g_{n-1-k+i} \\ &= \sum_{i=1}^{k-1} f_i f_{n-1-k+i} + \sum_{i=0}^{k} g_i g_{n-1-k+i}.\end{aligned}$$

As each of these $2k$ terms are $\pm 1$, by Lemma 3.3.1 one gets

$$g_0 g_{n-1} \Pi_{i=1}^{k-1} (f_i f_{n-1-k+i} g_i g_{n-1-k+i}) = (-1)^k.$$

However, it was shown for all integers $i < k$ that $f_i g_i f_{n-1-i} g_{n-1-i} = -1$. Therefore,

$$\begin{aligned}g_0 g_{n-1} \Pi_{i=1}^{k-1} (f_i f_{n-1-k+i} g_i g_{n-1-k+i}) &= g_0 g_{n-1} (-1)^{k-1} \\ &= (-1)^k,\end{aligned}$$

which implies $g_0 \neq g_{n-1}$ and thus $f_0 = f_{n-1}$. Examining the coefficients of $x^{n-2-k}$, $x^{n-3-k}, \ldots, x^1$ in $(ff^* + gg^*)(x))$ in this manner will yield for all $i < k$ that $f_i = f_{n-1-i}$ and $g_i \neq g_{n-1-i}$. Therefore, $f$ is symmetric-equivalent and $g - x^k$ is skew-equivalent. By Lemma 4.4.2, $2n - 2 \in \{0, 1, 4\}$, so $n = 1$ or $n = 3$. Furthermore, $(1, 0)$ and $(101, 11-)$ are two such pairs. □

**Lemma 4.5.2** (Gavish and Lempel, 1994 [11]). If $n \in \mathbb{Z}^+$ and $(f, g)$ is a normalized $TCP(n, 2n-2)$ and if $f_i = 0$, then one of $g_i$ or $g_{n-1-i}$ is 0.

*Proof.* Without loss of generality, assume $i$ is the least index such that $f_i, f_{n-1-i}, g_i$, or $g_{n-1-i}$ is zero. If all these other terms are 1, then the coefficient of $x^{n-1-i}$ in $(ff^* + gg^*)(x)$ is odd. If $f_{n-1-i} = 0$, then the coefficient of $x^{n-1-2i}$ in $(ff^* + gg^*)(x)$ is odd. Therefore one of $g_i$ and $g_{n-1-i}$ is 0. □

The deficiency 3 case follows more naturally in the Boolean complementary pair setting of Chapter 5. Therefore, a proof of Lemma 4.5.3 is delayed to Theorem 5.2.1.

**Lemma 4.5.3** (Gavish and Lempel, 1994 [11])**.** If $n \in \mathbb{Z}^+$ and $(f, g)$ is a normalized $TCP(n, 2n-3)$, then there exists an integer $m$ such that $n = 4m + 2$ and $f_m = g_{2m} = f_{3m+1} = 0$ or $g_m = f_{2m} = g_{3m+1} = 0$.

Although more can be said about $TCP$s than $GP$s, their structure is still largely mysterious. Results about $TCP$s so far have shown what one can do with a $TCP$, but have not shown why one might exist in the first place. It appears that any insight into why $TCP$s exist will come from a completely different perspective.

# 5

# Boolean Complementary Pairs

Boolean complementary pairs were introduced by Craigen [2] as a generalization of ternary complementary pairs. It will be shown that every $TCP$ corresponds to a $BCP$, but not every $BCP$ corresponds to a $TCP$. Craigen solved the structure of $BCP$s with even weight, and later discovered a factorization for the odd-weight case with his student Woodford [8]. This chapter follows Craigen's [2] paper on Boolean complementary pairs, in particular, what was known before the odd-weight factorization was developed.

## 5.1 Preliminaries

It is helpful to remember that if $u, w \in \mathbb{Z}_2$, then the condition that $u \neq w$ is equivalent to $u + w = 1$.

**Definition 5.1.1.** Let $n, w \in \mathbb{Z}^+$ and $f, g \in \mathbb{Z}_2[x, x^{-1}]$ have degree $n-1$ and a total of $w$ nonzero entries. Then $(f, g)$ is a **Boolean complementary pair** of length $n$ and weight $w$ (written $BCP(n, w)$) if and only if

$$(ff^* + gg^*)(x) = w. \tag{5.1.1}$$

The **deficiency** of the pair is $2n-w$. If $(f,g)$ is a $CP(n,w,\mathbb{Z}_2)$, then $(ff^*+gg^*)(x)$ is trivially $w$ by Lemma 2.1.8, hence being a $CP(n,w,\mathbb{Z}_2)$ is equivalent to being a $BCP(n,w)$. Odd-weight $BCP$s are often referred to as $BCP_1$s, and even-weight $BCP$s as $BCP_0$s.

**Example 5.1.1.** Let $f = 1+x+x^2+x^4+x^5$ and $g = 1+x^2+x^3+x^5$. Then $(f,g)$ has degree 5, weight 9, and

$$(ff^*+gg^*)(x) = 9.$$

Therefore, the pair $(f,g)$ is a $BCP(6,9)$. □

**Lemma 5.1.2** (Craigen, 2003 [2])**.** Let $n,w \in \mathbb{Z}^+$ and $(f,g)$ be a $TCP(n,w)$. Let $\phi : \mathbb{Z}[x,x^{-1}] \to \mathbb{Z}_2[x,x^{-1}]$ be the homomorphism mapping coefficients to their remainder modulo 2. Then $(\phi(f),\phi(g))$ is a $BCP(n,w)$.

*Proof.* The pair $(\phi(f),\phi(g))$ trivially has degree $n-1$ and weight $w$. As for orthogonality,

$$\begin{aligned}\phi(f)(x)\phi(f)(x^{-1}) + \phi(g)(x)\phi(g)(x^{-1}) &= \phi(f(x)f(x^{-1})) + \phi(g(x)g(x^{-1}))\\ &= \phi(f(x)f(x^{-1}) + g(x)g(x^{-1}))\\ &= \phi(w)\\ &= w.\end{aligned}$$ □

The $BCP$ in Example 5.1.1 has weight 9. Therefore, that $BCP$ cannot be the image of a $TCP$ under the homomorphism $\phi$ by Theorem 2.5.2.

Two important classes of $BCP$s shall now be discussed.

**Lemma 5.1.3** (Craigen, 2003 [2])**.** Let $n,m,u,w \in \mathbb{Z}^+$, and $f,g \in \mathbb{Z}_2[x,x^{-1}]$ be such that $f$ has degree $n-1$ and $w$ nonzero coefficients, and $g = \sum_{i=0}^{2m} g_i x^i$ has degree $2m$, has $u$ nonzero coefficients, and is symmetric equivalent. Then

1. the pair $(f, f)$ is a $BCP(n, 2w)$;

2. the pair $(g, g + x^m)$ is a $BCP(2m + 1, 2u \pm 1)$.

*Proof.*

1. Follows from
$$(ff^* + ff^*)(x) = 2ff^*(x) = 0.$$

2. Note that $x^{-m}g = x^m g^*$, and consider
$$(gg^* + (g + x^m)(g + x^m)^*)(x) = x^{-m}g(x) + x^m g^*(x) + 1 = 1. \qquad \square$$

**Definition 5.1.4.** Any shifted versions of $(f, f)$ and $(g, g+x^m)$ in Lemma 5.1.3 shall be referred to as an **identical twin pair** and a **siamese twin pair**, respectively.

**Example 5.1.2.** If $(f, g)$ is a $GP$, then under the homomorphism $\phi$ in Lemma 5.1.2, the pair $(\phi(f), \phi(g))$ is an identical twin pair. Let $p = x^{-1} + 1 - x$ and $q = x^{-1} + x$. The pair $(p, q)$ is a $TCP(3, 5)$, and $(\phi(p), \phi(q))$ form a siamese twin pair. $\square$

Identical and siamese twin pairs offer insight into which parameters $(n, w)$ are those of $BCP$s.

**Lemma 5.1.5** (Craigen, 2003 [2])**.** For all $n, w \in \mathbb{Z}^+$ with $w \leqslant n$, there exists a $BCP(n, 2w)$. For all $m \in \mathbb{Z}^+$ with $2w + 1 < 4m + 2$ and $w$ even, there exists a $BCP(2m + 1, 2w + 1)$.

*Proof.* Let $f$ be any degree $n - 1$ polynomial with $w$ nonzero entries. Then $(f, f)$ is a $BCP(n, 2w)$ by Lemma 5.1.3. Let $g = \sum_{i=0}^{m-1} g_i x^i$ have $\frac{w}{2}$ entries. Then $(g + x^{2m}g^*, g + x^{2m} + x^{2m}g^*)$ is a $BCP(2m + 1, 2w + 1)$ by Lemma 5.1.3. $\square$

Although Theorem 2.5.2 does not eliminate weights that have factors congruent to 3 (mod 4) for $BCP$s, it is still possible to eliminate certain weights through a different kind of analysis.

**Lemma 5.1.6** (Craigen, 2003 [2])**.** Let $n, w \in \mathbb{Z}^+$ and $(f, g)$ be a $BCP(n, w)$. Let $\alpha$ and $\beta$ be the number of nonzero coefficients of $x$ in $f(x)$ and $g(x)$, respectively. Then

1. $\alpha^2 + \beta^2 \equiv w \pmod 4$;
2. if $w$ is even, then $\alpha \equiv \beta \pmod 4$;
3. if $w \equiv 0 \pmod 4$, then $\alpha, \beta$ are even;
4. if $w \equiv 2 \pmod 4$, then $\alpha, \beta$ are odd;
5. if $w$ is odd, then $w \equiv 1 \pmod 4$.

*Proof.* As $f$ has $\alpha$ nonzero coefficients, and any two distinct coefficients contribute exactly one term in $\sum_{j=1}^{n-1} AF_F(j)$, prior to cancellation there are exactly $\binom{\alpha}{2} = \frac{\alpha(\alpha-1)}{2}$ nonzero terms in $\sum_{j=1}^{n-1} AF_F(j)$. Similarly, prior to cancellation there are $\binom{\beta}{2} = \frac{\beta(\beta-1)}{2}$ nonzero terms in $\sum_{j=1}^{n-1} AF_G(j)$. Since

$$AF_F(j) + AF_G(j) = 0 \text{ for all } j \in \mathbb{Z}^+,$$

one obtains

$$\begin{aligned}\sum_{j=1}^{n-1} AF_F(j) + \sum_{j=1}^{n-1} AF_G(j) &= \frac{\alpha(\alpha-1)}{2} + \frac{\beta(\beta-1)}{2} \\ &= \frac{\alpha^2 + \beta^2 - w}{2} \\ &\equiv 0 \pmod 2.\end{aligned}$$

Therefore,

$$\alpha^2 + \beta^2 \equiv w \pmod 4.$$

Numbers 2 to 5 follow by considering the possibilities that satisfy 1 as well as using $\alpha + \beta = w$. □

## 5.2 Small-deficiency pairs

Boolean complementary pairs up to deficiency 3 can be completely classified. These results can be used to put restrictions on the structure of ternary complementary pairs with the same deficiency. The proof of the following theorem uses some later results which will shorten the work.

**Theorem 5.2.1** (Craigen, 2003 [2]). Let $n, w \in \mathbb{Z}^+$, $\gamma = 1 + x + \cdots + x^{n-1}$, and $(f, g)$ be a pair of degree $n-1$ polynomials in $\mathbb{Z}_2[x, x^{-1}]$. Then

1. $(f, g)$ is a deficiency 1 $BCP$ if and only if there exists $k \in \mathbb{Z}^+$ such that $n = 2k + 1$ and $(f, g) \cong (\gamma, \gamma + x^k)$;

2. $(f, g)$ is a deficiency 2 $BCP$ if and only if there exists $k \in \mathbb{Z}^+$ such that $(f, g) \cong (\gamma + x^k, \gamma + x^k)$;

3. $(f, g)$ is a deficiency 3 $BCP$ if and only if there exists $k \in \mathbb{Z}^+$ such that $n = 4k + 2$ and $(f, g) \cong (\gamma + x^k + x^{3k+1}, \gamma + x^{2k})$.

*Proof.* Note that $x^{n-1} j^* = j$.

1. ($\Rightarrow$) By definition, there exists a $k \in \mathbb{Z}^+$ such that $(f, g) \cong (\gamma, \gamma + x^k)$. If $k \neq \frac{n-1}{2}$, then $AF_F(n-k) + AF_G(n-k) = 1$. ($\Leftarrow$) Follows from Lemma 5.1.3;

2. ($\Rightarrow$) Follows from Lemma 4.5.2. ($\Leftarrow$) Follows from Lemma 5.1.3;

3. ($\Rightarrow$) If $n$ is odd, then $w = 2n - 3 \equiv 3 \pmod 4$, which is impossible by part 5 of Lemma 5.1.6. Therefore, $n$ is even. Without loss of generality, assume $f$ and $g$ are normalized. If the three zeros occur in $f$, one can assume without loss of generality that two zeros are coefficients of powers of $x$ before $\frac{n-1}{2}$, as one could instead consider the equivalent pair $(f^*, g)$. By the later corollary 6.1.10 there exist $a, c \in \mathbb{Z}^+$ such that $1 \leqslant a < c \leqslant \frac{n-2}{2}$, and $f = \gamma + x^a + x^c + x^{n-1-a}$.

Now,

$$\begin{aligned}
(ff^* + \gamma\gamma^*)(x) &= (\gamma + x^a + x^c + x^{n-1-a})(\gamma^* + x^{-a} + x^{-c} + x^{-n+1+a}) + \gamma\gamma^* \\
&= (x^{-a} + x^{-c} + x^{-n+1+a})\gamma + (x^a + x^c + x^{n-1-a})\gamma^* \\
&\quad + (x^a + x^c + x^{n-1-a})(x^{-a} + x^{-c} + x^{-n+1+a}) \\
&= (x^{-a} + x^{-c} + x^{-n+1+a})\gamma + (x^a + x^c + x^{n-1-a})x^{-n+1}\gamma \\
&\quad + x^{a-c} + x^{-n+1+2a} + x^{c-a} + x^{-n+1+a+c} + x^{n-1-2a} \\
&\quad + x^{n-1-a-c} + 1 \\
&= (x^{-a} + x^{-c} + x^{-n+1+a} + x^{a-n+1} + x^{c-n+1} + x^{-a})\gamma \\
&\quad + x^{a-c} + x^{-n+1+2a} + x^{c-a} + x^{-n+1+a+c} + x^{n-1-2a} \\
&\quad + x^{n-1-a-c} + 1 \\
&= (x^{-c} + x^{c-n+1})\gamma + x^{a-c} + x^{-n+1+2a} + x^{c-a} \\
&\quad + x^{-n+1+a+c} + x^{n-1-2a} + x^{n-1-a-c} + 1 \\
&= 1.
\end{aligned}$$

Therefore,

$$\begin{aligned}
(x^{-c} + x^{c-n+1})\gamma = (x^{a-c} + x^{c-a}) + (x^{-n+1+a+c} + x^{n-1-a-c}) \\
+ (x^{-n+1+2a} + x^{n-1-2a}).
\end{aligned} \tag{5.2.1}$$

The highest power of $x$ on the left-hand side of equation (5.2.1) is $n-1-c$, and the highest power of $x$ on the right-hand side is $n-1-2a$, so $c = 2a$. equation (5.2.1) then becomes

$$\begin{aligned}
(x^{-2a} + x^{2a-n+1}) = (x^{-a} + x^a) + (x^{-n+1+3a} + x^{n-1-3a}) \\
+ (x^{-n+1+2a} + x^{n-1-2a}).
\end{aligned} \tag{5.2.2}$$

The second highest power of $x$ on the left-hand side of equation (5.2.2) is

$n-2-2a$. Since $2a = c \leqslant \frac{n-2}{2}$, it follows that $a \leqslant \frac{n-2}{4}$ and $3a \leqslant \frac{3}{4}(n-2) \leqslant n-1$. Therefore, $a, n-1-2a$, and $n-1-3a$ are the only positive powers of $x$ on the right-hand side of equation (5.2.2). It follows that the second highest power of $x$ on the right-hand side of equation (5.2.2) is either $a$ or $n-1-3a$. If the highest power was $a$, then $n-2-2a = a$, hence $a = \frac{n-2}{3}$. However, this can not be since it was shown that $a \leqslant \frac{n-2}{4}$. Therefore, the second highest power of $x$ on the right-hand side of equation (5.2.2) is $n-1-3a$. In this case, $n-2-2a = n-1-3a$, so $a = 1$. Note that as $a < \frac{n-1}{4}$ and $n$ is even, one obtains $n \geqslant 6$.

The third highest power of $x$ on the left-hand side of equation (5.2.2) is $n-3-2a = n-5$, and the third highest power of $x$ on the right-hand side is $a = 1$. Therefore, $n = 6$ and $f = 1+x^3+x^4+x^6$ and $g = 1+x+x^2+x^3+x^4+x^5+x^6$. However, one can check that $AF_F(1) + AF_G(1) = 1$, hence $f$ and $g$ are not complementary.

Assume without loss of generality that $f$ has two zeros and $g$ has one zero, without loss of generality say $a, b, c \in \mathbb{Z}^+$ with $a \neq b$ and $c \leqslant \frac{n-2}{2}$ are such that $f = \gamma + x^a + x^b$ and $g = \gamma + x^c$. Then again by the later Corollary 6.1.10, one can assume $b = n-1-a$ and $a < c < n-1-a$. Therefore, $f = 1+x^a+x^{n-1-a}$

and $g = \gamma + x^c$. Then

$$\begin{aligned}(ff^* + gg^*)(x) &= (\gamma + x^a + x^{n-1-a})(\gamma^* + x^{-a} + x^{-n+1+a}) \\ &\quad + (\gamma + x^c)(\gamma^* + x^{-c}) \\ &= (x^{-a} + x^{-n+1+a} + x^{a-n+1} + x^{-a})\gamma \\ &\quad + (x^a + x^{n-1-a})(x^{-a} + x^{-n+1+a}) \\ &\quad + (x^{-c} + x^{c-n+1})\gamma + 1 \\ &= x^{n-1-2a} + x^{-n+1+2a} + (x^{-c} + x^{c-n+1})\gamma + 1 \\ &= 1.\end{aligned}$$

Therefore, $(x^{n-1-2a} + x^{-n+1+2a}) = (x^{-c} + x^{c-n+1})\gamma$. As $a < c < \frac{n-2}{2}$, one has $n - 2 - 2a > 0$. The highest power of $x$ in $(x^{n-1-2a} + x^{-n+1+2a})$ is therefore $n - 1 - 2a$, and the highest power of $x$ in $(x^{-c} + x^{c-n+1})\gamma$ is $n - 1 - c$. Thus, $c = 2a$. Therefore,

$$\begin{aligned}x^{n-1-2a} + x^{-n+1+2a} &= (x^{-2a} + x^{2a-n+1})\gamma \\ &= x^{n-1}(x^{-2a} + x^{2a-n+1}) \\ &\quad + (1 + x + \cdots + x^{n-2})(x^{-2a} + x^{2a-n+1}),\end{aligned}$$

which implies

$$x^{-n+1+2a} + x^{2a} = (1 + x + \cdots + x^{n-2})(x^{-2a} + x^{2a-n+1}). \tag{5.2.3}$$

The highest power of $x$ on the left-hand side of equation (5.2.3) is $2a$, and the highest power of $x$ on the right-hand side is either $n - 2 - 2a$ or $2a - 1$. If it is the latter, then $2a = 2a - 1$, a contradiction. Thus $n - 2 - 2a$ is the highest power of $x$ on the right-hand side of equation (5.2.3) and so $n - 2 - 2a = 2a$, that is, $n = 4a + 2$. Therefore, $(f, g) \cong (\gamma + x^a + x^{3a+1}, \gamma + x^{2a})$.

