Comm. Algebra 36 (3) (2008) 1110-1114

REMARKS ON POLYNOMIAL PARAMETRIZATION OF SETS OF INTEGER POINTS

Sophie Frisch

Abstract. If, for a subset S of $\mathbb{Z}^k$, we compare the conditions of being parametrizable (a) by a single k-tuple of polynomials with integer coefficients, (b) by a single k-tuple of integer-valued polynomials and (c) by finitely many k-tuples of polynomials with integer coefficients (variables ranging through the integers in each case), then $a \Rightarrow b$ (obviously), $b \Rightarrow c$, and neither implication is reversible. Condition (b) is equivalent to S being the set of integer k-tuples in the range of a k-tuple of polynomials with rational coefficients, as the variables range through the integers. Also, we show that every co-finite subset of $\mathbb{Z}^k$ is parametrizable a single k-tuple of polynomials with integer coefficients.

If $f = (f_1, \dots, f_k) \in (\mathbb{Z}[x_1, \dots, x_n])^k$ is a k-tuple of polynomials with integer coefficients in several variables, we call range or image of f the range of the function $f\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^k$ defined by substitution of integers for the variables; and likewise for a k-tuple of integer-valued polynomials $(f_1, \dots, f_k) \in (\mathrm{Int}(\mathbb{Z}^n))^k$, where

$$\mathrm{Int}(\mathbb{Z}^n) = \{g \in \mathbb{Q}[x_1, \dots, x_n] \mid \forall a \in \mathbb{Z}^n : g(a) \in \mathbb{Z}\}.$$

If $S \subseteq \mathbb{Z}^k$ is the range of $f = (f_1, \dots, f_k)$, we say that f parametrizes S.

We want to compare two kinds of polynomial parametrization of sets of integers or k-tuples of integers: by integer-valued polynomials and by polynomials with integer coefficients. Consider for instance the set of integer Pythagorean triples: it takes two triples of polynomials with integer coefficients, $\big(c(a^2 - b^2),\ 2cab,\ c(a^2 + b^2)\big)$ and $\big(2cab,\ c(a^2 - b^2),\ c(a^2 + b^2)\big)$ to parametrize the set of integer triples (x, y, z)

2000 *Mathematics Subject Classification.* Primary 11D85; Secondary 11C08, 13F20.

Key words and phrases. polynomial parametrization, integer-valued polynomial, range, image of a polynomial, polynomial mapping..

This note was written while the author was enjoying hospitality at Université de Picardie, Amiens.

satisfying $x^2 + y^2 = z^2$, but the same set can be parametrized by a single triple of integer-valued polynomials [2]. Another reason for studying parametrization by integer-valued polynomials are various sets of integers in number theory and combinatorics that come parametrized by integer-valued polynomials in a natural way, for example, the polygonal numbers

$$p(n,k) = \frac{(n-2)k^2 - (n-4)k}{2}$$

where $p(n,k)$ represents the k-th n-gonal number [3].

Now for our comparison of different kinds of polynomial parametrization of sets of integer points.

Theorem. *For a set $S \subseteq \mathbb{Z}^k$ consider the conditions:*

(A) *S is parametrizable by a k-tuple of polynomials with integer coefficients, i.e., there exists $f = (f_1, \ldots, f_k)$ in $(\mathbb{Z}[x_1, \ldots, x_n])^k$ (for some n) such that $S = f(\mathbb{Z}^n)$.*

(B) *S is parametrizable by a k-tuple of integer-valued polynomials, i.e., there exists $g = (g_1, \ldots, g_k)$ in $(\mathrm{Int}(\mathbb{Z}^m))^k$ (for some m) such that $S = g(\mathbb{Z}^m)$.*

(C) *S is a finite union of sets, each parametrizable by a k-tuple of polynomials with integer coefficients.*

(D) *S is the set of integer k-tuples in the range of a k-tuple of polynomials with rational coefficients, as the variables range through the integers, i.e., there exists $h = (h_1, \ldots, h_k)$ in $(\mathbb{Q}[x_1, \ldots, x_r])^k$ (for some r) such that $S = h(\mathbb{Z}^r) \cap \mathbb{Z}^k$.*

Then the following implications hold:

$$\begin{array}{ccc} A & & \\ \Downarrow & & \\ B & \Leftrightarrow & D \\ \Downarrow & & \\ C & & \end{array}$$

and C $\not\Rightarrow$ B, B $\not\Rightarrow$ A.

