Universiteit
Antwerpen

This item is the archived peer-reviewed author-version of:

Integer programming with GCD constraints

Reference:
Défossez Rémy, Haase Christoph, Mansutti Alessio, Pérez Guillermo Alberto.- Integer programming with GCD constraints
Proceedings of the 2024 ACM-SIAM Symposium on Discrete Algorithms (SODA)- ISBN 978-1-61197-791-2 - 2024, p. 3605-3658
Full text (Publisher's DOI): https://doi.org/10.1137/1.9781611977912.128
To cite this reference: https://hdl.handle.net/10067/2050960151162165141

uantwerpen.be
Institutional repository IRUA

Integer Programming with GCD Constraints

Anonymous author(s)

Abstract

We study the non-linear extension of integer programming with greatest common divisor constraints of the form $\gcd(f, g) \sim d$, where f and g are linear polynomials, d is a positive integer, and $\sim$ is a relation among $\leq, =, \neq$ and $\geq$. We show that the feasibility problem for these systems is in NP, and that an optimal solution minimizing a linear objective function, if it exists, has polynomial bit length. To show these results, we identify an expressive fragment of the existential theory of the integers with addition and divisibility that admits solutions of polynomial bit length. It was shown by Lipshitz [*Trans. Am. Math. Soc.*, 235, pp. 271–283, 1978] that this theory adheres to a local-to-global principle in the following sense: a formula Φ is equi-satisfiable with a formula Ψ in this theory such that Ψ has a solution if and only if Ψ has a solution modulo every prime p. We show that in our fragment, only a polynomial number of primes of polynomial bit length need to be considered, and that the solutions modulo prime numbers can be combined to yield a solution to Φ of polynomial bit length. As a technical by-product, we establish a Chinese-remainder-type theorem for systems of congruences and non-congruences showing that solution sizes do not depend on the magnitude of the moduli of non-congruences.

1 Background and overview of main results

Integer programming, the problem of finding an (optimal) solution over the integers to a systems of linear inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$, is a central problem computer science and operations research. Feasibility of its 0-1 variant constituted one of Karp's 21 seminal NP-complete problems [10]. In the 1970s, membership of the unrestricted problem in NP was established independently by Borosh and Treybig [3], and von zur Gathen and Sieveking [25]. To show membership in NP, both groups of authors established a small witness property: if an instance of integer programming is feasible then there is a solution whose bit length is polynomially bounded in the size of the instance. Reductions to integer programming have become a standard tool to show membership of numerous problems in NP. In this paper, we study a non-linear generalization of integer programming which additionally allows to constrain the numerical value of the greatest common divisor (GCD) of two linear terms.

Throughout this paper, denote by $\mathbb{R}$ the set of real numbers, $\mathbb{Z}$ the set of integers, $\mathbb{N}$ the set of non-negative integers including zero, and $\mathbb{P}$ the set of all prime numbers. For $R \subseteq \mathbb{R}$, denote by $R_+ \coloneqq \{r \in R : r > 0\}$. Formally, an instance of integer programming with GCD constraints (IP-GCD) is a mathematical program of the following form:

$$\begin{aligned} \text{minimize} \quad & \boldsymbol{c}^\intercal \boldsymbol{x} \\ \text{subject to} \quad & A \cdot \boldsymbol{x} \leq \boldsymbol{b} \\ & \gcd(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) \sim_i d_i, \qquad\qquad 1 \leq i \leq k\,, \end{aligned}$$

where $\boldsymbol{c} \in \mathbb{Z}^n$, $A \in \mathbb{Z}^{m \times n}$, $\boldsymbol{b} \in \mathbb{Z}^m$, $d_i \in \mathbb{Z}_+$, $\boldsymbol{x} = (x_1, \ldots, x_n)$ is a vector of unknowns, the f_i and g_i are linear polynomials with integer coefficients, and $\sim_i \in \{\leq, =, \neq, \geq\}$. We call $\boldsymbol{a} \in \mathbb{Z}^n$ a solution if setting $\boldsymbol{x} = \boldsymbol{a}$ respects all constraints; $\boldsymbol{a}$ is an optimal solution if the value of $\boldsymbol{c}^\intercal \boldsymbol{a}$ is minimal among all solutions. We will first and foremost focus on the feasibility problem of IP-GCD and discuss finding optimal solutions later on in this paper. The main result of this paper is to establish a small witness property for IP-GCD and consequently membership of the problem in NP.

Theorem 1. *If an instance of IP-GCD is feasible then it has a solution (and an optimal solution, if one exists) of polynomial bit length. Hence, IP-GCD feasibility is* NP*-complete.*

We remark that IP-GCD feasibility is NP-hard even for a single variable, in contrast to classical integer programming, which is polynomial-time decidable for any fixed number of variables [9]. It is shown in [1, Theorem 5.5.7] that deciding a univariate system of non-congruences $x \not\equiv a_i \pmod{m_i}$, $1 \leq i \leq k$, is an NP-hard problem. Hardness of IP-GCD then follows from observing that a non-congruence $x \not\equiv a \pmod{m}$ is equivalent to $\gcd(x - a, m) \neq m$.

1.1 The NP upper bound at a glance

Even decidability of the IP-GCD feasibility problem is far from obvious, but can be approached by observing that deciding a GCD constraint is a *"Diophantine problem 'in disguise'"* [11]. It follows from Bézout's identity that $\gcd(x, y) = d$ if and only if there are $a, b, u, v \in \mathbb{Z}$ such that $u \cdot d = x$, $v \cdot d = y$, and $d = a \cdot x + b \cdot y$. While arbitrary systems of quadratic Diophantine equations are undecidable [16], we see that the unknowns a, b, u, v are only used to express divisibility properties. Hence, those equations can equivalently be expressed in the existential fragment of the first-order theory of the structure $L_{\text{div}} = (\mathbb{Z}, 0, 1, +, \leq, |)$, where $m \mid n$ holds whenever there exists a unique[1]

[1] This definition implies that $0 \mid n$ does not hold for any $n \in \mathbb{Z}$, 0 included. Throughout this paper, we assume wlog. that $f \neq 0$ for any divisibility $f \mid g$. For GCD, we instead use the standard interpretation where $\gcd(0, n) = n$ for any $n \in \mathbb{N}$; this mismatch between the interpretation of divisibility and GCD is for technical convenience only.

integer q such that $n = q \cdot m$:

$$u \cdot d = x \wedge v \cdot d = y \wedge d = a \cdot x + b \cdot y \iff \exists s \, \exists t \colon d \mid x \ \wedge \ d \mid y \ \wedge \ x \mid s \ \wedge \ y \mid t \ \wedge \ d = s + t \, .$$

The full first-order theory of L_{div} is easily seen to be undecidable [17]. However, decidability of its existential fragment was independently shown by Lipshitz [14, 15] and Bel'tyukov [2], and later also studied by van den Dries and Wilkie [23], Lechner et al. [12], and Starchak [21, 22]. The precise complexity of the existential fragment is a long-standing open problem. It is known to be NP-complete for a fixed number of variables [15, 12], and membership in NEXP has only more recently been established [12]. In particular, the bit length of smallest solutions can be exponential [12], as demonstrated by the family of formulae $\Phi_n \coloneqq x_n > 1 \wedge \bigwedge_{i=0}^{n-1} x_i > 1 \wedge x_i \mid x_{i+1} \wedge x_i + 1 \mid x_{i+1}$, for which any solution satisfies $x_n \geq 2^{2^n}$. From those results, it is possible to derive that IP-GCD feasibility is decidable in NEXP. However, IP-GCD does not require the full expressive power of L_{div}. In fact, the first-order theory of L_{div} can be seen to be equivalent to the theory of $(\mathbb{Z}, 0, 1, +, \leq, \gcd)$ in which the divisibility predicate is replaced by a full ternary relation $\gcd(x, y) = z$. In contrast, IP-GCD only requires countably many binary predicates $(\gcd(\cdot, \cdot) = d)_{d \in \mathbb{Z}_+}$ and $(\gcd(\cdot, \cdot) \geq d)_{d \in \mathbb{Z}_+}$ with the obvious interpretation. Several expressiveness results concerning (fragments of) the existential theory of the structure $(\mathbb{Z}, 0, 1, +, \leq, (\gcd(\cdot, \cdot) = d)_{d \in \mathbb{Z}_+})$ have recently been provided by Starchak [20]. The question of whether this theory admits solutions of polynomial bit length is explicitly stated as open in [20]. Theorem 1 answers this question positively.

Our starting point for establishing Theorem 1 is Lipshitz' [14, 15] decision procedure for the existential theory of L_{div} that was later refined by Lechner et al. [12]. Given a system of divisibility constraints $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^{m} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ for linear polynomials f_i and g_i, Lipshitz' algorithm first computes from Φ an equi-satisfiable formula Ψ in so-called *increasing form*. Informally speaking, Ψ is in increasing form whenever Ψ is a system of divisibility constraints augmented with constraints imposing a total (semantic) ordering on the values of the variables in Ψ, and whenever the largest variable with respect to that ordering occurring in any non-trivial divisibility $f \mid g$ implied by Ψ only appears in the right-hand side g. For instance, the system $x < y \wedge x + 1 \mid y - 2$ is in increasing form, but adding $x + 1 \mid x + y$ results in a non-increasing system, since $x + 1 \mid y - 2 \wedge x + 1 \mid x + y$ implies $x + 1 \mid x + y - (y - 2)$, i.e., $x + 1 \mid x + 2$. Such implied divisibilities are captured in [12] by the notion of a *divisibility module* that we later formalize in Section 1.3. One conceptual contribution of this paper is to identify a weaker notion of formulae in increasing form that is syntactic in nature, as it does not explicitly enforce a particular ordering among the variables. Informally speaking, a system of divisibility constraints Ψ is *r-increasing* whenever there exists a partial order $\prec$ over the free variables of Ψ whose longest chain is of length at most $r - 1$, and for any non-trivial divisibility $f \mid g$ implied by Ψ, the set of variables occurring in $f \mid g$ has a $\prec$-maximal variable that only appears in the right-hand side g. Referring to the previous example, we observe that $x + 1 \mid y - 2$ is 2-increasing, witnessed by the (total) order $x \prec y$. This concept is fundamental for establishing Theorem 1, since, as we discuss below, for fixed r, any satisfiable r-increasing formula Ψ of L_{div} has a smallest solution of polynomial bit length, and L_{div} formulae resulting from IP-GCD instances are 3-increasing.

Returning to Lipshitz' approach, the key property of existential L_{div} formulae in increasing form is that they enable appealing to a local-to-global property: Lipshitz shows that any Φ in increasing form has a solution over $\mathbb{Z}$ if and only if Φ has a solution in the p-adic integers $\mathbb{Z}_p$ for every prime p belonging to a finite set of difficult primes $\mathbf{P}_+(\Phi)$, the other primes being "easy" in the sense that a p-adic solution for them always exists and that they do not influence the bit length of the minimal solution of Φ. In order to combine the p-adic solutions to an integer solution of Φ, Lipshitz invokes (a generalized version of) the Chinese Remainder Theorem (CRT):

Theorem 2 (CRT)**.** *Let $M = \{m_1, \ldots, m_k\}$, $b_1, \ldots, b_k \in \mathbb{Z}$ be such that m_i and m_j are coprime for all $1 \le i \ne j \le k$. The system of simultaneous congruences $x \equiv b_i \bmod m_k$, $1 \le i \le k$, has a solution, and all solutions lie on the shifted lattice $a + \mathbb{Z} \cdot \Pi M$ for some $a \in \mathbb{Z}$.*

Here and below, for a finite set $M \subseteq \mathbb{Z}$, we denote by ΠM the product of all elements in M. It follows that the smallest non-negative solution of the system of congruences is of polynomial bit length. As a key technical contribution of this paper, required to establish Theorem 1, we develop the following Chinese-remainder-style theorem that includes additional non-congruences and yields a bound for the smallest solution that is, in certain settings, substantially better than the one that can be achieved by the CRT. For a finite set S, we write $\#S$ for its cardinality.

Theorem 3. *Let $d \in \mathbb{Z}_+$, $M \subseteq \mathbb{Z}_+$ finite, and $Q \subseteq \mathbb{P}$ be a non-empty finite set of primes such that the elements of $M \cup Q$ are pairwise coprime, $M \cap Q = \emptyset$, and $\min(Q) > d$. Consider the univariate system of simultaneous congruences and non-congruences $\mathcal{S}$ defined by*

$$\begin{aligned} x &\equiv b_m \pmod{m} && m \in M \\ x &\not\equiv c_{q,i} \pmod{q} && q \in Q,\ 1 \le i \le d\,. \end{aligned}$$

Then, for every $k \in \mathbb{Z}$, $\mathcal{S}$ has a solution in the interval $\{k, \ldots, k + \Pi M \cdot \mathfrak{f}(Q, d)\}$, where

$$\mathfrak{f}(Q, d) \coloneqq \big((d+1) \cdot \#Q\big)^{4(d+1)^2(3+\ln\ln(\#Q+1))}.$$

The strength of Theorem 3 can be seen as follows. While it is possible to deduce from the classical CRT that the solutions of $\mathcal{S}$ are periodic with period $\Pi Q \cdot \Pi M$, we have $\Pi Q \gg \mathfrak{f}(Q, d)$ as the magnitude of the primes in Q grows, as in particular $\mathfrak{f}(Q, d)$ only depends on $\#Q$ and d. We further discuss some results used to establish Theorem 3 in Section 1.2 below.

Another key technical contribution towards establishing Theorem 1 is to propose a refinement of the set of difficult primes $\mathbf{P}_+(\Phi)$. The definition of this set was changed from [14] to [12] to decrease its bit length from doubly to singly exponential. We refine the definition once more, and show that we obtain a set of polynomially many primes of polynomial bit length. This result is achieved by an in-depth analysis of how the integer solution for Φ is constructed starting from the p-adic solutions. The bound on $\mathbf{P}_+(\Phi)$ also enables us to derive an NP algorithm for increasing formulae. It is shown in [6] that, for every prime $p \in \mathbb{P}$, the existential theory of the p-adic integers with linear p-adic valuation constraints is decidable in NP. Deciding an increasing Φ thus reduces to a polynomial number of independent queries to an NP algorithm and is hence in NP. It is worth mentioning that the family of formulae Φ_n above is increasing only for the ordering $x_1 \prec x_2 \prec \cdots \prec x_n$ (i.e., it is n-increasing but not $(n-1)$-increasing). Hence, even though the smallest solution of Φ_n has exponential bit length, our bound on $\mathbf{P}_+(\Phi)$ enables us to witness the *existence* of a solution in NP.

Moreover, this bound leads to a further main result of this paper, showing that we can construct an integer solution for Φ from the relevant p-adic solutions that is asymptotically smaller when compared to the existing local-to-global approaches [14, 12]. These improved bounds also crucially rely on Theorem 3. To formally state this result, we require some further definitions. Given $\boldsymbol{v} \in \mathbb{Z}^d$, denote by $\|\boldsymbol{v}\|$ the maximum absolute value of the components of $\boldsymbol{v}$, and by $\langle \cdot \rangle$ the bit length encoding an object under some reasonable standard encoding in which numbers are encoded in binary. Furthermore, for a system of divisibility constraints $\Phi \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$, denote by $\mathbb{P}(\Phi)$ the set of all primes that are less or equal than m or that divide some number occurring in Φ. For $p \in \mathbb{P}$ and $a \in \mathbb{Z} \setminus \{0\}$, we write $v_p(a)$ for the largest $k \in \mathbb{N}$ such that $a = p^k b$ for some $b \in \mathbb{Z}$, and $v_p(0) \coloneqq \infty$. We say that Φ has a solution modulo p if there is some $\boldsymbol{b}_p \in \mathbb{Z}^d$ such that $f_i(\boldsymbol{b}_p) \ne 0$ and $v_p(f_i(\boldsymbol{b}_p)) \le v_p(g_i(\boldsymbol{b}_p))$ for all $1 \le i \le m$. Note that every integer solution is a solution modulo p for all $p \in \mathbb{P}$, and therefore if Φ does not have a solution modulo some prime p, then Φ is unsatisfiable over $\mathbb{Z}$. The following theorem now gives bounds on the bit length of an integer solution of Φ in terms of solutions modulo p for primes in $\mathbb{P}(\Phi)$.

Theorem 4. *Let $\Phi(\boldsymbol{x})$ be an r-increasing system of divisibility constraints such that Φ has a solution $\boldsymbol{b}_p \in \mathbb{Z}^d$ modulo p for every prime $p \in \mathbb{P}(\Phi)$. Then Φ has infinitely many solutions, and a solution $\boldsymbol{a} \in \mathbb{N}^d$ such that $\langle \|\boldsymbol{a}\| \rangle \leq (\langle \Phi \rangle + \max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.*

The bound achieved in Theorem 4 primarily improves upon existing upper bounds by being exponential only in r, as opposed to exponential in $\mathrm{poly}(d)$ as established in [12], where d is the number of variables of Φ. In particular, for r fixed, as is the case for systems of divisibility constraints resulting from IP-GCD systems, Theorem 4 yields small solutions of polynomial bit length. Observe that Theorem 4 does not explicitly invoke the set of difficult primes $\mathbf{P}_+(\Phi)$, but rather the set $\mathbb{P}(\Phi)$. The latter is the subset of those primes p in $\mathbf{P}_+(\Phi)$ for which solutions modulo p might not exist, and one of the initial steps in the proof Theorem 4 is to compute solutions modulo q for every prime $q \in \mathbf{P}_+(\Phi) \setminus \mathbb{P}(\Phi)$. We give further details on the proof of Theorem 4 in Section 1.3 and then outline in Section 1.4 how it can be used to obtain the NP upper bound for Theorem 1. But first, we continue with the promised discussion on some details on Theorem 3.

1.2 Small solutions to systems of congruences and non-congruences

Let us introduce some notation. Given $a, b \in \mathbb{Z}$, we define $[a, b] \coloneqq \{a, a+1, \dots, b\}$. We write $\mathrm{div}(a) \subseteq \mathbb{N}$ for the (positive) divisors of a and $\mathbb{P}(a)$ for $\mathbb{P} \cap \mathrm{div}(a)$. A function $m \colon \mathbb{Z}_+ \to \mathbb{R}_+$ is *multiplicative* if $m(a \cdot b) = m(a) \cdot m(b)$ for all $a, b \in \mathbb{N}$ coprime (so, $m(1) = 1$).

The proof of Theorem 3 is based on an abstract version of Brun's pure sieve [4]. Similarly to other results in sieve theory, Brun's pure sieve considers a finite set $A \subseteq \mathbb{Z}$ and a finite set of primes Q, and (subject to some conditions) derives bounds on the cardinality of the set $A \setminus \bigcup_{q \in Q} A_q$, where A_q is the subset of the elements in A that are divisible by q. In other words, the sieve studies the number of $x \in A$ satisfying $x \not\equiv 0 \pmod{q}$ for every $q \in Q$. In comparison, Theorem 3 requires x to be non-congruent modulo q to multiple integers, instead of non-congruent to just 0. The key insight in overcoming this difference is to notice that Brun's result can be established for arbitrary sets A_q, as long as a simple *independence* property holds together with Brun's *density* property (a formal statement is given below). A second technical issue concerns the bounds obtained from Brun's sieve. In its standard formulation (see e.g. [5, Ch. 6]), given an arbitrary $u \in \mathbb{Z}_+$, the sieve gives an estimate on the cardinality of the set $A \setminus \bigcup_{q \in Q \cap [2,u]} A_q$ that depends on u; and to estimate $\#\big(A \setminus \bigcup_{q \in Q} A_q\big)$ one sets u as the largest prime in Q. The resulting bound is, however, inapplicable in our setting as we seek to be independent of the bit length of the primes in Q. This issue is overcome by revisiting the analysis of Brun's pure sieve from [5], and by requiring an additional hypothesis: the multiplicative function $m \colon \mathbb{Z}_+ \to \mathbb{R}_+$ used to express Brun's *density* property must satisfy $m(q) \leq q - 1$ for all $q \in Q$. Those insights and requirements lead us to the following sieve.

Lemma 1. *Let $A \subseteq \mathbb{Z}$ and $Q \subseteq \mathbb{P}$ be non-empty finite sets, and let $n \coloneqq \Pi Q$ and $d \in \mathbb{Z}_+$. Consider a multiplicative function $m \colon \mathbb{Z}_+ \to \mathbb{R}_+$ satisfying $m(q) \leq q - 1$ on all $q \in Q$, and an (error) function $\sigma \colon \mathbb{N} \to \mathbb{R}$. Let $(A_r)_{r \in \mathrm{div}(n)}$ be a family of subsets of A satisfying the following two properties:*

independence: *$A_{r \cdot s} = A_r \cap A_s$, for every $r, s \in \mathrm{div}(n)$ coprime, and $A_1 = A$;*

density: *$\#A_r = \#A \cdot \frac{m(r)}{r} + \sigma(r)$, for every $r \in \mathrm{div}(n)$.*

Assume $|\sigma(r)| \leq m(r)$, and $m(q) \leq d$, for every $r \in \mathrm{div}(n)$ and $q \in Q$. Then,

$$\frac{1}{2} \cdot \#A \cdot W_m(Q) - \mathfrak{g}(Q, d) \;\leq\; \#\Big(A \setminus \bigcup_{q \in Q} A_q\Big) \;\leq\; \frac{3}{2} \cdot \#A \cdot W_m(Q) + \mathfrak{g}(Q, d),$$

where $W_m(Q) \coloneqq \prod_{q\in Q}\left(1-\frac{m(q)}{q}\right)$ *and* $\mathfrak{g}(Q,d) \coloneqq (d\cdot\#Q)^{4(d+1)^2(2+\ln\ln(\#Q+1))+2}$.

Note that setting $A_r = \{a \in A : r \mid a\}$ for every $r \in \operatorname{div}(n)$, as usually done in sieve theory, results in a family of subsets of A satisfying the *independence* property. We defer the proof of Lemma 1 and only sketch here how to establish Theorem 3. Both proofs are given in full details in Section 2.

Proof sketch of Theorem 3. Below, the set of primes Q and $d \in \mathbb{Z}_+$ defined in the statement of Theorem 3 coincide with their homonyms in Lemma 1. Let $n \coloneqq \Pi Q$. By the CRT, the system of congruences $\forall m \in M$, $x \equiv b_m \pmod m$ has a solution set S_M that is a shifted lattice with period ΠM. Fix some $k \in \mathbb{Z}$. We consider the parametric set $B(z) \coloneqq [k, k+z] \cap S_M$, and find a small value for $z \in \mathbb{N}$ ensuring that $B(z)$ contains at least one solution to $\mathcal{S}$. To do so we rely on Lemma 1: we set $A \coloneqq B(z)$, and for every $q \in Q$, define $A_q \coloneqq \{a \in A : \text{there is } i \in [1,d] \text{ s.t. } a \equiv c_{q,i} \pmod q\}$. By definition, the sieved set $A \setminus \bigcup_{q\in Q} A_q$ corresponds to the set of solutions of $\mathcal{S}$ that belong in $[k, k+z]$. The definition of A_q is extended to every $r \in \operatorname{div}(n)$ not prime as $A_r \coloneqq A \cap \bigcap_{q\in\mathbb{P}(r)} A_q$. We establish that these sets satisfy the *independence* and *density* properties of Lemma 1, subject to the following multiplicative function: $m(r) \coloneqq \prod_{q\in\mathbb{P}(r)} \#\{c_{q,i} \mod q : i \in [1,d]\}$, i.e., $m(r)$ is the product of the number of distinct values $(c_{q,i} \mod q)$, for every $q \in \mathbb{P}(r)$. By hypothesis $\min(Q) > d$, hence $m(q) \le d \le q-1$ for every $q \in Q$. Furthermore, we show that m and the error function $\sigma(r) \coloneqq \#A_r - \#A \cdot \frac{m(r)}{r}$ satisfy the assumption $|\sigma(r)| \le m(r)$, for all $r \in \operatorname{div}(n)$. Hence, by Lemma 1, we obtain a lower bound on the sieved set $A \setminus \bigcup_{q\in Q} A_q$. Lastly, we show that taking $z = \mathfrak{f}(Q,d)$ makes the lower bound strictly positive, concluding the proof.

1.3 Small solutions to r-increasing systems of divisibility constraints

We now provide an overview on the technical machinery underlying Theorem 4. Our main goal here is to formalize the notion of difficult primes $\mathbf{P}_+(\Phi)$ and to sketch the proof of Theorem 4. The full proof is given in Section 3. We first need several key definitions and auxiliary notation. Subsequently, $\mathbb{Z}[x_1,\dots,x_d]$ denotes the set of *linear* polynomials $f(x_1,\dots,x_d) = a_1\cdot x_1 + \dots + a_d \cdot x_d + c$, often written as $f(\boldsymbol{x}) = \boldsymbol{a}^\intercal\boldsymbol{x} + c$; when clear from the context, we omit the vector of variables $\boldsymbol{x}$ and write f instead of $f(\boldsymbol{x})$. The integers $a_1,\dots,a_d$ are the *coefficients* of f, c is its *constant.* A polynomial f is *primitive* if it is non-zero and $\gcd(f) = 1$, where $\gcd(f) \coloneqq \gcd(a_1,\dots,a_d,c)$. For any $b \in \mathbb{Z}$, we write $b\cdot f \coloneqq b\cdot\boldsymbol{a}^\intercal\boldsymbol{x} + b\cdot c$, and $\mathbb{Z}f \coloneqq \{b\cdot f : b \in \mathbb{Z}\}$. The *primitive part* of a polynomial g is the unique primitive polynomial f such that $g = \gcd(g)\cdot f$. Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ be a system of *divisibility constraints.* We let $\operatorname{terms}(\Phi) \coloneqq \{f_i, g_i : 1 \le i \le m\}$, and, given a finite sequence $\{(n_i, x_i)\}_{i\in I}$ of integer-variable pairs, write $\Phi[n_i \,/\, x_i : i \in I]$ for the system obtained from Φ by evaluating x_i as n_i, for all $i \in I$.

Divisibility modules and r-increasing form. As stated in Section 1.1, when dealing with a system of divisibility constraints $\Phi(\boldsymbol{x})$ one has to consider all divisibility constraints that are implied by Φ. This is done by relying on the notion of divisibility module. The *divisibility module* of a primitive polynomial f with respect to Φ, denoted by $\mathrm{M}_f(\Phi)$, is the smallest set such that (i) $f \in \mathrm{M}_f(\Phi)$; (ii) $\mathrm{M}_f(\Phi)$ is a $\mathbb{Z}$-module, i.e., $\mathrm{M}_f(\Phi)$ is closed under integer linear combinations; and (iii) if $g \mid h$ is a divisibility constraint in Φ and $b\cdot g \in \mathrm{M}_f(\Phi)$ for some $b \in \mathbb{Z}$, then $b\cdot h \in \mathrm{M}_f(\Phi)$. The following property holds: for every $g \in \mathrm{M}_f(\Phi)$ and solution $\boldsymbol{a}$ to Φ, the integer $f(\boldsymbol{a})$ divides $g(\boldsymbol{a})$. The divisibility module $\mathrm{M}_f(\Phi)$ is a vector subspace, hence it is spanned by linear polynomials $h_1,\dots,h_\ell \in \mathbb{Z}[x_1,\dots,x_d]$, that is $\mathrm{M}_f(\Phi) = \mathbb{Z}h_1 + \dots + \mathbb{Z}h_\ell$; where $+$ is the Minkowski sum.

We can now formalize the key concept of r-increasing formula. Let $\prec$ be a syntactic order on variables $\boldsymbol{x} = (x_1,\dots,x_d)$. Given $f \in \mathbb{Z}[x_1,\dots,x_d]$, we write $\mathrm{LV}_\prec(f)$ for the *leading variable* of

f, that is the variable with non-zero coefficient in f that is maximal wrt. $\prec$; if f is constant then $\mathrm{LV}_\prec(f) \coloneqq \bot$, and we postulate $\bot \prec x_i$ for all $1 \le i \le d$. We omit the subscript $\prec$ when it is clear from the context. A system of divisibility constraints Φ is in *increasing form (wrt. $\prec$)* whenever $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \dots, x_k] = \mathbb{Z}f$ for every primitive polynomial f with $\mathrm{LV}(f) = x_k$, for every $1 \le k \le d$. Given a partition $X_1, \dots, X_r$ of the variables $\boldsymbol{x}$, we write $(X_1 \prec \dots \prec X_r)$ for the set of all orders $\prec$ on $\boldsymbol{x}$ with the property that for any two x, x', if $x \in X_i$ and $x' \in X_j$ for some $i < j$ then $x \prec x'$.

Definition 1. *A system of divisibility constraints $\Phi(\boldsymbol{x})$ is* r-increasing *if there exists a partition $X_1, \dots, X_r$ of $\boldsymbol{x}$ such that Φ is in increasing form wrt. every ordering $\prec$ in $(X_1 \prec \dots \prec X_r)$.*

Observe that for any $\prec$ from $(X_1 \prec \dots \prec X_r)$, we have that for every primitive linear polynomial f and $g \in \mathrm{M}_f(\Phi)$, if $g \notin \mathbb{Z}f$ then $\mathrm{LV}_\prec(f) \in X_i$ and $\mathrm{LV}_\prec(g) \in X_j$ for some $i < j$.

The elimination property and S-terms. To handle systems in increasing form, two more concepts are required in the context of the local-to-global property. First, to compute the "global" integer solution starting from the "local" solutions modulo primes, the divisibility modules of all primitive parts of polynomials in a system of divisibility constraints Φ need to be taken into account. One way to do this, introduced in [12], is to add bases for these modules directly to Φ. This leads to the notion of elimination property: $\Phi(\boldsymbol{x})$ has the *elimination property* for the order $x_1 \prec \dots \prec x_d$ of the variables in $\boldsymbol{x}$ whenever for every primitive part f of a polynomial appearing in the left-hand side of some divisibility in Φ, and for every $0 \le k \le d$, $\{g : \mathrm{LV}(g) \preceq x_k \text{ and } f \mid g \text{ appears in } \Phi\}$ is a set of linearly independent polynomials that forms a basis for $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \dots, x_k]$, where $x_0 \coloneqq \bot$. We show that closing a formula under the elimination property can be done in polynomial time.

Lemma 2. *There is a polynomial-time algorithm that, given a system of divisibility constraints $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and an order $x_1 \prec \dots \prec x_d$ for $\boldsymbol{x}$, computes $\Psi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^n f_i' \mid g_i'$ with the elimination property for $\prec$ that is equivalent to $\Phi(\boldsymbol{x})$, both over $\mathbb{Z}$ and modulo each $p \in \mathbb{P}$.*

In a nutshell, for every primitive part f of a polynomial appearing in the left-hand side of a divisibility in Φ, the algorithm first computes a finite set S spanning $\mathrm{M}_f(\Phi)$. The algorithm then uses the Hermite normal form of a matrix, whose entries are the coefficients and constant of the elements of S, to obtain linearly independent polynomials $h_1, \dots, h_\ell$ with different leading variables with respect to $\prec$. The system Ψ is then obtained by replacing divisibility constraints of the form $f \mid g$ appearing in Φ with the divisibilities $f \mid h_1, \dots, f \mid h_\ell$. Full details are given in Appendix C.

The second concept is related to how Theorem 4 is proven. In a nutshell, in the proof we iteratively assign values to the variables in a way that guarantees the system of divisibility constraints to stay in increasing form. To do that, additional polynomials need to be considered. For an example, consider the following system of divisibility constraints Φ in increasing form for the order $u \prec v \prec x \prec y \prec z$, and with the elimination property for that order:

$$\Phi \;\coloneqq\; v \mid u + x + y \;\wedge\; v \mid x \;\wedge\; y + 2 \mid z + 1 \;\wedge\; v \mid z\,.$$

From the first two divisibility constraints, we have $(u + y) \in \mathrm{M}_v(\Phi)$; i.e., $(u - 2) + (y + 2) \in \mathrm{M}_v(\Phi)$. Therefore, if u were to be instantiated as 2, the resulting formula Φ' would satisfy $(y + 2) \in \mathrm{M}_v(\Phi')$ and hence $(z + 1) \in \mathrm{M}_v(\Phi')$, from the third divisibility constraint. Then, $1 \in \mathrm{M}_v(\Phi')$ would follow from the last divisibility, violating the constraints of the increasing form. The reason why increasingness is lost when setting $u = 2$ stems from the fact that in Φ' we have an implied divisibility $v \mid y + 2$, where $y + 2$ is a left-hand side that was not present in $\mathrm{M}_v(\Phi)$. We can avoid this problem by considering the polynomial $u - 2$ and forcing it to be non-zero. The main issue is then to identify all such problematic polynomials, which is done with the following notion of S-terms. Less refined versions of this notion, as considered in [14, 12], result in exponentially larger sets of polynomials.

Given polynomials $f(\boldsymbol{x})$ and $g(\boldsymbol{x})$ with $\mathrm{LV}(f) = x_l$ and $\mathrm{LV}(g) = x_k$, we define their *S-polynomial* $S(f, g) \coloneqq b_k \cdot f - a_l \cdot g$, where a_l and b_k are coefficients of x_l in f and x_k in g, respectively. For constant f (resp. g), i.e., $\mathrm{LV}(f) = \bot$, above $a_l \coloneqq f$ (resp. $b_k \coloneqq g$). Note that if f and g are non-constant and $\mathrm{LV}(f) = \mathrm{LV}(g)$ then $\mathrm{LV}(S(f, g)) \prec \mathrm{LV}(f)$. For any $X \subseteq \mathbb{Z}[x_1, \dots, x_n]$, we define $S(X) \coloneqq X \cup \{S(f, g) : f, g \in X\}$. Given a system of divisibility constraints Φ with the elimination property for $\prec$ and a primitive polynomial f, we define the set of *S-terms for f*, denoted as $\mathrm{S}_f(\Phi)$, to be the smallest set such that (i) $\mathrm{terms}(\Phi) \subseteq \mathrm{S}_f(\Phi)$, and (ii) if $f \mid g$ occurs in Φ and $h \in \mathrm{S}_f(\Phi)$ with $\mathrm{LV}(g) = \mathrm{LV}(h)$, then $S(g, h) \in \mathrm{S}_f(\Phi)$. We write $\Delta(\Phi)$ for the set of all S-terms for f, where f is any primitive part of a polynomial in $\mathrm{terms}(\Phi)$.

The set of difficult primes. We now turn towards identifying a small set of difficult primes $\mathbf{P}_+(\Phi)$ of polynomial bit length. There are two categories of difficult primes: those for which a solution to Φ modulo p is not guaranteed to exist, and those for which such a solution always exists, but which still influences the size of the minimal integer solution for Φ. The former is the set $\mathbb{P}(\Phi)$ defined in Section 1.1. The next lemma shows that Φ has a solution modulo any prime not in $\mathbb{P}(\Phi)$.

Lemma 3. *Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^{m} f_i \mid g_i$ and $p \in \mathbb{P} \setminus \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{b} \in \mathbb{N}^d$ modulo p such that $v_p(f_i(\boldsymbol{b})) = 0$ for every $1 \leq i \leq m$, and $\|\boldsymbol{b}\| \leq p - 1$.*

The proof of Lemma 3 is given in Appendix D. In a nutshell, $v_p(f_i(\boldsymbol{b})) = 0$ holds if and only if $f_i(\boldsymbol{b}) \not\equiv 0 \pmod p$, meaning that the solution $\boldsymbol{b}$ can be computed by considering a system of at most m non-congruences; one for each left-hand side of Φ. Consider an ordering $\prec$ of the variables in $\boldsymbol{x}$. Since $p \notin \mathbb{P}(\Phi)$, p does not divide any coefficient or constant appearing in some f_i. This means that if $f_i(\boldsymbol{x}) = f_i' + a \cdot x$, with $x = \mathrm{LV}_\prec(f_i)$, we can rewrite $f_i(\boldsymbol{x}) \not\equiv 0 \pmod p$ as $x \not\equiv -a^{-1} f_i' \pmod p$, where a^{-1} is the inverse of a modulo p. Then, since $p > m$, one can find $\boldsymbol{b}$ by picking suitable residues in $\{0, \dots, p-1\}$; this can be done inductively, starting from the $\prec$-minimal variable.

Extending $\mathbb{P}(\Phi)$ into $\mathbf{P}_+(\Phi)$, hence capturing the second of the two categories above, is a delicate matter. In fact, while $\mathbb{P}(\Phi)$ is defined for an arbitrary system of divisibility constraints, the set $\mathbf{P}_+(\Phi)$ can only meaningfully be defined on systems that have the elimination property for an order $\prec$. For systems without the elimination property, one must first appeal to Lemma 2. Let Φ be a system of divisibility constraints with the elimination property. The set of *difficult primes* $\mathbf{P}_+(\Phi)$ is the set of primes $p \in \mathbb{P}$ satisfying at least one the following conditions:

(P1) $p \leq \#S(\Delta(\Phi))$,

(P2) p divides any non-zero coefficient or constant of a polynomial in $S(\Delta(\Phi))$, or

(P3) p divides the smallest (in absolute value) non-zero $\lambda \in \mathbb{Z}$ such that $\lambda \cdot g \in \mathrm{M}_f(\Phi)$ for some primitive polynomial f occurring in Φ and $g \in \mathrm{S}_f(\Phi)$ (if such a λ exists).

Note that (P1) and (P2) imply $\mathbb{P}(\Phi) \subseteq \mathbf{P}_+(\Phi)$. The following lemma establishes bounds on these two sets that are central to the proof of Theorem 4.

Lemma 4. *Consider a system of divisibility constraints $\Phi(\boldsymbol{x})$ in d variables. Then, the set of primes $\mathbb{P}(\Phi)$ satisfies $\log_2(\Pi\mathbb{P}(\Phi)) \leq m^2(d+2) \cdot (\langle\|\Phi\|\rangle + 2)$. Furthermore, if Φ has the elimination property for an order $\prec$ on $\boldsymbol{x}$, then the set of primes $\mathbf{P}_+(\Phi)$ satisfies $\log_2(\Pi\mathbf{P}_+(\Phi)) \leq 64 \cdot m^5 (d+2)^4 (\langle\|\Phi\|\rangle + 2)$.*

The proof of Lemma 4 is given in Appendix D. Note that $\langle S \rangle = O(\log_2(\Pi S))$ for any finite set S of positive integers, and therefore the above lemma bounds $\langle\mathbb{P}(\Phi)\rangle$ and $\langle\mathbf{P}_+(\Phi)\rangle$ polynomially.

Proof sketch of Theorem 4. Recall that Theorem 4 establishes a local-to-global property for r-increasing systems of divisibility constraints $\Phi(\boldsymbol{x})$: if such a system has a solution $\boldsymbol{b}_p \in \mathbb{Z}^d$ modulo p for every prime $p \in \mathbb{P}(\Phi)$, then it has infinitely many integer solutions, and a solution $\boldsymbol{a} \in \mathbb{N}^d$ such that $\langle\|\boldsymbol{a}\|\rangle \leq (\langle\Phi\rangle + \max\{\langle\|\boldsymbol{b}_p\|\rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$. We give a high-level overview of the proof of this result, focusing on the part of the statement that constructs a solution over $\mathbb{N}$. The full proof is given in Section 3.2. Fix an order $\prec$ in $X_1 \prec \cdots \prec X_r$. We compute a map $\boldsymbol{\nu}\colon \left(\bigcup_{j=1}^r X_j\right) \to \mathbb{Z}_+$ such that $\boldsymbol{\nu}(\boldsymbol{x})$ is a solution for Φ by induction on r, populating $\boldsymbol{\nu}$ according the order $\prec$.

