Parametrizing over integral values of polynomials over

Giulio Peruginelli, Umberto Zannier

Comm. Algebra 38 (1), 119-130, 2010

Parametrizing over $\mathbb{Z}$ integral values of polynomials over $\mathbb{Q}$

G. Peruginelli U. Zannier

Abstract

Given a polynomial $f \in \mathbb{Q}[X]$ such that $f(\mathbb{Z}) \subset \mathbb{Z}$, we investigate whether the set $f(\mathbb{Z})$ can be parametrized by a multivariate polynomial with integer coefficients, that is, the existence of $g \in \mathbb{Z}[X_1, \dots, X_m]$ such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$. We offer a necessary and sufficient condition on f for this to be possible. In particular it turns out that some power of 2 is a common denominator of the coefficients of f and there exists a rational β with odd numerator and odd prime-power denominator such that $f(X) = f(\beta - X)$. Moreover if $f(\mathbb{Z})$ is likewise parametrizable, then this can be done by a polynomial in one or two variables.

1 Introduction

In this paper we shall consider *integral-valued polynomials*, by which we mean those taking integral values on $\mathbb{Z}$; they make up a ring, sometimes denoted $Int(\mathbb{Z})$ (as in [CC]). It contains the binomial polynomials $\binom{X}{n} \doteqdot \frac{X(X-1)\dots(X-(n-1))}{n!}$, showing that it is strictly larger than $\mathbb{Z}[X]$. (Actually, the binomial polynomials are free abelian-group generators for it, a well-known fact easy to prove by taking finite differences.)

For a given integral-valued f, we explore here if and how the subset $f(\mathbb{Z})$ of $\mathbb{Z}$ can be parametrized by values of polynomials with *integer coefficients*, even if f has merely rational coefficients. In this direction, note that if $Nf(X) \in \mathbb{Z}[X]$, $N \in \mathbb{N} \setminus \{0\}$, the polynomials $g_r(X) := f(r + NX)$ clearly have integer coefficients for any $r \in \mathbb{Z}$ and satisfy $\cup_{r=0}^{N-1} g_r(\mathbb{Z}) = f(\mathbb{Z})$; hence a parametrization over $\mathbb{Z}$ is immediately written down if we are allowed to use several polynomials for a given f.

However, it seems reasonable to seek a **single** polynomial $g = g_f$, in any number m of variables, but with integer coefficients, with the property that $g(\mathbb{Z}^m) = f(\mathbb{Z})$.

In other words, roughly speaking our question is:

Question: *For which integral-valued polynomials $f(X)$ does there exist a polynomial $g \in \mathbb{Z}[X_1, \dots, X_m]$ such that $g(\mathbb{Z}^m) = f(\mathbb{Z})$?* For instance: *does such a g always exist?*

And also: *How can we describe such a possible g in terms of f, and in particular how small can we take the number m of variables, provided some such g exists at all?*

To our knowledge these questions do not appear explicitly in the literature, but they are somewhat near to issues studied in [F] and [FV]. For instance, it follows from [FV]

that the set of Pythagorean Triples of $\mathbb{Z}^3$, although parametrizable by a single triple of integer-valued polynomials in four variables, cannot be parametrized by a single triple of integer-coefficient polynomials in any number of variables. However, neither the results nor the methods of these papers provide answers in the basic case considered here, that is for a single polynomial f depending on a single variable. Here we shall obtain a simple classification which may be considered in a sense complete and shall be stated very soon.

Three examples. Let us first see some simple examples illustrating what happens.

1. Consider the polynomial $f(X) = X(1-X)/2$, which is integral-valued but has not integer coefficients. Defining as above $g_r(X) = f(r+2X) \in \mathbb{Z}[X]$, we see that $f(\mathbb{Z}) = g_0(\mathbb{Z}) \cup g_1(\mathbb{Z})$. This leaves us with two polynomials; however now the identity $f(X) = f(1-X)$ yields $g_1(X) = f(-2X) = g_0(-X)$. So g_0 and g_1 take the same values on $\mathbb{Z}$ and the conclusion is that $f(\mathbb{Z})$ can be parametrized by the single polynomial $g_0(X) \in \mathbb{Z}[X]$. Also, the same remains true for $F(f(X))$ in place of $f(X)$, for any $F \in \mathbb{Z}[X]$, so any power of 2 may appear as a denominator in a similar example.

The same phenomenon does not occur with binomial polynomials of higher degree; in fact, we shall see that no odd prime number can divide the denominator of a polynomial such that $f(\mathbb{Z})$ is likewise parametrizable.

2. If we slightly change the data by setting $f^*(X) = 3X(1-3X)/2 = f(3X)$ where f is as at n. 1, we can easily realize that the same trick does not work (although $g_0(\mathbb{Z}) = f(\mathbb{Z})$, we do not have $g_0(3\mathbb{Z}) = f(3\mathbb{Z})$). Actually, a special case of our results says that the present $f^*(\mathbb{Z})$ cannot be parametrized by using a single variable. Nevertheless, by using two variables we can succeed. More precisely, set $L(Y_1, Y_2) := 3Y_1 + Y_2^2 - 1$; one may verify (or see the arguments for Theorem 1.2 below) that $f^*(\mathbb{Z}) = g_0(L(\mathbb{Z}^2))$.

3. Let us change further the first example by setting $f_*(X) = 15X(1-15X)/2$. Now neither the first nor the second trick work. Actually, it will follow that $f_*(\mathbb{Z})$ is not of the shape $g(\mathbb{Z}^m)$, no matter the integer m and the polynomial $g \in \mathbb{Z}[Y_1, \dots, Y_m]$.

