EXTREMAL SET THEORY, CUBIC FORMS ON $\mathbb{F}_2^n$ AND HURWITZ SQUARE IDENTITIES

SOPHIE MORIER-GENOUD AND VALENTIN OVSIENKO

Abstract. We consider a family, $\mathcal{F}$, of subsets of an n-set such that the cardinality of the symmetric difference of any two elements $F, F' \in \mathcal{F}$ is not a multiple of 4. We prove that the maximal size of $\mathcal{F}$ is bounded by $2n$, unless $n \equiv 3 \mod 4$ when it is bounded by $2n+2$. Our method uses cubic forms on $\mathbb{F}_2^n$ and the Hurwitz-Radon theory of square identities. We also apply this theory to obtain some information about Boolean cubic forms and so-called additive quadruples.

1. Introduction and the main results

In this note, we link different subjects: extremal set theory, Boolean cubic forms, non-associative algebras and the Hurwitz theory of "square identities".

Let $\mathcal{F}$ be a family of subsets of $\{1, 2, \ldots, n\}$. For $F, F' \in \mathcal{F}$, define the *symmetric difference*

$$F \oplus F' := \big(F \setminus F'\big) \cup \big(F' \setminus F\big).$$

Denote by $d(F, F')$ the cardinality of $F \oplus F'$, which is sometimes called the *Hamming distance* between the sets F and F'. The following is our most elementary statement.

Theorem 1. *If for every distinct $F, F' \in \mathcal{F}$, the distance $d(F, F')$ is not a multiple of 4, then*

$$|\mathcal{F}| \leq \begin{cases} 2n, & n \equiv 0, 1, 2 \mod 4 \\ 2n+2, & n \equiv 3 \mod 4. \end{cases}$$

This bound is sharp.

Note that replacing 4 by another integer, say 3 or 5, the bound for the size of $\mathcal{F}$ becomes quadratic in n.

Theorem 1 belongs to the vast domain of extremal set theory, see [6] and [20] for an overview. The classical Oddtown Theorem states: *if the cardinality of every $F \in \mathcal{F}$ is odd, and that of every intersection $F \cap F'$ is even, then* $|\mathcal{F}| \leq n$, see [3, 20] and references therein. It is well-known that the bound remains n if one switches "odd" and "even", but if one replaces "odd" by "even" or "even" by "odd", then the bound becomes exponential in n. In Theorem 1, we impose *a priori* no restriction on the members of the family $\mathcal{F}$.

Theorem 1 is related to the Oddtown Theorem by the formula

$$d(F, F') = |F| + |F'| - 2\,|F \cap F'|. \tag{1.1}$$

This suggests an idea to replace intersection of sets by symmetric difference, and parity condition by double parity condition. The Oddtown Theorem directly implies the upper bound $|\mathcal{F}| \leq 2n+2$

ovsienko@math.univ-lyon1.fr, tel:+33666824954.

for every n and $|\mathcal{F}| \leq 2n$ for $n \equiv 0 \pmod 4$. However, it seems that Theorem 1 cannot be entirely deduced from the Oddtown Theorem by elementary methods.

We will use linear algebra over the field $\mathbb{F}_2 = \{0,1\}$, replacing $\mathcal{F}$ by a subset $A \subset \mathbb{F}_2^n$. Symmetric difference of sets then corresponds to sum of vectors. However, unlike the case of the Oddtown Theorem, the proof of Theorem 1 is not reduced to linear algebra. Using cubic forms on $\mathbb{F}_2^n$, we deduce Theorem 1 from the celebrated Hurwitz-Radon theorem [13, 18].

The second main goal of this note is to study invariants of cubic forms on $\mathbb{F}_2^n$. The following statement is a strengthening of Theorem 1.

