Canad. Math. Bull. Vol. **56** (1), 2013 pp. 70–79
http://dx.doi.org/10.4153/CMB-2011-143-x
© Canadian Mathematical Society 2011

An Asymptotic Bound on the Composition Number of Integer Sums of Squares Formulas

P. Hrubeš, A. Wigderson, and A. Yehudayoff

Abstract. Let $\sigma_{\mathbb{Z}}(k)$ be the smallest n such that there exists an identity

$$(x_1^2 + x_2^2 + \cdots + x_k^2) \cdot (y_1^2 + y_2^2 + \cdots + y_k^2) = f_1^2 + f_2^2 + \cdots + f_n^2,$$

with $f_1, \dots, f_n$ being polynomials with integer coefficients in the variables $x_1, \dots, x_k$ and $y_1, \dots, y_k$. We prove that $\sigma_{\mathbb{Z}}(k) \geq \Omega(k^{6/5})$.

1 Introduction

Consider the following problem: given k, what is the smallest n so that there exist *real* polynomials $f_1, \dots, f_n$ in the variables $x_1, \dots, x_k$ and $y_1, \dots, y_k$ satisfying the polynomial identity

$$(1.1) \qquad (x_1^2 + x_2^2 + \cdots + x_k^2) \cdot (y_1^2 + y_2^2 + \cdots + y_k^2) = f_1^2 + f_2^2 + \cdots + f_n^2.$$

Let $\sigma_{\mathbb{R}}(k)$ denote the smallest n for which (1.1) holds. It is known that $\sigma_{\mathbb{R}}(k) = k$ for $k \in \{1, 2, 4, 8\}$. When $k = 1$, we have $x_1^2 y_1^2 = (x_1 y_1)^2$. When $k = 2$, we have

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1 y_1 - x_2 y_2)^2 + (x_1 y_2 + x_2 y_1)^2.$$

Interpreting (x_1, x_2) and (y_1, y_2) as complex numbers $x = x_1 + ix_2$ and $y = y_1 + iy_2$, this formula expresses the property $|x|^2 \cdot |y|^2 = |x \cdot y|^2$ of multiplication of complex numbers. When $k = 4$, there is a similar connection with multiplication of quaternions, when $k = 8$, multiplication of octonions.

This fact is the historical motivation for the study of the problem. Other motivations arise from geometry and topology, and ask whether certain maps between spheres exist (see [10] for survey). A classical result of Hurwitz [2] states that $\sigma_{\mathbb{R}}(k) = k$ can be achieved only for $k \in \{1, 2, 4, 8\}$. This is a special case of a more general theorem of Hurwitz and Radon [9], [3]. The theorem states that $(\sum_{i=1}^{s} x_i^2) \cdot (\sum_{i=1}^{k} y_i^2)$ can be written as a sum of k squares if and only if $s \leq \rho(k)$, where $\rho(k)$ is the so-called Radon–Hurwitz number. In [9], [3], the function $\rho(k)$ was exactly determined. Here are two properties of this function: the equality $\rho(k) = k$ holds only if $k \in \{1, 2, 4, 8\}$,

Received by the editors February 17, 2010; revised November 11, 2010.
Published electronically July 8, 2011.
AMS subject classification: **11E25**.
Keywords: composition formulas, sums of squares, Radon–Hurwitz number.

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

and asymptotically $\rho(k) = \Theta(\log k)$. In contrast, Pfister showed that when k is a power of two, we can always achieve $k = n$ in (1.1), if we allow $f_1, \dots, f_n$ to be real rational functions [8].