These examples give the complete picture, as in the following results:

Theorem 1.1 *Let $f(X) \in \mathbb{Q}[X] \setminus \mathbb{Z}[X]$ and suppose that there exists $g \in \mathbb{Z}[Y_1, \dots, Y_m]$ such that $f(\mathbb{Z}) = g(\mathbb{Z}^m)$.*

Then there exist odd coprime integers r, s, with s a prime power or 1, and a polynomial $F \in \mathbb{Z}[X]$ such that $f(X) = F(\frac{sX(r-sX)}{2})$. In particular $2^{\frac{\deg f}{2}} f(X/s) \in \mathbb{Z}[X]$.

If we can take $m = 1$, i.e. $g \in \mathbb{Z}[Y]$, then s is necessarily 1.

Finally, such r, s, F are uniquely determined by f.

Note that in particular $\deg f$ is even, $f(\frac{2X}{s})$ is in $\mathbb{Z}[X]$ and $f(X) = f(\frac{r}{s} - X)$, an invariance which determines r/s. This theorem admits the following strong converse.

Theorem 1.2 *Let $f(X) = F(\frac{sX(r-sX)}{2})$ for a polynomial $F \in \mathbb{Z}[X]$ and coprime odd integers r, s, with s a prime power or 1. Then there exists a polynomial $g \in \mathbb{Z}[Y_1, Y_2]$ such that $f(\mathbb{Z}) = g(\mathbb{Z}^2)$.*

If either $f \in \mathbb{Z}[X]$ or $s = 1$, there exists $g \in \mathbb{Z}[Y]$ with $f(\mathbb{Z}) = g(\mathbb{Z})$.

In particular, these theorems show that if $f(\mathbb{Z}) = g(\mathbb{Z}^m)$ for some $g \in \mathbb{Z}[\underline{Y}]$ then one can take $m = 1$ or 2. To test with little effort whether a given polynomial $f(X)$ is of the relevant shape, we have the following complementary result:

Criterion *The polynomial $f(X) \in \mathbb{Q}[X]$ is of the shape $F(\frac{sX(r-sX)}{2})$ for an $F \in \mathbb{Z}[X]$ and coprime odd integers r, s if and only if $f(\frac{r}{s} - X) = f(X)$ and $f(2X/s) \in \mathbb{Z}[X]$.*

These results will be proved in several steps, treated in separate sections. The proofs give further informations on the shape of all the possible parametrizations, not stated in the theorems for simplicity (see the final remarks).

Analogous results may hold over rings other than $\mathbb{Z}$, and the case of rings of S-integers in number fields will be the object of a future paper by the first author. Here we shall not consider any such generalization.

Remark. It follows from Theorem 1.1 and the proof-arguments for Theorem 1.2 that if $f(\mathbb{Z}) = g(\mathbb{Z}^m)$ for some $g \in \mathbb{Z}[Y_1, \ldots, Y_m]$, then the strong local conditions hold that *for every prime p there exists $g_p \in \mathbb{Z}_{(p)}[Y_1, Y_2]$ with $f(\mathbb{Z}_{(p)}) = g_p(\mathbb{Z}^2_{(p)})$*. (Can this be proved more directly?) However there is no *local-global principle* (i.e. a converse) in this sense: a counterexample comes e.g. from the polynomial $f_*(X)$ of Example 3 above.

Notation. We shall use throughout the following terminology.

- For a subset A of $\mathbb{Z}$ we say that A is **$\mathbb{Z}$-parametrizable** if there exist $m \in \mathbb{N}$ and a polynomial $g \in \mathbb{Z}[\underline{X}] = \mathbb{Z}[X_1, \ldots, X_m]$ such that $A = g(\mathbb{Z}^m)$.

- For a prime p, as usual we shall denote the localization of $\mathbb{Z}$ at p by $\mathbb{Z}_{(p)} = \{r/s : r, s \in \mathbb{Z}, p \nmid s\}$.

- Capital letters shall usually denote variables and lower-case letters specializations of them to integers. Also, we shall use e.g. $\underline{Y}$ to denote $(Y_1, \ldots, Y_m)$.

Acknowledgments

We wish to thank S. Frisch and A. Schinzel for their kind interest.

2 Equations $f(X) = f(Y)$

We shall need some facts on the equation $f(X) = f(Y)$ for a polynomial f. They are known, but for completeness we give short elementary proofs for them.

Proposition 2.1 *Let $f \in \mathbb{Q}[X]$ be not constant. If for infinitely many integers $n \in \mathbb{N}$ there exists $q = q_n \in \mathbb{Q}$ such that $f(q) = f(n)$ and $q \neq n$, then there exists $\beta \in \mathbb{Q}$ such that $f(X) = f(\beta - X)$. Moreover $q_n = -n + \beta$ for all but finitely many such n.*

Proof : Hilbert Irreducibility Theorem would be a comfortable tool; however for this special case of the rational field a simple self-contained (Runge's) argument is possible.

For n in our infinite set of integers, we have $f(q_n) = f(n)$ and $q_n \neq n$. Let $d = \deg f$ and let a be its leading coefficient. Since $f(x) = ax^d + O(x^{d-1})$ for large x, we obtain

that $q_n = O(n)$ and $q_n^d = n^d + O(n^{d-1}) = n^d(1 + O(n^{-1}))$. Hence $q_n = \epsilon n + O(1)$, where $\epsilon = \pm 1$ may depend on n. Also, the equation $f(q_n) - f(n) = 0$ implies that the rational numbers q_n have bounded denominators: if $Df(X) \in \mathbb{Z}[X]$ for $D \in \mathbb{Z}$, we have $Daq_n \in \mathbb{Z}$.