Theorem 2. *(i) Given a cubic form $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ and a subset $A \subset \mathbb{F}_2^n$, assume that for every $x \neq x' \in A$ one has $\alpha(x + x') = 1$, then $|A| \leq \rho(2^n)$, where ρ is the classical Hurwitz-Radon function.*

(ii) This bound is sharp, at least in the cases $n \equiv 1, 2$ or $3 \pmod 4$.

Classification of cubic forms on $\mathbb{F}_2^n$ is a fascinating problem which is solved only for $n \leq 9$; see [10, 4, 14]. The maximal cardinality of a subset $A \subset \mathbb{F}_2^n$ such that $\alpha\big|_{(A+A)\setminus\{0\}} \equiv 1$ is an interesting characteristic of a cubic form α. It resembles the Arf invariant of quadratic forms, but of course is not enough for classification.

The paper is organized as follows. First, we interpret Hurwitz sum of square identities in terms of extremal set theory int$\mathbb{F}_2^n$. This interpretation uses the Euclidean norm in some non-associative algebras. We then provide a construction of extremal sets reaching the upper bound of Theorem 1.

2. Cubic forms and square identities

2.1. **Hurwitz identities.** A sum of square identity of size $[r, s, N]$ is an identity of the form

$$(a_1^2 + \cdots + a_r^2)\,(b_1^2 + \cdots + b_s^2) = c_1^2 + \cdots + c_N^2,$$

where c_i are bilinear expressions in a_j and b_k with coefficients in $\mathbb{Z}$. In [12], Hurwitz formulated his famous problem to determine all the triples (r, s, N) such that there exists an identity of size $[r, s, N]$. The problem remains widely open, see [19] for a survey.

The *Hurwitz-Radon function* ρ is a function on the set of natural numbers $\rho : \mathbb{N} \to \mathbb{N}$. If $N = 2^n(2m + 1)$, then $\rho(N) = \rho(2^n)$ (i.e., it depends only on the dyadic part of N), and the latter number is given by

$$\rho(2^n) = \begin{cases} 2n+1, & n \equiv \; 0 \quad \mod 4 \\ 2n, & n \equiv \; 1,2 \quad \mod 4 \\ 2n+2, & n \equiv \; 3 \quad \mod 4. \end{cases}$$

The celebrated Hurwitz-Radon theorem [13, 18]; see also [19], is formulated as follows: *there exists an identity of size $[r, N, N]$ if and only if $r \leq \rho(N)$.* This is the only case where the Hurwitz problem is solved.

2.2. **Cubic forms.** A *cubic form* on $\mathbb{F}_2^n$ is a function $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ of the form

$$\alpha(x) = \sum_{1 \leq i \leq j \leq k \leq n} \alpha_{ijk}\, x_i x_j x_k,$$

where $x = (x_1, \ldots, x_n)$ and where $\alpha_{ijk} \in \{0, 1\}$. Note that, over $\mathbb{F}_2$, we have $x_i^2 = x_i$ and therefore every cubic polynomial can be viewed as a *homogeneous* cubic form.

Consider the following cubic function:

$$\alpha_{\mathbb{O}}(x) = \sum_{1\leq i<j<k\leq n} x_ix_jx_k + \sum_{1\leq i<j\leq n} x_ix_j + \sum_{1\leq i\leq n} x_i. \tag{2.1}$$

The function $\alpha_{\mathbb{O}}$ is a *counting function*. This means, it is invariant with respect to the action of the group of permutations on the coordinates and depends only on the *Hamming weight*[1] of x that we denote by $\mathrm{w}t(x)$. More precisely,

$$\alpha_{\mathbb{O}}(x) = \begin{cases} 0, & \text{if } \mathrm{w}t(x) \equiv 0 \mod 4 \\ 1, & \text{otherwise.} \end{cases}$$

