ON THE EFFECTIVE POURCHET'S THEOREM

TERESA CORTADELLAS BENÍTEZ, CARLOS D'ANDREA, ANA BELÉN DE FELIPE, JOEL HURTADO MORENO, AND M. EULÀLIA MONTORO

Abstract. With the aid of Hensel Lemma, we refine the 2-adic Newton polygon algorithm proposed in [MKV23] to express computationally a given positive univariate polynomial with rational coefficients as a sum of five squares of rational polynomials -the effective Pourchet's Theorem- and extend it to cover almost all the possible inputs. We also provide examples which are covered with our methods but cannot be detected by previous conjectural algorithms.

1. Introduction & statement of the main results

Pourchet's Theorem [Pou71, Corollaire 4] states that any polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(t) > 0$ for all $t \in \mathbb{R}$ can be expressed as

$$f(x) = f_1(x)^2 + f_2(x)^2 + f_3(x)^2 + f_4(x)^2 + f_5(x)^2, \tag{1.1}$$

with $f_i(x) \in \mathbb{Q}[x]$, $1 \leqslant i \leqslant 5$. This result, combined with the fact that there are polynomials with rational coefficients which cannot be sums of four squares (cf. [Pou71, Proposition 10]), shows that 5 is the minimal number of squares of rational polynomials needed to express *any* positive $f(x) \in \mathbb{Q}[x]$.

Pourchet's original approach is based on local-global p-adic methods, in particular the Haase-Minkowski theorem, see [Raj93, Chapter 17] for a presentation of this result. Hence, in principle it is not suitable for an algorithmic adaptation. Recently, Magron, Koprowski and Vaccon had developed algorithms to express rational polynomials as sums of two squares ([MKV23, Algorithm 1]) and three or four squares ([MKV23, Algorithm 5]) if that decomposition was possible. They went further to propose that one can substract to a positive $f(x) \in \mathbb{Q}[x]$, a suitable even power (i.e. a rational square) of $\frac{1}{2}$ to produce a decomposition in a sum of 4 squares which could be treated algorithmically. This is the content of their Algorithm 6 in [MKV23], which we describe in Algorithm 2.15 below. Their approach is proven to work provided that the 2-adic valuation of either the constant or the leading coefficient of $f(x)$ is odd, and it is because of this obstruction that they are able to produce an algorithm ([MKV23, Algorithm 7]) which decomposes any positive rational $f(x)$ as a sum of 6 squares of rational polynomials, one more than Pourchet's sharp bound.

At the end of that paper, the authors propose a procedure ([MKV23, Algorithm 9] described in Algorithm 2.16 in this text), which they conjecture succeeds in producing a decomposition of any positive rational polynomial as in (1.1).

The first main result of this paper is a negative response to this conjecture.

2020 *Mathematics Subject Classification.* Primary 1208; Secondary 68W30.

Key words and phrases. positive polynomials, sums of squares, Newton Polygon, Hensel Lemma.

Theorem 1.1. *Algorithm 2.16 does not stop after any finite number of steps for the following family of polynomials:*

$$f_{k,N}(x) := \frac{4}{N^2}x^{2(2k+1)} + \frac{1}{N^2}x^{2k+1} + \frac{4}{N^2},$$

with $k = 0, 1, \ldots,$ $N \in \mathbb{N}$ *odd,* $N > 64$.

The key aspect of this family of counterexamples is given in part by the fact that having leading or constant coefficients of odd 2-adic valuation is a necessary condition for the algorithms in [MKV23] to work, as the following extended family of examples show.

Proposition 1.2. *Let* $a \in \mathbb{Z}_{>0}$. *If* $f(x) = g(x)^2 + 8a - 1$ *with* $g(x) \in \mathbb{Z}[x]$ *of degree* $d = 2k + 1$ *and* $k \in \mathbb{Z}_{\geqslant 0}$, *then the procedure of Algorithm 2.15 fails, i.e. the hypothesis on the* 2*-adic valuation of the leading coefficient of* $f(x)$ *is necessary.*

Even though Theorem 1.1 implies that[MKV23, Algorithm 9] does not solve the effective Pourchet problem in its full generality, still we can show that a modification of it actually works in more cases than those shown in that paper. For instance, if the degree of $f(x)$ is a multiple of 4, our modified Algorithm 2.17 works independently of the valuation of the leading coefficient of $f(x)$.

Theorem 1.3. *If the degree of* $f(x)$ *is a multiple of* 4, *then Algorithm 2.17 stops after a finite number of steps and gives the right answer.*

It still remains to find an algorithm to make explicit Pourchet's theorem for more cases than those covered so far. By using the Newton polygon method -as in that paper- we can cover more situations like the following.

Theorem 1.4. *Let* $f(x) \in \mathbb{Z}[x]$ *be a polynomial of (even) degree* d *such that* $f(t) > 0$ *for all* $t \in \mathbb{R}$, *and* $f(0) = 2^{2a}(4k + 3)$ *with* $a, k \in \mathbb{Z}_{\geqslant 0}$. *Then, there exist* N, $\ell \in \mathbb{N}$, N *odd such that* $f(x) - \left(\frac{1}{2^\ell}x^{d/2} + \frac{2^a}{N}\right)^2$ *is a sum of four squares.*

Note that even though the family $f_{k,N}(x)$ of Theorem 1.3 does not fit directly with this statement, it turns out that the polynomial $N^2 \cdot f_{k,N}(x-1)$ satisfies the hypothesis of Theorem 1.4, and hence one cand find five elements in $\mathbb{Q}[x]$ such that the sum of their squares is equal to this polynomial. From here it is straightforward to get an expression of $f_{k,N}(x)$ as in (1.1).

One of the novelties of Theorem 1.4 is that we replace the constant $(\frac{1}{2^l})^2$ by the square of a polynomial of degree $d/2$. We will see in the proof of this result that we also use the 2-adic "Newton polygon test" which was the main tool in [MKV23] to prove that our proposed input is a sum of four squares of rational polynomials.

It turns out that one can also use the p-adic Hensel Lemma to get more flexibility and produce new decompositions of a positive $f(x) \in \mathbb{Q}[x]$ as a sum of five squares. The following theorems are proven by using this method.