Then the rational numbers $q_n - \epsilon n$ are bounded in absolute value and have bounded denominators, hence the function $n \mapsto q_n - \epsilon n$ takes values in a finite set. If β is any value taken infinitely many times for a fixed value of ϵ, we have $f(\epsilon n + \beta) = f(n)$ for an infinity of n, which implies $f(\epsilon X + \beta) = f(X)$ identically. If $\epsilon = 1$, this forces $\beta = 0$, hence $q_n = n$, which is excluded. Therefore for all but finitely many n in our set we must have $\epsilon = -1$ and $f(-X + \beta) = f(X)$ for each value β of $q_n + n$ taken infinitely often. If this also holds for β' in place of β, f is invariant for translation by $\beta' - \beta$, and so $\beta' = \beta$, showing that β is uniquely determined and concluding the proof. □

Proposition 2.2 *Let $f \in \mathbb{Q}[X]$ be nonconstant and let $R, S \in \mathbb{Q}[\underline{Y}]$ be also nonconstant and such that $f(R) = f(S)$. Then either $R = S$ or $R = -S + \beta$ for some $\beta \in \mathbb{Q}$ such that $f(X) = f(\beta - X)$ identically, and in this case β is uniquely determined by f.*

Proof : This can be easily derived from the previous proposition, but here is a direct short proof (a function field version of the previous one), which also leads to analogues over fields other than $\mathbb{Q}$. Write $f(X) = aX^d +$ lower degree terms, where $a \neq 0$ and $d \geq 1$. If $D = \max(\deg R, \deg S) > 0$ we see from $f(R) = f(S)$ that the degree of $a(R^d - S^d)$ is $\leq (d-1)D$. Now, $R^d - S^d$ is the product of factors $R - \zeta S$ over all d-th roots of unity ζ. Then, exactly one factor, say $R - \delta S$, vanishes or has degree $< D$. If this factor vanishes, then $\delta = \pm 1$ because R, S are over $\mathbb{Q}$. If the factor does not vanish, let D_1 be its degree. Then $\deg a(R^d - S^d) = D_1 + (d-1)D$, forcing $D_1 = 0$. Hence $R = \delta S + \beta$ for a constant β. Again, we must have $\delta = \pm 1$ and $\beta \in \mathbb{Q}$. If $\delta = 1$ then $f(S + \beta) = f(S)$, hence $f(X) = f(X + \beta)$ and $\beta = 0$, because f is nonconstant and S is transcendental. If $\delta = -1$ then $f(X) = f(-X + \beta)$ for the same reason. If β' has the same property, then $f(X) = f(X + \beta' - \beta)$, hence $\beta = \beta'$. □

3 Gauss norms

In the sequel we shall denote by v a valuation on a field K and we shall denote by O_v the valuation ring; also, we shall denote by $|\ |_v$ the associated norm, normalized in some way. As usual, $|\ |_p$ shall denote the p-adic norm on $\mathbb{Q}$.

We recall the definition of the **Gauss norm** of a polynomial $g \in K[X_1, \ldots, X_m]$, simply as the sup-norm of the coefficients with respect to $|\ |_v$; we shall denote it by $\|g\|_v$. Recall that if v is ultrametric the Gauss norm is multiplicative on $K[\underline{X}]$ (Gauss Lemma) and extends $|\ |_v$ to an ultrametric norm on $K(X)$.

Moreover, we have

$$|g(\underline{x})|_v \leq \|g\|_v \qquad \text{for all } \underline{x} \in O_v^m.$$

Proposition 3.1 *Let p be a prime number, let $f \in \mathbb{Q}[X]$, $Q \in \mathbb{Q}[X_1, \ldots, X_m]$ and suppose that $\|f(Q(\underline{X}))\|_p < \|f(X)\|_p$.*

Then either

(i) $Q(\underline{X}) = c + pR(\underline{X})$ where $c \in \mathbb{Z}_{(p)}$, $R \in \mathbb{Z}_{(p)}[\underline{X}]$ or

(ii) $Q(\underline{X}) = c(1 + pR(\underline{X}))$ where $c \in \mathbb{Q} \setminus \mathbb{Z}_{(p)}$, $R \in \mathbb{Z}_{(p)}[\underline{X}]$.

Proof : Let K be the splitting field over $\mathbb{Q}$ of the polynomial $f(X)$ of degree d, and let v be a valuation of K above p, with valuation ring $O_v \subset K$ and uniformizer π (that is, $v(\pi) = 1$). In $O_v[X]$ we may factor f as

$$f(X) = a \prod_{i=1}^{d} (\alpha_i X - \beta_i)$$

where $a \in K$ and where $\alpha_i, \beta_i \in O_v$ are coprime, $\alpha_i \neq 0$.

Now, $f \circ Q(\underline{X}) = a \prod_i (\alpha_i Q(\underline{X}) - \beta_i)$ whence by assumption

$$\prod_i \|\alpha_i Q(\underline{X}) - \beta_i\|_v < \prod_i \|\alpha_i X - \beta_i\|_v = 1.$$

So there is an index j such that $\|\alpha_j Q(\underline{X}) - \beta_j\|_v < 1$ which implies

$$\|Q(\underline{X}) - \xi_j\|_v < |\alpha_j|_v^{-1} \tag{1}$$

where $\xi_j = \beta_j/\alpha_j \in K$ is the corresponding root of f.

First we consider the case $\pi \nmid \alpha_j$, i.e. $|\alpha_j|_v = 1$. By (1), $\|Q(\underline{X}) - \xi_j\|_v < 1$.

