AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **34** (2006), Pages 269–280

Products and factorizations of ternary complementary pairs

R. Craigen*

Department of Mathematics
University of Manitoba
Winnipeg, Manitoba
CANADA R3T 2N2
craigenr@cc.umanitoba.ca

Abstract

Suppose both sequences of a ternary complementary pair $TCP(mn, vw)$ can be decomposed into uniform-length blocks that are linear combinations of the two sequences of a $TCP(n, w)$. Such a decomposition may be viewed as a factorization of the larger pair by the smaller one. A pattern of such blocks that always returns a longer TCP when a shorter one is substituted into it is regarded as a "block product" of TCP's.

It is shown that every block product is an instance of the known "standard" product of pairs (which multiplies $TCP(m, v)$ and $TCP(n, w)$, yielding $TCP(mn, vw)$), validating our recent claim that this product subsumes all known product constructions.

A new proper generalization of this standard product is introduced. We display factorizations (relative to this new product) of sequences previously considered primitive. Further, we produce an equivalent product that makes the set of integer pairs with zero autocorrelation into a semigroup with unity. Under a simple additional condition this product also preserves the set of ternary pairs.

1 Introduction and preliminaries

Let us begin by advising that [2] is recommended as prior reading. Initially we shall use that article's definitions and conventions and later modify them for our own purposes. Even so, we begin by summarizing a few definitions, facts and conventions that will be of use. The reader is directed to [3] for further background, motivation and applications of this material.

Let $S = (s_0, s_1, \ldots, s_{n-1})$ be a sequence of integers, of length n. The *Hall polynomial* of S is the polynomial, $f_S(x) := \sum_{i=0}^{n-1} s_i x^i$, of degree $n-1$. The *conjugate* of

* Supported by an NSERC grant

a polynomial $f(x)$ is $f^*(x) := f(x^{-1})$. A pair of sequences A;B is said to have *zero autocorrelation* if

$$(f_A f_A^* + f_B f_B^*)(x) = w \ (\in \mathbb{Z}). \tag{1}$$

That is, when this expression is expanded and like terms gathered (in integer powers of x), all x's cancel. The remaining number w is the *weight* of the pair. It is easy to see that w is equal to the sum of the squares of the entries of the two sequences.

A *ternary complementary pair* is a pair, A;B, of $(0, \pm 1)$-sequences with zero autocorrelation. The weight of a ternary pair is clearly equal to the total number of nonzero entries in the two sequences.

The following elementary operations preserve the set of ternary complementary pairs of weight w (though length is not preserved in all cases). Two pairs are *equivalent* if one can be obtained from the other by a combination of these operations.

1. *(Interchanging)* Exchange the two sequences for each other.
2. *(Shifting)* Append any number of 0's to either or both ends of either or both sequences.
3. *(Reversing)* Reverse one or both sequences.
4. *(Negating)* Negate one or both sequences.
5. *(Alternating)* Negate every second entry of both sequences.
6. *(Expanding)* Insert a fixed number of 0's between all pairs of consecutive entries of both sequences.
7. *(Interchanging, Reducing, Reversing, Negating, Alternating, Contracting)* The reverse of the above operations, respectively, when the reverse operation is possible.

A pair A;B is *reduced* if neither A nor B begins or ends with a 0, or in the exceptional case of a *trivial pair*—i.e., of the form $(\pm 1), (0)$ or (0);(± 1). Every pair is equivalent, by shifting, to a reduced pair. Considering the terms of highest degree in (1), it is evident that the two sequences of any reduced pair must have the same length. Even for non-reduced pairs, there is no harm in treating both pairs as having the same length as the longer pair. This way, every ternary complementary pair has a uniquely specified length, n, and weight, w. We denote such a pair by $TCP(n, w)$, or say it is a TCP or, if the weight is important but the length unspecified, a $TCP(*, w)$.

Observe also that every $TCP(n, w)$ is equivalent to a $TCP(m, w)$ for any $m \geq n$.