Theorem 1.5. *Let* $f(x) \in \mathbb{Z}[x]$ *be a square-free polynomial of degree* $d = 4k$, $k \in \mathbb{N}$. *If* $f(t) > 0$ *for all* $t \in \mathbb{R}$, *then there exists* $\ell_0 \in \mathbb{N}$ *such that if* $\ell \geqslant \ell_0$,

$$f(x) - \frac{1}{2^{2\ell}}(x^2 + x + 1)^{2k}$$

is a sum of four squares in $\mathbb{Q}[x]$.

It is easy to verify that if a square-free $f(x)$ is such that $f(t) > 0$ for all $t \in \mathbb{R}$, then for all $g(x) \in \mathbb{R}[x]$ of degree bounded by d, there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geqslant \ell_0$, $f(t) - \frac{1}{2^{2\ell}} g(t) > 0$, and one can find this bound algorithmically, see Proposition 2.2 and Remark 2.3.

Theorem 1.6. *Let $f(x) \in \mathbb{Z}[x]$ be a square-free polynomial of degree $d = 2(2k+1)$, $k \in \mathbb{N}$, such that $f(t) > 0$ for all $t \in \mathbb{R}$. Then, there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geqslant \ell_0$,*

$$f(x) - \frac{1}{2^{2\ell}}(x^2 + x + 1)^{2k} x^2$$

is a sum of four squares if $f(0)$ is not of the form $2^{2a}(8b+1)$, with $a, b \in \mathbb{Z}_{\geqslant 0}$. If this is not the case, then this expression fails to be a sum of four squares for $\ell \gg 0$ and $f(x)$.

Integers of the form $2^{2a}(8b+1)$ are squares in $\mathbb{Z}_2$, the ring of 2-adic integers, and all squares in this ring are of this form (it follows from Proposition 2.12). The condition on the constant coefficient of $f(x)$ in the hypothesis of Theorem 1.6 looks rather artificial, and one may argue that after a linear change of variables $f(x + \alpha)$, which does not change the structure of being a sum of four or five squares as we have done above with $f_{kN}(x)$ above, we just have to look for $\alpha \in \mathbb{Q}$ such that $f(\alpha)$ is not a square in $\mathbb{Q}_2$. If one finds such a change, then Theorem 1.6 would work in all the cases. But unfortunately, this cannot always be done as the following example due to Przemyslaw Koprowski shows it:

$$4x^6 + 4x^3 + 9 = (1 + 2x^3)^2 + 8 \tag{1.2}$$

is a polynomial such that evaluated in any rational number gives a square in $\mathbb{Q}_2$ and it is not the square of any polynomial. So, we cannot claim that with Theorems 1.5 and 1.6 we cover all the positive rational polynomials, and extra work is needed in order to have a complete effective approach to Pourchet's Theorem.

The rest of the paper is organized as follows: in Section 2 we establish the necessary notation and previous results needed for the proofs, which are then worked out in Section 3.

Acknowledgements: These results have been worked out at the Barcelona's Computational Algebra Seminar, hosted by the Math Institute of the University of Barcelona (IMUB). We are grateful to Przemyslaw Koprowski for useful conversations, and for sharing with us the example 1.2. T. Cortadellas is supported by MICINN research project PID2022-137283NB-C22. C. D'Andrea was supported by the Spanish State Research Agency, through the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in R&D (CEX2020-001084-M), and the European H2020-MSCA-ITN-2019 research project GRAPES and the Spanish MICINN research project PID2023-147642NB-I00. A.B. de Felipe was partially supported by the AGAUR project 2021 SGR 00603. M.E. Montoro is partially supported by grant PID2021-124827NB-I00 funded by MCIN/AEI/ 10.13039/501100011033 and by "ERDF A way of making Europe" by the "European Union".

2. Background & Algorithms

In this section we introduce some necessary notation, and known results and algorithms which will be used for the proof of our main results. We start with univariate polynomials, and algorithmic criteria for locating their roots and simplicity.

Let $f(x) = c_0 + c_1 x + \ldots + c_{d-1}x^{d-1} + c_d x^d = c_d \prod_{j=1}^{d}(x - \lambda_j)$ with $c_d \neq 0$, be a polynomial with coefficients in $\mathbb{C}$. For $k = 0, 1, \ldots, 2d-2$, denote

$$s_k = \lambda_1^k + \ldots + \lambda_d^k \in \mathbb{C},$$

and note that $s_k \in \mathbb{Q}(c_0, \ldots, c_d)$, to be more precisely each s_k is actually a polynomial in $c_0, \ldots, c_{d-1}$ and has as denominator a power of c_d (cf. (2.3) in [US92]).

Set now

$$S_f = \begin{pmatrix} s_0 & s_1 & \ldots & s_{d-1} \\ s_1 & s_2 & \ldots & s_d \\ \vdots & \vdots & \ldots & \vdots \\ s_{d-1} & s_d & \ldots & s_{2d-2} \end{pmatrix}.$$

Recall that by Sylvester's Law of Inertia ([Syl52]), any symmetric matrix with coefficients in a field K of characteristic different from 2 induces a quadratic form which can be diagonalized over K. If $K \subset \mathbb{R}$, the number of zeroes, positive and negative numbers in the diagonal is independent of the diagonalization. The rank of this matrix is the number of non-zero elements in the diagonal, and its signature the difference between the number of positive and negative numbers.

Theorem 2.1 ([Jac35, Jac36])**.** *The number of distinct roots of $f(x)$ is equal to the rank of S_f. If in addition $f(x) \in \mathbb{R}[x]$, its number of distinct real roots is equal to $\sigma(S_f)$, the signature of the real symmetric matrix S_f.*

For a modern proof of this result, see Theorem 2.2 in [US92]. As an easy consequence of this, we obtain the well-known fact that all the roots of $f(x) \in \mathbb{R}[x]$ are real if and only if S_f is definite positive. Also, none of the roots of $f(x) \in \mathbb{R}[x]$ is real if and only if the number of positive values in its diagonal form is equal to the number of negative values.

Note that if we also have $f(x) \in \mathbb{Q}[x]$, then $S_f \in \mathbb{Q}^{d\times d}$ and effective criteria to compute both the rank and the signature of S_f can be obtained by the standard computation of the sign sequence of the principal minors of this matrix, see for instance [Fra27].

