Available online at www.sciencedirect.com

ScienceDirect

Journal of Complexity 23 (2007) 82–107

Journal of COMPLEXITY

www.elsevier.com/locate/jco

Counting solutions to binomial complete intersections

Eduardo Cattani[a,1], Alicia Dickenstein[b,*,2]

[a] *Department of Mathematics and Statistics, University of Massachusetts, Amherst, MA 01003, USA*

[b] *Departamento de Matematica, FCEyN, Universidad de Buenos Aires, (1428) Buenos Aires, Argentina*

Received 25 October 2005; accepted 24 April 2006

Available online 21 June 2006

Abstract

We study the problem of counting the total number of affine solutions of a system of n binomials in n variables over an algebraically closed field of characteristic zero. We show that we may decide in polynomial time if that number is finite. We give a combinatorial formula for computing the total number of affine solutions (with or without multiplicity) from which we deduce that this counting problem is $\#P$-complete. We discuss special cases in which this formula may be computed in polynomial time; in particular, this is true for generic exponent vectors.

Keywords: Binomial ideal; Complete intersection; $\#P$-complete

1. Introduction

A *binomial ideal* in the ring $k[x_1, \ldots, x_n]$ of polynomials with coefficients in a field k, is an ideal generated by binomials: $ax^{\alpha} - bx^{\beta}$, where $\alpha, \beta \in \mathbb{N}^n$ and $a, b \in k^*$. Binomial ideals are quite ubiquitous in very different contexts particularly those involving toric geometry and its applications [10,28], in the study of semigroup algebras, and in the modern versions of hypergeometric systems of differential equations [25,7]. While binomial ideals are quite amenable to Gröbner and standard bases techniques [19,20], they also provide some of the “worst-case” examples in computational algebra, such as the Mayr–Meyer ideals [22].

* Corresponding author. Fax: +54 11 4576 3351.

E-mail addresses: cattani@math.umass.edu (E. Cattani), alidick@dm.uba.ar (A. Dickenstein).

[1] E. Cattani was partially supported by NSF Grant DMS-0099707. Part of this work was done while he was visiting the University of Buenos Aires supported by a Fulbright Fellowship for Lecturing and Research; he is grateful for their hospitality and sponsorship.

[2] A. Dickenstein is partially supported by UBACYT and CONICET, Argentina.

0885-064X/$ - see front matter
doi:10.1016/j.jco.2006.04.004

In this paper we consider ideals generated by n binomials in $R := k[x_1, \ldots, x_n]$, with $\mathrm{char}(k) = 0$. Let $\bar{k}$ denote the algebraic closure of k. We are interested in determining when the number of solutions in $\bar{k}^n$ is finite and non-zero (i.e., when the given binomials define a complete intersection in R) and, in this case, to count the number of solutions, with or without multiplicity. We will obtain properties of these ideals directly in terms of the given data: the exponents α, β, and the coefficients a, b.

Our starting point is then a system of n binomials in R, with non-zero coefficients. Thus, we may assume that they are of the form

$$p_j(c; x) := x^{\alpha_j} - c_j x^{\beta_j}, \quad j = 1, \ldots, n, \tag{1.1}$$

where $\alpha_j, \beta_j \in \mathbb{N}^n$, $\alpha_j \neq \beta_j$. Let $\mathcal{J}$ be the ideal generated by $p_1, \ldots, p_n$ in the polynomial ring $k(c)[x]$. Given a choice of coefficients $c \in (k^*)^n$, let $\mathcal{J}_c$ be the ideal in R generated by $p_1(c; x), \ldots, p_n(c; x)$ and $\mathbb{V}_c \subset \bar{k}^n$ the variety defined by $\mathcal{J}_c$.

Proposition 2.1, which is a restatement of results in [10], gives a complete picture of the number of solutions of system (1.1) in the algebraic torus $(\bar{k}^*)^n$. Let B be the matrix

$$B := \begin{pmatrix} \alpha_1 - \beta_1 \\ \alpha_2 - \beta_2 \\ \vdots \\ \alpha_n - \beta_n \end{pmatrix}, \tag{1.2}$$

whose jth row is the vector $\alpha_j - \beta_j$. Then, for generic coefficients $c \in (k^*)^n$, $\mathbb{V}_c \cap (\bar{k}^*)^n$ consists of $|\det B|$-many points all of which have multiplicity one (this may be seen directly or as a simple instance of Bernstein's theorem). In fact, if $\det B \neq 0$, this is true for all $c \in (k^*)^n$. On the other hand, if $\det B = 0$, then, for coefficients $c \in (k^*)^n$ not satisfying the algebraic conditions (2.2) it holds that $\mathbb{V}_c \cap (\bar{k}^*)^n = \emptyset$, while if the coefficients satisfy (2.2), the variety $\mathbb{V}_c \cap (\bar{k}^*)^n$ has codimension equal to the rank of B. We set $\delta := |\det B|$.

Deciding whether system (1.1) has a non-empty, finite set of solutions in $\bar{k}^n$ is more involved. We must, first of all, consider the possibility that some exponent vector α_j or β_j may vanish. This is equivalent to the statement that some variables x_j are invertible modulo the ideal $\mathcal{J}$. The reduction to the case when this does not happen is accomplished in Proposition 2.5. We may then assume that $0 \in \mathbb{V}_c$ for all choice of coefficients. Now, in the generic case $\det B \neq 0$, Theorem 2.6 gives a condition on the exponents of the system that guarantees that system (1.1) is a complete intersection for all $c \in (k^*)^n$. If, on the other hand, $\det B = 0$, Theorem 2.6 only implies that (1.1) is a complete intersection for a generic set of coefficients $c \in (k^*)^n$. Indeed, in this case, algebraic conditions such as (2.2) enter into play. This leads to the notion of *generic complete intersection*, that we will abbreviate by *gci*. We will say that $p_1, \ldots, p_n$ is a gci if $\mathcal{J}_c$ is a complete intersection in R , i.e., $\mathbb{V}_c$ is a finite non-empty set, for generic coefficients $c \in (k^*)^n$.

Even though Theorem 2.6 gives a combinatorial criterion for deciding if $p_1, \ldots, p_n$ is a gci, its verification requires 2^n steps. One of the main results of this paper is Theorem 2.12 where we describe a polynomial-time algorithm to decide whether $p_1, \ldots, p_n$ is a gci directly from the exponents α_j, β_j.

Given a generic complete intersection $p_1, \ldots, p_n$, let

$$d := \dim_k k[x_1, \ldots, x_n]/\mathcal{J}_c, \quad D := \dim_k k[x_1, \ldots, x_n]/\sqrt{\mathcal{J}_c} \tag{1.3}$$

be the total number of points in the variety $\mathbb{V}_c$, counted with and without multiplicity. Given an index set $L \subset \{1, \ldots, n\}$, we denote by μ_L, the number of points in $\mathbb{V}(\mathcal{J}) \cap \bar{k}^n_L$, $\bar{k}^n_L := \{x \in \bar{k}^n :$

$x_\ell = 0$ if and only if $\ell \in L\}$, counted with multiplicity. We set $[n] := \{1, \ldots, n\}$ and $\mu := \mu_{[n]}$, the multiplicity at the origin.

In Section 3 we compute d, D, and μ_L for a gci. A key ingredient is what we call *parametric reduction*, which allows us to reduce the study of generic complete intersection binomial ideals to a particular class of ideals with a normalized presentation. We show in Theorem 3.2 that we can keep track of the various multiplicities through the process of parametric reduction. We then compute d and D for so-called *irreducible systems*. We show that an irreducible system that is in normal form may behave in one of three possible ways: its binomials are a standard basis for either a global or a local term order, or they are weighted homogeneous. This allows us to read off the dimension and multiplicities from the exponents (cf. Theorem 3.5). Interestingly, the linear algebra problem that underlies these results appeared in the work of Vinberg about Cartan matrices [18, Theorem 4.3]. For generic exponents, a binomial system in normal form is irreducible and has $\det B \neq 0$. Hence, Theorem 3.5 gives a polynomial time algorithm for computing the number of solutions of a complete intersection binomial system with generic exponents and arbitrary non-zero coefficients.

We next consider the case of a general gci. Using a well-known quadratic-time algorithm, due to Tarjan [30], we find a block decomposition of the system into irreducible ones. From this decomposition we construct an acyclic directed graph naturally attached to the system. In Theorem 3.15, we give an explicit combinatorial formula to compute the dimensions and multiplicities of the system from this graph.

Section 4 is devoted to counting complexity issues. We reverse the correspondence from binomial systems to acyclic digraphs and assign to each such graph a simple binomial system. The number of solutions of this system corresponds to invariants of the graph whose computation is known to be $\#P$-complete. Indeed, we show that particular instances correspond to counting independent sets in bipartite graphs, or more generally, antichains in a poset; both of these problems are known to be $\#P$-complete [31,24]. Hence, even though the problem of deciding whether a system is a gci as well as the problem of counting the number zeros in the torus of the binomial system defined by (1.1), are solvable in polynomial time, we prove in Theorem 4.3 that counting the total number of affine solutions, with or without multiplicity, is a $\#P$-complete problem. Thus, binomial systems furnish a very simple example of the type of problems, “easy” to decide but “hard” to count that motivated Valiant’s introduction of the notion of counting complexity [31]. Finally, in Proposition 4.5 we identify another class of systems whose solutions may be computed in polynomial time.

The last section of the paper is devoted to brief discussions of some of the applications of this work which motivated our study. We show, first of all, how Theorem 3.15 may be applied to compute the multiplicity and geometric degree [2] of the primary components of a lattice basis ideal $J \subset k[x_1, \ldots, x_m]$. This, in turn, may be used to describe the holonomic rank of Horn systems of hypergeometric partial differential equations and to study sparse discriminants, generalizing the codimension-two case. [8,7]. Finally, we recall the results of [29, Chapter 10] relating the study of systems of partial differential equations with constant coefficients with that of the corresponding algebraic system.

2. Complete intersections and normal forms

We begin by considering the question of when binomials $p_1(c; x), \ldots, p_n(c; x)$ as in (1.1) define a complete intersection when viewed as elements of the Laurent polynomial ring $S := k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. Let B be the $n \times n$ exponent matrix defined in (1.2). We note that even though the rows of B are only defined up to sign, this will not affect our arguments. It follows from [10, Theorem 2.1] that if $\det B \neq 0$ then, for any choice of coefficients in $(k^*)^n$, $p_1(c;x),\ldots,p_n(c;x)$ define a regular sequence in S. Moreover, the system of equations

$$p_j(c;x)=0, \quad j=1,\ldots,n \tag{2.1}$$

has $|\det B|$-many solutions in the algebraic torus $(\bar{k}^*)^n$ and all of them are simple.