We deduce that all the coefficients of Q except the constant term lie in $p\mathbb{Z}_{(p)}$. Also, $|\alpha_j|_v = 1$ implies that ξ_j lies in O_v, hence the constant term of $Q(\underline{X})$ belongs to $\mathbb{Z}_{(p)}$.

All of this plainly yields the representation for Q written in case (i).

Suppose now that $\pi | \alpha_j$, which implies $\pi \nmid \beta_j$ since α_j and β_j are coprime. Hence $|\beta_j|_v = 1$ and $\xi_j = \beta_j/\alpha_j \notin O_v$ which means $|\xi_j|_v > 1$. From equation (1) we have

$$\|Q - \xi_j\|_v < |\xi_j|_v.$$

We deduce that the coefficient of the $\underline{i}$-th term in Q has the shape $\xi_j \pi^{n_{\underline{i}}} u_{\underline{i}}$ for $\underline{i} > \underline{0}$, whereas $Q(\underline{0}) = \xi_j u_{\underline{0}}$ where $n_{\underline{i}} > 0$ and $u_{\underline{i}} \in O_v^*$. So there exists a polynomial $S \in O_v[\underline{X}]$ such that $S(\underline{0}) = 0$ and

$$Q(\underline{X}) = Q(\underline{0})(1 + \pi S(\underline{X}))$$

Since Q has rational coefficients, πS has coefficients in $p\mathbb{Z}_{(p)}$. Note that $|Q(\underline{0})|_v = |\xi_j|_v > 1$, so $c := Q(\underline{0}) \in \mathbb{Q} \setminus \mathbb{Z}_{(p)}$, proving finally the stated representation. □

Proposition 3.2 *Let $H \in \mathbb{Q}[Y_1, \ldots, Y_m]$ and suppose that for a prime p the set $H(\mathbb{Z}_{(p)}^m) \cap \mathbb{Z}_{(p)}$ is not contained in a single class modulo p. Let $\sigma \in \mathbb{Q}$ be such that $|\sigma|_p = \|H\|_p$. Then for any $F \in \mathbb{Q}[X]$ we have the Gauss-norm inequalities*

$$\|F(X)\|_p \leq \|F(\sigma X)\|_p \leq \|F(H)\|_p.$$

Proof : This could be easily derived from the previous proposition, but a direct proof is perhaps even shorter. We remark at once that $|\sigma|_p \geq 1$, for otherwise $H(\mathbb{Z}^m_{(p)})$ would be contained in $p\mathbb{Z}_{(p)}$, against the assumptions. This proves the left-hand inequality.

As to the right-hand one, by factoring F over $\overline{\mathbb{Q}}$ it suffices to prove that for any algebraic number γ and for any valuation of $\overline{\mathbb{Q}}$ above p, we have

$$\|\sigma X - \gamma\|_v \leq \|H - \gamma\|_v.$$

For this, let $n \in T := H(\mathbb{Z}^m_{(p)}) \cap \mathbb{Z}_{(p)}$, so $n = H(\underline{y}_n)$ for some $\underline{y}_n \in \mathbb{Z}^m_{(p)}$. Then we have $n - \gamma = (H - \gamma)(\underline{y}_n)$; therefore, since $|\underline{y}_n|_v \leq 1$, we have for all $n \in T$

$$|n - \gamma|_v \leq \|H - \gamma\|_v.$$

Now, letting again $n \in T$ (T is not empty by assumption), note that:

1. If $|\gamma|_v \neq |\sigma|_v$, then trivially $\|H - \gamma\|_v = \max(\|H\|_v, |\gamma|_v) = \max(|\sigma|_v, |\gamma|_v)$.

2. If $|\gamma|_v = |\sigma|_v$ then $\|H - \gamma\|_v \geq |\gamma|_v$, for otherwise from the last displayed inequality we derive $|n - \gamma|_v < |\gamma|_v$ for every $n \in T$. But this implies that $|\gamma|_v = |\sigma|_v = 1$ and in turn that $n \in T$ is constant modulo p, contrary to the assumptions.

Hence we have $\|H - \gamma\|_v \geq \max\{|\sigma|_v, |\gamma|_v\}$, which is just what we need since the v-adic Gauss norm of $\sigma X - \gamma$ is precisely the right-hand side. □

4 Main arguments

In this section we prove Theorem 1.1. The proof will implicitly follow from a sequence of five lemmas.

From now on we shall suppose that $f \in \mathbb{Q}[X]$ is a nonconstant polynomial such that $f(\mathbb{Z})$ is $\mathbb{Z}$-parametrizable. For a suitable $g \in \mathbb{Z}[Y_1, \ldots, Y_m]$ we shall then have

$$f(\mathbb{Z}) = g(\mathbb{Z}^m). \tag{2}$$

We let a, d be respectively the leading coefficient and degree of f. We assume that $f \notin \mathbb{Z}[X]$ and we let p be a prime number occurring in the denominator of f. (This p shall be shown to be 2, and from that point onwards the letter p shall not be restricted in the present way.)

Let us express $f(X) - g(\underline{Y})$ as a product of factors in $\mathbb{Q}[X, \underline{Y}]$, writing

$$f(X) - g(\underline{Y}) = B(X, \underline{Y}) \prod_{i=1}^{k} (X - L_i(\underline{Y})), \tag{3}$$

where $L_i \in \mathbb{Q}[\underline{Y}]$ and where $B \in \mathbb{Q}[X, \underline{Y}]$ has no factor of degree < 2 in X.