The set of nonzero positions in a sequence is its *support*. A pair of sequences is *disjoint* if the two sequences have disjoint support, and *conjoint* if they have the same support.

Let us admit a general concept of a "product of TCP's", which is any well-defined construction that starts with one or more TCP's and yields from them a new TCP

whose weight is a multiple of the product of the weights of these "factors". Usually we expect the resulting pair to have larger weight and length than its factors, but multiplying by trivial pairs ($TCP(1,1)$'s) may leave these numbers unchanged. We deliberately include constructions that start with a single $TCP(n,w)$ and produce a $TCP(N,\lambda w)$ for some $N \geq n$, a case we might describe as "multiplying the TCP by the number λ".

The following product of TCP's is classical ($\otimes$ represents the Kronecker product).

Theorem 1 *If A;B is a $TCP(m,v)$ and C;D is a $TCP(n,w)$, with one of the two pairs disjoint, then*

$$\begin{aligned} U &= A \otimes C + B \otimes D; \\ V &= A^* \otimes D - B^* \otimes C \end{aligned}$$

is a $TCP(mn,vw)$.

In [2] it was claimed that Theorem 1 encompasses, up to equivalence, all known (at that time) products of TCP's. In particular, it was shown how a couple of the computer-generated products of the "multiply a TCP by λ" variety in [4] can be obtained by combining the product of Theorem 1 with equivalence operations.

A referee for [2] insisted that we should either withdraw this claim or provide constructions for all the products listed in [4]. But it was clear to us that the approach we had illustrated was sufficient for all the results in that paper, and there was no point in repeating essentially the same argument many times over, which would only labour the point, and would not fully establish our claim in any case, for that particular paper had been singled out only as the most likely source of a counterexample.

Here we shall lay this question to rest with a simple, but general, demonstration that no product among a broad class of constructions will generate anything new. It is a matter of record that all heretofore proposed products of ternary complementary pairs, including all those in [4], fall into this class.

Not surprisingly, this result acts as a guide to discovery. We therefore also offer a strict generalization of Theorem 1, in a couple of different forms. In the second form, the product is associative.

2 Block products

Let us say that a pair of sequences X;Y, of length mn, can be *(block-)factored* by the pair, C;D, of length n, if all of the $2m$ sequences obtained by parsing X and Y into blocks (contiguous subsequences) of length n are linear combinations of C and D. If X, Y, C and D are all to be ternary sequences, the only admissible linear combinations are clearly $0, \pm C, \pm D$ and $\pm C \pm D$ if C and D are disjoint, and $\frac{1}{2}(\pm C \pm D)$ if they are conjoint. (Strictly speaking, if $C = D$, other combinations are possible but never necessary—they all give $\pm C$).

Conversely, suppose U;V is a pair of (formal) sequences of length m whose entries are linear combinations of (symbols) C and D, and the pair X;Y results from the substitution of the corresponding linear combination of (ternary sequences of length n) C and D (and 0_n, the sequence of n 0's, for $\mathbf{0}$) into $U;V$ (stipulating that $C;D$ must be disjoint if $\pm C \pm D$ appears and conjoint if $\frac{1}{2}(\pm C \pm D)$ appears). Expressing U and V as linear combinations of sequences $A;B$ with scalar coefficients "C" and "D", we say that $X;Y$ is a *block product of the pairs* $A;B$ *and* $C;D$.

We show that all block products that preserve TCP's are instances of Theorem 1.

Note that $\mathbb{Z}[x, x^{-1}]$ is a unique factorization domain whose units are the monomials $\pm x^n$, $n \in \mathbb{Z}$. Multiplication of polynomials by units corresponds to shifting and negating sequences. Further, let us agree on the following conventions.

1. Sequences will be denoted by capital letters and their Hall polynomials by the corresponding lower-case letters and, whenever possible, the variable will be suppressed in our notation for polynomials. For example, $A = (1, 2, 3)$; $a = a(x) = 1 + 2x + 3x^2$; $a^* = 1 + 2x^{-1} + 3x^{-2}$.

