Products of Sums of Squares

Lecture notes for a mini-course at the Universidad de Talca, December 1999.

Daniel Shapiro

Lecture 2: Integer Compositions

Most examples of composition formulas have coefficients in $\{0, 1, -1\}$. It turns out that this restriction is equivalent to having coefficients in $\mathbb{Z}$, the ring of integers. Let's repeat the definition in this integer case.

Lemma 1. *Given r, s, n the following statements are equivalent.*

(1) There exists a formula

$$(x_1^2 + x_2^2 + \cdots + x_r^2) \cdot (y_1^2 + y_2^2 + \cdots + y_s^2) = z_1^2 + z_2^2 + \cdots + z_n^2$$

where each $z_k = z_k(X, Y)$ is a bilinear form in X and Y, with integer coefficients.

(2) There is a bilinear map $f : \mathbb{Z}^r \times \mathbb{Z}^s \to \mathbb{Z}^n$ which satisfies the norm condition $|f(x, y)| = |x| \cdot |y|$.

Our first goal is to explain how these compositions can be described in a discrete, combinatorial way. To avoid numerous subscripts, let A, B, C be the standard, orthonormal bases for $\mathbb{Z}^r, \mathbb{Z}^s, \mathbb{Z}^n$, respectively. For instance every $z \in \mathbb{Z}^n$ can be expressed uniquely as $z = \sum_{c \in C} z_c c$, for $z_c \in \mathbb{Z}$.

Suppose $a \in A$ and $b \in B$. For a normed f as above, $f(a, b)$ is also a unit vector and it is an *integral* linear combination of the basis vectors in C. Therefore it must equal $\pm c$, for one $c \in C$. This $c = \varphi(a, b)$ defines a function on $A \times B$ and $f(a, b) = \pm\varphi(a, b)$. Letting $\varepsilon(a, b)$ be that sign, we obtain functions

$$\varphi : A \times B \to C$$

$$\varepsilon : A \times B \to \{1, -1\}$$

such that $f(a, b) = \varepsilon(a, b)\varphi(a, b)$ for every $a \in A$ and $b \in B$.

The next step is to translate the norm condition on f into statements about these two new functions. As usual, $\langle x, y\rangle$ denotes the scalar product. If $x = \sum_{a\in A} x_a a$ and $y = \sum_{b\in B} y_b b$ then

$$|x|^2 \cdot |y|^2 = \sum_{a,b} x_a^2 y_b^2$$

and this equals

$$|f(x,y)|^2 = |\sum_{a,b} x_a y_b f(a,b)|^2 = \sum_{a,b}\sum_{a',b'} x_a x_{a'} y_b y_{b'} \langle f(a,b), f(a',b')\rangle.$$

Comparing coefficients of x_a^2 we find that if $b \neq b'$ then $\langle f(a,b), f(a,b')\rangle = 0$. Since C is an orthonormal set, this condition becomes: if $b \neq b'$ then $\varphi(a,b) \neq \varphi(a,b')$. The coefficients of y_b^2 provide the symmetric condition: if $a \neq a'$ then $\varphi(a,b) \neq \varphi(a',b)$.

Finally, suppose $a \neq a'$ and $b \neq b'$. Comparing coefficients in this case shows that

$$0 = \langle f(a,b), f(a',b')\rangle + \langle f(a,b'), f(a',b)\rangle.$$

Therefore: $\varphi(a,b) = \varphi(a',b')$ if and only if $\varphi(a,b') = \varphi(a',b)$. Moreover, if these equalities hold, the signs must cancel: $\varepsilon(a,b)\varepsilon(a',b') = -\varepsilon(a,b')\varepsilon(a',b)$.

To display these conditions on φ we tabulate it as an $r \times s$ matrix M. The entry $\varphi(a,b)$ appears in the (a,b) position, where the rows are indexed by A, and the columns by B. Following terminology introduced by Yiu, the entries of M are called "colors". The signs $\varepsilon(a,b)$ can be inserted into the same matrix.

Definition 2. *Suppose M is an $r \times s$ matrix with entries taken from a set of "colors". Let $M(i,j)$ denote the (i,j) entry of M.*

(a) M is an **intercalate** *matrix if:*

(1) The colors along each row (resp. column) are distinct.

(2) $M(i,j) = M(i',j')$ implies $M(i,j') = M(i',j)$.