If $r = 1$, the system Φ is of the form $\bigwedge_{i=1}^{\ell} c_i \mid g_i(\boldsymbol{x}) \wedge \bigwedge_{j=\ell+1}^{m} f_j(\boldsymbol{x}) \mid a_j \cdot f_j(\boldsymbol{x})$, with $c_i \in \mathbb{Z} \setminus \{0\}$ and $a_j \in \mathbb{Z}$, and $\boldsymbol{\nu}$ can be computed using the CRT. Given $p \in \mathbb{P}(\Phi)$, one considers the natural number $\mu_p \coloneqq \max\left\{v_p(f(\boldsymbol{b}_p)) : f(\boldsymbol{x}) \text{ left-hand side of a divisibility in } \Phi\right\}$, which determines up to what power of p the integer solution given by $\boldsymbol{\nu}$ has to agree with the solution $\boldsymbol{b}_p$. Then, the CRT instance to be solved is $x_k \equiv b_{p,k} \pmod{p^{\mu_p+1}}$ for every $p \in \mathbb{P}(\Phi)$ and $1 \leq k \leq d$, where $x_1 \prec \cdots \prec x_d$ are the variables in Φ and $b_{p,1}, \dots, b_{p,d}$ are their related values in $\boldsymbol{b}_p$.

When $r \geq 2$, the construction is much more involved. The goal is to define $\boldsymbol{\nu}$ for the variables in X_1 in such a way that the formula $\Phi' \coloneqq \Phi[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$ is increasing for $X_2 \prec \cdots \prec X_r$, and has solutions modulo p for every $p \in \mathbb{P}(\Phi')$. This allows us to invoke Theorem 4 inductively, obtaining a solution $\boldsymbol{\xi}\colon \left(\bigcup_{j=2}^r X_j\right) \to \mathbb{Z}_+$ for Φ'. An integer solution for Φ is then given by the union $\boldsymbol{\nu} \sqcup \boldsymbol{\xi}$ of $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$, i.e., the map defined as $\boldsymbol{\nu}(x)$ for $x \in X_1$ and as $\boldsymbol{\xi}(y)$ for $y \in \bigcup_{j=2}^r X_j$. To construct $\boldsymbol{\nu}$ for X_1, we first close Φ under the elimination property following Lemma 2, obtaining an equivalent system Ψ, and extend the solutions $\boldsymbol{b}_p$ to every $p \in \mathbf{P}_+(\Psi)$ thanks to Lemma 3. We then populate $\boldsymbol{\nu}$ following the order $\prec$, starting from the smallest variable. In the proof, this is done with a second induction. Values for the variables in X_1 are found using Theorem 3. When a new value $a_k \in \mathbb{Z}_+$ for a variable $x_k \in X_1$ is found, new primes need to be taken into account, since substituting a_k for x_k yields a complete evaluation of the polynomials in $S(\Delta(\Phi))$ with leading variable x_k, i.e., these polynomials become integers that may be divisible by primes not belonging to $\mathbf{P}_+(\Psi)$. For subsequent variables in X_1, we make sure to pick values that keep the evaluated polynomials as "coprime as possible" with respect to these new primes. This condition is necessary to obtain the new solutions $\boldsymbol{b}_p$ for the formula Φ', modulo every $p \in \mathbb{P}(\Phi')$. The precise system of (non-)congruences considered when computing x_k is

$$\begin{cases} x_k \equiv b_{p,k} & \pmod{p^{\mu_p+1}} \quad p \in \mathbf{P}_+(\Psi) \\ g(\boldsymbol{\nu}(\boldsymbol{y}), x_k) \not\equiv 0 & \pmod{q} \quad\quad\;\; q \in Q \setminus \mathbf{P}_+(\Psi),\ g(\boldsymbol{y}, x_k) \in S(\Delta(\Psi)) \text{ with } \mathrm{LV}_\prec(g) = x_k \end{cases}$$

where Q is the set of new primes obtained when fixing the variables $\boldsymbol{y} = (x_1, \dots, x_{k-1})$, and $\mu_p \coloneqq \max\left\{v_p(f(\boldsymbol{b}_p)) : f(\boldsymbol{x}) \text{ left-hand side of a divisibility in } \Psi\right\}$. Theorem 3 can be applied on the system above because primes in $Q \setminus \mathbf{P}_+(\Psi)$ do not satisfy the properties (P1) and (P2).

To show that Theorem 4 can be applied inductively on Φ', we rely on (P3) and the elimination property of Ψ to show that Φ' has solutions modulo every $p \in \mathbb{P}(\Phi')$, and on properties of S-terms and again on the elimination property of Ψ to show that Φ' is increasing for $X_2 \prec \cdots \prec X_r$.

1.4 Solving an instance of IP-GCD

We now briefly discuss the proof of Theorem 1, full details are deferred to Section 4. In a nutshell, this result is shown by giving an algorithm that reduces an *IP-GCD system* $\Phi(\boldsymbol{x}) \coloneqq A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{k} \gcd(f_i(\boldsymbol{x}), g_i(\boldsymbol{x})) \sim_i c_i$ into an equi-satisfiable disjunction of several 3-increasing systems of divisibility constraints with coefficients and constants of polynomial bit length. We then study bounds on the solutions of each of these systems modulo the primes required by the local-to-global property, and conclude that IP-GCD has a small witness property over the integers directly from Theorem 4.

Our arguments heavily rely on syntactic properties of the systems of divisibility constraints we obtain when translating an IP-GCD system Φ. These syntactic properties are captured in Section 4 with the notion of *gcd-to-div* triple. The formal definition is rather lengthy, for this overview it suffices to know that a triple $(\Psi, \boldsymbol{u}, E)$ is a gcd-to-div triple if Ψ is a system of divisibility constraints in which all numbers appearing are positive, and $\boldsymbol{u}$ and E are a vector and a matrix that act as a change of variables between the variables in Ψ and the variables in Φ. The following proposition formalizes the role of gcd-to-div triples.

Proposition 1. *Let Φ be an IP-GCD system in d variables. There is a set C of gcd-to-div triples such that the set of integer solutions to Φ is $\{\boldsymbol{u} + E \cdot \boldsymbol{\lambda} : (\Psi, \boldsymbol{u}, E) \in C$ and $\boldsymbol{\lambda} \in \mathbb{N}^m$ solution to $\Psi\}$. Every $(\Psi, \boldsymbol{u}, E) \in C$ has bit length polynomial in $\langle \Phi \rangle$ and is such that Ψ is in 3-increasing form.*

Above, m is the number of free variables in Ψ, which is also the number of columns in E. The algorithm showing this proposition, cf. Lemma 10 and Lemma 13 in Section 4, performs a series of equivalence-preserving syntactic transformations of Φ that are mainly divided into two steps: we first compute from Φ a set of gcd-to-div triples B satisfying $\{\boldsymbol{x} \in \mathbb{Z}^d : \boldsymbol{x}$ solution to $\Phi\} = \{\boldsymbol{u}+E\cdot\boldsymbol{\lambda} : (\Psi, \boldsymbol{u}, E) \in B$ and $\boldsymbol{\lambda} \in \mathbb{N}^m$ solution to $\Psi\}$, and then obtains C by manipulating every system of divisibility constraints in B to make it 3-increasing. Below we give a summary of these two steps.

Step I: from IP-GCD to divisibility constraints. This step is split into three sub-steps:

1. Reduce the input IP-GCD system Φ into an equi-satisfiable disjunction of IP-GCD system having GCD of the form $\gcd(f(\boldsymbol{x}), g(\boldsymbol{x})) = c$ or $\gcd(f(\boldsymbol{x}), g(\boldsymbol{x})) \geq c$, and a system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$ fixing a sign for every polynomial $h(\boldsymbol{x})$ appearing in a GCD constraint, i.e., $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$ has either $h(\boldsymbol{x}) \leq -1$ or $h(\boldsymbol{x}) \geq 1$ as a row.

2. Let G be the set of systems computed at the previous step. The algorithm erases the system of inequalities $A \cdot \boldsymbol{x} \leq \boldsymbol{b}$ from every IP-GCD system $\Psi \in G$ by performing a change of variables. In particular, relying on a well-known result by von zur Gathen and Sieveking [25], the algorithm computes a finite set $\{(\boldsymbol{u}_i, E_i) : i \in I_\Psi\}$ such that $\{\boldsymbol{x} \in \mathbb{Z}^d : A \cdot \boldsymbol{x} \leq \boldsymbol{b}\} = \{\boldsymbol{u}_i + E_i \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{N}^m,\ i \in I_\Psi\}$. For every $i \in I_\Psi$, the algorithm constructs a system of GCD constraints Ψ_i by replacing $\boldsymbol{x}$ in all GCD constraints of Ψ with $\boldsymbol{u}_i + E_i \cdot \boldsymbol{y}$, where $\boldsymbol{y}$ is a family of fresh variables. The latter transformation also ensures that all numbers in the Ψ_i are positive.

3. The algorithm translates every GCD constraint in every Ψ_i into a divisibility. Each constraint $\gcd(f(\boldsymbol{y}), g(\boldsymbol{y})) = c$ is replaced by $\exists z \in \mathbb{N} : \ c \mid f \wedge c \mid g \wedge f \mid z \wedge g \mid z + c$, following Bézout's identity, whereas $\gcd(f(\boldsymbol{y}), g(\boldsymbol{y})) \geq c$ becomes $\exists z \in \mathbb{N} : \ z + c \mid f \wedge z + c \mid g$. The triple $(\Psi_i, \boldsymbol{u}_i, E_i)$ obtained after these replacements is a gcd-to-div triple.

Step II: enforcing increasingness. The algorithm considers each gcd-to-div triple $(\Psi, \boldsymbol{u}, E)$ computed in the previous step and further manipulates it, producing a set of gcd-to-div triples D having only systems of divisibility constraints in 3-increasing form, and satisfying

$$\{\boldsymbol{u} + E \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{N}^m \text{ solution for } \Psi\} = \{\boldsymbol{u}' + E' \cdot \boldsymbol{\lambda} : (\Psi', \boldsymbol{u}', E') \in D,\ \boldsymbol{\lambda} \in \mathbb{N}^{m'} \text{ solution for } \Psi'\}. \quad (1)$$

The set D is computed as follows. If Ψ is already 3-increasing, then $D \coloneqq \{(\Psi, \boldsymbol{u}, E)\}$. Otherwise, properties of gcd-to-div triples ensure that there is a non-constant primitive polynomial f with positive coefficients and constant such that $\mathrm{M}_f(\Psi) \cap \mathbb{Z} \neq \{0\}$. The algorithm computes the smallest positive integer c belonging to $\mathrm{M}_f(\Psi)$. We have that Ψ entails $f \mid c$. Let $\lambda_1, \ldots, \lambda_j$ be all the variables in f. Since the coefficients and constant of f are all positive and variables are now interpreted over the naturals, such a divisibility constraint can only be satisfied by assigning to each variable an integer in $[0, c]$. The algorithm iterates over each assignment $\boldsymbol{\nu} \colon \{\lambda_1, \dots, \lambda_j\} \to [0, c]$ satisfying $f \mid c$, computing from $(\Psi, \boldsymbol{u}, E)$ the gcd-to-div triple $(\Psi_{\boldsymbol{\nu}}, \boldsymbol{u}_{\boldsymbol{\nu}}, E_{\boldsymbol{\nu}})$ where $\Psi_{\boldsymbol{\nu}} \coloneqq \Psi[\boldsymbol{\nu}(\lambda_i) / \lambda_i : i \in [1, j]]$, and $\boldsymbol{u}_{\boldsymbol{\nu}}$ and $E_{\boldsymbol{\nu}}$ are obtained from $\boldsymbol{u}$ and E based on $\boldsymbol{\nu}$ too. All such triples are added to D to replace $(\Psi, \boldsymbol{u}, E)$. However, some newly added system $\Psi_{\boldsymbol{\nu}}$ may not be 3-increasing. If that is the case, Step II is iteratively performed on $(\Psi_{\boldsymbol{\nu}}, \boldsymbol{u}_{\boldsymbol{\nu}}, E_{\boldsymbol{\nu}})$. Termination is guaranteed because $\Psi_{\boldsymbol{\nu}}$ has strictly fewer variables than Ψ and the set of computed gcd-to-div triples is the set C from Proposition 1.

Bounds on the solutions modulo primes and proof sketch of Theorem 1. Following Proposition 1, what is left to apply Theorem 4 is to compute the solutions modulo primes in $\mathbb{P}(\Psi)$, for all $(\Psi, \boldsymbol{u}, E) \in C$. In Section 4.2 we rely on properties of gcd-to-div triples to show the result below.

Lemma 5. *Let $(\Psi, \boldsymbol{u}, E)$ be a gcd-to-div triple in which Ψ has d variables, and consider $p \in \mathbb{P}(\Psi)$. If Ψ has a solution modulo p, then it has a solution $\boldsymbol{b}_p \in \mathbb{Z}^d$ modulo p with $\|\boldsymbol{b}_p\| \leq (d+1) \cdot \|\Psi\|^3 p^2$.*

Proposition 1, and Lemmas 4 and 5 imply the part of Theorem 1 not concerning optimization as a corollary of Theorem 4. For optimization, consider a linear objective $\boldsymbol{c}^\intercal \boldsymbol{x}$ to be minimized (the argument is analogous for maximization) subject to an IP-GCD system $\Phi(\boldsymbol{x})$, and let C be the set of gcd-to-div triples computed from Φ following Proposition 1. We show in Section 4.3 the following characterization that implies the optimization part of Theorem 1: an optimal solution exists if and only if (i) there is $(\Psi, \boldsymbol{u}, E) \in C$ such that Ψ satisfiable over $\mathbb{N}$, and (ii) for every $(\Psi, \boldsymbol{u}, E) \in C$ with Ψ satisfiable over $\mathbb{N}$, $\boldsymbol{c}^\intercal(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$ has no variable with a strictly negative coefficient. Moreover, if there is an optimal solution, then there is one with polynomial bit length with respect to $\langle \Phi \rangle$ and $\langle \boldsymbol{c} \rangle$. Briefly, the double implication comes from the fact that the construction required to establish Theorem 4 also shows that for each variable in $\boldsymbol{\lambda}$ there are infinitely many values that yield a solution to Ψ, both in the positive and negative direction, and therefore the existence of a variable in $\boldsymbol{c}^\intercal(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$ having a negative coefficient entails the non-existence of an optimum. For the bound, one shows that $\min\{\boldsymbol{c}^\intercal \boldsymbol{u} : (\Psi, \boldsymbol{u}, E) \in C\}$ is a lower bound to every solution of Φ. Then, the polynomial bound follows directly from Proposition 1.

1.5 Conclusion and future work

We have established a polynomial small witness property for integer programming with additional GCD constraints over linear polynomials. Our work also sheds new light on the feasibility problem for systems of divisibility constraints between linear polynomials over the integers, and more broadly on the existential fragment of the first-order theory of the structure $L_{\text{div}} = (\mathbb{Z}, 0, 1, +, \leq, |)$, which is known to be NP-hard and decidable in NEXP [15, 12]. Proposition 2 shows that systems of divisibility constraints in increasing form are decidable in NP. Thus, in order to improve the known NEXP upper bound of existential L_{div}, it would suffice to provide an algorithm that translates an arbitrary existential L_{div} formula in increasing form without the exponential blow-up that existing algorithms incur [14, 12].

Our work may also enable obtaining improved complexity results for other problems that reduce to the existential theory of L_{div}. For instance, [13] Lin and Majumdar reduce deciding a special class of word equations with length constraints and regular constraints to existential L_{div}, hence obtaining an NEXP for their problem. The formulas resulting from their reduction are of a special shape, and showing them to be r-increasing for some fixed r would directly yield a PSPACE decision procedure for the aforementioned class of word equations.

2 A Chinese remainder theorem with non-congruences

In this section, we prove our Chinese-remainder-style theorem for simultaneous congruences and non-congruences (Theorem 3) as well as the abstract version of Brun's pure sieve (Lemma 1). Throughout this paper, e is reserved for Euler's number, and $\exp(x) \coloneqq e^x$.

We start by providing the proof of Lemma 1, which following the original proof by Brun is established by analyzing a truncated inclusion-exclusion principle.

Lemma 1. *Let $A \subseteq \mathbb{Z}$ and $Q \subseteq \mathbb{P}$ be non-empty finite sets, and let $n \coloneqq \Pi Q$ and $d \in \mathbb{Z}_+$. Consider a multiplicative function $m \colon \mathbb{Z}_+ \to \mathbb{R}_+$ satisfying $m(q) \leq q-1$ on all $q \in Q$, and an (error) function $\sigma \colon \mathbb{N} \to \mathbb{R}$. Let $(A_r)_{r \in \operatorname{div}(n)}$ be a family of subsets of A satisfying the following two properties:*

independence: *$A_{r \cdot s} = A_r \cap A_s$, for every $r, s \in \operatorname{div}(n)$ coprime, and $A_1 = A$;*

density: *$\#A_r = \#A \cdot \frac{m(r)}{r} + \sigma(r)$, for every $r \in \operatorname{div}(n)$.*

Assume $|\sigma(r)| \leq m(r)$, and $m(q) \leq d$, for every $r \in \operatorname{div}(n)$ and $q \in Q$. Then,

$$\frac{1}{2} \cdot \#A \cdot W_m(Q) - \mathfrak{g}(Q,d) \;\leq\; \#\Big(A \setminus \bigcup\nolimits_{q \in Q} A_q\Big) \;\leq\; \frac{3}{2} \cdot \#A \cdot W_m(Q) + \mathfrak{g}(Q,d),$$

where $W_m(Q) \coloneqq \prod_{q \in Q} \Big(1 - \frac{m(q)}{q}\Big)$ and $\mathfrak{g}(Q,d) \coloneqq (d \cdot \#Q)^{4(d+1)^2(2+\ln\ln(\#Q+1))+2}$.

Proof. We define $S(A,Q) \coloneqq \#\big(A \setminus \bigcup_{q \in Q} A_q\big)$. By definition of $S(A,Q)$ we have:

$$\begin{aligned} S(A,Q) &= \#A - \sum_{q \in Q} \#A_q + \sum_{s \neq r \in Q} \#(A_s \cap A_r) - \dots \pm \#\Big(\bigcap_{p \in Q} A_p\Big) \\ &= \#A_1 - \sum_{q \in Q} \#A_q + \sum_{s \neq r \in Q} \#A_{s \cdot r} - \dots \pm \#A_{\Pi Q} \qquad \text{by the } \textit{independence} \text{ property.} \end{aligned}$$

Truncating the inclusion-exclusion sequence above, after an even (resp. odd) number of terms results in a lower bound (resp. upper bound) for $S(A,Q)$. Truncating the sequence too early would result in a useless bound; e.g., stopping at the second term might result in a negative lower bound for Q sufficiently large. Conversely, truncating it too late would make the hypotheses of the lemma too weak. To emphasize better this point, let us first clarify the truncation. Let $\omega(r) \coloneqq \#\mathbb{P}(r)$ be the prime omega function and, given $k \in \mathbb{N}$, define $Q(k) \coloneqq \{r \in \operatorname{div}(\Pi Q) : \omega(r) \leq k\}$. Fix $\ell \in \mathbb{N}_+$. We consider the (truncated) sequence $T(\ell, A, Q)$ given by

$$T(\ell, A, Q) \coloneqq \#A_1 - \sum_{q \in Q} \#A_q + \sum_{s \neq r \in Q} \#A_{s \cdot r} - \dots \pm \sum_{\substack{r \text{ product of} \\ \ell \text{ distinct primes in } Q}} \#A_r$$

which can be also written as $\sum_{r \in Q(\ell)} (-1)^{\omega(r)} \#A_r$. From the *density* property, $T(\ell, A, Q)$ equals

$$\#A \cdot \sum_{r \in Q(\ell)} \frac{(-1)^{\omega(r)} m(r)}{r} + \sum_{r \in Q(\ell)} (-1)^{\omega(r)} \sigma(r). \tag{2}$$

Note that $\mu(x) \coloneqq (-1)^{\omega(x)}$ is the Möbius function [7], which is multiplicative. Let us look at the two sides of the sum above. Note that for $\ell = \#Q$ the left term $\#A \cdot \sum_{r \in Q(\ell)} \frac{(-1)^{\omega(r)} m(r)}{r}$ can be factorized as $\#A \cdot \prod_{q \in Q} \big(1 + \frac{\mu(q) \cdot m(q)}{q}\big)$, because both μ and m are multiplicative. This is equal to

$\#A \cdot W_m(Q)$, by definition of $W_m(Q)$ and using the fact that $\mu(q) = -1$ for q prime. In practice, the higher the ℓ, the closer the left term of the sum in (2) becomes to $\#A \cdot W_m(Q)$. However, increasing ℓ comes at the cost of increasing the error term given by the right term in the sum. Indeed, note that for $\ell = \#Q$ the sum $\sum_{r \in Q(\ell)} (-1)^{\omega(r)} \sigma(r)$ can a priori be larger than $\sigma(\Pi Q)$, which from the hypotheses can at best be bounded as $|\sigma(\Pi Q)| \leq m(\Pi Q) \leq d^{\#Q}$. Hence, to obtain the bounds in the statement of Lemma 1, we need to find a value of ℓ making the left term in (2) close enough to $\#A \cdot W_m(Q)$ while keeping the error term small (in absolute value). Below, we first analyze the two terms of the sum in (2), and then optimize the value of ℓ. For brevity, we focus on computing the lower bound of $S(A, Q)$ (which is all we need for Theorem 3); thus setting ℓ to be odd, so that $S(A, Q) \geq T(\ell, A, Q)$. The computation of the upper bound is analogous.

Lower bound on the error term of (2)**:** Since $|\sigma(r)| \leq m(r) \leq d^{\omega(r)} \leq d^\ell$ when $\omega(r) \leq \ell$,

$$\sum_{r \in Q(\ell)} \mu(r) \cdot \sigma(r) \geq \sum_{r \in Q(\ell)} -|\sigma(r)| \geq \sum_{r \in Q(\ell)} -d^\ell \geq -\Big(\frac{e \cdot \#Q}{\ell}\Big)^\ell d^\ell, \tag{3}$$

where the rightmost inequality is derived by applying a well-known upper bound on the partial sums of binomial coefficients: $\#Q(\ell) = \sum_{i=0}^{\ell} \binom{\#Q}{i} \leq \big(\frac{e \cdot \#Q}{\ell}\big)^\ell$.

Lower bound on the left term of (2)**:** Correctly computing a lower bound for this term requires a long manipulation using properties of the Möbius function and bounds on prime numbers. The following claim (proven in Appendix A) summarizes this computation.

Claim 1. $\displaystyle\sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r} \geq W_m(Q) \left(1 - \Big(\frac{e \cdot \alpha}{\ell}\Big)^\ell \alpha \cdot e^\alpha\right)$, *with* $\alpha := (d+1)^2(2 + \ln\ln(\#Q+1))$.

Optimizing the value of ℓ: To obtain the lower bound for $S(A, Q)$ presented in the statement of the lemma, we want ℓ to be chosen so that

$$\#A \cdot \sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r} \geq \frac{1}{2} \cdot \#A \cdot W_m(Q).$$

Following Claim 1, it suffices to pick an ℓ making the inequality $\big(\frac{e \cdot \alpha}{\ell}\big)^\ell \alpha \cdot e^\alpha \leq \frac{1}{2}$ true. Note that, since $d \geq 1$ and $\#Q \geq 1$, we have $\alpha > 6.5$. Then, we see that $\ell \geq 1.44 \cdot e \cdot \alpha$ does the job:

$$\Big(\frac{e \cdot \alpha}{\ell}\Big)^\ell \alpha \cdot e^\alpha \leq \left(\frac{1}{1.44}\right)^{1.44 \cdot e \cdot \alpha} \cdot e^{\alpha + \ln \alpha} \leq \frac{e^{\alpha + \ln \alpha}}{1.44^{1.44 \cdot e \cdot \alpha}} \leq \frac{e^{1.3 \cdot \alpha}}{1.44^{1.44 \cdot e \cdot \alpha}} \leq \left(\frac{e^{1.3}}{1.44^{1.44 \cdot e}}\right)^{6.5} \leq \frac{1}{2}.$$

Hence, we pick ℓ to be an odd number in $[1.44 \cdot e \cdot \alpha,\ 1.44 \cdot e \cdot \alpha + 2]$. From Equation (3) we obtain

$$\sum_{r \in Q(\ell)} \mu(r) \cdot \sigma(r) \geq -\Big(\frac{e \cdot \#Q}{1.44 \cdot e \cdot \alpha + 2}\Big)^{1.44 \cdot e \cdot \alpha + 2} \cdot d^{1.44 \cdot e \cdot \alpha + 2} \geq -\big(d \cdot \#Q\big)^{4(d+1)^2(2 + \ln\ln(\#Q+1)) + 2}.$$

As $S(A, Q) \geq T(\ell, A, Q) = \#A \cdot \sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r} + \sum_{r \in Q(\ell)} \mu(r) \cdot \sigma(r)$, that completes the proof. $\square$

We now move to the proof of Theorem 3.

Theorem 3. *Let $d \in \mathbb{Z}_+$, $M \subseteq \mathbb{Z}_+$ finite, and $Q \subseteq \mathbb{P}$ be a non-empty finite set of primes such that the elements of $M \cup Q$ are pairwise coprime, $M \cap Q = \emptyset$, and $\min(Q) > d$. Consider the univariate system of simultaneous congruences and non-congruences $\mathcal{S}$ defined by*

$$\begin{aligned} x &\equiv b_m \pmod{m} & & m \in M \\ x &\not\equiv c_{q,i} \pmod{q} & & q \in Q,\ 1 \leq i \leq d\,. \end{aligned}$$

Then, for every $k \in \mathbb{Z}$, $\mathcal{S}$ has a solution in the interval $\{k, \dots, k + \Pi M \cdot \mathfrak{f}(Q,d)\}$, where

$$\mathfrak{f}(Q,d) \coloneqq \big((d+1) \cdot \#Q\big)^{4(d+1)^2(3+\ln\ln(\#Q+1))}.$$

Proof. Expanding on the sketch of the proof given in Section 1.2, recall that the set of primes Q and $d \in \mathbb{Z}_+$ defined in the statement of Theorem 3 coincide with their homonyms in Lemma 1. Furthermore, we let $n \coloneqq \Pi Q$, and define:

- S_M to be the solution set to the system of congruences $\forall m \in M$, $x \equiv b_m \pmod{m}$, which is a shifted lattice with period ΠM by the CRT,
- $B(z) \coloneqq [k, k+z] \cap S_M$, where k is the integer in the statement of the theorem,
- some integer z to be optimized. We will show that $z = \mathfrak{f}(Q,d)$ yield the theorem,
- $A \coloneqq B(z)$, and given $q \in Q$, $A_q \coloneqq \{a \in A : \text{there is } i \in [1,d] \text{ s.t. } a \equiv c_{q,i} \pmod{q}\}$,
- for $r \in \operatorname{div}(n)$ not prime, $A_r \coloneqq A \cap \bigcap_{q \in \mathbb{P}(r)} A_q$,
- for $r \in \operatorname{div}(n)$, $m(r) \coloneqq \prod_{q \in \mathbb{P}(r)} \#\{c_{q,i} \mod q : i \in [1,d]\}$, which is a multiplicative function,
- and we take $\sigma(r) \coloneqq \#A_r - \#A \cdot \frac{m(r)}{r}$ as an error function.

Note that, by definition, $A \setminus \bigcup_{q \in Q} A_q$ corresponds to the set of solutions of $\mathcal{S}$ that belong to $[k, k+z]$. We show that the objects above satisfy the hypothesis of Lemma 1, and that taking $z = \mathfrak{f}(Q,d)$ makes the cardinality of $A \setminus \bigcup_{q \in Q} A_q$ strictly positive, yielding Theorem 3.

The assumptions of Lemma 1 hold: By hypothesis $\min(Q) > d$, hence $m(q) \leq d \leq q-1$ for every $q \in Q$. Below, we show that the *independence* and *density* properties are satisfied, and that $|\sigma(r)| \leq m(r)$ for every $r \in \operatorname{div}(n)$. This allows us to apply Lemma 1 in the second part of the proof. The *independence* property is trivially satisfied: given $r, s \in \operatorname{div}(n)$ coprime, we have

$$A_{r \cdot s} = A \cap \bigcap_{q \in \mathbb{P}(r \cdot s)} A_q = \Big(A \cap \bigcap_{q \in \mathbb{P}(r)} A_q\Big) \cap \Big(A \cap \bigcap_{p \in \mathbb{P}(s)} A_p\Big) = A_r \cap A_s.$$

Below, fix $r \in \operatorname{div}(n)$. The *density* property and the condition $|\sigma(r)| \leq m(r)$ are proved together. By definition of A_r,

$$A_r = \bigcup_{\alpha\colon \mathbb{P}(r) \to [1,d]} (A \cap S_{\alpha,r})\,, \qquad \text{where } S_{\alpha,r} \coloneqq \{\ell \in \mathbb{Z} : \text{ for every } q \in \mathbb{P}(r),\ \ell \equiv c_{q,\alpha(q)} \pmod{q}\}.$$

The following claim bounds the cardinality of each $(A \cap S_{\alpha,r})$. It is proven in Appendix B.

Claim 2. $\dfrac{\#A}{r} - 1 \leq \#(A \cap S_{\alpha,r}) \leq \dfrac{\#A}{r} + 1.$

Directly form their definition, given two functions $\alpha_1, \alpha_2 \colon \mathbb{P}(r) \to [1, d]$, the sets $S_{\alpha_1,r}$ and $S_{\alpha_2,r}$ satisfy one of the two following properties:

- $S_{\alpha_1,r} \cap S_{\alpha_2,r} = \emptyset$ (this occurs when $c_{q,\alpha_1(q)} \not\equiv c_{q,\alpha_2(q)} \pmod q$ for some $q \in \mathbb{P}(r)$), or
- $S_{\alpha_1,r} = S_{\alpha_2,r}$ (this occurs when $c_{q,\alpha_1(q)} \equiv c_{q,\alpha_2(q)} \pmod q$, for every $q \in \mathbb{P}(r)$).

With this in mind, we note that the number of disjoint sets in $\{S_{\alpha,r} : \alpha \colon \mathbb{P}(r) \to [1, d]\}$ corresponds to the value of the multiplicative function $m(r)$. Then, by Claim 2, $(\frac{\#A}{r} - 1) \cdot m(r) \leq \#A_r \leq (\frac{\#A}{r} + 1) \cdot m(r)$. This implies that $\sigma(r) = \#A_r - \#A \cdot \frac{m(r)}{r}$ is such that $|\sigma(r)| \leq m(r)$, as required, and also shows that the *density* property holds.

Applying Lemma 1: The previous part of the proof shows that we can apply Lemma 1, from which we obtain $\#\Big(A \setminus \bigcup_{q\in Q} A_q\Big) \geq \frac{1}{2} \cdot \#A \cdot W_m(Q) - \mathfrak{g}(Q, d)$. Remember that $A = [k, k + z] \cap S_M$ and that $A \setminus \bigcup_{q\in Q} A_q$ corresponds to the set of solutions of $\mathcal{S}$ that belong to $[k, k + z]$. To conclude the proof it suffices to make $\frac{1}{2} \cdot \#A \cdot W_m(Q) - \mathfrak{g}(Q, d)$ greater or equal to 1 by opportunely selecting the value of the parameter z. We want $\#([k, k + z] \cap S_M) \geq 2 \cdot W_m(Q)^{-1}(1 + \mathfrak{g}(Q, d))$ which, from the fact that S_M is periodic in ΠM, holds as soon as $z \geq 2 \cdot W_m(Q)^{-1}(1 + \mathfrak{g}(Q, d)) \cdot \Pi M$.

The following claim on an upper bound for $W_m(Q)^{-1}$ is proven in Appendix B.

Claim 3. $W_m(Q)^{-1} \leq (d + 1)^{10d} \ln(\#Q + 1)^{3d}$.

Claim 3 and the definition of $\mathfrak{g}$ show that setting $z \coloneqq \big((d + 1) \cdot \#Q\big)^{4(d+1)^2(3+\ln\ln(\#Q+1))} \cdot \Pi M$ suffices to satisfy $z \geq 2 \cdot W_m(Q)^{-1}(1 + \mathfrak{g}(Q, d)) \cdot \Pi M$, concluding the proof. □

3 A novel strategy for Lipshitz's local-to-global property

In this section we establish Theorem 4, providing an asymptotical improvement over the local-to-global properties for systems of divisibility constraints discovered by Lipshitz [14] and later refined by Lechner et al. [12]. Most of the definitions and some intermediate lemmas required for this result were already formally presented in Section 1.3. To avoid repeating them, we refer the reader to that section, and consider here only concepts for which further details are required in order to give the proof of Theorem 4. On a high-level, recall that the main concepts discussed in Section 1.3 are:

- The notions of *divisibility module* and *r-increasing form*. In general, only systems of divisibility constraints in increasing form can be solved via the local-to-global property.
- The notions of *elimination property*, *S-polynomials* and *S-terms*. The first notion relies on *divisibility modules* to close a system under a finite representation of all its entailed divisibilities. The latter two terms are required to establish Theorem 4 inductively; we will use them to ensure that increasingness is not lost after fixing the value of a variable.
- The notion of *difficult primes* $\mathbf{P}_+(\Phi)$, that is primes p for which either the system of divisibility constraints Φ might not have a solution modulo p, or the solution always exists but still influences the minimal integer solution for Φ.

Except for Theorem 4, we defer all proofs of intermediate results to Appendices C and D.

Assumptions and further basic definitions. Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ be a system of divisibility constraints in d variables. Throughout the section, wlog. we tacitly assume the systems to be non-empty ($m \geq 1$) and *reduced*, that is such that the GCD of all coefficients and constants appearing in divisibilities $f \mid g$ is 1, i.e., $\gcd(\gcd(f), \gcd(g)) = 1$. Recall that we assume that $f_i \neq 0$ for all $1 \leq i \leq m$.

Given $\boldsymbol{b} \in \mathbb{Z}^i$ and a polynomial $f(x_1, \dots, x_d)$, we write $f(\boldsymbol{b}, x_{i+1}, \dots, x_d)$ for the polynomial in variables $(x_{i+1}, \dots, x_d)$ obtained from f by evaluating x_j as the j-th entry of $\boldsymbol{b}$, for all $j \in [1, i]$. Given $\boldsymbol{v} = (v_1, \dots, v_n) \in \mathbb{Z}^d$, $\|\boldsymbol{v}\| \coloneqq \max\{|v_i| : i \in [1, n]\}$ stands for the *(infinity) norm* of $\boldsymbol{v}$.

We define $\|S\| \coloneqq \max\{\|s\| : s \in S\}$, for every finite set S of objects having a defined notion of infinity norm. The norm $\|A\|$ of a matrix A is the norm of the set of its columns. Given a polynomial $f = \boldsymbol{a}^\intercal \boldsymbol{x} + c$, $\|f\| \coloneqq \max(\|\boldsymbol{a}\|, |c|)$. For a system of divisibility constraints Φ, $\|\Phi\| \coloneqq \|\text{terms}(\Phi)\|$.

We write $\langle a \rangle \coloneqq 1 + \lceil \log_2(|a| + 1) \rceil$ for the bit length of $a \in \mathbb{Z}$. The bit length of a set (or vector) S of n objects $s_1, \dots, s_n$ having a defined notion of bit length $\langle . \rangle$ is itself defined as $\langle S \rangle \coloneqq n + \sum_{i=1}^n \langle s_i \rangle$. We define $\langle f \rangle \coloneqq \langle \boldsymbol{a} \rangle + \langle c \rangle + 1$ and $\langle \Phi \rangle \coloneqq \langle \text{terms}(\Phi) \rangle$ for the bit length of a polynomial $f = \boldsymbol{a}^\intercal \boldsymbol{x} + c$ and of a system of divisibility constraints Φ, respectively. Note that $\langle \|S\| \rangle$ is simply the bit length of the infinity norm of S; where S is any object having a defined notion of infinity norm.

3.1 Bounds on divisibility modules, elimination property, S-terms, and $\mathbf{P}_+(\Phi)$

For the proof of Theorem 4 we need to refine some of the bounds given in Section 1.3. In that section we have briefly discussed the existence of an algorithm to close a system of divisibility constraints under the elimination property (Lemma 2). This algorithm relies on a procedure computing a span for the *divisibility module* $\mathrm{M}_f(\Phi)$ of a primitive polynomial f with respect to a system of divisibility constraints Φ. Recall that $\mathrm{M}_f(\Phi)$ is a vector subspace encoding all the divisibilities of the form $f \mid g$ implied by Φ. From the formal definition of divisibility module, it is simple to convince ourselves that a set spanning $\mathrm{M}_f(\Phi)$ can be found by taking f together with a subset of the right-hand sides of the divisibilities in Φ, possibly scaled. In Appendix C we show that computing such a span can be done in polynomial-time by a fix-point algorithm chaining computations of integer kernels.

Lemma 6. *There is a polynomial-time algorithm that, given a system $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and a primitive polynomial f, computes $c_1, \dots, c_m \in \mathbb{N}^m$ such that $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ spans $\mathrm{M}_f(\Phi)$ and $c_i \leq ((m+3) \cdot (\|\Phi\| + 2))^{(m+3)^3}$ for all $1 \leq i \leq m$.*

Regarding the computation of formulae with the elimination property, Lemma 2 is not precise enough for our purposes to establish Theorem 4. We restate it, tracking the growth of constants and coefficients, as well as structural properties of the output system of divisibility constraints.

Lemma 7. *There is a polynomial-time algorithm that, given a system of divisibility constraints $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and an order $x_1 \prec \dots \prec x_d$ for $\boldsymbol{x}$, computes $\Psi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^n f_i' \mid g_i'$ with the elimination property for $\prec$ that is equivalent to $\Phi(\boldsymbol{x})$, both over $\mathbb{Z}$ and modulo each $p \in \mathbb{P}$. The algorithm ensures that:*

1. *For any divisibility constraint $f \mid g$ such that f is not primitive, $f \mid g$ occurs in Φ if and only if $f \mid g$ occurs in Ψ. Moreover, for every $f_i' \mid g_i'$ in Ψ such that f_i' is primitive, there is some $f_j \mid g_j$ in Φ such that f_j' is the primitive part of f_j.*
2. *For every primitive polynomial f, $\mathrm{M}_f(\Phi) = \mathrm{M}_f(\Psi)$ (in particular, if Φ is increasing for some order $\prec'$ then so is Ψ, and vice versa).*
3. *$\|\Psi\| \leq (d+1)^{O(d)}(m + \|\Phi\| + 2)^{O(m^3 d)}$ and $n \leq m \cdot (d+2)$.*

Let us sketch this algorithm. For every primitive part f of a polynomial appearing in the left-hand side of a divisibility constraint in Φ, the algorithm first computes the set $S \coloneqq \{f,\, c_1 \cdot g_1,\, \dots,\, c_m \cdot g_m\}$ spanning $\mathrm{M}_f(\Phi)$, using the algorithm of Lemma 6. The set S can be represented as the matrix $A \in \mathbb{Z}^{(d+1)\times(m+1)}$ in which each column $(a_d, \dots, a_1, c)$ contains the coefficients and the constant of a distinct element of S, with a_i being the coefficient of x_i for $i \in [1, d]$, and c being the constant of the polynomial. The algorithm puts A in column-style Hermite normal form, obtaining linearly independent polynomials $h_1, \dots, h_\ell$ with different leading variables with respect to $\prec$. Because of how the coefficients and constants are arranged in A, we can obtain the system Ψ by simply replacing divisibility constraints of the form $f \mid g$ appearing in Φ with the divisibility constraints $f \mid h_1, \dots, f \mid h_\ell$. Items 1 and 2 are then easily seen to be satisfied, whereas Item 3 follows from the bound on $c_1, \dots, c_m$ given in Lemma 6 together with known bounds for putting an integer matrix in Hermite normal form [24]. Full details are given in Appendix C, together with the proof of the following lemma.

Lemma 8. *Let $\Phi(\boldsymbol{x}, \boldsymbol{y})$ and $\Psi(\boldsymbol{x}, \boldsymbol{y})$ be input and output of the algorithm in Lemma 7, respectively. For every $\boldsymbol{\nu} : \boldsymbol{x} \to \mathbb{Z}$ and primitive polynomial f, $\mathrm{M}_f(\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})) \subseteq \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$.*

This lemma, established by relying on the definition of divisibility module together with Items 1 and 2 of Lemma 7, is used in the proof of Theorem 4 to establish that if $\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ is in increasing form for some order, then so is $\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$.