2.3. **Twisted group algebras.** Let $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ be a function of two variables. The *twisted group algebra* associated to f is the real 2^n-dimensional algebra denoted by $(\mathbb{R}[\mathbb{F}_2^n], f)$, with basis $\{e_x \,|\, x \in \mathbb{F}_2^n\}$ and the product given by

$$e_x \cdot e_{x'} = (-1)^{f(x,x')}\, e_{x+x'}.$$

This algebra is, in general, neither commutative nor associative. The non-commutativity is measured by the function

$$\beta(x, y) := f(x, y) + f(y, x),$$

while the non-associativity is measured by the function

$$\delta f(x, y, z) := f(y, z) + f(x + y, z) + f(x, y + z) + f(x, y).$$

Many classical algebras, such as the algebras of quaternions $\mathbb{H}$, of octonions $\mathbb{O}$, and, more generally, the Clifford algebras and the Cayley-Dickson algebras, can be realized as twisted group algebras over $\mathbb{F}_2^n$; see [1].

2.4. **From cubic forms to algebra.** There exists an interesting subclass of twisted group algebras characterized by a cubic function in one variable, instead of the function f in two variables. It was introduced and studied in [16], and we give a very short account here.

Given a cubic form α, there exists a (unique modulo coboundary) "twisting function" f satisfying the conditions:

(a) First polarization formula:

$$\beta(x, y) = \alpha(x + y) + \alpha(x) + \alpha(y).$$

(b) Second polarization formula:

$$\delta f(x, y, z) = \alpha(x + y + z) + \alpha(x + y) + \alpha(x + z) + \alpha(y + z) + \alpha(x) + \alpha(y) + \alpha(z).$$

(c) Linearity of f in 2nd variable:

$$f(x, y + y') = f(x, y) + f(x, y').$$

(d) Reconstruction of α from f:

$$f(x, x) = \alpha(x).$$

[1] Recall that the Hamming weight of x is the number of components $x_i = 1$.

The existence of f follows from an explicit formula. We replace every monomial in α according to the following rule:

$$\begin{array}{rcl} x_i x_j x_k & \longmapsto & x_i x_j y_k + x_i y_j x_k + y_i x_j x_k, \\ x_i x_j & \longmapsto & x_i y_j, \\ x_i & \longmapsto & x_i y_i. \end{array} \tag{2.2}$$

where $i < j < k$, and obtain this way a function f in two arguments, satisfying properties (a)-(d).

In particular, the cubic form $\alpha_{\mathbb{O}}$ generates the following the twisting function:

$$f_{\mathbb{O}}(x, y) = \sum_{1 \le i < j < k \le n} (x_i x_j y_k + x_i y_j x_k + y_i x_j x_k) + \sum_{1 \le i \le j \le n} x_i y_j.$$

The obtained twisted group algebras, denoted by $\mathbb{O}_n$, generalize the classical algebra $\mathbb{O}$ of octonions (which is isomorphic to $\mathbb{O}_3$).

Remark 2.1. One cannot choose a polynomial of degree ≥ 4, instead of a cubic function, in order to construct a twisting function f satisfying properties (a)-(d). Indeed, let us apply the differential δ to the equation in property (b). Since $\delta^2 = 0$, one obtains after a short computation:

$$\begin{array}{rl} 0 = & \alpha(x + y + z + t) \\ & +\alpha(x + y + z) + \alpha(x + y + t) + \alpha(x + z + t) + \alpha(y + z + t) \\ & +\alpha(x + y) + \alpha(x + z) + \alpha(x + t) + \alpha(y + z) + \alpha(y + t) + \alpha(z + t) \\ & +\alpha(x) + \alpha(y) + \alpha(z) + \alpha(t). \end{array}$$

This is exactly the condition that α is a polynomial of degree at most 3.

