BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 17, Number 1, July 1987

ON THE DECIDABILITY OF DIOPHANTINE PROBLEMS IN COMBINATORIAL GEOMETRY

BERND STURMFELS

ABSTRACT. In spite of Matiyasevic's solution to Hilbert's 10th problem some fifteen years ago it is still unknown whether there exists an algorithm to decide the solvability of diophantine equations within the field of rational numbers. In this note we show the equivalence of this problem with a conjecture of B. Grünbaum [6] on rational coordinatizability in combinatorial geometry. Such an algorithm exists if and only if the rational realizability problems for matroids, oriented matroids, and convex polytopes (Steinitz problem) are decidable.

1. Introduction and statement of the result. Many realizability problems in combinatorial and computational geometry can be formulated in terms of polynomial equations and inequalities with integer coefficients, and so these problems are decidable over the real numbers by a well-known result of Tarski [14].

The situation is different if we focus our attention on solutions in the field Q of *rational* numbers. In view of Matiyasevic's negative solution [9] to Hilbert's 10th problem in 1971, B. Grünbaum has conjectured [6, Conjecture 2.14] that there is no algorithm to enumerate all (isomorphism types of) arrangements of lines in the rational projective plane. In [5, p. 92] the same question has been raised for convex polytopes in rational Euclidean d-space, $d \geq 4$. Matiyasevic's result "there exists no algorithm to decide whether a system of diophantine equations has a solution among the rational *integers*" cannot be applied to prove Grünbaum's conjecture, and, as B. Mazur points out in a recent survey article [10], the corresponding problem for rational *numbers* is still open; see also Klee and Wagon [8].

In this note we show that Grünbaum's conjectures for line arrangements and convex polytopes as well as the corresponding conjecture for matroids are equivalent to the above problem. See White [15], Bachem [1], Bokowski and Sturmfels [3] and the references given there for the basic concepts of matroid theory and oriented matroids and [13] for recent results on irrational oriented matroids and polytopes.

THEOREM. *The following statements are equivalent.*

(1) *There exists an algorithm to decide for an arbitrary polynomial* $f \in Z[x_1, \ldots, x_n]$, $n \in N$, *whether* f *has zeros in the field* Q *of rational numbers.*

(2) *There exists an algorithm to decide for an arbitrary matroid* M *whether* M *is coordinatizable over* Q.

Received by the editors January 23, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 52A25, 05B35; Secondary 11U05.

(3) *There exists an algorithm to decide for arbitrary polynomials* $f_1, \dots, f_r, g_1, \dots, g_s \in Z[x_1, \dots, x_n]$, $n \in N$, *whether there exist* $q_1, \dots, q_n \in Q$ *such that* $f_i(q_1, \dots, q_n) = 0$ *for* $i = 1, \dots, r$ *and* $g_j(q_1, \dots, q_n) > 0$ *for* $j = 1, \dots, s$.

(4) *There exists an algorithm to decide for an arbitrary oriented matroid* χ *whether* χ *is coordinatizable over* Q.

(5) *There exists an algorithm to decide for an arbitrary finite lattice* L *whether* L *is isomorphic to the face lattice of a convex polytope in rational Euclidean space.*

Note that by the correspondence of oriented matroids and arrangements of pseudo-spheres [**16**], Grünbaum's conjecture on line arrangements is equivalent to the statement (4).

The crucial part of the Theorem is the implication (2)⇒(1). The idea is to encode an arbitrary polynomial equation with integer coefficients by a finite set of matroids. In other words: arbitrary affine algebraic varieties can be decomposed into realization spaces of rank 3 matroids. This method is closely related to the approach of Mnëv [**12**].

2. Outline of the proof.

It is well known in projective geometry that the algebraic operations of addition and multiplication have their "geometric" analogues in certain projectively invariant constructions which are of considerable importance in the coordinatization of Desarguesian projective planes, e.g. [**7**, §VI.7. The algebra of points on a line]. This kind of construction can be used in matroid theory to impose arbitrary polynomial conditions on points on a line. For details see Mac Lane [**11**], where it is proved that every finite algebraic extension over Q is the unique "minimal" coordinatizing field of some rank 3 matroid, and [**13**; **5**, Chapter 5] where that technique is applied to construct irrational convex polytopes.