On the other hand, if $\det B=0$ then $p_1(c;x),\ldots,p_n(c;x)$ do not define a complete intersection in S for any choice of coefficients. Indeed, if system (2.1) has a solution $x\in(\bar{k}^*)^n$, it will necessarily have infinitely many. Let $\mathcal{R}$ be the lattice of relations

$$\mathcal{R}:=\left\{m\in\mathbb{Z}^n:\sum_{j=1}^n m_j(\alpha_j-\beta_j)=0\right\}.$$

For any $m\in\mathcal{R}$ we have a $\bar{k}^*$-action on the set of solutions of (2.1) defined by $(t;x)\mapsto(t^{m_1}x_1,\ldots,t^{m_n}x_n)$, and therefore the set of solutions could never be finite. Note also that if $\det B=0$ then, for generic coefficients c_j, (2.1) has no solutions. In fact, if $x\in(\bar{k}^*)^n$ is a solution of (2.1) we have

$$x^{\alpha_j-\beta_j}=c_j \quad \text{for all } j=1,\ldots,n,$$

and therefore

$$\prod_{j=1}^n c_j^{m_j}=1 \quad \text{for all } m\in\mathcal{R}.$$

Thus, if $v^1,\ldots,v^r$ is a basis of $\mathcal{R}$, a necessary condition for $p_1(c;x),\ldots,p_n(c;x)$ to have a solution in $(\bar{k}^*)^n$ is that

$$\prod_{j=1}^n c_j^{v_j^\ell}=1 \quad \text{for all } \ell=1,\ldots,r. \tag{2.2}$$

This condition is also sufficient. Suppose that (2.2) holds and let $\mathcal{L}$ be the sublattice of $\mathbb{Z}^n$ spanned by $\alpha_j-\beta_j$, $j=1,\ldots,n$. Denote by $\rho:\mathcal{L}\to\bar{k}^*$ the group homomorphism (i.e., the partial character) defined by

$$\rho(\alpha_j-\beta_j)=c_j.$$

The equalities in (2.2) imply that ρ is well-defined and, since up to a monomial (which is invertible in the Laurent polynomial ring),

$$p_j(x)=x^{\alpha_j-\beta_j}-\rho(\alpha_j-\beta_j),$$

it follows from [10, Theorem 2.6] that $p_1(c;x),\ldots,p_n(c;x)$ define an ideal in S of codimension equal to the rank of $\mathcal{L}$. Hence we obtain:

Proposition 2.1. *Let $p_1(c;x),\ldots,p_n(c;x)$ be as in* (1.1) *and B as above. For any choice of coefficients $c\in(k^*)^n$, the ideal they generated in S is a complete intersection if and only if*

$\det B \neq 0$. *If* $\det B = 0$ *and the identities* (2.2) *are satisfied then the binomials* (1.1) *define an ideal in S of codimension equal to the rank of B.*

In the remaining part of this section, we will discuss criteria for deciding when $p_1, \ldots, p_n$ is a gci. Since we are not assuming that $\operatorname{supp}(\alpha_j) \cap \operatorname{supp}(\beta_j) = \emptyset$, where, for $v \in \mathbb{R}^n$:

$$\operatorname{supp}(v) := \{i \in [n] : v_i \neq 0\},$$

the matrix B, by itself, does not allow us to recover the exponents of the binomials (1.1). It is useful to introduce the following concept, already present in the work of Scheja et al. [26]:

Definition 2.2. Let $p_j = x^{\alpha_j} - c_j x^{\beta_j}$, $j = 1, \ldots, n$, be a system of binomials in $k[x_1, \ldots, x_n]$. For each index set $K \subset [n]$, let

$$Z(K) := \{j \in [n] : \operatorname{supp}(\alpha_j) \cap K \neq \emptyset \text{ and } \operatorname{supp}(\beta_j) \cap K \neq \emptyset\}. \tag{2.3}$$

We start by showing that we can restrict ourselves to the case where $0 \in \mathbb{V}_c$. Since this property is equivalent to the statement that all exponent vectors are non-zero, it is independent of the choice of coefficients. We want to identify all indices i for which x_i is invertible modulo the ideal $\mathcal{J}$, i.e., the x_i coordinate of any solution to the system of binomials is necessarily non-zero. Set $I_0 = \emptyset$ and, for $\ell \geqslant 1$, let

$$I_\ell := \bigcup \{\operatorname{supp}(\alpha_j) : \operatorname{supp}(\beta_j) \subset I_{\ell-1}\} \cup \bigcup \{\operatorname{supp}(\beta_j) : \operatorname{supp}(\alpha_j) \subset I_{\ell-1}\}$$

and $I = \bigcup_\ell I_\ell$. Induction on ℓ shows easily that if $i \in I$, the variable x_i is invertible modulo the ideal $\mathcal{J}$ and, conversely, that these are all the variables invertible modulo $\mathcal{J}$. Thus, after reordering of variables and polynomials, we may assume that the variables $x_{r+1}, \ldots, x_n$ are invertible and that the binomials $p_{s+1}, \ldots, p_n$ involve only the variables $x_{r+1}, \ldots, x_n$, while for $j \leqslant s$ both monomials x^{α_j} and x^{β_j} are divisible by at least one of the variables x_i, $i \leqslant r$, i.e., that $Z([r]) = [s]$. Following [13] we define:

Definition 2.3. Let $x' := (x_1, \ldots, x_r)$, $c' := (c_1, \ldots, c_s)$. For $j \leqslant s$, set

$$\hat{p}_j(c'; x') = p_j(c'; (x_1, \ldots, x_r, 1, \ldots, 1)). \tag{2.4}$$

Then, the binomial system $\{\hat{p}_1, \ldots, \hat{p}_s\} \subset k(c')[x']$ is called the *derived system* of $p_1, \ldots, p_n$. We denote by $\hat{B}$ the associated $s \times r$ matrix as in (1.2).

Note that $0 \in \mathbb{V}(\hat{p}_1, \ldots, \hat{p}_s)$ and that the matrix B is of the form

$$B = \begin{pmatrix} \hat{B} & * \\ 0 & B_2 \end{pmatrix}.$$

Lemma 2.4. *Assume* $p_1, \ldots, p_n$ *as in* (1.1) *is a gci and let* r, s *be as above. Then,* $r = s$ *and* $\det(B_2) \neq 0$.

Proof. Since the variables $x_{r+1}, \ldots, x_n$ are all invertible modulo $\mathcal{J}$, the system of equations $p_{s+1} = \cdots = p_n = 0$, is equivalent to the system $x^{\alpha_j - \beta_j} = c_j$, for all $j = s + 1, \ldots, n$. Hence, arguing as in the discussion leading to Proposition 2.1, we see that each integer relation among the vectors $\alpha_j - \beta_j$, $j = s+1, \ldots, n$ imposes a polynomial condition on the coefficients as in (2.2). If $s < r$, then $n - r < n - s$ and so there exists a non-trivial relation. Therefore, $p_1, \ldots, p_n$ has generically no solutions, a contradiction. On the other hand, if $s > r$, or if $r = s$ and $\det(B_2) = 0$, then, generically, the system $p_{s+1}(x_{r+1}, \ldots, x_n) = \cdots = p_n(x_{r+1}, \ldots, n) = 0$ has either no solutions or infinitely many in $(\bar{k}^*)^{n-r}$. Since any solution of these equations may be extended to a solution of (2.1) by setting $x_1 = \cdots = x_r = 0$, we get a contradiction again. So $s = r$ and $\det(B_2) \neq 0$, as claimed. □

Proposition 2.5. *Let $p_1, \ldots, p_n$, B be as above. Assume that $s = r$ and $\det(B_2) \neq 0$. Let $\hat{p}_1, \ldots, \hat{p}_r$ be the derived system. Then $p_1, \ldots, p_n$ is a gci if and only if $\hat{p}_1, \ldots, \hat{p}_r$ is a gci.*

Proof. Assume $p_1, \ldots, p_n$ is a gci and let $\mathcal{U}$ be an open dense subset of $(\bar{k}^*)^n$ such that the binomials with coefficients in $\mathcal{U}$ define a complete intersection ideal in $\bar{k}[x_1, \ldots, x_n]$. It suffices to show that the intersection of $\mathcal{U}$ with the fiber $(\bar{k}^*)^r \times \{(1, \ldots, 1)\}$ is also Zariski dense in the fiber. Let $a'' \in (\bar{k}^*)^{n-r}$ be such that $\mathcal{U} \cap \left((\bar{k}^*)^r \times \{a''\}\right)$ is Zariski dense. Let $\lambda'' \in (\bar{k}^*)^{n-r}$ be a common zero of $p_{r+1}(a''; x), \ldots, p_n(a''; x)$. Then, since $s = r$, the change of variables that sends x_i to itself for $i = 1, \ldots, r$ and

$$x_j \mapsto x_j/\lambda''_j, \quad j = r+1, \ldots, n,$$

transforms any of the last $n - r$ polynomials p_j, $j = r+1, \ldots, n$, into a non-zero multiple of $x^{\alpha_j} - x^{\beta_j}$ and, for $i \leqslant r$, the binomial p_i into a non-zero multiple of

$$x^{\alpha_i} - (\lambda'')^{\alpha''_i - \beta''_i} c_i x^{\beta_i},$$

where $\alpha''_i, \beta''_i \in \mathbb{N}^{n-r}$ denote the vectors consisting of the last $n-r$ coordinates of α_i, β_i. Since this scalar transformation in the coefficient space $(\bar{k}^*)^r$ preserves Zariski dense subsets our assertion follows.

Conversely, assume that $\hat{p}_1, \ldots, \hat{p}_r$ is a gci and that $\det(B_2) \neq 0$. Let φ be a non-zero polynomial such that $\varphi(c') \neq 0$ for a given r-tuple of coefficients $c' = (c_1, \ldots, c_r)$ implies that the corresponding polynomials $\hat{p}_1(c'; x'), \ldots, \hat{p}_r(c'; x')$ define a complete intersection. Denote as before $c'' = (c_{r+1}, \ldots, c_n)$ and consider the rational function

$$\psi(c', c'') = \prod_{\lambda'' \in \mathbb{V}_{c''}} \varphi((\lambda'')^{\alpha''_1 - \beta''_1} c_1, \ldots, (\lambda'')^{\alpha''_r - \beta''_r} c_r).$$

If $\psi(c', c'')$ is defined and non-zero, then for any choice of the $|\det(B_2)|$-many roots λ'' of the last $n - r$ polynomials, the specialized system

$$p_1(c'; (x', \lambda'')) = \cdots = p_r(c'; (x', \lambda'')) = 0$$

has finitely many solutions and, consequently, $p_1, \ldots, p_n$ is a gci. □

The following result is a reformulation of Theorem 2.3 in [13].

Theorem 2.6. *Let $p_1, \ldots, p_n$ be as in* (1.1) *and suppose that* $0 \in \mathbb{V}(\mathcal{J})$. *Then, $p_1, \ldots, p_n$ is a gci if and only if $|Z(K)| \leqslant |K|$ for all $K \subset [n]$.*

Proof. Suppose there exists $K \subset [n]$ such that $|Z(K)| > |K|$. Assume that K is maximal with this property. After reordering, if necessary, we may assume that $K = \{r+1, \ldots, n\}$ and

$Z(K) = \{s+1, \dots, n\}$ where $s < r$. Since $0 \in \mathbb{V}(\mathcal{J})$, the maximality assumption implies that the first s binomials depend only on $x' = (x_1, \dots, x_r)$. Otherwise, we may assume that there exists $k_1 > r$, $k_1 \in \text{supp}(\alpha_s)$. Since $0 \in \mathbb{V}(\mathcal{J})$, $\text{supp}(\beta_s) \neq \emptyset$. If there exists $k_2 > r$, $k_2 \in \text{supp}(\beta_s)$, then $s \in Z(K)$ which is a contradiction. Therefore, $\text{supp}(\beta_s) \subset [r]$ and for any $\ell \in \text{supp}(\beta_s)$, $K' := K \cup \{\ell\}$ satisfies $Z(K) \cup \{s\} \subset Z(K')$. Hence $|Z(K')| > |K'|$ and this contradicts the maximality of K.

Thus, for a given choice of coefficients, the system

$$p_1(c; x') = \cdots = p_s(c; x') = 0 \tag{2.5}$$

is either inconsistent or its solution space has dimension at least $r - s > 0$. Since, any solution of (2.5) can be extended to a solution of the full system by setting the K-coordinates equal to zero, it follows that $p_1, \dots, p_n$ is not a gci.

