Latin squares and Hurwitz theorem

Serge Yagunov[1]

Fontanka 27, St.Petersburg, 191023, RUSSIA

Abstract

We give a combinatorial proof of Hurwitz theorem on the sums of squares for polynomials with integer coefficients. It is shown that n-square identities are in one-to-one correspondence with special types of Latin squares. This enables us to give a proof with minimal prerequisites.

Keywords: Latin squares, normed algebras, sums of squares identities.
2010 MSC: 08Axx, 17Axx

One of the oldest results in algebra is the so called Brahmagupta–Fibonacci identity (that was, probably, due to Diophantus of Alexandria), claiming that the product of two sums of two squares is itself a sum of two squares:

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2.$$

A similar identity for four squares was found by Leonard Euler in the 18th century and rediscovered a hundred years later by Hamilton. The case of eight squares was independently settled by Degen (1818), Graves (1843) and Cayley (1845). All attempts to extend these results to other numbers were unsuccessful. Finally, in the end of the 19th century, Hurwitz [2] proved his celebrated theorem which explained that these identities only exist for the sums of $1, 2, 4$, or 8 squares. Later it was established that this discovery has deep philosophical meaning and is connected to algebraic topology, K-theory and many other branches of mathematics. Explanation of some of these links and ample bibliography in the subject the reader can find in the excellent review of Baez [1]. A nice exposition of the classical result can be found in [3].

Some years ago, designing a lecture course on the Bott periodicity theorem, the author decided to make a short informal exposition of the Hurwitz result. Rereading the proof from [3], he found that it contains much linear algebra, obscuring the main idea in the brief explanation. When trying to get rid of as much algebra as possible, he amazingly found that it can be eliminated completely. Finally, the proof became purely combinatorial. The main roles in this new play were played by Latin squares. It is interesting to mention that these nice objects were also studied (for a different purpose) by Leonard Euler.

[1]St.Petersburg Department of Steklov Mathematical Institute

Complete removal of the linear algebra had its price. Playing with Latin squares enables us to prove only the integral version of Hurwitz theorem. However, since all existing sums of squares identities are, in fact, over integers, this price does not seem to be excessive.

Before we start, let us make some remarks about the notation. All mentioned numbers are, by default, integers. $\mathbb{F}_2$ denotes the finite field with two elements. As usual, δ_{ij} stands for Kronecker delta. We also denote by $\oplus$ the operation of modulo 2 addition of integers (exclusive "or" operation performed on the corresponding binary digits of operands).

Let us recall that a Latin square of order $n \geq 1$ is an $n \times n$ array, whose entries (cells) are marked by n different labels (colors) in such a way that every row and every column of the array contains all n labels. We will enumerate rows, columns, and labels with integers from 0 to $n-1$. Also we denote a name of the label attached to cell (i, j) by $[i, j]$.

It is easy to construct Latin squares of arbitrary orders. One starts from the naturally ordered set $[n] = [0, 1, \ldots, n-1]$ and take it as the 0-*th* row of the square. Then, just cyclically shifting this row at every step (setting $[i, j] = i + j \bmod n$), one obtains the whole square.

Some Latin squares have additional symmetries. For example, one can consider squares invariant with respect to a reflection interchanging rows and columns ($[i, j] \leftrightarrow [j, i]$). A less obvious symmetry appears if we consider every cell (i, j) and the attached label $k = [i, j]$ as a triple $\{i, j, k\}$ and require the square to be invariant with respect to all 3-permutations.

This suggests the following way to construct symmetric Latin squares. We start from a symmetric function f with the domain $[n] \times [n] \times [n]$. In addition, we have to assume that for every pair (i, j) the equation $f(i, j, x) = 0$ has a unique solution. Selecting the triples $\{i, j, k\}$ for which $f(i, j, k) = 0$, one obtains a Latin square of order n, having desired symmetry.