2. A *(integer) complementary pair* of sequences, denoted $CP(n, w)$, is a pair, $A;B$, of integer sequences of length n such that $aa^* + bb^* = w (\in \mathbb{Z})$. We admit the same equivalence operations for CP's as for TCP's.

3. It is convenient to abuse our terminology by blurring the distinction between the sequence pair $A;B$ and the corresponding pair of Hall polynomials $a;b$. When appropriate, either might be described as a $CP(n, w)$ or $TCP(n, w)$. Let us ignore the fact that some of our Laurent polynomials have terms of negative degree and so do not correspond to sequences—appropriate sequences can be obtained by shifting (multiplying by a unit).

Theorem 2 *Suppose* $a, b, e, f \in \mathbb{Z}[x, x^{-1}]$ *and* $\lambda \neq 0$ *is a real number. If, for any disjoint* $TCP(4, w)$, $C;D$,

$$ac + bd; ec + fd \tag{2}$$

is a $CP(*, \lambda w)$, *then* $(e, f) = u(-b^*, a^*)$, *where* u *is a unit and* $a;b$ *is a* $CP(*, w)$.

Proof: Taking $C;D = (1000);(0000)$, we obtain that $a;e$ is a $CP(*, \lambda)$. Similarly, $b;f$ is a $CP(*, \lambda)$. Taking $C;D = (1000);(0100)$ we obtain that $(a + xb);(e + xf)$ is a $CP(*, 2\lambda)$. Thus,

$$(a + xb)(a + xb)^* + (e + xf)(e + xf)^* = 2\lambda + x^{-1}(ab^* + ef^*) + x(a^*b + e^*f) = 2\lambda.$$

Therefore,

$$ab^* + ef^* = -x^2(ab^* + ef^*)^*. \tag{3}$$

Taking $C;D = (1010);(010-)$ gives that

$$((1 + x^2)a(x) + (x - x^3)b(x));((1 + x^2)e(x) + (x - x^3)f(x))$$

is a $CP(*, 4\lambda)$, and we calculate

$$\begin{aligned}&((1+x^2)a+(x-x^3)b)((1+x^2)a+(x-x^3)b)^* \\ &+((1+x^2)e+(x-x^3)f)((1+x^2)e+(x-x^3)f)^* \\ &=4\lambda+(x-x^{-3})(ab^*+ef^*)+(x^{-1}-x^3)(a^*b+e^*f)^*=4\lambda.\end{aligned}$$

It follows that

$$ab^*+ef^*=x^2(ab^*+ef^*)^*. \tag{4}$$

Adding (3) and (4) gives $ab^*+ef^*=0$. Thus

$$ab^*=-ef^*. \tag{5}$$

Now, since $a;e$ is a CP, $\gcd(a,e)=1$ (a common factor of degree >0 would violate (1)). Similarly, $\gcd(b,f)=1$, so $\gcd(b^*,f^*)=1$. It follows that $f^*|a$ and $a|f^*$, so $a=uf^*$, where u is a unit. Equivalently, $f=ua^*$.

From (5), $e=-ub^*$. So $bb^*=ee^*$; thus, $a;b$ is a $CP(*,\lambda)$ and $(e,f)=u(-b^*,a^*)$. □

We can now demonstrate the claim from [2].

Theorem 3 *Let $U;V$ be a pair of formal sequences of length m, all of whose entries are elements of the set (of expressions) $\{\mathbf{0}, \pm C, \pm D, \pm C \pm D\}$, and let $\lambda \in \mathbb{Q}$.*

1. *If, whenever symbols C and D are replaced by the sequences of a disjoint $TCP(n,w)$ (and 0_n for $\mathbf{0}$) $U;V$ becomes a $TCP(mn, \lambda w)$, then $U;V$ is equivalent to a pair of the form $(A\otimes C+B\otimes D);(A^*\otimes D-B^*\otimes C)$, where $A;B$ is a $TCP(m,\lambda)$.*
2. *If entries of the form $\pm C \pm D$ do not appear in $U;V$ and, whenever $C;D$ are replaced by a $TCP(n,w)$ (and 0_n for $\mathbf{0}$), $U;V$ becomes a $TCP(mn,\lambda w)$, then $U;V$ is equivalent to a pair of the form $(A\otimes C+B\otimes D);(A^*\otimes D-B^*\otimes C)$, where $A;B$ is a $TCP(m,\lambda)$, with A and B disjoint.*