($\Leftarrow$) Suppose $(f,g) = (\gamma + x^k + x^{3k+1}, \gamma + x^{2k})$. Then

$$\begin{aligned}
(ff^* + gg^*)(x) &= (\gamma + x^a + x^{3a+1})(\gamma^* + x^{-a} + x^{-3a-1}) + (\gamma + x^{2a})(\gamma^* + x^{-2a}) \\
&= (x^{-a} + x^{-3a-1} + x^{-3a-1} + x^{-a})\gamma \\
&\quad + (x^a + x^{3a+1})(x^{-a} + x^{-3a-1}) \\
&\quad + (x^{-2a} + x^{-2a-1})\gamma + 1 \\
&= (x^{2a+1} + x^{-2a-1}) + (x^{-2a} + x^{-2a-1})(1 + x + \cdots + x^{4a+1}) + 1 \\
&= (x^{2a+1} + x^{-2a-1}) + (x^{2a+1} + x^{-2a-1}) + 1 \\
&= 1.
\end{aligned}$$

□

## 5.3 Small-weight pairs

Boolean complementary pairs of weight $\leqslant 6$ have been completely classified. Some later results are used to simplify the work.

**Theorem 5.3.1** (Craigen, 2003 [2])**.** Let $n, w \in \mathbb{Z}^+$ and $(f,g)$ be a $BCP(n,w)$. Then

1. $w = 1$ if and only if $(f,g) \cong (1,0)$;
2. $w = 2$ if and only if $(f,g) \cong (1,1)$;
3. $w = 4$ if and only if $(f,g) \cong (1+x, 1+x)$;
4. $w = 5$ if and only if $(f,g) \cong (1+x+x^2, 1+x^2)$;
5. $w = 6$ if and only if there exists $a \in \mathbb{Z}^+$ with $gcd(a, n-1) = 1$ such that $(f,g) \cong (1+x^a+x^{n-1}, 1+x^a+x^{n-1})$.

*Proof.* Note that all such pairs can be directly verified to be $BCP$s.

1. One can assume the only nonzero entry occurs in $f$, which can be shifted to get $f = 1$.

2. Follows by shifting and the fact that the two polynomials have the same degree.

3. The two polynomials have the same degree, hence $(f, g) \cong (1 + x^{n-1}, 1 + x^{n-1})$. The pair can be deflated to $(1 + x, 1 + x)$.

4. Again, the pair are of equal degree so there is $a \in \mathbb{Z}^+$ such that $(f, g) \cong (1 + x^a + x^{n-1}, 1 + x^{n-1})$. By Corollary 6.1.10, $a = \frac{n-1}{2}$ and thus the pair can be deflated to $(1 + x + x^2, 1 + x^2)$.

5. Suppose $f$ has weight 4. Then by Corollary 6.1.10, there exists $a \in \mathbb{Z}^+$ such that $(f, g) \cong (1 + x^a + x^{n-1-a} + x^{n-1}, 1 + x^{n-1})$. However, this would yield $AF_F(n - 1 - 2a) + AF_G(n - 1 - 2a) = 1$, so this is impossible. Therefore, $f$ and $g$ both have weight 3 and by Corollary 6.1.10 one can assume without loss of generality that $(f, g) = (1 + x^a + x^{n-1}, 1 + x^a + x^{n-1})$. Through deflation, one can also assume without loss of generality that $\gcd(a, n - 1) = 1$. □

## 5.4 Even-weight Boolean complementary pairs

The structure of even-weight $BCP$s is noticeably different than that of odd-weight $BCP$s. Most notably, the structure of $BCP_0$s is immediately solved by Theorem 5.4.1, which itself is a straightforward extension of Theorem 2.5.2.

**Theorem 5.4.1** ([2])**.** A pair $(f, g)$ is a $BCP_0$ if and only if there exist $h, k \in \mathbb{Z}_2[x, x^{-1}]$ and $i \in \mathbb{Z}$ such that $f = hk$ and $g = x^i hk^*$.

*Proof.* Let $h = \gcd(f, g)$ and let $k, r$ be such that $f = hk$ and $g = hr$. Then

$$\begin{aligned}(ff^* + gg^*)(x) &= hh^*(kk^* + rr^*)(x) \\ &= 0.\end{aligned}$$

Similar to the the proof of Theorem 2.5.2, this implies the existence of $i \in \mathbb{Z}$ such that $r = x^i k^*$. □

Craigen [2] attempted to classify all $BCP$s where one polynomial is symmetric-equivalent. His results contained a flaw, however, as he omitted the possibility of a multiplicative symmetric-equivalent factor $b(x)$. The correct versions are given in Lemmas 5.4.2 and 5.5.1.

**Lemma 5.4.2** (Craigen, 2003 and Gobin, 2023)**.** Let $(f, g)$ be a $BCP_0$. Then $f$ is symmetric-equivalent if and only if there exist $a(x), b(x) \in \mathbb{Z}_2[x, x^{-1}]$ with $b(x)$ symmetric-equivalent and $i \in \mathbb{Z}$ such that $f = aa^*b$ and $g = x^i a^2 b$.

*Proof.* ($\Rightarrow$) By Theorem 5.4.1, there exists polynomials $h, k$ and $i \in \mathbb{Z}$ such that $f = hk$ and $g = x^i hk^*$. One can assume without loss of generality that $gcd(k, k^*) = 1$ as otherwise one can redefine $h$ to contain the symmetric-equivalent factors of $k$. As $f$ is symmetric-equivalent, there exists $m \in \mathbb{Z}$ such that $f = x^m f^*$, thus $f = hk = x^m h^* k^*$. As $gcd(k, k^*) = 1$, the polynomial $k^*$ divides $h$ and thus there exists a polynomial $b(x)$ such that $h = bk^*$. Therefore, $f = bkk^* = x^m b^* kk^*$ and so $b$ is symmetric-equivalent. One obtains $g = x^i bk^* k^*$, so the result follows by letting $a = k^*$.

($\Leftarrow$) Follows by direct verification. □

## 5.5 Odd-weight Boolean complementary pairs

Odd-weight pairs where one sequence is symmetric-equivalent can also be completely classified.

**Lemma 5.5.1** (Craigen, 2003 and Gobin, 2023 [2])**.** Let $n \in \mathbb{Z}^+$ and $(f, g)$ be an odd-weight degree $n - 1$ pair of polynomials with $f$ symmetric-equivalent.

1. If $n$ is odd, then $(f, g)$ is a $BCP_1$ if and only if there exist $a(x), b(x) \in \mathbb{Z}_2[x, x^{-1}]$ with $b(x)$ symmetric and $i, j \in \mathbb{Z}$ such that $f = x^j\,(aa^*b + 1)$ and $g = x^i a^2 b$;

2. If $n$ is even, then $(f, g)$ is a $BCP_1$ if and only if there exist $j \in \mathbb{Z}$ such that $f(x^2) = x^c(gg^*(x) + 1)$.

*Proof.*

1. ($\Rightarrow$) As $n$ is odd and $f$ is symmetric-equivalent, there exists $j \in \mathbb{Z}$ such that $x^j f$ is centred around $x^0$, that is, $(x^j f)^* = x^j f$. By Lemma 5.1.3, the pair $(x^j f + 1, g)$ is a $BCP(n, w+1)$, that is, an even-weight pair with $x^j f$ symmetric. Therefore, there exist $a(x), b(x)$ with $b$ symmetric-equivalent and $i \in \mathbb{Z}$ such that $x^j f + 1 = aa^*b$ and $g = x^i a^2 b$. As $(x^j f + 1)^* = x^{-j} f^* + 1^* = x^j f + 1$, one obtains $aa^*b = aa^*b^*$. Therefore, $b$ is symmetric and the result follows.
   ($\Leftarrow$) Direct verification.

2. ($\Rightarrow$) Although $n$ is even, the pair $f(x^2), g(x^2)$ has degree $2n - 2$ and thus part 1 applies. Therefore, there exist $a(x), b(x) \in \mathbb{Z}_2[x, x^{-1}]$ with $b(x)$ symmetric and $i, j \in \mathbb{Z}$ such that $f(x^2) = x^j((aa^*b)(x) + 1)$ and $g(x^2) = x^i a^2(x) b(x)$. As $\mathbb{Z}_2$ has characteristic 2, one obtains $a^2(x) = a(x^2)$. Therefore, $x^i b(x) = g(x^2)/a(x^2)$ and so there is some symmetric-equivalent $t(x)$, say with $e \in \mathbb{Z}$ such that $x^e t^*(x) = t(x)$, such that $t(x^2) = x^i b(x)$. Thus $g(x^2) = a(x^2)t(x^2)$,

so $g(x) = a(x)t(x)$, and

$$\begin{aligned} x^{-j}f(x^2) &= (aa^*b)(x) + 1 \\ &= x^{-i}(aa^*x^ib)(x) + 1 \\ &= x^{-i}(aa^*(x))t(x^2) + 1 \\ &= x^{-i}(aa^*(x))t(x)t(x) + 1 \\ &= x^{e-i}(aa^*(x))(t(x)t^*(x)) + 1 \\ &= x^{e-i}(at(x))(a^*t^*(x)) + 1 \\ &= x^{e-i}gg^*(x) + 1. \end{aligned}$$

($\Leftarrow$) Note that for any polynomial $h(x) \in \mathbb{Z}_2[x, x^{-1}]$, one has $h(x^2) = h(x)^2$ since $\mathbb{Z}_2[x, x^{-1}]$ has characteristic 2. Observe that

$$\begin{aligned} f(x^2)f^*(x^2) + g(x^2)g^*(x^2) &= (gg^*(x) + 1)(gg^*(x) + 1) + g(x^2)g^*(x^2) \\ &= g(x)^2g^*(x)^2 + 1 + g(x^2)g^*(x^2) \\ &= 2g(x^2)g^*(x^2) + 1 \\ &= 1. \end{aligned}$$

Therefore, by Theorem 2.3.1, the pair $(f(x^2), g(x^2))$ can be deflated to the equivalent Boolean complementary pair $(f(x), g(x))$. □

**Lemma 5.5.2** (Craigen, 2003 [2])**.** Let $n \in \mathbb{Z}^+$ and $(f, g)$ be a $BCP$ of degree $n-1$ where both $f$ and $g$ are symmetric-equivalent. Then

1. If $(f, g)$ has odd-weight, then $(f, g)$ is a siamese twin pair;
2. If $(f, g)$ has even-weight, then $(f, g)$ is an identical twin pair.

*Proof.* Without loss of generality, assume $f$ and $g$ are normalized. Therefore, one obtains $x^{n-1}f^* = f$ and $x^{n-1}g^* = g$.

1. Calculating, $(f+g)(f+g)^* = ff^* + fg^* + f^*g + gg^* = ff^* + x^{-n+1}fg + x^{-n+1}fg + gg^* = 1$. Suppose $m, t \in \mathbb{Z}^+$ are such that $m$ is the highest power of $x$ in $(f+g)(x)$, and $t$ is the lowest. The highest power of $(f+g)(f+g)^*$ is $m-t$, but $(f+g)(f+g)^* = 1$ so $m = t$. Therefore, $f$ and $g$ differ from one another in exactly one place. By Theorem 5.2.1, the pair $(f, g)$ is a siamese twin pair.

2. Similarly, one obtains $(f+g)(f+g)^* = ff^* + gg^* = 0$, so $f = g$. □

Similar to his paper on $TCP$s [7], Craigen sought to investigate odd-weight Boolean complementary pairs which were unobtainable through the multiplication of Theorem 2.4.1. However, he realized that there were no such pairs.

**Theorem 5.5.3** (Craigen, 2003 [2])**.** Let $(f, g)$ and $(h, k)$ be $BCP_1$s. Then there exists $(r, s)$, a $BCP_1$, such that $(f, g) = (hr + ks, h^*s + k^*r)$.

*Proof.* Let $(r, s) = (fh^* + gk, fk^* + gh)$. By Theorem 2.4.1, $(r, s)$ is a $BCP_1$. Furthermore,

$$\begin{aligned} hr + ks &= h(fh^* + gk) + k(fk^* + gh) \\ &= hh^*f + 2ghk + kk^*f \\ &= (hh^* + kk^*)f \\ &= f, \text{ and} \\ h^*s + k^*r &= h^*(fk^* + gh) + k^*(fh^* + gk) \\ &= fh^*k^* + ghh^* + fh^*k^* + gkk^* \\ &= hh^*g + kk^*g \\ &= g. \end{aligned}$$

Thus $(f, g) = (hr + ks, h^*s + k^*h)$. □

Theorem 5.5.3 says that for any $BCP$ is divisible by every other pair under the multiplication of Theorem 2.4.1. However, it is still possible to factor a $BCP$ into a unique product of $BCP$s, as will be shown in the next chapter.

# 6

# Pair Matrix Factorizations

In 2002, Craigen and Woodford [8] discovered an algebraic factorization for odd-weight Boolean complementary pairs which was markedly different than that of the even-weight pairs. The $BCP_0$ factorization is expressed entirely in polynomials: a pair $(f, g)$ is a $BCP_0$ if and only if there exist $h, k \in \mathbb{Z}_2[x, x^{-1}]$ such that $(f, g) \cong (hk, hk^*)$. The $BCP_1$ factorization involves $2 \times 2$ matrices, each of which determined by several properties about the pair one wishes to factor. Craigen and Woodford used this factorization to show the set of all $BCP_1$s forms a group, and it was this group that was the object of their investigation.

This author began investigating the $BCP_1$ factorization as an undergraduate researcher. Upon beginning this thesis as a graduate student, it became apparent that these factorizations have much broader application than initially perceived. Any pair of equal degree polynomials in $\mathbb{Z}_2[x, x^{-1}]$ has a nontrivial factorization; not just $BCP_1$s, not just $BCP_0$s, any pair at all. This chapter develops these factorizations, while the next demonstrates some of their structural implications to $BCP$s.

By the end of this chapter, one will know the sequence, polynomial, pair matrix, canonical factorization, and superfactorization forms of $BCP$s. To keep these dif-

ferent forms clear, Section 6.6 shows them all for a specific $BCP$. The reader is encouraged to visit Section 6.6 whenever confusion arises.

## 6.1 Preliminaries

### 6.1.1 Pair matrices

**Definition 6.1.1.** Let $f, g$ be Laurent polynomials over a ring. The **pair matrix** of the pair $(f, g)$ is

$$PM(f,g) := \begin{pmatrix} f & g \\ -g^* & f^* \end{pmatrix}.$$

**Lemma 6.1.2** (Craigen and Woodford, 2002 [8])**.** The set of pair matrices of polynomials over a ring has a unit and is closed under multiplication.

*Proof.* Let $f, g, h, k$ be polynomials in some ring. Then $I = PM(1, 0)$ is the identity, associativity follows from associativity of matrix multiplication, and

$$\begin{aligned} PM(f,g)PM(h,k) &= \begin{pmatrix} f & g \\ -g^* & f^* \end{pmatrix}\begin{pmatrix} h & k \\ -k^* & h^* \end{pmatrix} \\ &= \begin{pmatrix} fh - gk^* & fk + gh^* \\ -g^*h - f^*k^* & -g^*k + f^*h^* \end{pmatrix} \\ &= \begin{pmatrix} fh - gk^* & fk + gh^* \\ -(fk + gh^*)^* & (fh - gk^*)^* \end{pmatrix} \\ &= PM(fh - gk^*, fk + gh^*). \end{aligned}$$

□

Pair matrices capture the orthogonality or non-orthogonality of a pair of polynomials in a simple manner. To show this, conjugation is first extended to these matrices.

**Definition 6.1.3.** Define the operation **conjugation**, denoted by "$*$", on pair matrices to be $PM(f,g)^* := PM(f^*, -g)$. Equivalently, the conjugate of a pair matrix is the transpose of the matrix with the entries conjugated.

**Theorem 6.1.4** (Craigen and Woodford, 2002 [8])**.** Let $f, g, h, k$ be polynomials in some ring. Then

1. $PM(f,g)PM(f,g)^* = (ff^* + gg^*)I$;
2. $(PM(f,g)PM(h,k))^* = PM(h,k)^*PM(f,g)^*$;
3. If $(f,g)$ and $(h,k)$ are both complementary, then so is the pair $(r,s)$ defined by $PM(r,s) = PM(f,g)PM(h,k)$.

*Proof.*

1. By direct verification,

$$\begin{aligned} PM(f,g)PM(f,g)^* &= PM(f,g)PM(f^*,-g) \\ &= PM(ff^* + gg^*, -fg + fg) \\ &= (ff^* + gg^*)I. \end{aligned}$$

2. Simple calculation shows

$$\begin{aligned} (PM(f,g)PM(h,k))^* &= (PM(fh - gk^*, fk + gh^*))^* \\ &= PM(f^*h^* - g^*k, -fk - gh^*) \\ &= PM(h^*, -k)PM(f^*, -g) \\ &= PM(h,k)^*PM(f,g)^*. \end{aligned}$$

3. Straightforward verification shows

$$\begin{aligned} PM(r,s)PM(r,s)^* &= (PM(f,g)PM(h,k))\,(PM(f,g)PM(h,k))^* \\ &= PM(f,g)PM(h,k)PM(h^*,k)PM(f^*,g) \\ &= PM(f,g)(hh^*+kk^*)PM(f^*,g) \\ &= (hh^*+kk^*)PM(f,g)PM(f^*,g) \\ &= (ff^*+gg^*)(hh^*+kk^*)I. \end{aligned}$$ □

Theorem 6.1.4 is equivalent to Theorem 2.4.1. To see this, suppose $(f,g)$ and $(h,k)$ are complementary pairs over the same coefficient set. Then part 3 of Theorem 6.1.4 says the pair $(R,S)$ defined by $PM(R,S) = PM(f,g)PM(h,-k^*)$ is complementary. By inspection, one obtains $R = fh+gk$ and $S = -fk^*+gh^*$. Applying Theorem 2.4.1 to $(f,g)$ and $(h,k)$ results in the complementary pair $(R,-S)$, which is equivalent to $(R,S)$ by Theorem 2.3.1. Theorems 6.1.4 and 2.4.1 are equivalent, but Theorem 6.1.4 has a much quicker proof. This is often the case with pair matrices, they have the ability to express results about complementary pairs quicker than in the polynomial form. Part 3 of Theorem 6.1.4 has several immediate consequences to Boolean complementary pairs.

**Corollary 6.1.5** (Craigen and Woodford, 2002 [8])**.** Let $(f,g),(r,s)$, and $(h,k)$ be a $BCP_1$, a $BCP_0$, and a pair of polynomials over $\mathbb{Z}_2$, respectively. Then

1. $PM(f,g)PM(h,k)$ and $PM(h,k)PM(f,g)$ are $BCP_1$s if and only if $(h,k)$ is a $BCP_1$;

2. $PM(h,k)PM(r,s)$ and $PM(r,s)PM(h,k)$ are $BCP_0$s.

*Proof.* For any two pairs of polynomials $(\psi, \phi)$ and $(\zeta, \eta)$,

$$\begin{aligned}
&(PM(\psi,\phi)PM(\zeta,\eta))\,(PM(\psi,\phi)PM(\zeta,\eta))^* \\
&= (PM(\psi,\phi)PM(\zeta,\eta))\,(PM(\zeta,\eta)^*PM(\psi,\phi)^*) \\
&= (\psi\psi^* + \phi\phi^*)\,(\zeta\zeta^* + \eta\eta^*)\,I.
\end{aligned}$$

Furthermore, note that $PM(\psi\psi^* + \phi\phi^*, 0) = (\psi\psi^* + \phi\phi^*)I$ and thus commutes with any other pair matrix. The results follow easily from these two facts and Part 1 of Theorem 6.1.4. □

Corollary 6.1.5 demonstrates a stark contrast between odd and even-weight $BCP$s. In the odd-weight case, a product is orthogonal if and only if every factor is orthogonal. The odd-weight structure is exclusionary with respect to products, it is only maintained by other odd-weight pairs. In the even-weight case, any even-weight Boolean complementary pair $(r, s)$ forms two ideals in the ring of pair matrices of polynomials over $\mathbb{Z}_2$: let $I_L = \{PM(h,k)PM(r,s) : h, k \in \mathbb{Z}_2[x, x^{-1}]\}$ and $I_R = \{PM(r,s)PM(h,k) : h, k \in \mathbb{Z}_2[x, x^{-1}]\}$. Then $I_L$ and $I_R$ are left and right ideals, respectively, and the set of all $BCP_0$s is a union of such ideals.

**Definition 6.1.6.** Let $f, g$ be two nonzero polynomials. Then $\text{maxdeg}(PM(f,g))$ is the maximum degree of $f$ and $g$. If $f$ and $g$ have equal degrees, then the **degree** of $PM(f,g)$, written $\deg(PM(f,g))$ or $\deg(f,g)$, is the degree of the two polynomials. For $m \in \mathbb{Z}$, the degree of $PM(x^m, 0)$ and $PM(0, x^m)$ shall be considered to be zero.

