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

Sophie Morier-Genoud
Sorbonne Universités, UPMC Univ Paris 06, Institut de Mathématiques de Jussieu-Paris Rive Gauche, UMR 7586, CNRS, Univ Paris Diderot, Sorbonne Paris Cité, F-75005, Paris, France.
sophie.morier-genoud@imj-prg.fr

Valentin Ovsienko
CNRS, Laboratoire de Mathématiques, Université de Reims–Champagne–Ardenne, FR 3399 CNRS, F-51687, Reims, France
valentin.ovsienko@univ-reims.fr

Received: 3/27/14, Revised: 9/15/15, Accepted: 4/28/16, Published: 5/16/16

Abstract

We study cubic forms on $\mathbb{F}_2^n$ using the Hurwitz-Radon theory of square identities. As an application, we obtain the following elementary statement. Given 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, the maximal size of $\mathcal{F}$ is bounded by $2n$, unless $n \equiv 3 \mod 4$ when it is bounded by $2n+2$. 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 $\{1, 2, \dots, n\}$. For $F, F' \in \mathcal{F}$, define the *symmetric difference*

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

Denote by $d(F, F')$ the cardinality of $F \oplus F'$, which is sometimes called the *Hamming distance* between the sets F and F'. We will prove the following 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.

More generally, if we assume that the distance between elements of a family $\mathcal{F}$ is not a multiple of k, then the bound for the size of $\mathcal{F}$ is linear in n only for $k = 2$ and 4. The case $k = 2$ is elementary, but the case $k = 4$ is more surprising.

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. The "even version" of the Oddtown Theorem states that the bound remains n if one switches "odd" and "even." In Theorem 1, we impose no restriction on the elements of the family $\mathcal{F}$. In Section 2, we show that, for certain values of n, Theorem 1 can be easily deduced from the Oddtown Theorem.

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, our 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 main goal of this note is to study invariants of cubic forms on $\mathbb{F}_2^n$. The following result generalizes Theorem 1.

Theorem 2. *Given a cubic form $\alpha : \mathbb{F}_2^n \to \mathbb{F}_2$ and a subset $A \subset \mathbb{F}_2^n$, such that for every $x \neq x' \in A$ one has $\alpha(x + x') = 1$, the cardinality of A satisfies*

$$|A| \leq \rho(2^n),$$

where ρ is the classical Hurwitz-Radon function.

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, which has some similarity with the classical Arf invariant of quadratic forms.

2. Elementary Considerations

We first show that the Oddtown Theorem allows one to obtain the upper bound $|\mathcal{F}| \leq 2n + 2$ for every n, and $|\mathcal{F}| \leq 2n$ for $n \equiv 0 \mod 4$, under the assumptions of Theorem 1. We remark that we failed to deduce Theorem 1 entirely from the Oddtown Theorem, and wonder if this can be done by elementary methods.

We will be using the obvious formula

$$d(F, F') = |F| + |F'| - 2\,|F \cap F'|. \tag{1}$$

Given a family $\mathcal{F}$, write $\mathcal{F} = \mathcal{F}_0 \cup \mathcal{F}_1$, where $\mathcal{F}_0$ (resp. $\mathcal{F}_1$) is the subfamily of sets of even (resp. odd) cardinality. Since the distance is translation-invariant:

$$d(X + Z, Y + Z) = d(X, Y)$$

for all Z, we can assume without loss of generality that $\mathcal{F}_0$ contains the empty set. Every non-empty set $X \in \mathcal{F}_0$ must have $4k+2$ elements for some k, since its distance from the empty set is not a multiple of 4. Formula (1) then implies that two different non-empty even sets must have odd intersection. We conclude by Eventown Theorem that $|\mathcal{F}_0| \leq n+1$. The bound $|\mathcal{F}_1| \leq n+1$ can be obtained by analogous arguments. This implies the upper bound $|\mathcal{F}| \leq 2n+2$.

Moreover, in the case where $n \equiv 0 \mod 4$, the bound can be easily improved to $|\mathcal{F}| \leq 2n$. Indeed, consider the element of maximal cardinality:

$$\omega = \{1, \ldots, n\}. \tag{2}$$

Then for every X and Y

$$d(X,Y) = 0 \mod 4 \qquad \Leftrightarrow \qquad d(\omega \setminus X, Y) = 0 \mod 4,$$

since n is a multiple of 4. Every $X \in \mathcal{F}$ can be replaced by $\omega \setminus X$. Doing this replacement if necessary, we can assume $n \notin X$ for all $X \in \mathcal{F}$, and then apply the bound $|\mathcal{F}| \leq 2n+2$ replacing n by $n-1$.

3. Cubic Forms and Square Identities

In this section, we formulate the classical Hurwitz problem of composition of quadratic forms. This problem remains widely open, and is related to many different areas of mathematics including number theory and topology; see [19] for a survey. We then give a brief account of the method developed in [16, 15, 17], where the Hurwitz problem was tackled using cubic forms on $\mathbb{F}_2^n$.

Square 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 of positive integers (r,s,N) such that there exists an identity of size $[r,s,N]$.