Proposition 2.2. *Suppose that $f(x) \in \mathbb{R}[x]$ has degree d, is square-free and satisfies $f(t) > 0$ for all $t \in \mathbb{R}$. For any $g(x) \in \mathbb{R}[x]$ of degree bounded by d, there exists $\varepsilon_0 > 0$ such that, if $\varepsilon_0 \geqslant \varepsilon > 0$, $f(t) + \varepsilon\, g(t) > 0$ $\forall t \in \mathbb{R}$.*

Proof. For a new variable s, the symmetric matrix $S_{f+s\,g}$ has its entries in $\mathbb{R}(s)$, and each of its coefficients is actually regular in $s = 0$ (i.e. they can be evaluated in $s = 0$). So, we have that $S_{f+s\,g} \to S_f$ when $s \to 0$. Here the matrix convergence is meant "coefficient by coefficient". Since $f(x)$ is square-free, the rank of S_f is maximal by Theorem 2.1. Then, for s small enough, the same will happen with $S_{f+s\,g}$. In addition, as there are no real zeroes for $f(x)$ and all the complex roots are different, S_f has maximal rank, and there is an invertible real matrix C such that $C \cdot S_f \cdot C^T$ has $d/2$ positive values in the diagonal, the other $d/2$ values being negative as they must satisfy $\sigma(S_f) = 0$ thanks to Theorem 2.1. By continuity, we get that each of the principal minors of $C \cdot S_{f+s\,g} \cdot C^T$ will have the same sign of the corresponding principal minor of $C \cdot S_f \cdot C^T$ if s is small enough. This implies that $f(x) + \varepsilon_0\, g(x)$ has no real roots if $\varepsilon_0 > 0$ is small enough. In addition, as $f(0) > 0$, for small ε_0 we also have that $f(0) + \varepsilon\, g(0) > 0$, which shows that this polynomial is positive everywhere. The result then follows by picking $1 \gg \varepsilon_0 > 0$ satisfying all these conditions. □

Remark 2.3. If both $f(x)$ and $g(x)$ are polynomials with rational coefficients, explicit bounds for ε_0 can be found in terms of d and the absolute value of the coefficients of the input polynomials. Indeed, the principal k-th minor of $S_{f+s\,g}$ is a polynomial in s of degree less than or equal to kd having non-zero constant coefficient. One can then get straightforwardly a bound for the value of small s keeping this sign.

To test if a given polynomial $f(x)$ with coefficients in a field is square-free, one uses the so-called *discriminant* of this polynomial, which can be defined as the resultant between $f(x)$ and $f'(x)$. We will denote it with $\mathrm{disc}_x(f(x))$. To compute it, one can use the determinant of a $(2d-1)\times(2d-1)$ matrix whose inputs are coefficients of $f(x)$ or of $f'(x)$, see Section 5 of [CLO07] for more on this. From this matrix expression one deduces straightforwardly the following result.

Proposition 2.4. *If $f(x)\in\mathbb{C}[x]$ is square-free, and $g(x)\in\mathbb{C}[x]$ of degree bounded by the degree of $f(x)$, then for a new parameter λ, $\mathrm{disc}_x(\lambda\, f(x)+g(x))$ is a nonzero polynomial in λ, with leading coefficient equal to $\mathrm{disc}_x(f(x))$.*

We now turn our attention to local fields, and algorithms to detect sums of squares of polynomials with rational coefficients via testing them in these fields. For a prime $p\in\mathbb{N}$, we denote with $\mathbb{Q}_p$ the field of p-adic numbers, which is the completion of $\mathbb{Q}$ with respect to the topology given by the metric $d(a,b):=p^{-\,\mathrm{ord}_p\,(a-b)}$. The ring $\mathbb{Z}_p:=\{a\in\mathbb{Q}_p\,/\,d(a,0)\leqslant 1\}$ of p-adic integers is a principal ideal domain with the unique maximal ideal $\{a\in\mathbb{Z}_p\,/\,d(a,0)<1\}$.

Finding roots of polynomials in $\mathbb{Z}_p[x]$ is an easier task as in $\mathbb{Z}[x]$, this is one of the reasons why working in this ring is convenient in several cases. For instance, the following p-adic version of Newton's method is going to be useful in the text.

Theorem 2.5. [BS66, Theorem 3 in Section 5.2] *Suppose that $g(x)\in\mathbb{Z}_p[x]$, $\gamma\in\mathbb{Z}_p$, and $\delta\in\mathbb{N}$ are such that*

- $g(\gamma)\equiv 0 \mod p^{2\delta+1}\mathbb{Z}_p$,
- $g'(\gamma)\equiv 0 \mod p^{\delta}\mathbb{Z}_p$, *and*
- $g'(\gamma)\not\equiv 0 \mod p^{\delta+1}\mathbb{Z}_p$,

then there exists $\overline{\gamma}\in\mathbb{Z}_p$ such that $g(\overline{\gamma})=0$, and $\overline{\gamma}\equiv\gamma \mod p^{\delta+1}\mathbb{Z}_p$.

Irreducibility tests are also easier to find in the p-adics. For instance, the following statement is "Gauss'Lemma" for polynomials in $\mathbb{Z}_p[x]$.

Proposition 2.6. [Gou93, Lemma 6.3.7 and Problem 133] *Suppose that $f(x)\in\mathbb{Z}_p[x]$ factors in a non-trivial way as a product $f(x)=g(x)\,h(x)$, with $g(x)$ and $h(x)\in\mathbb{Q}_p[x]$. Then, there exist non-constant polynomials $g_0(x)$ and $h_0(x)\in\mathbb{Z}_p[x]$ such that $f(x)=f_0(x)\,g_0(x)$. If in addition $f(x)$, $g(x)$ and $h(x)$ are monic, then both $g(x)$ and $h(x)$ are also in $\mathbb{Z}_p[x]$ (so one can take $g_0(x)$ as $g(x)$ and $h_0(x)$ as $h(x)$).*

Corollary 2.7. *If a monic $f(x)\in\mathbb{Z}_p[x]$ has a root $x_0\in\mathbb{Q}_p$, then $x_0\in\mathbb{Z}_p$.*

Another very useful tool for dealing with polynomials and factorizations in $\mathbb{Z}_p[x]$ is the so-called "Hensel's Lemma for Polynomials". To state it properly, recall that $\mathbb{Z}_p/p\mathbb{Z}_p\simeq\mathbb{Z}/p\mathbb{Z}=:\mathbb{F}_p$, the field of integers modulo p. For $f(x)\in\mathbb{Z}_p[x]$, we denote with $[f(x)]\in(\mathbb{Z}_p/p\mathbb{Z}_p)[x]$ the polynomial whose coefficients are the classes modulo p of the coefficients of $f(x)$.