**Example 6.1.1.** Let $f = x^{-2} + 1 + x^5$ and $g = x^{14} + x^{15}$. Then $\deg(f(x)) = 5 - (-2) = 7$ and $\deg(g(x)) = 15 - 14 = 1$. Therefore, $\text{maxdeg}(PM(f,g)) = \max\{7, 1\} = 7$. □

### 6.1.2 Dints and offsets

Before proceeding, a quick note on the degree of pairs is made. In previous chapters, one would consider complementary pairs of some length $n \in \mathbb{Z}^+$, which correspond to a pair of degree $n-1$ polynomials. However, the length of pairs are not of much interest from now on. Therefore, for sake of visual appeal, it will become standard to refer to degree $n$ pairs rather than degree $n-1$ pairs.

**Definition 6.1.7.** Let $a, a_L, a_R, n \in \mathbb{Z}^+$, $j, k \in \mathbb{Z}$, and

$$(f, g) = \left( x^j \sum_{i=0}^{n} f_i x^i, x^k \sum_{i=0}^{n} g_i x^i \right)$$

be a pair of degree $n$ polynomials over $\mathbb{Z}_2$ (thus $f_0 = g_0 = f_n = g_n = 1$). In particular, note that $f_i$ and $g_i$ are the coefficients of $x^{i+j}$ and $x^{i+k}$ in $f$ and $g$, respectively. Then $PM(f, g)$ has **left dint** $a_L$ if and only if $a_L$ is the least positive integer such that $f_{a_L} \neq g_{a_L}$, and has **right dint** $a_R$ if and only if $a_R$ is the least positive integer such that $f_{n-a_R} \neq g_{n-a_R}$. The pair $(f, g)$ has **dint** $a$ (written $\text{dint}(f, g) = a$) if and only if $a = a_L = a_R$.

In essence, one is "lining up" the two polynomials $f(x)$ and $g(x)$ at $x^0$, then calling the first place where they differ from the left the "left dint" and calling the first place where they differ from the right the "right dint".

Note that two equal-degree polynomials either have a left and right dint or are an identical twin pair.

The term dint comes from this author, and is a shortening of "differing integer", meaning a dint is the first place where two polynomials in $\mathbb{Z}_2[x, x^{-1}]$ differ from one another.

**Definition 6.1.8.** Let $b, d \in \mathbb{Z}$, and $f(x), g(x)$ be two polynomials whose least powers of $x$ with nonzero coefficient are $b$ and $d$, respectively. The **offset** of $PM(f, g)$ is $d - b$.

**Example 6.1.2.** Let $f(x) = x + x^4 + x^5 + x^6 + x^7 + x^8 + x^9$ and $g(x) = x^{-4} + x^{-2} + x^{-1} + 1 + x^3 + x^4$. The pair $(f, g)$ is a $BCP(9, 13)$, has degree 8, offset $-4 - 1 = -5$, and

$$PM(f,g) = PM(x + x^4 + x^5 + x^6 + x^7 + x^8 + x^9, x^{-4} + x^{-2} + x^{-1} + 1 + x^3 + x^4)$$

$$= \begin{pmatrix} x + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 & x^{-4} + x^{-2} + x^{-1} + 1 + x^3 + x^4 \\ x^4 + x^2 + x + 1 + x^{-3} + x^{-4} & x^{-1} + x^{-4} + x^{-5} + x^{-6} + x^{-7} + x^{-8} + x^{-9} \end{pmatrix}.$$

To find the left and right dint of the pair, write

$$f = x \sum_{i=0}^{8} f_i x^i = x(1 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8), \text{ and}$$
$$g = x^{-4} \sum_{i=0}^{8} g_i x^i = x^{-4}(1 + x^2 + x^3 + x^4 + x^7 + x^8).$$

One sees that 2 is the least integer $i$ such that $f_i \neq g_i$, and 2 is the least integer $i$ such that $f_{8-i} \neq g_{8-i}$. Therefore, the pair $(f, g)$ has left and right dint 2, so $\text{dint}(f, g) = 2$. □

**Lemma 6.1.9** (Craigen and Woodford, 2002 [8])**.** Let $a_L, a_R, n \in \mathbb{Z}^+$ and $(f, g)$ be a pair of degree $n$ polynomials with left and right dint $a_L$ and $a_R$, respectively. Without loss of generality, assume $a_L \leqslant a_R$. Then for integers $k < a_L$, one has $AF_F(n - k) + AF_G(n - k) = 0$. The term $AF_F(n - a_L) + AF_G(n - a_L)$ is zero if and only if $a_L = a_R$.

*Proof.* One sees that

$$\begin{aligned} AF_F(n-k) + AF_G(n-k) &= \sum_{i=0}^{k} (f_i f_{n-k+i} + g_i g_{n-k+i}) \\ &= \sum_{i=0}^{k} (f_i f_{n-k+i} + f_i f_{n-k+i}) \\ &= 2\sum_{i=0}^{k} f_i f_{n-k+i} \\ &= 0. \end{aligned}$$

Similarly,

$$\begin{aligned} AF_F(n-a_L) + AF_G(n-a_L) &= \sum_{i=0}^{a_L} (f_i f_{n-a_L+i} + g_i g_{n-a_L+i}) \\ &= f_0 f_{n-a_L} + g_0 g_{n-a_L} + \sum_{i=1}^{a_L-1} (f_i f_{n-a_L+i} + f_i f_{n-a_L+i}) \\ &\quad + f_{a_L} f_n + g_{a_L} g_n \\ &= (f_{n-a_L} + g_{n-a_L}) + (f_{a_L} + g_{a_L}) \\ &= (f_{n-a_L} + g_{n-a_L}) + 1, \end{aligned}$$

which is zero if and only if $f_{n-a_L} \neq g_{n-a_L}$, which occurs if and only if $a_L = a_R$ as $a_L \leqslant a_R$. □

**Corollary 6.1.10** (Craigen and Woodford, 2002 [8])**.** Any $BCP$ that is not an identical twin pair or a trivial pair has a dint.

*Proof.* The autocorrelation function is zero for all nonzero values for a $BCP$. Therefore, if a $BCP$ has a left and right dint, its left and right dints are equal by Lemma 6.1.9. If the pair does not have a left and right dint, then its either a trivial pair or the polynomials do not differ from one another, that is, the pair is an identical twin pair. □

### 6.1.3 Decomposing matrices

The final preliminary for these factorizations is to define the matrices which appear in the decompositions and establish some of their properties. These matrices have been changed slightly from those used by Craigen and Woodford [8], which causes their results to take a different form in this thesis. This author's presentation should be simpler to read and interpret.

**Definition 6.1.11.** Let $a, b \in \mathbb{Z}$. Define $p(x) := x^{-1} + 1 + x$, $q(x) := x^{-1} + x$, and $V_{a,b} := PM(p(x^a), x^b q(x^a))$. Note that $(p(x^a), x^b q(x^a))$ is a weight-five siamese twin pair of degree $2|a|$. Furthermore, note that $p^*(x^a) = p(x^a)$ and $q^*(x^a) = q(x^a)$, which shows that $V_{a,b} = V_{-a,b} = V_{a,b}^*$. Also, the dint and offset of the pair corresponding to $V_{a,b}$ is $a$ and $b$, respectively.

**Lemma 6.1.12.** For all $a, b \in \mathbb{Z}$, the matrix $V_{a,b}$ is idempotent.

*Proof.* Using the comments in Definition 6.1.11 and Part 1 of Theorem 6.1.4, one obtains $V_{a,b}^2 = V_{a,b}V_{a,b}^* = (pp^* + qq^*)(x^a)I = 5I = I$. □

**Lemma 6.1.13.** For all $a, b, c, d \in \mathbb{Z}$, the matrices $V_{a,b}$ and $V_{c,d}$ commute if and only if their corresponding polynomial pairs have the same offset, that is, if and only if $b = d$.

*Proof.* Consider the following products:

$$\begin{aligned} V_{a,b}V_{c,d} &= PM(p(x^a), x^b q(x^a))PM(p(x^c), x^d q(x^c)) \\ &= PM(p(x^a)p(x^c) + x^{b-d}q(x^a)q(x^c), x^d p(x^a)q(x^c) + x^b p(x^c)q(x^a)), \end{aligned}$$

and

$$V_{c,d}V_{a,b} = PM(p(x^a)p(x^c) + x^{d-b}q(x^a)q(x^c), x^b p(x^c)q(x^a) + x^d p(x^a)q(x^c)).$$

($\Rightarrow$) Suppose $V_{a,b}V_{c,d} = V_{c,d}V_{a,b}$. Then $p(x^a)p(x^c) + x^{b-d}q(x^a)q(x^c) = p(x^a)p(x^c) + x^{d-b}q(x^a)q(x^c)$, which implies $(x^{b-d} + x^{d-b})q(x^a)q(x^c) = 0$ and so $b = d$.

($\Leftarrow$) Follows easily by comparing $V_{a,b}V_{c,b}$ to $V_{c,b}V_{a,b}$ when $b = d$. □

**Theorem 6.1.14** (Craigen and Woodford, 2002 [8])**.** The set

$$G = \langle V_{a,b} : a, b \in \mathbb{Z} \rangle$$

is a group with respect to multiplication.

*Proof.* For $m \in \mathbb{Z}^+$ and integers $a_1, b_1, \ldots, a_m, b_m$,

$$\begin{aligned}
&(V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m})\,(V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m})^* \\
&= (V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m})\left(V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}\right) \\
&= I \\
&= V_{0,0}.
\end{aligned}$$

Therefore, all elements are invertible. Associativity is inherited from matrix and polynomial algebra. Therefore, $G$ is a group. □

It will be shown that every $BCP_1$ has an equivalent pair in the group $G$ in Theorem 6.1.14.

In order to express the operation of shifting a complementary pair in pair matrix form, the following definition is made:

**Definition 6.1.15.** Let $z$ be an indeterminate such that $z^2 = x$. Define the matrices $X := PM(x, 0)$ and $Z := PM(z, 0)$.

The introduction of $z$ comes from Craigen [4], who introduced the variable for the canonical factorizations of complementary pairs modulo 3.

For an odd-weight Boolean complementary pair $(f, g)$ and $c \in \mathbb{Z}$, one has $X^c PM(f, g) = PM(x^c f(x), x^c g(x))$. Now notice that

$$\begin{aligned} Z^c PM(f,g) Z^{-c} &= PM(z,0) PM(f(x), g(x)) PM(z^{-1}, 0) \\ &= PM(z^c f(x), z^c g(x)) Z^{-c} \\ &= PM(z^0 f(x), z^{2c} g(x)) \\ &= PM(f(x), x^c g(x)). \end{aligned}$$

Thus the matrix $X$ can be used to shift both polynomials in a pair, and the matrix $Z$ can be used to shift a single polynomial.

**Lemma 6.1.16.** Let $a_1, b_1, \ldots, a_m, b_m \in \mathbb{Z}$. Then

$$Z V_{a_1,b_1} V_{a_2,b_2} \cdots V_{a_m,b_m} Z^{-1} = V_{a_1,b_1+1} V_{a_2,b_2+1} \cdots V_{a_m,b_m+1}.$$

*Proof.* By direct verification, for all $a, b \in \mathbb{Z}$,

$$\begin{aligned} Z V_{a,b} Z^{-1} &= PM(z,0) PM(p(x^a), x^b q(x^a)) PM(z^{-1}, 0) \\ &= PM(zp(x^a), z x^b q(x^a)) PM(z^{-1}, 0) \\ &= PM(p(x^a), z^2 x^b q(x^a)) \\ &= V_{a,b+1}. \end{aligned}$$

Therefore,

$$\begin{aligned} Z V_{a_1,b_1} V_{a_2,b_2} \cdots V_{a_m,b_m} Z^{-1} &= \left(Z V_{a_1,b_1} Z^{-1}\right) \left(Z V_{a_2,b_2} Z^{-1}\right) \cdots \left(Z V_{a_m,b_m} Z^{-1}\right) \\ &= V_{a_1,b_1+1} V_{a_2,b_2+1} \cdots V_{a_m,b_m+1}. \end{aligned}$$

□

## 6.2 The decomposition result

Theorem 6.2.1, the fundamental result in all dint-based factorizations, is ready to be stated and proved. It is inspired by the work of Craigen and Woodford [8], who proved Theorem 6.2.1 in the case where the pair is a $BCP_1$. In essence, any polynomial pair with a left and right dint can be multiplied by a suitable decomposing factor $V_{a,b}$ which will decrease the maximum degree of the pair while preserving the pair's Gram-sum. When the pair in question is a $BCP$, the decomposing factor $V_{a,b}$ is uniquely determined. This process may be repeated until one is left with a trivial pair, an identical twin pair, or a pair of unequal degree.

**Theorem 6.2.1** (Craigen and Woodford, 2002 [8], and Gobin, 2022)**.** Let $a_L, a_R, c \in \mathbb{Z}^+$, $b, d \in \mathbb{Z}$, and $(f, g)$ be a pair of equal degree polynomials over $\mathbb{Z}_2$ with left dint $a_L$, right dint $a_R$, and offset $b$. Let $a = \min\{a_L, a_R\}$. Then

1. If $(c, d) = (a, b)$, then $\operatorname{maxdeg}(PM(f, g)V_{c,d}) < \deg(PM(f, g))$;
2. If $c < a$ and $d = b$, then $\deg(PM(f, g)V_{c,d}) = \deg(PM(f, g))$;
3. If $c > a$ and $c \neq \max\{a_L, a_R\}$, or if $d \neq b$, then $\deg(PM(f, g)V_{c,d}) > \deg(PM(f, g))$.

Suppose $(f, g)$ is a $BCP$, but is nontrivial and not an identical twin pair. Then $(f, g)$ has a dint and thus Part 1 shows the unique way to decrease the degree of the pair $(f, g)$, that is, there is a unique pair $(c, d) \in \mathbb{Z}^+ \times \mathbb{Z}$ such that

$$\deg(PM(f, g)V_{c,d}) < \deg(PM(f, g)).$$

*Proof.* Let $\zeta, \eta \in \mathbb{Z}$, $n \in \mathbb{Z}^+$, and write

$$f(x) = x^\zeta \sum_{i=0}^{n} f_i x^i, g(x) = x^\eta \sum_{i=0}^{n} g_i x^i,$$

with $f_0 = g_0 = f_n = g_n = 1$. It follows that $b = \eta - \zeta$. Let

$$\begin{aligned} PM(h(x), k(x)) &= PM(f(x), g(x))V_{c,d} \\ &= PM(f(x), g(x))PM(p(x^c), x^d q(x^c)) \\ &= PM(f(x)p(x^c) + x^{-d}g(x)q(x^c), x^d f(x)q(x^c) + g(x)p(x^c)). \end{aligned}$$

For all $j \in \mathbb{Z}$, let $h_j$ and $k_j$ denote the coefficients of $x^j$ in $h$ and $k$, respectively. The degrees of $h(x)$ and $k(x)$ shall now be examined based on the values of $c$ and $d$.

1.) Suppose $(c, d) = (a, b)$. Then

$$\begin{aligned} h(x) &= f(x)p(x^a) + x^{-b}g(x)q(x^a) \\ &= x^\zeta \left( \sum_{i=0}^{n} f_i x^i \right) p(x^a) + x^{\eta-\eta+\zeta} \left( \sum_{i=0}^{n} g_i x^i \right) q(x^a) \\ &= x^\zeta \left( \sum_{i=0}^{n} f_i x^i \right) p(x^a) + x^\zeta \left( \sum_{i=0}^{n} g_i x^i \right) q(x^a), \end{aligned}$$

and

$$\begin{aligned} k(x) &= x^b f(x)q(x^a) + g(x)p(x^a) \\ &= x^\eta \left( \sum_{i=0}^{n} f_i x^i \right) q(x^a) + x^\eta \left( \sum_{i=0}^{n} g_i x^i \right) p(x^a). \end{aligned}$$

As the $x^\zeta$ and $x^\eta$ may be factored out the equations and is hence irrelevant to the discussion of the degree of the pair, assume without loss of generality that $\zeta = \eta = 0$.

Then

$$\begin{aligned} h_j &= f_j + (f_{j+a} + g_{j+a}) + (f_{j-a} + g_{j-a}) \text{ and} \\ k_j &= g_j + (f_{j+a} + g_{j+a}) + (f_{j-a} + g_{j-a}). \end{aligned}$$

For $j < 0$, one has $a - j < a$ and hence $f_{a-j} = g_{a-j}$ and $f_{n-a+j} = g_{n-a+j}$.

Therefore, for $j < 0$, one has $f_{j+a} + g_{j+a} = f_j = f_{j-a} = g_{j-a} = 0$, and thus

$$h_j = f_j + (f_{j+a} + g_{j+a}) + (f_{j-a} + g_{j-a}) = 0 \text{ and similarly}$$
$$h_{n-j} = f_{n-j} + (f_{n-j+a} + g_{n-j+a}) + (f_{n-j-a} + g_{n-j-a}) = 0.$$

Lastly,

$$h_0 = f_0 + (f_a + g_a) + (f_{-a} + g_{-a}) = 1 + 1 + 0 = 0$$
$$h_n = f_n + (f_{n+a} + g_{n+a}) + (f_{n-a} + g_{n-a}) = 1 + 0 + 1 = 0.$$

Therefore, the smallest power of $x$ in $h$ is at least 1, and the largest is at most $n-1$. Therefore, $\deg(h(x)) \leqslant n-2$. The fact that $\deg(k(x)) \leqslant n-2$ follows similarly.

2.) Suppose $c < a$ and $d = b = 0$. Then for integers $j < 0$, one has $j + c < c < a$ and hence $f_j = 0$, $f_{j+c} = g_{j+c}$, and $f_{n-j-c} = g_{n-j-c}$. Therefore,

$$h_j = f_j + (f_{j+c} + g_{j+c}) + (f_{j-c} + g_{j-c}) = 0, \text{ and}$$
$$h_{n-j} = f_{n-j} + (f_{n-j+c} + g_{n-j+c}) + (f_{n-j-c} + g_{n-j-c}) = 0.$$

Now,

$$h_0 = f_0 + (f_c + g_c) + (f_{-c} + g_{-c}) = 1 + 0 + 0 = 1 \text{ and}$$
$$h_n = f_n + (f_{n+c} + g_{n+c}) + (f_{n-c} + g_{n-c}) = 1 + 0 + 0 = 1.$$

Therefore, $\deg(h(x)) = n$. It follows similarly that $\deg(k(x)) = n$.

3.) Suppose $d \neq b$. Then one sees that the greatest powers of $x$ in $f(x)p(x^c)$ and $x^{-d}g(x)q(x^c)$ are not equal, nor their lowest. As such, the degree of $h(x)$ is necessarily greater than $n$. Similar analysis shows the degree of $k(x)$ is necessarily greater than $n$, and that $h(x)$ and $k(x)$ have equal degrees.

Now suppose without loss of generality that $\zeta = \eta = d = b = 0$ and that $a < c < \max\{a_L, a_R\}$. One can see that it does not matter which of $a_L$ and $a_R$ is the minimum and which is the maximum, hence assume without loss of generality that $a_L = a$. Recall that for all $j < 0$, one has $f_j = g_j = f_{n-j} = g_{n-j} = 0$, $f_{a_L+j} = g_{a_L+j}$, and $f_{n-a_R+j} = g_{n-a_R+j}$. Also note that for all $j \leqslant 0$, one obtains $a - c + j < 0$. When $j < 0$, one obtains

$$h_{a-c+j} = f_{a-c+j} + (f_{a+j} + g_{a+j}) + (f_{a-2c+j} + g_{a-2c+j}) = 0 + 0 + 0 = 0, \text{ and}$$
$$h_{n-a+c-j} = f_{n-a+c-j} + (f_{n-a+2c-j} + g_{n-a+2c-j}) + (f_{n-a-j} + g_{n-a-j}) = 0 + 0 + 0 = 0.$$

Now,

$$h_{a-c} = f_{a-c} + (f_a + g_a) + (f_{a-2c} + g_{a-2c}) = 0 + 1 + 0 = 1, \text{ and}$$
$$h_{n-a+c} = f_{n-a+c} + (f_{n-a+2c} + g_{n-a+2c}) + (f_{n-a} + g_{n-a}) = 0 + 0 + 1 = 1.$$

Therefore, $\deg(h(x)) = n + 2(c-a) > n$. The fact that $\deg(k(x)) = n + 2(c-a) > n$ follows similarly.

