Privacy Structure and Blackwell Frontier*

Zhang Xu† Wei Zhao‡

November 14, 2025

Abstract

This paper characterizes the set of feasible posterior distributions subject to graph-based inferential privacy constraint, including both differential and inferential privacy. This characterization can be done through enumerating all extreme points of the feasible posterior set. A connection between extreme posteriors and strongly connected semi-chains is then established. All these semi-chains can be constructed through successive unfolding operations on semi-chains with two partitions, which can be constructed through classical spanning tree algorithm. A sharper characterization of semi-chains with two partitions for differential privacy is provided.

*We are grateful for valuable comments and discussions from Yang Sun. All errors are our own.

†School of Economics, Renmin University of China, China. *Email*: xuzhang@ruc.edu.cn

‡School of Economics and Management, Tsinghua University. *Email*: wei.zhao@outlook.fr

Contents

1 Introduction

Information plays a critical role in decision making and effectiveness of mechanisms. Recent technological development facilitates the collection, storage, acquisition and usage of data. At the same time as efficiency improvement, growing concerns on information leakage have been drawn. Various privacy constraints have been imposed to address these concerns. This paper tries to, subject to exogenous privacy constraint, characterize the feasible information which can be disclosed, through characterizing the feasible posterior distributions.

The significance of this result is both theoretical and practical. A key insight of Bayesian persuasion (c.f. Kamenica and Gentzkow 2011) is that the set of information structures can be mapped to the set of Bayesian-plausible posterior distributions. Since then, information disclosure is often characterized directly on the space of posterior distributions. In this spirit, theoretically, our work identifies the restrictions that privacy constraints impose on posterior distributions. Practically, characterizing the set of feasible posterior distributions guides optimal, privacy-constrained decision-making. This, in turn, enables the endogenous determination of the optimal degree of privacy protection (c.f. Abowd and Schmutte 2019). More generally, the characterization of feasible posterior distributions provides a foundation for privacy-constrained information design (c.f. Schmutte and Yoder 2022 and Pan et al. 2025), which can be derived through concavification over the set of feasible posteriors. The second application is on the characterization of feasible data queries subject to privacy constraints on a sensitive variable (For perfect privacy preservation, see Strack and Yang 2024, He et al. 2021; for relaxed constraints, see Wang et al. 2025, Xu and Zhao 2025). Our companion paper, Xu and Zhao (2025), shows that this query characterization problem reduces to characterizing the privacy-constrained posterior distributions on the sensitive variable. This characterization of feasible queries is fundamental to optimal decision-making under such constraints (e.g., price discrimination with perfect privacy preservation; Strack and Yang 2025).

The most intuitive privacy requirement for signals is based on *pairwise indistinguishability*: after observing a signal, the additional information should not allow the receiver to distinguish a pair of realizations (θ_i, θ_j) much more precisely than under the prior. Formally, for almost every posterior belief $\mu \in \Delta(\Theta)$ induced by the signal,

$$e^{-\varepsilon}\frac{\mu_0(\theta_i)}{\mu_0(\theta_j)} \leq \frac{\mu(\theta_i)}{\mu(\theta_j)} \leq e^{\varepsilon}\frac{\mu_0(\theta_i)}{\mu_0(\theta_j)}, \tag{1}$$

where μ_0 is the prior belief and $\varepsilon \geq 0$ controls the allowable degree of distinguishability.

This condition provides a *linear* measure of how much additional information about the pair (θ_i, θ_j) the signal may reveal. When this requirement is imposed on all pairs of realizations, it induces ε-inferential privacy (Definition 1). When it is imposed only on neighboring realizations, it induces ε-differential privacy (Definition 2). More generally, the pairwise indistinguishability structure can be represented by a graph on Θ, where an edge between two realizations indicates that the information disclosed about this pair must satisfy the privacy requirement. We call this definition of privacy as graph-based inferential privacy.

In this paper, we focus on graph-based inferential privacy. Our objective is to characterize the Blackwell frontier of privacy-preserving signals. Lemma 1 establishes that a privacy-preserving signal is Blackwell-undominated if and only if almost every possible posterior belief is an extreme point. Therefore, to characterize the Blackwell frontier, it suffices to identify the extreme points of the feasible belief set.

Our first result establishes a connection between extreme points and semi-chains of the underlying graph (Theorem 1). An L-semi-chain is a specific structure imposed on a graph that partitions its nodes into L levels such that every edge connects either two nodes within the same level or nodes in two adjacent levels. Given an L-semi-chain, the posterior assigns to each realization in l-level a probability that is proportional to l times its prior probability.