Let us define

$$\Omega_i := \{\underline{y} \in \mathbb{Z}^m \ : \ L_i(\underline{y}) \in \mathbb{Z}\}, \qquad C_i := L_i(\Omega_i). \tag{4}$$

Note that

$$C_i = L_i(\Omega_i) = \mathbb{Z} \cap L_i(\mathbb{Z}^m) \tag{5}$$

Lemma 4.1 *We have* $\bigcup_{i=1}^{k} \Omega_i = \mathbb{Z}^m$. *In particular,* $k \geq 1$.

Proof : Note that if $q \in \mathbb{N}$ is a common denominator for all the coefficients of all the L_i, then each Ω_i is a finite union of arithmetic progressions in $\mathbb{Z}^m$ of modulus q, by which we mean subsets of $\mathbb{Z}^m$ of the shape $\underline{\alpha} + q\mathbb{Z}^m$. Suppose that the conclusion is false. Then there exists a whole arithmetic progression $\Omega = \underline{\rho} + q\mathbb{Z}^m \subset \mathbb{Z}^m$ disjoint from $\bigcup_{i=1}^{k} \Omega_i$, i.e. such that for all $i = 1, \ldots, k$ and all $\omega \in \Omega$, $L_i(\omega) \notin \mathbb{Z}$.

By Hilbert Irreducibility Theorem there exists $\underline{y} \in \mathbb{Z}^m$ such that each factor of $B(X, \underline{\rho}+q\underline{y})$ irreducible over $\mathbb{Q}$ has still degree > 1 in X; then the equation $B(X, \underline{\rho}+q\underline{y}) = 0$ has no rational root. Also, since $\underline{\rho} + q\underline{y} \in \Omega$, no factor $X - L_i(\underline{y})$ can have an integral root. However, this is a contradiction with equation (3), because $g(\underline{\rho} + q\underline{y})$ is supposed to be in the image $f(\mathbb{Z})$. This contradiction completes the proof. $\square$

Lemma 4.2 *We have either* $k = 1$ *or* $k = 2$. *In this last case there exists a unique* $\beta \in \mathbb{Q}$ *such that* $f(X) = f(\beta - X)$ *and* $L_1(\underline{Y}) + L_2(\underline{Y}) = \beta$.

Proof : Note that for $i, j = 1, \ldots, k$ we have $f(L_i(\underline{Y})) = f(L_j(\underline{Y})) = g(\underline{Y})$.

Clearly no L_i can be constant and we may apply Proposition 2.2 to deduce that for each i either $L_i = L_1$ or $L_i = \beta_i - L_1$ for a rational β_i such that $f(X) = f(\beta_i - X)$.

Now, the first case cannot occur for $i > 1$ because $f(X) - g(\underline{Y})$ has no multiple factors in X (as its derivative $f'(X)$ is nonzero). Also, for the same reason the second case cannot occur for more than one index i, because β_i, if it exists, is uniquely determined by f (see Prop. 2.2). Hence either $k = 1$, or $k = 2$, in which case $L_2 = \beta - L_1$ for a $\beta \in \mathbb{Q}$, uniquely determined, such that $f(X) = f(\beta - X)$. $\square$.

Lemma 4.3 *We have* $k = p = 2$ *and, for* $i = 1, 2$, $L_i(\underline{Y}) = c_i + 2R_i(\underline{Y})$ *where* $c_i \in \mathbb{Z}_{(2)}$, $R_i \in \mathbb{Z}_{(2)}[\underline{Y}]$, *and also* $\beta = L_1 + L_2 \in \mathbb{Z}_{(2)} \setminus 2\mathbb{Z}_{(2)}$. *Further,* C_i *contains all large integers in the class* c_i *modulo* 2 *and is contained in this class. Finally,* $C_1 \cup C_2$ *contains all large integers, and* $C_1 \cap C_2$ *is empty.*

Proof : Since f has not p-integer coefficients but $f(L_i) = g$ does, we may apply Proposition 3.1 with L_i in place of Q. If the first alternative (i) of that lemma occurs for $i = 1$ or $i = 2$ (if $k = 2$), then clearly $L_i(\Omega_i)$, which equals $L_i(\mathbb{Z}^m) \cap \mathbb{Z}$ (see equation (5)), is either empty or anyway contained in a single class modulo p. If the second alternative (ii) holds, then Ω_i is certainly empty. In both cases we deduce that $C_i = L_i(\Omega_i) = L_i(\mathbb{Z}^m) \cap \mathbb{Z}$ is contained in a single class modulo p, and in particular C_i has upper density $\leq 1/p$.

Now, $f(\mathbb{Z}) = g(\mathbb{Z}^m)$, so for all $n \in \mathbb{Z}$ there exists $\underline{y}_n \in \mathbb{Z}^m$ such that $f(n) = g(\underline{y}_n) = f(L_1(\underline{y}_n))$. The values $L_1(\underline{y}_n)$ are rational so by Proposition 2.1 for all large n we have either $n = L_1(\underline{y}_n)$ or $n = \beta - L_1(\underline{y}_n)$ where $f(\beta - X) = f(X)$. This last alternative holds only if $k = 2$, in which case $\beta - L_1 = L_2$ and, for the relevant integers n, we have $n = \beta - L_1(\underline{y}_n) = L_2(\underline{y}_n)$. Hence all large elements of $\mathbb{Z}$ must lie in C_1, if $k = 1$, or in $C_1 \cup C_2$ if $k = 2$.

