Solving Linear Inequalities over Convex Sets & its Applications to Cryptography and Hydrodynamics

Saugata Basu Hamidreza Amini Khorasgani Hemanta K. Maji
Hai H. Nguyen

December 18, 2024

Abstract

Is a two-party function, possibly with randomized output, securely computable? We give a finite procedure to answer this question, settling this foundational three-decade-old open problem in secure computation and information complexity.

Beaver-Chor-Kushilevitz [CK89, Kus89, Bea89] answered this question for deterministic output functions. Basu et al. [BKMN22] recently gave a geometric characterization of randomized functions securely computable with bounded communication complexity. Randomized functions can have arbitrarily high communication complexity, even for fixed input-output sets [BKMN23]. Without an upper bound on the communication complexity, the decidability of the question, whether a given two-party function with randomized output is securely computable, was a formidable challenge.

We reduce answering this question to proving specific lamination hulls are semi-algebraic. Lamination hulls are an infinite union of recursively defined sets independently motivated by the hydrodynamics literature. We connect this technical objective to solving a system of linear inequalities over convex sets in high dimensions, where inequalities represent the natural containment relation. We present a Gaussian elimination-inspired algorithm to compute the smallest simultaneous solutions to such systems. After that, using these solutions, we prove that our lamination hulls are semi-algebraic.

Our technical solution introduces a novel set operator called *positive geometric join*. In our application context, it characterizes algebraically well-behaved sets that generalize polytopes, which we call *hemihedra*. The positive geometric join operator and hemihedral sets should interest the broader mathematics and computer science community.

Contents

1 Introduction

This work settles a long-standing open problem in the foundations of cryptography. To achieve this, we develop new mathematical tools to solve systems of inequalities involving convex shapes in high dimensions. The first is a new set operator that systematically reduces any system into its "reduced row-echelon form." After that, we identify well-behaved convex sets to characterize the minimal solutions to such linear systems with respect to the partial order induced by inclusion. Consequently, we show that certain classes of lamination hulls are semi-algebraic, resolving in these cases an open problem in the study of lamination hulls, an important geometric object of interest in the study of partial differential equations. These advancements should help further information complexity investigations in general through the recently established connection by Basu et al. [BKMN22].

Cryptographic application. Secure multi-party computation helps compute using sensitive data. Consider the two-party information-theoretic setting with honest but curious adversaries: Alice and Bob want to securely evaluate a function $f\colon X \times Y \to \mathbb{R}^Z$ of their private inputs. Here, $f(x,y)_z$ is the output probability of $z \in Z$ when Alice and Bob have inputs $x \in X$ and $y \in Y$, respectively. (Note that we consider real-valued functions f, and our model of computation is the Blum-Shub-Smale model [BSS89].)

Cryptographic question: Is there a secure protocol for the function $f\colon X \times Y \to \mathbb{R}^Z$?

Beaver-Chor-Kushilevitz [CK89, Kus89, Bea89] answered this question for deterministic functions – functions whose inputs fix the output. In its full generality, where output is randomized, this foundational question has remained open for over three decades; c.f. [MPR13]. Investigating the information complexity of private-coin protocols at the interface of security and information complexity has been challenging in general [Bra21, Wei15]. Recently, Basu et al. [BKMN22] made partial progress; they answered it when protocols are restricted to a communication budget. However, the communication complexity of secure protocols could be arbitrarily high even for small domains like $X = Y = \{0,1\}$ and $Z = \{1,2,3,4,5\}$ [BKMN23].

This work presents a finite procedure to answer the cryptographic question posed above.

Note that if a secure protocol exists for computing a given function f, then using the main result in Basu et al. [BKMN22] one can find it. The main technical challenge is to decide whether such a protocol exists; i.e., to reject the no instances. (This is similar to the well-known *halting problem* for Turing machines which is recursively enumerable but not recursive.) In this paper, we give a finite procedure to decide the existence of a secure protocol for computing any given function.

Lamination hulls. Lamination hulls are geometric objects that arise naturally in our procedure to answer the cryptographic question discussed above. Lamination hulls are subsets of $\mathbb{R}^d$ and are parameterized by a set $\Lambda \subseteq \mathbb{R}^d$. Beginning with an initial set $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^d$, recursively define the following sets for $i \in \{0,1,2,\dots\}$.

$$\mathcal{S}^{(i+1,\Lambda)} := \left\{ \alpha \cdot P + (1-\alpha)\cdot P' \ : \ P, P' \in \mathcal{S}^{(i,\Lambda)}, \alpha \in [0,1], \text{ and } P - P' \in \Lambda \right\}. \tag{1}$$

The following set is the *lamination hull* of $\mathcal{S}^{(0,\Lambda)}$.

$$\mathcal{S}^{(\infty,\Lambda)} := \bigcup_{i \in \{0,1,2,\dots\}} \mathcal{S}^{(i,\Lambda)}. \tag{2}$$

Figure 1 illustrates the evolution of the lamination hull with an example.

Lamination hulls appear naturally in many applications, for example in modeling interaction between agents [BKMN22]. When $\Lambda = \mathbb{R}^d$, the lamination hull is the convex hull of the initial set. With other choices of Λ, lamination hulls play a role in computing the stationary solutions to the differential equations underlying incompressible porous media [CG07, DLSJ09, CFG11, HL21]. *Computing descriptions of lamination hull was posed as an open problem at the Oberwolfach Workshop on "New Directions in Real Algebraic Geometry" [BKNV23, Page 20].* Our paper will prove that the hull $\mathcal{S}^{(\infty,\Lambda)}$ is semi-algebraic for a specific Λ (semi-algebraic sets are defined in Section 1.1). This result will, in turn, answer the cryptographic question due to their connection established in [BKMN22].

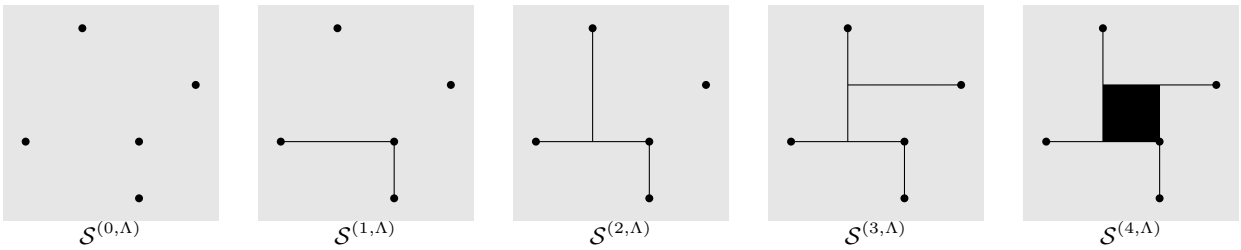


Figure 1: 2D Tartar square. Consider $\Lambda := \mathbb{R} \times \{0\} \bigcup \{0\} \times \mathbb{R} \subseteq \mathbb{R}^2$. The figure illustrates the evolution of the sets $\mathcal{S}^{(0,\Lambda)} \to \mathcal{S}^{(1,\Lambda)} \to \cdots$. This specific Λ ensures that, for any two axis-aligned points $P, P' \in \mathcal{S}^{(i,\Lambda)}$, the line segment $\overline{PP'}$ is added to the set $\mathcal{S}^{(i+1,\Lambda)}$. These sets stabilize $\mathcal{S}^{(i,\Lambda)} = \mathcal{S}^{(4,\Lambda)}$, for all $i \in \{4, 5, \dots\}$. For this example, the lamination hull $\mathcal{S}^{(\infty,\Lambda)} = \mathcal{S}^{(4,\Lambda)}$.

Connecting lamination hulls and the cryptographic application. We denote the cardinality of a set S by $\text{card}(S)$. Let X, Y, Z be finite sets, and let $\Lambda^* \subset \mathbb{R}^{\text{card}(X)+\text{card}(Y)+\text{card}(Z)}$ be defined as follows.

$$\Lambda^* := \mathbb{R}^{\text{card}(X)} \times \{0\}^{\text{card}(Y)} \times \mathbb{R}^{\text{card}(Z)} \bigcup \{0\}^{\text{card}(X)} \times \mathbb{R}^{\text{card}(Y)} \times \mathbb{R}^{\text{card}(Z)}. \tag{3}$$

Basu et al. [BKMN22] proved that for any given function $f\colon X \times Y \to \mathbb{R}^Z$, there exists (an effectively computable) point $Q(f) \in \mathbb{R}^{\text{card}(X)+\text{card}(Y)+\text{card}(Z)}$, such that f has a c-bit secure protocol if and only if $Q(f) \in \mathcal{S}^{(c,\Lambda^*)}$, for some appropriately defined initial set $\mathcal{S}^{(0,\Lambda^*)}$.

Therefore, to answer our cryptographic question, it suffices to test the membership of the query point $Q(f)$ in the lamination hull $\mathcal{S}^{(\infty,\Lambda^*)}$ defined in Equation 2.

1.1 Our Contributions

We prove the following technical result.

Theorem 1 (Answering Membership Queries in Lamination Hull)**.** *Fix arbitrary $a, b \in \{1, 2, \dots\}$ and $c \in \{0, 1, 2, \dots\}$, and define*

$$\Lambda := \mathbb{R}^a \times \{0\}^b \times \mathbb{R}^c \bigcup \{0\}^a \times \mathbb{R}^b \times \mathbb{R}^c.$$

Consider any finite initial set of points $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^{a+b+c}$ and a query point $Q \in \mathbb{R}^{a+b+c}$. Figure 3 presents a finite procedure determining the membership of $Q \in \mathcal{S}^{(\infty,\Lambda)}$.

The recursive construction of Equation 1 for this specific parameter Λ adds any convex-linear combination of any two points P and P' if (and only if) their first a coordinates or the following b coordinates are identical. Two corollaries of this technical theorem are immediate.

A subset $S \subseteq \mathbb{R}^d$ is a *semi-algebraic set* if S is a finite union of sets defined by a finite number of polynomial equations and inequalities (also called basic semi-algebraic sets).

Corollary 1 (Lamination Hull is Semi-algebraic)**.** *Fix arbitrary $a, b \in \{1, 2, \dots\}$, $c \in \{0, 1, 2, \dots\}$, and define $\Lambda := \mathbb{R}^a \times \{0\}^b \times \mathbb{R}^c \bigcup \{0\}^a \times \mathbb{R}^b \times \mathbb{R}^c$. For any finite initial set of points $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^{a+b+c}$, the lamination hull $\mathcal{S}^{(\infty,\Lambda)}$ is a semi-algebraic set.*

Computing the lamination hull for general Λ is an open problem; in particular, it was also open for the specific Λ considered in Corollary 1.

Proof of Corollary 1. Each procedure step in Figure 3 is either computing a polynomial or branching according to a sign of a polynomial already computed. This procedure is a computation tree testing membership in the lamination hull. Since the tree is finite, each path to a leaf node corresponds to a basic semi-algebraic set. There are only finitely many leaves, so the lamination hull is a union of finitely many basic semi-algebraic sets. Therefore, it is semi-algebraic. □

Corollary 2 (Secure Protocols for Functions)**.** *Given any randomized output function $f\colon X \times Y \to \mathbb{R}^Z$, a finite procedure can determine if it has a secure protocol. If such a protocol exists, it constructs one with the minimum communication complexity. Otherwise, it presents an obstruction to security.*

The time complexity of our membership algorithm is an elementary recursive function of $\mathrm{card}(X) + \mathrm{card}(Y) + \mathrm{card}(Z)$; optimizing it isn't the focus of this work and is left as an open research direction. In the cryptographic application, as is the convention in that line of work, the input-output sets have constant size, so our procedure's running time is (an enormous) constant.

Proof of Corollary 2. Consider a two-party randomized output function $f\colon X \times Y \to \mathbb{R}^Z$. If f has Kilian's obstruction [Kil00], then f does not have a secure protocol. Henceforth, assume that f does not have Kilian's obstruction. In this case, Basu et al. [BKMN22] constructed a point $Q(f) \in \mathbb{R}^{a+b+c}$ [BKMN22, Equation 7], where $a = \mathrm{card}(X)$, $b = \mathrm{card}(Y)$, and $c = \mathrm{card}(Z)$, and an initial set $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^{a+b+c}$ [BKMN22, Equation 5], where $\Lambda := \mathbb{R}^a \times \{0\}^b \times \mathbb{R}^c \bigcup \{0\}^a \times \mathbb{R}^b \times \mathbb{R}^c$. They proved that f has a secure protocol with communication complexity (at most) $c \in \{0, 1, 2, \dots\}$, if (and only if) $Q(f) \in \mathcal{S}^{(c,\Lambda)}$. Therefore, f has a secure protocol if (and only if) $Q(f) \in \mathcal{S}^{(\infty,\Lambda)} := \bigcup_{i \geqslant 0} \mathcal{S}^{(i,\Lambda)}$; Theorem 1 gives a procedure to test this membership. Consider the case when the query point $Q(f)$ is outside the lamination hull. In that case, there is no secure protocol, and the description of the lamination hull and the query point certifies the obstruction to security. On the other hand, if the query point is inside the lamination hull, then iterate over $c \in \{0, 1, 2, \dots\}$ and identify the minimum communication complexity protocol for f using Basu et al. [BKMN22, Theorem 2]. □

Summary of our technical contributions. We introduce far-reaching generalizations of techniques to *solve systems of linear inequalities over the semi-ring of arbitrary convex subsets*. Our cryptographic applications need an accurate estimate of the solutions to these systems. Existing techniques would significantly overestimate their solutions, which leads to mistaking insecure functions as secure – a catastrophic blunder.

For example, when solutions are restricted to polytopes,[1] the cancellation law for the semi-ring of polytopes can recover the smallest one for a system with one unknown.[2] However, solutions to some systems modeling our application scenarios are not polytopes [BKMN23]; apriori, *they need not even be tame* (like semi-algebraic sets). Iterative techniques in formal languages (such as those in [KS86, SS78]) have investigated the evolution of recursively constructed systems in the limit. Taking the limit introduces spurious points in the solution, which, again, overestimates the solutions.

We introduce a new set operator to address these shortcomings: the *positive geometric join* of two sets. This operator allows for accurately and succinctly representing the smallest solution of a system of inequalities (in several unknowns) and reasoning about them. We develop a Gaussian elimination-inspired algebraic technique to incrementally simplify the system of inequalities while preserving their smallest solution. After performing these simplifications, the algebraic representation of the smallest solution becomes obvious. In our applications, these solutions have a special structure; they are convex sets expressible as the finite unions of the relative interiors of polytopes (see Figure 16 for examples), which we call *hemihedra*.

1.2 Proof Overview of Theorem 1

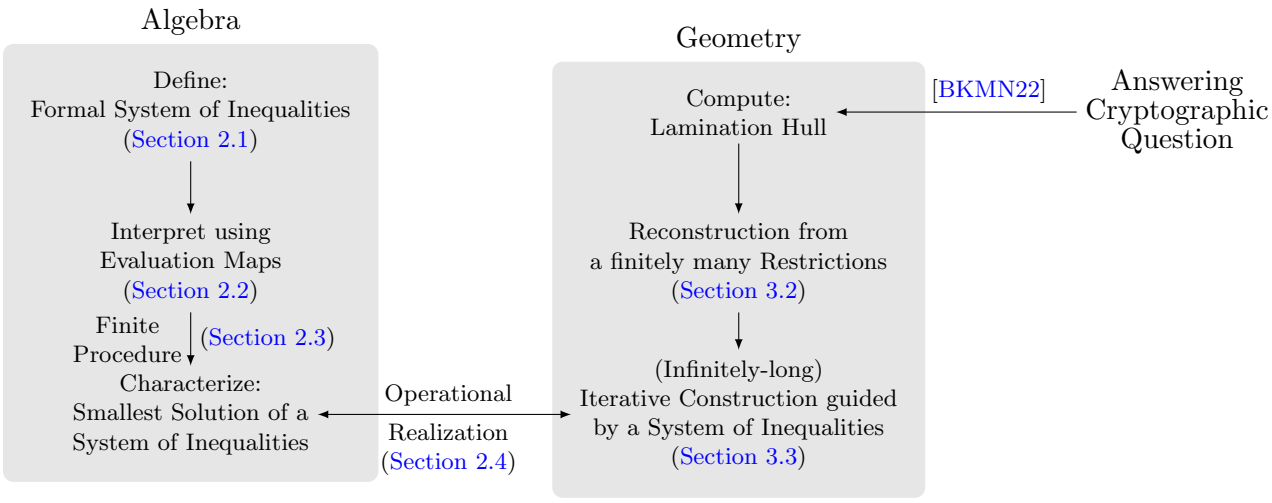


Figure 2: High-level overview of our work. [BKMN22] reduced the cryptographic question to a specific lamination hull computation; the rest is this work's contribution.

This presentation below is a (very) high-level overview of the technical ingredients of proving Theorem 1; use Figure 1.2 for reference. To begin, we identify finitely many *grid points* $\mathcal{G} \subseteq \mathbb{R}^a \times \mathbb{R}^b$. Instead of reconstructing the entire lamination hull $\mathcal{S}^{(\infty,\Lambda)}$, our strategy is to compute the restriction of the lamination hull to these grid points. For any grid point $g \in \mathcal{G}$, define the restriction

$$\mathcal{S}^{(\infty,\Lambda)}\Big|_g \coloneqq \left\{ (g, w) \in \mathcal{S}^{(\infty,\Lambda)} \right\}. \tag{4}$$

[1] A polytope is the convex hull of a finite number of points [Grü03].

[2] The cancellation law for polytopes states that for any two polytopes X and A and $0 < \rho < 1$, $X \supseteq \rho \cdot X + (1-\rho) \cdot A$, if and only if $X \supseteq A$. [jh].

We prove a *structural lemma* (Lemma 3) to determine the membership $Q \in \mathcal{S}^{(\infty,\Lambda)}$ from these finitely many restrictions

$$\left\{ \mathcal{S}^{(\infty,\Lambda)}\big|_g \ : \ g \in \mathcal{G} \right\}. \tag{5}$$

First, we prove that these restrictions $\mathcal{S}^{(\infty,\Lambda)}\big|_g$, where $g \in \mathcal{G}$, are convex sets. Next, to compute them, we introduce unknowns X_g for each grid point $g \in \mathcal{G}$, where each unknown represents a *convex set* in $\mathbb{R}^{a+b+c}$. Next, Section 3.3 defines a system $\mathcal{I}$ of linear inequalities involving these unknowns using the natural containment relationship among convex sets. For example, the linear inequality

$$X_g \supseteq \frac{1}{3} \cdot X_{g'} + \frac{2}{3} \cdot A$$

represents the semantics that "the convex set X_g contains the Minkowski sum of the convex set $\frac{1}{3} \cdot X_{g'}$ and the polytope $\frac{2}{3} \cdot A$." Here, X_g and $X_{g'}$ are unknowns representing convex subsets, and A is a polytope (to be thought of as a constant). Suppose $\left(X_g^{(*)} \ : \ g \in \mathcal{G} \right)$ is the *smallest simultaneous solution* to this system $\mathcal{I}$ of inequalities. Then, we prove that $\mathcal{S}^{(\infty,\Lambda)}\big|_g = X_g^{(*)}$, for all $g \in \mathcal{G}$, see Lemma 4.

Finally, we present a procedure for finding the smallest simultaneous solution of *any system of inequalities* – the technical workhorse of our work. We present a Gaussian elimination-inspired algorithm that outputs an algebraic expression for the smallest solution of any system of inequalities. These smallest solutions are certainly not polytopes (see the example in Appendix K). In fact, at the outset, it is unclear that the smallest solutions should even be semi-algebraic. *What type of convex sets are they?*

To this end, we introduce *positive geometric join*, an operation on two sets A and B that contains all the relative interiors of line segments $\overline{ab}$, where $a \in A$ and $b \in B$. For finite A and B, which is the case in the cryptographic application, the smallest solution is expressible as the finite unions of positive geometric joins of sets; we call such a set *hemihedron*. In particular, hemihedral sets are semi-algebraic.

1. Determine the grid points $\mathcal{G} \subseteq \mathbb{R}^{a+b}$ from the initial set of points $\mathcal{S}^{(0,\Lambda)} \subseteq \mathbb{R}^{a+b+c}$ using Equation 18.
2. Construct the appropriate system of linear inequalities $\mathcal{I}$ with unknowns $\{X_g \colon g \in \mathcal{G}\}$ as presented in Figure 8.
3. Theorem 2 computes the smallest simultaneous solution $\left(X_g^{(*)} \colon g \in \mathcal{G}\right)$ for the linear system of inequalities $\mathcal{I}$ using the procedure in Figure 4.
4. Define the restrictions $\mathcal{S}^{(\infty,\Lambda)}\big|_g \coloneqq X_g^{(*)}$ for every grid point $g \in \mathcal{G}$.
5. The structural lemma (Lemma 3) determines the membership $Q \in \mathcal{S}^{(\infty,\Lambda)}$ from the restrictions $\left\{ \mathcal{S}^{(\infty,\Lambda)}\big|_g : g \in \mathcal{G} \right\}$.

Figure 3: Algorithm for determining the membership of Q in the lamination hull $\mathcal{S}^{(\infty,\Lambda)}$.

Appendix J estimates the run-time of the algorithm in Figure 3. In particular, Equation 41 presents the running time to answer the cryptographic question.

2 Solving System of Linear Inequalities over the Semi-Ring of Convex Sets

Overview. This section will introduce *systems of inequalities involving formal symbols* (see Section 2.1). These inequalities will be interpreted using an *evaluation map* introduced in Section 2.2; the inequalities will correspond to containment relationships between subsets of $\mathbb{R}^d$ under this map. Under any evaluation map, our objective will be to identify the *smallest solutions of a system* – smallest w.r.t. the containment relationship among sets produced by that evaluation map. To that end, Section 2.3 will present a general *Gaussian elimination-inspired algebraic technique* to formally transform a system of inequalities while preserving its smallest solution under any evaluation map. After completing the transformation, the smallest solution will be easily characterized. Finally, Section 2.4 will present an *operational realization* of the smallest solution targeting applications, including the ones in mathematics and cryptography considered in this work. The entire presentation will include a working example to illustrate the abstractions concretely.

The formal algebra and the evaluation maps will involve four set operations. The first three are the standard *scalar multiplication*, *Minkowski sum*, and *union* operators. The fourth one, namely, *positive geometric join*, defined in Equation 10, is our work's contribution, including the conceptualization, definition, and recognition of its central role in solving this problem. This operator is necessary for succinctly and accurately capturing the smallest solution, even if the system itself could be specified without this operation. Furthermore, this operation facilitates reasoning about the properties of these systems during transformations.

2.1 Notation: System of Inequalities

The set of all formal symbols is $\Omega \coloneqq \{X_1, \ldots, X_n, P_1, \ldots, P_t\}$. Here $X_1, X_2, \ldots, X_n$ are *unknowns* and $P_1, P_2, \ldots, P_t$ are *constants*. The set of all *convex linear combinations* of Ω is denoted by:

$$\mathrm{CL}(\Omega) \coloneqq \left\{ \sum_{\omega \in \Omega} \lambda_\omega \cdot \omega \; : \; \text{for } \omega \in \Omega, \lambda_\omega \geqslant 0 \text{ and } \sum_{\omega \in \Omega} \lambda_\omega = 1 \right\}. \tag{6}$$

The "+" symbol above will represent the Minkowski sum operator, and the "$\cdot$" symbol will represent the scaling operator.

A *monomial* M over $\mathrm{CL}(\Omega)$ is $E_1 \mathbin{\mathring{\star}} E_2 \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} E_k$, where $k \in \{1, 2, \ldots\}$ and $E_1, E_2, \ldots, E_k \in \mathrm{CL}(\Omega)$. The "$\mathring{\star}$" symbol will represent the positive geometric join operator (see Equation 10 below). Furthermore, the set of elements $\mathrm{supp}(M) \coloneqq \{E_1, E_2, \ldots, E_k\}$ is the monomial M's *support*, and its degree $\deg(M) \coloneqq k$.

A *polynomial* φ over $\mathrm{CL}(\Omega)$ is either $\emptyset$ or $M_1 \oplus M_2 \oplus \cdots M_k$, for $k \in \{1, 2, \ldots\}$ and monomials $M_1, M_2, \ldots, M_k$ over $\mathrm{CL}(\Omega)$. Here, the "$\oplus$" symbol will represent the union operator. The set of all monomials of a polynomial $\mathrm{mono}(\varphi) \coloneqq \{M_1, M_2, \ldots, M_k\}$. For the $\varphi = \emptyset$ polynomial, $\mathrm{mono}(\varphi) \coloneqq \emptyset$. For example, the following identity holds for any polynomial φ.

$$\varphi = \bigoplus_{M \in \mathrm{mono}(\varphi)} \; \mathring{\bigstar}_{E \in \mathrm{supp}(M)} E.$$

A *system of inequalities* is a collection $\{X_i \geqslant \varphi_i\}_{i=1}^n$, where $\varphi_1, \varphi_2, \ldots, \varphi_n$ are polynomials over $\mathrm{CL}(\Omega)$. The "$\geqslant$" symbol will represent the set containment relation.

Working example. We will use a concrete example to illustrate the concepts (as they appear) in this section. Consider $n = 2$ and $t = 4$. In this case, the set of formal symbols is $\Omega = \{X_1, X_2, P_1, P_2, P_3, P_4\}$. Consider the following system of equations.

$$X_1 \geqslant P_1 \ \oplus \ X_1 \overset{\circ}{\star} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)$$
$$X_2 \geqslant P_2 \ \oplus \ X_2 \overset{\circ}{\star} \left(\frac{1}{2}\cdot X_1 + \frac{1}{2}\cdot P_4\right)$$

The semantics of these equations and their properties are investigated under an "evaluation map" introduced in Section 2.2 below; it will assign subsets of $\mathbb{R}^d$ to these formal objects.

2.2 Evaluation Map

We will assign subsets of $\mathbb{R}^d$, where $d \in \{1, 2, \dots\}$, to the formal symbols in Ω. Under this assignment, the sequel defines how to evaluate polynomials. To begin, for two sets $A, B \subseteq \mathbb{R}^d$ and $0 < \rho \leqslant 1$, define the following set operators.

$$\begin{aligned}
\text{Scaling:} \quad & \rho \cdot A \ \coloneqq \ \{\rho \cdot x \ : \ x \in A\} && (7)\\
\text{Minkowski sum:} \quad & A + B \ \coloneqq \ \{a + b \ : \ a \in A, b \in B\} && (8)\\
\text{Union:} \quad & A \oplus B \ \coloneqq \ \{x \ : \ x \in A \text{ or } x \in B\} && (9)\\
\text{Positive Geometric Join:} \quad & A \overset{\circ}{\star} B \ \coloneqq \ \{\lambda \cdot a + (1-\lambda)\cdot b \ : \ 0 < \lambda < 1, a \in A, b \in B\} && (10)
\end{aligned}$$

Here the $\cdot$, $+$, and $\oplus$ operations denote the standard scaling, Minkowski sum, and union operations. The $\overset{\circ}{\star}$ is a specialized operation introduced by our work that represents the set of all points in the relative interior of the line segment joining some points $a \in A$ and $b \in B$.

Remark 1 (Geometric Join)**.** *The standard geometric join*

$$A \star B \ \coloneqq \ \{\lambda \cdot a + (1-\lambda)\cdot b \ : \ 0 \leqslant \lambda \leqslant 1, a \in A, b \in B\}$$

is homeomorphic to the join $A \star B$ [MBZ+03, 4.2.4 Proposition]. Note that, in contrast, our definition of $\overset{\circ}{\star}$ restricts to $0 < \lambda < 1$, and, hence, the name positive geometric join. The geometric join, in fact, can be expressed as $A \star B = A \ \oplus \ A \overset{\circ}{\star} B \ \oplus \ B$.

Proposition 1 (Associativity of $\overset{\circ}{\star}$)**.** *For any $A, B, C \subseteq \mathbb{R}^d$, $(A \overset{\circ}{\star} B) \overset{\circ}{\star} C = A \overset{\circ}{\star} (B \overset{\circ}{\star} C)$.*

Lemma C.1 summarizes several properties of the four set operations above; one among them is this associativity of $\overset{\circ}{\star}$, appearing as Equation 29.

The relation $A \geqslant B$ holds if and only if $B \subseteq A$. Let $\mathcal{C}_d(\mathbb{R})$ be the set of all convex subsets of $\mathbb{R}^d$. For example, $\emptyset \in \mathcal{C}_d(\mathbb{R})$, any polytope in $\mathbb{R}^d$ is in $\mathcal{C}_d(\mathbb{R})$, and the relative interiors of such polytopes are also in $\mathcal{C}_d(\mathbb{R})$. Given any $A \subseteq \mathbb{R}^d$, its *convex hull*, represented by $\text{conv}(A) \in \mathcal{C}_d(\mathbb{R})$, is the smallest convex set containing it.

We also define an equivalence relation on the set of subsets of $\mathbb{R}^d$. For $A, B \subseteq \mathbb{R}^d$, we denote $A \sim B$ holds if (and only if) $\text{conv}(A) = \text{conv}(B)$.

Consider $\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_n \in \mathcal{C}_d(\mathbb{R})$ and arbitrary $\mathbf{P}_1, \mathbf{P}_2, \dots, \mathbf{P}_t \subseteq \mathbb{R}^d$. We will assign $X_i = \mathbf{X}_i$, for $i \in \{1, 2, \dots, n\}$, and $P_j = \mathbf{P}_j$, for $j \in \{1, 2, \dots, t\}$. Under such an assignment, we will define our evaluation map.

Definition 1 (Evaluation Map)**.** *The evaluation of a polynomial φ over* $\text{CL}(\Omega)$ *with an assignment* $\mathbf{X}, \mathbf{P}$ *is*

$$\text{eval}\,(\varphi \ ; \ \mathbf{X}, \mathbf{P}) \ \coloneqq \ \bigoplus_{M \in \text{mono}(\varphi)} \ \overset{\circ}{\bigstar}_{E \in \text{supp}(M)} \ \text{eval}(E \ ; \ \mathbf{X}, \mathbf{P}),$$

where $E = \lambda_1 \cdot X_1 + \cdots + \lambda_n \cdot X_n + \lambda_{n+1} \cdot P_1 + \cdots + \lambda_{n+t} \cdot P_t \in \mathrm{CL}(\Omega)$ *and* $\mathrm{eval}(E\ ;\ \mathbf{X}, \mathbf{P}) \coloneqq (\sum_{i=1}^{n} \lambda_i \cdot \mathbf{X}_i) + \left(\sum_{j=1}^{t} \lambda_{n+j} \cdot \mathbf{P}_j\right)$. *We clarify that here, '$\sum$' represents the Minkowski summation. Specifically,* $\mathrm{eval}(\emptyset\ ;\ \mathbf{X}, \mathbf{P}) \coloneqq \emptyset$.

Fix an assignment $\mathbf{P}$ for the constants. Then, $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_n) \in \mathcal{C}_d(\mathbb{R})^n$ is a *solution* of a system I of inequalities $\{X_i \geqslant \varphi_i\}_{i=1}^n$, if $\mathbf{X}_i \supseteq \mathrm{eval}(\varphi_i; \mathbf{X}, \mathbf{P})$, for all $i \in \{1, 2, \ldots, n\}$. Let $\mathrm{sol}(I; \mathbf{P}) \subseteq \mathcal{C}_d(\mathbb{R})^n$ denote the set of all solutions of this system I and constant assignment $\mathbf{P}$.

Proposition 2. $\mathrm{sol}(I; \mathbf{P}) \neq \emptyset$.

Proof. Note that $\mathbf{X}_1 = \cdots = \mathbf{X}_n = U$, where U is the convex hull of $\mathbf{P}_1 \oplus \cdots \oplus \mathbf{P}_t$, is a solution. This is because U contains the evaluation of any element in $\mathrm{CL}(\Omega)$ with assignments that are subsets of U. After that, the containment of monomials and polynomials is also immediate. □

For $\mathbf{X}, \mathbf{Y} \in \mathcal{C}_d(\mathbb{R})^n$, their intersection defined below is also an element of $\mathcal{C}_d(\mathbb{R})^n$.

$$\mathbf{X} \cap \mathbf{Y} \ \coloneqq\ (\mathbf{X}_1 \cap \mathbf{Y}_1, \mathbf{X}_2 \cap \mathbf{Y}_2, \ldots, \mathbf{X}_n \cap \mathbf{Y}_n)\,. \tag{11}$$

Proposition 3. *If* $\mathbf{X}, \mathbf{Y} \in \mathrm{sol}(I; \mathbf{P})$, *then* $\mathbf{X} \cap \mathbf{Y} \in \mathrm{sol}(I; \mathbf{P})$.