Beyond the classical, little is known about the function $\sigma_{\mathbb{R}}(k)$. The immediate bounds are $k \le \sigma_{\mathbb{R}}(k) \le k^2$. One can improve the upper bound to $k \cdot \lceil \frac{k}{\rho(k)} \rceil$ which, together with the estimate on $\rho(k)$, gives

$$k \le \sigma_{\mathbb{R}}(k) \le O\Big(\frac{k^2}{\log k}\Big). \tag{1.2}$$

Using topological means, the lower bound has been increased by James [4], and gives an asymptotic lower bound $\sigma_{\mathbb{R}}(k) \ge \big(2 - o(1)\big)\, k$ (see also [6]). The gap between the lower and upper bounds, however, remains wide open. Most importantly, we do not have a lower bound $k^{1+\epsilon}$, or an upper bound $k^{2-\epsilon}$, for some $\epsilon > 0$. The authors recently showed in [1] that such a lower bound for squares with *complex* coefficients[1] will resolve an important problem in arithmetic circuit complexity.

A simplified version of the problem has been considered, *e.g.*, in [5], [11]; we can require the polynomials $f_1, \dots, f_n$ to have *integer* coefficients. Define $\sigma_{\mathbb{Z}}(k)$ as the smallest n so that (1.1) holds with $f_1, \dots, f_n$ polynomials with integer coefficients. So far, research has mainly focused on computing the exact value of $\sigma_{\mathbb{Z}}(k)$ for small integers k, and little was known about the asymptotic behavior of $\sigma_{\mathbb{Z}}(k)$. In this paper, we prove the following theorem.

Theorem 1.1 $\sigma_{\mathbb{Z}}(k) \ge \Omega(k^{6/5})$.

It is a remarkable fact that the best-known real sum of squares formulas actually involve polynomials with integer coefficients (see [13] and [7]). Namely, the upper bound (1.2) is obtained with $f_1, \dots, f_n$ that have integer coefficients. It is an open question whether the use of real numbers as opposed to integers can decrease n, that is, whether $\sigma_{\mathbb{R}}(k) = \sigma_{\mathbb{Z}}(k)$ holds for every k (and even for $k = 11$).

2 Sums of Squares and Intercalate Matrices

We call a polynomial identity over $\mathbb{R}$ of the form (1.1) a *real sum of squares formula* of type $[k, n]$. If the polynomials $f_1, \dots, f_n$ have only integer coefficients, we call (1.1) an *integer* sum of squares formula.

Let us first show that in the case of real numbers, the polynomials $f_1, \dots, f_n$ are bilinear. (We define $[k]$ to be the set $\{1, \dots, k\}$.)

Lemma 2.1 *If $f_1, \dots, f_n$ are real polynomials that satisfy* (1.1)*, then $f_1, \dots, f_n$ are in fact bilinear forms, that is, f_i are of the form $f_i = \sum_{p,q \in [k]} a_{i,p,q} x_p y_q$.*

Proof It is sufficient to show that $f_1, \dots, f_n$ are homogeneous polynomials of degree one in the variables $X = \{x_1, \dots, x_k\}$, and similarly for $Y = \{y_1, \dots, y_k\}$. For a polynomial g, let $g^{(j)}$ denote the j-homogeneous part of g with respect to the variables X.

[1] Where we require $f_1, \dots, f_n$ to be bilinear.

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

We want to show that $f_i^{(j)} = 0$ whenever $j \neq 1$. Let m be the largest j so that there exists $i \in [n]$ with $f_i^{(j)} \neq 0$. Assume, for the sake of contradiction, that $m > 1$. The maximality of m implies

$$(f_1^2 + \cdots + f_n^2)^{(2m)} = (f_1^{(m)})^2 + \cdots + (f_n^{(m)})^2.$$

The left-hand side is zero, and so the right-hand side is zero as well. Over the real numbers, this implies $f_1^{(m)} = \cdots = f_n^{(m)} = 0$, which is a contradiction. In a similar fashion,

$$(f_1^2 + \cdots + f_n^2)^{(0)} = (f_1^{(0)})^2 + \cdots + (f_n^{(0)})^2,$$

which implies $f_1^{(0)} = \cdots = f_n^{(0)} = 0$. Applying similar reasoning to Y, we conclude that every f_i is a bilinear form as claimed. ■

