Subtractive Reductions and Complete Problems for Counting Complexity Classes

Arnaud Durand
LACL
Dept. of Computer Science
Université Paris 12
94010 Créteil, France.
durand@univ-paris12.fr

Miki Hermann
LORIA (CNRS)
BP 239
54506 Vandœuvre-lès-Nancy
France.
hermann@loria.fr

Phokion G. Kolaitis*
Computer Science Department
University of California
Santa Cruz, CA 95064, U.S.A.
kolaitis@cse.ucsc.edu

Abstract

We introduce and investigate a new type of reductions between counting problems, which we call *subtractive reductions*. We show that the main counting complexity classes #P, #NP, as well as all higher counting complexity classes $\#\cdot\Pi_k^{\mathrm{P}}$, $k \geq 2$, are closed under subtractive reductions. We then pursue problems that are complete for these classes via subtractive reductions. We focus on the class #NP (which is the same as the class #·coNP) and show that it contains natural complete problems via subtractive reductions, such as the problem of counting the minimal models of a Boolean formula in conjunctive normal form and the problem of counting the cardinality of the set of minimal solutions of a homogeneous system of linear Diophantine inequalities.

1 Introduction and Summary of Results

Decision problems ask whether a "solution" exists, whereas counting problems ask how many different "solutions" exist. Valiant [Val79a, Val79b] developed a computational complexity theory of counting problems by introducing the class #P of functions that count the number of accepting paths of nondeterministic polynomial-time Turing machines; thus, #P captures counting problems whose underlying decision problem (is there a "solution"?) is in NP. Moreover, Valiant demonstrated that #P contains a wealth of complete problems, that is, there are problems in #P such that every problem in #P can be reduced to them via a suitable polynomial-time Turing reduction. Clearly, a counting problem is at least as hard as its underlying decision problem. Valiant's seminal discovery was that there can be a dramatic gap in inherent computational complexity between a counting problem and its underlying decision problem. Specifically, Valiant [Val79a] showed that there are #P-complete problems whose underlying decision problem is solvable in polynomial time. The first problem to exhibit this "easy-to-decide, but hard-to-count" behavior

*Research partially supported by NSF Grant CCR-9732041.

was #PERFECT MATCHINGS, which is the problem of counting the number of perfect matchings in a given bipartite graph. Indeed, Valiant [Val79a] showed that #PERFECT MATCHINGS is #P-complete via polynomial-time 1-Turing reductions, that is, Turing reductions that only allow a single call to an oracle. Subsequent research in this area revealed an abundance of other natural #P-complete problems possessing these properties [Val79b, PB83, Lin86].

In addition to introducing #P, Valiant [Val79a] also developed a machine-based framework for introducing higher counting complexity classes. In this framework, the first class beyond #P is the class #NP of functions that count the number of accepting paths of polynomial-time nondeterministic Turing machines with access to NP oracles. More recently, Hemaspaandra and Vollmer [HV95] developed a predicate-based framework for introducing higher counting complexity classes, which subsumes Valiant's framework and makes it possible to introduce other counting classes that draw finer distinctions. In particular, Valiant's class #NP coincides with the class $\#\cdot$coNP of the Hemaspaandra-Vollmer framework.

As regards complete problems for these higher counting complexity classes, the state of affairs is rather complicated. Toda and Watanabe [TW92] showed if a problem is #P-hard via polynomial-time 1-Turing reductions, then it is also $\#\cdot$coNP-hard and $\#\cdot\Pi_k^{\mathrm{P}}$-hard, for each $k \geq 2$, where $\#\cdot\Pi_k^{\mathrm{P}}$ is the counting version of the class Π_k^{P} at the k-th level of the polynomial hierarchy PH. This surprising result yields an abundance of problems that are complete for these higher counting classes; for instance, #PERFECT MATCHINGS is such a problem. At the same time, it strongly suggests that #P, $\#\cdot$coNP, and all other higher counting classes are not closed under polynomial-time 1-Turing reductions. In turn, this means that problems like #PERFECT MATCHINGS do not capture the inherent complexity of the higher counting complexity classes. Needless to say that these classes are closed under *parsimonious* reductions, i.e., polynomial-time reductions that preserve the number of solutions. The parsimonious reductions, however, also preserve the complexity of the underlying decision problem; thus, they cannot be used to discover the existence of problems that are complete for the higher counting complexity classes and exhibit an "easy-to-decide, but hard-to-count" behavior.

In this paper, we introduce a new type of reductions between counting problems, which we call *subtractive reductions*, since they make it possible to count the number of solutions by first overcounting them and then carefully subtracting any surplus. We make a case that the subtractive reductions are perfectly tailored for the study of $\#\cdot$coNP and of the higher counting complexity classes $\#\cdot\Pi_k^{\mathrm{P}}$, $k \geq 2$. To this effect, we first show that each of these higher counting complexity classes is closed under subtractive reductions. We then focus on the class $\#\cdot$coNP and show that it contains natural complete problems via subtractive reductions, such as the problem of counting the minimal models of a Boolean formula in conjunctive normal form and the problem of counting the cardinality of the set of minimal solutions of a homogeneous system of linear Diophantine inequalities. These two particular counting problems have the added feature that the complexity of their underlying decision problems is lower than Σ_2^{P}-complete, which is the complexity of the decision problem underlying $\#\Pi_1$SAT, the generic $\#\cdot$coNP-complete problem via parsimonious reductions.

2 Counting Problems and Counting Complexity Classes

A *counting problem* is typically presented using a suitable *witness* function which for every input x, returns a set of *witnesses* for x. Formally, a *witness* function is a function $w\colon \Sigma^* \longrightarrow \mathcal{P}^{<\omega}(\Gamma)$, where Σ and Γ are two alphabets, and $\mathcal{P}^{<\omega}(\Gamma)$ is the collections of all finite subsets of Γ. Every such witness function gives rise to the following *counting problem*: given a string $x \in \Sigma$, find the cardinality $|w(x)|$ of the *witness* set $w(x)$. In the sequel, we will refer to the function $w \mapsto |w(x)|$ as the *counting function* associated with the above counting problem; moreover, we will identify counting problems with their associated counting functions.

Valiant [Val79a, Val79b] was the first to investigate the computational complexity of counting problems. To this effect, he introduced the class #P of counting functions that count the number of accepting paths of nondeterministic polynomial-time Turing machines. The prototypical problem in #P is #SAT, which is the counting version of Boolean satisfiability.

#SAT
Input: A Boolean formula φ in conjunctive normal form.
Output: Number of truth assignments to the variables of φ that satisfy φ.

Valiant [Val79a] showed that #SAT is #P-*complete* via *parsimonious* reductions, that is, every counting problem in #P can be reduced to #SAT via a polynomial-time reduction that preserves the cardinalities of the witness sets. Moreover, the same holds true for the counting versions of many other NP-complete problems. Valiant's seminal discovery, however, was the existence of a plethora of problems that exhibit an "easy-to-decide, but hard-to-count" behavior. More precisely, if a counting problem is described via a witness function w, then the *underlying decision problem for* w asks: given a string x, is $w(x) \neq \emptyset$? Valiant [Val79a, Val79b] showed that there are #P-complete problems such that their underlying decision problems is solvable in polynomial time. The first important problem shown to possess these properties was #PERFECT MATCHINGS, which is the problem of counting the number of perfect matchings in a bipartite graph. Clearly, unless P = NP, #PERFECT MATCHINGS (and any other problem exhibiting the easy-to-decide, but hard-to-count behavior) cannot be #P-complete under parsimonious reductions. As it turns out, #PERFECT MATCHINGS is #P-complete via *polynomial-time 1-Turing reductions*, which are a restricted form of Turing reductions allowing a single query to an oracle. More precisely, a counting problem v is *polynomial-time 1-Turing reducible* to a counting problem w, if there is a deterministic Turing machine M that computes $|v(x)|$ in polynomial time by making a single call to an oracle that computes $|w(y)|$. Note that parsimonious reductions constitute the special case of polynomial-time 1-Turing reductions in which $v = w \circ g$, for some polynomial-time computable total function g. In other words, the oracle for $|w(y)|$ is queried once and no computation is performed after the oracle's answer is received.