When the graph is complete, corresponding to ε-inferential privacy, the definition of a semi-chain implies that only 2-semi-chains exist, and any such partition corresponds to an extreme posterior belief (Corollary 1). In contrast, for a general graph, the question arises: how can we systematically generate all of its semi-chains? Our second main result shows that any L-semi-chain can be generated from a 2-semi-chain through *unfolding* (Theorem 2). Unlike L-semi-chains with $L \geq 3$, 2-semi-chains have only two levels, so we do not need to enforce the constraint that edges cannot exist between non-adjacent levels. This simplification allows us to generate all 2-semi-chains by enumerating the spanning trees of the graph.

Under the setting of ε-differential privacy, where each realization is a K-dimensional vector, L-semi-chains exist if and only if $L \leq K + 1$ (Proposition 1). In the binary case, where each dimension takes values in $\{0, 1\}$, there exists a unique 2-semi-chain up to reversing the first and second levels (Proposition 2). For the two-dimensional case, we provide an algorithm that generates all 2-semi-chains without duplication (Proposition 3).

2 Graph-Based Inferential Privacy

Database. A sensitive database is a random variable θ, distributed according to an interior distribution μ_0 over a finite set $\Theta := \{\theta_1, \ldots, \theta_J\}$. In practice, θ may be multidimensional and capture all relevant characteristics of an agent or a set of agents, such as history records, income, age, gender, race, address, etc.

Signals. A signal is a mapping $\pi : \Theta \to \Delta(S)$, where $S \subseteq \mathbb{R}$ is the signal space. Observing a signal realization $s \in S$ induces a posterior $\mu_s \in \Delta(\Theta)$. The signal π thus induces a distribution over posteriors, denoted by $\langle \pi \rangle$.

Graph-Based Inferential Privacy. Let $\mathbf{G} = (g_{ij})_{i,j=1}^{J} \in \{0,1\}^{J \times J}$ denote an undirected, connected graph over the set of nodes Θ. For any pair $(\theta_i, \theta_j) \in \Theta^2$, we set $g_{ij} = 1$ if there is a link between θ_i and θ_j, and $g_{ij} = 0$ otherwise. The graph is symmetric, i.e., $g_{ij} = g_{ji}$ for all $i, j \in \{1, \ldots, J\}$, and, without loss of generality, $g_{ii} = 0$ for all i. With a slight abuse of notation, we write $(\theta_i, \theta_j) \in \mathbf{G}$ whenever $g_{ij} = 1$.

Given a $\mathbf{G}$ and some $\varepsilon \geq 0$, we define

$$\mathcal{M}_{\mathbf{G}}^{\varepsilon} := \left\{ \mu \in \Delta(\Theta) : \frac{\mu(\theta_i)}{\mu_0(\theta_i)} \leq e^{\varepsilon} \frac{\mu(\theta_j)}{\mu_0(\theta_j)} \text{ for all } (\theta_i, \theta_j) \in \mathbf{G} \right\},$$

which is a closed convex subset of $\Delta(\Theta)$. Let $\operatorname{ext} \mathcal{M}_{\mathbf{G}}^{\varepsilon}$ as the set of extreme points of $\mathcal{M}_{\mathbf{G}}^{\varepsilon}$, i.e., $\operatorname{ext} \mathcal{M}_{\mathbf{G}}^{\varepsilon} := \{\mu \in \mathcal{M}_{\mathbf{G}}^{\varepsilon} : \nexists \mu' \neq \mu'' \in \mathcal{M}_{\mathbf{G}}^{\varepsilon}, \alpha \in (0,1) \text{ such that } \mu = \alpha\mu' + (1-\alpha)\mu''\}$. For any $\mu \in \operatorname{ext} \mathcal{M}_{\mathbf{G}}^{\varepsilon}$, we refer to it as an extreme posterior (with respect to $\mathcal{M}_{\mathbf{G}}^{\varepsilon}$).