To prove Theorem 4 we also need a bound on the number of S-terms of a system of divisibility constraints. We have already claimed in Section 1.3 that systems with the elimination property only have polynomially many S-terms. The precise bound, computed following the relevant definitions, is given in the following lemma (see Appendix D for the complete proof).

Lemma 9. *Let $\Phi \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ be a system of divisibility constraints in d variables with the elimination property for $\prec$. Then, (i) $\#\Delta(\Phi) \leq 2 \cdot m^2(d+2)$ and (ii) $\langle \|\Delta(\Phi)\| \rangle \leq (d+2) \cdot (\langle \|\Phi\| \rangle + 1)$.*

Lastly, let us restate the two lemmas from Section 1.3 analyzing properties of $\mathbf{P}_+(\Phi)$ and $\mathbb{P}(\Phi)$; they are proven in Appendix D and are fundamental to obtain the upper bound in the statement of Theorem 4. Recall that $\mathbb{P}(\Phi) \coloneqq \{p \in \mathbb{P} : p \leq m$ or p divides a coefficient or constant appearing in some $f_i\}$ is the set of primes p for which Φ may not have a solution modulo p. For primes that lie outside $\mathbb{P}(\Phi)$ we always have a small solution:

Lemma 3. *Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and $p \in \mathbb{P} \setminus \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{b} \in \mathbb{N}^d$ modulo p such that $v_p(f_i(\boldsymbol{b})) = 0$ for every $1 \leq i \leq m$, and $\|\boldsymbol{b}\| \leq p - 1$.*

Following the next lemma, the bit lengths of $\mathbb{P}(\Phi)$ and $\mathbf{P}_+(\Phi)$ are polynomially bounded:

Lemma 4. *Consider a system of divisibility constraints $\Phi(\boldsymbol{x})$ in d variables. Then, the set of primes $\mathbb{P}(\Phi)$ satisfies $\log_2(\Pi\mathbb{P}(\Phi)) \leq m^2(d+2) \cdot (\langle \|\Phi\| \rangle + 2)$. Furthermore, if Φ has the elimination property for an order $\prec$ on $\boldsymbol{x}$, then the set of primes $\mathbf{P}_+(\Phi)$ satisfies $\log_2(\Pi\mathbf{P}_+(\Phi)) \leq 64 \cdot m^5(d+2)^4(\langle \|\Phi\| \rangle + 2)$.*

3.2 Proof of Theorem 4: the local-to-global property

We are now ready to formalize the local-to-global property (Theorem 4). Simliar to Lipshitz' approach [14], the proof of this property is constructive and yields a procedure that given an r-increasing system of divisibility constraints Φ and solutions for Φ modulo p for every $p \in \mathbb{P}(\Phi)$, constructs an integer solution for Φ. Algorithm 1 provides the pseudocode of this procedure, which we mainly give as a way of summarizing the various steps of the proof of Theorem 4.

Algorithm 1 An algorithmic summary of the local-to-global property

Input: a system of divisibility constraints $\Phi(\boldsymbol{x})$ increasing for $X_1 \prec \cdots \prec X_r$,
and a solution $\boldsymbol{b}_p$ for Φ modulo p for every $p \in \mathbb{P}(\Phi)$.
Output: a solution $\boldsymbol{\nu}\colon \boldsymbol{x} \to \mathbb{Z}_+$ for Φ.

$\boldsymbol{\nu} \coloneqq \boldsymbol{\epsilon}$ ▷ *empty map*
let $\prec$ be an ordering in $(X_1 \prec \cdots \prec X_r)$
$(x_1, \dots, x_d) \coloneqq$ variables in X_1, in increasing order for $\prec$
if $r = 1$ **then** ▷ *base case*
  for $p \in \mathbb{P}(\Phi)$ **do** $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f(\boldsymbol{x}) \text{ left-hand side of a divisibility in } \Phi\}$
  for ℓ from 1 to d **do**
    for $p \in \mathbb{P}(\Phi)$ **do** $b_{p,\ell} \coloneqq$ value of $\boldsymbol{b}_p$ for the variable x_ℓ
    insert $(x_\ell \mapsto a)$ in $\boldsymbol{\nu}$ **where** $a \in \mathbb{Z}_+$ is a solution for the system ▷ *CRT*
$$\begin{cases} x_\ell \equiv b_{p,\ell} \pmod{p^{\mu_p+1}} & p \in \mathbb{P}(\Phi) \end{cases}$$
  return $\boldsymbol{\nu}$
else ▷ $r \geq 2$, *recursive case*
  $\Psi \leftarrow$ closure of Φ for the elimination property for the order $\prec$ ▷ *Lemma 7*
  for $p \in \mathbf{P}_+(\Psi) \setminus \mathbb{P}(\Phi)$ **do**
    $\boldsymbol{b}_p \coloneqq$ solution for Φ modulo p satisfying $v_p(f(\boldsymbol{b}_p)) = 0$ for every
      $f(\boldsymbol{x})$ in the left-hand side of a divisibility in Φ ▷ *Lemma 3*
  for $p \in \mathbf{P}_+(\Psi)$ **do** $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f(\boldsymbol{x}) \text{ left-hand side of a divisibility in } \Psi\}$
  $Q \coloneqq \emptyset$
  for ℓ from 1 to d **do**
    for $p \in \mathbf{P}_+(\Psi)$ **do** $b_{p,\ell} \coloneqq$ value of $\boldsymbol{b}_p$ for the variable x_ℓ
    insert $(x_\ell \mapsto a)$ in $\boldsymbol{\nu}$ **where** $a \in \mathbb{Z}_+$ is a solution for the system ▷ *Theorem 3*
$$\begin{cases} x_\ell \equiv b_{p,\ell} \pmod{p^{\mu_p+1}} & p \in \mathbf{P}_+(\Psi) \\ g(\boldsymbol{\nu}(\boldsymbol{y}), x_\ell) \not\equiv 0 \pmod{q} & q \in Q \setminus \mathbf{P}_+(\Psi),\ g(\boldsymbol{y}, x_\ell) \in S(\Delta(\Psi)) \text{ with } \mathrm{LV}_\prec(g) = x_\ell \end{cases}$$
    $Q \leftarrow Q \cup \{p \in \mathbb{P} : \text{there is } h(\boldsymbol{y}) \in S(\Delta(\Psi)) \text{ such that } \mathrm{LV}_\prec(h) = x_\ell \text{ and } p \mid h(\boldsymbol{\nu}(\boldsymbol{y}))\}$
  $\Phi' \coloneqq \Phi[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$
  for $p \in \mathbb{P}(\Phi')$ **do** $\boldsymbol{b}'_p \coloneqq$ solution for Φ' modulo p ▷ *Claim 7*
  $\boldsymbol{\xi} \coloneqq$ result of calling Algorithm 1 on Φ', $X_2 \prec \cdots \prec X_r$ and $\{\boldsymbol{b}'_p : p \in \mathbb{P}(\Phi')\}$
  return $\boldsymbol{\nu} \sqcup \boldsymbol{\xi}$ ▷ *union of disjoint functions*

Theorem 4. *Let $\Phi(\boldsymbol{x})$ be an r-increasing system of divisibility constraints such that Φ has a solution $\boldsymbol{b}_p \in \mathbb{Z}^d$ modulo p for every prime $p \in \mathbb{P}(\Phi)$. Then Φ has infinitely many solutions, and a solution $\boldsymbol{a} \in \mathbb{N}^d$ such that $\langle\|\boldsymbol{a}\|\rangle \leq (\langle\Phi\rangle + \max\{\langle\|\boldsymbol{b}_p\|\rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$.*

Proof. Throughout the proof, fix and order $(\prec) \in (X_1 \prec \cdots \prec X_r)$. For simplicity, we focus on the part of the statement that builds a solution over $\mathbb{N}$ (in fact, we will build a solution over $\mathbb{Z}_+$). The fact that there are infinitely many solutions follows from the fact that the solution is built by solely relying on systems of (non-)congruences over the integers.

Let us first expand on the overview of the proof given in Section 1.3 by referring to the pseudocode in Algorithm 1. The goal is to compute a map $\boldsymbol{\nu}\colon \left(\bigcup_{j=1}^{r} X_j\right) \to \mathbb{Z}_+$ such that $\boldsymbol{\nu}(\boldsymbol{x})$ is a solution for Φ. The proof proceeds by induction on r, populating the map $\boldsymbol{\nu}$ according the order $\prec$.

When $r = 1$ (line 4 in Algorithm 1) $\boldsymbol{\nu}$ can be computed using the (standard) Chinese remainder theorem, with little to no problem (line 8). The main ingredient here is given by the natural number $\mu_p := \max\left\{v_p(f(\boldsymbol{b}_p)) : f(\boldsymbol{x}) \text{ left-hand side of a divisibility in } \Phi\right\}$ (line 5), that given $p \in \mathbb{P}(\Phi)$ tells us up to what power of p should the integer solution given by $\boldsymbol{\nu}$ agree with the solution $\boldsymbol{b}_p$.

When $r \geq 2$, the goal is to define $\boldsymbol{\nu}$ for the variables in X_1 in such a way that the formula $\Phi' := \Phi[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$ is increasing for $X_2 \prec \dots \prec X_r$, and has solutions modulo p for every $p \in \mathbb{P}(\Phi')$. This allows us to call for Theorem 4 inductively (line 25), obtaining a solution $\boldsymbol{\xi} \colon \left(\bigcup_{j=2}^{r} X_j\right) \to \mathbb{Z}_+$ for Φ'. An integer solution for Φ is then given by the union $\boldsymbol{\nu} \sqcup \boldsymbol{\xi}$ of $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$, i.e., the map defined as $\boldsymbol{\nu}(x)$ for $x \in X_1$ and as $\boldsymbol{\xi}(y)$ for $y \in \bigcup_{j=2}^{r} X_j$, (line 26). To construct $\boldsymbol{\nu}$ for X_1, we first close Φ under the elimination property following Lemma 7 (line 12), and extend the solutions $\boldsymbol{b}_p$ to every $p \in \mathbf{P}_+(\Psi)$ thanks to Lemma 3 (line 13). We then populate $\boldsymbol{\nu}$ following the order $\prec$, starting from the smallest variable (line 18). In the proof, this is done with a second induction. Values for the variables in X_1 are found using Theorem 3 (line 20). When a new value $a \in \mathbb{Z}_+$ for a variable $x \in X_1$ is found, new primes need to be taken into account (line 22), since substituting a for x yields a complete evaluation of the polynomials in $S(\Delta(\Phi))$ with leading variable x, and the resulting integers might be divisible by primes not belonging to $\mathbf{P}_+(\Psi)$. For subsequent variables in X_1, we make sure to pick values that keep the evaluated polynomials as "coprime as possible" with respect to these new primes (see the induction hypothesis (IH2) below, as well as the system of (non-)congruences in line 20). This condition is necessary to obtain the new solutions $\boldsymbol{b}_p$ for the formula Φ', modulo every $p \in \mathbb{P}(\Phi')$ (line 24).

We now formalize the proof. To ease the presentation, we postpone the analysis on the bound of the minimal positive solution to after the main induction showing the existence of such a solution. In a nutshell, the bound fundamentally comes from repeated applications of Theorem 3.

Base case $r = 1$: As Φ is 1-increasing, it is of the form $\bigwedge_{i=1}^{\ell} c_i \mid g_i(\boldsymbol{x}) \land \bigwedge_{j=\ell+1}^{m} f_j(\boldsymbol{x}) \mid a_j \cdot f_j(\boldsymbol{x})$, where every c_i and a_j are in $\mathbb{Z}$. By hypothesis, every c_i and f_j is non-zero. If $c_i = 1$ for every $i \in [1, \ell]$, then $\boldsymbol{x} = \boldsymbol{0}$ is trivially a solution. Otherwise, $\mathbb{P}(\Phi)$ is non-empty. Let $\boldsymbol{x} = (x_1, \dots, x_d)$ and, given $p \in \mathbb{P}(\Phi)$, let $\mu_p := \max\{v_p(f(\boldsymbol{b}_p)) : f \text{ is in the left-hand side of a divisibility of } \Phi\}$. Note that since $\boldsymbol{b}_p$ is a solution for Φ modulo p, we have $f_j(\boldsymbol{b}_p) \neq 0$ for every $j \in [\ell+1, m]$, and thus $v_p(f(\boldsymbol{b}_p)) \in \mathbb{N}$. Denote with $b_{p,k}$ the value of $\boldsymbol{b}_p$ for the variable x_k, with $p \in \mathbb{P}(\Phi)$ and $k \in [1, d]$. Consider the system of congruences

$$x_k \equiv b_{p,k} \pmod{p^{\mu_p+1}} \qquad\qquad p \in \mathbb{P}(\Phi),\ 1 \leq k \leq d. \tag{4}$$

According to the Chinese remainder theorem, this system has a positive solution $\boldsymbol{a} = (a_1, \dots, a_d)$. To conclude the base case, it suffices to show that $f_j(\boldsymbol{a}) \neq 0$ for every $j \in [\ell + 1, m]$, and that $c_i \mid g_i(\boldsymbol{a})$ for every $i \in [1, \ell]$. First, consider $j \in [\ell + 1, m]$ and pick a prime $p \in \mathbb{P}(\Phi)$. From the system of congruences in Equation (4) we have $f_j(\boldsymbol{a}) \equiv f_j(\boldsymbol{b}_p) \pmod{p^{\mu_p+1}}$, and by definition of μ_p, $f_j(\boldsymbol{b}_p) \not\equiv 0 \pmod{p^{\mu_p+1}}$. We conclude that $f_j(\boldsymbol{a}) \not\equiv 0 \pmod{p^{\mu_p+1}}$, and so $f_j(\boldsymbol{a}) \neq 0$.

Consider now $i \in [1, \ell]$. To prove that $c_i \mid g_i(\boldsymbol{a})$, concluding the base case, we show that for every prime p dividing c_i, $v_p(c_i) \leq v_p(g_i(\boldsymbol{a}))$. By definition, any such prime p satisfies $p \in \mathbb{P}(\Phi)$ and moreover $v_p(c_i) \leq \mu_p$. We distinguish two cases:

- if $v_p(g_i(\boldsymbol{b}_p)) \leq \mu_p$, then according to Equation (4) we have $v_p(g_i(\boldsymbol{b}_p)) = v_p(g_i(\boldsymbol{a}))$. Since $\boldsymbol{b}_p$ is a solution for Φ modulo p, this implies $v_p(c_i) \leq v_p(g_i(\boldsymbol{a}))$.
- If $v_p(g_i(\boldsymbol{b}_p)) > \mu_p$, then $g_i(\boldsymbol{b}_p) \equiv 0 \pmod{p^{\mu_p+1}}$ and so $g_i(\boldsymbol{a}) \equiv 0 \pmod{p^{\mu_p+1}}$ by Equation (4). Therefore $v_p(g_i(\boldsymbol{a})) > \mu_p$ and by definition of μ_p we get $v_p(c_i) \leq v_p(g_i(\boldsymbol{a}))$.

Induction step $r \geq 2$: by induction hypothesis, we assume the theorem to be true for every s-increasing system with $s < r$. By Lemma 3, for every prime $p \in \mathbb{P} \setminus \mathbb{P}(\Phi)$ there is a solution $\boldsymbol{b}_p$ for Φ modulo p such that $\max\{v_p(f(\boldsymbol{b}_p)) : f$ in the left-hand side of a divisibility of $\Phi\} = 0$. Together with the solutions $\boldsymbol{b}_p$ for primes $p \in \mathbb{P}(\Phi)$, this means that Φ has solutions modulo every prime. We apply Lemma 7 in order to obtain from Φ a system Ψ with the elimination property for $\prec$. The system Ψ is used to produce the map $\boldsymbol{\nu}$ for the variables in X_1. Adding the elimination property does not change the set of solutions (neither over the integers nor modulo a prime), and therefore the above solutions $\boldsymbol{b}_p$ are still solutions for Ψ modulo p. Below, among these solutions we only consider the ones for primes $p \in \mathbf{P}_+(\Psi)$. Given such a prime $p \in \mathbf{P}_+(\Psi)$, define $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f$ is in the left-hand side of a divisibility of $\Psi\}$. As already observed in the base case, given f left-hand side of a divisibility in Ψ, $f(\boldsymbol{b}_p) \neq 0$ and so $v_p(f(\boldsymbol{b}_p)) \in \mathbb{N}$. Moreover, from Item 1 in Lemma 7 we conclude that $\mu_p = 0$ for every $p \in \mathbf{P}_+(\Psi) \setminus \mathbb{P}(\Phi)$.

As Ψ is r-increasing (see Item 1 in Lemma 7), it is of the form

$$\left(\bigwedge_{i=1}^{\ell} c_i \mid g_i(\boldsymbol{x})\right) \wedge \left(\bigwedge_{i=\ell+1}^{n} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x}) + g_i'(\boldsymbol{y})\right) \wedge \left(\bigwedge_{i=n+1}^{t} f_i(\boldsymbol{x}) + f_i'(\boldsymbol{y}) \mid g_i(\boldsymbol{x}) + g_i'(\boldsymbol{y})\right), \qquad (5)$$

where $\boldsymbol{x}$ are the variables appearing in X_1, $\boldsymbol{y}$ are the variables appearing in $\bigcup_{j=2}^{r} X_j$, $\ell \leq n \leq t$, and for every $i \in [n+1, t]$, $f_i'(\boldsymbol{y})$ and $g_i'(\boldsymbol{y})$ have 0 as a constant and are non-constant. Moreover, since Ψ is increasing, for every $i \in [\ell+1, n]$ $g_i(\boldsymbol{x})$ and $g_i'(\boldsymbol{y})$ are such that either $g_i' = 0$ and $g_i = a \cdot f_i$ for some $a \in \mathbb{Z}$, or g_i' is non-constant and has 0 as a constant. Let $X_1 = \{x_1, \dots, x_d\}$, with $x_1 \prec \dots \prec x_d$. Denote by $b_{p,k}$ the value of $\boldsymbol{b}_p$ for the variable x_k, with $p \in \mathbf{P}_+(\Psi)$ and $k \in [1, d]$. We build the map $\boldsymbol{\nu}$ defined on the variables in X_1, inductively starting from x_1. In the induction step, when searching for a value to the variable x_{k+1}, the following induction hypotheses hold:

IH1: For every $p \in \mathbf{P}_+(\Psi)$ and $j \in [1, k]$, $\boldsymbol{\nu}(x_j) \equiv b_{p,j} \pmod{p^{\mu_p+1}}$,

IH2: For every prime $p \notin \mathbf{P}_+(\Psi)$, for every $h, h' \in \Delta(\Psi)$ with leading variable at most x_k, if $S(h, h')$ is not identically zero, then p does not divide both $h(\boldsymbol{\nu}(x_1, \dots, x_k))$ and $h'(\boldsymbol{\nu}(x_1, \dots, x_k))$.

IH3: $h(\boldsymbol{\nu}(x_1, \dots, x_k)) \neq 0$ for every $h \in \Delta(\Psi)$ that is non-zero and with $\mathrm{LV}(h) \preceq x_k$.

base case $k = 0$. In this case, (IH1) and (IH3) trivially hold (for (IH3) note that h is constant). In (IH2) we only consider constant polynomials h, h', hence $S(h, h') = 0$ by definition.

induction step. Let us assume that $\boldsymbol{\nu}$ is defined for the variables $x_1, \dots, x_k$ with $k \in [0, d-1]$, so that the induction hypotheses hold. Let us provide a value for x_{k+1} so that $\boldsymbol{\nu}$ still fulfils the induction hypotheses. We define the following set of primes:

$$P_k \coloneqq \{p \in \mathbb{P} : p \in \mathbf{P}_+(\Psi) \text{ or } p \mid h(\boldsymbol{\nu}(x_1, \dots, x_k)) \text{ for } h \in S(\Delta(\Psi)) \setminus \{0\} \text{ with } \mathrm{LV}(h) \preceq x_k\}.$$

In the hypothesis that $P_k = \mathbf{P}_+(\Psi)$, we add to P_k the smallest prime not in $\mathbf{P}_+(\Psi)$. Hence, below, assume $P_k \neq \mathbf{P}_+(\Psi)$. We consider the following system of (non-)congruences:

$$\begin{aligned}
x_{k+1} &\equiv b_{p,k+1} && \pmod{p^{\mu_p+1}} && p \in \mathbf{P}_+(\Psi)\\
h(\boldsymbol{\nu}(x_1, \dots, x_k),\, x_{k+1}) &\not\equiv 0 && \pmod{q} && q \in P_k \setminus \mathbf{P}_+(\Psi) \text{ and}\\
&&&&& h \in S(\Delta(\Psi)) \text{ s.t. } \mathrm{LV}(h) = x_{k+1}.
\end{aligned}$$

With respect to the h above, let us write $h(\boldsymbol{\nu}(x_1, \dots, x_k), x_{k+1}) = c_h + a_h \cdot x_{k+1}$, where c_h is the constant term obtained by partially evaluating h with respect to $\boldsymbol{\nu}(x_1, \dots, x_k)$, and a_h is the coefficient of x_{k+1} in h. Since $q \in P_k \setminus \mathbf{P}_+(\Psi)$, then $q \nmid a_h$ from Condition (P2). Then a_h has an inverse a_h^{-1} modulo q, and the system of (non-)congruences above is equivalent to

$$\begin{aligned} &x_{k+1} \equiv b_{p,k+1} && \pmod{p^{\mu_p+1}} && p \in \mathbf{P}_+(\Psi) \\ &x_{k+1} \not\equiv -a_h^{-1} c_h && \pmod{q} && q \in P_k \setminus \mathbf{P}_+(\Psi) \text{ and } h \in S(\Delta(\Psi)) \text{ s.t. } \mathrm{LV}(h) = x_{k+1}. \end{aligned} \tag{6}$$

In this system of (non-)congruences, elements in $\mathbf{P}_+(\Psi)$ and $P_k \setminus \mathbf{P}_+(\Psi)$ are pairwise coprime, $P_k \setminus \mathbf{P}_+(\Psi)$ is a set of primes, and moreover $\min(P_k \setminus \mathbf{P}_+(\Psi)) > \# S(\Delta(\Psi))$ by Condition (P1). Hence, we can apply Theorem 3 and conclude that Equation (6) has a solution $w \in \mathbb{Z}_+$. Let us update $\boldsymbol{\nu}$ so that $\boldsymbol{\nu}(x_{k+1}) = w$. We show that $\boldsymbol{\nu}$ satisfies the induction hypotheses.

1. By the congruences in Equation (6), $\boldsymbol{\nu}(x_{k+1}) \equiv b_{p,k+1} \pmod{p^{\mu_p+1}}$, hence (IH1) holds.
2. Consider $h, h' \in \Delta(\Psi)$ such that $\mathrm{LV}(h) \preceq \mathrm{LV}(h') = x_{k+1}$ and $S(h, h')$ is not identically zero. Note that the case where $\mathrm{LV}(h') \preceq \mathrm{LV}(h) = x_{k+1}$ is analogous, whereas if both $\mathrm{LV}(h)$ and $\mathrm{LV}(h')$ are at most x_k then (IH2) already holds by induction hypothesis. We divide the proof into two cases, depending on $\mathrm{LV}(h)$.
   - if $\mathrm{LV}(h) \prec x_{k+1}$, consider $p \notin \mathbf{P}_+(\Psi)$ such that $p \mid h(\boldsymbol{\nu}(x_1, \dots, x_k))$. By definition, $p \in P_k$, and thus from the non-congruences in Equation (6), $p \nmid h(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$.
   - if $\mathrm{LV}(h) = \mathrm{LV}(h') = x_{k+1}$, assume *ad absurdum* that there is $p \notin \mathbf{P}_+(\Psi)$ such that $p \mid h(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$ and $p \mid h'(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$. Then, $p \mid S(h, h')$ by definition of S. However, $S(h, h') \in S(\Delta(\Psi)) \setminus \{0\}$ and $\mathrm{LV}(S(h, h')) \preceq x_k$, from which we conclude that $p \in P_k$. Again from the non-congruences in Equation (6), this implies $p \nmid h(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$ and $p \nmid h'(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$, a contradiction.

   In both cases, we conclude that (IH2) holds.
3. Let $h \in \Delta(\Psi)$ with $\mathrm{LV}(h) = x_{k+1}$ (else (IH3) directly holds by induction hypothesis). As there is a prime $p \in P_k \setminus \mathbf{P}_+(\Psi)$, from the non-congruences of Equation (6) we conclude $p \nmid h(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$, and thus $h(\boldsymbol{\nu}(x_1, \dots, x_{k+1}))$ cannot be 0. Hence, (IH3) holds.

The innermost induction we have just completed yields a map $\boldsymbol{\nu}$ defined for the variables in X_1 and satisfying (IH1)–(IH3) for every $k \in [1, d]$. Consider the system $\Psi'(\boldsymbol{y}) \coloneqq \Psi[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$ obtained from Ψ by evaluating as $\boldsymbol{\nu}(x)$ every variable x in X_1. With reference to Equation (5), we note that the subsystem $\bigwedge_{i=1}^{\ell} c_i \mid g_i(\boldsymbol{\nu}(\boldsymbol{x}))$ evaluates to true (proof as in the base case $r = 1$ of the induction and by using (IH1)). Then, $\Psi'(\boldsymbol{y})$ is of the form

$$\left(\bigwedge_{i=\ell+1}^{n} \alpha_i \mid \beta_i + g_i'(\boldsymbol{y}) \right) \land \left(\bigwedge_{i=n+1}^{t} \alpha_i + f_i'(\boldsymbol{y}) \mid \beta_i + g_i'(\boldsymbol{y}) \right), \tag{7}$$

where $\alpha_i = f_i(\boldsymbol{\nu}(\boldsymbol{x})) \in \mathbb{Z}$ and $\beta_i = g_i(\boldsymbol{\nu}(\boldsymbol{x})) \in \mathbb{Z}$, for every $i \in [\ell+1, t]$. Note that $\alpha_i \neq 0$ for every $i \in [\ell+1, n]$, thanks to (IH3), so $\boldsymbol{\nu}$ satisfies all trivial divisibilities of the form $f(\boldsymbol{x}) \mid a \cdot f(\boldsymbol{x})$.

The next step is to show that Ψ' is increasing for $(X_2 \prec \dots \prec X_r)$ and to provide solutions modulo p for every $p \in \mathbf{P}_+(\Psi')$. These two properties, formalized below in Claim 4 and Claim 5, follow from the induction hypotheses (IH1)–(IH3) we kept during the construction of $\boldsymbol{\nu}$, together with the fact that the system Ψ has the elimination property. Their proofs are very technical and lengthy, and we therefore defer them to Appendix E. Observe that the condition (P3) of the difficult primes is required to establish Claim 5, but otherwise does not appear anywhere else in this proof.

Claim 4. *The system Ψ' is increasing for $(X_2 \prec \dots \prec X_r)$.*

Claim 5. *For every $p \in \mathbf{P}_+(\Psi)$, the solution $\boldsymbol{b}_p$ for Ψ modulo p is, when restricted to $\boldsymbol{y}$, a solution for $\Psi'(\boldsymbol{y})$ modulo p. For every prime $p \notin \mathbf{P}_+(\Psi)$, there is a solution $\boldsymbol{b}_p$ for Ψ' modulo p such that (i) every entry of $\boldsymbol{b}_p$ belongs to $[0, p^{u+1} - 1]$, where $u \coloneqq \max\{v_p(\alpha_i) : i \in [\ell+1, n]\}$, and (ii) for every $g \in \operatorname{terms}(\Psi')$, $v_p(g(\boldsymbol{b}_p))$ is either 0 or u.*

Thanks to Claim 4 and Claim 5, we can inductively apply the statement of Theorem 4 on Ψ' in order to obtain an integer solution for Ψ, and thus a solution for the original system Φ. While this would prove the local-to-global property, it is not enough to obtain the upper bound on the size of the minimal positive solution stated in Theorem 4. Instead, we wish to apply the induction hypothesis on the system $\Phi'(\boldsymbol{y}) \coloneqq \Phi[\boldsymbol{\nu}(\boldsymbol{x}) \,/\, x : x \in X_1]$, hence disregarding the work done to close Φ under the elimination property. The main point in favour of this strategy is that the subsequent applications of Lemma 7, required to inductively construct the integer solutions for the remaining variables $\boldsymbol{y}$, yield smaller systems of divisibility constraints (for instance, note that Φ' has at most m divisibilities, whereas Ψ' can have close to $m \cdot (d+2)$ divisibilities).

To prove that we can apply the induction hypothesis on Φ', we need to show that this system satisfies properties analogous to the ones in Claim 4 and Claim 5. While the proofs of these claims require the elimination property to be established, we can transfer them to Φ' thanks to the fact that Ψ is defined from Φ following the algorithm of Lemma 7.

Claim 6. *The system Φ' is increasing for $(X_2 \prec \cdots \prec X_r)$.*

Proof. *Ad absurdum*, assume that $\Phi'(\boldsymbol{y})$ is not increasing for some order $(\prec') \in (X_2 \prec \cdots \prec X_r)$. Let $\boldsymbol{y} = (y_1, \ldots, y_j)$ with $y_1 \prec' \cdots \prec' y_j$. There is $i \in [1, j]$ and a primitive term f with $\operatorname{LV}(f) = y_i$ such that $\mathbb{Z}f \subsetneq \operatorname{M}_f(\Phi') \cap \mathbb{Z}[y_1, \ldots, y_i]$. By Lemma 8 we get $\mathbb{Z}f \subsetneq \operatorname{M}_f(\Psi') \cap \mathbb{Z}[y_1, \ldots, y_i]$. However, this implies that Ψ' is not increasing for $\prec'$, contradicting Claim 4. $\square$

Claim 7. *For every $p \in \mathbb{P}$, the solution $\boldsymbol{b}_p$ for Ψ' modulo p ensured in Claim 5 is also a solution for Φ' modulo p. If $p \notin \mathbf{P}_+(\Psi)$, then for every polynomial f' appearing in the left-hand side of a divisibility of Φ', we have either $v_p(f'(\boldsymbol{b}_p)) = 0$ or $v_p(f'(\boldsymbol{b}_p)) = \max\{v_p(\alpha_i) : i \in [\ell+1, n]\}$.*

Proof. For the first statement of the claim, consider a solution $\boldsymbol{b}_p$ for $\Psi'(\boldsymbol{y})$ modulo p (such as the one ensured by Claim 5). From the definition of Ψ', the tuple $(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{b}_p)$ is a solution for $\Psi(\boldsymbol{x}, \boldsymbol{y})$ modulo p. Then, by Lemma 7, $(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{b}_p)$ is a solution for $\Phi(\boldsymbol{x}, \boldsymbol{y})$ modulo p; and so by definition of Φ', $\boldsymbol{b}_p$ is a solution for $\Phi'(\boldsymbol{y})$ modulo p.

The second statement of this claim follows from Claim 5 together with the property (1) of Lemma 7, and by definitions of Ψ' and Φ'. In particular, for every polynomial $f'(\boldsymbol{y})$ occurring in a left-hand side of a divisibility of Φ', there is a polynomial $f(\boldsymbol{x}, \boldsymbol{y})$ occurring in a left-hand side of Φ such that $f'(\boldsymbol{y}) = f(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. From (1) of Lemma 7, f occurs in a left-hand side of Ψ and thus f' occurs in a left-hand side of Ψ'. The statement then follows by Claim 5. $\square$

From Claim 6 and Claim 7, and by induction hypothesis, there is a map $\boldsymbol{\xi} \colon \left(\bigcup_{j=2}^{r} X_j\right) \to \mathbb{Z}_+$ such that $\boldsymbol{\xi}(\boldsymbol{y})$ is a solution for Φ'. Note that in constructing $\boldsymbol{\xi}$ we can rely on the order $\prec$ restricted to $\bigcup_{j=2}^{r} X_j$; since Φ' is increasing for that order. Then, by definition of Φ', a positive integer solution for Φ is given by the union $\boldsymbol{\nu} \sqcup \boldsymbol{\xi}$ of $\boldsymbol{\nu}$ and $\boldsymbol{\xi}$. This concludes the proof of existence of a solution. We now study its bit length.

In what follows, let $\underline{O} \in \mathbb{Z}_+$ be the minimal positive integer greater or equal than 4 such that the map $x \mapsto \underline{O}(x+1)$ upper bounds the linear functions hidden in the $O(.)$ appearing in Lemma 7. We write $\Gamma(r, \ell, w, m, d)$, with $r, \ell, w, m, d \in \mathbb{Z}_+$ and $r \leq d$, for the maximum bit length of the minimal positive solution of any system of divisibility constraints Φ such that:

- Φ is r-increasing.

- The maximum bit length of a coefficient or constant appearing in Φ, i.e., $\langle\|\Phi\|\rangle$, is at most ℓ.
- For every $p \in \mathbb{P}(\Phi)$, consider a solution $\boldsymbol{b}_p$ of Φ modulo p minimizing $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f$ is in the left-hand side of a divisibility in $\Phi\}$. Then, $\log_2\left(\prod_{p\in\mathbb{P}(\Phi)} p^{\mu_p+1}\right) \leq w$.
- Φ has at most m divisibilities.
- Φ has at most d variables.

The constraint $r \leq d$ is without loss of generality, as every increasing formula is d-increasing.

Since we want to find an upper bound for Γ, assume without loss of generality that $\Gamma(r, \ell, w, m, d)$ is always at least $\min(\ell, w)$. In Appendix F we study the growth of Γ and prove the following claim.

Claim 8.
$$\begin{cases} \Gamma(1, \ell, w, m, d) \leq w + 3 \\ \Gamma(r+1, \ell, w, m, d) \leq \Gamma(r, \\ \qquad 2^{105} m^{27} (d+2)^{38} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w) \cdot (\log_2(\ell + w))^6, \\ \qquad 2^{109} m^{29} (d+2)^{39} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w) \cdot (\log_2(\ell + w))^6, \\ \qquad m, \\ \qquad d). \end{cases}$$

Let us show that the recurrence system above yields the bound in the statement of the theorem. Remark that Γ is monotonous by definition. By induction on $k \in [0, r-1]$ we show that

$$\Gamma(r, \ell, w, m, d) \leq \Gamma(r-k, \delta_k, \delta_k, m, d) \text{ where } \delta_k \coloneqq \frac{1}{2} \cdot (2^{110} m^{29} (d+2)^{39} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w))^{2(k+1)}.$$

base case $k = 0$**.** Directly follows from $\delta_0 \geq \max(\ell, w)$ and the fact that Γ is monotonous.

induction case $k \geq 1$**.** Let us define $C \coloneqq 2^{110} m^{29} (d+2)^{39} \underline{O} \cdot \log_2(\underline{O})^6$. By induction hypothesis, $\Gamma(r, \ell, w, m, d) \leq \Gamma(r-(k-1), \delta_{k-1}, \delta_{k-1}, m, d)$. By Claim 8 and the monotonicity of Γ:

$$\begin{aligned} & \Gamma(r-(k-1), \delta_{k-1}, \delta_{k-1}, m, d) \\ \leq & \Gamma(r-k,\ \frac{C}{2} \cdot (2 \cdot \delta_{k-1}) \cdot (\log_2(2 \cdot \delta_{k-1}))^6,\ \frac{C}{2} \cdot (2 \cdot \delta_{k-1}) \cdot (\log_2(2 \cdot \delta_{k-1}))^6,\ m,\ d) \\ \leq & \Gamma(r-k,\ \delta_k,\ \delta_k\ m,\ d), \end{aligned}$$

as indeed

$$\begin{aligned} & \frac{C}{2} \cdot (2 \cdot \delta_{k-1}) \cdot (\log_2(2 \cdot \delta_{k-1}))^6 \\ \leq & \frac{C}{2} \cdot \big(C \cdot (\ell + w)\big)^{2k} \big(\log_2((C \cdot (\ell + w))^{2k})\big)^6 \\ \leq & \frac{C}{2} \cdot \big(C \cdot (\ell + w)\big)^{2k} (2 \cdot k)^6 \log_2(C \cdot (\ell + w))^6 \\ \leq & \frac{C}{2} \cdot \big(C \cdot (\ell + w)\big)^{2k} \cdot \sqrt{C} \cdot \log_2(C \cdot (\ell + w))^6 && \text{from } k < r \leq d \text{ and } (2 \cdot d)^6 \leq \sqrt{C} \\ \leq & \frac{C}{2} \cdot \big(C \cdot (\ell + w)\big)^{2k} \cdot \sqrt{C} \cdot \sqrt{C \cdot (\ell + w)} && \text{from } \log_2(x)^6 \leq \sqrt{x} \text{ for } x \geq 2^{75} \\ \leq & \frac{1}{2} \cdot \big(C \cdot (\ell + w)\big)^{2(k+1)} = \delta_k. \end{aligned}$$

The inequality we just showed, together with the base case of the recurrence system, entails

$$\Gamma(r, \ell, w, m, d) \leq (2^{110} m^{29} (d+2)^{39} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w))^{2 \cdot r}. \tag{8}$$

Take now the formula Φ in the statement of the theorem. This formula belongs to $\Gamma(r, \ell, w, m, d)$ where $\ell \coloneqq \langle \|\Phi\| \rangle$ and $w \coloneqq \log_2 \left(\prod_{p \in \mathbb{P}(\Phi)} p^{\mu_p + 1} \right)$. We have

$$\begin{aligned}
w &\leq \max\{1 + v_p(f(\boldsymbol{b}_p)) : f \text{ is in a left-hand side of } \Phi,\, p \in \mathbb{P}(\Phi)\} \cdot \log_2 \Big(\prod_{p \in \mathbb{P}(\Phi)} p \Big) \\
&\leq \max\{\langle f(\boldsymbol{b}_p) \rangle : f \text{ is in a left-hand side of } \Phi,\, p \in \mathbb{P}(\Phi)\} \cdot \log_2 \Big(\prod_{p \in \mathbb{P}(\Phi)} p \Big) \\
&\leq (\max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\} + \langle \|\Phi\| \rangle + d + 1) \cdot \log_2 \Big(\prod_{p \in \mathbb{P}(\Phi)} p \Big) \\
&\leq (\max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\} + \langle \|\Phi\| \rangle + d + 1) \cdot m^2 (d+2) \cdot (\langle \|\Phi\| \rangle + 2) && \text{Lemma 4} \\
&\leq (\max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\} + 1) \cdot m^2 (d+2)^2 (\langle \|\Phi\| \rangle + 2)^2.
\end{aligned}$$

Then, following Equation (8), the minimal positive solution of Φ is bounded by

$$\left(2^{111} \underline{O} \cdot \log_2(\underline{O})^6 m^{31} (d+2)^{41} (\langle \|\Phi\| \rangle + 2)^2 (\max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\} + 2)\right)^{2r},$$

which is in $(\langle \Phi \rangle + \max\{\langle \|\boldsymbol{b}_p\| \rangle : p \in \mathbb{P}(\Phi)\})^{O(r)}$. ☐

Remark 1. *Let us briefly discuss how the infinitely many solutions of Φ ensured by Theorem 4 look like. Since solutions are constructed by solving the systems of (non-)congruences in Equations* (4) *and* (6) *(see Algorithm 1 for a summary), Theorem 3 ensures that Φ has infinitely many solutions. More precisely, the following property holds: let $(\prec) \in (X_1 \prec \cdots \prec X_r)$, $x \in \bigcup_{j=1}^r X_j$, and $\boldsymbol{\nu} \colon \bigcup_{j=1}^r X_j \to \mathbb{Z}$ be the solution of Φ computed by Algorithm 1. The system $\Phi[\boldsymbol{\nu}(y) \,/\, y : y \prec x]$ has a solution for infinitely many positive and negative values of x.*

3.3 Deciding systems of divisibility constraints in increasing form in NP

Theorem 4 provides a way of constructing integer solutions of bit length exponential in r for r-increasing systems of divisibility constraints. A different approach not relying on constructing integer solutions shows that the feasibility problem for systems of divisibility constraints in increasing form is in NP.

Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ be a formula in increasing form for an order $\prec$. According to Theorem 4, Φ is satisfiable over the integers if and only if there are solutions $\boldsymbol{b}_p$ for Φ modulo p for every prime p belonging to $\mathbb{P}(\Phi)$. From Lemma 4, the bit length of $\mathbb{P}(\Phi)$ is polynomial in $\langle \Phi \rangle$, and therefore only polynomially many primes of polynomial bit length need to be considered. Recall that Φ has a solution modulo p whenever the system $\bigwedge_{i=1}^m v_p(f_i(\boldsymbol{x})) \leq v_p(g_i(\boldsymbol{x})) \wedge f_i(\boldsymbol{x}) \neq 0$ has a solution. In [6] it is shown that the feasibility problem for these constraint systems is in NP (this result holds for solutions over the integers, p-adic integers, and p-adic numbers), and therefore there are certificates of feasibility having size polynomial in $\langle p \rangle$ and $\langle \Phi \rangle$. The set of these certificates, one for each prime in $\mathbb{P}(\Phi)$, is a polynomial size certificate for the feasibility of Φ.

Proposition 2. *Feasibility for systems of divisibility constraints in increasing form is in* NP.

Of course, we know from the family of formulae Φ_n introduced in Section 1.1 (and the one after Theorem 4) that systems in increasing form might have minimal solutions of exponential bit length. Therefore, Proposition 2 is of no use when establishing Theorem 1. However, it still has an interesting implication: if the feasibility problem for systems of divisibility constraints lies outside NP, then there is no polynomial time non-deterministic Turing machine for finding an equisatisfiable system in increasing form.

4 IP-GCD systems have polynomial size solutions

In this section we expand the summary provided Section 1.4 and establish Theorem 1, i.e., that every feasible IP-GCD system has solutions of polynomial bit length, and that this polynomial bound still holds when looking at minimization or maximization of linear objectives. As explained in Section 1.4, we prove Theorem 1 by designing an algorithm that reduces an IP-GCD system into a disjunction of (exponentially many) 3-increasing systems of divisibility constraints with coefficients and constants of polynomial size, to then study bounds on their solutions modulo primes. Then, the polynomial small witness property follows from Theorem 4.

Without loss of generality, throughout the section we consider IP-GCD systems of the form

$$A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{k} \gcd(y_i, z_i) \sim_i c_i \,,$$

where, $A \in \mathbb{Z}^{m \times d}$, $\boldsymbol{b} \in \mathbb{Z}^m$, $c_i \in \mathbb{Z}_+$, $\boldsymbol{x} = (x_1, \dots, x_d)$ is a vector of variables, $\sim_i \;\in \{\leq, =, \neq, \geq\}$, and the y_i and z_i are variables occurring in $\boldsymbol{x}$. Systems with GCD constraints $\gcd(f(\boldsymbol{w}), g(\boldsymbol{w})) \sim c$ can be put into this form by replacing $\gcd(f(\boldsymbol{w}), g(\boldsymbol{w})) \sim c$ with $y = f(\boldsymbol{w}) \wedge z = g(\boldsymbol{w}) \wedge \gcd(y, z) \sim c$, where y and z are fresh variables.

4.1 Translation into 3-increasing systems

The procedure generating the 3-increasing systems of divisibility constraints starting from an IP-GCD system Φ is divided into two steps: we first (Algorithm 2) compute several systems of divisibility constraints whose disjunction is equivalent to Φ (under some changes of variables). We now describe these two steps in detail, and study bounds on the obtained 3-increasing formulae (Lemma 13). Both steps rely on the following notion of gcd-to-div triple, which highlights properties of the system of divisibility constraints obtained by translation from IP-GCD systems. A triple $(\Psi, \boldsymbol{u}, E)$ is said to be a *gcd-to-div* triple whenever there are $d, m \in \mathbb{N}$ and three disjoint families of variables $\boldsymbol{z}$, $\boldsymbol{y}$ and $\boldsymbol{w}$ for which the following properties hold:

1. $\Psi(\boldsymbol{z}, \boldsymbol{y}, \boldsymbol{w})$ is a system of divisibility constraints in m variables, $\boldsymbol{u} \in \mathbb{Z}^d$ and $E \in \mathbb{Z}^{d \times m}$, where each column of E (implicitly) corresponds to a variable in Ψ.

2. Each divisibility in Ψ is of the form $h(\boldsymbol{z}) \mid f(\boldsymbol{y})$ or of the form $f(\boldsymbol{y}) \mid g(\boldsymbol{w})$, with g being a non-constant polynomial. Each polynomial only features non-negative coefficients and constants, and each left-hand side of a divisibility has a (strictly) positive constant.

3. In Ψ, each variable in $\boldsymbol{z}$ appears in a single polynomial $h(\boldsymbol{z})$, where $h(\boldsymbol{z})$ is of the form $z + c$, for some $c \in \mathbb{Z}_+$, and occurs in precisely two divisibilities (as left-hand side).

4. In Ψ, each variable in $\boldsymbol{w}$ appears in exactly two polynomials $g_1(\boldsymbol{w})$ and $g_2(\boldsymbol{w})$, each occurring in Ψ exactly once (as right-hand sides). They have the form $g_1(\boldsymbol{w}) = w$ and $g_2(\boldsymbol{w}) = w + c$, for some $c \in \mathbb{Z}_+$.

Algorithm 2 Translate a IP-GCD system into gcd-to-div triples

Input: An IP-GCD system $\Phi(\boldsymbol{x}) = A \cdot \boldsymbol{x} \leq \boldsymbol{b} \wedge \bigwedge_{i=1}^{k} \gcd(y_i, z_i) \sim_i c_i$ with $\boldsymbol{x} = (x_1, \dots, x_d)$.
Output: A finite set B of gcd-to-div triples satisfying $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ solution to } \Phi\} = [\![B]\!]$.

1: $G \coloneqq \{\Psi_1(\boldsymbol{x}), \dots, \Psi_\ell(\boldsymbol{x})\}$ such that Φ is equivalent to $\bigvee_{i=1}^{\ell} \Psi_i$ and every $\Psi \in G$ is a IP-GCD system in which every GCD constraint $\gcd(y, z) \sim c$ is such that (i) for both $w \in \{y, z\}$ either $w \leq -1$ or $w \geq 1$ appear in Ψ, and (ii) the relation $\sim$ is either $=$ or $\geq$
2: $B \coloneqq \emptyset$ ▷ *Set to be returned by the procedure*
3: **for** Ψ **in** G **do**
4: $\quad\Psi' \coloneqq$ linear inequalities in Ψ
5: $\quad S \coloneqq \{(\boldsymbol{u}_i, E_i) : i \in I\}$ s.t. $\bigcup_{i \in I}\{\boldsymbol{u}_i + E_i \cdot \boldsymbol{y} : \boldsymbol{y} \in \mathbb{N}^\ell\}$ solutions set of Ψ' ▷ *Proposition 3*
6: $\quad$**for** $(\boldsymbol{u}, E)$ **in** S **do**
7: $\quad\quad\Psi'' \coloneqq$ system of GCD constraints obtained from Ψ by performing the change of variables $\boldsymbol{x} \leftarrow \boldsymbol{u} + E \cdot \boldsymbol{y}$, where $\boldsymbol{y}$ is a vector of fresh variables (over $\mathbb{N}$)
8: $\quad\quad$replace every polynomial f in Ψ'' having only negative coefficients or constant with $-f$
9: $\quad\quad$replace every constraint $\gcd(f, g) = c$ in Ψ'' with $(c \mid f) \wedge (c \mid g) \wedge (f \mid w) \wedge (g \mid w + c)$, where w is a fresh variable (distinct GCD constraints gets distinct fresh variables)
10: $\quad\quad$replace every constraint $\gcd(f, g) \geq c$ in Ψ'' with $(z + c \mid f) \wedge (z + c \mid g)$, where z is a fresh variable (distinct GCD constraints gets distinct fresh variables)
11: $\quad\quad$add to B the triple $(\Psi'', \boldsymbol{u}, E')$ where E' is obtained form E by adding a zero column for each auxiliary variable z and w added in lines 9 and 10
12: **return** B

5. Every column in E corresponding to a variable in $\boldsymbol{z}$ or $\boldsymbol{w}$ is zero (see line 11 of Algorithm 2).

For a set of gcd-to-div triples S, let $[\![S]\!] \coloneqq \{\boldsymbol{u} + E \cdot \boldsymbol{\lambda} \,:\, (\Psi, \boldsymbol{u}, E) \in B \text{ and } \boldsymbol{\lambda} \in \mathbb{N}^m \text{ solution to } \Psi\}$.

Step I: from IP-GCD to systems of divisibility constraints. This step is implemented by Algorithm 2. As highlighted in its signature, given as input an IP-GCD system $\Phi(\boldsymbol{x})$ having d variables and k GCD constraints, this procedure returns a set B of gcd-to-div triples satisfying the equivalence $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ solution to } \Phi\} = [\![B]\!]$. This equivalence clarifies the role of the vector $\boldsymbol{u}$ and matrix E of a gcd-to-div triple $(\Psi, \boldsymbol{u}, E)$: they are used to perform a change of variables between the variables $(\boldsymbol{z}, \boldsymbol{y}, \boldsymbol{w})$ in Ψ and the variables $\boldsymbol{x}$ in Φ. Note that, according to the definition of $[\![B]\!]$, the values of $(\boldsymbol{z}, \boldsymbol{y}, \boldsymbol{w})$ range over $\mathbb{N}$ instead of $\mathbb{Z}$. This discrepancy stems from the use of the forthcoming Proposition 3.

Let us discuss how Algorithm 2 computes B. As a preliminary step, the procedure computes the formula $\bigvee_{i=1}^{\ell} \Psi_i$ in line 1. The role of this formula is to reduce the problem of translating IP-GCD systems into systems of divisibility constraints to only those systems in which the GCD constraints $\gcd(y, z) \leq c$ and $\gcd(y, z) \neq c$ do not appear, and given a GCD constraint $\gcd(y, z) \sim c$ (with $\sim$ either $=$ or $\geq$), the variables y and z are forced to be positive or negative (in particular, non-zero). The formula $\bigvee_{i=1}^{\ell} \Psi_i$ can be computed from Φ by opportunely applying the following tautologies:

$$y \leq -1 \vee y = 0 \vee y \geq 1\,, \qquad \gcd(y, z) \neq c + 2 \iff \gcd(y, z) \leq c + 1 \vee \gcd(y, z) \geq c + 3 \quad (c \in \mathbb{N})\,,$$

$$\gcd(y, z) \neq 1 \iff y = z = 0 \vee \gcd(y, z) \geq 2\,, \qquad \gcd(y, z) \leq c \iff \bigvee_{j=1}^{c} \gcd(y, z) = j\,,$$

$$y = 0 \implies (\gcd(y, z) \sim c \iff |z| \sim c)\,, \qquad y \neq 0 \wedge z = 0 \implies (\gcd(y, z) \sim c \iff |y| \sim c)\,,$$

where in the last two tautologies $\sim$ is $=$ or $\geq$, and $|x| \sim c \coloneqq (x \geq 0 \land x \sim c) \lor (x < 0 \land -x \sim c)$. Let $G \coloneqq \{\Psi_1, \dots, \Psi_\ell\}$ (as defined in line 1). The next step of the algorithm is to remove the system of inequalities from every formula $\Psi \in G$ via changes of variables (lines 4–7). This can be done thanks to a fundamental result by von zur Gathen and Sieveking [25] that characterises the set of solutions of linear inequalities as a union of discrete shifted cones. The following formulation of this result is from [12, Theorem 3].

Proposition 3 ([25]). *Consider matrices $A \in \mathbb{Z}^{m\times d}$, $C \in \mathbb{Z}^{n\times d}$, and vectors $\boldsymbol{b} \in \mathbb{Z}^m$, $\boldsymbol{d} \in \mathbb{Z}^n$. Let $r \coloneqq \operatorname{rank}(A)$ and $s \coloneqq \operatorname{rank}\binom{A}{C}$. Then,*

$$\{\boldsymbol{x} \in \mathbb{Z}^d : A \cdot \boldsymbol{x} = \boldsymbol{b} \land C \cdot \boldsymbol{x} \leq \boldsymbol{d}\} = \bigcup_{i\in I} \{\boldsymbol{u}_i + E_i \cdot \boldsymbol{y} \,:\, \boldsymbol{y} \in \mathbb{N}^{d-r}\},$$

where I is a finite set, $\boldsymbol{u}_i \in \mathbb{Z}^d$, $E_i \in \mathbb{Z}^{d\times(d-r)}$ and $\|\boldsymbol{u}_i\|, \|E_i\| \leq (d{+}1)(s{\cdot}\max(2, \|A\|, \|C\|, \|\boldsymbol{b}\|, \|\boldsymbol{d}\|))^s$.

Let $S = \{(\boldsymbol{u}_i, E_i) : i \in I\}$ be the set of pairs given by Proposition 3 on the linear inequalities of Ψ, as written in line 5, and given $(\boldsymbol{u}, E) \in S$ consider the system Ψ'' defined in line 7. Following Proposition 3, Ψ'' is interpreted over $\mathbb{N}$. By definition of G, in Ψ, every variable x appearing in a GCD constraint also appears in a (non-zero) sign constraint $x \leq -1$ or $x \geq 1$. This means that in the system $\boldsymbol{x} = \boldsymbol{u} + E \cdot \boldsymbol{y}$, the row corresponding to x is of the form $x = f(\boldsymbol{y})$ where f is a linear polynomial having coefficients and constant with the same polarity, i.e., they are all negatives (if $x \leq -1$) or positives (if $x \geq 1$). Therefore, all GCD constraints in Ψ'' are of the form $\gcd(f, g) \sim c$ where f and g are polynomials with coefficients and constant having the same polarity. Line 8 modifies Ψ'' so that every polynomial in it becomes of positive polarity, thanks to the equalities $\gcd(f, g) = \gcd(-f, g)$ and $\gcd(f, g) = \gcd(g, f)$. What is left is to translate Ψ'' into a system of divisibilities. This is done in lines 9 and 10 by simply relying on the following two tautologies:

$$\begin{gathered}\gcd(f, g) = c \land f \neq 0 \land g \neq 0 \iff \exists w \in \mathbb{N} :\; c \mid f \;\land\; c \mid g \;\land\; f \mid w \;\land\; g \mid w + c\,,\\ \gcd(f, g) \geq c \iff \exists z \in \mathbb{N} :\; z + c \mid f \;\land\; z + c \mid g.\end{gathered} \tag{9}$$

Above, note that we can assume $f \neq 0 \land g \neq 0$ in Ψ'', again because of the sign constraints appearing in Ψ. While the second tautology should be self-explanatory, the first one merits a formal proof:

$$\begin{aligned}
&\gcd(f, g) = c \land f \neq 0 \land g \neq 0 &&\\
\iff{}& \exists a, b \in \mathbb{Z} :\; c \mid f \;\land\; c \mid g \;\land\; a \cdot f + b \cdot g = c && \text{Bézout's identity}\\
\iff{}& \exists w, z \in \mathbb{Z} :\; w \leq 0 \;\land\; c \mid f \;\land\; c \mid g \land f \mid w \land g \mid z \land w + z = c && \text{set } w = a \cdot f \text{ and } z = b \cdot g\\
& && \text{Bézout's identity allows picking } w \leq 0\\
\iff{}& \exists w \in \mathbb{Z} :\; w \leq 0 \;\land\; c \mid f \;\land\; c \mid g \land f \mid -w \land g \mid c - w && \text{eliminate } z\text{, and } f \mid w \Leftrightarrow f \mid -w\\
\iff{}& \exists w \in \mathbb{N} :\; c \mid f \land c \mid g \land f \mid w \land g \mid w + c && \text{change of variable } -w \leftarrow w.
\end{aligned}$$

Note that the divisibilities in (9) ensure that Ψ'' satisfies the constraints required by gcd-to-div triples. After translating GCDs into divisibilities, the procedure computes a matrix E' by enriching E with zero columns corresponding to the new variables z and w, and adds the resulting triple $(\Psi'', \boldsymbol{u}, E')$ to B (line 11). We obtain the following result:

Lemma 10. *Algorithm 2 respects its specification. Given as input a system Φ with d variables and k GCD constraints, every triple $(\Psi, \boldsymbol{u}, E)$ in the output set B is such that Ψ has at most $d{+}k$ variables and $4k$ divisibilities, E has at most d non-zero columns, and $\|\Psi\|, \|\boldsymbol{u}\|, \|E\| \leq (d{+}1)^{d+2}(\|\Phi\|{+}1)^{d+1}$.*

Algorithm 3 Translates the systems in gcd-to-div triples into 3-increasing form

Input: A finite set B of gcd-to-div triples.
Output: A finite set C of gcd-to-div triples such that $[\![B]\!] = [\![C]\!]$
and for every $(\Psi, \boldsymbol{u}, E) \in C$, Ψ is a 3-increasing system of divisibility constraints.

1: $C \coloneqq \emptyset$ ▷ *Set to be returned by the procedure*
2: **while** $(\Psi, \boldsymbol{u}, E) \leftarrow \mathrm{pop}(B)$ **do** ▷ *exits when B becomes empty*
3:     **if** $\mathrm{M}_f(\Psi) \cap \mathbb{Z} = \{0\}$ for every non-constant f primitive part of some l.h.s. in Ψ **then**
4:         add to C the triple $(\Psi, \boldsymbol{u}, E)$ ▷ *Ψ in increasing form*
5:     **else**
6:         $f \coloneqq$ non-constant primitive part of some l.h.s. in Ψ, satisfying $\mathrm{M}_f(\Psi) \cap \mathbb{Z} \neq \{0\}$
7:         $\lambda_1, \dots, \lambda_j \coloneqq$ the variables appearing in f
8:         $c \coloneqq$ minimum positive integer in $\mathrm{M}_f(\Psi)$
9:         **for** $\boldsymbol{\nu} \colon \{\lambda_1, \dots, \lambda_j\} \to [0, c]$ such that $f(\boldsymbol{\nu}(\lambda_1), \dots, \boldsymbol{\nu}(\lambda_j))$ divides c **do**
10:             $\Psi_{\boldsymbol{\nu}} \coloneqq \Psi[\boldsymbol{\nu}(\lambda_i) \,/\, \lambda_i : i \in [1, j]]$ ▷ *$\Psi_{\boldsymbol{\nu}}$ has fewer variables than Ψ*
11:             $\boldsymbol{u}_{\boldsymbol{\nu}} \coloneqq \boldsymbol{u} + \sum_{i=1}^{j} \boldsymbol{\nu}(\lambda_i) \cdot \boldsymbol{p}_i$ where $\boldsymbol{p}_i$ is the column of E corresponding to the variable λ_i
12:             $E_{\boldsymbol{\nu}} \coloneqq E$ without the columns corresponding to $\lambda_1, \dots, \lambda_j$
13:             add to B the triple $(\Psi_{\boldsymbol{\nu}}, \boldsymbol{u}_{\boldsymbol{\nu}}, E_{\boldsymbol{\nu}})$ ▷ *triple to be considered again in line 2*
14: **return** C

Proof. The fact that Algorithm 2 respects its specification follows from the discussion given above. In particular, $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ solution of } \Phi\} = [\![B]\!]$ stems from the fact that the procedure treats the original formula Φ by only relying on tautologies and on Proposition 3.

Let us study the bounds on $(\Psi, \boldsymbol{u}, E)$. For the bound on the number of variables in Ψ and non-zero columns in E, note that by Proposition 3, the change of variables of line 7 does not increase the number of variables, and therefore the only lines where the number of variables increases are lines 9 and 10. Overall, these two lines introduce k many variables, one for each GCD constraint; so the number of variables in Ψ is bounded by $d+k$. Each new variable introduces a zero column in E, which has thus at most d non-zero columns (line 11). For the bound on the number of divisibilities, only lines 9 and 10 matter, and they introduce at most 4 divisibilities per GCD constraint; hence Ψ has at most $4k$ divisibilities. Lastly, let us derive the bound on the infinity norm of Ψ, $\boldsymbol{u}$ and E. The rewritings done in line 1 increase the infinity norm by at most 1; this occurs when relying on the tautology $\gcd(y, z) \neq c + 2 \iff \gcd(y, z) \leq c + 1 \lor \gcd(y, z) \geq c + 3$. The bound on $\boldsymbol{u}$ and E then follows from a simple application of Proposition 3: $\|\boldsymbol{u}\|, \|E\| \leq (d+1) \cdot (d \cdot (\|\Phi\| + 1))^d$. The change of variables in line 7 yields $\|\Psi''\| \leq (d+1) \cdot \max(\|\boldsymbol{u}\|, \|E\|) \cdot (\|\Phi\| + 1)$. Lines 8–11 do not change the infinity norm, and therefore we obtain the bound in the statement of the lemma. ☐

Step II: force increasingness. We now move to Algorithm 3, whose role is to translate the systems of divisibility constraints computed by Algorithm 2 into 3-increasing systems. As such, the procedure takes as input a set B of gcd-to-div triples. We first need the following result:

Lemma 11. *Let $(\Psi, \boldsymbol{u}, E)$ be a gcd-to-div triple. If the system Ψ is not in increasing form, then there is a non-constant polynomial f primitive part of a left-hand side in Ψ such that $\mathrm{M}_f(\Psi) \cap \mathbb{Z} \neq \{0\}$. If Ψ is in increasing form, then it is increasing for $\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w}$, where $\boldsymbol{z}$, $\boldsymbol{y}$ and $\boldsymbol{w}$ are the families of variables appearing in the definition of gcd-to-div triple.*

Proof. For the first statement, we prove a stronger result: if Ψ is not increasing for $\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w}$, then there is a non-constant polynomial f primitive part of a left-hand side in Ψ s.t. $\mathrm{M}_f(\Psi) \cap \mathbb{Z} \neq \{0\}$.

Observe that then, by definition of divisibility module and increasing form, Ψ cannot be in increasing form for any order; which shows the second statement in the lemma by contrapositive.

Consider an order $x_1 \prec \cdots \prec x_d$ of the variables in Ψ that belongs to $\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w}$, and suppose that Ψ is not in increasing form for this order. Therefore, there is a primitive part f of a left-hand side of a divisibility in Ψ such that $\mathrm{M}_f(\Psi) \cap \mathbb{Z}[x_1, \dots, x_j] \neq \mathbb{Z}f$, where $x_j = \mathrm{LV}(f)$. Let $g \in \mathrm{M}_f(\Psi) \cap \mathbb{Z}[x_1, \dots, x_j] \setminus \mathbb{Z}f$. We show that g must be a constant polynomial. We distinguish two cases, depending on whether the leading variable of f belongs to $\boldsymbol{z}$ or to $\boldsymbol{y}$ (note that it cannot belong to $\boldsymbol{w}$, as no left-hand sides with variables from this family exists).

case $\mathrm{LV}(f)$ **is in** $\boldsymbol{z}$**.** Since $\mathrm{LV}(g) \preceq \mathrm{LV}(f)$, all variables in g are from $\boldsymbol{z}$. By Property 2 of gcd-to-div triple, each divisibility in Ψ is of the form $h(\boldsymbol{z}) \mid h'(\boldsymbol{y})$ or of the form $h(\boldsymbol{y}) \mid h'(\boldsymbol{w})$. By Lemma 6, a set spanning $\mathrm{M}_f(\Psi)$ is given by $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ where $c_i \in \mathbb{N}$ and g_i is a right-hand side of a divisibility in Ψ, for every $i \in [1, m]$. This means that every g_i has variables from $\boldsymbol{y}$ or $\boldsymbol{w}$. Since g does not have any variable from $\boldsymbol{y}$ or $\boldsymbol{w}$ and belongs to $\mathbb{Z}f$, we conclude that it must be a constant polynomial.

case $\mathrm{LV}(f)$ **is in** $\boldsymbol{y}$**.** Again from Property 2 of gcd-to-div triple, f only appears as left-hand side in divisibilities of the form $a \cdot f(\boldsymbol{y}) \mid h(\boldsymbol{w})$, with $a \in \mathbb{Z} \setminus \{0\}$. Since no non-constant polynomial $h(\boldsymbol{w})$ appears in a left-hand side of Ψ, the set $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ spanning $\mathrm{M}_f(\Psi)$ computed via Lemma 6 is such that $c_i \neq 0$ if and only if g_i only has variables from $\boldsymbol{w}$, for every $i \in [1, m]$. Since $\prec$ belongs to $\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w}$, from $\mathrm{LV}(g) \prec \mathrm{LV}(f)$ we then conclude that g must be a constant polynomial. $\square$

Consider $(\Psi, \boldsymbol{u}, E) \in B$. Algorithm 3 relies on Lemma 11 to test whether Ψ is increasing (line 3). If it is not, it computes the minimum positive integer $c \in \mathrm{M}_f(\Psi)$, for some f non-constant (line 8). By definition of divisibility module, for every primitive polynomial f and polynomial $g \in \mathrm{M}_f(\Psi)$, we have that Ψ entails $f \mid g$, that is for every $\boldsymbol{a} \in \mathbb{Z}^m$ solution to Ψ, $f(\boldsymbol{a})$ divides $g(\boldsymbol{a})$; and therefore Ψ entails $f \mid c$. We can now eliminate all variables that occur in f: by definition of gcd-to-div triple, f has coefficients and constant that are all positive, and Ψ is interpreted over $\mathbb{N}$. We conclude that every solution of Ψ is such that it assigns an integer in $[0, c]$ to every variable in f. The **for** loop in line 9 iterates over the subset of these (partial) assignments satisfying $f \mid c$. Each of these assignments $\boldsymbol{\nu}$ yields a new triple $(\Psi_{\boldsymbol{\nu}}, \boldsymbol{u}_{\boldsymbol{\nu}}, E_{\boldsymbol{\nu}})$, defined as in lines 10–12, which is a gcd-to-div triple thanks to the lemma below (that follows directly from the definition of gcd-to-div triple).

Lemma 12. *Let $(\Psi, \boldsymbol{u}, E)$ be a gcd-to-div triple, with $\boldsymbol{u} \in \mathbb{Z}^d$, and X be a subset of the variables appearing in left-hand sides of Ψ. Consider a map $\boldsymbol{\nu} \colon X \to \mathbb{Z}$. Let $\Psi' \coloneqq \Psi[\boldsymbol{\nu}(x) \,/\, x : x \in X]$, $\boldsymbol{u}' \in \mathbb{Z}^d$, and E' be the matrix obtained from E by removing the columns corresponding to variables in X. The triple $(\Psi', \boldsymbol{u}', E')$ is a gcd-to-div triple.*

The key equivalence, from which the correctness of the algorithm directly stems, is:

$$\{\boldsymbol{u} + E \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{N}^m \text{ solution for } \Psi\} = \bigcup_{\substack{\boldsymbol{\nu} \text{ substitution} \\ \text{considered in line 9}}} \{\boldsymbol{u}_{\boldsymbol{\nu}} + E_{\boldsymbol{\nu}} \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{N}^{m-j} \text{ solution for } \Psi_{\boldsymbol{\nu}}\}, \quad (10)$$

where $j \geq 1$ is the number of variables in f. The procedure adds each triple $(\Psi_{\boldsymbol{\nu}}, \boldsymbol{u}_{\boldsymbol{\nu}}, E_{\boldsymbol{\nu}})$ to the set B (line 13), so that it will be tested for increasingness in a later iteration of the **while** loop of line 2. Termination is guaranteed from the fact that f is non-constant and so each $\Psi_{\boldsymbol{\nu}}$ has strictly fewer variables than Ψ.

Lemma 13. *Algorithm 3 respects its specification. On input B such that, for every $(\Psi, \boldsymbol{u}, E) \in B$, Ψ has at most d variables and k GCD constraints, and E has at most ℓ non-zero columns, each output triple $(\Psi', \boldsymbol{u}', E') \in C$ is such that Ψ' has at most d variables and k GCD constraints, E' has at most ℓ non-zero columns, $\|\Psi'\| \leq 2^{15}(d+1) \cdot (\|B\|+1)^7$, $\|\boldsymbol{u}'\| \leq (\ell+1) \cdot \|B\|^2$, and $\|E'\| \leq \|B\|$.*

Above, $\|B\|$ is the maximum among $\|\Psi\|$, $\|\boldsymbol{u}\|$, and $\|E\|$, over all gcd-to-div triples $(\Psi, \boldsymbol{u}, E) \in B$. The most difficult parts of the proof are the bounds on Ψ' and $\boldsymbol{u}'$. These, however, follow from the properties of gcd-to-div triples and, in particular, from the special shape of the divisibility constraints that they allow. Together, Lemmas 10 and 13 imply Proposition 1 in Section 1.4.

Proof. The fact that Algorithm 3 respects its specification follows from the discussion given above, and in particular from Lemma 11 and Equation (10). Let us then focus on the bounds on an output triple $(\Psi', \boldsymbol{u}', E')$. Note that $\|B\| \geq 1$, if B contains at least one divisibility. Following the **while** loop of Algorithm 3, there is a sequence of triples

$$(\Psi_1, \boldsymbol{u}_1, E_1) \;\to\; (\Psi_2, \boldsymbol{u}_2, E_2) \;\to\; \dots \;\to (\Psi_k, \boldsymbol{u}_k, E_k) = (\Psi', \boldsymbol{u}', E'),$$

where $(\Psi_1, \boldsymbol{u}_1, E_1) \in B$ and for every $i \in [1, k-1]$, the triple $(\Psi_{i+1}, \boldsymbol{u}_{i+1}, E_{i+1})$ is computed from $(\Psi_i, \boldsymbol{u}_i, E_i)$ following lines 6–13. In particular, given $i \in [1, k-1]$:

- there is a non-constant polynomial $\widehat{f}_i$ that is the part of a left-hand side in Ψ_i satisfying $\mathrm{M}_{\widehat{f}_i}(\Psi_i) \cap \mathbb{Z} \neq \{0\}$ and with variables $\widehat{\boldsymbol{\lambda}}_i \coloneqq (\lambda_{i,1}, \dots, \lambda_{i,j_i})$, and

- there is a map $\boldsymbol{\nu}_i : \{\lambda_{i,1}, \dots, \lambda_{i,j_i}\} \to [0, \widehat{c}_i]$ such that $\widehat{f}_i(\boldsymbol{\nu}_i(\widehat{\boldsymbol{\lambda}}_i))$ divides $\widehat{c}_i$, where $\widehat{c}_i$ is the minimum positive integer in $\mathrm{M}_{\widehat{f}_i}(\Psi_i)$,

such that $\Psi_{i+1} = \Psi_i[\boldsymbol{\nu}_i(\lambda_{i,r}) \;/\; \lambda_{i,r} : r \in [1, j_i]]$, $\boldsymbol{u}_{i+1} = \boldsymbol{u}_i + \sum_{r=1}^{j} \boldsymbol{\nu}_i(\lambda_{i,r}) \cdot \boldsymbol{p}_r$, where $\boldsymbol{p}_r$ is the column of E_i corresponding to the variable $\lambda_{i,r}$, and E_{i+1} is obtained from E_i by removing the columns corresponding to variables in $\widehat{\boldsymbol{\lambda}}_i$. Note that this implies that $\|E'\| \leq \|E_i\| \leq \|B\|$ and that E' and E_i have at most ℓ non-zero columns, as required by the lemma.

We show the remaining bounds in the statement of the lemma by induction on $i \in [1, k]$, with the induction hypothesis stating that $(\Psi_i, \boldsymbol{u}_i, E_i)$ is a gcd-to-div triple where:

(A) Ψ_i is a system with at most d variables and k GCD constraints, having the form

$$\Psi_i = \bigwedge_{j=1}^{l} c_j \mid f_j(\boldsymbol{y}) \wedge \bigwedge_{j=l+1}^{n} \Big(z_j + c_j \mid f_j(\boldsymbol{y}) \wedge z_j + c_j \mid g_j(\boldsymbol{y})\Big) \wedge \bigwedge_{j=n+1}^{m} \Big(f_j(\boldsymbol{y}) \mid w_j \wedge g_j(\boldsymbol{y}) \mid w_j + c_j\Big),$$

where $\boldsymbol{y}$, $\boldsymbol{z} = (z_{l+1}, \dots, z_n)$ and $\boldsymbol{w} = (w_{n+1}, \dots, w_m)$ are disjoint families of variables (according to the definition of gcd-to-div triple), $c_j \in \mathbb{Z}_+$ for every $j \in [1, m]$, and

(B) for every $j \in [1, l]$, $c_j \leq 2^{15} \cdot (2 + \|B\|)^7$, and for every $j \in [l+1, m]$, $c_j \leq \|B\|$, and

(C) for every $j \in [l+1, m]$, $h(\boldsymbol{y}) \in \{f_j(\boldsymbol{y}), g_j(\boldsymbol{y})\}$ has variable coefficients bounded by $\|B\|$, and constant bounded by $(d + 1 - d') \cdot \|B\|^2$, where d' is the number of variables in h, and

(D) if $i \in [2, k]$, then for every $r \in [1, j_{i-1}]$, if $\lambda_{i-1,r}$ belongs to $\boldsymbol{y}$ then $\boldsymbol{\nu}_i(\lambda_{i-1,r}) \leq \|B\|$, and if $\lambda_{i-1,r}$ belongs to $\boldsymbol{z}$ then $\boldsymbol{\nu}_i(\lambda_{i-1,r}) \leq 2^{14}(2 + \|B\|)^7$.

Note that Item (D) implies $\|\boldsymbol{u}'\| \leq (\ell + 1) \cdot \|B\|^2$, since all non-zero columns of E_1 correspond to variables in $\boldsymbol{y}$, by definition of gcd-to-div triple. Items (B) and (C) imply $\|\Psi'\| \leq 2^{15}(d{+}1) \cdot (\|B\|{+}1)^7$.

base case $i = 1$. In this case $(\Psi_1, \boldsymbol{u}_1, E_1) \in B$ and the hypothesis above trivially holds since $(\Psi_1, \boldsymbol{u}_1, E_1)$ is a gcd-to-div triple and Properties 2–4 ensure that Ψ_1 has the form in Item (A).

induction step $i + 1 \geq 2$. We assume the induction hypothesis for $(\Psi_i, \boldsymbol{u}_i, E_i)$, and establish it for $(\Psi_{i+1}, \boldsymbol{u}_{i+1}, E_{i+1})$. By Lemma 12, $(\Psi_{i+1}, \boldsymbol{u}_{i+1}, E_{i+1})$ is a gcd-to-div triple, hence Item (A) follows. So, let us focus on establishing the part of the induction hypothesis related to the infinity norm of Ψ_{i+1} and $\boldsymbol{\nu}_i$ (Items (B) to (D)). Let $\boldsymbol{z}$, $\boldsymbol{y}$ and $\boldsymbol{w}$ be the families of variables witnessing that $(\Psi_i, \boldsymbol{u}_i, E_i)$ is a gcd-to-div triple, according to the definition of such triples. By Property 2, $\widehat{f_i}$ has variables from either $\boldsymbol{z}$ or $\boldsymbol{y}$ (not both). We divide the proof depending on these two cases.

case $\widehat{f_i}$ has only variables from $\boldsymbol{y}$. From Property 2 of gcd-to-div triples, $\widehat{f_i}$ only appears as a left-hand side in divisibilities of the form $a \cdot \widehat{f_i}(\boldsymbol{y}) \mid h(\boldsymbol{w})$, with $a \in \mathbb{Z} \setminus \{0\}$. From Property 4 of gcd-to-div triples together with the fact that $\mathrm{M}_{\widehat{f_i}}(\Psi_i) \cap \mathbb{Z} \neq \{0\}$, we conclude that there must be a variable w in $\boldsymbol{w}$ and $c \in \mathbb{Z}_+$ such that $a_1 \cdot \widehat{f_i} \mid w$ and $a_2 \cdot \widehat{f_i} \mid w + c$ are divisibilities in Ψ_i, for some $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$. Then, $c \in \mathrm{M}_{\widehat{f_i}}(\Psi_i)$ and by definition $\widehat{c_i} \leq c$. By induction hypothesis (Item (B)), $\widehat{c_i} \leq \|B\|$, which shows Item (D) directly by definition of $\boldsymbol{\nu}_i$. Item (B) is also trivially satisfied: since we are replacing only variables in $\boldsymbol{y}$, all polynomials in Ψ_{i+1} with variables from $\boldsymbol{z}$ or $\boldsymbol{w}$ are polynomials in Ψ_i, and no new coefficient c' can appear in divisibilities of the form $c' \mid f(\boldsymbol{y})$.

To prove Item (C), let h' be a polynomial obtained from some $h(\boldsymbol{y})$ in Ψ_i by evaluating each $\lambda_{i,r}$ as $\boldsymbol{\nu}_i(\lambda_{i,r})$ ($r \in [1, j]$). By induction hypothesis (Item (C)), h has variable coefficients bounded by $\|B\|$, and constants bounded by $(d + 1 - d') \cdot \|B\|^2$, where d' is the number of variables in h. Let d'' be the number of variables in h'. Because of the substitutions done by $\boldsymbol{\nu}_i$, we conclude that the coefficients of h' are bounded by $\|B\|$, whereas its constant is bounded by $(d+1-d') \cdot \|B\|^2 + (d'-d'') \cdot \|B\|^2 = (d+1-d'') \cdot \|B\|^2$.

case $\widehat{f_i}$ has only variables from $\boldsymbol{z}$. In this case, $\widehat{f_i}$ is of the form $z + c$ for some $c \in \mathbb{Z}_+$, and by Property 3 of gcd-to-div triple it appears in exactly two divisibilities $z + c \mid f(\boldsymbol{y})$ and $z + c \mid g(\boldsymbol{y})$. In order to upper bound $\widehat{c_i}$, we divide the proof in two cases, depending on whether $(\mathbb{Z}f + \mathbb{Z}g) \cap \mathbb{Z} = \{0\}$.

case $(\mathbb{Z}f + \mathbb{Z}g) \cap \mathbb{Z} = \{0\}$. Since $\mathrm{M}_{\widehat{f_i}}(\Psi_i) \cap \mathbb{Z} \neq \{0\}$, by Properties 2 and 4 of gcd-to-div triples there must be two polynomials $f'(\boldsymbol{y})$ and $g'(\boldsymbol{y})$, a variable w in $\boldsymbol{w}$ and $a', b', c' \in \mathbb{Z}_+$ such that $f'(\boldsymbol{y}) \mid w$, $g'(\boldsymbol{y}) \mid w + c'$ and $\{a' \cdot f', b' \cdot g'\} \subseteq (\mathbb{Z}f + \mathbb{Z}g)$. Then, by definition of divisibility module, $a' \cdot b' \cdot c' \in \mathrm{M}_{\widehat{f_i}}(\Psi_i)$. By induction hypothesis $c' \leq \|B\|$ (Item (B)), and therefore to find a bound on $\widehat{c_i}$ is suffices to bound a' and b'. Let us study the case of a' (the bound is the same for b'). The set $S \coloneqq \{-f', f, g\}$ can be represented as a matrix $A \in \mathbb{Z}^{(d+1)\times 3}$ in which each column contains the coefficients and the constant of a distinct element of S. We apply Proposition 3 on the system $A \cdot (x_1, x_2, x_3) = \mathbf{0}$, and conclude that a' is bounded by $4 \cdot (3 \cdot \max(2, \|A\|))^3 \leq 108 \cdot (\|B\| + 1)^3$. Therefore, $\widehat{c_i} \leq 2^{14}(\|B\| + 1)^7$.

case $(\mathbb{Z}f + \mathbb{Z}g) \cap \mathbb{Z} \neq \{0\}$. In this case, we consider the set $S \coloneqq \{f, g\}$ and the matrix $A \in \mathbb{Z}^{(d+1)\times 2}$ in which each column contains the coefficients and the constant of a distinct element in S, with the constant being places in the last row. To find a non-zero value $c' \in (\mathbb{Z}f + \mathbb{Z}g) \cap \mathbb{Z}$, we solve the system $A \cdot (x_1, x_2) + x_3 \cdot (\mathbf{0}, 1) = \mathbf{0}$. By Proposition 3, $\widehat{c_i} \leq |c'| \leq 4 \cdot (3 \cdot \max(2, \|A\|))^3 \leq 108 \cdot (\|B\| + 1)^3$.

