Boolean and ternary complementary pairs

R. Craigen

Department of Mathematics, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

Received 19 July 2002

Abstract

A ternary complementary pair, TCP\((n, w)\), is a pair of \((0, \pm 1)\)-sequences of length \(n\) with zero autocorrelation and weight \(w\). These are of theoretical interest in combinatorics as well as of practical consequence in coding, transmitting and processing various kinds of signals. When one attempts to construct a TCP of given length and weight, the first thing to decide is where to place the zeros, if any. Thus arise Boolean complementary pairs, BP\((n, w)\)—pairs of \((0, 1)\)-sequences of length \(n\) with zero autocorrelation over \(\mathbb{Z}_2\) and a total of \(w\) 1’s. The unique pair of \((0, 1)\)-sequences having the same support as a TCP\((n, w)\) is a BP\((n, w)\) (but the converse is not necessarily true); thus, Boolean complementary pairs establish candidate zero patterns for ternary complementary pairs. This cleanly separates the construction of ternary complementary pairs into two stages: deciding where to put the zeros, and determining the sign of the nonzero entries. We obtain some necessary conditions for the existence of Boolean complementary pairs. We conduct an exhaustive survey of pairs of small lengths and construct some infinite classes clearly of fundamental importance in the theory. We completely characterize all pairs of even weight and give a product construction for pairs of odd weight that gives a greater variety of new pairs than similar product methods used in the ternary case.

1. Introduction

A pair of sequences, \(A = (a_1, \ldots, a_n)\); \(B = (b_1, \ldots, b_n)\), with entries in a ring \(R\), has zero autocorrelation if

\[
(aa^* + bb^*) = \lambda \in R,
\]

where \(a(x) = \sum a_ix^{i-1}\) and \(b(x) = \sum b_ix^{i-1}\) are (formal) Laurent polynomials (in \(R(x)\)), called the Hall polynomials of the sequences, and the involution

\[E-mail address: craigenr@cc.umanitoba.ca.\]
\[ : R(x) \rightarrow R(x) \text{ is defined by } f^*(x) := f(x^{-1}). \] A; B is a ternary complementary pair, TCP(n, w), if (1) holds with \( R = \mathbb{Z}, w = \lambda \), and A and B are ternary, or \((0, \pm 1)\)-sequences of length n. Observe that the weight, w, is the number of nonzero elements in the two sequences.

Another convenient number is the deficiency of the pair, \( \delta = \delta(A, B) = 2n - w \), the total number of zeros.

For example, with \( A = (1, 0, 1); B = (1, 1, -1) \), we have \( a(x); b(x) = 1 + x^2; 1 + x - x^2, \) and \( (aa^* + bb^*)(x) = (1 + x^2)(1 + x^{-2}) + (1 + x - x^2)(1 + x^{-1} - x^{-2}) = (2 + x^2 + x^{-2}) + (3 - x^2 - x^{-2}) = 5, \) and so \( A; B = TCP(3, 5) \), which has deficiency \( \delta = 1 \).

Sequences with zero autocorrelation are of interest because they can be used to construct orthogonal matrices, and because of applications in signal processing and spectroscopy. Ternary complementary pairs have received some attention lately [2,4–6].

We shall consider in this article the case \( R = \mathbb{Z}_2 \); thus, all sequences will be Boolean, or \((0, 1)\)-sequences, and all arithmetic will be reduced mod 2.

For convenience we shall use \( a(x) = \sum a_i x^{-i}, b(x) = \sum b_i x^{-i}, c(x) = c_i x^{-i}, \) ... for the Hall polynomials of sequences \( A = (a_1, ...), B = (b_1, ...), C = (c_1, ...), \) ... as above, throughout this paper. For a ternary sequence A, write \(|A|\) for the \((0, 1)\)-sequence with the same zero pattern.

A Boolean complementary pair is a pair of Boolean sequences, \( A; B \), satisfying (1) (over \( \mathbb{Z}_2(x) \)). We will use \( w \) for the weight, or total number of nonzero entries, in the pair; thus, \( \lambda = (0 \text{ or } 1) \equiv w \mod 2; \) thus, \( \lambda \neq w \) if \( w > 1 \). We shall denote a Boolean complementary pair of length \( n \) and weight \( w \) by \( BP(n, w) \).

**Lemma 1.** If \( A; B \) is a TCP(n, w), then \(|A|; |B| \) is a \( BP(n, w) \).

**Proof.** Apply the natural map \( \pi : \mathbb{Z} \rightarrow \mathbb{Z}_2 \) to (1). \( \square \)

From the example above, we obtain \(|A|; |B| = (101); (111) \) (commas are unnecessary), with Hall polynomials \(|a||b|(x) = 1 + x^2; 1 + x + x^2, \) and \((|a||a^* + |b||b^*|(x) = (1 + x^2)(1 + x^{-2}) + (1 + x + x^2)(1 + x^{-1} + x^{-2}) = 5 + 2x + 2x^{-1} + 2x^2 + 2x^{-2} = 5 \) (remember that all arithmetic is mod 2; here \( w = 5, \lambda = 1 \), so \(|A|; |B| = BP(3, 5) \), as predicted by Lemma 1.

Lemma 1 states that every ternary complementary pair has the same support—set of nonzero positions—as a Boolean complementary pair. (The converse is evidently false, for \((111); (111) \) is a \( BP(3, 5) \), but there is no \( TCP(3, 6) \).) Boolean complementary pairs thus arise naturally in the construction of TCPs—which divides naturally into two parts: first, decide where to place the zeros; then, determine the sign of all nonzero entries.

One might ask, “Why not first decide how many positive and negative entries there should be, and then try them in all possible positions instead?” By comparing the search space for this method to that of the two-part program suggested above, it is
clear that our division of the problem is well advised. The first stage of the process then affords a considerable economy of effort in the second—the work of finding a TCP is made considerably less by eliminating impossible zero patterns, i.e., by first characterizing the corresponding BPs [1,2,5].

That certain types of ternary pairs can be eliminated by considering only the Boolean case is particularly evident in cases where \( \delta \) is small, as we shall see in Section 4.

