What is in #P and what is not?

1st Christian Ikenmeyer
Department of Computer Science
University of Liverpool
Liverpool, United Kingdom
christian.ikenmeyer@liverpool.ac.uk

2nd Igor Pak
Department of Mathematics
University of California, Los Angeles
Los Angeles, USA
pak@math.ucla.edu

***Abstract*—For several classical nonnegative integer functions we investigate if they are members of the counting complexity class #P or not. We prove #P membership in surprising cases, and in other cases we prove non-membership, relying on standard complexity assumptions or on oracle separations.**

We initiate the study of the polynomial closure properties of #P on affine varieties, i.e., if all problem instances satisfy algebraic constraints. This is directly linked to classical combinatorial proofs of algebraic identities and inequalities. We investigate #TFNP and obtain oracle separations that prove the strict inclusion of #P in all standard syntactic subclasses of #TFNP minus 1.

***Index Terms*—Counting complexity, combinatorial proofs, TFNP, #P, GapP**

I. Introduction

This is an extended abstract. All technical details can be found in the full version on the arXiv under the label 2204.13149v1.

A. Foreword

Finding a *combinatorial interpretation* is an everlasting problem in Combinatorics. Having combinatorial objects assigned to numbers brings them depth and structure, makes them alive, sheds light on them, and allows them to be studied in a way that would not be possible otherwise. Once combinatorial objects are found, they can be related to other objects via bijections, while the numbers' positivity and asymptotics can then be analyzed.

Historically, this approach was pioneered by J.J. Sylvester in his "*constructive theory of partitions*" [Syl82]. There, Sylvester was able to rederive a host of old partition identities and prove many new ones by interpreting the coefficients on both sides as the numbers of certain *Ferrers shapes* (now called *Young diagrams*), and relating two sides to each other. G.H. Hardy marveled at such proofs, calling them "striking" and "unlike any other" [Har40], see also [Pak06].

Since the 1960s, this approach became a staple in *Enumerative Combinatorics*, reaching as far as undergraduate textbooks [SW86], monographs [Loe11] and multimedia compendia [Vie16]. In *Algebraic Combinatorics*, even one combinatorial interpretation can introduce revolutionary changes. Notably, a Young tableau interpretation of the *Littlewood–Richardson* (LR-) *coefficients* $c_{\mu\nu}^{\lambda}$ was discovered in [LR34]. These numbers describe the structure constants of the *Schur functions* multiplication [Mac95], [Sta12]. Over the last few decades, this result led to an avalanche of developments, culminating with a complete resolution of the *Horn problem* [Kly98] (see also [Ful98]), proof of the *saturation conjecture* [KT99], and polynomial time algorithms for the vanishing of the LR–coefficients [BI13b], [MNS12], [Ike16].

When a combinatorial interpretation exists it is a modern wonder, a starting point of a combinatorial investigation. *But what if none is known?* Such examples in Enumerative Combinatorics are too numerous to be listed, see e.g. [Pak18, §4]. In Algebraic Combinatorics, the following are the top three "most wanted" combinatorial interpretations, all from *Stanley's list* [Sta00]:

- *Kronecker coefficients* $g(\lambda, \mu, \nu)$ which generalize LR–coefficients and give structure constants of tensor products of $\mathfrak{S}_n$-modules. This celebrated problem goes back to Murnaghan [Mur38] and plays a crucial role in *Geometric Complexity Theory* (GCT), see [Mul09]. See [BDO15], [IMW17], [PP17], [PPY19] for some recent combinatorial and complexity work on the subject.
- *plethysm coefficients* $p_\lambda(\mu, \nu)$ which describe decompositions of Schur functors of $\mathfrak{S}_n$-modules, and is the main subject of GCT7 [Mul07], see also [BIP19], [FI20], [IP17]. They also appear in connection to the *Foulkes conjecture* in Representation Theory, see [Bri93], [CIM17], [Lan15].
- *Schubert coefficients* $c(u, v, w)$ which give structure constants of the product of Schubert polynomials, defined by Lascoux and Schützenberger [LS82] in the context of *cohomology of the Grassmannian*, see [Mac91], [Man01]. We refer to [Knu16], [KZ20], [MPP14] for examples of positive results.

In all three cases, there is a widespread belief that these coefficients must have a combinatorial interpretation. A positive resolution of either problem would be a major breakthrough culminating decades long study. In the context of GCT, Mulmuley conjectured [Mul09] that both Kronecker and plethysm coefficients are in #P (see [Val79]), as a step towards proving that $\mathsf{P} \neq \mathsf{NP}$. Note that all three functions are in $\mathsf{GapP}_{\geq 0}$, suggesting commonality of the obstacles.

Now, *what if the community is wrong*, and these functions are not in #P? Such a possibility has only been raised recently [Pak19], [Spe11]. Until now there has been little effort towards

The first author was partially supported by the DFG grant IK 116/2-1 and the EPSRC grant EP/W014882/1. The second author was partially supported by the NSF grant CCF-2007891.

proving that some natural combinatorial functions are not in #P (see below). With this paper we initiate a systematic study of this problem.

We show that many natural combinatorial functions are not in #P under various complexity assumptions. In a positive direction, we prove that many functions *are* in #P, some strikingly close to those that are not.

B. Motivational examples of #P functions

Let $\mathsf{GapP}_{\geq 0}$ be the class of nonnegative functions in $\mathsf{GapP} := \{f_1 - f_2 \mid f_1, f_2 \in \#\mathsf{P}\}$.[1] More generally, we consider the class $\mathsf{PolynP} := \big\{\varphi(f_1, \ldots, f_k) \mid \varphi \in \mathbb{Q}[x_1, \ldots, x_k], f_i \in \#\mathsf{P}\big\}$, and study the class $\mathsf{PolynP}_{\geq 0}$ of nonnegative functions in PolynP. The place to start is to look for natural integer functions in these classes and ask if they lie in #P. For the three functions as above the problem remains open, but what is known in other cases? Consider the following motivating examples:

(1) Let $e : P \to \mathbb{N}$ be the number of linear extensions of P, where $P = (X, \prec)$ is a poset with n elements. Recall that $e(P) \geq 1$, so $e'(P) := e(P) - 1 \in \mathsf{GapP}_{\geq 0}$. Now observe that $e' \in \#\mathsf{P}$ simply because finding the lex-smallest linear extension L can be done in polynomial time (see e.g. [CW95]), so $e'(P)$ counts linear extensions of P that are different from L. Note aside that since e is #P-complete [BW91], then so is e'.

(2) Recall *Sperner's lemma* which states that for every $\{1, 2, 3\}$-coloring χ of interior vertices in a side-length n-triangle region Δ_n of the plane whose sides are colored 1, 2 and 3, respectively, there is a *rainbow* (123) triangle. We trust the reader is familiar with the setting, see e.g. [Pap94a] and [MM11, §6.7]. Here n is given in binary and χ is given by a polynomial size circuit. Denote by $t(\chi)$ the number of rainbow triangles, so that $t(\chi) - 1 \in \mathsf{GapP}_{\geq 0}$.

Since the typical proof of Sperner's lemma involves tracing down the path of non-rainbow triangles until a rainbow triangle is reached, it may come as a surprise that $t(\chi) - 1 \in \#\mathsf{P}$. Indeed, simply observe that $t(\chi) - 1 = 2t_-(\chi)$, where $t_\pm(\chi)$ denotes the number of rainbow triangles with positive/negative orientation. This follows from $t(\chi) = t_+(\chi) + t_-(\chi)$ and $t_+(\chi) - t_-(\chi) = 1$ equations, see e.g. [Pak03, §8].

(3) Let G be a simple graph with at least one edge, and let $f(G)$ be the number of proper 3-colorings of G. Then $f(G)/6$ is an integer valued function in $\mathsf{PolynP}_{\geq 0}$ by taking into account permutations of colors. Of the six possible 3-colorings corresponding to a given 3-coloring one can easily choose the lex-smallest, implying that $f(G)/6 \in \#\mathsf{P}$.[2] Such solution is not always possible in other problems, see §I-C(4), and algorithmic approaches to equivalence problems have been studied in [BG83], [BG84], [FG11].

(4) Let $\delta(k, G) := m_k(G)^2 - m_{k-1}(G)m_{k+1}(G)$, where $m_k(G)$ is the number of k-matchings in graph G. The function $\delta \in \mathsf{GapP}$ by definition. By the celebrated result of Heilmann and Lieb [HL72], the sequence $m_1(G), m_2(G), \ldots$ is *log-concave*, implying that $\delta \in \mathsf{GapP}_{\geq 0}$. This result is a starting point of many combinatorial investigations [God93], including notably the "interlacing families" series [MSS13]. While all signs point to δ being "difficult to handle", it was observed in [Pak19] that a beautiful proof in [Kra96] easily implies that $\delta \in \#\mathsf{P}$.

(5) Recall *Fermat's little theorem*: For every prime p and $a \in \mathbb{N}$, we have: $a^p \equiv a \pmod p$. This is one of the most basic and most celebrated results in Number Theory, see e.g. [IR82, §3.4], and is the starting point of the *Miller–Rabin primality test*, see e.g. [MM11, §10.8.2]. The theorem can be rephrased as: for all $a \in \mathbb{N}$, we have $\varphi(a) := \frac{1}{p}(a^p - a) \in \mathbb{N}$. It is readily converted into a PolynP function by substituting $a \leftarrow N(\phi)$ as follows: $\frac{1}{p}\big(N(\phi)^p - N(\phi)\big) \in \varphi(\#\mathsf{P}) \subseteq \mathsf{PolynP}$, where $N(\phi)$ is the number of satisfying assignments of a Boolean formula ϕ. It was shown by Peterson [Pet72] (see also [Gol56]) that this function is actually in #P by giving a combinatorial interpretation for $\varphi(a)$, and in this way reproving Fermat's little theorem. In other words, we have $\varphi(\#\mathsf{P}) \subseteq \#\mathsf{P}$, i.e., the class #P is closed under the *Frobenius map* φ. At the heart of the proof is a polynomial-time algorithm for identifying lex-smallest elements as in §I-B(3), but here in a $\mathbb{Z}/p\mathbb{Z}$ orbit.

(6) Consider the following inequality by Grimmett [Gri76]: $\tau(G) \leq \frac{1}{n}\left(\frac{2m}{n-1}\right)^{n-1}$ for the *number of spanning trees* $\tau(G)$ in a simple graph $G = (V, E)$ with $|V| = n$ vertices and $|E| = m$ edges. One can turn this into a $\mathsf{GapP}_{\geq 0}$ function as follows: $f(G) := (2m)^{n-1} - n(n-1)^{n-1}\tau(G)$. On the other hand, *given that the inequality holds*, the claim $f \in \#\mathsf{P}$ is trivial since $\tau \in \mathsf{FP}$. Indeed, since $f(G)$ can be computed in polynomial time by the matrix-tree theorem, we conclude that $f(G)$ counts the set of n-bit binary strings from 0 to $f(G) - 1$.[3] [4] This is why it is important in the examples above that our functions are not obviously in FP (e.g., being #P-hard is a good indication), since otherwise the problem becomes trivial.

C. Motivational non-examples

It may come as a surprise that the non-example comes from the simplest of the inequalities.

(1) *Cauchy–Schwarz inequality*[5]:

$$a^2 + b^2 \;\geq\; 2ab \quad \text{where} \quad a, b \in \mathbb{R}. \tag{I-C.1}$$

[1] The closure $\mathsf{GapP} = \#\mathsf{P} - \#\mathsf{P}$ of #P under subtraction was introduced in [FFK94] and indep. in [Gup95].

[2] It is important to emphasize that while $f(G)$ is #P-complete, it is completely irrelevant to the conclusion. Crucially, the *lex-smallest test* is in P in both this and the previous example. In non–#P examples of this kind, the lex-smallest test is NP-hard (see below).

[3] Combinatorialists would argue that a combinatorial interpretation should explain *why* the inequality holds in the first place. In fact, there are several schools of thought on this issue (see a discussion in [Pak18, §4]). We believe that the computational complexity approach is both the least restrictive and the most formal way to address this.