Following Yiu [11], we phrase $\sigma_{\mathbb{Z}}(k)$ in a more combinatorial language (though we deviate from Yiu's notation). We call a $k \times k$ matrix $M = (M_{i,j})_{i,j\in[k]}$ with nonzero integer entries an *intercalate matrix*, if
(1) $|M_{i,j_1}| \neq |M_{i,j_2}|$, whenever $j_1 \neq j_2$,
(2) $|M_{i_1,j}| \neq |M_{i_2,j}|$, whenever $i_1 \neq i_2$,
(3) if $i_1 \neq i_2$, $j_1 \neq j_2$ and $M_{i_1,j_1} = \pm M_{i_2,j_2}$, then $M_{i_1,j_2} = \mp M_{i_2,j_1}$.
We call $C = C(M) = \{|M_{ij}| : i, j \in [k]\}$ the *set of colors* in M. We say that *M has n colors* if $|C| = n$.

Condition (1) says that no color appears twice in the same row of M, condition (2) says that no color appears twice in the same column of M. Condition (3) then requires that for every 2×2 submatrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of M, either $|a|, |b|, |c|, |d|$ are all different, or the submatrix is of the form

$$\begin{pmatrix} \epsilon_1 a & \epsilon_2 b \\ \epsilon_3 b & \epsilon_4 a \end{pmatrix}$$

where $|a| \neq |b|$ and $\epsilon_i \in \{+1, -1\}$ satisfy $\epsilon_1\epsilon_2\epsilon_3\epsilon_4 = -1$. The following are examples of 2×2 intercalate matrices:

$$\begin{pmatrix} 1 & 2 \\ 3 & -4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & -2 \\ 2 & -1 \end{pmatrix}.$$

The following matrices are *not* intercalate:

$$\begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}.$$

The following proposition relates intercalate matrices and integer sum of squares formulas.

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

Proposition 2.2 *The following are equivalent:*
(1) There exists an integer sum of squares formula of type $[k, n]$*.*
(2) There exists an intercalate $k \times k$ *matrix with* n *colors.*

Proof Let us first show that existence of real sum of squares formula of type $[k, n]$ is equivalent to the following: there exists a family V of k^2 vectors $\mathbf{v}_{i,j} \in \mathbb{R}^n$, $i, j \in [k]$, with the following properties ($\mathbf{v}\cdot\mathbf{u}$ denotes the usual inner product in $\mathbb{R}^n$)

(i) $\mathbf{v}_{i,j}\cdot\mathbf{v}_{i,j} = 1$, for every i, j,
(ii) $\mathbf{v}_{i,j_1}\cdot\mathbf{v}_{i,j_2} = 0$, whenever $j_1 \neq j_2$,
(iii) $\mathbf{v}_{i_1,j}\cdot\mathbf{v}_{i_1,j} = 0$, whenever $i_1 \neq i_2$,
(iv) $\mathbf{v}_{i_1,j_1}\cdot\mathbf{v}_{i_2,j_2} + \mathbf{v}_{i_1,j_2}\cdot\mathbf{v}_{i_2,j_1} = 0$, for every $i_1 \neq i_2$, $j_1 \neq j_2$.

Assume first that we have a real sum of squares formula of type $[k, n]$ with bilinear forms $f_1, \dots, f_n$, as guaranteed by Lemma 2.1. For $\ell \in [n]$ and $i, j \in [k]$, let $v_{i,j}[\ell]$ be the coefficient of $x_i y_j$ in f_ℓ, and let $\mathbf{v}_{i,j} = (v_{i,j}[1], \dots, v_{i,j}[n])$. Equation (1.1) can be written as

$$(2.1) \qquad (x_1^2 + \cdots + x_k^2) \cdot (y_1^2 + \cdots + y_k^2) = \Big(\sum_{i,j\in[k]} \mathbf{v}_{i,j} x_i y_j\Big) \cdot \Big(\sum_{i,j\in[k]} \mathbf{v}_{i,j} x_i y_j\Big).$$