This proposition extends to the intersection of an arbitrary number of solutions (possibly infinitely many).

Proposition 4. *Consider an index set* Z *and solutions* $\mathbf{X}^{(\zeta)} \in \mathrm{sol}(I; \mathbf{P})$, *for every* $\zeta \in Z$. *Then,* $\bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)} \in \mathrm{sol}(I; \mathbf{P})$.

Proof. For each $\zeta \in Z$, and $i \in \{1, 2, \ldots, n\}$, we have:

$$\begin{aligned}
\mathbf{X}_i^{(\zeta)} &\supseteq \mathrm{eval}\left(\varphi_i; \mathbf{X}^{(\zeta)}, \mathbf{P}\right) && \text{(Since } \mathbf{X}^{(\zeta)} \in \mathrm{sol}(I; \mathbf{P})\text{)} \\
&\supseteq \mathrm{eval}\left(\varphi_i; \bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)}, \mathbf{P}\right). && \text{(By Lemma D.5 and } \mathbf{X}^{(\zeta)} \supseteq \bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)}\text{)}
\end{aligned}$$

Thus, we conclude that $\bigcap_{\zeta \in Z} \mathbf{X}_i^{(\zeta)} \supseteq \mathrm{eval}\left(\varphi_i; \bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)}, \mathbf{P}\right)$. Therefore, we have the following for every $i \in \{1, 2, \ldots, n\}$:

$$\left(\bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)}\right)_i = \bigcap_{\zeta \in Z} \mathbf{X}_i^{(\zeta)} \supseteq \mathrm{eval}\left(\varphi_i; \bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)}, \mathbf{P}\right),$$

which implies that $\bigcap_{\zeta \in Z} \mathbf{X}^{(\zeta)} \in \mathrm{sol}(I; \mathbf{P})$. □

This proposition implies that the intersection of all solutions in $\mathrm{sol}(I; \mathbf{P})$ is also an element of $\mathrm{sol}(I; \mathbf{P})$ – the *smallest solution* of I.

$$\mathrm{ss}(I; \mathbf{P}) \ \coloneqq\ \bigcap_{\mathbf{X} \in \mathrm{sol}(I; \mathbf{P})} \mathbf{X}. \tag{12}$$

Given a system I and assignments of the constants $\mathbf{P} = (\mathbf{P}_1, \ldots, \mathbf{P}_t)$, we aim to identify the smallest solution of this system.

Intuition behind the $\overset{\circ}{\star}$ operation. First, let us elaborate on the evaluation of an expression $A \overset{\circ}{\star} B$, where $A, B \subseteq \mathbb{R}^d$. When A and B are singleton sets, $A \overset{\circ}{\star} B$ represents the relative interior of the line segment joining the two points. Likewise, for singleton sets $A, B, \ldots, C \subseteq \mathbb{R}^d$, the set $A \overset{\circ}{\star} B \overset{\circ}{\star} \cdots \overset{\circ}{\star} C$ represents the relative interior of the convex hull $\text{conv}(A \oplus B \oplus \cdots \oplus C)$.

In general (when A and B are not singleton sets), the set $A \overset{\circ}{\star} B$ is the set of all points that can be expressed as $\lambda \cdot a + (1-\lambda) \cdot b$ for some $a \in A$ and $b \in B$. Intuitively, these points are in the relative interior of the line segment $\overline{ab}$ for some $a \in A$ and $b \in B$. Clearly, $A \overset{\circ}{\star} B$ is contained in $\text{conv}(A \oplus B)$ and contains the relative interior of $\text{conv}(A \oplus B)$. We do not know how to characterize this set using other elementary set operators precisely. However, the set $A \overset{\circ}{\star} B \overset{\circ}{\star} \cdots \overset{\circ}{\star} C$ is semi-algebraic if the sets $A, B, \ldots, C$ are semi-algebraic, using standard quantifier elimination (see, for example, [BPRon, Chapter 14]). These sets will be crucial to *characterizing the smallest solution to our systems with a succinct closed-form expression.*

We note that even if the original system does not have $\overset{\circ}{\star}$ in the inequalities, its smallest solutions may contain $\overset{\circ}{\star}$. For example, the following system of equations, which does not use the $\overset{\circ}{\star}$ operator in its inequalities, has a solution set identical to that of the example system we have been considering.

$$X_1 \supseteq P_1 \ \oplus \ \left(\frac{1}{2} \cdot X_1 + \frac{1}{4} \cdot X_2 + \frac{1}{4} \cdot P_3\right)$$
$$X_2 \supseteq P_2 \ \oplus \ \left(\frac{1}{2} \cdot X_2 + \frac{1}{4} \cdot X_1 + \frac{1}{4} \cdot P_4\right)$$

This fact follows from the property that $X \in \mathcal{C}_d(\mathbb{R})$ satisfies $X \supseteq \rho \cdot X + (1-\rho) \cdot A$ if (and only if) $X \supseteq X \overset{\circ}{\star} A$, for any $A \subseteq \mathbb{R}^d$ and $0 < \rho < 1$ (see Lemma D.4).

Working example. For illustrative purposes, consider $d = 2$. Here, $\mathcal{C}_d(\mathbb{R})$ denotes the set of all convex subsets of $\mathbb{R}^2$. Fix arbitrary assignment $\mathbf{P}$ to the constants. The semantics of the first equation in our system is

$$X_1 \text{ contains the set } \mathbf{P}_1, \text{ and}$$
$$X_1 \text{ contains the set } X_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot \mathbf{P}_3\right)$$

The semantics of the second equation is analogous. The smallest solution of our example system has the following closed-form expression.

$$\text{ss}(I;\mathbf{P})_1 = \text{conv}\left(\ \mathbf{P}_1 \ \oplus \ \mathbf{P}_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot \mathbf{P}_2 + \frac{1}{2} \cdot \mathbf{P}_3\right) \ \oplus \ \mathbf{P}_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot \mathbf{P}_2 + \frac{1}{2} \cdot \mathbf{P}_3\right) \overset{\circ}{\star} \left(\frac{2}{3} \cdot \mathbf{P}_3 + \frac{1}{3} \cdot \mathbf{P}_4\right) \ \right)$$
$$\text{ss}(I;\mathbf{P})_2 = \text{conv}\left(\ \mathbf{P}_2 \ \oplus \ \mathbf{P}_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot \mathbf{P}_1 + \frac{1}{2} \cdot \mathbf{P}_4\right) \ \oplus \ \mathbf{P}_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot \mathbf{P}_1 + \frac{1}{2} \cdot \mathbf{P}_4\right) \overset{\circ}{\star} \left(\frac{2}{3} \cdot \mathbf{P}_4 + \frac{1}{3} \cdot \mathbf{P}_3\right) \ \right)$$

Note that the formal expression for the smallest solution on the RHS is independent of the specific constant assignment $\mathbf{P}$ used; the expression holds for any constant assignment. Our algebraic approach to identifying the smallest solution of a system will also be independent of the specific constant assignment. Determining the evaluation of the smallest solution will need $\mathbf{P}$. The next section presents a finite procedure to obtain their succinct closed-form expression.

Consider singleton sets $\mathbf{P}_1, \mathbf{P}_2, \mathbf{P}_3, \mathbf{P}_4$ for the intuition of the smallest solution; refer to Appendix A.1 for an illustration of an example. The set $\text{ss}(I;\mathbf{P})_1$ is the smallest convex set containing:

1. the point in $\mathbf{P}_1$,

2. the relative interior of the line segment joining the two points in $\mathbf{P}_1$ and $\frac{1}{2}\cdot\mathbf{P}_2+\frac{1}{2}\cdot\mathbf{P}_3$, and
3. the relative interior of the triangle formed by the three points in $\mathbf{P}_1$, $\frac{1}{2}\cdot\mathbf{P}_2+\frac{1}{2}\cdot\mathbf{P}_3$, and $\frac{2}{3}\cdot\mathbf{P}_3+\frac{1}{3}\cdot\mathbf{P}_4$.

Note that the union of the three sets above happens to be a convex set in this case. The set $\mathrm{ss}(I;\mathbf{P})_2$ is similarly defined. As we will see later, our Gaussian elimination-inspired solution methodology will recover these solutions, albeit possibly with slightly different descriptions.

Remark 2 (Solutions Restricted to Polytopes)**.** *Consider the objective of restricting solutions to polytopes (instead of allowing arbitrary convex sets). In this case, our positive geometric join operator $\overset{\circ}{\star}$ is not needed to represent the smallest solution because the smallest polytope containing the set $A\overset{\circ}{\star}B$ is identical to the polytope containing $A\oplus B$. Thus, "linear" polynomials (i.e., polynomials with only degree-1 monomials) can express the constraints for polytope solutions.*

2.3 Algebraic Characterization of the Smallest Solution

We introduce a Gaussian elimination-inspired algorithm to algebraically characterize the smallest solution of a system I of inequalities.

Theorem 2. *Let $\Omega=\{X_1,\ldots,X_n,P_1,\ldots,P_t\}$ and $\Omega_P=\{P_1,\ldots,P_t\}$. Consider an arbitrary system I of inequalities $\{X_i\geqslant\varphi_i\}_{i=1}^n$, where $\varphi_1,\ldots,\varphi_n$ are polynomials over $\mathrm{CL}(\Omega)$. Figure 4 presents a finite procedure to compute polynomials $\varphi_1^*,\ldots,\varphi_n^*$ over $\mathrm{CL}(\Omega_P)$ with the guarantee that $\mathrm{ss}(I;\mathbf{P})_j=\mathrm{conv}\Big(\ \mathrm{eval}(\varphi_j^*;\mathbf{P})\ \Big)$ for every $j\in\{1,2,\ldots,n\}$ and constant assignment $\mathbf{P}$.*

Appendix E estimates the number of monomials and degree of these polynomials $\varphi_1^*,\ldots,\varphi_n^*$; i.e., their "complexity." Theorem 2 can be applied in certain very concrete situations to deduce that if the members of the set Ω_P (using the notation in Theorem 2 belong to a certain class of sets, then each so do each $\mathrm{ss}(I;\mathbf{P})_j, j\in\{1,2,\ldots,n\}$. In particular, classes of subsets of $\mathbb{R}^d, d>0$, for which the above statement is true include the class of all semi-algebraic sets, and more generally the definable sets in any o-minimal expansion of the $\mathbb{R}$ ([vdD98]). We thus have the following corollary of Theorem 2.

Corollary 3. *When the constant assignments $\mathbf{P}_1,\ldots,\mathbf{P}_t\subseteq\mathbb{R}^d$ are definable (resp., semi-algebraic), the set $\mathrm{ss}(I;\mathbf{P})_j$ is definable (resp., semi-algebraic) for $j\in\{1,2,\ldots,n\}$.*

More specifically, if $\mathbf{P}_1,\ldots,\mathbf{P}_t$ are singleton sets, then the smallest solution is always a (finite) union of the relative interiors of polytopes; we call such sets *hemihedral sets*.

We introduce additional notation to elaborate on this theorem, its proof, and our Gaussian elimination-inspired algorithm.

Notation. For an unknown $X\in\Omega$, let φ_X be a polynomial over $\mathrm{CL}(\Omega\setminus\{X\})$. Given an assignment $\mathbf{X},\mathbf{P}$, the assignment $(\mathbf{X},\mathbf{P})\,[\![X\leftarrow\varphi_X]\!]\in\mathcal{C}_d(\mathbb{R})^n$ is defined as follows:

$$(\mathbf{X},\mathbf{P})\,[\![X\leftarrow\varphi_X]\!]_Y=\begin{cases}\mathrm{conv}\Big(\ \mathrm{eval}\left(\varphi_X\ ;\ \mathbf{X},\mathbf{P}\right)\ \Big), & \text{if } Y=X.\\ \mathbf{X}_Y, & \text{otherwise.}\end{cases}\tag{13}$$

Here, $Y\in\Omega\setminus\{X\}$ can be a constant. Read this assignment as "$\mathbf{X}$ *with the unknown X substituted by φ_X evaluation.*" The intuition is to replace $\mathbf{X}_X$ in the assignment $\mathbf{X}\in\mathcal{C}_d(\mathbb{R})^n$ by the evaluation of the polynomial φ_X, a polynomial that doesn't depend on the unknown X.

Next, for a polynomial φ over $\mathrm{CL}(\Omega)$ and φ_X over $\mathrm{CL}(\Omega \setminus \{X\})$, we will define the polynomial $\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right]$ over $\mathrm{CL}(\Omega \setminus \{X\})$. Our final target is to replace every occurrence of X with the evaluation of φ_X. However, formally substituting every symbol X in φ with the polynomial φ_X does not yield a polynomial. So, we define this new polynomial with an identical evaluation for all assignments; it is unclear that such a polynomial exists. First, for $E = \left(\rho \cdot X + (1-\rho) \cdot E'\right) \in \mathrm{CL}(\Omega)$, where $0 \leqslant \rho \leqslant 1$ and $E' \in \mathrm{CL}(\Omega \setminus \{X\})$, we define the following polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$.

$$E\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \coloneqq \bigoplus_{N \in \mathrm{mono}(\varphi_X)} \mathop{\circ\!\!\star}_{F \in \mathrm{supp}(N)} \underbrace{\left(\rho \cdot F + (1-\rho) \cdot E'\right)}_{E\left[\!\left[X \leftarrow F\right]\!\right]}. \tag{14}$$

Note that the $E \longmapsto E\left[\!\left[X \leftarrow F\right]\!\right]$ is a $\mathrm{CL}(\Omega) \to \mathrm{CL}(\Omega \setminus \{X\})$ map. When $E \in \mathrm{CL}(\Omega \setminus \{X\})$, this is an identity map. For a monomial M over $\mathrm{CL}(\Omega)$, define the following polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$.

$$M\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \coloneqq \bigoplus_{\vec{N} \in \mathrm{mono}(\varphi_X)^{\mathrm{supp}(M)}} \mathop{\circ\!\!\star}_{E \in \mathrm{supp}(M)} \left(\mathop{\circ\!\!\star}_{F \in \mathrm{supp}\left(\vec{N}(E)\right)} E\left[\!\left[X \leftarrow F\right]\!\right] \right) \tag{15}$$

Here $\vec{N}$ enumerates all possible $\mathrm{supp}(M) \to \mathrm{mono}(\varphi_X)$ functions; there are $\mathrm{card}\left(\mathrm{mono}(\varphi_X)\right)^{\deg(M)}$ of them. And, $\vec{N}(E)$ is the evaluation of the function at E. Finally, for a polynomial φ over $\mathrm{CL}(\Omega)$, define the following polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$.

$$\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \coloneqq \bigoplus_{M \in \mathrm{mono}(\varphi)} M\left[\!\left[X \leftarrow \varphi_X\right]\!\right]. \tag{16}$$

We will prove the following property of the substituted polynomial

Lemma 1 (Substituted Polynomial)**.** *Consider a polynomial φ over $\mathrm{CL}(\Omega)$, an unknown $X \in \Omega$, and a polynomial φ_X over $\mathrm{CL}(\Omega \setminus \{X\})$. For all assignments $\mathbf{X}$ and $\mathbf{P}$, the following identity holds for the polynomial $\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right]$ over $\mathrm{CL}\left(\Omega \setminus \{X\}\right)$.*

$$\mathrm{eval}\left(\varphi\ ;\ (\mathbf{X}, \mathbf{P})\left[\!\left[X \leftarrow \varphi_X\right]\!\right]\right) \sim \mathrm{eval}\left(\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right]\ ;\ \mathbf{X}, \mathbf{P}\right).$$

Appendix D.3 proves this lemma.

Proof overview of Theorem 2. Beginning with the system $I^{(0)} = I$, we will inductively construct new systems of equations $I^{(j)}$ with polynomials over $\mathrm{CL}\left(\{X_{j+1}, \ldots, X_n, P_1, \ldots, P_t\}\right)$ such that the smallest solution $\mathrm{ss}\left(I^{(0)}; \mathbf{P}\right) = \mathrm{ss}\left(I^{(j)}; \mathbf{P}\right)$ for any assignment $\mathbf{P}$ to the constants. However, it is possible that their sets of solutions are not identical. The system $I^{(n)}$ is $\{X_i \geqslant \varphi_i^*\}_{i=1}^n$ and every φ_i^* is a polynomial over $\mathrm{CL}(\Omega_P)$. After that, it follows that $\mathrm{ss}\left(I^{(n)}\ ;\ \mathbf{P}\right)_i = \mathrm{conv}(\,\mathrm{eval}(\varphi_i^*\ ;\ \mathbf{P})\,)$ for every $i \in \{1, 2, \ldots, n\}$.

Consider the inner loop $j \in \{1, 2, \ldots, n\}$. The system $I^{(j-1)}$ will have polynomials over $\mathrm{CL}(\{X_j, \ldots, X_n, P_1, \ldots, P_t\})$. We consider the j-th inequality in this system: $X_j \geqslant \varphi_j^{(j-1)}$. Lemma D.1 and Lemma D.2 present an explicit polynomial $\widetilde{\varphi}$ over $\mathrm{CL}(\{j+1, \ldots, X_n, P_1, \ldots, P_t\})$ with the following guarantee: replacing the inequality $X_j \geqslant \varphi_j^{(j-1)}$ with the inequality $X_j \geqslant \widetilde{\varphi}$ preserves the smallest solution. The overview paragraph on Appendix D elaborates more on this step. Let I' represent this new system.

Next, in the system I', our objective is to substitute every instance of X_j with the polynomial $\widetilde{\varphi}$ in the polynomials

$$\left\{\ \varphi_\ell^{(j-1)}\ :\ \ell \in \{1, \ldots, j-1, j+1, \ldots, n\}\ \right\}$$

1. Initialize $I^{(0)} = I$
2. For $j \in \{1, 2, \ldots, n\}$:
   (a) Suppose $I^{(j-1)}$ is the system $\left\{X_i \geqslant \varphi_i^{(j-1)}\right\}_{i=1}^{n}$, each $\varphi_i^{(j-1)}$ is a polynomial over $\mathrm{CL}(\{X_j, \ldots, X_n, P_1, \ldots, P_t\})$
   (b) **Canceling X_j step.** Use the rearrangement lemma (Lemma D.1) and cancellation lemma (Lemma D.2) to obtain a polynomial $\widetilde{\varphi}$ over $\mathrm{CL}(\Omega \setminus \{X_1, X_2, \ldots, X_j\})$. Define the new system I' identical to $I^{(j-1)}$ except that the inequality $X_j \geqslant \varphi_j^{(j-1)}$ is replaced by $X_j \geqslant \widetilde{\varphi}$.
   (c) **Substituting X_j step.** Define the new system $I^{(j)}$ as the system $\left\{X_i \geqslant \varphi_i^{(j)}\right\}_{i=1}^{n}$, where

$$\varphi_i^{(j)} \coloneqq \begin{cases} \widetilde{\varphi}, & \text{if } i = j \\ \varphi_i^{(j-1)}\left[\!\left[X_j \leftarrow \widetilde{\varphi}\right]\!\right], & \text{otherwise.} \end{cases}$$

3. **Characterizing the smallest solution for a constant assignment.** For a constant assignment $\mathbf{P}$, output $\mathbf{X} \in \mathcal{C}_d(\mathbb{R})^n$, where $\mathbf{X}_i = \mathrm{conv}\left(\mathrm{eval}\left(\varphi_i^{(n)} ; \mathbf{P}\right)\right)$ for $i \in \{1, 2, \ldots, n\}$.

Figure 4: Our Gaussian elimination-inspired algorithm to solve the system of inequalities I.

These are the polynomials $\varphi_\ell^{(j-1)}\left[\!\left[X_j \leftarrow \widetilde{\varphi}\right]\!\right]$ defined according to Equation 16. The substitution lemma (Lemma D.3) proves that these substitutions preserve the smallest solution for any constant assignment $\mathbf{P}$. Note that $\widetilde{\varphi}$ and the $\varphi_\ell^{(j-1)}\left[\!\left[X_j \leftarrow \widetilde{\varphi}\right]\!\right]$ are polynomials over $\mathrm{CL}(\{X_{j+1} \ldots, X_n, P_1, \ldots, P_t\})$. Therefore, at the end of the j-th loop, the unknowns $X_1, \ldots, X_j$ are eliminated from the RHS of every inequality. After the n-th iteration of the loop, our system will have polynomials only over $\mathrm{CL}(\Omega_P)$.

Working example. Appendix A elaborates how our algorithm solves our example system.

Remark 3. *The procedure above eliminates unknowns $X_1, X_2, \ldots, X_n$ from the polynomials, one at a time. Changing the elimination order may change the description of the smallest solution.*

Remark 4. *The transformation steps above may result in $\widetilde{\varphi} = \emptyset$ inside the loop, which can lead to $\emptyset$ polynomials on the RHS of the last system $I^{(n)}$. This occurrence depends on the structure of the initial system I, not on the specific constant assignment $\mathbf{P}$ as long as they are non-empty.*

2.4 Operational Realization of the Smallest Solution

This section presents an alternative characterization of the smallest solution of a system of inequalities. Applications will reduce their research objectives to characterizing the smallest solution of a system via this alternative characterization.

Consider a system I of inequalities $\{X_j \geqslant \varphi_j\}_{j=1}^{n}$ and arbitrary assignment $\mathbf{P}_1, \ldots, \mathbf{P}_t \subseteq \mathbb{R}^d$ of the constants. Figure 5 recursively defines a construction of nested sequence $\mathbf{X}^{(0)} \to \mathbf{X}^{(1)} \to \mathbf{X}^{(2)} \to \cdots$ where each $\mathbf{X}^{(i)} \in \mathcal{C}_d(\mathbb{R})^n$, for $i \in \{0, 1, \ldots\}$. These sets are nested: $\mathbf{X}^{(i+1)} \geqslant \mathbf{X}^{(i)}$ for

$i \in \{0, 1, \dots\}$, because, for any $j \in \{1, 2, \dots, n\}$, we have:

$$\mathbf{X}_j^{(i+1)} = \text{conv}\Big(\text{eval}\Big(\varphi_j \,;\, \mathbf{X}^{(i)}, \mathbf{P}\Big)\Big) \overset{*}{\supseteq} \text{conv}\Big(\text{eval}\Big(\varphi_j \,;\, \mathbf{X}^{(i-1)}, \mathbf{P}\Big)\Big) = \mathbf{X}_j^{(i)},$$

where step $(*)$ relies on the inductive hypothesis. Appendix A.3 illustrates the evolution of these sets for our example system when the constants are assigned singleton sets in $\mathbb{R}^2$. We denote $\text{itr}(i, I; \mathbf{P}) \coloneqq \mathbf{X}^{(i)}$.

1. Fix an arbitrary assignment $\mathbf{P}$ of the constants
2. $\mathbf{X}^{(0)} = (\emptyset, \emptyset, \dots, \emptyset) \in \mathcal{C}_d(\mathbb{R})^n$
3. For $i \in \{0, 1, \dots\}$, define $\mathbf{X}^{(i+1)} \in \mathcal{C}_d(\mathbb{R})^n$ as follows: For all $j \in \{1, 2, \dots, n\}$, let

$$\mathbf{X}_j^{(i+1)} \coloneqq \text{conv}\Big(\text{eval}\Big(\varphi_j \,;\, \mathbf{X}^{(i)}, \mathbf{P}\Big)\Big).$$

Figure 5: Definition of $\mathbf{X}^{(i)}$ for $i \in \{0, 1, 2, \dots\}$ for a system I and assignment $\mathbf{P}$ of the constants.

We define the vectorized version of set union. For arbitrary sets $A_1, \dots, A_n, B_1, \dots, B_n \subseteq \mathbb{R}^d$, define

$$(A_1, A_2, \dots, A_n) \cup (B_1, B_2, \dots, B_n) \coloneqq (A_1 \cup B_1, A_2 \cup B_2, \dots, A_n \cup B_n)\,.$$

Finally, define

$$\text{itr}(I; \mathbf{P}) \coloneqq \bigcup_{i \geqslant 0} \text{itr}(i, I; \mathbf{P}). \tag{17}$$

Since each $\text{itr}(i, I; \mathbf{P}) \in \mathcal{C}_d(\mathbb{R})^n$ and they are nested sets, their union $\text{itr}(I; \mathbf{P})$ is also an element of $\mathcal{C}_d(\mathbb{R})^n$. Lemma 2 states that the set $\text{itr}(I; \mathbf{P})$ is identical to the smallest solution $\text{ss}(I; \mathbf{P})$.

Lemma 2 (Iterative Construction of the Smallest Solution)**.** *Consider a system I of inequalities and an arbitrary assignment $\mathbf{P}$ to its constants. Then,* $\text{itr}(I; \mathbf{P}) = \text{ss}(I; \mathbf{P})$.

Appendix F proves this result. In fact, it proves a stronger statement: Starting with an *arbitrary initialization* $\mathbf{X}^{(0)} \in \mathcal{C}_d(\mathbb{R})^n$, $\text{itr}(I; \mathbf{P})$ is the smallest solution containing $\mathbf{X}^{(0)}$. For any $\mathbf{X}^{(0)}$ satisfying $\text{ss}(I; \mathbf{P}) \supseteq \mathbf{X}^{(0)}$, it will be the case that $\text{itr}(I; \mathbf{P}) = \text{ss}(I; \mathbf{P})$. In particular, this happens for $\mathbf{X}^{(0)} = (\emptyset, \emptyset, \dots, \emptyset)$.

Remark 5. *Starting with $\mathbf{X}^{(0)} = (\emptyset, \dots, \emptyset) \in \mathcal{C}_d(\mathbb{R})^n$ and an assignment where $\mathbf{P}_1, \dots, \mathbf{P}_t$ are polytopes, note that each $\mathbf{X}_j^{(i)}$ is a convex set. The complexity of describing them may increase indefinitely with $i \in \{0, 1, 2, \dots\}$ (i.e. be unbounded as a function of i); for example, see Appendix A.3. However, their infinite union, the set $\text{itr}(I; \mathbf{P})_j$, has a finite algebraic complexity.*

3 Lamination Hull: Grid Points, Structure Lemma, Reduction to System of Inequalities

We aim to answer membership queries into the lamination hull $\mathcal{S}^{(\infty,\Lambda)}$, where $\Lambda = \{0\}^a \times \mathbb{R}^b \times \mathbb{R}^c \bigcup \mathbb{R}^a \times \{0\}^b \times \mathbb{R}^c$. Starting with a finite $\mathcal{S}^{(0,\Lambda)} \subset \mathbb{R}^{a+b+c}$, this section presents the construction of

the grid points $\mathcal{G} \subset \mathbb{R}^{a+b}$. Using the notation introduced in Section 3.1, define $\mathcal{G}^{(a)} \coloneqq \mathcal{VAS}^{(0,\Lambda)}_{[a]} \subset \mathbb{R}^a$ and $\mathcal{G}^{(b)} \coloneqq \mathcal{VAS}^{(0,\Lambda)}_{[b]} \subset \mathbb{R}^b$. Here, for a set $\mathcal{S} \subseteq \mathbb{R}^{a+b+c}$, we are denoting

$$\begin{aligned}\mathcal{S}_{[a]} &\coloneqq \{\ (P_1, P_2, \ldots, P_a)\ :\ P \in \mathcal{S}\ \} \subseteq \mathbb{R}^a\\ \mathcal{S}_{[b]} &\coloneqq \{\ (P_{a+1}, P_{a+2}, \ldots, P_{a+b})\ :\ P \in \mathcal{S}\ \} \subseteq \mathbb{R}^b\end{aligned}$$

Above, P_i represents the i-th coordinate of $P \in \mathbb{R}^{a+b+c}$. Finally, define the grid

$$\mathcal{G} \coloneqq \mathcal{G}^{(a)} \times \mathcal{G}^{(b)} \subset \mathbb{R}^{a+b}. \tag{18}$$

Section 3.2 presents our structure lemma, which reconstructs any restriction of the lamination hull from its restrictions to grid points. Finally, Section 3.3 obtains these restrictions by finding the smallest solution to a system of inequalities over convex sets using Lemma 4.

3.1 Arrangements

For a finite set $T \subset \mathbb{R}^d$, its convex hull is

$$\operatorname{conv}(T) \coloneqq \left\{ \sum_{P\in T} \lambda_P \cdot P :\ \sum_{P\in T} \lambda_P = 1 \text{ and } \lambda_P \geqslant 0 \text{ for all } P \in T \right\}. \tag{19}$$

The relative interior of $\operatorname{conv}(T)$ is

$$\operatorname{conv}^o(T) \coloneqq \left\{ \sum_{P\in T} \lambda_P \cdot P :\ \sum_{P\in T} \lambda_P = 1 \text{ and } \lambda_P > 0 \text{ for all } P \in T \right\}. \tag{20}$$

We clarify that when $\operatorname{card}(T) = 1$, then $\operatorname{conv}^o(T)$ is the point contained in T.

For a finite set $S \subset \mathbb{R}^a$, we let $\binom{S}{\leqslant k}$ denote the set of all subsets of S with cardinality $\leqslant k$. The *incidence vector* of a point $A \in \mathbb{R}^a$ with respect to the set of points $S \subseteq \mathbb{R}^a$ is the unique element of $\{0,1\}^{\binom{S}{\leqslant (a+1)}}$ satisfying for all $R \in \binom{S}{\leqslant (a+1)}$:

$$\operatorname{inc}(A;S)_R \coloneqq \begin{cases} 1, & \text{if } A \in \operatorname{conv}^o(R)\\ 0, & \text{otherwise.}\end{cases} \tag{21}$$

The total number of incidence vectors is $\leqslant 2^{2^{\operatorname{card}(S)}}$. Given an incidence vector $I \in \{0,1\}^{\binom{S}{\leqslant (a+1)}}$, its *realization* is the set

$$\mathbb{R}^a \supseteq \operatorname{realize}(I;S) \coloneqq \{\ A \in \mathbb{R}^a\ :\ \operatorname{inc}(A;S) = I\ \}. \tag{22}$$

For a point $A \in \mathbb{R}^a$, $\operatorname{inc}(A;S) = \mathbf{0}$ implies that $A \in \mathbb{R}^a \setminus \operatorname{conv}(S)$. Furthermore, $\operatorname{realize}(\mathbf{0};S) = \mathbb{R}^a \setminus \operatorname{conv}(S)$. Finally, the *arrangement* of S is the set of all non-empty realizations with non-zero incidence vector

$$\mathcal{AS} \coloneqq \left\{\ \emptyset \neq \operatorname{realize}(I;S)\ :\ \mathbf{0} \neq I \in \{0,1\}^{\binom{S}{\leqslant (a+1)}}\ \right\}. \tag{23}$$

Observe that for any incidence vector $I \neq \mathbf{0}$, we have $\operatorname{realize}(I;S) \subseteq \operatorname{conv}(S)$ because there is an $R \in \binom{S}{\leqslant (a+1)}$ such that $I_R = 1$; so $\operatorname{realize}(I;S) \subseteq \operatorname{conv}^o(S) \subseteq \operatorname{conv}(S)$. The *vertices* of the arrangement $\mathcal{AS}$ is the set

$$\mathcal{VAS} \coloneqq \{\ V\ :\ \{V\} \in \mathcal{AS}\ \} \subseteq \mathbb{R}^a. \tag{24}$$

So, if a realization in the arrangement $\mathcal{AS}$ is the singleton set $\{V\}$, then $V \in \mathbb{R}^a$ is included in the vertex set.

We will also the notion of a *simplicial decomposition* af an arrangement $\mathcal{A}S$. A simplicial decomposition $\mathcal{SA}S$ is a set of subsets of $\mathbb{R}^a$; each subset is the relative interior of some simplex, and these subsets partition $\text{conv}(S)$. It is possible to obtain such a decomposition without adding any new vertices [Edm70].

Examples. Let us illustrate these notions with a few examples. When $a = 1$, the arrangement of $S = \{S^{(1)}, S^{(2)}, \ldots, S^{(t)}\} \subset \mathbb{R}^a$, where $S^{(1)} < S^{(2)} < \cdots < S^{(t)}$, contains the following realizations (refer to Figure 6):

1. The vertices $S^{(i)}$, where $i \in \{1, 2, \ldots, t\}$, and
2. $\text{conv}^o\big(\{S^{(i)}, S^{(i+1)}\}\big)$, where $i \in \{1, 2, \ldots, t-1\}$.