Theorem 2.8. [Gou93, Theorem 4.7.2] *Let $f(x) \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$, and assume that there exist $g_1(x)$ and $h_1(x) \in \mathbb{Z}_p[x]$ such that*

(1) *$g_1(x)$ is monic,*
(2) *$[g_1(x)]$ and $[h_1(x)]$ are coprime, and*
(3) *$[f(x)] = [g_1(x)][h_1(x)]$.*

Then there exist polynomials $g(x), h(x) \in \mathbb{Z}_p[x]$ such that

(1) *$g(x)$ is monic,*
(2) *$[g(x)] = [g_1(x)]$, and $[h(x)] = [h_1(x)]$, and*
(3) *$f(x) = g(x)h(x)$.*

Definition 2.9. The *Newton diagram* $N(f)$ of $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Q}_p[x]$ is the lower boundary of the convex hull of the subset of $\mathbb{R}^2$ consisting of all points $(i, \operatorname{ord}_p(a_i))$ for all $a_i \neq 0$.

Definition 2.10. We say that $f(x) \in \mathbb{Q}_p[x]$ is *pure* if $f(0) \neq 0$ and $N(f)$ is a segment.

There are very straightforward algorithms to deal with irreducible polynomials which are pure.

Proposition 2.11. [CG00, "Generalized Eisenstein Criterion" Lemma 3.5] *Suppose that $f(x) \in \mathbb{Q}_p[x]$ is a pure polynomial with $N(f)$ having slope $k/\deg(f)$, where $\gcd(k, \deg(f)) = 1$. Then, $f(x)$ is irreducible.*

Another useful tool we will need is a characterization of squares in $\mathbb{Q}_2$.

Proposition 2.12. [Gou93, Problem 124] *A unit $u \in \mathbb{Z}_2$ is a square in $\mathbb{Q}_2$ if and only if $u \equiv 1 \bmod 8\mathbb{Z}_2$.*

The connection between irreducibility and sums of squares of polynomials is given by the following result.

Theorem 2.13. [Pou71, Proposition 10] *Let $f(x) = \sum_{i=0}^{d} c_i x^i \in \mathbb{Q}[x]$ with $c_d \neq 0$. The following conditions are equivalent:*

(1) *$f(x)$ is a sum of 4 squares in $\mathbb{Q}[x]$;*
(2) *$c_d > 0$ and for all prime factor $p(x)$ of $f(x)$ of odd multiplicity, -1 is a sum of two squares in $\mathbb{Q}[x]/(p(x))$;*
(3) *$f(t) \geqslant 0$ $\forall t \in \mathbb{R}$, and in $\mathbb{Q}_2[x]$, every prime factor of $f(x)$ of odd multiplicity has even degree.*

We now turn to present the effective versions of Pourchet's Theorem given in [MKV23]. We start by recalling their key algorithm on the effective decomposition of a given positive polynomial as a sum of squares when this is possible.

Algorithm 2.14. [MKV23, Algorithm 5 "Decomposition into a sum of 3 of 4 squares"]
Input: A polynomial $f(x) \in \mathbb{Q}[x]$, which is a priori known to be a sum of 3 or 4 squares.
Output: Polynomials $f_1(x), \ldots, f_4(x) \in \mathbb{Q}[x]$ such that $f(x) = f_1(x)^2 + \ldots + f_4(x)^2$.

We now describe with more detail two more of their algorithms, as we will need to use their steps in the text. From now on, log will denote logarithm in base 2.

Algorithm 2.15. [MKV23, Algorithm 6 "Reduction to a sum of 4 squares: odd valuation case"]

Input: A positive square-free polynomial $f(x) = c_0 + c_1x + \ldots + c_dx^d \in \mathbb{Q}[x]$. The 2-adic valuations of the coefficients of $f(x)$ are $k_j := \mathrm{ord}_2(c_j)$ for $0 \leqslant j \leqslant d$. Ensure k_d is odd. It is assumed that $f(x)$ is not a sum of 4 squares.
Output: A polynomial $h(x) \in \mathbb{Q}[x]$ such that $f(x) - h(x)^2$ is a sum of 4 or fewer squares.

(1) Find a positive number ε such that $\varepsilon < \inf\{f(x),\, x \in \mathbb{R}\}$.
(2) Set $l_1 := \lceil -\frac{1}{2} \cdot \log \varepsilon \rceil$.
(3) Set $l_2 := \lceil -\frac{k_0}{2} \rceil + 1$.
(4) Set $l_3 := \left\lceil \max\left\{ \frac{jk_d - dk_j}{2d-2j},\ 0 < j < d \right\} \right\rceil$.
(5) Initialize $l := \max\{l_1, l_2, l_3\}$.
(6) While $\gcd(d, 2l + k_d) \neq 1$ do $l := l + 1$.
(7) Return $h(x) := 2^{-l}$.

Both algorithms 2.14 and 2.15 have been shown to work in [MKV23]. At the end of that paper, the authors propose the following 'procedure, show that it works experimentally in all the cases, and conjecture their validity in general.

Algorithm 2.16. [MKV23, Algorithm 9 "Reduction to sum of 4 squares"]
Input: A positive square-free polynomial $f(x) = c_0 + c_1x + \ldots + c_dx^d \in \mathbb{Q}[x]$.
Output: A polynomial $h(x) \in \mathbb{Q}[x]$ such that $f(x) - h(x)^2$ is a sum of 4 or fewer squares.