Since the 'density' of C_i is $\leq p^{-1}$, all of this proves that $k = 2$, that $p = 2$, that no C_i can be empty and that $C_1 \cap C_2$ is empty (because C_1, C_2 are contained in single residue classes mod p which must be distinct since $C_1 \cup C_2$ contains all large integers).

In particular, for no index $i = 1, 2$ the second alternative (ii) of Proposition 3.1 can occur, so (i) holds in both cases and for $i = 1, 2$ we have the representation $L_i = c_i + 2R_i(\underline{Y})$, for 2-integral c_i, R_i. Since $C_1 \cup C_2$ contains all large integers and since C_1, C_2 are disjoint, we deduce that each of them contains all large integers in a corresponding residue class modulo 2, i.e. the class of c_i. Since $\beta = L_1 + L_2$ it also follows that $\beta \in \mathbb{Z}_{(2)} \setminus 2\mathbb{Z}_{(2)}$. The lemma is thus proved. □

At the light of these facts, we may renumber the indices $1, 2$ and change c_1, c_2 in their class modulo $2\mathbb{Z}_{(2)}$ to assume that $c_1 = 0$ and $c_2 = 1$, so

$$L_1(\underline{Y}) = 2R_1(\underline{Y}), \qquad L_2(\underline{Y}) = \beta - L_1(\underline{Y}) = 1 + 2R_2(\underline{Y}) \qquad R_1, R_2 \in \mathbb{Z}_{(2)}[\underline{Y}]. \tag{6}$$

Also, we write, as we may,

$$\beta = \frac{r}{s}, \qquad B(X) = B_\beta(X) := \frac{sX(r - sX)}{2}. \tag{7}$$

where r, s are coprime odd integers, $s > 0$. Note that $B(X) = B(\beta - X)$ and that $B(X)$ is integral-valued but does not lie in $\mathbb{Z}[X]$.

Lemma 4.4 *There exists a polynomial $F \in \mathbb{Z}[X]$ such that $f(X) = F(B_\beta(X))$ where β is the unique rational such that $f(X) = f(\beta - X)$. In particular, the degree d of f is even and $2^{\frac{d}{2}} f(X/s) \in \mathbb{Z}[X]$.*

Proof : Note that $[\mathbb{Q}(X) : \mathbb{Q}(B)] = 2$ and $\mathbb{Q}(B)$ is contained in the subfield of $\mathbb{Q}(X)$ invariant under the automorphism $X \mapsto \beta - X$. Since this automorphism has order 2, $\mathbb{Q}(B)$ is the full field of invariants, hence $f \in \mathbb{Q}(B)$. But X is integral over $\mathbb{Q}[B]$ so also $f(X)$ is integral. Since $\mathbb{Q}[B]$ is integrally closed, we conclude that $f \in \mathbb{Q}[B]$, so

$$f(X) = F(B(X))$$

for a polynomial $F \in \mathbb{Q}[X]$ (which could of course also be shown directly). This implies that $d = \deg f = 2 \deg F$, so d is even. To go on, we prove that F has integral coefficients.

For convenience we put $u(X) := f(X/s) = F(X(r - X)/2)$.

Let p be a possible odd prime in the denominator of F. (This has not to be confused with the possible prime divisor of the denominator of f, which has been shown to be 2.) We shall distinguish some cases.

Suppose first that $p|s$ (so p is odd). Since $L_1 + L_2 = \beta$, there is an index $i \in \{1, 2\}$ such that $\|L_i\|_p \geq |\beta|_p = |s^{-1}|_p$. By Lemma 4.3, $\mathbb{Z} \cap L_i(\mathbb{Z}^m)$ contains all large integers in a class modulo 2, hence is not contained in a single class modulo p. Therefore we may apply (the right-hand inequality of) Proposition 3.2 with f in place of F and L_i in place of H. We obtain, letting $\sigma \in \mathbb{Q}$ be such that $|\sigma|_p = \|L_i\|_p \geq |s^{-1}|_p$,

$$\|f(\sigma X)\|_p \leq \|f(L_i)\|_p.$$

The right side is ≤ 1 because $f(L_i) = g$ has integer coefficients. Hence $f(\sigma X)$ has p-integral coefficients and *a fortiori* this is true of $u(X)$. Suppose that $G := p^t F$, $t > 0$, has

p-integral coefficients not all divisible by p in $\mathbb{Z}_{(p)}$. Then $G(X(r-X)/2) = p^t u(X) \equiv 0 \pmod{p}$, the reduction of $X(r-X)/2$ being defined since $p > 2$. But $X(r-X)/2$ has nonconstant reduction mod p, hence this implies $G \equiv 0 \pmod{p}$, a contradiction.

If $p > 2$ and p does not divide s, then $u(X)$ has again p-adic integer coefficients, since this is true of $f(X)$, and then the last argument again proves that $F \in \mathbb{Z}_{(p)}[X]$.

Hence no prime $p \neq 2$ may occur in the denominator of F. Let us now deal with the case $p = 2$. We have

$$g(\underline{Y}) = f(L_1(\underline{Y})) = F(\frac{s^2 L_1 L_2}{2}) = F(s^2 R_1(1 + 2R_2)).$$