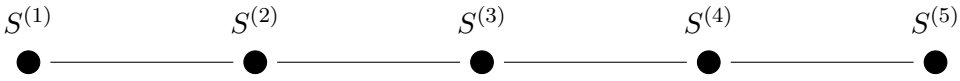
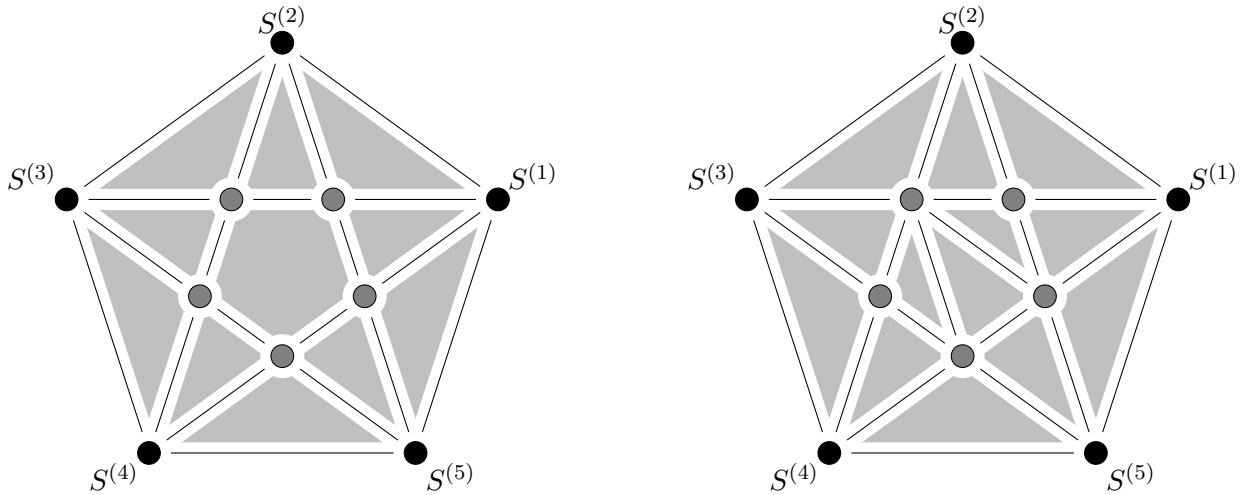


Figure 6: The arrangement $\mathcal{AS}$ (and its simplicial decomposition), where $S := \{S^{(1)}, S^{(2)}, \ldots, S^{(5)}\} \subset \mathbb{R}^a$ and $a = 1$. In this case, $S = \mathcal{VA}S$.

For $a > 1$, the arrangements could be significantly more sophisticated. Figure 7 illustrates an arrangement, its simplicial decomposition, and its vertices using an example for $a = 2$. Appendix G will state and prove the properties of these arrangements useful in the context of the presentation below.



$\mathcal{A}S$ A simplicial decomposition of $\mathcal{A}S$

Figure 7: The arrangement $\mathcal{A}S$, where $S := \{S^{(1)}, S^{(2)}, \ldots, S^{(5)}\} \subseteq \mathbb{R}^a$, where $a = 2$ and its simplicial decomposition. The filled circles (both gray and black) represent the vertices $\mathcal{VA}S$.

3.2 Computing any Restriction of the Lamination Hull

We aim to answer the membership query $Q = (u, v, w) \in \mathbb{R}^{a+b+c}$ in $\mathcal{S}^{(\infty,\Lambda)}$. This is equivalent to answering the membership of Q in $\mathcal{S}^{(\infty,\Lambda)}\big|_q$, where $q = (u, v) \in \mathbb{R}^{a+b}$. The following structure lemma will compute the restriction $\mathcal{S}^{(\infty,\Lambda)}\big|_q$ from the restrictions of the hull to the grid points.

Lemma 3 (Structure Lemma)**.** *Given the simplicial decompositions* $\mathcal{S}^{(a)} \coloneqq \mathcal{SAS}^{(0,\Lambda)}_{[a]}, \mathcal{S}^{(b)} \coloneqq \mathcal{SAS}^{(0,\Lambda)}_{[b]}$*, and the restriction of the lamination hull at the grid points* $\left\{ \mathcal{S}^{(\infty,\Lambda)}\big|_g \;:\; g \in \mathcal{G} \right\}$*, Figure 11 presents a finite procedure to compute* $\mathcal{S}^{(\infty,\Lambda)}\big|_q$*, for any* $q \in \mathbb{R}^{a+b}$*.*

3.3 Reduction to a System of Inequalities

Our objective is to design a system of linear inequalities over convex sets so that its smallest solution corresponds to the restrictions $\left\{ \mathcal{S}^{(\infty,\Lambda)}\big|_g \;:\; g \in \mathcal{G} \right\}$. Figure 8 presents our system $\mathcal{I}$ of linear inequalities.

We introduce unknown $X_{(u,v)}$, for each grid point $(u, v) \in \mathcal{G}$. Our algorithm will incrementally add constraints to a system of inequalities. We will start with the system $\{X_g \supseteq \emptyset\}_{g\in\mathcal{G}}$. Suppose the current system is $\{X_g \supseteq \varphi_g\}_{g\in\mathcal{G}}$. When we *add an inequality* $X_{g^*} \supseteq \varphi'$ to this system, then the updated inequality for X_{g^*} becomes $X_{g^*} \supseteq \varphi_{g^*} \oplus \varphi'$.

1. Introduce unknown $X_{(u,v)}$, for each grid point $(u, v) \in \mathcal{G}$, representing a convex set in $\mathbb{R}^{a+b+c}$.
2. *Base case constraints.* For each point $P \in \mathcal{S}^{(0,\Lambda)}$, add the following inequality to the system $\mathcal{I}$.
$$X_{(u,v)} \supseteq P, \text{ where } u = P_{[a]} \text{ and } v = P_{[b]}. \tag{25}$$
3. *Spatial information constraints.* For all $u, u^{(1)}, u^{(2)}, \ldots, u^{(k)} \in \mathcal{G}^{(a)}$ and $v \in \mathcal{G}^{(b)}$ such that (A) $2 \leqslant k \leqslant a+1$, (B) $u^{(1)}, u^{(2)}, \ldots, u^{(k)}$ form a simplex, and (C) $u = \alpha^{(1)} \cdot u^{(1)} + \alpha^{(2)} \cdot u^{(2)} + \cdots + \alpha^{(k)} \cdot u^{(k)}$, $\sum_{i=1}^{k} \alpha^{(i)} = 1$ and $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(k)} > 0$, add the constraint
$$X_{(u,v)} \supseteq \sum_{i=1}^{k} \alpha^{(i)} \cdot X_{(u^{(i)},v)}. \tag{26}$$
Likewise, for $u \in \mathcal{G}^{(a)}$ and $v^{(1)}, v^{(2)}, \ldots, v^{(k)} \in \mathcal{G}^{(b)}$ satisfying (A) $2 \leqslant k \leqslant b+1$, (B) $v^{(1)}, v^{(2)}, \ldots, v^{(k)}$ form a simplex, and (C) $v = \alpha^{(1)} \cdot v^{(1)} + \alpha^{(2)} \cdot v^{(2)} + \cdots + \alpha^{(k)} \cdot v^{(k)}$, $\sum_{i=1}^{k} \alpha^{(i)} = 1$ and $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(k)} > 0$, add the constraint
$$X_{(u,v)} \supseteq \sum_{i=1}^{k} \alpha^{(i)} \cdot X_{(u,v^{(i)})}. \tag{27}$$

Figure 8: Definition of our system $\mathcal{I}$ of inequalities for finding $\mathcal{S}^{(\infty,\Lambda)}\big|_g$ for $g \in \mathcal{G}$.

Base-case inequalities like Equation 25 capture the the semantics that $X_{(u,v)}$ contains the point P in the initial set $\mathcal{S}^{(0,\Lambda)}$, where $u = P_{[a]}$ and $v = P_{[b]}$.

Next, we present the semantics associated with the spatial information inequalities like Equation 26. Consider a simplex $u^{(1)}, u^{(2)}, \ldots, u^{(k)} \in \mathcal{G}^{(a)}$ such that $2 \leqslant k \leqslant a+1$. Suppose any $u \in \mathcal{G}^{(a)}$

is in the relative interior of this simplex; that is, there are unique $\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(k)} > 0$, such that $\sum_{i=1}^{k} \alpha^{(i)} = 1$ and

$$u = \sum_{i=1}^{k} \alpha^{(i)} \cdot u^{(i)}.$$

Consider arbitrary $v \in \mathcal{G}^{(b)}$. For arbitrary points $P^{(i)} \in X_{(u^{(i)},v)}$, for $i \in \{1, 2, \ldots, k\}$, Equation 26 ensures that their convex linear combination $\sum_{i=1}^{k} \alpha^{(i)} \cdot P^{(i)}$ is in the set $X_{(u,v)}$. Inequalities like Equation 27 are also encoding similar spatial information.

Finally, note that the total number of unknowns is $\text{card}(\mathcal{G})$, and the total number of inequalities added is $\leqslant \text{card}\left(\mathcal{S}^{(0,\Lambda)}\right) + \left(\text{card}\left(\mathcal{G}^{(a)}\right)^{a+2} \text{card}\left(\mathcal{G}^{(b)}\right) + \text{card}\left(\mathcal{G}^{(a)}\right) \text{card}\left(\mathcal{G}^{(b)}\right)^{b+2}\right)$.

We prove the following result.

Lemma 4 (Reduction to Solving System of Linear Inequalities over Convex Sets)**.** *Let* $\left(\mathbf{X}_g^{(*)} \ : \ g \in \mathcal{G} \right)$ *denote the smallest solution of this system* $\mathcal{I}$ *in Figure 8. Then,* $\mathcal{S}^{(\infty,\Lambda)}\big|_g = \mathbf{X}_g^{(*)}$ *for every* $g \in \mathcal{G}$.

Appendix I presents the proof of this lemma. This result's proof relies on the operational realization interpretation of Section 2.4.

References

[Bea89] Donald Beaver. Perfect privacy for two-party protocols. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing And Cryptography, Proceedings of a DIMACS Workshop, Princeton, New Jersey, USA, October 4-6, 1989*, volume 2 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 65–78. DIMACS/AMS, 1989. doi:10.1090/dimacs/002/03. 1, 3

[BKMN22] Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Geometry of secure two-party computation. In *63rd Annual Symposium on Foundations of Computer Science*, pages 1035–1044, Denver, CO, USA, October 31 – November 3, 2022. IEEE Computer Society Press. doi:10.1109/FOCS54457.2022.00101. 1, 3, 4, 5, 6, 48

[BKMN23] Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, and Hai H. Nguyen. Randomized functions with high round complexity. In Guy N. Rothblum and Hoeteck Wee, editors, *TCC 2023: 21st Theory of Cryptography Conference, Part I*, volume 14369 of *Lecture Notes in Computer Science*, pages 319–348, Taipei, Taiwan, November 29 – December 2, 2023. Springer, Cham, Switzerland. doi:10.1007/978-3-031-48615-9_12. 1, 3, 6

[BKNV23] Saugata Basu, Mario Kummer, Tim Netzer, and Cynthia Vinzant. New directions in real algebraic geometry, 2023. https://publications.mfo.de/bitstream/handle/mfo/4031/OWR_2023_15.pdf?sequence=-1&isAllowed=y. 4

[BPRon] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2006 (second edition). 11, 63

[Bra21] Mark Braverman. Information complexity, 2021. https://mbraverm.princeton.edu/research/information-complexity/. 3

[BSS89] LENORE BLUM, MIKE SHUB, and STEVE SMALE. On a theory of computation and complexity over the real numbers: NP–completeness, recursive functions and universal machines. *AMERICAN MATHEMATICAL SOCIETY*, 21(1), 1989. 3

[Car07] Constantin Carathéodory. Über den variabilitätsbereich der koeffizienten von potenzreihen, die gegebene werte nicht annehmen. *Mathematische Annalen*, 64(1):95–115, 1907. 61

[CFG11] Diego Cordoba, Daniel Faraco, and Francisco Gancedo. Lack of uniqueness for weak solutions of the incompressible porous media equation. *Archive for rational mechanics and analysis*, 200:725–746, 2011. 4

[CG07] Diego Córdoba and Francisco Gancedo. Contour dynamics of incompressible 3-d fluids in a porous medium with different densities. *Communications in Mathematical Physics*, 273:445–471, 2007. 4

[CK89] Benny Chor and Eyal Kushilevitz. A zero-one law for Boolean privacy (extended abstract). In *21st Annual ACM Symposium on Theory of Computing*, pages 62–72, Seattle, WA, USA, May 15–17, 1989. ACM Press. doi:10.1145/73007.73013. 1, 3

[DLSJ09] Camillo De Lellis and László Székelyhidi Jr. The euler equations as a differential inclusion. *Annals of mathematics*, pages 1417–1436, 2009. 4

[Edm70] Allan L Edmonds. Simplicial decompositions of convex polytopes. *Pi Mu Epsilon Journal*, 5(3):124–128, 1970. 17, 47

[Grü03] Branko Grünbaum. *Convex polytopes*, volume 221 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2003. Prepared and with a preface by Volker Kaibel, Victor Klee and Günter M. Ziegler. doi:10.1007/978-1-4613-0019-9. 6, 64

[GV09] Andrei Gabrielov and Nicolai Vorobjov. Approximation of definable sets by compact families, and upper bounds on homotopy and homology. *J. Lond. Math. Soc. (2)*, 80(1):35–54, 2009. doi:10.1112/jlms/jdp006. 64

[GV17a] Andrei Gabrielov and Nicolai Vorobjov. On topological lower bounds for algebraic computation trees. *Found. Comput. Math.*, 17(1):61–72, 2017. doi:10.1007/s10208-015-9283-7. 64

[GV17b] Andrei Gabrielov and Nicolai Vorobjov. On topological lower bounds for algebraic computation trees. *Found. Comput. Math.*, 17(1):61–72, 2017. doi:10.1007/s10208-015-9283-7. 64

[HL21] Lauri Hitruhin and Sauli Lindberg. Lamination convex hull of stationary incompressible porous media equations. *SIAM Journal on Mathematical Analysis*, 53(1):491–508, 2021. 4

[jh] joriki (https://math.stackexchange.com/users/6622/joriki). Cancellation law for minkowski sums. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/175016 (version: 2012-08-18). URL: https://math.stackexchange.com/q/175016, arXiv:https://math.stackexchange.com/q/175016. 6

[Kil00] Joe Kilian. More general completeness theorems for secure two-party computation. In *32nd Annual ACM Symposium on Theory of Computing*, pages 316–324, Portland, OR, USA, May 21–23, 2000. ACM Press. doi:10.1145/335305.335342. 5

[KS86] Werner Kuich and Arto Salomaa. *Semirings, automata, languages*, volume 5 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, Berlin, 1986. doi:10.1007/978-3-642-69959-7. 6

[Kus89] Eyal Kushilevitz. Privacy and communication complexity. In *30th Annual Symposium on Foundations of Computer Science*, pages 416–421, Research Triangle Park, NC, USA, October 30 – November 1, 1989. IEEE Computer Society Press. doi:10.1109/SFCS.1989.63512. 1, 3

[MBZ+03] Jiří Matoušek, Anders Björner, Günter M Ziegler, et al. *Using the Borsuk-Ulam theorem: lectures on topological methods in combinatorics and geometry*, volume 2003. Springer, 2003. 9

[MPR13] Hemanta K. Maji, Manoj Prabhakaran, and Mike Rosulek. Complexity of multi-party computation functionalities. In Manoj Prabhakaran and Amit Sahai, editors, *Secure Multi-Party Computation*, volume 10 of *Cryptology and Information Security Series*, pages 249–283. IOS Press, 2013. doi:10.3233/978-1-61499-169-4-249. 3

[SS78] Arto Salomaa and Matti Soittola. *Automata-theoretic aspects of formal power series*. Texts and Monographs in Computer Science. Springer-Verlag, New York-Heidelberg, 1978. 6

[vdD98] Lou van den Dries. *Tame topology and o-minimal structures*, volume 248 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1998. doi:10.1017/CBO9780511525919. 12, 64

[Wei15] Omri Weinstein. *Interactive Information Complexity and Applications*. PhD thesis, Princeton University, 2015. 3

[Yao97] Andrew Chi-Chih Yao. Decision tree complexity and Betti numbers. volume 55, pages 36–43. 1997. 26th Annual ACM Symposium on the Theory of Computing (STOC '94) (Montreal, PQ, 1994). doi:10.1006/jcss.1997.1495. 64

[Zie95] Günter M. Ziegler. *Lectures on polytopes*, volume 152 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. doi:10.1007/978-1-4613-8431-1. 64

A Solving Example System

We will find the smallest solution of the following system over arbitrary convex sets using the algorithm in Figure 4.

$$X_1 \geqslant P_1 \oplus X_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right)$$

During our presentation, it will be instructive to shadow along with the presentation on Appendix D. Three terminologies will be used below.

1. Rearrangement as in Lemma D.1
2. Cancellation as in Lemma D.2
3. Substitution as in Lemma D.3

The equation of X_1 does not need to be rearranged; we can proceed with cancellation. After the cancellation of X_1, we get the following system.

$$X_1 \geqslant P_1 \oplus P_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right)$$

Next, we aim to substitute X_1 with the RHS of the first inequality in X_2's inequality (step 2.c. in Figure 4 with $j = 1$). Below, we will illustrate how the substituted polynomial is obtained.

$$X_2 \geqslant P_2 \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right) \qquad \text{(original equation of } X_2\text{)}$$
$$\geqslant P_2 \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot \left[P_1 \oplus P_1 \overset{\circ}{\star} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)\right] + \frac{1}{2} \cdot P_4\right)$$
(substituting the symbol X_1 with the RHS of X_1's inequality)

(Remark: this expression in *not* a polynomial)
$$= P_2 \oplus X_2 \overset{\circ}{\star} \left(\left[\frac{1}{2} \cdot P_1 \oplus \frac{1}{2} \cdot P_1 \overset{\circ}{\star} \left(\frac{1}{4} \cdot X_2 + \frac{1}{4} \cdot P_3\right)\right] + \frac{1}{2} \cdot P_4\right)$$
(scalar multiplication distributes over $\oplus$ and $\overset{\circ}{\star}$)

(Remark: this expression in *not* a polynomial)
$$\sim P_2 \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \overset{\circ}{\star} \left(\frac{1}{4} \cdot X_2 + \frac{1}{4} \cdot P_3 + \frac{1}{2} \cdot P_4\right)$$
(Minkowski sum distributes over $\oplus$ and $\overset{\circ}{\star}$)

This final expression is a polynomial. Verify that this "derivation" of the substituted polynomial, capturing what we intend to achieve, matches with the polynomial computed using our definition of substituted polynomials in Example 1 of Appendix A.2. After substitution, we get the system:

$$
\begin{aligned}
X_1 &\geqslant P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\\
X_2 &\geqslant P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot X_2 + \frac{1}{4}\cdot P_3 + \frac{1}{2}\cdot P_4\right)
\end{aligned}
$$

At this point, note that X_1 has been eliminated from the RHS of every inequality. This corresponds to completing the $j = 1$ loop in Figure 4.

After that, in $j = 2$ loop, we begin by rearranging the inequality for X_2 as follows:

$$
\begin{aligned}
& X_2 \geqslant P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 \oplus \frac{1}{2}\cdot P_4\right) \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot X_2 + \frac{1}{4}\cdot P_3 + \frac{1}{2}\cdot P_4\right)\\
\iff\quad & X_2 \geqslant P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 \oplus \frac{1}{2}\cdot P_4\right) \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right)
\end{aligned}
$$

This derivation relies on the fact that $X \geqslant (\rho \cdot X + (1-\rho)\cdot A) \mathbin{\overset{\circ}{\star}} B$ if (and only if) $X \geqslant X \mathbin{\overset{\circ}{\star}} A \mathbin{\overset{\circ}{\star}} B$, for arbitrary sets $X \in \mathcal{C}_d(\mathbb{R})$, $A, B \subseteq \mathbb{R}^d$ and $0 < \rho < 1$ (see Lemma D.4). After that, we cancel X_2 from this rewritten inequality to get the following system.

$$
\begin{aligned}
X_1 &\geqslant P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\\
X_2 &\geqslant P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right)
\end{aligned}
$$

Next, we aim to substitute the RHS of X_2's inequality into the symbol X_2 in X_1's inequality. To illustrate how the substituted polynomial is defined, we elaborate on the substitution process.

$$
\begin{aligned}
X_1 &\geqslant P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right) && \text{(original equation)}\\
&\geqslant P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot \left[P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right)\right] + \frac{1}{2}\cdot P_3\right)\\
& && \text{(substituting the symbol } X_2 \text{ with the RHS of } X_2\text{'s inequality)}\\
& && \text{(Remark: this expression in } \textit{not} \text{ a polynomial)}\\
&= P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\left[\frac{1}{2}\cdot P_2 \oplus \frac{1}{2}\cdot P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4\right) \oplus \frac{1}{2}\cdot P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{6}\cdot P_3 + \frac{1}{3}\cdot P_4\right)\right] + \frac{1}{2}\cdot P_3\right)\\
& && \text{(scalar multiplication distributes over } \oplus \text{ and } \mathbin{\overset{\circ}{\star}}\text{)}\\
& && \text{(Remark: this expression is } \textit{not} \text{ a polynomial)}\\
&\sim P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right)\\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\right)\\
& && \text{(Minkowski sum distributes over } \oplus \text{ and } \mathbin{\overset{\circ}{\star}}\text{)}
\end{aligned}
$$

This final expression is a polynomial, and it is used on the RHS of the substituted system below. Example 2 of Appendix A.2 elaborates on how this polynomial is computed using our definition of substituted polynomial.

$$
\begin{aligned}
X_1 &\geqslant P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\right) \\
X_2 &\geqslant P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right)
\end{aligned}
$$

This system, at the end of $j = 2$ loop, has eliminated all unknowns from the inequalities. As a result, the smallest convex solution is straightforward to obtain; it is just the convex hull of the RHS expressions. So, the smallest solution is:

$$
\begin{aligned}
X_1 = \operatorname{conv}\Bigg(& P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \\
& \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\right) \Bigg) \\
X_2 = \operatorname{conv}\Bigg(& P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right) \Bigg)
\end{aligned}
$$

Note that the smallest solution characterized here for X_2 is identical to the predicted solution $\mathrm{ss}(I;\mathbf{P})_2$ in Section 2.2. The expression for X_1 appears different; however, it describes the same set (for any constant assignment $\mathbf{P}$). The extra expression $\frac{1}{4}\cdot\mathbf{P}_1 + \frac{1}{4}\cdot\mathbf{P}_4 + \frac{1}{2}\cdot\mathbf{P}_3$ is redundant in the expression. It is a convex linear combination of the sets $\mathbf{P}_1$ and $\frac{2}{3}\cdot\mathbf{P}_3 + \frac{1}{3}\cdot\mathbf{P}_4$. After accounting for this geometric property, it turns out to be identical to the solution $\mathrm{ss}(I;\mathbf{P})_1$ predicted in Section 2.2.

$$
\begin{aligned}
X_1 &= \operatorname{conv}\Bigg(P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\right) \Bigg) \\
X_2 &= \operatorname{conv}\Bigg(P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right) \Bigg)
\end{aligned}
$$

This optimization in representing the sets is not the focus of our current work, so it is foregone here. Additionally, if we eliminated X_2 first and X_1 next, our expressions would have a similar redundancy in the $\mathrm{ss}(I;\mathbf{P})_2$ expression. If P_1, P_2, P_3, P_4 are assigned convex sets, then the expressions within the "conv(·)" are already convex; this may not hold in general.

Appendix A.1 will illustrate the solution for a specific assignment. Appendix B will solve this system by restricting the solution to polytopes; it will contain spurious additional points.

A.1 Figure of the Smallest Solution for an Assignment

Suppose P_1, P_2, P_3, P_4 are assigned singleton sets in $\mathbb{R}^2$. For that constant assignment Figure 9 presents the smallest solution to our example system from Section 2.4.

A.2 Examples of Substitution

Example 1. We will show the computation of $\varphi\left[\!\left[X_1 \leftarrow \varphi_{X_1}\right]\!\right]$ where

$$
\varphi = P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_1 + \frac{1}{2}\cdot P_4\right) \text{ and } \varphi_{X_1} = P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right).
$$

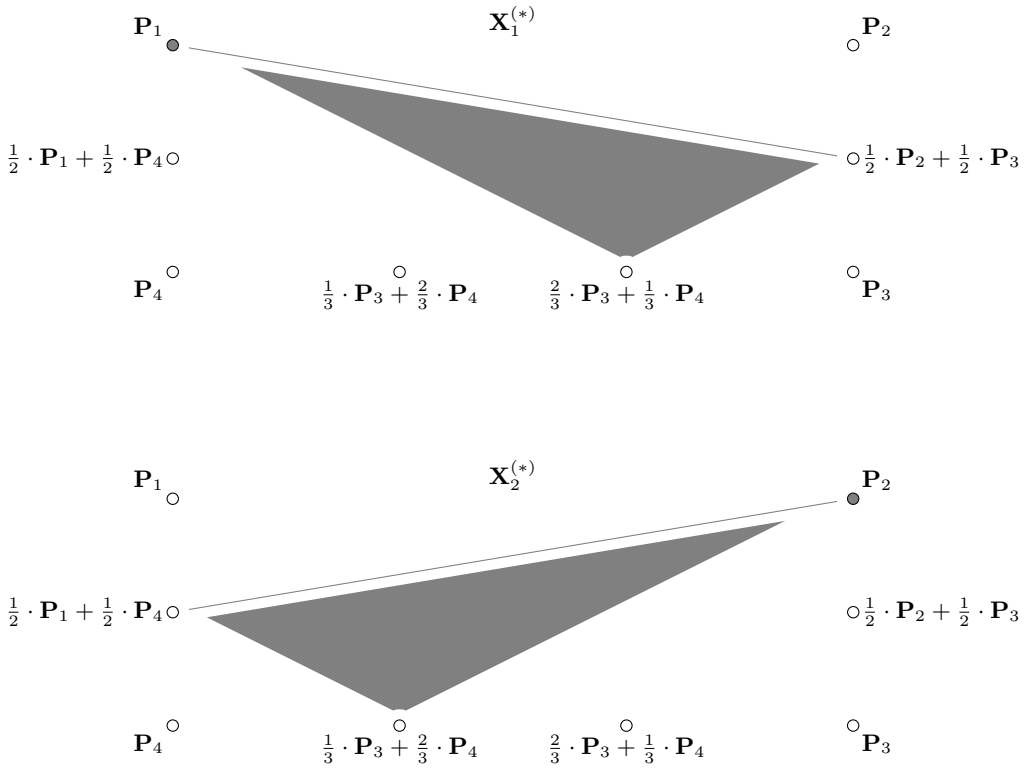


Figure 9: The smallest convex solutions $\left(\mathbf{X}_1^{(*)}, \mathbf{X}_2^{(*)}\right)$ of the example system from Section 2.

By Equation 16, we have

$$\varphi\left[\!\left[X_1 \leftarrow \varphi_{X_1}\right]\!\right] = P_2\left[\!\left[X_1 \leftarrow \varphi_{X_1}\right]\!\right] \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right)\left[\!\left[X_1 \leftarrow \varphi_{X_1}\right]\!\right].$$

Let us demonstrate the computation of the two substitutions on the RHS expression above.

Part 1.
$$\begin{aligned} P_2\left[\!\left[X_1 \leftarrow \varphi_{X_1}\right]\!\right] &= P_2\left[\!\left[X_1 \leftarrow P_1\right]\!\right] \oplus P_2\left[\!\left[X_1 \leftarrow P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)\right]\!\right] \\ &\qquad \text{(first step in the step-wise application of Equation 15)} \\ &= P_2\left[\!\left[X_1 \leftarrow P_1\right]\!\right] \oplus P_2\left[\!\left[X_1 \leftarrow P_1\right]\!\right] \mathbin{\overset{\circ}{\star}} P_2\left[\!\left[X_1 \leftarrow \frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right]\!\right] \\ &\qquad \text{(final step in the step-wise application of Equation 15)} \\ &= P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} P_2 \qquad \text{(using Equation 14)} \\ &\sim P_2. \qquad \text{(using idempotence laws)} \end{aligned}$$

Idempotence laws are applied only for brevity in presentation; our proposed algorithms do not perform this optimization.

In the substitution computation below, we will need all $\mathrm{supp}(M) \to \mathrm{mono}(\varphi_{X_1})$ functions, where $M = X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right)$. That is, functions of the following form.

$$\left\{X_2, \frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right\} \to \left\{P_1, P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)\right\}.$$

Part 2. $X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_1 + \frac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow \varphi_{X_1}]\!]$

$$
\begin{aligned}
&= X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \\
&\quad \oplus X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)\left[\!\!\left[X_1 \leftarrow P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right)\right]\!\!\right] \\
&\quad \oplus X_2\left[\!\!\left[X_1 \leftarrow P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right)\right]\!\!\right] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \\
&\quad \oplus X_2\left[\!\!\left[X_1 \leftarrow P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right)\right]\!\!\right] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)\left[\!\!\left[X_1 \leftarrow P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right)\right]\!\!\right] \\
&\qquad\qquad \text{(first step in the step-wise application of Equation 15)} \\
&= X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \\
&\quad \oplus X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)\left[\!\!\left[X_1 \leftarrow \tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right]\!\!\right] \\
&\quad \oplus X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} X_2\left[\!\!\left[X_1 \leftarrow \tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right]\!\!\right] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \\
&\quad \oplus X_2[\![X_1 \leftarrow P_1]\!] \mathbin{\overset{\circ}{\star}} X_2\left[\!\!\left[X_1 \leftarrow \tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right]\!\!\right] \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)[\![X_1 \leftarrow P_1]\!] \\
&\qquad\qquad \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_1 + \tfrac{1}{2}\cdot P_4\right)\left[\!\!\left[X_1 \leftarrow \tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right]\!\!\right] \\
&\qquad\qquad \text{(final step in the step-wise application of Equation 15)} \\
&= X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \\
&\quad \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{4}\cdot X_2 + \tfrac{1}{4}\cdot P_3 + \tfrac{1}{2}\cdot P_4\right) \\
&\quad \oplus X_2 \mathbin{\overset{\circ}{\star}} X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \\
&\quad \oplus X_2 \mathbin{\overset{\circ}{\star}} X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{4}\cdot X_2 + \tfrac{1}{4}\cdot P_3 + \tfrac{1}{2}\cdot P_4\right) \qquad \text{(using Equation 14)} \\
&\sim X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{4}\cdot X_2 + \tfrac{1}{4}\cdot P_3 + \tfrac{1}{2}\cdot P_4\right). \\
&\qquad\qquad \text{(using idempotence laws)}
\end{aligned}
$$

We want to emphasize that every step of the derivation above is a polynomial. To conclude, putting these two derivations together, we have:

$$\varphi[\![X_1 \leftarrow \varphi_{X_1}]\!] \sim P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{4}\cdot X_2 + \tfrac{1}{4}\cdot P_3 + \tfrac{1}{2}\cdot P_4\right).$$

Example 2. We will show the computation of $\varphi[\![X_2 \leftarrow \varphi_{X_2}]\!]$ where

$$
\begin{aligned}
\varphi &= P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right) \\
\varphi_{X_2} &= P_2 \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \oplus P_2 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot P_1 + \tfrac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{3}\cdot P_3 + \tfrac{2}{3}\cdot P_4\right)
\end{aligned}
$$

By Equation 16, we have

$$\varphi[\![X_2 \leftarrow \varphi_{X_2}]\!] = P_1[\![X_2 \leftarrow \varphi_{X_2}]\!] \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\tfrac{1}{2}\cdot X_2 + \tfrac{1}{2}\cdot P_3\right)[\![X_2 \leftarrow \varphi_{X_2}]\!].$$

Next, we compute the substituted polynomials (short-circuiting the trivial substitutions).

$$\begin{aligned}
\varphi\,[\![X_2 \leftarrow \varphi_{X_2}]\!] &= P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)[\![X_2 \leftarrow P_2]\!] \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\left[\!\!\left[X_2 \leftarrow P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right)\right]\!\!\right] \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\left[\!\!\left[X_2 \leftarrow P_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right)\right]\!\!\right] \\
&= P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)[\![X_2 \leftarrow P_2]\!] \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)[\![X_2 \leftarrow P_2]\!] \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\left[\!\!\left[X_2 \leftarrow \frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right]\!\!\right] \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)[\![X_2 \leftarrow P_2]\!] \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\left[\!\!\left[X_2 \leftarrow \frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\right]\!\!\right] \\
&\qquad\qquad \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right)\left[\!\!\left[X_2 \leftarrow \frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\right]\!\!\right] \\
&= P_1 \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \\
&\quad \oplus P_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\right) \mathbin{\overset{\circ}{\star}} \left(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\right)
\end{aligned}$$

This concludes the derivation of the substituted polynomial.