In addition to initiating the study of #P, Valiant [Val79a, Val79b] developed a framework for introducing higher counting complexity classes. Specifically, for every complexity class $\mathcal{C}$ of decision problems, he defined $\#\mathcal{C}$ to be the union $\bigcup_{A\in\mathcal{C}}(\#\mathrm{P})^A$, where $(\#\mathrm{P})^A$ is the collection of all functions that count the accepting paths of nondeterministic polynomial-time Turing machines having A as their oracle. Thus, in this framework, #NP is the class of functions that count the number of accepting paths of $\mathrm{NP}^{\mathrm{NP}}$ machines. Note that, since there is no difference between querying the oracle or its complement, $\#\mathcal{C} = \#\mathrm{co}\mathcal{C}$ holds for every complexity class $\mathcal{C}$. In particular, we have that #NP = #coNP; more generally, $\#\Sigma_k^{\mathrm{P}} = \#\Pi_k^{\mathrm{P}}$, for every $k \geq 1$, where Σ_k^{P} is the k-th level of the polynomial hierarchy PH and $\Pi_k^{\mathrm{P}} = \mathrm{co}\Sigma_k^{\mathrm{P}}$ (recall that $\Sigma_1^{\mathrm{P}} = \mathrm{NP}$ and $\Pi_1^{\mathrm{P}} = \mathrm{coNP}$).

More recently, researchers have introduced higher complexity counting classes using a predicate-based framework that focuses on the complexity of membership in the witness sets. Specifically, if $\mathcal{C}$ is a complexity class of decision problems, then Hemaspaandra and Vollmer [HV95] define $\#\cdot\mathcal{C}$ to be the class of all counting problems whose witness function w satisfies the following conditions:

1. There is a polynomial $p(n)$ such that for every x and every $y \in w(x)$, we have that $|y| \leq p(|x|)$, where $|x|$ is the length of x and $|y|$ is the length of y;

2. The decision problem "given x and y, is $y \in w(x)$?" is in $\mathcal{C}$.

What is the relationship between counting complexity classes in these two different frameworks? It is easy to verify that $\#\mathrm{P} = \#\cdot\mathrm{P}$, that is, Valiant's class $\#\mathrm{P}$ coincides with the class of witness functions for which membership in the witness set can be tested in polynomial time. As regards higher counting complexity classes, information about this relationship is provided by the following result, which is essentially due to Toda [Tod91] (see also [HV95]).

Theorem 2.1 *For every $k \geq 1$, $\#\cdot\Sigma_k^{\mathrm{P}} \subseteq \#\Sigma_k^{\mathrm{P}} = \#\cdot\mathrm{P}^{\Sigma_k^{\mathrm{P}}} = \#\cdot\Pi_k^{\mathrm{P}}$. In particular, $\#\cdot\mathrm{NP} \subseteq \#\mathrm{NP} = \#\cdot\mathrm{P}^{\mathrm{NP}} = \#\cdot\mathrm{coNP}$.*

Proof: (*Hint*) It is easy to verify that $\#\Sigma_k^{\mathrm{P}} = \#\cdot\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$ holds for every $k \geq 1$. It is harder, however, to establish that $\#\cdot\mathrm{P}^{\Sigma_k^{\mathrm{P}}} = \#\cdot\Pi_k^{\mathrm{P}}$ holds for every $k \geq 1$. For $k = 1$, this was proved by Toda [Tod91] in his Ph.D. thesis; a self-contained proof can be found in Hemaspaandra and Vollmer [HV95]. For $k > 1$, the proof proceeds along the lines of the proof for $k = 1$ in [HV95] by defining a predicate B that describes paths of computations of a $\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$-machine, and showing that B is in Π_k^{P}. Details will appear in the full paper. Finally, the containment $\#\cdot\Sigma_k^{\mathrm{P}} \subseteq \#\cdot\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$ follows from the containment $\Sigma_k^{\mathrm{P}} \subseteq \mathrm{P}^{\Sigma_k^{\mathrm{P}}}$. □

Theorem 2.1 shows that the predicate-based framework not only subsumes the machine-based framework, but also makes it possible to make finer distinctions between counting complexity classes that were absent in the machine-based framework. Indeed, for each $k \geq 1$, Valiant's class $\#\Sigma_k^{\mathrm{P}}$ (which is the same as $\#\Pi_k^{\mathrm{P}}$) coincides with $\#\cdot\Pi_k^{\mathrm{P}}$. Moreover, the class $\#\cdot\Pi_k^{\mathrm{P}}$ appears to be different and, hence, larger than $\#\cdot\Sigma_k^{\mathrm{P}}$. In particular, results by Köbler, Schöning, and Torán [KST89] imply that $\#\cdot\mathrm{NP} = \#\cdot\mathrm{coNP}$ if and only if $\mathrm{NP} = \mathrm{coNP}$.

In general, what makes a complexity class interesting is the existence of natural problems that are complete for the class. As mentioned earlier, $\#\mathrm{P}$ is a particularly interesting complexity class because it contains natural complete problems, such as #PERFECT MATCHINGS, whose underlying decision problem is solvable in polynomial time. Do the higher counting complexity classes $\#\cdot\Pi_k^{\mathrm{P}}$ (and $\#\cdot\Sigma_k^{\mathrm{P}}$) contain natural complete problems and, if so, do some of these problems have an easier underlying decision problem than others? We begin exploring these questions by considering counting problems based on quantified Boolean formulas with a bounded number of quantifier alternations. In what follows, k is a fixed positive integer.

$\#\Pi_k$SAT
Input: A formula $\varphi(y_1, \ldots, y_n) = \forall x_1 \exists x_2 \cdots Q_k x_k\ \psi(x_1, \ldots, x_k, y_1, \ldots, y_n)$, where ψ is a Boolean formula.
Output: Number of truth assignment to the variables $y_1, \ldots, y_n$ that satisfy φ.

Proposition 2.2 *$\#\Pi_k$SAT is $\#\cdot\Pi_k^{\mathrm{P}}$-complete via parsimonious reductions. In addition, if k is odd (even), then the problem remains $\#\cdot\Pi_k^{\mathrm{P}}$-complete when restricted to inputs in which the quantifier-free part is a Boolean formula in disjunctive normal form (respectively, in conjunctive normal form).*

The above result seems to be part of the folklore, although we are not able to locate a specific reference; a self-contained proof of Proposition 2.2 can be found in the Appendix. One can also define the counting problem $\#\Sigma_k$SAT in a similar manner and show that it is $\#\cdot\Sigma_k^{\mathrm{P}}$-complete via parsimonious reductions.

Note that the decision problem underlying $\#\Pi_k$SAT is Σ_{k+1}SAT, which is the prototypical $\Sigma_{k+1}^{\mathrm{P}}$-complete problem. Thus, the question becomes: are there any natural $\#\cdot\Pi_k^{\mathrm{P}}$-complete problems such that their underlying decision problem is of lower computational complexity (i.e., lower than

$\Sigma^{\mathrm{P}}_{k+1}$-complete)? Clearly, unless $\Sigma^{\mathrm{P}}_{k+1}$ collapses to a lower complexity class, no such problem can be $\#\cdot\Pi^{\mathrm{P}}_k$-complete via parsimonious reductions, which means that a broader class of reductions has to be considered. To this effect, Toda and Watanabe [TW92] proved the following surprising and quite significant result: if a counting problem is #P-hard via polynomial-time 1-Turing reductions, then it is also $\#\cdot\Pi^{\mathrm{P}}_k$-complete via the same reductions, for every $k \geq 1$. Consequently, #PERFECT MATCHINGS is $\#\cdot\Pi^{\mathrm{P}}_k$-complete via polynomial-time 1-Turing reductions. At first sight, Toda and Watanabe's theorem [TW92] can be interpreted as providing an abundance of $\#\cdot\Pi^{\mathrm{P}}_k$-complete problems such that their underlying decision problem is of low complexity. A moment's reflection, however, reveals that this theorem provides strong evidence that #P, #·coNP, and all other higher counting complexity $\#\cdot\Pi^{\mathrm{P}}_k$, $k \geq 2$, are *not* closed under polynomial-time 1-Turing reduction. Moreover, it implies that polynomial-time 1-Turing reductions cannot help us discover complete problems that embody the inherent difficulty of each counting complexity classes $\#\cdot\Pi^{\mathrm{P}}_k$, $k \geq 1$, and allow us to draw meaningful distinctions between these classes. Consequently, the challenge is to discover a different class of reductions that have the following two crucial properties: (1) each class $\#\cdot\Pi^{\mathrm{P}}_k$, $k \geq 1$, is closed under these reductions; (2) each class $\#\cdot\Pi^{\mathrm{P}}_k$, $k \geq 1$, contains natural problems that are complete for the class via these reductions. In what follows, we take the first steps towards confronting this challenge.