An intercalate matrix M has **type** *(r,s,n) if it is an $r \times s$ matrix with at most n colors.*

(b) An intercalate matrix M is **signed consistently** *if there exist $\varepsilon_{ij} = \pm 1$ such that*

$$\varepsilon_{ij}\varepsilon_{ij'}\varepsilon_{i'j}\varepsilon_{i'j'} = -1 \quad \textit{whenever} \quad M(i,j) = M(i',j') \quad \textit{and} \quad i \neq i',\ j \neq j'.$$

The "intercalacy condition" (2) says that every 2×2 submatrix of M involves an even number of distinct colors. The sign consistency condition says that every 2×2 submatrix with two distinct colors must have an odd number of minus signs.

For example $\left[\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right]$ is intercalate. (It is essentially the only one of type $(2, 2, 2)$.) Here is a consistent signing for this matrix: $\left[\begin{smallmatrix} +1 & +2 \\ +2 & -1 \end{smallmatrix}\right]$

This path from composition formulas to intercalate matrices is reversible:

Lemma 3. *There is an integer composition formula of size $[r, s, n]$ if and only if there is a consistently signed intercalate matrix of type (r, s, n).*

Here is the connection between the formula for Z and the matrix M:

Color k occurs in $M(i, j)$ $\iff$ Term $x_i y_j$ occurs in z_k.

For example in the signed 2×2 matrix above, color 1 occurs twice: in the $(1, 1)$-position with $+$, and in the $(2, 2)$-position with $-$. This means that $z_1 = +x_1y_1 - x_2y_2$. Similarly, $z_2 = +x_1y_2 + x_2y_1$.

You should check that the following 3×5 matrix is intercalate with 7 colors. Can you find a consistent signing and then write down the corresponding composition formula of size $[3, 5, 7]$?

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 3 & 2 & 5 \\ 2 & 3 & 0 & 1 & 6 \end{bmatrix}$$

The integer composition problem naturally separates into two questions:

(1) When does there exist an intercalate matrix of type (r, s, n)?

(2) Given an intercalate matrix, does it have a consistent signing?

This interpretation of integer composition formulas as signed intercalate matrices was pioneered by Yuzvinsky (1981) and greatly extended by Yiu (1987), (1990) and (1994).

Here are several methods for constructing new intercalate matrices from old ones. In some cases these methods provide consistent signings as well.

Restriction. If M is an intercalate matrix, then any submatrix is also intercalate. On the level of formulas, this construction is the same as setting some of the x_i's and some of the y_j's equal to zero.

Direct Sum. Let A, A' be intercalate matrices of types (r, s, n) and (r, s', n'), and suppose that they involve disjoint sets of colors. Define $M = [A\ A']$. Then M is an intercalate matrix of type $(r, s+s', n+n')$. If A and A' are consistently signed, then so is M. For example, the intercalate $(3, 5, 7)$ written on page 3 above can be expressed as a direct sum: $(3, 4, 4) \oplus (3, 1, 3)$. What is the corresponding construction for composition formulas?

Of course this construction may be done with the rôles of r and s reversed: $(r, s, n) \oplus (r', s, n') \Rightarrow (r+r', s, n+n')$. For example, let A be a consistently signed intercalate $(8, 8, 8)$. Define A', A'', A''' to be copies of A, using disjoint sets of 8 colors. Then the double direct sum is

$$M = \begin{bmatrix} A & A' \\ A'' & A''' \end{bmatrix}.$$

It is a consistently signed intercalate matrix of type (16, 16, 32).

Tensor Product. Suppose $A = (a_{ij})$ and $B = (b_{k\ell})$ are intercalate matrices of types (r_1, s_1, n_1) and (r_2, s_2, n_2) respectively. Then $A \otimes B = (a_{ij}b_{k\ell})$ is an intercalate matrix of type (r_1r_2, s_1s_2, n_1n_2). This $A \otimes B$ is the usual "Kronecker product" of matrices, and the way it is written depends on how the indices (i, j) and (k, ℓ) are ordered. Typically, $A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots \\ a_{21}B & a_{22}B & \dots \\ \vdots & \vdots & \vdots\vdots\vdots \end{bmatrix}$.