Example 1. Setting $f(x, y, z) = x + y + z \bmod n$, one gets a simple example of a symmetric square of order n.

The following example is the most interesting for us in this paper.

Example 2. Let us assume, first, that $n = 2^m$. Take the function $f(x, y, z) = x \oplus y \oplus z$. This function, obviously, satisfies the symmetry condition above. The second condition holds, since $z = x \oplus y$ is, clearly, the unique solution of the equation $f(x, y, z) = 0$. Our choice of n guarantees that in this case $0 \leq x \oplus y < n$. For $m = 1$ our function gives the usual coloring of a 2×2 chess board. For bigger values of m one gets multicolored boards of different sizes. We call these Latin squares *chess squares of order* n and denote them by $c(n)$.

Remark 1. Since every row of a Latin square determines a permutation, one can try to compute the sum of two rows, just composing corresponding permutations. For the chess square of order n this procedure gives a well-defined commutative operation on the set of rows. Taking the 0-*th* row as the origin, one, finally, obtains a vector space of dimension n over the field $\mathbb{F}_2$. Obviously, the same is true for columns.

Besides symmetry, chess squares also have the following nice property.

Definition 1. We call a Latin square *well-painted* if it satisfies the following condition: for any two cells (i, j) and (k, l) the equality $[i, j] = [k, l]$ implies $[i, l] = [k, j]$. We denote the set of all well-painted Latin squares of order n by $\mathcal{L}(n)$.

Lemma 1. *All chess squares are well-painted.*

Proof. We have to show that for indexes i, j, k, l the equality $[i, j] = [k, l]$ implies the equality $[i, l] = [k, j]$. Taking into account that $[i, j] = i \oplus j$, one has: $i \oplus j = k \oplus l$. Then, $i \oplus j \oplus (j \oplus l) = k \oplus l \oplus (l \oplus j)$. Because $x \oplus x = 0$ for any x, it implies: $[i, l] = [k, j]$. □

Our current aim is to completely describe all well-painted squares.

Definition 2. We call two Latin squares *isotopic* if they can be transformed into each other using permutations of rows, columns, and label names. We call the corresponding transformation an *isotopy.*

The isotopy is, obviously, an equivalence relation, so one can consider isotopy classes of Latin squares. Moreover, the isotopy preserves the set of well-painted squares. Therefore, one can define a function ψ, setting $\psi(n)$ to be the number of isotopy classes of well-painted Latin squares of order n.

Theorem 2.

$$\psi(n) = \begin{cases} 1, & \textit{for } n = 2^m; \\ 0, & \textit{otherwise.} \end{cases}$$

In other words, for every non-negative integer m there exists a unique isotopy class of well-painted Latin squares of order 2^m and there are no well-painted squares of other orders.

We prove the theorem in several steps.

Lemma 3. *There are no well-painted Latin squares of odd order.*

Proof. The first two rows of a well-painted square split in rectangles of the form

$$\begin{matrix} \cdots & x & \cdots & y & \cdots \\ \cdots & y & \cdots & x & \cdots \end{matrix}$$

Hence, every row has an even number of entries. □

It is often useful to consider Latin squares that have naturally ordered sets of label names in their 0-th column and 0-th row. These squares are called *normalized.* Every Latin square is isotopic to a normalized one (usually, this normalized form is not unique).

Similarly, using some isotopy one can always transform a given well-painted square into the form:

$$\begin{array}{cccccc} 0 & 1 & \cdots & 2q & 2q+1 & \cdots \\ 1 & 0 & \cdots & 2q+1 & 2q & \cdots \\ \vdots & \vdots & & & & \\ 2p & 2p+1 & & & & \\ 2p+1 & 2p & & & & \\ \vdots & \vdots & & & & \end{array}$$

We will call such squares *normalized well-painted squares.*

The relations $[i,i] = 0$ and $[i,j] = [j,i]$ $(0 \leq i,j < n)$, obviously, hold for normalized well-painted squares of order n.