3 Subtractive Reductions

Researchers in structural complexity theory have extensively investigated various *closure properties* of #P and of certain other counting complexity classes (see [HO92, OH93]). For instance, it is well known and easy to prove that #P is closed under both addition and multiplication.[1] In turn, this has motivated researchers to introduce reductions that take advantage of closure properties. Indeed, Saluja, Subrahmanyam and Thakur [SST95] and Sharell [Sha98] used the closure of #P under addition and multiplication to introduce approximation-preserving reductions between counting problems. In particular, Sharell's [Sha98] *PL-reductions* involve positive linear combinations that approximate the desired value from below. Unfortunately, these reductions do not seem to be suited for our purposes. Instead, we adopt a different approach and introduce the class of *subtractive reductions* that first overcount and then subtract any surplus items. It should be emphasized that defining such reductions is a delicate matter, since many counting complexity classes, including #P, do *not* appear to be closed under subtraction. Specifically, Ogiwara and Hemachandra [OH93] have shown that #P is closed under subtraction if and only if the class PP of problems solvable in probabilistic polynomial time coincides with the class UP of problems solvable by an unambiguous Turing machine in polynomial time, which is considered an unlikely eventuality. Before defining the class of subtractive reductions, we need to introduce certain auxiliary concepts and establish notation.

Let D be a non-empty set. Intuitively, a *multiset* on D is a collection of elements of D in which elements may have multiple occurrences. More formally, a *multiset* M on D can be viewed as a function $M\colon D \longrightarrow \mathbb{N}$ that assigns to each element $x \in D$ the number $M(x)$ of the occurrences of x in M. The multisets on D can be equipped with the operations of *union* and *difference* as follows.

Let A and B be two multisets on D. The *union* of A and B is the multiset $A \oplus B$ such that $(A \oplus B)(x) = A(x) + B(x)$ for every $x \in D$. The *difference* of A and B is the multiset $A \ominus B$ such that $(A \ominus B)(x) = \max(A(x) - B(x), 0)$ for every $x \in D$. We say that A is *contained* in B, and write $A \subseteq B$, if $A(x) \leq B(x)$ for every $x \in D$. Note that if $B \subseteq A$, then $(A \ominus B)(x) = A(x) - B(x)$ holds for all $x \in D$. With each element $x \in D$ we associate the membership function m_x that satisfies the

[1] Apparently, K. Regan was the first to observe this closure property of #P, see [HO92].

following equations: $m_x(A) = A(x)$, $m_x(A \oplus B) = A(x) + B(x)$, and $m_x(A \ominus B) = A(x) - B(x)$, provided that $B \subseteq A$. Hence, whenever multiset difference is taking place between two multisets such that one is contained in the other, then the multiset operations can be replaced by the ordinary arithmetic operations. Finally, if $A_1, \ldots, A_n$ are multisets, then we write $\bigoplus_{i=1}^n A_i$ to denote the union $A_1 \oplus \cdots \oplus A_n$.

Let Σ, Γ be two alphabets and let $R \subseteq \Sigma^* \times \Gamma^*$ be a binary relation between strings such that, for each $x \in \Sigma^*$, the set $R(x) = \{y \in \Gamma^* \mid R(x,y)\}$ is finite. We write $\#\cdot R$ to denote the following counting problem: given a string $x \in \Sigma^*$, find the cardinality $|R(x)|$ of the witness set $R(x)$ associated with x. It is easy to see that every counting problem is of the form $\#\cdot R$ for some R.

Definition 3.1 Let Σ, Γ be two alphabets and let A and B be two binary relations between strings from Σ and Γ. We say that *the counting problem $\#\cdot A$ reduces to the counting problem $\#\cdot B$ via a subtractive reduction*, and write $\#\cdot A \leq_s \#\cdot B$, if there exist a positive integer n and polynomial-time computable functions f_i and g_i, $i = 1, \ldots, n$, such that for every string $x \in \Sigma^*$:

- $\bigoplus_{i=1}^n B(f_i(x)) \subseteq \bigoplus_{i=1}^n B(g_i(x))$;
- $|A(x)| = \sum_{i=1}^n |B(g_i(x))| - \sum_{i=1}^n |B(f_i(x))|$.

Clearly, parsimonious reductions constitute a special case of subtractive reductions. Our first result about subtractive reductions is that they compose nicely. The proof of this result, which uses certain basic algebraic properties of multisets, can be found in the Appendix.

Theorem 3.2 *Reducibility via subtractive reductions is a transitive relation, that is, if $\#\cdot A \leq_s \#\cdot B$ and $\#\cdot B \leq_s \#\cdot C$, then $\#\cdot A \leq_s \#\cdot C$.*

Next we establish the main result of this section; it asserts that Valiant's counting complexity classes are closed under subtractive reductions.

Theorem 3.3 $\#\mathrm{P}$ *and all higher counting complexity class $\#\cdot\Pi_k^{\mathrm{P}} = \#\Sigma_k^{\mathrm{P}}$, $k \geq 1$, are closed under subtractive reductions.*

Proof: (*Sketch*) Let k be a fixed positive integer. In what follows, we sketch the proof that the class $\#\cdot\Pi_k^{\mathrm{P}}$ is closed under subtractive reductions; the proof for $\#\mathrm{P}$ requires only minor modifications. Recall that $\#\cdot\Pi_k^{\mathrm{P}} = \#\Sigma_k^{\mathrm{P}} = \#\cdot\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$, as asserted in Theorem 2.1. Let $\#\cdot A$ and $\#\cdot B$ be two counting problems such that $\#\cdot B \in \#\cdot\Pi_k^{\mathrm{P}}$ and $\#\cdot A$ reduces to $\#\cdot B$ via subtractive reduction. We will show that $\#\cdot A$ belongs to $\#\cdot\Pi_k^{\mathrm{P}}$ by constructing a predicate A' in $\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$ such that

$$|A'(x)| \quad = \quad \textstyle\sum_i^n |B(g_i(x))| - \sum_i^n |B(f_i(x))| \quad = \quad |A(x)|\,,$$

where f_i and g_i, $1 \leq i \leq n$, are the polynomial-time computable function in the subtractive reduction of $\#\cdot A$ to $\#\cdot B$. The elements of the predicate A' will be pairs of strings (x, y') such that $y' = f_1(x) * \cdots * f_n(x) * g_1(x) * \cdots * g_n(x) * y * z$, where z is an integer ranging from 1 to the number b of occurrences of y in the multiset $\bigoplus_i^n B(g_i(x)) \ominus \bigoplus_i^n B(f_i(x))$, and $*$ is just a delimiter symbol.

The predicate A' is constructed as follows. A pair (x, y') belongs to A' if and only if (x, y') is accepted by the following algorithm:

1. extract $f_1(x)$, …, $f_n(x)$, $g_1(x)$, …, $g_n(x)$, y from y';
2. find the number c_g of pairs $(g_i(x), y)$, $1 \leq i \leq n$, that belong to B;

3. find the number c_f of pairs $(f_i(x), y)$, $1 \le i \le n$, that belong to B;

4. check that $z \le c_g - c_f$.