The right-hand side can be written as

$$\sum_{i,j}\big((\mathbf{v}_{i,j}\cdot\mathbf{v}_{i,j})x_i^2 y_j^2\big) + 2\sum_{i,j_1<j_2}\big((\mathbf{v}_{i,j_1}\cdot\mathbf{v}_{i,j_2})x_i^2 y_{j_1} y_{j_2}\big) + 2\sum_{i_1<i_2,j}\big((\mathbf{v}_{i_1,j}\cdot\mathbf{v}_{i_2,j})x_{i_1}x_{i_2}y_j^2\big)$$
$$+\, 2\sum_{i_1<i_2,j_1<j_2}\big((\mathbf{v}_{i_1,j_1}\cdot\mathbf{v}_{i_2,j_2} + \mathbf{v}_{i_1,j_2}\cdot\mathbf{v}_{i_2,j_1})x_{i_1}x_{i_2}y_{j_1}y_{j_2}\big).$$

On the left-hand side, the coefficients of the monomials $x_i^2 y_j^2$, $i, j \in [k]$ are equal to one, and the other monomials have coefficient zero. Since (2.1) is equality of formal polynomials, $\mathbf{v}_{i,j}$ satisfy the four conditions above. Conversely, if we are given vectors with such properties, we can construct a sum of squares formula by means of (2.1).

In the case of *integer* sum of squares formula, the vectors $\mathbf{v}_{ij}$ have integer entries. In the integer case, condition (i) implies a stronger property:

(v) $\mathbf{v}_{ij} \in \{0, 1, -1\}^n$ and $\mathbf{v}_{ij}$ has exactly one nonzero entry.

Here is how a family V with properties (i) through (v) corresponds to an intercalate matrix. Given an intercalate matrix M with colors $\{a_1, \dots, a_n\}$, define V as follows: for every $\ell \in [n]$ and $i, j \in [k]$, define $v_{i,j}[\ell] = \operatorname{sgn}(M_{i,j})$, if $M_{i,j} = a_\ell$, and $v_{i,j}[\ell] = 0$ otherwise. Conversely, given such a family V, define an intercalate matrix with colors $\{1, \dots, n\}$ as $M_{i,j} = v_{i,j}[\ell] \cdot \ell$, where ℓ is the unique coordinate such that $v_{i,j}[\ell] \neq 0$. It is straightforward to verify that the required properties of V, resp. M, are satisfied. ∎

3 The Number of Colors in Intercalate Matrices

We say that two integer matrices M and M' *are equivalent*, if M' can be obtained from M by

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

(1) permuting rows and columns,
(2) multiplying rows and columns by minus one, and
(3) renaming colors, that is, if $\theta\colon \mathbb{Z} \to \mathbb{Z}$ is a one-to-one map such that $\theta(-a) = -\theta(a)$ for every a, we have $M'_{i,j} = \theta(M_{i,j})$, for every $i, j \in [k]$.

Here are two elementary properties of intercalate matrices.

Fact 3.1 *A submatrix of an intercalate matrix is an intercalate matrix.*

Fact 3.2 *If M and M' are equivalent, then M is intercalate if and only if M' is intercalate.*

We say that a $k \times k$ matrix M is *full*, if for every $i \in [k]$, we have $M_{i,i} = 1$.

The following lemma, which will be proved in Section 3.1, is the main step in the proof of our main theorem.

Lemma 3.3 *Let M be a $k \times k$ full intercalate matrix. Then M has at least $\Omega(k^{3/2})$ colors.*

Lemma 3.3 implies the following theorem, which gives Theorem 1.1 by Proposition 2.2.

