An. Şt. Univ. Ovidius Constanţa Vol. 19(2), 2011, 89–100

Small solutions to systems of polynomial equations with integer coefficients

Mihai Cipu

Abstract

The paper discusses a series of conjectures due to A. Tyszka aiming to describe boxes in which there exists at least one solution to a system of polynomial equations with integer coefficients. A proof of the bound valid in the linear case is given.

1 Two basic questions

When facing systems of equations whose solutions are hard to determine, one is satisfied to determine (or at least estimate) the number and the size of solutions. A satisfactory answer could be an algorithm, if a definite formula is unavailable. These questions are completely answered only for univariate polynomials over the ring of integers or the field of rational, real or complex numbers. Many important results, such as Falting's result on rational points on irreducible algebraic curves of genus at least 2, ensures the finiteness of the solution set to specific systems without giving any hint on its cardinality.

A great deal of mathematics appeared as a result of attempts to solve such problems. One of the first results of the kind is Bézout's theorem, according to which the total number of intersection points of two plane projective curves that have no common component with coordinates in an algebraically closed field, counted with their multiplicities, is equal to the product of degrees of the two curves. More generally, the product of degrees is an upper bound for the number of solutions to n polynomials in n variables, provided that the system has finitely many solutions. D. N. Bernshtein [3] and A. G. Kushnirenko [13]

Key Words: systems of polynomial equations; quantifier elimination; Hilbert's tenth problem; Waldi's determinantal inequality
Mathematics Subject Classification: 12D10; 15A06; 15A15; 15A45

proved that the number of isolated roots in the torus of a polynomial system is at most the mixed volume of the Newton polytopes of the given polynomials. Improved bounds take into account various refined (combinatorial, topological, numerical) invariants of the system under study. Thus, a theorem of Blum, Cucker, Shub, Smale [4] says that if a system of m polynomials of total degree at most d in n variables has real solutions then the number of connected components of the real variety is at most $d(2d-1)^{n-1}$. In particular, if a system of quadratic polynomials has finitely many real solutions then their number is at most $2 \cdot 3^{n-1}$.

A typical result answering an instance of the second problem is Siegel's lemma which assures one that a linear system of m equations in n unknowns $Ax = 0$ with the entries of the integer matrix at most M in module has a nontrivial integer solution x whose entries have absolute value at most $1 + (nM)^{m/(n-m)}$, provided of course that $m < n$. Bombieri and Vaaler [5] greatly improved and extended this result to rings of integers of number fields.

Other answers to the basic questions are given in terms of various numerical information extracted from the given equations. For instance, A. Baker [1] showed that the integer solutions to an elliptic equation $y^2 = f(x)$, with $f(X) = X^3 + aX + b \in \mathbb{Z}[X]$, satisfy

$$\max\{|x|, |y|\} \leq \exp\left(\left(10^6\, H(f)^{10^6}\right)\right).$$

Here, $H(f) := \max\{1, |a|, |b|\}$ is the height of f. This bound has been considerably improved and generalised to rings of integers of number fields K (see, e.g., [7]). In this framework, there are known bounds that depend on the degree of K over $\mathbb{Q}$ and on the discriminant of f. For instance, Y. Bugeaud [8] gives an upper bound for the size of integer solutions depending only on the prime factors of the discriminant of f, provided the coefficients a and b are coprime and the discriminant is sufficiently large. Such a variant is important because the discriminant can be arbitrarily smaller than the height.

Since Tarski it is known that the theory of real closed fields is decidable. Collins' cylindrical algebraic decomposition algorithm allows one to check the consistency over the real field of each system $\mathcal{E}$ of polynomial equations with integer coefficients and, for such a compatible system, to determine a positive a such that there exists a solution in the hypercube $[-a, a]^n$. The value a is unpredictable, it is only known when the algorithm ends, and a priori depends on the considered system.