Step 4 ensures that, for every y, there are as many accepted strings y' as the number of occurrences of y in the multiset $\bigoplus_i^n B(g_i(x)) \ominus \bigoplus_i^n B(f_i(x))$. Therefore, the number of pairs (x, y') accepted by A' is equal to the number of pairs $(x, -)$ accepted by A. Step 1 can be carried out in polynomial time. For each pair in Step 2, the test is in Π_k^{P}; moreover, c_g is bounded by the fixed number n of the functions g_i. Hence, Step 2 is in $\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$. For each pair in Step 3, the test is in Σ_k^{P}; moreover, c_f is bounded by also bounded by n. Hence, as above, Step 3 is in $\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$. Step 4 can be carried out in polynomial time. Consequently, the predicate A' is in $\mathrm{P}^{\Sigma_k^{\mathrm{P}}}$. □

In view of the preceding Theorem 3.3, it is natural to ask whether the classes $\#\cdot\Sigma_k^{\mathrm{P}}$, $k \ge 1$, introduced by Hemaspaandra and Vollmer [HV95], are also closed under subtractive reductions. We now provide evidence to the effect that *no* class $\#\cdot\Sigma_k^{\mathrm{P}}$ is closed under subtractive reductions. For this, we observe that $\#\Pi_k$SAT, the generic complete problem for $\#\cdot\Pi_k^{\mathrm{P}}$, can easily be reduced to $\#\Sigma_k$SAT, the generic complete problem for $\#\cdot\Sigma_k^{\mathrm{P}}$, via a subtractive reduction. Consequently, if $\#\cdot\Sigma_k^{\mathrm{P}}$ were closed under subtractive reductions, then $\#\cdot\Pi_k^{\mathrm{P}}$ would collapse to $\#\cdot\Sigma_k^{\mathrm{P}}$, which is generally considered as highly unlikely.

Let $\varphi(y_1, \ldots, y_n)$ be any Π_k-formula $\forall x_1 \exists x_2 \cdots Q_k x_k\ \phi(x_1, \ldots, x_k, y_1, \ldots, y_n)$. Let $\bar{\varphi}(y_1, \ldots, y_n)$ be the Σ_k formula that is equivalent to $\neg\varphi$ and is obtained from φ by propagating the negation symbol through the quantifiers and applying de Morgan laws to the quantifier-free part of φ. Let $\psi(y_1, \ldots, y_n)$ be the tautology $y_1 \vee \neg y_1 \vee y_2 \vee \neg y_2 \vee \cdots \vee y_n \vee \neg y_n$. It is obvious that every satisfying truth assignment of $\bar{\varphi}$ is a satisfying truth assignment of ψ and that $\#(\varphi) = \#(\psi) - \#(\bar{\varphi})$, where $\#(\varphi)$ denotes the number of satisfying truth assignments of φ (and similarly for ψ and $\bar{\varphi}$). Consequently, the polynomial-time computable functions $f_1(\varphi) = \bar{\varphi}$ and $g_1(\varphi) = \psi$ constitute a subtractive reduction of $\#\Pi_k$SAT to $\#\Sigma_k$SAT.

Observe that the preceding argument can also be applied to a Boolean formula φ in conjunctive normal form (i.e., assume $k = 0$) to produce a subtractive reduction of #SAT to #DNF, where #DNF is the following counting problem.

#DNF
Input: A Boolean formula θ in disjunctive normal form.
Output: Number of truth assignments to the variables of θ that satisfy θ.

Consequently, we obtain a well-known #P-completeness result by means of our new reduction.

Proposition 3.4 *#DNF is #P-complete via subtractive reductions.*

Observe that #DNF cannot be #P-complete via parsimonious reductions, since its underlying decision problem is easily solvable in polynomial time. As stated earlier, #PERFECT MATCHINGS is #P-complete via polynomial-time 1-Turing reductions. It is an interesting open problem to determine whether #PERFECT MATCHINGS is also #P-complete via subtractive reductions.

4 #·coNP-complete Problems via Subtractive Reductions

Many important counting problems are known to be #P-complete via polynomial-time 1-Turing reductions and have the property that their underlying decision problem is solvable in polynomial time [Val79a, Val79b, PB83, Lin86]. The current state of knowledge, however, is very different for the higher counting complexity classes $\#\cdot\Pi_k^{\mathrm{P}}$ and $\#\cdot\Sigma_k^{\mathrm{P}}$, $k \ge 1$. We do know that they possess generic complete problem, such as $\#\Sigma_k$SAT and $\#\Pi_k$SAT, that are complete for these classes via parsimonious reductions, but have inherently high computational complexity (see Proposition 2.2). We also know that every counting problem that is #P-complete via polynomial-time 1-Turing reductions is also complete for these classes under the same reductions [TW92]. Up to this point, however, it is not known if these higher counting complexity classes contain any problems that have the following two properties: (1) they are complete for the class via reductions under which the class is closed; (2) their underlying decision problems has complexity lower than that of the generic complete problem for the class.

In this section, we focus on the class #·coNP and establish that it contains certain natural counting problems that possess the above two properties. Recall that #·coNP is the first higher counting complexity class that arises in Valiant's framework, since #·coNP = #NP. Moreover, it is quite robust, since, as shown by Toda [Tod91], #·coNP = #NP = $\#\cdot\mathrm{P}^{\mathrm{NP}}$ (see Theorem 2.1).

Circumscription is a well-developed formalism of common-sense reasoning introduced by McCarthy [McC80] and extensively studied by the artificial intelligence community. The key idea behind circumscription is that one is interested in the *minimal models* of formulas, since they are the ones that have as few "exceptions" as possible and, therefore, embody common sense. In the context of Boolean logic, circumscription amounts to the study of satisfying assignments of Boolean formulas that are *minimal* with respect to the *pointwise partial order* on truth assignments. More precisely, if $s = (s_1, \ldots, s_n)$ and $s' = (s'_1, \ldots, s'_n)$ are two elements of $\{0,1\}^n$, then we write $s < s'$ to denote that $s \neq s'$ and $s_i \leq s'_i$ holds for every $i \leq n$. Let $\varphi(x_1, \ldots, x_n)$ be a Boolean formula having $x_1, \ldots, x_n$ as its variables and let $s \in \{0,1\}^n$ be a truth assignment. We say that s is a *minimal model of* φ if s is a satisfying truth assignment of φ and there is no satisfying truth assignment s' of φ such that $s < s'$. This concept gives rise to the following natural counting problem.

#CIRCUMSCRIPTION
Input: A Boolean formula $\varphi(x_1, \ldots, x_n)$ in conjunctive normal form.
Output: Number of minimal models of $\varphi(x_1, \ldots, x_n)$.

The underlying decision problem for #CIRCUMSCRIPTION is NP-complete, since a Boolean formula has a minimal model if and only if it is satisfiable. Thus, it has lower complexity than Σ_2^{P}-complete, which is the complexity of the underlying decision problem for $\#\Pi_1$SAT, the generic problem for #·coNP.

Theorem 4.1 #CIRCUMSCRIPTION *is #·coNP-complete via subtractive reductions.*

Proof: It is clear that the problem belongs to #·coNP, since testing whether a given truth assignment is a minimal model of a given formula is in coNP (actually, this decision problem is coNP-complete [Cad92]).

For the lower bound, we construct a subtractive reduction of $\#\Pi_1$SAT to #CIRCUMSCRIPTION. In what follows, we write $A(F)$ to denote the set of all satisfying assignments of a Π_1-formula F; we also write $B(\psi)$ to denote the set of all minimal models of a Boolean formula ψ. Let $F(x) = \forall y\ \phi(x,y)$ be a Π_1-formula, where $\phi(x,y)$ is a Boolean formula in disjunctive normal form, and $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_m)$ are tuples of Boolean variables. Let $x' = (x'_1, \ldots, x'_n)$ be a tuple of new Boolean variables, let z be a single new Boolean variable, let $P(x, x')$ be the formula $(x_1 \equiv \neg x'_1) \wedge \cdots \wedge (x_n \equiv \neg x'_n)$, let $Q(y)$ be the formula $y_1 \wedge \cdots \wedge y_m$, and, finally, let $F'(x, x', y, z)$ be the formula

$$P(x,x') \wedge (z \rightarrow Q(y)) \wedge (\phi(x,y) \rightarrow z).$$

There is a polynomial-time computable function g such that, given a Π_1-formula F as above, it returns as value a Boolean formula $g(F)$ in conjunctive normal form that is logically equivalent to the formula $F'(x, x', y, z)$ (this is so, because $\phi(x,y)$ is in disjunctive normal form). Now let

$F''(x, x', y, z)$ be the formula $F'(x, x', y, z) \wedge (z \rightarrow \neg Q(y))$ and let f be a polynomial-time computable function such that, given a Π_1-formula F as above, it returns as value a Boolean formula $f(F)$ that is logically equivalent to the formula $F''(x, x', y, z)$.