[4] In the context of GCT, motivated by the work on LR–coefficients, Mulmuley asks if Kronecker and plethysm coefficients count the number of integer points in a polytope defined by the inequalities with polynomial description [Mul09]. We do not work with this narrower notion in this paper. See, however, [KM18].

[5] actually a quick corollary thereof. (I-C.1) follows from $\langle (1,1), (a,b)\rangle^2 \leq \langle (1,1), (1,1)\rangle \cdot \langle (a,b), (a,b)\rangle$.

Now take a, b to be counting functions. Formally, for two Boolean formulas ϕ and ψ, let

$$h(\phi,\psi) \,:=\, N(\phi)^2+N(\psi)^2-2N(\phi)N(\psi) \,=\, \big(N(\phi)-N(\psi)\big)^2. \tag{I-C.2}$$

By definition, the function $h \in \mathsf{GapP}_{\geq 0}$. Note, however, that if $h \in \#\mathsf{P}$, then we get a polytime witness for $N(\phi) \neq N(\psi)$. This is unlikely, as it would imply the collapse of polynomial hierarchy to the second level: $\mathsf{PH} = \Sigma_2^{\mathsf{p}}$ (see Proposition II-C.1). Colloquially, this says that under the natural complexity assumption $\mathsf{PH} \neq \Sigma_2^{\mathsf{p}}$, the Cauchy–Schwarz inequality (I-C.1) does not have a combinatorial interpretation in full generality.

(2) The *Hadamard inequality* for real $d \times d$ matrices states:

$$\det \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & \ddots & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix}^2 \;\leq\; \textstyle\prod_{i=1}^d \big(a_{i1}^2 + \ldots + a_{id}^2\big). \tag{I-C.3}$$

Geometrically, it says that the volume of a parallelepiped in $\mathbb{R}^d$ is at most the product of its basis edge lengths, with equality when these edges are orthogonal. Note that standard proofs of (I-C.3) involve the eigenvalues of $A = (a_{ij})$, see e.g. [HLP52, §2.13] and [BB61, §2.11], suggesting that translation into combinatorial language would be difficult.

Substitute all $a_{ij} \leftarrow N(\phi_{ij})$ in (I-C.3), where ϕ_{ij} are Boolean formulas. Denote by H_d the resulting counting function written in the style of (I-C.2), i.e, H_d is the difference of the right-hand side and the left-hand side of (I-C.3). It is easy to see that $H_2 \in \#\mathsf{P}$, see §II-A. For $d \geq 3$, we prove that $H_d \notin \#\mathsf{P}$ under an assumption that we call the *univariate binomial basis conjecture*. This is a general conjecture about the structure of $\#\mathsf{P}$. Formally, we show the existence of an oracle $A \subseteq \{0,1\}^*$ with $H_3(\overrightarrow{\#\mathsf{P}^A}) \not\subseteq \#\mathsf{P}^A$.

(3) For a simple graph G on n vertices, denote by $\boldsymbol{d}(G) = (d_1, \ldots, d_n)$ the degree sequence. Consider the following natural inequality:

$$\mathbb{P}[G \text{ is planar}] \,\leq\, \mathbb{P}[G \text{ is planar} \,|\, \boldsymbol{d}(G) \leqslant \boldsymbol{c}], \tag{I-C.4}$$

where $\boldsymbol{c} = (c_1, \ldots, c_n)$ is a given sequence, the inequality $\boldsymbol{d}(G) \leqslant \boldsymbol{c}$ is coordinate-wise: $d_i \leq c_i$ for all $1 \leq i \leq n$, and where the probability is over uniform random graphs on $[n] = \{1, \ldots, n\}$. This says that being planar correlates with having small degrees.[6]

We can convert (I-C.4) it into a $\mathsf{GapP}_{\geq 0}$ function as follows: $\varrho(\boldsymbol{c}) := 2^{\binom{n}{2}} \#\big\{\text{planar graphs } G \text{ on } [n] \text{ with } \boldsymbol{d}(G) \leqslant \boldsymbol{c}\big\} - \#\big\{\text{plan. graphs on } [n]\big\} \cdot \#\big\{\text{graphs } G \text{ on } [n] \text{ with } \boldsymbol{d}(G) \leqslant \boldsymbol{c}\big\}$. This inequality is a simple special case of the *Kleitman inequality* [Kle66], which is a corollary of the *Ahlswede–Daykin inequality* [AD78] (see full version). In Proposition II-E.1, we show that the polynomial inequality implied by the Ahlswede–Daykin inequality is not in $\#\mathsf{P}$, again under the univariate binomial basis conjecture.

(4) Recall the following *Smith's theorem* [Tut46]. Let $e = (v, w)$ be an edge in a cubic graph G. Then the number $N_e(G)$ of Hamiltonian cycles in G containing e is always even. Denote $f(G, e) := N_e(G)/2$ and observe that $f \in \mathsf{PolynP}_{\geq 0}$. Is $f \in \#\mathsf{P}$? We don't know. This seems unlikely and remains out of reach with existing technology. But let us discuss the context behind this problem.

Tutte's original proof in [Tut46] uses a double counting argument. The *Price–Thomason algorithm* for finding another Hamiltonian cycle in a cubic graph [Pri77], [Tho78] gives a more direct combinatorial proof of Smith's theorem and implies that this search problem is in PPA, the class defined by the polynomial parity argument. In fact, AnotherHamiltonianCycle is a motivational problem for PPA, while Sperner, see §I-B(2), is a motivational problem for PPAD [Pap94a][7].

Note that the Price–Thomason algorithm partitions the set of all Hamiltonian cycles into pairs, but this pairing algorithm is known to require an exponential number of steps in the worst case, see [Cam01], [Kra99]. A polynomial-time algorithm instead would allow us to search for Hamiltonian cycles and only count the ones that are lexicographically smaller than their pairing partner, which would show that $N_e(G)/2 \in \#\mathsf{P}$, and $(\text{AllOtherHamiltonianCyclesThroughEdge} - 1)/2 \in \#\mathsf{P}$. Note that such a pairing algorithm (not for the symmetric group $\mathfrak{S}_2$, but for $\mathfrak{S}_3$) is the reason why $f(G)/6 \in \#\mathsf{P}$ in §I-B(3).

We study the basic search problem Leaf[8] that is used to define PPA, and that arises directly from Sperner by a parsimonious reduction from the PPAD-complete problem SourceOrSink and removing the edge directions. We show that for the corresponding counting problem we have an oracle separation that shows $\text{AllLeaves}^A/2 \notin \#\mathsf{P}^A$. In fact, for the counting version of Leaf, where we are given one leaf and count all others, we show that $\text{Leaf}^A - 1 \notin \#\mathsf{P}^A$. This has to be contrasted to Sperner, where the membership $\text{Sperner} - 1 \in \#\mathsf{P}$ relativizes, i.e., holds with respect to all oracles. The oracle instances are significantly more complicated than for the Hadamard problem, see §I-C(2).

(5) We have seen that $\text{Sperner}(\chi) - 1 = 2t_-(\chi)$, hence $(\text{Sperner} - 1)/2 \in \#\mathsf{P}$. It is easy to see that the reverse inclusion holds: The counting class

[6] Note aside that the number of labeled planar graphs on n vertices can be computed in time polynomial in n using Tutte's generating function formulas [Tut63], see also [Noy14], [Sch15]. On the other hand, the number of labeled graphs with a given upper bound on the degrees is likely not in FP, cf. [Wor18].

[7] Several versions of Sperner on non-orientable manifolds are PPA-complete [Gri01], [DEF+21], as well as e.g. the problems Consensus-Halving/Necklace Splitting [FRG18], [FRH+20], [DFHM22], and integer factoring (assuming the GRH) [Jeř16]. Main PPAD-complete problems include *Nash equilibrium* [DGP09], [CD09] and *hairy ball* [GH21].

[8] Search problems are often of the type AnotherSolution, but the name does not suggest that. Leaf for example could reasonably be called AnotherLeaf. We adapt the search problem notation and drop the Another prefix and mean the corresponding problem of *counting* all but the given leaf. The problem of counting *all* leaves when we are *not* given one is called AllLeaves. Since all our problems are counting problems, we drop the customary # in front of the problem name, also to avoid having two # in the class names, see §III-D.

$\#\mathsf{PPAD}(\textsc{Sperner})$ defined by the SPERNER problem contains $2\#\mathsf{P}+1$, or, in other words, $\#\mathsf{P} = (\#\mathsf{PPAD}(\textsc{Sperner})-1)/2$. For the other classes in TFNP we similarly get $\#\mathsf{P} = \big(\#\mathsf{PPAD}(\textsc{Sperner}) - 1\big)/2 = \#\mathsf{PPADS}(\textsc{Sink}) - 1 = \#\mathsf{CLS}(\textsc{EitherSolution}(\textsc{Sperner},\textsc{Iter})) - 1$ and these equalities relativize. But for the more complex classes we get oracle separations: $(\#\mathsf{PPA}(\textsc{Leaf}) - 1)/2$, $\#\mathsf{PPP}(\textsc{Pigeon}) - 1$ and $\#\mathsf{PLS}(\textsc{Iter}) - 1$ strictly contain $\#\mathsf{P}$ with respect to an oracle.

But this does not give the complete picture, since non-parsimonious reductions between complete problems give different counting classes. For example if instead of leaves in a graph we count the nodes that are adjacent to leaves (which we call preleaves), then this does not change the complexity of the search problem, but it changes the counting class from $\#\mathsf{PPA}(\textsc{Leaf})$ to the class $\#\mathsf{PPA}(\textsc{Preleaf})$ (note that the functions in $\#\mathsf{PPA}(\textsc{Leaf})$ always attain odd values, while the functions in $\#\mathsf{PPA}(\textsc{Preleaf})$ do not have this restriction). The underlying argument is the *chessplayer algorithm*, see e.g. [Pap90], [BCE+98], which results in non-parsimonious reductions, which then give rise to a complexity class inclusion diagram where we have an oracle with respect to which we have a strict inclusion of $\#\mathsf{P}$ in *all* the classes $\#\mathsf{PPAD} - 1$, $\#\mathsf{PPADS}-1$, $\#\mathsf{CLS}-1$, $\#\mathsf{PPA}-1$, $\#\mathsf{PPP}-1$ and $\#\mathsf{PLS}-1$. The full class inclusion diagram of our results can be found in Figure 1. The definitions of the classes and problems can be found in the full version.

These problems are syntactically guaranteed to be nonnegative, but in contrast to the HADAMARD problem (for example), here the oracle separations are much more delicate, as we have to fool the Turing machine while producing instances of the correct cardinality (which is easier if the problem is a polynomial evaluated at arbitrary $\#\mathsf{P}$ functions). To overpass these obstacles, we introduce the notion of a set-instantiator in the full version. We will also treat cases where we have a nonnegativity guarantee, but no further information about the reason. This requires extra care, see Propositions II-C.3 and see Proposition 7.5.5 in the full version.

II. DEFINITIONS, NOTATIONS AND FIRST STEPS

We start in §II-B with the concept of polynomial closure properties of $\#\mathsf{P}$. We then prove some simple separations in §II-C and §II-D, as a warmup before our main results in the next section.

A. Basic notation

Let $\mathbb{N} = \{0, 1, 2, \ldots\}$, $\mathbb{Q}_+ = \{x \in \mathbb{Q}, x \geq 0\}$. For $i \in \mathbb{N}$ and $x \in \mathbb{R}$, we write

$$\binom{x}{i} \;=\; \frac{1}{i!}\, x(x-1)\cdots(x-i+1).$$

In particular, $\binom{i}{0} = \binom{i}{i} = 1$. We think of $\binom{x}{i}$ as a rational polynomial of degree i. Note that for $0 \leq x < i$, $x \in \mathbb{N}$, we have $\binom{x}{i} = 0$. For a vector $(a_1, \ldots, a_n) \in \mathbb{R}^n$, we use both $\vec{a}$ and $\boldsymbol{a}$ to denote this vector.