Proof: In both cases, write

$$\begin{aligned}U=&CA'+DB'\\ V=&CE'+DF'\end{aligned}$$

(C, D are scalars and A', B', E', F' $(0,\pm1)$-vectors here). The sequences obtained by substitution of an actual $TCP(n,w)$ for $C;D$ can be expressed in polynomial form as

$$a(x^n)c(x)+b(x^n)d(x), \quad e(x^n)c(x)+f(x^n)d(x).$$

Observe that knowing a, b, e and f is equivalent to knowing the formal sequences $U;V$.

Thus, $a(x^4), b(x^4), e(x^4), f(x^4)$ and λ satisfy the conditions of Theorem 2; it follows that $e = -ub^*$ and $f = ua^*$, for some unit u. Therefore, the corresponding sequences are equivalent to $(A \otimes C + B \otimes D);(A^* \otimes D - B^* \otimes C)$, as claimed. That A and B are disjoint in part 2 follows from the fact that symbols C and D do not both contribute to any one position in U and V. □

All previously known "products" of TCP's are equivalent to one of one of the two forms covered in Theorem 3, which shows that all such "products" are therefore equivalent to special cases of the product in Theorem 1.

I enumerate here a few anticipated objections and my answers to them.

Objection Theorem 1 does not look the same as the product in [2],

$$\begin{aligned} X &= A \otimes C + B \otimes D; \\ Y &= A \otimes D^* - B \otimes C^*. \end{aligned}$$

Answer As a matter of convenience for our demonstration we have chosen an equivalent product for this article. Obviously $U = X$, and $V = -Y^*$, an equivalent pair.

Objection In [4], some of the products multiply the weight of a TCP by a rational noninteger value of λ, and involve sequences in which $0, \pm C, \pm D, \pm\frac{1}{2}(C \pm D)$ may appear.

Answer Observe that in all such instances, sequences C and D are required to be conjoint. Thus, $C_1;D_1 = \frac{1}{2}(C+D);\frac{1}{2}(C-D)$ is a $TCP(n, \frac{w}{2})$. Using C_1 and D_1 as the fundamental symbols and observing that $C_1 \pm D_1 = C$ or D reveals that this is merely an instance of part 1 of Theorem 3, presented differently.

Objection In [4], mixtures of C, D, C^* and D^* appear in some products and so these cases do not satisfy our definition of a block product.

Answer Nevertheless, this variety is obtained by combinations of block products. In both of the instances of such a mixture given in [4], C^* and D^* appear in the same set of positions in the two sequences. The first of these products is

$$((P+Q)(P-Q)^*QP^*(P-Q)(-P-Q)^*);((-P-Q)(P-Q)^*(-Q)P^*(Q-P)(-P-Q)^*)$$

which is obtained by multiplying (1;1) by pair

$$(\mathbf{0}(P-Q)^*\mathbf{0}P^*\mathbf{0}(-P-Q)^*);((P+Q)\mathbf{0}Q\mathbf{0}(P-Q)\mathbf{0}),$$

which in turn is obtained by shifting and reversing the equivalent pair

$$((-P-Q)\mathbf{0}P\mathbf{0}(P-Q));((P+Q)\mathbf{0}Q\mathbf{0}(P-Q)),$$

a product of $(-0101);(-000-)$ by the disjoint pair $P;Q$. So this product decomposes into two uses of the standard product and some equivalence operations.

Theorem 3 does not address such mixtures, but our method can be generalized to include them. Observe that all sequences $X = C$ or D used in Theorem 2 have the property that X^* is a unit multiple of X; accordingly, C^* and D^*, in a similar expression using these pairs can be eliminated by making appropriate choices for a, b, e and f. The remaining details are left to the reader.