Therefore, $\boldsymbol{\nu}_i(z) \leq \widehat{c_i} \leq 2^{14}(\|B\|+1)^7$, which shows Item (D) of the induction hypothesis. Item (C) is trivially satisfied, since $\boldsymbol{\nu}_i$ replaces only the variable z, which does not belong to $\boldsymbol{y}$. Item (B) follows from the fact that in the polynomial $z+c$ the integer c is bounded by $\|B\|$ by induction hypothesis, and therefore $\boldsymbol{\nu}(z)+c \leq 2^{15}(\|B\|+1)^7$. $\square$

4.2 Bound on the solutions modulo primes

Through Algorithms 2 and 3 we are able to compute from a IP-GCD system Φ a set of gcd-to-div triples C such that $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ is a solution to } \Phi\} = [\![C]\!]$. To apply Theorem 4, what is left is to study bounds on the solutions modulo primes in $\mathbb{P}(\Psi)$, for every $(\Psi, \boldsymbol{u}, E) \in C$.

Lemma 5. *Let $(\Psi, \boldsymbol{u}, E)$ be a gcd-to-div triple in which Ψ has d variables, and consider $p \in \mathbb{P}(\Psi)$. If Ψ has a solution modulo p, then it has a solution $\boldsymbol{b}_p \in \mathbb{Z}^d$ modulo p with $\|\boldsymbol{b}_p\| \leq (d+1)\cdot\|\Psi\|^3 p^2$.*

Proof. Let us assume there exists a solution $\boldsymbol{\nu}\colon \boldsymbol{\lambda} \to \mathbb{Z}$ to $\Psi(\boldsymbol{\lambda})$ modulo p. We build another solution $\boldsymbol{\nu}'\colon \boldsymbol{\lambda} \to \mathbb{Z}$ to $\Psi(\boldsymbol{\lambda})$ modulo p such that $\|\boldsymbol{\nu}'(\boldsymbol{\lambda})\| \leq (d+1)\cdot\|\Psi\|^3 p^2$. According to Properties 2–4 of gcd-to-div triples, the formula Ψ is of the form:

$$\Psi = \bigwedge_{i=1}^{l} c_i \mid f_i(\boldsymbol{y}) \wedge \bigwedge_{i=l+1}^{n} \Big(z_i + c_i \mid f_i(\boldsymbol{y}) \wedge z_i + c_i \mid g_i(\boldsymbol{y})\Big) \wedge \bigwedge_{i=n+1}^{m} \Big(f_i(\boldsymbol{y}) \mid w_i \wedge g_i(\boldsymbol{y}) \mid w_i + c_i\Big),$$

where $\boldsymbol{y}$, $\boldsymbol{z} = (z_{l+1},\dots,z_n)$ and $\boldsymbol{w} = (w_{n+1},\dots,w_m)$ are disjoint families of variables, and $c_i \in \mathbb{Z}_+$ for every $i \in [1,m]$. Recall that the variables z_i ($i \in [l+1,n]$) are all distinct, and the same holds true for the variables w_i ($i \in [n+1,m]$). We define $\mu_i \coloneqq v_p(c_i)$, $\mu \coloneqq \max_{i=1}^{m} \mu_i$, and $\boldsymbol{\nu}'$ as:

$$\boldsymbol{\nu}'(x) \coloneqq \begin{cases} (\boldsymbol{\nu}(x) \text{ modulo } p^{\mu}) & \text{if } x \text{ belongs to } \boldsymbol{y},\\ 1 & \text{if } x = z_i \text{ for some } i \in [l+1,n] \text{ and } p \text{ divides } c_i,\\ 0 & \text{if } x = z_i \text{ for some } i \in [l+1,n] \text{ and } p \text{ does not divide } c_i,\\ p^{\mu+1} g_i(\boldsymbol{\nu}'(\boldsymbol{y})) - c_i & \text{if } x = w_i \text{ for some } i \in [n+1,m] \text{ and } p^{\mu_i+1} \text{ does not divide } f_i(\boldsymbol{\nu}(\boldsymbol{y})),\\ p^{\mu+1} f_i(\boldsymbol{\nu}'(\boldsymbol{y})) & \text{otherwise } (x = w_i \text{ for some } i \in [n+1,m]). \end{cases}$$

Note that $\boldsymbol{\nu}'$ is defined recursively in the last two cases; this recursion is on variables from $\boldsymbol{y}$ and thus $\boldsymbol{\nu}'$ is well-defined. By definition, $p^{\mu+1} \leq \|\Psi\|\cdot p$, and therefore $\|\boldsymbol{\nu}'(x)\| \leq (d+1)\cdot\|\Psi\|^3 p^2$ for every variable x in $\boldsymbol{\lambda}$. To conclude the proof, let us show that $\boldsymbol{\nu}'$ is a solution for Ψ modulo p. The fact that $f(\boldsymbol{\nu}'(\boldsymbol{\lambda})) \neq 0$ for every polynomial f in the left-hand side of a divisibility in Ψ stems from $\boldsymbol{\nu}'$ being defined to be non-negative for every variable in $\boldsymbol{z}$ and $\boldsymbol{y}$, and f having a positive constant by Property 2 of gcd-to-div triples. So, we focus on showing that $v_p(f(\boldsymbol{\nu}'(\boldsymbol{\lambda}))) \leq v_p(g(\boldsymbol{\nu}'(\boldsymbol{\lambda})))$ for every divisibility $f \mid g$ in Ψ.

Let $i \in [1,l]$, and consider $c_i \mid f_i(\boldsymbol{y})$. By definition of $\boldsymbol{\nu}'$, $f_i(\boldsymbol{\nu}'(\boldsymbol{y})) \equiv f_i(\boldsymbol{\nu}(\boldsymbol{y})) \pmod{p^{\mu+1}}$, and therefore $v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y}))) = \min(\mu+1, v_p(f_i(\boldsymbol{\nu}(\boldsymbol{y}))))$. By definition of μ, we have $c_i \not\equiv 0 \pmod{p^{\mu+1}}$, i.e., $v_p(c_i) < \mu+1$. We conclude that $v_p(c_i) \leq v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y})))$.

Let $i \in [l+1,n]$, and consider the divisibilities $z_i+c_i \mid f_i(\boldsymbol{y})$ and $z_i+c_i \mid g_i(\boldsymbol{y})$. By definition of $\boldsymbol{\nu}'$ we have $v_p(\boldsymbol{\nu}'(z_i)+c_i) = 0$, and so $v_p(\boldsymbol{\nu}'(z_i)+c_i) \leq v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y})))$ and $v_p(\boldsymbol{\nu}'(z_i)+c_i) \leq v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y})))$.

Let $i \in [n+1,m]$. Assume first that p^{μ_i+1} does not divide $f_i(\boldsymbol{\nu}(\boldsymbol{y}))$, and so $\boldsymbol{\nu}'$ is defined so that $\boldsymbol{\nu}'(w_i) = p^{\mu+1} g_i(\boldsymbol{\nu}'(\boldsymbol{y})) - c_i$. The divisibility $g_i(\boldsymbol{y}) \mid w_i + c$ is trivially satisfied by $\boldsymbol{\nu}'$ over the integers, and thus also modulo p. By definition of $\boldsymbol{\nu}'$ we have $f_i(\boldsymbol{\nu}'(\boldsymbol{y})) \equiv f_i(\boldsymbol{\nu}(\boldsymbol{y})) \pmod{p^{\mu+1}}$ and therefore p^{μ_i+1} does not divide $f_i(\boldsymbol{\nu}'(\boldsymbol{y}))$. By definition of μ_i, this implies $v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y}))) \leq v_p(c_i)$. From the definition of μ, $v_p(p^{\mu+1} g_i(\boldsymbol{\nu}'(\boldsymbol{y}))) > v_p(c_i)$ and therefore $v_p(\boldsymbol{\nu}'(w_i)) = v_p(c_i)$, which yield $v_p(f_i(\boldsymbol{\nu}'(\boldsymbol{y}))) \leq v_p(\boldsymbol{\nu}'(w_i))$. Let us now assume that p^{μ_i+1} divides $f_i(\boldsymbol{\nu}(\boldsymbol{y}))$, and so $\boldsymbol{\nu}'$ is defined so that $\boldsymbol{\nu}'(w_i) = p^{\mu+1} f_i(\boldsymbol{\nu}'(\boldsymbol{y}))$. Clearly, the divisibility $f_i(\boldsymbol{y}) \mid w_i$ is satisfied by $\boldsymbol{\nu}'$ over the integers, and thus also modulo p. Since $\boldsymbol{\nu}$ is a solution for Ψ modulo p, and $p^{\mu+1}$ divides $f_i(\boldsymbol{\nu}(\boldsymbol{y}))$, we conclude that $p^{\mu+1}$ divides $\boldsymbol{\nu}(w_i)$. Then, by definition of μ, $v_p(\boldsymbol{\nu}(w_i)) > v_p(c_i)$ and therefore $v_p(g_i(\boldsymbol{\nu}(\boldsymbol{y}))) \leq v_p(\boldsymbol{\nu}(w_i) + c_i) = v_p(c_i)$. By definition of $\boldsymbol{\nu}'$, $g_i(\boldsymbol{\nu}'(\boldsymbol{y})) \equiv g_i(\boldsymbol{\nu}(\boldsymbol{y})) \pmod{p^{\mu+1}}$ and $v_p(\boldsymbol{\nu}'(w_i) + c_i) = v_p(c_i)$. We conclude that $v_p(g_i(\boldsymbol{\nu}'(\boldsymbol{y}))) \leq v_p(\boldsymbol{\nu}'(w_i) + c_i)$. ☐

4.3 Proof of Theorem 1

Thanks to Lemmas 4, 5, 10 and 13, we obtain the part of Theorem 1 not concerning optimization as a corollary of Theorem 4.

Corollary 1. *Each feasible IP-GCD system has a solution of polynomial bit length.*

Let us now discuss the related integer programming optimization problem. Consider an IP-GCD system $\Phi(\boldsymbol{x})$ and the problem of minimizing (or maximizing) a linear objective $\boldsymbol{c}^\intercal \boldsymbol{x}$ subject to $\Phi(\boldsymbol{x})$. We apply Lemmas 10 and 13 on $\Phi(\boldsymbol{x})$ to obtain a set C of gcd-to-div triples only featuring 3-increasing systems of divisibility constraints , and with $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ solution to } \Phi\} = [\![C]\!]$. We show the following characterization that implies the optimization part of Theorem 1:

I. if for every $(\Psi, \boldsymbol{u}, E) \in C$, Ψ is unsatisfiable over $\mathbb{N}$, then Φ is unsatisfiable;

II. else, if there is $(\Psi, \boldsymbol{u}, E) \in C$ such that Ψ is satisfiable over $\mathbb{N}$ and the linear polynomial $\boldsymbol{c}^\intercal(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$ has a variable in $\boldsymbol{\lambda}$ with strictly negative (resp. positive) coefficient, then an optimal solution minimizing (resp. maximizing) $\boldsymbol{c}^\intercal \boldsymbol{x}$ subject to $\Phi(\boldsymbol{x})$ does not exist;

III. else, an optimal solution does exist, and in particular one with polynomial bit length with respect to $\langle \Phi \rangle$ and $\langle \boldsymbol{c} \rangle$.

Item I. follows directly from the equivalence $\{\boldsymbol{a} \in \mathbb{Z}^d : \boldsymbol{a} \text{ solution ot } \Phi\} = [\![C]\!]$. Let us focus on Item II., which we show for the case of minimization (the case of maximization being analogous). Consider a triple $(\Psi, \boldsymbol{u}, E) \in C$ such that Ψ is satisfiable and the linear polynomial $f(\boldsymbol{\lambda}) \coloneqq \boldsymbol{c}^\intercal(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$ has a variable in $\boldsymbol{\lambda}$ with strictly negative coefficient. Let $\boldsymbol{z}$, $\boldsymbol{y}$ and $\boldsymbol{w}$ be the disjoint families of variable witnessing the fact that $(\Psi, \boldsymbol{u}, E)$ is a gcd-to-div triple, according to the definition of such triples. By Lemma 11, Ψ is increasing for $\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w}$, and from Property 5 of gcd-to-div triples, all variables appearing in $f(\boldsymbol{\lambda})$ with a non-zero coefficient are from $\boldsymbol{y}$. Let $\widehat{y}$ be a variable appearing in f with a negative coefficient, and consider an order $(\prec) \in (\boldsymbol{z} \prec \boldsymbol{y} \prec \boldsymbol{w})$ for which $\widehat{y}$ is the largest of the variables appearing in $\boldsymbol{y}$. Since Ψ is satisfiable over $\mathbb{N}$, it is satisfiable modulo every prime in $\mathbb{P}(\Psi)$, and we can apply Algorithm 1 to compute a solution $\boldsymbol{\nu}$ over $\mathbb{N}$ satisfying the property highlighted in Remark 1: the formula $\Psi[\boldsymbol{\nu}(x) \,/\, x : x \prec \widehat{y}]$ has a solution for infinitely many positive values of $\widehat{y}$. Since $\widehat{y}$ is the largest (for $\prec$) variable appearing in f, and its coefficient in f is negative, we conclude that $\min\{f(\boldsymbol{\lambda}) \in \mathbb{Z} : \boldsymbol{\lambda} \text{ is a solution to } \Psi\}$ is undefined, which in turn implies that an optimal solution minimizing $\boldsymbol{c}^\intercal \boldsymbol{x}$ subject to $\Phi(\boldsymbol{x})$ does not exist.

Lastly, let us consider Item III.. Again we focus on the case of minimization. Below, let $C' \coloneqq \{(\Psi, \boldsymbol{u}, E) \in C : \Psi \text{ is satisfiable over } \mathbb{N}\}$ and note that $\{\boldsymbol{x} \in \mathbb{Z}^d : \Phi(\boldsymbol{x})\} = [\![C']\!]$. As Items I. and II. do not hold, $C' \neq \emptyset$ and every gcd-to-div triple $(\Psi, \boldsymbol{u}, E) \in C'$ is such that the linear polynomial $\boldsymbol{c}^\intercal(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$ only has non-negative coefficients. Since the variables $\boldsymbol{\lambda}$ are interpreted over $\mathbb{N}$, this means that $\ell \coloneqq \min\{\boldsymbol{c}^\intercal \boldsymbol{u} : (\Psi, \boldsymbol{u}, E) \in C'\}$ is a lower bound to the values that $\boldsymbol{c}^\intercal \boldsymbol{x}$ can take when $\boldsymbol{x}$ is a solution to Φ; i.e., the optimal solution exists. Lemmas 10 and 13 ensure that the lower bound ℓ has polynomial bit length with respect to $\langle \Phi \rangle$ and $\langle \boldsymbol{c} \rangle$. We also have an upper bound u to the optimal solution: it suffices to take the minimum of the values $(\boldsymbol{u} + E \cdot \boldsymbol{\lambda})$, where $(\Psi, \boldsymbol{u}, E) \in C'$ and $\boldsymbol{\lambda}$ is the positive integer solution to Ψ computed with Algorithm 1 using the solutions modulo $p \in \mathbb{P}(\Psi)$ of Lemma 5. Again, u has polynomial bit length with respect to $\langle \Phi \rangle$ and $\langle \boldsymbol{c} \rangle$, thanks to Lemmas 4, 10 and 13, and Theorem 4. Item III. then follows by reduction from the feasibility problem of IP-GCD systems: it suffices to find the minimal $v \in [\ell, u]$ such that the IP-GCD system $\Phi_v(\boldsymbol{x}) \coloneqq \Phi(\boldsymbol{x}) \wedge (\boldsymbol{c}^\intercal \boldsymbol{x} \leq v)$ is feasible. Since every $v \in [\ell, u]$ is of polynomial bit length, by Corollary 1 if $\Phi_v(\boldsymbol{x})$ is satisfiable, then it has a solution $\boldsymbol{x} \in \mathbb{Z}^d$ such that $\langle \boldsymbol{x} \rangle \leq \text{poly}(\langle \Phi \rangle, \langle \boldsymbol{c} \rangle)$.

A Lemma 1: proof of Claim 1

In this appendix, we present the technical manipulation yielding Claim 1, hence finishing the proof of Lemma 1. Below, μ and ω stand for the Möbius function and the prime omega function, respectively. Recall that $\mu(n) = (-1)^{\omega(n)}$ and $\omega(n) = \#\mathbb{P}(n)$, for every $n \in \mathbb{Z}_+$.

Proposition 4 (Möbius inversion [7, Theorem 266])**.** *Consider two functions $f, g\colon \mathbb{Z}_+ \to \mathbb{R}$ such that for every $n \in \mathbb{Z}_+$, $f(n) = \sum_{d\in\operatorname{div}(n)} g(d)$. For every $m \in \mathbb{Z}_+$, $g(m) = \sum_{d\in\operatorname{div}(m)} f(d) \cdot \mu(\frac{m}{d})$.*

Proposition 5 (Möbius sums [7, Theorem 263])**.** *For $n \in \mathbb{Z}_+$ greater than 1, $\sum_{s\in\operatorname{div}(n)} \mu(s) = 0$.*

The following lemma tells us what to expect when we truncate the sum of the previous proposition so that it only considers elements with at most ℓ divisors.

Lemma 14. *Let $n, \ell \in \mathbb{N}$ with n square-free. If $\omega(n) > \ell$ then $\sum_{r\in\operatorname{div}(n),\, \omega(r)\le\ell} \mu(r) = (-1)^\ell\binom{\omega(n)-1}{\ell}$.*

Proof. We write LHS (resp. RHS) for the left-hand (resp. right-hand) side of the equivalence in the statement. Note that $\omega(n) > \ell$ implies $n \geq 1$. The proof is by induction on ℓ.

Base case: $\ell = 0$: In this case, LHS $= \mu(1) = 1 = (-1)^0\binom{\omega(n)-1}{0} =$ RHS.

Induction step: $\ell \geq 1$: We have,

$$\begin{aligned}
\text{LHS} &= \sum_{r\in\operatorname{div}(n),\,\omega(r)<\ell} \mu(r) + \sum_{s\in\operatorname{div}(n),\,\omega(r)=\ell} \mu(s) \\
&= (-1)^{\ell-1}\binom{\omega(n)-1}{\ell-1} + \sum_{s\in\operatorname{div}(n),\,\omega(r)=\ell} \mu(s) && \text{by induction hypothesis; recall } \omega(n) > \ell \\
&= (-1)^{\ell-1}\left(\binom{\omega(n)-1}{\ell-1} - \sum_{r\in\operatorname{div}(n),\,\omega(r)=\ell} 1\right) && \text{since } \mu(r) = (-1)^\ell \text{ iff } \omega(r) = \ell \\
&= (-1)^{\ell-1}\left(\binom{\omega(n)-1}{\ell-1} - \binom{\omega(n)}{\ell}\right) && \text{from } n \text{ square-free} \\
&= (-1)^{\ell}\binom{\omega(n)-1}{\ell} = \text{RHS} && \text{Pascal's rule.}
\end{aligned}$$

□

We are now ready to prove Claim 1:

Claim 1. $\displaystyle\sum_{r\in Q(\ell)} \frac{\mu(r)\cdot m(r)}{r} \geq W_m(Q)\left(1 - \left(\frac{e\cdot\alpha}{\ell}\right)^\ell \alpha \cdot e^\alpha\right)$*, with $\alpha := (d+1)^2(2+\ln\ln(\#Q+1))$.*

Let us recall the hypothesis under which this claim must be proved: $\ell \in \mathbb{N}_+$ is odd, $d \geq 1$, Q is a non-empty finite set of primes, $Q(\ell) := \{r \in \operatorname{div}(\Pi Q) : \omega(r) \leq \ell\}$, m is a multiplicative function such that $m(q) \leq q - 1$ and $m(q) \leq d$ on all $q \in Q$, and $W_m(Q) := \prod_{q\in Q}\left(1 - \frac{m(q)}{q}\right)$.

Proof. We start by defining the truncated Möbius function μ_ℓ and its companion function ψ_ℓ:

$$\mu_\ell(x) := \begin{cases} \mu(x) & \text{if } \omega(x) \leq \ell \\ 0 & \text{otherwise} \end{cases} \qquad \text{and} \qquad \psi_\ell(x) := \sum_{r\in\operatorname{div}(x)} \mu_\ell(x).$$

The proof proceeds by performing two term manipulations. In the first one, we use the fact that m is multiplicative, together with properties of the Möbius function (e.g. Proposition 4), to show that

$$\sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r} = W_m(Q) \cdot \left(1 + \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right). \tag{11}$$

In the second manipulation, we look at the sum $\sum_{s \in \mathrm{div}(\Pi Q) \setminus \{1\}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))}$ from the equation above, and (also thanks to Lemma 14) bound it in absolute terms as follows:

$$\left| \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right| \leq \left(\frac{e \cdot \alpha}{\ell} \right)^\ell \cdot \alpha \cdot e^\alpha, \quad \text{where } \alpha \coloneqq (d+1)^2 (2 + \ln\ln(\#Q + 1)). \tag{12}$$

Claim 1 follows directly from Equation (11) and Equation (12). Note that these equations can be used to also establish the upper bound to $\sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r}$ required for the upper bound of Lemma 1.

Manipulation resulting in Equation (11):

$$\begin{aligned}
& \sum_{r \in Q(\ell)} \frac{\mu(r) \cdot m(r)}{r} \\
&= \sum_{r \in \mathrm{div}(\Pi Q)} \frac{\mu_\ell(r) \cdot m(r)}{r} && \text{by def. of } \mu_\ell \\
&= \sum_{r \in \mathrm{div}(\Pi Q)} \frac{\left(\sum_{s \in \mathrm{div}(r)} \psi_\ell(s) \cdot \mu\left(\frac{r}{s}\right)\right) \cdot m(r)}{r} && \text{by Proposition 4} \\
&= \sum_{r \in \mathrm{div}(\Pi Q)} \sum_{s \in \mathrm{div}(r)} \frac{\psi_\ell(s) \cdot \mu\left(\frac{r}{s}\right) \cdot m(r)}{r} \\
&= \sum_{s \in \mathrm{div}(\Pi Q)} \sum_{r \in \mathrm{div}\left(\frac{\Pi Q}{s}\right)} \frac{\psi_\ell(s) \cdot \mu(r) \cdot m(r \cdot s)}{r \cdot s} && \begin{array}{r}\text{invert summations using the} \\ \text{change of variable } r \leftarrow r \cdot s\end{array} \\
&= \sum_{s \in \mathrm{div}(\Pi Q)} \frac{\psi_\ell(s) \cdot m(s)}{s} \cdot \sum_{r \in \mathrm{div}\left(\frac{\Pi Q}{s}\right)} \frac{\mu(r) \cdot m(r)}{r} && \text{multiplicity of } m \\
&= \sum_{s \in \mathrm{div}(\Pi Q)} \frac{\psi_\ell(s) \cdot m(s)}{s} \cdot \prod_{q \in Q \setminus \mathrm{div}(s)} \left(1 + \frac{\mu(q) \cdot m(q)}{q} \right) && \begin{array}{r}\text{multiplicity of } \mu \text{ and } m; \\ \text{factorization thanks to } r \text{ being} \\ \text{square-free, for all } r \in \mathrm{div}\left(\frac{\Pi Q}{s}\right)\end{array} \\
&= \sum_{s \in \mathrm{div}(\Pi Q)} \frac{\psi_\ell(s) \cdot m(s)}{s} \cdot \frac{\prod_{q \in Q} \left(1 - \frac{m(q)}{q} \right)}{\prod_{q \in \mathbb{P}(s)} \left(1 - \frac{m(q)}{q} \right)} && \begin{array}{r}\mu(q) = -1 \text{ for } q \text{ prime} \\ \text{and simple manipulation}\end{array} \\
&= \sum_{s \in \mathrm{div}(\Pi Q)} \frac{\psi_\ell(s) \cdot m(s)}{s} \cdot \frac{W_m(Q)}{W_m(\mathbb{P}(s))} && \text{by def. of } W_m
\end{aligned}$$

$$= W_m(Q) \cdot \sum_{s \in \mathrm{div}(\Pi Q)} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))}$$

$$= W_m(Q) \cdot \left(\sum_{s \in Q(\ell)} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} + \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right) \quad \text{split depending on } \omega(s) \leq \ell, \text{ and by def. of } Q(\ell)$$

$$= W_m(Q) \cdot \left(\sum_{s \in Q(\ell)} \frac{\left(\sum_{r \in \mathrm{div}(s)} \mu(r)\right) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} + \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right) \quad \text{def. of } \psi_\ell$$

$$= W_m(Q) \cdot \left(1 + \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right) \quad \begin{array}{r} \text{in the left summation:} \\ \text{for } s = 1 \text{ the addend is 1,} \\ \text{and for } s > 1 \text{ the addend is 0} \\ \text{by Proposition 5.} \end{array}$$

Manipulation resulting in Equation (12):

$$\left| \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \frac{\psi_\ell(s) \cdot m(s)}{s \cdot W_m(\mathbb{P}(s))} \right| \leq \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) > \ell}} \binom{\omega(s) - 1}{\ell} \cdot \frac{m(s)}{s \cdot W_m(\mathbb{P}(s))} \quad \text{by Lemma 14 and def. of } \psi_\ell$$

$$= \sum_{k=\ell+1}^{\#Q} \left(\binom{k-1}{\ell} \cdot \sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) = k}} \frac{m(s)}{s \cdot W_m(\mathbb{P}(s))} \right) \quad \text{split on the value of } \omega(s).$$

We focus on the summation $\sum_{s \in \mathrm{div}(\Pi Q), \omega(s) = k} \frac{m(s)}{s \cdot W_m(\mathbb{P}(s))}$. Since the function m is multiplicative, and similarly $W_m(A \cup B) = W_m(A) \cdot W_m(B)$ for A, B disjoint finite sets of primes (and $W_m(\emptyset) = 1$ by definition), for $k \geq 1$ we have:

$$\sum_{\substack{s \in \mathrm{div}(\Pi Q) \\ \omega(s) = k}} \frac{m(s)}{s \cdot W_m(\mathbb{P}(s))} = \sum_{q_1 < \dots < q_k \in Q} \left(\prod_{i=1}^{k} \frac{m(q_i)}{q_i \cdot W_m(\{q_i\})} \right) \leq \frac{1}{k!} \sum_{q_1, \dots, q_k \in Q} \left(\prod_{i=1}^{k} \frac{m(q_i)}{q_i \cdot W_m(\{q_i\})} \right)$$

$$= \frac{1}{k!} \left(\sum_{q \in Q} \frac{m(q)}{q \cdot W_m(\{q\})} \right)^k = \frac{1}{k!} \left(\sum_{q \in Q} \frac{m(q)}{q - m(q)} \right)^k.$$

We further analyse the summation $\sum_{q \in Q} \frac{m(q)}{q - m(q)}$. Below, we write Q_{d+1} for the set of the first $\min(\#Q, d+1)$ many primes in Q (recall $d \geq 1$), and denote by p_i the i-th prime.

$$\sum_{q \in Q} \frac{m(q)}{q - m(q)} = \sum_{q \in Q_{d+1}} \frac{m(q)}{q - m(q)} + \sum_{q \in Q \setminus Q_{d+1}} \frac{m(q)}{q - m(q)}$$

$$\leq \sum_{q \in Q_{d+1}} d + \sum_{q \in Q \setminus Q_{d+1}} \frac{m(q)}{q - m(q)} \quad \begin{array}{r} \text{since } m(q) \leq d \\ \text{and } q - m(q) \geq 1 \end{array}$$

$$
\begin{aligned}
&\le d\cdot(d+1)+\sum_{q\in Q\setminus Q_{d+1}}\frac{d}{q-d} && m(q)\le d<q,\text{ for all } q\in Q\setminus Q_{d+1}\\
&\le d\cdot(d+1)+\sum_{i=d+2}^{\#Q}\frac{d}{p_i-d} && \text{def. of } Q\setminus Q_{d+1} \text{ and } p_i>d \text{ for } i\ge d+2\\
&\le d\cdot(d+1)+d\cdot\sum_{i=d+2}^{\#Q}\frac{1}{(i\ln i)-d} && p_i\ge i\ln i\ [18] \text{ and } i\ln i>d \text{ for } i\ge d+2\\
&\le d\cdot(d+1)+d\cdot(d+1)\sum_{i=d+2}^{\#Q}\frac{1}{i\ln i} && \text{since } \frac{1}{x\ln x-y}\le\frac{y+1}{x\ln x} \text{ for all } x\ge 3 \text{ and } 0\le y\le x-1\\
&\le d\cdot(d+1)\cdot\Big(1+\sum_{i=3}^{\#Q}\frac{1}{i\ln i}\Big)\\
&\le d\cdot(d+1)\cdot\Big(1+\int_2^{\#Q+1}\frac{1}{x\ln x}\mathrm{d}x\Big) && \text{Riemann over-approximation note: } \#Q+1\ge 2\\
&\le d\cdot(d+1)\cdot(1+\ln\ln(\#Q+1)-\ln\ln 2)\\
&\le (d+1)^2(2+\ln\ln(\#Q+1)) \ = \ \alpha.
\end{aligned}
$$

We combine this bound with the previous two to obtain complete the proof of Equation (12):

$$
\begin{aligned}
\left|\sum_{\substack{s\in\mathrm{div}(\Pi Q)\\ \omega(s)>\ell}}\frac{\psi_\ell(s)\cdot m(s)}{s\cdot W_m(\mathbb{P}(s))}\right| &\le \sum_{k=\ell+1}^{\#Q}\left(\binom{k-1}{\ell}\cdot\frac{1}{k!}\cdot\alpha^k\right)\\
&= \sum_{j=0}^{\#Q-\ell-1}\left(\binom{\ell+j}{\ell}\cdot\frac{1}{(\ell+1+j)!}\cdot\alpha^{\ell+1+j}\right) && \text{change of variable } k\leftarrow \ell+1+j\\
&= \sum_{j=0}^{\#Q-\ell-1}\left(\frac{(\ell+j)!}{\ell!\cdot j!\cdot(\ell+1+j)!}\cdot\alpha^{\ell+1+j}\right)\\
&\le \frac{\alpha^{\ell+1}}{\ell!}\cdot\sum_{j=0}^{\infty}\frac{\alpha^j}{j!} && \text{note: all terms in the summation are non-negative}\\
&\le \frac{\alpha^{\ell+1}}{\ell!}\cdot e^\alpha && \text{def. of } e^x \text{ as a series i.e., } e^x=\textstyle\sum_{i=0}^\infty\frac{x^i}{i!}\\
&\le \left(\frac{e\cdot\alpha}{\ell}\right)^\ell\cdot\alpha\cdot e^\alpha && \text{from } x!\ge\frac{x^x}{e^x}.
\end{aligned}
$$

1109 This completes the proof of Claim 1. □

1110 B Theorem 3: proofs of Claim 2 and Claim 3

1111 The mathematical objects appearing in the statements of the two claims below are defined in the
1112 proof of Theorem 3 and the statement of Lemma 1; see Section 2.

1113 **Claim 2.** $\frac{\#A}{r}-1\le\#(A\cap S_{\alpha,r})\le\frac{\#A}{r}+1.$

Proof. Recall that $A = [k, k+z] \cap S_M$, and so $A \cap S_{\alpha,r} = [k, k+z] \cap S_M \cap S_{\alpha,r}$. Since that elements in $M \cup Q$ are pairwise coprime and $M \cap Q = \emptyset$, we can apply the CRT and conclude that $S_M \cap S_{\alpha,r}$ is an arithmetic progression with period $r \cdot \Pi M$. Let u be the largest element of $S_M \cap S_{\alpha,r}$ that is strictly smaller than k. By definition of u and from the fact that $S_M \cap S_{\alpha,r}$ has period $r \cdot \Pi M$, we get $\#(A \cap S_{\alpha,r}) = \left\lfloor \frac{k+z-u}{r \cdot \Pi M} \right\rfloor$. Similarly, because S_M is periodic in ΠM, $\left\lfloor \frac{k+z-u}{\Pi M} \right\rfloor$ is over counting $\#A$ by at most $r-1$, i.e., there is $\tau_{\alpha,r} \in [0, r-1]$ such that $\#A = \left\lfloor \frac{k+z-u}{\Pi M} \right\rfloor - \tau_{\alpha,r}$. Since $\left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{\lfloor a \rfloor}{b} \right\rfloor$ for every $a \in \mathbb{R}$ and $b \in \mathbb{Z}_+$, we get $\#(A \cap S_{\alpha,r}) = \left\lfloor \frac{1}{r} \cdot (\#A + \tau_{\alpha,r}) \right\rfloor$. With a simple manipulation using $\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \leq \lfloor a \rfloor + \lfloor b \rfloor + 1$ and $\left\lfloor \frac{\tau_{\alpha,r}}{r} \right\rfloor = 0$, we derive $\frac{\#A}{r} - 1 \leq \#(A \cap S_{\alpha,r}) \leq \frac{\#A}{r} + 1$. $\square$

Claim 3. $W_m(Q)^{-1} \leq (d+1)^{10d} \ln(\#Q+1)^{3d}$.

Proof. Let Q_d be the set containing the $\min(\#Q, d)$ smallest primes in Q. Recall that by definition $m(q) \leq d \leq q-1$ for every $q \in Q$. We have,

$$W_m(Q)^{-1} = \prod_{q \in Q} \frac{q}{q - m(q)} \;\leq \prod_{q \in Q} \frac{q}{q-d} \;\leq\; \prod_{q \in Q_d} \frac{q}{q-d} \cdot \prod_{q \in Q \setminus Q_d} \frac{q}{q-d} \;\leq\; (d+1)^d \cdot \prod_{q \in Q \setminus Q_d} \frac{q}{q-d},$$

where the last inequality holds because $\frac{x}{x-c} \leq c+1$ for every $x \geq c+1$ and $c \in \mathbb{Z}_+$. Below, let us denote by p_i the i-th prime. We further inspect the product $\prod_{q \in Q \setminus Q_d} \frac{q}{q-d}$:

$$\begin{aligned}
&\prod_{q \in Q \setminus Q_d} \frac{q}{q-d} \leq \prod_{i=d+1}^{\#Q} \frac{p_i}{p_i - d} \leq \prod_{i=d+1}^{\#Q} \frac{i \cdot \ln i}{i \cdot \ln i - d} && p_i \geq i \cdot \ln i \text{ for all } i \in \mathbb{Z}_+, \text{ see [18];} \\
& && x \mapsto \frac{x}{x-d} \text{ decreasing for } x > 1 \\
&\leq \exp\left(\sum_{i=d+1}^{\#Q} \ln\left(\frac{i \cdot \ln i}{i \cdot \ln i - d} \right) \right) = \exp\left(- \sum_{i=d+1}^{\#Q} \ln\left(1 - \frac{d}{i \cdot \ln i}\right) \right) \\
&\leq \exp\left(\sum_{i=d+1}^{\#Q} \frac{3 \cdot d}{i \cdot \ln i} \right) \leq \exp\left(\sum_{i=2}^{\#Q} \frac{3 \cdot d}{i \cdot \ln i} \right) && \text{first term from } \ln\left(1 - \frac{1}{x}\right) \geq -\frac{3}{x} \text{ for all } x \geq \ln 3; \\
& && \text{for corner case } d = 1 \text{ and } i = 2, \text{ note } 2\ln 2 > \ln 3 \\
&\leq \exp\left(\frac{3 \cdot d}{2 \cdot \ln 2} + \sum_{i=3}^{\#Q} \frac{3 \cdot d}{i \cdot \ln i} \right) \leq \exp\left(\frac{3 \cdot d}{2 \cdot \ln 2} + \int_2^{\#Q+1} \frac{3 \cdot d}{x \ln x} \mathrm{d}x \right) && \text{Riemann over-approximation} \\
& && \text{note: } \#Q + 1 \geq 2 \\
&\leq \exp\left(\frac{3 \cdot d}{2 \cdot \ln 2} + 3 \cdot d \cdot \big(\ln\ln(\#Q+1) - \ln\ln 2 \big) \right) \leq \exp\big(3 \cdot d \cdot \big(2 + \ln\ln(\#Q+1)\big)\big) .
\end{aligned}$$

We plug this bound on the afore-derived bound for $W_m(Q)^{-1}$ to complete the proof of Claim 3:

$$\begin{aligned}
W_m(Q)^{-1} &\leq\; (d+1)^d \exp\big(3 \cdot d \cdot \big(2 + \ln\ln(\#Q+1)\big)\big) \;\leq\; (d+1)^d \cdot e^{6 \cdot d} \ln(\#Q+1)^{3 \cdot d} \\
&\leq\; (d+1)^d \cdot 2^{9 \cdot d} \ln(\#Q+1)^{3 \cdot d} \;\leq\; (d+1)^{10 \cdot d} \ln(\#Q+1)^{3 \cdot d}.
\end{aligned}$$

$\square$

C Algorithms related to the elimination property

In this appendix we establish Lemma 6 and Lemma 7. Proving these lemmas require the standard notion of kernel and Hermite normal form of a matrix, which we now recall for completeness. Consider a matrix $A \in \mathbb{Z}^{n \times d}$. The *kernel* of A is the vector space $\ker(A) \coloneqq \{\boldsymbol{v} \in \mathbb{Z}^d : A \cdot \boldsymbol{v} = \boldsymbol{0}\}$. We represent *bases* of $\ker(A)$ as matrices $K \in \mathbb{Z}^{d \times (d-r)}$, where r is the rank of A and $\ker(A) = \{K \cdot \boldsymbol{v} : \boldsymbol{v} \in \mathbb{Z}^{d-r}\}$. A matrix $H \in \mathbb{Z}^{n \times d}$ is said to be the *column-style Hermite normal form* of A (*HNF*, in short) if there is a square unimodular matrix $U \in \mathbb{Z}^{d \times d}$ such that $H = A \cdot U$ and

1. H is lower triangular,

2. the *pivot* (i.e., the first non-zero entry in a column, from the top) of a non-zero column is positive and it is strictly below the pivot of the column before it, and

3. elements to the right of pivots are 0 and elements to the left are non-negative and smaller than the pivot.

Recall that U being unimodular means that it is invertible over the integers.

Given a vector $\boldsymbol{v}$, we write $\boldsymbol{v}[i]$ for the i-th entry of $\boldsymbol{v}$, starting at $i = 1$. Similarly, for a matrix A, we write $A[i]$ for its i-th row, again starting at $i = 1$.

Proposition 6 ([19, Section 4.2]). *The HNF H of a matrix $A \in \mathbb{Z}^{n \times d}$ always exits, it is unique, and A and H generate the same lattice, i.e., $\{A \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{Z}^d\} = \{H \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{Z}^d\}$.*

The following proposition refers to the LLL-based algorithm for the HNF in [8]. A basis for the integer kernel can be retrieved from the HNF together with the associated unimodular matrix.

Proposition 7 ([24]). *There is a* PTIME *algorithm computing a basis K of the integer kernel and the HNF H of an input matrix $A \in \mathbb{Z}^{n \times d}$. The algorithm yields $\|K\|, \|H\| \leq (n \cdot \|A\| + 1)^{O(n)}$.*

Note that we can also upper bound the GCDs of the rows of the integer kernel K in terms of the rank of A by appealing to Proposition 3.

Corollary 2. *Consider a basis K of the integer kernel of a matrix $A \in \mathbb{Z}^{n \times d}$. Let $r \coloneqq \mathrm{rank}(A)$. For every $i \in [1, d]$, $\|\gcd(K[i])\| \leq (d + 1) \cdot (r \cdot \max(2, \|A\|))^r$.*

C.1 Computing a set spanning the divisibility module

Lemma 6. *There is a polynomial-time algorithm that, given a system $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and a primitive polynomial f, computes $c_1, \dots, c_m \in \mathbb{N}^m$ such that $\{f,\, c_1 \cdot g_1,\, \dots,\, c_m \cdot g_m\}$ spans $\mathrm{M}_f(\Phi)$ and $c_i \leq ((m + 3) \cdot (\|\Phi\| + 2))^{(m+3)^3}$ for all $1 \leq i \leq m$.*

This lemma follows from the forthcoming Proposition 8 and Proposition 9.