Conversely, suppose $|Z(K)| \leqslant |K|$ for all $K \subset [n]$. In order to show that $p_1, \dots, p_n$ is a gci it suffices to prove that given any subset $L \subset [n]$, for generic coefficients $p_1(c; x), \dots, p_n(c; x)$ has at most finitely many solutions with zeros in $\bar{k}^n_L$, where

$$\bar{k}^n_L = \{x \in \bar{k}^n : x_\ell = 0 \text{ if and only if } \ell \in L\}. \tag{2.6}$$

Assume that for some choice of coefficients, there exists a solution in $\bar{k}^n_L$. Then, for any $i \notin Z(L)$, p_i depends only on the variables in J, the complement of L in $[n]$ and hence, since $0 \in \mathbb{V}(\mathcal{J})$, $Z(L)^c \subset Z(J)$. Since, by assumption $|Z(L)| \leqslant |L|$ and $|Z(J)| \leqslant |J|$, we deduce that

$$|L| \leqslant |Z(J)^c| \leqslant |Z(L)| \leqslant |L|,$$

and therefore $|Z(L)| = |L|$. Reordering we may assume that $J = Z(J) = [r]$ and let $B_1(L)$ denote the $r \times r$ exponent matrix as in (1.2). If $\det B_1(L) = 0$, then for generic coefficients the first r binomials have no solutions in $(\bar{k}^*)^r$ and hence, generically, $p_1(c; x), \dots, p_n(c; x)$ have no solutions in $\bar{k}^n_L$. On the other hand, if $\det B_1(L) \neq 0$ then, for all choices of coefficients in $(k^*)^r$, there exists finitely many solutions of $p_1 = \cdots = p_r = 0$ in $(\bar{k}^*)^r$ and hence finitely many solutions of $p_1(c; x), \dots, p_n(c; x)$ with zeros exactly in L. $\square$

Remark 2.7. Note that in the proof of Theorem 2.6 we have shown that if $p_1, \dots, p_n$ is a gci, $L \subset [n]$, and $\bar{k}^n_L$ is as in (2.6), then, for generic coefficients, there exists a solution in $\bar{k}^n_L$ if and only if $|Z(L)| = |L|$ and, after reordering so that $Z(L) = L = \{r+1, \dots, n\}$, the binomials $p_1, \dots, p_r$ depend only on the first r variables, and the corresponding $r \times r$ exponent matrix $B_1(L)$ is non-singular. Moreover, for generic $c \in (k^*)^n$, there are $|\det B_1(L)|$-many points (counted without multiplicity) in $\mathbb{V}_c \cap \bar{k}^n_L$. Then, the number of points in $\mathbb{V}_c$, counted without multiplicity, is given by

$$D = \sum_{\mu_L \neq 0} |\det B_1(L)|, \tag{2.7}$$

where μ_L is the total number of points in $\mathbb{V}_c \cap \bar{k}^n_L$ counted with multiplicity. We will develop in Section 3 the combinatorics needed to describe all sets L with $\mu_L \neq 0$ and we shall show in Section 4 that counting the number of such sets is a $\#P$-complete problem.

Note that if $0 \in \mathbb{V}(\mathcal{J})$, the condition that $p_1, \dots, p_n$ is a gci depends only on the combinatorics of the exponents α_j, β_j. It follows from Proposition 2.1 and Theorem 2.6 that when $\det(B) \neq 0$, if $p_1, \ldots, p_n$ is a gci, then it is a complete intersection for any choice of the coefficients (as long as $c_j \in k^*$).

The variant of the Fischer–Shapiro criterion embodied in Theorem 2.6 allows us to determine whether $p_1, \ldots, p_n$ is a gci. However, this involves checking exponentially many conditions, one for each subset $K \subset [n]$. We will now show how this can be done in a number of steps that depends polynomially (on n). We begin with the following simple corollary to Theorem 2.6.

Corollary 2.8. *Suppose $p_1, \ldots, p_n$ is a gci and $0 \in \mathbb{V}(\mathcal{J})$. Let*

$$\mathcal{M} = \{x^{\alpha_j}, x^{\beta_j};\ j = 1, \ldots, n\}$$

denote the set of monomials appearing in $p_1, \ldots, p_n$. Then for each $i \in [n]$ there exists $r_i > 0$ such that $x_i^{r_i} \in \mathcal{M}$.

Proof. If for some $i \in [n]$, $x_i^{r_i} \notin \mathcal{M}$ for all $r_i > 0$, then $Z(\{1, \ldots, \hat{i}, \ldots, n\}) = [n]$, contradicting Theorem 2.6. □

One can easily give examples showing that the necessary condition in Corollary 2.8 is not sufficient to guarantee that $p_1, \ldots, p_n$ define a gci. However, the following stronger notion provides a sufficient condition.

Definition 2.9. We say that $p_1, \ldots, p_n$ are in *normal form* if and only if for all $i \in [n]$

$$p_i = x_i^{r_i} - c_i x^{\beta_i}, \quad r_i > 0, \quad \beta_i \neq 0.$$

Note that if the system is in normal form then $0 \in \mathbb{V}(\mathcal{J})$.

Proposition 2.10. *Assume $p_1, \ldots, p_n$ are in normal form. Then $p_1, \ldots, p_n$ is a gci.*

Proof. For any $K \subset [n]$, $Z(K) \subset K$ and the result follows from Theorem 2.6. □

We will next show how to reduce ourselves to systems $p_1, \ldots, p_n$ in normal form.

2.1. Parametric reduction

Let $p_1, \ldots, p_n$ be a binomial system and suppose that they satisfy the necessary condition in Corollary 2.8, but that it is not possible to relabel variables and binomials, or invert the coefficient of one or more binomials, so as to put the system in normal form. This means that one of the binomials must contain two monomials of the form $x_i^{r_i}$ and $x_j^{r_j}$ with $i \neq j$. Then, after relabeling we may assume that p_n is of the form

$$p_n = x_n^{\ell} - c_n x_{n-1}^{m}, \quad \ell, m > 0. \tag{2.8}$$

Let $q := \gcd(m, \ell)$ and set $m' := m/q$, $\ell' := \ell/q$. We will consider the polynomial map that sends polynomials in n variables $x_1, \ldots, x_n$ to polynomials in $n-1$ variables $u_1, \ldots, u_{n-1}$:

$$x_i \mapsto u_i, \quad i = 1, \ldots, n-2; \quad x_{n-1} \mapsto u_{n-1}^{\ell'}; \quad x_n \mapsto u_{n-1}^{m'}. \tag{2.9}$$

Let $\tilde{p}_j$, $j = 1, \ldots, n-1$ be the image of the binomials $p_1, \ldots, p_{n-1}$. We will refer to $\tilde{p}_1, \ldots, \tilde{p}_{n-1}$ as a *parametric reduction* of $p_1, \ldots, p_n$ and denote by $\tilde{\mathcal{J}}$ the ideal they generate in $k(c_1, \ldots, c_{n-1})[u_1, \ldots, u_{n-1}]$.

Proposition 2.11. *Suppose $\tilde{p}_1, \dots, \tilde{p}_{n-1}$ is a parametric reduction of $p_1, \dots, p_n$ and let $\tilde{B}$ and B be the associated matrices. Then $|\det B| = q \cdot |\det \tilde{B}|$. Moreover, $0 \in \mathbb{V}(\mathcal{J})$ if and only if $0 \in \mathbb{V}(\tilde{\mathcal{J}})$ and, in this case, $p_1, \dots, p_n$ is a gci if and only if $\tilde{p}_1, \dots, \tilde{p}_{n-1}$ is gci.*

Proof. The matrix B is of the form

$$B = \begin{pmatrix} \tilde{b}_1 & \dots & \tilde{b}_{n-2} & \tilde{b}_{n-1} & \tilde{b}_n \\ 0 & \dots & 0 & -m & \ell \end{pmatrix},$$

where $\tilde{b}_1, \dots, \tilde{b}_n$ are vectors in $\mathbb{Z}^{n-1}$. On the other hand, the matrix $\tilde{B}$ is given by

$$\tilde{B} = \begin{pmatrix} \tilde{b}_1 & \dots & \tilde{b}_{n-2} & \ell' \tilde{b}_{n-1} + m' \tilde{b}_n \end{pmatrix}.$$

The first assertion now follows from a last-row expansion of $\det B$.

Suppose now that $p_1, \dots, p_n$ is not a gci. By Theorem 2.6 there exists $K \subset [n]$ such that $|Z(K)| > |K|$. If $K \subset [n-1]$, then $Z(K) \subset [n-1]$ as well and therefore by Theorem 2.6 $\tilde{p}_1, \dots, \tilde{p}_{n-1}$ is not a gci either. If $n \in K$, then taking $\tilde{K} = K \setminus \{n\}$ we get that $Z(K) \setminus \{n\} \subset Z(\tilde{K})$. Hence $|Z(\tilde{K})| > |\tilde{K}|$ and $\tilde{p}_1, \dots, \tilde{p}_{n-1}$ is not a gci.

Conversely, if $\tilde{p}_1, \dots, \tilde{p}_{n-1}$ is not a gci then there exists $\tilde{K} \subset [n-1]$ such that $|Z(\tilde{K})| > |\tilde{K}|$. If $\tilde{K} \subset [n-2]$ we take $K = \tilde{K}$ and then $Z(K) = Z(\tilde{K})$; if, on the other hand, $n-1 \in \tilde{K}$, then we take $K = \tilde{K} \cup \{n\}$ in which case $Z(K) = Z(\tilde{K}) \cup \{n\}$. In either case $|Z(K)| > |K|$ and we are done. □

The results of this section may be summarized in a polynomial-time algorithm to check whether a binomial system is a gci.

Theorem 2.12. *We may decide in polynomial time whether $p_1, \dots, p_n$ is a gci. Moreover, if it is known that* $\det B \neq 0$ *we can check if $p_1(c; x), \dots, p_n(c; x)$ is a complete intersection in time $O(n^2)$.*

Proof. It is easy to see from the procedure for constructing the derived system that this step may be accomplished in at most $O(n^2)$ steps. If the number of non-invertible variables does not equal the number of binomials in the derived system then, by Lemma 2.4, $p_1, \dots, p_n$ is not a gci. Again by Lemma 2.4 we next check whether $\det B_2 \neq 0$ (this is, of course, unnecessary if it is known that $\det B \neq 0$). If so, Proposition 2.5 allows us to restrict ourselves to the derived system. We move down the list of binomials searching for binomials of the form $x_i^{r_i} - c x_j^{r_j}$. Whenever such a binomial is found we do parametric reduction and reduce by one the number of binomials and of variables. This step is then repeated until there are no longer any binomials of that form. Clearly, this process stops after a quadratic number of steps. Then $p_1, \dots, p_n$ is a gci if and only if Corollary 2.8 holds. This verification can certainly be carried out in quadratically many steps. □

Example 2.13. Consider the following binomials in $k[x_1, \dots, x_8]$:

$$\begin{aligned} &p_1 = x_1^2 - x_2^3, \quad p_2 = x_1 x_2 - x_1 x_3, \quad p_3 = x_1^2 x_2 x_3 - x_3^7, \\ &p_4 = x_4^2 - x_1^2 x_4^3, \quad p_5 = x_5^2 - x_6^4, \quad p_6 = x_5 x_6 - x_2 x_3 x_7^2 x_8, \\ &p_7 = x_5 x_7 - x_7^2, \quad p_8 = x_8^3 - x_1 x_6 x_7 x_8, \end{aligned}$$

where, since $\det B \neq 0$, we have set all coefficients $c_j = 1$. Although the system satisfies the necessary condition in Corollary 2.8, it is not in normal form. We may apply parametric reduction simultaneously to the binomials p_1 and p_5 by considering the polynomial map from $k[x_1, \ldots, x_8]$ to $k[u_1, \ldots, u_6]$ that sends

$$\begin{aligned}
&x_1 \mapsto u_1^3, \quad x_2 \mapsto u_1^2, \quad x_3 \mapsto u_2, \quad x_4 \mapsto u_3,\\
&x_5 \mapsto u_4^2, \quad x_6 \mapsto u_4, \quad x_7 \mapsto u_5, \quad x_8 \mapsto u_6.
\end{aligned}$$

Here we have taken into account that the gcd of the exponents in p_5 is 2. After changing signs when necessary, the new system $\tilde{p}_1, \ldots, \tilde{p}_6$ is in normal form:

$$\begin{aligned}
&\tilde{p}_1 = u_1^5 - u_1^3 u_2, \quad \tilde{p}_2 = u_2^7 - u_1^8 u_2,\\
&\tilde{p}_3 = u_3^2 - u_1^6 u_3^3, \quad \tilde{p}_4 = u_4^3 - u_1^2 u_2 u_5^2 u_6,\\
&\tilde{p}_5 = u_5^2 - u_4^2 u_5, \quad \tilde{p}_6 = u_6^3 - u_1^3 u_4 u_5 u_6.
\end{aligned}$$

Thus, we conclude that $p_1, \ldots, p_8$ defines a complete intersection. We will compute the numerical invariants of this system in Example 3.17.