Objection TCP's obtained by interleaving, such as $(A/B);(A/(-B))$, mentioned in [4] and elsewhere, do not appear to be block products.

Answer These are degenerate block products. The blocks are not from A and B, but from the pair (1);(1), obtained by multiplying $(A/0);(0/B)$ (obtained from $A;B$ by shifting and expanding) by this pair of weight 2 and applying equivalence operations.

Theorem 2 does *not* say that, if $(ac+bd);(ec+fd)$ is a CP and $c;d$ is a $TCP(n,w)$ then $e;f$ is equivalent to $(-b^*);a^*$. For a counterexample, $a(x) = 1 - x^4$, $b(x) = -x^6 + x^8$, $c = 1 - x^3$, $d = 1 + x^3$, $e(x) = x^8 - x^7$, $f(x) = 1 + x$ gives the following $TCP(12,16)$:

$$(ac+bd);(ec+fd) = (1-x^3-x^4-x^6+x^7+x^8-x^9+x^{11});(1+x+x^3+x^4-x^7+x^8+x^{10}-x^{11}).$$

The proof of Theorem 2 requires only that a complementary pair is obtained when $c;d$ is any of the pairs (1);(0), (0);(1), (1);(x), $(1+x^2);(x-x^3)$.

3 A new product of TCP's

Theorem 2 suggests a simple generalization of Theorem 1, using polynomial arithmetic.

Theorem 4 *Let* $(a(x) = \sum a_i x^i);(b(x) = \sum b_i x^i)$ *be a* $TCP(m,u)$ *and* $(c(s) = \sum c_i x^i);(d(x) = \sum d_i x^i)$ *be a* $TCP(n,v)$ *such that:*

$$\begin{aligned} &i - j = k - h \textit{ implies } p_i q_j r_h s_k = 0 \textit{ for all } i,j,h,k,\\ &\textit{where } (p,q,r,s) = (a,b,c,d) \textit{ and, for } i \neq j, k \neq h, \textit{ with}\\ &(p,q,r,s) \in \{(a,a,c,c),(a,a,d,d),(b,b,c,c),(b,b,d,d)\}. \end{aligned} \tag{6}$$

Then $f;g = (ac+bd);(a^*d - b^*c)$ *is a* $TCP(m+n-1, uv)$.

Proof: Condition (6) guarantees that f, g are ternary polynomials, because there is at most one term of each degree in the expressions giving these polynomials.

For example, with $(p,q,r,s) = (a,b,c,d)$, (6) says that $i - j = k - h$ implies $a_i b_j c_h d_k = 0$. Since $i - j = k - h$ is equivalent to both $i + h = j + k$ and $k - i = h - j$, this is precisely the condition that the terms of $a(x)c(x)$ are distinct from those of $b(x)d(x)$ and also that the terms of $a^*(x)d(x)$ are distinct from those of $b^*(x)c(x)$.

Taking $(p,q,r,s)=(a,a,c,c)$ ensures that all terms of $a(x)c(x)$ are distinct, and so on. Further,

$$\begin{aligned} ff^*(x)+&gg^*(x)\\ &=(ac+bd)(a^*c^*+b^*d^*)+(a^*d-b^*c)(ad^*-bc^*)\\ &=aa^*cc^*+ab^*cd^*+ba^*dc^*+bb^*dd^*+a^*add^*-a^*bdcc^*-b^*acd^*+b^*bcc^*\\ &=(aa^*+bb^*)(cc^*+dd^*)=uv, \end{aligned}$$

so (1) is satisfied. □

Observe that Theorem 1 is subsumed by Theorem 4: instead of $a(x);b(x)$, use the equivalent, inflated, pair $a(x^n);b(x^n)$, which guarantees that (6) is satisfied, as long as one of the pairs is disjoint.