Theorem 3.4 *Any $k \times k$ intercalate matrix has at least $\Omega(k^{6/5})$ colors.*

Proof Let M be a $k \times k$ intercalate matrix with n colors. We show that M contains a $s \times s$ submatrix $M^{(0)}$ which is equivalent to a full intercalate matrix, with $s \geq k^2/n$. For a color a, let $M_a = \{(i, j) \in [k] \times [k] : |M_{i,j}| = a\}$. The sets M_a form a partition of $[k] \times [k]$ to n pairwise disjoint sets, and hence there exists some a so that $s := |M_a| \geq k^2/n$. Let $M^{(0)}$ be the submatrix of M obtained by deleting rows and columns that do not contain a. Since the color a never occurs twice in the same row or column in $M^{(0)}$, $M^{(0)}$ is $s \times s$ matrix, and we can permute rows and columns of $M^{(0)}$ to obtain a matrix $M^{(1)}$ in which the diagonal entries satisfy $|M^{(1)}_{i,i}| = a$. We can thus multiply some of the rows of $M^{(1)}$ by minus one to obtain a matrix $M^{(2)}$ in which the diagonal entries have $M^{(2)}_{i,i} = a$. Finally, we can rename the colors of $M^{(2)}$ to obtain a matrix $M^{(3)}$ with $M^{(3)}_{i,i} = 1$ for every $i \in [k]$. Altogether, $M^{(3)}$ is a full intercalate matrix equivalent to $M^{(0)}$.

$M^{(0)}$ contains at most n colors. Hence Lemma 3.3 tells us that $n \geq \Omega(s^{3/2})$. Since $s \geq k^2/n$, we have $n \geq \Omega(k^3/n^{3/2})$, which implies $n \geq \Omega(k^{6/5})$. ■

3.1 Number of Colors in Full Intercalate Matrices

The definition of intercalateness immediately implies the following fact.

Fact 3.5 *If M is a full intercalate matrix, then $M_{i,j} = -M_{j,i}$ for every $i \neq j$.*

We now describe a few combinatorial properties of full intercalate matrices.

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

Lemma 3.6 *Assume that M is a 6×6 intercalate matrix of the form*

$$\begin{pmatrix} 1 & 2 & 3 & & & \\ & 1 & 4 & & & \\ & & 1 & & & \\ & & & 1 & 2 & 3 \\ & & & & 1 & b \\ & & & & & 1 \end{pmatrix},$$

where the empty entries are some unspecified integers. Then $b = -4$.

Proof Let $M_{1,4} = c$. By Fact 3.5, M has the form

$$\begin{pmatrix} 1 & 2 & 3 & c & & \\ -2 & 1 & 4 & & & \\ -3 & -4 & 1 & & & \\ -c & & & 1 & 2 & 3 \\ & & & & 1 & b \\ & & & & & 1 \end{pmatrix}.$$

Property (3) in the definition of intercalate matrices implies that $M_{2,5} = M_{3,6} = M_{4,1} = -c$, as $M_{2,1} = -M_{4,5}$ and $M_{3,1} = -M_{4,6}$. Using Fact 3.5, we thus conclude that M has the form

$$\begin{pmatrix} 1 & 2 & 3 & c & & \\ -2 & 1 & 4 & & -c & \\ -3 & -4 & 1 & & & -c \\ -c & & & 1 & 2 & 3 \\ & c & & & 1 & b \\ & & c & & & 1 \end{pmatrix}.$$

Here we have $M_{5,2} = -M_{3,6}$ and hence $M_{5,6} = M_{3,2}$. In other words, $b = -4$. ■

Let M be a $k \times k$ matrix. A triple (i, j_1, j_2) such that $1 \leq i < j_1 < j_2 \leq k$ is called a *position* in M. Let (a, b) be an ordered pair of natural numbers. We say that (a, b) *occurs* in position (i, j_1, j_2) in M, if $|M_{i,j_1}| = a$ and $|M_{i,j_2}| = b$.