For the whole section, let $\Phi \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and f be a primitive polynomial. As already explained in Section 3, the algorithm Lemma 6 refers to performs a fix-point computation where, at the ℓ-th iteration, the values contained in $\boldsymbol{v}$ characterize a spanning set of a particular submodule $\mathrm{M}_f^\ell(\Phi)$ of $\mathrm{M}_f(\Phi)$. More precisely, we define $\mathrm{M}_f^0(\Phi) \subseteq \mathrm{M}_f^1(\Phi) \subseteq \dots \subseteq \mathrm{M}_f^\ell(\Phi) \subseteq \dots$ to be the sequence of sets given by

1. $\mathrm{M}_f^0(\Phi) \coloneqq \mathbb{Z}f$, and

2. for $\ell \in \mathbb{N}$, $\mathrm{M}_f^{\ell+1}(\Phi) \coloneqq \mathrm{M}_f^\ell(\Phi) + \left\{\sum_{j=1}^m a_j \cdot g_j : \text{ for all } i \in [1, m],\, a_i \in \mathbb{Z} \text{ and } a_i \cdot f_i \in \mathrm{M}_f^\ell(\Phi)\right\}$.

Let $\ell \in \mathbb{N}$. Note that, by definition, $\mathrm{M}_f^\ell(\Phi)$ is a $\mathbb{Z}$-module and moreover if $\mathbb{Z}f_i \cap \mathrm{M}_f^\ell(\Phi) = \{0\}$ for some $i \in [1, m]$, then a_i in the definition of $\mathrm{M}_f^{\ell+1}(\Phi)$ equals 0. We define the *canonical representation* of $\mathrm{M}_f^\ell(\Phi)$ as the vector $(v_1, \dots, v_m) \in \mathbb{N}^m$ such that for every $i \in [1, m]$,

- if $\ell = 0$ then $v_i \coloneqq 0$,

- if $\ell \geq 1$ then $v_i \coloneqq \gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i \in \mathrm{M}_f^{\ell-1}(\Phi)\}$.

Lemma 16 shows that this vector represents a spanning set of $\mathrm{M}^{\ell}_{f}(\Phi)$, but first we need an auxiliary lemma.

Lemma 15. *Let $\ell \in \mathbb{N}$. Let $(v_1, \dots, v_m)$ and $(v'_1, \dots, v'_m)$ be the canonical representations of* $\mathrm{M}^{\ell}_{f}(\Phi)$ *and* $\mathrm{M}^{\ell+1}_{f}(\Phi)$*, respectively. For every $i \in [1, m]$, $v_i = v'_i = 0$ or v'_i divides v_i (so, $v'_i \neq 0$ if $v_i \neq 0$).*

Proof. Let $i \in [1, m]$. If $v_i = 0$ then either v'_i is 0 or it divides v_i, hence the statement is trivially satisfied for that particular i. Suppose that $v_i \neq 0$. By definition of canonical representation, $\ell \geq 1$ and $v_i \cdot f_i \in M^{\ell-1}_{f}(\Phi)$. By definition of $\mathrm{M}^{\ell}_{f}(\Phi)$, we conclude that $v_i \cdot f_i \in M^{\ell}_{f}(\Phi)$. By definition of canonical representation $v'_i = \gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i \in \mathrm{M}^{\ell}_{f}(\Phi)\}$, and therefore v'_i divides v_i. □

Lemma 16. *Let $\ell \in \mathbb{N}$ and let $(v_1, \dots, v_m) \in \mathbb{N}^m$ be the canonical representation of* $\mathrm{M}^{\ell}_{f}(\Phi)$*. Then, the set of linear polynomials $\{f,\ v_1 \cdot g_1,\ \dots,\ v_m \cdot g_m\}$ spans $M^{\ell}_{f}(\Phi)$.*

Proof. The statement follows by induction on $\ell \in \mathbb{N}$.

base case $\ell = 0$. From $\mathrm{M}^{0}_{f}(\Phi) = \mathbb{Z}f$ we have $(v_1, \dots, v_m) = (0, \dots, 0)$ and $\{f\}$ spans $M^{0}_{f}(\Phi)$.

induction step $\ell \geq 1$. From the induction hypothesis, $\{f,\ v^*_1 \cdot g_1,\ \dots,\ v^*_m \cdot g_m\}$ spans $M^{\ell-1}_{f}(\Phi)$; with $(v^*_1, \dots, v^*_m)$ being the canonical representation of $M^{\ell-1}_{f}(\Phi)$. We consider the two inclusions of the equivalence $\mathbb{Z}f + \mathbb{Z}(v_1 \cdot g_1) + \dots + \mathbb{Z}(v_m \cdot g_m) = M^{\ell}_{f}(\Phi)$.

($\subseteq$) : This direction follows directly by definition of $M^{\ell}_{f}(\Phi)$.

($\supseteq$) : Let $h \in \mathrm{M}^{\ell}_{f}(\Phi)$. By definition, $h = h_1 + h_2$ where $h_1 \in \mathbb{Z}f + \mathbb{Z}(v^*_1 \cdot g_1) + \dots + \mathbb{Z}(v^*_m \cdot g_m)$ and $h_2 = \sum_{i=1}^{m} a_i \cdot g_i \in \mathrm{M}^{\ell}_{f}(\Phi)$ satisfying $a_i \cdot f_i \in \mathrm{M}^{\ell-1}_{f}(\Phi)$ for every $i \in [1, m]$. By Lemma 15 $\mathbb{Z}(v^*_i \cdot g_i) \subseteq \mathbb{Z}(v_i \cdot g_i)$ and therefore $h_1 \in \mathbb{Z}f + \mathbb{Z}(v_1 \cdot g_1) + \dots + \mathbb{Z}(v_m \cdot g_m)$. By definition $v_i = \gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i \in \mathrm{M}^{\ell-1}_{f}(\Phi)\}$ and thus $v_i \mid a_i$. So, $h \in \mathbb{Z}f + \mathbb{Z}(v_1 \cdot g_1) + \dots + \mathbb{Z}(v_m \cdot g_m)$. □

Lemma 17. *(A) For every $\ell \in \mathbb{N}$, $\mathrm{M}^{\ell}_{f} \subseteq \mathrm{M}^{\ell+1}_{f} \subseteq \mathrm{M}_{f}(\Phi)$.*

(B) There is $\ell \in \mathbb{N}$ such that $\mathrm{M}^{\ell}_{f}(\Phi) = \mathrm{M}^{\ell+1}_{f}(\Phi)$.

(C) For every $\ell \in \mathbb{N}$, if $\mathrm{M}^{\ell}_{f}(\Phi) = \mathrm{M}^{\ell+1}_{f}(\Phi)$ then $\mathrm{M}^{\ell}_{f}(\Phi) = \mathrm{M}_{f}(\Phi)$.

Proof. Proof of (A): By definition, $\mathrm{M}^{\ell}_{f} \subseteq \mathrm{M}^{\ell+1}_{f}$. An induction on $\ell \in \mathbb{N}$ shows $M^{\ell}_{f}(\Phi) \subseteq \mathrm{M}_{f}(\Phi)$:

base case $\ell = 0$: By definition of $\mathrm{M}^{\ell}_{f}(\Phi)$ and of divisibility module, $M^{0}_{f}(\Phi) = \mathbb{Z}f \subseteq \mathrm{M}_{f}(\Phi)$.

induction case $\ell \geq 1$: From the induction hypothesis, $M^{\ell-1}_{f}(\Phi) \subseteq \mathrm{M}_{f}(\Phi)$. By definition, $M^{\ell}_{f}(\Phi)$ is defined from $M^{\ell-1}_{f}(\Phi)$ by taking linear combinations of elements in $M^{\ell-1}_{f}(\Phi)$ together with elements $b \cdot h$ such that $b \cdot g \in M^{\ell-1}_{f}(\Phi)$ and $g \mid h$ is a divisibility of Φ. From the definition of divisibility module, $\mathrm{M}_{f}(\Phi)$ is closed under such combinations, since for every $b \cdot g \in \mathrm{M}_{f}(\Phi)$ and $g \mid h$ divisibility of Φ, $b \cdot h \in \mathrm{M}_{f}(\Phi)$ (see Property (iii) in the def. of divisibility module). From $M^{\ell-1}_{f}(\Phi) \subseteq \mathrm{M}_{f}(\Phi)$ we then conclude that $M^{\ell}_{f}(\Phi) \subseteq \mathrm{M}_{f}(\Phi)$.

Proof of (B): This statement follows from Lemma 15. Indeed, for a given $\ell \in \mathbb{N}$, consider the canonical representations $(v_1, \dots, v_m)$ and $(v'_1, \dots, v'_m)$ of $\mathrm{M}^{\ell}_{f}(\Phi)$ and $\mathrm{M}^{\ell+1}_{f}(\Phi)$, respectively. By Lemma 15, if $\mathrm{M}^{\ell}_{f}(\Phi) \neq \mathrm{M}^{\ell+1}_{f}(\Phi)$ then one of the following holds:

1. there is $i \in [1, m]$ such that $v_i = 0$ and $v'_i \neq 0$, or
2. there is $i \in [1, m]$ such that $v_i \neq 0$, $v'_i \neq v_i$ and v'_i divides v_i.

Algorithm 4 Computes a set spanning a divisibility module

Input: A system of divisibility constraints $\Phi(\boldsymbol{x}) = \bigwedge_{i=1}^{m} f_i(\boldsymbol{x}) \mid g_i(\boldsymbol{x})$ and a primitive polynomial f.

Output: A tuple $(c_1, \dots, c_m) \in \mathbb{N}^m$ such that $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ spans $\mathrm{M}_f(\Phi)$.

1: $\boldsymbol{v} \coloneqq (0, \dots, 0) \in \mathbb{N}^m$
2: **while true do**
3: $\quad \boldsymbol{u} \coloneqq \boldsymbol{v}$
4: $\quad$ **for** i **in** $[1, m]$ **do**
5: $\quad\quad F_i \coloneqq \{-f_i, f, \boldsymbol{u}[1] \cdot g_1, \dots, \boldsymbol{u}[m] \cdot g_m\}$
6: $\quad\quad K_i \coloneqq$ basis of the integer kernel of the matrix representing F_i
7: $\quad\quad \boldsymbol{v}[i] \leftarrow \gcd(\text{row of } K_i \text{ corresponding to } -f_i)$
8: $\quad$ **if** $\boldsymbol{v} = \boldsymbol{u}$ **then return** $\boldsymbol{v}$

Again from Lemma 15, for every $j \in [1, m]$, if $v_j \neq 0$ then v_j' divides v_j. This implies that both Items (1) and (2) cannot occur infinitely often, and therefore $\mathrm{M}_f^r(\Phi) = \mathrm{M}_f^{r+1}(\Phi)$ for some $r \in \mathbb{N}$.

Proof of (C): From Part (A), $\mathrm{M}_f^\ell(\Phi) \subseteq \mathrm{M}_f(\Phi)$. We show that $\mathrm{M}_f^\ell(\Phi)$ satisfies the Properties (i)–(iii) of divisibility modules. Then, $\mathrm{M}_f(\Phi) \subseteq \mathrm{M}_f^\ell(\Phi)$ follows from the minimality condition required by these modules. Properties (i) and (ii) are trivially satisfied. To establish Property (iii), consider $b \cdot g \in \mathrm{M}_f^\ell(\Phi)$ and a divisibility $g \mid h$ of Φ. By definition $b \cdot h \in \mathrm{M}_f^{\ell+1}(\Phi)$, and from $\mathrm{M}_f^\ell = \mathrm{M}_f^{\ell+1}(\Phi)$ we get $b \cdot h \in \mathrm{M}_f^\ell(\Phi)$. Therefore, $\mathrm{M}_f^\ell(\Phi)$ satisfies Property (iii). $\square$

In view of Lemmas 16 and 17, the algorithm required by Lemma 6 presents itself: it suffices to iteratively compute canonical representations of every $\mathrm{M}_f^\ell(\Phi)$ until reaching a fix-point. Algorithm 4 performs this computation. In a nutshell, during the ℓ-th iteration ($\ell \geq 1$) of the **while** loop of line 2, the variable $\boldsymbol{u}$ contains the canonical representation of $\mathrm{M}_f^{\ell-1}(\Phi)$, and the algorithm updates the vector $\boldsymbol{v}$ with the canonical representation of $\mathrm{M}_f^\ell(\Phi)$. To update the value $\boldsymbol{v}[i]$ associated to g_i the algorithm needs to compute $\gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i \in \mathrm{M}_f^{\ell-1}(\Phi)\}$ (line 7). This is done by finding a finite representation for all the scalars λ, which is given by those entries corresponding to $-f_i$ in a basis of the integer kernel of the matrix for the set F_i defined in line 5. As explained in Section 3.1, a set of polynomials $F \coloneqq \{h_1, \dots, h_\ell\}$ in variables $x_1 \prec \dots \prec x_d$ (where $\prec$ is an arbitrary order) can be represented as the matrix $A \in \mathbb{Z}^{(d+1) \times \ell}$ in which each column $(a_d, \dots, a_1, c)$ contains the coefficients and the constant of a distinct element h of F, with a_i being the coefficient of x_i for $i \in [1, d]$, and c being the constant of h. This matrix is unique up-to permutation of columns.

It might not be clear for the moment whether Algorithm 4 runs in PTIME: in each iteration, the integer kernel computation done in line 6 might a priori increase the bit length of the entries in the canonical representation by a polynomial factor, yielding entries of exponential bit length after polynomially many iterations – an effect similar to naïve implementations of Gaussian elimination or kernel computations via suboptimal algorithms for the Hermite normal form of a matrix. We show later that our worries are unjustified, as the GCD computed in line 7 prevents this blow-up. For the moment, let us formally argue on the correctness of Algorithm 4.

Proposition 8. *Algorithm 4 respects its specification.*

Proof. We write $\boldsymbol{u}_\ell$ for the value that the tuple $\boldsymbol{u}$ declared in line 3 of Algorithm 4 takes during the $(\ell + 1)$-th iterations of the **while** loop of line 2, with $\ell \in \mathbb{N}$ and assuming that the **while** loop is iterated at least $\ell + 1$ times. We show the following claim:

Claim 9. *For every $\ell \in \mathbb{N}$, the tuple $\boldsymbol{u}_\ell$ is the canonical representation of $\mathrm{M}_f^\ell(\Phi)$.*

Since Algorithm 4 terminates when $\boldsymbol{u}_{\ell-1}$ is found to be equal to $\boldsymbol{u}_\ell$ for some $\ell \geq 1$, its correctness follows directly from Lemma 16 and Lemma 17. The proof of this claim is by induction on ℓ.

base case. We have $\boldsymbol{u}_0 = (0, \dots, 0) \in \mathbb{N}^m$, which is the canonical representation of $\mathrm{M}_f^0(\Phi)$.

induction step. By induction hypothesis, let us assume that $\boldsymbol{u}_\ell = (v_1, \dots, v_m)$ is the canonical representation of $\mathrm{M}_f^\ell(\Phi)$. We show that when exiting the **for** loop of line 4, for every $i \in [1, m]$, $\boldsymbol{v}[i]$ equals $v_i' \coloneqq \gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i \in \mathrm{M}_f^\ell(\Phi)\}$. Thanks to the declaration of line 3, this implies that $\boldsymbol{u}_{\ell+1}$ is the canonical representation of $\mathrm{M}_f^{\ell+1}(\Phi)$. Since $\boldsymbol{u}_\ell = (v_1, \dots, v_m)$ is the canonical representation of $\mathrm{M}_f^\ell(\Phi)$, by Lemma 16 we have $\mathrm{M}_f^\ell(\Phi) = \mathbb{Z}f + \mathbb{Z}(v_1 \cdot g_1) + \dots + \mathbb{Z}(v_m \cdot g_m)$. Therefore, $v_i' = \gcd\{\lambda \in \mathbb{N} : \lambda \cdot f_i = \mu_0 \cdot f + \sum_{i=1}^m \mu_i \cdot (v_i \cdot g_i) \text{ for some } \mu_0, \dots, \mu_m \in \mathbb{Z}\}$. The set of tuples $(\lambda, \mu_0, \dots, \mu_m) \in \mathbb{Z}^{m+2}$ such that $\lambda \cdot f_i = \mu_0 \cdot f + \sum_{i=1}^m \mu_i \cdot (v_i \cdot g_i)$ corresponds to the solutions to the system of equations $A \cdot (\lambda, \mu_0, \dots, \mu_m) = \boldsymbol{0}$ over the integers, where A is the matrix representing the set $\{-f_i,\ f,\ v_i \cdot g_1,\ \dots,\ \boldsymbol{v}_m \cdot g_m\}$, i.e., F_i in line 5. This set corresponds to $\ker(A)$, and so can be finitely represented with an integer kernel basis, i.e., K_i in line 6. Computing v_i' only requires to compute the GCD of the row of K_i corresponding to the variable λ of $-f_i$. This is exactly how $\boldsymbol{v}[i]$ is defined in line 7. $\square$

We move to the runtime analysis of Algorithm 4. We need the following lemma studying the growth of the GCDs of the rows of bases K of $\ker(A)$ when columns of A are scaled by positive integers. In the lemma below, $\mathrm{diag}(c_1, \dots, c_d)$ stands for the $d \times d$ diagonal matrix having $c_1, \dots, c_d$ in the main diagonal.

Lemma 18. *Consider a matrix $A \in \mathbb{Z}^{n \times d}$ of rank r, integers $c_1, \dots, c_d > 0$, and let $K, K' \in \mathbb{Z}^{d \times (d-r)}$ be bases of the integer kernels of A and $A' \coloneqq A \cdot \mathrm{diag}(c_1, \dots, c_d)$, respectively. For every $i \in [1, d]$,*

1. *if $\gcd(K[i]) = 0$ then $\gcd(K'[i]) = 0$, and*
2. *if $\gcd(K[i]) > 0$ then $\gcd(K'[i]) \neq 0$ and $\gcd(K'[i])$ divides $\mathrm{lcm}(c_1, \dots, c_d) \cdot \gcd(K[i])$.*

Proof. Note that A' is the matrix obtained from A by scaling the j-th column of A by c_j ($j \in [1, d]$). Let $i \in [1, d]$ and $(M, J) \in \{(A, K), (A', K')\}$. By definition of kernel, $\{J \cdot \boldsymbol{\lambda} : \boldsymbol{\lambda} \in \mathbb{Z}^m\} = \{\boldsymbol{x} \in \mathbb{Z}^d : M \cdot \boldsymbol{x} = \boldsymbol{0}\}$. This fact has three direct consequences:

(A) if $\gcd(J[i]) = 0$, then no vector $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ satisfies both $x_i \neq 0$ and $M \cdot \boldsymbol{x} = 0$,

(B) if $\gcd(J[i]) > 0$, then there is $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ such that $x_i = \gcd(J[i])$ and $M \cdot \boldsymbol{x} = 0$,

(C) if $\gcd(J[i]) > 0$, then for every $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ satisfying $M \cdot \boldsymbol{x} = 0$ we have $\gcd(J[i]) \mid x_i$.

Items 1 and 2 in the statement of the lemma are derived from these three properties.

Proof of (1): By contrapositive, assume that $\gcd(K'[i]) \neq 0$. Hence, $\gcd(K'[i]) > 0$ and by Item (B) there is $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ such that $x_i = \gcd(K'[i])$ and $A' \cdot \boldsymbol{x} = \boldsymbol{0}$. Let $\boldsymbol{y} \coloneqq (c_1 \cdot x_1, \dots, c_d \cdot x_d)$. We have $A \cdot \boldsymbol{y} = A \cdot (\mathrm{diag}(c_1, \dots, c_d) \cdot \boldsymbol{x}) = (A \cdot \mathrm{diag}(c_1, \dots, c_d)) \cdot \boldsymbol{x} = A' \cdot \boldsymbol{x} = \boldsymbol{0}$. Since $c_i > 0$ we have $c_i \cdot x_i \neq 0$, which together with $A \cdot \boldsymbol{y} = \boldsymbol{0}$ implies $\gcd(K[i]) \neq 0$ by Item (A).

Proof of (2): Suppose $\gcd(K[i]) > 0$. By Item (B), there is $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ with $A \cdot \boldsymbol{x} = \boldsymbol{0}$

and $x_i = \gcd(K[i])$. Define $C \coloneqq \operatorname{lcm}(c_1, \dots, c_d)$ and $\boldsymbol{y} \coloneqq (\frac{C}{c_1} \cdot x_1, \dots, \frac{C}{c_d} \cdot x_d)$. Note that $\boldsymbol{y} \in \mathbb{Z}^d$ is well-defined, since $c_1, \dots, c_d > 0$. Moreover, $\frac{C}{c_i} \cdot x_i = \frac{C}{c_i} \cdot \gcd(K[i]) > 0$. We have,

$$\begin{aligned} A' \cdot \boldsymbol{y} = A' \cdot (\operatorname{diag}(\tfrac{C}{c_1}, \dots, \tfrac{C}{c_d}) \cdot \boldsymbol{x}) \;&=\; (A \cdot \operatorname{diag}(c_1, \dots, c_d)) \cdot (\operatorname{diag}(\tfrac{C}{c_1}, \dots, \tfrac{C}{c_d}) \cdot \boldsymbol{x}) \\ = A \cdot (\operatorname{diag}(c_1, \dots, c_d) \cdot \operatorname{diag}(\tfrac{C}{c_1}, \dots, \tfrac{C}{c_d})) \cdot \boldsymbol{x} \;&=\; C \cdot A \cdot \boldsymbol{x} \;=\; \boldsymbol{0}. \end{aligned}$$

Then, by Item (A), $\gcd(K'[i]) > 0$, which in turn implies that $\gcd(K'[i]) \mid \frac{C}{c_i} \cdot x_i$, directly from Item (C). Therefore, $\gcd(K'[i])$ divides $\operatorname{lcm}(c_1, \dots, c_d) \cdot \gcd(K[i])$. $\square$

We are now ready to discuss the runtime of Algorithm 4.

Proposition 9. *Algorithm 4 runs in* PTIME*, and on an input* (Φ, f) *such that* $\Phi = \bigwedge_{i=1}^m f_i \mid g_i$ *it returns a vector* $\boldsymbol{v}$ *satisfying* $\|\boldsymbol{v}\| \leq ((m+3) \cdot (\|\Phi\| + 2))^{(m+3)^3}$.

Proof. As done in the proof of Proposition 8, let $\boldsymbol{u}_\ell \in \mathbb{Z}^m$ be the value that the tuple $\boldsymbol{u}$ declared in line 3 takes during the $(\ell+1)$-th iteration of the **while** of line 2, with $\ell \in \mathbb{N}$ and assuming that the **while** loop is iterated at least $\ell + 1$ times. Similarly, given $j \in [1, m]$, let $F_{\ell,j}$ and $K_{\ell,j}$ be the set of polynomial and matrix declared in lines 5 and 6, respectively, during the $(\ell+1)$-th iteration of the **while** loop and at the end of the iteration of the **for** loop of line 5 where the index variable i takes value j. Lastly, following the code in line 7, we define $v_{\ell,j} \coloneqq \gcd(\text{row of } K_{\ell,j} \text{ corresponding to } -f_j)$. A few preliminary remarks that follow directly form the definitions above:

For the runtime of the algorithm, first consider the case where $\mathrm{M}_f(\Phi) \cap \mathbb{Z}f_j = \{0\}$ for every $j \in [1, m]$, which implies $\mathrm{M}_f(\Phi) = \mathbb{Z}f$, by definition of divisibility module. Focus on the first execution of the body of the **while** loop. Since $\boldsymbol{u}_0 = (0, \dots, 0)$, for every $j \in [1, m]$, $F_{0,j} = \{-f_j,\, f\}$. Since $\mathrm{M}_f(\Phi) \cap \mathbb{Z}f_j = \{0\}$, the row of $K_{0,j}$ corresponding to $-f_j$ contains only zeros. This implies $\boldsymbol{v} = (0, \dots, 0) = \boldsymbol{u}_0$ in line 8, and Algorithm 4 returns $(0, \dots, 0)$ after a single iteration of the **while**.

Consider now the case where $\mathrm{M}_f(\Phi) \cap \mathbb{Z}f_j \neq \emptyset$ for some $j \in [1, m]$. Note that this implies $f_j = a \cdot f$ for some $a \in \mathbb{Z} \setminus \{0\}$ and $j \in [1, m]$, hence $\langle f \rangle \leq \operatorname{poly}(\langle \Phi \rangle)$. This allows us to bound the size of the output of Algorithm 4 in terms of Φ, hiding factors that depend on f (as done in the statement of the proposition). A few auxiliary definitions are handy ($\ell \in \mathbb{N}$ and $j \in [1, m]$):

- We associate to $\boldsymbol{u}_\ell$ the vector $\widehat{\boldsymbol{u}}_\ell \in \{0,1\}^m$ given by $\widehat{\boldsymbol{u}}_\ell[i] = 1$ iff $\boldsymbol{u}_\ell[i] \neq 0$, for every $i \in [1, m]$.
- We associate to $F_{\ell,j}$ the set $\widehat{F}_{\ell,j} \coloneqq \{-f_j,\, f,\, \widehat{\boldsymbol{u}}_\ell[1] \cdot g_1,\, \dots,\, \widehat{\boldsymbol{u}}_\ell[m] \cdot g_m\}$.
- We associate to $K_{\ell,j}$ a basis $\widehat{K}_{\ell,j}$ for the integer kernel of the matrix representing $\widehat{F}_{\ell,j}$.
- We associate to $v_{\ell,j}$ the integer $\widehat{v}_{\ell,j} \coloneqq \gcd(\text{row of } \widehat{K}_{\ell,j} \text{ corresponding to } -f_j)$.

In a nutshell, $\widehat{\boldsymbol{u}}_\ell$ "forgets" the magnitude of the integers stored in $\boldsymbol{u}_\ell$, keeping only whether their value was 0 or not. The other objects defined above reflect this change at the level of matrices, kernels and GCDs. Up to permutation of columns, the matrix representing $F_{\ell,j}$ can be obtained by multiplying the matrix of $\widehat{F}_{\ell,j}$ by a diagonal matrix having in the main diagonal (a permutation of) $(1, 1, \boldsymbol{u}_\ell[1], \dots, \boldsymbol{u}_\ell[m])$. From the definition of $\widehat{K}_{\ell,j}$ and by Lemma 18, we conclude that

$$\text{if } \widehat{v}_{\ell,j} = 0 \text{ then } v_{\ell,j} = 0, \text{ and if } \widehat{v}_{\ell,j} \neq 0 \text{ then } v_{\ell,j} \neq 0 \text{ and } v_{\ell,j} \text{ divides } \operatorname{lcm}(\boldsymbol{u}_\ell) \cdot \widehat{v}_{\ell,j}. \qquad (\dagger)$$

Recall that the matrix representing $\widehat{F}_{\ell,j}$ has $d+1$ rows and $m+2$ columns. Since $\|\widehat{F}_{\ell,j}\| \leq \|\Phi\|$ for every $\ell \in \mathbb{N}$ and $j \in [1, m]$, by Corollary 2 there an integer $N \in [2, ((m+3) \cdot (\|\Phi\| + 2))^{(m+3)}]$ such that N is greater than $\widehat{v}_{\ell,j}$, for every $\ell \in \mathbb{N}$ and $j \in [1, m]$. We use ($\dagger$) above to bound the number of iterations and magnitude of the entries of $\boldsymbol{u}_\ell$ during the procedure. We show that

1. $\max_{\ell \in \mathbb{N}}(\operatorname{lcm}(\boldsymbol{u}_\ell)) = \max_{\ell=0}^{m}(\operatorname{lcm}(\boldsymbol{u}_\ell)) \leq N^{m^3}$ and for every $j \in [1,m]$, $\boldsymbol{u}_m[j] \leq N^{m^2}$, and
2. the **while** loop of line 2 is iterated at most $m^3 \cdot \log_2(N) + m$ many times.

In Item (1) above we slightly abused our notation, as $\boldsymbol{u}_\ell$ is undefined for $\ell \in \mathbb{N}$ greater or equal than the number of iterations of the **while** loop performed by the algorithm. In these cases, we postulate $\operatorname{lcm}(\boldsymbol{u}_\ell) = 0$ in order to make the equivalence in Item (1) well-defined. From the bound $N \leq ((m+3) \cdot (\|\Phi\| + 2))^{(m+3)}$, Items (1) and (2) imply that Algorithm 4 runs in PTIME and outputs a vector $\boldsymbol{v}$ with $\|\boldsymbol{v}\| \leq ((m+3) \cdot (\|\Phi\| + 2))^{(m+3)^3}$; proving the proposition.

Proof of (1): Informally, Item (1) states that $\operatorname{lcm}(\boldsymbol{u})$ is always bounded by N^{m^2}, and that $\operatorname{lcm}(\boldsymbol{u})$ achieves its maximum at most after the first m iterations of the **while** loop. We start by proving that $\max_{\ell=0}^{m}(\operatorname{lcm}(\boldsymbol{u}_\ell)) \leq N^{m^3}$ and that for every $j \in [1,m]$, $\boldsymbol{u}_m[j] \leq N^{m^2}$ This is done by induction on $\ell \in [1,m]$, by showing that (whenever defined) $\boldsymbol{u}_\ell$ is such that, for every $j \in [1,m]$, if $\boldsymbol{u}_\ell[j] \neq 0$ then $\widehat{v}_{\ell-1,j} \neq 0$ and $\boldsymbol{u}_\ell[j]$ divides $\big(\widehat{v}_{\ell-1,j} \cdot \prod_{i=0}^{\ell-2} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m})\big)$. Note that then $\boldsymbol{u}_\ell[j] \leq N^{m(\ell-1)+1}$, since N is an upper bound on every $\widehat{v}_{\ell,j}$, and thus for $\ell = m$ we get $\boldsymbol{u}_m[j] \leq N^{m^2}$ and $\operatorname{lcm}(\boldsymbol{u}_m) \leq N^{m^3}$, as required. Below, let $\boldsymbol{u}_\ell = (c_1,\dots,c_m)$. Note that, from line 7 of the algorithm, if $\ell \geq 1$, then $c_j = v_{\ell-1,j}$ for every $j \in [1,m]$.

base case $\ell = 1$. From $\boldsymbol{u}_0 = (0,\dots,0)$ we have $F_{0,j} = \widehat{F}_{0,j} = \{-f_j, f\}$ for every $j \in [1,m]$. This implies $\widehat{v}_{0,j} = v_{0,j}$. From $c_j = v_{0,j}$, we conclude that $c_j = \widehat{v}_{0,j}$, completing the base case.

induction step $\ell \geq 2$. Let $j \in [1,m]$ such that $c_j \neq 0$. From (†) and $c_j = v_{\ell-1,j}$, we get $\widehat{v}_{\ell-1,j} \neq 0$ and $c_j \mid (\operatorname{lcm}(\boldsymbol{u}_{\ell-1}) \cdot \widehat{v}_{\ell-1,j})$. Let $\boldsymbol{u}_{\ell-1} = (c_1^*,\dots,c_m^*)$. From the induction hypothesis, for every $k \in [1,m]$, if $c_k^* \neq 0$ then $\widehat{v}_{\ell-2,k} \neq 0$ and $c_k^* \mid \big(\widehat{v}_{\ell-2,k} \cdot \prod_{i=0}^{\ell-3} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m})\big)$. Therefore,

$$\operatorname{lcm}(\boldsymbol{u}_{\ell-1}) \;\mid\; \operatorname{lcm}\Big((\widehat{v}_{\ell-2,1} \cdot \prod_{i=0}^{\ell-3} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m})),\dots,(\widehat{v}_{\ell-2,m} \cdot \prod_{i=0}^{\ell-3} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m}))\Big).$$

From the equivalence $\operatorname{lcm}(a \cdot b, c \cdot b) = \operatorname{lcm}(a,c) \cdot b$, the right-hand side of the divisibility above equals $\prod_{i=0}^{\ell-2} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m})$. Then, the fact that c_j divides $\big(\widehat{v}_{\ell-1,j} \cdot \prod_{i=0}^{\ell-2} \operatorname{lcm}(\widehat{v}_{i,1},\dots,\widehat{v}_{i,m})\big)$ follows directly from $c_j \mid (\operatorname{lcm}(\boldsymbol{u}_{\ell-1}) \cdot \widehat{v}_{\ell-1,j})$.

To complete the proof of (1), we now show that $\max_{\ell \in \mathbb{N}}(\operatorname{lcm}(\boldsymbol{u}_\ell)) = \max_{\ell=0}^{m}(\operatorname{lcm}(\boldsymbol{u}_\ell))$. Directly from Claim 9 in the proof of Proposition 8, we have that for every $\ell \geq 1$, the vector $\boldsymbol{u}_\ell$ is the canonical representation of $\mathrm{M}_f^\ell(\Phi)$. We have,

(A) for every $j \in [1,m]$, if $\boldsymbol{u}_\ell[j] \neq 0$ then $\boldsymbol{u}_{\ell+1}[j]$ divides $\boldsymbol{u}_\ell[j]$ (assuming both $\boldsymbol{u}_\ell$ and $\boldsymbol{u}_{\ell+1}$ defined).

This follows directly from Lemma 15.

(B) If $\boldsymbol{u}_\ell$, $\boldsymbol{u}_{\ell+1}$ and $\boldsymbol{u}_{\ell+2}$ are defined, and $\boldsymbol{u}_\ell$ and $\boldsymbol{u}_{\ell+1}$ have the same zero entries, then also $\boldsymbol{u}_\ell$ and $\boldsymbol{u}_{\ell+2}$ have the same zero entries.

Indeed, in this case $\widehat{\boldsymbol{u}}_\ell = \widehat{\boldsymbol{u}}_{\ell+1}$ which implies $\widehat{v}_{\ell,j} = \widehat{v}_{\ell+1,j}$ for every $j \in [1,m]$. Now, if $\boldsymbol{u}_{\ell+2}[j] \neq 0$ then $v_{\ell+1,j} \neq 0$ and so $\widehat{v}_{\ell+1,j} \neq 0$ by (†). Then $\widehat{v}_{\ell,j} \neq 0$, and again by (†) we get $v_{\ell,j} \neq 0$. If instead $\boldsymbol{u}_{\ell+2}[j] = 0$, then $\boldsymbol{u}_\ell[j] = 0$ follows from Lemma 15.

Since $\boldsymbol{u}$ is a tuple with m entries, Item ((B)) above ensures that every $\boldsymbol{u}_\ell$ and $\boldsymbol{u}_r$ with $\ell, r \geq m$ share the same zero entries. Item ((A)) states instead that every non-zero entry of $\boldsymbol{u}_\ell$ upper bounds the corresponding entry of $\boldsymbol{u}_{\ell+r}$, for every $r \in \mathbb{N}$, and that this latter entry is always non-zero.

Together, Items ((A)) and ((B)) imply that $\max_{\ell\in\mathbb{N}}(\mathrm{lcm}(\boldsymbol{u}_\ell)) = \max_{\ell=0}^{m}(\mathrm{lcm}(\boldsymbol{u}_\ell))$.

Proof of (2): Assume that the **while** loop iterates at least $m+1$ times (otherwise (2) is trivially satisfied). From (2), the vector $\boldsymbol{u}_m$ such that $\boldsymbol{u}_m[j] \le N^{m^2}$ for every $j \in [1,m]$. As we have just discussed above, by Item ((B)), every subsequent $\boldsymbol{u}_{m+r}$ with $r \in \mathbb{N}$ has the same zero entries as $\boldsymbol{u}_m$. Whenever $\boldsymbol{u}_{m+r}$ and $\boldsymbol{u}_{m+r+1}$ are both defined (meaning in particular that $\boldsymbol{u}_{m+r} \neq \boldsymbol{u}_{m+r+1}$), there must be $j \in [1,m]$ such that $\boldsymbol{u}_{m+r}[j] \neq \boldsymbol{u}_{m+r+1}[j]$, and moreover by Item ((A)), $\boldsymbol{u}_{m+r+1}[i]$ divides $\boldsymbol{u}_{m+r}[i]$ for every $i \in [1,m]$, which in particular implies that $\boldsymbol{u}_{m+r+1}[j] \le \frac{\boldsymbol{u}_{m+r}[j]}{2}$. Therefore, the product of all non-zero entries of $\boldsymbol{u}$ (at least) halves at each iteration of the **while** loop after the m-th one. By (1), for every $j \in [1,m]$ we have $\boldsymbol{u}_m[j] \le N^{m^2}$, so the product of all non-zero entries in $\boldsymbol{u}_m$ is bounded by N^{m^3}. We conclude that the number of iterations of the **while** loop after the m-th one is bounded by $\log_2(N^{m^3}) = m^3 \cdot \log_2(N)$; i.e., $m^3 \cdot \log_2(N) + m$ many iterations overall. ☐

C.2 Closing a system of divisibility constraints under the elimination property

Lemma 7. *There is a polynomial-time algorithm that, given a system of divisibility constraints* $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^{m} f_i \mid g_i$ *and an order* $x_1 \prec \dots \prec x_d$ *for* $\boldsymbol{x}$*, computes* $\Psi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^{n} f_i' \mid g_i'$ *with the elimination property for* $\prec$ *that is equivalent to* $\Phi(\boldsymbol{x})$*, both over* $\mathbb{Z}$ *and modulo each* $p \in \mathbb{P}$*. The algorithm ensures that:*

1. *For any divisibility constraint* $f \mid g$ *such that* f *is not primitive,* $f \mid g$ *occurs in* Φ *if and only if* $f \mid g$ *occurs in* Ψ*. Moreover, for every* $f_i' \mid g_i'$ *in* Ψ *such that* f_i' *is primitive, there is some* $f_j \mid g_j$ *in* Φ *such that* f_j' *is the primitive part of* f_j*.*
2. *For every primitive polynomial* f*,* $\mathrm{M}_f(\Phi) = \mathrm{M}_f(\Psi)$ *(in particular, if* Φ *is increasing for some order* $\prec'$ *then so is* Ψ*, and vice versa).*
3. $\|\Psi\| \le (d+1)^{O(d)}(m + \|\Phi\| + 2)^{O(m^3 d)}$ *and* $n \le m \cdot (d+2)$*.*

Proof. The algorithm is simple to state:

1: $F \coloneqq \{f$ primitive $: a \cdot f$ is in the left-hand side of a divisibility of Φ, for some $a \in \mathbb{Z} \setminus \{0\}\}$
2: **for** $f \in F$ **do**
3: $\quad \boldsymbol{v} \coloneqq (c_1, \dots, c_m) \in \mathbb{Z}^m$ s.t. $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ spans $\mathrm{M}_f(\Phi)$ ▷ Lemma 6
4: $\quad H \coloneqq$ HNF of the matrix representing $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ ▷ Proposition 7
5: $\quad \Phi \leftarrow \Phi$ purged of all divisibilities of the form $f \mid g$ for some polynomial g
6: $\quad$ **for** $(a_d, \dots, a_1, a_0)$ non-zero column of H **do**
7: $\quad\quad \Phi \leftarrow \Phi \wedge (f \mid a_d \cdot x_d + \dots + a_1 \cdot x_1 + a_0)$
8: **return** Φ

Below, let Ψ be the system returned by the algorithm on input Φ.

The fact that Ψ has the elimination property follows from properties of the Hermite normal form. Consider F defined as in line 1, and $f \in F$. Starting from the matrix $A \in \mathbb{Z}^{(d+1)\times(m+1)}$ representing the spanning set $S \coloneqq \{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ computed in line 3, by Proposition 6 we conclude that H in line 4 spans $\mathrm{M}_f(\Phi)$. Moreover, by properties of the HNF, all non-zero columns of H are linearly independent, hence the **for** loop in line 6 is adding divisibilities $f \mid h_1, \dots, f \mid h_\ell$ where $h_1, \dots, h_\ell$ is a basis of $\mathrm{M}_f(\Phi)$; and $\ell \le m+1$. Note that line 5 has previously removed all divisibilities of the form $f \mid g$. Hence, in Ψ only the divisibilities $f \mid h_1, \dots, f \mid h_\ell$ have f as a left-hand side. Recall now that each column $(a_d, \dots, a_1, c)$ of the matrix A contains the coefficients and the constant of a distinct element $h \in S$, with a_i being the coefficient of x_i for $i \in [1,d]$, and c being the constant of h. Again since H is in HNF, it is lower triangular, and the pivot of each non-zero column is strictly below the pivot of the column before it. Following the order $x_1 \prec \cdots \prec x_d$, this allows us to conclude that, for every $k \in [0,d]$, the family $\{g_1,\dots,g_j\} \coloneqq \{g : \mathrm{LV}(g) \preceq x_k \text{ and } f \mid g \text{ appears in } \Psi\}$ is such that $g_1,\dots,g_j$ are linearly independent polynomials forming a basis for $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1,\dots,x_k]$; i.e., Ψ has the elimination property. We also note that, by virtue of the updates done in 7, Items 1 and 2 in the statement of Lemma 7 directly follow.