We will show in a sequence of four claims that there is a bijection between the satisfying assignments of F and the minimal models of F' that do not satisfy F''.

Claim 1: (x, x', y, z) is a model of F' if and only if either $P(x, x') = 1$ and $Q(y) = 1$ and $z = 1$, or $P(x, x') = 1$ and $z = 0$ and $\phi(x, y) = 0$. This is obvious from the definition of F', since $z = 1$ implies $Q(y) = 1$.

Claim 2: (x, x', y, z) is a minimal model of F' if and only if either $\phi(x, y) = 1$ for all y and $P(x, x') = 1$ and $Q(y) = 1$ and $z = 1$, or $P(x, x') = 1$ and $z = 0$ and $\phi(x, y) = 0$ and there is no y' such that $y' < y$ and $\phi(x, y') = 0$. Consider the models $(x, x', 1, \dots, 1, 1)$. Assume that $(x, x', 1, \dots, 1, 1)$ is a minimal model of F'. Then for every y we must have that $\phi(x, y) = 1$, since otherwise $(x, x', y, 0)$ would be a model of F' smaller than $(x, x', 1, \dots, 1, 1)$. Assume that x is such that $\forall y\ \phi(x, y) = 1$. Then $(x, x', 1, \dots, 1, 1)$ is a minimal model of F', since the only way to have a smaller model would be to have one of the form $(x, x', y, 0)$ with $\phi(x, y) = 0$, which contradicts the hypothesis on x. Now, consider models of the form $(x, x', y, 0)$. From Claim 1 it follows that such a model is minimal if and only if there is no $y' < y$ such that $\phi(x, y') = 0$.

Claim 3: (x, x', y, z) is a model of F'' if and only if $P(x, x') = 1$ and $z = 0$ and $\phi(x, y) = 0$. This follows easily from the definition of F''.

Claim 4: (x, x', y, z) is a minimal model of F'' if and only if $P(x, x') = 1$ and $z = 0$ and $\phi(x, y) = 0$ and there is no y' such that $y' < y$ and $\phi(x, y') = 0$. This follows from the definition of F'' and Claim 3.

From Claims 1 to 4, it follows that the set difference of minimal models of F' and F'' is equal to the set $\{(x, x', 1, \dots, 1, 1) \mid \forall y\ \phi(x, y) \wedge P(x, x')\}$. Note that this set is isomorphic to the set of satisfying assignments of the formula F, since the variables x' are functionally dependent on the variables x through the formula $P(x, x')$. Hence, we have that $|A(F)| = |B(F')| - |B(F'')|$, which establishes that the polynomial-time computable functions f and g constitute a subtractive reduction of $\#\Pi_1$SAT to #CIRCUMSCRIPTION. □

The following result is an immediate consequence of Theorems 3.3 and 4.1.

Corollary 4.2 $\#\cdot$coNP $=$ #P *if and only if* #CIRCUMSCRIPTION *is in* #P.

We now move from counting problems in Boolean logic to counting problems in integer linear programming. A *system of linear Diophantine inequalities over the non-negative integers* is a system of the form $S\colon Ax \leq b$, where A is an integer matrix, b is an integer vector, and we are interested in the non-negative integer solutions of this system. If b is the zero-vector $(0, \dots, 0)$, then we say that the system is *homogeneous*. A non-negative integer solution s of S is *minimal* if there is no non-negative solution s' of S such that $s' < s$ in the pointwise partial order on integer vectors. It is well known that the set of all minimal solutions plays an important role in analyzing the space of all non-negative integer solutions of linear Diophantine systems (see Schrijver [Sch86]). Clearly, every homogeneous system has $(0, \dots, 0)$ as a trivial minimal solution. Here, we are interested in counting the number of non-trivial minimal solutions of homogeneous systems.

#HOMOGENEOUS MIN SOL
Input: A homogeneous system $S\colon Ax \leq 0$ of linear Diophantine inequalities.
Output: Number of non-trivial minimal solutions of S.

Note that the underlying decision problem of #HOM MIN SOL amounts to whether a given homogeneous system of linear Diophantine inequalities has a non-negative integer solution other than the trivial solution $(0, \ldots, 0)$. It is easy to show that this problem is solvable in polynomial time, since it can be reduced to LINEAR PROGRAMMING. In contrast, counting the number of non-trivial minimal solutions turns out to be a hard problem.

Theorem 4.3 #HOMOGENEOUS MIN SOL *is* #·coNP*-complete via subtractive reductions.*

Proof: (*Hint*) The problem is in #·coNP, because deciding membership in the witness sets is in coNP; indeed, the size of minimal solutions is bounded by a polynomial in the size of the system (see Corollary 17.1b in [Sch86, page 239]). The lower bound is established through a sequence of subtractive reductions. First, #CIRCUMSCRIPTION can be reduced to #SATISFIABLE CIRC, the restriction of #CIRCUMSCRIPTION to satisfiable Boolean formulas. In turn, this problem has a subtractive reduction to #SATISFIABLE MIN SOL, which asks for the number of minimal solutions of a system $S : Ax \leq b$ of linear Diophantine inequalities having at least one non-negative integer solutions (details of these two reductions can be found in the Appendix). Finally, #SATISFIABLE MIN SOL has a subtractive reduction to #HOMOGENEOUS MIN SOL, which we outline in what follows

Let $S\colon Ax \leq b$ be a system of linear Diophantine inequalities with at least one non-negative integer solution and such that A is $k \times n$ integer matrix. First construct the system $S'\colon Ax - b\bar{y} \leq 0, 2z - t = y, x_i \leq y, x_i \geq y - t$, where $\bar{y} = (y, \ldots, y)$ is a vector of length k having the same variable y in each coordinate, and z and t are additional new variables. After this, construct the system $S'' = S' \cup \{x_1 = \cdots = x_n = y\}$.

Let $A(S)$ be the set of minimal solutions of the system S, and let $B(S')$ and $B(S'')$ be the sets of nontrivial minimal solutions of S' and S'', respectively. In the Appendix we show that $B(S'') \subseteq B(S')$ and that $|A(S)| = |B(S')| - |B(S'')|$. This establishes that the polynomial-time computable functions $f(S) = S'$ and $g(S) = S''$ constitute a subtractive reduction of #SATISFIABLE MIN SOL to #HOMOGENEOUS MIN SOL. □

Corollary 4.4 #·coNP = #P *if and only if* #HOMOGENEOUS MIN SOL *is in* #P.

To the best of our knowledge, the above result provides the first example of a counting problem whose underlying decision problem is solvable in polynomial time, but the counting problem itself is not in #P, unless higher counting complexity classes collapse to #P.

5 Concluding Remarks

We conclude by recalling Valiant's assertion from his influential paper [Val79b] to the effect that *"The completeness class for* #P *appears to be rivalled only by that for* NP *in relevance to naturally occurring computational problems."* The passage of time and the subsequent research in this area certainly proved this to be the case. We believe that the results reported here suggest that also #·coNP contains complete problems of computational significance. Furthermore, we believe that subtractive reductions are the right tool for investigating #·coNP and identifying other natural problems that are #·coNP-complete via these reductions. The next challenge in this vein is to determine whether #HILBERT is #·coNP-complete via subtractive reductions. #HILBERT is the problem of computing the cardinality of the *Hilbert basis* of a homogeneous system $S\colon Ax = 0$ of linear Diophantine equations, i.e., counting the number of non-trivial minimal solutions of such a system. We note that this counting problem was first studied by Hermann, Juban and Kolaitis [HJK99], where it was shown to be a member of #·coNP and also to be #P-hard under polynomial-time 1-Turing reductions.

References

[Cad92] M. Cadoli. The complexity of model checking for circumscriptive formulae. *Information Processing Letters*, 44(3):113–118, 1992.

[HJK99] M. Hermann, L. Juban, and P. G. Kolaitis. On the complexity of counting the Hilbert basis of a linear Diophantine system. In H. Ganzinger, D. McAllester, and A. Voronkov, editors, *Proceedings 6th LPAR'99, Tbilisi (Republic of Georgia)*, volume 1705 of Lecture Notes in Artificial Intelligence, pages 13–32, September 1999. Springer-Verlag.