Proposition 3.7 *Let M be a full intercalate matrix. Then every pair (a, b) occurs in at most two different positions in M.*

Proof Assume that (a, b) occurs at three distinct positions $\bigl(i(p), j_1(p), j_2(p)\bigr)$, $p \in \{0, 1, 2\}$, in M. By renaming colors, we can assume without loss of generality that $(a, b) = (2, 3)$. We show that M contains 9×9 submatrix M' equivalent to a matrix of the form

$$\begin{pmatrix} A_1 & & \\ & A_2 & \\ & & A_3 \end{pmatrix},$$

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

where

$$A_i = \begin{pmatrix} 1 & 2 & 3 \\ & 1 & c_i \\ & & 1 \end{pmatrix}.$$

This will imply a contradiction: Lemma 3.6 implies that $c_2 = -c_1$, $c_3 = -c_1$ and $c_3 = -c_2$, and hence $c_1 = -c_1$, which is impossible, as $c_1 \neq 0$.

We first show that the nine indices $I = \big\{ i(p), j_1(p), j_2(p) : p \in \{0,1,2\}\big\}$ are all distinct. There are a few cases to consider.

(1) The definition of position guarantees that

$$|\{i(p), j_1(p), j_2(p)\}| = 3$$

for every $p \in \{0,1,2\}$.

(2) Since no color can appear twice in the same row,

$$|\{i(0), i(1), i(2)\}| = |\{j_1(0), j_1(1), j_1(2)\}| = |\{j_2(0), j_2(1), j_2(2)\}| = 3.$$

(3) Since $|M_{i(p),j_1(p)}| = |M_{i(q),j_1(q)}| = 2$, M being intercalate implies

$$|M_{i(p),j_1(q)}| = |M_{i(q),j_1(p)}|.$$

Assume, for the sake of contradiction, that $j_2(p) = j_1(q)$ for some $p \neq q$. Thus, $|M_{i(p),j_1(q)}| = |M_{i(p),j_2(p)}| = 3$, and so $|M_{i(q),j_1(p)}| = 3$. But $j_1(p) \neq j_2(q)$, as $j_1(p) < j_2(p) = j_1(q) < j_2(q)$. This contradicts property (1) in the definition of intercalate matrices, since $|M_{i(q),j_1(p)}| = |M_{i(q),j_2(q)}|$.

(4) Assume, for the sake of contradiction, that $i(q) = j_e(p)$ for some $p \neq q$ and $e = 1,2$. Since M is full, $M_{i(q),j_e(p)} = 1$. As above, we conclude that $|M_{i(p),j_e(q)}| = 1$. But $i(p) \neq j_e(q)$, since $i(p) < j_e(p) = i(q) < j_e(q)$. Thus the color 1 appears twice in the row $i(p)$, which is a contradiction.

Let M' be the 9×9 submatrix of M defined by the set of rows and columns I. Permuting rows and columns of M', we obtain a matrix of the form

$$\begin{pmatrix} B_1 & & \\ & B_2 & \\ & & B_3 \end{pmatrix},$$

where

$$B_i = \begin{pmatrix} 1 & \epsilon_i 2 & \delta_i 3 \\ & 1 & \\ & & 1 \end{pmatrix}$$

and $\epsilon_i, \delta_i \in \{1,-1\}$. Multiplying rows and columns by minus one where appropriate, we conclude that M' is of the desired form. ■

We are now ready for the proof of the lemma.

Proof of Lemma 3.3 There are at least $k^3/8$ different positions in M. From n colors, one can build at most n^2 ordered pairs. Proposition 3.7 implies that any such pair appears in at most two positions in M. Thus, $2n^2 \geq k^3/8$ and so $n \geq \Omega(k^{3/2})$. ■

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

4 Comments and Open Problems

Full Intercalate Matrices

An obvious way to improve the bound in Theorem 1.1 is to improve the exponent $3/2$ in Lemma 3.3. In the current proof, we employ a simple counting argument to show that a matrix M, in which every pair occurs in at most two positions, must have at least $\Omega(k^{3/2})$ colors. This is true for any such matrix (not only intercalate), and remains true if we allow pairs to repeat any constant number of times (not just two). In this sense, we could have saved some work in the proof of Proposition 3.7, for it would be sufficient to show that every pair occurs at most c times in M, for some constant c. Interestingly, if we do not use additional properties of M, the bound $\Omega(k^{3/2})$ is tight, as the following proposition shows.