Now assume $a_L < a_R < c$. Then $a_L - c < 0$ and $a_R - c < 0$, so for all $j \leqslant 0$ one obtains $f_{a_L-c+j} = f_{a_L-2c+j} = g_{a_L-2c+j} = f_{n+c-a_R-j} = g_{n+c-a_R-j} = 0$. Thus for $j < 0$ one obtains

$$\begin{aligned} h_{a_L-c+j} &= f_{a_L-c+j} + (f_{a_L+j} + g_{a_L+j}) + (f_{a_L-2c-j} + g_{a_L-2c-j}) \\ &= 0 + 0 + 0 \\ &= 0, \text{ and} \\ h_{n+c-a_R-j} &= f_{n+c-a_R-j} + (f_{n+2c-a_R-j} + g_{n+2c-a_R-j}) + (f_{n-a_R-j} + g_{n-a_R-j}) \\ &= 0 + 0 + 0 \\ &= 0. \end{aligned}$$

Furthermore,

$$h_{a_L-c} = f_{a_L-c} + (f_{a_L} + g_{a_L}) + (f_{a_L-2c} + g_{a_L-2c}) = 0 + 1 + 0 = 1, \text{ and}$$
$$h_{n+c-a_R} = f_{n+c-a_R} + (f_{n+2c-a_R} + g_{n+2c-a_R}) + (f_{n-a_R} + g_{n-a_R}) = 0 + 0 + 1 = 1.$$

Therefore, $\deg(h(x)) = (n + c - a_R) - (a_L - c) = n + (2c - a_R - a_L) > n$. One similarly verifies that $\deg(k(x)) = n + c - a_R - a_L + c = n + (2c - a_R - a_L) > n$. □

Theorem 6.2.1 omits the case when $a_L \neq a_R$, $c = \max\{a_L, a_R\}$, and $d = b$. In this case there is insufficient information to predict if $\text{maxdeg}\,(PM(f, g)V_{c,d})$ is larger, smaller, or equal to $\deg(PM(f, g))$, as the following example illustrates:

**Example 6.2.1.** Consider the pairs $f(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$ and $g(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$, $h(x) = 1 + x + x^2 + x^3 + x^5 + x^8$ and $k(x) = 1 + x + x^3 + x^4 + x^5 + x^8$, $r(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^8$ and $s(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^8$, each with degree 8, offset 0, left dint 2, and right dint 4.

The maximum degree of the following pairs

$$PM(f, g)V_{4,0} = PM(x^7 + x^5 + x^3 + x^2 + x + x^{-2}, x^7 + x^5 + x^4 + x^3 + x + x^{-2}),$$
$$PM(h, k)V_{4,0} = PM(x^6 + x^5 + x^3 + x^2 + x + x^{-2}, x^6 + x^5 + x^4 + x^3 + x + x^{-2}),$$
and
$$PM(r, s)V_{4,0} = PM(x^5 + x^3 + x^2 + x + x^{-2}, x^5 + x^4 + x^3 + x + x^{-2})$$

are 9, 8, and 7, respectively. □

**Example 6.2.2.** In order to illustrate Theorem 6.2.1, consider $f(x) = 1 + x + x^2 + x^3 + x^5 + x^6 + x^7 + x^8$ and $g(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$, which form a pair with degree 8, offset 0, left dint 2 and right dint 4. By Part 1 of Theorem 6.2.1, the maximum degree of $PM(f, g)V_{2,0}$ is smaller than the degree

of $(f, g)$. By Part 2 of Theorem 6.2.1, the degree of $PM(f, g)V_{1,0}$ is equal to the degree of $(f, g)$. Lastly, by Part 3 of Theorem 6.2.1, the degrees of $PM(f, g)V_{3,0}$, $PM(f, g)V_{5,0}$, and $PM(f, g)V_{2,4}$ are larger than the degree of $(f, g)$. Indeed, one has

$$\begin{aligned}
PM(f,g)V_{2,0} =& PM(x^8+x^7+x^5+x^4+x^3+x, x^8+x^7+x^5+x^3+x^2+x)\\
PM(f,g)V_{1,0} =& PM(x^8+x^7+x^6+x^3+x^2+1, x^8+x^7+x^6+x^4+x^3+1),\\
PM(f,g)V_{3,0} =& PM(x^8+x^6+x^3+x^2+1+x^{-1}, x^8+x^6+x^4+x^3+1+x^{-1}),\\
PM(f,g)V_{5,0} =& PM(x^9+x^8+x^6+x^5+x^3+x^2+x+1+x^{-1}+x^{-3},\\
& \quad x^9+x^8+x^6+x^5+x^4+x^3+x+1+x^{-1}+x^{-3}),\\
PM(f,g)V_{2,4} =& PM(x^{10}+x^9+x^6+x^4+1+x^{-1}+x^{-2}+x^{-3}+x^{-5}+x^{-6},\\
& \quad x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^4+x^2+1+x^{-1}+x^{-2}).
\end{aligned}$$

□

Now that the decomposition result has been established, the factorizations one obtains for different pairs of Boolean polynomials shall be derived.

## 6.3 Factorizations of odd-weight Boolean complementary pairs

Let $(f, g)$ be a $BCP_1$. Then as $(ff^* + gg^*)(1) = f(1)^2 + g(1)^2 = 1$, either $f(1) = 1$ and $g(1) = 0$ or vice-versa. For convenience, it will always be assumed that $f(1) = 1$ and $g(1) = 0$.

### 6.3.1 Canonical factorizations

**Corollary 6.3.1** (Craigen and Woodford, 2002 [8])**.** Let $m \in \mathbb{Z}^+$. A pair of polynomials $(f, g)$ is a $BCP_1$ if and only if there exist $a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$ and

$c, b_1, b_2, \ldots, b_m \in \mathbb{Z}$ such that

$$PM(f,g) = X^c V_{a_1,b_1} V_{a_2,b_2} \cdots V_{a_m,b_m}.$$

*Proof.* ($\Rightarrow$) Let $(f,g)$ be a $BCP_1$. If the pair has degree zero, then as $PM(f(1), g(1)) = I$, there exists an integer $c$ such that $PM(f,g) = PM(x^c, 0)$, and thus the pair has the desired form.

Assume $(f,g)$ has degree greater than or equal to 1. As $(f,g)$ has odd weight, the pair is not an identical twin pair and thus $(f,g)$ has a dint, call it $a$. Suppose the offset of the pair is $b$. Then by Theorem 6.2.1, the maximum degree of $PM(f,g)V_{a,b}$ is strictly less than that of $PM(f,g)$. However, the resultant pair $PM(f,g)V_{a,b}$ is another $BCP_1$ by Corollary 6.1.5. By Corollary 6.1.10, the resultant pair either has a dint or is a pair of degree zero. Therefore, it is seen that the decomposition process of Theorem 6.2.1 can be repeated until one is left with the pair matrix of a degree zero pair, which by the same reasoning as above is some power of $X$. Therefore, there exist $m, a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$ and $b_1, b_2, \ldots, b_m, c \in \mathbb{Z}$ such that

$$PM(f,g) V_{a_m,b_m} V_{a_{m-1},b_{m-1}} \cdots V_{a_1,b_1} = X^c. \tag{6.3.1}$$

By Lemma 6.1.12, $V_{a,b}^{-1} = V_{a,b}$ and thus

$$\begin{aligned} PM(f,g) &= PM(f,g) \left(V_{a_m,b_m} V_{a_{m-1},b_{m-1}} \cdots V_{a_1,b_1}\right) \left(V_{a_1,b_1} V_{a_2,b_2} \cdots V_{a_m,b_m}\right) \\ &= X^c V_{a_1,b_1} V_{a_2,b_2} \cdots V_{a_m,b_m}. \end{aligned} \tag{6.3.2}$$

($\Leftarrow$) Follows from Corollary 6.1.5. □

**Example 6.3.1.** Consider the polynomials $f(x) = 1 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$ and $g(x) = 1 + x^2 + x^3 + x^4 + x^7 + x^8$, which form a $BCP(9, 13)$. The pair has dint

2 and offset 0. To decompose the pair, one calculates

$$PM(f,g)V_{2,0} = PM(x^6 + x^5 + x^4, x^4 + x^2).$$

The pair $(x^6 + x^5 + x^4, x^4 + x^2)$ has dint 1 and offset $-2$. Again, one calculates

$$PM(f,g)V_{2,0}V_{1,-2} = PM(x^5, 0).$$

Therefore, by Lemma 6.1.12,

$$\begin{aligned} PM(f,g) &= (PM(f,g)V_{2,0}V_{1,-2})\,(V_{1,-2}V_{2,0}) \\ &= PM(x^5,0)V_{1,-2}V_{2,0} \\ &= X^5V_{1,-2}V_{2,0}. \end{aligned}$$ □

Assume for the remainder of the thesis that $m \in \mathbb{Z}^+$ and for all $i \in \mathbb{Z}^+$, that $a_i \in \mathbb{Z}^+$ and $b_i \in \mathbb{Z}$.

As noted in Lemma 6.1.13, there is commutativity among the $V_{a_i,b_i}$s that have the same offset $b_i$. Therefore, one does not necessarily have a unique way to express some $BCP_1$s as a product $X^cV_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$—an additional condition is required to obtain uniqueness.

**Definition 6.3.2.** For positive integers $i$, let $h_i, k_i \in \mathbb{Z}_2[x, x^{-1}]$. The product

$$PM(h_1,k_1)PM(h_2,k_2)\cdots PM(h_m,k_m)$$

is a **climbing product** if and only if for all $i$ such that $1 \leqslant i < m$, one has

$$\begin{aligned} &\deg(PM(h_1,k_1)PM(h_2,k_2)\cdots PM(h_i,k_i)) \\ &< \deg(PM(h_1,k_1)PM(h_2,k_2)\cdots PM(h_{i+1},k_{i+1})). \end{aligned}$$

**Lemma 6.3.3.** Let $(h, k)$ be a $BCP$ and let

$$PM(f, g) = PM(h, k)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m},$$

a climbing product. Then $(f, g)$ has dint $a_m$ and offset $b_m$.

*Proof.* The degree of a climbing product is always increasing, hence

$$\begin{aligned}\deg(PM(f,g)V_{a_m,b_m}) &= \deg(PM(h,k)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}}V_{a_m,b_m}^2)\\ &= \deg(PM(h,k)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}})\\ &< \deg(PM(h,k)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m})\\ &= \deg(PM(f,g)).\end{aligned}$$

Therefore, by Theorem 6.2.1, $V_{a_m,b_m}$ is the unique $V_{c,d}$ which decreases $PM(f, g)$'s degree through post-multiplication. Therefore, by Theorem 6.2.1 again, the pair $(f, g)$ has dint $a_m$ and offset $b_m$. □

**Definition 6.3.4.** Let $(f, g)$ be a $BCP_1$. The climbing product $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ is the **canonical factorization** of $(f, g)$ if and only if there exists $c \in \mathbb{Z}$ such that

$$PM(f, g) = X^c V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}.$$

In a canonical factorization, the $V_{a_i,b_i}$s are referred to as **canonical factors**.

**Lemma 6.3.5.** Let $(f, g)$ be a $BCP_1$. There exist unique $a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$ and $c, b_1, b_2, \ldots, b_m \in \mathbb{Z}$ such that $PM(f, g)$ equals the climbing product $X^c V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$.

*Proof.* Let $c_1, c_2, \ldots, c_n \in \mathbb{Z}^+$, $\mu, \lambda, d_1, d_2, \ldots, d_n \in \mathbb{Z}$, and suppose $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ and $V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_n,d_n}$ are two climbing products such that

$$PM(f, g) = X^\mu V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m} = X^\lambda V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_n,d_n}.$$

Since $PM(f,g)$ is equal to the climbing product $X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$, Lemma 6.3.3 implies that $PM(f,g)$ has dint $a_m$ and offset $b_m$. Therefore,

$$\begin{aligned} PM(f,g)V_{a_m,b_m} &= X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}}\left(V_{a_m,b_m}V_{a_m,b_m}\right) \\ &= X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}}, \end{aligned}$$

and $X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}}$ is a climbing product. However, $PM(f,g)$ is also equal to the climbing product $X^{\lambda}V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_n,d_n}$, hence Lemma 6.3.3 also implies that $PM(f,g)$ has dint $c_n$ and offset $d_n$. Therefore,

$$\begin{aligned} PM(f,g)V_{c_n,d_n} &= X^{\lambda}V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_{n-1},d_{n-1}}\left(V_{c_n,d_n}V_{c_n,d_n}\right) \\ &= X^{\lambda}V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_{n-1},d_{n-1}}, \end{aligned}$$

and $X^{\lambda}V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_{n-1},d_{n-1}}$ is a climbing product. As each $BCP_1$ has a unique dint and offset, it follows that $a_m = c_n$ and $b_m = d_n$. Therefore,

$$PM(f,g)V_{a_m,b_m} = X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{m-1},b_{m-1}} = X^{\lambda}V_{c_1,d_1}V_{c_2,d_2}\cdots V_{c_{n-1},d_{n-1}}.$$

Repeating this procedure will show that $m = n$, $a_i = c_i, b_i = d_i$, and $\mu = \lambda$. □

**Theorem 6.3.6.** Odd-weight Boolean complementary pairs have a unique canonical factorization. Pairs with the same canonical factorization differ by a shift.

*Proof.* Uniqueness of canonical factorizations for a fixed $BCP_1$ follows from Lemma 6.3.5. Suppose $PM(f,g)$ and $PM(h,k)$ both have canonical factorization $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$. Then there exist $\mu, \lambda \in \mathbb{Z}$ such that

$$\begin{aligned} PM(f,g) &= X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}, \text{ and} \\ PM(h,k) &= X^{\lambda}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}. \end{aligned}$$

Therefore,

$$\begin{aligned} PM(x^{\lambda-\mu}f, x^{\lambda-\mu}g) &= X^{\lambda-\mu}PM(f,g) \\ &= X^{\lambda-\mu}X^{\mu}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m} \\ &= X^{\lambda}V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m} \\ &= PM(h,k). \end{aligned}$$ □

One can easily obtain the canonical factorization of a $BCP_1$ by decomposing it then applying Lemma 6.1.12. Explicitly, suppose $PM(f,g)$ is a $BCP_1$ which has been decomposed by Theorem 6.2.1 so that

$$PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1} = X^c.$$

By Lemma 6.1.12, one obtains

$$\begin{aligned} X^cV_{a_1,b_1} &= \left(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}V_{a_1,b_1}\right)V_{a_1,b_1} \\ &= \left(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}\right)(V_{a_1,b_1}V_{a_1,b_1}) \\ &= PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}. \end{aligned}$$

Since post-multiplying $PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}$ by $V_{a_1,b_1}$ decreased the degree of $PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}$, one sees that

$$\deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}) < \deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}).$$

Therefore,

$$\begin{aligned} \deg(X^c) &= \deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}) \\ &< \deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}) \\ &= \deg(X^cV_{a_1,b_1}). \end{aligned}$$

Thus $X^c V_{a_1,b_1}$ is a climbing product. Similarly, post-multiplying $PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_3,b_3}$ by $V_{a_2,b_2}$ decreased the degree of $PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_3,b_3}$, so

$$\begin{aligned}\deg(X^c V_{a_1,b_1}) &= \deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_2,b_2}) \\ &< \deg(PM(f,g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_3,b_3}) \\ &= \deg(X^c V_{a_1,b_1}V_{a_2,b_2}).\end{aligned}$$

Therefore, $X^c V_{a_1,b_1}V_{a_2,b_2}$ is also a climbing product. Continuing in this way shows that $PM(f,g)$ is equal to the climbing product $X^c V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$, hence $V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}$ is $PM(f,g)$'s canonical factorization.

When working with an arbitrary $BCP_1$, it can often be assumed without loss of generality that the pair is equal to its canonical factorization and has offset zero. To see why this can be done, suppose $c,d \in \mathbb{Z}$ and $PM(f,g) = X^c V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ has offset $d$. By Lemma 6.1.16, one has

$$Z^{-2c-d}PM(f,g)Z^d = PM(x^{-c}f, x^{-c-d}g) = V_{a_1,b_1-d}V_{a_2,b_2-d}\cdots V_{a_m,b_m-d}.$$

As $(f,g)$ has offset $b_m = d$, the pair $(x^{-c}f, x^{-c-d}g)$ has offset zero and is equal to its canonical factorization. Results about the pair $(x^{-c}f, x^{-c-d}g)$ are easily extended to the pair $(f,g)$, hence nothing is lost with these assumptions.

Section 7.4 contains tables of canonical factorizations of $BCP_1$s. These $BCP_1$s come from the $TCP$s in Craigen and Koukouvinos' paper [7], which were turned into $BCP$s through the homomorphism in Lemma 5.1.2 then factored using Theorem 6.2.1.

### 6.3.2 Superfactorizations

Certain results are difficult to state through canonical factorizations, but are easy to state through superfactorizations (Definition 6.3.10). The main ingredient in superfactorizations is the canonical factorizations of siamese twin pairs, which are solved for as a consequence of the following lemma.

First note that if $(f, g)$ is a siamese twin pair, then there exist $n \in \mathbb{Z}^+$, $b, d \in \mathbb{Z}$, and $s_1, s_2, \ldots, s_n \in \{0, 1\}$ such that

$$(f, g) = \left( x^b \sum_{i=1}^{n} s_i(x^i + x^{-i}) + x^b, x^d \sum_{i=1}^{n} s_i(x^i + x^{-i}) \right).$$

For instance, suppose $(f, g) = (x^3(x^{-2} + x^{-1} + 1 + x + x^2), x^{-5}(x^{-2} + x^{-1} + x + x^2))$, which is a degree 4 siamese twin pair. Let $s_1 = s_2 = 1$. Then

$$(f, g) = \left( x^3 \sum_{i=1}^{2} s_i(x^i + x^{-i}) + x^3, x^{-5} \sum_{i=1}^{2} s_i(x^i + x^{-i}) \right).$$

**Lemma 6.3.7.** Let $n \in \mathbb{Z}^+$, and for $i = 1, 2, \ldots, n$, let $s_i \in \{0, 1\}$ and let $s = \sum_{i=1}^{n} s_i(x^i + x^{-i})$. Then for all $b \in \mathbb{Z}$, the siamese twin pair $(s + 1, x^b s)$ satisfies

$$PM(s + 1, x^b s) = V_{s_1,b} V_{2s_2,b} \cdots V_{ns_n,b}.$$

*Proof.* (Induction on $n$) If this result is true, then by Lemma 6.1.16 one obtains

$$\begin{aligned} PM(s + 1, x^b s) &= Z^b PM(s + 1, s) Z^{-b} \\ &= Z^b V_{s_1,0} V_{2s_2,0} \cdots V_{ns_n,0} Z^{-b} \\ &= V_{s_1,b} V_{2s_2,b} \cdots V_{ns_n,b}. \end{aligned}$$

Thus it may be assumed without loss of generality that $b = 0$.

