POLYNOMIAL PARAMETRIZATION OF THE SOLUTIONS OF CERTAIN SYSTEMS OF DIOPHANTINE EQUATIONS

FRANZ HALTER-KOCH AND GÜNTER LETTL

Abstract. Let $f_1, f_2, \dots, f_k \in \mathbb{Z}[X_0, X_1, \dots, X_N]$ be non-constant homogeneous polynomials which define a projective variety V over $\mathbb{Q}$. Under the hypothesis that, for some $n \in \mathbb{N}$, there is a surjective morphism $\varphi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$, we show that all integral solutions of the system of Diophantine equations $f_1 = 0, \dots, f_k = 0$ (outside some exceptional set) can be parametrized by a single k-tuple of integer-valued polynomials. This result only depends on φ, but not on the embedding given by $f_1, f_2, \dots, f_k$. If, in particular, φ is a normalization of V, then the exceptional set is really small.

Many questions in number theory deal with the problem whether a set $S \subset \mathbb{Z}^k$ has a polynomial parametrization, i.e. whether there exist polynomials $h_1, \dots, h_k \in \mathbb{Z}[T_1, \dots, T_r]$ such that S is the image of $\mathbb{Z}^r$ under the map $\boldsymbol{h} = (h_1, \dots, h_k)\colon \mathbb{Z}^r \to \mathbb{Z}^k$; see e.g. L. Vaserstein [9]. This is also tightly connected with the notion of "Diophantine set", see e.g. the book of P. Ribenboim [8, Chap. 3.III], which is intrinsic to Matiyasevich's solution of Hilbert's tenth problem.

S. Frisch [2] proved an interesting connection between parametrizations by polynomials with integral coefficients and by integer-valued polynomials. Let us recall that a polynomial $g \in \mathbb{Q}[U_1, U_2, \dots, U_m]$ is called *integer-valued* if for any $\boldsymbol{u} = (u_1, \dots, u_m) \in \mathbb{Z}^m$ one has $g(\boldsymbol{u}) \in \mathbb{Z}$. S. Frisch and L. Vaserstein showed in [4] that the set of Pythagorean triples cannot be parametrized by any triple of polynomials with integral coefficients, but indeed it can be parametrized by a triple of integer-valued polynomials.

Recently, the affirmative part of this result was generalized by S. Frisch and the second author to the solution set of any homogeneous Diophantine equation in 3 variables, which defines an irreducible, plane curve with a rational function field [3]. This corresponds to the special case $N = 2$ and $k = 1$ of Theorem 1 of the present paper.

Let V be a variety defined over $\mathbb{Q}$ and suppose that for some $n \in \mathbb{N}$ there is a surjective morphism $\varphi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$. For a point $p \in V$, let $\mathcal{O}_{V,p}$ be the local ring of V at p, $\mathsf{k}_V(p)$ its residue field and $\varphi^{-1}(p) = \mathbb{P}^n_{\mathbb{Q}} \times_V \operatorname{spec} \mathsf{k}_V(p)$ the fibre of φ at p. For each point $\overline{p} \in \varphi^{-1}(p)$, φ induces an embedding $\varphi_{\overline{p}}\colon \mathsf{k}_V(p) \hookrightarrow \mathsf{k}_{\mathbb{P}^n_{\mathbb{Q}}}(\overline{p})$. We call a $\mathbb{Q}$-rational point $p \in V(\mathbb{Q})$ *strongly* $\mathbb{Q}$*-rational* (with respect to φ) if there exists some $\overline{p} \in \pi^{-1}(p)$ such that $\varphi_{\overline{p}}$ is the identity, that is, $\mathsf{k}_{\mathbb{P}^n_{\mathbb{Q}}}(\overline{p}) = \mathsf{k}_V(p) = \mathbb{Q}$. Let $V_\varphi(\mathbb{Q})^*$ denote the set of all strongly $\mathbb{Q}$-rational points of V.