We apply Proposition 3.2 with $p = 2$, with this same F and with $H = s^2 R_1(1 + 2R_2)$. Note that by Lemma 4.3 (and taking into account the present index-numbering) the set $L_1(\mathbb{Z}^m)$ contains all large integers $\equiv 0 \pmod{2}$, hence $R_1(\mathbb{Z}^m)$ contains all large integers. Since $s^2(1 + 2R_2(\mathbb{Z}^m))$ consists of odd elements in $\mathbb{Z}_{(2)}$, we deduce that $H(\mathbb{Z}^m_{(2)}) \cap \mathbb{Z}_{(2)} = H(\mathbb{Z}^m_{(2)})$ is not contained in a single class modulo 2. Hence the assumptions of the lemma are verified and we deduce that

$$\|F(X)\|_2 \leq \|F(H)\|_2 = \|g\|_2.$$

However g has integer coefficients, hence the right side is ≤ 1 and we deduce that F has 2-integer coefficients, as required. This completes the proof that F has coefficients in $\mathbb{Z}$. The final assertion is a consequence of the fact that F has degree $d/2$. $\square$

Lemma 4.5 *The integer s has at most one prime factor.*

Proof : Suppose by contradiction that s is divisible by pq, where p, q are distinct (odd) primes, so in particular $\beta = r/s$ is not an integer. By Lemma 4.1 we have $\Omega_1 \cup \Omega_2 = \mathbb{Z}^m$, i.e. for every $\underline{y} \in \mathbb{Z}^m$ either $L_1(\underline{y}) \in \mathbb{Z}$ or $L_2(\underline{y}) \in \mathbb{Z}$. Since $L_1 + L_2 = \beta$ (by Lemma 4.3) we have $L_1(\mathbb{Z}^m) \subset \mathbb{Z} \cup (\beta + \mathbb{Z})$.

Moreover $L_1(\mathbb{Z}^m)$ is neither contained in $\mathbb{Z}$ nor in $\beta + \mathbb{Z}$; for otherwise, since β is not an integer, either the set Ω_2 or Ω_1 would be empty, which is not possible (for instance because by Lemma 4.3 $L_i(\Omega_i)$ contains all large integers in a class modulo 2).

Let now $D > 0$ be an integer such that $Q := DsL_1$ has integer coefficients. Then $Q(\mathbb{Z}^m) \subset Ds\mathbb{Z} \cup (Dr + Ds\mathbb{Z})$ and there is no inclusion in either of the two sets on the right. This means that for any $\underline{y} \in \mathbb{Z}^m$ we have either $Q(\underline{y}) \equiv 0 \pmod{Ds}$ or $Q(\underline{y}) \equiv Dr \pmod{Ds}$, and that both cases occur. Hence there exist $\underline{y}_1, \underline{y}_2 \in \mathbb{Z}^m$ such that

$$Q(\underline{y}_1) \equiv 0 \pmod{Ds}, \qquad Q(\underline{y}_2) \equiv Dr \pmod{Ds}.$$

Let now p^a, q^b be the exact powers of p, q dividing D. Pick with the Chinese Theorem $\underline{z} \in \mathbb{Z}^m$ so that $\underline{z} \equiv \underline{y}_1 \pmod{p^{a+1}}$ and $\underline{z} \equiv \underline{y}_2 \pmod{q^{b+1}}$. Since Ds is divisible by $p^{a+1}q^{b+1}$ we have $Q(\underline{z}) \equiv 0 \pmod{p^{a+1}}$ and $Q(\underline{z}) \equiv Dr \pmod{q^{b+1}}$.

Now, suppose that $Q(\underline{z}) \equiv 0 \pmod{Ds}$. Then $Dr \equiv 0 \pmod{q^{b+1}}$, which is false since r is coprime with s and hence with q. Hence $Q(\underline{z}) \equiv Dr \pmod{Ds}$, but then we obtain $0 \equiv Dr \pmod{p^{a+1}}$, which is also impossible by the same reason.

This contradiction proves the lemma. □

Now observe that, as in Proposition 2.2, a β with $f(X) = f(\beta - X)$ is unique if it exists; since $\beta = r/s$, with r, s coprime integers with $s > 0$, also r, s are uniquely determined, and hence so is the polynomial F. Therefore, combining the five lemmas in this section, we immediately obtain Theorem 1.1, except for the assertion concerning one-variable parametrizations.

Let us then suppose that some such parametrization exists, that is with $m = 1$ in the above arguments. Then the polynomials L_1, L_2 introduced above depend only on a single variable Y. By Lemma 4.3, $L_i(\Omega_i)$ consists of all large integers in a class modulo 2, apart from finitely many exceptions. Therefore L_1, L_2 are linear, and as in equation (6) we may write $L_1 = 2R_1$, $L_2 = 1 + 2R_2 = \beta - L_1$ where R_1, R_2 are polynomials over $\mathbb{Z}_{(2)}$ of the shape $R_1(Y) = \mu Y + \rho_1$, $R_2 = -\mu Y + \rho_2$, where $\mu, \rho_1, \rho_2 \in \mathbb{Z}_{(2)}$. Since $\Omega_1 \cup \Omega_2 = \mathbb{Z}$ (by Lemma 4.1) we see that μ must be in $\mathbb{Z}$ (for otherwise $\Omega_1 \cup \Omega_2$ would be contained in the union of two residue classes modulo an integer $l \geq 3$). In turn, this forces $2\rho_1, 2\rho_2 \in \mathbb{Z}$ (and hence $\rho_1, \rho_2 \in \mathbb{Z}$). Finally, $\beta = L_1 + L_2 = 1 + 2\rho_1 + 2\rho_2$ also lies in $\mathbb{Z}$, hence $s = \pm 1$ as required.

The proof of the theorem (and more) is now complete.

5 Proofs of remaining assertions

In this section we retain the notation of the previous one.

We start by proving that if $f(X)$ is of the stated shape $F(\frac{sX(r-sX)}{2})$ for a polynomial $F \in \mathbb{Z}[X]$ and r, s coprime odd integers, with $s > 0$ divisible by at most one prime, then $f(\mathbb{Z})$ may be parametrized by a polynomial in two variables with integer coefficients. In doing this, we see on composing on the left with F that it suffices to consider the case $f(X) = sX(r - sX)/2$.