Here we generalize this idea to construct arbitrary affine algebraic Q-varieties by matroids. Given two elements e_1 and e_2 on a line l spanned by elements 0, 1, and ∞ in a matroid M, by a *construction of the product* or *sum* $e_1 + e_2$ on l we mean an extension $\overline{M}$ of M by the points needed to projectively construct the product or sum in any realization of M. Thereby the dependencies among the new points describe the linear construction.

Observe that the use of the indefinite article is necessary because such an extension is not unique. For example, the newly constructed point $e_1 + e_2$ might but need not coincide with a certain old point on the line l. Nevertheless, the set of those matroids is certainly finite and algorithmically computable.

(2)⇒(1): Given a decision procedure for rational coordinatizability of matroids, the following algorithm decides whether f has rational roots.

Let c be the largest absolute value of the coefficients of the polynomial f. Consider the projectively unique matroid M of rank 3 in which, starting from a projective basis, all integers between $-c$ and c have been constructed on a line l. Denote by $M_1, \dots, M_\rho$ all possible extensions of M with n points $e_1, \dots, e_n$ on the line l. For any such M_i consider the set of all possible matroid extensions which are constructions of the point $f := f(e_1, \dots, e_n)$ on the line l. Let $M_i^1, \ldots, M_i^{\sigma_i}$ denote all such constructions for which $\mathrm{rk}\{0, f\} = 1$, i.e. $f = 0$ in every projective realization.

The set of matroids $\{M_i^j\}$ is algorithmically constructible, and $f(x_1, \ldots, x_n) = 0$ has a rational solution if and only if one of the matroids in $\{M_i^j\}$ is coordinatizable over Q.

(4)⇒(2). For any matroid M the set $\mathcal{O}(M)$ of oriented matroids with underlying matroid M is computable. Clearly, M is Q-realizable if and only if there exists a Q-realizable $\chi \in \mathcal{O}(M)$. Consequently, every Q-realizability test for oriented matroids yields also a Q-realizability test for matroids.

(3)⇒(4). Let χ be an oriented matroid of rank d on $\{1, \ldots, n\}$. Writing $\chi\colon \{1, \ldots, n\}^d \to \{-1, 0, +1\}$ for the corresponding *chirotope*, i.e. oriented bases map, then χ is Q-realizable if and only if the inequality system

$$\det \begin{pmatrix} x_{\lambda_1}^1 & \cdots & x_{\lambda_d}^1 \\ \vdots & \ddots & \vdots \\ x_{\lambda_1}^d & \cdots & x_{\lambda_d}^d \end{pmatrix} = \chi(\lambda_1, \ldots, \lambda_d) \text{ for all } \lambda_1, \ldots, \lambda_d \in \{1, \ldots, n\}$$

has a solution over Q; see [**3**].

(5)⇒(4). In [**13**] the author introduced the concept of *rigid* oriented matroids, that is, oriented matroids with only extreme vertices which have the property that no other such oriented matroid has the same face lattice. Clearly, a rigid oriented matroid is Q-realizable if and only if its face lattice is Q-polytopal.

The following construction due to J. Lawrence assigns to every oriented matroid χ of rank d with n vertices a rigid oriented matroid $\Lambda(\chi)$ of rank $2n - d$ with $2n$ vertices which is realizable over a field K if and only if χ is. Given an oriented matroid χ on a set E, let χ' denote the extension by $|E|$ vertices antipodal to the original vertices, i.e., for every $e \in E$ introduce a new vertex e' such that $\{e, e'\}$ is a positive circuit of χ'. The oriented matroid $\Lambda(\chi)$ dual to χ' is rigid; see Billera and Munson [**2**, Theorem 2.2].

Assuming there was an algorithm that decides the rational Steinitz problem, we obtain a Q-realizability test for an arbitrary oriented matroid χ by applying this algorithm to the face lattice of the Lawrence construction $\Lambda(\chi)$ of χ.