If, in particular, φ is a normalization of V and $\mathbb{Q}(V)$ denotes the rational function field of V, then, for every $p \in V$, $\varphi^{-1}(p) = \operatorname{spec} \overline{\mathcal{O}_{V,p}}$ is finite, where $\overline{\mathcal{O}_{V,p}}$ denotes the integral closure of $\mathcal{O}_{V,p}$ in $\mathbb{Q}(V)$, and the exceptional set $V(\mathbb{Q}) \setminus V_\varphi(\mathbb{Q})^*$ of non strongly $\mathbb{Q}$-rational points of V is contained in the set of singular points of V and thus in a lower-dimensional

2000 *Mathematics Subject Classification.* Primary 11D85; secondary 14G05, 14M20, 13F20, 11D41.
Key words and phrases. integer-valued polynomials, rational variety.
This work was supported by the Austrian Science Fund FWF, project number P20120-N18.

subset. Let us remark that "strongly $\mathbb{Q}$-rational" just generalizes the notion of "not bad", as given in [3] for $\mathbb{Q}$-rational points of curves, to higher dimensions.

Let V be a projective variety over $\mathbb{Q}$ and fix an embedding $V \subset \mathbb{P}^N_{\mathbb{Q}}$ as a closed subvariety. Then $V = \operatorname{Proj}\big(\mathbb{Q}[X_0,\ldots,X_N]/(f_1,\ldots,f_k)\big)$, where $f_1,\ldots,f_k \in \mathbb{Q}[X_0,\ldots,X_N]$ are homogeneous polynomials, and

$$V(\mathbb{Q}) = \big\{(x_0 : \ldots : x_N) \in \mathbb{P}^N(\mathbb{Q}) \mid f_j(x_0,\ldots,x_N) = 0 \ \text{ for all } 1 \le j \le k\big\}\,.$$

Obviously, one can even choose $f_1,\ldots,f_k \in \mathbb{Z}[X_0,\ldots,X_N]$.

Theorem 1. *Let $f_1,\ldots,f_k \in \mathbb{Z}[X_0,\ldots,X_N]$ be non-constant homogeneous polynomials such that $V = \operatorname{Proj}\big(\mathbb{Q}[X_0,\ldots,X_N]/(f_1,\ldots,f_k)\big)$ is a projective variety admitting a surjective morphism $\varphi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$. Put*

$$\begin{aligned}\mathcal{L} &= \big\{(x_0,\ldots,x_N) \in \mathbb{Z}^{N+1} \mid f_j(x_0,\ldots,x_N) = 0 \ \textit{ for all } 1 \le j \le k\big\}\\ &= \big\{(x_0,\ldots,x_N) \in \mathbb{Z}^{N+1} \mid (x_0 : \ldots : x_N) \in V(\mathbb{Q})\big\} \cup \big\{(0,\ldots,0)\big\}\end{aligned}$$

and

$$\mathcal{L}^* = \big\{(x_0,\ldots,x_N) \in \mathbb{Z}^{N+1} \mid (x_0 : \ldots : x_N) \in V_\varphi(\mathbb{Q})^*\big\} \cup \big\{(0,\ldots,0)\big\} \subset \mathcal{L}\,.$$

Then there exist some $m \in \mathbb{N}$ and integer-valued polynomials $g_0,\ldots,g_N \in \mathbb{Q}[U_1,\ldots,U_m]$ such that

$$\mathcal{L}^* = \big\{(g_0(\boldsymbol{u}),\ldots,g_N(\boldsymbol{u})) \mid \boldsymbol{u} \in \mathbb{Z}^m\big\}\,.$$

Remark.

1. Note that in Theorem 1 the existence of a parametrization by integer-valued polynomials only depends on the variety V, but not on the explicit embedding given by $f_1, f_2, \ldots, f_k$. In contrast, the existence of a parametrization by polynomials with integral coefficients does depend on the embedding, as can be seen from [4] (unit circle) and [3, Ex. 1] (equilateral hyperbola).

2. If $\dim V = 1$, then the normalization $\overline{V}$ of V is non-singular, and $\overline{V} \cong \mathbb{P}^1_{\mathbb{Q}}$ holds if and only if the function field $\mathbb{Q}(V)$ is rational. In the higher-dimensional case, Theorem 1 applies if one supposes that $\overline{V} \cong \mathbb{P}^n_{\mathbb{Q}}$, which is a much stronger assumption.