Definition 1. *A signal π is $(\mathbf{G}, \varepsilon)$-inferential privacy-preserving if $\langle \pi \rangle (\mathcal{M}_{\mathbf{G}}^{\varepsilon}) = 1$.*

Since $\mathbf{G}$ is undirected and symmetric, for any $(\theta_i, \theta_j) \in \mathbf{G}$, if $\mu \in \mathcal{M}_{\mathbf{G}}^{\varepsilon}$, then

$$e^{-\varepsilon} \frac{\mu(\theta_j)}{\mu_0(\theta_j)} \leq \frac{\mu(\theta_i)}{\mu_0(\theta_i)} \leq e^{\varepsilon} \frac{\mu(\theta_j)}{\mu_0(\theta_j)}.$$

When $\varepsilon = 0$, if the database is either θ_i or θ_j, then the receiver's posterior belief over θ_i and θ_j coincides with the prior, i.e.

$$\frac{\mu(\theta)}{\mu(\theta_i) + \mu(\theta_j)} = \frac{\mu_0(\theta)}{\mu_0(\theta_i) + \mu_0(\theta_j)}, \quad \forall \theta \in \{\theta_i, \theta_j\}.$$

In other words, the receiver cannot make any additional inference from the signal to distinguish between θ_i and θ_j. When $\varepsilon > 0$ but sufficiently small, this inference remains limited.

The graph $\mathbf{G}$ specifies which pairs of information are not allowed to be inferred from the signal.

Graph-based inferential privacy is developed within the framework introduced by Kifer and Machanavajjhala (2014). In their framework, one may specify a subset of prior distributions, and the privacy constraints are required to hold only with respect to those priors. In contrast, we focus on a fixed information structure that is independent of the prior belief. Consequently, if the privacy constraints are satisfied under any interior prior, they are satisfied under all priors.

One important special case of graph-based inferential privacy is *differential privacy*, originally proposed by Dwork et al. (2006). This notion has achieved remarkable success: beyond an extensive and growing academic literature, it has been adopted as a core privacy framework by major institutions such as Google, Microsoft, and the U.S. Census Bureau (Abowd 2018). Under differential privacy, only information differences between *neighboring* realizations of the dataset are protected. Specifically, let $\Theta = \prod_{k=1}^{K} \Theta^{(k)}$, where each $\Theta^{(k)}$ is finite and $\theta = (\theta^{(1)}, \ldots, \theta^{(K)})$. Two realizations $\theta_i, \theta_j \in \Theta$ are said to be neighboring if and only if there exists $\hat{k} \in \{1, \ldots, K\}$ such that

$$\theta_i^{(\hat{k})} \neq \theta_j^{(\hat{k})}, \quad \theta_i^{(-\hat{k})} = \theta_j^{(-\hat{k})},$$

where $\theta^{(-k)} := (\theta^{(1)}, \ldots, \theta^{(k-1)}, \theta^{(k+1)}, \ldots, \theta^{(K)})$. We can then define $\mathbf{G}_{\text{diff}}$ as the *differential graph*, where $(\theta_i, \theta_j) \in \mathbf{G}_{\text{diff}}$ if and only if θ_i and θ_j are neighboring.

Definition 2. *A signal π is ε-differential privacy if it is $(\mathbf{G}_{\text{diff}}, \varepsilon)$-inferential privacy.*

Another special case arises when $\mathbf{G}$ is a complete graph, denoted by $\mathbf{G}^*$, where $(\theta_i, \theta_j) \in \mathbf{G}^*$ for all $i \neq j$. This formulation was introduced by Ghosh and Kleinberg (2016) and subsequently applied by Wang et al. (2025) to study privacy-preserving information disclosure.

Definition 3. *A signal π is ε-inferential-preserving if it is $(\mathbf{G}^*, \varepsilon)$-inferential privacy, where $\mathbf{G}^*$ is the complete graph on Θ.*

2.1 Blackwell Frontier and Extreme Posteriors

Definition 4 (Blackwell Dominance)**.** *A signal π is Blackwell-dominated by a signal π', denoted by $\pi \preceq \pi'$, if for any action set A and measurable function $u : \Theta \times A \to \mathbb{R}$,*

$$\mathbb{E}_{s\sim\pi}\left[\sup_{a\in A} \mathbb{E}[u(\theta, a)|s]\right] \leq \mathbb{E}_{s\sim\pi'}\left[\sup_{a\in A} \mathbb{E}[u(\theta, a)|s]\right].$$

A signal π is Blackwell-equivalent to π', written $\pi \sim \pi'$, if $\pi \preceq \pi'$ and $\pi' \preceq \pi$. It is strictly Blackwell-dominated, written $\pi \prec \pi'$, if $\pi \preceq \pi'$ but not $\pi' \preceq \pi$.