Finally, we shall see that the study of Boolean complementary pairs recommends itself by the strength of the results found and the beautiful objects one is led to consider. The theory is quite elegant in comparison to that for ternary complementary pairs and, with relatively little effort, we can use it to gain considerable ground in answering key questions in the latter field; yet we shall leave some strikingly simple questions unresolved.

Let us use \( A^* \) to denote the sequence obtained by reversing the order of the entries of \( A \). \( A \) is symmetric if \( A^* = A \).

It will be convenient at times to ignore factors of the form \( x^k \) in polynomials. (Note that introduction of such factors into Hall polynomials will not affect relation (1) at all since, if \( u(x) = x^k v(x) \), then \( uu^* = vv^* \).) Let us write

\[
\hat{f} \equiv g
\]

to indicate that \( g(x) = x^k f(x) \) for some integer \( k \). Thus, for example, the Hall polynomial of a sequence \( A \) satisfies \( a(x) \equiv \sum_{i=1}^n a_i x^i \) and \( a^*(x) \equiv \sum_{i=1}^n a_i x^{n-i} \)—the Hall polynomial of \( A^* \). Note that this is not a modular congruence, though it is an equivalence relation that preserves multiplication; Laurent polynomials factor uniquely (treating \( x \) as a unit) over \( \mathbb{Z}_2 \), modulo this equivalence.

2. The basics of BPs

We say that a sequence \( A = (a_1, \ldots, a_n) \) is reduced if \( a_1, a_n \neq 0 \); a pair is reduced if it consists of two reduced sequences or if it is the pair \((1);(0)\). Observe that, for every \( BP(n,w) \), there is a unique \( n' \) (necessarily \( n' \leq n \)) and reduced \( BP(n',w) \) with equivalent (i.e., \( \equiv \)) Hall polynomials. Moreover, for any \( n'' > n' \), one can trivially also obtain \( BP(n'',w) \) with equivalent Hall polynomials, by appending sufficiently many 0's.

Since \( f f^*(x) = \sum_{i=1}^{n-1} c_i x^i \) is invariant with respect to interchanging \( x \) and \( x^{-1} \), it follows that \( c_{-i} = c_i, i = 1, \ldots, n-1 \). So, to verify (1) it suffices to consider only coefficients of positive degree terms. For \( i > 0 \), \( c_i \) is called the \( i \)th autocorrelation coefficient of \( F \), and \( c_0 \) is the constant coefficient of the sequence, which is the residue of its weight—number of nonzero entries—mod 2.

The following handy characterization of Boolean complementary pairs, whose proof is immediate from (1), refers only to the autocorrelation coefficients.
Lemma 2. A pair of Boolean sequences $A;B$ is a BP if and only if $A$ and $B$ have the same autocorrelation coefficients $\text{mod} 2$. Further, $\lambda = 0$ or 1 according as their weights are equal or different $\text{mod} 2$.

If we admit pairs of sequences of different lengths (observe that padding one sequence with zeros does not affect the autocorrelation of a pair), reduced BPs would still necessarily have the same length.

Lemma 3. If $A$ is any nonzero Boolean sequence of length greater than 1, and $A;B$ is a reduced Boolean complementary pair, then $A$ and $B$ have the same length.

Proof. This follows immediately from Lemma 2, by considering the autocorrelation coefficients of largest index. \square

We now describe two elementary classes of BPs, which we shall call, respectively, identical and siamese twin pairs or, collectively, twin pairs.

Lemma 4. Let $A$ be any Boolean sequence of length $n$ having a nonzero entries. Then

1. $A;A$ is a BP($n,2a$).
2. If $A$ is symmetric, $n$ is odd, and $B$ is the sequence differing from $A$ only in the center position, then $A;B$ is a BP($n,2a+1$).

Proof. The first part follows from Lemma 2; for the second, observe that there is a (unique) Laurent polynomial $c$ such that $a \equiv c$, $c = c^*$, and $b \equiv c + 1$. So, $aa^* + bb^* = c^2 + (c + 1)^2 = 2c^2 + 2c + 1 = 1$. \square

Although twin pairs are trivial to come by in large numbers, and we may thus regard them as elementary, they are not uninteresting; it is quite common for important ternary complementary pairs (such as Golay complementary pairs!) to correspond to such BPs. However, I regard primitive ternary complementary pairs \cite{2} as the (theoretically) most fundamental cases; these do not have identical twin patterns if $n \geq 3$, and it seems unlikely that any have siamese twin patterns if $n > 3$.

We use commas to indicate concatenation of sequences: $(A,C)$ is the concatenation of sequences $A$ and $C$; $(A,1)$ is the sequence obtained by concatenating $A$ and $(1)$, and so on.

Theorem 5. For even $w \leq 2n$, $n \geq 1$, there exists an identical twin BP($n,w$). For all $w \leq 2n - 1$, $w \equiv 1 \text{ mod } 4$, $n$ odd, there exists a siamese twin BP($n,w$).

Proof. For the first part, let $A$ be any sequence of length $n$ with $\frac{w}{2}$ nonzero entries; apply Lemma 4. For the second part, let $A = (S,0,S^*)$ where $S$ is any sequence of length $\frac{w-1}{4}$ with $\frac{w-1}{4}$ entries, and apply Lemma 4. \square
In the first four cases, we have, respectively:

If \(A;B\) exist with parameters \(n, w\) other than those provided by the twin pairs of Theorem 5? The following result shows that pairs with \(n\) even and \(w \equiv 1 \mod 4\) are the only such cases. We shall soon see that such pairs exist; they are necessarily nontwin, since Theorem 5 accounts for all twin pairs. Note that, although pairs with odd length or even weight have the same parameters as twin pairs, they are not necessarily twin, as we shall also see.

Let us write \(x\) and \(\beta\) for the weights of \(A\) and \(B\), respectively.

**Lemma 6.** If \(A;B\) is a \(BP(n, w)\), then \(x^2 + \beta^2 \equiv w \mod 4\). If \(w\) is even, then \(x \equiv \beta \mod 4\). If \(w \equiv 0 \mod 4\), then \(x, \beta\) are even; if \(w \equiv 2 \mod 4\), then \(x, \beta\) are odd; if \(w\) is odd, then \(w \equiv 1 \mod 4\).