(1) If $f(x)$ is a sum of 4 squares, then return $h(x) := 0$.
(2) Set $f_*(x) = c_d + c_{d-1}x + \ldots + c_0x^d$.
(3) Find a positive number ε such that
$$\varepsilon < \inf\{f(x),\ x \in \mathbb{R}\} \text{ and } \varepsilon < \inf\{f_*(x),\ x \in \mathbb{R}\}.$$
(4) Initialize $l := \lceil -\frac{1}{2} \cdot \log \varepsilon \rceil$.
(5) While True do
  (a) if $f(x) - 2^{-2l}$ is irreducible in $\mathbb{Q}_2[x]$, then return $h(x) := 2^{-l}$.
  (b) if $f(x) - 2^{-2l}x^d$ is irreducible in $\mathbb{Q}_2[x]$, then return $h(x) := 2^{-l}x^{d/2}$.
  (c) $l := l + 1$.

We conclude this section by proposing our extension of Algorithm 2.15 to cover all polynomials $f(x) \in \mathbb{Q}[x]$ of degree multiple of 4. Note that the main difference is given in the computation of the gcd in one of the lines of the algorithm.

Algorithm 2.17.
Input: A positive square-free polynomial $f(x) = c_0 + c_1x + \ldots + c_dx^d \in \mathbb{Q}[x]$ of degree $d = 4d_0$, which is not a sum of 4 squares. The 2-adic valuations of the coefficients of $f(x)$ are $k_j := \mathrm{ord}_2(c_j)$ for $0 \leqslant j \leqslant d$.
Output: A polynomial $h(x) \in \mathbb{Q}[x]$ such that $f(x) - h(x)^2$ is a sum of 4 or fewer squares.

(1) If k_d is odd, then apply Algorithm 2.15 to the input. Otherwise,
  (a) Find a positive number ε such that $\varepsilon < \inf\{f(x),\, x \in \mathbb{R}\}$.
  (b) Set $l_1 := \lceil -\frac{1}{2} \cdot \log \varepsilon \rceil$.
  (c) Set $l_2 := \lceil -\frac{k_0}{2} \rceil + 1$.
  (d) Set $l_3 := \left\lceil \max\left\{ \frac{jk_d - dk_j}{2d-2j},\ 0 < j < d \right\} \right\rceil$.

(e) Initialize $l := \max\{l_1, l_2, l_3\}$.
(f) While $\gcd(d, 2l + k_d) \neq 2$ do $l := l + 1$.
(g) Return $h(x) := 2^{-l}$.

3. The proofs

In this section we provide the proofs of the results announced in the introduction.

Proof of Theorem 1.1. Note that $f_{k,N}(x) = \left(\frac{2}{N}x^{2k+1} + \frac{1}{4N}\right)^2 + \frac{63}{2^4 \cdot N^2}$.

From Proposition 2.12, we have that $\frac{63}{2^4 \cdot N^2} = -\alpha^2$, with $\alpha \in \mathbb{Q}_2$, so from the factorization

$$f_{k,N}(x) = \Big(\frac{2}{N}x^{2k+1} + \frac{1}{4N} + \alpha\Big)\Big(\frac{2}{N}x^{2k+1} + \frac{1}{4N} - \alpha\Big),$$

we deduce that this polynomial is square-free and must have an irreducible factor of odd degree. Hence, $f_{k,N}(x)$ is not a sum of 4 squares thanks to Theorem 2.13. So, Algorithm 2.16 does not stop at step (1).

To continue, notice that $(f_{k,N})_* = f_{k,N}$, so ε in (3) of Algorithm 2.16 can be taken as any number $0 < \varepsilon < \frac{63}{2^4 \cdot N^2}$. Therefore we have that l should be initialized as 6 or a larger value if $N > 64$. For all these cases, we have

$$f_{k,N}(x) - \frac{1}{2^{2l}} = \Big(\frac{2}{N}x^{2k+1} + \frac{1}{4N}\Big)^2 + \frac{63}{2^4 \cdot N^2} - \frac{1}{2^{2l}} = \Big(\frac{2}{N}x^{2k+1} + \frac{1}{4N}\Big)^2 - \alpha_l^2, \tag{3.1}$$

where $\alpha_l \in \mathbb{Q}_2$ because $\frac{63}{2^4 \cdot N^2} - \frac{1}{2^{2l}} = \frac{2^{2(l-2)} \cdot 63 - N^2}{N^2 \cdot 2^{2l}}$, and $2^{2(l-2)} \cdot 63 - N^2$ is congruent to -1 modulo $8\mathbb{Z}_2$ (recall that $l \geqslant 6$). Here, we are using Proposition 2.12 again. From Theorem 2.13, we deduce then that the algorithm will not stop at (5) a because (3.1) factors as a product of two polynomials of odd degree. The case (5) b is similar, as $(f_{k,N})_* = f_{k,N}$. This concludes with the proof of the claim. □

Proof of Proposition 1.2. Note first that $f(t) > 0$ for all $t \in \mathbb{R}$, and that k_{2d} is even. We will check that this is the only restriction of the input that $f(x)$ does not fulfill.

To do so, note that $-8a + 1$ is a square in $\mathbb{Q}_2$ thanks to Proposition 2.12. So, there exists $\alpha \in \mathbb{Q}_2$ such that

$$f(x) = (g(x) + \alpha) \cdot (g(x) - \alpha).$$

Each of the factors $(g(x) \pm \alpha)$ has degree $2k + 1$, so they are either irreducible or have an irreducible factor of odd degree. From Theorem 2.13, we then deduce that $f(x)$ is not a sum of 4 squares in $\mathbb{Q}[x]$, so the input of the algorithm is correct except for k_{2d} being even.

To continue, note that if $l \geqslant 2$,

$$\begin{aligned} 2^{2l}\big(f(x) - \tfrac{1}{2^{2l}}\big) &= 2^{2l}f(x) - 1 = 2^{2l}g(x)^2 + (2^{2l}(8a - 1) - 1) \\ &= 2^{2l}g(x)^2 - \alpha_l^2 = (2^l g(x) + \alpha_l)(2^l g(x) - \alpha_l), \end{aligned}$$

with $\alpha_l \in \mathbb{Q}_2$ thanks to Proposition 2.12. We then have that this expression has an irreducible factor of odd multiplicity and odd degree, so again thanks to Theorem 2.13 we deduce that $f(x) - \frac{1}{2^{2l}}$ is not a sum of four squares in $\mathbb{Q}[x]$ for all $l \geqslant 2$. □

Proof of Theorem 1.3. If k_d is odd, then the algorithm clearly holds. Suppose now that $k_d = 2k$. Then we have that

$$\gcd(d, 2l + k_d) = \gcd(4d_0, 2l + 2k) = 2\gcd(2d_0, l + k)$$

is always a multiple of 2 and at some point -at most up to $2d_0$ iterations, it will be 2. Denote l_0 the value of l that satisfies this. Then, the Newton diagram of $f(x) - \frac{1}{2^{2l_0}}$ is a segment with three lattice points: $(0, -2l_0), (2d_0, k - l_0), (4d_0, 2k)$.