Lemma 4. *Every normalized well-painted square splits in 2×2 blocks. Each block has either the form*

$$\boxed{\begin{array}{cc} 2k & 2k{+}1 \\ 2k{+}1 & 2k \end{array}} \quad \textit{or} \quad \boxed{\begin{array}{cc} 2k{+}1 & 2k \\ 2k & 2k{+}1 \end{array}}$$

Proof. Let us take a cell with even indexes i and j. Assume, that the number $k = [i,j]$ is also even. Since $[0,j] = j$, $[0,k] = k$, one has: $[i,k] = j$ (see the table below). Similarly, considering the cells $(1,k),(1,j+1),(i,k),(i,j+1)$, one gets: $[1,k] = k+1$, $[1,j+1] = j$, hence $[i,j+1] = k+1$. Transposing the square, one gets: $[i+1,j] = k+1$. Finally, considering the cells $(i,j),(i+1,j),(i,j+1)$, and $(i+1,j+1)$, one has: $[i+1,j+1] = k$. Thus we obtain a block of the first type.

$$\begin{array}{cccccc} 0 & \cdots & k & \cdots & j & j+1 \\ 1 & \cdots & k+1 & \cdots & j+1 & j \\ \vdots & & \vdots & & \vdots & \vdots \\ i & \cdots & j & \cdots & \multicolumn{2}{|c|}{k \quad k+1} \\ i+1 & \cdots & & \cdots & \multicolumn{2}{|c|}{k+1 \quad k} \end{array}$$

For the case of an odd number k we get, as one can easily see, a block of the second type. □

We will denote the set of all well-painted block squares (not necessary normalized) of order n by $B(n)$.

Now we introduce one more type of objects.

Definition 3. Let us start with a well-painted Latin square of order n and endow each cell with an additional $+$ or $-$ label, in such a way that the following property holds. *Vertices of every rectangle of the form*

$$\begin{array}{ccccccc} \cdots & a & \cdots & b & \cdots \\ & \vdots & & \vdots & \\ \cdots & b & \cdots & a & \cdots \end{array}$$

should be labeled with an even number of + (and −) labels. We will call these squares *signed squares* and denote their set by $\mathcal{L}^{\pm}(n)$.

There exist natural maps $I\colon \mathcal{L}(n) \to \mathcal{L}^{\pm}(n)$, just assigning the + sign to every cell and $F\colon \mathcal{L}^{\pm}(n) \to \mathcal{L}(n)$, forgetting the sign labels.

Every isotopy acting on $\mathcal{L}(n)$ lifts to a transformation on $\mathcal{L}^{\pm}(n)$. We call two squares in $\mathcal{L}^{\pm}(n)$ isotopic if they can be transformed into each other after performing a lifted isotopy transformation and a chain of the following operations:

- κ_i changes signs assigned to all cells that have label i;
- λ_i changes all signs in row number i;
- μ_i changes all signs in column number i.

It is easy to check that the introduced isotopy of signed Latin squares is an equivalence relation. So, we can consider classes of isotopy and define the function $\psi^{\pm}$ in a similar way as before, setting $\psi^{\pm}(n)$ to be the number of isotopy classes of signed squares of order n.

Lemma 5. *There is a natural bijection between the set $B(2n)$, introduced after Lemma 4 and the set $\mathcal{L}^{\pm}(n)$. Moreover, every isotopy of signed squares can be lifted to an isotopy on block squares.*

Proof. For a given square in $B(2n)$ we must construct a signed well-painted Latin square of order n. Consider the cell of the initial square with index $(2i, 2j)$. It belongs to a block that contains labels $2k$ and $2k+1$ for some number k. In the new signed square of order n we assign:

$$[i,j] = \begin{cases} +k, & \text{if} \quad [2i,2j] = 2k; \\ -k, & \text{if} \quad [2i,2j] = 2k+1. \end{cases}$$