3. Computing the number of solutions

We recall that if $p_1, \ldots, p_n$ is a gci then we denote by d (respectively, D) the number of points in $\mathbb{V}_c \cap \bar{k}^n$ counted with multiplicity (respectively, without multiplicity), for a generic choice of non-zero coefficients. Similarly, recall that for any index set $L \subset \{1, \ldots, n\}$ we denote by μ_L the number of points in $\mathbb{V}_c \cap \bar{k}_L^n$ counted with multiplicity, where $\bar{k}_L^n$ is the set of points in affine space whose coordinate $x_\ell = 0$ precisely when $\ell \in L$. In particular, $\mu = \mu_{[n]}$ denotes the multiplicity at the origin.

If $p_1, \ldots, p_n$ is a gci but $0 \notin \mathbb{V}(\mathcal{J})$, then it follows from Lemma 2.4 and Proposition 2.5 that the invariants d and D of $p_1, \ldots, p_n$ are obtained from those of the derived system by multiplying times $|\det B_2|$. We will assume from now on that no variable is invertible modulo $\mathcal{J}$, i.e., that $0 \in \mathbb{V}(\mathcal{J})$.

We begin this section by showing that it is enough to compute the desired numerical invariants d, D, μ_L, for ideals in normal form. We then show that if the system is irreducible, in a sense made precise below, then the only zero outside the torus is the origin and its multiplicity may be easily computed from the exponents of the system. Finally, we consider the general case and show how the various dimensions depend on the combinatorics of the irreducible components.

3.1. Multiplicities and parametric reduction

Suppose $p_1(c; x), \ldots, p_n(c; x)$ is as in (1.1) with $p_n = x_n^\ell - c_n x_{n-1}^m$, $\ell, m > 0$. Let $q = \gcd(\ell, m)$ and

$$p'_n = x_n^{\ell'} - c'_n x_{n-1}^{m'}.$$

We will denote by d', D', μ'_L the corresponding invariants for $p_1, \ldots, p_{n-1}, p'_n$.

We show, first of all, that by keeping track of q we may assume without loss of generality that m and ℓ are coprime.

Lemma 3.1. *With notation as above, set $m' = m/q$, $\ell' = \ell/q$, $p'_n = x_n^{\ell'} - c'_n x_{n-1}^{m'}$ and let B and B' be the corresponding matrices.*

(1) $|\det B| = q \cdot |\det B'|$.
(2) $p_1, \ldots, p_n$ *is a gci if and only if* $p_1, \ldots, p_{n-1}, p'_n$ *is a gci.*

(3) *For any index set* $L \subset \{1, \ldots, n\}$, $\mu_L = q \cdot \mu'_L$.
(4) $d = q \cdot d'$ *and* $D = q \cdot D'$.

Proof. The first assertion is trivial while the second one follows from Theorem 2.6. In order to prove assertion 3, let $(c_1, \ldots, c_n) \in (k^*)^n$ be such that $\mathcal{J}_c$ is a complete intersection and decompose

$$p_n = x_n^\ell - c_n x_{n-1}^m = \prod_{\xi \in W_q} (x_n^{\ell'} - \xi x_{n-1}^{m'}), \tag{3.1}$$

where W_q denotes the qth roots of c_n. For any $\lambda \in \mathbb{V}_c$, we have

$$\dim_k (R_\lambda/(\mathcal{J}_c)_\lambda) = \sum_{\xi \in W_q} \dim_k \left(R_\lambda/(\mathcal{J}_\xi)_\lambda\right),$$

where $\mathcal{J}_\xi := \langle p_1(c; x), \ldots, p_{n-1}(c; x), x_n^{\ell'} - \xi x_{n-1}^{m'}\rangle$. Therefore,

$$\sum_{\lambda \in \mathbb{V}_c \cap \bar{k}_L^n} \dim_k (R_\lambda/(\mathcal{J}_c)_\lambda) = \sum_{\xi \in W_q} \sum_{\lambda \in \mathbb{V}(\mathcal{J}_\xi) \cap \bar{k}_L^n} \dim_k \left(R_\lambda/(\mathcal{J}_\xi)_\lambda\right).$$

By a scalar change of variables it follows that

$$\sum_{\lambda \in \mathbb{V}(\mathcal{J}_\xi) \cap \bar{k}_L^n} \dim_k \left(R_\lambda/(\mathcal{J}_\xi)_\lambda\right),$$

is independent of $\xi \in W_q$ and, since it agrees with μ'_L, we obtain that

$$\mu_L = q\mu'_L$$

as claimed. The last assertion follows directly from the previous one and factorization (3.1). □

We next show that multiplicities are not altered under parametric reduction. If the binomial system $p_1, \ldots, p_n$ is a gci, and $p_n = x_n^\ell - c_n x_{n-1}^m$, $\ell, m > 0$ coprime, let $\tilde{p}_1, \ldots, \tilde{p}_{n-1}$ be the binomial system obtained through parametric reduction. We will denote by $\tilde{d}$, $\tilde{D}$ and $\mu_{\tilde{L}}$ the corresponding invariants.

Given $L \subset [n]$ we denote by $\tilde{L} := L \cap [n-1]$. Conversely, given $\tilde{L} \subset [n-1]$ set $L = \tilde{L}$ if $n-1 \notin \tilde{L}$ and $L = \tilde{L} \cup \{n\}$ otherwise. Note that if $L \subset [n]$ is such that $\mu_L \neq 0$ then either $L \subset [n-2]$ or both $n-1, n \in L$. Hence, the correspondence $L \mapsto \tilde{L}$ establishes a bijection between index sets $L \subset [n]$ such that $\mu_L \neq 0$ and subsets $\tilde{L} \subset [n-1]$ such that $\mu_{\tilde{L}} \neq 0$.

Theorem 3.2. *Suppose that* $p_1, \ldots, p_n$ *is a gci and* $p_n = x_n^\ell - c_n x_{n-1}^m$, *with* ℓ, m *coprime positive integers. Let* $\tilde{p}_1, \ldots, \tilde{p}_{n-1}$ *be the binomial system obtained through parametric reduction. Then* $D = \tilde{D}$ *and, for any* $L \subset [n]$,

$$\mu_L = \mu_{\tilde{L}}. \tag{3.2}$$

Consequently, $d = \tilde{d}$ *as well.*

Proof. Let $c = (c_1, \ldots, c_n) \in (k^*)^n$ be such that $\mathcal{J}_c$ is a complete intersection. We may assume without loss of generality that $c_n = 1$. Let $\tilde{c} = (c_1, \ldots, c_{n-1})$ and denote by $\tilde{\mathcal{J}}_{\tilde{c}}$ the ideal generated by $\tilde{p}_1(\tilde{c}; u), \ldots, \tilde{p}_{n-1}(\tilde{c}; u)$ in the ring $k[u]$. Given any $\tilde{\lambda} = (\lambda_1, \ldots, \lambda_{n-1}) \in \mathbb{V}(\tilde{\mathcal{J}}_{\tilde{c}}) \subset \bar{k}^{n-1}$, let us denote by λ the point $(\lambda_1, \ldots, \lambda_{n-2}, \lambda_{n-1}^{\ell}, \lambda_{n-1}^{m}) \in \mathbb{V}(\mathcal{J}_c) \subset \bar{k}^n$. This assignment $\tilde{\lambda} \mapsto \lambda$ defines a bijection between $\mathbb{V}(\tilde{\mathcal{J}}_{\tilde{c}})$ and $\mathbb{V}(\mathcal{J}_c)$ since ℓ, m are coprime, and so $D = \tilde{D}$. To show that $d = \tilde{d}$ it suffices to prove that at the level of local rings

$$\dim_{\bar{k}}(R \otimes_k \bar{k})_{\lambda}/(\mathcal{J}_c)_{\lambda} = \dim_{\bar{k}}(\tilde{R} \otimes_k \bar{k})_{\tilde{\lambda}}/(\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}. \tag{3.3}$$

We will denote by A_1 the localization of $\bar{k}[u_1, \ldots, u_{n-1}]$ at $\tilde{\lambda}$ and by A_2 the localization of $\bar{k}[u_1, \ldots, u_{n-2}, u_{n-1}^{\ell}, u_{n-1}^{m}]$ at $\tilde{\lambda}$. Let $(\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}$ be the ideal generated by $\tilde{p}_1(\tilde{c}; u), \ldots, \tilde{p}_{n-1}(\tilde{c}; u)$ in A_2 so that $(\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}} = A_1 \cdot (\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}$. Again, since m and ℓ are coprime it is clear that

$$\dim_{\bar{k}}(R \otimes_k \bar{k})_{\lambda}/(\mathcal{J}_c)_{\lambda} = \dim_{\bar{k}} A_2/(\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}.$$

Thus, the result will follow if we show that

$$\dim_{\bar{k}} A_1/(\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}} = \dim_{\bar{k}} A_2/(\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}} \tag{3.4}$$

The following proof of (3.4) was suggested to us by Mircea Mustata.

We recall from [21, §14] the following notion of *multiplicity*: let $(R, \mathfrak{m})$ be a d-dimensional Noetherian local ring, M a finite R-module and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal. The multiplicity of M with respect to $\mathfrak{q}$ equals

$$\mathfrak{e}(\mathfrak{q}, M) = \lim_{m \to \infty} \frac{d!}{m^d} \operatorname{length}(M/\mathfrak{q}^{m+1}M). \tag{3.5}$$

Since both A_1 and A_2 are Cohen–Macaulay rings of dimension $n-1$ and

$$\tilde{p}_1(\tilde{c}; u), \ldots, \tilde{p}_{n-1}(\tilde{c}; u)$$

define a regular sequence in A_2, hence in A_1 as well, it follows from [21, Theorem 14.11] that

$$\dim_{\bar{k}} A_2/(\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}} = \mathfrak{e}((\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_2) \quad \text{and} \quad \dim_{\bar{k}} A_1/(\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}} = \mathfrak{e}((\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_1).$$

On the other hand, A_1 may be considered as a A_2-module and it is clear from (3.5) that

$$\mathfrak{e}((\tilde{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_1) = \mathfrak{e}((\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_1).$$

Finally, [21, Theorem 14.8] gives that

$$\mathfrak{e}((\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_1) = \operatorname{rank}_{A_2} A_1 \cdot \mathfrak{e}((\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_2) = \mathfrak{e}((\hat{\mathcal{J}}_{\tilde{c}})_{\tilde{\lambda}}, A_2),$$

since the assumption that m and ℓ are coprime implies that the two domains A_1, A_2 have the same fraction field and so $\operatorname{rank}_{A_2} A_1 = 1$. This proves (3.4). □

3.2. Irreducible systems

Definition 3.3. A binomial system $p_1, \ldots, p_n$ is said to be irreducible if it is in normal form and it is not possible to reorder it so as to find a proper index subset $I \subset [n]$ such that for every $i \in I$ the binomial p_i depends only on the variables x_j, $j \in I$.

Recalling that a system in normal form is a gci and that $0 \in \mathbb{V}(\mathcal{J})$, we easily have:

Lemma 3.4. *Let $p_1, \dots, p_n$ be an irreducible system as in* (1.1) *and let $c \in (k^*)^n$ be such that $\mathcal{J}_c$ is a complete intersection. Then if $a \in \mathbb{V}_c$, either $a = 0$ or $a \in (\bar{k}^*)^n$.*

Proof. Given $a \in \mathbb{V}_c$, let $I = \{i \in [n] : a_i \neq 0\}$. If $i \in I$ then, since $p_1, \dots, p_n$ is in normal form,

$$p_i(c; x) = x_i^{r_i} - c_i x^{\beta_i}, \quad r_i > 0, \;\; \beta_i \neq 0,$$

and, since $a_i \neq 0$, we must have $\mathrm{supp}(\beta_i) \subset I$ for all $i \in I$. This contradicts the irreducibility of $p_1, \dots, p_n$ unless $I = [n]$ or $\emptyset$. □

The following theorem identifies d and μ for irreducible systems. Recall that $\delta = |\det B|$ is the cardinality of $\mathbb{V}_c \cap (\bar{k}^*)^n$. Our arguments are built on the proof of a result of Vinberg (cf. [18, Theorem 4.3]).