Denote $\Pi_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}}$ as the set of $(\mathbf{G}, \varepsilon)$-inferential privacy-preserving signals and $\overline{\Pi}_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}}$ is its Blackwell frontier, i.e.,

$$\overline{\Pi}_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}} := \left\{\pi \in \Pi_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}} : \nexists\, \pi' \in \Pi_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}} \text{ such that } \pi \prec \pi'\right\}.$$

Lemma 1. *1. A signal is $(\mathbf{G}, \varepsilon)$-inferential privacy-preserving if and only if it is Blackwell-dominated by some signal in $\overline{\Pi}_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}}$.*

2. A signal $\pi \in \overline{\Pi}_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}}$ if and only if $\langle \pi \rangle (\operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}) = 1$.

According to Lemma 1: (i) to characterize all $(\mathbf{G}, \varepsilon)$-inferentially private signals, it suffices to describe their Blackwell frontier, since any other privacy-preserving signal can be obtained by garbling (Blackwell 1953); (ii) to characterize the Blackwell frontier, it is enough to identify all extreme posteriors, as $\overline{\Pi}_{\mathcal{M}^{\varepsilon}_{\mathbf{G}}}$ can be generated by convex combinations of extreme posteriors with respect to μ_0.

2.2 Notation

To streamline the subsequent analysis, we introduce several graph-theoretic concepts that will be used throughout the paper.

Definition 5 (Spanning Tree)**.** *A graph $\mathbf{T}$ is said to be a spanning tree of $\mathbf{G}$ if it is a connected subgraph of $\mathbf{G}$ with no cycles.*

Note that a spanning tree always has $J - 1$ edges.

Definition 6 (Ordered Partition)**.** *$\{\Theta_l\}_{l=1}^{L}$ is a L-partition of Θ if $\Theta_l \neq \emptyset$ for all $l \in \{1, \ldots, L\}$, $\Theta_l \cap \Theta_{l'} = \emptyset$ for any $l \neq l'$ and $\cup_{l=1}^{L} \Theta_l = \Theta$. A partition $\{\Theta_l\}_{l=1}^{L}$ with an order such that Θ_l is strictly lower than Θ_{l+1} for any $l \in \{1, \ldots, L-1\}$, is called an ordered partition, denoted by $(\Theta_l)_{l=1}^{L}$.*

Definition 7 (Semi-Chain)**.** *An ordered partition $C^L = (\Theta_l)_{l=1}^{L}$ with $L \geq 2$ is called an L-semi-chain of $\mathbf{G}$, if for any $\theta \in \Theta$, if $\theta \in \Theta_l$, then $N(\theta) \subseteq \Theta_{l-1} \cup \Theta_l \cup \Theta_{l+1}$, where*

$$N(\theta) := \{\theta' \in \Theta : (\theta, \theta') \in \mathbf{G}\}$$

is the neighboring set of θ *and* $\Theta_0, \Theta_{L+1} := \emptyset$*. The* l*-th element* Θ_l *is referred to as the* l*-level of* C^L*. Given a semi-chain, an edge* $(\theta_i, \theta_j) \in \mathbf{G}$ *is called a within-level edge if* θ_i *and* θ_j *belong to the same level, and a between-level edge otherwise.*

A semi-chain C *is strongly connected if, after deleting all within-level edges, the remaining graph of* $\mathbf{G}$ *is still connected.*

In Concas et al. (2021), a graph is said to be L-semi-chained if there exists an L-semi-chain based on this graph, and L-chained if there exists an L-chain, that is, an L-semi-chain without within-level edges.

3 Extreme Points of Feasible Posteriors

In this section, we establish the connection between the extreme points of $\mathcal{M}^{\varepsilon}_{\mathbf{G}}$ and the strongly connected semi-chains of the graph $\mathbf{G}$. The later can be enumerated by leveraging the spanning trees of the graph $\mathbf{G}$, for which efficient enumeration algorithms are well established in the graph theory literature. To this end, we first associate each $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ with a weighted directed graph $\mathbf{W} = (w_{ij})_{i,j=1}^{J} \in \mathbb{R}^{J\times J}$. This representation allows us to reformulate the linear programming problem in terms of $\mathbf{W}$.