(On the right-hand side we have the labels of the initial square of order $2n$.) In order to construct the inverse map, one should send labels $+k$ and $-k$ to blocks

2k	2k+1
2k+1	2k

and

2k+1	2k
2k	2k+1

correspondingly. One can easily check that these maps are well-defined and mutually inverse. Moreover, one can see that the map from $\mathcal{L}^{\pm}(n)$ to $B(2n)$ preserves the isotopy. It is sufficient to check that all transformations κ, λ and μ can be realized by some isotopies in $B(2n)$. For example, the isotopy λ_i corresponds to the isotopy that swaps rows $2i$ and $2i+1$. □

Corollary 6. *One has: $\psi(2n) \leq \psi^{\pm}(n)$.*

Proof. The map $\mathcal{L}^{\pm}(n) \to B(2n)$ defined above determines a map of isotopy classes. Since every square in $\mathcal{L}(2n)$ is isotopic to some (normalized) square in $B(2n)$, this isotopy class map is a surjection. □

Lemma 7. *Every square from the set $F^{-1}(c(2^m))$ can be transformed to the form $I(c(2^m))$, using only operations κ, λ, and μ, introduced above.*

Proof. Using operations λ_i (resp. μ_i), one can arrange that every sign in the 0-th row (resp. column) is "+". Consider now the following sequence of cells:

$$(1,2),(1,4),\ldots,(1,n-2),(2,4),(2,8),\ldots,(2,n-4)\ldots,(n/4,n/2).$$

A general entry of this list has the form $(2^i, j2^{i+1})$, where $0 \le i \le m-2$ and $1 \le j \le 2^{m-i-2}$. One can easily check that the choice of signs assigned to cells $(1,2),\ldots,(2^i, j2^{i+1})$ from the list, completely determines all the signs assigned to cells in three subsquares of order 2^{i+1} with diagonals:

$$\begin{array}{ccc}(0,b) & - & (a,a+b),\\ (b,0) & - & (a+b,a),\\ (b,b) & - & (a+b,a+b),\end{array}$$

where $a = 2^{i+1}-1$ and $b = j2^{i+1}$. Hence the choice of signs in the whole list above determines all signs in the square. Therefore, it suffices to show that using only transformations $\kappa, \lambda,$ and μ, we can change every sign attached to a listed cell to $+$.

Consider some cell $(2^i, j2^{i+1})$ from the list. Let $q = [2^i, j2^{i+1}] = 2^i \oplus j2^{i+1} = 2^i(2j+1)$. Denote $\omega_q := \kappa_q \circ \lambda_q \circ \mu_q$. Then, one can see that the transformation $\omega_q \circ \omega_{q+1} \circ \cdots \circ \omega_{q+2^i-1}$ changes the sign of the cell $(2^i, 2j2^i)$ and affects no cells in the list before. We should also mention that operations $\omega_\bullet$ preserve signs in cells $(*,0)$ and $(0,*)$. □

Now we can complete the proof of Theorem 2. Let us take an integer n such that $\psi(2n) > 0$. By Corollary 6, one has: $\psi(2n) \le \psi^{\pm}(n)$, hence $\psi^{\pm}(n) \ge 1$ and $\psi(n) > 0$. (The equality $\psi(n) = 0$ would trivially imply $\psi^{\pm}(n) = 0$.) This observation, together with Lemma 3 implies, in particular, that $\psi(2^m l) = 0$, provided that $l > 1$ is odd. Hence we can set $n = 2^m$. By Lemma 1 we know that $\psi(2^m) > 0$. Suppose that m is the minimal number such that $\psi(2^m) > 1$. Obviously, $m > 0$. By the choice of m, $\psi(2^{m-1}) = 1$, hence, every signed square of order 2^{m-1} is isotopic to some element of the set $F^{-1}(c(2^{m-1}))$. By Lemma 7, every element of $F^{-1}(c(2^{m-1}))$ is isotopic to $I(c(2^{m-1}))$, which implies that $\psi^{\pm}(2^{m-1}) = 1$. Applying, again, Corollary 6, we have: $\psi(2^m) \le \psi^{\pm}(2^{m-1}) = 1$, that leads to a contradiction and completes the proof. □

In the proof of Theorem 2 we considered well-painted squares endowed with additional sign labels in such a way that every special type rectangle should have an even number of $+$ labels in its vertices. Let us now consider the opposite case.