**Proof.** First note that \(x + \beta = w\), by definition. The sums of the autocorrelation coefficients of the two sequences are (by simple counting) \(\frac{x(x-1)}{2}\) and \(\frac{\beta(\beta-1)}{2}\), respectively, whose sum, \(\frac{x^2 + \beta^2 - w}{2}\), must be \(\equiv 0 \mod 2\), by (1). Thus, \(x^2 + \beta^2 \equiv w \mod 4\).

If \(w\) is even, then \(x, \beta\) are both even or both odd, since they sum to \(w\). Since \(x^2 + \beta^2 \equiv w \mod 4\), if \(w \equiv 2 \mod 4\), then \(x\) and \(\beta\) are both odd, and if \(w \equiv 0 \mod 4\), then they are both even. In either of these cases, \(x + \beta = w\) now implies \(x \equiv \beta \mod 4\).

If \(w\) is odd, then \(w \equiv 1 \mod 4\), since \(w \equiv x^2 + \beta^2 \equiv 0 \mod 4\).

The following result provides a set of operations preserving the class of Boolean complementary pairs of weight \(w\); for each operation we introduce a name. We shall regard pairs related by combinations of these operations as equivalent.

The notation 0, indicates a sequence of \(t\) 0’s.

**Lemma 7.** Let \(A;B\) be a Boolean complementary pair of weight \(w\). Then so are \(A;B' = \)

1. \((A, 0_r);(0_r, B)\) (shifting by \(t\) places);
2. \(B:A\) (interchanging);
3. \(A:B^r\) (reversing);
4. \((a_1, 0_{r-1}, a_2, 0_{r-1}, \ldots, 0_{r-1}, a_n);(b_1, 0_{r-1}, b_2, 0_{r-1}, \ldots, 0_{r-1}, b_n)\) (inflating by factor \(t\));
5. any pair obtained by undoing any of the above operations (respectively: reducing, interchanging, reversing, deflating).

**Proof.** In the first four cases, we have, respectively: \(a' (x); b'(x) = a(x); x'b'(x), a'; b' = b; a, a'(x); b'(x) = a(x); x^{a^{-1}}b(x^{-1}), and a'(x); b'(x) = a(x'); b(x'). In each case it may be directly verified that (1) is satisfied by \(a'; b'\) if and only if it is satisfied by \(a; b\).

For example, we regard the pairs \((b_n, 0, b_{n-1}, 0, \ldots, 0, b_1, 0, 0)\); \((0, a_1, 0, a_2, 0, \ldots, 0, a_n, 0)\) and \((0_p, A^r, 0_q);(0_r, B^r, 0_s)\), \(p + q = r + s\), as equivalent to \(A;B = (a_1, \ldots, a_n);(b_1, \ldots, b_n)\), for each can be obtained from the other by combinations of operations from Lemma 7.
3. Pairs with small weight

Pairs with weight less than 8 are easily characterized; all such pairs are equivalent to twin pairs. (Weights 3 and 7 are inadmissible, by Lemma 6.)

Theorem 8. Let \( A;B \) be a \( BP(n,w) \).

1. If \( w = 1 \), then \( A;B \) is equivalent to \((1);(0)\).
2. If \( w = 2 \), then \( A;B \) is equivalent to \((1);(1)\).
3. If \( w = 4 \), then \( A;B \) is equivalent to \((11);(11)\).
4. If \( w = 5 \), then \( A;B \) is equivalent to \((111);(101)\).
5. If \( w = 6 \), then \( A;B \) is equivalent to \((10,10,1);(10,10,1) \), where \( s + 1 \) and \( t + 1 \) are relatively prime positive integers.

Proof. If \( w = 1 \), then there is a single nonzero entry in \( A;B \) and the result follows immediately. If \( w = 2 \), Lemma 6 implies that each of \( A,B \) has a single nonzero entry, and the result follows. If \( w = 4 \), Lemma 6 implies that each of \( A,B \) has two nonzero entries. By Lemma 3, assuming the pair is reduced, then \( A \) and \( B \) are both of the form \((10k;1)\); deflating yields \( A;B = (11);(11) \).

If \( w = 5 \), Lemma 6 implies either that one sequence has five nonzero entries and the other 0, or that one has three and the other two. The former case is easily eliminated since it implies a single sequence of weight \( > 1 \) with zero autocorrelation—impossible, as noted earlier. So, without loss of generality, their Hall polynomials are \( a(x);b(x) = 1 + x^k + x^n;1 + x^n, k < n \). Now, \((aa^* + bb^*)(x) = 5 + 2(x^n + x^{-n}) + x^k + x^{k-h} + x^{n-h} + x^{a-k} + x^{a-h} \). For zero autocorrelation, we must have \( k = n - k \), so that \( a(x);b(x) = 1 + x^k + (x^k)^2;1 + (x^k)^2 \). Deflating \( A;B \) yields \((111);(101) \).

If \( w = 6 \), we similarly obtain \( a(x);b(x) = 1 + x^h + x^n;1 + x^k + x^n, h,k < n \), so \((aa^* + bb^*)(x) = 6 + 2(x^n + x^{-n}) + x^h + x^{k-h} + x^{k-h} + x^{a-k} + x^{a-k} + x^{a-n} \). For zero autocorrelation, positive terms must match, so (i) \( h = n - h \), (ii) \( h = k \), or (iii) \( h = n - k \). Case (i) reduces to case (ii), since we must also have \( k = n - k \). Case (iii) also reduces to case (ii) by reversing \( B \). So we obtain the twin pair with both Hall polynomials equal to \( 1 + x^h + x^n \). The pair can be deflated if \( (h,n) \neq 1 \), so we can assume that \( (h,n) = 1 \). Then \((h,n-h) = 1 \) as well. The result follows, with \( s = h - 1 \), \( t = n - h - 1 \). \(\square\)