(4)⇒(5). Conversely, it is well known that the question whether a certain finite lattice is isomorphic to the face lattice of a convex polytope can be algorithmically reduced to the realizability problem for oriented matroids. For details of this algorithmic reduction see [**4**]. Since all operations are independent of the realization field, every Q-realizability test for oriented matroids solves the rational Steinitz problem as well.

(1)⇒(3). The rational inequality system in (3) can be reduced to a single equation by the following standard method. Introduce $8s$ new variables p_k^j, $j = 1, \ldots, s$, $k = 1, \ldots, 8$, and replace each inequality $g_j(q_1, \ldots, q_n) > 0$ by the equation

$$\begin{aligned} h_j(q_1, \ldots, q_n, p_1^j, \ldots, p_8^j) := g_j(q_1, \ldots, q_n) \cdot ((p_1^j)^2 + (p_2^j)^2 + (p_3^j)^2 + (p_4^j)^2) \\ - ((p_5^j)^2 + (p_6^j)^2 + (p_7^j)^2 + (p_8^j)^2 + 1) = 0. \end{aligned}$$

The inequality $q_j > 0$ has a rational solution if and only if the equation $h_j = 0$ has a rational solution. For, by Lagrange's four-square theorem, an integer $n \in Z$ is nonnegative if and only if there exist integers a, b, c, and d such that $n = a^2 + b^2 + c^2 + d^2$ [8].

Finally, replace the equations $f_1 = 0, \ldots, f_r = 0$, $h_1 = 0, \ldots, h_s = 0$ by the single equation

$$f := (f_1)^2 + \cdots + (f_r)^2 + (h_1)^2 + \cdots + (h_s)^2 = 0$$

in $n + 8s$ variables. This equation has a rational solution if and only if its summands have common rational zeros. □

REFERENCES

1. A. Bachem, *Convexity and optimization in discrete structures*, Convexity and Applications (P. M. Gruber and J. Wills, eds.), Birkhäuser, Basel, 1983.

2. L. J. Billera and B. S. Munson, *Polarity and inner products in oriented matroids*, European J. Combin. **5** (1984), 293–308.

3. J. Bokowski and B. Sturmfels, *On the coordinatization of oriented matroids*, Discrete and Computational Geometry **1** (1986), 293–306.

4. ———, *Polytopal and nonpolytopal spheres—an algorithmic approach*, Israel J. Math. (to appear).

5. B. Grünbaum, *Convex polytopes*, Interscience, London, 1967.

6. ———, *Arrangements and spreads*, CBMS Regional Conf. Ser., no. 10, Amer. Math. Soc., Providence, R.I., 1972.

7. W. V. D. Hodge and D. Pedoe, *Methods of algebraic geometry*, Cambridge Univ. Press, Cambridge, 1947.

8. V. Klee and S. Wagon, *Unsolved problems in mathematics* (in preparation).

9. Y. V. Matiyasevic, *Diophantine representation of enumerable predicates*, Izv. Akad. Nauk SSSR **35** (1971), 3–30.

10. B. Mazur, *Arithmetic on curves*, Bull. Amer. Math. Soc. (N.S.) **14** (1986), 207–259.

11. S. Mac Lane, *Some interpretations of abstract linear dependence in terms of projective geometry*, Amer. J. Math. **58** (1936), 236–240.

12. N. E. Mnëv, *On manifolds of combinatorial types of projective configurations and convex polyhedra*, Soviet. Math. Dokl. **32** (1985), 335–337.

13. B. Sturmfels, *Boundary complexes of convex polytopes cannot be characterized locally*, J. London Math. Soc. (to appear).

14. A. Tarski, *A decision method for elementary algebra and geometry*, 2nd rev. ed., Univ. of California Press, Berkeley, 1951.

15. N. L. White (ed.), *Theory of matroids*, Cambridge Univ. Press, Cambridge, 1986.

16. J. Folkman and J. Lawrence, *Oriented matroids*, J. Combin. Theory Ser. B **25** (1978), 199–236.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON, SEATTLE, WASHINGTON 98195

Current address: Institute for Mathematics and its Applications, University of Minnesota, Minneapolis, Minnesota 55455