Definition 4. We call a Latin square *polarized* if it is well-painted and its cells are supplied (in addition to the number labels) with either $+$ or $-$ signs in such a way that *vertices of every rectangle of the form*

$$\begin{array}{ccccc} \cdots & a & \cdots & b & \cdots \\ & \vdots & & \vdots & \\ \cdots & b & \cdots & a & \cdots \end{array}$$

are labeled with an odd number of + (and −) labels.

In the table below one can see an example of a polarized square of order eight containing polarized subsquares of all possible smaller orders.

+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
+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

Proposition 8. *There are unique isotopy classes of polarized squares of orders* $1, 2, 4, 8$ *and this list is exhaustive.*

Proof. Since every well-painted Latin square is isotopic to the chess square $c(n)$ for some n, it is sufficient to consider only the squares that belong to $F^{-1}(c(n))$.

Set $\{i, j\} = 1$ if the cell (i, j) is marked by the minus sign and $\{i, j\} = 0$ otherwise. Then, polarization conditions can be rewritten as linear equations over the field $\mathbb{F}_2$. The whole system reads as follows:

$$\{i, j\} + \{i, k\} + \{l, j\} + \{l, k\} = 1, \text{ provided that } i \oplus j = k \oplus l.$$

Let us verify that there are no polarized squares of order 16. Since every polarized chess square of order 2^m contains (as subsquares) polarized chess squares of orders $1, 2, \ldots, 2^{m-1}$ (see, for example, the table above), this will complete the proof. Assume that such a square exists.

Changing, if necessary, signs in some rows and columns, one can get: $\{j, 0\} = \{0, j\} = 0$ for $0 \leq j < 16$. By polarization relations, one has: $\{0, 0\} + \{i, 0\} + \{0, i\} + \{i, i\} = 1$, which implies that $\{i, i\} = 1$ for $i > 0$. Similarly, one can show that $\{i, j\} + \{j, i\} = 1$ for $i \neq j$ and $i, j > 0$.

Let us now compute the sum

$$S = \{4, 5\} + \{4, 6\} + \{5, 6\} + \{9, 8\} + \{10, 8\} + \{10, 9\}$$

in two different ways.

Firstly, one has:

$$\begin{array}{rlll} \{4,5\} &= \{4,1\}+\{0,1\}+\{0,5\}+1 & \text{since} & 4\oplus 5 = 0\oplus 1 = 1 \\ \{4,6\} &= \{4,1\}+\{3,1\}+\{3,6\}+1 & & 4\oplus 6 = 3\oplus 1 = 2 \\ \{5,6\} &= \{5,0\}+\{3,0\}+\{3,6\}+1 & \vdots & \vdots \\ \{9,8\} &= \{9,0\}+\{1,0\}+\{1,8\}+1 & & \\ \{10,8\} &= \{10,3\}+\{1,3\}+\{1,8\}+1 & & \\ \{10,9\} &= \{10,3\}+\{0,3\}+\{0,9\}+1 & & \end{array}$$

Adding these equalities and taking into account that $\{j,0\} = \{0,j\} = 0$, one gets the relation: $S = \{3,1\}+\{1,3\} = 1$.