4. Pairs with small deficiency

The pair \((1\cdots 1;1\cdots 1)\) of length \( n \) is a \( BP(n,2n) \); evidently, \( \delta = 0 \) is the least interesting case of Boolean complementary pairs. (Ironically, this is probably the case of most interest in the application of TCPs!)
Let us denote by \( J \) the sequence of 1’s, above; the Hall polynomial of \( J \) is \( j(x) = \frac{x^{n+1}}{x+1}. \) Now,
\[
j^*(x) = \frac{1 + x^{-n}}{1 + x^{-1}} = x^{-n+1}j(x).
\]

Consider a pair \( A;B \) with deficiency \( \delta = 1. \) Without loss of generality, we assume that it is reduced, so that, for some \( k, \) \( a(x) = j(x) + x^k; b = j. \) Using (2), we have
\[
(aa^* + bb^*)(x) = (j(x)j^*(x) + x^{-k}j(x) + x^kj^*(x) + 1) + j(x)j^*(x)
= 1 + j(x)(x^{k-n+1} + x^{-k}).
\]
So, the pair has zero autocorrelation if and only if \( k - n + 1 = -k \)—that is, \( k = \frac{n-1}{2}, \)
which establishes the following result.

**Theorem 9.** A pair of reduced Boolean sequences, \( A;B, \) is a \( BP(n, 2n - 1) \) if and only if \( n \) is odd, one of the sequences is \( (1, n) \) and the other is \( (1, 1, 0, 1, 2). \)

That is, the only reduced \( BP(n, 2n - 1)s \) are siamese twin pairs—uniquely determined for each odd \( n. \) Similarly, identical twin pairs are the only possibilities when \( \delta = 2. \)

**Theorem 10.** A pair of reduced Boolean sequences \( A;B \) is a \( BP(n, 2n - 2) \) if and only if \( B \) contains a single 0 and \( B = A \) or \( B = A^*. \)

**Proof.** Assume that \( A;B = BP(n, 2n - 2). \) By Lemma 6, one zero must appear in each of the sequences. Therefore,
\[
a(x) = j(x) + x^h; b(x) = j(x) + x^k,
\]
for some \( h, k. \) Thus,
\[
(aa^* + bb^*)(x) = j(x)(x^{-h} + x^{-k} + x^{h-n+1} + x^{k-n+1}) = 0.
\]
So the terms of \( x^{-h} + x^{-k} + x^{h-n+1} + x^{k-n+1} \) must match in pairs. If \( -h = -k, \) or if \( -h = h - n + 1 \) and \( -k = k - n + 1, \) then \( h = k, \) so \( A = B; \) if \( -h = k - n + 1, \) then \( h + k = n - 1, \) so \( A = B^* \) as required.

Conversely, all such pairs are identical twins and, therefore, \( BP(n, 2n - 2)s. \)

The case \( \delta = 3 \) provides our first class of nontwin pairs.

**Theorem 11.** A pair of reduced sequences \( A;B \) is a \( BP(n, 2n - 3) \) if and only if \( n = 4m + 2, \) for some integer \( m, \) and \( A;B \) is equivalent to a pair with \( a_{m+1} = a_{3m+2} = b_{2m+1} = 0. \)

**Proof.** Assume that \( A;B = BP(n, 2n - 3). \) By Lemma 6, \( n \) is even.
First suppose that all three zeros occur in one pair, so
\[ a(x) = f(x) + x^p + x^q + x^r; b = j, \]
where \(1 \leq p < q < r \leq n - 2\). By Lemma 7, we can assume that
\[ q \leq \frac{n}{2}. \] (3)
So \((aa^* + bb^*)(x)\) is calculated as
\[
\begin{align*}
j(x)(x^{-p} + x^{-q} + x^{-r} + x^{p-n+1} + x^{q-n+1} + x^{r-n+1}) \\
+ x^{p-q} + x^{q-r} + x^{r-p} + x^{q-p} + x^{r-q} + 1 = 1.
\end{align*}
\]
The terms of largest degree, \(x^r\) and \(x^{a-p-1}\), must cancel, so \(p + r = n - 1\). Cancelling, we obtain
\[
x^{-q}j(x) + x^{p}j^*(x) = x^{p-q} + x^{q-r} + x^{r-p} + x^{q-p} + x^{r-q}.
\]
Counting uncancelled terms of positive degree on both sides, we obtain \(n - 2q - 1 = 1\) or \(3\). By (3), the largest term on the left is \(x^{a-q-1}\), and the largest term on the right is clearly \(x^{r-p}\), so \(r - p = n - 1 - q\). From above, \(r + p = n - 1\). So \(r < r + p + 2(r - p) = (n - 1) + 2(n - 1 - q) = n - 2q - 1 = 1\) or \(3\)—a contradiction, since \(r \geq 3\).

Therefore, two zeros occur in one sequence and one in the other. By Lemma 7, we can write
\[ a(x) = f(x) + x^p + x^q; b(x) = j(x) + x^q, \]
with \(1 \leq p < r \leq n - p - 1\) and \(q < n - q - 1\). This time,
\[
(aa^* + bb^*)(x) = j(x)(x^{-p} + x^{-q} + x^{-r} + x^{p-n+1} + x^{q-n+1} + x^{r-n+1}) \\
+ x^{p-r} + x^{q-r} + 1 = 1. \] (4)
Now, \(x^r\) and one of \(x^{a-p-1}\), \(x^{a-q-1}\) are the largest degree terms—which must cancel. So either (i) \(r + q = n - 1\) or (ii) \(p + r = n - 1\). In the first case, by cancelling in (4), we obtain
\[
j^*(x)(x^{-p} + x^{a-p-1}) = x^{p-r} + x^{r-p}.
\]
The largest terms on the two sides are \(x^{a-p-1} = x^{r-p}\), so \(r = n - 1\), a contradiction.