[HO92] L. A. Hemachandra and M. Ogiwara. Is #P closed under subtraction? *Bulletin of the European Association for Theoretical Computer Science*, 46:107–122, February 1992.

[HV95] L. A. Hemaspaandra and H. Vollmer. The satanic notations: Counting classes beyond #P and other definitional adventures. *SIGACT News*, 26(1):2–13, March 1995.

[Imm99] N. Immerman. *Descriptive complexity.* Springer-Verlag, 1999.

[KST89] J. Köbler, U. Schöning, and J. Torán. On counting and approximation. *Acta Informatica*, 26(4):363–379, 1989.

[Lin86] N. Linial. Hard enumeration problems in geometry and combinatorics. *SIAM Journal on Algebraic and Discrete Methods*, 7(2):331–335, 1986.

[McC80] J. McCarthy. Circumscription — A form of non-monotonic reasoning. *Artificial Intelligence*, 13(1-2):27–39, 1980.

[OH93] M. Ogiwara and L. A. Hemachandra. A complexity theory for feasible closure properties. *Journal of Computer and System Science*, 46(3):295–325, 1993.

[PB83] J. S. Provan and M. O. Ball. The complexity of counting cuts and of computing the probability that a graph is connected. *SIAM Journal on Computing*, 12(4):777–788, 1983.

[Sch86] A. Schrijver. *Theory of linear and integer programming.* John Wiley & Sons, 1986.

[Sha98] A. Sharell. *Descriptive complexity and approximation of counting functions.* PhD thesis, Université Paris 11, Orsay (France), February 1998.

[SST95] S. Saluja, K. V. Subrahmanyam, and M. N. Thakur. Descriptive complexity of #P functions. *Journal of Computer and System Science*, 50(3):493–505, 1995.

[Sto76] L. J. Stockmeyer. The polynomial-time hierarchy. *Theoretical Computer Science*, 3(1):1–22, 1976.

[Tod91] S. Toda. *Computational complexity of counting complexity classes.* PhD thesis, Tokyo Institute of Technology, Department of Computer Science, Tokyo, Japan, 1991.

[TW92] S. Toda and O. Watanabe. Polynomial-time 1-Turing reductions from #PH to #P. *Theoretical Computer Science*, 100(1):205–221, 1992.

[Val79a] L. G. Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8(2):189–201, 1979.

[Val79b] L. G. Valiant. The complexity of enumeration and reliability problems. *SIAM Journal on Computing*, 8(3):410–421, 1979.

Appendix

Proof of Theorem 2.2

A bijection can be defined between each binary string x of length n and structures of the form $str(x) = \langle \mathcal{U} = \{0, \ldots, n-1\}, X^{\mathcal{U}}, <^{\mathcal{U}} \rangle$, where $\mathcal{U}$ represents the sets of positions of x, $<$ is the natural total ordering of the set $\{0, \ldots, n-1\}$ and $X^{\mathcal{U}}(i)$ holds if and only if the i-th position of the string x equals 1. As an example, the word $x = 1010$ is represented by the structure $\langle \mathcal{U} = \{0,1,2,3\}, X = \{0,2\}, < \rangle$. Note that the mapping is not bijective in absence of the ordering relation. In the same way, every pair (x, y) with $|x|^k = n^k = |y|$ can be represented by a unique structure $str(x,y) = \langle \mathcal{U}, X^{\mathcal{U}}, Y^{\mathcal{U}}, <^{\mathcal{U}} \rangle$ with Y being a k-ary relation on $\mathcal{U}$ such that the predicate $Y^{\mathcal{U}}(i_0, \ldots, i_{k-1})$ holds if and only if position $i_0 + i_1 n + \cdots + i_{k-1} n^{k-1}$ of the string y equals 1. We say that the structure $str(x,y)$ extends $str(x)$ as the pair (x,y) is an extension of x.

Recall that Σ_i^{P} is the i-th existential level of the polynomial-time hierarchy PH, and let Σ_i^1 be the i-th level of the second-order logic, i.e., the second-order logic with the formulas in prenex normal form with i alternations of second-order quantifier starting with an *existential* one. In an analogous manner, Π_i^1 will be the i-th level of the second-order logic starting with a *universal* quantifier. In [Sto76], Stockmeyer generalized Fagin's theorem and showed that every level Σ_i^{P} of the polynomial hierarchy corresponds to Σ_i^1. By a straightforward modification of the proof, it holds that for every binary predicate $R \in \Sigma_i^{\mathrm{P}}$, there exists a formula Φ such that $(x,y) \in R$ if and only if $str(x,y) \models \Phi$.

Consider the following counting problem, issued from a direct generalization of the descriptive complexity ideas to the counting classes.

$\#\cdot\boldsymbol{\Sigma_i^1}$GEN-SAT
Input: A formula $\Phi(X, Y, <) \in \Sigma_i^1$ and a structure $str(x)$.
Output: Number of extensions $str(x,y)$ of $str(x)$ that are models of $\Phi(X, Y, <)$.

The problem $\#\cdot\Pi_i^1$GEN-SAT is defined analogously. Note that the counting complexity classes $\#\cdot\Sigma_i^{\mathrm{P}}$ and $\#\cdot\Pi_i^{\mathrm{P}}$, for $i \geq 1$, are closed under parsimonious reductions. This is just a consequence of the result that the classes of decision problems Σ_i^{P} and Π_i^{P} are closed under polynomial many-one reductions.

Proposition 5.1 $\#\cdot\Sigma_i^1$GEN-SAT *(resp.* $\#\cdot\Pi_i^1$GEN-SAT*) is $\#\cdot\Sigma_i^{\mathrm{P}}$-complete (resp. $\#\cdot\Pi_i^{\mathrm{P}}$-complete) with respect to parsimonious reductions.*

Proof: The proof follows from Stockmeyer's characterizations. Let R be a binary predicate in Σ_i^{P}. Then there exists a Σ_i^1 formula Φ such that $(x,y) \in R$ if and only if $str(x,y) = \langle \mathcal{U}, X^{\mathcal{U}}, Y^{\mathcal{U}}, <^{\mathcal{U}} \rangle \models \Phi$.

The bijective encoding of words into structures implies that, for any fixed x, the number of word y, satisfying the membership $(x,y) \in R$, corresponds to the number of extensions $str(x,y)$ of $str(x)$ that are models of Φ, thus giving a parsimonious reductions from $\#\cdot R$ to $\#\cdot\Sigma_i^1$GEN-SAT. □

We are able now to prove Proposition 2.2.

Proposition 2.2. $\#\Pi_k$SAT is $\#\cdot\Pi_k^{\mathrm{P}}$-complete via parsimonious reductions. Moreover, if k is odd (even), then the problem remains $\#\cdot\Pi_k^{\mathrm{P}}$-complete, even if the quantifier-free part of the input is restricted to be a Boolean formula in disjunctive normal form (respectively, in conjunctive normal form).

Proof: The proof mimics the method to derive the completeness of SAT from Fagin's theorem (see [Imm99] for example). We give a parsimonious reduction from $\#\cdot\Sigma_i^1$GEN-SAT to $\#\cdot\Sigma_i$SAT. Let $str(x) = \langle \mathcal{U}, X^{\mathcal{U}}, Y^{\mathcal{U}}, <^{\mathcal{U}} \rangle$ be the considered structure and

$$\Phi(X, Y, <) \quad = \quad \exists R_1 \forall R_2 \cdots Q_i R_i \phi(R_1, \ldots, R_i, X, Y, <)$$

be an instance of $\#\cdot\Sigma_i^1$GEN-SAT. Let $|\mathcal{U}| = n$. We construct an instance $\varphi(y)$ of $\#\cdot\Sigma_i$SAT as follows.

The formula $\varphi(y)$ will contain the boolean variables $R_j(e_1, \ldots, e_{\alpha_j})$ and $Y(e_1, \ldots, e_k)$ for $j = 1, \ldots, i$ and $e_1, \ldots, e_{\alpha_j} \in \mathcal{U}$. First, each block of existentially (resp. universally) quantified second-order variable R_j is replaced by a block of n^{α_j} existentially (resp. universally) quantified boolean variables $R_j(0, 0, \ldots, 0)$, $R_j(0, 0, \ldots, 1)$,..., $R_j(n-1, n-1, \ldots, n-1)$.