Of the implications in the theorem, A $\Rightarrow$ B and B $\Rightarrow$ D are trivial. We now show the nontrivial ones.

For D $\Leftrightarrow$ B, we first construct, for any $f \in \mathbb{Q}[x_1, \ldots, x_n]$, a parametrization of $f^{-1}(\mathbb{Z})$ by polynomials with integer coefficients, which we then plug into f to obtain an integer-valued polynomial.

Lemma 1. *If $q_1, \ldots, q_r$ are powers of different primes and for each i, S_i is a union of residue classes of $q_i\mathbb{Z}^k$ in $\mathbb{Z}^k$ then $\bigcap_{i=1}^r S_i \subseteq \mathbb{Z}^k$ is parametrizable by a k-tuple of polynomials with integer coefficients.*

Proof. We will first parametrize a union of residue classes of $q\mathbb{Z}^k$ in $\mathbb{Z}^k$ for a single prime power q. Let $a_0, \dots, a_s \in \mathbb{Z}^k$ be representatives of the residue classes in question, and let t such that $2^t > s$. Expressing $l \in \{0, 1, \dots, s\}$ in base 2, we obtain a sequence of digits $[l\,]_2 = (\varepsilon_0^{(l)}, \dots, \varepsilon_{t-1}^{(l)})$. Let m be a natural number such that z^m is either congruent to 0 or to 1 mod q for every integer z. Then

$$(qy_1, \dots, qy_k) + \sum_{l=0}^{s} a_l \prod_{i=0}^{t-1} e_i^{(l)}(x_i), \qquad \text{with} \quad e_i^{(l)}(x_i) = \begin{cases} x_i^m & \text{if } \varepsilon_i^{(l)} = 1 \\ 1 - x_i^m & \text{if } \varepsilon_i^{(l)} = 0 \end{cases}$$

parametrizes $\bigcup_{l=0}^{s}(q\mathbb{Z}^k + a_l)$.

Now let $q_1, \dots, q_r$ be powers of different primes, and for $1 \le i \le r$ let S_i be a union of residue classes mod $q_i\mathbb{Z}^k$ parametrized by a k-tuple of polynomials g_i. By Chinese remainder theorem there are $c_1, \dots, c_r$ with $c_i \equiv 1$ mod q_i and $c_i \equiv 0$ mod q_j for $j \neq i$. We may choose $c_1, \dots, c_r$ with $\gcd(c_1, \dots, c_r) = 1$. (E.g. by applying Dirichlet's theorem on primes in arithmetic progressions to find primes $p_i \in b_i + q_i\mathbb{Z}$, where b_i is the inverse of $\prod_{j\neq i} q_j$ mod q_i, and setting $c_i = p_i \prod_{j\neq i} q_j$, with $p_1, \dots, p_r$ different primes coprime to all q_j.) Finally, we set $h = \sum_{i=1}^{r} c_i g_i$. Then h parametrizes $\bigcap_{i=1}^{r} S_i$. $\square$

Lemma 2 (B $\Leftrightarrow$ *D*)**.** *Let $S \subseteq \mathbb{Z}^k$. Then there exists a k-tuple of integer-valued polynomials whose range is S if and only if there exists a k-tuple of polynomials with rational coefficients such that S is the set of integer points in its range* (*as the variables range through the integers*)*.*

Proof. The "only if" direction (that's B $\Rightarrow$ D) is trivial. For the other direction, D $\Rightarrow$ B, first consider the case $k = 1$ of a single rational polynomial $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)/c$ with $g(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ and $c \in \mathbb{N}$.