From here we deduce that, either $f(x) - \frac{1}{2^{2l_0}}$ is irreducible in $\mathbb{Q}_2[x]$ (and hence this polynomial is the sum of 4 squares in $\mathbb{Q}[x]$ thanks to Theorem 2.13), or $f(x) - \frac{1}{2^{2l_0}}$ factors in $\mathbb{Q}_2[x]$ as the product of two polynomials whose Newton diagrams are parallel to the segment with endpoints $(0, 0), (2d_0, k + l_0)$, and have the same length as it. As $\gcd(2d_0, k+l_0) = 1$, there are no interior lattice points in this segment, so each of these factors are irreducible thanks to Proposition 2.11. So, $f(x) - \frac{1}{2^{2l_0}}$ actually factors in $\mathbb{Q}_2[x]$ as the product of two irreducible factors of even degree $2d_0$. By using Theorem 2.13 again, we conclude that it is a sum of four squares in $\mathbb{Q}[x]$. □

Proof of Theorem 1.4. As in the proof of Proposition 2.2, it can be shown $g(x) := f(x) - \left(\frac{1}{2^\ell}x^{d/2} + \frac{2^a}{N}\right)^2$ is positive everywhere for N, ℓ big enough, as the coefficients of $\left(\frac{1}{2^\ell}x^{d/2} + \frac{2^a}{N}\right)^2$ tend to 0 when ℓ, $N \to \infty$.

We choose a large odd $N \in \mathbb{N}$, and compute the 2-adic valuation of the constant coefficient of $g(x)$: as $N^2 \equiv 1 \bmod 4$, it is equal to

$$f(0) - \frac{2^{2a}}{N^2} = \frac{2^{2a}(4k' + 2)}{N^2} = \frac{2^{2a+1}(2k' + 1)}{N^2},$$

for a suitable $k' \in \mathbb{N}$. So its valuation is equal to $2a + 1$. Working around the leading coefficient of $g(x)$, we easily get that its 2-adic valuation is equal to -2ℓ. Note also that there is another coefficient of $g(x)$ with very low valuation if $\ell \gg 0$: the one corresponding to $x^{d/2}$, with valuation $a + 1 - \ell$.

To compute the Newton diagram of $g(x)$, one should pay attention to the relative position of the points $(0, 2a+1)$, $(d/2, a+1-\ell)$, and $(d, -2\ell)$. The point in the middle lies above the segment S with endpoints $(0, 2a+1)$ and $(d, -2\ell)$. In addition, the points of the form $(i, \mathrm{ord}_2(c_i))$, where c_i is a non-zero coefficient of $f(x)$, belong to the first quadrant. We conclude that the segment S is equal to $N(g)$ for ℓ big enough. One can then choose ℓ big enough such that S has no interior lattice points, which then proves that $g(x)$ is irreducible in $\mathbb{Q}_2[x]$ (see Proposition 2.11) and hence the result follows from Theorem 2.13. □

Proof of Theorem 1.5. From Proposition 2.2 applied to $f(x) = \sum_{i=0}^{4k} c_i x^i$ and $g(x) = -(x^2 + x + 1)^{2k}$, we deduce that there exists $\ell_0 \in \mathbb{N}$ such that if $\ell \geqslant \ell_0$ then $f(t) - \frac{1}{2^{2\ell}}(t^2 + t + 1)^{2k} > 0$ for all $t \in \mathbb{R}$. Next, we factor $2^{2\ell}f(x) - (x^2 + x + 1)^{2k}$ as a product of irreducible polynomials in $\mathbb{Q}_2[x]$: as its leading coefficient is $u := 2^{2\ell}c_{4k} - 1$, which is a unit in $\mathbb{Z}_2$, we then have that

$$2^{2\ell}f(x) - (x^2 + x + 1)^{2k} = u \prod_{i=1}^{N} p_i(x)^{r_i}, \tag{3.2}$$

with $p_i(x) \in \mathbb{Q}_2[x]$ monic and irreducible, $1 \leqslant i \leqslant N$. This implies, thanks to Proposition 2.6, that the factorization (3.2) takes place in $\mathbb{Z}_2[x]$. We then take classes in both sides in the quotient ring $\mathbb{Z}_2[x]/2\mathbb{Z}_2[x] \simeq \mathbb{F}_2[x]$, to obtain

$$[x^2+x+1]^{2k} = \prod_{i=1}^{N} [p_i(x)]^{r_i}.$$

The polynomial $[x^2+x+1]$ is irreducible in $\mathbb{F}_2[x]$, and note that each of the $[p_i(x)]$ has the same degree as $p_i(x)$ (because the latter is monic), which implies that each of them must be a power of a quadratic polynomial in the quotient ring. We deduce then that all the $p_i(x)$'s have even degree, and the claim now follows from Theorem 2.13. □

Proof of Theorem 1.6. Write $f(x) = \sum_{j=0}^{d} c_j x^j$ and denote $k_0 = \mathrm{ord}_2(c_0)$ and $k_1 = \mathrm{ord}_2(c_1)$. By Proposition 2.2, there exists $\ell' \in \mathbb{N}$ such that if $\ell \geqslant \ell'$ then $f(t) - \frac{1}{2^{2\ell}}(t^2+t+1)^{2k}t^2 > 0$ for all $t \in \mathbb{R}$.