It is not hard to identify sequences A,B,C,D from which Theorem 4 yields a pair that is primitive according to the definition of [2], which demonstrates that Theorem 4 is more general than Theorem 1 and, therefore, new. The smallest such example is as follows. Let $A;B=(100000100000-000);(0001000000000001)$, a $TCP(16,5)$ and $C;D=(1010-);(10001)$, a $TCP(5,5)$. Condition (6) is satisfied, so Theorem 4 gives

$$\begin{aligned} f(x)&=(1+x^6-x^{12})(1+x^2-x^4)+(x^3+x^{15})(1+x^4)\\ &=1+x^2+x^3-x^4+x^6+x^7+x^8-x^{10}-x^{12}-x^{14}+x^{15}+x^{16}+x^{19};\\ g(x)&=(1+x^{-6}-x^{-12})(1+x^4)-(x^{-3}+x^{-15})(1+x^2-x^4)\\ &=(x^{-15})(-1-x^2-x^3+x^4-x^7+x^9-x^{12}+x^{13}-x^{14}+x^{15}+x^{16}+x^{19}). \end{aligned}$$

The corresponding reduced sequences are

$$F;G=(1011-01110-0-0-11001);(-0--100-0100-1-11001),$$

a $TCP(20,25)$ listed in [1] as primitive.

Suppose $A;B$ is a $TCP(k+2,2k)$ of the form

$$(10S01);(10T0-), \tag{7}$$

where S and T are (±1)-sequences of length $k-2$. Let $X;Y$ be a Golay pair (i.e., a TCP with no 0's) of length n. Take $X'=\frac{1}{2}(X+Y)$ and $Y'=\frac{1}{2}(X-Y)$, a $TCP(n,n)$. Let $C;D$ be obtained by inflating $X';Y'$ by k, and we obtain suitable pairs A,B,C,D for Theorem 4 (but not for Theorem 1), which yields $TCP(2kn+2,2kn)$. In this way we recursively obtain infinitely many pairs of form (7).

Pairs of form (7) can be used several ways to construct Hadamard matrices with two or four circulant matrices. The above recursive construction, then, yields infinite classes of Hadamard matrices.

If the length, $m+n-1$, of the constructed pair in Theorem 4 seems a bit disconcerting next to its weight, uv, which might seem to be too large, in general, one must keep in mind that (6) is a sparseness condition.

4 Checking condition (6)

Condition (6) in Theorem 4 may look a bit daunting for practical checking, but there is a very simple way to look at it, that leads to an effective procedure for doing so.

For polynomials $f(x) = \sum_i f_i x^i$ and $g(x) = \sum_i g_i x^i$, define sets

$$\begin{aligned} \mathrm{Diff}(f,g) &:= \{j-i | g_j f_i \neq 0\}, \text{ and} \\ \mathrm{Aut}(f,g) &:= \{j-i | i \neq j, \text{ and either } f_i f_j \text{ or } g_i g_j \neq 0\}. \end{aligned}$$

Condition (6) can now be restated as follows:

$$\mathrm{Diff}(a,b) \cap \mathrm{Diff}(c,d) = \mathrm{Aut}(a,b) \cap \mathrm{Aut}(c,d) = \emptyset \tag{8}$$

A simple procedure for identifying candidate sequences for Theorem 4, then, would be to record, for all known pairs $f;g$, the sets $\mathrm{Diff}(f,g)$, and $\mathrm{Aut}(f,g)$. Then (8) is easily checked.

For example, the $TCP(16,5)$ considered after Theorem 4 gives

$$\mathrm{Diff}(a,b) = \{\pm 3, \pm 9, 15\}, \quad \mathrm{Aut}(a,b) = \{\pm 6, \pm 12\};$$

while the $TCP(5,5)$ given there gives

$$\mathrm{Diff}(c,d) = \{0, \pm 2, \pm 4\}, \quad \mathrm{Aut}(c,d) = \{\pm 2, \pm 4\}.$$

It is immediate that condition (8) is satisfied. So, then, is (6).

5 A revised version of primitivity

The result of Theorem 4 creates a minor difficulty with the notion of primitive pairs as introduced in [2]: The point of isolating primitive pairs is to determine a basic class of sequences from which all others are obtained by elementary means. Theorem 4 gives a product that is both natural and elementary. I propose to modify the notion of primitivity accordingly, for the sake of economy and theoretical propriety.