Given a $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$, for any pair $(\theta_i, \theta_j) \in \Theta^2$, there is a w_{ij} such that

$$\delta_j = \delta_i + w_{ij}\varepsilon, \tag{2}$$

where $\delta_j := \ln \mu(\theta_j) - \ln \mu_0(\theta_j)$ for all $j \in \{1, \ldots, J\}$.[1] Then, the constraints defining $\mathcal{M}^{\varepsilon}_{\mathbf{G}}$ can be expressed as restrictions on $\mathbf{W} = (w_{ij})_{i,j=1}^{J} \in \mathbb{R}^{J\times J}$, i.e.,

$$w_{ij} \in [-1, 1] \quad \text{for all } (\theta_i, \theta_j) \in \mathbf{G}. \tag{3}$$

Given a $\mu \in \Delta(\Theta)$, there is a unique corresponding $\mathbf{W}$; conversely, given a $\mathbf{W}$, there is at most one corresponding μ. However, not every $\mathbf{W}$ can induce a distribution.

Lemma 2. *A matrix* $\mathbf{W}$ *can be obtained by* $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ *if and only if it satisfies* (3) *and*

$$w_{ij} = -w_{ji} \quad \text{for any } i, j \in \{1, \ldots, J\}, \tag{4}$$

$$w_{j_1 j_r} = \sum_{r'=1}^{r-1} w_{j_{r'} j_{r'+1}} \quad \text{for any } j_1, j_2, \ldots, j_r \in \{1, \ldots, J\}. \tag{5}$$

[1] Since $\mathbf{G}$ is connected, when $\varepsilon > 0$, for any $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ and $\theta \in \Theta$, $\mu(\theta) > 0$.

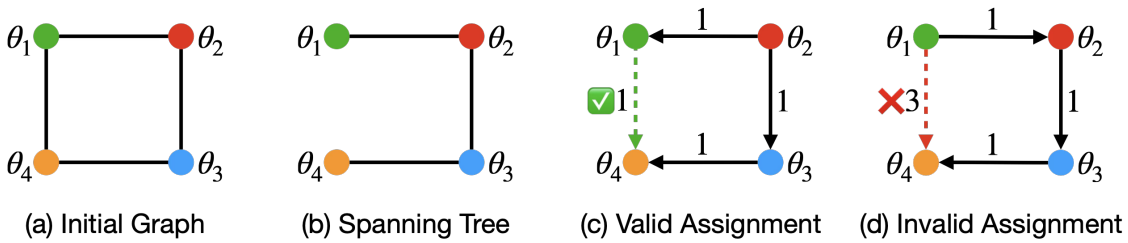


Figure 1: Illustration of Weight Assignments on a Spanning Tree

Note: Panels (c) and (d) illustrate two different weight assignments on the spanning tree shown in Panel (b). In both panels, the notation "$\theta_i \xrightarrow{1} \theta_j$" indicates that $w_{ij} = 1$. In Panel (c), the assignment induces $w_{14} = 1$, which satisfies condition (3), whereas in Panel (d), $w_{14} = 3 > 1$ violates condition (3).

Here, equations (4) and (5) characterize the interdependence among the entries. Since a $\mu \in \Delta(\Theta)$ only have $(J-1)$ freedom, once the values of a sequence $w_{j_1 j_2}, \ldots, w_{j_{J-1} j_J}$ are fixed, all other entries of $\mathbf{W}$ are endogenously determined by (4) and (5).[2] By the correspondence between basic feasible solutions and extreme points (Theorem 3.1, pp.102, Bazaraa et al. (2011)), each extreme point of $\mathcal{M}^{\varepsilon}_{\mathbf{G}}$ is uniquely characterized by $(J-1)$ independent entries w_{ij} satisfying $|w_{ij}| = 1$. This assertion can be expressed as Lemma 3.

Lemma 3. *Suppose* $\mathbf{W}$ *corresponds to some* $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$. $\mu \in \operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ *if and only if there exists a spanning tree* $\mathbf{T}$ *of* $\mathbf{G}$ *such that* $w_{ij} = \pm 1$ *for every* $(\theta_i, \theta_j) \in \mathbf{T}$.

The prerequisite of Lemma 3 is that the matrix $\mathbf{W}$ is induced by some $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$. Once this holds, Lemma 3 allows us to verify whether $\mathbf{W}$ corresponds to an extreme posterior. However, note that for a given spanning tree $\mathbf{T}$ of $\mathbf{G}$, not every arbitrary assignment of ± 1 weights to its edges yields a valid matrix $\mathbf{W}$ via (4) and (5), as the resulting $\mathbf{W}$ may violate condition (3). Figure 1 illustrates this point.