We are assuming the reader is familiar with basic complexity theory and standard complexity classes: P, NP, UP, PH, FP, $\#\mathsf{P}$, GapP, PPA and PPAD. We refer to [AB09], [MM11], [Pap94b] for the definitions and standard results, and to [Aar16], [Wig19] for further background.

B. Closure properties

We say that a map $\varphi : \mathbb{N}^k \to \mathbb{Q}$ is *integer-valued* if it only attains integer values. Similarly, map φ is *nonnegative*, write $\varphi \geqslant 0$, if it only attains nonnegative values.

We say that φ is a *closure property* of $\#\mathsf{P}$, if for all $f_1, \ldots, f_k \in \#\mathsf{P}$ we have $\varphi(f_1, \ldots, f_k) \in \#\mathsf{P}$. More concisely, we also write: $\varphi\big(\overrightarrow{\#\mathsf{P}}\big) \subseteq \#\mathsf{P}$.

This is a generalization of the notation $\mathsf{GapP} = \#\mathsf{P} - \#\mathsf{P}$ from [FFK94].[9] Let $S \subseteq \mathbb{N}^k$ be a fixed subset. We say that φ is a *closure property* of $\#\mathsf{P}$ *restricted* to S (or *on* S), if for all $f_1, \ldots, f_k \in \#\mathsf{P}$ which satisfy $\big(f_1(w), \ldots, f_k(w)\big) \in S$ for all $w \in \{0,1\}^*$, we have $\varphi(f_1, \ldots, f_k) \in \#\mathsf{P}$.

Note that we evaluate these $\#\mathsf{P}$ functions on the same input. For example, in the notation of §I-B(2), the map $\varphi(t_-, t_+) := t(\chi) - 1 = t_+ + t_- - 1$ is restricted to $S = \{(t_-, t_+) \mid t_+ - t_- = 1\}$. Similarly, in the notation of §I-B(3), we have $S = 6\mathbb{N}$.

We write the restriction to S as a subscript, usually denoted $\overrightarrow{\#\mathsf{P}}_{\in S}$, but the property "$\in S$" is sometimes notationally replaced by other properties such as "≥ 1" (in which case $S = \mathbb{N}_{\geq 1}$) or "even" (in which case $S = 2\mathbb{N}$). For example, in notation of §I-B(1), we have $e(P) \in \#\mathsf{P}_{\geq 1}$. Similarly, in the notation of §I-C(4), we have $N_e(G) \in \#\mathsf{P}_{\text{even}}$. This allows us to write statements such as $\#\mathsf{P}_{\geq 1} + 1 \subseteq \#\mathsf{P}$, and $\#\mathsf{P}^A_{\text{even}}/2 \not\subseteq \#\mathsf{P}^A$ for the oracle A separation. More generally, in the multivariate case we write $\varphi\big(\overrightarrow{\#\mathsf{P}}_{\in S}\big) \subseteq \#\mathsf{P}$ for the closure property of $\#\mathsf{P}$ restricted to S. [HR00] study the univariate case and call such a restriction a counting property. These univariate restrictions also play a role in [CGH+89] and are the main focus of [GW87]. The most famous example is probably $\mathsf{UP} = \#\mathsf{P}_{\in\{0,1\}}$ (if one identifies languages with their characteristic functions, which we do), see [Val76], [GS88], [Ko85], [HT03]. In some contexts it is natural to consider a promise version of UP, see [VV85], but that is *different* from what we consider here. To make connections to TFNP more visible, we define $\#\mathsf{TFNP} := \#\mathsf{P}_{\geq 1}$.

Let $\varphi, \psi \in \mathbb{Q}[x_1, \ldots, x_k]$ be rational polynomials. We write $\varphi \geqslant_{\#} \psi$ if

$$\varphi(f_1, \ldots, f_k) - \psi(f_1, \ldots, f_k) \in \#\mathsf{P} \quad \text{for all} \quad f_1, \ldots, f_k \in \#\mathsf{P},$$

or, equivalently, $(\varphi - \psi)(\overrightarrow{\#\mathsf{P}}) \subseteq \#\mathsf{P}$. For example, $x^2 + 3x \geqslant_{\#} 0$. Less obviously, $x^2 \geqslant_{\#} x$, since $x^2 - x = 2\binom{x}{2}$ which counts unordered pairs (i, j), where $1 \leq i < j \leq x$. For the

[9] When defining $\overrightarrow{\#\mathsf{P}}$, two different definitions are equivalent (in the same way as for GapP). First, one can define $\overrightarrow{\#\mathsf{P}}$ via k many nondeterministic polynomial time Turing machines and consider the k-vector of their number of accepting paths as the output. Alternatively, one can define it via one nondeterministic polynomial time Turing machine that has k many different states of acceptance and one reject state (these states of acceptance are usually labeled with $+1$ and -1 in GapP). This is a complexity class of multi-output functions, as, for example, considered in [Val76].

Hadamard inequality (I-C.3), we easily have $H_2 \geqslant_{\#} 0$, since $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 = (ad-bc)^2 = a^2d^2 - 2abcd + b^2c^2 \leqslant_{\#} a^2c^2+a^2d^2+b^2c^2+b^2d^2 = (a^2+b^2)(c^2+d^2)$. We emphasize again that over the reals this is *not* a valid proof of the Hadamard inequality for 2×2 matrices since the $2abcd$ term can be negative. The inequality $H_2(a,b,c,d) \geq 0$ over the reals follows from the Cauchy–Schwarz inequality in this case.

C. Complete squares

As in the introduction, we have $\mathsf{GapP} = \#\mathsf{P} - \#\mathsf{P} = \{f_1 - f_2 \mid f_1, f_2 \in \#\mathsf{P}\}$. We use the notation $[\mathsf{C} = 0]$ to denote the class of languages $L \subseteq \{0,1\}^*$ for which there exists a function $f \in \mathsf{C}$ with: $w \in L$ if and only if $f(w) = 0$. For example, $[\#\mathsf{P} = 0] = \mathsf{coNP}$ and $[\mathsf{GapP} = 0] = \mathsf{C_{=}P}$. The following proposition about k-th powers of GapP functions is well known:

II-C.1 Proposition. *Let* $\mathsf{GapP}^k := \{f^k \mid f \in \mathsf{GapP}\}$*, where the exponent* k *denotes the exponentiation of integers. If* $\mathsf{GapP}^k \subseteq \#\mathsf{P}$ *for some even* k*, then* $\mathsf{PH} = \Sigma_2^{\mathsf{p}}$.

Proof. Recall that $\mathsf{PH} \subseteq \mathsf{NP}^{\mathsf{C_{=}P}}$, which can be found for example in [Tar91], [Gre93] and [Cur16], which follows from Toda's $\mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$ theorem (see [Toda91], [KVVY93], [For97], [For09]) as follows: $\mathsf{PH} = \mathsf{NP}^{\mathsf{PH}} \subseteq \mathsf{NP}^{\mathsf{P}^{\#\mathsf{P}}} = \mathsf{NP}^{\#\mathsf{P}} = \mathsf{NP}^{\mathsf{GapP}} =^{10} \mathsf{NP}^{\mathsf{C_{=}P}}$. We now observe: $\mathsf{PH} \subseteq \mathsf{NP}^{\mathsf{C_{=}P}} = \mathsf{NP}^{[\mathsf{GapP}=0]} = \mathsf{NP}^{[\mathsf{GapP}^k=0]} \subseteq \mathsf{NP}^{[\#\mathsf{P}=0]} = \mathsf{NP}^{\mathsf{coNP}} = \Sigma_2^{\mathsf{p}}$. □

II-C.2 Corollary (Cauchy–Schwarz inequality)**.** $a^2 + b^2 \not\geqslant_{\#} 2ab$ *unless* $\mathsf{PH} = \Sigma_2^{\mathsf{p}}$.

This innocent looking corollary has immediate negative consequences on the existence of combinatorial proofs for inequalities (in the sense of #P interpretations of the difference of both sides of the inequality), for example the Cauchy inequality or the Alexandrov–Fenchel inequality, see the full version for the details.

Given the success in our *matching polynomial* example §I-B(4), one can ask if this example is generalizable to other log-concave properties. Formally, is it true that $g^2 \geqslant_{\#} fh$ when functions (f,g,h) are restricted to $S = \{(f,g,h) \in \mathbb{N}^3 \mid g^2 - fh \geq 0\}$? We give a negative answer to this question, suggesting that many log-concavity results and open problems (see full version) are unlikely to have a direct combinatorial proof.

II-C.3 Proposition (Log-concavity)**.** *Let* $\varphi(f,g,h) := g^2 - fh$*, and let* $S := \{(f,g,h) \in \mathbb{N}^3 \mid g^2 - fh \geq 0\}$*. Then* $\varphi\big(\#\mathsf{P}^{\times 3}_{\in S}\big) \not\subseteq \#\mathsf{P}$ *unless* $\mathsf{PH} = \Sigma_2^{\mathsf{p}}$.

Proof. Let $f := 1$, $g := (x+y)$ and $h := 4xy$. Observe that $g^2 - fh = (x-y)^2 \geq 0$ for all $x, y \in \mathbb{R}$. The resulting complete square allows us to use Corollary II-C.2 and prove the result. We now formalize this approach in the notation above.

Let $\vec{\gamma} : \mathbb{N}^2 \to \mathbb{N}^3$ defined by $(x,y) \mapsto \big(1, (x+y), 4xy\big)$. Then $\vec{\gamma}\big(\#\mathsf{P}^{\times 2}\big) \subseteq \#\mathsf{P}^{\times 3}_{\in S}$. Note that on the left-hand side we have no subscript anymore, as the image is guaranteed to lie in S. If we have $\varphi\big(\#\mathsf{P}^{\times 3}_{\in S}\big) \subseteq \#\mathsf{P}$, then it follows $\varphi\big(\vec{\gamma}\big(\#\mathsf{P}^{\times 2}\big)\big) \subseteq \#\mathsf{P}$. But we have $\varphi\big(\vec{\gamma}\big(\#\mathsf{P}^{\times 2}\big)\big) = \mathsf{GapP}^2$. We conclude: if $\varphi\big(\#\mathsf{P}^{\times 3}_{\in S}\big) \subseteq \#\mathsf{P}$ then $\mathsf{GapP}^2 \subseteq \#\mathsf{P}$. Hence, by Proposition II-C.1, we have $\mathsf{PH} = \Sigma_2^{\mathsf{p}}$. □

D. Non-monotone closure properties

A map $\varphi : \mathbb{N}^k \to \mathbb{Q}$ is called *monotone* if $\varphi(a_1, \ldots, a_k) \leq \varphi(a'_1, \ldots, a'_k)$ for all integer $a_1 \leq a'_1$, …, $a_k \leq a'_k$. For example, polynomials $x/2$, $x-1$ and $x+y$ are monotone, but $x^2 - 2x$ and $(x-y)^2$ are not.

II-D.1 Proposition (Non-monotone closure properties)**.** *Fix* $k \geq 1$*. If* $\varphi : \mathbb{N}^k \to \mathbb{N}$ *is a non-monotone closure property of* #P*, then* $\mathsf{UP} = \mathsf{coUP}$.

Proof. Let φ be a k-variate non-monotone closure property of #P. Then there exists $\vec{c} \in \mathbb{N}^k$ and $i \in [k]$ with $\varphi(\vec{c}) > \varphi(\vec{c} + \vec{e_i})$, where $\vec{e_i}$ is the i-th standard basis vector. Let $D := \varphi(\vec{c})$, and let $d := \varphi\big(\vec{c} + \vec{e_i}\big)$. Note that

$$\psi : f \mapsto \begin{pmatrix} \varphi(f \cdot \vec{e_i} + \vec{c}) \\ D \end{pmatrix}$$

is a univariate closure property of #P.