It would seem inappropriate to periodically modify our means of classification just because new constructions are found. However, Theorem 4 is probably the ultimate generalization of Theorem 1, at least in one direction. It is unlikely that we will see a further extension of the same variety.

Therefore, let us henceforth define (the new version of) a *primitive* TCP to be a pair that is not equivalent to any obtainable by Theorem 4.

The pairs $S;T$ in Table 1 were listed in [1] as primitive. We show that they are not primitive in the new sense by giving factors $a;b$ and $c;d$ such that

$$s(x);t(x) = (a(x)c(x) + b(x)d(x));x^k(a^*(x)d(x) - b^*(x)c(x)),$$

where x^k is a unit chosen to perform the appropriate shift. With one exception (we must use reversal for the first pair) this factors $S;T$ as it appears in [1]. (We also give the first two pairs in polynomial form $s(x);t(x)$.)

Observe how the supports of the two sequences in the first pair are the same as the supports of those in the fourth pair, as mentioned in [1]. It is evident that the first four pairs, all $TCP(19,25)$'s, have the same pattern of 0's, modulo the operations of reversal and interchanging. Similarly for the second group of four, which are $TCP(20,25)$'s, and the last four, also $TCP(20,25)$'s, but with a different pattern.

Note that in all twelve factorizations, all factors are equivalent $TCP(*,5)$'s.

6 An associative product of TCP's

The Kronecker product of matrices is well-known to be associative. But although the standard product of TCP's is derived from the Kronecker product (of sequences as single-row matrices), is not associative—that is, the product of pair $A;B$ with the product of pairs $C;D$ and $E;F$ is not necessarily the same as the pair obtained by multiplying the product of $A;B$ and $C;D$ with $E;F$. (Nor is the product of Theorem 4.)

There are several versions of the standard product in the literature, equivalent in the sense that they can all be transformed into each other by applying equivalence relations to either the factors or the product obtained. The form of the product in Theorem 4 was chosen for the convenience of stating criterion (6).

The following is an equivalent form of the new product that happens to be associative.

Theorem 5 *Define a product of pairs of (integer) sequences, as follows:*

$$(a;b) \star (c;d) := (ac - bd^*);(ad + bc^*). \tag{9}$$

For pairs $a;b$, $c;d$ and $e;f$:

1. $(1);(0)$ *is a two-sided identity for* $\star$*;*
2. $((a;b)\star(c;d))\star(e;f) = (a;b)\star((c;d)\star(e;f))$ *(so both may be written* $(a;b)\star(c;d)\star(e;f)$*);*
3. *if $a;b$ is a $CP(m,u)$ and $c;d$ is a $CP(n,v)$ then $(s;t) = (a;b)\star(c;d)$ is a $CP(m+n-1,uv)$;*
4. *if $a;b$ and $c;d$ are ternary, then (9) is ternary if and only if $a;b$ and $c;d^*$ satisfy (6).*

Proof: For any pair of Laurent polynomials $a;b$, define

$$M_{a;b} = M_{a;b}(x) := \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}$$
$$= \begin{pmatrix} a(x) & b(x) \\ -b(x^{-1}) & a(x^{-1}) \end{pmatrix},$$

Table 1: TCP's listed as primitive in [1], factored into a;b and c;d as in Theorem 4