Thus, \(p + r = n - 1\). After cancellation in (4), we have
\[
j^*(x)(x^{-q} + x^{r-q-1}) = x^{p-r} + x^{r-p}.
\]
Since there must be one term of positive degree on the left, we must have \(q = n - q - 2\), or \(q = \frac{n}{2} - 1\). Further, that term is then \(x^\frac{n}{2} = x^{r-p}\). Since \(r + p = n - 1\), we have \(p = \frac{n-2}{3}\), so \((p, q, r) = (m, 2m, 3m + 1)\), and \(a_{m+1} = a_{3m+2} = b_{2m+1} = 0\), for some \(m\).

Conversely, all such pairs are \(BP(n, n - 3)\)s, for \((aa^* + bb^*)(x) = j(x)(x^{-m} + x^{-2m} + x^{-3m-1} + x^{m-(4m+2)+1} + x^{2m-(4m+2)+1} + x^{3m+1-(4m+2)+1} + x^{2m-1} + x^{1-2m} + 1 = j(x)(x^{-2m} + x^{-2m-1}) + x^{2m-1} + x^{1-2m} + 1 = x^{-2m-1}. (x^{4m+2} + 1) + x^{2m+1} + x^{-2m-1} + 1 = 1. \) \(\Box\)
Observe that these pairs are never twins, so we now have a third simple class of Boolean complementary pairs. Theorem 11 immediately implies Lemma 3 of [4] (which is stated without proof) and part (i) of Lemma 3 of [6] (the two-line sketched proof of which omits all details).

5. Small Boolean complementary pairs

Table 1 is the result of an exhaustive manual search for reduced Boolean complementary pairs of length up to 9, excluding twin pairs. Only one pair of the type given in Theorem 11 appears in this table; the next one is of length 10.

Observe that some sequences appear in more than one pair, which might be taken as evidence that not necessarily all TCPs are uniquely determined by one sequence (see comments in [2]). Note also that Boolean complementary pairs occur with

<table>
<thead>
<tr>
<th>Reduced $BP(n, w)$s, $n \leq 9$, up to equivalence, omitting twin pairs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$BP(n, w)$s, by length</td>
</tr>
<tr>
<td>$w$</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>All pairs of length $\leq 5$ are twin</td>
</tr>
<tr>
<td>$n = 6$</td>
</tr>
<tr>
<td>$(101101)_(111011)$</td>
</tr>
<tr>
<td>$n = 7$</td>
</tr>
<tr>
<td>$(1010001)_(111101)$</td>
</tr>
<tr>
<td>$(1010001)_(1111111)$</td>
</tr>
<tr>
<td>$n = 8$</td>
</tr>
<tr>
<td>$(10000001)_(11110011)$</td>
</tr>
<tr>
<td>$(11000001)_(11110101)$</td>
</tr>
<tr>
<td>$(11000001)_(11001101)$</td>
</tr>
<tr>
<td>$(10110001)_(11000011)$</td>
</tr>
<tr>
<td>$(10110101)_(11100011)$</td>
</tr>
<tr>
<td>$n = 9$</td>
</tr>
<tr>
<td>$(101010001)_(11000011)$</td>
</tr>
<tr>
<td>$(101010001)_(110010011)$</td>
</tr>
<tr>
<td>$(110000001)_(11100101)$</td>
</tr>
<tr>
<td>$(101000001)_(110101111)$</td>
</tr>
<tr>
<td>$(101000001)_(110111111)$</td>
</tr>
<tr>
<td>$(100100001)_(111101111)$</td>
</tr>
<tr>
<td>$(111000001)_(11010101)$</td>
</tr>
<tr>
<td>$(110110001)_(11100010)$</td>
</tr>
<tr>
<td>$(110001101)_(111011011)$</td>
</tr>
<tr>
<td>$(111111011)_(11001110)$</td>
</tr>
<tr>
<td>$(111011011)_(10101101)$</td>
</tr>
<tr>
<td>$(111011101)_(101111101)$</td>
</tr>
</tbody>
</table>
weights not possible in the ternary case—specifically here: \( w = 9, 12 \) and \( 14 \). \( w = 6 \) is another small example, but it does not appear in Table 1, for Theorem 8 tells us that it is attained only by identical twin pairs.

6. \( BP(n, w) \) s with even weight

The following version of the factorization obtained as the pivotal step in the proof of an important theorem of Eliahou et al. [3] supplies a complete algebraic characterization of even weight \( BP \) s.

**Theorem 12.** A pair of Boolean sequences \( A;B \) with even weight \( w \) is a \( BP(n, w) \) if and only if there exist Boolean polynomials \( h,k \) such that \( a = hk \) and \( b \equiv hk^* \).

**Proof.** First, let \( h,k \) be any Boolean polynomials. Let \( a = hk \) and \( b \equiv hk^* \). Then

\[
\begin{align*}
a^* + b^* &= hh^*(hk)^* + hh^*(hk^*)^* = 2hh^*kk^* = 0.
\end{align*}
\]

Thus, \( A;B \) is a \( BP(n, w) \), where \( w \) is even.

Conversely, suppose that \( A;B \) is a \( BP(n, w) \), \( w \) even. Then \( aa^* + bb^* = 0 \). Let \( h = gcd(a, b) \), \( a = hk \) and \( b = hu \). Then

\[
\begin{align*}
hk(hk)^* + hu(hu)^* &= hh^*(kk^* + uu^*) = 0.
\end{align*}
\]

Since \( hh^* \neq 0 \), it follows that \( kk^* = uu^* \). Now, \( gcd(k, u) = 1 \), so \( u|k^* \). Since \( k \) and \( u^* \) have the same degree, \( u \equiv k^* \), and so \( b \equiv hk^* \), as required. \( \square \)

In this way, the Hall polynomials of all even weight Boolean complementary pairs are generated from the Hall polynomials, \( h;k \), of two Boolean sequences \( H;K \)—with no constraints on the choice of \( H, K \)! What do we thus learn about the structure of \( A \) and \( B \)? The following result characterizes major structural features of even weight Boolean complementary pairs by the factorizations of their Hall polynomials; its proof is immediate.

**Lemma 13.** \( A;B = BP(n, w) \), where \( a;b \equiv hk;hk^* \), is an identical twin pair if and only if \( K \) is symmetric. \( A;B^* \) is an identical twin pair if and only if \( H \) is symmetric. \( A \) is symmetric if and only if \( h \equiv k^*;b \) is symmetric if and only if \( h \equiv k \).