2.5. **From algebra to square identities.** Consider a twisted group algebra $(\mathbb{R}[\mathbb{F}_2^n], f)$, its elements are of the form

$$a = \sum_{x \in \mathbb{F}_2^n} a_x \, e_x,$$

with coefficients $a_x \in \mathbb{R}$. Define the Euclidean norm by

$$\|a\|^2 := \sum_{x \in \mathbb{F}_2^n} a_x^2.$$

Consider two sets $A, B \subset \mathbb{F}_2^n$ and the coordinate subspaces $\mathcal{A}$ and $\mathcal{B} \subset (\mathbb{R}[\mathbb{F}_2^n], f)$:

$$\big\{a \mid a = \sum_{x \in A} a_x \, e_x\big\} \quad \text{and} \quad \big\{b \mid b = \sum_{y \in B} b_y \, e_y\big\}.$$

The condition

$$\|a\|^2 \, \|b\|^2 = \|a \, b\|^2, \tag{2.3}$$

gives a square identity of size $[|A|, |B|, |A + B|]$.

Consider the twisted group algebra $(\mathbb{R}[\mathbb{F}_2^n], f)$ corresponding to a cubic function α as explained in Section 2.4. It turns out that the condition (2.3) can be very easily expressed in terms of the form α.

The following statement is proved in [16, 15, 17].

Lemma 2.2. *The condition* (2.3) *is equivalent to the following: for all $x \neq x' \in A$ and $y \neq y' \in B$ such that $x + x' = y + y'$, one has $\alpha(x + x') = 1$.*

We will apply the above lemma in the case $\alpha = \alpha_{\mathbb{O}}$, and choosing $B = \mathbb{F}_2^n$. The condition on the set A then reads $\mathrm{w}t(x + x')$ is not a multiple of 4, for all distinct $x, x' \in A$.

3. Construction of Hurwitzian sets

In this section, we construct examples of sets $A \subset \mathbb{F}_2^n$ of cardinality $|A| = \rho(2^n)$ satisfying the condition: $\mathrm{w}t(x + x')$ is not a multiple of 4, for all distinct $x, x' \in A$. Such sets were already considered in [15] where they were called *Hurwitzian sets*. In particular, we discuss a relation to the binary Hadamard matrices.

3.1. **Cases $n \equiv 1, 2 \pmod 4$.** In this case, $\rho(2^n) = 2n$. The following choice of a Hurwitzian set is perhaps the most obvious. Choose the following set:

$$A = \{0,\ e_1,\ e_2,\ \ldots,\ e_n,\ e_1 + e_2,\ e_1 + e_3,\ \ldots,\ e_1 + e_n\}\,.$$

For all $x, x' \in A$, the weight of the sum satisfies $\mathrm{w}t(x + x') \leq 3$, and thus $\alpha_{\mathbb{O}}(x + x') = 1$, provided $x + x' \neq 0$. Therefore A is a Hurwitzian set.

Note that the above choice is not unique. However, it is easy to see that the set A is the only Hurwitzian set which is a "shift-minimal downset" according to the terminology of [8].

3.2. **Case $n \equiv 3 \pmod 4$.** In this case, $\rho(2^n) = 2n + 2$ which is the most interesting situation for many reasons.

Consider the element of maximal weight:

$$\omega = (1\,1\,\ldots\,1) = e_1 + \cdots + e_n. \tag{3.1}$$

One can choose the above set A, completed by ω and $e_1 + \omega$. Let us give a more symmetric example.

Choose the set

$$A = \{0,\ \omega,\ e_1,\ e_2,\ \ldots,\ e_n,\ e_1 + \omega,\ e_2 + \omega,\ \ldots,\ e_n + \omega\}\,.$$

The weight of a non-zero element of the sumset $A + A$ can be one of the following four values: $1, 2, n - 1$, or $n - 2$. Since this is never a multiple of 4, we conclude that A is a Hurwitzian set. Moreover, it is not difficult to show that the above set is the only Hurwitzian set invariant with respect to the group of permutations $\mathfrak{S}_n$.

3.3. **Another choice in the case $n \equiv 3 \pmod 8$, relation to the Hadamard matrices.** The case $n \equiv 3 \pmod 8$ is a subcase of the above one. Remarkably, there is a choice of Hurwitzian set based on the classical Hadamard matrices.