To construct all valid weight assignments on a spanning tree, we now shift our focus to the concept of semi-chains.

[2]By permuting $\mathbf{W}$, specifying the values of $w_{j_1 j_2}, w_{j_2 j_3}, \ldots, w_{j_{J-1} j_J}$ is equivalent to specifying the entries of the first superdiagonal $(w_{j,j+1})$. The second superdiagonal $(w_{j,j+2})$ can then be determined from $(w_{j,j+1})$ via (5), and the third superdiagonal can be determined from the second, and so on. By (4) the diagonal entries are equal to zero and the lower triangular part can be determined by the upper counterpart.

3.1 Connection Between Extreme Posteriors and Semi-Chains

Theorem 1. *A posterior $\mu \in \operatorname{ext} \mathcal{M}_{\mathbf{G}}^{\varepsilon}$ if and only if there exists a strongly connected L-semi-chain $C = (\Theta_l)_{l=1}^{L}$ such that the corresponding matrix $\mathbf{W}$ of μ satisfies*

$$w_{ij} = \begin{cases} 1 & \text{if there exists } l \in \{1, \dots, L-1\} \text{ such that } \theta_i \in \Theta_l, \theta_j \in \Theta_{l+1} \\ 0 & \text{if there exists } l \in \{1, \dots, L\} \text{ such that } \theta_i, \theta_j \in \Theta_l \end{cases}.$$

In Theorem 1, given an L-semi-chain C, the corresponding matrix $\mathbf{W}$ is determined endogenously: the weight of any within-level edge equals 0, and the absolute value of the weight of any between-level edge equals 1, with direction oriented from the lower to the higher level. All remaining entries of $\mathbf{W}$ are then uniquely determined by the condition (5). In what follows, unless stated otherwise, we say that a posterior μ is generated by C, implicitly referring to the $\mathbf{W}$ defined as in Theorem 1.

Since there are no edges between nodes in non-adjacent levels of a semi-chain, the corresponding $\mathbf{W}$ automatically satisfies condition (3). Moreover, every strongly connected semi-chain contains a spanning tree whose edges have weights ± 1. Therefore, a semi-chain naturally determines a valid weight assignment on a spanning tree.

Theorem 1 establishes a one-to-one correspondence between the extreme points of $\operatorname{ext} \mathcal{M}_{\mathbf{G}}^{\varepsilon}$ and the set of all strongly connected L-semi-chains. Given an L-semi-chain $C = (\Theta_l)_{l=1}^{L}$, the corresponding posterior distribution μ is generated by

$$\mu(\theta_i) = \frac{e^{l\varepsilon}\mu_0(\theta_i)}{\sum_{l'=1}^{L} e^{l'\varepsilon}\mu_0(\Theta_{l'})}, \quad \text{if } \theta_i \in \Theta_l.$$

That is, for any $\theta \in \Theta_l$, the posterior probability is proportional to $e^{l\varepsilon}\mu_0(\theta)$, up to normalization. For example, suppose $C = (\Theta_l)_{l=1}^{3}$ with $\Theta_1 = \{\theta_1\}$, $\Theta_2 = \{\theta_2\}$, and $\Theta_3 = \{\theta_3\}$ is a 3-semi-chain of some graph. Then the corresponding posterior μ is given by

$$\begin{aligned} \mu(\theta_1) &= \frac{\mu_0(\theta_1)}{\mu_0(\theta_1) + e^{\varepsilon}\mu_0(\theta_2) + e^{2\varepsilon}\mu_0(\theta_3)}, \\ \mu(\theta_2) &= \frac{e^{\varepsilon}\mu_0(\theta_2)}{\mu_0(\theta_1) + e^{\varepsilon}\mu_0(\theta_2) + e^{2\varepsilon}\mu_0(\theta_3)}, \\ \mu(\theta_3) &= \frac{e^{2\varepsilon}\mu_0(\theta_3)}{\mu_0(\theta_1) + e^{\varepsilon}\mu_0(\theta_2) + e^{2\varepsilon}\mu_0(\theta_3)}. \end{aligned}$$

When we consider ε-inferential privacy, since $\mathbf{G}^*$ is a complete graph, only 2-semi-chains

exist. Moreover, any partition of Θ can generate a pair of strongly connected 2-semi-chains.