For example, starting from $D_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ we obtain

$$D_2 = D_1 \otimes D_1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 01 & 00 & 11 & 10 \\ 10 & 11 & 00 & 01 \\ 11 & 10 & 01 & 00 \end{bmatrix}.$$

The matrix D_1 is the addition table for the group $\mathbb{Z}/2\mathbb{Z}$, and D_2 is the addition table for the group $(\mathbb{Z}/2\mathbb{Z})^2$. Tensoring with D_1 several times yields the $2^t \times 2^t$ matrix D_t, which is exactly addition table for the group $(\mathbb{Z}/2\mathbb{Z})^t$. Of course this group is the same as the t-dimensional vector space over the field of two elements $\mathbb{F}_2$. With this interpretation the intercalacy condition for D_t becomes a trivial property of elements of an $\mathbb{F}_2$-vector space:

$$\text{If } \ i+j = i'+j' \ \text{ then } \ i+j' = i'+j.$$

For larger sizes, writing those bit-strings becomes clumsy, so let's change the notation: in these matrices D_t, every bit-string is translated into an integer using the standard dyadic (base 2) notation. For example,

$$D_2 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{and} \quad D_3 = \left[\begin{array}{cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 3 & 2 & 1 & 0 & 7 & 6 & 5 & 4 \\ \hline 4 & 5 & 6 & 7 & 0 & 1 & 2 & 3 \\ 5 & 4 & 7 & 6 & 1 & 0 & 3 & 2 \\ 6 & 7 & 4 & 5 & 2 & 3 & 0 & 1 \\ 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{array}\right].$$

Define an intercalate matrix to be *dyadic* if it is equivalent to a submatrix of some D_t. The "standard" $r \times s$ dyadic matrix $D_{r,s}$ is defined to be the upper left $r \times s$ corner of some large D_t. For example the 3×5 matrix on page 3 above is exactly $D_{3,5}$. It involves 7 colors.

How many colors are involved in $D_{r,s}$? Surprisingly the answer is exactly the Hopf-Stiefel function $r \circ s$ discussed in Lecture 1.

Lemma 4. *$D_{r,s}$ involves exactly $r \circ s$ colors.*

Proof. See Exercise 2. □

This observation was first made by Yuzvinsky (1981). He went on to conjecture that this is the smallest possible number of colors.

Yuzvinsky's Conjecture 5. *Any $r \times s$ intercalate matrix has at least $r \circ s$ colors.*

Yuzvinsky proved his conjecture in the dyadic case. That result can be restated in terms of subsets of an $\mathbb{F}_2$-vector space. Here $|C|$ stands for the number of elements in a set C, and $A + B$ is the set of all sums $a + b$ for $a \in A$ and $b \in B$.

Proposition 6. *Yuzvinsky's Conjecture is true for dyadic intercalate matrices. Equivalently:*

If $A, B \subseteq V$ are subsets of an $\mathbb{F}_2$-vector space V, then $|A+B| \geq |A| \circ |B|$.

A simple new proof of this result has been found by Eliahou and Kervaire (1998). For the non-dyadic cases Yiu has proved the conjecture when $r, s \leq 16$. This is done using the characterization of small intercalate matrices given in Yiu (1990) and (1994). Larger cases of Yuzvinsky's Conjecture remain unknown.

The classical n-square identities can be generated by the so-called Cayley-Dickson doubling process. For example, an octonion is defined as a pair of quaternions, and the product of two octonions is given by the formula

$$(a, b) \cdot (c, d) = (ac - \overline{d}b,\ da + b\overline{c}),$$

where a, b, c, d are quaternions. This process can be repeated to yield the Cayley-Dickson algebra of dimension 2^t. Its multiplication table is easily seen to be a signed version of our matrix D_t. Of course if $t > 3$ this signing cannot be consistent, by the Hurwitz 1, 2, 4, 8 Theorem. However the case $t = 4$ is useful for discovering some new examples. That signed 16×16 matrix is displayed below. Check that the $[4, 4, 4]$ given at the start of Lecture 1 corresponds to the upper left 4×4 submatrix (with all indices increased by 1).

There are several places where the signing is not consistent. For example, colors 3 and 13 in rows 7, 9 and columns 4, 10 do not satisfy the consistency condition. Those entries are marked in the picture with a little circle (°). (Can you find some other inconsistencies there?) However there are some interesting submatrices which are consistent. Certainly the upper left 8×8 block is consistent because it is the classical 8-square identity coming from the octonions. In fact the $D_{9,16}$ and the $D_{10,10}$ submatrices are also consistently signed. These provide explicit composition formulas of sizes $[9, 16, 16]$ and $[10, 10, 16]$.