A.3 Iterated Solution Evolution for an Assignment

Suppose P_1, P_2, P_3, P_4 are assigned singleton sets in $\mathbb{R}^2$. Figure 10 illustrates the evolution of the iterated solutions $\mathbf{X}^{(i)}$, for $i \in \{0, 1, \dots\}$ introduced in Section 2.4, corresponding to our example system.

B Solving Example System: Restricted to Polytopes

We aim to find the smallest solution of the following system *restricted to polytopes*, not arbitrary convex sets.

$$\begin{aligned}
X_1 &\geqslant P_1 \oplus X_1 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_2 + \frac{1}{2}\cdot P_3\right) \\
X_2 &\geqslant P_2 \oplus X_2 \mathbin{\overset{\circ}{\star}} \left(\frac{1}{2}\cdot X_1 + \frac{1}{2}\cdot P_4\right)
\end{aligned}$$

We will follow the solution strategy in Section 2.3 with an additional *simplification rule*: For polytopes X, A, B, the following identity holds.

$$X \geqslant A \mathbin{\overset{\circ}{\star}} B \iff X \geqslant A \oplus B,$$

For polytope constant assignments, we can simplify the original system directly into the system:

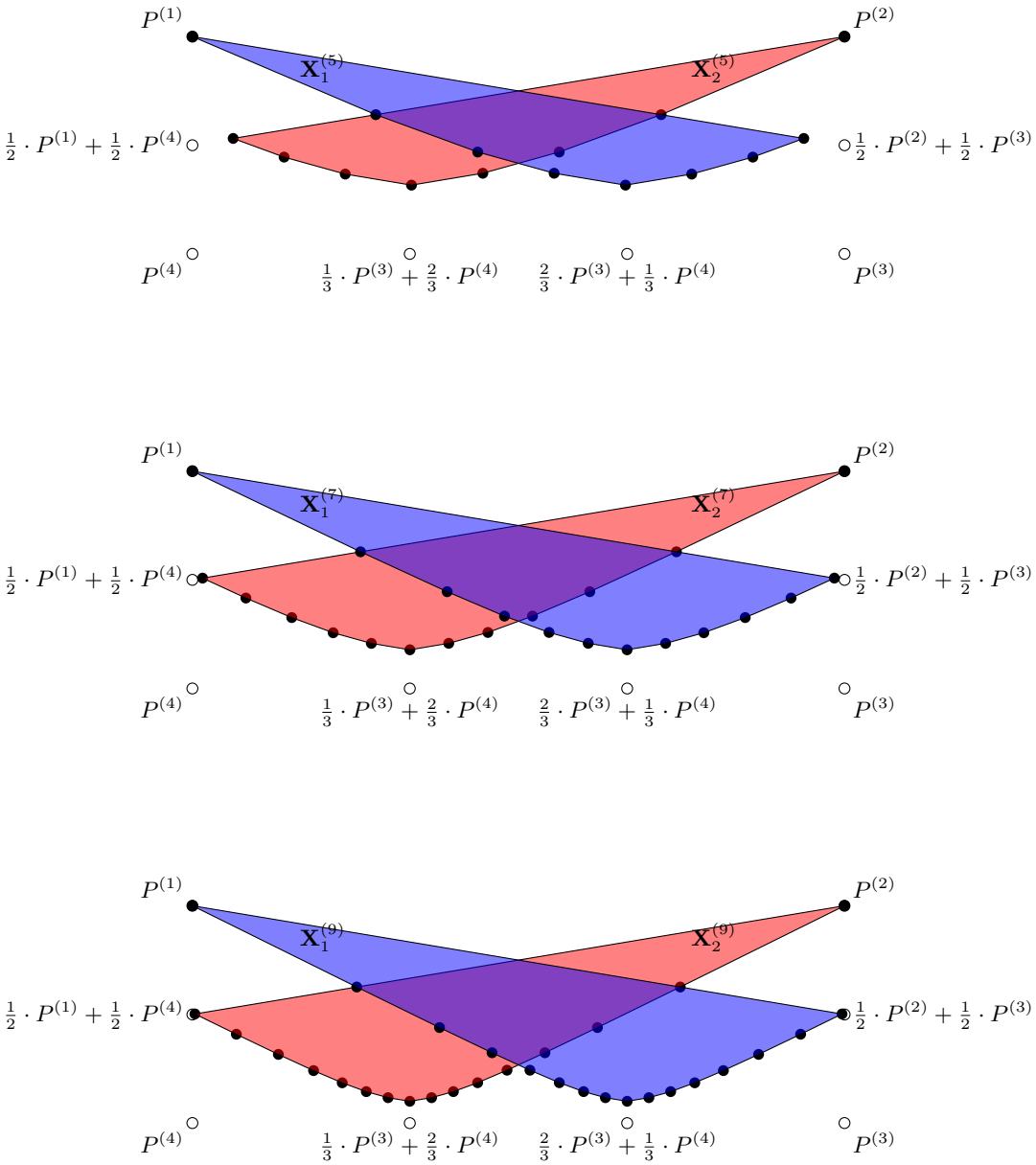


Figure 10: Illustration of the iterated convex sets $\left\{\mathbf{X}^{(i)}\right\}_{i \geqslant 0}$ in $\mathbb{R}^2$ proposed in Section 2.4 for the system in Section 2, when $i \in \{5, 7, 9\}$. When $i = 5$, $i = 7$, and $i = 9$, the polytopes have 8, 12, and 16 edges each, respectively.

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right) \oplus X_1$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right) \oplus X_2$$

After canceling X_1 (and using the idempotence $A \oplus A = A$), we get the system:

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot X_1 + \frac{1}{2} \cdot P_4\right) \oplus X_2$$

After substituting X_1 into X_2, we get the system:

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus \left(\frac{1}{4} \cdot X_2 + \frac{1}{4} \cdot P_3 + \frac{1}{2} \cdot P_4\right) \oplus X_2$$

Rewriting X_2's equation gives the system:

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus X_2 \overset{\circ}{\star} \left(\frac{1}{3} \cdot P_3 + \frac{2}{3} \cdot P_4\right) \oplus X_2$$
$$= P_2 \oplus \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus \left(\frac{1}{3} \cdot P_3 + \frac{2}{3} \cdot P_4\right) \oplus X_2 \qquad \text{(using simplification)}$$

Canceling X_2 gives the system:

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot X_2 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus \left(\frac{1}{3} \cdot P_3 + \frac{2}{3} \cdot P_4\right)$$

Substituting X_2 into X_1 gives the system:

$$X_1 \geqslant P_1 \oplus \left(\frac{1}{2} \cdot P_2 + \frac{1}{2} \cdot P_3\right) \oplus \left(\frac{2}{3} \cdot P_3 + \frac{1}{3} \cdot P_4\right) \oplus \left(\frac{1}{4} \cdot P_1 + \frac{1}{4} \cdot P_4 + \frac{1}{2} \cdot P_3\right)$$
$$X_2 \geqslant P_2 \oplus \left(\frac{1}{2} \cdot P_1 + \frac{1}{2} \cdot P_4\right) \oplus \left(\frac{1}{3} \cdot P_3 + \frac{2}{3} \cdot P_4\right)$$

From this final system, we conclude that the smallest polytope solution is

$$
\begin{aligned}
X_1 &= \mathrm{conv}\Big(P_1 \oplus \Big(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\Big) \oplus \Big(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\Big) \oplus \Big(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\Big) \Big) \\
&\overset{*}{=} \mathrm{conv}\Big(P_1 \oplus \Big(\frac{1}{2}\cdot P_2 + \frac{1}{2}\cdot P_3\Big) \oplus \Big(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\Big) \Big) \\
X_2 &= \mathrm{conv}\Big(P_2 \oplus \Big(\frac{1}{2}\cdot P_1 + \frac{1}{2}\cdot P_4\Big) \oplus \Big(\frac{1}{3}\cdot P_3 + \frac{2}{3}\cdot P_4\Big) \Big)
\end{aligned}
$$

The $(*)$ redundancy removal step uses the geometric fact that $\big(\frac{1}{4}\cdot P_1 + \frac{1}{4}\cdot P_4 + \frac{1}{2}\cdot P_3\big)$ is a convex linear combination of P_1 and $\big(\frac{2}{3}\cdot P_3 + \frac{1}{3}\cdot P_4\big)$ to drop that term (just like in Appendix A). Our algorithm foregoes such redundancy removal using geometric facts.

C Properties of Our Set Operations

Lemma C.1. *For subsets $A, B, C \subseteq \mathbb{R}^d$ and $0 < \rho < 1$, the following identities hold.*

$$A \mathbin{\overset{\circ}{\star}} A \sim A \tag{28}$$

$$A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C) = (A \mathbin{\overset{\circ}{\star}} B) \mathbin{\overset{\circ}{\star}} C \tag{29}$$

$$A \mathbin{\overset{\circ}{\star}} (B \oplus C) = (A \mathbin{\overset{\circ}{\star}} B) \ \oplus \ (A \mathbin{\overset{\circ}{\star}} C) \tag{30}$$

$$\rho \cdot (A \oplus B) = (\rho \cdot A) \ \oplus \ (\rho \cdot B) \tag{31}$$

$$\rho \cdot (A \mathbin{\overset{\circ}{\star}} B) = (\rho \cdot A) \ \mathbin{\overset{\circ}{\star}} \ (\rho \cdot B) \tag{32}$$

$$(A \mathbin{\overset{\circ}{\star}} B) + C \sim (A + C) \ \mathbin{\overset{\circ}{\star}} \ (B + C) \tag{33}$$

Proof of Equation 28 $A \mathbin{\overset{\circ}{\star}} A \sim A$. We will show that $\mathrm{conv}\Big(A \mathbin{\overset{\circ}{\star}} A\Big) = \mathrm{conv}(A)$.

First direction. To prove $\mathrm{conv}(A) \subseteq \mathrm{conv}\Big(A \mathbin{\overset{\circ}{\star}} A\Big)$, it suffices to prove that $A \subseteq A \mathbin{\overset{\circ}{\star}} A$. This result follows from the observation that, for any point $a \in A$, we can rewrite $a = \frac{1}{2}\cdot a + \frac{1}{2}\cdot a \in A \mathbin{\overset{\circ}{\star}} A$.

Second direction. To prove $\mathrm{conv}\Big(A \mathbin{\overset{\circ}{\star}} A\Big) \subseteq \mathrm{conv}(A)$, it suffices to prove that $A \mathbin{\overset{\circ}{\star}} A \subseteq \mathrm{conv}(A)$. For this result, consider a point $\lambda \cdot a + (1-\lambda)\cdot a' \in A \mathbin{\overset{\circ}{\star}} A$, for some $a, a' \in A$ and $0 < \lambda < 1$. By the convexity of the set $\mathrm{conv}(A)$, it is immediate that $\lambda \cdot a + (1-\lambda)\cdot a' \in \mathrm{conv}(A)$ for any $a, a' \in A \subseteq \mathrm{conv}(A)$. □

Proof of Equation 29 $A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C) = (A \mathbin{\overset{\circ}{\star}} B) \mathbin{\overset{\circ}{\star}} C$. We show that both sets $A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C)$ and $(A \mathbin{\overset{\circ}{\star}} B) \mathbin{\overset{\circ}{\star}} C$ are equal to the following set:

$$L \ \coloneqq \ \Big\{ \alpha\cdot a + \beta\cdot b + \gamma\cdot c : \ a \in A, b \in B, c \in C, \text{ and } \alpha, \beta, \gamma > 0 \text{ satisfying } \alpha + \beta + \gamma = 1 \Big\}.$$

Proof of $L = A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C)$:

First direction. $L \subseteq A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C)$. Consider arbitrary points $a \in A, b \in B, c \in C$ and reals $\alpha, \beta, \gamma \in (0,1)$, where $\alpha + \beta + \gamma = 1$. Then, we can rewrite the point $\alpha\cdot a + \beta\cdot b + \gamma\cdot c \in L$ as follows:

$$\alpha\cdot a + (1-\alpha)\cdot\left(\frac{\beta}{1-\alpha}\cdot b + \frac{\gamma}{1-\alpha}\cdot c\right).$$

This element belongs to $A \mathbin{\overset{\circ}{\star}} (B \mathbin{\overset{\circ}{\star}} C)$ because $\alpha, \frac{\beta}{1-\alpha}, \frac{\gamma}{1-\alpha} \in (0,1)$, and $\frac{\beta}{1-\alpha} + \frac{\gamma}{1-\alpha} = 1$

Second direction. $A \mathbin{\mathring{\star}} (B \mathbin{\mathring{\star}} C) \subseteq L$. Consider arbitrary points $a \in A, b \in B, c \in C$, and reals $\alpha, \lambda \in (0,1)$. Then, we can rewrite the point $\alpha \cdot a + (1-\alpha) \cdot (\lambda \cdot b + (1-\lambda) \cdot c) \in A \mathbin{\mathring{\star}} (B \mathbin{\mathring{\star}} C)$ as follows:

$$\alpha \cdot a + (1-\alpha)\lambda \cdot b + (1-\alpha)(1-\lambda) \cdot c.$$

This element belongs to L because $\alpha, (1-\alpha)\lambda, (1-\alpha)(1-\lambda)$ are positive reals adding to 1.

Proof of $L = (A \mathbin{\mathring{\star}} B) \mathbin{\mathring{\star}} C$: It follows from previous proof by exchanging A and C. □

Proof of Equation 30 $A \mathbin{\mathring{\star}} (B \oplus C) = (A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C)$. We show that $A \mathbin{\mathring{\star}} (B \oplus C) \subseteq (A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C)$ and $(A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C) \subseteq A \mathbin{\mathring{\star}} (B \oplus C)$.

First direction $A \mathbin{\mathring{\star}} (B \oplus C) \subseteq (A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C)$. Consider arbitrary point $e \in A \mathbin{\mathring{\star}} (B \oplus C)$. Then, there are points $a \in A, d \in B \oplus C$ and real $\lambda \in (0,1)$ such that $e = \lambda \cdot a + (1-\lambda) \cdot d$. Since $d \in B \oplus C$, we have $d \in B$ or $d \in C$. If $d \in B$, then $e \in A \mathbin{\mathring{\star}} B$, and if $d \in C$, then $e \in A \mathbin{\mathring{\star}} C$. Thus, we have $e \in (A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C)$.

Second direction $(A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C) \subseteq A \mathbin{\mathring{\star}} (B \oplus C)$. Consider arbitrary $e \in A \mathbin{\mathring{\star}} B$. Then, there are $a \in A, b \in B$, and real $\lambda \in (0,1)$ such that $e = \lambda \cdot a + (1-\lambda) \cdot b$. Since $b \in B \oplus C$, we have $e \in A \mathbin{\mathring{\star}} (B \oplus C)$. This implies that $A \mathbin{\mathring{\star}} B \subseteq A \mathbin{\mathring{\star}} (B \oplus C)$. Similarly, we can show that $A \mathbin{\mathring{\star}} C \subseteq A \mathbin{\mathring{\star}} (B \oplus C)$. Thus, we have $(A \mathbin{\mathring{\star}} B) \oplus (A \mathbin{\mathring{\star}} C) \subseteq A \mathbin{\mathring{\star}} (B \oplus C)$. □

Proof of Equation 31 $\rho \cdot (A \oplus B) = (\rho \cdot A) \oplus (\rho \cdot B)$. We will prove the following two directions.

First direction. $\rho \cdot (A \oplus B) \subseteq (\rho \cdot A) \oplus (\rho \cdot B)$. Consider arbitrary point $d \in \rho \cdot (A \oplus B)$. Then, there is a point $c \in A \oplus B$ such that $d = \rho \cdot c$. It follows from $c \in A \oplus B$ that $c \in A$ or $c \in B$. If $c \in A$, then we have $d = \rho \cdot c \in \rho \cdot A$, and if $c \in B$, then we have $d = \rho \cdot c \in \rho \cdot B$. Thus, we conclude that $d \in \rho \cdot A \oplus \rho \cdot B$.

Second direction. $(\rho \cdot A) \oplus (\rho \cdot B) \subseteq \rho \cdot (A \oplus B)$. Since $A \subseteq A \oplus B$, we have $\rho \cdot A \subseteq \rho \cdot (A \oplus B)$. Similarly, we have $\rho \cdot B \subseteq \rho \cdot (A \oplus B)$. This implies that $(\rho \cdot A) \oplus (\rho \cdot B) \subseteq \rho \cdot (A \oplus B)$. □

Proof of Equation 32 $\rho \cdot (A \mathbin{\mathring{\star}} B) = (\rho \cdot A) \mathbin{\mathring{\star}} (\rho \cdot B)$. We prove the following two directions.

First direction. $\rho \cdot (A \mathbin{\mathring{\star}} B) \subseteq (\rho \cdot A) \mathbin{\mathring{\star}} (\rho \cdot B)$. Consider arbitrary points $a \in A, b \in B$, and real $\lambda \in (0,1)$. Then, we can rewrite the point $\rho \cdot (\lambda \cdot a + (1-\lambda) \cdot b) \in \rho \cdot (A \mathbin{\mathring{\star}} B)$ as $\lambda \cdot (\rho \cdot a) + (1-\lambda) \cdot (\rho \cdot b) \in (\rho \cdot A) \mathbin{\mathring{\star}} (\rho \cdot B)$.

Second direction. $(\rho \cdot A) \mathbin{\mathring{\star}} (\rho \cdot B) \subseteq \rho \cdot (A \mathbin{\mathring{\star}} B)$. Consider arbitrary points $a \in A, b \in B$, and real $\lambda \in (0,1)$. Then, we can rewrite the point $\lambda \cdot (\rho \cdot a) + (1-\lambda) \cdot (\rho \cdot b) \in (\rho \cdot A) \mathbin{\mathring{\star}} (\rho \cdot B)$ as $\rho \cdot (\lambda \cdot a + (1-\lambda) \cdot b) \in \rho \cdot (A \mathbin{\mathring{\star}} B)$. □

Proof of Equation 33 $(A \mathbin{\mathring{\star}} B) + C \sim (A + C) \mathbin{\mathring{\star}} (B + C)$. We need to prove that $\operatorname{conv}\Big((A \mathbin{\mathring{\star}} B) + C\Big) = \operatorname{conv}\Big((A + C) \mathbin{\mathring{\star}} (B + C)\Big)$.

First direction $\operatorname{conv}\Big((A \mathbin{\mathring{\star}} B) + C\Big) \subseteq \operatorname{conv}\Big((A + C) \mathbin{\mathring{\star}} (B + C)\Big)$. It suffices to prove that $(A \mathbin{\mathring{\star}} B) + C \subseteq (A + C) \mathbin{\mathring{\star}} (B + C)$. Consider a point $(\lambda \cdot a + (1 - \lambda) \cdot b) + c \in \Big(A \mathbin{\mathring{\star}} B\Big) + C$ for some $a \in A, b \in B, c \in C$, and $0 < \lambda < 1$. We rewrite this point as $\lambda \cdot (a + c) + (1 - \lambda) \cdot (b + c)$, which is an element in $(A + C) \mathbin{\mathring{\star}} (B + C)$.

Second direction $\operatorname{conv}\Big((A + C) \mathbin{\mathring{\star}} (B + C)\Big) \subseteq \operatorname{conv}\Big((A \mathbin{\mathring{\star}} B) + C\Big)$. It suffices to prove that $(A + C) \mathbin{\mathring{\star}} (B + C) \subseteq \operatorname{conv}\Big((A \mathbin{\mathring{\star}} B) + C\Big)$. Consider a point $\lambda \cdot (a + c) + (1 - \lambda) \cdot (b + c') \in (A + C) \mathbin{\mathring{\star}} (B + C)$ for some $a \in A, b \in B$, $c, c' \in C$, and $0 < \lambda < 1$. We rewrite the point as follows

$$\lambda \cdot ((\lambda \cdot a + (1 - \lambda) \cdot b) + c) + (1 - \lambda) \cdot \big((\lambda \cdot a + (1 - \lambda) \cdot b) + c'\big) \in \operatorname{conv}\Big((A \mathbin{\mathring{\star}} B) + C\Big).$$

□

D Gaussian Elimination Algorithm

For brevity, for this section, we extend the evaluation map to Boolean predicates of the following form: $\operatorname{eval}(X \geqslant \varphi; \mathbf{X}, \mathbf{P})$ is true if (and only if) $\operatorname{eval}(X; \mathbf{X}, \mathbf{P}) \geqslant \operatorname{eval}(\varphi; \mathbf{X}, \mathbf{P})$, where X is an unknown and φ is a polynomial over $\mathrm{CL}(\Omega)$. To prove Theorem 2, we will need the following results.

Overview. We present a high-level overview of the results proven in this section and how they will be used.

1. Rearrangement lemma (Lemma D.1): Given an inequality $X \geqslant \varphi$, this lemma rewrites it as an "equivalent" inequality with a very specific structure:

   $$X \geqslant \varphi' \oplus X \mathbin{\mathring{\star}} M_1 \oplus \cdots \oplus X \mathbin{\mathring{\star}} M_k,$$

   where φ' is a polynomial and $M_1, \ldots, M_k$ are monomials over $\mathrm{CL}(\Omega \setminus \{X\})$. Here, two inequalities are considered equivalent when both are simultaneously true or both are simultaneously false for all assignments.

2. Cancellation lemma (Lemma D.2): Consider a system where the inequality for X has the structure promised by the rearrangement lemma above. Cancellation lemma presents a polynomial $\widetilde{\varphi}$ over $\mathrm{CL}(\Omega \setminus \{X\})$ such that replacing the structured inequality with $X \geqslant \widetilde{\varphi}$ preserves the smallest solution for all assignments. Together with the rearrangement lemma above, the cancellation lemma eliminates X from the RHS of the inequality for the unknown X.

3. Substitution lemma (Lemma D.3): Consider a system with inequalities $X \geqslant \varphi_X$ and $Y \geqslant \varphi_Y$, where φ_X is a polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$. Our objective is to construct a new system where $Y \geqslant \varphi_X$ is replaced by the inequality $Y \geqslant \varphi_Y [\![X \leftarrow \varphi_X]\!]$. The substitution lemma will prove that the new system's smallest solution is identical to the smallest solution of the original system. We can iteratively use this lemma for all unknowns $Y \in \Omega \setminus \{X\}$ to remove the dependence on the unknown X from every polynomial in the system.

D.1 Rearrangement and Cancellation Lemmas

Lemma D.1 (Rearrangement Lemma)**.** *For an unknown $X \in \Omega$, and a polynomial φ over $\mathrm{CL}(\Omega)$, there is a polynomial φ' and monomials $M_1, M_2, \ldots, M_k$ over $\mathrm{CL}(\Omega \setminus \{X\})$, where $k \geqslant 0$, such that (for any assignment $\mathbf{X}$ and $\mathbf{P}$) the following identity holds.*

$$\mathrm{eval}(X \geqslant \varphi \,;\, \mathbf{X}, \mathbf{P}) = \mathrm{eval}\left(X \geqslant \varphi' \;\oplus\; X \mathbin{\mathring{\star}} M_1 \;\oplus \cdots \oplus\; X \mathbin{\mathring{\star}} M_k \,;\, \mathbf{X}, \mathbf{P}\right).$$

Proof. If $\varphi = \emptyset$, then $\varphi' = \emptyset$ and $k = 0$.

Otherwise, suppose $\varphi = N_1 \;\oplus\; \cdots \;\oplus\; N_\ell$ and $\ell \geqslant 1$. We say that a monomial $M = E_1 \mathbin{\mathring{\star}} E_2 \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} E_u$ *depends on* X if there is $i \in \{1, 2, \ldots, u\}$ such that $E_i = \rho \cdot X + (1 - \rho) \cdot E'$, where $0 < \rho < 1$ and $E' \in \mathrm{CL}(\Omega \setminus \{X\})$. If the polynomial φ has no monomial depending on X, then $\varphi' = \varphi$ and $k = 0$.

Otherwise, $I \subseteq \{1, 2, \ldots, u\}$ be the subset of indices i such that the monomial N_i does not depend on X. The complement $J = \{1, 2, \ldots, u\} \setminus I$ be the subset of indices i such that the monomial N_i depends on X. Without loss of generality, let $J = \{1, 2, \ldots, k\}$, where $k \geqslant 1$, and $I = \{k + 1, \ldots, \ell\}$. For index $i \in J$, let

$$N_i = (\rho_1 \cdot X + (1 - \rho_1) \cdot E_1) \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} (\rho_{v_i} \cdot X + (1 - \rho_{v_i}) \cdot E_{v_i}) \mathbin{\mathring{\star}} E_{v_i+1} \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} E_{u_i},$$

such that $1 \leqslant v_i \leqslant u_i$, $E_1, \ldots, E_{u_i} \in \mathrm{CL}(\Omega \setminus \{X\})$, and $\rho_1, \rho_2, \ldots, \rho_{v_i} \in (0, 1)$. Define the following monomial over $\mathrm{CL}(\Omega \setminus \{X\})$.

$$M_i \;\coloneqq\; E_1 \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} E_{v_i} \mathbin{\mathring{\star}} E_{v_i+1} \mathbin{\mathring{\star}} \cdots \mathbin{\mathring{\star}} E_{u_i}.$$

Define the following polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$.

$$\varphi' \;\coloneqq\; N_{k+1} \;\oplus \cdots \oplus\; N_\ell.$$

Now, for any assignment $\mathbf{X}$ and $\mathbf{P}$, we have the following argument.

$$\begin{aligned}
\mathrm{eval}\,(X \geqslant \varphi \,;\, \mathbf{X}, \mathbf{P}) &= \mathrm{eval}\,(X \geqslant N_1 \;\oplus \cdots \oplus\; N_\ell \,;\, \mathbf{X}, \mathbf{P}) \\
&= \bigwedge_{i=1}^{\ell} \mathrm{eval}\,(X \geqslant N_i \,;\, \mathbf{X}, \mathbf{P}) \\
&= \left(\bigwedge_{1 \leqslant i \leqslant k} \mathrm{eval}\,(X \geqslant N_i \,;\, \mathbf{X}, \mathbf{P})\right) \wedge \left(\bigwedge_{k+1 \leqslant i \leqslant \ell} \mathrm{eval}\,(X \geqslant N_i \,;\, \mathbf{X}, \mathbf{P})\right) \\
&= \mathrm{eval}\left(X \geqslant \varphi' \,;\, \mathbf{X}, \mathbf{P}\right) \wedge \left(\bigwedge_{1 \leqslant i \leqslant k} \mathrm{eval}\,(X \geqslant N_i \,;\, \mathbf{X}, \mathbf{P})\right) \\
&\overset{\dagger}{=} \mathrm{eval}\left(X \geqslant \varphi' \,;\, \mathbf{X}, \mathbf{P}\right) \wedge \left(\bigwedge_{1 \leqslant i \leqslant k} \mathrm{eval}\left(X \geqslant X \mathbin{\mathring{\star}} M_i \,;\, \mathbf{X}, \mathbf{P}\right)\right) \\
&= \mathrm{eval}\left(X \geqslant \varphi' \;\oplus\; X \mathbin{\mathring{\star}} M_1 \;\oplus \cdots \oplus\; X \mathbin{\mathring{\star}} M_k \,;\, \mathbf{X}, \mathbf{P}\right)
\end{aligned}$$

The explanation of (†) is that $\mathrm{eval}\,(X \geqslant N_i \,;\, \mathbf{X}, \mathbf{P}) = \mathrm{eval}\left(X \geqslant X \mathbin{\mathring{\star}} M_i \,;\, \mathbf{X}, \mathbf{P}\right)$ by using Lemma D.4 on $E_1, \ldots, E_{v_i}$, and, finally, using the idempotence $X = X \mathbin{\mathring{\star}} X$ (when $X \in \mathcal{C}_d(\mathbb{R})$) from Equation 28. □

Lemma D.2 (Cancellation Lemma)**.** *Consider a system I with an inequality*

$$X \geqslant \left(\bigoplus_{i=1}^{k'} M_i' \right) \oplus \left(\bigoplus_{j=1}^{k} X \overset{o}{\star} M_j \right),$$

where $M_1, \ldots, M_k, M_1', \ldots, M_{k'}'$ are monomials over $\mathrm{CL}(\Omega \setminus \{X\})$. Define a new system I' identical to I except that the inequality above is replaced by

$$X \geqslant \bigoplus_{i=1}^{k'} \left(M_i' \oplus \left(\bigoplus_{j=1}^{k} M_i' \overset{o}{\star} M_j \right) \right)$$

Then, $\mathrm{ss}(I; \mathbf{P}) = \mathrm{ss}(I'; \mathbf{P})$ for all constant assignments $\mathbf{P}$.

Proof. Our proof will have two components. For arbitrary constant assignments $\mathbf{P}$, we have:

1. $\mathrm{sol}(I; \mathbf{P}) \subseteq \mathrm{sol}(I'; \mathbf{P})$.
2. $\mathrm{ss}(I'; \mathbf{P}) \in \mathrm{sol}(I; \mathbf{P})$.

These two results imply that $\mathrm{ss}(I; \mathbf{P}) = \mathrm{ss}(I'; \mathbf{P})$.

Part 1. For this part, it suffices to prove that

$$\mathrm{eval}\left(X \geqslant \left(\bigoplus_{i=1}^{k'} M_i' \right) \oplus \left(\bigoplus_{j=1}^{k} X \overset{o}{\star} M_i \right) \;;\; \mathbf{X}, \mathbf{P} \right)$$

implies $\mathrm{eval}\left(X \geqslant M_i' \;;\; \mathbf{X}, \mathbf{P}\right)$ and $\mathrm{eval}\left(X \geqslant M_i' \overset{o}{\star} M_j \;;\; \mathbf{X}, \mathbf{P}\right)$, for all $i \in \{1, 2, \ldots, k'\}$ and $j \in \{1, 2, \ldots, k\}$. Note that the implication $\mathrm{eval}\left(X \geqslant M_i' \;;\; \mathbf{X}, \mathbf{P}\right)$ is obvious. Next, observe that we also have the implication $\mathrm{eval}\left(X \geqslant X \overset{o}{\star} M_j \;;\; \mathbf{X}, \mathbf{P}\right)$, which (in turn) implies $\mathrm{eval}\left(X \geqslant M_i' \overset{o}{\star} M_j \;;\; \mathbf{X}, \mathbf{P}\right)$. This concludes the proof of the first part.

Part 2. Let $\mathrm{ss}(I'; \mathbf{P})_X \coloneqq \mathrm{eval}\left(X \;;\; \mathrm{ss}(I'; \mathbf{P}), \mathbf{P}\right)$, the assignment to the unknown X in the smallest solution $\mathrm{ss}(I'; \mathbf{P})$. Similarly, let $\mathrm{ss}(I'; \mathbf{P})_{\setminus X}$ represent the assignment to unknowns other than X by $\mathrm{ss}(I'; \mathbf{P})$. Define

$$A_{\mathbf{P}} \coloneqq \mathrm{eval}\left(\bigoplus_{i=1}^{k'} \left(M_i' \oplus \left(\bigoplus_{j=1}^{k} M_i' \overset{o}{\star} M_j \right) \right) \;;\; \mathrm{ss}(I'; \mathbf{P})_{\setminus X}, \mathbf{P} \right).$$

Here, we are using the fact that M_i' and M_j being monomials over $\mathrm{CL}(\Omega \setminus \{X\})$. Note that $\mathrm{ss}(I'; \mathbf{P})_X = \mathrm{conv}(A_{\mathbf{P}})$; otherwise, replacing $\mathrm{ss}(I'; \mathbf{P})_X$ by $\mathrm{conv}(A_{\mathbf{P}})$ (and leaving the other unknown assignments identical) creates a smaller solution in $\mathrm{sol}(I'; \mathbf{P})$.