A qualitatively different result is due to Vorobjov [19], who succeeded to prove that there exists a bivariate polynomial H such that any system $\mathcal{E}$ solvable over $\mathbb{R}$ has a real solution with

$$|x_j| \leq 2^{H(r,L)}, \quad j = 1, 2, \ldots, n,$$

where

$$d = \sum_{i=1}^{m} \deg(f_i), \quad r = \binom{n+2d}{n},$$

and L is the maximum of the bit-sizes of the coefficients. Many similar results are nowadays known (see, for instance, [2]). However, since the bound denoted above H works for all compatible systems over the real field, it is possible that for specific classes of systems much lower bounds exist. Strikingly simple, yet tight, bounds have been stated by A. Tyszka.

2 Conjectural answers

In the rest of the paper, A denotes a subring of the field of complex numbers $\mathbb{C}$ and n a positive integer.

In a series of papers (among which [15, 16, 17, 18]), Tyszka discusses the following conjectural answers to the basic questions.

Conjecture $\mathcal{N}_n(A)$**.** *Let $\mathcal{S}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ or $x_i = x_j \cdot x_k$ for some i, j, k between 1 and n. If $\mathcal{S}$ has finitely many solutions in A then their number is at most 2^n.*

It is easily seen that the bound is sharp for all $n \geq 1$: there are precisely 2^n solutions to the system $x_1 \cdot x_1 = x_1, \ldots, x_n \cdot x_n = x_n$.

Conjecture $\mathcal{C}_n(A)$**.** *Let $\mathcal{S}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ or $x_i = x_j \cdot x_k$ for some i, j, k between 1 and n. If $\mathcal{S}$ has a solution in the ring A then there exists $(x_1, x_2, \ldots, x_n) \in A^n$ satisfying the system and $|x_i| \leq 2^{2^{n-2}}$ for $i = 1, 2, \ldots, n$.*

A stronger conjecture is found in [17] and [18].

Conjecture $\mathcal{F}_n(A)$**.** *Let $\mathcal{S}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ or $x_i = x_j \cdot x_k$ for some i, j, k between 1 and n. If $\mathcal{S}$ has only finitely many solutions in A then any solution $(x_1, x_2, \ldots, x_n)$ in A satisfies*

$$|x_j| \leq 2^{2^{n-1}}, \quad j = 1, 2, \ldots, n.$$

The bound on the size of solutions is sharp for $n > 1$, as the example of the system

$$x_1 \cdot x_1 = x_2,\ x_1 + x_1 = x_2,\ x_2 \cdot x_2 = x_3,\ \ldots,\ x_{n-1} \cdot x_{n-1} = x_n$$

with unique nonzero solution

$$\left(2, 2^2, 2^4, \ldots, 2^{2^{n-1}}\right)$$

shows.

The apparent simplicity of equations in the above statements is misleading. Actually, to any given polynomials $f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_s]$ one can associate a system of the type specified in Conjecture $\mathcal{C}_n(A)$ for a huge value of n depending on r, s, the degree and height of the given polynomials. The algorithm is conceptually simple, based on natural ideas, but is somewhat cumbersome to properly write it down because of the explosion of the number of unknowns. Instead of formally introducing the algorithm, we prefer to use it in an example and refer the interested reader to [15]. This example also illustrates how tricky is to rewrite a given system of polynomial equations into the form required in the statement of conjectures above.

Example. Let us consider the system of generalized Pell equations

$$x^2 - 3z^2 = 1, \quad y^2 - 783z^2 = 1, \tag{1}$$

for which the solution $(2, 28, 1)$ is easy to spot. It is less easy to notice that a second solution is $(97, 1567, 56)$. In [10] it is shown that any system $ax^2 - bz^2 = 1$, $cy^2 - dz^2 = 1$, with a, b, c, d positive integers such that $ad \neq bc$, has at most two solutions in positive integers. (The same sharp bound was established for another family of simultaneous Pell equations in [9].) Taking into account solutions with a third entry 0, one concludes that our system has precisely $8 + 8 + 4 = 20$ solutions in the ring of integers and all of them have entries with absolute value at most 1567.