Corollary 1. *A signal π is ε-inferential-privacy-preserving if and only if for almost every $\mu \in \text{supp}(\langle\pi\rangle)$, there exists a partition of Θ, $\{\Theta_1, \Theta_2\}$ such that*

$$\mu(\theta) = \begin{cases} \dfrac{e^{\varepsilon}\mu(\theta)}{e^{\varepsilon}\mu(\Theta_1) + \mu(\Theta_2)} & \text{if } \theta \in \Theta_1 \\ \dfrac{\mu(\theta)}{e^{\varepsilon}\mu(\Theta_1) + \mu(\Theta_2)} & \text{if } \theta \in \Theta_2 \end{cases}.$$

Corollary 1 provides an explicit characterization of all extreme posteriors in ε-inferential privacy. Xu and Zhao (2025) further shows that Corollary 1 continues to hold even when Θ is an infinite set.

3.2 Connection Between Semi-Chains and Spanning Trees

Translating extreme posteriors into strongly connected semi-chains is only the first step; we must also establish how to systematically enumerate all strongly connected semi-chains for a given graph.

Firstly, for a strongly connected 2-semi-chain, it can be constructed from a spanning tree of the initial graph $\mathbf{G}$. Given such a spanning tree, if one node is assigned to a particular level, then all its neighboring nodes are placed on the opposite level. Since a spanning tree contains no cycles, this assignment is well-defined and uniquely determines a strongly connected 2-semi-chain. Moreover, each spanning tree corresponds to two strongly connected 2-semi-chains, which are inverses of each other. Figure 2 demonstrates this relationship. Therefore, to generate all possible strongly connected 2-semi-chains, it suffices to enumerate all spanning trees of $\mathbf{G}$. Efficient algorithms for generating spanning trees are well established in the literature.

However, for any strongly connected L-semi-chain with $L \geq 3$, it cannot be directly generated from a spanning tree. The difficulty lies in satisfying the constraint that no edges exist between nodes belonging to non-adjacent (or identical) levels, which is precisely the issue illustrated in Figure 1.

To resolve this issue, we first introduce the operation *unfolding* and then demonstrate that any strongly connected L-semi-chain with $L \geq 3$ can be generated from a strongly connected 2-semi-chain through successive applications of unfolding.

Definition 8. *Let $C^L = (\Theta_l)_{l=1}^L$ be an L-semi-chain for some $L \geq 2$.*

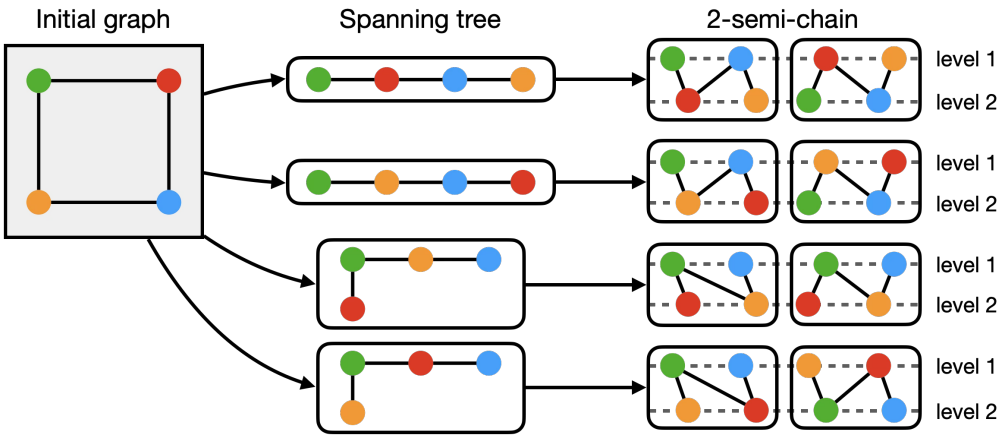


Figure 2: Generating Strongly Connected 2-Semi-Chains Through Spanning Trees

1. *An ordered partition* $(\Theta_2^1, \Theta_1, \Theta_2^2, (\Theta_l)_{l=3}^L)$ *is an upward unfolding of* C^L *if* $\{\Theta_2^1, \Theta_2^2\}$ *is a partition of* Θ_2 *such that*

$$(\theta_i, \theta_j) \notin \mathbf{G}, \quad \text{for all } \theta_i \in \Theta_2^1 \text{ and } \theta_j \in \Theta_2^2 \cup \Theta_3.$$