Let $n \in \mathbb{Z}^+$ and let $P(n)$ denote the statement that for $s(x) = \sum_{i=1}^{n} s_i(x^i + x^{-i})$, one has

$$PM(s+1, s) = V_{s_1,0} V_{2s_2,0} \cdots V_{ns_n,0}.$$

**Base case:** For $n = 1$, the statement $P(n)$ is trivially true as one has

$$PM(s+1, s) = PM(1, 0) = V_{0,0}, \text{ or}$$
$$PM(s+1, s) = PM(x^{-1} + 1 + x, x^{-1} + x) = V_{1,0}.$$

**Inductive step:** Fix $k \geqslant 1$ and suppose $P(k)$ is true. Let $s = \sum_{i=1}^{k} s_i x^i + 1 + \sum_{i=1}^{k} s_i x^{-i}$. Then by $P(k)$, one has

$$PM(s+1, s) = V_{s_1,0} V_{2s_2,0} \cdots V_{ks_k,0}.$$

Let $s_{k+1} \in \{0, 1\}$ and define the new polynomial $S(x)$ as $S = \sum_{i=1}^{k+1} s_i x^i + \sum_{i=1}^{k+1} s_i x^{-i}$. If $s_{k+1} = 0$, then $S = s$ and the result follows as $V_{(k+1)s_{k+1},0} = I$. Therefore, assume $s_{k+1} = 1$. Then

$$\begin{aligned}
PM(s+1, s) V_{(k+1)s_{k+1},0} &= PM(s+1, s) V_{k+1,0} \\
&= PM(s+1, s) PM(p(x^{k+1}), q(x^{k+1})) \\
&= PM((s+1)p(x^{k+1}) + sq(x^{k+1}), \\
&\quad (s+1)q(x^{k+1}) + sp(x^{k+1})) \\
&= PM(p(x^{k+1}) + s(p(x^{k+1}) + q(x^{k+1})), \\
&\quad q(x^{k+1}) + s(p(x^{k+1}) + q(x^{k+1}))) \\
&= PM(p(x^{k+1}) + s, q(x^{k+1}) + s) \\
&= PM(\sum_{i=1}^{k+1} s_i x^i + 1 + \sum_{i=1}^{k+1} s_i x^{-i}, \sum_{i=1}^{k+1} s_i x^i + \sum_{i=1}^{k+1} s_i x^{-i}) \\
&= PM(S+1, S).
\end{aligned}$$

Therefore, $P(k+1)$ is true. Observe that when $s_{k+1} = 1$, one has

$$\deg(PM(s+1,s)V_{k+1,0}) > \deg(PM(s+1,s)),$$

and when $s_{k+1} = 0$, one has

$$\deg(PM(s+1,s)V_{k+1,0}) = \deg(PM(s+1,s)).$$

**Conclusion:** Therefore, by the Principle of Mathematical Induction, for all $t \in \mathbb{Z}^+$, the statement $P(t)$ is true. □

Consider the siamese twin pair $(s+1, x^b s)$ in the statement of Lemma 6.3.7. If $s_i = 0$, then $V_{is_i,b} = I$ and so there exists $j \in \mathbb{Z}^+$ and integers $a_1, a_2, \ldots, a_j$ with $0 < a_1 < a_2 < \ldots < a_j$ such that $PM(s+1, x^b s) = V_{a_1,b}V_{a_2,b}\cdots V_{a_j,b}$. It is seen from the proof of Lemma 6.3.7 that $V_{a_1,b}V_{a_2,b}\cdots V_{a_j,b}$ is a climbing product and thus the canonical factorization of the pair. Thus far, siamese twin pairs are the only type of $BCP_1$s whose canonical factorization (and the later superfactorization) can be derived without any computation.

**Example 6.3.2.** Let $s = x^{-4} + x^{-3} + x^3 + x^4$ and $b \in \mathbb{Z}$. Then $(s+1, x^b s)$ is a siamese twin pair, and for $s_1 = s_2 = 0$ and $s_3 = s_4 = 1$, the polynomial $s$ can equivalently be expressed as $s = \sum_{i=1}^{4} s_i(x^i + x^{-i})$. By Lemma 6.3.7, one has

$$PM(s+1, x^b s) = V_{0,b}V_{0,b}V_{3,b}V_{4,b} = I^2 V_{3,b}V_{4,b} = V_{3,b}V_{4,b},$$

and $V_{3,b}V_{4,b}$ is the canonical factorization of $PM(s+1, x^b s)$. □

**Corollary 6.3.8.** The pair $(f, g)$ is a $BCP_1$ if and only if there exist $c \in \mathbb{Z}$, $M \in \mathbb{Z}^+$,

and siamese twin pairs $S_1, S_2, \ldots, S_M$ such that

$$PM(f,g) = X^c S_1 S_2 \cdots S_M.$$

*Proof.* The result follows from Corollary 6.3.1 and Lemma 6.3.8. □

For the remainder of the thesis, assume for any $i, b \in \mathbb{Z}$ that there exist $j \in \mathbb{Z}^+$, positive integers $a_1, a_2, \ldots, a_j$ with $a_1 < a_2 < \cdots < a_j$, and a tuple $\vec{\alpha}_i = (a_1, a_2, \ldots, a_j)$ such that

$$S_{\vec{\alpha}_i, b} = V_{a_1,b} V_{a_2,b} \cdots V_{a_j,b}.$$

Note that by Lemma 6.3.7, $V_{a_1,b} V_{a_2,b} \cdots V_{a_j,b}$ is a climbing product.

Also assume for the remainder of the thesis that $M \in \mathbb{Z}^+$.

**Definition 6.3.9.** Suppose for integers $i$ such that $1 \leqslant i \leqslant M-1$, the product $S_{\vec{\alpha}_i,b_i} S_{\vec{\alpha}_{i+1},b_{i+1}}$ is not a siamese twin pair. By Lemma 6.3.7, this condition is equivalent to saying $b_i \neq b_{i+1}$. Then $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is a **superproduct** if and only if it is a climbing product.

**Definition 6.3.10.** Let $(f,g)$ be a $BCP_1$, and for integers $i$ such that $1 \leqslant i \leqslant M$, let the term $S_{\vec{\alpha}_i,b_i}$ be a siamese twin pair with offset $b_i$, and suppose $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is a superproduct. Then $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is $(f,g)$'s **superfactorization** if and only if there exists $c \in \mathbb{Z}$ such that

$$PM(f,g) = X^c S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}.$$

The factors $S_{\vec{\alpha}_i,b_i}$ in $(f,g)$'s superfactorization are called **superfactors**.

**Lemma 6.3.11.** Every $BCP_1$ has a unique superfactorization. Two $BCP_1$s have the same superfactorization if and only if they differ by a shift.

*Proof.* Similar to that of Theorem 6.3.6. □

Note that it is easy to derive a superfactorization from a canonical factorization and vice versa. Suppose $PM(f,g)$ has canonical factorization $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$, and let $k_1 \in \mathbb{Z}^+$ be such that $b_1 = b_2 = \cdots = b_{k_1} \neq b_{k_1+1}$. Then by Lemma 6.3.7, the product $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{k_1},b_{k_1}}$ is a siamese twin pair (with dint $a_{k_1}$ and offset $b_{k_1}$), but $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{k_1},b_{k_1}}V_{a_{k_1+1},b_{k_1+1}}$ is not a siamese twin pair. Therefore,

$$S_{(a_1,a_2,\ldots,a_{k_1}),b_{k_1}} = V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_{k_1},b_{k_1}}$$

is the first superfactor in $(f,g)$'s superfactorization. One then moves on to $V_{a_{k_1+1},b_{k_1+1}}$, and looks for the integer $k_2$ such that $b_{k_1+1} = b_{k_1+2} = \cdots b_{k_1+k_2} \neq b_{k_1+k_2+1}$, and similarly gets that

$$S_{(a_{k_1+1},a_{k_1+2},\ldots,a_{k_1+k_2}),b_{k_1+k_2}} = V_{a_{k_1+1},b_{k_1+1}}V_{a_{k_1+2},b_{k_1+2}}\cdots V_{a_{k_1+k_2},b_{k_1+k_2}}$$

is the second superfactor in $(f,g)$'s superfactorization. This process repeats until the end of $(f,g)$'s canonical factorization.

Conversely, suppose $PM(f,g)$ has superfactorization $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$. Fix a superfactor $S_{\vec{\alpha}_i,b_i}$, and suppose $j \in \mathbb{Z}^+$ is such that $\vec{\alpha}_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,j})$. Then

$$S_{\vec{\alpha}_i,b_i} = V_{a_{i,1},b_i}V_{a_{i,2},b_i}\cdots V_{a_{i,j},b_i}.$$

Since $V_{a_{i,1},b_i}V_{a_{i,2},b_i}\cdots V_{a_{i,j},b_i}$ is a climbing product and consecutive superfactors have different offsets, expressing each factor $S_{\vec{\alpha}_i,b_i}$ as the product of its constituent canonical factors in $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$ yields a climbing product. This product is therefore the pair $(f,g)$'s canonical factorization.

**Example 6.3.3.** Consider the primitive $TCP(14, 13)$

$$(\texttt{11001001-0-001, 1000-0000-10--}),$$

which corresponds to the $BCP(14, 13)$

$$(F, G) = (\texttt{11001001101001, 10001000011011})$$

under the homomorphism in Lemma 5.1.2. The pair $(F, G)$'s associated polynomial pair $(f, g)$ has canonical factorization $V_{2,-1}V_{3,-1}V_{1,1}V_{1,0}$ and superfactorization $S_{(2,3),-1}S_{(1),1}S_{(1),0}$. To derive the superfactorization from the canonical factorization, one begins by noticing the consecutive factors $V_{2,-1}$ and $V_{3,-1}$ have offset $-1$, so $V_{2,-1}V_{3,-1}$ is a siamese twin pair of dint 3 and offset $-1$. The next canonical factor is $V_{1,1}$, which has offset 1, not $-1$, hence $V_{2,-1}V_{3,-1}V_{1,1}$ is not a siamese twin pair. Therefore, the first superfactor of $(f, g)$ is $S_{(2,3),-1} = V_{2,-1}V_{3,-1}$. Similarly, $V_{1,0}$ and $V_{1,1}$ have different offsets, so $V_{1,1}V_{1,0}$ is not a siamese twin pair either. Thus $S_{(1),1} = V_{1,1}$ is the second superfactor, and $S_{(1),0} = V_{1,0}$ is the third. Therefore, $S_{(2,3),-1}S_{(1),1}S_{(1),0}$ is $(f, g)$'s superfactorization.

To derive the canonical factorization from the superfactorization, one sees that $S_{(2,3),-1} = V_{2,-1}V_{3,-1}$, $S_{(1),1} = V_{1,1}$, and $S_{(1),0} = V_{1,0}$. Therefore, $(f, g)$'s canonical factorization is $(V_{2,-1}V_{3,-1})(V_{1,1})(V_{1,0}) = V_{2,-1}V_{3,-1}V_{1,1}V_{1,0}$.

Now consider the primitive $TCP(17, 13)$

$$(\texttt{100-0-011-0101001, 100000-0-0000000-}),$$

which corresponds to the $BCP(17, 13)$

$$(H, K) = (\texttt{10010101110101001, 10000010100000001})$$

under the homomorphism in Lemma 5.1.2. The pair $(H, K)$'s associated polynomial pair $(h, k)$ has canonical factorization $V_{1,0}V_{3,0}V_{1,-1}V_{1,0}V_{3,0}$ and superfactorization $S_{(1,3),0}S_{(1),-1}S_{(1,3),0}$. To derive the superfactorization from the canonical factorization, one sees that $V_{1,0}$ and $V_{3,0}$ are consecutive canonical factors with the same offset, but $V_{1,-1}$ has a different offset. Thus $S_{(1,3),0} = V_{1,0}V_{3,0}$ is $(h, k)$'s first superfactor. Next, $V_{1,-1}$ has a different offset than the next canonical factor $V_{1,0}$, hence $S_{(1),-1} = V_{1,-1}$ is the next superfactor. Lastly, the remaining two canonical factors $V_{1,0}$ and $V_{3,0}$ have the same offset, hence $S_{(1,3),0} = V_{1,0}V_{3,0}$ is the final superfactor in $(h, k)$'s superfactorization.

From $(h, k)$'s superfactorization $S_{(1,3),0}S_{(1),-1}S_{(1,3),0}$, one reads that

$$\begin{aligned} S_{(1,3),0} &= V_{1,0}V_{3,0}, \\ S_{(1),-1} &= V_{1,-1}, \text{ and} \\ S_{(1,3),0} &= V_{1,0}V_{3,0}. \end{aligned}$$

Thus

$$(V_{1,0}V_{3,0})(V_{1,-1})(V_{1,0}V_{3,0}) = V_{1,0}V_{3,0}V_{1,-1}V_{1,0}V_{3,0}$$

is $(h, k)$'s superfactorization. □

## 6.4 Factorizations of even-weight Boolean complementary pairs

Even-weight Boolean complementary pairs have pair matrix factorizations similar to those of $BCP_1$s.

**Corollary 6.4.1.** A pair $(f, g)$ is a $BCP_0$ if and only if there exist $a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$, $c, b_1, b_2, \ldots, b_m \in \mathbb{Z}$, and $h \in \mathbb{Z}_2[x, x^{-1}]$ such that

$$PM(f, g) = PM(h, x^c h)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}.$$

Furthermore, if $PM(h, x^c h)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ is a climbing product, then this expression of $PM(f, g)$ is unique.

*Proof.* ($\Rightarrow$) If $(f, g)$ is an identical twin pair, then $PM(f, g)$ is in the desired form. Suppose $(f, g)$ is not an identical twin pair. Then by Corollary 6.1.10, the pair $(f, g)$ has a dint, call it $a_m$. Let $b_m$ be the offset of $(f, g)$. Then by Theorem 6.2.1, $\deg(PM(f, g)V_{a_m,b_m}) < \deg(PM(f, g))$. By Corollary 6.1.5, the pair obtained by the product $PM(f, g)V_{a_m,b_m}$ is a $BCP_0$. Repeatedly apply Theorem 6.2.1 in this way to get $a_1, a_2, \ldots, a_m \in \mathbb{Z}^+$, $b_1, b_2, \ldots, b_m \in \mathbb{Z}$, and $h, k \in \mathbb{Z}_2[x, x^{-1}]$ where $(h, k)$ does not have a dint, such that

$$PM(f, g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1} = PM(h, k).$$

By applying Lemma 6.1.12, one obtains

$$\begin{aligned} PM(f, g) &= PM(f, g)\left(V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}\right)\left(V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}\right) \\ &= \left(PM(f, g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}}\cdots V_{a_1,b_1}\right)\left(V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}\right) \\ &= PM(h, k)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}. \end{aligned}$$

Since $(h,k)$ does not have a dint, $(h,k)$ is either an identical twin pair or there exists $e \in \mathbb{Z}$ such that $(h,k) \in \{(x^e,0),(0,x^e)\}$. However, if $(h,k) \in \{(x^e,0),(0,x^e)\}$, then by Corollary 6.1.5 the pair $(f,g)$ is a $BCP_1$, not a $BCP_0$. Therefore, $(h,k)$ is an identical twin pair and thus there exists $c \in \mathbb{Z}$ such that

$$PM(f,g) = PM(h,x^c h)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}.$$

The fact that $PM(h,x^c h)V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ is a climbing product and the unique way to express $PM(f,g)$ as a climbing product is the same as in the proof of Lemma 6.3.5.

($\Leftarrow$) Follows by Corollary 6.1.5. □

**Example 6.4.1.** Consider $f = x^{-2}(1+x^5+x^7+x^9+x^{10})$ and $g = x^{-2}(+x^3+x^6+x^9+x^{10})$, which form a $BCP(11,10)$ with dint 3 and offset 0. Decomposing, one sees

$$PM(f,g)V_{3,0} = PM(1+x+x^2+x^3+x^4+x^5+x^6, 1+x^2+x^6)$$

The resultant pair has dint 1 and offset 0. One computes

$$\begin{aligned} PM(f,g)V_{3,0}V_{1,0} &= PM(x^3+x^4+x^6, 1+x+x^3) \\ &= PM(x^3(1+x+x^3), 1+x+x^3) \end{aligned}$$

The pair $(x^3(1+x+x^3), 1+x+x^3)$ is an identical twin pair, and thus

$$PM(f,g) = PM(x^3(1+x+x^3), 1+x+x^3)V_{1,0}V_{3,0}.$$ □

Notice that since any product of the form $V_{a_1,b_1}V_{a_2,b_2}\cdots V_{a_m,b_m}$ is the pair matrix of a $BCP_1$, Corollary 6.4.1 shows that the pair matrix of a $BCP_0$ equals the pair

matrix of an identical twin pair multiplied by the pair matrix of a $BCP_1$.

One could derive a canonical factorization and a superfactorization for $BCP_0$s similar to $BCP_1$s, but pair matrix factorizations are only of interest in this thesis for their application to $BCP_1$s.

## 6.5 Factorizations of non-complementary pairs

Non-complementary pairs also have dint-based factorizations. These factorizations are nontrivial as long as the polynomials have equal degrees, and in general these factorizations are not unique.

Observe that if a pair of polynomials $(f, g)$ is not complementary, then there exists a nonconstant polynomial $r(x)$ such that $(ff^* + gg^*)(x) = r(x)$. As $(ff^* + gg^*)(x)$ is symmetric, then so is $r(x)$. Moreover, recall that by specifying the degree of a symmetric polynomial one immediately specifies its highest and lowest powers of $x$ since that polynomial is centred around $x^0$. It also follows that every symmetric polynomial has even degree.

**Corollary 6.5.1.** Let $f(x), g(x) \in \mathbb{Z}_2[x, x^{-1}]$ and suppose there exist $d \in \mathbb{Z}^+$ and a symmetric polynomial $r(x)$ of degree $2d$ such that

$$(ff^* + gg^*)(x) = r(x). \tag{6.5.1}$$

Then there exist $h(x), k(x) \in \mathbb{Z}_2[x, x^{-1}]$ with one of $h(x)$ and $k(x)$ having degree $d$ and the other strictly less than $d$, and $m \in \mathbb{N}$ such that

$$PM(f, g) = PM(h, k)V_{a_1,b_1}V_{a_2,b_2} \cdots V_{a_m,b_m}.$$

Furthermore, for any $a \in \mathbb{Z}^+$ and $b \in \mathbb{Z}$, one obtains $\operatorname{maxdeg}(PM(h, k)V_{a,b}) \geqslant d$.

*Proof.* Let $n_f, n_g$ be the degrees of $f$ and $g$ and let $c, d \in \mathbb{Z}$ be such that $f = x^c \sum_{i=0}^{n_f} f_i x^i$ and $g = x^d \sum_{i=0}^{n_g} g_i x^i$. Suppose $f$ and $g$ have unequal degrees, say $n_f > n_g$. Then by examining equation (6.5.1), one sees that the highest and lowest powers of $x$ in $r(x)$ are $n_f$ and $-n_f$. Therefore, $r(x)$ has degree $2d = 2n_f$, and thus the desired factorization is obtained by taking $h$ and $k$ to be $PM(h, k) = PM(f, g)$.

Assume $f$ and $g$ have equal degrees. If the pair does not have a left and right dint, then $(f, g)$ is either an identical twin pair or a trivial pair, both of which are complementary and thus do not satisfy equation (6.5.1). Therefore, let $(f, g)$ have left and right dint $a_L$ and $a_R$, respectively. Let $a = \min\{a_L, a_R\}$ and $b$ be the offset of $(f, g)$. Then by Theorem 6.2.1,

$$\text{maxdeg}(PM(f, g)V_{a,b}) < \deg(PM(f, g)).$$

One can continue the decomposition process until a pair without a left or right dint is obtained, say

$$PM(f, g)V_{a_m,b_m}V_{a_{m-1},b_{m-1}} \cdots V_{a_1,b_1} = PM(h, k).$$

Again, $h$ and $k$ have unequal degrees, as otherwise the decomposition process can continue. As in the proof of Corollary 6.1.5, one has $(ff^* + gg^*)(x) = (hh^* + kk^*)(x) = r(x)$, and by the same reasoning as above, this implies that one of $h$ and $k$ has degree $d$ and the other has degree less than $d$. By Lemma 6.1.12, one obtains the desired factorization

$$PM(f, g) = PM(h, k)V_{a_1,b_1}V_{a_2,b_2} \cdots V_{a_m,b_m}. \qquad \square$$

**Example 6.5.1.** Consider the pair

$$f = x^{19} + x^{18} + x^{17} + x^{14} + x^{12} + x^{11} + x^{10} + x^6 + x^2 + x + 1,$$
$$g = x^{19} + x^{18} + x^{17} + x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

The pair satisfies

$$(ff^* + gg^*)(x) = x^{-4} + x^{-3} + 1 + x^3 + x^4,$$

and hence is not complementary. By inspection, the pair has degree 19, left and right dint 4, and offset 0. One computes

$$PM(f, g)V_{4,0} = PM(x^{14} + x^{10} + x^8 + x^6 + x^4, x^{15} + x^{13} + x^{10} + x^5).$$

The resultant pair has degree 10, left and right dint 2, and offset 1. Continuing,

$$PM(f, g)V_{4,0}V_{2,1} = PM(x^{12} + x^{11} + x^{10} + x^8 + x^7, x^{12} + x^{10} + x^8 + x^7).$$

The resultant pair has degree 5, left dint 1, right dint 4, and offset 0. One computes

$$PM(f, g)V_{4,0}V_{2,1}V_{1,0} = PM(x^{11} + x^8 + x^7, x^8 + x^7).$$

The resultant polynomials have unequal degrees and satisfy

$$(x^{11} + x^8 + x^7)(x^{-11} + x^{-8} + x^{-7}) + (x^8 + x^7)(x^{-8} + x^{-7}) = x^{-4} + x^{-3} + 1 + x^3 + x^4.$$

Therefore, $PM(x^{11} + x^8 + x^7, x^8 + x^7)V_{1,0}V_{2,1}V_{4,0}$ is a factorization for $PM(f, g)$ in the form of Corollary 6.5.1. □

The following example demonstrates that the factorization in Corollary 6.5.1 is not unique, however, even if one requires the product to be a climbing product:

**Example 6.5.2.** Let

$$r = 1 + x + x^2 + x^3 + x^5 + x^6 + x^8, \text{ and}$$
$$s = 1 + x + x^3 + x^4 + x^5 + x^6 + x^8.$$

Then $(rr^* + ss^*)(x) = x^6 + x^4 + x^{-4} + x^{-6}$, and

$$\begin{aligned} PM(r, s) &= PM(x^3 + x^2 + x^{-2}, x^4 + x^3 + x^{-2})V_{1,0}V_{4,0} \\ &= PM(x^8 + x^4 + x^3, x^8 + x^3 + x^2)V_{1,0}V_{2,0}. \end{aligned}$$

As

$$\begin{aligned} &PM(x^3 + x^2 + x^{-2}, x^4 + x^3 + x^{-2})V_{1,0} \\ &= PM(x^5 + x^3 + x^2 + x + x^{-2}, x^5 + x^4 + x^3 + x + x^{-2}), \text{ and} \\ &PM(x^8 + x^4 + x^3, x^8 + x^3 + x^2)V_{1,0} \\ &= PM(x^8 + x^5 + x^4 + x^3 + x, x^8 + x^5 + x^3 + x^2 + x), \end{aligned}$$

one sees that

$$PM(x^3 + x^2 + x^{-2}, x^4 + x^3 + x^{-2})V_{1,0}V_{4,0} \text{ and}$$
$$PM(x^8 + x^4 + x^3, x^8 + x^3 + x^2)V_{1,0}V_{2,0}$$

are both climbing products and pair matrix factorizations of $PM(r, s)$. □

## 6.6 The different expressions for a $BCP$

As there are many different expressions for a $BCP$, it may be helpful to the reader to see all of these different forms in one place.