In order to invoke Conjecture $\mathcal{F}_n(\mathbb{Z})$, for a suitable value of n, we transform the system in the following way. The equations

$$x_1 = 1, \quad x_2 = x_1 + x_1, \quad x_4 = x_2 + x_2, \quad x_3 + x_1 = x_4, \quad x_5 = x_4 \cdot x_4,$$

$$x_6 + x_1 = x_5, \quad x_7 = x_5 \cdot x_5, \quad x_8 = x_3 \cdot x_7, \quad x_9 = x_5 + x_8, \quad x_1 + x_{10} = x_9$$

have a unique solution, in which $x_3 = 3$ and $x_{10} = 783$. Therefore, the simultaneous Pell equations (1) are equivalent to the system consisting of the previous equations together with the following ones

$$x_{12} = x_{11} \cdot x_{11}, \quad x_{14} = x_{13} \cdot x_{13}, \quad x_{16} = x_{15} \cdot x_{15}, \quad x_{17} = x_3 \cdot x_{16},$$

$$x_{18} = x_{10} \cdot x_{16}, \quad x_{12} = x_1 + x_{17}, \quad x_{14} = x_1 + x_{18}.$$

Clearly, one has $x = x_{11}$, $y = x_{13}$, and $z = x_{15}$. Supposing Conjecture $\mathcal{F}_{18}(\mathbb{Z})$ to be true, it would result that

$$\max\{|x|, |y|, |z|\} \leq 2^{2^{18-1}} = 2^{131072} \approx 4.015 \cdot 10^{39456}.$$

However, a clever rewritting of the system (1) allows one to diminish the value of n. For instance, the equations

$$x_1 = 1, \quad x_2 = x_1 + x_1, \quad x_4 = x_2 + x_2, \quad x_3 + x_1 = x_4, \quad x_5 = x_4 \cdot x_4,$$

$$x_6 = x_5 \cdot x_5, \quad x_7 = x_4 + x_6, \quad x_8 = x_1 + x_7,$$

yield $x_8 = 261$. Combined with

$$x_{10} = x_9 \cdot x_9, \quad x_{12} = x_{11} \cdot x_{11}, \quad x_{14} = x_{13} \cdot x_{13},$$

$$x_{15} = x_3 \cdot x_{14}, \quad x_{16} = x_8 \cdot x_{15}, \quad x_{10} = x_1 + x_{15}, \quad x_{12} = x_1 + x_{16},$$

it results that (1) is equivalent to a system of equations in $n = 16$ unknowns. This time one gets from $\mathcal{F}_{16}(\mathbb{Z})$

$$\max\{|x|, |y|, |z|\} \leq 2^{2^{16-1}} = 2^{32768} \approx 2.601 \cdot 10^{9864}.$$

Even better, if first one replaces the system (1) by the equivalent one

$$x^2 - 3z^2 = 1, \quad x^2 + 780z^2 = y^2,$$

and then one put this into the form

$$x_1 = 1, \quad x_2 = x_1 + x_1, \quad x_4 = x_2 + x_2, \quad x_3 + x_1 = x_4, \quad x_5 = x_4 \cdot x_4,$$

$$x_6 = x_5 \cdot x_5, \quad x_7 = x_4 + x_6, \quad x_9 = x_8 \cdot x_8, \quad x_{11} = x_{10} \cdot x_{10},$$

$$x_{13} = x_{12} \cdot x_{12}, \quad x_{14} = x_3 \cdot x_{13}, \quad x_{15} = x_7 \cdot x_{14},$$

$$x_9 = x_1 + x_{14}, \quad x_{11} = x_9 + x_{15},$$

one deduces from Conjecture $\mathcal{F}_{15}(\mathbb{Z})$

$$\max\{|x|, |y|, |z|\} \leq 2^{2^{15-1}} = 2^{16384} \approx 1.190 \cdot 10^{4392}.$$

To help reader to have an idea on the order of magnitude of the bounds thus obtained, it suffices to mention that the number of electrons on the earth is estimated to be about 10^{60}, while 10^{80} is said to be the number of electrons in the visible universe. Having in view that each year consists of about $3.16 \cdot 10^7$ seconds, if one would succeed to examine one billion of integer triples each second with the help of each of the $3 \cdot 10^8$ computers sold up to date in the whole world, one would have to admit that a blind search for the solutions in positive integers to the system (1) will need a time much longer than the most optimistic estimate for the existence of our planet.