Theorem 3.5. *Given an irreducible system*

$$p_i(c; x) = x_i^{r_i} - c_i x^{\beta_i}, \quad i = 1, \dots, n,$$

where $r_i > 0$, $\beta_i \in \mathbb{N}^n$, $\beta_i \neq 0$, then:

- *If all principal minors of B are positive*

  $$d = r_1 \cdots r_n, \quad \mu = d - \delta.$$

  Such a system will be called a global irreducible system.
- *Otherwise, $\mu = r_1 \cdots r_n$ and $d = \mu + \delta$. In this case we say that the system is local.*

Proof. Let us fix throughout coefficients $c \in (k^*)^n$ such that $\mathcal{J}_c$ is a complete intersection. Since the system is in normal form, the entries of B are $b_{ii} = r_i - (\beta_i)_i$ and $b_{ij} = -(\beta_i)_j$, $i \neq j$. Hence, its off-diagonal terms are non-positive. Moreover, the irreducibility of the system implies that B is indecomposable in the sense of [18]. In fact, the irreducibility of the system implies a stronger condition, namely [18, Lemma 4.3]: suppose $u \in \mathbb{R}^n$ is a vector with non-negative entries and that $B \cdot u \geqslant 0$ in the sense that all its entries are non-negative as well. Then either $u = 0$, or $u > 0$, i.e., all its entries are strictly positive. Indeed, let $I = \{i \in [n] : u_i = 0$, then for any $i \in I$, $(B \cdot u)_i \leqslant 0$ and equality occurs if and only if $b_{ij} = 0$ for all $j \notin I$. Hence, by irreducibility we must have $I = [n]$ or $\emptyset$.

Given that [18, Lemma 4.3] holds in our case, we can apply Theorem 4.3 in [18] and conclude that three cases are possible:

- There exists $w \in \mathbb{Q}^n$ all of whose entries are positive such that $B \cdot w > 0$.
- There exists $w \in \mathbb{Q}^n$, all of whose entries are positive such that $B \cdot w < 0$.
- $\mathrm{rank}(B) = n - 1$ and there exists $w \in \mathbb{Q}^n$ all of whose entries are positive such that $B \cdot w = 0$.

According to [3, Theorem 2.3], the first condition is equivalent to the statement that all principal minors of B are positive which implies, in particular, that all the diagonal entries of B are strictly positive. These are the so-called M-matrices of [3]. Moreover, if we consider a term order in $k[x_1, \dots, x_n]$ that refines the weight order defined by w, the term $x_i^{r_i}$ will be the leading term in $p_i(c; x)$, and hence $p_1(c; x), \dots, p_n(c; x)$ is a Gröbner basis. It then follows [5, §5.3, Proposition 4] that $d = r_1 \cdots r_n$ and, by Lemma 3.4, $\mu = d - \delta$.

In the second case we can similarly define a local order (cf. [14]) for which the leading term of $p_i(c; x)$ is $x_i^{r_i}$. Hence $p_1(c; x), \ldots, p_n(c; x)$ is a standard basis in the local quotient ring at the origin and, consequently, $\mu = r_1 \cdots r_n$ and $d = \mu + \delta$. We note that this is valid even if $\det B = 0$ since, in that case, $\mathcal{J}_c$ is a complete intersection if and only if $\mathbb{V}_c = \{0\}$.

In the third case, the binomials $p_i(c; x)$ are weighted homogeneous relative to the weight w and therefore $\mu = r_1 \cdots r_n$ and $d = \mu + \delta$ since, again, $\mathbb{V}_c$ consists of only the origin. Thus, this case behaves as the previous one and we will also refer to it as a local case. □

Remark 3.6. We note that if $n = 1$, the system $p = x^\alpha - cx^\beta$, $\alpha \neq \beta$, will be local if $\alpha < \beta$ and global if $\alpha > \beta$.

3.3. The general case

We consider now general gci systems in normal form. Throughout this subsection we will, again, fix coefficients $c \in (k^*)^n$ so that $\mathcal{J}_c$ is a complete intersection. For economy of notation we will denote simply by p_i the corresponding binomials in $k[x_1, \ldots, x_n]$. If the system $p_1, \ldots, p_n$ is not irreducible, then, as Lemma 3.8 shows, it is possible to choose an increasing sequence

$$0 = v_0 < v_1 < \cdots < v_s = n \tag{3.6}$$

so that if $I_a = \{v_{a-1} + 1, \ldots, v_a\}$, then the following holds:

- For $i \in I_a$, $p_i \in k[x_j;\, j \in I_1 \cup \cdots \cup I_a]$.
- The system $\hat{p}_i := p_i(1, \ldots, 1, x_{v_{a-1}+1}, \ldots, x_{v_a})$, $i \in I_a$, is irreducible.

Definition 3.7. A system of this form will be said to be in *triangular* form relative to the blocks $I_1, \ldots, I_s$. Given a reducible system in triangular form, we will refer to the system $\{\hat{p}_i, i \in I_a\}$ as the restriction of $p_1, \ldots, p_n$ to I_a and denote it, for short, by $\hat{p}^a$.

Lemma 3.8. *Any system of n binomials $p_1, \ldots, p_n$ in normal form* (2.9) *can be put in triangular form in time $O(n^2)$.*

Proof. Consider the occurrence matrix N: this is a 0-1 matrix with $n_{ij} \neq 0$ if and only if $i \neq j$ and p_i depends on x_j (i.e., if $p_i = x_i^{r_i} - c_i x^{\beta_i}$ with $\beta_{ij} \neq 0$). This is a standard construction, first used by Steward [27], for the analysis of the structure of large systems of equations. Note that, because the system is in normal form, putting $p_1, \ldots, p_n$ in triangular form corresponds precisely to finding a permutation matrix P such that ${}^tPNP$ is block lower triangular, with the irreducible subsystems of $p_1, \ldots, p_n$ corresponding to the irreducible diagonal square blocks along the diagonal of ${}^tPNP$.

Tarjan's algorithm [30] to search for the strongly connected components of the directed graph associated to N provides an efficient method for finding such permutation matrix P [9,23]; it runs in time linear in the number of vertices plus the number of edges of the graph. □

Given a system in normal form and triangular relative to $I_1, \ldots, I_s$, let $\delta_a = |\det B_a|$, where B_a is the matrix associated with the system $\hat{p}^a$ and

$$\rho_a = \prod_{j \in I_a} r_j.$$

We also denote by μ_a the multiplicity of $\hat{p}^a$ at 0 and by d_a the total number of solutions of $\hat{p}^a$ counted with multiplicity.

For a triangular system $p_1, \ldots, p_n$, its associated matrix is block lower-triangular:

$$B = \begin{pmatrix} B_1 & 0 & \ldots & 0 \\ C_{21} & B_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_{s1} & C_{s2} & \ldots & B_s \end{pmatrix}. \tag{3.7}$$

The number of solutions of the system $p_1, \ldots, p_n$ and the patterns of possible zero coordinates of the solutions are best described in terms of the directed acyclic graph G with s vertices labeled $\{1, \ldots, s\}$ and an arrow from node a to node b if and only if the rectangular submatrix C_{ba} is not identically zero. We recall that a vertex is called a *source* if it is not the head of any arrow. The subset of sources of the vertex set of a subgraph H of G will be denoted by $S(H)$.

Remark 3.9. We can think of G as a weighted graph, where each vertex $a \in [s]$ comes with the weights δ_a, ρ_a, μ_a (or δ_a, d_a, μ_a). Equivalently, we can think that the information at each node is coded by the weights δ_a, ρ_a plus an additional label *global* or *local* according to where B_a is global or local, which prescribes the relation among δ_a, ρ_a and μ_a (or δ_a, d_a and μ_a).

Theorem 3.10. *The multiplicity μ of $\mathcal{J}_c$ at the origin equals*

$$\mu = \left(\prod_{a \in G \setminus S(G)} \rho_a \right) \left(\prod_{b \in S(G)} \mu_b \right). \tag{3.8}$$

Proof. We will prove formula (3.8) by induction in the number s of blocks. If $s = 1$, the system is irreducible and $\{1\} \in S(G)$ so the formula holds. Consider $s > 1$ and assume that the result is true for systems with $s - 1$ blocks. Let B be as in (3.7), set $n' := v_{s-1}$, where v_{s-1} is as in (3.6), and consider the ideal $\mathcal{J}'_c := \langle p_1, \ldots, p_{n'} \rangle$, in the polynomial ring in the first n' variables. Clearly, $p_1, \ldots, p_{n'}$ is in normal and triangular form. Let G' be the corresponding graph; it is obtained by erasing from G the vertex s and all edges ending at s. By inductive hypothesis, we have that the multiplicity μ' of $\mathcal{J}'_c$ at $0'$ equals

$$\mu' = \left(\prod_{a \in G' \setminus S(G')} \rho_a \right) \left(\prod_{b \in S(G')} \mu_b \right). \tag{3.9}$$

The matrix B has the form

$$B = \left(\begin{array}{c|c} B' & 0 \\ \hline C & B_s \end{array} \right). \tag{3.10}$$

If the rectangular matrix C is identically zero, then the last $n - n'$ polynomials depend only on the last $n - n'$ variables, and we have that

$$\mu = \mu' \cdot \mu_s,$$

as wanted, since in this case $S(G) = S(G') \cup \{s\}$.

On the other hand, if C is not zero, it is possible to find a positive weight vector w such that the initial monomial $in_{-w}(p_j) = x_j^{r_j}$, for all $n' < j \leqslant n$. Indeed, set $J_0 = [n']$, and, for $l \geqslant 1$ define

$$J_\ell := \left\{ k \in [n] \Bigg\backslash \left(\bigcup_{a=0}^{\ell-1} J_a \right) : J_{\ell-1} \cap \operatorname{supp}(\beta_k) \neq \emptyset \right\}.$$

Note that $C \neq 0$ implies that J_1 is non-empty. Also, the assumption that B_s is irreducible guarantees that there exists $L \leqslant n - n'$ such that $[n]\backslash[n'] = \bigcup_{1 \leqslant \ell \leqslant L} J_\ell$. Now, choose $w_k = 1$ for $k \in J_L$. Then assuming that the weights for the variables $k \in J_a$, $\ell \leqslant a \leqslant L-1$, have been chosen so that $in_{-w}(p_j) = x_j^{r_j}$ for all $j \in J_b$, $b \geqslant \ell + 1$, we may choose positive weights w_k for $k \in J_{\ell-1}$ that are sufficiently large so that $in_{-w}(p_j) = x_j^{r_j}$ for all $j \in J_\ell$ as well.

Consider now any local order $\prec$ in $k[x_1, \ldots, x_n]$ refining the weight $-w$. Let $\{q_1, \ldots, q_t\}$ be a standard basis for the ideal $\mathcal{J}_c'$ with respect to the local order induced by $\prec$ in $k[x_1, \ldots, x_{n'}]$. Then, $\{q_1, \ldots, q_t, p_{n'+1}, \ldots, p_n\}$ is a standard basis for $\mathcal{J}_c$ relative to $\prec$ since, for every $i = 1, \ldots, t$, the leading monomials of the polynomial q_i is coprime with those of the p_j, $n' < j \leqslant n$, and, therefore, the weak normal form of the corresponding S-polynomial is 0 [14]. The corresponding initial ideal $L_\prec(\mathcal{J}_c)$ will be generated by some monomials in the first n' variables (generating the initial ideal $L_{\prec'}(\mathcal{J}_c'))$ and the pure powers $x_j^{r_j}$ for all $j > n'$. Therefore, the multiplicity μ of $\mathcal{J}_c$ at 0 equals

$$\begin{aligned} &\dim_{\bar{k}} \left(\bar{k}[x_1 \ldots, x_n]/\mathcal{J}_c\right)_0 = \dim_{\bar{k}} \left(\bar{k}[x_1 \ldots, x_n]/L_\prec(\mathcal{J}_c)\right)_0 \\ &\quad = \dim_{\bar{k}} \left(\bar{k}[x_1 \ldots, x_{n'}]/L_{\prec'}(\mathcal{J}_c')\right)_0 \cdot \dim_{\bar{k}} \left(\bar{k}[x_{n'+1} \ldots, x_n]/\langle x_{n'+1}^{r_{n'+1}} \cdots x_n^{r_n}\rangle\right)_0 \\ &\quad = \dim_{\bar{k}} \left(\bar{k}[x_1 \ldots, x_{n'}]/\mathcal{J}_c'\right)_0 \cdot \rho_s. \end{aligned}$$

In this case $s \notin S(G)$, and so $S(G) = S(G')$. Since the dimension of the local quotient by $\mathcal{J}_c'$ at the origin equals (3.9), we get that

$$\mu = \mu' \cdot \rho_s = \left(\prod_{a \in \backslash S(G)} \rho_a \right) \left(\prod_{b \in S(G)} \mu_b \right),$$

as wanted. $\square$

Remark 3.11. Using Theorem 3.5 we can translate (3.8) as

$$\mu = \left(\prod_{a \in G_1} d_a \right) \left(\prod_{b \in G_2} \mu_b \right), \tag{3.11}$$

where G_1 is the set of nodes of G corresponding to the global, non-sources of G and G_2 is its complement.