After this, to prove $\mathrm{ss}(I'; \mathbf{P}) \in \mathrm{sol}(I; \mathbf{P})$, it suffices to prove that

$$\mathrm{eval}\left(X \geqslant \left(\bigoplus_{i=1}^{k'} M_i' \right) \oplus \left(\bigoplus_{j=1}^{k} X \overset{o}{\star} M_j \right) \;;\; \mathrm{ss}(I'; \mathbf{P}), \mathbf{P} \right) \text{ is true.}$$

It is equivalent to proving

$$\mathrm{eval}\left(\mathrm{conv}(A_{\mathbf{P}}) \geqslant \left(\bigoplus_{i=1}^{k'} M_i' \right) \oplus \left(\bigoplus_{j=1}^{k} \mathrm{conv}(A_{\mathbf{P}}) \overset{o}{\star} M_j \right) \;;\; \mathrm{ss}(I'; \mathbf{P})_{\setminus X}, \mathbf{P} \right) \text{ is true.}$$

For brevity, let us introduce some notation. Define

$$U_{\mathbf{P}} \coloneqq \operatorname{eval}\left(\bigoplus_{i=1}^{k'} M_i' \;;\; \operatorname{ss}(I';\mathbf{P})_{\setminus X}, \mathbf{P}\right)$$
$$V_{\mathbf{P}} \coloneqq \operatorname{eval}\left(\bigoplus_{j=1}^{k} M_j \;;\; \operatorname{ss}(I';\mathbf{P})_{\setminus X}, \mathbf{P}\right).$$

Note that $\operatorname{conv}(A_{\mathbf{P}}) = \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big)$. Using this new notation, we need to prove that

$$\begin{aligned}
& \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; \operatorname{conv}\Big(U_{\mathbf{P}} \oplus U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \mathbin{\mathring{\star}} V_{\mathbf{P}} \\
\iff \quad & \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; \Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \mathbin{\mathring{\star}} V_{\mathbf{P}} \\
\iff \quad & \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \\
\iff \quad & \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} \operatorname{conv}(V_{\mathbf{P}}) \qquad \text{(By Equation 28)} \\
\iff \quad & \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}} \\
\iff \quad & \operatorname{conv}\Big(U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}}\Big) \geqslant U_{\mathbf{P}} \;\oplus\; U_{\mathbf{P}} \mathbin{\mathring{\star}} V_{\mathbf{P}},
\end{aligned}$$

which is trivially true, completing the proof of part 2. □

D.2 Substitution Lemma

Lemma D.3 (Substitution Lemma)**.** *Consider a system I' containing two inequalities $X \geqslant \varphi_X$ and $Y \geqslant \varphi_Y$, where φ_X is a polynomial over $\operatorname{CL}(\Omega \setminus \{X\})$ and φ_Y is a polynomial over $\operatorname{CL}(\Omega)$. Define a new system I'' identical to I' except that the inequality $Y \geqslant \varphi_Y$ is replaced by $Y \geqslant \varphi_Y[\![X \leftarrow \varphi_X]\!]$. Then, $\operatorname{ss}(I';\mathbf{P}) = \operatorname{ss}(I'';\mathbf{P})$ for all constant assignments $\mathbf{P}$.*

Proof. Our proof will have two components. For arbitrary constant assignments $\mathbf{P}$, we have:

1. $\operatorname{sol}(I';\mathbf{P}) \subseteq \operatorname{sol}(I'';\mathbf{P})$.
2. $\operatorname{ss}(I'';\mathbf{P}) \in \operatorname{sol}(I';\mathbf{P})$.

These two result imply that $\operatorname{ss}(I';\mathbf{P}) = \operatorname{ss}(I'';\mathbf{P})$.

Part 1. For this part, it suffices to prove that $\operatorname{eval}(X \geqslant \varphi_X \;;\; \mathbf{X}, \mathbf{P})$ and $\operatorname{eval}(Y \geqslant \varphi_Y \;;\; \mathbf{X}, \mathbf{P})$ implies $\operatorname{eval}(Y \geqslant \varphi_Y[\![X \leftarrow \varphi_X]\!] \;;\; \mathbf{X}, \mathbf{P})$ when $\mathbf{X}$ is an assignment. Note that (read the derivation left to right).

$$\operatorname{eval}(\varphi_Y[\![X \leftarrow \varphi_X]\!] \;;\; \mathbf{X}, \mathbf{P}) \overset{*}{\sim} \operatorname{eval}(\varphi_Y \;;\; (\mathbf{X}, \mathbf{P})[\![X \leftarrow \varphi_X]\!]) \overset{\dagger}{\leqslant} \operatorname{eval}(\varphi_Y \;;\; \mathbf{X}, \mathbf{P}) \overset{\ddagger}{\leqslant} \operatorname{eval}(Y \;;\; \mathbf{X}, \mathbf{P}),$$

which completes the proof. The explanations for the derivation steps are below.

1. Step $*$ is true by the definition of substituted polynomial, see Lemma 1
2. Step $\dagger$ holds because $\operatorname{eval}(X \geqslant \varphi_X \;;\; \mathbf{X}, \mathbf{P})$
3. Step $\ddagger$ holds because $\operatorname{eval}(Y \geqslant \varphi_Y \;;\; \mathbf{X}, \mathbf{P})$

Part 2. It will suffice to prove that $\mathrm{eval}\,(Y \geqslant \varphi_Y \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P})$.

We first claim that $\mathrm{ss}(I'';\mathbf{P})_X \sim \mathrm{eval}\,(\varphi_X \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P})$; otherwise, we will find a smaller solution of I'', which is a contradiction. Suppose not; i.e., $\mathrm{ss}(I'';\mathbf{P})_X \in \mathcal{C}_d(\mathbb{R})$ is a strict superset of $A_{\mathbf{P}} \coloneqq \mathrm{conv}(\mathrm{eval}(\varphi_X \;;\; \mathrm{ss}(I'';\mathbf{P});\mathbf{P}))$. Recall that φ_X is a polynomial over $\mathrm{CL}(\Omega \setminus \{X\})$. Thus, replacing $\mathrm{ss}(I'';\mathbf{P})_X$ by $A_{\mathbf{P}}$ in the smallest solution creates a smaller solution.

As a result of the claim, for any polynomial φ over $\mathrm{CL}(\Omega)$, we have $\mathrm{eval}\,(\varphi \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P}) \sim \mathrm{eval}\,(\varphi \;;\; (\mathrm{ss}(I'';\mathbf{P}),\mathbf{P})\,[\![X \leftarrow \varphi_X]\!])$. In particular,

$$\mathrm{eval}\left(\varphi_Y \;;\; (\mathrm{ss}(I'';\mathbf{P}),\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]\right) \sim \mathrm{eval}\left(\varphi_Y \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P}\right).$$

By the definition of the polynomial $\varphi_Y\,[\![X \leftarrow \varphi_X]\!]$ over $\mathrm{CL}(\Omega \setminus \{X\})$ (see Lemma 1), we have

$$\mathrm{eval}\left(\varphi_Y \;;\; (\mathrm{ss}(I'';\mathbf{P}),\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]\right) \sim \mathrm{eval}\left(\varphi_Y\,[\![X \leftarrow \varphi_X]\!] \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P}\right).$$

Consequently, we have

$$\mathrm{eval}\left(\varphi_Y \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P}\right) \sim \mathrm{eval}\left(\varphi_Y\,[\![X \leftarrow \varphi_X]\!] \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P}\right).$$

At this point, we have the conclusion that evaluations of φ_Y and $\varphi_Y\,[\![X \leftarrow \varphi_X]\!]$ have the same convex hull.

Recall that $\mathrm{ss}(I'';\mathbf{P}) \in \mathcal{C}_d(\mathbb{R})^n$ is a solution of I'' and (as a result) $\mathrm{eval}\,(Y \geqslant \varphi_Y\,[\![X \leftarrow \varphi_X]\!] \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P})$ holds. Therefore, $\mathrm{eval}\,(Y \geqslant \varphi_Y \;;\; \mathrm{ss}(I'';\mathbf{P}),\mathbf{P})$ also holds, because φ_Y and $\varphi_Y\,[\![X \leftarrow \varphi_X]\!]$ have the same convex hull. This completes the proof of part 2. □

D.3 Proof of Substitution Correctness: Proof of Lemma 1

It suffices to prove the result when φ is a monomial (Equation 15). As a warmup, it is instructive to prove the result for a degree-1 monomial, i.e., an element of $\mathrm{CL}(\Omega)$ (Equation 14).

Warmup. Suppose $\varphi = E = (\rho \cdot X + (1-\rho)\cdot E')$, where E' is an element of $\mathrm{CL}(\Omega \setminus \{X\})$. We use properties of our set operations presented in Lemma C.1 for the following derivation in † and ‡ steps.

$$\begin{aligned}
&\mathrm{eval}\,(\varphi \;;\; (\mathbf{X},\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]) \\
&\quad= \mathrm{eval}\left(\rho \cdot X + (1-\rho)\cdot E' \;;\; (\mathbf{X},\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]\right) && \text{(By the definition of } \varphi) \\
&\quad= \rho \cdot \mathrm{eval}\,(X \;;\; (\mathbf{X},\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]) + (1-\rho)\cdot \mathrm{eval}\left(E' \;;\; (\mathbf{X},\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]\right) \\
&\qquad\qquad && \text{(By the definition of the evaluation map)} \\
&\quad= \rho \cdot \mathrm{eval}\left(\varphi_X \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) + (1-\rho)\cdot \mathrm{eval}\left(E' \;;\; (\mathbf{X},\mathbf{P})\,[\![X \leftarrow \varphi_X]\!]\right) \\
&\qquad\qquad && (\mathbf{X}_{\setminus X} \text{ is the unknown assignment restricted to unknowns} \neq X) \\
&\qquad\qquad && \text{(By the definition of } \mathbf{X}\,[\![X \leftarrow \varphi_X]\!] \text{ and } \varphi_X \text{ is polynomial over } \mathrm{CL}(\Omega \setminus \{X\})) \\
&\quad= \rho \cdot \mathrm{eval}\left(\varphi_X \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) + (1-\rho)\cdot \mathrm{eval}\left(E' \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) \\
&\qquad\qquad && \text{(Because } E' \in \mathrm{CL}(\Omega \setminus \{X\})) \\
&\quad= \rho \cdot \mathrm{eval}\left(\bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\bigstar}_{F \in \mathrm{supp}(M)} F \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) + (1-\rho)\cdot \mathrm{eval}\left(E' \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) \\
&\qquad\qquad && \text{(By the definition of the polynomial } \varphi_X) \\
&\quad= \rho \cdot \left(\bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\bigstar}_{F \in \mathrm{supp}(M)} \mathrm{eval}\left(F \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right)\right) + (1-\rho)\cdot \mathrm{eval}\left(E' \;;\; \mathbf{X}_{\setminus X},\mathbf{P}\right) \\
&\qquad\qquad && \text{(By the definition of the evaluation map)}
\end{aligned}$$

$$
\begin{aligned}
&\overset{\dagger}{=} \left(\bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\star}_{F \in \mathrm{supp}(M)} \rho \cdot \mathrm{eval}\left(F \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \right) + (1-\rho) \cdot \mathrm{eval}\left(E' \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \\
&\qquad\qquad \text{(Because scalar multiplication distributes over } \oplus \text{ and } \overset{\circ}{\star}\text{)} \\
&\overset{\ddagger}{\sim} \bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\star}_{F \in \mathrm{supp}(M)} \left(\rho \cdot \mathrm{eval}\left(F \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) + (1-\rho) \cdot \mathrm{eval}\left(E' \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \right) \\
&\qquad\qquad \text{(Because Minkowski sum distributes over } \oplus \text{ and } \overset{\circ}{\star}\text{)} \\
&= \bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\star}_{F \in \mathrm{supp}(M)} \mathrm{eval}\left(E[\![X \leftarrow F]\!] \,;\, \mathbf{X}_{\setminus X}, \mathbf{P} \right) \\
&\qquad\qquad \text{(By the definition of } E[\![X \leftarrow F]\!]\text{)} \\
&= \mathrm{eval}\left(\bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\star}_{F \in \mathrm{supp}(M)} E[\![X \leftarrow F]\!] \,;\, \mathbf{X}_{\setminus X}, \mathbf{P} \right) \\
&\qquad\qquad \text{(By the definition of the evaluation map)} \\
&= \mathrm{eval}\left(\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \\
&\qquad\qquad \text{(By the definition of the polynomial } \varphi[\![X \leftarrow \varphi_X]\!] \text{ over } \mathrm{CL}(\Omega \setminus \{X\})\text{)} \\
&= \mathrm{eval}\left(\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \,;\, \mathbf{X}, \mathbf{P}\right).
\end{aligned}
$$

This completes the proof of the warmup case.

Primary case: φ is a monomial. The full proof is similar to the warmup proof.

$$
\begin{aligned}
&\mathrm{eval}\left(\varphi \,;\, (\mathbf{X}, \mathbf{P})[\![X \leftarrow \varphi_X]\!]\right) \\
&\quad = \mathrm{eval}\left(\overset{\circ}{\star}_{E \in \mathrm{supp}(\varphi)} E \,;\, (\mathbf{X}, \mathbf{P})[\![X \leftarrow \varphi_X]\!] \right) \\
&\qquad\qquad \text{(By the definition of } \varphi\text{)} \\
&\quad = \overset{\circ}{\star}_{E \in \mathrm{supp}(\varphi)} \mathrm{eval}\left(E \,;\, (\mathbf{X}, \mathbf{P})[\![X \leftarrow \varphi_X]\!]\right) \\
&\qquad\qquad \text{(By the definition of the evaluation map)} \\
&\quad \sim \overset{\circ}{\star}_{E \in \mathrm{supp}(\varphi)} \left(\bigoplus_{M \in \mathrm{mono}(\varphi_X)} \overset{\circ}{\star}_{F \in \mathrm{supp}(M)} \mathrm{eval}\left(E[\![X \leftarrow F]\!] \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \right) \\
&\qquad\qquad \text{(By the derivation in the warmup case to one step after the } \ddagger \text{ step)} \\
&\quad = \bigoplus_{\vec{N} \in \mathrm{mono}(\varphi_X)^{\mathrm{supp}(\varphi)}} \overset{\circ}{\star}_{E \in \mathrm{supp}(\varphi)} \left(\overset{\circ}{\star}_{F \in \mathrm{supp}(\vec{N}(E))} \mathrm{eval}\left(E[\![X \leftarrow F]\!] \,;\, \mathbf{X}_{\setminus X}, \mathbf{P}\right) \right) \\
&\qquad\qquad \text{(Because } \overset{\circ}{\star} \text{ distributes over } \oplus\text{)} \\
&\quad = \mathrm{eval}\left(\bigoplus_{\vec{N} \in \mathrm{mono}(\varphi_X)^{\mathrm{supp}(\varphi)}} \overset{\circ}{\star}_{E \in \mathrm{supp}(\varphi)} \left(\overset{\circ}{\star}_{F \in \mathrm{supp}(\vec{N}(E))} E[\![X \leftarrow F]\!] \right) \,;\, \mathbf{X}_{\setminus X}, \mathbf{P} \right) \\
&\qquad\qquad \text{(By the definition of the evaluation map)} \\
&\quad = \mathrm{eval}\left(\varphi\left[\!\left[X \leftarrow \varphi_X\right]\!\right] \,;\, \mathbf{X}, \mathbf{P}\right). \\
&\qquad\qquad \text{(By the definition of the polynomial } \varphi[\![X \leftarrow \varphi_X]\!] \text{ over } \mathrm{CL}(\Omega \setminus \{X\})\text{)}
\end{aligned}
$$

This completes the proof of Lemma 1

D.4 Technical Results

Lemma D.4. *Consider convex $X \in \mathcal{C}_d(\mathbb{R})$, arbitrary sets $A, B \subseteq \mathbb{R}^d$, and $0 < \rho < 1$.*

1. $X \geqslant (\rho \cdot X + (1-\rho) \cdot A)$ *if and only if* $X \geqslant X \mathbin{\mathring{\star}} A$

2. $X \geqslant (\rho \cdot X + (1-\rho) \cdot A) \mathbin{\mathring{\star}} B$ *if and only if* $X \geqslant X \mathbin{\mathring{\star}} A \mathbin{\mathring{\star}} B$

Proof of (1). We prove the following two directions.

Proof of 'if'. By definition, we have $\rho \cdot X + (1-\rho) \cdot A \subseteq X \mathbin{\mathring{\star}} A$ when $\rho \in (0,1)$. Therefore, $X \geqslant X \mathbin{\mathring{\star}} A$ implies $X \geqslant (\rho \cdot X + (1-\rho) \cdot A)$.

Proof of 'only if'. Suppose that $X \geqslant (\rho \cdot X + (1-\rho) \cdot A)$. Consider arbitrary $x \in X$, and $a \in A$. It follows from the assumption that $\rho \cdot x + (1-\rho) \cdot a \in X$. We will show that if $\rho \cdot x + (1-\rho) \cdot a \in X$ then $\lambda \cdot x + (1-\lambda) \cdot a \in X$, for all $\lambda \in (0,1)$. The proof will rely on the convexity of $X \in \mathcal{C}_d(\mathbb{R})$.

Define $x^{(0)} \coloneqq x$ and recall that $x^{(0)} \in X$. Then, inductively for $i \in \{0,1,2,\dots\}$, the point $x^{(i+1)} \coloneqq \rho \cdot x^{(i)} + (1-\rho) \cdot a$ also belongs to X using the fact that $X \geqslant \rho \cdot X + (1-\rho) \cdot A$. By convexity of X, the line segment joining the points x and $x^{(i)}$ is a subset of X.

Note that $x^{(i)} = \rho^i \cdot x + (1-\rho^i) \cdot a$. Consider arbitrary $\lambda \in (0,1)$ and any $i_\lambda \in \{0,1,2,\dots\}$ satisfying $\lambda < \rho^{i_\lambda}$. Then, the point $\lambda \cdot x + (1-\lambda) \cdot a$ is on the line segment joining x and $x^{(i_\lambda)}$, which is a subset of X.

This demonstrates that $\lambda \cdot X + (1-\lambda) \cdot A \subseteq X$, for any $\lambda \in (0,1)$; in turn, implying that $X \geqslant X \mathbin{\mathring{\star}} A$. Thus, $X \geqslant (\rho \cdot X + (1-\rho) \cdot A)$ implies $X \geqslant X \mathbin{\mathring{\star}} A$. □

Proof of part (2). We prove the following two directions.

Proof of 'if'. By definition, we have $(\rho \cdot X + (1-\rho) \cdot A) \mathbin{\mathring{\star}} B \subseteq \left(X \mathbin{\mathring{\star}} A\right) \mathbin{\mathring{\star}} B = X \mathbin{\mathring{\star}} A \mathbin{\mathring{\star}} B$ when $\rho \in (0,1)$. Therefore, $X \geqslant X \mathbin{\mathring{\star}} A \mathbin{\mathring{\star}} B$ implies $X \geqslant (\rho \cdot X + (1-\rho) \cdot A) \mathbin{\mathring{\star}} B$.

Proof of 'only if'. Suppose $X \geqslant (\rho \cdot X + (1-\rho) \cdot A) \mathbin{\mathring{\star}} B$. Consider arbitrary $x \in X, a \in A$, and $b \in B$, and reals $u, v \in (0,1)$. Let $\overline{u} = 1-u, \overline{v} = 1-v$. We will show that the point $p \coloneqq u \cdot x + \overline{u} \cdot (v \cdot a + \overline{v} \cdot b) \in X \mathbin{\mathring{\star}} A \mathbin{\mathring{\star}} B$ is also in X. This proof will again rely on the convexity of $X \in \mathcal{C}_d(\mathbb{R})$.

Inductively define a sequence of points $x^{(i)}$, for $i \in \{0,1,2,\dots\}$. To begin, define $x^{(0)} \coloneqq x$, and define

$$x^{(i+1)} \coloneqq \frac{v}{v + \overline{v}\,\overline{\rho}} \cdot \left(\rho \cdot x^{(i)} + \overline{\rho} \cdot a\right) + \frac{\overline{v}\,\overline{\rho}}{v + \overline{v}\,\overline{\rho}} \cdot b,$$

where $\overline{\rho} = 1-\rho$. Note that, inductively, if $x^{(i)} \in X$, then $x^{(i+1)} \in (\rho \cdot X + (1-\rho) \cdot A) \mathbin{\mathring{\star}} B$, so $x^{(i+1)} \in X$ according to the assumption. In summary, $\{x^{(0)}, x^{(1)}, \dots\} \subseteq X$.

We will prove that $x^{(i)}$ can be written as the following form:

$$x^{(i)} = \mu^{(i)} \cdot x + v(1-\mu^{(i)}) \cdot a + \overline{v}(1-\mu^{(i)}) \cdot b.$$

For (base case) $i = 0$, we know $\mu^{(0)} = 1$. By the recursive definition, we have:

$$\mu^{(i+1)} = \frac{v\rho}{v + \overline{v}\,\overline{\rho}} \cdot \mu^{(i)}$$

Let $\mu = \frac{v\rho}{v+\overline{v}\,\overline{\rho}}$, then we conclude that, for $i \in \{0,1,2,\dots\}$, we have:

$$x^{(i)} = \mu^i \cdot x + v(1-\mu^i) \cdot a + \overline{v}(1-\mu^i) \cdot b.$$

Observe that $0 < \mu < 1$. Let $i_u \in \{0, 1, 2, \dots\}$ be an index such that $\mu^{i_u} < u$. Then, the point p belongs to the line segment joining the points x and $x^{(i_u)}$. By convexity of X, we conclude that $p \in X$. □

Lemma D.5. *For any unknown assignments* $\mathbf{X} \geqslant \mathbf{Y}$ *and constant assignments* $\mathbf{P} \geqslant \mathbf{Q}$*, and any polynomial* φ *over* $\mathrm{CL}(\Omega)$*, we will have* $\mathrm{eval}(\varphi\,;\,\mathbf{X},\mathbf{P}) \geqslant \mathrm{eval}(\varphi\,;\,\mathbf{Y},\mathbf{Q})$*. Furthermore,* $\mathrm{eval}(\varphi\,;\,\mathbf{X},\mathbf{P}) \sim \mathrm{eval}(\varphi\,;\,\mathbf{Y},\mathbf{Q})$ *if* $\mathbf{X}_i \sim \mathbf{Y}_i$ *and* $\mathbf{P}_j \sim \mathbf{Q}_j$ *for every* $i \in \{1, 2, \dots, n\}$ *and* $j \in \{1, 2, \dots, t\}$*.*

Proof. It suffices to prove the result for monomials. Suppose $\mathbf{X} \geqslant \mathbf{Y}$, and $\mathbf{P} \geqslant \mathbf{Q}$. Then, $\mathbf{Y}_i \subseteq \mathbf{X}_i$ for each $i \in \{1, \dots, n\}$, and $\mathbf{Q}_i \subseteq \mathbf{P}_i$ for each $i \in \{1, \dots, t\}$. Let φ be a monomial M. For each $E = \lambda_1 \cdot X_1 + \cdots + \lambda_n \cdot X_n + \lambda_{n+1} \cdot P_1 + \cdots + \lambda_{n+t} \cdot P_t \in \mathrm{supp}(M)$, we have,

$$\begin{aligned}\mathrm{eval}(E; \mathbf{Y}, \mathbf{Q}) &= \lambda_1 \cdot \mathbf{Y}_1 + \cdots + \lambda_n \cdot \mathbf{Y}_n + \lambda_{n+1} \cdot \mathbf{Q}_1 + \cdots + \lambda_{n+t} \cdot \mathbf{Q}_t \\ &\subseteq \lambda_1 \cdot \mathbf{X}_1 + \cdots + \lambda_n \cdot \mathbf{X}_n + \lambda_{n+1} \cdot \mathbf{P}_1 + \cdots + \lambda_{n+t} \cdot \mathbf{P}_t \\ &= \mathrm{eval}(E; \mathbf{X}, \mathbf{P})\,.\end{aligned}$$

Thus, we have,

$$\begin{aligned}\mathrm{eval}(M\,;\,\mathbf{Y},\mathbf{Q}) &= \mathop{\overset{\circ}{\star}}_{E \in \mathrm{supp}(M)} \mathrm{eval}(E\,;\,\mathbf{Y},\mathbf{Q}) \\ &\subseteq \mathop{\overset{\circ}{\star}}_{E \in \mathrm{supp}(M)} \mathrm{eval}(E\,;\,\mathbf{X},\mathbf{P}) \\ &= \mathrm{eval}(M\,;\,\mathbf{X},\mathbf{P})\,.\end{aligned}$$

This implies that $\mathrm{eval}(M; \mathbf{X}, \mathbf{P}) \geqslant \mathrm{eval}(M; \mathbf{Y}, \mathbf{Q})$.

Now, suppose that $\mathbf{X}_i \sim \mathbf{Y}_i$ and $\mathbf{P}_j \sim \mathbf{Q}_j$ for every $i \in \{1, 2, \dots, n\}$ and $j \in \{1, 2, \dots, t\}$. Thus, $\mathrm{conv}(\mathbf{X}_i) = \mathrm{conv}(\mathbf{Y}_i)$, and $\mathrm{conv}(\mathbf{P}_j) = \mathrm{conv}(\mathbf{Q}_j)$ for every $i \in \{1, 2, \dots, n\}$ and $j \in \{1, 2, \dots, t\}$. For each $E = \lambda_1 \cdot X_1 + \cdots + \lambda_n \cdot X_n + \lambda_{n+1} \cdot P_1 + \cdots + \lambda_{n+t} \cdot P_t \in \mathrm{supp}(M)$, we have,

$$\begin{aligned}\mathrm{eval}(E\,;\,\mathbf{Y},\mathbf{Q}) &\subseteq \mathrm{conv}(\mathrm{eval}(E\,;\,\mathbf{Y},\mathbf{Q})) \\ &= \mathrm{conv}(\lambda_1 \cdot \mathbf{Y}_1 + \cdots + \lambda_n \cdot \mathbf{Y}_n + \lambda_{n+1} \cdot \mathbf{Q}_1 + \cdots + \lambda_{n+t} \cdot \mathbf{Q}_t) \\ &= \lambda_1 \cdot \mathrm{conv}(\mathbf{Y}_1) + \cdots + \lambda_n \cdot \mathrm{conv}(\mathbf{Y}_n) + \lambda_{n+1} \cdot \mathrm{conv}(\mathbf{Q}_1) + \cdots + \lambda_{n+t} \cdot \mathrm{conv}(\mathbf{Q}_t) \\ &= \lambda_1 \cdot \mathrm{conv}(\mathbf{X}_1) + \cdots + \lambda_n \cdot \mathrm{conv}(\mathbf{X}_n) + \lambda_{n+1} \cdot \mathrm{conv}(\mathbf{P}_1) + \cdots + \lambda_{n+t} \cdot \mathrm{conv}(\mathbf{P}_t) \\ &= \mathrm{conv}(\lambda_1 \cdot \mathbf{X}_1 + \cdots + \lambda_n \cdot \mathbf{X}_n + \lambda_{n+1} \cdot \mathbf{P}_1 + \cdots + \lambda_{n+t} \cdot \mathbf{P}_t) \\ &= \mathrm{conv}(\mathrm{eval}(E\,;\,\mathbf{X},\mathbf{P}))\end{aligned}$$

This implies that

$$\begin{aligned}\mathrm{eval}(M\,;\,\mathbf{Y},\mathbf{Q}) &= \mathop{\overset{\circ}{\star}}_{E \in \mathrm{supp}(M)} \mathrm{eval}(E\,;\,\mathbf{Y},\mathbf{Q}) \\ &\subseteq \mathop{\overset{\circ}{\star}}_{E \in \mathrm{supp}(M)} \mathrm{conv}(\mathrm{eval}(E\,;\,\mathbf{X},\mathbf{P})) \\ &\subseteq \mathrm{conv}\left(\mathop{\overset{\circ}{\star}}_{E \in \mathrm{supp}(M)} \mathrm{eval}(E\,;\,\mathbf{X},\mathbf{P})\right) && \text{(By Lemma D.7)} \\ &= \mathrm{conv}(\mathrm{eval}(M\,;\,\mathbf{X},\mathbf{P}))\,.\end{aligned}$$

Thus, we have,

$$\mathrm{conv}(\mathrm{eval}(M\,;\,\mathbf{Y},\mathbf{Q})) \subseteq \mathrm{conv}(\mathrm{eval}(M\,;\,\mathbf{X},\mathbf{P}))\,.$$

Similarly, we can show that $\text{conv}(\text{eval}\,(M\ ;\ \mathbf{X}, \mathbf{P})) \subseteq \text{conv}(\text{eval}\,(M\ ;\ \mathbf{Y}, \mathbf{Q}))$. Thus, we have

$$\text{conv}(\text{eval}\,(M\ ;\ \mathbf{X}, \mathbf{P})) = \text{conv}(\text{eval}\,(M\ ;\ \mathbf{Y}, \mathbf{Q})),$$

as desired. □

Lemma D.6. *Suppose I is a system and $X \geqslant \varphi_X$ is an inequality in it, where φ_X is a polynomial over $\text{CL}(\Omega \setminus \{X\})$. Then, $\text{ss}(I;\mathbf{P})_X = \text{conv}\big(\text{eval}(\varphi_X\ ;\ \text{ss}(I;\mathbf{P})_{\setminus X}, \mathbf{P})\big)$.*

Proof. Since $\text{ss}(I;\mathbf{P})$ is a solution of I, we have:

$$\begin{aligned}
\text{ss}(I;\mathbf{P})_X &\geqslant \text{eval}(\varphi_X; \text{ss}(I;\mathbf{P}), \mathbf{P}) \\
&= \text{eval}(\varphi_X; \text{ss}(I;\mathbf{P})_{\setminus X}, \mathbf{P}). && (\varphi_X \text{ is a polynomial over } \text{CL}(\Omega \setminus \{X\}))
\end{aligned}$$

This implies that $\text{ss}(I;\mathbf{P})_X \geqslant \text{conv}\big(\text{eval}(\varphi_X; \text{ss}(I;\mathbf{P})_{\setminus X}, \mathbf{P})\big)$. Now, it follows from the following claim that

$$\mathbf{Z}_Y = \begin{cases} \text{conv}\big(\ \text{eval}(\varphi_X\ ;\ \text{ss}(I;\mathbf{P})_{\setminus X}, \mathbf{P})\ \big) & \text{if } Y = X \\ \\ \text{ss}(I;\mathbf{P})_Y, & \text{if } Y \in \{X_1, \ldots, X_n\} \setminus \{X\} \end{cases}$$

is also a solution. This implies that $\text{ss}(I;\mathbf{P})_X = \text{conv}\big(\text{eval}(\varphi_X; \text{ss}(I;\mathbf{P})_{\setminus X}, \mathbf{P})\big)$.