Now, even weight Boolean complementary pairs need not be twin; in Table 1, there are 10 such pairs, starting with length 7. Factorizations for their Hall polynomials are given in Table 2.

7. \( BP(n, w) \) s with odd weight

In light of Theorem 12, odd weight Boolean complementary pairs are somewhat more interesting than even weight pairs, not being so easily characterized. However,
Table 2
Factoring $a:b$ as $hk;hk^*$, where $A:B$ is a nontwin even weight $CP(n,w)$, $n \leq 9$

<table>
<thead>
<tr>
<th>$A:B$</th>
<th>$a:b$</th>
<th>$hk$</th>
<th>$H.K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1010001);(111111)</td>
<td>$1 + x^2 + x^6;$</td>
<td>$1 + x + x^3;1 + x + x^3$</td>
<td>(1101);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^3 + x^4 + x^5 + x^6$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10000001);(1110011)</td>
<td>$1 + x^7$</td>
<td>$1 + x^2 + x^3 + x^4;1 + x^2 + x^3$</td>
<td>(10111);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^3 + x^6 + x^7$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10110101);(11000011)</td>
<td>$x^3 + x^2 + 1 + x^3 + x^7; $</td>
<td>$1 + x + x^3;1 + x + x^3$</td>
<td>(11001);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^6 + x^7$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10100001);(11011011)</td>
<td>$1 + x^2 + x^8;$</td>
<td>$1 + x + x^4;1 + x + x^4$</td>
<td>(11001);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^3 + x^5 + x^7 + x^8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(11100001);(11001010)</td>
<td>$1 + x + x^2 + x^6;$</td>
<td>$1 + x^2 + x^3;1 + x + x^3 + x^4 + x^5$</td>
<td>(10111);(110111)</td>
</tr>
<tr>
<td></td>
<td>$x^4 + x + 1 + x^3 + x^8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(10101001);(11000001)</td>
<td>$1 + x^2 + x^4 + x^8; $</td>
<td>$1 + x^3 + x^4 + x^3;1 + x^2 + x^3$</td>
<td>(100011);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^3 + x^8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(11001001);(11111011)</td>
<td>$1 + x + x^3 + x^7; $</td>
<td>$1 + x;1 + x^5 + x^6 + x^7$</td>
<td>(11);(100011)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(11010011);(11010010)</td>
<td>$1 + x + x^4 + x^2 + x^8; $</td>
<td>$1 + x + x^3;1 + x^3 + x^5$</td>
<td>(1011);(100101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x + x^2 + x^5 + x^8$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(11101101);(10111010)</td>
<td>$1 + x + x^2 + x^4 + x^5 + x^7 + x^8; $</td>
<td>$1 + x + x^3;1 + x^2 + x^3$</td>
<td>(110001);(1101)</td>
</tr>
<tr>
<td></td>
<td>$1 + x^2 + x^3 + x^4 + x^3 + x^6 + x^8$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

odd weight pairs in which one partner is symmetric do admit a complete algebraic characterization.

Theorem 14. A pair, $A:B$, of reduced Boolean sequences of length $n$ is a $BP(n,w)$, with $w$ odd and $A^* = A$, if and only if

1. $n$ is odd and $a \equiv hh^* + 1$ and $b \equiv h^2$, for some Boolean polynomial $h$; or
2. $n$ is even and $a(x^2) \equiv bb^*(x) + 1$.

Proof. Suppose $A:B = BP(n,w)$, with $A$ symmetric.

If $n$ is odd, then $a \equiv a'$, where $(a')^* = a'$. Thus, $d + 1; b$ is equivalent to a pair of Hall polynomials for a $BP(n,w \pm 1)$. By Lemma 13, $a' = hh^*$ and $b = h^2$; part 1 follows.

Now suppose $n$ is even. Then $a(x^2); b(x^2) = BP(2n - 1,w)$; applying part 1, we infer that $a(x^2) \equiv hh^*(x) + 1, b(x^2) \equiv h^2(x)$ for some Boolean polynomial $h$. Now, since $f^2(x) = f(x^2)$ for all Boolean polynomials $f$, and Boolean polynomials factor uniquely, it follows that $h = b$.

Conversely, if $a \equiv hh^* + 1$ and $b \equiv h^2$, or $a(x^2) \equiv bb^*(x) + 1$, then $A$ is symmetric and it may be directly verified that $A:B$ satisfies (1). $\square$

Siamese twins are precisely those sequences obtained by using symmetric $H$ in part 1 of Theorem 14. The deficiency three pairs of Theorem 11 are examples of the sequences obtained in part 2.
What if both partners in a Boolean complementary pair are symmetric? The following result tells us this can happen only with twin pairs.

**Theorem 15.** Let $A;B$ be a pair of reduced Boolean sequences. Then $A;B = BP(n,w)$ with both sequences symmetric if and only if

1. $w$ is odd and $A;B$ is a siamese twin pair; or
2. $w$ is even and $A;B$ is an identical twin pair of symmetric sequences.

**Proof.** If $A;B = BP(n,w)$, $w$ odd, then $(a+b)(a+b)^* = aa^* + bb^* + ab^* + ba^* = aa^* + bb^* = 1$. It follows that $a+b$ is a monomial; that is, $A$ and $B$ differ only in one entry—their middle entry, by symmetry. So they comprise a siamese twin pair.

By Lemma 13, if $w$ is even then $b ≡ hh^*$ and $a ≡ h^2$. Also, since $A$ is symmetric, $h^* ≡ h$. Thus, $A = B$.

Lemma 4 provides the reverse implications. $\Box$

The product of pairs given in the following result can be used to recursively construct many new odd weight pairs.

**Theorem 16.** If $A;B$ and $C;D$ are Boolean complementary pairs of odd weight, then so is $U;V$, where $u ≡ ac + bd$ and $v ≡ ad^* + bc^*$.