We will also need the following terminology.

Definition 3.12. A vertex b of (the directed acyclic graph) G is said to be a *descendant* (respectively, a *direct descendant*) of the vertex a if there is a directed path (respectively, a directed edge) from a to b. A (directed) subgraph H of G is said to be *full* if, for any of its vertices j, all its descendants and all the directed paths starting from j also belong to H. The collection of full subgraphs of G will be denoted by $\mathcal{F}(G)$.

The empty subgraph is full and even if G is connected, a full subgraph H may be disconnected. Note also that a full subgraph is completely determined by its sources.

The following result refines the description given in Remark 2.7 of subsets $L \subset [n]$ with $\mu_L \neq 0$.

Proposition 3.13. *Let $p_1, \ldots, p_n$ be a binomial complete intersection in normal and triangular form and $L \subset [n]$. Then $\mu_L = 0$ unless there exists a full subgraph H of G such that*

$$\prod_{a \notin H} \delta_a \neq 0 \tag{3.12}$$

and L coincides with the union of all the indices belonging to blocks that are vertices of H.

Proof. With the above notations, let $\lambda = (\lambda_1, \ldots, \lambda_n) \in \mathbb{V}(\mathcal{J}_c)$ and $L = L(\lambda) = \{i \in [n] : \lambda_i = 0\}$. Set $H = \{a \in G : I_a \cap L \neq \emptyset\}$. If $a \in H$ then we may argue as in Lemma 3.4 to conclude that $I_a \subset L$. Suppose now that $a \in H$ and that (a, b) is an edge in G. Since $C_{ba} \neq 0$, there exists $i \in I_a$ and $j \in I_b$ such that $i \in \operatorname{supp}(\beta_j)$ and, consequently, $\lambda_j = 0$, i.e., $j \in I_b \cap L$, and $b \in H$. This shows that H is a full subgraph of H. The need for condition (3.12) was already noted in Remark 2.7. $\square$

With notation as in Proposition 3.13, given a full subgraph $H \subset G$, we will denote by $L(H)$ the set of indices belonging to blocks associated with vertices of H.

Proposition 3.14. *Given a full subgraph H of G, the number $D_{L(H)}$ of points in $\mathbb{V}(\mathcal{J}_c) \cap \bar{k}^n_{L(H)}$ counted without multiplicity equals*

$$D_{L(H)} = \left(\prod_{a \notin H} \delta_a\right) \tag{3.13}$$

while the number $\mu_{L(H)}$ of points in $\mathbb{V}(\mathcal{J}_c) \cap \bar{k}^n_{L(H)}$ counted with multiplicity equals

$$\mu_{L(H)} = \left(\prod_{a \notin H} \delta_a\right) \left(\prod_{b \in H \setminus S(H)} \rho_b\right) \left(\prod_{e \in S(H)} \mu_e\right). \tag{3.14}$$

Proof. The first assertion follows easily from Proposition 3.13. In order to prove (3.14), let $\lambda \in \mathbb{V}(\mathcal{J}_c) \cap \bar{k}^n_{L(H)}$, write $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(s)})$ with $\lambda^{(a)} \in \bar{k}^{|I_a|}$ for all $a \in [s]$. Since H is a full subgraph, there are no edges starting at a node in H and ending at a node outside of H; i.e., $C_{ba} = 0$ for all $a \in H$ and $b \notin H$. Therefore, it is possible to relabel the variables and the binomials $p_1, \ldots, p_n$ so that the system remains in normal form and satisfies that $a < b$ for all $a \notin H$ and $b \in H$. Thus, we may assume without loss of generality that $H = \{t + 1, \ldots, s\}$ and therefore $\lambda = (\lambda^{(1)}, \ldots, \lambda^{(t)}, 0, \ldots, 0)$ with $\lambda^{(a)} \in (\bar{k}^*)^{|I_a|}$ for $a = 1, \ldots, t$. Equivalently,

$$\lambda = (\lambda', 0) \in (\bar{k}^*)^{n'} \times (\bar{k})^{n-n'}, \quad n' := v_t.$$

We let x' stand for the first n' variables $x_1, \ldots, x_{n'}$ and x'' for the remaining $n - n'$ variables. Then

$$\mathcal{J}'_c := \langle p_1, \ldots, p_{n'} \rangle \subset k[x']$$

and λ' is a simple zero of $\mathcal{J}'_c$. Hence $p_1, \ldots, p_{n'}$ define the maximal ideal in the local ring $\left(\bar{k}[x']\right)_{\lambda'}$. We then have

$$\begin{aligned}\mu_\lambda &:= \dim_{\bar{k}} \left(\bar{k}[x]/\mathcal{J}_c\right)_\lambda \\ &= \dim_{\bar{k}} \left(\bar{k}[x]/\langle x_1 - \lambda_1, \ldots, x_{n'} - \lambda_{n'}, p_{n'+1}, \ldots, p_n\rangle\right)_\lambda \\ &= \dim_{\bar{k}} \left(\bar{k}[x'']/\langle p_{n'+1}(\lambda', x''), \ldots, p_n(\lambda', x'')\rangle\right)_0 \\ &= \dim_{\bar{k}} \left(\bar{k}[x'']/\langle p_{n'+1}(1, \ldots, 1, x''), \ldots, p_n(1, \ldots, 1, x'')\rangle\right)_0 .\end{aligned}$$

So, μ_λ equals the multiplicity at the origin $0 \in \bar{k}^{n-n'}$ of the system $\{\hat{p}_{n'+1}, \ldots, \hat{p}_n\}$. Formula (3.14) now follows from Theorem 3.10, and the fact that the system $p_1, \ldots, p_{n'}$ has $\delta_1 \cdots \delta_t$ simple solutions in $(\bar{k}^*)^{n'}$. $\square$

The following explicit formulas for d and D follow by adding (3.13) and (3.14) over all full subgraphs of G.

Theorem 3.15. *Suppose that $p_1, \ldots, p_n$ are in normal, triangular form. For generic parameters $c \in (k^*)^n$, the total number of solutions of the system $p_1(c; x) = \cdots = p_n(c; x) = 0$, counted without multiplicity, equals*

$$D = \sum_{H \in \mathcal{F}(G)} \left(\prod_{a \notin H} \delta_a\right), \tag{3.15}$$

and the total number of solutions counted with multiplicity equals

$$d = \sum_{H \in \mathcal{F}(G)} \left(\prod_{a \notin H} \delta_a\right) \left(\prod_{b \in H \setminus S(H)} \rho_b\right) \left(\prod_{e \in S(H)} \mu_e\right). \tag{3.16}$$

We end this section with a recursive formula to compute d. In order to state the following proposition we define, for $1 \leqslant r \leqslant s$, the binomial system $q^{(r)}$:

$$p_i(1, \ldots, 1, x_{v_{r-1}+1}, \ldots, x_n), \quad i \in I_r \cup \cdots \cup I_s.$$

Note that the matrix associated with $q^{(r)}$ is

$$B^{(r)} = \begin{pmatrix} B_r & 0 & \ldots & 0 \\ C_{(r+1)r} & B_{r+1} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ C_{sr} & C_{s(r+1)} & \ldots & B_s \end{pmatrix}. \tag{3.17}$$

Clearly if $p_1, \ldots, p_n$ is in normal, triangular form, so is $q^{(r)}$. We denote by F_r the number of solutions in $\bar{k}^{n-v_{r-1}}$, counted with multiplicity, of the system $q^{(r)}$.

Proposition 3.16. *F_r is a polynomial function of $\{\delta_a, \mu_a, \rho_a,\ a = r, \ldots, s\}$. It may be computed recursively as*

$$F_s = d_s = \delta_s + \mu_s,$$

$$F_r = \delta_r \cdot F_{r+1} + \mu_r \cdot F_{r+1}|_{\delta_b=0,\mu_b=\rho_b}, \tag{3.18}$$

where b runs over all indices in $\{r+1,\dots,s\}$ such that $C_{br} \neq 0$.

Proof. We may assume without loss of generality that $r = 1 < s$. Let G be the graph of B and $G^{(2)}$ the subgraph of G associated to the submatrix $B^{(2)}$ defined by (3.17).

Any full subgraph $H \in \mathcal{F}(G^{(2)})$ may be thought of as a full subgraph in G. We denote by $\mathcal{F}' \subset \mathcal{F}(G)$ the collection of such subgraphs. Clearly $\mathcal{F}'$ consists of all full subgraphs of G not containing vertex 1. Let $\mathcal{F}''$ denote the complement of $\mathcal{F}'$ in $\mathcal{F}(G)$. Removing vertex 1 from a subgraph $H \in \mathcal{F}''$ defines a full subgraph $H^{(2)}$ of $G^{(2)}$ with the property that no direct descendant of 1 in G may be in $G^{(2)} \setminus H^{(2)}$. Let us denote by $\mathcal{F}''(G^{(2)})$ the collection of such full subgraphs of $G^{(2)}$. We can write

$$F_1 = \sum_{H\in\mathcal{F}'} \mu_{L(H)} + \sum_{H\in\mathcal{F}''} \mu_{L(H)}. \tag{3.19}$$

Since, for $H \in \mathcal{F}'$, $1 \notin H$, in view of (3.14), the first sum may be computed as

$$\sum_{H\in\mathcal{F}'} \mu_{L(H)} = \delta_1 \sum_{H\in\mathcal{F}(G^{(2)})} \mu_{L(H)} = \delta_1 F_2, \tag{3.20}$$

since $S(H)$ is the same whether we view H as a subgraph of G or of $G^{(2)}$.

Thus, in order to complete the proof we need to show that the second sum in (3.19) equals

$$\mu_1 \cdot F_2|_{\delta_b=0,\mu_b=\rho_b},$$

where b runs over all vertices in $G^{(2)}$ that are direct descendants of 1 in G. We note first of all, that setting $\delta_b = 0$ for all direct descendants b of 1 has the effect of restricting the sum in (3.16) to $\mathcal{F}''(G^{(2)})$. Moreover, given $H \in \mathcal{F}''$, let $H^{(2)}$ denote the full subgraph of $G^{(2)}$ obtained by removing the vertex 1 from H. Then $S(H^{(2)})$ consists of $S(H) \cap G^{(2)}$ together with all direct descendants of 1 in H. This change may be accomplished by replacing μ_b by ρ_b whenever $b \in H^{(2)}$ is a direct descendant of 1 in H. Since $1 \in S(H)$ for all $H \in \mathcal{F}''$, we obtain the desired equality. $\square$

Example 3.17. We return to Example 2.13. We recall that the reduced system $\tilde{p}_1,\dots,\tilde{p}_6$ is

$$\tilde{p}_1 = u_1^5 - u_1^3u_2, \quad \tilde{p}_2 = u_2^7 - u_1^8u_2,$$
$$\tilde{p}_3 = u_3^2 - u_1^6u_3^3, \quad \tilde{p}_4 = u_4^3 - u_1^2u_2u_5^2u_6,$$
$$\tilde{p}_5 = u_5^2 - u_4^2u_5, \quad \tilde{p}_6 = u_6^3 - u_1^3u_4u_5u_6$$

and, therefore, its associated matrix is

$$B = \begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 \\ -8 & 6 & 0 & 0 & 0 & 0 \\ -6 & 0 & -1 & 0 & 0 & 0 \\ -2 & -1 & 0 & 3 & -2 & -1 \\ 0 & 0 & 0 & -2 & 1 & 0 \\ -3 & 0 & 0 & -1 & -1 & 2 \end{pmatrix}.$$

Therefore, the system is in normal triangular form with blocks relative to the index sets $I_1 = \{1, 2\}$, $I_2 = \{3\}$, and $I_3 = \{4, 5, 6\}$. The block B_1 is global, while B_2 and B_3 are local. The graph G has 3 vertices $\{1, 2, 3\}$ and arrows from 1 to 2 and 1 to 3. Hence $S(G) = \{1\}$. The weights are

$$\delta_1 = 4, \quad \delta_2 = 1, \quad \delta_3 = 5, \quad \rho_1 = 35, \quad \rho_2 = 2, \quad \rho_3 = 18,$$

and, taking into account the local/global label, we get $\mu_1 = 31$, $\mu_2 = 2$, $\mu_3 = 18$.