Claim: $\mathbf{Y} \in \text{sol}(I;\mathbf{P})$ implies $\mathbf{Z} \in \text{sol}(I;\mathbf{P})$, where

$$\mathbf{Z}_Y = \begin{cases} \text{conv}(\ \text{eval}(\varphi_X\ ;\ \mathbf{Y}, \mathbf{P})\ ) & \text{if } Y = X \\ \\ \mathbf{Y}_Y, & \text{if } Y \in \{X_1, \ldots, X_n\} \setminus \{X\} \end{cases}$$

Proof. We show that $\mathbf{Z}_Y \geqslant \text{eval}(\varphi_Y; \mathbf{Z}, \mathbf{P})$ for each Y. We have the following two cases:

Case $Y = X$. We have:

$$\begin{aligned}
\mathbf{Z}_X &= \text{conv}(\ \text{eval}(\varphi_X\ ;\ \mathbf{Y}, \mathbf{P})\ ) \\
&\geqslant \text{eval}(\varphi_X\ ;\ \mathbf{Y}, \mathbf{P}) \\
&= \text{eval}(\varphi_X\ ;\ \mathbf{Z}, \mathbf{P}) && (\varphi_X \text{ is a polynomial over } \text{CL}(\Omega \setminus \{X\}), \text{ and } \mathbf{Y}_W = \mathbf{Z}_W \text{ for } W \neq X)
\end{aligned}$$

Case $Y \neq X$. First, note that $\mathbf{Y}_X \geqslant \text{eval}(\varphi_X; \mathbf{Y}, \mathbf{P})$ because $\mathbf{Y} \in \text{ss}(I;\mathbf{P})$. In particular, this implies that $\mathbf{Y}_X \geqslant \text{conv}(\text{eval}(\varphi_X; \mathbf{Y}, \mathbf{P})) = \mathbf{Z}_X$. This implies that $\mathbf{Y} \geqslant \mathbf{Z}$. So, we have:

$$\begin{aligned}
\mathbf{Z}_Y &= \mathbf{Y}_Y \\
&\geqslant \text{eval}(\varphi_Y\ ;\ \mathbf{Y}, \mathbf{P}) && (\text{Since } \mathbf{Y} \in \text{sol}(I;\mathbf{P})) \\
&\geqslant \text{eval}(\varphi_Y; \mathbf{Z}, \mathbf{P}) && (\text{Since } \mathbf{Y} \geqslant \mathbf{Z})
\end{aligned}$$

□

□

Lemma D.7. *Let $A, B \subseteq \mathbb{R}^d$. Then, $\text{conv}(A) \overset{o}{\star} \text{conv}(B) \subseteq \text{conv}\Big(A \overset{o}{\star} B\Big)$*

Proof. Consider an arbitrary element $z \in \mathrm{conv}(A) \mathbin{\mathring{\star}} \mathrm{conv}(B)$. It follows from Carathéodory's theorem that there are subsets $A' \subseteq A, B' \subseteq B$ of size at most $(d+1)$ such that

$$z = \lambda \cdot \left(\sum_{a \in A'} \lambda_a \cdot a \right) + \overline{\lambda} \cdot \left(\sum_{b \in B'} \lambda_b \cdot b \right),$$

where $\lambda_a \in [0,1]$ for each $a \in A'$, $\lambda_b \in [0,1]$ for each $b \in B'$, and $\lambda \in (0,1)$; and $\sum_{a \in A'} \lambda_a = 1$, $\sum_{b \in B'} \lambda_b = 1$, and $\lambda + \overline{\lambda} = 1$. Then, since

$$\sum_{a \in A',\, b \in B'} \lambda_a \lambda_b = \left(\sum_{a \in A'} \lambda_a \right) \left(\sum_{b \in B'} \lambda_b \right) = 1,$$

we have,

$$z = \lambda \cdot \left(\sum_{a \in A'} \lambda_a \cdot a \right) + \overline{\lambda} \cdot \left(\sum_{b \in B'} \lambda_b \cdot b \right) = \sum_{a \in A',\, b \in B'} \lambda_a \lambda_b \cdot \left(\lambda \cdot a + \overline{\lambda} \cdot b \right) \in \mathrm{conv}\Big(A \mathbin{\mathring{\star}} B \Big).$$

This completes the proof. □

E Algebraic Complexity of the Smallest Solution of a System of Inequalities

In this section, we will prove the following result.

Lemma E.1. *Let I be a system of inequalities over n unknowns. Suppose every inequality in a system I has (at most) k monomials, and each monomial has degree (at most) D. After our Gaussian elimination-inspired algorithm in Figure 4 terminates, every inequality in our system $I^{(n)}$ has (at most) $k^{(D+1)^n}$ monomials and each monomial has a degree (at most) D^{3^n}.*

Preparatory work. We say that the *complexity of a polynomial* φ over $\mathrm{CL}(\Omega)$ is (k, D) if it has (at most) k monomials, each of degree (at most) D.

Proposition 5. *Let φ and φ_X have complexities (k, D) and (k_X, D_X) respectively. The polynomial $\varphi[\![X \leftarrow \varphi_X]\!]$ has complexity $(k \cdot k_X^D,\ D \cdot D_X)$.*

Note that it suffices to prove this result for $k = 1$, i.e., when $\varphi = M$ is a monomial. By Equation 15, the number of monomials is k_X^D. The degree of each monomial in the substituted polynomial is $\underbrace{D_X + D_X + \cdots + D_X}_{D\text{-times}}$ in Equation 15.

In a system of inequalities $\{X_i \geqslant \varphi_i\}_{i=1}^n$, we say that the *complexity of the unknown* X_i is the complexity of the corresponding polynomial φ_i.

Proposition 6. *Let (k, D) be the complexity of X_j in the system I. Let I' be the system produced from I by rearranging X_j using the rearrangement lemma (Lemma D.1) and then canceling X_j using the cancellation lemma (Lemma D.2) Then, the complexity of X_j in the system I' is (k^2, D^2).*

Any element $\rho \cdot X_j + (1-\rho) \cdot E'$ is rearranged into $X \mathbin{\mathring{\star}} E'$, where $0 < \rho < 1$. Otherwise, the element is left unchanged if $\rho = 0$ or $\rho = 1$. Using the idempotence of $\mathring{\star}$, the degree of any monomial can either remain unchanged or increase by 1 during rearrangement. By the definition of the cancellation lemma, the degree of each monomial is at most D^2. The total number of monomials is at most $(\ (k+1)/2\ )^2 \leqslant k^2$.

Proof of Lemma E.1. We say that the *complexity of a system* is (k, D) if every unknown has complexity (k, D). Suppose we start with a system $I^{(0)}$ with complexity (k, D). Suppose $j = 1$. At the end of step 2.b. in Figure 4, the system I' has the following properties.

1. Complexity of X_1 is $\left(k^2, D^2\right)$
2. Complexity of any other variable is (k, D)

After substitution in step 2.c., the system $I^{(1)}$ has the following properties.

1. Complexity of X_1 is $\left(k^2, D^2\right)$
2. Complexity of any other variable is $\left(k^{D+1}, D^3\right)$

Thus, $I^{(1)}$ has complexity $\left(k^{D+1}, D^3\right)$. Iterating in this manner, we conclude that the system $I^{(n)}$ has complexity $\left(k^{(D+1)^n}, D^{3^n}\right)$.

F Operational Realization: Proof of Lemma 2

We prove that $\mathrm{itr}(I; \mathbf{P}) \in \mathcal{C}_d(\mathbb{R})^n$ is the smallest solution that contains the initialization set $\mathbf{X}^{(0)}$. This result will follow from the following two claims.

1. $\mathrm{itr}(I; \mathbf{P}) \in \mathrm{sol}(I; \mathbf{P})$, and
2. Any solution $\mathbf{Y} \in \mathcal{C}_d(\mathbb{R})^n$ satisfying $\mathbf{Y} \geqslant \mathbf{X}^{(0)}$, also satisfyies $\mathbf{Y} \geqslant \mathrm{itr}(I; \mathbf{P})$.

Part 1. Let us first show that $\mathrm{itr}(I; \mathbf{P}) \in \mathcal{C}_d(\mathbb{R})^n$ is a solution. We already know that it is an element of $\mathcal{C}_d(\mathbb{R})^n$. All that remains is to prove that it satisfies all the constraints. We will prove that $\mathrm{itr}(I; \mathbf{P})_j \geqslant \mathrm{eval}(\varphi_j \,;\, \mathrm{itr}(I, \mathbf{P}), \mathbf{P})$ for $j \in \{1, 2, \ldots, n\}$. Consider an arbitrary element

$$\mathbf{x}' = (\mathbf{x}'_1, \ldots, \mathbf{x}'_n) \in \mathrm{itr}(I; \mathbf{P}) = \bigcup_{i \geqslant 0} \mathrm{itr}(i, I; \mathbf{P}) = \bigcup_{i \geqslant 0} \mathbf{X}^{(i)} = \left(\bigcup_{i \geqslant 0} \mathbf{X}_1^{(i)}, \ldots, \bigcup_{i \geqslant 0} \mathbf{X}_n^{(i)} \right).$$

Then, for each $j \in \{1, \ldots, n\}$, there exists i_j such that $\mathbf{x}'_j \in \mathbf{X}_j^{(i_j)}$. Let $i^* = \max(i_1, \ldots, i_n)$. Then, we have $\mathbf{x}'_j \in \mathbf{X}_j^{(i_j)} \subseteq \mathbf{X}_j^{(i^*)}$. Then, for each $j \in \{1, \ldots, n\}$,

$$\mathrm{eval}(\varphi_j; \mathbf{x}', \mathbf{P}) \subseteq \mathrm{eval}(\varphi_j; \mathbf{X}^{(i^*)}, \mathbf{P}) \subseteq \mathrm{conv}\Big(\mathrm{eval}(\varphi_j; \mathbf{X}^{(i^*)}, \mathbf{P})\Big) = \mathbf{X}_j^{(i^*+1)} \subseteq \bigcup_{i \geqslant 0} \mathbf{X}_j^{(i)} = \mathrm{itr}(I; \mathbf{P})_j.$$

This implies that $\mathrm{eval}(\varphi_j; \mathrm{itr}(I; \mathbf{P}), \mathbf{P}) \subseteq \mathrm{itr}_j(I; \mathbf{P})$. Thus, for each $j \in \{1, \ldots, n\}$, $\mathrm{itr}(I; \mathbf{P})_j \geqslant \mathrm{eval}(\varphi_j; \mathrm{itr}(I; \mathbf{P}), \mathbf{P})$. So, $\mathrm{itr}(I; \mathbf{P})$ is a solution.

Part 2. Consider an arbitrary solution $\mathbf{Y} \in \mathcal{C}_d(\mathbb{R})^n$ such that $\mathbf{Y} \geqslant \mathbf{X}^{(0)}$. We will prove that $\mathbf{Y} \geqslant \mathrm{itr}(I; \mathbf{P})$. We plan to prove this statement by contradiction. If possible, suppose the statement is false; then there is $j' \in \{1, 2, \ldots, n\}$ such that $\mathbf{Z}_{j'} \cap \mathbf{Y}_{j'} \subsetneq \mathrm{itr}(I; \mathbf{P})_{j'}$, where $\mathbf{Z} \coloneqq \mathrm{itr}(I; \mathbf{P}) \cap \mathbf{Y}$. Using Proposition 3, the intersection of solutions is also a solution. Consequently, $\mathbf{Z}$ is a (strictly) smaller solution than these two solutions and $\mathbf{Z} \geqslant \mathbf{X}^{(0)}$; below, we prove its impossibility.

Consider the sequence of nested sets $\mathbf{X}^{(0)} \to \mathbf{X}^{(1)} \to \cdots$. Note that $\mathbf{Z} \geqslant \mathbf{X}^{(0)} = \mathrm{itr}(0; I, \mathbf{P})$ but $\mathbf{Z} \not\geqslant \mathrm{itr}(I; \mathbf{P}) = \bigcup_{i \geqslant 0} \mathrm{itr}(i, I; \mathbf{P})$.[3] Therefore, there is an $i \in \{1, 2, \dots, \}$ such that

$$\mathbf{Z} \geqslant \mathrm{itr}(i-1, I; \mathbf{P}) = \mathbf{X}^{(i-1)} \text{ but } \mathbf{Z} \not\geqslant \mathrm{itr}(i, I; \mathbf{P}) = \mathbf{X}^{(i)}.$$

This implies that there is $j^* \in \{1, 2, \dots, n\}$ such that

$$\mathbf{Z}_{j^*} \geqslant \mathbf{X}^{(i-1)}_{j^*} \text{ but } \mathbf{Z}_{j^*} \not\geqslant \mathbf{X}^{(i)}_{j^*}. \tag{34}$$

Recall that $\mathbf{X}^{(i)}_{j^*}$ is the smallest convex set containing $\mathrm{eval}(\varphi_{j^*} \,;\, \mathbf{X}^{(i-1)}, \mathbf{P})$, i.e.,

$$\mathbf{X}^{(i)}_{j^*} = \mathrm{conv}\Big(\mathrm{eval}\left(\varphi_{j^*} \,;\, \mathbf{X}^{(i-1)}, \mathbf{P}\right) \Big). \tag{35}$$

On the other hand, $\mathbf{Z} \in \mathrm{sol}(I; \mathbf{P})$, in particular, entailing that $\mathbf{Z}_{j^*} \geqslant \mathrm{eval}(\varphi_{j^*} \,;\, \mathbf{Z}, \mathbf{P})$. We know that $\mathbf{Z} \geqslant \mathbf{X}^{(i-1)}$, which implies that$\mathbf{Z}_{j^*} \geqslant \mathrm{eval}(\varphi_{j^*} \,;\, \mathbf{X}^{(i-1)}, \mathbf{P})$. As a result, from Equation 35, we conclude that

$$\mathbf{Z}_{j^*} \geqslant \mathbf{X}^{(i)}_{j^*},$$

which contradicts Equation 34.

G Preliminaries: Arrangements

This section presents some fundamental properties of arrangements. Define $d = a + b + c$ with the assumptions that $c \geqslant 0$, $a \geqslant 1$, and $b \geqslant 1$. It follows that $d = a+b+c \geqslant a+b \geqslant \max\{a+1, b+1\} \geqslant 2$.

For brevity, this section will use the following definitions and notation. For a finite set $S \subseteq \mathbb{R}^d$, the set S^o denotes the relative interior of the convex hull of S; i.e., $S^o = \mathrm{conv}^o(S)$. The set ∂S denotes the *boundary* of $\mathrm{conv}(S)$; i.e., $\partial S \coloneqq \mathrm{conv}(S) \setminus \mathrm{conv}^o(S)$.

According to the first property below, which is an essential property of an arrangement, the realization of an incidence vector $I \in \{0,1\}^{\binom{S}{\leqslant (a+1)}}$ is the intersection of the sets of relative interior points of those subsets of S that are in the support of I. Below, we state propositions crucial for our proof and prove them in Appendix G.1.

Proposition 7. *Any incidence vector* $I \in \{0,1\}^{\binom{S}{\leqslant (a+1)}}$ *such that* $\mathrm{realize}(I; S) \in \mathcal{A}S$*, satisfies*

$$\mathrm{realize}(I; S) = \bigcap_{\substack{R \in \binom{S}{\leqslant (a+1)} \\ I_R = 1}} \mathrm{conv}^o(R).$$

The non-triviality in proving this result is that the incidence vector also encodes the subsets T such that the realization does not intersect $\mathrm{conv}(T)$. The complement of $\mathrm{conv}(T)$ is not convex. So, these "negative constraints" lead to an intersection with non-convex sets; the result need not necessarily be convex. However, the proposition above states that any realization is expressible as the intersection of convex sets, and the negative constraints are redundant.

From the above proposition, we conclude the following proposition, which states that any realization of an incidence vector $I \in \{0,1\}^{\binom{S}{\leqslant (a+1)}}$ is the relative interior of a polytope whose vertices are in $\mathcal{V}\mathcal{A}S$.

[3] That is, there is $j \in \{1, 2, \dots, n\}$ such that $\mathbf{Z}_j$ does *not* contain $\mathrm{itr}(I; \mathbf{P})_j$.

Proposition 8. *The closure of any non-empty* $\text{realize}(I;S) \subseteq \text{conv}(S)$ *is a polytope with vertices in* $\mathcal{VAS}$.

According to the next proposition, the arrangement of a finite set S is a partition for the convex hull of S.

Proposition 9. *The sets in* $\mathcal{AS}$ *partition* $\text{conv}(S)$.

The next proposition states that the set of vertices of an arrangement of a set S contains it.

Proposition 10. $S \subseteq \mathcal{VAS}$

Notation. The set $\text{imm}(A;\mathcal{SAS})$ denotes the *immediate neighbors* of a point $A \in \mathbb{R}^a$ in the simplicial decomposition $\mathcal{SAS}$. That is, $\text{imm}(A;\mathcal{SAS})$ denotes the (unique) subset of vertices $Q \subseteq \mathcal{VAS}$ such that $A \in \text{conv}^o(Q) \in \mathcal{SAS}$.

We can uniquely express a point $A \in \mathbb{R}^a$ in $\mathcal{SAS}$ as a convex linear combination of the vertices $\text{imm}(A;\mathcal{SAS})$, and represent the corresponding coefficients as $\text{lin}(A;\mathcal{SAS}) \in \mathbb{R}^{\text{imm}(A;\mathcal{SAS})}$. That is, the following identity holds.

$$A = \sum_{V \in \text{imm}(A;\mathcal{SAS})} \text{lin}(A;\mathcal{SAS})_V \cdot V \tag{36}$$

Because $A \in \text{conv}^o(\text{imm}(A;\mathcal{SAS}))$, we must have $\text{lin}(A;\mathcal{SAS})_V > 0$ for every $V \in \text{imm}(A;\mathcal{SAS})$.

G.1 Proofs of Proposition 7, Proposition 8, Proposition 9, Proposition 10

This section presents the proof of the propositions introduced in Appendix G.

We start with the proof of Proposition 7. We use Lemma G.1 to prove Proposition 7. We present the proof of Lemma G.1 in Appendix G.2.

Lemma G.1. *Let* $T, S \subseteq \mathbb{R}^a$ *be two finite sets such that* $T \subseteq \text{conv}(S)$. *Then, there is a simplicial decomposition of* $\text{conv}(S) \setminus \text{conv}^o(T)$ *such that the vertices of each simplex are in the set* $S \cup T$.

Proof of Proposition 7. Define

$$B \coloneqq \bigcap_{\substack{R \in \binom{S}{\leqslant (a+1)} \\ I_R = 1}} \text{conv}^o(R).$$

We want to show that $\text{realize}(I;S) = B$. Note that according to the definition of $\text{realize}(I;S) \in \mathcal{AS}$, we have the following:

$$\text{realize}(I;S) = \underbrace{\left(\bigcap_{\substack{R \in \binom{S}{\leqslant (a+1)} \\ I_R = 1}} \text{conv}^o(R) \right)}_{B} \bigcap \left(\bigcap_{\substack{T \in \binom{S}{\leqslant (a+1)} \\ I_T = 0}} \text{conv}(S) \setminus \text{conv}^o(T) \right) \tag{37}$$

We show that $B \cap (\text{conv}(S) \setminus \text{conv}^o(T)) = B$ for any $T \in \binom{S}{\leqslant (a+1)}$ that $I_T = 0$. Thus, it follows from Equation 37 that $\text{realize}(I;S) = B$.

Take an arbitrary set $T \in \binom{S}{\leqslant(a+1)}$ such that $I_T = 0$. We show that $\text{conv}^o(T) \cap B = \emptyset$. Since

$$B = \bigcap_{\substack{R \in \binom{S}{\leqslant(a+1)} \\ I_R = 1}} \text{conv}^o(R) \subseteq \text{conv}(S),$$

it follows from $B \cap \text{conv}^o(T) = \emptyset$ that $B \subseteq (\text{conv}(S) \setminus \text{conv}^o(T))$ i.e. $B \cap (\text{conv}(S) \setminus \text{conv}^o(T)) = B$.

Let us prove that $\text{conv}^o(T) \cap B = \emptyset$. According to Lemma G.1, the set $\text{conv}(S) \setminus \text{conv}^o(T)$ can be written as the union of disjoint simplices $\text{conv}^o\big(R^{(1)}\big), \ldots, \text{conv}^o\big(R^{(t)}\big)$, for some sets $R^{(1)}, R^{(2)}, \ldots, R^{(t)} \in \binom{S}{\leqslant(a+1)}$, as follows:

$$\text{conv}(S) \setminus \text{conv}^o(T) = \uplus_{j=1}^{t} \text{conv}^o\Big(R^{(j)}\Big)$$

We emphasize that the sets $R^{(1)}, \ldots, R^{(t)} \subseteq S$ because $T \subseteq S$, and according to Lemma G.1, the sets $R^{(1)}, \ldots, R^{(t)} \subseteq S \cup T = S$.
It follows from $I_T = 0$ that

$$\text{realize}(I; S) \subseteq (\text{conv}(S) \setminus \text{conv}^o(T)) = \uplus_{j=1}^{t} \text{conv}^o\Big(R^{(j)}\Big).$$

Since the simplices $\text{conv}^o\big(R^{(1)}\big), \ldots, \text{conv}^o\big(R^{(t)}\big)$ are disjoint, there is a unique $j' \in \{1, \ldots, t\}$ such that

$$\text{realize}(I; S) \subseteq \text{conv}^o\Big(R^{(j')}\Big).$$

This implies that $I_{R_{j'}} = 1$, and so $B = \bigcap_{\substack{R \in \binom{S}{\leqslant(a+1)} \\ I_R = 1}} \text{conv}^o(R) \subseteq \text{conv}^o\Big(R^{(j')}\Big)$. It follows from $\text{conv}^o\Big(R^{(j')}\Big) \subseteq (\text{conv}(S) \setminus \text{conv}^o(T))$ that $\text{conv}^o\Big(R^{(j')}\Big) \cap \text{conv}^o(T) = \emptyset$. Thus, $B \cap \text{conv}^o(T) = \emptyset$. □

Proof of Proposition 8. We prove by induction on the dimension of $\text{realize}(I; S)$. In the base case, the the dimension of the set $\text{realize}(I; S)$ is 0, and it has only one element. Then, according to the definition of $\mathcal{VAS}$, that element is a vertex in $\mathcal{VAS}$. Then, according to Proposition 7, the closure of any non-empty set $\text{realize}(I; S)$ is

$$\overline{\text{realize}(I; S)} = \bigcap_{\substack{R \in \binom{S}{\leqslant(a+1)} \\ I_R = 1}} \text{conv}(R).$$

This set is an intersection of a finite number of convex polytopes. Therefore, it is a polytope. Now, suppose our claim is true when the dimension of $\text{realize}(I; S)$ is k. We want to prove that our claim holds when the dimension of $\text{realize}(I; S)$ is $k+1$. Now, note that each facet of the polytope $\overline{\text{realize}(I; S)}$ is itself a polytope that can be described as the closure of $\text{realize}(I'; S)$ for some I', and it has dimension k. According to the induction hypothesis, the vertices of each facet belong to $\mathcal{VAS}$. Therefore, the vertices of $\overline{\text{realize}(I; S)}$, which is the union of the vertices of its facet are also in $\mathcal{VAS}$. □

Proof of Proposition 9. Consider two distinct $I, J \in \{0,1\}^{\binom{S}{\leqslant(a+1)}}$. Then, according to the definition, we have $B = \text{realize}(I; S) \cap \text{realize}(J; S) = \emptyset$. Otherwise, if $P \in B$, then for any $R \in \binom{S}{\leqslant(a+1)}$, we have $I_R = \text{inc}(P; S)_R = J_R$, which is a contradiction. On the other hand, for any $P \in S$, we have $P \in \text{realize}(\text{inc}(P; S); S)$. So, we have $S \subseteq \bigcup_{P \in \mathbb{R}^a} \text{realize}(\text{inc}(P; S); S) = \bigcup_{W \in \mathcal{AS}} W$. This completes the proof. □

Proof of Proposition 10. It follows from the observation that realize$(I;S) = \{P\}$, where $I_{\{P\}} = 1$ and $P \in S$. □

G.2 Proof of Lemma G.1

To prove the claim, we use the lifting technique. Define the two sets $U := \{(p,1) \in \mathbb{R}^{a+1} : p \in S \setminus T\}$ and $V := \{(p,0) \in \mathbb{R}^{a+1} : p \in T\}$. Let $\mathcal{L}$ be the lower convex hull of $W := U \cup V$. Each face of $\mathcal{L}$ is a polytope and has a simplicial decomposition without adding any additional vertices [Edm70]. Note that conv(V) is a face of $\mathcal{L}$. Let $\mathcal{SL}$ denote a simplicial decomposition of $\mathcal{L}$ achieved by considering an arbitrary simplicial decomposition for each face of $\mathcal{L}$. Let $\mathcal{SL}^*$ be the same as $\mathcal{SL}$ without considering the simplicial decomposition of conv$^o(V)$.

Let $\pi\colon \mathbb{R}^{a+1} \to \mathbb{R}^a$ be a projection that maps $(p_1, \ldots, p_a, p_{a+1}) \in \mathbb{R}^{a+1}$ to $(p_1, \ldots, p_a) \in \mathbb{R}^a$. For an arbitrary subset $A \subseteq \mathbb{R}^{a+1}$, define $\pi(A) := \{\pi(x)\colon x \in A\}$. Define $\pi(\mathcal{SL})$, and $\pi(\mathcal{SL}^*)$ as follows:

$$\begin{aligned}\pi(\mathcal{SL}) &:= \{\pi(\text{conv}^o(R))\colon \text{conv}^o(R) \in \mathcal{SL}, R \subseteq W\}\\ \pi(\mathcal{SL}^*) &:= \{\pi(\text{conv}^o(R))\colon \text{conv}^o(R) \in \mathcal{SL}^*, R \subseteq W\}\end{aligned}$$

Then, $\pi(\mathcal{SL})$ is a simplicial decomposition of conv(S) because $\pi(\mathcal{L})$ is equal to conv(S). Similarly, $\pi(\mathcal{SL}^*)$ is a simplicial decomposition of conv$(S) \setminus$ conv$^o(T)$ since the set $\pi(\mathcal{L} \setminus \text{conv}^o(T))$ is equal to the set conv$(S) \setminus$ conv$^o(T)$.
Since the vertices of the simplices in $\mathcal{SL}^*$ are in the set $W = U \cup V$, the vertices of $\pi(\mathcal{SL}^*)$, which is the achieved simplicial decomposition for conv$(S) \setminus$ conv$^o(T)$, are in $\pi(W) = S \cup T$.

H Lamination Hull Restricted to Grid Points is Sufficient: Proof of Lemma 3

This section will prove our Structure Lemma (Lemma 3). Instead of directly working with $\mathcal{S}^{(\infty,\Lambda)}$, we will define a new (related) sequence of recursively defined sets.

1. Initialization.
$$\mathcal{T}^{(0)} := \mathcal{S}^{(0,\Lambda)}.$$

2. Recursive definition. For $i \in \{0,1,2,\ldots\}$, define
$$\mathcal{T}^{(i+1)} := \left\{ \sum_{j=1}^{k} \lambda_j \cdot Q^{(j)} : \begin{array}{c} k \in \{1,2,\ldots,d\}, \lambda_1, \lambda_2, \ldots, \lambda_k > 0, \\ \lambda_1 + \lambda_2 + \cdots + \lambda_k = 1 \\ \text{distinct } Q^{(1)}, Q^{(2)}, \ldots, Q^{(k)} \in \mathcal{T}^{(i)} \\ Q^{(1)}_{[a]} = \cdots = Q^{(k)}_{[a]} \text{ or } Q^{(1)}_{[b]} = \cdots = Q^{(k)}_{[b]} \end{array} \right\}$$

3. Hull.
$$\mathcal{T}^{(\infty)} := \bigcup_{i \geqslant 0} \mathcal{T}^{(i)}.$$

We have the following relation between the two hulls.

Lemma H.1. $\mathcal{S}^{(\infty,\Lambda)} = \mathcal{T}^{(\infty)}$.

Proof. It is clear that $\mathcal{S}^{(i,\Lambda)} \subseteq \mathcal{T}^{(i)}$, for all $i \in \{0, 1, 2, \dots\}$. We can prove this by induction on i. The base case of $i = 0$ has $\mathcal{S}^{(i,\Lambda)} = \mathcal{T}^{(i)}$ by definition. In every recursive step, any two points joined by a line segment in $\mathcal{S}^{(i+1,\Lambda)}$ are also joined in $\mathcal{T}^{(i+1)}$. Therefore, we have $\mathcal{S}^{(\infty,\Lambda)} \subseteq \mathcal{T}^{(\infty)}$.

For the other direction, [BKMN22, Corollary 1] proved that $\mathcal{T}^{(i)} \subseteq \mathcal{S}^{(d\cdot i,\Lambda)}$ for $i \in \{0, 1, 2, \dots\}$. So, $\mathcal{T}^{(\infty)} \subseteq \mathcal{S}^{(\infty,\Lambda)}$. The intuition is that $\mathcal{T}^{(i+1)}$ permits convex linearly combining d points of $\mathcal{T}^{(i)}$. This can be emulated by iteratively convex linearly combining two points at a time. □

Due to this equivalence, to prove our structure lemma, it suffices to show that $\mathcal{T}^{(\infty)}\big|_q$ can be computed from $\left\{ \mathcal{T}^{(\infty)}\big|_g \ : \ g \in \mathcal{G} \right\}$. We will prove that the algorithm in Figure 11 is correct.

Define $\mathcal{S}^{(a)} \coloneqq \mathcal{SAS}^{(0,\Lambda)}_{[a]}$, $\mathcal{S}^{(b)} \coloneqq \mathcal{SAS}^{(0,\Lambda)}_{[b]}$, $\mathcal{G}^{(a)} \coloneqq \mathcal{VAS}^{(0,\Lambda)}_{[a]}$, $\mathcal{G}^{(b)} \coloneqq \mathcal{VAS}^{(0,\Lambda)}_{[b]}$, $\mathcal{G} = \mathcal{G}^{(a)} \times \mathcal{G}^{(b)}$ and $(u, v) \coloneqq q$.

1. If $(u, v) \in \mathcal{G}$, return $\mathcal{T}^{(\infty)}\big|_q$.
2. If $u \in \mathcal{G}^{(a)}$ but $v \notin \mathcal{G}^{(b)}$, return
$$\sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(\infty)}\Big|_{(u,v')}.$$
3. If $v \in \mathcal{G}^{(b)}$ but $u \notin \mathcal{G}^{(a)}$, return
$$\sum_{u' \in \mathrm{imm}(u;\mathcal{S}^{(a)})} \mathrm{lin}(u;\mathcal{S}^{(a)})_{u'} \cdot \mathcal{T}^{(\infty)}\Big|_{(u',v)}.$$
4. Else (i.e., $u \notin \mathcal{G}^{(a)}$ and $v \notin \mathcal{G}^{(b)}$), return
$$\sum_{u' \in \mathrm{imm}(u;\mathcal{S}^{(a)})} \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(u;\mathcal{S}^{(a)})_{u'} \cdot \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(\infty)}\Big|_{(u',v')}.$$

Figure 11: Algorithm to compute $\mathcal{T}^{(\infty)}\big|_q$ from $\left\{ \mathcal{T}^{(\infty)}\big|_g \ : \ g \in \mathcal{G} \right\}$.

Lemma H.2 (Technical Result)**.** *The algorithm in Figure 11 is correct.*

Observe that the returned answer always combines restrictions of $\mathcal{T}^{(\infty)}$ to grid points. Appendix H.4 presents the proof of Lemma H.2. This proof will require characterizing properties of the $\mathcal{T}^{(i)}$ sets, which are elaborated in the section below.

H.1 Notation: Witness trees

We introduce some notation to state and prove our results.

For a point $Q \in \mathbb{R}^d$, we use t_Q to denote the first time it appears in the sequence $\left\{\mathcal{T}^{(i)}\right\}_{i \geqslant 0}$:

$$t_Q \coloneqq \min \left\{ i \ : \ Q \in \mathcal{T}^{(i)}, i \in \{0, 1, 2, \dots\} \right\}. \tag{38}$$

For a point $P \in \mathcal{T}^{(\infty)} \subseteq \mathbb{R}^d$, we can associate a natural *witness tree* Π with it. This tree has P at its root, and its children are the points that were convex linearly combined to produce P. The subtrees rooted at these children are their witnesses, respectively. The leaves of a witness tree are points in $\mathcal{T}^{(0)}$. Based on the recursive definition of the sequence $\left\{\mathcal{T}^{(i)}\right\}_{i \geqslant 0}$, if P' is a child of P

then $P_{[a]} = P'_{[a]}$ or $P_{[b]} = P'_{[b]}$. We highlight that a node in the witness tree may have one child; this is permitted by the recursive definition of $\mathcal{T}^{(i+1)}$ from $\mathcal{T}^{(i)}$, where $i \geqslant 0$. So, any point has multiple witness trees.

Next, we aim to measure the structure of points in $\mathcal{T}^{(\infty)}$. A point $P \in \mathcal{T}^{(\infty)} \subseteq \mathbb{R}^d$ is *gridded* if $P_{[a]} \in \mathcal{G}^{(a)}$ and $P_{[b]} \in \mathcal{G}^{(b)}$. It is *grid-aligned* if (1) $P_{[a]} \in \mathcal{G}^{(a)}$ but $P_{[b]} \notin \mathcal{G}^{(b)}$, or (2) $P_{[b]} \in \mathcal{G}^{(b)}$ but $P_{[a]} \notin \mathcal{G}^{(a)}$. It is *unaligned* if $P_{[a]} \notin \mathcal{G}^{(a)}$ and $P_{[b]} \notin \mathcal{G}^{(b)}$. Note that the leaves of any witness tree are gridded by the definition of $\mathcal{T}^{(0)}$, $\mathcal{G}^{(a)}$, and $\mathcal{G}^{(b)}$.

Now, we will identify structured witness trees for points in $\mathcal{T}^{(\infty)}$.