Proposition 4.1 *There exists $n = O(k^{3/2})$ and sets $S_1, \dots, S_k \subseteq [n]$ such that*

(i) $|S_i| \geq k$, for every $i \in [k]$, but

(ii) for every distinct $i_1, i_2, i_3 \in [k]$, we have $|S_{i_1} \cap S_{i_2} \cap S_{i_3}| \leq 1$.

This means that to improve the bound in Lemma 3.3, we must employ more properties of M.

The proposition will follow from the following construction of the dual of this set system, namely, the sets $T_j \subseteq [k]$ with $j \in [n]$ defined by $T_j = \{i : j \in S_i\}$. It suffices to construct the T_j's, and show that for any two distinct $j, j' \in [n]$, we have $|T_j \cap T_{j'}| \leq 2$. This construction, which is sometimes called a 3-design, may be interesting in its own right. For this we need some notation.

For any field $\mathbb{F}$, let $H(\mathbb{F}) = \mathrm{SL}_2(\mathbb{F})$ be the group of 2×2 matrices of determinant one over $\mathbb{F}$, and let $P(\mathbb{F}) = \mathbb{F} \cup \{\infty\}$ denote the projective line. We will need the cardinalities of these objects: if $\mathbb{F}$ is finite, we have $|H(\mathbb{F})| = (|\mathbb{F}| + 1)|\mathbb{F}|(|\mathbb{F}| - 1)$ and $|P(\mathbb{F})| = |\mathbb{F}| + 1$.

The Mobius action of $H(\mathbb{F})$ on $P(\mathbb{F})$ is defined by $gx = (ax + b)/(cx + d)$, for g the matrix whose rows are (a, b) and (c, d). This action is well known to be 3-transitive: let x_1, x_2, x_3 and y_1, y_2, y_3 be two triples of elements from $P(\mathbb{F})$, then there is a unique $g \in H(\mathbb{F})$ such that $gx_i = y_i$ for every $i \in \{1, 2, 3\}$. In particular, if $x_i = y_i$ for all i, then that g is the identity of $H(\mathbb{F})$. For a subset $R \subseteq P(\mathbb{F})$ and $g \in H(\mathbb{F})$, denote $gR = \{gx : x \in R\}$.

Let q be a prime power. We will use the objects above with the fields of size q and q^2. For $b \in \{1, 2\}$, let $\mathbb{F}_b$ be the field with q^b elements, and let $H_b = H(\mathbb{F}_b)$ and $P_b = P(\mathbb{F}_b)$. We have $P_1 \subseteq P_2$ and H_1 is a subgroup of H_2. Let $C = \{g_1, g_2, \dots, g_n\}$ denote a complete set of left-coset representatives of H_1 in H_2. We assume that the identity of H_2 is in C.

Our set system can now be defined. Let $T_j = g_j P_1$ for all $j \in [n]$. In words, we consider the n shifts of P_1 under the Mobius action of all members of the coset representatives in C.

Let us check the parameters, and then prove the intersection property. We have $k = |P_2| = q^2 + 1$ and $n = (q^2 + 1)q^2(q^2 - 1)/(q + 1)q(q - 1) = q(q^2 + 1) = \Theta(k^{3/2})$.

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

We have $|T_j| = q + 1$ for each j, and symmetry thus implies that each S_i in the proposition has size $|S_i| = q(q + 1) > k$.