We may now apply (3.8) to compute the multiplicity $\tilde{\mu}$ of $\langle \tilde{p}_1, \ldots, \tilde{p}_6 \rangle$ at the origin

$$\tilde{\mu} = \mu_1 \cdot \rho_2 \cdot \rho_3 = 1116.$$

In order to compute $\tilde{d}$ we use the inductive procedure of Proposition 3.16. Since the subgraph with vertices $\{2, 3\}$ is disconnected we have

$$F_2 = (\delta_2 + \mu_2) \cdot (\delta_3 + \mu_3).$$

Hence, $F_1 = \delta_1 \cdot (\delta_2 + \mu_2) \cdot (\delta_3 + \mu_3) + \mu_1 \cdot \rho_2 \cdot \rho_3$. This gives $\tilde{d} = 1392$. We note that this is far from the Bézout bound of 43740.

Using Lemma 3.1 and Theorem 3.2 we see that the total number of solutions for the original system $p_1, \ldots, p_8$ are given by $d = 2\tilde{d}$ and $\mu = 2\tilde{\mu}$. These values may be easily verified using a computer algebra system such as Singular [15].

Finally, we note that G has five full subgraphs with vertex sets: $\{1, 2, 3\}$, $\{2, 3\}$, $\{2\}$, $\{3\}$, and $\emptyset$. This means that there are five index sets $\tilde{L} \subset [6]$, such that $\mu_L \neq 0$. They are $\tilde{L}_1 = [6]$, $\tilde{L}_2 = \{3, 4, 5, 6\}$, $\tilde{L}_3 = \{3\}$, $\tilde{L}_4 = \{4, 5, 6\}$ and $\tilde{L}_5 = \emptyset$. The corresponding multiplicities are according to (3.14):

$$\mu_{\tilde{L}_1} = \tilde{\mu} = 1116, \quad \mu_{\tilde{L}_2} = 144, \quad \mu_{\tilde{L}_3} = 40, \quad \mu_{\tilde{L}_4} = 72, \quad \mu_{\tilde{L}_5} = \tilde{\delta} = 20.$$

Moreover, the total number of solutions counted without multiplicity is given by

$$\tilde{D} = \delta_1 + \delta_1 \cdot \delta_3 + \delta_1 \cdot \delta_2 + \delta_1 \cdot \delta_2 \cdot \delta_3 = 48.$$

This information may be lifted to the original system using the bijection $L \to \tilde{L}$ discussed before Theorem 3.2. We get that $\mu_L = 0$ except for the following subsets:

$$L_1 = [8], \quad L_2 = \{4, 5, 6, 7, 8\}, \quad L_3 = \{4\}, \quad L_4 = \{5, 6, 7, 8\}, \quad L_5 = \emptyset.$$

Once again, $\mu_{L_i} = 2\mu_{\tilde{L}_i}$.

4. Counting complexity

In this section we will study the counting complexity, in the sense of [31], of computing the numerical invariants d, D, δ, μ, and μ_L associated with a gci $p_1, \ldots, p_n$.

We have already proved that we may decide in polynomial time if $p_1, \ldots, p_n$ is a gci and that the property of being a complete intersection is independent of the coefficients if $\det B \neq 0$. Moreover, if $p_1, \ldots, p_n$ is a gci we may also transform it into normal and triangular form in quadratic time. Also, since a system with generic exponents is irreducible and satisfies $\det B \neq 0$, we may compute its invariants in time polynomial in n for any choice of coefficients by

Theorem 3.5. In the general case, we may compute δ, μ, and μ_L, for a particular choice of L, directly from the invariants δ_a, ρ_a, and μ_a associated with the diagonal blocks of the system. Thus, δ, μ, and μ_L may be computed in polynomial time as well.

However, we will show below in Theorem 4.3 that the computation of d or D is a $\#P$-complete problem, and therefore it is at least as hard as an NP-complete problem [31]. In order to do this we begin by reversing the relationship between binomial systems and weighted acyclic directed graphs. We recall that to a binomial system $p_1, \ldots, p_n$ in normal and triangular form we associate an acyclic-directed graph G whose vertices $\{1, \ldots, s\}$ correspond to the diagonal blocks of the associated matrix B and that each vertex has weights δ_a, ρ_a, $a \in [s]$, plus a label “local” or “global”. In the first case we set $\mu_a = \rho_a$, while in the global case we set $\mu_a = \rho_a - \delta_a$. In any case $d_a = \delta_a + \mu_a$. The proof of the following proposition is straightforward.

Proposition 4.1. *Let $G = (V, E)$, $V = [s]$, be an acyclic-directed graph, with weights $\delta_a, \rho_a \in \mathbb{Z}_{>0}$ and labels local/global attached to each vertex. Let μ_a and d_a be defined as above. Then, the system of binomials defined by*

$$p_a(x_1, \ldots, x_s) = x_a^{d_a} - c_a \left(\prod_{(b,a)\in E} x_b \right) x_a^{\mu_a},$$

for all global vertices a, and

$$p_a(x_1, \ldots, x_s) = x_a^{\mu_a} - c_a \left(\prod_{(b,a)\in E} x_b \right) x_a^{d_a},$$

for all local vertices a, has as weighted graph $(G, \delta_a, \rho_a, \mu_a)$.

Remark 4.2. The total number of solutions d and D of the system in Proposition 4.1 are given by (3.16) and (3.15), for generic parameters c_a. For any order on the set of vertices of G such that $i < j$ if there is a path from node i to node j (i.e., for any linear extension of G), it is clear that the corresponding matrix B of the system will be lower triangular, with diagonal entries $\pm(d_a - \mu_a)$. Thus, whenever $d_a \neq \mu_a$, we have that $\det(B) \neq 0$ and we may simply choose $c_a = 1$ for all $a \in [s]$.

Note also that if a is a source of G, then we get $p_a = x_a^{d_a} - c_a x_a^{\mu_a}$ in the global case, and $p_a = x_a^{\mu_a} - c_a x_a^{d_a}$ in the local case. This is compatible with Remark 3.6.

In the particular case when all vertices $\{1, \ldots, s\}$ of a directed acyclic graph G are local, and their weights are $\delta_a = 1$, $\rho_a = 1$, for all $a \in [s]$, the binomial system defined in Proposition 4.1 takes a very simple form:

$$p_a(x_1, \ldots, x_s) = x_a - \left(\prod_{(b,a)\in E} x_b \right) x_a^2, \quad a = 1, \ldots, s. \tag{4.1}$$

We will refer to this system as the *standard binomial system* associated with G.

Theorem 4.3. *Computing d and D for binomial complete intersections $p_1, \ldots, p_n$ in normal, triangular form are $\#P$-complete problems.*

Proof. By Theorem 3.15, the problems of computing d and D are in the complexity class $\#P$. We will show that computing these invariants gives, for special binomial systems, the number of independent subsets of a bipartite graph G. Since, by [24], this is known to be a $\#P$-complete problem the result will follow.

Let G be a bipartite graph with vertices $\{1, \ldots, s\}$. Let $p_1, \ldots, p_s$ be the standard binomial system of G as in (4.1). Then, for each full subgraph $H \subset G$ we have, by (3.14), that $\mu_{L(H)} = 1$. Hence, according to (3.16) and (3.15), both d and D are equal to the number of full subgraphs of G. But, as has been noted earlier, a full subgraph is completely determined by its sources and, for a bipartite graph G, a subset of vertices is the set of sources of a full subgraph H if and only if it is an independent subset of G. Thus, d and D agree with the number of independent subsets of G. $\square$

Recall that a directed acyclic graph $G = (V, E)$ is called *transitive* if there is an edge $(a, b) \in E$ each time that there is a directed path from a to b, Transitive directed acyclic graphs are in correspondence with partial orders $\prec$ on V, where $a \prec b$ if and only if $(a, b) \in E$. Given a partial order $\prec$ on V, a subset A of V is called an antichain if given $a_1, a_2 \in A$, neither $a_1 \prec a_2$, nor $a_2 \prec a_1$. It is shown in [24] that counting the number of antichains in posets is a $\#P$-complete problem. Given any directed acyclic graph $G = (V, E)$, it is possible to compute its transitive closure $G^+ = (V, E^+)$, in time $O(|V|^3)$ by the well-known Floyd–Warshall's algorithm. It follows from (3.16) and (3.15) that d and D are the same for the standard binomial systems associated with G and with G^+.

Proposition 4.4. *The number of* (*simple*) *solutions of the standard binomial system associated with a directed acyclic graph G equals the number of antichains in the associated partial order.*

Proof. As in the proof of Theorem 4.3, for the standard binomial system of G we have $d = D$ and this number agrees with the number of full subgraphs of G. These subgraphs are determined by their sources, which correspond exactly to the antichains in the associated partial order on V. $\square$

Although, as the previous results show, the problem of computing the total number of solutions for a general binomial system in normal and triangular form is $\#P$-complete, there are classes of binomial systems whose invariants may be computed in polynomial time. For example, if the graph is totally disconnected then $d = d_1 \cdots d_s = \prod_{i=1}^{s}(\delta_i + \mu_i)$. At the other extreme if G is a (complete) directed graph with vertices $\{1, \ldots, s\}$ and (b, a) is an edge of G for all $a, b \in [s]$ with $a < b$, then it is easy to see that there are only $s + 1$ full subgraphs of G and, consequently, the sums in (3.15) and (3.16) consist of $s + 1$ terms.

Even if the number of full subgraphs is exponential in s and G has few connected components, a bound on the number of local blocks guarantees that d can be computed in polynomial time in n. For instance, if all blocks are global, then B is an M-matrix and $p_1, \ldots, p_n$ is a Gröbner basis for a positive weight order, and so $d = \rho_1 \cdots \rho_s$. We end with the following "positive" complexity result.

Proposition 4.5. *Let $N \in \mathbb{Z}_{\geqslant 0}$. Assume $p_1, \ldots, p_n$ is in normal and triangular form with s blocks of which at most N are local. Then, there is a formula to compute the total multiplicity d with at most 2^N summands, each involving s products. Thus, if the number of local blocks of a binomial system in normal and triangular form is bounded independently of n, the number of affine solutions of the system can be computed in time polynomial in n.*

Proof. Recall the notation in Proposition 3.16. We may write the polynomial formula $F_r((\delta_a, \rho_a, \mu_a), a \in [s])$ for the computation of the total number of solutions of the system $q^{(r)}$ purely in terms of δ_a and ρ_a by keeping track of the local/global character of each vertex and replacing μ_a by ρ_a if a is local and by $\rho_a - \delta_a$ in the case of a global vertex. We call $\tilde{F}_r((\delta_a, \rho_a), a \in [s])$ the polynomial obtained after these substitutions. Then, for a global vertex r, the recursion (3.18) becomes

$$\tilde{F}_r = \delta_r \cdot \tilde{F}_{r+1} + (\rho_r - \delta_r) \cdot \tilde{F}_{r+1}|_{\delta_a=0}, \tag{4.2}$$

where a runs over all direct descendants of r. Let us write $\tilde{F}_{r+1} = F'_{r+1} + F''_{r+1}$, where F'_{r+1} consists of all summands containing a factor δ_a with a a direct descendant of 1. Hence, F'_{r+1} vanishes when we set such $\delta_a = 0$ and (4.2) becomes

$$\tilde{F}_r = \delta_r \cdot (F'_{r+1} + F''_{r+1}) + (\rho_r - \delta_r) \cdot F''_{r+1} = \delta_r \cdot F'_{r+1} + \rho_r \cdot F''_{r+1}$$

and, consequently, the total number of summands does not change when adding a global vertex.