The proof of Theorem 1 will use the implication (D) $\Rightarrow$ (B) of the main result of [2], which for the sake of completeness we state in the following

Proposition 2. *Let $k,\ r \in \mathbb{N}$, $h_1,\ldots,h_k \in \mathbb{Q}[T_1,\ldots,T_r]$ and*

$$S = \big\{(h_1(\boldsymbol{t}),\ldots,h_k(\boldsymbol{t})) \mid \boldsymbol{t} \in \mathbb{Z}^r\big\} \cap \mathbb{Z}^k\,.$$

Then there exist integer-valued polynomials $g_1,\ldots,g_k \in \mathbb{Q}[U_1,\ldots,U_m]$ for some $m \in \mathbb{N}$ such that

$$S = \big\{(g_1(\boldsymbol{u}),\ldots,g_k(\boldsymbol{u})) \mid \boldsymbol{u} \in \mathbb{Z}^m\big\}\,.$$

Proof of Theorem 1. Let $\varphi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$ be a surjective morphism. Choose homogeneous polynomials of the same degree, say $h_0,\ldots,h_N \in \mathbb{Z}[T_0,\ldots,T_n]$, such that on geometric points $(t_0 : \ldots : t_n) \in \mathbb{P}^n(\overline{\mathbb{Q}})$ the map φ is given by

$$\varphi(t_0 : \ldots : t_n) = \big(h_0(t_0,\ldots,t_n) : \ldots : h_N(t_0,\ldots,t_n)\big)\,.$$

In particular, it follows that $h_0, \dots, h_N$ have no common zero. Hence, by the projective Nullstellensatz [10, Ch. VII, §4], the radical of the homogeneous ideal $(h_0, \dots, h_N)$ is given by

$$\sqrt{(h_0, \dots, h_N)} = (T_0, \dots, T_n) \ \triangleleft \ \mathbb{Q}[T_0, \dots, T_n]\,.$$

For $p \in V(\mathbb{Q})$, there exists some $z \in \mathbb{P}^n(\mathbb{Q})$ with $p = \varphi(z)$ if and only if $p \in V_\varphi(\mathbb{Q})^*$. Thus we obtain

$$\mathcal{L}^* = \Big\{ \big(wh_0(\boldsymbol{t}), \dots, wh_N(\boldsymbol{t})\big) \bigm| \boldsymbol{t} \in \mathbb{Q}^{n+1},\, w \in \mathbb{Q} \Big\} \cap \mathbb{Z}^{N+1}\,,$$

and the assertion of Theorem 1 follows by the subsequent Lemma. □

Lemma 3. *Let $h_0, \dots, h_N \in \mathbb{Z}[T_0, \dots, T_n]$ be homogeneous polynomials of the same degree such that $\sqrt{(h_0, \dots, h_N)} = (T_0, \dots, T_n) \ \triangleleft \ \mathbb{Q}[T_0, \dots, T_n]$ and*

$$L = \big\{ \big(wh_0(\boldsymbol{t}), \dots, wh_N(\boldsymbol{t})\big) \bigm| \boldsymbol{t} \in \mathbb{Q}^{n+1}\,,\ w \in \mathbb{Q}\ \big\} \cap \mathbb{Z}^{N+1}\,.$$

Then there exists some $m \in \mathbb{N}$ and integer-valued polynomials $g_0, \dots, g_N \in \mathbb{Q}[U_1, \dots, U_m]$ such that

$$L = \big\{ \big(g_0(\boldsymbol{u}), \dots, g_N(\boldsymbol{u})\big) \bigm| \boldsymbol{u} \in \mathbb{Z}^m \big\}\,.$$

Proof. We assert that there exists some $d \in \mathbb{N}$ such that, for all $\boldsymbol{t} = (t_0, \dots, t_n) \in \mathbb{Z}^{n+1}$ with $\gcd(t_0, \dots, t_n) = 1$ we have

$$\gcd\big\{h_0(\boldsymbol{t}), \dots, h_N(\boldsymbol{t})\big\} \bigm| d\,.$$

Indeed, since $\sqrt{(h_0, \dots, h_N)} = (T_0, \dots, T_n) \ \triangleleft \ \mathbb{Q}[T_0, \dots, T_n]$ we obtain, by clearing up denominators, polynomials $q_{j,i} \in \mathbb{Z}[T_0, \dots, T_n]$ (for $0 \le i \le N$ and $0 \le j \le n$) and integers $d,\, b \in \mathbb{N}$ such that

$$dT_j^b = \sum_{i=0}^{N} h_i\, q_{j,i} \quad \text{for all } 0 \le j \le n\,.$$

Now, if $\boldsymbol{t} = (t_0, \dots, t_n) \in \mathbb{Z}^{n+1}$ with $\gcd(t_0, \dots, t_n) = 1$, then

$$dt_j^b = \sum_{i=0}^{N} h_i(\boldsymbol{t})\, q_{j,i}(\boldsymbol{t}) \quad \text{for all } 0 \le j \le n\,, \quad \text{and thus } \gcd\big\{h_0(\boldsymbol{t}), \dots, h_N(\boldsymbol{t})\big\} \bigm| d\,.$$