Next, replace every first-order universal quantification $\forall x$ in Φ by the conjunction $\bigwedge_{x=0}^{n-1}$ and every existential quantification $\exists x$ by the disjunction $\bigvee_{x=0}^{n-1}$ and unroll the resulting formula, replacing x by its successive value 0, 1 and $n-1$. We then obtain a boolean formula with only variables $Y(e_1, \ldots, e_k)$ (shorten by the vector y) as free variables and whose terms are among $R_j(e_1, \ldots, e_{\alpha_j})$, $Y(e_1, \ldots, e_k)$, but also $e_i < e_j$ and $X(e)$. The final step consist of replacing every term $e_i < e_j$ and $X(e)$ by their boolean value *true* or *false* depending on whether this is true or false in the structure $str(x)$. There is no exponential blow-up because the constructed formula is of polynomial length in the size of the structure $str(x)$, which is part of the input of the reduced problem.

We have now a one-to-one correspondence between the satisfiability of Φ in the structure $str(x, y)$ and the formula $\varphi(y)$ being an instance of the counting problem $\#\cdot\Sigma_i$SAT: $str(x, y) \models \Phi(X, Y, <)$ if and only if $\varphi(y)$ is satisfiable.

Moreover, the cardinality of the set $\{Y^{\mathcal{U}} \mid \langle \mathcal{U}, X^U, Y^{\mathcal{U}}, < \rangle \models \Phi(X, Y, <)\}$ is equal to the number of distinct assignments of y that satisfy $\varphi(y)$. This concludes the completeness proof for the counting problem $\#\cdot\Sigma_i$SAT. The proof is similar for the counting problem $\#\cdot\Pi_i$SAT. $\square$

Proof of Theorem 3.2

For proving that the subtractive reductions compose, we will need the following properties of multisets.

Lemma 5.2 *Let A_i, B_i, for $i = 1, \ldots, n$, A, B, C, and D be multisets.*

1. *If $B_i \subseteq A_i$ for each i, then*

$$\bigoplus_{i=1}^{n}(A_i \ominus B_i) \quad = \quad (\bigoplus_{i=1}^{n} A_i) \ominus (\bigoplus_{i=1}^{n} B_i).$$

2. *If $B \subseteq A$, $D \subseteq C$, and $C \ominus D \subseteq A \ominus B$ then*

$$(A \ominus B) \ominus (C \ominus D) \quad = \quad (A \oplus D) \ominus (B \oplus C).$$

Proof: Let x be an arbitrary element of the domain. Since $B_i \subseteq A_i$ holds for each i, we have that

$$m_x(A_i \ominus B_i) \quad = \quad m_x(A_i) - m_x(B_i).$$

Hence,

$$\begin{aligned} m_x(\bigoplus_{i=1}^{n}(A_i \ominus B_i)) &= \sum_{i=1}^{n}(m_x(A_i) - m_x(B_i)) \\ &= \sum_{i=1}^{n} m_x(A_i) - \sum_{i=1}^{n} m_x(B_i) \\ &= m_x(\bigoplus_{i=1}^{n} A_i) - m_x(\bigoplus_{i=1}^{n} B_i). \end{aligned}$$

The inclusion $B_i \subseteq A_i$ for each i implies

$$\bigoplus_{i=1}^{n} B_i \quad \subseteq \quad \bigoplus_{i=1}^{n} A_i.$$

Hence,

$$m_x(\bigoplus_{i=1}^{n} A_i) - m_x(\bigoplus_{i=1}^{n} B_i) \quad = \quad m_x(\bigoplus_{i=1}^{n} A_i \ominus \bigoplus_{i=1}^{n} B_i).$$

For the second case,

$$\begin{aligned} & m_x((A \ominus B) \ominus (C \ominus D)) = \\ &= m_x(A \ominus B) - m_x(C \ominus D) \\ &= (m_x(A) - m_x(B)) - (m_x(C) - m_x(D)) \\ &= (m_x(A) + m_x(D)) - (m_x(B) + m_x(C)) \\ &= m_x(A \oplus D) - m_x(B \oplus C) \\ &= m_x((A \oplus D) \ominus (B \oplus C)). \end{aligned}$$

$\square$

We are able now to prove Theorem 3.2 showing that a composition of two subtractive reductions produces another subtractive reduction.

Theorem 3.2. Reducibility via subtractive reductions is a transitive relation, that is, if $\#{\cdot}A \leq_s \#{\cdot}B$ and $\#{\cdot}B \leq_s \#{\cdot}C$, then $\#{\cdot}A \leq_s \#{\cdot}C$.

Proof: Suppose that $\#{\cdot}A$ reduces to $\#{\cdot}B$ via subtractive reduction with the functions f_i^1 and g_i^1. Suppose also that $\#{\cdot}B$ reduces to $\#{\cdot}C$ via subtractive reduction with the functions f_i^2 and g_i^2. We prove that there exists a subtractive reduction from $\#{\cdot}A$ to $\#{\cdot}C$ with the functions f_k and g_k.

Let

$$M \quad = \quad \bigoplus_i B(g_i^1(x)) \ominus \bigoplus_i B(f_i^1(x))$$

i.e., $|M| = |A(x)|$. Since there is a subtractive reduction from $\#{\cdot}B$ to $\#{\cdot}C$, the set M is isomorphic to

$$\begin{aligned} &\bigoplus_i (\bigoplus_j C(g_j^2(g_i^1(x))) \ominus \bigoplus_j C(f_j^2(g_i^1(x)))) \\ &\ominus \quad \bigoplus_i (\bigoplus_j C(g_j^2(f_i^1(x))) \ominus \bigoplus_j C(f_j^2(f_i^1(x)))). \end{aligned}$$

Since the inclusions are satisfied, following property 1 of Lemma 5.2, the previous set is equal to

$$\begin{aligned} &(\bigoplus_i \bigoplus_j C(g_j^1(g_i^1(x))) \ominus \bigoplus_i \bigoplus_j C(f_j^2(g_i^1(x)))) \\ &\ominus \quad (\bigoplus_i \bigoplus_j C(g_j^2(f_i^1(x))) \ominus \bigoplus_i \bigoplus_j C(f_j^2(f_i^1(x)))). \end{aligned}$$

Following property 2 of Lemma 5.2, the latter set is equal to

$$\begin{aligned} &\bigoplus_i \bigoplus_j (C(g_j^2(g_i^1(x))) \oplus C(f_j^2(f_i^1(x)))) \\ &\ominus \quad \bigoplus_i \bigoplus_j (C(f_j^2(g_i^1(x))) \oplus C(g_j^2(f_i^1(x)))). \end{aligned}$$

Hence, we choose the functions $g_j^2(g_i^1(x))$ and $f_j^2(f_i^1(x))$ for $g_k(x)$, whereas the functions $f_j^2(g_i^1(x))$ and $g_j^2(f_i^1(x))$ become the functions $f_k(x)$. Therefore, we derive the equality

$$|A(x)| \quad = \quad \sum_k |C(g_k(x))| - \sum_k |C(f_k(x))|$$

$\square$

Proof of Theorem 4.3

As stepping stones towards proving Theorem 4.3, we will introduce and use two other technical counting problems.

#SATISFIABLE CIRC
Input: A satisfiable Boolean formula $\varphi(x_1, \ldots, x_n)$ in conjunctive normal form.
Output: Number of minimal models of $\varphi(x_1, \ldots, x_n)$.

Proposition 5.3 #SATISFIABLE CIRC *is* $\#\cdot$coNP*-complete via subtractive reductions.*

Proof: Deciding membership in the witness sets for this problem is in P^{NP}, because deciding satisfiability of a Boolean formula φ is in NP and deciding minimality of a model of φ is in coNP. Hence, #SATISFIABLE CIRC belongs to $\#\cdot\mathrm{P}^{\mathrm{NP}} = \#\cdot\mathrm{coNP}$.