Now let $f \in \mathsf{UP} = \#\mathsf{P}_{\in\{0,1\}}$ be arbitrary. Let $\beta = f(w)$ for an arbitrary $w \in \{0,1\}^*$. We have $\beta = 0$ if and only if $\beta \cdot \vec{e_i} + \vec{c} = \vec{c}$, and if and only if $\varphi(\beta \cdot \vec{e_i} + \vec{c}) = D$. Similarly, we have $\beta = 1$ if and only if $\beta \cdot \vec{e_i} + \vec{c} = \vec{c} + \vec{e_i}$, and if and only if $\varphi(\beta \cdot \vec{e_i} + \vec{c}) = d$. Therefore, $\psi(\beta) = 1 - \beta$. Hence, we have seen that $\psi(f) = 1 - f$ and that $\psi(f) \in \mathsf{UP}$. It follows that $f \in 1 - \mathsf{UP} = \mathsf{coUP}$. □

A similar use of binomial coefficients can also be found in [BG92]. Curiously, $x(x-1)^2 \geqslant_{\#} 0$ since $x(x-1)^2 = 6\binom{x}{3} + 2\binom{x}{2}$, yet by Proposition II-D.1 we have:

II-D.2 Corollary. $(x-1)^2 \not\geqslant_{\#} 0$ *unless* $\mathsf{UP} = \mathsf{coUP}$.

Note that $a^2+b^2 \geqslant ab$ holds over $\mathbb{N}$, and is halfway between $a^2+b^2 \geqslant 2ab$ and $a^2+b^2 \geqslant 0$. So one can ask if $a^2+b^2 \geqslant_{\#} ab$. Observe that $\varphi(a,b) := a^2 - ab + b^2$ is non-monotone: $\varphi(0,2) = 4$ and $\varphi(1,2) = 3$. Proposition II-D.1 then gives:

II-D.3 Corollary. $a^2 + b^2 \not\geqslant_{\#} ab$ *unless* $\mathsf{UP} = \mathsf{coUP}$.

Recall the *Motzkin polynomial* $M(x,y) := x^2y^4 + x^4y^2 - 3x^2y^2 + 1$. It follows from the AM-GM inequality applied to positive terms, that $M(x,y) \geq 0$ for all $x, y \in \mathbb{R}$. On the other hand, this polynomial is famously not a *sum of squares*, and is a fundamental example in Semidefinite Optimization, see e.g. [Ble13], [Mar08]. Now, observe that $M(x,y)$ is not monotone: $M(0,1) = 1$ and $M(1,1) = 0$. Proposition II-D.1 then gives:

II-D.4 Corollary. $M(x,y) \not\geqslant_{\#} 0$ *unless* $\mathsf{UP} = \mathsf{coUP}$.

[10] $\mathsf{NP}^{\mathsf{GapP}} \subseteq \mathsf{NP}^{\mathsf{C_{=}P}}$ holds because instead of calling the oracle for a function $g \in \mathsf{GapP}$ we can nondeterministically guess its return value $i = g(w)$ and call the $\mathsf{C_{=}P}$ oracle $[g - i = 0]$ on the input w to check for correctness (continue the computation if the guess was correct; reject the computation if the guess was wrong).

E. The binomial basis theorem

In this section we recall a classical result, describing all relativizing polynomial closure properties of #P and GapP. Note that we considered only non-monotone examples in §II-C and §II-D, while many natural polynomials are monotone. Clearly, every polynomial with integer coefficients is a closure property of GapP, but might not be a closure property of #P. If all coefficients of φ are nonnegative integers, then φ is clearly a closure property of #P, but we have seen that there are more, e.g. $\frac{1}{2}x^2 - \frac{1}{2}x = \binom{x}{2} \geqslant_{\#} 0$.

The main tool to shed light onto these issues is the binomial basis for the polynomial ring $\mathbb{Q}[x_1, \ldots, x_k]$, which is given by the polynomials $\beta_{\boldsymbol{a}} \in \mathbb{Q}[x_1, \ldots, x_k]$, $\boldsymbol{a} = (a_1, \ldots, a_k) \in \mathbb{N}^k$, via

$$\beta_{\boldsymbol{a}}(x_1, \ldots, x_k) := \binom{x_1}{a_1} \cdots \binom{x_k}{a_k}.$$

Every polynomial has a unique expression of finite support in this basis. The univariate version is well-known under the name of classical numerical polynomials. The study of the multivariate version goes back to Nagell [Nag19]. This basis explains the behavior we observe, as stated in the following fundamental theorem, for which the proof is split up into the #P part, see [HVW95, Thm. 3.13], and the GapP part, see [Bei97, Thm. 6] (see also the bibliographic notes in [HO02, §5.6]). The GapP part can be obtained as a direct consequence of the algebraic properties of the binomial basis, see the full version. We will reprove the #P part as a direct corollary of our much more general Diagonalization Theorem (see §III-A).

Theorem (Binomial basis theorem)**.** *The following four properties for a multivariate polynomial φ over $\mathbb{Q}$ are equivalent:*
- *φ is a closure property of* GapP
- *φ is a relativizing closure property of* GapP
- *φ is integer-valued*
- *the expression of φ over the binomial basis has only integer coefficients.*

Moreover, the following are equivalent:
- *φ is a closure property of* $\mathsf{GapP}_{\geq 0}$
- *φ is a relativizing closure property of* $\mathsf{GapP}_{\geq 0}$
- *φ is integer-valued and attains only nonnegative integers*
- *the expression of φ over the binomial basis has integer coefficients and φ attains only nonnegative integers if evaluated at integer points in the nonnegative cone.*

Moreover, the following are equivalent:
- *φ is a relativizing closure property of* #P*,*
- *the expression of φ over the binomial basis has only nonnegative integer coefficients.*

Note that even though #P and $\mathsf{GapP}_{\geq 0}$ have different relativizing closure properties, this does not unconditionally separate these two classes. Note also that the theorem implies that *all polynomial closure properties of* GapP *and* $\mathsf{GapP}_{\geq 0}$ *relativize*. We conjecture that this is true for #P as well, which we call the *Binomial Basis Conjecture* (which would immediately imply that $\mathsf{GapP}_{\geq 0} \neq \#\mathsf{P}$). Proving this, however, would imply $\#\mathsf{P} \neq \#\mathsf{P}^{\mathsf{NP}}$ (and hence $\mathsf{P} \neq \mathsf{NP}$), even just for the univariate $\varphi = \binom{x-1}{2}$ (see the full version). We get the following sequence of implications: $\mathsf{P} = \mathsf{NP} \implies \#\mathsf{P} = \#\mathsf{P}^{\mathsf{NP}} \overset{\text{full version}}{\implies} \binom{\#\mathsf{P}-1}{2} \subseteq \#\mathsf{P} \overset{\text{Prop. II-D.1}}{\implies} \mathsf{UP} = \mathsf{coUP}$. We call polynomials φ whose expression over the binomial basis has only nonnegative integer coefficients *binomial-good*, all others are called *binomial-bad*.

The fact that H_d in §I-C(2) is binomial-bad gives us the described separation. One famous instance of a binomial-good polynomial is the Frobenius map from §I-B(5). There, binomial-goodness can be interpreted as a combinatorial proof of Fermat's little theorem, see Peterson's proof in the full version.

The Binomial Basis Theorem is proved in [HVW95, Thm. 3.13] together with [Bei97, Thm. 6], which is in fact an extension of an argument of [CGH+89, Thm 3.1.1] and [OH93, p. 310] about the weakness of #P machines in the presence of oracles. We prove it as a corollary of our Diagonalization Theorem (see §III-A), which greatly extends the Binomial Basis Theorem.

1) The Ahlswede–Daykin inequality: More advanced problems, where the set S is given as a semialgebraic set, are also possible, for example for the Ahlswede–Daykin inequality, see §I-C(3) with more details in the full version.

II-E.1 Proposition (Ahlswede–Daykin inequality)**.** *Let* $S := \Big\{(\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1, \delta_0, \delta_1, h_1, h_2, h_3, h_4) \in \mathbb{N}^{12} \;\Big|\; \alpha_0\beta_0 + h_1 = \gamma_0\delta_0, \alpha_0\beta_1 + h_2 = \gamma_0\delta_1, \alpha_1\beta_0 + h_3 = \gamma_0\delta_1, \alpha_1\beta_1 + h_4 = \gamma_1\delta_1\Big\}$ *and let* $\varphi := \big(\gamma_0 + \gamma_1\big)\big(\delta_0 + \delta_1\big) - \big(\alpha_0 + \alpha_1\big)\big(\beta_0 + \beta_1\big)$*. Then, under the Univariate Binomial Basis Conjecture we have* $\varphi(\overrightarrow{\#\mathsf{P}}_{\in S}) \not\subseteq \#\mathsf{P}$.

Proof. Define $\vec{\gamma} : \mathbb{N} \to \mathbb{N}^{12}$ via $\gamma(x) = \big(1, 1, x, x, x, 1, 1, x, 0, 2\binom{x}{2}, 2\binom{x}{2}, 0\big)$. Then $\vec{\gamma}(\#\mathsf{P}) \subseteq \#\mathsf{P}^{\times 12}_{\in S}$. Note that on the left-hand side we have no index anymore, as the image is guaranteed to lie in S. Assume for the sake of contradiction that we have an inclusion $\varphi(\#\mathsf{P}^{\times 12}_{\in S}) \subseteq \#\mathsf{P}$. Then it follows that we have an inclusion $\varphi\big(\vec{\gamma}(\#\mathsf{P})\big) \subseteq \#\mathsf{P}$. The Binomial Basis Conjecture implies that this inclusion relativizes. Therefore, by the Binomial Basis Theorem the univariate polynomial $\varphi \circ \vec{\gamma}$ is binomial-good. But we have $\varphi\big(\vec{\gamma}(f)\big) = f^2 - 2f + 1 = 2\binom{f}{2} - f + 1$, which is binomial-bad, a contradiction. □

III. Main results

In this section we state our main results. In §III-A we state the Diagonalization Theorem and we give Karamata's inequality as an involved example for its application. In §III-D we lift these techniques to handle TFNP and its subclasses. We obtain several oracle separations from #P in this way, see Figure 1.

A. The diagonalization theorem

In Proposition II-E.1 the set S lies on an affine algebraic variety, and the proof goes by embedding a curve given by binomial-good polynomials. This is a way of finding separations, but it remains unclear if such curves always exist

or how we can find them. In general, if S lies on an affine variety Z with vanishing ideal I, then we know that if there exists a polynomial $\xi \in I$ such that $\varphi + \xi$ is binomial-good, then φ is a polynomial closure property of #P on S. This is exactly the insight that gives SPERNER $- 1 \in$ #P, where all instances lie on the variety $\{(t_+, t_-) \in \mathbb{N}^2 : t_+ - t_- - 1 = 0\}$.

The reverse is true in the important case of graph varieties (all our examples fall in this category), as we show in the following Diagonalization Theorem. Formally, assume that there exist $\ell \in \{0, \ldots, k\}$, and polynomial maps $\zeta_b : \mathbb{Q}^\ell \to \mathbb{Q}$, where $b \in \{\ell + 1, \ldots, k\}$, such that Z is the image $\big(f_1, \ldots, f_\ell, \zeta_{\ell+1}(f_1, \ldots, f_\ell), \ldots, \zeta_k(f_1, \ldots, f_\ell)\big)$. In this case the vanishing ideal I is generated by the $\zeta_b - f_b$ (see the full version). We call a coset $\varphi + I$ binomial-good, if it contains a binomial-good polynomial, otherwise $\varphi + I$ is binomial-bad.

Informally, the Diagonalization Theorem states that in many situations we have: if $\varphi + I$ is binomial-bad, then for all sets S and for all functions MULTIPLICITIES we have that for $p_A = \varphi(\text{MULTIPLICITIES}(A))$ for which we have set-instantiators there exists an oracle A such that $p_A \notin \#\mathsf{P}^A$. This is not only useful for proving $\varphi(\#\mathsf{P}_S^A) \not\subseteq \#\mathsf{P}^A$, but will also be used for problems where the relations among the input #P functions are guaranteed syntactically, see §III-D.

To state the Diagonalization Theorem we first introduce set-instantiators in the next subsection.