What is the present status of the above mentioned conjectures? A brute force attack (with some computer assistance) suffices to establish the validity of $\mathcal{C}_n(A)$ for $n \leq 4$ and any subring A of $\mathbb{C}$. Decidability of the theory of real closed fields entails $\mathcal{C}_n(\mathbb{R})$ and $\mathcal{C}_n(\mathbb{C})$ are decidable for fixed n. Tyszka mentions availability of Mathematica, MuPAD, Perl and Python codes for checking this by solving randomly chosen systems.

However, there is evidence that the statements do not hold for rings relevant in number theory, except maybe for very small n. Matiyasevich's solution to Hilbert's tenth problem imply that $\mathcal{C}_n(\mathbb{Z})$ is false for $n \gg 0$. By tracing some work reported in the literature [12], Tyszka was able to give an explicit example showing that $\mathcal{C}_{21}(\mathbb{Z})$ fails (see [15]). Moreover, $\mathcal{C}_{10}(\mathbb{Z}[\frac{1}{p}])$ fails for any prime p greater than 2^{256}. Similarly, if $k \geq 273$ is an integer such that $t := k^2 + 2$ is prime then one can prove that the system

$$x_1 = 1, \quad x_1 + x_1 = x_2, \quad x_3 \cdot x_3 = x_4, \quad x_2 + x_4 = x_5, \quad x_5 \cdot x_6 = x_1$$

has the solutions

$$\big(1, 2, \lambda, \lambda^2, \lambda^2 + 2, (\lambda^2 + 1)^{-1}\big) \qquad \text{for} \qquad \lambda \in \mathbb{C} \setminus \{\pm\sqrt{-1}\}.$$

If one insists that $\lambda \in \mathbb{Z}[t^{-1}]$ then it readily follows that $\lambda \geq k$ and therefore $\lambda^2 + 2 > 2^{2^{6-2}}$. This inequality contradicts $\mathcal{C}_6(\mathbb{Z})[t^{-1}]$.

Tyszka [15, 18] also shows that $\mathcal{C}_5(\mathbb{Z}[\sqrt{4s^4 - 1}])$ is false for any $s \geq 13$ such that $4s^4 - 1$ is square-free. We shall improve below on this result.

Proposition 2.1. *$\mathcal{C}_5(\mathbb{Z}[\sqrt{d}])$ is false for any integer $d \geq 16384$.*

Proof. Consider the system

$$x_1 = 1,\ x_2 \cdot x_3 = x_1,\ x_2 + x_3 = x_4,\ x_5 \cdot x_5 = x_4. \tag{2}$$

All complex solutions are of the form

$$\Big(1, \lambda, \lambda^{-1}, \lambda + \lambda^{-1}, \pm\sqrt{\lambda + \lambda^{-1}}\Big) \qquad \text{for} \qquad \lambda \in \mathbb{C}, \quad \lambda \neq 0.$$

Assume that the system above is solvable in $\mathbb{Z}[\sqrt{d}]$. Then $x_2 = \lambda = a + b\sqrt{d}$, with a, b integers. Note that for d perfect square or $b = 0$, from $\lambda^{-1} \in \mathbb{Z}[\sqrt{d}]$ it would result $\lambda = \pm 1$ and therefore $\sqrt{\lambda + \lambda^{-1}} \notin \mathbb{Z}[\sqrt{d}]$. Hence, $x_3 = \lambda^{-1} = u + v\sqrt{d}$, with u, v integers and $v \cdot b \neq 0$. The second equation in (2) is equivalent to $av + bu = 0$, $au + dbv = 1$, whence it readily follows $u = a$, $v = -b$ and $a^2 - db^2 = 1$. Therefore,

$$\max\big\{|\lambda|, |\lambda^{-1}|\big\} \geq |a| + |b|\sqrt{d} \geq \sqrt{d+1} + \sqrt{d} > 2\sqrt{d} \geq 2^8 = 2^{2^{5-2}}.$$

□

3 The linear case

Tyszka made an analogous conjecture on systems in which the multiplication is prohibited. Below G denotes an additive subgroup of $\mathbb{C}$, while n stands for a positive integer.