### 6.6.1 Sequence

Let $F = (\texttt{101100010101001})$ and $G = (\texttt{101001100100001})$. Then $(F, G)$ has length 15, weight 13, deficiency $2 \times 15 - 13 = 17$, and satisfies

$$AF_F(k) + AF_G(k) = 0 \text{ for all } k \in \mathbb{N}. \tag{6.6.1}$$

Therefore, the pair $(F, G)$ is a $BCP(15, 13)$.

### 6.6.2 Polynomial

If $F$ and $G$ are indexed starting at 0, then their polynomial forms are $f(x) = 1 + x^2 + x^3 + x^7 + x^9 + x^{11} + x^{14}$ and $g(x) = 1 + x^2 + x^5 + x^6 + x^9 + x^{14}$, respectively. The pair $(f, g)$ has degree 14, weight 13, and deficiency 17. One can check that (in $\mathbb{Z}_2[x, x^{-1}]$) one has

$$\begin{aligned}
(ff^* + gg^*)(x) &= (1 + x^2 + x^3 + x^7 + x^9 + x^{11} + x^{14})(1 + x^{-2} + x^{-3} \\
&\quad + x^{-7} + x^{-9} + x^{-11} + x^{-14}) \\
&\quad + (1 + x^2 + x^5 + x^6 + x^9 + x^{14})(1 + x^{-2} + x^{-5} \\
&\quad + x^{-6} + x^{-9} + x^{-14}) \\
&= 13 \\
&= 1.
\end{aligned}$$

By Theorem 2.1.7, the odd-weight pair $(F, G)$ satisfying 6.6.1 is equivalent to $(f(x), g(x))$ satisfying $(ff^* + gg^*)(x) = 1$.

### 6.6.3 Pair matrix

The pair matrix form of $(f, g)$ is

$$\begin{pmatrix} 1 + x^2 + x^3 + x^7 + x^9 + x^{11} + x^{14} & 1 + x^2 + x^5 + x^6 + x^9 + x^{14} \\ 1 + x^{-2} + x^{-5} + x^{-6} + x^{-9} + x^{-14} & 1 + x^{-2} + x^{-3} + x^{-7} + x^{-9} + x^{-11} + x^{-14} \end{pmatrix}.$$

One can verify that $PM(f, g)PM(f, g)^* = I$, which is equivalent to the pair $(f, g)$ being a $BCP_1$ by Theorem 6.1.4.

### 6.6.4 Canonical factorization

The canonical factorization of $(f, g)$ is $V_{1,-2}V_{2,-2}V_{1,-1}V_{3,0}$, and

$$\begin{aligned} PM(f, g) &= X^8 V_{1,-2}V_{2,-2}V_{1,-1}V_{3,0} \\ &= PM(x^8, 0)PM(x^{-1} + 1 + x, x^{-3} + x^{-1})PM(x^{-2} + 1 + x^2, x^{-4} + 1) \\ &\quad \cdot PM(x^{-1} + 1 + x, x^{-2} + 1)PM(x^{-3} + 1 + x^3, x^{-3} + x^3) \end{aligned}$$

### 6.6.5 Superfactorization

The superfactorization of $(f, g)$ is $S_{(1,2),-2}S_{(1),-1}S_{(3),0}$, and

$$\begin{aligned} PM(f, g) &= X^8 S_{(1,2),-2}S_{(1),-1}S_{(3),0} \\ &= PM(x^8, 0)PM(x^{-2} + x^{-1} + 1 + x + x^2, x^{-4} + x^{-3} + x^{-1} + 1) \\ &\quad \cdot PM(x^{-2} + 1 + x^2, x^{-4} + 1)PM(x^{-1} + 1 + x, x^{-2} + 1) \\ &\quad \cdot PM(x^{-3} + 1 + x^3, x^{-3} + x^3). \end{aligned}$$

# 7

# Superfactorizations

With the pair matrix factorizations established, some of their structural implications regarding Boolean complementary pairs are now shown. Sections 7.1 and 7.2 are from this author's 2020 undergraduate research project. For $a \in \mathbb{Z}^+$, this includes a complete classification of all affixes over $\mathbb{Z}_2$ of length $2a+1$ with dint $a$.

## 7.1 Basic results

### 7.1.1 Degree calculation

**Lemma 7.1.1.** Let $n, a \in \mathbb{Z}^+$, let $\vec{\alpha}$ be a tuple over $\mathbb{Z}^+$, let $b, d \in \mathbb{Z}$, and let $(f, g)$ be a degree $n$ polynomial pair in $\mathbb{Z}_2[x, x^{-1}]$ with offset $d$. Suppose $b \neq d$ and $S_{\vec{\alpha},b}$ has dint $a$. Then

$$\deg(PM(f,g)S_{\vec{\alpha},b}) = n + 2a + |b-d|.$$

*Proof.* Let $k \in \mathbb{Z}$ and $(f,g) = \left(x^k \sum_{i=0}^{n} f_i x^i, x^{k+d} \sum_{i=0}^{n} g_i x^i\right)$. Let $s = \sum_{i=1}^{a} s_i \left(x^i + x^{-i}\right)$ be such that $S_{\vec{\alpha},b} = PM(s+1, x^b s)$. By direct verification,

$$PM(f,g)PM(s+1,x^b s) = PM((s+1)f + x^{-b}gs, x^b fs + (s+1)g).$$

By inspection, the highest and lowest powers of $x$ in $(s+1)f$ are $a+k+n$ and $-a+k$, respectively. Similarly, the highest and lowest powers of $x$ in $x^{-b}gs$ are $-b+k+d+n+a = (a+k+n)+(d-b)$ and $-b+k+d-a = (-a+k)+(d-b)$, respectively. Since $d \neq b$, the polynomials $(s+1)f$ and $x^{-b}gs$ do not have the same highest power of $x$, nor do they have the same lowest power of $x$. If $d-b>0$, then the highest and lowest powers of $x$ in $(s+1)f + x^{-b}gs$ are $(a+k+n)+(d-b)$ and $-a+k$, which yields a degree of $(a+k+n)+(d-b)-(-a+k) = n+2a+(d-b)$. If $d-b<0$, one similarly calculates a degree of $n+2a+(b-d)$. As $(s+1)f+x^{-b}gs$ and $x^b fs+(s+1)g$ form a nontrivial $BCP_1$, they have equal degree and the result follows. □

Let $\vec{\alpha}$ be a tuple over $\mathbb{Z}^+$, $b \in \mathbb{Z}$, and $(f,g)$ be a polynomial pair with offset $b$. There is insufficient information about $(f,g)$ in order to predict the degree of $PM(f,g)S_{\vec{\alpha},b}$, as discussed following Theorem 6.2.1.

**Corollary 7.1.2.** Let $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$ be a superproduct and suppose $S_{\vec{\alpha}_i,b_i}$ has dint $c_i$. Then

$$\deg(S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}) = 2\sum_{i=1}^{M} c_i + \sum_{i=1}^{M-1} |b_{i+1}-b_i|.$$

*Proof.* The degree of any superfactor $S_{\vec{\alpha}_i,b_i}$ is $2c_i$, hence Lemma 7.1.1 implies the result. □

**Corollary 7.1.3.** The only positive integers which are not the degree of a $BCP_1$ are 1 and 3.

*Proof.* By Corollary 6.3.8, any $BCP_1$ can be written as a superproduct. If that superproduct has a single superfactor, then its degree is even. If that superproduct has more than one superfactor, then Corollary 7.1.2 shows that its degree is at least 4 and so no $BCP_1$ has degree 1 or 3.

The pair $V_{1,0}$ is a degree 2 siamese twin pair. Let $n \geqslant 4$ be a positive integer. If $n$ is even, then $V_{\frac{n}{2},0}$ is a degree $n$ siamese twin pair. If $n$ is odd, then let $k, b \in \mathbb{Z}^+$ such that $n = 4k + b$. By Lemma 7.1.1, the pair obtained by the product $V_{k,0}V_{k,b}$ has degree $n = 4k + b$. □

### 7.1.2 Equivalence

The following lemma implies that once one knows the superfactorization of a pair, one knows the superfactorizations and canonical factorizations of all equivalent pairs.

**Lemma 7.1.4.** Let $PM(f, g)$ be equal to the superproduct $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$, and let $t \in \mathbb{Z}$ be nonzero. Then

1. $PM(f^*, g) = S_{\vec{\alpha}_M,b_M}S_{\vec{\alpha}_{M-1},b_{M-1}}\cdots S_{\vec{\alpha}_1,b_1}$;
2. $PM(f^*, g^*) = S_{\vec{\alpha}_1,-b_1}S_{\vec{\alpha}_2,-b_2}\cdots S_{\vec{\alpha}_M,-b_M}$;
3. $PM(f, g^*) = S_{\vec{\alpha}_M,-b_M}S_{\vec{\alpha}_{M-1},-b_{M-1}}\cdots S_{\vec{\alpha}_1,-b_1}$;
4. $PM(f(x^t), g(x^t)) = S_{t\overrightarrow{\alpha_1},tb_1}S_{t\overrightarrow{\alpha_2},tb_2}\cdots S_{t\overrightarrow{\alpha_M},tb_M}$;

and all are superproducts.

*Proof.* By using Lemma 7.1.1 and the fact that $t \neq 0$, one sees that these products are all superproducts.

1. Follows from Theorem 6.1.4.
2. Mapping $x \mapsto x^{-1}$ in $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$ yields $S_{-\vec{\alpha}_1,-b_1}S_{-\vec{\alpha}_2,-b_2}\cdots S_{-\vec{\alpha}_M,-b_M}$. Recall from Definition 6.1.11 that for all $a, b \in \mathbb{Z}$, one has $V_{a,b} = V_{-a,b}$. Therefore, $S_{-\vec{\alpha}_i,-b_i} = S_{\vec{\alpha}_i,-b_i}$. The result follows.
3. Follows by combining 1 and 2.
4. Follows by mapping $x \mapsto x^t$ in $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$. □

Recall that by Lemmas 6.3.5 and 6.3.11, two pairs have the same canonical factorization/superfactorization if and only if they differ by a shift. The canonical factorizations/superfactorizations of pairs obtained through other equivalence operations follows easily from the Lemma 7.1.1: one simply exchanges the superfactors for their canonical form. Explicitly, use the comment proceeding Lemma 6.3.11 to convert a canonical factorization into its superfactorization, apply Lemma 7.1.4, then use Lemma 6.3.11 again to convert the resultant superfactorization back into a canonical factorization. For example, suppose $PM(f,g) = V_{1,0}V_{2,0}V_{4,-12}$. As $V_{1,0}V_{2,0}V_{4,-12} = S_{(1,2),0}S_{(4),-12}$, by Lemma 7.1.1 one obtains $PM(f^*,g) = S_{(4),-12}S_{(1,2),0}$
$= V_{4,-12}V_{1,0}V_{2,0}$, which is the canonical factorization of $PM(f^*,g)$.

## 7.2 Symmetric classification

Lemma 7.1.4 can be used to easily classify all $BCP_1$s where one polynomial in the pair is symmetric-equivalent based on their superfactorization.

**Theorem 7.2.1.** Let $b \in \mathbb{Z}$ and $PM(f,g) = X^b S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$, where $S_{\vec{\alpha}_1,b_1}S_{\vec{\alpha}_2,b_2}\cdots S_{\vec{\alpha}_M,b_M}$ is a superproduct. Then

1. $f$ is symmetric-equivalent with $d \in \mathbb{Z}$ such that $x^d f^* = f$ if and only if $d = 2b$ and for integers $i = 1,2,\ldots,M$, one has $S_{\vec{\alpha}_i,b_i} = S_{\vec{\alpha}_{M-i+1},b_{M-i+1}}$;

2. $g$ is symmetric-equivalent with $d \in \mathbb{Z}$ such that $x^d g^* = g$ if and only if for integers $i = 1,2,\ldots,M$, one has $S_{\vec{\alpha}_i,b_i} = S_{\vec{\alpha}_{M-i+1},d-2b-b_{M-i+1}}$.

*Proof.*

1. ($\Rightarrow$) Consider

$$\begin{aligned} PM(x^d f^*, g) &= Z^d PM(f^*, g) Z^d \\ &= Z^d S_{\vec{\alpha}_M, b_M} S_{\vec{\alpha}_{M-1}, b_{M-1}} \cdots S_{\vec{\alpha}_1, b_1} X^{-b} Z^d \\ &= Z^d S_{\vec{\alpha}_M, b_M} S_{\vec{\alpha}_{M-1}, b_{M-1}} \cdots S_{\vec{\alpha}_1, b_1} Z^{d-2b} \\ &= Z^{2d-2b} Z^{-d+2b} S_{\vec{\alpha}_M, b_M} Z^{d-2b} Z^{-d+2b} S_{\vec{\alpha}_{M-1}, b_{M-1}} Z^{d-2b} \cdots Z^{-d+2b} \\ &\quad \cdot S_{\vec{\alpha}_1, b_1} Z^{d+2b} \\ &= X^{d-b} S_{\vec{\alpha}_M, b_M - d + 2b} S_{\vec{\alpha}_{M-1}, b_{M-1} - d + 2b} \cdots S_{\vec{\alpha}_1, b_1 - d + 2b}. \end{aligned}$$

As $PM(x^d f^*, g) = PM(f, g)$, one obtains

$$X^{d-b} S_{\vec{\alpha}_M, b_M - d + 2b} S_{\vec{\alpha}_{M-1}, b_{M-1} - d + 2b} \cdots S_{\vec{\alpha}_1, b_1 - d + 2b} = X^b S_{\vec{\alpha}_1, b_1} S_{\vec{\alpha}_2, b_2} \cdots S_{\vec{\alpha}_M, b_M}.$$

As both products are superproducts, one can iteratively apply Theorem 6.2.1 to obtain for integers $i = 1, 2, \ldots, M$, that $S_{\vec{\alpha}_i, b_i} = S_{\vec{\alpha}_{M-i+1}, b_{M-i+1} - d + 2b}$. This leaves $X^{d-b} = X^b$, and so $d = 2b$. Therefore, $S_{\vec{\alpha}_i, b_i} = S_{\vec{\alpha}_{M-i+1}, b_{M-i+1}}$.

($\Leftarrow$) If $PM(f, g) = X^b S_{\vec{\alpha}_1, b_1} S_{\vec{\alpha}_2, b_2} \cdots S_{\vec{\alpha}_M, b_M}$, then

$$PM(x^{-b} f, x^{-b} g) = S_{\vec{\alpha}_1, b_1} S_{\vec{\alpha}_2, b_2} \cdots S_{\vec{\alpha}_M, b_M}.$$

By Part 1 of Lemma 7.1.4, conjugating $x^{-b} f$ shows

$$\begin{aligned} PM((x^{-b} f)^*, x^{-b} g) &= PM(x^b f^*, x^{-b} g) \\ &= S_{\vec{\alpha}_M, b_M} S_{\vec{\alpha}_{M-1}, b_{m-1}} \cdots S_{\vec{\alpha}_1, b_1} \\ &= S_{\vec{\alpha}_1, b_1} S_{\vec{\alpha}_2, b_2} \cdots S_{\vec{\alpha}_M, b_M} \\ &= PM(x^{-b} f, x^{-b} g), \end{aligned}$$

hence $x^b f^* = x^{-b} f$, showing the result.

2. ($\Rightarrow$) Similar to Part 1,

$$\begin{aligned}
PM(f, x^d g^*) &= Z^d PM(f, g^*) Z^{-d} \\
&= Z^d S_{\vec{\alpha}_M, -b_M} S_{\vec{\alpha}_{M-1}, -b_{M-1}} \cdots S_{\vec{\alpha}_1, -b_1} X^b Z^{-d} \\
&= Z^d S_{\vec{\alpha}_M, -b_M} S_{\vec{\alpha}_{M-1}, -b_{M-1}} \cdots S_{\vec{\alpha}_1, -b_1} Z^{-d+2b} \\
&= Z^{2b} Z^{d-2b} S_{\vec{\alpha}_M, -b_M} Z^{-d+2b} Z^{d-2b} S_{\vec{\alpha}_{M-1}, -b_{M-1}} Z^{-d+2b} \cdots Z^{d-2b} \\
&\quad \cdot S_{\vec{\alpha}_1, -b_1} Z^{-d+2b} \\
&= X^b S_{\vec{\alpha}_M, -b_M+d-2b} S_{\vec{\alpha}_{M-1}, -b_{M-1}+d-2b} \cdots S_{\vec{\alpha}_1, -b_1+d-2b}.
\end{aligned}$$

As $PM(f, x^d g^*) = PM(f, g)$, one has

$$X^b S_{\vec{\alpha}_M, -b_M+d-2b} S_{\vec{\alpha}_{M-1}, -b_{M-1}+d-2b} \cdots S_{\vec{\alpha}_1, -b_1+d-2b} = X^b S_{\vec{\alpha}_1, b_1} S_{\vec{\alpha}_2, b_2} \cdots S_{\vec{\alpha}_M, b_M},$$

and thus by iteratively applying Theorem 6.2.1, one obtains for integers $i = 1, 2, \ldots, M$ that $S_{\vec{\alpha}_i, b_i} = S_{\vec{\alpha}_{M-i+1}, d-2b-b_{M-i+1}}$.

($\Leftarrow$) Similar to the converse of Part 1. □

**Example 7.2.1.** Consider the product $PM(f, g) = V_{1,0} V_{3,-1} V_{1,0}$. By Part 1 of Theorem 7.2.1, $f$ is not only symmetric-equivalent but symmetric since no nonzero power of $X$ appears in front of $V_{1,0} V_{3,-1} V_{1,0}$. Indeed,

$$\begin{aligned}
PM(f, g) = PM(&x^{-6} + x^{-5} + x^{-4} + x^{-3} + x^{-2} + x^{-1} + 1 + x + x^2 + x^3 \\
&+ x^4 + x^5 + x^6, x^{-6} + x^{-2} + x^4 + x^6).
\end{aligned}$$

For $PM(h, k) = PM(x^5 f, x^5 g) = X^5 V_{1,0} V_{3,-1} V_{1,0}$, Part 1 of Theorem 7.2.1 shows that $h$ is symmetric-equivalent with $x^{10} h^* = h$. □

Theorem 7.2.1 offers another proof of Lemma 5.5.2, as is now shown:

**Corollary 7.2.2.** Let $(f, g)$ be a $BCP_1$ where both $f$ and $g$ are symmetric-equivalent. Then $(f, g)$ is a siamese twin pair.