We already knew that there is a $[9, 16, 16]$ from Hurwitz-Radon, because $\rho(16) = 9$. But let's look more closely at that submatrix. The upper 8×16 piece is just a direct sum of two copies of the classical 8×8, using disjoint colors. Moreover, the bottom row comes from the top rows of those 8×8's, interchanged and with certain signs reversed. This same procedure works more generally and provides the following "Doubling Construction".

$$
\left[\begin{array}{cccccccc|cccccccc}
+0 & +1 & +2 & +3 & +4 & +5 & +6 & +7 & +8 & +9 & +10 & +11 & +12 & +13 & +14 & +15 \\
+1 & -0 & +3 & -2 & +5 & -4 & -7 & +6 & +9 & -8 & -11 & +10 & -13 & +12 & +15 & -14 \\
+2 & -3 & -0 & +1 & +6 & +7 & -4 & -5 & +10 & +11 & -8 & -9 & -14 & -15 & +12 & +13 \\
+3 & +2 & -1 & -0 & +7 & -6 & +5 & -4 & +11 & -10 & +9 & -8 & -15 & +14 & -13 & +12 \\
+4 & -5 & -6 & -7 & -0 & +1 & +2 & +3 & +12 & +13 & +14 & +15 & -8 & -9 & -10 & -11 \\
+5 & +4 & -7 & +6 & -1 & -0 & -3 & +2 & +13 & -12 & +15 & -14 & +9 & -8 & +11 & -10 \\
+6 & +7 & +4 & -5 & -2 & +3 & -0 & -1 & +14 & -15 & -12 & +13 & +10 & -11 & -8 & +9 \\
+7 & -6 & +5 & +4 & -3^{\circ} & -2 & +1 & -0 & +15 & +14 & -13^{\circ} & -12 & +11 & +10 & -9 & -8 \\
\hline
+8 & -9 & -10 & -11 & -12 & -13 & -14 & -15 & -0 & +1 & +2 & +3 & +4 & +5 & +6 & +7 \\
+9 & +8 & -11 & +10 & -13^{\circ} & +12 & +15 & -14 & -1 & -0 & -3^{\circ} & +2 & -5 & +4 & +7 & -6 \\
+10 & +11 & +8 & -9 & -14 & -15 & +12 & +13 & -2 & +3 & -0 & -1 & -6 & -7 & +4 & +5 \\
+11 & -10 & +9 & +8 & -15 & +14 & -13 & +12 & -3 & -2 & +1 & -0 & -7 & +6 & -5 & +4 \\
+12 & +13 & +14 & +15 & +8 & -9 & -10 & -11 & -4 & +5 & +6 & +7 & -0 & -1 & -2 & -3 \\
+13 & -12 & +15 & -14 & +9 & +8 & +11 & -10 & -5 & -4 & +7 & -6 & +1 & -0 & +3 & -2 \\
+14 & -15 & -12 & +13 & +10 & -11 & +8 & +9 & -6 & -7 & -4 & +5 & +2 & -3 & -0 & +1 \\
+15 & +14 & -13 & -12 & +11 & +10 & -9 & +8 & -7 & +6 & -5 & -4 & +3 & +2 & -1 & -0
\end{array}\right].
$$

Lemma 7. *Any consistently signed intercalate matrix of type (r, s, n) can be enlarged to one of type $(r+1, 2s, 2n)$.*

Of course this Doubling Construction applied to the classical $[8, 8, 8]$-formula provides the $[9, 16, 16]$ just described. If we double again, this time with the rôles of r and s reversed, we obtain a formula of size $[18, 17, 32]$, improving on the earlier one of size $[16, 16, 32]$.

More formulas have been constructed by similar techniques. Many of them can be found by manipulating known intercalate matrices, twisting them in various ways. For a survey of those ideas see Smith and Yiu (1992).

However, it is *far* more difficult to prove that certain sizes of formulas are the best possible. In the case of real coefficients we mentioned results of this type, proved using of the machinery of algebraic topology. For this integer case, Yiu investigated the combinatorial theory of intercalate matrices. (See Yiu (1987), (1990) and (1994).) As a first step, he developed techniques for telling when an intercalate matrix has no consistent signing. One basic result of this sort is given in Exercise 4.

Following the notation $r * s$ introduced in the real case, define $r *_{\mathbb{Z}} s$ to be the smallest n for which there exists a consistently signed intercalate matrix of type (r, s, n). It is not hard to show that

$$r *_{\mathbb{Z}} s = r \circ s \quad \text{whenever} \quad r \leq 9 \text{ or } s \leq 9.$$

Yiu's work culminated in the following theorem. The proof is an elementary, but quite intricate, analysis of small intercalate matrices and their signings. This Theorem determines all the possible sizes of integer composition formulas when $r, s \leq 16$.