Conjecture $\mathcal{L}_n(G)$**.** *Let $\mathcal{T}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ for some i, j, k between 1 and n. If $\mathcal{T}$ has a solution in the group G then there exists $(x_1, x_2, \ldots, x_n) \in (G \cap \mathbb{Q})^n$ satisfying the system and $|x_i| \leq 2^{n-1}$ for $i = 1, 2, \ldots, n$.*

For $n > 1$ the bound can not be improved in general, as the system

$$x_1 = 1,\ x_1 + x_1 = x_2,\ x_2 + x_2 = x_3,\ \ldots,\ x_{n-1} + x_{n-1} = x_n$$

has a unique solution $\left(1, 2, 2^2, 2^3, \ldots, 2^{n-1}\right)$.

In [15] and [18] one may find a proof that a system of the type considered in Conjecture $\mathcal{L}_n(G)$ which is solvable in integers (or in a group G containing $\mathbb{Q}$) must have an integer solution (rational solution, respectively), all of whose entries have absolute value at most $5^{(n-1)/2}$. The aim of this paper is to improve on these results.

Theorem 3.1. *Let $\mathcal{T}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ for some i, j, k between 1 and n. If $\mathcal{T}$ has a solution in a subgroup G of $\mathbb{C}$ containing $\mathbb{Q}$ or in $\mathbb{Z}$ then there exists $(x_1, x_2, \ldots, x_n) \in (G \cap \mathbb{Q})^n$, respectively in $\mathbb{Z}^n$, satisfying the system and $|x_i| \leq 2^n$ for $i = 1, 2, \ldots, n$.*

On the way to the proof of this result we establish an other conjecture of Tyszka [15, Conjecture 4].

Theorem 3.2. *Let B be a matrix with $m < n$ rows and n columns. Assume that each row of B, after deleting all zero entries, has one of the forms*

$$(1),\ (1,1),\ (-1,2),\ (2,-1),\ (-1,1,1),\ (1,-1,1),\ (1,1,-1).$$

Then any maximal minor of B has the module at most 2^{n-1}.

We start the proof of Theorem 3.1 by associating a system of linear equations $My = b$ with integer coefficients to a given system $\mathcal{T}$ of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ (i, j, $k \in \{1, 2, \ldots, n\}$).

Below, all indices appearing in the same equation are pairwise distinct. We may assume that $x_1 = 1$ is the only equation from $\mathcal{T}$ of the type $x_i = 1$, otherwise either there exists the obvious solution with all components zero or $\mathcal{T}$ is equivalent to a system of the kind described in Conjecture $\mathcal{L}_t(\mathbb{Z})$ for some positive integer t smaller than n (system obtained by replacing each

variable x_i appearing in an equation $x_i = 1$ by x_1 and decreasing by 1 all indices greater than i). To equation $x_1 = 1$ one associates a row in the matrix M with entries $1, 0, \ldots, 0$, whereas the corresponding entry in b is 1. A permutation of this row corresponds to each equation of the type $x_1 + x_i = x_1$ or $x_i + x_i = x_i$ or $x_i + x_j = x_i$ (recall that $i, j > 1$, $i \neq j$), with a null entry in the appropriate place of b. The only nonzero entries in a row associated to an equation $x_1 + x_i = x_j$ or $x_1 + x_1 = x_i$ are 1 and -1, while the appropriate entry of b is 1. To an equation $x_k + x_i = x_j$ or $x_i + x_j = x_1$ $(i, j, k > 1)$ it corresponds a row consisting of 1, 1 and -1 in the appropriate places and only zeros in the other places, while the entry of b is 0. An equation of the type $x_i + x_i = x_j$ generates a row of M whose nonzero entries are 2 and -1, and the corresponding entry in b is 0.

Since $\mathcal{T}$ is supposed to be compatible, no equations of the type $x_1 + x_1 = x_1$ or $x_i + x_1 = x_i$ appear in it. Moreover, if one supposes the existence of integer solutions, no equation of the form $x_i + x_i = x_1$ exists.