Definition 2 (Gridded Witness)**.** *A witness tree* Π *for a point* $P \in \mathcal{T}^{(\infty)} \subseteq \mathbb{R}^d$ *is* gridded *if the following (mutually exclusive) conditions are satisfied.*

1. *If* P *is gridded: Every node in the witness tree* Π *is also gridded.*
2. *If* P *is grid-aligned: Except for the root, every node in the witness tree* Π *is gridded.*
3. *If* P *is unaligned: Except for the root and its children, every node in the witness tree* Π *is gridded. The root's children in the witness tree* Π *are grid-aligned.*

We will prove the following result.

Lemma H.3. *Any point* $P \in \mathcal{T}^{(\infty)}$ *has a gridded witness.*

This salient feature may not exist for the witness trees for the recursive construction of $\mathcal{S}^{(\infty,\Lambda)}$, which only convex linearly combines two points. For example, the barycenter of a triangle cannot be expressed as the pairwise linear combination of its vertices such that each intermediate linear combination is also a vertex of the triangle. This is one reason for defining and using the $\{\mathcal{T}^{(i)}\}_{i\geqslant 0}$ sequence for the proofs. Appendix H.3 proves this result. We emphasize that the depth of a gridded witness for a point may be greater than that of its shortest-depth witness.

We define another form of structure in witness trees.

Definition 3 (Immediate Witness)**.** *A witness tree* Π *for a grid-aligned or unaligned point* $P \in \mathcal{T}^{(\infty)} \subseteq \mathbb{R}^d$ *is* immediate *if the following (mutually exclusive) conditions are satisfied.*

1. *If* P *is grid-aligned and* $P_{[a]} \in \mathcal{G}^{(a)}$*: Any child* P' *of the root* P *in* Π *satisfies* $P'_{[b]} \in \mathrm{imm}(P_{[b]}; \mathcal{S}^{(b)})$.
2. *If* P *is grid-aligned and* $P_{[b]} \in \mathcal{G}^{(b)}$*: Any child* P' *of the root* P *in* Π *satisfies* $P'_{[a]} \in \mathrm{imm}(P_{[a]}; \mathcal{S}^{(a)})$.
3. *If* P *is unaligned: Any child* P' *of the root* P *in* Π *satisfies* $P'_{[a]} \in \mathrm{imm}(P_{[a]}; \mathcal{S}^{(a)})$ *or* $P'_{[b]} \in \mathrm{imm}(P_{[b]}; \mathcal{S}^{(b)})$*. Any grandchild* P'' *of the root* P *in* Π *satisfies* $P''_{[a]} \in \mathrm{imm}(P_{[a]}; \mathcal{S}^{(a)})$ *and* $P''_{[b]} \in \mathrm{imm}(P_{[b]}; \mathcal{S}^{(b)})$.

We will prove the following result.

Lemma H.4. *Any grid-aligned point* $P \in \mathcal{T}^{(\infty)}$ *has an immediate and gridded witness. Any unaligned* $P \in \mathcal{T}^{(\infty)}$ *has two immediate and gridded witnesses* $\Pi^{(a)}$ *and* $\Pi^{(b)}$ *satisfying:*

1. *Except for the children of the root* P*, all nodes are identical in* $\Pi^{(a)}$ *and* $\Pi^{(b)}$.
2. *Any child* P' *of the root* P *in* $\Pi^{(a)}$ *satisfies* $P'_{[a]} = P_{[a]}$.
3. *Any child* P' *of the root* P *in* $\Pi^{(b)}$ *satisfies* $P'_{[b]} = P_{[b]}$.

Appendix H.2 will prove this result. Note that Lemma H.4 is a stronger version of Lemma H.3 for aligned and unaligned P. Lemma H.3 for gridded P will be used in a later proof.

H.2 Proof of Lemma H.4

We prove Lemma H.4 using an extremal argument. Let $\mathcal{B} \subseteq \mathcal{T}^{(\infty)}$ be the set of points for which the lemma does not hold. We want to show that $\mathcal{B} = \emptyset$. We prove this by contradiction. Suppose $\mathcal{B} \neq \emptyset$. Let t^* denote $\min\{t_Q : Q \in \mathcal{B}\}$, where t_Q is defined in Equation 38. Consider a point $Q \in \mathcal{B}$ such that $t_Q = t^*$. Let Π be a witness tree for Q of depth t^*. Let $Q^{(1)}, \ldots, Q^{(k)}$ be the set of children of Q in Π. Without loss of generality, let us assume that $Q_{[a]} = Q^{(1)}_{[a]} = \cdots = Q^{(k)}_{[a]} = u$. For each $j = 1, \ldots, k$, we have $t_{Q^{(j)}} < t_Q = t^*$. Thus, for each $j = 1, \ldots, k$, the lemma holds for the point $Q^{(j)} \in \mathcal{T}^{(\infty)}$. There are two cases that we need to consider:

Case I. [Q **is grid-aligned**] There are two cases:

Subcase (A). The first subcase is $u \in \mathcal{G}^{(a)}$ and $v \notin \mathcal{G}^{(b)}$. For each $j = 1, \ldots, k$, the child $Q^{(j)}$ is grid-aligned or gridded because $Q^{(j)}_{[a]} = u \in \mathcal{G}^{(a)}$ (refer to Figure 12). First, for any child $Q^{(j)}$ that is grid-aligned, we replace it with its immediate and gridded witness (For example, the child $Q^{(1)}$ in Figure 12). The children of $Q^{(j)}$ are aligned with Q in that witness tree. Thus, in the next step, we can remove any grid-aligned child $Q^{(j)}$ by replacing it with the subtrees rooted at its children. Thus, there is a gridded witness tree for Q. Now, according to Lemma H.5 (Part 1), the point $Q \in \mathcal{T}^{(\infty)}$ has an immediate and gridded witness, which is a contradiction.

Subcase (B). The second subcase is that $Q_{[a]} = u \notin \mathcal{G}^{(a)}$ and $Q_{[b]} = v \in \mathcal{G}^{(b)}$. Then, for each $j = 1, \ldots, k$, the child $Q^{(j)}$ is grid-aligned or unaligned (refer to Figure 13). Consider some grid-aligned child $Q^{(i)}$ where $Q^{(i)}_{[a]} = u$ and $Q^{(i)}_{[b]} = v^{(i)}$ (for example, see $Q^{(2)}$ in Figure 13). Since $u \notin \mathcal{G}^{(a)}$ and $Q^{(i)}$ is grid-aligned, it must be the case that $v^{(i)} \in \mathcal{G}^{(b)}$. Remember $t_{Q^{(i)}} < t^*$. Thus, there is an immediate and gridded witness tree for $Q^{(i)}$. Similarly, there is an immediate and gridded witness for any unaligned child $Q^{(\ell)}$ (for example, the point $Q^{(1)}$ in Figure 13).

Consider an arbitrary child $Q^{(j)}$. Let $Q^{(j,1)}, \ldots, Q^{(j,r)}$ be the children of $Q^{(j)}$ in its immediate and gridded witness. Note that for the case that $Q^{(j)}$ is unaligned, there are two immediate and gridded witnesses. We choose the one that $r = \left|\text{imm}(u; \mathcal{S}^{(a)})\right|$, $Q^{(j,1)}_{[b]} = \cdots = Q^{(j,r)}_{[b]} = Q^{(j)}_{[b]}$, and $\text{imm}(u; \mathcal{S}^{(a)}) = \left\{Q^{(j,1)}_{[a]}, \ldots, Q^{(j,r)}_{[a]}\right\}$ (For example, see the immediate and gridded witness of $Q^{(1)}$ in Figure 13). We do the same for the case that $Q^{(j)}$ is gridded-aligned (For example, see the immediate and gridded witness of $Q^{(2)}$ in Figure 13).

Now, replace each child with the corresponding immediate and gridded witness tree. Then, we have a new witness tree for Q. We apply the swap lemma (refer to Lemma H.6) to construct another witness for Q. In the resulting witness, the point Q is grid-aligned and any child Q' of Q is gridded and $Q'_{[b]} = Q_{[b]} \in \mathcal{G}^{(b)}$, and $Q'_{[a]} \in \text{imm}(u; \mathcal{S}^{(a)})$. Thus, the resulting witness is an immediate and gridded one for Q. This is a contradiction.

Case II. [Q **is unaligned**] In this case, $u \notin \mathcal{G}^{(a)}, v \notin \mathcal{G}^{(b)}$. For each $j = 1, 2, \ldots, k$, the child $Q^{(j)}$ is grid-aligned or unaligned (refer to Figure 14). Consider some child $Q^{(i)}$ that is grid-aligned (For example, child $Q^{(2)}$ in Figure 14). $Q^{(i)}$ has an immediate and gridded witness. Let $Q^{(i,1)}, \ldots, Q^{(i,r)}$ be the children of $Q^{(i)}$ in that immediate and gridded witness. Note that $r = \left|\text{imm}(u; \mathcal{S}^{(a)})\right|$, and $Q^{(i,1)}_{[b]} = \cdots = Q^{(i,r)}_{[b]} = Q^{(i)}_{[b]}$, and $\text{imm}(u; \mathcal{S}^{(a)}) = \left\{Q^{(i,1)}_{[a]}, \ldots, Q^{(i,r)}_{[a]}\right\}$. Consider some child $Q^{(\ell)}$ that is unaligned (For example, child $Q^{(1)}$ in Figure 14). It has an immediate and gridded witness with children $Q^{(\ell,1)}, \ldots, Q^{(\ell,r)}$. Note that $r = \left|\text{imm}(u; \mathcal{S}^{(a)})\right|$, and $Q^{(\ell,1)}_{[b]} = \cdots = Q^{(\ell,r)}_{[b]} = Q^{(\ell)}_{[b]}$. Replace

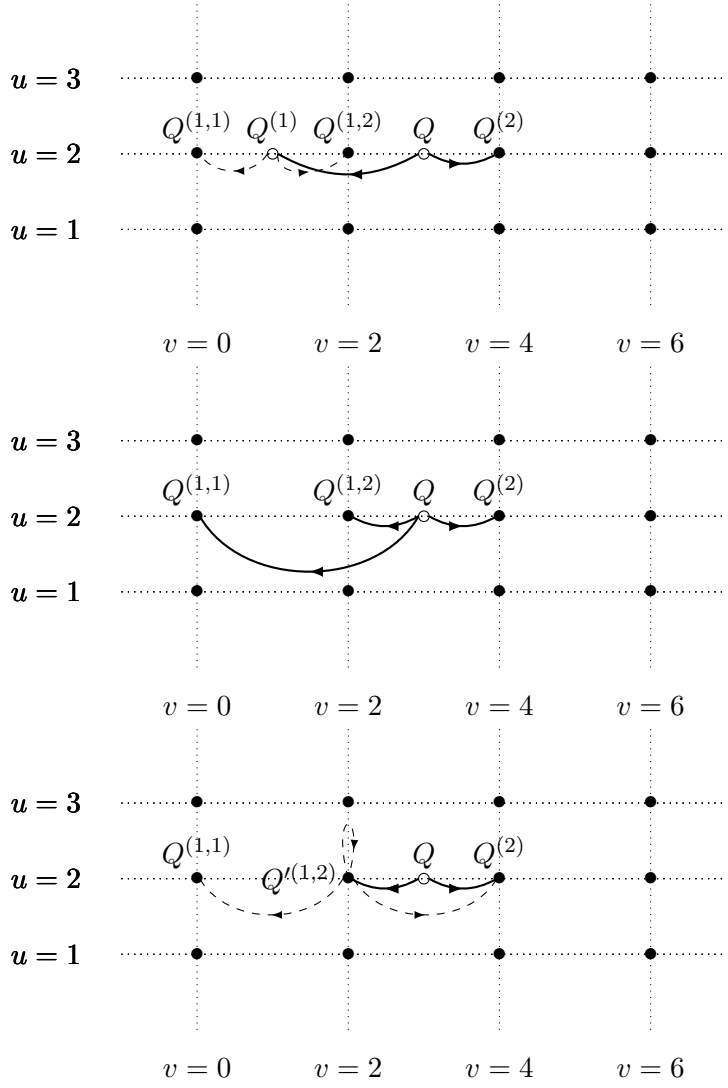


Figure 12: This figure illustrates the proof of Lemma H.4, Case I, Subcase (A), presented in Appendix H.2. In this figure, $a = 1, b = 1$. The bullet points are grid points. The point $Q \in \mathbb{R}^d$ is a grid-aligned point, where $u \in \mathcal{G}^{(a)}, v \notin \mathcal{G}^{(b)}$. The figure at the top represents a witness for Q. The child $Q^{(1)}$ is grid-aligned and the child $Q^{(2)}$ is gridded. We represent the immediate and gridded witness tree of $Q^{(1)}$ with dashed arrows. The figure in the middle represents a gridded witness for Q after replacing $Q^{(1)}$ with its children. According to Lemma H.5, we can transform the gridded witness to an immediate and gridded witness, represented in the figure at the bottom.

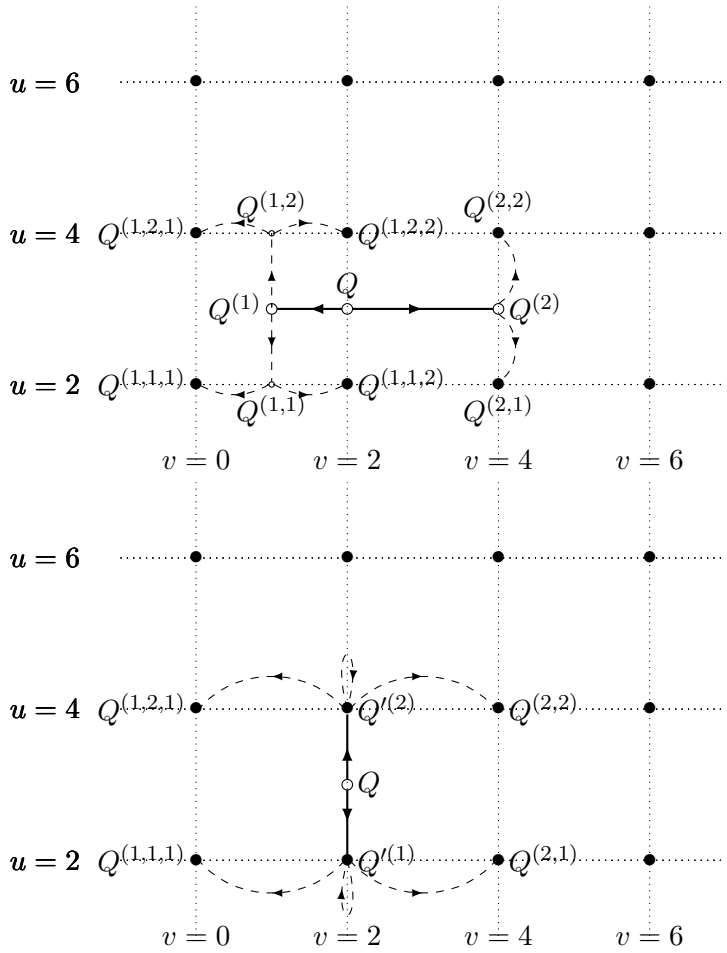


Figure 13: This figure illustrates the proof of Lemma H.4, Case I, Subcase (B), presented in Appendix H.2. In this figure, $a = 1, b = 1$. The bullet points represent grid points. In the figure at the top, the point $Q \in \mathbb{R}^d$ is a grid-aligned point, where $u \notin \mathcal{G}^{(a)}, v \in \mathcal{G}^{(b)}$. Its children are $Q^{(1)}$, and $Q^{(2)}$; $Q^{(1)}$ is unaligned, and $Q^{(2)}$ is grid-aligned. We represent the immediate and gridded witnesses of $Q^{(1)}$, and $Q^{(2)}$ with dashed arrows. The figure at the bottom represents an immediate and gridded witness for Q.

any such grid-aligned child $Q^{(i)}$ and unaligned child $Q^{(\ell)}$ with their corresponding immediate and gridded witnesses previously discussed. Now, we have a new witness tree for Q. We apply the swap lemma (refer to Lemma H.6) to construct another witness for Q. In the resulting witness, the point Q is unaligned and any child Q' of Q is grid-aligned, and $Q'_{[b]} = Q_{[b]} \notin \mathcal{G}^{(b)}$, and $Q'_{[a]} \in \mathrm{imm}(u; \mathcal{S}^{(a)}) \subseteq \mathcal{G}^{(a)}$. Since $t_{Q'} < t_Q$, there is an immediate and gridded witness for each child Q' of Q.

Thus, Q has an immediate and gridded witness such that any child Q' of the root Q satisfies $Q'_{[b]} = Q_{[b]}$. According to swap lemma (Lemma H.6), this witness can be transformed into another witness with an immediate and gridded witness such that any child Q' of the root Q satisfies $Q'_{[a]} = Q_{[a]}$. This is a contradiction.

H.3 Proof of Lemma H.3

It follows directly from Lemma H.4 that P has a gridded witness if it is grid-aligned or unaligned. The result remains to be proven when P is gridded. We prove by contradiction and use an extremal argument similar to the proof of Lemma H.4.

Suppose that there is some gridded point that does not have a gridded witness. Let Q be one such point with the smallest t_Q, which is defined in Equation 38 as the smallest i such that $Q \in \mathcal{T}^{(i)}$. Let Π be a witness for Q. It suffices to prove the result for the case that any child Q' of Q in Π satisfies $Q'_{[a]} = Q_{[a]}$ (the proof for the other case is analogous).

Observe that any child of Q in Π_Q is either gridded or grid-aligned because Q is gridded (refer to Figure 15). By Lemma H.4, every grid-aligned child of Q in Π_Q has a gridded witness. For every such child Q' (of Q), let $\Pi_{Q'}$ be a gridded witness. Then, any child Q'' of Q' in $\Pi_{Q'}$ satisfies $Q''_{[a]} = Q'_{[a]} = Q_{[a]}$; otherwise $Q'_{[b]} = Q''_{[b]}$ which would imply that Q' is gridded, contradicting that Q' is grid-aligned. Therefore, we can construct Q by a tree Π' achieved by replacing every subtree rooted at a grid-aligned child Q' in Π_Q by subtrees in $\Pi_{Q'}$ rooted at the children of Q' in $\Pi_{Q'}$.

The degree of Q in Π' could be more than d. We use Carathéodory's theorem to transform it into a valid witness tree. Let $R = \{Q^{(1)}, \dots, Q^{(r)}\}$ of size $r \leqslant a+1$, be a subset of the children of Q in Π' such that $R_{[a]} := \left\{Q^{(1)}_{[a]}, \dots, Q^{(r)}_{[a]}\right\}$ forms a simplex and $Q_{[a]} \in \mathrm{conv}^o\big(R_{[a]}\big)$. Thus, there are $\lambda^{(1,R)}, \dots, \lambda^{(r,R)} > 0$ such that $Q_{[a]} = \sum_{i=1}^r \lambda^{(i,R)} \cdot Q^{(i)}_{[a]}$, and $\sum_{i=1}^r \lambda_i = 1$. Define $Q^{(R)} := \sum_{i=1}^r \lambda^{(i,R)} \cdot Q^{(i)}$. By Carathéodory's theorem, for each such R there is $\lambda^{(R)} > 0$ such that $Q = \sum_R \lambda^{(R)} \cdot Q^{(R)}$, and $\sum_R \lambda^{(R)} = 1$. Therefore, we can have a gridded witness for Q. This is a contradiction.

H.4 Proof of Lemma H.2

The proof proceeds by an exhaustive case analysis.

Case 1: $u \in \mathcal{G}^{(a)}, v \in \mathcal{G}^{(b)}$**.** Then $q \in \mathcal{G}$. In this case, $\mathcal{T}^{(\infty)}\big|_q$ is an element in the set $\left\{ \mathcal{T}^{(\infty)}\big|_g \ : \ g \in \mathcal{G} \right\}$, so we return the appropriate element from that set.

Case 2: $u \in \mathcal{G}^{(a)}, v \notin \mathcal{G}^{(b)}$**.** Consider any $Q \in \mathcal{T}^{(\infty)}\big|_q$. Then, Q is grid-aligned. It follows from Lemma H.4 that Q has an immediate and gridded witness Π. By Equation 36,

$$Q_{[b]} = v = \sum_{v' \in \mathrm{imm}(v; \mathcal{S}^{(b)})} \mathrm{lin}(v; \mathcal{S}^{(b)})_{v'} \cdot v'$$

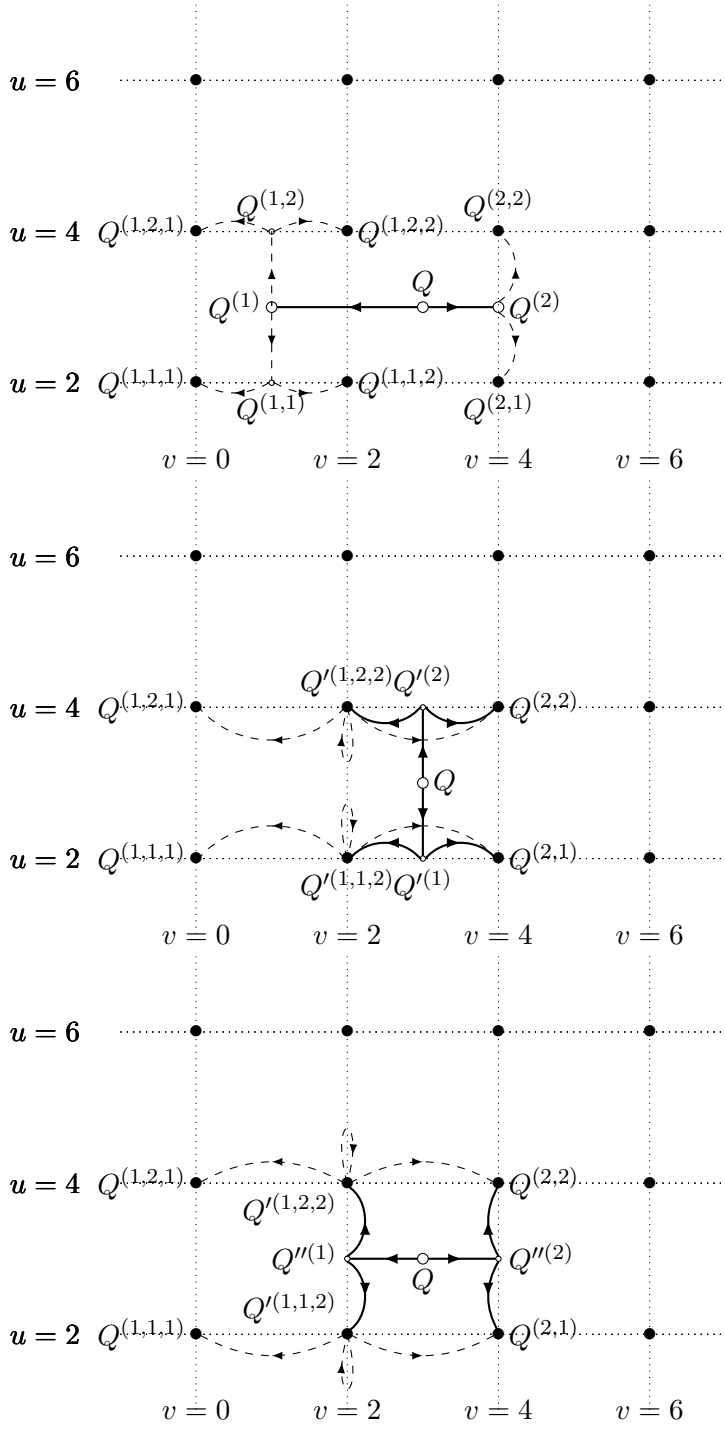


Figure 14: This figure illustrates the proof of Lemma H.4, Case II, presented in Appendix H.2. In this figure, $a = 1, b = 1$. The bullet points represent grid points. In the figure at the top, the point $Q \in \mathbb{R}^d$ is unaligned. Its children, $Q^{(1)}$, and $Q^{(2)}$ are unaligned and grid-aligned respectively. We represent the immediate and gridded witnesses of Q in the middle and bottom figures.

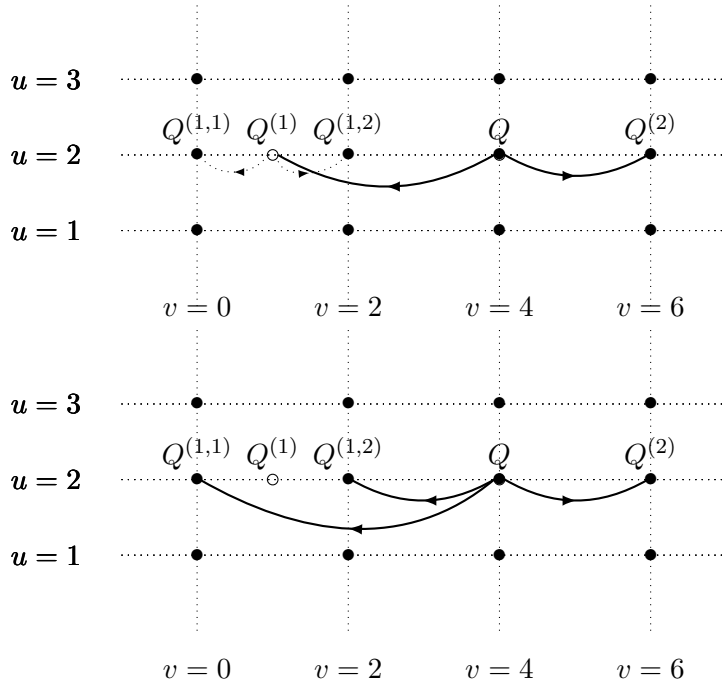


Figure 15: This figure illustrates the proof of Lemma H.3. The lemma states that any point of $\mathcal{T}^{(\infty)}$ has a gridded witness. In this figure, $a = 1, b = 1$. The bullet points are grid points. The point Q is gridded. The figure at the top represents a witness for Q. Children of Q are the points $Q^{(1)}$, and $Q^{(2)}$. The child $Q^{(1)}$ is grid-aligned. The child $Q^{(2)}$ is gridded. We represent a gridded witness of $Q^{(2)}$ by dashed arrows. The figure at the bottom represents a gridded tree for Q. This tree is achieved by replacing $Q^{(1)}$ with its children. We can transform it into a valid witness tree by using the Carathéodory's theorem.

This implies that

$$Q = \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot Q^{(v')},$$

where $Q^{(v')}$ is the child of Q in Π such that $Q^{(v')}_{[a]} = u$ and $Q^{(v')}_{[b]} = v'$. Observe that $Q^{(v')} \in \mathcal{T}^{(\infty)}\big|_{(u,v')}$, and hence

$$Q \in \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(\infty)}\Big|_{(u,v')}.$$

We have shown that

$$\mathcal{T}^{(\infty)}\Big|_{(u,v)} \subseteq \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(\infty)}\Big|_{(u,v')}.$$

For the other direction, for any point $Q \in \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(\infty)}\big|_{(u,v')}$, there is some i (since $\mathcal{T}^{(0)}\big|_q \subseteq \mathcal{T}^{(1)}\big|_q \subseteq \dots$), such that

$$Q \in \sum_{v' \in \mathrm{imm}(v;\mathcal{S}^{(b)})} \mathrm{lin}(v;\mathcal{S}^{(b)})_{v'} \cdot \mathcal{T}^{(i)}\Big|_{(u,v')} \subseteq \mathcal{T}^{(i+1)}\Big|_{(u,v)} \subseteq \mathcal{T}^{(\infty)}\Big|_{(u,v)},$$

Therefore, the two sets are equal.

Case 3: $u \notin \mathcal{G}^{(a)}, v \in \mathcal{G}^{(b)}$**.** The proof is similar to case 2.

Case 4: $u \notin \mathcal{G}^{(a)}, v \notin \mathcal{G}^{(b)}$**.** Proof is similar to case 2. However, this time, it follows from the immediate and gridded witness for an unaligned $Q \in \mathcal{T}^{(\infty)}$ mentioned in Lemma H.4.

H.5 Technical Results: Statement and Proof of Lemma H.5 and Lemma H.6

Lemma H.5 (Immediate Witnesses)**.** *Let $Q \in \mathcal{T}^{(\infty)}$. The following statements hold.*

1. *If Q is grid-aligned and has a gridded witness such that $Q'_{[a]} = Q_{[a]} \in \mathcal{G}^{(a)}$ for any child Q', then Q has a gridded witness such that any children Q'' of Q satisfies $Q''_{[b]} \in \mathrm{imm}(Q_{[b]};\mathcal{S}^{(b)})$.*
2. *If Q is grid-aligned and has a gridded witness such that $Q'_{[b]} = Q_{[b]} \in \mathcal{G}^{(b)}$ for any child Q', then Q has a gridded witness such that any children Q'' of Q satisfies $Q''_{[a]} \in \mathrm{imm}(Q_{[a]};\mathcal{S}^{(a)})$.*
3. *If Q is unaligned and has a gridded witness, then Q has a gridded witness such that any children Q'' of Q satisfies $\left(Q''_{[a]}, Q''_{[b]}\right) \in \{(u',v') \colon u' \in \mathrm{imm}(Q_{[a]},\mathcal{S}^{(a)}), v' \in \mathrm{imm}(Q_{[b]},\mathcal{S}^{(b)})\}$.*

Proof of Lemma H.5. We will prove part 1 and part 3. The proof of part 2 is similar to the proof of part 1.

Proof of part 1. Suppose Q is a grid-aligned point. Let $Q_{[a]} = u \in \mathcal{G}^{(a)}, Q_{[b]} = v \notin \mathcal{G}^{(b)}$. Suppose Q has a gridded witness tree Π with gridded children $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)}$ such that $Q^{(1)}_{[a]} = Q^{(2)}_{[a]} = \cdots = Q^{(t)}_{[a]} = Q_{[a]} = u \in \mathcal{G}_a$, and $Q^{(1)}_{[b]}, \ldots, Q^{(t)}_{[b]} \in \mathcal{G}^{(b)}$. Thus, $Q \in \operatorname{conv}\big(Q^{(1)}, \ldots, Q^{(t)}\big)$.

Note that $\mathcal{S}^{(b)} = \mathcal{SAS}^{(0,\Lambda)}_{[b]}$ is a simplicial decomposition of the arrangement $\mathcal{AS}^{(0,\Lambda)}_{[b]}$. Thus, $Q_{[b]} \in \operatorname{conv}\Big(Q^{(1)}_{[b]}, \ldots, Q^{(t)}_{[b]}\Big) \subseteq \operatorname{conv}\Big(\mathcal{S}^{(0,\Lambda)}_{[b]}\Big)$. It follows from Proposition 7 that $\operatorname{imm}(v; \mathcal{S}^{(b)}) \subseteq \operatorname{conv}(R)$ for any $R \subseteq \mathcal{S}^{(0,\Lambda)}_{[b]}$ such that $Q_{[b]} \in \operatorname{conv}^o(R)$.

Therefore, any gridded point Q' satisfying $Q'_{[b]} \in \operatorname{imm}(v; \mathcal{S}^{(b)})$ can be constructed by a witness such that any children Q'' of Q' is a grid point that satisfies $Q''_{[b]} \in \mathcal{S}^{(0,\Lambda)}_{[b]}$. Therefore, since $Q_{[b]} \in \operatorname{conv}^o\big(\operatorname{imm}(v; \mathcal{S}^{(b)})\big)$, we can construct a gridded witness for Q such that any children Q'' of Q satisfies $Q''_{[b]} \in \operatorname{imm}(v; \mathcal{S}^{(b)})$.

Proof of part 3. For the third part, we again have $Q \in \operatorname{conv}\big(Q^{(1)}, \ldots, Q^{(t)}\big)$. Each $Q^{(i)}$ is grid-aligned according to the assumption. Without loss of generality, we can assume that $Q^{(i)}_{[a]} = Q_{[a]} = u$ and $Q^{(i)}_{[b]} = v^{(i)}$. For each i, the point $Q^{(i)}$ is grid aligned and it is aligned with Q, but Q itself is unaligned (Q is not a grid point or even aligned with a grid point). This implies that $Q^{(i)}_{[b]} \in \mathcal{G}^{(b)}$. Thus, according to part (b), there is a witness for $Q^{(i)}$ whose children are the set of grid points $\{Q^{(i,j)}\}_{j=1}^{r}$ such that $Q^{(i,j)}_{[b]} = Q^{(i)}_{[b]} =: v^{(i)}$ and $Q^{(i,j)}_{[a]} \in \operatorname{imm}(u; \mathcal{S}^{(a)})$ for each j, and $r = \big|\operatorname{imm}(u, \mathcal{S}^{(a)})\big|$.