For a subset $B \subseteq \{0,1\}^j$, we write $\widetilde{B} \subseteq \{0,1\}^{j-1}$ to denote the set of suffixes of all strings in B that start with 1. For a subset $B \subseteq \{0,1\}^{j-1}$, we write $\{1\} \boxplus B \subseteq \{0,1\}^j$ to denote the union of $\{0^j\}$ with the set of strings that start with 1 and continue with a string from B.

B. Set-instantiators

We want to consider computation paths of nondeterministic Turing machines, but the actual computational device we are arguing about is a nondeterministic Turing machine with oracle access to an oracle that is defined up to strings of length $< j$, and where the oracle answers with 0 for all oracle queries of length $> j$. We capture this in the following definition.

III-B.1 Definition. *A* computation path τ *of a nondeterministic Turing machine on some input is defined as the sequence of its nondeterministic choice bits and the answers to its length j oracle queries* (*both types of bits appear in the same list, ordered chronologically*). *Formally, it is an element of* $\{0,1\}^*$.

The same Turing machine can yield the same computation path on different inputs (for example, when not the whole input is read) or when having access to different oracles, because the oracles can differ in positions that are not queried. We are especially interested in the case where the input is 0^j and the oracles differ in exactly the set $A_j \subseteq \{0,1\}^j$ of length j strings.

Given a nondeterministic Turing machine M and an oracle $A_{<j} := \bigcup_{j'<j} A_{j'}$ where $A_{j'} \subseteq \{0,1\}^{j'}$, and given a subset $B \subseteq \{0,1\}^{j-1}$, we are interested in the number of accepting paths of M when given oracle access to $A_{<j} \cup (\{1\} \boxplus B)$, where $A_{<j}$ is fixed. We define

$$h_M^B(w) \;:=\; \#\mathsf{acc}_{M^{A_{<j} \cup (\{1\} \boxplus B)}}(w). \qquad \text{(III-B.2)}$$

It is instructive to think of $A_{<j}$ and M as together forming a computational device that has oracle access to some subset $B \subseteq \{0,1\}^{j-1}$.

For $\vec{b} \in \mathbb{N}^k$, we write $\mathscr{B}(\vec{b}) := \mathscr{B}([b_1]) \times \cdots \times \mathscr{B}([b_k])$, where $\mathscr{B}([a])$ is the set of all subsets of $[a] = \{1, \ldots, a\}$. For $\vec{s}, \vec{t} \in \mathscr{B}(\vec{b})$, we write $\vec{s} \subseteq \vec{t}$ if $s_a \subseteq t_a$ for all $1 \le a \le k$. For an element $\vec{s} \in \mathscr{B}(\vec{b})$, we write $|\vec{s}| := \big(|s_1|, \ldots, |s_k|\big)$.

III-B.3 Definition (Set-instantiator against $(M, j, A_{<j}, S, \vec{b})$)**.** *Let M be a nondeterministic Turing machine, let $j \in \mathbb{N}$, and let $A_{<j} \subseteq \{0,1\}^*$ be a language that contains only strings of length $< j$. Let $S \subseteq \mathbb{N}^k$ be a set and let $\vec{b} \in \mathbb{N}^k$. We set $\mathscr{B}(\vec{b})_S := \big\{\vec{s} \in \mathscr{B}(\vec{b}) : |\vec{s}| \in S\big\}$.*

Let $\top$ be a symbolic top element above $\mathscr{B}(\vec{b})$, i.e. $\vec{s} \subsetneq \top$ for all $\vec{s} \in \mathscr{B}(\vec{b})$. A set-instantiator $\mathcal{SI}$ *is a pair of*

- *an instantiation function* $\mathsf{inst}_{\mathcal{SI}} : \mathscr{B}(\vec{b})_S \to \{0,1\}^{[2^{j-1}]}$, *and*
- *a perception function* $\mathsf{perc}_{\mathcal{SI}} : \{0,1\}^* \to \mathscr{B}(\vec{b}) \cup \{\top\}$,

such that the following property holds for all $\vec{s} \in \mathscr{B}(\vec{b})_S$:

- *$\tau \in \{0,1\}^*$ is an accepting path for the computation $h_M^{\mathsf{inst}_{\mathcal{SI}}(\vec{s})}(0^j)$ if and only if $\mathsf{perc}_{\mathcal{SI}}(\tau) \subseteq \vec{s}$.*

The intuition is that a computation path queries the oracle and sees the existence of several objects (k different types of objects), and then decides to accept or not based solely on the set of objects perceived, independent of whether or not there are actually other unqueried objects in the oracle. The Turing machine might even *know* that there must be other objects for some syntactic reason and can take that information into account.

For example, in SPERNER we have $k = 2$, and we consider rainbow triangles of positive/negative orientation. We know that $t_+ - t_- - 1 = 0$, so if we see $t_+ \ge 3$ and $t_- \ge 3$, then we know that there must be at least one rainbow triangle of positive orientation that we have not seen. Note that if an accepting path τ sees an object in the oracle and then we remove that object by changing the oracle, then running the same computation we will at some point get a different oracle answer, and hence τ will not be a computation path of this (input, oracle) tuple.

Formally, in the above definition we think of accepting paths as having a perception from $\mathscr{B}(\vec{b})$, while computation paths that never accept on any of the instantiations are given perception $\top$. Note also that from the definition it is immediately clear that from a set-instantiator with a set S, we get a set-instantiator with the same parameters for every subset of S.

We usually do not mention $A_{<j}$ in the context of set-instantiators, as it has no effect on the construction of set-instantiators, and is also understood from the context. When discussing polynomial closure properties of #P, set-instantiators almost trivially exist, but for counting classes

coming from TFNP this is not obvious. We create the necessary set-instantiators in the full version.

C. Formal statement of the diagonalization theorem

Our main tool for constructing oracles that separate from #P is the following Diagonalization Theorem, which depends on the parameters φ, ζ, S, MULTIPLICITIES, and $\vec{t}$. In most situations $\vec{t} \in S$ can be arbitrary, so $\vec{t}$ is often not specified. To use the theorem well, MULTIPLICITIES should map into S.

For $A_{<j} \in \{0,1\}^{<j}$, we say that a nondeterministic oracle Turing machine M *answers consistently* for $(j, A_{<j}, \text{MULTIPLICITIES})$, if for every $B \subseteq \{0,1\}^{j-1}$ we must have the number $\#\mathsf{acc}_M^{A_{<j} \cup (\{1\} \boxplus B)}(w)$ is the same for all B that have the same MULTIPLICITIES(B), for all $w \in \{0,1\}^*$. In other words, we must have:

$$\#\mathsf{acc}_M^{A_{<j} \cup (\{1\} \boxplus B)}(w) \;=\; \#\mathsf{acc}_M^{A_{<j} \cup (\{1\} \boxplus C)}(w)$$

for all $C \in \{0,1\}^{j-1}$ with MULTIPLICITIES(B) = MULTIPLICITIES(C).

III-C.1 Theorem (Diagonalization Theorem)**.** *Fix k and $0 \le \ell \le k$. We write $\vec{f} = (f_1, \ldots, f_k)$ and $\vec{v} = (v_1, \ldots, v_\ell)$. Let $\varphi \in \mathbb{Q}[\vec{f}]$. Fix non-constant functions $\zeta_b \in \mathbb{Q}[\vec{v}]$, $\ell+1 \le b \le k$. Set I to be the ideal generated by the $\zeta_b(\vec{v}) - f_b$, where $\ell+1 \le b \le k$.*

Define $Z := \{\vec{f} \in \mathbb{Q}^k \mid \mathsf{eq}_{\ell+1}(\vec{f}) = \ldots = \mathsf{eq}_k(\vec{f}) = 0\}$, where $\mathsf{eq}_b := \zeta_b(\vec{v}) - f_b$. Denote $T := \mathbb{N}^k_{\ge 0} \cap Z$ and let $S \subseteq T$. Consider a map $\tau : \mathbb{Q}^\ell \to Z$ defined as

$$\tau(\vec{v}) \;:= \big(\vec{v}, \zeta_{\ell+1}(\vec{v}), \ldots, \zeta_k(\vec{v})\big).$$

Set $C'_S := \big\{\vec{v} \in \mathbb{Q}^\ell_{\ge 0} : |\tau^{-1}(S) \cap \mathbb{Q}\vec{v}| = \infty\big\}$. Assume that

(1) Z contains at least one integer point,

(2) The Zariski closures coincide: $\overline{C'_S}^{\text{Zar}} = \overline{C'_T}^{\text{Zar}}$, and

(3) there exists a point $\vec{v} \in \mathbb{Q}^\ell_{\ge 0}$ that satisfies strict inequalities

$$\zeta_b^{\text{hom}}(\vec{v}) > 0 \quad \textit{for all} \quad \ell+1 \le b \le k,$$

where $\zeta_b^{\text{hom}} \in \mathbb{Q}[\vec{v}]$ is the top nonzero homogeneous part of ζ_b.

Fix a set of multivariate functions MULTIPLICITIES $: \mathscr{B}\big(\{0,1\}^{j-1}\big) \to \mathbb{N}^k_{\ge 0}$. *Assume that for every nondeterministic polynomial-time Turing machine M and for every $\vec{f}$ there exist infinitely many $j \in \mathbb{N}$ such that for every $A_{<j} \in \{0,1\}^{<j}$ either M does not answer consistently for $\big(j, A_j, \text{MULTIPLICITIES}\big)$ or there is a set-instantiator $\mathcal{SI}$ against $\big(M, j, A_{<j}, S, \vec{f}\big)$ with* MULTIPLICITIES$\big(\mathsf{inst}_{\mathcal{SI}}(\vec{s})\big) = |\vec{s}|$ *for all $\vec{s} \in \mathscr{B}(\vec{f})_S$.*

Fix any $\vec{t} \in S$. For $A \subseteq \{0,1\}^*$, we write: $A = \bigcup_{j \ge 0} A_j$, where $A_j \subseteq \{0,1\}^j$. Define

$$p_A(w) \;:=\; \begin{cases} \varphi\big(\text{MULTIPLICITIES}\big(\widetilde{A}_{|w|}\big)\big) & \textit{if } A_{|w|}(0^{|w|}) = 1 \\ \varphi(\vec{t}) & \textit{otherwise,} \end{cases}$$

where $\widetilde{A}_j$ is the set of length $j-1$ suffixes of the strings in A_j that start with a 1.

Finally, suppose $\varphi + I$ is binomial-bad. Then there exists an oracle $A \subseteq \{0,1\}^*$ such that for every nondeterministic polynomial-time Turing machine M there exists j such that $p_A(0^j) \ne \#\mathsf{acc}_{M^A}(0^j)$ and whenever $A(0^j) = 1$, then $A_j = \{1\} \boxplus \mathsf{inst}_{\mathcal{SI}}(\vec{s})$ for some $\vec{s}$ and one of the $\mathcal{SI}$ above.

Note that the technical conditions (1), (2), and (3) are very easy to check in most situations. They exist to prevent degenerate cases.

The Diagonalization Theorem is the technical heart of this paper. It is stated in high generality, and we apply it to a large set of examples of very different flavors, such as for example the Hadamard inequality or $\#\mathsf{PPA}-1$. Its proof relies on the Witness Theorem (see full version), whose proof uses methods from several areas of mathematics including algebraic geometry and Ramsey theory.