Let $T = \{a \in \mathbb{Z}^n \mid f(a) \in \mathbb{Z}\}$. If $c = q_1 \cdot \ldots \cdot q_r$ is the factorization of c into prime powers and $T_i = \{a \in \mathbb{Z}^n \mid g(a) \in q_i\mathbb{Z}\}$, then $T = \bigcap_{i=1}^{r} T_i$. For each i, T_i is a union of residue classes of $q_i\mathbb{Z}^n$. Hence T is parametrizable by an n-tuple of polynomials $(h_1, \dots, h_n) \in \mathbb{Z}[\underline{x}]^n$. Substituting h_i for x_i in f, we obtain an integer-valued polynomial $p(\underline{x}) = f(h_1(\underline{x}), \dots, h_n(\underline{x}))$ whose range is exactly the set of integers in the range of f.

In the case $k > 1$, the argument for the set of integer points in the range of a k-tuple of rational polynomials $(f_1, \dots, f_k)$, with $f_j(x_1, \dots, x_n) = g_j(x_1, \dots, x_n)/c$, is similar, using $T_i = \{a \in \mathbb{Z}^n \mid \forall j : \ g_j(a) \in q_i\mathbb{Z}\}$. $\square$

Lemma 3 (B $\Rightarrow$ C)**.** *If a set $S \subseteq \mathbb{Z}^k$ is parametrizable by a single k-tuple of integer-valued polynomials, it is parametrizable by a finite number of k-tuples of polynomials with integer coefficients.*

Proof. First consider an integer-valued polynomial $f(x)$ in one variable of degree d. Recall that the binomial polynomials $\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$ form a basis of the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$, so that there exist integers $a_0, \dots, a_d$ with $f = \sum_{n=0}^{d} a_n \binom{x}{n}$.

It is easy to see that $\binom{cy+j}{n} \in \mathbb{Z}[y]$ for any j whenever c is a common multiple of $1, 2, \ldots, n$. Therefore for $c = \mathrm{lcm}(1, 2, \ldots, d)$ and arbitrary j,

$$f_j(y) = f(cy + j) = \sum_{n=0}^{d} a_n \binom{cy + j}{n}$$

is in $\mathbb{Z}[y]$; and clearly the image of f is the union of the images of f_j, for $j = 0, \ldots, c - 1$.

Regarding integer-valued polynomials in several variables, products of binomial polynomials in one variable each $\prod_{i=1}^{n} \binom{x_i}{n_i}$ form a basis of $\mathrm{Int}(\mathbb{Z}^n)$ [1, Prop. XI.1.12]. So, if $f \in \mathrm{Int}(\mathbb{Z}^n)$ is of degree d_i in x_i, and c_i is a common multiple of $1, 2, \ldots, d_i$ then for each choice of $j_1, \ldots, j_n$, $f_{j_1,\ldots,j_n} = f(c_1y_1+j_1, \ldots, c_ny_n+j_n)$, as a $\mathbb{Z}$-linear combination of polynomials $\prod_{i=1}^{n} \binom{c_iy_i+j_i}{n_i} \in \mathbb{Z}[y_1, \ldots, y_n]$, is a polynomial with integer coefficients and the image of f is the union of the images of the polynomials $f_{j_1,\ldots,j_n}$ with $0 \le j_m < c_m$.

The same argument shows that the image of a vector of polynomials $(g_1, \ldots, g_k)$ in $(\mathrm{Int}(\mathbb{Z}^n))^k$ is the union of the images of $c_1 \cdot \ldots \cdot c_n$ vectors of polynomials in $(\mathbb{Z}[y_1, \ldots, y_n])^k$, where $c_i = \mathrm{lcm}(1, 2, \ldots, d_i)$, d_i denoting the highest degree of any g_m in the i-th variable. $\square$

Remark. B $\not\Rightarrow$ *A and* $C \not\Rightarrow$ B*: Finite sets of more than one element witness* $C \not\Rightarrow$ B*. The set of integer Pythagorean triples mentioned above is parametrizable by a single triple of polynomials in* $\mathrm{Int}(\mathbb{Z}^4)$*, but not by any triple of polynomials with integer coefficients in any number of variables* [2] *therefore* B $\not\Rightarrow A$*.*

This completes the proof of the theorem. The remainder of this note is devoted to the fact that every co-finite set is parametrizable by a single vector of polynomials with integer coefficients. (I was asked by Leonid Vaserstein in connection with a remark in [4] to publish a proof of this.)