Recall that a *Hadamard matrix* is an $m \times m$-matrix H with entries ± 1, such that ${}^tHH = m\mathcal{I}$, where ${}^tH$ is the transpose of H and $\mathcal{I}$ is the identity matrix. It is known that a Hadamard matrix can exist only if $m = 1, 2$ or $m = 4s$; existence for arbitrary s is the classical Hadamard conjecture.

The construction is as follows. We remove the first column of H and construct two $(m-1) \times m$-matrices, H_1, H_2 with entries $0, 1$. The matrix H_1 is obtained by replacing 1 by 0 and -1 by 1, the matrix H_2 is obtained by replacing -1 by 0.

Lemma 3.1. *The rows of H_1 and H_2 form a Hurwitzian set in $\mathbb{F}_2^{4s-1}$, provided s is odd.*

Proof. It follows from the definition of a Hadamard matrix that every sum of two distinct rows of H_1 is of weight $2s$, and similarly for H_2. The sum of a row of H_1 with a row of H_2 is of weight $2s-1$ or $4s-1$. $\square$

Example 3.2. The (unique up to equivalence) 12×12 Hadamard matrix H corresponds to the following 12×11 binary matrices:

$$
H_1 = \begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1\\
0&1&0&1&1&1&0&0&0&1&0\\
0&0&1&0&1&1&1&0&0&0&1\\
1&0&0&1&0&1&1&1&0&0&0\\
0&1&0&0&1&0&1&1&1&0&0\\
0&0&1&0&0&1&0&1&1&1&0\\
0&0&0&1&0&0&1&0&1&1&1\\
1&0&0&0&1&0&0&1&0&1&1\\
1&1&0&0&0&1&0&0&1&0&1\\
1&1&1&0&0&0&1&0&0&1&0\\
0&1&1&1&0&0&0&1&0&0&1\\
1&0&1&1&1&0&0&0&1&0&0
\end{pmatrix}
\qquad
H_2 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&1&1&1&0&1\\
1&1&0&1&0&0&0&1&1&1&0\\
0&1&1&0&1&0&0&0&1&1&1\\
1&0&1&1&0&1&0&0&0&1&1\\
1&1&0&1&1&0&1&0&0&0&1\\
1&1&1&0&1&1&0&1&0&0&0\\
0&1&1&1&0&1&1&0&1&0&0\\
0&0&1&1&1&0&1&1&0&1&0\\
0&0&0&1&1&1&0&1&1&0&1\\
1&0&0&0&1&1&1&0&1&1&0\\
0&1&0&0&0&1&1&1&0&1&1
\end{pmatrix}
$$

(which are related to the extended Golay code). The rows of the matrices H_1 and H_2 constitute a Hurwitzian set in $\mathbb{F}_2^{11}$ of cardinality 24.

An idea of further development is to understand the relations of Theorem 1 to doubly even binary codes. Existence of such relations is indicated by the above example where the celebrated Golay code appears explicitly.

3.4. **Case $n\equiv 0\,(\bmod 4)$.** Recall that $\rho(2^n)=2n+1$ in this case. However, we will show in the next section that there are no Hurwitzian sets in the case. Moreover, we are convinced that a similar situation holds for any cubic form.

Conjecture 1. *Given a Boolean cubic function α on $\mathbb{F}_2^n$ with $n\equiv 0\,(\bmod 4)$, there is no set A such that $\alpha\big|_{(A+A)\setminus\{0\}}\equiv 1$ and $|A|=2n+1$.*

This conjecture is easily verified for $n=4$, as well as for $\alpha=\alpha_{\mathbb{O}}$ and arbitrary n.