As an illustration we now apply the Diagonalization Theorem to Karamata's inequality, see the full version for the full details. In the Karamata setting we are given $f_i, g_i \in \#\mathsf{P}$, $1 \le i \le n$, such that the following functions h_i, $1 \le i < n$, are also all in #P :

$$h_i \;:=\; f_1 + \ldots + f_i - g_1 - \ldots - g_i,$$

and we are also guaranteed that

$$f_1 + \ldots + f_n - g_1 - \ldots - g_n \;=\; 0. \qquad \text{(III-C.2)}$$

This assumption is called *majorization*. Moreover, the functions

$$d_i := f_i - f_{i+1} \quad \text{and} \quad e_i := g_i - g_{i+1} \qquad \text{(III-C.3)}$$

are also in #P for all $1 \le i < n$. Let $Z \subseteq \mathbb{Q}^{5n-3}$ denote the variety of points that satisfy the constraints (III-C.2) and (III-C.3), and let $S = Z \cap \mathbb{N}^{5n-3}$. Let $\gamma \in \mathsf{GapP}_{\ge 0}$ be any monotone integer-valued convex function. Define the Karamata function as

$$K_{n,\gamma}(\vec{f}, \vec{g}) \;:=\; \textstyle\sum_{i=1}^n \gamma(f_i) \;-\; \sum_{i=1}^n \gamma(g_i).$$

Clearly $K_{n,\gamma}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \mathsf{GapP}$. In fact, even $K_{n,\gamma}(\overrightarrow{\mathsf{GapP}}) \subseteq \mathsf{GapP}$. Karamata's inequality implies that the answer is always nonnegative for inputs from S. Hence, $K_{n,\gamma}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \mathsf{GapP}_{\ge 0}$. For which γ do we have $K_{n,\gamma}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \#\mathsf{P}$?

- For affine linear γ we clearly have $K_{n,\gamma} = 0 \in \#\mathsf{P}$.
- For $\gamma(t) = t^2$, we have $K_{2,\gamma}(f_1, f_2, g_1, g_2) = (d_1 + e_1)h_1$ on S. This can be seen by plugging in $d_1 = f_1 - f_2$, $e_1 = g_1 - g_2$, and $g_2 = f_1 + f_2 - g_1$. Clearly $(d_1 + e_1)h_1 \in \#\mathsf{P}$. There are other proofs, for example instead of $(d_1+e_1)h_1$ we could have taken $2h_1 + 2e_1h_1 + 4\binom{h_1}{2}$ with the same argument.
- For $\gamma(t) = t^2$, we have $K_{3,\gamma}(f_1, f_2, f_3, g_1, g_2, g_3) = (d_1 + e_1)h_1 + (d_2 + e_2)h_2 \in \#\mathsf{P}$ on S.
- For $\gamma(t) = \binom{t}{2}$, we have $K_{2,\gamma}(f_1, f_2, g_1, g_2) = (e_1 + 1)h_1 + 2\binom{h_1}{2} \in \#\mathsf{P}$ on S.
- For $\gamma(t) = \binom{t}{2}$, we observe that for the *double* we have $2K_{3,\gamma}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \#\mathsf{P}$ via the observation that $2K_{3,\binom{t}{2}} = K_{3,t^2}$ on S (the affine linear parts cancel out).

All inclusions $K_{n,\gamma}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \#\mathsf{P}$ in this section so far relativize. The next proposition shows that the doubling we just used was in fact necessary, because otherwise we obtain an oracle separation.

Proposition. *$\exists A \subseteq \{0,1\}^*$ such that $K_{3,\binom{t}{2}}\big(\overrightarrow{\#\mathsf{P}}^A_{\in S}\big) \not\subseteq \#\mathsf{P}^A$.*

Proof sketch. We use the Diagonalization Theorem. We have $5n-3=12$, so $S = Z \cap \mathbb{N}^{12}$. We fix an arbitrary order of the 12 variables: $\big(f_1, f_2, f_3, g_1, g_2, g_3, d_1, d_2, e_1, e_2, h_1, h_2\big)$. The variety Z is then given as the kernel of the linear map given by the following top matrix:

$$\begin{pmatrix}
1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\
1 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}$$

$$\downarrow \text{Gauss-Jordan}$$

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & -1 & -1 & -1 & 0 \\
0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 1 & -1 \\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 & -2 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 & 1 & -2
\end{pmatrix}$$

To obtain the necessary parametrization ζ of Z, we convert it to row echelon form (the fact that the entries are integer is convenient, but not necessary for our techniques to apply), which is the bottom matrix. We set $\ell = 5$, $k = 12$. Permuting the order of the columns to $(6, 9, 10, 11, 12, 1, 2, 3, 4, 5, 7, 8)$, we obtain affine linear functions $\zeta_8, \ldots, \zeta_{12}$, each ζ_b depends linearly on the first 5 variables. We set $\textsc{Multiplicities} = \textsc{OccurrenceMulti}_{12}$, which is the function defined as follows: on input $w \in \{0,1\}^*$ we split w into 12 parts of roughly the same size, and the output is the vector that specifies how many 1s are in the first part, how many 1s are in the second part, and so on. We set $\varphi\big(f_1, f_2, f_3, g_1, g_2, g_3, d_1, d_2, e_1, e_2, h_1, h_2\big) := f_1^2 + f_2^2 + f_3^2 - g_1^2 - g_2^2 - g_3^2$. After verifying the technical assumptions, to apply the theorem it remains to show that $\varphi + I$ is binomial-bad. Since all ζ_b are affine linear, this claim boils down to checking that polyhedron $\mathcal{P}_{\varphi,\zeta}$ does not have integer points. We formalize and generalize this implication in the Polyhedron Theorem (see full version). Here we have a polyhedron in $\mathbb{Q}^{91}$ given by 21 linear equations intersected with the nonnegative orthant. We use a computer to set up the polyhedron. Indeed, it contains the half-integer point that shows that $2K_{3,\binom{t}{2}}(\overrightarrow{\#\mathsf{P}}_{\in S}) \subseteq \#\mathsf{P}$, but it *does not* contain an integer point, which gives A such that $\varphi(p_A) \notin \#\mathsf{P}^A$, but $\varphi(p_A) \in K_{3,\binom{t}{2}}(\overrightarrow{\#\mathsf{P}}^A_{\in S})$. □

Let us point out that the proof above illustrates how the existence of an oracle separation between counting classes is reduced to a finite calculation. The Polyhedron Theorem is also what we use for studying counting classes from TFNP (see §III-D), but the corresponding polyhedra there are very simple. The polyhedron for SPERNER for example has the integer point $(2, 0)$ to represent that $\varphi = 2t_- + 0t_+$ on the variety. The technical difficulty in those cases is not the polyhedron, but the existence of set-instantiators (see the full version, §6.1). If we just study closure properties of #P, then trivial set-instantiators can be used.

D. Counting classes and TFNP

In this section define the counting classes for which we claimed in (4) in §I-C that many of them coincide with #P, while others are strictly stronger w.r.t. an oracle. In order to do so, we attach oracles to the syntactic subclasses of TFNP.[11]

Consider for example the relation RLONELY. This is for PPA, as the other classes are handled analogously. Let $(C, x) \in \textsc{rLonely}$ if and only if $x \neq 0 \ \wedge \ \big(C'(x) = x \ \vee \ C'(C'(x)) \neq x\big)$, where C is the description of a polynomially-sized multi-output Boolean circuit that describes the partner function on an exponentially large graph, and C' is the syntactic modification to C that ensures that $C'(0) = 0$.

Now, let rPPA be the set of polynomially balanced relations R for which a pair (α, β) of polytime computable maps exists with $(C, \beta(x)) \in R$ if and only if $(\alpha(C), x) \in \textsc{rLonely}$. These are the relations that correspond to search problems in PPA. Let rP denote the set of polynomially balanced relations that can be evaluated in polynomial time. By definition, $\mathsf{rPPA} \subseteq \mathsf{rP}$.

For a language $A \subseteq \{0,1\}^*$ we define analogously $(C, x) \in \textsc{rLonely}^A$ if and only if $\big(C(x) = x \vee C(C(x)) \neq x\big)$, but now we allow the circuit C to have arbitrary arity oracle gates that query the oracle A. Let rPPA^A be the set of polynomially balanced relations R for which a pair (α, β) of polynomial-time computable maps exists with $(C, \beta(x)) \in R$ if and only if $(\alpha(C), x) \in \textsc{rLonely}^A$. Note here that the only difference is that $\alpha(C)$ can have oracle gates. Let rP^A denote the set of polynomially balanced relations that can be evaluated in polynomial time with access to A. By definition, we have $\mathsf{rPPA}^A \subseteq \mathsf{rP}^A$.[12]

We define the corresponding counting class $\#\mathsf{PPA}^A$ via $f \in \#\mathsf{PPA}^A \Leftrightarrow \exists R \in \mathsf{rPPA}^A : \ f(w) = \sum_{y \in \{0,1\}^*} R(w, y)$. Recall that $f \in \#\mathsf{P}^A \Leftrightarrow \exists R \in \mathsf{rP}^A : \ f(w) = \sum_{y \in \{0,1\}^*} R(w, y)$. Hence, clearly $\#\mathsf{PPA}^A \subseteq \#\mathsf{P}^A$, and in fact $\#\mathsf{PPA}^A \subseteq \#\mathsf{P}^A_{\geq 1}$ for all languages A.[13] [14]

For the study of whether or not a problem is in #P we need the finer viewpoint that is obtained when insisting on (α, β) being a *parsimonious reduction*, i.e., $\big((C, \beta(x)) \in R$ and $(C, \beta(y)) \in R\big)$ implies $x = y$. Since not all PPA-complete problems are equivalent to each other via parsimonious reductions, this gives rise to different counting complexity classes, depending on the PPA-complete problem. We

[11] We consider CLS, PLS, PPAD, PPADS, PPA, and PPP here, see e.g. [GP17]. The instances are exponentially large (di)graphs given succinctly by circuits or lists of circuits. For the sake of simplicity, we will assume in this discussion that finite lists of circuits are merged into a single circuit with additional input bits.

[12] We use the r-prefix to avoid notational issues similar to the ones discussed in [HV95], [BS01]. We do not claim to have found a particularly good notation, but a suggestive one.

[13] In fact, $\#\mathsf{P}_{\geq 1}$ can be thought of as the counting analogue of TFNP, i.e., it is reasonable to define $\#\mathsf{TFNP} := \#\mathsf{P}_{\geq 1}$.

[14] We choose this approach, which is different from the type-2 complexity approach in [BCE+98], [BM04], because we want to compare our counting classes to $\#\mathsf{P}^A$.

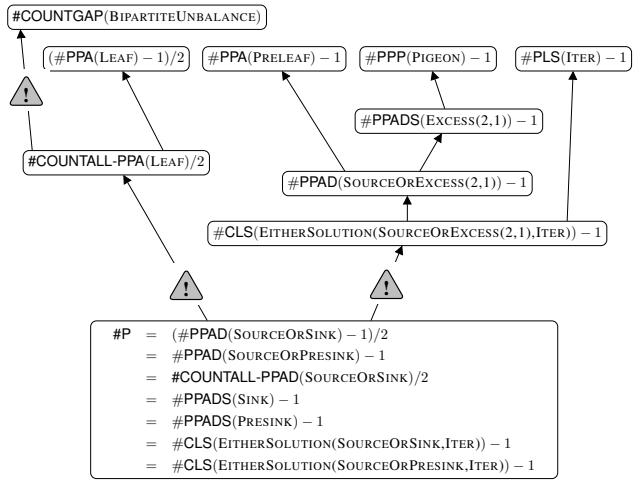

Fig. 1. The relativizing equalities and inclusions; and the oracle separations. All equalities with #P are shown via relativizing parsimonious reductions. A solid arrow represents a relativizing parsimonious reduction. An arrow with a ⚠ represents a relativizing parsimonious reduction where there is an oracle separation in the other direction.

write $\#\mathsf{PPA}(\mathrm{P})$ to indicate that we mean the counting class defined by problem P under parsimonious reductions.[15] For example, observe that all functions in $\#\mathsf{PPA}(\textsc{Lonely})$ output odd integers on every input, while the class $\#\mathsf{PPA}$ contains more functions than that (as we will see when discussing PRELEAF). In fact, for that reason it makes sense to study the class $(\#\mathsf{PPA}(\textsc{Lonely})+1)/2$ and $(\#\mathsf{PPA}(\textsc{Lonely})-1)/2$ and ask if they are subsets of #P.