Now, we use swap lemma (Lemma H.6) to construct a new witness for Q, such that the children of Q is the set $\{P^{(j)} \in \mathcal{T}^{(\infty)}|_{p^{(j)}}\}_{j=1}^{r}$, where $r = \big|\operatorname{imm}(u, \mathcal{S}^{(a)})\big|$, and $p^{(j)} = (u^{(j)}, v)$ ($u^{(j)} \in \operatorname{imm}(u, \mathcal{S}^{(a)})$) and the children of each $P^{(j)}$, $\{P^{(j,i)}\}_{i=1}^{t}$ are such that $P^{(j,i)}_{[b]} = v^{(i)}$. Now, we use part (a) of our lemma for each $P^{(j)}$ to construct it using immediate grid points whose projection on $\mathbb{R}^b$ is in the set $\operatorname{imm}(v, \mathcal{S}^{(b)})$. Thus, Q has a witness whose children are the set of grid points $\{(u', v') \colon u' \in \operatorname{imm}(u, \mathcal{S}^{(a)}), v' \in \operatorname{imm}(v, \mathcal{S}^{(b)})\}$. □

Lemma H.6 (Swap Lemma)**.** *Let $Q \in \mathcal{T}^{(\infty)}$. Let $\operatorname{imm}(Q_{[a]}, \mathcal{S}^{(a)}) = \{u^{(1)}, u^{(2)}, \ldots, u^{(r)}\}$. Suppose there is a witness Π for Q with t children $Q^{(1)}, Q^{(2)}, \ldots, Q^{(t)}$ such that*

1. *$Q = \sum_{i=1}^{t} \beta_i \cdot Q^{(i)}$, where $\beta = (\beta_1, \ldots, \beta_t)$, $\sum_{i=1}^{t} \beta_i = 1$ and $\beta_i > 0$ for all $1 \leqslant i \leqslant t$,*
2. *$Q^{(1)}_{[a]} = Q^{(2)}_{[a]} = \cdots = Q^{(t)}_{[a]} = Q_{[a]}$,*
3. *every child $Q^{(i)}$ has r children $Q^{(i,1)}, Q^{(i,2)}, \ldots, Q^{(i,r)}$ satisfying $Q^{(i,j)}_{[a]} = u^{(j)}$ for all $1 \leqslant j \leqslant r$.*

Then, there is a witness Π' for Q with r children $P^{(1)}, P^{(2)}, \ldots, P^{(r)}$ such that

1. *$P^{(j)}_{[a]} = u^{(j)}$ and $P^{(j)}_{[b]} = Q_{[b]}$ for all $1 \leqslant j \leqslant r$,*
2. *Every child $P^{(j)}$ has t children $Q^{(1,j)}, Q^{(2,j)}, \ldots, Q^{(t,j)}$ satisfying $P^{(j)} = \sum_{i=1}^{t} \beta_i \cdot Q^{(i,j)}$.*

Proof of Swap Lemma (Lemma H.6). Recall that every point $u \in \mathcal{S}^{(a)}$ can be uniquely written as the convex combination of of its immediate neighbors (refer to Equation 36). In particular, there is a unique $(\alpha_1, \alpha_2, \ldots, \alpha_r)$ such that $\sum_{j=1}^{r} \alpha_j = 1$, $\alpha_j > 0$ for all $1 \leqslant j \leqslant r$, and $Q_{[a]} = \sum_{j=1}^{r} \alpha_j \cdot u^{(j)}$.

Therefore, in the subtree rooted at $Q^{(i)}$ of Π, it holds that $Q^{(i)} = \sum_{j=1}^{r} \alpha_j \cdot Q^{(i,j)}$ for all $1 \leqslant i \leqslant t$. This implies that

$$Q = \sum_{i=1}^{t} \beta_i \cdot Q^{(i)} = \sum_{i=1}^{t} \sum_{j=1}^{r} \beta_i \alpha_j \cdot Q^{(i,j)}.$$

The above equation naturally suggests the following construction of Π'.

1. Let the tree be rooted at Q'.
2. Let $P^{(1)}, P^{(2)}, \ldots, P^{(r)}$ be children of Q' such that $P^{(j)}_{[a]} = u^{(j)}$ and $P^{(j)}_{[b]} = Q_{[b]}$ for all $1 \leqslant j \leqslant r$, and $Q' = \sum_{j=1}^{r} \alpha_j \cdot P^{(j)}$.
3. Every child $P^{(j)}$ has t children $Q^{(1,j)}, Q^{(2,j)}, \ldots, Q^{(t,j)}$ satisfying $P^{(j)} = \sum_{i=1}^{t} \beta_i \cdot Q^{(i,j)}$, and $Q^{(1,j)}_{[a]} = Q^{(1,j)}_{[a]} = \cdots = Q^{(t,j)}_{[a]} = P^{(j)}_{[a]} = u^{(j)}$.
4. The subtree rooted at $Q^{(i,j)}$ is the same as the subtree rooted at $Q^{(i,j)}$ in Π.

It is clear that $Q' = Q$ and so Π' is a witness tree with all the desired properties. □

I Bridging Lamination Hulls and Solutions of Systems of Inequalities: Proof of Lemma 4

This section proves Lemma 4, bridging the lamination hull computation and the smallest solution of a system of inequalities. Let $\left(\mathbf{X}_g^{(*)} : g \in \mathcal{G} \right)$ be the smallest solution of the system of inequalities $\mathcal{I}$ built in Figure 8. Our objective is to prove that $\mathcal{S}^{(\infty,\Lambda)}\big|_g = \mathbf{X}_g^{(*)}$, for every grid point $g \in \mathcal{G}$.

Our proofs will rely on the nested property of the sets $\mathcal{S}^{(i,\Lambda)}$ for $i \in \{0, 1, 2, \ldots\}$. Note that $\mathbf{0}$ is in the specific Λ we consider. So, by considering $P = Q$ in Equation 1, for every $i \in \{0, 1, 2, \ldots\}$, we conclude that

$$\mathcal{S}^{(i,\Lambda)} \subseteq \mathcal{S}^{(i+1,\Lambda)}. \tag{39}$$

Now, we proceed to the proof.

Direction 1: $\mathbf{X}_g^{(*)} \subseteq \mathcal{S}^{(\infty,\Lambda)}\big|_g$. Our strategy is to prove that $\left(\mathcal{S}^{(\infty,\Lambda)}\big|_g : g \in \mathcal{G} \right)$ is a solution of the system $\mathcal{I}$; Lemma I.1 will prove it below. $\left(\mathbf{X}_g^{(*)} : g \in \mathcal{G} \right)$ is the smallest solution of the system of inequalities $\mathcal{I}$ built in Figure 8. By definition of the smallest solution, we have $\mathbf{X}_g^{(*)} \subseteq \mathcal{S}^{(\infty,\Lambda)}\big|_g$ for every grid point $g \in \mathcal{G}$. This completes the first direction of the proof.

Direction 2: $\mathcal{S}^{(\infty,\Lambda)}\big|_g \subseteq \mathbf{X}_g^{(*)}$. Instead of directly working with $\mathcal{S}^{(\infty,\Lambda)}$, we will define a new (related) sequence of recursively defined sets. Appendix H had previously also defined these sets and proved several properties that we will use in our proof.

1. Initialization.

$$\mathcal{T}^{(0)} \coloneqq \mathcal{S}^{(0,\Lambda)}.$$

2. Recursive definition. For $i \in \{0, 1, 2, \dots\}$, define

$$\mathcal{T}^{(i+1)} := \left\{ \sum_{j=1}^{k} \lambda_j \cdot Q^{(j)} : \begin{array}{c} k \in \{1, 2, \dots, d\}, \lambda_1, \lambda_2, \dots, \lambda_k > 0, \\ \lambda_1 + \lambda_2 + \cdots + \lambda_k = 1 \\ \text{distinct } Q^{(1)}, Q^{(2)}, \dots, Q^{(k)} \in \mathcal{T}^{(i)} \\ Q^{(1)}_{[a]} = \cdots = Q^{(k)}_{[a]} \text{ or } Q^{(1)}_{[b]} = \cdots = Q^{(k)}_{[b]} \end{array} \right\}$$

3. Hull.

$$\mathcal{T}^{(\infty)} := \bigcup_{i \geqslant 0} \mathcal{T}^{(i)}.$$

Roughly speaking, $\mathcal{T}^{(i+1)}$ contains the convex hull of any $\leqslant d$ points in $\mathcal{T}^{(i)}$ if their first a coordinates or their next b coordinates match. On the other hand, the recursive construction of $\mathcal{S}^{(i+1,\Lambda)}$ contains the convex hull of only $\leqslant 2$ points in $\mathcal{S}^{(i,\Lambda)}$. Intuitively, the $\{\mathcal{T}^{(i)}\}_{i \geqslant 0}$ evolves "faster." However, a convex linear combination of more points can be emulated by iteratively taking convex linear combinations of only 2 points at a time. So, any point in $\mathcal{T}^{(i)}$ will also lie in $\mathcal{S}^{(i',\Lambda)}$ for a (possibly) larger i'. We will need the following results.

Result 1. $\mathcal{S}^{(\infty,\Lambda)} = \mathcal{T}^{(\infty)}$. Lemma H.1 states this result, and we have proved it previously.

Result 2. $\mathcal{T}^{(i)}\big|_g \subseteq \mathbf{X}_g^{(i+1)}$, where $g \in \mathcal{G}$ is a grid point and $i \in \{0, 1, 2, \dots\}$. Lemma I.2 will state and prove this result below.

For an arbitrary grid point $g \in \mathcal{G}$, using the results above, the proof follows from the following sequence of reasoning.

$$\begin{aligned} \mathcal{S}^{(\infty,\Lambda)}\big|_g &= \mathcal{T}^{(\infty)}\big|_g && \text{(by result 1 above)} \\ &= \bigcup_{i \geqslant 0} \mathcal{T}^{(i)}\big|_g && \text{(by definition)} \\ &\subseteq \bigcup_{i \geqslant 0} \mathbf{X}_g^{(i+1)} && \text{(by result 2 above)} \\ &\subseteq \mathbf{X}_g^{(*)} \quad . && \text{(by definition)} \end{aligned}$$

This completes the final direction of the proof.

At this point, all that remains to complete the proof of Lemma 4 is to prove Lemma I.1 and Lemma I.2, which are stated and proved below.

I.1 Statement and Proof of Lemma I.1

Lemma I.1. $\left(\mathcal{S}^{(\infty,\Lambda)}\big|_g : g \in \mathcal{G} \right)$ *is a solution of the system* $\mathcal{I}$ *introduced in Figure 8.*

Proof. First, we will prove that $\mathcal{S}^{(\infty,\Lambda)}\big|_g$ is convex, for each grid point $g \in \mathcal{G}$. Then, we will prove that $\left(\mathcal{S}^{(\infty,\Lambda)}\big|_g : g \in \mathcal{G} \right)$ is a solution of the system $\mathcal{I}$.

Part 1: Convexity. Consider any grid point $g \in \mathcal{G}$ and arbitrary points $P, Q \in \mathcal{S}^{(\infty,\Lambda)}\big|_g$. There there are $r, k \in \{0, 1, 2, \dots\}$ such that $P \in \mathcal{S}^{(r,\Lambda)}\big|_g$ and $Q \in \mathcal{S}^{(k,\Lambda)}\big|_g$. The nested guarantee of Equation 39, implies that $P, Q \in \mathcal{S}^{(t,\Lambda)}\big|_g$, where $t := \max\{r, k\}$. Moreover, $P, Q \in \mathcal{S}^{(t,\Lambda)}\big|_g$ implies that $P_{[a]} = Q_{[a]}$; therefore, $P - Q \in \Lambda$. So, all convex linear combinations of P and Q are contained in $\mathcal{S}^{(t+1,\Lambda)}\big|_g$. This proves that the set $\mathcal{S}^{(\infty,\Lambda)}\big|_g$ is convex.

Part 2: Solution of our system. Now, we will prove that $\left(\mathcal{S}^{(\infty,\Lambda)}\big|_g \,:\, g \in \mathcal{G} \right)$ is a solution of the system $\mathcal{I}$ when we assign $X_g = \mathcal{S}^{(\infty,\Lambda)}\big|_g$ for grid point $g \in \mathcal{G}$.

Base case constraints. Consider any point $P \in \mathcal{S}^{(0,\Lambda)}$ and define $g = \big(P_{[a]}, P_{[v]}\big)$. Let us focus on the base case constraint $X_g \geqslant \{P\}$ in our system I. Note that $P \in \mathcal{S}^{(0,\Lambda)}\big|_g$. The nested property of our sets imply $\mathcal{S}^{(i,\Lambda)} \subseteq \mathcal{S}^{(i+1,\Lambda)}$ for all $i \in \{0, 1, 2, \dots\}$. Therefore, we conclude that $P \in \mathcal{S}^{(\infty,\Lambda)}\big|_g = \bigcup_{i \geqslant 0} \mathcal{S}^{(i,\Lambda)}\big|_g$; thus, satisfying the inequality under consideration.

Spatial information constraints. Consider a spatial information constraint Equation 26 in Figure 8

$$X_{(u,v)} \geqslant \sum_{i=1}^{k} \alpha^{(i)} \cdot X_{(u^{(i)},v)}$$

such that $u = \sum_{i=1}^{k} \alpha^{(i)} \cdot u^{(i)}$. Consider arbitrary points $P^{(i)} \in \mathcal{S}^{(\infty,\Lambda)}\big|_{(u^{(i)},v)}$ for $i \in \{1, 2, \dots, k\}$. That implies $P^{(i)} \in \mathcal{S}^{(t_i,\Lambda)}\big|_{(u^{(i)},v)}$ for some $t_i \in \{0, 1, \dots\}$. By the nested property of our sets in Equation 39, we conclude that $P^{(i)} \in \mathcal{S}^{(t,\Lambda)}\big|_{(u^{(i)},v)}$ for $t = \max\{t_1, t_2, \dots, t_k\}$ and $i \in \{1, 2, \dots, k\}$.

Note that $\mathcal{S}^{(t+1,\Lambda)}$ will contain the convex hull of any two points $P^{(i_1)}, P^{(i_2)}$, where $i_1, i_2 \in \{1, 2, \dots, k\}$, because $P^{(i_1)}_{[b]} = P^{(i_2)}_{[b]}$. The indices i_1, i_2 need not be distinct. Next, $\mathcal{S}^{(t+2,\Lambda)}$ will contain the convex hull of any four (or fewer) points in $\{P^{(1)}, P^{(2)}, \dots, P^{(k)}\}$. Continuing in this manner, $\mathcal{S}^{(t+\Delta,\Lambda)}$ will contain $\mathrm{conv}\big(P^{(1)}, P^{(2)}, \dots, P^{(k)}\big)$, where $\Delta = \lceil \log_2 k \rceil$. In particular, the point $P := \sum_{i=1}^{k} \alpha^{(i)} \cdot P^{(i)}$ belongs to the set $\mathcal{S}^{(t+\Delta,\Lambda)}$. Since $(u, v) = \sum_{i=1}^{k} \alpha^{(i)} \cdot \big(u^{(i)}, v\big)$, we have $P \in \mathcal{S}^{(t+\Delta,\Lambda)}\big|_{(u,v)} \subseteq \mathcal{S}^{(\infty,\Lambda)}\big|_{(u,v)}$ specifically. Therefore, we conclude that

$$\mathcal{S}^{(\infty,\Lambda)}\Big|_{(u,v)} \geqslant \sum_{i=1}^{k} \alpha^{(i)} \cdot \mathcal{S}^{(\infty,\Lambda)}\Big|_{(u^{(i)},v)},$$

which implies that the spatial constraint above is satisfied. Spatial constraints of the form Equation 27 are also analogously satisfied.

This proves that $\left(\mathcal{S}^{(\infty,\Lambda)}\big|_g \,:\, g \in \mathcal{G} \right)$ is a solution of the system $\mathcal{I}$. □

I.2 Statement and Proof of Lemma I.2

Lemma I.2. *For a grid point $g \in \mathcal{G}$ and $i \in \{0, 1, 2, \dots\}$, we have $\mathcal{T}^{(i)}\big|_g \subseteq \mathbf{X}_g^{(i+1)}$.*

Proof. Consider the system of inequalities of Figure 8. To prove this statement, we proceed by induction on $i \in \{0, 1, 2, \dots\}$.

Base case $i = 0$. By definition, for any grid point $g \in \mathcal{G}$, we have

$$\mathcal{T}^{(0)}\Big|_g = \Big\{ P \in \mathcal{S}^{(0,\Lambda)} \,:\, g = \big(P_{[a]}, P_{[b]}\big) \Big\}.$$

When constructing $\mathbf{X}^{(1)}$ from $\mathbf{X}^{(0)}$ according to the iterative procedure in Figure 5 of Section 2.4, the base case constraints imply that

$$\mathbf{X}_g^{(1)} \geqslant \{P\},$$

for every $P \in \mathcal{T}^{(0)} = \mathcal{S}^{(0,\Lambda)}$ satisfying $g = \big(P_{[a]}, P_{[b]}\big)$. Therefore, we have $\mathcal{T}^{(i)}\big|_g \subseteq \mathbf{X}_g^{(i+1)}$ for $i = 0$.

Inductive hypothesis. For some $i \in \{0, 1, 2, \dots\}$, assume that $\mathcal{T}^{(i)}\big|_g \subseteq \mathbf{X}_g^{(i+1)}$ for every grid point $g \in \mathcal{G}$.

Induction. Now, we need to prove that $\mathcal{T}^{(i+1)}\big|_g \subseteq \mathbf{X}_g^{(i+2)}$ for any grid point $g \in \mathcal{G}$. We will use the following result.

Result. It follows from Lemma H.3 that for any $P \in \mathcal{T}^{(i+1)}\big|_g$, there are appropriate grid points $g^{(1)}, g^{(2)}, \dots, g^{(\ell)} \in \mathcal{G}$ such that $P \in \sum_{j=1}^{\ell} \alpha^{(j)} \cdot \mathcal{T}^{(i)}\big|_{g^{(j)}}$ and $g = \sum_{j=1}^{\ell} \alpha^{(j)} \cdot g^{(j)}$. Moreover, $g_{[a]} = g_{[a]}^{(1)} = \cdots = g_{[a]}^{(\ell)}$ or $g_{[b]} = g_{[b]}^{(1)} = \cdots = g_{[b]}^{(\ell)}$. The parameter ℓ may be larger than $(a+1)$ or $(b+1)$.

By the inductive hypothesis, we have $\mathbf{X}_{g^{(j)}}^{(i+1)} \geqslant \mathcal{T}^{(i)}\big|_{g^{(j)}}$ for $j \in \{1, 2, \dots, \ell\}$. Without loss of generality, assume that $g_{[b]} = g_{[b]}^{(1)} = \cdots = g_{[b]}^{(\ell)} =: v$ (the proof for the other case is analogous). Denote $u := g_{[a]} = \sum_{j=1}^{\ell} \alpha^{(j)} \cdot g_{[a]}^{(j)}$.

Consider each simplex C with vertices $g^{(j_1,C)}, g^{(j_2,C)}, \dots, g^{(j_k,C)}$, where $k \leqslant a+1$ (by Carathéodory's theorem [Car07], such that g is in its relative interior. Corresponding to this simplex, we have a spatial constraint in Equation 26; say

$$X_g \geqslant \sum_{t=1}^{k} \alpha^{(t,C)} \cdot X_{g^{(j_t,C)}}.$$

The iterative definition of $\mathbf{X}_g^{(i+2)}$ ensures that

$$\mathbf{X}_g^{(i+2)} \geqslant \sum_{t=1}^{k} \alpha^{(t,C)} \cdot \mathbf{X}_{g^{(j_t,C)}}^{(i+1)} \overset{\dagger}{\geqslant} \sum_{t=1}^{k} \alpha^{(t,C)} \cdot \mathcal{T}^{(i)}\Big|_{g^{(j_t,C)}}.$$

The (†) inequality above uses the inductive hypothesis.

The point P lies in the set $\sum_{j=1}^{\ell} \alpha^{(j)} \cdot \mathcal{T}^{(i)}\big|_{g^{(j)}}$. This expression can be written as the convex linear combination of expressions corresponding to simplices that contain g in their relative interior.[4] Therefore, by considering all possible simplices containing g in its relative interior, we conclude that

$$\mathbf{X}_g^{(i+2)} \geqslant \sum_{j=1}^{\ell} \alpha^{(j)} \cdot \mathcal{T}^{(i)}\Big|_{g^{(j)}}$$

is also satisfied. Consequently, any $P \in \mathcal{T}^{(i+1)}\big|_g$ also satisfies $P \in \mathbf{X}_g^{(i+2)}$, and, therefore, $\mathcal{T}^{(i+1)}\big|_g \subseteq \mathbf{X}_g^{(i+2)}$. □

J Complexity of Answering Lamination Hull Membership Queries

This section presents the run-time analysis of our algorithm in Figure 3.

The initial set is $S^{(0,\Lambda)} \subset \mathbb{R}^{a+b+c}$, where $a, b \geqslant 1$ and $c \geqslant 0$. Let $s \geqslant 2$ denote the cardinality of $S^{(0,\Lambda)}$. The total number of grid points is $\operatorname{card}\left(\mathcal{G}^{(a)}\right) \cdot \operatorname{card}\left(\mathcal{G}^{(b)}\right)$, which is

$$\overset{\dagger}{\leqslant} 2^{s^{a+1}+s^{b+1}} \leqslant 2^{s^{a+b+1}}.$$

[4] Even if $\ell > (a+1)$, this decomposition is possible due to Carathéodory's theorem.

The (†) bound follows from estimating the number of arrangements in Equation 23.

So, the procedure in Figure 8 creates a system of inequalities with n unknowns, where

$$n \;\coloneqq\; \operatorname{card}(\mathcal{G}) = \operatorname{card}\left(\mathcal{G}^{(a)}\right) \cdot \operatorname{card}\left(\mathcal{G}^{(b)}\right) \leqslant 2^{s^{a+b+1}}. \tag{40}$$

There are s base case constraints. The number of spatial information constraints like Equation 26 is

$$\leqslant \operatorname{card}(\mathcal{G}) \cdot \operatorname{card}\left(\mathcal{G}^{(a)}\right)^{a+1} = \operatorname{card}\left(\mathcal{G}^{(b)}\right) \cdot \operatorname{card}\left(\mathcal{G}^{(a)}\right)^{a+2} \leqslant 2^{s^{b+1}+(a+2)\cdot s^{a+1}} \leqslant 2^{(a+b+2)\cdot 2^{a+b}}.$$

Likewise, the number of spatial constraints like Equation 27 is

$$\leqslant 2^{(a+b+2)\cdot s^{a+b}}.$$

So, the total number of constraints is

$$\leqslant s + 2^{(a+b+3)\cdot s^{a+b}} \leqslant 2^{(a+b+4)\cdot s^{a+b}}.$$

Therefore, every inequality in the system has $\leqslant 2^{(a+b+4)\cdot s^{a+b}} =: k$ monomials, each of degree (at most) $\max\{a+1, b+1\} \leqslant (a+b) =: D$.

Lemma E.1 states that after running our Gaussian elimination-inspired algorithm of Figure 4 on this system, we get a system such that each polynomial in it has the following properties:

1. The number of monomials is (at most)

$$k^{(D+1)^n} = 2^{(a+b+1)^n\cdot(a+b+4)\cdot s^{a+b}} \leqslant 2^{(a+b+1)^{2^{s^{a+b+1}}}\cdot(a+b+4)\cdot s^{a+b}} \leqslant 2^{2^{2^{2^{\mathcal{O}(a+b+s)}}}}.$$

2. The degree of each monomial is (at most)

$$D^{3^n} \leqslant (a+b)^{3^{2^{s^{a+b+1}}}} \leqslant 2^{2^{2^{2^{\mathcal{O}(a+b+s)}}}}.$$

All that remains is to estimate the time taken to determine the membership of Q in Figure 3. It is dominated by the time taken to determine the membership of a point in the convex hull of $k^{(D+1)^n}$ subsets of $\mathbb{R}^{a+b+c}$, each of these subsets is the relative interior of a polytope with (at most) D^{3^n} vertices. Lemma J.1 presents this estimate; it is stated and proved below. Using this estimate, we conclude that the running time of Figure 3 is at most

$$2^{2^{2^{2^{\mathcal{O}(d+s)}}}},$$

where $d = a+b+c$. In our cryptographic application, we have $s \leqslant c$ and $d = \operatorname{card}(X) + \operatorname{card}(Y) + \operatorname{card}(Z)$. Hence, for that specific application, the running time is

$$2^{2^{2^{2^{\mathcal{O}(\operatorname{card}(X)+\operatorname{card}(Y)+\operatorname{card}(Z))}}}}. \tag{41}$$

Technical result. We will prove the following technical result here.

Lemma J.1. *Suppose φ^* be a polynomial over $\mathrm{CL}(\Omega_P)$, where Ω_P is the set of all constants. Suppose φ^* has k' monomials with degree (at most) D'. Let $\mathbf{P}$ be a constant assignment such that each constant is assigned singleton elements in $\mathbb{R}^d$. One can answer whether a point $Q \in \mathbb{R}^d$ lies in $\mathrm{conv}(\mathrm{eval}(\varphi^*; \mathbf{P}))$ or not in time*

$$\left(k'\right)^{O((D'+d)^2)}.$$

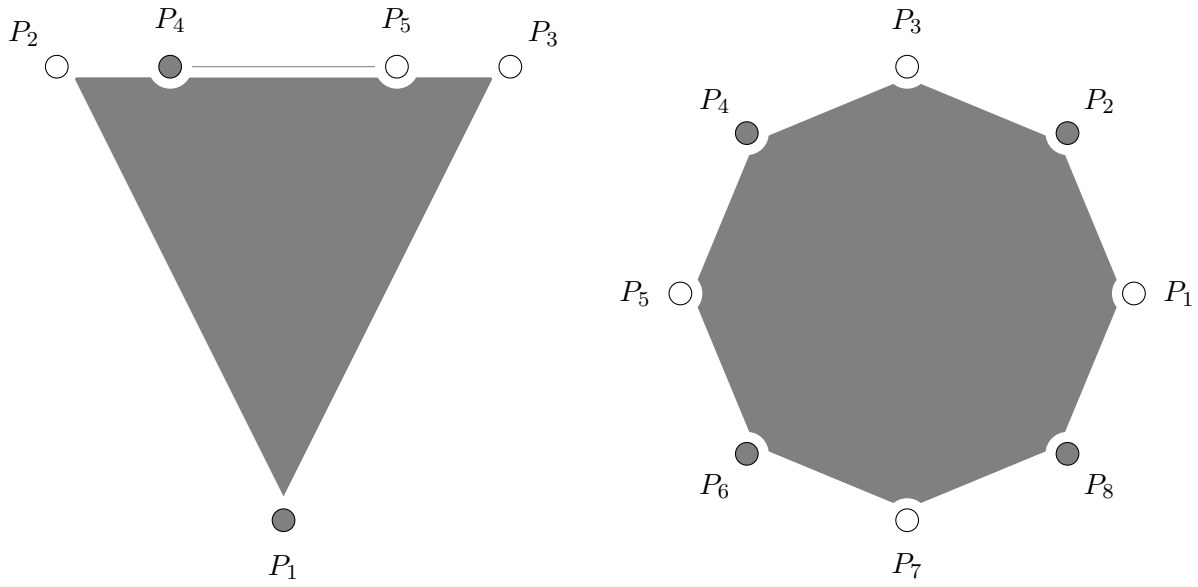
Proof. The evaluation of a monomial of degree (at most) D' is the relative interior of a polytope with (at most) D' vertices. We remind the reader that the relative interior of a point is the point itself. Consider k' sets, one for the evaluation of each monomial. By Carathéodory's theorem, it suffices to test the membership of the point Q in the convex hull of all possible $\leqslant (d+1)$ choices of sets among these k' sets.

At this point, we have the following subproblem. Consider sets $S^{(1)}, S^{(2)}, \ldots, S^{(d')} \subset \mathbb{R}^d$, such that $1 \leqslant d' \leqslant (d+1)$, and each of these sets is the relative interior of a polytope with (at most) D' vertices. Using quantifier elimination [BPRon, Chapter 14], we can determine the membership of Q in $\mathrm{conv}\left(S^{(1)} \cup S^{(2)} \cup \cdots \cup S^{(d')}\right)$ with complexity that can be bounded singly exponentially (in the parameters D' and d) using the complexity of the quantifier elimination algorithm in [BPRon].

Consider all $\binom{k'}{\leqslant (d+1)}$ subsets, we get the final estimate of the running time. □

K Hemihedra

Figure 16 presents a few examples illustrating hemihedral sets.



(a) $\mathrm{conv}^o(\{P_1, P_2, P_3\}) \bigcup \mathrm{conv}^o(\{P_4, P_5\}) \bigcup \mathrm{conv}^o(\{P_1\}) \bigcup \mathrm{conv}^o(\{P_4\})$

(b) $\mathrm{conv}^o(\{P_1, P_2, \ldots, P_8\}) \bigcup \mathrm{conv}^o(\{P_2\}) \bigcup \mathrm{conv}^o(\{P_4\}) \bigcup \mathrm{conv}^o(\{P_6\}) \bigcup \mathrm{conv}^o(\{P_8\})$

Figure 16: Examples of Hemihedra. Here $\mathrm{conv}^o(S)$ represents the relative interior of the convex hull of a finite set of points S. If S is a singleton set, then $\mathrm{conv}^o(S)$ is the point in S itself.

A motivating example. Let $X \subseteq \mathbb{R}$ be a convex set satisfying:

1. It contains the point $P \in \mathbb{R}$ and
2. It contains the midpoint of any point in X and the point $Q \in \mathbb{R}$.

The following system represents these constraints.

$$X \supseteq \{P\} \ \oplus \ \left(\frac{1}{2} \cdot X + \frac{1}{2} \cdot \{Q\}\right).$$

The smallest convex X is the union of P and the relative interior of the line segment $\overline{PQ}$, i.e., $\{P\} \ \oplus \ \{P\} \overset{\circ}{\star} \{Q\}$. The smallest *polytope* simultaneously satisfying the equation is the line segment $\overline{PQ}$, which contains the spurious point Q.

Perspective: Hemihedra-like geometric objects in mathematics. Convex polytopes (as well as polyhedra) in $\mathbb{R}^d$ are exceptionally well studied [Grü03, Zie95]. By definition, they are closed subsets of $\mathbb{R}^d$. This paper proves that lamination hulls of finite sets of points (for certain choices of Λ) are not necessarily closed or even locally closed, but their closure is a convex polytope. This necessitates a definition of a class of convex subsets, which we call hemihedra. Note that non-closed convex polyhedra appear naturally when convex hull operators are applied, starting from closed convex sets. For instance, the convex hull of the closed convex polyhedra in $\mathbb{R}^2$, $\{(0,0)\}$ and $\{(x,y)\colon x \geqslant 1\}$ is the convex set

$$\Big\{(0,0)\Big\} \bigcup \Big\{(x,y)\colon x > 0\Big\},$$

which is not closed or even locally closed. (Technically, it is not a hemihedron as per our definition since it is not bounded). In semi-algebraic geometry, semi-algebraic sets that are not locally closed arise naturally and create severe mathematical difficulties (for instance, in questions regarding their topological complexity). Hence, such sets have been the object of special attention (see, for example, [GV09, GV17a]). For example, the problem of proving lower bounds on the depths of algebraic computation trees for membership testing in semi-algebraic sets is considerably more difficult when the set is not locally closed. The fundamental result of Yao [Yao97] in this direction has only recently been extended to the non-locally closed case [GV17b]. From the point of view of topology, hemihedra are much more complicated objects than convex polytopes. For instance, the generalized Euler-Poincaré characteristic [vdD98] of a convex polytope in $\mathbb{R}^d$ always equals 1. Yet, it can be arbitrarily large for a hemihedron. For instance, the union of the interior of a regular $2n$-gon in the plane (with vertices $P_1, \ldots, P_{2n}$) with the set of even-numbered vertices is a hemihedron (see Figure 16 (b)), and has generalized Euler-Poincaré characteristic equal to $(n+1)$. Since the generalized Euler-Poincaré characteristic of semi-algebraic sets is a homeomorphism invariant – this implies, in particular, that even though the number of topologically distinct non-empty polytopes (i.e., up to homeomorphisms) in $\mathbb{R}^d$ is $d+1$ (one in each dimension $\leqslant d$), there are infinitely many topologically distinct hemihedra.