*Proof.* Let $b \in \mathbb{Z}$ and $PM(f, g) = X^b S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$, where $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is a superproduct. Without loss of generality, assume $b = b_M = 0$ (pre- and post-multiply $PM(f, g)$ by the appropriate powers of $Z$ and $X$ otherwise). Suppose $d \in \mathbb{Z}$ is such that $x^d g^* = g$. If $PM(f, g)$ has one superfactor, that is, if $PM(f, g) = X^b S_{\vec{\alpha}_1,b_1}$, the result is true. Therefore, assume $PM(f, g)$ has at least two superfactors.

Since $f$ is symmetric-equivalent, by Part 1 of Theorem 7.2.1 one obtains $\vec{\alpha}_1 = \vec{\alpha}_M$ and $b_1 = b_M = 0$. Since $g$ is symmetric-equivalent, by Part 2 of Theorem 7.2.1 one obtains $b_1 = d - 2b - b_M = d = 0$. If $(f, g)$ has exactly two superfactors, then $PM(f, g) = S_{\vec{\alpha}_1,0} S_{\vec{\alpha}_M,0} = S^2_{\vec{\alpha}_1,0} = I$, which would imply $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is not a superproduct. Therefore, assume the pair has more than two superfactors. By Part 1 of Theorem 7.2.1 one obtains $b_2 = b_{M-1}$, and by Part 2 one obtains $b_2 = -b_{M-1}$. As $b_{M-1} = -b_{M-1}$, one sees that $b_{M-1} = 0$. However, since $S_{\vec{\alpha}_1,b_1} S_{\vec{\alpha}_2,b_2} \cdots S_{\vec{\alpha}_M,b_M}$ is a superproduct, consecutive offsets are not equal and thus one has $0 = b_{M-1} \neq b_M = 0$, a contradiction. Therefore, $(f, g)$ has exactly one superfactor, that is, $(f, g)$ is a siamese twin pair. □

## 7.3 Affixes over $\mathbb{Z}_2$

Lemma 6.3.11 shows that for a Boolean complementary pair $(f, g)$, there is a unique superfactor $S_{\vec{\alpha},b}$ such that $\deg(PM(f, g) S_{\vec{\alpha},b}) < \deg(PM(f, g))$. It turns out that the degree reduction from $PM(f, g)$ to $PM(f, g) S_{\vec{\alpha},b}$ occurs in a very specific manner—one that reveals further structure of Boolean complementary pairs. Most notably, for $a, n \in \mathbb{Z}^+$ and a dint $a$ pair of degree $n$ polynomials $(f, g)$ that are not

necessarily complementary, the manner in which the degree reduction occurs results in a set of conditions that is equivalent to, for all $j \leqslant 2a$, the pair $(f, g)$ satisfying

$$AF_F(n-j) + AF_G(n-j) = 0.$$

A consequence of this is that all affixes over $\mathbb{Z}_2$ of length $2a+1$ with dint $a$ are found. This is useful in finding affixes for $TCP$s, as one can start with a known affix over $\mathbb{Z}_2$ then figure out where the "$-1$"s go within the sequences.

**Lemma 7.3.1.** Let $n, a \in \mathbb{Z}^+$, $\vec{\alpha}$ be a tuple over $\mathbb{Z}^+$, and let $(f, g)$ $= (\sum_{i=0}^{n} f_i x^i, \sum_{i=0}^{n} g_i x^i)$ have degree $n$ and dint $a$. For all $j \leqslant 2a$, the pair $(f, g)$ satisfies

$$AF_F(n-j) + AF_G(n-j) = 0$$

if and only if there exists a siamese twin pair $S_{\vec{\alpha},0}$ such that for the polynomials $h(x)$ and $k(x)$ defined by $PM(h, k) = PM(f, g)S_{\vec{\alpha},0}$, one has

1. $h_a = k_{n-a} \neq k_a = h_{n-a}$, and
2. $h_j = k_j = h_{n-j} = k_{n-j} = 0$ for all $j < a$.

*Proof.* ($\Rightarrow$) Suppose for all $j \leqslant 2a$, the pair $(f, g)$ $(f, g)$ satisfies

$$AF_F(n-j) + AF_G(n-j) = 0 \text{ for all } j \leqslant 2a.$$

By Lemma 6.3.11, the pair $(f, g)$ has a decomposing superfactor $S_{\vec{\alpha},0}$. Define the polynomial $s(x) = \sum_{i=1}^{a} s_i(x^i + x^{-i})$ by $PM(s+1, s) = S_{\vec{\alpha},0}$. Then

$$\begin{aligned} PM(h, k) &= PM(f, g)S_{\vec{\alpha},0} \\ &= PM(f, g)PM(s+1, s) \\ &= PM((s+1)f + sg, sf + (s+1)g). \end{aligned}$$

By inspection, for all $j \in \mathbb{Z}$ one sees that

$$h_j = f_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}), \text{ and}$$
$$k_j = g_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}).$$

For all negative $j$, one obtains $f_j = g_j = f_{n-j} = g_{n-j} = 0$. Since $(f, g)$ has dint $a$, then for all $i < a$ one sees that $f_i = g_i$ and $f_{n-i} = g_{n-i}$. Therefore, for $j < 0$, one obtains

$$h_j = f_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}) = 0.$$

One can similarly check that $k_j = h_{n-j} = k_{n-j} = 0$ as well. Therefore, the only possibly nonzero coefficients of $x$ in $h(x)$ and $k(x)$ are $h_0, h_1, \ldots, h_n$ and $k_0, k_1, \ldots, k_n$, respectively.

Next, note that for $j < a$ one has

$$\begin{aligned} h_j &= f_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}) \\ &= g_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}) \\ &= k_j. \end{aligned}$$

One can similarly show that $h_{n-j} = k_{n-j}$. Furthermore, $f_a \neq g_a$ and $f_{n-a} \neq g_{n-a}$, so

$$\begin{aligned} h_a &= f_a + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}) \\ &\neq g_a + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}) \\ &= k_a. \end{aligned}$$

Similarly, $h_{n-a} \neq k_{n-a}$.

Now the maximum degree of $(h(x), k(x))$ shall be considered. If $\deg(h(x)) = \deg(k(x))$, then Lemma 7.1.1 shows that $\deg(h(x), k(x)) < n - 2a$. If $\deg(h(x)) \neq \deg(k(x))$, then suppose $\text{maxdeg}(h(x), k(x)) = n - d$. As shown in Lemma 2.1.12, $h(x)$ and $k(x)$ having unequal degrees implies $AF_H(n-d) + AF_K(n-d) = 1$. By Part 2 of Theorem 6.1.4, one has

$$\begin{aligned}(hh^* + kk^*)(x) &= (ff^* + gg^*)(x)((s+1)(s+1)^* + ss^*)(x) \\ &= (ff^* + gg^*)(x)(1 + 2ss^*)(x) \\ &= (ff^* + gg^*)(x),\end{aligned}$$

hence the autocorrelation coefficients of $(f, g)$ and $(h, k)$ are all equal. Therefore, one obtains

$$AF_F(n-d) + AF_G(n-d) = AF_H(n-d) + AF_K(n-d) = 1,$$

hence $n - d < n - 2a$. Therefore, in either case one obtains $\text{maxdeg}(h(x), k(x)) < n - 2a$.

It will now be shown for all integers $j = 0, 1, \ldots, a-1$, that $h_j = k_j = h_{n-j} = k_{n-j} = 0$. Suppose to the contrary that $j$ is the least nonnegative integer less than $a$ such that $h_j = k_j = 1$ or $h_{n-j} = k_{n-j} = 1$. Recall that $h_j = k_j$ and $h_{n-j} = k_{n-j}$ for all $j < a$, hence these are the only cases. First suppose $h_j = k_j = 1$. Then the least power of $x$ in $h(x)$ is $j$, and since

$$\text{maxdeg}(h(x), k(x)) < n - 2a = (n - 2a + j) - j,$$

the greatest power of $x$ in $h(x)$ is less than $n-2a+j=(n-a)+(j-a)<n-a$. Similarly, the least power of $x$ in $k(x)$ is $j$ so the greatest power of $x$ in $k(x)$ is less than $n-a$. Therefore, one obtains $h_{n-a}=k_{n-a}=0$, as otherwise $\text{maxdeg}(h(x),k(x))=(n-a)-j>n-2a$. However, $h_{n-a}\neq k_{n-a}$, hence a contradiction is obtained. In the case when $h_{n-j}=k_{n-j}=1$, one obtains $h_a=k_a$, another contradiction. Therefore, for all integers $j<a$, one has $h_j=k_j=h_{n-j}=k_{n-j}=0$.

Lastly, one knows that $h_a\neq k_a$ and $h_{n-a}\neq k_{n-a}$. If $h_a=h_{n-a}=1$ and $k_a=k_{n-a}=0$ or vice-versa, then

$$AF_F(n-a)+AF_G(n-a)=AF_H(n-a)+AF_K(n-a)=h_ah_{n-a}+k_ak_{n-a}=1,$$

which is a contradiction. Therefore, $h_a=k_{n-a}\neq k_a=h_{n-a}$.

($\Leftarrow$) For all $j\leqslant 2a$, if the pair $(h,k)$ satisfies

1. $h_a=k_{n-a}\neq k_a=h_{n-a}$, and
2. $h_j=k_j=h_{n-j}=k_{n-j}=0$,

then $\text{maxdeg}(h(x),k(x))<n-2a$. Then one sees that

$$AF_H(n-j)+AF_K(n-j)=0$$

because all the terms involved are equal to 0. Therefore, for all $j\leqslant 2a$, the pair $(f,g)$ satisfies

$$AF_F(n-j)+AF_G(n-j)=AF_H(n-j)+AF_K(n-j)=0. \qquad \square$$

For $a \in \mathbb{Z}^+$, Lemma 7.3.1 completely solves the structure of all affixes of length $2a+1$ over $\mathbb{Z}_2$ with dint $a$. To see this, let $n \in \mathbb{Z}^+$ be arbitrary and let

$$\widetilde{F} = (f_0, f_1, \ldots, f_{2a}, \#, f_{n-2a}, f_{n-2a+1}, \ldots, f_n),$$
$$\widetilde{G} = (g_0, g_1, \ldots, g_{2a}, \#, g_{n-2a}, g_{n-2a+1}, \ldots, g_n)$$

be a pair of sequences with dint $a$ and $f_0 = g_0 = f_n = g_n = 1$. Define the polynomials $f(x)$ and $g(x)$ by

$$f(x) = \sum_{i=0}^{2a} f_i x^i + \sum_{i=n-2a}^{n} f_i x^i \text{ and}$$
$$g(x) = \sum_{i=0}^{2a} g_i x^i + \sum_{i=n-2a}^{n} g_i x^i.$$

Suppose $(\widetilde{F}, \widetilde{G})$ is an affix of length $2a+1$ with dint $a$, then Theorem 6.2.1 shows that there exists a siamese twin pair $S_{\vec{\alpha},0}$ such that

$$\text{maxdeg}(PM(f,g)S_{\vec{\alpha},0}) < \deg(PM(f,g)).$$

Let $h(x)$ and $k(x)$ be polynomials defined by $PM(h,k) = PM(f,g)S_{\vec{\alpha},0}$. Then Lemma 7.3.1 shows that for all $j \leqslant 2a$, the pair $(h,k)$ satisfies

1. $h_a = k_{n-a} \neq k_a = h_{n-a}$, and
2. $h_j = k_j = h_{n-j} = k_{n-j} = 0$.

Now suppose $(\widetilde{F}, \widetilde{G})$ is such that $(h,k)$ satisfies Conditions 1 and 2. Let $(F,G)$ denote the sequence version of $(f,g)$. Lemma 7.3.1 shows that $(F,G)$ satisfies

$$AF_F(n-j) + AF_G(n-j) = 0 \text{ for all } j \leqslant 2a.$$

By inspection, for all $j \leqslant 2a$ one obtains

$$AF_{\widetilde{F}}(2(2a+1)+1-j) + AF_{\widetilde{G}}(2(2a+1)+1-j) = AF_F(n-j) + AF_G(n-j) = 0,$$

hence $(\widetilde{F}, \widetilde{G})$ is an affix of length $2a+1$ with dint $a$. Thus $(\widetilde{F}, \widetilde{G})$ is an affix of dint $a$ and length $2a+1$ if and only if the pair $(h, k)$ satisfies Conditions 1 and 2.

Moreover, note that

$$h_j = f_j + \sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i}).$$

Thus, if one is starting with an arbitrary pair $(f, g)$, the value of $h_j$ can be controlled by choosing $f_j$. For example, if for all integers $j < a$ one wishes to have $h_j = 0$, then set $f_j$ to $\sum_{i=1}^{a} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{a} s_i(f_{j-i} + g_{j-i})$. Similarly, the values of $k_j, h_{n-j}$, and $k_{n-j}$ can be controlled by choosing $g_j, f_{n-j}$, and $g_{n-j}$, respectively. Thus one can create an affix of length $2a+1$ with dint $a$ by setting $f_j, g_j, f_{n-j}$, and $g_{n-j}$ to the appropriate values. This is illustrated in the following example.

**Example 7.3.1.** Suppose one wishes to find all affixes of length 5 with dint 2. Begin with

$$\widetilde{F} = (f_0, f_1, \ldots, f_4, \#, f_{n-4}, f_{n-3}, \ldots, f_n),$$
$$\widetilde{G} = (g_0, g_1, \ldots, g_4, \#, g_{n-4}, g_{n-3}, \ldots, g_n),$$

and set $f_0 = g_0 = f_n = g_n = 1$ so that the resulting affix has length 5, then set $f_1 = g_1$, $f_{n-1} = g_{n-1}$, $g_2 = 1 + f_2$ and $g_{n-2} = 1 + f_{n-2}$ so that $(\widetilde{F}, \widetilde{G})$ has dint 2. Define the polynomials $f(x)$ and $g(x)$ by

$$(f(x), g(x)) = \left( \sum_{i=0}^{4} f_i x^i + \sum_{i=n-4}^{n} f_i x^i, \sum_{i=0}^{4} g_i x^i + \sum_{i=n-4}^{n} g_i x^i \right).$$

One wishes to choose the remaining values of $f_j$ and $g_j$ so that there exists a siamese twin pair $S_{\vec{\alpha},0}$ such that for the polynomials $(h(x), k(x))$ defined by

$$PM(h(x), k(x)) = PM(f(x), g(x))S_{\vec{\alpha},0},$$

one has for all $j < 2$, that

1. $h_2 = k_{n-2} \neq k_2 = h_{n-2}$, and
2. $h_j = k_j = h_{n-j} = k_{n-j} = 0$.

As $(f, g)$ has dint 2, the decomposing siamese twin pair $S_{\vec{\alpha},0}$ must also have dint 2 by Theorem 6.2.1. The two superfactors that can decompose a dint 2 pair with offset 0 are $S_{(2),0}$ and $S_{(2,1),0}$. Therefore, by setting $s_2 = 1$ and letting $s_1$ be arbitrary, the decomposing superfactor is of the form

$$S_{\vec{\alpha},0} = PM(\sum_{i=1}^{2} s_i(x^i + x^{-i}) + 1, \sum_{i=1}^{2} s_i(x^i + x^{-i})).$$

Define $PM(h(x), k(x)) = PM(f(x), g(x))S_{\vec{\alpha},0}$. Then for $j \in \mathbb{Z}$, one obtains

$$h_j = f_j + \sum_{i=1}^{2} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{2} s_i(f_{j-i} + g_{j-i}), \text{ and}$$
$$k_j = g_j + \sum_{i=1}^{2} s_i(f_{j+i} + g_{j+i}) + \sum_{i=1}^{2} s_i(f_{j-i} + g_{j-i}).$$

Since

$$\begin{aligned}
h_2 + k_{n-2} &= f_2 + \sum_{i=1}^{2} s_i(f_{2+i} + g_{2+i}) + \sum_{i=1}^{2} s_i(f_{2-i} + g_{2-i}) \\
&\quad + g_{n-2} + \sum_{i=1}^{2} s_i(f_{n-2+i} + g_{n-2+i}) + \sum_{i=1}^{2} s_i(f_{n-2-i} + g_{n-2-i}) \\
&= f_2 + s_1(f_3 + g_3) + (f_4 + g_4) + s_1(f_1 + g_1) + (f_0 + g_0) \\
&\quad + g_{n-2} + s_1(f_{n-1} + g_{n-1}) + (f_n + g_n) + s_1(f_{n-3} + g_{n-3}) + (f_{n-4} + g_{n-4}) \\
&= f_2 + g_{n-2} + s_1(f_3 + g_3 + f_{n-3} + g_{n-3}) + (f_4 + g_4 + f_{n-4} + g_{n-4}),
\end{aligned}$$

the equality $h_2 = k_{n-2}$ is obtained by setting $f_2$ equal to

$$g_{n-2} + s_1(f_3 + g_3 + f_{n-3} + g_{n-3}) + (f_4 + g_4 + f_{n-4} + g_{n-4}).$$

Since $g_2 = 1 + f_2$ and $g_{n-2} = 1 + f_{n-2}$, one sees that $h_2 = k_{n-2} \neq k_2 = h_{n-2}$. For $j \leqslant 0$, one can use the facts that $f_1 = g_1$ and $f_{n-1} = g_{n-1}$ to verify directly that $h_j = k_j = h_{n-j} = k_{n-j} = 0$. Since $f_1 = g_1$ and $f_{n-1} = g_{n-1}$, one can also verify that $h_1 = k_1$ and $h_{n-1} = k_{n-1}$. Now,

$$\begin{aligned}
h_1 &= f_1 + \sum_{i=1}^{2} s_i(f_{1+i} + g_{1+i}) + \sum_{i=1}^{2} s_i(f_{1-i} + g_{1-i}) \\
&= f_1 + s_1(f_2 + g_2) + s_2(f_3 + g_3) \\
&= f_1 + s_1 + f_3 + g_3 \\
&= 0,
\end{aligned}$$

hence by setting $f_1$ (and thus $g_1$) to $s_1 + f_3 + g_3$, one obtains $h_1 = k_1 = 0$. Similarly, examining $h_{n-1}$ will show that setting $f_{n-1}$ (and thus $g_{n-1}$) to $s_1 + f_{n-3} + g_{n-3}$ results in $h_{n-1} = k_{n-1} = 0$. In summary, the obtained equations are

1. $f_0 = g_0 = f_n = g_n = 1$,

2. $f_1 = g_1$ and $f_{n-1} = g_{n-1}$,

3. $g_2 = 1 + f_2$ and $g_{n-2} = 1 + f_{n-2}$,

4. $f_1 = s_1 + f_3 + g_3$,

5. $f_{n-1} = s_1 + f_{n-3} + g_{n-3}$, and

6. $f_2 = g_{n-2} + s_1(f_3 + g_3 + f_{n-3} + g_{n-3}) + (f_4 + g_4 + f_{n-4} + g_{n-4})$.

Though note that Conditions 1, 2, and 3 are simply to make the pair $(\widetilde{F}, \widetilde{G})$ have length 5 and dint 2, they had nothing to do with complementarity. Lemma 7.3.1 shows that once Conditions 1,2, and 3 have been established, satisfying Conditions 3,4, and 5 is equivalent to satisfying for all $j \leqslant 4$, the conditions

$$AF_{\widetilde{F}}(11 - j) + AF_{\widetilde{G}}(11 - j) = 0,$$

hence every affix of length 5 with dint 2 is of the form $(\widetilde{F}, \widetilde{G})$. In particular, note that the terms $f_3, f_4, g_3, g_4, f_{n-4}, f_{n-3}, g_{n-4}, g_{n-3}$, and $f_{n-2}$ can take any value.