Aside from the classical problems we study slightly adjusted problems that are not equivalent via parsimonious reductions (see the detailed list in the full version). Each class is defined via parsimonious reductions to a complete problem. The naming prefixes #COUNTALL-PPA and #COUNTGAP are essentially flavor. By definition we have $\#\mathsf{PPA}(\mathrm{P}) \subseteq \#\mathsf{PPA}$ for all search problems $\mathrm{P} \in \mathsf{PPA}$, and analogously for all other search problems. The relativizing inclusions and oracle separations that we find are depicted in Figure 1. All equalities with #P are shown in the full version via relativizing parsimonious reductions. A solid arrow represents a relativizing parsimonious reduction. An arrow with a ⚠ represents a relativizing parsimonious reduction where there is an oracle separation in the other direction. This means that all classes that are above #P in the figure strictly contain #P (with respect to an oracle).

We find a surprisingly large number of counting problem classes that, if adjusted properly with "-1" and "$/2$" are *equal to* #P. This includes the canonical counting versions of PPAD, PPADS and CLS. Only after making slight changes to the problems via non-parsimonious polytime equivalences (similar to the *chessplayer algorithm*, see e.g. [Pap90], [BCE+98]), we obtain that the non-parsimonious counting classes strictly contain #P, which puts the new problems outside of #P.

[15]Note that the prefix PPA is actually superfluous in this case, but we keep it for clarity.

We identify two main "reasons" (i.e., oracle separations), one for "-1", and one for "$/2$". There are two versions of $\#\mathsf{PPA}$ at the top of the diagram, one for each of the two reasons, and they are not easily comparable.[16] It is also noteworthy that we know of no counting version of PPA, PLS or PPP that equals #P.[17]

Since the polynomials $x-1$, $\frac{x}{2}$, and $\frac{x-1}{2}$ are monotone, the tool to prove the separations is the Diagonalization Theorem. The main difference from all separations so far is that now the instances are much more involved. In the halving separation we have to "hide" the partner vertex from the #P machine, and in the decrementation separation we have to "hide" which of the solutions is connected to the zero vertex. This is especially difficult for $\#\mathsf{PLS}(\textsc{Iter})-1$ (and hence for $\#\mathsf{CLS}-1$).[18] We formalize our approach in the definition of a set-instantiator and create the necessary set-instantiators in the full version.

Even though we are mainly interested in membership and non-membership in #P, with only a little extra work our techniques directly give us another oracle separation $\#\mathsf{COUNTALL\text{-}PPA}(\textsc{Leaf})^A/2 \subsetneq \#\mathsf{COUNTGAP}(\textsc{BipartiteUnbalance})^A$. This is because after doubling we have $\#\mathsf{COUNTALL\text{-}PPA}(\textsc{Leaf})^A \subseteq \#\mathsf{P}^A$, while still $\#\mathsf{P}^A \subsetneq 2\#\mathsf{COUNTGAP}(\textsc{BipartiteUnbalance})^A$ (see the full version).

ACKNOWLEDGMENTS

We are grateful to Swee Hong Chan, Nikita Gladkov and Greta Panova for numerous helpful discussions and remarks on the subject. We thank Joshua Grochow and Greg Kuperberg for many inspiring conversations on computational complexity over the years. We learned about [HVW95] and [Bei97] only after the paper was written; we thank Lane Hemaspaandra who kindly for pointed out these references. We thank Markus Bläser and Paul Goldberg for helpful comments on a draft version of this paper. The anonymous reviewers pointed out typos and made very useful suggestions concerning the presentation, for which we are very grateful.

We are grateful to the Oberwolfach Research Institute for Mathematics where we started this project in the innocent times of February of 2020. The first author was partially supported by the DFG grant IK 116/2-1 and the EPSRC grant EP/W014882/1. The second author was partially supported by the NSF grant CCF-2007891.

REFERENCES

[Aar16] S. Aaronson, $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$, in *Open problems in mathematics*, Springer, Cham, 2016, 1–122.

[AD78] R. Ahlswede and D. E. Daykin, An inequality for the weights of two families of sets, their unions and intersections, *Z. Wahrsch. Verw. Gebiete* **43** (1978), 183–185.

[16]It is not even clear if $\#\mathsf{PPA}(\textsc{Leaf})-1$ is contained in $(\#\mathsf{PPA}(\textsc{Leaf})-1)/2$. One would want to just double a LEAF instance, but that will end up creating 2 leaves too many. In other words, the class $\#\mathsf{PPA}(\textsc{Leaf})-1$ seems to not be closed under the operation of scaling a function by 2.

[17]Note that since PTFNP (see [GP18]) contains CLS, the decrementation separation also shows $\#\mathsf{PTFNP}^A - 1 \not\subseteq \#\mathsf{P}^A$.

[18]Notably, PLS is also missing from the oracle separations in [BCE+98].

[AB09] S. Arora and B. Barak, *Computational complexity. A modern approach*, Cambridge Univ. Press, Cambridge, 2009, 579 pp.

[BCE+98] P. Beame, S. Cook, J. Edmonds, R. Impagliazzo and T. Pitassi, The relative complexity of NP search problems, in *Proc. 27th STOC* (1995), 303–314; *J. Comput. System Sci.* **57** (1998), 3–19.

[BB61] E. Beckenbach and R. Bellman, *Inequalities*, Springer, Berlin, 1961, 198 pp.

[Bei97] R. Beigel, Closure properties of GapP and #P, in *Proc. 5th Israeli Symposium on Theory of Computing and Systems* (1997), 144–146.

[BG92] R. Beigel and J. Gill, Counting classes: Thresholds, parity, mods, and fewness, in *Proc. 7th STACS* (1990), 49–57; *Theoret. Comput. Sci.* **103** (1992), 3–23.

[BG83] A. Blass and Yu. Gurevich, Equivalence relations, invariants, and normal forms. II, in *Symposium on Recursive Combinatorics*, Springer, Berlin, 1983, 24–42.

[BG84] A. Blass and Yu. Gurevich, Equivalence relations, invariants, and normal forms, *SIAM J. Comput.* **13** (1984), 682–689.

[Ble13] G. Blekherman, Nonnegative polynomials and sums of squares, in *Semidefinite optimization and convex algebraic geometry* (Edited by G. Blekherman, P. A. Parrilo and R. R. Thomas), SIAM, Philadelphia, PA, 2013, 159–202.

[BS01] B. Borchert and R. Silvestri, Dot operators, in *Proc. 12th CCC* (1997), 36–44; *Theoret. Comput. Sci.* **262** (2001), 501–523.

[BDO15] C. Bowman, M. De Visscher and R. Orellana, The partition algebra and the Kronecker coefficients, *Trans. AMS* **367** (2015), 3647–3667.

[BW91] G. Brightwell and P. Winkler, Counting linear extensions, in *Proc. 39th STOC* (1991), 175–181; *Order* **8** (1991), 225–247.

[Bri93] M. Brion, Stable properties of plethysm: on two conjectures of Foulkes, *Manuscripta Math.* **80** (1993), 347–371.

[BM04] J. Buresh-Oppenheim and T. Morioka, Relativized NP search problems and propositional proof systems, in *Proc. 19th CCC* (2004), 54–67.

[BI13b] P. Bürgisser and C. Ikenmeyer, Deciding positivity of Littlewood–Richardson coefficients, in *Proc. 21st FPSAC* (2009), 265–276; *SIAM J. Discrete Math.* **27** (2013), 1639–1681.

[BIP19] P. Bürgisser, C. Ikenmeyer and G. Panova, No occurrence obstructions in geometric complexity theory, in *Proc. 57th FOCS* (2016), 386–395; *Jour. AMS* **32** (2019), 163–193.

[CGH+89] J.-Yi Cai, T. Gundermann, J. Hartmanis, L. A. Hemachandra, V. Sewelson, K. Wagner and G. Wechsung, The Boolean hierarchy. II. Applications, *SIAM J. Comput.* **18** (1989), 95–111.

[Cam01] K. Cameron, Thomason's algorithm for finding a second Hamiltonian circuit through a given edge in a cubic graph is exponential on Krawczyk's graphs, *Discrete Math.* **235** (2001), 69–77.

[CW95] E. R. Canfield and S. G. Williamson, A loop-free algorithm for generating the linear extensions of a poset, *Order* **12** (1995), 57–75.

[CD09] Xi Chen and X. Deng, On the complexity of 2D discrete fixed point problem, in *Proc. 33rd ICALP* (2006), 489–500; *Theoret. Comput. Sci.* **410** (2009), 4448–4456.

[CIM17] M.-W. Cheung, C. Ikenmeyer and S. Mkrtchyan, Symmetrizing tableaux and the 5th case of the Foulkes conjecture, *J. Symbolic Comput.* **80** (2017), 833–843.

[Cur16] R. Curticapean, Parity separation: A scientifically proven method for permanent weight loss, in *Proc. 43rd ICALP* (2016), Art. 47, 14 pp.

[DGP09] C. Daskalakis, P. W. Goldberg and C. H. Papadimitriou, The complexity of computing a Nash equilibrium, in *Proc. 38th STOC* (2006), 71–78; *SIAM J. Comput.* **39** (2009), 195–259.

[DFHM22] A. Deligkas, J. Fearnley, A. Hollender and T. Melissourgos, Constant inapproximability for PPA, in *Proc. 54th STOC* (2022), to appear; `arXiv:2201.10011`.

[DEF+21] X. Deng, J. R. Edmonds, Z. Feng, Z. Liu, Qi Qi and Z. Xu, Understanding PPA-completeness, in *Proc. 31st CCC* (2016), Art. 23, 25 pp.; *J. Comput. System Sci.* **115** (2021), 146–168.

[FFK94] S. A. Fenner, L. Fortnow and S. A. Kurtz, Gap-definable counting classes, in *Proc. 6th CCC* (1991), 30–42; *J. Comput. System Sci.* **48** (1994), 116–148.

[FRH+20] A. Filos-Ratsikas, A. Hollender, K. Sotiraki and M. Zampetakis, Consensus-halving: Does it ever get easier?, in *Proc. 21st ACM-EC* (2020), 381–399.

[FRG18] A. Filos-Ratsikas and P. W. Goldberg, Consensus halving is PPA-complete, in *Proc. 50th STOC* (2018), 51–64.

[FI20] N. Fischer and C. Ikenmeyer, The computational complexity of plethysm coefficients, *Comput. Complexity* **29** (2020), no. 2, Paper 8, 43 pp.

[For97] L. Fortnow, Counting complexity, in *Complexity theory retrospective* II, Springer, New York, 1997, 81–107.

[For09] L. Fortnow, A simple proof of Toda's theorem, *Theory Comput.* **5** (2009), 135–140.

[FG11] L. Fortnow and J. A. Grochow, Complexity classes of equivalence problems revisited, *Inform. and Comput.* **209** (2011), 748–763.

[Ful98] W. Fulton, Eigenvalues of sums of Hermitian matrices (after A. Klyachko), *Astérisque* **252** (1998), No. 845, 255–269.

[God93] C. D. Godsil, *Algebraic combinatorics*, Chapman & Hall, New York, 1993, 362 pp.

[GH21] P. W. Goldberg and A. Hollender, The hairy ball problem is PPAD-complete, in *Proc. 46th ICALP* (2019), Art. 65, 14 pp.; *J. Comput. System Sci.* **122** (2021), 34–62.

[GP17] P. W. Goldberg and C. H. Papadimitriou, TFNP: an update, in *Algorithms and complexity*, Springer, Cham, 2017, 3–9.

[GP18] P. W. Goldberg and C. H. Papadimitriou, Towards a unified complexity theory of total functions, *J. Comput. System Sci.* **94** (2018), 167–192.

[Gol56] S. W. Golomb, Combinatorial Proof of Fermat's "Little" Theorem, *Amer. Math. Monthly* **63** (1956), no. 10, 718.

[Gre93] F. Green, On the power of deterministic reductions to $\mathrm{C}_{=}\mathrm{P}$, *Math. Systems Theory* **26** (1993), 215–233.

[Gri01] M. Grigni, A Sperner lemma complete for PPA, *Inform. Process. Lett.* **77** (2001), 255–259.

[Gri76] G. R. Grimmett, An upper bound for the number of spanning trees of a graph, *Discrete Math.* **16** (1976), 323–324.

[GS88] J. Grollmann and A. L. Selman, Complexity measures for public-key cryptosystems, in *Proc. 25th FOCS* (1984), 495–503; *SIAM J. Comput.* **17** (1988), 309–335.