The only case where the Hurwitz problem is solved is the case where $s = N$. The *Hurwitz-Radon function* ρ is a function on the set of natural numbers $\rho : \mathbb{N} \to \mathbb{N}$ defined as follows. Writing $N = 2^n(2m+1)$, one has $\rho(N) := \rho(2^n)$, i.e., the Hurwitz-Radon function depends only on the dyadic part of N. Furthermore,

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

The Hurwitz-Radon theorem [13, 18] states that *an identity of size* $[r, N, N]$ *exists if and only if* $r \leq \rho(N)$.

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:

$$\alpha_{\mathbb{O}}(x) = \sum_{1 \leq i < j < k \leq n} x_i x_j x_k + \sum_{1 \leq i < j \leq n} x_i x_j + \sum_{1 \leq i \leq n} x_i. \tag{3}$$

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* of x, which we denote by $\mathrm{w}t(x)$. More precisely,

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

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 with f is the real 2^n-dimensional algebra on the space $\mathbb{R}[\mathbb{F}_2^n]$, with basis $\{e_x \mid x \in \mathbb{F}_2^n\}$ 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

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

Note that 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].

From cubic forms to algebra. Given a cubic form α, there exists a (unique modulo coboundary) "twisting function" f satisfying the following 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 second variable:

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

(d) Reconstruction of α from f:

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

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

$$\begin{aligned} x_ix_jx_k &\longmapsto x_ix_jy_k + x_iy_jx_k + y_ix_jx_k, \\ x_ix_j &\longmapsto x_iy_j, \\ x_i &\longmapsto x_iy_i. \end{aligned} \tag{4}$$

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 twisting function:

$$f_{\mathbb{O}}(x,y) = \sum_{1\le i<j<k\le n} (x_ix_jy_k + x_iy_jx_k + y_ix_jx_k) + \sum_{1\le i\le j\le n} x_iy_j.$$

The twisted group algebras thus obtained generalize the classical algebra of octonions.

Remark 1. One cannot choose a polynomial of degree ≥ 4 instead of a cubic function 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:

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

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

From algebra to square identities. Consider a twisted group algebra $\mathbb{R}[\mathbb{F}_2^n]$. 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 their coordinate subspaces $\mathcal{A}$ and $\mathcal{B} \subset \mathbb{R}[\mathbb{F}_2^n]$:

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

The condition

$$\|a\|^2\, \|b\|^2 = \|a\, b\|^2, \tag{5}$$

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

Consider the twisted group algebra corresponding to a cubic function α as explained in the previous paragraph. It turns out that the condition (5) can be expressed in terms of α.

Lemma 1 ([16, 15]). *Condition* (5) *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 $\alpha = \alpha_{\mathbb{O}}$, taking B to be $\mathbb{F}_2^n$. The condition on the set A then reduces to $\mathrm{wt}(x + x')$ not a multiple of 4 for all distinct $x, x' \in A$.

4. 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 following condition: $\mathrm{wt}(x + x')$ 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*.

`Cases` $n \equiv 1, 2 \pmod 4$. Here $\rho(2^n) = 2n$. The following choice of a Hurwitzian set is perhaps the most obvious. Define

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

For all $x, x' \in A$, the weight of the sum satisfies $\mathrm{wt}(x + x') \leq 3$, and therefore $\alpha_{\mathbb{O}}(x + x') = 1$, provided that $x + x' \neq 0$. Therefore A is a Hurwitzian set.

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

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

Consider the element of maximal weight $\omega := (1\,1\,\ldots\,1)$. One can then choose the set A in the following symmetric way:

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

Indeed, the weight of a non-zero element of the sumset $A+A$ can be one of the four values $1, 2, n-1$, or $n-2$. Since these are not multiples of 4, we conclude that A is a Hurwitzian set. Moreover, it is not difficult to show that A is the only Hurwitzian set invariant with respect to the group of permutations $\mathfrak{S}_n$.

Remark 2. Let us also mention that, in the case $n \equiv 3 \pmod 8$, there is an interesting choice of Hurwitzian set based on the classical Hadamard matrices.

Case $n \equiv 0 \pmod 4$ Recall that here $\rho(2^n) = 2n+1$. However, we have shown in Section 2 that there are no Hurwitzian sets in the case. 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 $n \equiv 0 \pmod 4$, 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.

5. Proof of Theorems 1 and 2

Let us first 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 1 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 $|A| \le \rho(2^n)$. Theorem 2 follows.

Taking $\alpha = \alpha_{\mathbb{O}}$, we obtain the statement of Theorem 1 in the cases where $n \equiv 1, 2, 3 \pmod 4$. This bound for $|A|$ is sharp, as follows from the constructions of Hurwitzian sets; see Section 4. In the last case $n = 4m$, the bound $|A| \le 2n$ has already been proved in the end of Section 2. Theorem 1 is proved.

6. 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 the same cardinality $|A| = |B| = r$, such that for all proper additive quadruples (x, x', y, y') one has $\alpha(x + x') = \alpha(y + y') = 1$. Then 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. □

The Balog-Szemerédi-Gowers theorem [2, 9] in the $\mathbb{F}_2^n$ case [7, 5] states, roughly speaking, that the sumset $A + B$ grows slowly, provided that there are "many" additive quadruples (of order $|A|^3$). The above result is a form of converse statement.

Acknowledgments. This project was partially supported by the PICS05974 "PENTAFRIZ" of CNRS. We are grateful to John Conway for stimulating discussions, and to Charles Conley for a careful reading of this manuscript.

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, 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.