4. Proof of Theorems 1 and 2

Let us prove Theorem 2. Fix an arbitrary cubic form α, and let $A\subset\mathbb{F}_2^n$ be a set such that

$$\alpha\,\Big|_{\,(A+A)\setminus\{0\}}\equiv 1.$$

Lemma 2.2 then implies $\|a\|\,\|b\|=\|ab\|$ for all $a\in\mathcal{A}$ and arbitrary b. We therefore obtain a square identity of size $[|A|,\,2^n,\,2^n]$. The Hurwitz-Radon Theorem implies that $|A|\le\rho(2^n)$. This bound is sharp as follows from the constructions of Hurwitzian sets; see Section 3. Theorem 2 follows.

Fixing $\alpha=\alpha_{\mathbb{O}}$, we obtain the statement of Theorem 1 in the cases where $n\equiv 1,2,3\,(\bmod 4)$. In the last case $n=4m$, Theorem 2 implies that $|A|\le 2n+1$. It remains to show that if $n=4m$, then $|A|\le 2n$.

Suppose that $n=4m$ and A is a Hurwitzian set. Every element $x\in A$ can be replaced by $\widetilde{x}=x+\omega$, where ω is the "longest" element (3.1). Indeed, one has

$$x+x'=x+x'+\omega.$$

Replacing x by $\widetilde{x}$ whenever $x_n = 1$, we obtain another Hurwitzian set, $\widetilde{A}$, such that $x_n = 0$ for all $x \in \widetilde{A}$. But then $|\widetilde{A}| \leq \rho(2^{n-1}) = 2n$.

Theorem 1 is proved.

Remark 4.1. Note that the Oddtown Theorem easily implies the upper bound $|\mathcal{F}| \leq 2n+2$ for every n. Indeed, let $\mathcal{F}_0 \subset \mathcal{F}$ be the family of subsets of even cardinality, without loss of generality we assume that $\mathcal{F}_0$ contains the empty set. It follows from the assumption of Theorem 1, that for every $F(\neq \emptyset) \in \mathcal{F}_0$, one has $|F| \equiv 2 \pmod 4$, and for every two elements, $|F \cap F'| \equiv 1 \pmod 2$. The Oddtown Theorem then implies $|\mathcal{F}_0| \leq n+1$. Similarly, $|\mathcal{F}_1| \leq n+1$, where $\mathcal{F}_1$ is the odd subfamily of $\mathcal{F}$.

5. Additive quadruples

Our next statement concerns so-called *additive quadruples*. If $A, B \subset \mathbb{F}_2^n$, four elements $x, x' \in A$, $y, y' \in B$ form an additive quadruple (x, x', y, y') if

$$x + x' + y + y' = 0.$$

We call an additive quadruple *proper* if $x \neq x'$ and $y \neq y'$.

Theorem 3. *Let $A, B \subset \mathbb{F}_2^n$ with $|A| \leq |B|$. If every proper additive quadruple (x, x', y, y') satisfies $\alpha(x + x') = 1$, then $|A + B| \geq \Omega(|A|^{\frac{6}{5}})$.*

Proof. Fix, as above, an arbitrary cubic form α. Suppose that A and B are two subsets of same cardinality $|A| = |B| = r$, and such that for all proper additive quadruples (x, x', y, y') one has $\alpha(x + x') = \alpha(y + y') = 1$. One obtains an identity of size $[r, r, N]$, where $N = |A + B|$. The Hurwitz problem is still open in this particular case and even an asymptotic of the least value $N_{\min}$ as a function of r is not known exactly. However, it is known that asymptotically

$$C_1 \, r^{\frac{6}{5}} \leq N_{\min}(r) \leq C_2 \, \frac{r^2}{\log(r)}.$$

where C_1 and C_2 are some constants. The upper bound follows easily from the Hurwitz-Radon theorem, and the lower bound was recently obtained in [11], which is precisely the statement of Theorem 3. $\square$

The Balog-Szemerédi-Gowers theorem [2, 9], in the $\mathbb{F}_2^n$ case (see [7]) states, roughly speaking, that the sumset $A + B$ grows slowly, provided there are "many" additive quadruples (of order $|A|^3$). The above result is a sort of converse statement.