Lemma 4.2 *For every two distinct j, j', we have $|T_j \cap T_{j'}| \leq 2$.*

Proof Assume for contradiction that for two distinct coset representatives $g, g' \in C$, we have $|gP_1 \cap g'P_1| \geq 3$. Then there must be an element $h \in C$ (in the same coset as $g^{-1}g'$) such that h maps some three distinct elements $x_1, x_2, x_3 \in P_1$ respectively to three distinct elements $y_1, y_2, y_3 \in P_1$. Let $r \in H_1$ be the unique element such that $ry_i = x_i$ for $i \in \{1, 2, 3\}$. Then rh (which is in the same coset as h) fixes x_1, x_2, x_3, and so must be the identity of H_2. But this means that g, g' are in the same coset, completing the contradiction. ■

Sums of Squares over Gaussian Integers

The sum of squares problem can be posed over any field or a ring. However, one should explicitly require the polynomials $f_1, \dots, f_n$ in (1.1) to be bilinear. This requirement rules out trivial solutions; over $\mathbb{C}$, *e.g.*, every polynomial can be written as sum of two squares. For a ring S, define $\sigma_S(k)$ as the smallest n so that there exists an identity of the form (1.1) with $f_1, \dots, f_n$, bilinear forms over S. Here, one can assume that the characteristic of S is not 2 for otherwise $\sigma_S(k) = 1$. No superlinear lower bound on $\sigma_{\mathbb{F}}(k)$ is known over any field $\mathbb{F}$. It would be especially interesting to have such a bound over an algebraically closed field. Our lower bound, apart from not working over a field, significantly employs the fact that -1 does not have a square root. It would be interesting to remove this restriction.

Problem *Prove a superlinear lower bound on $\sigma_G(k)$, where G is the ring of Gaussian integers.*

References

[1] P. Hrubeš, A. Wigderson, and A. Yehudayoff, *Non-commutative circuits and the sum-of-squares problem.* J. Amer. Math. Soc. **24**(2011), 871–898. http://dx.doi.org/10.1090/S0894-0347-2011-00694-2

[2] A. Hurwitz, *Über die Komposition der quadratischen Formen von beliebig vielen Variabeln.* Nach. Ges. Wiss. Göttingen (1898), 309–316.

[3] ———, *Über die Komposition der quadratischen Formen.* Math. Ann. **88**(1923), 1–25. http://dx.doi.org/10.1007/BF01448439

[4] I. M. James. *On the immersion problem for real projective spaces.* Bull. Amer. Math. Soc. **69**(1967), 231–238. http://dx.doi.org/10.1090/S0002-9904-1963-10930-1

[5] T. Kirkman, *On pluquatemions, and horaoid products of sums of n squares.* Philos. Mag. (ser. 3) **33**(1848), 447–459, 494–509.

[6] K. Y. Lam, *Some new results on composition of quadratic forms.* Invent. Math. **79**(1985), 467–474. http://dx.doi.org/10.1007/BF01388517

[7] T. Y. Lam and T. Smith, *On Yuzvinsky's monomial pairings.* Quart. J. Math. Oxford (2) **44**(1993), 215–237. http://dx.doi.org/10.1093/qmath/44.2.215

[8] A. Pfister, *Multiplikative quadratische Formen.* Arch. Math. **16**(1965), 363–370.

[9] J. Radon, *Lineare scharen orthogonalen matrizen.* Abh. Math. Sem. Univ. Hamburg **1**(1922), 2–14.

[10] D. B. Shapiro, *Compositions of quadratic forms.* de Gruyter Expositions in Mathematics **33**, Walter de Gruyter & Co., Berlin, 2000.

[11] P. Yiu, *Sums of squares formulae with integer coefficients.* Canad. Math. Bull. **30**(1987), 318–324. http://dx.doi.org/10.4153/CMB-1987-045-6

https://doi.org/10.4153/CMB-2011-143-x Published online by Cambridge University Press

[12] ———, *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. http://dx.doi.org/10.1093/qmath/41.4.463

[13] S. Yuzvinsky, *A series of monomial pairings.* Linear and Multilinear Algebra **15**(1984), 19–119. http://dx.doi.org/10.1080/03081088408817582

School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA
e-mail: pahrubes@gmail.com avi@ias.edu amir.yehudayoff@gmail.com