The fact that Ψ and Φ are equivalent both over $\mathbb{Z}$ and for solutions modulo a prime follows from Items 1 and 2 together with the following property of divisibility modules: given a system of divisibility constraints Φ' and a primitive term f,

- for every $\boldsymbol{a}$ integer solution of Φ' and every $g \in \mathrm{M}_f(\Phi')$, $f(\boldsymbol{a})$ divides $g(\boldsymbol{a})$,
- for every $p \in \mathbb{P}$, $\boldsymbol{b}$ solution of Φ' modulo p and every $g \in \mathrm{M}_f(\Phi')$, $v_p(f(\boldsymbol{b})) \leq v_p(g(\boldsymbol{b}))$.

  Here, note that given polynomials g_1 and g_2 with $v_p(f(\boldsymbol{b})) \leq v_p(g_1(\boldsymbol{b}))$ and $v_p(f(\boldsymbol{b})) \leq v_p(g_2(\boldsymbol{b}))$ we have $v_p(f(\boldsymbol{b})) \leq v_p(a_1 \cdot g_1(\boldsymbol{b}) + a_2 \cdot g_2(\boldsymbol{b}))$ for every $a_1, a_2 \in \mathbb{Z}$, as the p-adic evaluation satisfies $v_p(x \cdot y) = v_p(x) + v_p(y)$ and $\min(v_p(x), v_p(y)) \leq v_p(x+y)$, for all $x, y \in \mathbb{Z}$.

Let us now move to the bounds on Ψ stated in Item 3. Directly from $\#F \leq m$ and the fact that H is lower triangular we conclude that at most $m \cdot (d+1)$ divisibilities are added, and so Ψ has at most $m \cdot (d+2)$ divisibilities. We analyze the norm of Ψ. It suffices to consider a single $f \in F$. By definition, $\|f\| \leq \|\Phi\|$, and from Lemma 6, the infinity norm of the matrix A representing $\{f, c_1 \cdot g_1, \dots, c_m \cdot g_m\}$ is bounded by $((m+3) \cdot (\|\Phi\|+2))^{(m+3)^3} \cdot \|\Phi\|$. Note that A has $d+1$ many rows. By Proposition 7, the matrix H in line 4 is such that

$$\begin{aligned}
\|H\| &\leq ((d+1) \cdot \|A\| + 1)^{O(d)} \\
&\leq \Big((d+1) \cdot \big(((m+3) \cdot (\|\Phi\|+2))^{(m+3)^3} \cdot \|\Phi\|\big) + 1\Big)^{O(d)} \\
&\leq (d+1)^{O(d)} (m + \|\Phi\| + 2)^{O(m^3 d)}.
\end{aligned}$$

From the updates done in line 7, we conclude that $\|\Psi\| \leq (d+1)^{O(d)} (m + \|\Phi\| + 2)^{O(m^3 d)}$. $\square$

Lemma 8. *Let $\Phi(\boldsymbol{x}, \boldsymbol{y})$ and $\Psi(\boldsymbol{x}, \boldsymbol{y})$ be input and output of the algorithm in Lemma 7, respectively. For every $\boldsymbol{\nu} : \boldsymbol{x} \to \mathbb{Z}$ and primitive polynomial f, $\mathrm{M}_f(\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})) \subseteq \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$.*

Proof. Let f be a primitive polynomial. By definition of divisibility module, the lemma is true as soon as we prove (i) $f \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$, (ii) $\mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$ is a $\mathbb{Z}$-module, and (iii) for every divisibility $g' \mid h'$ (with g' non-zero) appearing in $\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$, if $b \cdot g' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$ for some $b \in \mathbb{Z}$, then $b \cdot h' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$. Indeed, by definition $\mathrm{M}_f(\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$ is the smallest set fulfilling these three properties, and therefore it must then be included in $\mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$.

The first two properties trivially follow by definition of $\mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$, hence let us focus on Property ((iii)). Consider a divisibility $g' \mid h'$ appearing in $\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and such that $b \cdot g' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$. By definition of $\Phi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$, there is a divisibility $g \mid h$ appearing in Φ such that $(g \mid h)[\boldsymbol{\nu}(\boldsymbol{x}) \,/\, \boldsymbol{x}] = (g' \mid h')$. We split the proof depending on whether g is a primitive polynomial.

g **is not a primitive polynomial.** By Item 1 in Lemma 7 the divisibility $g \mid h$ occurs in Ψ. So, $g' \mid h'$ is in $\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and directly by definition of divisibility module, $b \cdot h' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$.

g **is a primitive polynomial.** Let $\widetilde{g}$ and $c' \in \mathbb{Z} \setminus \{0\}$ be such that $g' = c' \cdot \widetilde{g}$. By Item 2 in Lemma 7, since $g \mid h$ appears in Φ, $h \in \mathrm{M}_g(\Psi)$. By the elimination property of Ψ, there are divisibilities $g \mid h_1, \dots, g \mid h_k$ such that $h = \lambda_1 \cdot h_1 + \cdots + \lambda_k \cdot h_k$ for some $\lambda_1, \dots, \lambda_k \in \mathbb{Z} \setminus \{0\}$. Every divisibility $(g \mid h_i)[\boldsymbol{\nu}(\boldsymbol{x}) \,/\, \boldsymbol{x}]$ with $i \in [1,k]$ appears in $\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. Since $g' = g(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and

$b \cdot g' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$ we have $b \cdot h_i(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$ for every $i \in [1, k]$. Note that $h' = h(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) = \lambda_1 \cdot h_1(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) + \cdots + \lambda_k \cdot h_k(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$, and therefore since the divisibility module is a $\mathbb{Z}$-module, $b \cdot h' \in \mathrm{M}_f(\Psi(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}))$. ☐

D Bounding the number of difficult primes

In this appendix, we establish Lemmas 3, 4 and 9.

Lemma 3. *Let $\Phi(\boldsymbol{x}) \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ and $p \in \mathbb{P} \setminus \mathbb{P}(\Phi)$. Then, Φ has a solution $\boldsymbol{b} \in \mathbb{N}^d$ modulo p such that $v_p(f_i(\boldsymbol{b})) = 0$ for every $1 \leq i \leq m$, and $\|\boldsymbol{b}\| \leq p - 1$.*

Proof. We remark that p not dividing any coefficients nor constants appearing in the left-hand sides of Φ implies that all the left-hand sides are non-zero. We show that the system of non-congruences defined by $f_i \not\equiv 0 \pmod{p}$ for every $i \in [1, m]$, admits a solution $\boldsymbol{b}$. This solution can clearly be taken with entries in $[0, p-1]$. Furthermore, $v_p(f_i(\boldsymbol{b})) = 0$ and $f_i(\boldsymbol{b}) \neq 0$ for every $i \in [1, m]$, and therefore $\boldsymbol{b}$ is a solution for Φ modulo p no matter the values of $v_p(g_i(\boldsymbol{b}))$ $(i \in [1, m])$.

Consider an arbitrary ordering $x_1 \prec \cdots \prec x_d$ on the variables in $\boldsymbol{x}$. We construct $\boldsymbol{b}$ by induction on $k \in [0, d]$. At the k-th step of the induction we deal with the linear terms h having $\mathrm{LV}(h) = x_k$. Below, we write F_0 for the set of the left-hand sides in Φ that are constant polynomials, and F_k with $k \in [1, d]$ for the set of the left-hand sides f in Φ such that $\mathrm{LV}(f) \preceq x_k$.

base case: $k = 0$**.** Every $f \in F_0$ is a non-zero integer. Then, $f \not\equiv 0 \pmod{p}$ directly follows from the hypothesis that p does not divide any constant appearing in the left-hand sides of Φ.

induction step: $k \geq 1$**.** From the induction hypothesis, there is $\boldsymbol{b}_{k-1} = (b_1, \ldots, b_{k-1}) \in \mathbb{Z}^{k-1}$ such that for every $f \in F_{k-1}$, $f(\boldsymbol{b}_{k-1}) \not\equiv 0 \pmod{p}$. We find a value b_k for x_k so that the following system of non-congruences is satisfied

$$f(\boldsymbol{b}_{k-1}, x_k) \not\equiv 0 \pmod{p} \qquad\qquad f \in F_k \setminus F_{k-1}.$$

Linear polynomials f in $F_k \setminus F_{k-1}$ are of the form $f(\boldsymbol{x}) = f'(x_1, \ldots, x_{k-1}) + c_f \cdot x_k$. Since by hypothesis $p \nmid c_f$, we consider the multiplicative inverse c_f^{-1} of c_f modulo p, and rewrite the above system as $x_k \not\equiv -c_f^{-1} \cdot f'$ for every $f \in F_k \setminus F_{k-1}$. This system as a solution directly from the fact that $p > m \geq \#(F_k \setminus F_{k-1})$. ☐

Before proving Lemmas 4 and 9, we need the following result on system of divisibility constraints with the elimination property, that will later be used also in the proof of Claim 4.

Lemma 19. *Let $\Phi(x_1, \ldots, x_d)$ be a system of divisibility with the elimination property for the order $x_1 \prec \cdots \prec x_d$. For every primitive term f and $j \in [1, d]$, the set $F \coloneqq \{g : (f \mid g) \text{ appears in } \Phi\}$ has at most one element with leading variable x_j.*

Proof. If f does not appear in the left-hand side of a divisibility of Φ, then $F = \emptyset$ and the lemma holds. Suppose f in a left-hand side. For simplicity, let us define $x_0 \coloneqq \bot$. By definition, for every $k \in [0, d]$, the elimination property forces $\{g_1, \ldots, g_\ell\} \coloneqq \{g : \mathrm{LV}(g) \preceq x_k \text{ and } f \mid g \text{ appears in } \Phi\}$ to be such that $g_1, \ldots, g_\ell$ are linearly independent polynomials forming a basis for $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \ldots, x_k]$. Given $k \in [0, d]$, let us write $F_k \coloneqq \{g : \mathrm{LV}(g) \preceq x_k \text{ and } (f \mid g) \text{ appear in } \Phi\}$. For $j \in [1, d]$, by the elimination property, F_{j-1} and F_j are sets of linearly independent vectors, that respectively generates $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \ldots, x_{j-1}]$ and $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \ldots, x_j]$. To conclude the proof, we show by induction on j that the set F_j has at most one element with leading variable x_j.

base case $j = 0$. In this case F_0 only contains constant polynomials (and might be empty, in that case it generates the subspace $\{0\}$). By elimination property, F is a set of linearly independent vectors, hence F_0 contains at most one element.

induction step $j \geq 1$. *Ad absurdum*, suppose there are two distinct $g_1, g_2 \in F_j \setminus F_{j-1}$ such that $\mathrm{LV}(g_1) = \mathrm{LV}(g_2) = x_j$. By definition of S-polynomial, $S(g_1, g_2) \in \mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \dots, x_{j-1}]$. Since F_{j-1} generates $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \dots, x_{j-1}]$, there is a sequence of integers $(\lambda_h)_{h \in F_{j-1}}$ such that $\sum_{h \in F_{j-1}} \lambda_h \cdot h = S(g_1, g_2)$. However, $F_{j-1} \cup \{g_1, g_2\} \subseteq F_j$ (by definition) and F_j is a set of linearly independent vectors. Therefore, every λ_h above must be 0, and we obtain $S(g_1, g_2) = 0$, i.e., g_1 and g_2 are linearly dependent, in contradiction with $g_1, g_2 \in F_j$. $\square$

Lemma 9. *Let $\Phi \coloneqq \bigwedge_{i=1}^m f_i \mid g_i$ be a system of divisibility constraints in d variables with the elimination property for $\prec$. Then, (i) $\#\Delta(\Phi) \leq 2 \cdot m^2(d+2)$ and (ii) $\langle \|\Delta(\Phi)\| \rangle \leq (d+2) \cdot (\langle \|\Phi\| \rangle + 1)$.*

Proof. Consider a primitive term f. If f is not a primitive part of any f_i, with $i \in [1, m]$, then $\mathrm{S}_f(\Phi) = \mathrm{terms}(\Phi)$ and so $\mathrm{S}_f(\Phi)$ is included in any $\mathrm{S}_{f'}(\Phi)$ where f' is a primitive part of a left-hand side of Φ. Hence, we can upper bound $\#\Delta(\Phi)$ and $\langle \|\Phi\| \rangle$ by only looking at these primitive parts.

Proof of (i): For f primitive part of some polynomials in a left-hand side of Φ, the elements of $\mathrm{S}_f(\Phi)$ have the form $S\big(g_k, S(g_{k-1}, \dots S(g_1, h))\big)$ where $h \in \mathrm{terms}(\Phi)$ and $f \mid g_i$ is a divisibility in Φ, for all $i \in [1, k]$. Moreover, each g_i has the same leading variable as $h_i \coloneqq S(g_{i-1}, S(g_{i-2}, \dots, S(g_1, h)))$. Since Φ has the elimination property, by Lemma 19, given h_i there is at most one g such that $f \mid g$ and $\mathrm{LV}(g) = \mathrm{LV}(h_i)$; that is g_i. Therefore, each element of $\mathrm{S}_f(\Phi)$ can be characterized by a pair (k, h) where $h \in \mathrm{terms}(\Phi)$ and $k \in [0, d+1]$, i.e., $\#\mathrm{S}_f(\Phi) \leq \#\mathrm{terms}(\Phi) \cdot (d+2) \leq 2 \cdot m \cdot (d+2)$, since $\#\mathrm{terms}(\Phi) \leq 2 \cdot m$. The number of f to be considered is bounded by m, i.e., the number of left-hand sides, which means $\#\Delta(\Phi) \leq 2 \cdot m^2(d+2)$.

Proof of (ii): Recall that $\langle \|f\| \rangle$ is the maximum bit length of a coefficient or constant of a polynomial f, and that $\langle \|R\| \rangle = \max_{f \in R} \langle \|f\| \rangle$ for a finite set R of polynomials. By examinating the definition of S-polynomial, we get that for every f and g, $\langle \|S(f, g)\| \rangle \leq \langle \|f\| \rangle + \langle \|g\| \rangle + 1$. Let f be a primitive polynomial. As discussed in the proof of ((i)), an element of $\mathrm{S}_f(\Phi)$ is of the form $S\big(g_k, S(g_{k-1}, \dots S(g_1, h))\big)$, where $h \in \mathrm{terms}(\Phi)$, $f \mid g_i$ is a divisibility in Φ, for all $i \in [1, k]$, and $k \leq d+1$. Then, $\langle \|S\big(g_k, S(g_{k-1}, \dots S(g_1, h))\big)\| \rangle \leq \langle \|h\| \rangle + \big(\sum_{i=1}^k \langle \|g_i\| \rangle\big) + k$. We conclude that $\langle \|\Delta(\Phi)\| \rangle \leq (d+2) \cdot (\langle \|\Phi\| \rangle + 1)$. $\square$

Lemma 4. *Consider a system of divisibility constraints $\Phi(\boldsymbol{x})$ in d variables. Then, the set of primes $\mathbb{P}(\Phi)$ satisfies $\log_2(\Pi \mathbb{P}(\Phi)) \leq m^2(d+2) \cdot (\langle \|\Phi\| \rangle + 2)$. Furthermore, if Φ has the elimination property for an order $\prec$ on $\boldsymbol{x}$, then the set of primes $\mathbf{P}_+(\Phi)$ satisfies $\log_2(\Pi \mathbf{P}_+(\Phi)) \leq 64 \cdot m^5(d+2)^4(\langle \|\Phi\| \rangle + 2)$.*

Proof. We first analyse $\log_2(\Pi \mathbb{P}(\Phi))$. Recall that $\mathbb{P}(\Phi)$ is the set of those primes p such that either (i) $p \leq m$ or (ii) p divide a coefficient or a constant of a left-hand side of Φ. The product of the primes satisfying (i) is bounded by $m! \leq m^m$. The product of the primes satisfying (ii) is bounded by the product of the coefficients or the constants in the left-hand sides of Φ, which is at most $\|\Phi\|^{m \cdot (d+1)}$. From these two bounds, we obtain the bound on $\log_2(\Pi \mathbb{P}(\Phi))$ stated in the lemma.

Let us analyse $\log_2(\Pi \mathbf{P}_+(\Phi))$. Without loss of generality, assume that the order $\prec$ is such that $x_1 \prec \dots \prec x_d$. We consider the three conditions defining $\mathbf{P}_+(\Phi)$ separately, and establish upper bounds for each of them. Recall that the number of primes dividing $n \in \mathbb{Z}$ is bounded by $\log_2(n)$, and that Lemma 9 implies $\#S(\Delta(\Phi)) \leq 8 \cdot m^4(d+2)^2$ and $\langle \|S(\Delta(\Phi))\| \rangle \leq 2 \cdot (d+2) \cdot (\langle \|\Phi\| \rangle + 1) + 1$.

(P1): Directly from the bounds above, the primes satisfying (P1) are at most $8 \cdot m^4(d+2)^2$, and thus the $\log_2$ of their product is at most $8 \cdot m^4(d+2)^2 \log_2(8 \cdot m^4(d+2)^2)$, which is bounded by $64 \cdot m^5(d+2)^3$.

(P2): The product of the primes dividing a coefficient or constant of a polynomial f in $S(\Delta(\Phi))$ is bounded by the product of these coefficients and constants. There are at most $(d+1) \cdot \#S(\Delta(\Phi))$ such coefficients and constants. Therefore, the $\log_2$ of this product is bounded by $(d+1) \cdot \#S(\Delta(\Phi)) \cdot \langle \|S(\Delta(\Phi))\| \rangle$, which is bounded by $16 \cdot m^4 (d+2)^4 (\langle \|\Phi\| \rangle + 2)$.

(P3): If f is a primitive term such that $a \cdot f$ does not occur in the left-hand sides of Φ, for any $a \in \mathbb{Z} \setminus \{0\}$, then $\mathrm{S}_f(\Phi) = \mathrm{terms}(\Phi)$ and $\mathrm{M}_f(\Phi) = \mathbb{Z}f$, and therefore λ, if it exists, equals to 1. Consider f primitive such that $a \cdot f \in \mathrm{terms}(\Phi)$ appears on the left-hand side of a divisibility in Φ, for some $a \in \mathbb{Z} \setminus \{0\}$, and consider $g \in \mathrm{S}_f(\Phi)$. We first compute a bound on the minimal positive λ such that $\lambda \cdot g \in \mathrm{M}_f(\Phi)$, if such a λ exists. Let $x_j \coloneqq \mathrm{LV}(g)$, with $j \in [0, d]$ and $x_0 \coloneqq \bot$. Consider the set $\{h_1, \dots, h_\ell\} \coloneqq \{h : \mathrm{LV}(h) \leq \mathrm{LV}(g) \text{ and } f \mid h \text{ is in } \Phi\}$; where $\ell \leq m$. From the elimination property, this set is a basis for $\mathrm{M}_f(\Phi) \cap \mathbb{Z}[x_1, \dots, x_j]$, and therefore λ exists if and only if $\mathbb{Z}g \cap \mathbb{Z}h_1 + \dots + \mathbb{Z}h_\ell \neq \{0\}$. Then let K be a basis for the kernel of the matrix representing the set $\{-g, h_1, \dots, h_\ell\}$. As observed in the context of Algorithm 4, if λ exists then it is the GCD of the row of K corresponding to $-g$. From Corollary 2, $\lambda \leq (m+3)^{m+3} \max(2, \|\Phi\|)^{m+2}$. In the proof of Lemma 9 we have shown $\#\mathrm{S}_f(\Phi) \leq 2 \cdot m \cdot (d+2)$, hence the number of pairs (f, g) to consider is bounded by $2 \cdot m^2 \cdot (d+2)$. Similarly to (P2), the product of the primes dividing all λs is bounded by the product of these λs, which is at most $\big((m+3)^{m+3} \max(2, \|\Phi\|)^{m+2}\big)^{2 \cdot m^2 \cdot (d+2)}$. Therefore, the $\log_2$ of the product of the primes satisfying (P3) is at most $32 \cdot m^4 (d+2) \cdot (\langle \|\Phi\| \rangle + 1)$.

Summing up the bounds we have just obtained yield the bound stated in the lemma. $\square$

E Theorem 4: proofs of Claim 4 and Claim 5

In this section, we prove Claim 4 and Claim 5, which are required to establish Theorem 4. In the context of this theorem, recall that $\Psi(\boldsymbol{x}, \boldsymbol{y})$ is a formula that is increasing for $(X_1 \prec \dots \prec X_r)$ and has the elimination property for an order $(\prec) \in (X_1 \prec \dots \prec X_r)$. Here, $\boldsymbol{x} = (x_1, \dots, x_d)$ are the variables appearing in X_1, ordered as $x_1 \prec \dots \prec x_d$, and $\boldsymbol{y}$ are the variables appearing in $\bigcup_{j=2}^{r} X_j$. We also have solutions $\boldsymbol{b}_p$ for Ψ modulo p, for every $p \in \mathbf{P}_+(\Psi)$, and we have inductively computed a map $\boldsymbol{\nu} \colon X_1 \to \mathbb{Z}$ the following three properties:

IH1: For every $p \in \mathbf{P}_+(\Psi)$ and $x \in X_1$, $\boldsymbol{\nu}(x) \equiv b_{p,x} \pmod{p^{\mu_p+1}}$, where $b_{p,x}$ is the entry of $\boldsymbol{b}_p$ corresponding to x, and $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) \in \mathbb{N} : f \text{ is in the left-hand side of a divisibility of } \Psi\}$.

IH2: For every prime $p \notin \mathbf{P}_+(\Psi)$ and for every $h, h' \in \Delta(\Psi)$ with leading variable in X_1, if $S(h, h')$ is not identically zero, then p does not divide both $h(\boldsymbol{\nu}(\boldsymbol{x}))$ and $h'(\boldsymbol{\nu}(\boldsymbol{x}))$.

IH3: $h(\boldsymbol{\nu}(\boldsymbol{x})) \neq 0$ for every $h \in \Delta(\Psi)$ that is non-zero and with $\mathrm{LV}(h) \in X_1$.

The formula $\Psi'(\boldsymbol{y})$ considered in Claim 4 and Claim 5 is defined as $\Psi' \coloneqq \Psi[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$.

Claim 4. *The system Ψ' is increasing for $(X_2 \prec \dots \prec X_r)$.*

At first glance, Claim 4 might appear intuitively true: since the notion of r-increasing form is mainly a property on sets $X_1 \prec \dots \prec X_r$ of orders of variables, and during the proof of Theorem 4 we are inductively handling the smallest set X_1, it might seem trivial that instantiating the variables in X_1 preserve increasingness for $X_2 \prec \dots \prec X_r$. However, in general, this is not the case. To see this, we repropose the example given in Section 1.3. Consider the system of divisibility constraints Ψ in increasing form for the order $u \prec v \prec x \prec y \prec z$ and with the elimination property for that order:

$$\begin{aligned} v &\mid u + x + y \\ v &\mid x \\ y + 2 &\mid z + 1 \\ v &\mid z\,. \end{aligned}$$

From the first two divisibilities, we have $(u+y) \in \mathrm{M}_v(\Psi)$; i.e., $(u-2)+(y+2) \in \mathrm{M}_v(\Psi)$. Therefore, if u were to be instantiated as 2, the resulting formula Ψ' would satisfy $(y + 2) \in \mathrm{M}_v(\Psi')$ and hence $(z + 1) \in \mathrm{M}_v(\Psi')$, from the third divisibility. Then, $1 \in \mathrm{M}_v(\Psi')$ would follow from the last divisibility, violating the constraints of the increasing form. Fortunately, due to the definition of $\mathrm{S}_f(\Psi)$, $u = 2$ contradicts the property (IH3) kept during the proof of Theorem 4, meaning that the above issue does not occur in our setting. Indeed, note that $S(y + 2, u + x + y) = 2 - u - x$ is in $\mathrm{S}_v(\Psi)$, and so is $S(2-u-x, x) = 2-u$. Then, (IH3) forces $2-u \neq 0$, excluding $u = 2$ as a possible solution. This observation is the key to establish Claim 4.

Given a set A of polynomials, an integer $a \in \mathbb{Z}$ and a variable x occurring in those polynomials, we define $A[a\,/\,x] \coloneqq \{f(a, \boldsymbol{y}) : f(x, \boldsymbol{y}) \in A\}$, that is the set obtained by partially evaluating x as a in all polynomials in A. This notion is extended to sequences of value-variable pairs as $A[a_i\,/\,x_i : i \in I]$.

Proof of Claim 4. To show the statement, we consider an order $\prec'$ in $(X_1 \prec \dots \prec X_r)$. Note that any order $(X_2 \prec \dots \prec X_r)$ can be constructed from elements in $(X_1 \prec \dots \prec X_r)$ by simply forgetting X_1. Let $\boldsymbol{y} = (y_1, \dots, y_j)$, with $y_1 \prec' \dots \prec' y_j$, be the variables in $\bigcup_{i=2}^{r} X_i$. To simplify the presentation, we denote by $a', b', \dots$ and $f', g', \dots$ integers and polynomials related to Ψ', and by $a, b, \dots$ and $f, g, \dots$ integers and polynomials related to Ψ. By definition of increasing form, we need to establish that for every $k \in [1, j]$ and primitive polynomial $f'(\boldsymbol{y})$ such that $a' \cdot f'$ appears in the left-hand side of a divisibility in Ψ', for some $a' \in \mathbb{Z} \setminus \{0\}$, and $\mathrm{LV}(f') = y_k$, we have $\mathrm{M}_{f'}(\Psi') \cap \mathbb{Z}[y_1, \dots, y_k] = \mathbb{Z}f'$. By definition of Ψ' and since $a' \cdot f'$ appears in a left-hand side, there is a primitive polynomial $f(\boldsymbol{x}, \boldsymbol{y})$ and a scalar $a \in \mathbb{Z} \setminus \{0\}$ such that $a \cdot f$ is in the left-hand side of some divisibility in Ψ, and $a' \cdot f'(\boldsymbol{y}) = a \cdot f(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. Note that this implies $a \mid a'$ and $\mathrm{LV}(f) \notin X_1$. We prove that $\frac{a'}{a} \cdot \mathrm{M}_{f'}(\Psi') \subseteq \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$. Note that this inclusion implies Ψ' in increasing form. To see this, take $g' \in \mathrm{M}_{f'}(\Psi') \cap \mathbb{Z}[y_1, \dots, y_k]$. We have $\frac{a'}{a} \cdot g' \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$, and thus there is $g(\boldsymbol{x}, \boldsymbol{y}) \in \mathrm{M}_f(\Psi)$ such that $\frac{a'}{a} \cdot g' = g(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. Since $\mathrm{LV}(g') \prec' y_k$, we have $\mathrm{LV}(g) \prec' y_k$. Since Ψ is increasing for $\prec'$, we conclude that $g \in \mathbb{Z}f$. Note that $(\mathbb{Z}f)[\boldsymbol{\nu}(x)\,/\,x \in X_1] \subseteq \mathbb{Z}f'$. Then $\frac{a'}{a} \cdot g' \in \mathbb{Z}f'$. Since f' is primitive, we get $g' \in \mathbb{Z}f'$. This shows $\mathrm{M}_{f'}(\Psi') \cap \mathbb{Z}[y_1, \dots, y_k] \subseteq \mathbb{Z}f'$, and the other inclusion directly follows by definition of $\mathrm{M}_{f'}(\Psi')$. We conclude that Ψ' is increasing.

To conclude the proof of Claim 4, let us show that $\frac{a'}{a} \cdot \mathrm{M}_{f'}(\Psi') \subseteq \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$. By definition of $\mathrm{M}_{f'}(\Psi')$, this follows as soon as we prove the following three properties:

(A) $\frac{a'}{a} \cdot f'$ belongs to $\mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$,

(B) $\mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$ is a $\mathbb{Z}$-module, and

(C) If $g' \mid h'$ is a divisibility in Ψ' and $b' \cdot g' \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$ for some $b' \in \mathbb{Z} \setminus \{0\}$, then $b' \cdot h' \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$.

By definition of divisibility module, $\frac{a'}{a} \cdot \mathrm{M}_{f'}(\Psi')$ is the smallest set that satisfies the three properties above, and therefore it must be included in $\mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x)\,/\,x : x \in X_1]$.

Proof of (A): By definition of f, $a' \cdot f' = a \cdot f(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and $a \mid a'$, hence $\frac{a'}{a} \cdot f' = f(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$, and by definition of divisibility module $f(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$.

Proof of (B): This follows directly from the definition of divisibility module being a $\mathbb{Z}$-module. Indeed, substitutions preserve the notion of $\mathbb{Z}$-module.

Proof of (C): This property follows from our definition of $\mathrm{S}_f(\Psi)$ together with the property (IH3) and the fact that Ψ has the elimination property for the order $\prec$ (not to be confused with the order $\prec'$, which does not guarantee the elimination property). Consider a divisibility $g'(\boldsymbol{y}) \mid h'(\boldsymbol{y})$ occurring in Ψ' and $b' \in \mathbb{Z} \setminus \{0\}$ such that $b' \cdot g' \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$. By definition of Ψ', there is a divisibility $g(\boldsymbol{x}, \boldsymbol{y}) \mid h(\boldsymbol{x}, \boldsymbol{y})$ in Ψ such that $g' = g(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and $h' = h(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. Also, by definition of $\mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$, there is a polynomial $\widehat{g}(\boldsymbol{x}, \boldsymbol{y}) \in \mathrm{M}_f(\Psi)$ such that $b' \cdot g' = \widehat{g}(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$.

To conclude the proof, it suffices to show that $b' \cdot g = \widehat{g}$. Indeed, since $g \mid h$ appears in Ψ and $\widehat{g} \in \mathrm{M}_f(\Psi)$, we then get $b' \cdot h \in \mathrm{M}_f(\Psi)$ by the definition of divisibility module, which implies $b' \cdot h' \in \mathrm{M}_f(\Psi)[\boldsymbol{\nu}(x) \,/\, x : x \in X_1]$ by definition of h; concluding the proof.

Since $\widehat{g} \in \mathrm{M}_f(\Psi)$ and Ψ has the elimination property for $\prec$, there are linearly independent polynomials $h_1, \dots, h_\ell$ such that the divisibilities $f \mid h_i$ appear in Ψ and there are $\lambda_1, \dots, \lambda_\ell \in \mathbb{Z} \setminus \{0\}$ such that $\widehat{g} = \sum_{i=1}^{\ell} \lambda_i \cdot h_i$. Thanks to Lemma 19, we can arrange these polynomials so that $\mathrm{LV}(h_1) \prec \dots \prec \mathrm{LV}(h_\ell)$. We write c_i for the coefficient corresponding to the leading variable of h_i. Since $\mathrm{LV}(f) \notin X_1$ (stated earlier) and Ψ is increasing, $\mathrm{LV}(h_i) \in \bigcup_{k=2}^{r} X_k$ holds for every $i \in [1, \ell]$. From $g' = g(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ and $b' \cdot g' = \widehat{g}(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$ we directly get $b' \cdot g(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) = \widehat{g}(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y})$. Therefore, $(b' \cdot g - \widehat{g})(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) = 0$, implying that $b' \cdot g - \widehat{g}$ is either constant or has its leading variable in X_1. This implies that $b' \cdot g - \sum_{i=1}^{\ell} \lambda_i \cdot h_i$ is either constant or has its leading variable in X_1. Since the λ_i are non-zero, and moreover $\mathrm{LV}(h_i)$ is not in X_1 and $\mathrm{LV}(h_1) \prec \dots \prec \mathrm{LV}(h_\ell)$, we have $\mathrm{LV}(b' \cdot g - \sum_{i=k+1}^{\ell} \lambda_i \cdot h_i) = \mathrm{LV}(h_k)$ for every $k \in [1, \ell]$, and the coefficient corresponding to the leading variable of $b' \cdot g - \sum_{i=k+1}^{\ell} \lambda_i \cdot h_i$ is exactly $\lambda_k \cdot c_k$.

We show by induction on $k \in [1, \ell+1]$, with base case $k = \ell+1$, that $\alpha_k \cdot (b' \cdot g - \sum_{i=k}^{\ell} \lambda_i \cdot h_i) = b' \cdot S(g, h_\ell, \dots, h_k)$, where $\alpha_k \coloneqq \prod_{i=k}^{\ell} c_i$, and $S(f_1, \dots, f_n)$ is short for $S(\dots(S(f_1, f_2), \dots), f_n)$; e.g., $S(f_1, f_2, f_3) = S(S(f_1, f_2), f_3)$.

base case $k = \ell + 1$: For the base case, $\alpha_{\ell+1} = 1$ and the equivalence becomes $b' \cdot g = b' \cdot g$.

induction step $k \leq \ell$: we have $\alpha_{k+1}(b' \cdot g - \sum_{i=k+1}^{\ell} \lambda_i \cdot h_i) = b' \cdot S(g, h_\ell, \dots, h_{k+1})$ by induction hypothesis. Note that, from the left-hand side of this equation, the coefficient corresponding to the leading variable of $b' \cdot S(g, h_\ell, \dots, h_{k+1})$ is $c_k \cdot \alpha_{k+1} \cdot \lambda_k$. Then,

$$
\begin{aligned}
&\alpha_k \cdot (b' \cdot g - \sum_{i=k}^{\ell} \lambda_i \cdot h_i) \\
&= c_k \cdot \alpha_{k+1}(b' \cdot g - \sum_{i=k}^{\ell} \lambda_i \cdot h_i) && \text{definition of } \alpha_k \\
&= c_k \cdot \alpha_{k+1}(b' \cdot g - \sum_{i=k+1}^{\ell} \lambda_i \cdot h_i) - c_k \cdot \alpha_{k+1} \cdot \lambda_k \cdot h_k \\
&= c_k \cdot (b' \cdot S(g, h_\ell, \dots, h_{k+1})) - (c_k \cdot \alpha_{k+1} \cdot \lambda_k) \cdot h_k && \text{induction hypothesis} \\
&= S(b' \cdot S(g, h_\ell, \dots, h_{k+1}), h_k) && \text{coeff. leading var. } h_k \text{ is } c_k \\
& && \text{coeff. leading var. } (b' \cdot S(g, h_\ell, \dots, h_{k+1})) \text{ is } c_k \cdot \alpha_{k+1} \cdot \lambda_k
\end{aligned}
$$

$$= b' \cdot S(g, h_\ell, \dots, h_k) \qquad\qquad S(b' \cdot f_1, f_2) = b' \cdot S(f_1, f_2), \text{by definition of } S\text{-polynomial.}$$

Thanks to the equality $\alpha_k \cdot (b' \cdot g - \sum_{i=k}^{\ell} \lambda_i \cdot h_i) = b' \cdot S(g, h_\ell, \dots, h_k)$ we just established, we conclude that $\alpha_1 \cdot (b' \cdot g - \widehat{g}) = b' \cdot S(g, h_\ell, \dots, h_1)$. Moreover, from $\mathrm{LV}(b' \cdot g - \sum_{i=k+1}^{\ell} \lambda_i \cdot h_i) = \mathrm{LV}(h_k)$ we conclude that $\mathrm{LV}(S(g, h_\ell, \dots, h_{k+1})) = \mathrm{LV}(h_k)$, for every $k \in [1, \ell]$. Then, since $g \in \mathrm{terms}(\Psi)$ and the divisibilities $f \mid h_1, \dots, f \mid h_\ell$ appear in Ψ, by definition of $\mathrm{S}_f(\Psi)$, we conclude that $S(g, h_\ell, \dots, h_1) \in \mathrm{S}_f(\Psi)$. Recall that $b' \cdot g - \widehat{g}$ is either constant or has its leading variable in X_1. The same is true for $S(g, h_\ell, \dots, h_1)$, and we have $(\alpha_1 \cdot (b' \cdot g - \widehat{g}))(\boldsymbol{\nu}(\boldsymbol{x})) = b' \cdot S(g, h_\ell, \dots, h_1)(\boldsymbol{\nu}(\boldsymbol{x}))$. From $(b' \cdot g - \widehat{g})(\boldsymbol{\nu}(\boldsymbol{x})) = (b' \cdot g - \widehat{g})(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{y}) = 0$ and $b' \neq 0$ we get $S(g, h_\ell, \dots, h_1)(\boldsymbol{\nu}(\boldsymbol{x})) = 0$. From the property (IH3), this can only occur when $S(g, h_\ell, \dots, h_1) = 0$, and so $\alpha_1 \cdot (b' \cdot g - \widehat{g}) = 0$. By definition $\alpha_1 \neq 0$, and therefore $b' \cdot g = \widehat{g}$, concluding the proof of ((C)). ☐

Claim 5. *For every $p \in \mathbf{P}_+(\Psi)$, the solution $\boldsymbol{b}_p$ for Ψ modulo p is, when restricted to $\boldsymbol{y}$, a solution for $\Psi'(\boldsymbol{y})$ modulo p. For every prime $p \notin \mathbf{P}_+(\Psi)$, there is a solution $\boldsymbol{b}_p$ for Ψ' modulo p such that (i) every entry of $\boldsymbol{b}_p$ belongs to $[0, p^{u+1} - 1]$, where $u \coloneqq \max\{v_p(\alpha_i) : i \in [\ell+1, n]\}$, and (ii) for every $g \in \mathrm{terms}(\Psi')$, $v_p(g(\boldsymbol{b}_p))$ is either 0 or u.*

Proof. The first statement of the claim follows from (IH1) and the definition of μ_p (the reasoning is analogous to the one in the base case $r = 1$ of the induction of Theorem 4). For the second statement, consider a prime p not belonging to $\mathbf{P}_+(\Psi)$. We provide a solution $\boldsymbol{b}_p$ for $\Psi'(\boldsymbol{y})$ modulo p. Let $\boldsymbol{y} = (y_1, \dots, y_j)$ with $y_1 \prec \dots \prec y_j$. To compute $\boldsymbol{b}_p = (b_{p,1}, \dots, b_{p,j})$, where $b_{p,k}$ is the value assigned to y_k, we consider two cases that depend on whether p divides some α_i appearing in the first block of divisibilities of Equation (7) (i.e., these are the α_i with $i \in [\ell+1, n]$).

case $p \nmid \alpha_i$ for all $i \in [\ell+1, n]$. This case is relatively simple. Starting from y_1 and proceeding in increasing order of variables, we compute $b_{p,k+1}$ ($k \in \mathbb{N}$) by solving the system

$$h(b_{p,1}, \dots, b_{p,k},\ y_{k+1}) \not\equiv 0 \qquad \pmod p \qquad h \in \mathrm{terms}(\Psi') \text{ s.t. } \mathrm{LV}(h) = y_{k+1}. \tag{13}$$

With respect to the h above, let us write $h(b_{p,1}, \dots, b_{p,k}\ y_{k+1}) = c_h + a_h \cdot y_{k+1}$ where c_h is the constant term obtained by partially evaluating h with respect to $(b_{p,1}, \dots, b_{p,k})$ and a_h is the coefficient of y_{k+1} in h. By definition of Ψ', the term h is obtained by substituting $\boldsymbol{x}$ for $\boldsymbol{\nu}(\boldsymbol{x})$ in a polynomial of Ψ, and in that polynomial y_{k+1} has coefficient a_h. Since $p \notin \mathbf{P}_+(\Psi)$, from Condition (P2) we conclude that $p \nmid a_h$, and so a_h has an inverse a_h^{-1} modulo p. The system of non-congruences above is equivalent to the system $\mathcal{S}_{k+1}$ given by

$$y_{k+1} \not\equiv -a_h^{-1} \cdot c_h \qquad \pmod p \qquad h \in \mathrm{terms}(\Psi') \text{ s.t. } \mathrm{LV}(h) = y_{k+1}.$$

From Condition (P1) we have $p > \#\mathrm{terms}(\Psi) \geq \#\mathrm{terms}(\Psi')$, and so it suffices to take $b_{p,k+1}$ to be an element in $[0, p-1]$ that differs from every $-a_h^{-1} \cdot c_h$ appearing in the rows of $\mathcal{S}_{k+1}$.