**Proof.** $uu^* + vv^* = (ac + bd)(ac + bd)^* + (ad^* + bc^*)(ad^* + bc^*)^* = aa^*cc^* + bb^*dd^* + aa^*dd^* + bb^*cc^* + 2(acb^*d^* + bda^*c^*) = (aa^* + bb^*) \cdot (cc^* + dd^*) = 1$. $\Box$

Interestingly, there is no obvious formula that predicts the weight of $U;V$ from the weight and lengths of $A;B, C;D$. The reduced length is easy to infer in many cases, but nontrivial in cases involving considerable cancellation of largest and smallest terms. But clearly the reduced length of $U;V$ is at most one less than the sum of the lengths of the given pairs, and its weight at most the product of their weights.

Even weight pairs may be used in this product, but in this case odd weight pairs cannot result.

Quite a variety of odd weight pairs can be generated recursively using nothing but a few “seed” pairs, Theorem 16, and the equivalence operations of Lemma 7, as we demonstrate in Table 3, which uses just one seed pair—the smallest nontrivial odd weight pair, $(111);(101)$. $U;V$ in each line in the table is the result of applying Theorem 16, with $a;b = 1 + x + x^2; 1 + x^2$, the Hall polynomials of $A;B = (111);(101)$, and the given $c;d$ equivalent to sequences constructed in a previous line of the table (except in the first line, where we use the Hall polynomials of the trivial $BP, (1);(0)$). Thus, all pairs in the table are descendents of the original, $A;B$. 
Table 3
Sequences \( U;V \) recursively generated from \( A:B = (111);(101) \) by Theorem 16

<table>
<thead>
<tr>
<th>( U;V )</th>
<th>( u:v )</th>
<th>( c:d )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(111);(101)</td>
<td>1 + x + x^2; 1 + x^2</td>
<td>1:0</td>
</tr>
<tr>
<td>(111011);(101101)</td>
<td>1 + x + x^2 + x^4 + x^6; 1 + x^2 + x^3 + x^5</td>
<td>1 + x + x^2; x + x^3</td>
</tr>
<tr>
<td>(1000101);(1110111)</td>
<td>1 + x^2 + 3x^3 + 1 + x + x^2 + x^4 + x^6 + x^5</td>
<td>1 + x + x^2; x^2 + x^4</td>
</tr>
<tr>
<td>(10111001);(11000011)</td>
<td>1 + x^2 + x + x^3 + x^5; 1 + x + x^6 + x^7</td>
<td>1 + x + x^2; x^3 + x^5</td>
</tr>
<tr>
<td>(10100001);(1101010111)</td>
<td>1 + x^2 + x^3; 1 + x + x^3 + x^5 + x^7 + x^9</td>
<td>1 + x + x^2; x^4 + x^6</td>
</tr>
<tr>
<td>(101011001);</td>
<td>1 + x^2 + x^4 + x^5 + x^9; 1 + x + x^2</td>
<td>x^5 + x^7</td>
</tr>
<tr>
<td>(11011101);</td>
<td>1 + x + x^2 + x^4 + x^5 + x^6 + x^8 + x^9;</td>
<td>x^5 + x^7</td>
</tr>
<tr>
<td>(11001001);</td>
<td>1 + x + x^3 + x^5 + x^6;</td>
<td>x + x^2 + x^3 + x^5 + x^6;</td>
</tr>
<tr>
<td>(100010101)</td>
<td>1 + x^4 + x^6 + x^8; 1 + x^2 + x^3 + x^5</td>
<td>1 + x^2 + x^3 + x^5</td>
</tr>
<tr>
<td>(1011000101);</td>
<td>1 + x^2 + x^3 + x^5 + x^9;</td>
<td>x^2 + x^3 + x^4 + x^6 + x^7;</td>
</tr>
<tr>
<td>(1101101111)</td>
<td>1 + x + x^3 + x^4 + x^6 + x^7 + x^8 + x^9;</td>
<td>1 + x^2 + x^3 + x^5</td>
</tr>
<tr>
<td>(111011011);</td>
<td>1 + x + x^2 + x^4 + x^5 + x^7 + x^8;</td>
<td>1 + x + x^2 + x^4 + x^5;</td>
</tr>
<tr>
<td>(101101101);</td>
<td>1 + x^2 + x^3 + x^5 + x^6 + x^8;</td>
<td>x + x^3 + x^4 + x^6</td>
</tr>
<tr>
<td>(1000011101);</td>
<td>1 + x^5 + x^6 + x^7 + x^9;</td>
<td>1 + x + x^2 + x^4 + x^5;</td>
</tr>
<tr>
<td>(1111101111)</td>
<td>1 + x + x^2 + x^3 + x^4 + x^6 + x^7 + x^8 + x^9;</td>
<td>x^2 + x^4 + x^5 + x^7</td>
</tr>
</tbody>
</table>

8. Further observations

Given a product construction, such as is given in Theorem 16, it is natural to ask which pairs are “prime”—that is, cannot be obtained from other pairs by multiplying, except in a trivial way (like the primitive TCPs introduced in [2])? Characterizing these pairs would normally provide a complete classification of all pairs. But it is rather astounding, for one familiar with such products, to learn that there are no primes in the case at hand! In fact, every pair can be obtained from every other pair by multiplying by an appropriate third pair, as Theorem 17 shows.

**Theorem 17.** Let \( A:B \) and \( C:D \) be Boolean complementary pairs with odd weight. Then \( a:b \equiv ec + fd; ed^* + fc^* \), where \( E:F \) is an odd weight Boolean complementary pair.

**Proof.** Let \( e:f = ac^* + bd; ad^* + bc \). One can verify directly that \( ee^* + ff^* = 1 \), so \( e:f \) corresponds to a Boolean complementary pair with odd weight. Further, \( ec + fd = (ac^* + bd)c + (ad^* + bc)d = acc^* + bcd + add^* + bcd = a(ce^* + dd^*) + 2bcd = a \); similarly, \( ed^* + fc^* = b \), as required. \( \square \)

To understand what this result says about Boolean complementary pairs, we must be clear about the sense in which a pair is said to be a product of other pairs by Theorem 16. Evidently there is no one, unique pair \( U;V \) obtained as “the” product of pairs \( A:B, C:D \) by this theorem. In fact, \( ad^* + bc^* \) is not, in general, the Hall polynomial of any sequence, since it may have terms of negative degree; this is why we write \( v \equiv ad^* + bc^*; v \) is not uniquely determined.