Suppose first that $k > 0$. Choose $\ell \in \mathbb{N}$ such that $\ell > \max\{1, \ell', k_0/2 - k_1 + 2\}$. Denote $q(x) := 2^{2\ell} f(x) - (x^2+x+1)^{2k}x^2$. By using Hensel's Lemma (Theorem 2.8) with $(x^2+x+1)^{2k}$ and x^2, we deduce that $q(x) = g(x)h(x)$, where $g(x) \in \mathbb{Z}_2[x]$ has degree $4k$, $h(x) \in \mathbb{Z}_2[x]$ has degree 2, and $[g(x)] = [x^2+x+1]^{2k}$ and $[h(x)] = [x]^2$ in $\mathbb{F}_2[x]$. Reasoning as in the proof of Theorem 1.5, we deduce that all the irreducible factors of $g(x)$ have even degree. The proof of the claim would be complete -Thanks to Theorem 2.13 again- if we show that $h(x)$ is irreducible in $\mathbb{Q}_2[x]$. For this it will be enough to show that $q(x)$ does not have roots in $\mathbb{Q}_2$.

Suppose that this is not the case, and denote with $\alpha_\ell \in \mathbb{Q}_2$ a root of $q(x)$. The leading coefficient of $q(x)$ equals $u := 2^{2\ell}c_d - 1$, which is a unit in $\mathbb{Z}_2$. Since α_ℓ is a root of the monic polynomial $u^{-1}q(x) \in \mathbb{Z}_2[x]$, by Corollary 2.7 we get that $\alpha_\ell \in \mathbb{Z}_2$. Hence we can write $\alpha_\ell = 2^{a_\ell}(1+2q_\ell)$, with $a_\ell \in \mathbb{Z}_{\geqslant 0}$ and $q_\ell \in \mathbb{Z}_2$.

We then have

$$2^{2\ell} f(\alpha_\ell) = (\alpha_\ell^2+\alpha_\ell+1)^{2k}\alpha_\ell^2 = 2^{2a_\ell}(1+2q_\ell)^2(\alpha_\ell^2+\alpha_\ell+1)^{2k}. \tag{3.3}$$

Since $\alpha_\ell^2+\alpha_\ell+1 \neq 0$, the 2-adic valuation of the right-hand-side of (3.3) is equal to $2a_\ell$. On the left hand side, we have

$$2^{2\ell} f(\alpha_\ell) = 2^{2\ell+k_0}\tilde{c}_0 + 2^{2\ell+k_1+a_\ell}\tilde{c}_1(1+2q_\ell) + 2^{2a_\ell}\sum_{j=2}^{d} c_j(1+2q_\ell)^j 2^{2\ell+a_\ell(j-2)}, \tag{3.4}$$

where $\tilde{c}_0 = 2^{-k_0}c_0, \tilde{c}_1 = 2^{-k_1}c_1 \in \mathbb{Z}$. As $\ell > 0$, the third of the three summands of the right-hand-side of (3.4) has 2-adic valuation strictly larger than $2a_\ell$. So we must have either $2\ell+k_1+a_\ell = 2a_\ell \leqslant 2\ell+k_0$ or $2\ell+k_0 = 2a_\ell < 2\ell+k_1+a_\ell$. For the first case we have $a_\ell = 2\ell+k_1$. But note then that this implies that $2a_\ell = 4\ell+2k_1 \leqslant 2\ell+k_0 \iff 2\ell \leqslant k_0 - 2k_1$, which contradicts the choice of ℓ.

So, we must have that $a_\ell = \ell + \frac{k_0}{2} < 2\ell+k_1$, which holds thanks to the hypothesis on ℓ. Note that this implies that k_0 must be even. We now factor 2^{2a_ℓ} from each side of (3.3) and we obtain (recall that $2a_\ell = 2\ell+k_0$):

$$\tilde{c}_0 + 2^{k_1+a_\ell-k_0}\tilde{c}_1(1+2q_\ell) + \sum_{j=2}^{d} c_j(1+2q_\ell)^j 2^{2\ell+a_\ell(j-2)} = ((1+2q_\ell)(\alpha_\ell^2+\alpha_\ell+1)^k)^2. \tag{3.5}$$

As $k_1 + a_\ell - k_0 = k_1 + \ell - k_0/2 > 2$ because of our choice of $\ell > 1$, we deduce that the left-hand-side of (3.5) is congruent to $\tilde{c}_0 \bmod 8\mathbb{Z}_2$. The right-hand-side of (3.5) is the square of a unit in $\mathbb{Z}_2$, thus it is congruent to 1 modulo $8\mathbb{Z}_2$. Therefore, $c_0 = 2^{k_0}(8b+1)$ with $k_0 \in 2\mathbb{Z}$ and $b \in \mathbb{Z}_{\geqslant 0}$. This concludes the proof of the claim if $k > 0$.

For the case $k = 0$, take $\ell \in \mathbb{N}$ such that $\ell > \max\{2, \ell', (k_0+5)/2\}$. We only have to check that the quadratic polynomial $q(x) := 2^{2\ell} f(x) - x^2$ does not have roots in $\mathbb{Q}_2$ if c_0 is as in the hypothesis. But it is easy to check that the discriminant Δ of $q(x)$ is equal to

$$\Delta = 2^{4\ell} c_1^2 - 2^{2\ell+2}(2^{2\ell} c_2 - 1)c_0 = 2^{2\ell+2+k_0}(2^{2\ell-2-k_0} c_1^2 - (2^{2\ell} c_2 - 1)\tilde{c}_0), \tag{3.6}$$

where $\tilde{c}_0 = 2^{-k_0} c_0$ is a unit of $\mathbb{Z}_2$, and $\operatorname{ord}_2 \Delta = 2\ell + 2 + k_0$. If $q(x)$ has a root in $\mathbb{Q}_2$, then Δ is a square in $\mathbb{Q}_2$. We deduce then that k_0 must be even. Hence $c_0 = 2^{2a}\tilde{c}_0$ for some $a \in \mathbb{Z}_{\geqslant 0}$. Moreover, $2^{2\ell-2-k_0} c_1^2 - (2^{2\ell} c_2 - 1)\tilde{c}_0 \in \mathbb{Z}_2$ is a unit that is a square in $\mathbb{Q}_2$ and is congruent to $\tilde{c}_0$ modulo $8\mathbb{Z}_2$. Proposition 2.12 implies that $\tilde{c}_0$ is of the form $8b + 1$ with $b \in \mathbb{Z}_{\geqslant 0}$. The claim follows for this case.