As a demonstration, by using Conditions 1 to 6, one sees that

$$\begin{aligned}
AF_{\widetilde{F}}(7) + AF_{\widetilde{G}}(7) &= f_0f_{n-4} + f_1f_{n-3} + f_2f_{n-2} + f_3f_{n-1} + f_4f_n \\
&\quad + g_0g_{n-4} + g_1g_{n-3} + g_2g_{n-2} + g_3g_{n-1} + g_4g_n \\
&= f_{n-4} + (s_1 + f_3 + g_3)\, f_{n-3} + f_2f_{n-2} \\
&\quad + f_3\,(s_1 + f_{n-3} + g_{n-3}) + f_4 \\
&\quad + g_{n-4} + (s_1 + f_3 + g_3)\, g_{n-3} + g_2g_{n-2} \\
&\quad + g_3\,(s_1 + f_{n-3} + g_{n-3}) + g_4 \\
&= (f_4 + g_4 + f_{n-4} + g_{n-4}) + (f_2f_{n-2} + g_2g_{n-2}) \\
&\quad + (f_{n-3} + g_{n-3})\,(s_1 + f_3 + g_3) + (f_3 + g_3)\,(s_1 + f_{n-3} + g_{n-3}) \\
&= (f_4 + g_4 + f_{n-4} + g_{n-4}) + (f_2(1 + g_{n-2}) + (1 + f_2)g_{n-2}) \\
&\quad + s_1(f_3 + g_3 + f_{n-3} + g_{n-3}) + 2(f_3 + g_3)\,(f_{n-3} + g_{n-3}) \\
&= (f_4 + g_4 + f_{n-4} + g_{n-4} + s_1(f_3 + g_3 + f_{n-3} + g_{n-3})) \\
&\quad + (f_2 + g_{n-2}) \\
&= (f_2 + g_{n-2}) + (f_2 + g_{n-2}) \\
&= 0.
\end{aligned}$$

One can similarly check that for $j \leqslant 3$, one obtains $AF_{\widetilde{F}}(11-j)+AF_{\widetilde{G}}(11-j) = 0$. $\square$

Observe that to find all $TCP$ affixes of a specified length, one can begin with the set of all affixes over $\mathbb{Z}_2$ of that length then figure out if "$-1$"s can be placed within the sequences to form an affix over $\{0, \pm 1\}$.

## 7.4 Tables of canonical factorizations

The following are tables of canonical factorizations of $BCP_1$s listed according to degree. These $BCP_1$s come from the $TCP$s in Craigen and Koukouvinos' paper

[7], which were turned into $BCP$s through the homomorphism in Lemma 5.1.2 then factored using basic Maple code. The "sequences" column shows the $TCP$ corresponding to the $BCP$, the "$w$" column shows the pair's weight, and the "$\delta$" and "$\hat{\delta}$" columns refer to the pair's deficiency and the conjectured lower bound on their deficiency given by the later Conjecture 8.0.1, respectively. Pairs that correspond to an imprimitive $TCP$ are indicated with a "†", the rest are primitive. The superfactors are separated by bars "|". For a discussion on primitive pairs, see Section 4.3.

There are a few observed patterns in these factorizations. Note the abundance of dint 1 canonical factors, how close neighbouring offsets are, and how frequently the number of places the two sequences in a pair differ from each other is twice the number of superfactors in their superfactorization plus or minus 1.

**Degree 8**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,-2}\|V_{2,0}$ | -00111-11<br>-01-100-- | 13 | 5 | 4 |

**Degree 10**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,0}\|V_{1,2}\|V_{1,0}$ | -1-011-0111<br>-0-0001000- | 13 | 9 | 6 |

**Degree 12**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{3,4}\|V_{1,0}$ | 1-110-0110-0-<br>10111000-01-1 | 17 | 9 | 7 |

**Degree 13**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{2,-1}V_{3,-1}\|V_{1,1}\|V_{1,0}$ | `11001001-0-001`<br>`1000-0000-10--` | 13 | 15 | 7 |
| $V_{1,1}V_{3,1}\|V_{1,0}V_{3,0}$ | `1-0-00--00-01-`<br>`1-00110---00-1` | 17 | 11 | 6 |
| $V_{1,-1}\|V_{1,-2}\|V_{1,-3}\|V_{1,0}$ | `1000-11100-00-`<br>`110110-010-1-1` | 17 | 11 | 8 |
| $V_{1,-3}\|V_{1,-4}\|V_{1,-1}\|V_{1,0}$ | `1001-011--1001`<br>`11010-000101-1` | 17 | 11 | 8 |

**Degree 14**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,-2}V_{2,-2}\|V_{1,-1}\|V_{3,0}$ | `101-00010-01001`<br>`10100--00-0000-` | 13 | 17 | 7 |
| $V_{1,2}\|V_{1,0}V_{3,0}V_{5,0}$ | `101-0000010-111`<br>`101-01001001---` | 17 | 13 | 7 |
| $V_{1,-4}V_{2,-4}\|V_{1,-2}\|V_{2,0}$ | `10000111-00-00-`<br>`10100-1-0111-01` | 17 | 13 | 8 |

**Degree 16**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,0}V_{3,0}\|V_{1,-1}\|V_{1,0}V_{3,0}$ | `100-0-011-0101001`<br>`100000-0-0000000-` | 13 | 21 | 8 |

**Degree 17**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,3}\|V_{2,2}\|V_{1,3}\|V_{1,2}\|V_{1,0}$ | 1000-1111101---10-<br>11-010010-0011-1-1 | 25 | 11 | 10 |
| $V_{1,-1}\|V_{1,0}V_{2,0}V_{3,0}V_{4,0}V_{5,0}V_{6,0}V_{7,0}$ | 1001--1010--111011<br>1001-1-100011--0-- | 25 | 11 | 8 |
| $V_{1,-1}V_{2,-1}\|V_{1,0}V_{2,0}V_{5,0}V_{6,0}$ | 11-1-0010--0001011<br>11-1-0--11--00-0-- | 25 | 11 | 8 |

**Degree 18**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{2,-6}\|V_{2,-3}\|V_{2,0}$ | 10-0101000-00000101<br>1000001-000--00000- | 13 | 25 | 11 |
| $V_{1,-2}\|V_{4,-1}V_{6,-1}\|V_{1,0}$ | 1000-00000101010-01<br>110000100000-00001- | 13 | 25 | 9 |
| $V_{1,-2}\|V_{2,0}\|V_{2,1}V_{3,1}\|V_{1,0}$ | 10-1--000110--00-0-<br>1-01-0-1-00110-1111 | 25 | 13 | 10 |
| $V_{1,0}V_{2,0}\|V_{2,2}\|V_{1,1}\|V_{1,0}V_{2,0}$ | -11-0001-0-1010----<br>-1010-000-011-11011 | 25 | 13 | 10 |
| $V_{1,-10}\|{V_{3,0}}^{\dagger}$ | 10100010101--1---11<br>101-0--0-01--0001-- | 25 | 13 | 13 |

**Degree 19**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{2,9}\|{V_{3,0}}^{\dagger}$ | 10-1----111001010001<br>10-0-010-1-0-10--00- | 25 | 15 | 13 |
| $V_{2,3}\|{V_{6,0}}^{\dagger}$ | 1011-01110-0-0-11001<br>1011-0010-001-1--00- | 25 | 15 | 10 |

**Degree 20**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{2,2}V_{4,2}\|V_{1,1}\|V_{1,0}V_{2,0}V_{3,0}V_{4,0}$ | 10111-00000-11-0-1101<br>101100-001-10-010--0- | 25 | 17 | 10 |
| $V_{1,-2}\|V_{1,0}V_{2,0}V_{3,0}\|V_{2,1}V_{3,1}\|V_{1,0}$ | 1--1001-0-0-100-00---<br>10-01001100--0-1--001 | 25 | 17 | 11 |
| $V_{1,-2}\|V_{1,0}V_{3,0}\|V_{2,-1}V_{3,-1}\|V_{1,0}$ | 1-0010-00-0--01-10---<br>10-00100---000-11-101 | 25 | 17 | 11 |
| $V_{1,4}\|V_{1,1}\|V_{1,2}\|V_{1,3}V_{2,3}\|V_{1,0}$ | 1-1-0011--10-0000----<br>1011-000-00-10110-001 | 25 | 17 | 13 |
| $V_{1,-6}\|V_{1,-5}\|V_{1,-2}\|V_{2,-1}\|V_{1,0}V_{2,0}$ | 100101011-1-00001--11<br>10-01100-0010101--0-- | 25 | 17 | 12 |
| $V_{2,-2}\|V_{1,0}V_{2,0}V_{3,0}V_{6,0}V_{7,0}$ | 111--1-000-1000000011<br>111--1--0-1-0-00000-- | 25 | 17 | 10 |
| $V_{1,-2}\|V_{1,-3}\|V_{2,-1}\|V_{1,0}V_{2,0}V_{3,0}V_{4,0}$ | 10-1--10-0-1-0-0--011<br>10--00000101--000-0-- | 25 | 17 | 11 |

**Degree 21**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{2,-1}\|V_{1,3}\|V_{1,2}\|V_{3,0}$ | 10010000-010--01000-0-<br>10000000001-000-101101 | 17 | 25 | 13 |
| $V_{1,-5}\|V_{1,-6}\|V_{1,0}\|V_{1,-2}\|V_{1,0}$ | 1110101-011--0001-00-1<br>10001-1100-0-01001100- | 25 | 17 | 15 |

**Degree 22**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,2}\|V_{1,-2}V_{3,-2}\|V_{3,0}V_{4,0}$ | `1001-0001-001-001-01111`<br>`10010-10000001-0011----` | 25 | 21 | 13 |
| $V_{1,-8}\|V_{1,-6}V_{2,-6}\|V_{1,-3}\|V_{2,0}V_{3,0}$ | `1001000-0-0000-1-110-11`<br>`10001-0---111--0-0--1--` | 29 | 17 | 14 |

**Degree 24**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,-4}\|V_{1,-7}\|V_{1,-6}\|V_{1,-5}\|V_{1,0}V_{3,0}$ | `11100-11101000--1-0001-01`<br>`11--11000--00-1-100000-0-` | 29 | 21 | 16 |

**Degree 27**

| Factorization | Sequences | $w$ | $\delta$ | $\hat{\delta}$ |
|---|---|---|---|---|
| $V_{1,-7}\|V_{1,-6}\|V_{1,-4}\|V_{1,0}V_{2,0}V_{4,0}V_{6,0}V_{7,0}$ | `10010001-1-1001--100--011011`<br>`10010000000-011-0-00010--0--` | 29 | 27 | 16 |

# 8

# Conclusion

This author has gone much further in the investigation of pair matrix factorizations of Boolean complementary pairs than what is presented in this thesis. However, there are still plenty of extensions of this research that one can pursue without knowing these omitted results. This chapter presents some of these extensions.

A valuable pursuit would be to prove or disprove the following conjecture:

**Conjecture 8.0.1.** Suppose $(f, g)$ is a $BCP_1$ with superfactorization

$$S_{\vec{\alpha_1},b_1} S_{\vec{\alpha_2},b_2} \cdots S_{\vec{\alpha_M},b_M}.$$

Suppose $(f, g)$ is not a siamese twin pair (thus $M > 1$) and $S_{\vec{\alpha_i},b_i}$ has dint $c_i$. Then the deficiency of $(f, g)$ is bounded below by

$$\hat{\delta} = \sum_{i=1}^{M} c_i + \sum_{i=1}^{M-1} |b_{i+1} - b_i| - 1. \tag{8.0.1}$$

Section 7.4 lists $BCP_1$s with their deficiency and the lower bound $\hat{\delta}$ given by Conjecture 8.0.1. Most $BCP$s in Section 7.4 exceed the bound in equation (8.0.1), but equality is met once with the nonprimitive pair corresponding to $V_{1,-10}V_{3,0}$. The heuristic behind Conjecture 8.0.1 is that every dint signifies at least one zero in the polynomial pair, and observing the decomposition of a pair shows that changes in consecutive offsets also force

zeros within the polynomials.

If Conjecture 8.0.1 is true, then small-deficiency pairs necessarily have few superfactors and thus have a "simple" structure. Therefore, $BCP_1$s corresponding to ternary complementary pairs with small-deficiency (and thus are "almost" Golay pairs) under the homomorphism in Lemma 5.1.2 have a simple modulo 2 structure as well. Intuitively this makes sense as Golay pairs themselves are identical twin pairs under the homomorphism of Lemma 5.1.2, which have a trivial modulo 2 structure.

Craigen [4] showed that a pair matrix factorization exists for complementary pairs over $\mathbb{Z}_3$. A simple extension of his work shows that for a prime $p \equiv 3 \pmod 4$, a pair matrix factorization exists for complementary pairs over $\mathbb{Z}_p$: let $n \in \mathbb{Z}^+$, $(f, g)$ be a degree $n$ normalized complementary pair over $\mathbb{Z}_p$, and define $Y_{a,b} := PM(a, x^b)$. It is straightforward to show that $PM(f, g)Y_{a,b}$ is a complementary pair for all $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}$, and $\deg(PM(f, g)Y_{a,b}) < \deg(PM(f, g))$ if and only if $a \in \{f_0^{-1}g_0, f_n^{-1}g_n\}$ and $b$ is the offset of $PM(f, g)$ (hence there is not necessarily uniqueness in these factorizations). Similar to Lemma 5.1.2, the homomorphism $\phi_p : \mathbb{Z}[x, x^{-1}] \to \mathbb{Z}_p[x, x^{-1}]$ that maps coefficients to their modulo $p$ equivalent maps $TCP$s to complementary pairs over $\mathbb{Z}_p$. One can take $TCP$s and different primes $p \equiv 3 \pmod 4$, map the $TCP$s into $\mathbb{Z}_p$ through $\phi_p$, then compare the pair matrix factorizations obtained. Perhaps some patterns will emerge within these factorizations that will yield insight into the general structure of $TCP$s. One could also take results in this thesis and look for comparables among complementary pairs over $\mathbb{Z}_p$. Note that the matrices $Y_{a,b}$ work in decomposing every pair over $\mathbb{Z}_p$ when $p \equiv 1 \pmod 4$, but one can not necessarily write every complementary pair as a product of the $Y_{a,b}$s. This is because if $a^2 = -1$, then $Y_{a,b}$ does not have an inverse, so while one can always get something like $PM(f, g)Y_{a_m,b_m} \cdots Y_{a_1,b_1} = PM(c, 0)$, one can not necessarily express $PM(f, g)$ as the product $PM(c, 0)Y_{a_1,b_1} \cdots Y_{a_m,b_m}$. For example, $(f, g) = (1 + x + 4x^2, 2 + x + 3x^2)$ satisfies $(ff^* + gg^*)(x) = 2 \in \mathbb{Z}_5[x, x^{-1}]$ and can not be expressed as a climbing product $PM(c, 0)Y_{a_1,b_1} \cdots Y_{a_m,b_m}$.

One can generalize complementary pairs and investigate potential matrix factorizations of these generalized pairs. One way to generalize complementary pairs is to introduce an involution $*$ on the coefficient set and update the autocorrelation function: let $R$ be an integral domain, $S \subseteq R$, $n \in \mathbb{Z}^+$, and $A = (a_i)_{i=1}^n$ be a sequence over $S$. One could redefine the autocorrelation function of $A$ to be $AF_A : \mathbb{N} \to R$, where

$$AF_A(k) := \sum_{i=0}^{n-1-k} a_i a_{i+k}^* \text{ for } k < n$$

and is zero otherwise. One could then say a pair of sequences $(F, G)$ is complementary over $S$ with respect to $*$ if and only if for all positive integers $k$, the pair satisfies $AF_F(k) + AF_G(k) = 0$. An example of this is with **complex Golay pairs**, which are pairs of $(\pm 1, \pm i)$-sequences with complex conjugation as the involution $*$. These pairs can be used in the construction of Hadamard matrices [6].

One could also generalize the number of sequences in a complementary pair. This is done with Turyn sequences, which for a positive integer $n$ are 4 $(\pm 1)$-sequences of lengths $n+1, n+1, n$, and $n$ with zero autocorrelation and extra symmetry conditions. Turyn sequences can be used to construct orthogonal designs and Hadamard matrices [26] in a very similar fashion to how orthogonal matrices were constructed from complementary pairs in Section 2.6.

There is still much to understand when it comes to the structure of Golay, ternary, and Boolean complementary pairs. Although there is an algebraic characterization of Boolean complementary pairs in both the even- and odd-weight cases, it is still difficult to use this information to understand where the zeros go within the two sequences. The enigma of complementary pairs is enriched by the numerous applications of complementary pairs to engineering; that something so useful should remain so mysterious is truly enticing. It is this author's hope that this thesis, along with Craigen and Woodford's work, will provide not only a useful perspective to investigate complementary pairs but one that will contribute significantly to the understanding of $GP$s and $TCP$s.

# Index

# References


[1] P. B. Borwein and R. A. Ferguson, A complete description of Golay pairs for lengths up to 100, *Math. Comp.* **73** (2004), 967-985.

[2] R. Craigen, Boolean complementary pairs, *J. Combin. Theory Ser. A* **104** (2003), 1-16.

[3] R. Craigen, Products and factorizations of ternary complementary pairs, *Australas. J. Combin.* **34** (2006), 269-280.

[4] R. Craigen, Complementary pairs modulo 3, Unpublished manuscript, 2019.

[5] R. Craigen, S. Georgiou, W. Gibson, and C. Koukouvinos, Further explorations into ternary complementary pairs, *J. Combin. Theory Ser. A* **113** (2006), 952-965.

[6] R. Craigen, W. Holzmann, and H. Kharaghani, Complex Golay sequences: structure and application, *Discrete Math.* **252** (2002), 73-89.

[7] R. Craigen and C. Koukouvinos, A theory of ternary complementary pairs, *J. Combin. Theory Ser. A* **96** (2001), 358-375.

[8] R. Craigen and R. Woodford, Odd-weight Boolean complementary pairs, Unpublished manuscript, 2002.

[9] M. Eliahou, S. Kervaire, and B. Saffari, A new restriction on the lengths of Golay complementary sequences, *J. Combin. Theory Ser. A* **55** (1990), 49-59.

[10] M. Eliahou, S. Kervaire, and B. Saffari, On Golay polynomial pairs, *Adv. Appl. Math.* **12** (1991), 235-292.

[11] A. Gavish and A. Lempel, On ternary complementary pairs, *IEEE Trans. Inform. Theory* **40** (1994), 522-526.

[12] A. Geramita and J. Seberry, *Orthogonal Designs: Quadratic Forms and Hadamard Matrices*, Marcel Dekker Inc, New York and Basel **45** (1979).

[13] J. M. Goethals and J. J. Seidel, A skew-Hadamard matrix of order 36, *Austral. Math. Soc. A* **11** (1970), 343-344.

[14] M. Golay, Multislit spectrometry, *J. Opt. Soc. Amer.* **39** (1949), 437-444.

[15] M. Golay, Static multislit spectrometry and its application to the panormaic display of infrared spectra, *J. Opt. Soc. Amer.* **41** (1951), 468-472.

[16] M. Golay, Complementary series, *I.R.E. Trans. Inf. Theory* **7** (1961), 82-87.

[17] M. Golay, Note on complementary series, *Proc. I.R.E.* **50** (1962), 84.

[18] M. Gysin and J. Seberry, Multiplications of ternary complementary pairs, *Australas. J. Combin.* **14** (1996), 165-180.

[19] M. Gysin and J. Seberry, On ternary complementary pairs, *Australas. J. Combin.* **23** (2001), 153-170.

[20] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. des Sci. Math.* **17** (1893), 240-246.

[21] D. J. Katz and E. Moore, Sequence pairs with lowest combined autocorrelation and crosscorrelation, *IEEE Trans, Inform. Theory* **17** (2022), 1-17.

[22] C. Koukouvinos and J. Seberry, Weighing matrices and their applications, *J. Stat. Plan. Inference* **62** (1997), 91-101.

[23] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers, Wiley,* New York **2** (1960).

[24] I. Pellejero, M. Zivanovic, I. Arroabarren, and A. Carlosena, Application of multitone signals in room acoustics measurements, IEEE Instrumentation and Measurement Technology Conference, Budapest, Hungary 2001, 566-571.

[25] B. M. Popović, Synthesis of power efficient multitone signals with flat amplitude spectrum, *IEEE Trans. Commun.* **39** (1991), 1031-1033.

[26] J. Seberry, *Orthogonal Designs*, Springer, Cham **1** (2017).

[27] R. J. Turyn, Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory* **16** (1974), 313-333.

[28] J. Williamson, Hadamard's determinant theorem and the sum of four squares, *Duke Math. J.* **11** (1944), 65-81.