We cannot simply cease distinguishing between polynomials \( f \) and \( g \) with \( f \equiv g \) in order to resolve the ambiguity in this context, as Table 3 shows, for
multiplying one of the polynomials \(a, b, c, d\) by a power of \(x\) can lead to major changes in the product—possibly different weights and, even after reduction, different lengths.

A better resolution is to admit that Laurent polynomials summarize the requisite information more exactly than the sequences they represent. We can modify our understanding of sequences to record this information by allowing them to “begin before they start,” by permitting positions to be indexed by arbitrary integers—positive, negative or 0—the degrees of terms in the Laurent polynomials. In this way, we obtain an exact correspondence between polynomials and sequences. To illustrate, I am suggesting that the Laurent polynomial \(x^{-3} + x^{-1} + x^2\) would correspond to the sequence \((101, 001)\)—the comma marking the division between the position with index \(-1\) and the position with index 0, like the familiar decimal point. On the other hand, \(x^3 + x^7 + x^9\) would correspond to \((0001000101)\); it makes no difference to write \((0, 00010001010)\) for the same sequence, as with decimal numbers. Put another way, the sequence corresponding to Laurent polynomial \(f\) is the (reverse) binary expansion of the rational number \(f(2)\).

Under this interpretation, the meaning of Theorem 17 is clear: every \(BP(n, w)\) of odd weight (corresponding to \(a; b\)) is divisible, with respect to the product of Theorem 16, by any other such pair (corresponding to \(c; d\)). The quotient (corresponding to \(e; f\)) can be obtained from the original pairs by yet another product similar (in fact, equivalent) to that of Theorem 16! It is not hard to show that the resulting product and quotient are uniquely defined. In our presentation, however, we have not recorded this information, so our product and quotient are defined only up to equivalence.

The restriction on \(b\) implied in case 2 of Theorem 14 is interesting; \(bb^*\) must have no terms of even degree, except the constant term, which is 1. What does this imply about the polynomial \(b\)? There is no corresponding restriction in case 1; any Boolean polynomial \(h\) will generate a Boolean complementary pair of the form \(hh^* + 1; h^2\). So it seems likely that one ought to be able to more completely characterize the odd weight pairs of even length with one symmetric sequence. In Table 4, we give all such pairs up to length 14; this table was generated by considering all candidate sequences \(b\) and applying Theorem 14.

More questions are raised by this table than answered. For example, why does \(w = 13\) appear so often in it, compared to 9? (It is possible to show that all \(w \equiv 1 \mod 4\) occur infinitely many times among these sequences, but the evidence at hand suggests that some weights are more prevalent than others; 13 appears here to be a “lucky number.”)

Observe that it is possible for the symmetric partner, \(A\), in case 2 of Theorem 14 to occur in more than one pair (this never happens with \(B\), since \(A\) is determined by \(B\)). Evidence on hand suggests that this is quite common—in length 14, there are four such cases, accounting for 8 out of the 11 pairs in Table 4.

To understand the structure of \(B\), one might ask how far it is from being symmetric. In many cases, it is about as close as possible. Perfect symmetry is, of course, impossible for any pair of reduced Boolean sequences with odd weight and even length. Among the 21 pairs up to length 14 in Table 4, \(B\) and \(B^*\) differ in only
one place (among the first \(\frac{n}{2}\) positions) in 15 pairs—most of the time! In the remaining
six cases, \(B\) and \(B'\) differ in exactly three positions. Why never in two or four
positions? Perhaps this is related to the further observation that the weight (number
of nonzero entries) of \(A\) appears to always be a multiple of 4—predominantly 8. Or
since, by Lemma 6, the weight of the pair must be \(\equiv 1 \text{ mod } 4\); then the weight of \(B\)
appears to always be \(\equiv 1 \text{ mod } 4\):
What explains these patterns?
A particular instance in which one partner is symmetric and the other not occurs
when the symmetric sequence is \(j = (1, \ldots, 1)\). We have seen \(BP(3, 5)\) and \(BP(7, 10)\)
of this type—both of which can be signed to obtain known primitive TCPs! Are there
others, besides the obvious examples of twin pairs? The next case is the following
\(BP(23, 30)\):
\[
(1111111111111111111111111); \quad (10100000001010100010001).
\]
There is no TCP with these parameters, so, unfortunately, such BPs cannot be
expected to provide zero patterns for TCPs.
More generally, one might ask if there is an easily identifiable, large class of BPs
for which a canonical signing always produces TCPs with the same parameters.
(That is, aside from classes associated with already known, and uninteresting,
constructions for TCPs—the point here is to obtain previously unknown TCPs by first constructing BPs, not the other way around.) Though this seems likely, we have been unsuccessfull so far in identifying such a class.

What have we accomplished with this study? We have identified a few major classes and constructions for Boolean complementary pairs, and completely determined their algebraic structure when the weight is even or when the weight is odd and one sequence is symmetric. This characterization gives a general construction for all pairs in these cases except when the weight is odd, the length is even and neither sequence is symmetric.

We have also provided a powerful recursive construction for pairs of odd weight. Although we have shown that all pairs can be obtained in this way, because of Theorem 17, we have not yet identified, in a useful way, a canonical set of pairs from which all others can be constructed in a systematic way. If this could be done, then we could claim to “know” all pairs in a way appropriate for the two-stage construction of ternary complementary pairs, and we could consider the first stage of this process effectively complete.

Unfortunately, even if we could complete the final step of algebraic characterization, one substantial aspect of “knowing” Boolean complementary pairs would remain largely incomplete—a simple, direct characterization of their zero patterns. To have such a characterization would, of course, be even more useful in practise than having the algebraic characterization, since it is the zero patterns that are needed in the study of ternary pairs. Nevertheless, it seems unlikely that this will be done until after a complete algebraic characterization is obtained.

References