We may write $s = p^t$ with p an odd prime and $t \in \mathbb{N}$. Observe that in this case there exists a polynomial $P \in \mathbb{Z}[Y]$ such that for all $y \in \mathbb{Z}$ we have $2P(y) \equiv 0$ or $r \pmod{s}$, and such that both congruences can be attained. It suffices e.g. to set $P(y) = \frac{r+s}{2} y^{\varphi(s)}$, where $\varphi(s)$ is Euler's function: if y is divisible by p, then $y^{\varphi(s)}$ is divisible by $p^{p^{t-1}(p-1)}$, hence by $p^t = s$, whereas if y is coprime to p, $y^{\varphi(s)} \equiv 1 \pmod{s}$.

Let us define

$$R(Y_1, Y_2) := sY_1 + P(Y_2), \qquad G(X) := X(r - 2X), \qquad g := G \circ R.$$

We contend that $f(\mathbb{Z}) = g(\mathbb{Z}^2)$, by proving separately two inclusions.

1. Let $(y_1, y_2) \in \mathbb{Z}^2$. Suppose first that $R(y_1, y_2) \equiv 0 \pmod{s}$ and write $R(y_1, y_2) = sl$ for $l \in \mathbb{Z}$. Then $g(y_1, y_2) = sl(r - 2sl) = f(2l)$.

If instead $2R(y_1, y_2) \equiv r \pmod{s}$, write $r - 2R(y_1, y_2) = sl$ with $l \in \mathbb{Z}$. Now $g(y_1, y_2) = 2R(y_1, y_2)(r - 2R(y_1, y_2))/2 = (r - sl)sl/2 = f(l)$.

This proves that $g(\mathbb{Z}^2) \subset f(\mathbb{Z})$.

2. Let now $n \in \mathbb{Z}$. If $n = 2l$ is even, let us solve in integers $R(y_1, y_2) = sl$: we may do this by choosing any y_2 with $P(y_2) \equiv 0 \pmod{s}$ and then defining $y_1 := l - (P(y_2)/s)$. Then $g(y_1, y_2) = sl(r - 2sl) = f(2l) = f(n)$, as wanted.

If instead n is odd, let us solve $2R(y_1, y_2) = r - sl$. Again, this is possible because $r - sl$ is even and congruent to $r \pmod{s}$: it suffices to find y_2 so that $2P(y_2) \equiv r \pmod{s}$ and determine y_1 accordingly, as before. We now find $g(y_1, y_2) = f(n)$.

This proves that $f(\mathbb{Z}) \subset g(\mathbb{Z}^2)$, concluding the proof of the first part of Theorem 1.2.

If $s = 1$ we need no congruence modulo s (just modulo 2), and this allows us to use just one variable. The argument is completely similar, and simpler: We define $R(X) = X$ so $g(X) = X(r - 2X)$, and we may check as above that $f(\mathbb{Z}) = g(\mathbb{Z})$: we have $f(2l) = g(l)$ and $f(2l + 1) = f(r - 1 - 2l) = g(\frac{r-1}{2} - l)$. (See also Example 1 in the Introduction.)

This completes the proof of Theorem 1.2. □

Let us now conclude by proving the Criterion. The 'only if' part is immediate. Conversely, let us suppose that $f(\frac{r}{s} - X) = f(X)$ and $f(2X/s) \in \mathbb{Z}[X]$. The first property implies, as at the beginning of the proof of Lemma 4.4, that $f(2X/s) = F(X(r - 2X))$ for some polynomial $F \in \mathbb{Q}[X]$. Suppose now by contradiction that F has not integral coefficients, so $\|F\|_p > 1$ for some prime p. Then, setting $Q(X) = X(r - 2X)$, we have $\|F(Q)\|_p < \|F\|_p$, hence we may apply Proposition 3.1 (with F in place of f). Since r is odd it is however immediately checked that neither (i) nor (ii) in the conclusion of that proposition apply to the present $Q(X)$, which yields the required contradiction. □

Final remarks. As already observed, the proofs give more precise conclusions on the structure of the parametrizations than what is stated in the theorems. For instance:

1. We have seen that if $f(\mathbb{Z}) = g(\mathbb{Z}^m)$ for an integer valued f not in $\mathbb{Z}[X]$, then g is necessarily of the shape $f \circ L$, where L is a polynomial satisfying suitable conditions, e.g. of congruence type.

2. Concerning the parametrizations in two variables appearing in Theorem 1.2, the proofs show that L may be taken linear in one variable. (The question whether one can take it linear in all variables reduces to the case of one variable.)

References

[CC] P.-J. Cahen and J.-L. Chabert. *Integer-Valued Polynomials* Amer. Math. Soc. Surveys and Monographs, 48, Providence, 1997.

[F] S. Frisch. *Remarks on polynomial parametrization of sets of integer points.* Comm. Algebra 36 (2008), no. 3, 1110-1114.

[FV] S. Frisch, L. Vaserstein. *Parametrization of Pythagorean triples by a single triple of polynomials.* Pure Appl. Algebra 212 (2008), no. 1, 271-274.

G. Peruginelli

Dipartimento di Matematica
Università di Pisa
Largo Bruno Pontecorvo, 5
56127, Pisa, Italy
perugine@mail.dm.unipi.it

U. Zannier

Scuola Normale Superiore

Piazza dei Cavalieri, 7
56126, Pisa, Italy
u.zannier@sns.it