$S;T = (11---1--10101000101);(11-00011-0101101-0-)$ $s(x) = 1+x-x^2-x^3-x^4+x^5-x^6-x^7+x^8+x^{10}+x^{12}+x^{16}+x^{18};$ $t(x) = 1+x-x^2+x^6+x^7-x^8+x^{10}+x^{12}+x^{13}+x^{15}-x^{16}-x^{18}$ $a(x);b(x) = x^{10}+x^{16};1-x^3-x^6$ $c(x);d(x) = 1+x^2;1+x-x^2$ (In this instance, reverse S.)
$S;T = (11-00011-0-0--0-101);(11---1--10-0-000-0-)$ $s(x) = 1+x-x^2+x^6+x^7-x^8-x^{10}-x^{10}-x^{12}-x^{13}-x^{15}+x^{16}+x^{18}$ $t(x) = 1+x-x^2-x^3-x^4+x^5-x^6-x^7+x^8-x^{10}-x^{12}-x^{16}-x^{18}$ $a(x);b(x) = -x^{10}-x^{13}+x^{16};1+x^6$ $c(x);d(x) = 1+x^2;1+x-x^2$
$S;T = (11-00011-0-0-101101);(11-11---10-0-000-0-)$ $a(x);b(x) = -x^{10}+x^{13}+x^{16};1+x^6$ $c(x);d(x) = 1+x^2;1+x-x^2$
$S;T = (11-11---10101000101);(11-00011-0101-0--0-)$ $a(x);b(x) = x^{10}+x^{16};1+x^3-x^6$ $c(x);d(x) = 1+x^2;1+x-x^2$
$S;T = (100010100111----1-01);(100110-101-10-01010-)$ $a(x);b(x) = 1+x^6;x^9-x^{12}-x^{15}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (100110-10---010-0-01);(100010100-1-1111-10-)$ $a(x);b(x) = 1+x^3-x^6;-x^9-x^{15}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1010-0101--01-011001);(1011-1----100-0-000-)$ $a(x);b(x) = -x^9+x^{12}+x^{15};1+x^6$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1011-1---11001010001);(1010-01011-0-10--00-)$ $a(x);b(x) = x^9+x^{15};1+x^3-x^6$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1001110-01011-0-1-01);(100111--00-0-001-10-)$ $a(x);b(x) = 1+x^{12};x^3+x^9-x^{15}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1001110-0-0-110-1-01);(1001111-0010-001-10-)$ $a(x);b(x) = 1+x^{12};x^3-x^9-x^{15}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1011-01110-0-0-11001);(1011-0010-001-1--00-)$ $a(x);b(x) = x^3+x^{15};1+x^6-x^{12}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$
$S;T = (1011-0-1-010-0-11001);(1011-0010100111--00-)$ $a(x);b(x) = x^3+x^{15};1-x^6-x^{12}$ $c(x);d(x) = 1+x^4;1+x^2-x^4$

and also

$$M^*_{a;b} := (M_{a^*;b^*})^t = \begin{pmatrix} a^* & -b \\ b^* & a \end{pmatrix}.$$

Observe that $M_{(a;b)\star(c;d)} = M_{a;b}M_{c;d}$. Obviously, $M_{(1);(0)} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an identity for $\star$, and part 2 follows from associativity of matrix multiplication.

Now $a;b$ is a $CP(*, w)$ if and only if $M_{a;b}M^*_{a;b} = wI_2$—thus complementary pairs correspond precisely to orthogonal matrices. Since orthogonality is preserved by multiplication, CP's are preserved by (9), which demonstrates part 3. Part 4 follows from the observation that (9) is equivalent to a pair obtained by by replacing d with $-d^*$ in Theorem 4. □

Theorem 5 tells us that $\star$ makes the set of CP's into a semigroup with unity. The set of TCP's is merely the intersection of this semigroup with the set of ternary pairs.

References

[1] R. Craigen, W. Gibson, S. Georgiou and C. Koukouvinos, *Further explorations into ternary complementary pairs*, Submitted to Electronic J. Combin. (2004).

[2] R. Craigen and C. Koukouvinos, *A theory of ternary complementary pairs*, J. Combinatorial Theory 96 (2001), 358–375.

[3] A. Geramita and J. Seberry, *Quadratic Forms, Orthogonal Designs, and Hadamard Matrices*, vol. 45, Lec. Notes Pure Applied Mathematics, Marcel Dekker Inc., New York and Basel, 1979.

[4] M. Gysin and J. Seberry, *Multiplications of ternary complementary pairs*, Australas. J. Combin. 14 (1996), 165–180.

(Received 13 Aug 2004)