For the lower bound, it is not hard to verify that a subtractive reduction of #CIRCUMSCRIPTION to #SATISFIABLE CIRC can be obtained as follows: given a Boolean formula $\varphi(x_1, \ldots, x_n)$ in conjunctive normal form the new formula

$$\psi(x_0, x_0', x_1, \ldots, x_n) \quad = \quad ((x_0 \wedge x_1 \wedge \cdots \wedge x_n) \vee (\neg x_0 \wedge \phi(x_1, \ldots, x_n))) \wedge (x_0 \not\equiv x_0').$$

The formula ψ has at least one model, namely $m_0 = (x_0 = 1, x_0' = 0, x_1 = \cdots = x_n = 1)$.

We show that m_0 is minimal for ψ. Suppose that there exists a smaller model m_0'. Then $m_0'(x_0) = 0$ or $m_0'(x_i) = 0$ for some i. If $m_0'(x_0) = 0$ then $m_0'(x_0') = 1$, hence the models m_0 and m_0' are incomparable. If $m_0'(x_i) = 0$ for some i, then $x_0 \wedge x_1 \wedge \cdots \wedge x_n = 0$. Hence, $\neg x_0 \wedge \phi(x_1, \ldots, x_n) = 1$ From this follows that $\neg x_0 = 1$, i.e., $m_0'(x_0) = 0$. This once more leads to $m_0'(x_0') = 1$ and the two models are incomparable. There is a contradiction in both cases, therefore m_0 is minimal.

Now, we show that $(x_1, \ldots, x_n)$ is a minimal model of ϕ if and only if $m_1 = (x_0 = 0, x_0' = 1, x_1, \ldots, x_n)$ is a minimal model of ψ. Construct the new formula $\psi' = \psi \wedge x_0 \wedge x_1 \wedge \cdots \wedge x_n \wedge (x_0 \not\equiv x_0')$. The formula ψ' has exactly one model, namely m_0. This model is therefore also minimal for ψ'.

Let $A(\phi)$ be the set of minimal solutions of ϕ and $B(\rho)$ be the set of minimal solutions of a satisfiable formula ρ. The inclusion $B(\psi') \subseteq B(\psi)$ holds, since ψ' has only one model m_0 which is also minimal for ψ. It is clear that every model of ϕ also satisfies ψ. Moreover, the only model of ψ that does not satisfy ϕ is the unique model of ψ', $m_0 = (x_0 = 1, x_0' = 0, x_1 = \cdots = x_n = 1)$. This implies that the equality $|A(\phi)| = |B(\psi)| - |B(\psi')|$ holds. The formulas ψ and ψ' can be written in conjunctive normal form without exponential explosion. Hence, we have a subtractive reduction. $\square$

#SATISFIABLE MIN SOL
Input: A system $S\colon Ax \leq b$ of linear Diophantine inequalities having at least one non-negative integer solution.
Output: Number of minimal solutions of S.

Proposition 5.4 #SATISFIABLE MIN SOL *is* $\#\cdot$coNP*-complete via subtractive reductions.*

Proof: Deciding membership in the witness sets for this problem is in P^{NP} and, hence, the problem is in $\#\cdot\mathrm{P}^{\mathrm{NP}} = \#\cdot\mathrm{coNP}$. Indeed, testing the system for solvability is in NP, whereas testing a given solution for minimality is in coNP. In both tests, we use the fact that the size of minimal solutions is bounded by a polynomial in the size of the system (see Corollary 17.1b in [Sch86, page 239]).

For the lower bound, observe that the standard reduction of Boolean satisfiability to integer linear programming also constitutes a parsimonious reduction of #SATISFIABLE CIRC to #SATISFIABLE MIN SOL. □

We are able now to prove Theorem 4.3.

Theorem 4.3. #HOMOGENEOUS MIN SOL is #·coNP-complete via subtractive reductions.

Proof: The problem is in #·coNP, because deciding membership in the witness sets is in coNP, using the bounds in the size of minimal solutions (see the proof of Proposition 5.4).

For the lower bound, we exhibit a subtractive reduction from #SATISFIABLE MIN SOL. Let $S\colon Ax \leq b$ be a system of linear Diophantine inequalities with at least one non-negative integer solution and such that A is $k \times n$ integer matrix. First construct the system

$$S'\colon \quad Ax - b\bar{y} \leq 0, \quad 2z - t = y, \quad x_i \leq y, \quad x_i \geq y - t,$$

where $\bar{y} = (y, \ldots, y)$ is a vector of length k having the same variable y in each coordinate, and z and t are additional new variables.

Claim 1: The vector $s_0 = (x_1 = x_2 = \cdots = x_n = y = 0, z = 1, t = 2)$ is a minimal solution of S'. This is obviously a solution. The only smaller solution is the trivial all-zero solution.

Claim 2: The nontrivial minimal solutions of S', except s_0, are of the form $(x_1, \ldots, x_n, y = 2k, z = k, t = 0)$ or $(x_1, \ldots, x_n, y = 2k + 1, z = k + 1, t = 1)$. Suppose s is a solution different from s_0 and $y = 2k \geq 2$. In this case, the second equation has for admissible values of z and t the pairs $(k + i, 2i)$ for every i. Once $i \geq 1$ holds, s is greater than s_0. Therefore only the pair $(k, 0)$ is convenient. If $y = 2k + 1$ and $k \geq 0$, z and t have for admissible values the pairs $(k + i, 2i - 1)$ with $i \geq 1$. Once $i \geq 2$ holds, s becomes greater than s_0. Therefore only the pair $(k + 1, 1)$ is convenient.

Claim 3: There exists a minimal solution of S' with $y \geq 3$ and y odd if and only if there are no solutions for $y = 1$ and $y = 2$. If there exists a solution with $y = 1$ or $y = 2$, then there exists also a minimal solution with the same value of y. Suppose that there exists a minimal solution with $y \geq 3$ and $y = 2k + 1$, then $t = 1$. From this follows $x_i \geq 2k$ for each i. We have that $k \geq 1$ since $y \geq 3$, therefore $x_i \geq 2$ holds for each i. From $2z - t = y$, $t = 1$, and $y \geq 3$ follows $z \geq 2$. Let $s_3 = (x_1 \geq 2, \ldots, x_n \geq 2, y \geq 3, z \geq 2, t = 1)$ be a minimal solution of S'. If there is a minimal solution with $y = 1$, it is of the form $s_1 = (x_1 \leq 1, \ldots, x_n \leq 1, y = 1, z = 1, t = 1)$ and s_1 is smaller than s_3. Contradiction. If there is a minimal solution with $y = 2$, it is $s_2 = (x_1 \leq 2, \ldots, x_n \leq 2, y = 2, z = 1, t = 0)$ and s_2 is smaller than s_3. Contradiction.

Claim 4: If there exists a minimal solution with y even, then this solution is $(x_1 = \cdots = x_n = 2 = y, z = 1, t = 0)$. For $y = 2k$ and $t = 0$ we must have $x_1 = \cdots = y = 2k$ and $z = k$ for some $k \geq 1$. Since S' is a homogeneous system, we can divide the solution by k.

Now, we use the knowledge that The known minimal model in #SATISFIABLE CIRC and also the known minimal solution of $Ax \leq b$ for #SATISFIABLE MIN SOL has a value $x_i = 0$ for some i. Hence, this solution falsifies the system of equations $x_1 = \cdots = x_n$.

After this, construct the system $S'' = S' \cup \{x_1 = \cdots = x_n = y\}$. Clearly, the system S'' has the minimal solution $s_0 = (x_1 = \cdots = x_n = 0, y = 0, z = 1, t = 2)$ and also $s_2 = (x_1 = \cdots x_n = 2, y =$

$2, z = 1, t = 0)$ if s_2 is a solution of S'. Therefore the minimal solutions of S'' are included in the minimal solutions of S'.

We know that S' has at least one minimal solution s for $y = 1$, since $S\colon Ax \leq b$ has one solution. Moreover, s is *not* a minimal solution of S''.

Let $A(S)$ be the set of minimal solutions of the system S, and let $B(S')$ and $B(S'')$ be the sets of nontrivial minimal solutions of S' and S'', respectively. From the previous reasoning follows that $B(S'') \subseteq B(S')$ and that $|A(S)| = |B(S')| - |B(S'')|$. This establishes that the polynomial-time computable functions $f(S) = S'$ and $g(S) = S''$ constitute a subtractive reduction of #SATISFIABLE MIN SOL to #HOMOGENEOUS MIN SOL. $\square$