[Gup95] S. Gupta, Closure properties and witness reduction, *J. Comput. System Sci.* **50** (1995), 412–432.

[GW87] T. Gundermann and G. Wechsung, Counting classes with finite acceptance types, *Comput. Artificial Intelligence* **6** (1987), 395–409.

[Har40] G. H. Hardy, *Ramanujan. Twelve lectures on subjects suggested by his life and work*, Cambridge Univ. Press, Cambridge, UK, 1940, 236 pp.

[HLP52] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities* (Second ed.), Cambridge Univ. Press, 1952, 324 pp.

[HL72] O. J. Heilmann and E. H. Lieb, Theory of monomer-dimer systems, *Comm. Math. Phys.* **25** (1972), 190–243.

[HO02] L. A. Hemaspaandra and M. Ogiwara, *The complexity theory companion*, Springer, Berlin, 2002, 369 pp.

[HR00] L. A. Hemaspaandra and J. Rothe, A second step towards complexity-theoretic analogs of Rice's theorem, in *Proc. 23rd MFCS* (1998), 418–426; *Theoret. Comput. Sci.* **244** (2000), 205–217.

[HV95] L. A. Hemaspaandra and H. Vollmer, The satanic notations: counting classes beyond #P and other definitional adventures, *SIGACT News* **26** (1995), no. 1, 2–13.

[HVW95] U. Hertrampf, H. Vollmer and K. Wagner, On the power of number-theoretic operations with respect to counting, in *Proc. 10th CCC* (1995), 299–314.

[HT03] C. M. Homan and M. Thakur, One-way permutations and self-witnessing languages, in *Proc. 2nd IFIP TCS* (2002), 243–254; *J. Comput. System Sci.* **67** (2003), 608–622.

[IMW17] C. Ikenmeyer, K. D. Mulmuley and M. Walter, On vanishing of Kronecker coefficients, *Comput. Complexity* **26** (2017), 949–992.

[Ike16] C. Ikenmeyer, Small Littlewood–Richardson coefficients, *J. Algebraic Cominatorics* **44** (2016), 1–29.

[IP17] C. Ikenmeyer and G. Panova, Rectangular Kronecker coefficients and plethysms in geometric complexity theory, in *Proc. 57th FOCS* (2016), 396–405; *Adv. Math.* **319** (2017), 40–66.

[IR82] K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, Springer, New York, 1982, 341 pp.

[Jeř16] E. Jeřábek, Integer factoring and modular square roots, *J. Comput. System Sci.* **82** (2016), 380–394.

[KM18] T. Kahle and M. Michałek, Obstructions to combinatorial formulas for plethysm, *Electron. J. Combin.* **25** (2018), no. 1, Paper 1.41, 9 pp.

[KVVY93] R. Kannan, H. Venkateswaran, V. Vinay and A. C. Yao, A circuit-based proof of Toda's theorem, *Inform. and Comput.* **104** (1993), 271–276.

[Kle66] D. J. Kleitman, Families of non-disjoint subsets, *J. Combin. Theory* **1** (1966), 153–155.

[Kly98] A. A. Klyachko, Stable bundles, representation theory and Hermitian operators, *Selecta Math.* **4** (1998), 419–445.

[Knu16] A. Knutson, Schubert calculus and puzzles, in *Schubert calculus*, Math. Soc. Japan, Tokyo, 2016, 185–209.

[KT99] A. Knutson and T. Tao, The honeycomb model of $\mathrm{GL}_n(\mathbb{C})$ tensor products I: Proof of the saturation conjecture, *Jour. AMS* **12** (1999), 1055–1090.

[KZ20] A. Knutson and P. Zinn-Justin, Schubert puzzles and integrability I: Invariant trilinear forms, preprint (2020), 51 pp.; arXiv:1706.10019v6.

[Ko85] K.-I. Ko, On some natural complete operators, *Theoret. Comp. Sci.* **37** (1985), 1–30.

[Kra96] C. Krattenthaler, Combinatorial proof of the log-concavity of the sequence of matching numbers, *J. Combin. Theory Ser. A* **74** (1996), 351–354.

[Kra99] A. Krawczyk, The complexity of finding a second Hamiltonian cycle in cubic graphs, *J. Comput. System Sci.* **58** (1999), 641–647.

[Lan15] J. M. Landsberg, Geometric complexity theory: an introduction for geometers, *Ann. Univ. Ferrara Sez. VII Sci. Mat.* **61** (2015), 65–117.

[LS82] A. Lascoux and M.-P. Schützenberger, Polynômes de Schubert (in French), *C. R. Acad. Sci. Paris Sér I, Math.* **294** (1982), 447–450.

[LR34] D. E. Littlewood and A. R. Richardson, Group characters and algebra, *Phil. Trans. Royal Soc. London, Ser. A* **233** (1934), 99–141.

[Loe11] N. A. Loehr, *Bijective combinatorics*, CRC Press, Boca Raton, FL, 2011, 590 pp.

[Mac91] I. G. Macdonald, *Notes on Schubert polynomials*, Publ. LaCIM, UQAM, Montreal, 1991, 116 pp.

[Mac95] I. G. Macdonald, *Symmetric functions and Hall polynomials* (Second ed.), Oxford U. Press, New York, 1995, 475 pp.

[Man01] L. Manivel, *Symmetric functions, Schubert polynomials and degeneracy loci*, SMF/AMS, Providence, RI, 2001, 167 pp.

[MSS13] A. Marcus, D. A. Spielman and N. Srivastava, Interlacing families I: Bipartite Ramanujan graphs of all degrees, in *Proc. 54th FOCS* (2013), 529–537; *Ann. of Math.* **182** (2015), 307–325.

[Mar08] M. Marshall, *Positive polynomials and sums of squares*, AMS, Providence, RI, 2008, 187 pp.

[MPP14] K. Mészáros, G. Panova and A. Postnikov, Schur times Schubert via the Fomin–Kirillov algebra, *Electron. J. Combin.* **21** (2014), no. 1, Paper 1.39, 22 pp.

[MM11] C. Moore and S. Mertens, *The nature of computation*, Oxford Univ. Press, Oxford, 2011, 985 pp.

[Mul07] K. D. Mulmuley, Geometric Complexity Theory VII: Nonstandard quantum group for the plethysm problem, preprint (2007), 59 pp.; arXiv:0709.0749.

[Mul09] K. D. Mulmuley, Geometric Complexity Theory VI: The flip via saturated and positive integer programming in representation theory and algebraic geometry, preprint (2009), 139 pp.; arXiv:0704.0229v4.

[MNS12] K. D. Mulmuley, H. Narayanan and M. Sohoni, Geometric Complexity Theory III: On Deciding Positivity of Littlewood–Richardson Coefficients, *J. Algebraic Cominatorics* **36** (2012), 103–110.

[Mur38] F. D. Murnaghan, The analysis of the direct product of irreducible representations of the symmetric groups, *Amer. J. Math.* **60** (1938), 44–65.

[Nag19] T. Nagell, Über zahlentheoretische Polynome (in German), *Norsk. Mat. Tidsskr* **1** (1919), 14–23; available at https://www.math.ucla.edu/~pak/hidden/papers/Nagel-Uber_zahlentheoretische_Polynome-1919.pdf

[Noy14] M. Noy, Random planar graphs and beyond, in *Proc. ICM Seoul*, Vol. IV, 2014, 407–430.

[OH93] M. Ogiwara and L. A. Hemachandra, A complexity theory for feasible closure properties, in *Proc. 6th CCC* (1991), 16–29; *J. Comput. System Sci.* **46** (1993), 295–325.

[Pak03] I. Pak, Tile invariants: new horizons, *Theoret. Comput. Sci.* **303** (2003), 303–331.

[Pak06] I. Pak, Partition bijections, a survey, *Ramanujan J.* **12** (2006), 5–75.

[Pak18] I. Pak, Complexity problems in enumerative combinatorics, in *Proc. ICM Rio de Janeiro*, Vol. IV, World Sci., Hackensack, NJ, 2018, 3153–3180; an expanded version of the paper is available at arXiv:1803.06636

[Pak19] I. Pak, Combinatorial inequalities, *Notices AMS* **66** (2019), 1109–1112; an expanded version of the paper is available at https://www.math.ucla.edu/~pak/papers/full-story1.pdf

[PP17] I. Pak and G. Panova, On the complexity of computing Kronecker coefficients, *Computational Complexity* **26** (2017), 1–36.

[PPY19] I. Pak, G. Panova and D. Yeliussizov, On the largest Kronecker and Littlewood–Richardson coefficients, *J. Combin. Theory, Ser. A* **165** (2019), 44–77.

[Pap90] C. H. Papadimitriou, On graph-theoretic lemmata and complexity classes, in *Proc. 31st FOCS* (1990), 794–801.

[Pap94a] C. H. Papadimitriou, On the complexity of the parity argument and other inefficient proofs of existence, *J. Comput. System Sci.* **48** (1994), 498–532.

[Pap94b] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley, Reading, MA, 1994, 523 pp.

[Pet72] J. Peterson, Beviser for Wilsons og Fermats Theoremer (in Danish, Proofs of the theorems of Wilson and Fermat), *Tidsskr. Math.* **2** (1872), 64–65.

[Pri77] W. L. Price, A topological transformation algorithm which relates the Hamiltonian circuits of a cubic planar map, *J. London Math. Soc.* **15** (1977), 193–196.

[Sch15] G. Schaeffer, Planar maps, in *Handbook of enumerative combinatorics*, CRC Press, Boca Raton, FL, 2015, 335–395.

[Spe11] D. E Speyer, How can I show a GapP problem is outside #P?, CSTheoryStackExchange (2011); cstheory.stackexchange.com/q/8178/

[Sta00] R. P. Stanley, Positivity problems and conjectures in algebraic combinatorics, in *Mathematics: frontiers and perspectives*, AMS, Providence, RI, 2000, 295–319.

[Sta12] R. P. Stanley, *Enumerative Combinatorics*, vol. 1 (Second ed.) and vol. 2, Cambridge Univ. Press, 2012 and 1999, 626 pp. and 581 pp.

[SW86] D. Stanton and D. White, *Constructive combinatorics*, Springer, New York, 1986, 183 pp.

[Syl82] J. J. Sylvester, A constructive theory of partitions, arranged in three acts, an interact and an exodion, *Amer. J. Math.* **5** (1882), 251–330.

[Tar91] J. Tarui, Randomized polynomials, threshold circuits, and the polynomial hierarchy, in *Proc. 8th STACS* (1991), 238–250.

[Tho78] A. G. Thomason, Hamiltonian cycles and uniquely edge colourable graphs, *Ann. Discrete Math.* **3** (1978), 259–268.

[Toda91] S. Toda, PP is as hard as the polynomial-time hierarchy, *SIAM J. Comput.* **20** (1991), 865–877.

[Tut46] W. T. Tutte, On Hamiltonian circuits, *J. London Math. Soc.* **21** (1946), 98–101.

[Tut63] W. T. Tutte, A census of planar maps, *Canadian J. Math.* **15** (1963), 249–271.

[Val76] L. G. Valiant, Relative complexity of checking and evaluating, *Inf. Process. Lett.* **5** (1976), 20–23.

[Val79] L. G. Valiant, The complexity of computing the permanent, *Theor. Comput. Sci.* **8** (1979), 189–201.

[VV85] L. G. Valiant and V. V. Vazirani, NP is as easy as detecting unique solutions, in *Proc. 7th STOC* (1985), 458–463; *Theoret. Comput. Sci.* **47** (1986), 85–93.

[Vie16] X. G. Viennot, *The Art of Bijective Combinatorics*, a video-book (2016); viennot.org/abjc.html

[Wig19] A. Wigderson, *Mathematics and computation*, Princeton Univ. Press, Princeton, NJ, 2019, 418 pp.

[Wor18] N. Wormald, Asymptotic enumeration of graphs with given degree sequence, in *Proc. ICM Rio de Janeiro*, Vol. 3, 2018, 3229–3248.