With d as above, we set $h_i^* = d^{-1}h_i \in \mathbb{Q}[T_0, \dots, T_n]$ (for $0 \le i \le N$), and we assert that

$$L = \big\{ \big(wh_0^*(\boldsymbol{t}), \dots, wh_N^*(\boldsymbol{t})\big) \bigm| w \in \mathbb{Z}\,,\ \boldsymbol{t} \in \mathbb{Z}^{n+1}\ \big\} \cap \mathbb{Z}^{N+1}\,. \tag{1}$$

Once this is proved, the Lemma follows by Proposition 2.

The inclusion "$\supset$" of (1) is obvious, and both sets contain the trivial solution. Thus assume that $(0, \dots, 0) \ne (x_0, \dots, x_N) \in L$, and let $\boldsymbol{t} \in \mathbb{Q}^{n+1}$ and $w \in \mathbb{Q}$ be such that $x_i = wh_i(\boldsymbol{t})$ for all $0 \le i \le N$. Then $\boldsymbol{t} = c^{-1}\boldsymbol{t'}$, where $c \in \mathbb{N}$, $\boldsymbol{t'} = (t'_0, \dots, t'_n) \in \mathbb{Z}^{n+1}$ and $\gcd(t'_0, \dots, t'_n) = 1$. For $0 \le i \le N$ this implies

$$x_i = wc^{-\delta}h_i(\boldsymbol{t'})$$

with $\delta = \deg(h_i)$. Since $x_i \in \mathbb{Z}$ and $\gcd\{h_0(\boldsymbol{t'}), \dots, h_N(\boldsymbol{t'})\}$ divides d, it follows that $w' = dwc^{-\delta} \in \mathbb{Z}$ and $(x_0, \dots, x_N) = \big(w'h_0^*(\boldsymbol{t'}), \dots, w'h_N^*(\boldsymbol{t'})\big)$. □

In the following Lemma 4 we give a simple criterion for the normalization of V to be isomorphic to a projective space without mentioning this normalization explicitly.

Lemma 4. *Let V be a projective variety over $\mathbb{Q}$. Then the following assertions are equivalent:*

(a) *The normalization of V is isomorphic to $\mathbb{P}^n_{\mathbb{Q}}$.*

(b) *There exists a finite birational morphism $\mathbb{P}^n_{\mathbb{Q}} \to V$.*

Proof. Let $\pi\colon \overline{V} \to V$ be a normalization of V.

(a) $\Rightarrow$ (b) If $\phi\colon \mathbb{P}^n_{\mathbb{Q}} \to \overline{V}$ is an isomorphism, then $\pi \circ \phi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$ is a finite birational morphism.

(b) $\Rightarrow$ (a) Let $\varphi\colon \mathbb{P}^n_{\mathbb{Q}} \to V$ be a finite birational morphism. Then $\varphi(\mathbb{P}^n_{\mathbb{Q}}) \subset V$ is closed, and since φ is birational, it follows that $\varphi(\mathbb{P}^n_{\mathbb{Q}}) \subset V$ is equidimensional. Hence φ is surjective, and the assertion follows by [7, Th. 2.24]. □

Obviously, Theorem 1 applies for rational varieties which are isomorphic to $\mathbb{P}^n_{\mathbb{Q}}$ for some $n \in \mathbb{N}$. We conclude with examples of rational varieties which are not isomorphic to some projective space and for which Theorem 1 can be used.