To sum up, the extended matrix of the linear system $My = b$ is an integer matrix $\left(M \vdots b\right)$ with $n+1$ columns whose rows are obtained by filling out with suitably many zeroes one of the vectors

$$(1 \vdots 0),\ (1 \vdots 1),\ (1, -1 \vdots 1),\ (-1, 1 \vdots 1),\ (-1, 2 \vdots 0), \tag{3}$$

$$(2, -1 \vdots 0),\ (-1, 1, 1 \vdots 0),\ (1, -1, 1 \vdots 0),\ (1, 1, -1 \vdots 0).$$

Compatible systems of linear equations with integer coefficients have solutions restricted as in the following result.

Theorem A. ([6]) *Let M be an integer $m \times n$ matrix of rank r and $b \in \mathbb{Z}^m$ such that the system $My = b$ has integer solutions. Denote by D the maximum of the absolute values of the r-minors of the augmented matrix $(M \vdots b)$. Then there is a solution $y \in \mathbb{Z}^n$ satisfying $|y_j| \leq D$, $j = 1, 2, \ldots, n$.*

In order to get the bound D, Tyszka applies Hadamard's determinantal inequality, which is an algebraic statement of a geometric fact: the volume of a parallelepiped is at most the product of the Euclidean lengths of its edges. Instead of this classical result, we employ a more recent one, due to R. Waldi [20]. For reader's convenience, we quote it bellow. Although it might not be apparent, Waldi's theorem is a common generalisation to Bézout's theorem and Hadamard's inequality.

Theorem B. ([20]) *Consider on $\mathbb{R}^n$ the norm*

$$L(y_1, y_2, \ldots, y_n) = \frac{1}{2}\big(|y_1| + |y_2| + \cdots + |y_n| + |y_1 + y_2 + \cdots + y_n|\big).$$

Then for any matrix M with rows $r_1, r_2, \ldots, r_n \in \mathbb{R}^n$ one has

$$|\det(M)| \leq L(r_1)L(r_2)\cdots L(r_n).$$

It is clear that the vectors $v \in \mathbb{R}^n$ whose nonzero entries are restricted as in (3) satisfy $L(v) \leq 2$. Hence, the proof of Theorem 3.2 is easily concluded by noticing that the rank of the matrix B is at most $m \leq n-1$.

Now we can complete the proof of Theorem 3.2 for systems $\mathcal{T}$ solvable in integers. We apply Theorems A and B to the system $Mx = b$ obtained as explained above.

The proof of the case of systems compatible over a group G is similar. Cramer's formula gives the value of each basic variable as the quotient of two maximal minors of the extended matrix, while the secondary variables are equal to zero. Therefore, the nonzero entries of each solution of the given system $\mathcal{T}$ are rational numbers, bounded in module by the module of the numerator. One concludes as in the previous paragraph, by invoking Theorem 3.2.

Notice that the conclusion of Theorem 3.1 is closer to the bound claimed in Conjectures $\mathfrak{L}_n(\mathbb{Z})$ and $\mathfrak{L}_n(G)$ than Tyszka's bound $5^{(n-1)/2}$ for all $n \geq 8$. Moreover,

$$\frac{2^n}{2^{n-1}} = 2 \quad \text{for all} \quad n \geq 1, \quad \text{while} \quad \lim_{n\to\infty} \frac{5^{(n-1)/2}}{2^{n-1}} = \infty.$$

The result below lists several cases where systems as in Conjecture $\mathfrak{L}_n(\mathbb{Z})$ have solutions whose entries are bounded in module by 2^{n-1}.

Proposition 3.3. *Let $\mathcal{T}$ be a system of equations of the type $x_i = 1$ or $x_i = x_j + x_k$ for some i, j, k between 1 and n. Suppose $\mathcal{T}$ has integer solutions. Then there exists $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ satisfying the system and $|x_i| \leq 2^{n-1}$ for $i = 1, 2, \ldots, n$ if any of the following conditions holds:*

- α) *the matrix of the system has rank less than n,*
- β) *$n \geq 5$ and there is no equation of the form $2x_i = x_j$ $(1 \leq i \neq j \leq n)$,*
- γ) *$n \geq 37$ is odd and the system contains at most $n/2$ equations of the form $2x_i = x_j$ $(1 \leq i \neq j \leq n)$,*
- δ) *$n \geq 44$ is even and the system contains at most $n/2$ equations of the form $2x_i = x_j$ $(1 \leq i \neq j \leq n)$.*