To conclude, we need to prove that if $c_0 = 2^{2a}(8b+1)$ and $f(x)$ is square-free, then $g(x) := f(x) - \frac{1}{2^{2\ell}}(x^2 + x + 1)^{2k} x^2$ is not a sum of four squares for $\ell \gg 0$. Indeed, if we set $\gamma = 2^{\ell+a}$, $\delta = \ell + a + 1$, and $q(x) = 2^{2\ell} f(x) - (x^2 + x + 1)^{2k} x^2$, then we deduce that

$$\begin{aligned} q(\gamma) &= 2^{2\ell} \textstyle\sum_{j=0}^{d} c_j \, 2^{(\ell+a)j} - 2^{2(\ell+a)} \big(2^{2(\ell+a)} + 2^{\ell+a} + 1\big)^{2k} \\ &= 2^{2(\ell+a)} \big(\textstyle\sum_{j=1}^{d} c_j 2^{(\ell+a)j-2a} + 8b + 1 - (2^{2(\ell+a)} + 2^{\ell+a} + 1)^{2k} \big). \end{aligned}$$

If $\ell \geqslant a + 3$, it is straightforward to verify that the expression between parenthesis above is a multiple of 8, which shows then that $q(\gamma) \equiv 0 \bmod 2^{2\delta+1}\mathbb{Z}_2$. In addition, it is not hard to verify that $q'(\gamma) \equiv 0 \mod 2^{\delta}\mathbb{Z}_2$, and $q'(\gamma) \not\equiv 0 \mod 2^{\delta+1}\mathbb{Z}_2$. From Theorem 2.5 we deduce then that there exists $\overline{\gamma} \in \mathbb{Z}_2$ which is a root of $g(x)$. If this is a simple root, then because of Theorem 2.13 this polynomial cannot be a sum of four squares, as it has a linear irreducible factor in its factorization. If $\overline{\gamma}$ is a mutiple root, then $2^{2\ell}$ would be a root of $p(\lambda) := \operatorname{disc}_x(\lambda f(x) - (x^2 + x + 1)^{2k} x^2) \in \mathbb{Z}[\lambda]$. As $f(x)$ is square-free, from Proposition 2.4 we deduce that $p(\lambda)$ is not identically zero, and hence it has a finite number of roots. If $\ell \gg 0$ then it is clear that $p(2^{2\ell}) \neq 0$, and hence the claim follows. □

Remark 3.1. The conditions on c_0 imposed in the hypothesis of Theorem 1.6 are necessary, as if we pick for instance $f(x) = x^2 + 1$, for all $\ell > 1$, thanks to Proposition 2.12 we have a factorization $(2^{2\ell} - 1)x^2 + 2^{2\ell} = (2^{\ell} - \alpha_\ell x)(2^{\ell} + \alpha_\ell x)$ with $\alpha_\ell \in \mathbb{Z}_2$. From Theorem 2.13 we deduce then that this polynomial is not a sum of 4 squares.

References

[BS66] Borevich, A. I.; Shafarevich, I. R. *Number theory.* Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol. 20. Academic Press, New York–London, 1966.

[CG00] Cantor, David G.; Gordon, Daniel M. *Factoring polynomials over p-adic fields.* Algorithmic number theory (Leiden, 2000), 185–208, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[CLO07] Cox, David; Little, John; O'Shea, Donal. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[Fra27] Franklin, Philip. *A theorem of Frobenius on quadratic forms.* Bull. Amer. Math. Soc. 33 (1927), no. 4, 447–452.

[Gou93] Gouvêa, Fernando Q. *p-adic numbers.* An introduction. Universitext. Springer-Verlag, Berlin, 1993.

[Jac35] Jacobi, C. G. J. *Theoremata nova algebraica circa systema duarum aequationum inter duas variabiles propositarum (1835),* in Gesummelte Werke, Reimer, Berlin, 1884, Vol. 3, 287–294.

[Jac36] Jacobi, C. G. J. *De relationibus, quae locum habere debeunt inter puncta intersectionis duarum curvarum vel trium superficierum algebraicarum dati ordi- nis, simul cum enodatione paradoxi algebraici (1836),* in Gesummelte Werke, Reimer, Berlin, 1884, Vol. 3, 331–354.

[MKV23] Magron, Victor; Koprowski, Przemyslaw; Vaccon, Tristan. *Pourchet's theorem in action: decomposing univariate nonnegative polynomials as sums of five squares.* Proceedings of the International Symposium on Symbolic & Algebraic Computation (ISSAC 2023), 425–433, ACM, New York, 2023.

[Pou71] Pourchet, Y. Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques. Acta Arith. 19 (1971), 89–104.

[Raj93] Rajwade, A. R. *Squares.* London Mathematical Society Lecture Note Series, 171. Cambridge University Press, Cambridge, 1993.

[Syl52] Sylvester, James Joseph. *A demonstration of the theorem that every homogeneous quadratic polynomial is reducible by real orthogonal substitutions to the form of a sum of positive and negative squares.* Philosophical Magazine. 4th Series. 4 (23): 138–142, 1852

[US92] Uteshev, Alexei Yu.; Shulyak, Sergei G. *Hermite's method of separation of solutions of systems of algebraic equations and its applications.* Linear Algebra Appl. 177 (1992), 49–88.

Departament de Matemàtiques i Analítica de Dades, IQS School of Engineering, Universitat Ramon Llull. Via Augusta 390, 08017 Barcelona, Spain
Email address: teresa.cortadellas@iqs.url.edu

Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain & Centre de Recerca Matemàtica, Edifici C, Campus Bellaterra, 08193 Bellaterra, Spain
Email address: cdandrea@ub.edu
URL: http://www.ub.edu/arcades/cdandrea.html

Department of Mathematics, Barcelona East School of Engineering (EEBE), Universitat Politècnica de Catalunya - BarcelonaTech (UPC), Campus Diagonal Besòs, Ed. A, Avda. Eduard Maristany, 16, 08019 Barcelona, Spain.
Email address: ana.belen.de.felipe@upc.edu

Departament de Matemàtiques, Universitat Politècnica de Catalunya, Av. Diagonal 647, 08028 Barcelona, Spain
Email address: joel.hurtado@estudiantat.upc.edu

Departament de Matemàtiques i Informàtica, Universitat de Barcelona. Gran Via 585, 08007 Barcelona, Spain
Email address: eula.montoro@ub.edu