On the other hand:

$$\begin{aligned} \{4,5\}+\{9,8\} &= \{4,8\}+\{9,5\}+1 \\ \{4,6\}+\{10,8\} &= \{4,8\}+\{10,6\}+1 \\ \{5,6\}+\{10,9\} &= \{5,9\}+\{10,6\}+1 \end{aligned}$$

Again, adding the equalities, one gets: $S = \{5,9\}+\{9,5\}+1 = 0$. Contradiction.

Examples of polarized squares of orders $1, 2, 4$, and 8 were given above. The statement that two polarized chess squares of the same order are isotopic can be proven using the same technique as in the proof of Lemma 7 and is left to the reader. □

Remark 2. One can easily check that for chess squares of order n the polarization conditions give a system of $\frac{1}{4}n^2(n-1)$ linear equations over $\mathbb{F}_2$ with n^2 variables. Certainly, many of these equations are linearly dependent, that does not allow us to make the exact estimation of the system rank. However, it gives some informal explanation of why polarized squares of order ≥ 16 might not exist and makes the previous proof less artificial.

Theorem 9 (Hurwitz)**.** *The family $G_1, G_2, \ldots, G_n \in \mathbb{Z}[x_1,\ldots,x_n,y_1,\ldots,y_n]$ of homogeneous polynomials of degree 1 separately on $\{x_\bullet\}$ and $\{y_\bullet\}$ that satisfies the condition*

$$\left(\sum_{i=1}^n x_i^2\right)\left(\sum_{i=1}^n y_i^2\right) = \sum_{i=1}^n G_i\left(x_1\ldots,x_n,y_1,\ldots,y_n\right)^2$$

exists if and only if $n \in \{1,2,4,8\}$. Moreover, renumbering the sequences $\{x_\bullet\}$, $\{y_\bullet\}$, and $\{G_\bullet\}$ and changing, if necessary, the signs of $x_\bullet$ and $y_\bullet$ in the main equality, one can transform every two such families of the same length into each other.

Proof. We are going to build a one-to-one correspondence between the set of polynomial families having the desired property and the set of polarized chess squares. Writing $G_i = \sum_{p,q} a_i^{pq} x_p y_q$ and substituting $x_p = \delta_{kp}$ and $y_q = \delta_{ql}$ in the main equality, we see that $\sum_i (a_i^{kl})^2 = 1$. Since all the polynomial coefficients are integers, the sequence $\{a_\bullet^{kl}\}$ consists of only one non-zero element equal to ± 1.

Let us now construct an $n \times n$ array, setting $[k, l] = \text{sign}(a_i^{kl})i$ for the only non-zero element a_i^{kl} in the sequence $\{a_\bullet^{kl}\}$. Expanding theorem's main equality one can see that it holds if and only if the resulting array happens to be a polarized Latin square of order n. Proposition 8 now implies the theorem. $\square$

Remark 3. It also seems interesting to figure out the algebraic meaning of non-polarized well-painted squares. They give us a way to construct arbitrary long polynomial sequences satisfying the sums of squares equality over fields of characteristic 2. Unfortunately, this result seems to be useless, since in fields of characteristic 2 the sum of two squares is always a square.

Acknowledgement

The author is in debt to to Anton Petrunin and Nikolai Vavilov who convinced him to publish the current observation. He is deeply grateful to the referee, whose valuable comments helped to improve the paper. He also thanks the "Russian Science Foundation" grant 14-11-00456 for financial support during his work.

Finally, I should say that this paper would never be published without prompt and excellent help of doctor Michail L.Gordeev (M.D., Ph.D) and all his team, to whom I am grateful from the bottom of my heart.

Bibliography

[1] J.Baez, The Octonions. *Bull. Amer. Math. Soc.* **39** (2002), 145–205

[2] A.Hurwitz, Über die Composition der quadratichen Formen von beliebig vielen Variabeln. Werke, Band II, Basel 1932, 565–571.

[3] I.Kantor and A.Solodovnikov, Hypercomplex numbers. An elementary introduction to algebras. (Translated from the Russian) Springer-Verlag, New York, 1989. x+169 pp.