On the other hand, if B_r is local then (3.18) becomes

$$\tilde{F}_r = \delta_r \cdot \tilde{F}_{r+1} + \rho_r \cdot \tilde{F}_{r+1}|_{\delta_a=0}$$

and the number of summands is, at worst, doubled.

It follows that when N is bounded independently of the number n of variables, d can be computed by adding a constant number of summands. Each of these summands has $s \leqslant n$ products of factors involving the computation of determinants of the square diagonal blocks of the associated matrix B or products of the exponents r_j. $\square$

5. Applications

In this section we will briefly discuss some of the problems that led us to the study of systems of n binomials in n variables.

An important subfamily of binomial ideals is given by the toric ideals associated to configurations $A = \{a_1, \ldots, a_m\} \subset \mathbb{Z}^k$ of integral points spanning $\mathbb{Z}^k$:

$$I_A = \langle x^u - x^v;\ A \cdot (u - v) = 0 \rangle,$$

where $u, v \in \mathbb{N}^m$. In particular, beginning with the work of Herzog [16] and Delorme [6] the question of classifying complete intersection toric ideals (and the corresponding semigroup algebras) has been extensively studied by many authors [1,4,11–13,26]. A key step in many of these works is the study of the ideal generated by binomials $x^{u_i} - x^{v_i}$ associated with a $\mathbb{Z}$-basis of the kernel of A. More generally, given $\mathbb{Q}$-linearly independent elements $v_1, \ldots, v_r \in \mathbb{Z}^m$, consider the associated lattice basis ideal $J \subset k[x_1, \ldots, x_m]$, generated by the binomials

$$b_j = x^{u_j} - x^{v_j}, \quad j = 1, \ldots, r,$$

where $v_j = u_j - v_j$, and $u_j, v_j \in \mathbb{N}^m$ have disjoint support. Let $\mathcal{L} \subset \mathbb{Z}^m$ denote the lattice spanned by $v_1, \ldots, v_r$ and let $I_{\mathcal{L}} := \langle x^u - x^v : u - v \in \mathcal{L} \rangle$ be the corresponding lattice ideal. We assume that these ideals are homogeneous, i.e., $w_1 + \cdots + w_m = 0$, for every $w \in \mathcal{L}$.

The ideal $I_{\mathcal{L}}$ is prime if and only if the lattice $\mathcal{L}$ is saturated. If $\mathcal{L}$ is not saturated, then $I_{\mathcal{L}}$ has g radical primary components, where g is the index of $\mathcal{L}$ in its saturation. Moreover, all these components have the same degree, equal to the degree $d_{\mathcal{L}}$ of the associated toric variety [10].

We can apply Theorem 3.15 to compute the multiplicity and geometric degree [2] of the primary components of J. This may be used to describe the holonomic rank of Horn systems of hypergeometric partial differential equations and to study sparse discriminants, generalizing the codimension-two case [8,7].

A straightforward extension of the results of [17] to non-saturated lattices gives the following description of all primary components $\mathfrak{q}$ of J. Let $K \subset \{1, \ldots, m\}$ and $Z(K) \subset \{1, \ldots, r\}$ as in (2.3). Assume that $n := |Z(K)| = |K|$ and for all $j \notin Z(K)$

$$\operatorname{supp}(u_j) \cap K = \operatorname{supp}(v_j) \cap K = \emptyset.$$

Let $\mathfrak{p}'$ be a primary component of the lattice ideal $I_{\mathcal{L}'}$ associated to the sublattice of $\mathbb{Z}^{m-n}$ spanned by v_j, $j \notin Z(K)$. Then, the ideal

$$\mathfrak{q} = \mathfrak{p}' + \langle b_i, i \in Z(K) \rangle$$

is a primary component of J with associated prime

$$\mathfrak{p} = \mathfrak{p}' + \langle x_k, k \in K \rangle.$$

Note that for $K = \emptyset$ we recover the components of $I_{\mathcal{L}}$.

In order to describe the multiplicity and geometric degree of a component $\mathfrak{q}$, let us assume that $K = Z(K) = \{1, \ldots, n\}$ and for any $w \in \mathbb{Z}^m$, denote $\pi(w) = (w_1, \ldots, w_n)$. Let $\alpha_j = \pi(u_j)$, $\beta_j = \pi(v_j)$ and set

$$p_j(c; x) = x^{\alpha_j} - c_j x^{\beta_j}, \quad c_j \in k^*.$$

Since J is a complete intersection, $p_1, \ldots, p_n$ is a gci. Let μ denote the multiplicity at the origin. Fix coefficients $c \in (k^*)^n$ such that $\mathcal{J}_c$ is a complete intersection. Since

$$\mu = \text{length}\,(k[x_1, \ldots, x_n]/\mathcal{J}_c)_0 = \text{length}\,(k[x_1, \ldots, x_m]/J)_{\mathfrak{p}}\,,$$

and the degree of $\mathfrak{p}$ equals that of $\mathfrak{p}'$, we have

Proposition 5.1. *With notation as above, the multiplicity of* $\mathfrak{q}$ *equals* μ *and the geometric degree of* $\mathfrak{q}$ *equals* $d_{\mathcal{L}'} \cdot \mu$.

As a second application, consider a system of constant coefficient partial differential equations defined by n operators of the form

$$a_j \partial^{\alpha_j} - b_j \partial^{\beta_j}, \quad j = 1, \ldots, n, \tag{5.1}$$

where $a_j, b_j \in k^*$, $\alpha_j, \beta_j \in \mathbb{N}^n$, $\alpha_j \neq \beta_j$. Assume moreover that the ideal J in $k[x_1, \ldots, x_n]$ be generated by the binomials $a_j x^{\alpha_j} - b_j x^{\beta_j}$ is zero-dimensional. As before, let μ_L be the number of points in $\mathbb{V}(J) \cap \bar{k}^n_L$ counted with multiplicity. From [29, Chapter 10], we have the following characterization.

Proposition 5.2. *Let* $L \subseteq \{1, \ldots, n\}$. *The dimension of the space of solutions to* (5.1) *which depend polynomially on the variables* x_ℓ, $\ell \in L$, *and exponentially on the remaining variables* x_j, $j \notin L$, *equals* μ_L.

These dimensions can then be computed using the results in Section 3, particularly formula (3.14).

Acknowledgments

We acknowledge the generous help of many colleagues and friends. We are grateful to Bernd Sturmfels for the first discussions that lead to this project. We thank Mircea Mustata for his key suggestions for the proof of Theorem 3.2. We are indebted to Peter Bürgisser for listening to our questions for many hours, and for pointing out the connection of our formulas with the problem of counting independent sets, which is the key to our main complexity result. We also thank Martín Mereb and Martin Lotz for useful discussions, and Daniel Szyld for pointing out the references on non-negative matrices.

References

[1] M. Barile, M. Morales, A. Thoma, On simplicial toric varieties which are set-theoretic complete intersections, J. Algebra 226 (2) (2000) 880–892.

[2] D. Bayer, D. Mumford, What can be computed in algebraic geometry?, in: Computational Algebraic Geometry and Commutative Algebra, Cortona, 1991, Symposium on Mathematics, XXXIV, Cambridge University Press, Cambridge, 1993, pp. 1–48.

[3] A. Berman, R.J. Plemmons, Nonnegative matrices in the mathematical sciences, Classics in Applied Mathematics, vol. 9, Society for Industrial and Applied Mathematics, SIAM, Philadelphia, PA, 1994. (Revised reprint of the 1979 original.)

[4] E. Cattani, R. Curran, A. Dickenstein, Complete intersections in toric ideals, Proceedings of the American Mathematical Society, 2006, in press.

[5] D. Cox, J. Little, D. O'Shea, Ideals, varieties, and algorithms, Undergraduate Texts in Mathematics, Springer, New York, second ed., 1997, An introduction to computational algebraic geometry and commutative algebra.

[6] C. Delorme, Sous-monoı¨des d'intersection complète de N, Ann. Sci. École Norm. Sup. (4) 91 (1) (1976) 145–154.

[7] A. Dickenstein, L.F. Matusevich, T. Sadykov, Bivariate hypergeometric D-modules, Adv. Math. 196 (1) (2005) 78–123.

[8] A. Dickenstein, B. Sturmfels, Elimination theory in codimension two, J. Symbolic Comput. 4 (2002) 119–135.

[9] I.S. Duff, J.K. Reid, An implementation of Tarjan's algorithm for the block triangularization of a matrix, ACM Trans. Math. Software 4 (2) (1978) 137–147.

[10] D. Eisenbud, B. Sturmfels, Binomial ideals, Duke Math. J. 84 (1) (1996) 1–45.

[11] K.G. Fischer, W. Morris, J. Shapiro, Affine semigroup rings that are complete intersections, Proc. Amer. Math. Soc. 125 (11) (1997) 3137–3145.

[12] K.G. Fischer, W. Morris, J. Shapiro, Mixed dominating matrices, Linear Algebra Appl. 270 (1998) 191–214.

[13] K.G. Fischer, J. Shapiro, Mixed matrices and binomial ideals, J. Pure Appl. Algebra 113 (1) (1996) 39–54.

[14] G.M. Greuel, G. Pfister, A Singular Introduction to Commutative Algebra, Springer, Berlin, Heidelberg, New York, 2002.

[15] G.-M. Greuel, G. Pfister, H. Schönemann, Singular 3.0. A computer algebra system for polynomial computations, Centre for Computer Algebra, University of Kaiserslautern, 2001, ⟨http://www.singular.uni-kl.de⟩.

[16] J. Herzog, Generators and relations of abelian semigroups and semigroup rings, Manuscripta Math. 3 (1970) 175–193.

[17] S. Hoşten, J. Shapiro, Primary decomposition of lattice basis ideals, J. Symbolic Comput. 29 (4–5) (2000) 625–639.

[18] V.G. Kac, Infinite-Dimensional Lie Algebras, third ed., Cambridge University Press, Cambridge, 1990.

[19] U. Koppenhagen, E.W. Mayr, An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals, J. Symbolic Comput. 28 (1999) 317–338.

[20] U. Koppenhagen, E.W. Mayr, An optimal algorithm for constructing the reduced Gröbner basis of binomial ideals and applications to commutative semigroups, J. Symbolic Comput. 31 (2001) 259–276;
U. Koppenhagen, E.W. Mayr, Computational Algebra and Number Theory, Milwaukee, WI, 1996.

[21] H. Matsumura, Commutative ring theory, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989. (Translated from the Japanese by M. Reid.)

[22] E.W. Mayr, A.R. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. Math. 46 (3) (1982) 305–329.

[23] I. Ponzoni, M.C. Sánchez, N.B. Brignole, Permutation of sparse matrices to a specific lower btf using graph decompositions, Electron. J. Sociology 1 (1) (1998) 76–87.

[24] J.S. Provan, M.O. Ball, The complexity of counting cuts and of computing the probability that a graph is connected, SIAM J. Comput. 12 (4) (1983) 777–788.
[25] M. Saito, B. Sturmfels, N. Takayama, Gröbner deformations of hypergeometric differential equations, Algorithms and Computation in Mathematics, vol. 6, Springer, Berlin, 2000.
[26] G. Scheja, O. Scheja, U. Storch, On regular sequences of binomials, Manuscripta Math. 98 (1) (1999) 115–132.
[27] D.V. Steward, On an approach to techniques for the analysis of the structure of large systems of equations, SIAM Rev. 4 (1962) 321–342.
[28] B. Sturmfels, Gröbner bases and convex polytopes, University Lecture Series, vol. 8, American Mathematical Society, Providence, RI, 1996.
[29] B. Sturmfels, Solving Systems of Polynomial Equations, CBMS Regional Conference Series in Mathematics, vol. 97, AMS, Providence, RI, 2002.
[30] R. Tarjan, Depth-first search and linear graph algorithms, SIAM J. Comput. 1 (2) (1972) 146–160.
[31] L.G. Valiant, The complexity of enumeration and reliability problems, SIAM J. Comput. 8 (1979) 410–421.