Example.
Let $V \subset \mathbb{P}^3$ be any *Steiner surface* defined over $\mathbb{Q}$ (see [5, Ch. 4] and [1]). Such a surface is a suitable projection of the Veronese surface $V_0 \subset \mathbb{P}^5$ into $\mathbb{P}^3$. Thus there is a surjective morphism $\mathbb{P}^2_{\mathbb{Q}} \to V$ and Theorem 1 applies. Since V has singular points, it is not isomorphic to $\mathbb{P}^2_{\mathbb{Q}}$.

As a special example, let $V \subset \mathbb{P}^3_{\mathbb{Q}}$ be the *Roman surface*, given by the homogeneous equation

$$X_1^2X_2^2 + X_2^2X_3^2 + X_3^2X_1^2 - X_0X_1X_2X_3 = 0\,, \tag{2}$$

whose singular locus is the union of the three lines

$$X_1 = X_2 = 0\,,\ X_2 = X_3 = 0 \text{ and } X_3 = X_1 = 0\,.$$

There is a surjective morphism $\varphi\colon \mathbb{P}^2_{\mathbb{Q}} \to V$, given on geometric points by

$$(t_0 : t_1 : t_2) \mapsto (t_0^2 + t_1^2 + t_2^2 : t_0t_1 : t_1t_2 : t_2t_0)\,.$$

For coprime integers $t_0,\, t_1,\, t_2 \in \mathbb{Z}$ we obviously have $\gcd\{t_0^2+t_1^2+t_2^2, t_0t_1, t_1t_2, t_2t_0\} = 1$, and thus we obtain for the set of solutions of the Diophantine equation (2) – up to those coming from non strongly $\mathbb{Q}$-rational points –

$$\begin{aligned}\mathcal{L}^* &= \big\{(x_0,x_1,x_2,x_3) \in \mathbb{Z}^4 \mid (x_0 : x_1 : x_2 : x_3) \in V_\varphi(\mathbb{Q})^*\big\} \cup \big\{(0,0,0,0)\big\}\\ &= \big\{(s(t_0^2+t_1^2+t_2^2), st_0t_1, st_1t_2, st_2t_0) \mid s, t_0, t_1, t_2 \in \mathbb{Z}\big\}\,.\end{aligned}$$

Let us finally remark that for the Roman surface V we have $V_\varphi(\mathbb{Q})^* \subsetneq V(\mathbb{Q})$. Indeed, for every $\mathbb{Q}$-rational point $p = (m : n : 0 : 0) = \varphi(t_0 : t_1 : t_2)$ of the singular line $X_2 = X_3 = 0$ with $n \neq 0$ we have

$$0 \neq r = \frac{m}{n} = \frac{t_0^2 + t_1^2}{t_0t_1} = \frac{t_0}{t_1} + \frac{t_1}{t_0}\,.$$

Therefore $p \in V_\varphi(\mathbb{Q})^*$ if and only if $r = x + x^{-1}$ for some $x \in \mathbb{Q}^\times$, which is equivalent to $r^2 - 4$ being the square of a rational number.

References

[1] A. Coffman, Steiner Surfaces, http://www.ipfw.edu/math/Coffman/steinersurface.html.
[2] S. Frisch, Remarks on polynomial parametrization of sets of integer points, *Comm. Algebra* **36** (2008), 1110-1114.
[3] S. Frisch and G. Lettl, Polynomial parametrization of the solutions of Diophantine equations of genus 0, *Funct. Approximatio, Comment. Math.* (to appear).
[4] S. Frisch and L. Vaserstein, Parametrization of Pythagorean triples by a single triple of polynomials, *J. Pure Appl. Algebra* **212** (2008), 271-274.
[5] P. Griffiths and J. Harris, Principles of Algebraic Geometry, J. Wiley & Sons, 1978.
[6] R. Hartshorne, Algebraic Geometry, GTM 52, Springer, 1977.
[7] S. Iitaka, Algebraic Geometry, GTM 76, Springer, 1982.
[8] P. Ribenboim, The new book of prime number records, Springer, 1996.
[9] L. Vaserstein, Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups, *Ann of Math.* (to appear).
[10] O. Zariski and P. Samuel, Commutative Algebra vol. II, GTM 29, Springer, 1960.

Institut für Mathematik und wissenschaftliches Rechnen, Karl-Franzens-Universität, Heinrichstrasse 36, A-8010 Graz, AUSTRIA

E-mail address: `franz.halterkoch@uni-graz.at`

E-mail address: `guenter.lettl@uni-graz.at`