Proof. Sufficiency of condition α) is obvious from the arguments exposed in the proof of the previous theorem. If hypothesis β) holds then the matrix has only rows whose nonzero entries are 1, $(1, 1, -1)$, $(1, -1, 1)$ or $(-1, 1, 1)$. Applying Hadamard' inequality, one obtains $D \leq 3^{n/2}$. As is easily seen, for $n \geq 5$ one has $3^{n/2} < 2^{n-1}$. Suppose now that among the equations of the system $\mathcal{T}$ there are precisely r $(1 \leq r \leq n/2)$ equations of the form $2x_i = x_j$ $(1 \leq i \neq j \leq n)$. The maximal minors of the matrix are bounded according to Hadamard by $3^{(n-r)/2}5^{r/2}$, which is at most $3^{\lfloor (n+1)/2 \rfloor}5^{\lfloor n/2 \rfloor}$. This number is smaller than 2^{n-1} if n is subject to restrictions indicated in γ) and δ). □

Acknowledgements. The author thanks the referees for comments and suggestions.

References

[1] A. Baker, The Diophantine equation $y^2 = ax^3 + bx^2 + cx + d$, *J. London Math. Soc.*, **43**(1968), 1–9.

[2] S. Basu, R. Pollack, M. F. Roy, *Algorithms in real algebraic geometry*, 2nd ed., Springer, Berlin, 2006.

[3] D. N. Bernshtein, The number of roots of a system of equations, *Anal. Appl.*, **9**(1975), 183–185.

[4] L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and real computation*, Springer, New York, 1998.

[5] E. Bombieri, J. Vaaler, On Siegel's lemma, *Invent. Math.*, **7**(1983), 11–32.

[6] I. Borosh, M. Flahive, D. Rubin, B. Treybig, A sharp bound for solutions of linear Diophantine equations, *Proc. Amer. Math. Soc.*, **105**(1989), 844–846.

[7] Y. Bugeaud, On the size of integer solutions of elliptic equations, *Bull. Austral. Math. Soc.*, **57**(1998), 199–206.

[8] Y. Bugeaud, On the size of integer solutions of elliptic equations, II, *Bull. Greek Math. Soc.*, **43**(2000), 125–130.

[9] M. A. Bennett, M. Cipu, M. Mignotte, R. Okazaki, On the number of solutions of simultaneous Pell equations, II, *Acta Arith.*, **122**(2006), 407–417.

[10] M. Cipu, M. Mignotte, On the number of solutions to systems of Pell equations, *J. Number Th.*, **125**(2007), 356–392.

[11] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.*, **73**(1983), 349–366. Erratum *ibidem*, **75**(1984), 381.

[12] J. P. Jones, D. Sato, H. Wada, D. Wiens, Diophantine representation of the set of prime numbers, *Amer. Math. Monthly*, **83**(1976), 449–464.

[13] A. G. Kushnirenko, Polyèdres de Newton et nombres de Milnor, *Invent. Math.*, **32**(1976), 1–31.

[14] Yu. V. Matiyasevich, *Hilbert's tenth problem*, MIT Press, Cambridge, MA, 1993.

[15] A. Tyszka, Bounds of some real (complex) solution of a finite system of polynomial equations with rational coefficients, available at the address http://arxiv.org/abs/math/0702558v84.

[16] A. Tyszka, Some conjectures on addition and multiplication of complex (real) numbers, *Int. Math. Forum*, **4**(2009), 521–530.

[17] A. Tyszka, A hypothetical upper bound for the solutions (the number of solutions) of a Diophantine equation with a finite number of solutions, http://arxiv.org/0901.2093v80.

[18] A. Tyszka, Two conjectures on the arithmetic in $\mathbb{R}$ and $\mathbb{C}$, *Math. Log. Quart.*, **56**(2010), 175–184.

[19] N. N. Vorobjov, Jr., Estimates of real roots of a system of algebraic equations, *J. Sov. Math.*, **34**(1986), 1754–1762.

[20] R. Waldi, Über ein Analogon zu Hadamards Ungleichung, *Arch. Math.*, **59**(1992), 15–20.

Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, RO-014700 Bucharest, ROMANIA