The solution $\boldsymbol{b}_p$ resulting from the systems of non-congruences $\mathcal{S}_1, \dots, \mathcal{S}_j$ is such that, for every $h \in \mathrm{terms}(\Psi')$, $v_p(h(\boldsymbol{b}_p)) = 0$. Therefore, $\boldsymbol{b}_p$ is a solution for Ψ' modulo p.

case $p \mid \alpha_i$ for some $i \in [\ell+1, n]$. This case is involved. Since p divides some $\alpha_i = f_i(\boldsymbol{\nu}(\boldsymbol{x}))$, and $p \notin \mathbf{P}_+(\Psi)$, by Condition (P2) we have $p \mid f(\boldsymbol{\nu}(\boldsymbol{x}))$, where f is the primitive polynomial obtained by dividing every coefficient and constant of f_i by $\gcd(f_i)$. Recall that $\boldsymbol{x} = (x_1, \dots, x_d)$ with $x_1 \prec \dots \prec x_d \prec y_1 \prec \dots \prec y_j$, and note that $\mathrm{LV}(f) \preceq x_d$. Below, let us define $u \coloneqq v_p(f(\boldsymbol{\nu}(\boldsymbol{x})))$. The idea is to use f to iteratively construct the solution $\boldsymbol{b}_p$ for $\boldsymbol{y} = (y_1, \dots, y_j)$. We rely on the following induction hypotheses ($k \in [0, j]$):

IH1′: for every non-zero polynomial $g(\boldsymbol{x}, y_1, \dots, y_t) \in \mathrm{terms}(\Psi)$ such that $t \leq k$, if $\mathbb{Z}g \cap \mathrm{M}_f(\Psi) \neq \{0\}$ then $v_p(g(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1}, \dots, b_{p,t})) = u$, and

IH2′: for every non-zero polynomial $h(\boldsymbol{x}, y_1, \dots, y_t) \in \mathrm{S}_f(\Psi)$ such that $t \leq k$, if $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) = \{0\}$ then $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1}, \dots, b_{p,t})) = 0$.

Let us first show that by constructing $\boldsymbol{b}_p$ so that it satisfies the hypotheses above for $k = j$ implies that $\boldsymbol{b}_p$ is a solution for Ψ' modulo p. Consider a divisibility $\alpha_i + f_i'(\boldsymbol{y}) \mid \beta_i + g_i'(\boldsymbol{y})$ in Ψ', with $i \in [\ell+1, m]$ and $f_i' = 0$ if $i \leq n$. Recall that $\alpha_i = f_i(\boldsymbol{\nu}(\boldsymbol{x}))$ and $\beta_i = g_i(\boldsymbol{\nu}(\boldsymbol{x}))$, and given $h \coloneqq f_i + f_i'$ and $h' \coloneqq g_i + g_i'$, the divisibility $h \mid h'$ occurs in Ψ. We have two cases:

- $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) \neq \{0\}$. In this case, by definition of $\mathrm{M}_f(\Psi)$ we have $\mathbb{Z}h' \cap \mathrm{M}_f(\Psi) \neq \{0\}$. According to (IH1′), $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{b}_p)) = v_p(h'(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{b}_p)) = u$. By definition of h and h', we get $v_p(\alpha_i + f_i'(\boldsymbol{b}_p)) = v_p(\beta_i + g_i'(\boldsymbol{b}_p)) = u$. Note that $f(\boldsymbol{\nu}(\boldsymbol{x}))$ is non-zero by (IH3), hence its p-adic evaluation u belongs to $\mathbb{N}$, which forces $\alpha_i + f_i'(\boldsymbol{b}_p)$ to be non-zero.
- $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) = \{0\}$. Recall that $\mathrm{terms}(\Psi) \subseteq \mathrm{S}_f(\Psi)$, by definition. Hence, directly from (IH2′) we get $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}), \boldsymbol{b}_p)) = v_p(\alpha_i + f_i'(\boldsymbol{b}_p)) = 0$. This implies $\alpha_i + f_i'(\boldsymbol{b}_p)$ non-zero, and moreover $v_p(\alpha_i + f_i'(\boldsymbol{b}_p)) \leq v_p(\beta_i + g_i'(\boldsymbol{b}_p))$ no matter what is the value of $v_p(\beta_i + g_i'(\boldsymbol{b}_p))$.

Note moreover that (IH1′) and (IH2′) directly imply $\max\{v_p(g(\boldsymbol{b}_p)) \in \mathbb{N} : g \in \mathrm{terms}(\Psi')\} \leq u$.

To conclude the proof, we show how to construct $\boldsymbol{b}_p$ satisfying (IH1′) and (IH2′).

base case $k = 0$**.** We establish (IH1′) and (IH2′) for polynomials with variables in $\boldsymbol{x}$, by showing the three properties below, for every non-zero polynomial $h \in \Delta(\Psi)$ with $\mathrm{LV}(h) \preceq x_d$.

(A) Either $\mathbb{Z}f \cap \mathbb{Z}h \neq \{0\}$ or $p \nmid h(\boldsymbol{\nu}(\boldsymbol{x}))$.

(B) If $\mathbb{Z}f \cap \mathbb{Z}h \neq \{0\}$, then $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = v_p(f(\boldsymbol{\nu}(\boldsymbol{x})))$.

(C) If $p \nmid h(\boldsymbol{\nu}(\boldsymbol{x}))$ then $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = 0$ and $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) = \{0\}$.

These three items imply (IH1′) and (IH2′). To establish (IH1′), take $g(\boldsymbol{x}) \in \mathrm{terms}(\Psi)$ such that $\mathbb{Z}g \cap \mathrm{M}_f(\Psi) \neq \{0\}$. From ((C)) we must have $p \mid g(\boldsymbol{\nu}(\boldsymbol{x}))$. Hence, $\mathbb{Z}f \cap \mathbb{Z}h \neq \{0\}$ by ((A)), and from ((B)) we get $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = v_p(f(\boldsymbol{\nu}(\boldsymbol{x})))$. For (IH2′), take $h(\boldsymbol{x}) \in \mathrm{S}_f(\Psi)$ such that $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) = \{0\}$. By definition of $\mathrm{M}_f(\Psi)$, $\mathbb{Z}h \cap \mathbb{Z}f = \{0\}$ and so $p \nmid h(\boldsymbol{\nu}(\boldsymbol{x}))$ by ((A)). From ((C)), $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = 0$. We conclude the base case by establishing ((A))–((C)).

Proof of ((A)): Since Ψ has the elimination property, $f \in \mathrm{terms}(\Psi)$. Then, ((A)) follows directly from (IH2); remark that $S(f, h) = 0$ is equivalent to $\mathbb{Z}f \cap \mathbb{Z}h \neq \{0\}$.

Proof of ((B)): By $\mathbb{Z}f \cap \mathbb{Z}h \neq \{0\}$ there are $\lambda_1, \lambda_2 \in \mathbb{Z} \setminus \{0\}$ such that $\lambda_1 \cdot f = \lambda_2 \cdot h$. Without loss of generality, $\gcd(\lambda_1, \lambda_2) = 1$, and thus $\gcd(\lambda_2, \gcd(f)) = \lambda_2$. The polynomial f is primitive, hence $\lambda_2 = 1$ and we get $h = \lambda_1 \cdot f$. Since $p \notin \mathbf{P}_+(\Psi)$, from Condition (P2) and $\lambda_1 \mid \gcd(h)$ we derive $p \nmid \lambda_1$. Therefore, $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = v_p(\lambda_1 \cdot f(\boldsymbol{\nu}(\boldsymbol{x}))) = v_p(f(\boldsymbol{\nu}(\boldsymbol{x})))$.

Proof of ((C)): Trivially, $p \nmid h(\boldsymbol{\nu}(\boldsymbol{x}))$ equals $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}))) = 0$. To show $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) = \{0\}$, first note that $\mathbb{Z}h \cap \mathbb{Z}f = \{0\}$, directly from $p \mid f(\boldsymbol{\nu}(\boldsymbol{x}))$ and ((B)). *Ad absurdum*, assume $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) \neq \{0\}$. Since Ψ is increasing for $\boldsymbol{\chi} \coloneqq (X_1 \prec \dots \prec X_r)$, and $\mathrm{LV}(h)$ and $\mathrm{LV}(f)$ are both in X_1, Ψ is increasing no matter the order of the variables imposed on X_1. Take an order $(\prec') \in \boldsymbol{\chi}$ for which $\mathrm{LV}_{\prec'}(h) \preceq' \mathrm{LV}_{\prec'}(f)$, and let $x_1' \prec' \dots \prec' x_d'$ be the order for the variables $x_1, \dots, x_d$. Since Ψ is increasing for $\prec'$, $\mathrm{M}_f(\Psi) \cap \mathbb{Z}[x_1', \dots, x'_{\mathrm{LV}_{\prec'}(f)}] = \mathbb{Z}f$. However, $\mathbb{Z}h \subseteq \mathbb{Z}[x_1', \dots, x'_{\mathrm{LV}_{\prec'}(f)}]$ by definition of $\prec'$, hence from $\mathbb{Z}h \cap \mathrm{M}_f(\Psi) \neq \{0\}$ we obtain $\mathbb{Z}h \cap \mathbb{Z}f \neq \{0\}$, a contradiction. This proves ((C)).

induction step. Let us assume that $b_{p,1},\dots,b_{p,k}$ are defined for the variables $y_1,\dots,y_k$ with $k \in [0, j-1]$, so that the induction hypotheses hold. We provide the value $b_{p,k+1}$ for y_{k+1} while keeping (IH1′) and (IH2′) satisfied. We divide the proof into two cases, depending on whether there is a term $g \in \text{terms}(\Psi)$ with $\text{LV}(g) = y_{k+1}$ such that $\mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\}$.

case g does not exist. In this case, (IH1′) is fulfilled no matter the value of $b_{p,k+1}$, so we focus on finding such a value satisfying (IH2′). It suffices to consider the system

$$h(b_{p,1},\dots,b_{p,k},\, y_{k+1}) \not\equiv 0 \pmod{p} \qquad h \in \text{S}_f(\Psi) \text{ s.t. } \text{LV}(h) = y_{k+1}.$$

Similarly to the system in Equation (13), writing $c_h + a_h \cdot y_{k+1}$ for $h(b_{p,1},\dots,b_{p,k},\, y_{k+1})$, we obtain the equivalent system of non-congruences

$$y_{k+1} \not\equiv -a_h^{-1} \cdot c_h \pmod{p} \qquad h \in \text{S}_f(\Psi) \text{ s.t. } \text{LV}(h) = y_{k+1}.$$

Since $p \notin \mathbf{P}_+(\Psi)$ and from (P1), this system admits a solution $b_{p,k+1}$ in $[0, p-1]$. Note that (IH2′) is satisfied, since every polynomial in that hypothesis is considered in these non-congruence systems.

case g exists. Recall that g is a polynomial in terms(Ψ) such that $\text{LV}(g) = y_{k+1}$ and $\mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\}$. Let $u \coloneqq v_p(f(\boldsymbol{\nu}(\boldsymbol{x})))$. In order to satisfy (IH1′) it suffices to find $b_{p,k+1} \in \mathbb{Z}$ satisfying the following (non-empty) system of non-congruences

$$\begin{aligned}
&\forall g \in \text{terms}(\Psi) \text{ s.t. } \text{LV}(g) = y_{k+1} \text{ and } \mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\},\\
&\quad g(b_{p,1},\dots,b_{p,k},\, y_{k+1}) \equiv 0 \pmod{p^u}\\
&\quad g(b_{p,1},\dots,b_{p,k},\, y_{k+1}) \not\equiv 0 \pmod{p^{u+1}}.
\end{aligned}$$

Similarly to the system in Equation (13), writing $c_g + a_g \cdot y_{k+1}$ for $g(b_{p,1},\dots,b_{p,k},\, y_{k+1})$, we obtain the equivalent system of non-congruences

$$\begin{aligned}
&\forall g \in \text{terms}(\Psi) \text{ s.t. } \text{LV}(g) = y_{k+1} \text{ and } \mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\},\\
&\quad y_{k+1} \equiv -a_g^{-1} \cdot c_g \pmod{p^u}\\
&\quad y_{k+1} \not\equiv -a_g^{-1} \cdot c_g \pmod{p^{u+1}}.
\end{aligned} \tag{14}$$

Focus on the congruences $y_{k+1} \equiv -a_g^{-1} \cdot c_g \pmod{p^u}$ of this system. These only have a solution if the right-hand side is the same modulo p^u for every $g \in \text{terms}(\Psi)$ with $\text{LV}(g) = y_{k+1}$ and $\mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\}$. We prove that this is indeed the case. Consider g_1 and g_2 such that $g_i \in \text{terms}(\Psi)$ with $\text{LV}(g_i) = y_{k+1}$ and $\mathbb{Z}g_i \cap \text{M}_f(\Psi) \neq \{0\}$, for $i \in \{1, 2\}$. Let λ_1 and λ_2 be the smallest positive integers such that both $\lambda_1 \cdot g_1$ and $\lambda_2 \cdot g_2$ belong to $\text{M}_f(\Psi)$. By definition of divisibility module and S-polynomial, $S(\lambda_1 \cdot g_1, \lambda_2 \cdot g_2) \in \text{M}_f(\Psi) \cap \mathbb{Z}[x_1,\dots,x_d,y_1,\dots,y_k]$. According to the elimination property of Ψ, there is a (finite) basis B for $\text{M}_f(\Psi) \cap \mathbb{Z}[x_1,\dots,x_d,y_1,\dots,y_k]$ such that for every $h \in B$, $f \mid h$ is a divisibility in Ψ. Moreover, $\text{LV}(h) \preceq y_k$ and thus by (IH1′) we get $v_p(h(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1},\dots,b_{p,k})) = u$. Now, since $S(\lambda_1 \cdot g_1, \lambda_2 \cdot g_2)$ is a linear combination of elements in B, we conclude that $p^u \mid S(\lambda_1 \cdot g_1, \lambda_2 \cdot g_2)$. By writing $g_i(\boldsymbol{x}, y_1,\dots,y_{k+1})$ as $g_i'(\boldsymbol{x}, y_1,\dots,y_k) + a_i \cdot y_{k+1}$, for $i \in \{1, 2\}$, this divisibility can be rewritten as the congruence:

$$(\lambda_2 \cdot a_2) \cdot (\lambda_1 \cdot g_1') \equiv (\lambda_1 \cdot a_1) \cdot (\lambda_2 \cdot g_2') \pmod{p^u}.$$

From $p \notin \mathbf{P}_+(\Psi)$, (P2) and (P3), we conclude that $p \nmid \lambda_1 \cdot \lambda_2 \cdot a_1 \cdot a_2$. By multiplying both sides of the above congruence by the inverse $(\lambda_1 \cdot \lambda_2 \cdot a_1 \cdot a_2)^{-1}$ of $\lambda_1 \cdot \lambda_2 \cdot a_1 \cdot a_2$

modulo p^u, we conclude that $a_1^{-1} \cdot g_1' \equiv a_2^{-1} \cdot g_2' \pmod{p^u}$. This shows that the right-hand side is the same across all the congruences and non-congruences of the system in Equation (14). Moreover, $p > \#\text{terms}(\Psi)$ by (P1), and therefore this system is feasible, and more precisely has a solution $b_{p,k+1}$ of the form $b_{p,k+1} \coloneqq p^u \cdot \gamma$ for some $\gamma \in [1, p-1]$. Pick such a solution, which by construction satisfies (IH1′).

We show that $b_{p,k+1}$ also satisfies (IH2′). Here is where the existence of the polynomial $g \in \text{terms}(\Psi)$ satisfying $\text{LV}(g) = y_{k+1}$ and $\mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\}$ plays a role. From $\mathbb{Z}g \cap \text{M}_f(\Psi) \neq \{0\}$ and since Ψ has the elimination property, we can find a polynomial g_0 such that $f \mid g_0$ is in Ψ, and $\text{LV}(g_0) = y_{k+1}$. We prove (IH2′) arguing by contraposition. Let $h \in \text{S}_f(\Psi)$ such that $\text{LV}(h) = y_{k+1}$ and $p \mid h(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1}, \dots, b_{p,k+1})$. If $S(h, g_0)$ is zero, i.e., h and g_0 are linearly dependent, then $\mathbb{Z}h \cap \text{M}_f(\Psi) \neq \{0\}$ follows by definition of g_0, and (IH2′) holds for h. Suppose that $S(h, g_0)$ is non-zero. From the construction of $b_{p,k+1}$ and since g_0 is a polynomial considered in Equation (14), we have $p \mid g_0(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1}, \dots, b_{p,k+1})$. Then, by definition of S-polynomial, $p \mid S(h, g_0)(\boldsymbol{\nu}(\boldsymbol{x}), b_{p,1}, \dots, b_{p,k})$. By definition of $\text{S}_f(\Psi)$, note that $h \in \text{S}_f(\Psi)$ and $g_0 \in \text{terms}(\Psi)$ implies $S(h, g_0) \in \text{S}_f(\Psi)$. Since $S(h, g_0)$ is non-zero, the induction hypothesis (IH2′) implies that $\mathbb{Z}S(h, g_0) \cap \text{M}_f(\Psi) \neq \{0\}$. Then, $\mathbb{Z}h \cap \text{M}_f(\Psi) \neq \{0\}$ follows directly from the fact that $f \mid g_0$ appears in Ψ (and so $\mathbb{Z}g_0 \cap \text{M}_f(\Psi)$). Once more, we conclude that (IH2′) holds for h.

Following the case analysis above, we construct solutions $\boldsymbol{b}_p$ for $\Psi'(\boldsymbol{y})$ modulo p, for every $p \in \mathbf{P}_+(\Psi')$. This concludes the proof of Claim 5. □

F Theorem 4: proof of Claim 8

We recall that $\underline{O} \in \mathbb{Z}_+$ is the minimal positive integer greater or equal than 4 such that the map $x \mapsto \underline{O}(x+1)$ upper bounds the linear functions hidden in the $O(.)$ appearing in Lemma 7. The integer $\Gamma(r, \ell, w, m, d)$, with $r, \ell, w, m, d \in \mathbb{Z}_+$ and $r \leq d$, is the maximum bit length of the minimal positive solution of any system of divisibility constraints Φ such that:

- Φ is r-increasing.
- The maximum bit length of a coefficient or constant appearing in Φ, i.e., $\langle \|\Phi\| \rangle$, is at most ℓ.
- For every $p \in \mathbb{P}(\Phi)$, consider a solution $\boldsymbol{b}_p$ of Φ modulo p minimizing $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) :$ f is in the left-hand side of a divisibility in $\Phi\}$. Then, $\log_2\left(\prod_{p \in \mathbb{P}(\Phi)} p^{\mu_p+1}\right) \leq w$.
- Φ has at most m divisibilities.
- Φ has at most d variables.

Since we want to find an upper bound for Γ, assume without loss of generality that $\Gamma(r, \ell, w, m, d)$ is always at least $\min(\ell, w)$. Let us prove Claim 8.

Claim 8.
$$\begin{cases} \Gamma(1, \ell, w, m, d) \leq w + 3 \\ \Gamma(r+1, \ell, w, m, d) \leq \Gamma(r, \\ \qquad 2^{105} m^{27} (d+2)^{38} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w) \cdot (\log_2(\ell + w))^6, \\ \qquad 2^{109} m^{29} (d+2)^{39} \underline{O} \cdot \log_2(\underline{O})^6 (\ell + w) \cdot (\log_2(\ell + w))^6, \\ \qquad m, \\ \qquad d). \end{cases}$$

Analysis on $\Gamma(1,\ell,w,m,d)$: This case corresponds to the base case of the main induction, where the solutions are found thanks to the system of congruences in Equation (4), where for $p \in \mathbb{P}(\Phi)$, $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f$ is in the left-hand side of a divisibility of $\Phi\}$. From the Chinese remainder theorem, this system of congruences has a solution where every variable is in $[1, \prod_{p\in\mathbb{P}(\Phi)} p^{\mu_p+1}]$. Therefore, every variable is bounded by 2^w by definition of w, and therefore its bit length is bounded by $w+3$, since $\langle x\rangle = 1 + \lceil \log_2(|x|+1)\rceil \le \lceil \log_2(|x|)\rceil + 2 \le \log_2(|x|) + 3$, and w is positive.

Analysis on $\Gamma(r,\ell,w,m,d)$ with $r \ge 2$: This case corresponds to the induction step of the main induction, where the solutions are found thanks to the system of (non)congruences in Equation (6). At the start of the induction, we add the elimination property to Φ. According to Lemma 7, we obtain a system Ψ with $n \le m\cdot(d+2)$ divisibilities and $\langle\|\Psi\|\rangle \le \underline{O}(m^3 d+1)\cdot\log_2((d+1)(m+\|\Phi\|+2))+3$. We find solutions $\boldsymbol{b}_p$ for Ψ modulo p, for every $p \in \mathbf{P}_+(\Psi)$. For $p\in\mathbb{P}(\Phi)$, these are the solutions $\boldsymbol{b}_p$ for Φ modulo p stated in the hypothesis of the theorem. For $p \in \mathbf{P}_+(\Psi)\setminus\mathbb{P}(\Phi)$, we compute $\boldsymbol{b}_p$ as a solution for Φ modulo p, taken such that for every f left-hand side of a divisibility in Φ, $v_p(f(\boldsymbol{b}_p)) = 0$. The existence of such a solution is guaranteed by Lemma 3, and as discussed when presenting the procedure the vector $\boldsymbol{b}_p$ is a solution for Ψ modulo p such that for every f left-hand side of a divisibility in Ψ, $v_p(f(\boldsymbol{b}_p)) = 0$. As usual, given $p\in\mathbf{P}_+(\Psi)$, let $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f$ is in the left-hand side of a divisibility of $\Psi\}$.

Suppose that the set $X_1 = \{x_1,\dots,x_{d'}\}$ of variables considered in this step is ordered as $x_1 \prec \dots \prec x_{d'}$ (with $d' \le d$). Recall that the values assigned to these variables are chosen inductively, starting with x_1 and following the order $\prec$. Let $\boldsymbol{\nu}$ be the map computed in this way. Given $k\in[0,d-1]$, at the $(k+1)$-th iteration we defined the set P_k as

$$P_k \coloneqq \{p\in\mathbb{P} : p\in\mathbf{P}_+(\Psi) \text{ or there is } h\in S(\Delta(\Psi))\setminus\{0\} \text{ s.t. } \mathrm{LV}(h)\preceq x_k \text{ and } p \mid h(\boldsymbol{\nu}(x_1,\dots,x_k))\},$$

and added to it the smallest prime not in $\mathbf{P}_+(\Psi)$, if the above definition yields $P_k = \mathbf{P}_+(\Psi)$.

For simplicity, below let $s \coloneqq \#S(\Delta(\Psi))$, $t\coloneqq\|S(\Delta(\Psi))\|$ and $w_1 \coloneqq \log_2(\prod_{p\in\mathbf{P}_+(\Psi)} p^{\mu_p+1})$, which are all at least 1.

Inductively on $k\in[0,d-1]$, we show that $\log_2(\boldsymbol{\nu}(x_{k+1}))\le B$ where

$$B \coloneqq C\cdot(\log_2(C))^3 \quad\text{and}\quad C\coloneqq 2^4\cdot w_1\cdot s^3\cdot\big(5+\log_2\log_2(t\cdot(d+1))\big)^2.$$

Therefore, $\langle\boldsymbol{\nu}(x_{k+1})\rangle \le B+3 \le 2^{18}\cdot s^4\cdot\big(5+\log_2\log_2(t\cdot(d+1))\big)^3\cdot w_1\cdot(\log_2(w_1)+2)^3$, where this last inequality follows from a straightforward computation together with the fact that $(\log_2(x))^3 \le 5\cdot x$ for every $x\ge 1$. Note that we do not simplify $(\log_2(w_1+2))^3$ into $5\cdot(w_1+2)$, as this would yield an exponentially worse bound for $\Gamma(r,\ell,\eta,m,d)$ later on.

base case $k=0$. In this case, $P_0 = \mathbf{P}_+(\Psi)\cup\{p\}$ where p is the smallest prime not in $\mathbf{P}_+(\Psi)$. Then, $\#P_0 = \#\mathbf{P}_+(\Psi)+1$. We bound $\boldsymbol{\nu}(x_1)\in\mathbb{Z}_+$ by applying Theorem 3 to the system of (non)congruences in Equation (6). We get:

$$\begin{aligned}\boldsymbol{\nu}(x_1) &\le \Big(\prod_{p\in\mathbf{P}_+(\Psi)} p^{\mu_p+1}\Big)\cdot\big((s+1)\cdot\#(P_0\setminus\mathbf{P}_+(\Psi))\big)^{4\cdot(s+1)^2(3+\ln\ln(\#(P_0\setminus\mathbf{P}_+(\Psi))+1))}\\ &\le \Big(\prod_{p\in\mathbf{P}_+(\Psi)} p^{\mu_p+1}\Big)\cdot(s+1)^{12\cdot(s+1)^2}\end{aligned}$$

Therefore, $\log_2(\boldsymbol{\nu}(x_1)) \le w_1 + 12\cdot(s+1)^2\log(s+1)$.

induction step $k \geq 1$. Let us first bound $\#(P_k \setminus \mathbf{P}_+(\Psi))$. By definition,

$$P_k \setminus \mathbf{P}_+(\Psi) = \{p \in \mathbb{P} \setminus \mathbf{P}_+(\Psi) : \mathrm{LV}(h) \preceq x_k \text{ and } p \mid h(\boldsymbol{\nu}(x_1, \dots, x_k)) \text{ for some } h \in S(\Delta(\Psi)) \setminus \{0\}\}.$$

By induction hypothesis, for every $h \in S(\Delta(\Psi))$, $|h(\boldsymbol{\nu}(x_1, \dots, x_k))| \leq (k \cdot 2^B + 1) \cdot t$, and therefore $\#(P_k \setminus \mathbf{P}_+(\Psi)) \leq s \cdot \log_2((k \cdot 2^B + 1) \cdot t) \leq s \cdot \log_2(2^B \cdot t \cdot (d+1))$. Note that $s \cdot \log_2(2^B \cdot t \cdot (d+1)) \geq 1$, hence this bound on $\#(P_k \setminus \mathbf{P}_+(\Psi))$ already capture the case where one prime had to be added to P_k in order to make this set different form $\mathbf{P}_+(\Psi)$. We bound $\boldsymbol{\nu}(x_1) \in \mathbb{Z}_+$ by applying Theorem 3 to the system of (non)congruences in Equation (6):

$$\begin{aligned}
\boldsymbol{\nu}(x_{k+1}) &\leq \Big(\prod_{p \in \mathbf{P}_+(\Psi)} p^{\mu_p + 1} \Big) \cdot \big((s+1) \cdot \#(P_k \setminus \mathbf{P}_+(\Psi)) \big)^{4 \cdot (s+1)^2 (3 + \ln \ln (\#(P_k \setminus \mathbf{P}_+(\Psi)) + 1))} \\
&\leq \Big(\prod_{p \in \mathbf{P}_+(\Psi)} p^{\mu_p + 1} \Big) \cdot \big((s+1)^2 \cdot \log_2(2^B t \cdot (d+1)) \big)^{4 \cdot (s+1)^2 (3 + \ln \ln (1 + s \cdot \log_2(2^B t \cdot (d+1))))}.
\end{aligned}$$

Then, a simple analysis using properties of logarithms shows that $\log_2(\boldsymbol{\nu}(x_{k+1}))$ is at most

$$\begin{aligned}
&2^4 \cdot w_1 \cdot s^3 \cdot \big(5 + \log_2 \log_2 (t \cdot (d+1))\big)^2 \cdot (\log_2(B))^2 \\
=\, &C \cdot (\log_2(B))^2 && \text{definition of } C. \\
\leq\, &B,
\end{aligned}$$

where the latter inequality holds from the fact that, whenever $C \geq 45$, every element x_i of the recurrence relation $\big(x_0 = C,\ x_{i+1} = C \cdot (\log_2(x_i))^2\big)$ is bounded by $C \cdot (\log_2(C))^3$, i.e., B.

We have established that the bit length of the solutions for the variables in X_1 can be bounded with $B + 3$. Next, we want to bound $B + 3$ using the arguments of Γ. To do so, we first derive upper bounds for s, t and w_1. For s and t, from Lemma 9 we obtain $s \leq 8 \cdot m^4 \cdot (d+2)^6$ and $\log_2(t) \leq 2 \cdot (d+2) \cdot (\langle \|\Phi\| \rangle + 1) + 1$. For w_1, we have

$$\begin{aligned}
w_1 &\leq \log_2 \Big(\prod_{p \in \mathbf{P}_+(\Psi)} p^{\mu_p + 1} \Big) \\
&\leq \log_2 \Big(\prod_{p \in \mathbf{P}_+(\Psi) \setminus \mathbb{P}(\Phi)} p^{\mu_p + 1} \cdot \prod_{p \in \mathbb{P}(\Phi)} p^{\mu_p + 1} \Big) \\
&\leq \log_2 \Big(\prod_{p \in \mathbf{P}_+(\Psi) \setminus \mathbb{P}(\Phi)} p^{\mu_p + 1} \Big) + w \\
&\leq \log_2 \Big(\prod_{p \in \mathbf{P}_+(\Psi) \setminus \mathbb{P}(\Phi)} p \Big) + w && \mu_p = 0 \text{ for all } p \notin \mathbb{P}(\Phi) \\
&\leq \log_2 \Big(\prod_{p \in \mathbf{P}_+(\Psi)} p \Big) + w \\
&\leq 64 \cdot n^5 (d+2)^4 (\langle \|\Psi\| \rangle + 2) + w && \text{by Lemma 4} \\
&\leq 64 \cdot (m \cdot (d+2))^5 (d+2)^4 (\underline{O}(m^3 d + 1) \cdot \log_2((d+1)(m + \|\Phi\| + 2)) + 5) + w \\
&\leq 128 \cdot \underline{O} \cdot m^9 (d+2)^{11} \cdot (\ell + w).
\end{aligned}$$

Then, $B + 3$ is bounded as follows:

$$B + 3 \leq 2^{18} \cdot s^4 \cdot \big(5 + \log_2 \log_2 (t \cdot (d+1))\big)^3 \cdot w_1 \cdot (\log_2(w_1) + 2)^3$$

$$
\begin{aligned}
&\leq 2^{30} \cdot m^{16}(d+2)^{24}\big(5+\log_2\log_2(t\cdot(d+1))\big)^3 \cdot w_1 \cdot (\log_2(w_1)+2)^3 && \text{bound on } s\\
&\leq 2^{38} \cdot m^{16}(d+2)^{25}(1+\log_2(\langle\|\Psi\|\rangle+1))^3 \cdot w_1 \cdot (\log_2(w_1)+2)^3 && \text{bound on } \log_2(t)\\
&\leq 2^{54} \cdot m^{17}(d+2)^{26}\log_2(\underline{O})^3 \cdot (2+\log_2(\ell))^3 \cdot w_1 \cdot (\log_2(w_1)+2)^3 && \text{bound on } \langle\|\Psi\|\rangle\\
&\leq 2^{104} \cdot m^{27}(d+2)^{38}\underline{O} \cdot \log_2(\underline{O})^6 \cdot (\ell+w) \cdot (\log_2(\ell+w))^6 && \text{bound on } w_1.
\end{aligned}
$$

The procedure continues by recursively computing a positive integer solution for the formula $\Phi'(\boldsymbol{y}) \coloneqq \Phi[\boldsymbol{\nu}(\boldsymbol{x}) \,/\, x : x \in X_1]$, which is s-increasing for some $s \leq r-1$. In the recursion, the procedure uses solutions $\boldsymbol{b}_p$ for Φ' modulo p for every $p \in \mathbb{P}(\Phi')$, computed according to Claim 7. Hence, to conclude the analysis on Γ, it suffices to find positive integers ℓ', w', m', d' such that Φ' is one of the formulae considered for $\Gamma(r-1,\ell',w',m',d')$. Let us bound these integers:

- Φ' has fewer variables and divisibilities than Φ, therefore we can choose $m' = m$ and $d' = d$.
- The coefficients of the variables in the polynomials of Φ' are all from Φ, therefore their bit-length is bounded by ℓ. Let us bound the constants of the polynomials in Φ'. These constants have the form $f(\boldsymbol{\nu}(\boldsymbol{x}))$ with f being a polynomial with coefficients and constant bounded from Φ. So, $\langle\|f(\boldsymbol{\nu}(\boldsymbol{x}))\|\rangle \leq \langle 2^B \cdot \|\Phi\| \cdot d + \|\Phi\|\rangle$, and from the bounds on $B+3$ we can set
$$\ell' = 2^{105} \cdot m^{27}(d+2)^{38}\underline{O} \cdot \log_2(\underline{O})^6 \cdot (\ell+w) \cdot (\log_2(\ell+w))^6.$$
- Let $\mu_p \coloneqq \max\{v_p(f(\boldsymbol{b}_p)) : f \text{ is in the left-hand side of a divisibility in } \Phi'\}$. Thanks to Claim 7, if $p \in \mathbf{P}_+(\Psi)$, then $\mu_p = \max\{v_p(f(\boldsymbol{b}_p)) : f \text{ is in the left-hand side of a divisibility in } \Psi\}$, and otherwise if $p \notin \mathbf{P}_+(\Psi)$, then μ_p is the p-adic valuation of a constant left-hand side of Φ'. We derive the following bound on $\log_2\Big(\prod_{p\in\mathbb{P}(\Phi')} p^{\mu_p+1}\Big)$, which yields a value for w':
$$
\begin{aligned}
&\log_2\Big(\prod_{p\in\mathbb{P}(\Phi')} p^{\mu_p+1}\Big)\\
&= \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')\setminus\mathbf{P}_+(\Psi)} p^{\mu_p+1}\Big) + \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')\cap\mathbf{P}_+(\Psi)} p^{\mu_p+1}\Big)\\
&\leq \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')\setminus\mathbf{P}_+(\Psi)} p^{\mu_p}\Big) + \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')\setminus\mathbf{P}_+(\Psi)} p\Big) + \log_2\Big(\prod_{p\in\mathbf{P}_+(\Psi)} p^{\mu_p+1}\Big)\\
&\leq \log_2\Big(\prod_{\substack{\alpha \text{ constant and}\\ \text{left-hand side in } \Phi'}} \alpha\Big) + \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')} p\Big) + w_1 && \text{from Claim 7}\\
&\leq m \cdot \langle\|\Phi'\|\rangle + \log_2\Big(\prod_{p\in\mathbb{P}(\Phi')} p\Big) + w_1\\
&\leq m \cdot \langle\|\Phi'\|\rangle + m^2(d+2)(\langle\|\Phi'\|\rangle+2) + w_1 && \text{from Lemma 4}\\
&\leq 2^{109} \cdot m^{29}(d+2)^{39}\underline{O} \cdot \log_2(\underline{O})^6 \cdot (\ell+w) \cdot (\log_2(\ell+w))^6 = w'.
\end{aligned}
$$

Note that since the bound we obtained for ℓ' is greater than $B+3$, the value
$$\Gamma(r-1,\ 2^{104} \cdot m^{27}(d+2)^{38}\underline{O} \cdot \log_2(\underline{O})^6 \cdot (\ell+w) \cdot (\log_2(\ell+w))^6,\ w',\ m,\ d)$$
bounds not only the bit length of the minimal positive solution of Φ', but also of the solutions assigned to variables in X_1. This concludes the proof of Claim 8.

References

[1] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Vol 1: Efficient Algorithms.* Foundations of Computing. MIT Press, 1996. ISBN 978-0262024051.

[2] A. P. Bel'tyukov. Decidability of the universal theory of natural numbers with addition and divisibility. *J. Sov. Math.*, pages 1436–1444, 1980. doi: 10.1007/BF01693974.

[3] Itshak Borosh and Leon Bruce Treybig. Bounds on positive integral solutions of linear diophantine equations. *Proc. Am. Math. Soc.*, 55(2):299–304, 1976. doi: 10.2307/2041711.

[4] Viggo Brun. *Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare*, volume 34(8) of *Arch. Math. Naturvidenskab.* 1915.

[5] Alina Carmen Cojocaru and M. Ram Murty. *An Introduction to Sieve Methods and Their Applications.* Cambridge University Press, 2005. doi: 10.1017/CBO9780511615993.

[6] Florent Guépin, Christoph Haase, and James Worrell. On the existential theories of Büchi arithmetic and linear p-adic fields. In *Proc. Symposium on Logic in Computer Science, LICS*, pages 1–10, 2019. doi: 10.1109/LICS.2019.8785681.

[7] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* 4th edition, 1975.

[8] George Havas, Bohdan S. Majewski, and Keith R. Matthews. Extended GCD and Hermite normal form algorithms via lattice basis reduction. *Exp. Math.*, 7(2):125–136, 1998.

[9] Hendrik W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983. doi: 10.1287/moor.8.4.538.

[10] Richard M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, The IBM Research Symposia Series, pages 85–103, 1972.

[11] Jochen Koenigsmann. *Undecidability in Number Theory*, pages 159–195. Springer Berlin Heidelberg, 2014. doi: 10.1007/978-3-642-54936-6.

[12] Antonia Lechner, Joël Ouaknine, and James Worrell. On the complexity of linear arithmetic with divisibility. In *Proc. Symposium on Logic in Computer Science, LICS*, pages 667–676, 2015. doi: 10.1109/LICS.2015.67.

[13] Anthony W. Lin and Rupak Majumdar. Quadratic word equations with length constraints, counter systems, and Presburger arithmetic with divisibility. *Log. Methods Comput. Sci.*, 17 (4), 2021. doi: 10.46298/lmcs-17(4:4)2021.

[14] Leonard Lipshitz. The Diophantine problem for addition and divisibility. *Trans. Am. Math. Soc*, pages 271–283, 1978. doi: 10.2307/1998219.

[15] Leonard Lipshitz. Some remarks on the Diophantine problem for addition and divisibility. *Bull. Soc. Math. Belg. Sér. B*, 33(1):41–52, 1981.

[16] Yuri Matijasevič. Enumerable sets are diophantine. *J. Sov. Math.*, 11:354–357, 1970. doi: 10.2307/2272763.

[17] Julia Robinson. Definability and decision problems in arithmetic. *J. Symb. Log.*, 14(2):98–114, 1949. doi: 10.2307/2266510.

[18] Barkley Rosser. The n-th prime is greater than $n \log(n)$. *Proc. London Math. Soc.*, pages 21–44, 1939. doi: 10.1112/plms/s2-45.1.21.

[19] Alexander Schrijver. *Theory of linear and integer programming.* Wiley-Interscience series in discrete mathematics and optimization. Wiley, 1999. ISBN 978-0-471-98232-6.

[20] Mikhail R. Starchak. Positive existential definability with unit, addition and coprimeness. In *Proc. International Symposium on Symbolic and Algebraic Computation, ISSAC*, pages 353–360, 2021. doi: 10.1145/3452143.3465515.

[21] Mikhail R. Starchak. A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. I. definitions and GCD-lemma. *Vestnik St. Petersb. Univ. Math.*, 54:264–272, 2021. doi: 10.1134/S1063454121030080.

[22] Mikhail R. Starchak. A proof of Bel'tyukov–Lipshitz theorem by quasi-quantifier elimination. II. the main reduction. *Vestnik St. Petersb. Univ. Math.*, 54:372–380, 2021. doi: 10.1134/S106345412104018X.

[23] Lou van den Dries and Andrew J. Wilkie. The laws of integer divisibility, and solution sets of linear divisibility conditions. *J. Symb. Log.*, 68(2):503–526, 2003. doi: 10.2178/jsl/1052669061.

[24] Wilberd Van Der Kallen. Complexity of the Havas, Majewski, Matthews LLL Hermite normal form algorithm. *J. Symb. Comput.*, 30(3):329–337, 2000. doi: 10.1006/jsco.2000.0374.

[25] Joachim von zur Gathen and Malte Sieveking. A bound on solutions of linear integer equalities and inequalities. *Proc. Am. Math. Soc.*, 72(1):155–158, 1978. doi: 10.2307/2042554.