Acknowledgments. This project was partially supported by the PICS05974 "PENTAFRIZ" of CNRS. We are grateful to John Conway for stimulating discussions.

References

[1] H. Albuquerque, S. Majid, *Quasialgebra structure of the octonions*, J. Algebra **220** (1999), 188–224.
[2] A. Balog and E. Szemerédi, *A statistical theorem of set addition*, Combinatorica **14** (1994), 263–268.
[3] E.R. Berlekamp, *On subsets with intersections of even cardinality*, Canad. Math. Bull. **12** (1969), 471–474.
[4] E. Brier, P. Langevin, *The classification of Boolean cubics of nine variables*, 2003 IEEE Information Theory Workshop, La Sorbonne, Paris, France (2003).
[5] J.-M. Deshouillers, F. Hennecart, A. Plagne, *On small sumsets in* $(\mathbb{Z}/2\mathbb{Z})^n$, Combinatorica **24** (2004), 53–68.
[6] P. Frankl, R.M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), 357–368.

[7] B. Green, T. Tao, *A note on the Freiman and Balog-Szemerédi-Gowers theorems in finite fields*, J. Aust. Math. Soc. **86** (2009), 61–74.
[8] B. Green, T. Tao, *Freiman's theorem in finite fields via extremal set theory,* Combin. Probab. Comput. **18** (2009), 335–355.
[9] W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Funct. Anal. **8** (1998), 529–551.
[10] X.-D. Hou, $\mathrm{GL}(m,2)$ *acting on* $R(r,m)/R(r-1,m)$, Discrete Math. **149** (1996), 99–122.
[11] P. Hrubes, A. Wigderson, A. Yehudayoff, *Non-commutative circuits and the sum-of-squares problem*, J. Amer. Math. Soc. **24** (2011), 871–898.
[12] A. Hurwitz, *Über die Komposition der quadratischen Formen von beliebig vielen Variablen*, Nahr. Ges. Wiss. Göttingen (1898), 309–316.
[13] A. Hurwitz, *Über die Komposition der quadratischen Formen*, Math. Ann. 88 (1922), 1–25.
[14] P. Langevin, *Website*: http://langevin.univ-tln.fr/project.
[15] A. Lenzhen, S. Morier-Genoud, V. Ovsienko, *New solutions to the Hurwitz problem on square identities*, J. Pure Appl. Algebra **215** (2011), 2903–2911.
[16] S. Morier-Genoud, V. Ovsienko, *A series of algebras generalizing the octonions and Hurwitz-Radon identity*, Comm. Math. Phys. **306** (2011), 83–118.
[17] S. Morier-Genoud, V. Ovsienko, *Orthogonal designs and a cubic binary function*, IEEE Trans. Information Theory, **59**:3 (2013) 1583–1589.
[18] J. Radon, *Lineare Scharen orthogonaler Matrizen*, Abh. Math. Sem. Univ. Hamburg **1** (1922) 1–14.
[19] D. Shapiro, Compositions of quadratic forms, Walter de Gruyter & Co., Berlin, 2000.
[20] H. Vu Van, *Extremal set systems with weakly restricted intersections*, Combinatorica **19** (1999), 567–587.

Sophie Morier-Genoud, Sorbonne Universités, UPMC Univ Paris 06, UMR 7586, Institut de Mathématiques de Jussieu- Paris Rive Gauche, Case 247, 4 place Jussieu, F-75005, Paris, France

Valentin Ovsienko, CNRS, Laboratoire de Mathématiques, Université de Reims-Champagne-Ardenne, FR 3399 CNRS, F-51687, Reims, France

E-mail address: sophie.morier-genoud@imj-prg.fr, ovsienko@math.univ-lyon1.fr