Proposition. *Let* $S \subseteq \mathbb{Z}^k$ *such that* $\mathbb{Z}^k \setminus S$ *is finite. Then there exists a* k*-tuple of polynomials with integer coefficients whose range is* S*.*

Proof. We may suppose that the complement of S in $\mathbb{Z}^k$ is contained in a cuboid $\prod_{i=1}^{k}[0, n_i] = [0, n_1] \times \ldots \times [0, n_k]$, with n_i a non-negative integer for $1 \le i \le k$. We will first construct a polynomial vector whose image is $\mathbb{Z}^k \setminus \prod_{i=1}^{k}[0, n_i]$, by induction on k.

$k = 1$: for $n \ge 0$, the range of the polynomial f below is $\mathbb{Z} \setminus [0, n]$:

$$f = -x_5^2(x_1^2 + x_2^2 + x_3^2 + x_4^2 + 1) + (1 - x_5^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2 + n + 1).$$

Once we have a polynomial vector $(f_1, \ldots, f_{k-1})$ parametrizing $\mathbb{Z}^{k-1} \setminus \prod_{i=1}^{k-1}[0, n_i]$ and a polynomial f with range $\mathbb{Z} \setminus [0, n_k]$, we set

$$g_i = (1 + {x_i}^2)(1 - z^2)^{2m} f_i + z^2 x_i \quad (1 \le i < k)$$
$$\text{and} \quad g_k = (1 + y^2) z^{2m} f + (1 - z^2) y$$

with m sufficiently large, see below, and check that the range of $(g_1, \dots, g_k)$ is $\mathbb{Z}^k \setminus \prod_{i=1}^k [0, n_i]$: For $z = x_1 = \dots = x_{k-1} = 0$ we get $(f_1, \dots, f_{k-1}, y)$, while for $z \in \{1, -1\}$ and $y = 0$, we have $(x_1, \dots, x_{k-1}, f)$, so that $(g_1, \dots, g_k)$ certainly covers the desired range.

Also, we stay within the desired range. Indeed, for $z = 0$, the first $k-1$ coordinates become $(1 + {x_i}^2) f_i$, and their image lies within the image of $(f_1, \dots, f_{k-1})$, and for $z \in \{1, -1\}$ the last coordinate is $(1 + y^2) f$, whose image is contained in the image of f.

Let $n = \max_i\{n_i\}$. By choosing m sufficiently large such that

$$|(1 + x^2)(1 - z^2)^{2m}| > |z^2 x| + n \quad \text{and} \quad |(1 + y^2) z^{2m}| > |(1 - z^2) y| + n$$

for all z with $|z| \geq 2$ and all values of x and y, we make sure that $(g_1, \dots, g_k)$ stays within the desired range also for $|z| \geq 2$.

Having constructed a polynomial vector with range $\mathbb{Z}^k \setminus \prod_{i=1}^k [0, n_i]$, we can add additional values to the range, one by one, as follows.

If $g = (g_1, \dots, g_k)$ is a polynomial vector whose image contains $\mathbb{Z}^k \setminus \prod_{i=1}^k [0, n_i]$, but does not contain $0 \in \mathbb{Z}^k$, and c is in $\prod_{i=1}^k [0, n_i]$, let

$$h = w^{2t} g + (1 - w^2) c,$$

with t such that $2^{2t-2} > \max_i\{n_i\}$ then the range of h is exactly the range of g together with the (possibly additional) value c. If the value $c = 0 \in \mathbb{Z}^k$ is to be added to the range of g, it must be added last. $\square$

References

1. Paul-Jean Cahen and Jean-Luc Chabert, *Integer-valued polynomials*, Amer. Math. Soc., Providence, RI, 1997.
2. Sophie Frisch and Leonid Vaserstein, *Parametrization of Pythagorean triples by a single triple of polynomials*, J. Pure Appl. Algebra 212 (2008) 271–274.
3. Melvyn B. Nathanson, *Additive number theory. The classical bases.*, Springer, New York, 1996.
4. Leonid Vaserstein, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, to appear in Ann. of Math..

Institut für Mathematik A, Technische Universität Graz, A-8010 Graz, Austria
frisch@tugraz.at