Yiu's Theorem 8. *The values of* $r *_{\mathbb{Z}} s$ *for* $10 \leq r, s \leq 16$ *are listed in the following table.*

	10	11	12	13	14	15	16
10	16	26	26	27	27	28	28
11	26	26	26	28	28	30	30
12	26	26	26	28	30	32	32
13	27	28	28	28	32	32	32
14	27	28	30	32	32	32	32
15	28	30	32	32	32	32	32
16	28	30	32	32	32	32	32

For example there is no composition formula of size $[16, 16, 31]$ over $\mathbb{Z}$. As mentioned in the previous lecture, the corresponding result is not known over $\mathbb{R}$.

Exercises.

EXERCISE 1. **A non-dyadic intercalate.** Let $M = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 4 & 5 & 6 & 7 \\ 5 & 4 & 8 & 9 \end{bmatrix}$.
Show that M is intercalate but not dyadic (i.e. not equivalent to any submatrix of D_t).

EXERCISE 2. **Counting the colors.** Prove Lemma 4.
Here's the idea: Let $r \diamond s$ be the number of colors in $D_{r,s}$. This function is symmetric and non-decreasing in each slot, and $2^m \diamond 2^m = 2^m$. Show that $2^m \diamond (2^m + 1) = 2^{m+1}$ and that if $r, s \leq 2^m$ then $r \diamond (s + 2^m) = (r \diamond s) + 2^m$. Prove inductively that $r \diamond s = r \circ s$.

EXERCISE 3. (a) Inside the large matrix given on page 7 above, verify that the upper-left 10×10 submatrix is consistently signed. This gives an explicit $[10, 10, 16]$

(b) Notice how that 10×10 intercalate matrix is built from the 8×8 by adding four 2×2 blocks on the right and symmetrically along the bottom. Repeat that idea, adjoining five 2×2 blocks to the given 10×10. Show that the resulting 12×12 can be consistently signed. This provides a composition of size $[12, 12, 26]$.

EXERCISE 4. **Yiu's inconsistency lemma.** Show that the following matrix M is intercalate of type $(7, 7, 15)$, but it cannot be consistently signed.

$$M = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 9 & 13 \\ 2 & 1 & 4 & 3 & 6 & 10 & 14 \\ 3 & 4 & 1 & 2 & 7 & 11 & 15 \\ 5 & 6 & 7 & 8 & 1 & 13 & 9 \\ 6 & 5 & 8 & 7 & 2 & 14 & 10 \\ 9 & 10 & 11 & 12 & 13 & 1 & 5 \\ 11 & 12 & 9 & 10 & 15 & 3 & 7 \end{bmatrix}.$$

(Hint. If there is a consistent signing, then there is one with "+" along the first row and column, and "+" for one occurrence of each of the remaining colors 7, 8, 10, 12, 14, 15. Derive all the consequences of the consistency. Attach some indeterminate sign to a remaining spot, deduce all the consequences, and repeat. An inconsistency comes up at the end.)

References

[1] S. Eliahou and M. Kervaire, Sumsets in vector spaces over finite fields, *J. Number Theory* **71** (1998) 12-39.

[2] T. L. Smith and P. Yiu, Construction of sums of squares formulae with integer coefficients, *Bol. Soc. Mat. Mexicana* **37** (1992) 479-495.

[3] P. Yiu, Sums of squares formulae with integer coefficients, *Canad. Math. Bull.* **30** (1987) 318-324.

[4] P. Yiu, On the product of two sums of 16 squares as a sum of squares of integral bilinear forms, *Quart. J. Math.* Oxford (2) **41** (1990) 463-500.

[5] P. Yiu, Composition of sums of squares with integer coefficients. In: *Deformations of Mathematical Structures II: Hurwitz-Type Structures and Applications to Surface Physics,* (J. Ławrynowicz, ed.), Kluwer Acad. Publ., 1994, pp. 7-100.

[6] S. Yuzvinsky, Orthogonal pairings of Euclidean spaces, *Michigan Math. J.* **28** (1981) 1-7.

All the topics mentioned in these lectures will appear in greater detail in:

D. Shapiro, *Compositions of Quadratic Forms*, W. deGruyter, Berlin, 2000.

Department of Mathematics
The Ohio State University
Columbus, OH 43210, U.S.A.
email: shapiro@math.ohio-state.edu