2. *An ordered partition* $((\Theta_l)_{l=1}^{L-2}, \Theta_{L-1}^1, \Theta_L, \Theta_{L-1}^2)$ *is a downward unfolding of* C^L *if* $\{\Theta_{L-1}^1, \Theta_{L-1}^2\}$ *is a partition of* Θ_{L-1} *such that*

$$(\theta_i, \theta_j) \notin \mathbf{G}, \quad \text{for all } \theta_i \in \Theta_{L-1}^2 \text{ and } \theta_j \in \Theta_{L-1}^1 \cup \Theta_L.$$

3. *An* L_+*-semi-chain* C^{L_+}*, for some* $L_+ > L$*, is obtained from* C^L *by successive upward (resp. downward) unfolding if there exists a sequence* $C^L, C^{L+1}, \ldots, C^{L_+}$ *such that each* $C^{L'}$ *is an upward (resp. downward) unfolding of* $C^{L'-1}$*, for all* $L' \in \{L+1, \ldots, L_+\}$.

Theorem 2. *An ordered partition* $(\Theta_l)_{l=1}^L$ *for some* $L \geq 3$ *is a (strongly connected)* L*-semi-chain if and only if it can be obtained from a (strongly connected)* 2*-semi-chain by successive upward unfolding (and symmetrically, by successive downward unfolding).*

In Figure 3, we give an example to show how to generate all semi-chain trough upward unfolding of 2-semi-chain. Consequently, all strongly connected semi-chains can be obtained by enumerating the spanning trees and applying the possible unfolding operations. However, directly generating 2-semi-chains through spanning trees may lead to duplication. As illustrated in Figure 2, different spanning trees can produce the same pair of 2-semi-chains. In the next section, we present more efficient methods to characterize 2-semi-chains within differential privacy.

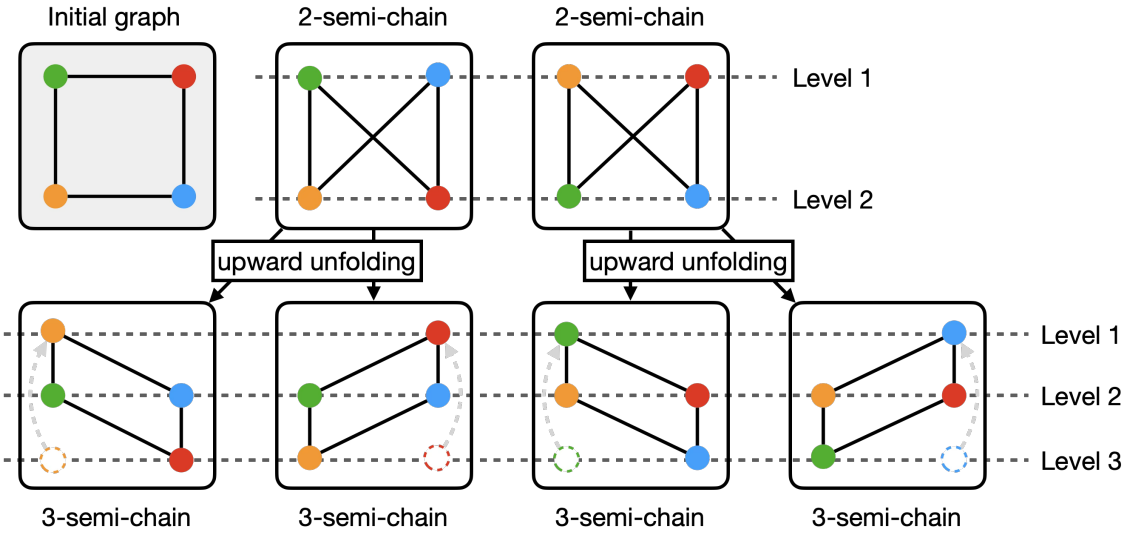


Figure 3: Illustration of Upward Unfolding

4 Differential Privacy

In this section, we focus on differential privacy (Definition 2). When $\Theta = \prod_{k=1}^{K} \Theta^{(k)}$ with $|\Theta^{(k)}| \geq 2$, we refer to it as the K-dimensional case. We first show that for any K-dimensional differential privacy setting, regardless of the number of possible values in each dimension, the number of levels in a semi-chain depends only on the dimensionality K.

Proposition 1. *For the differential graph* $\mathbf{G}_{\text{diff}}$ *in the* K*-dimensional case, a (strongly connected)* L*-semi-chain exists if and only if* $L \leq K + 1$.

Proposition 1 consists of two parts. First, the number of levels in a semi-chain cannot exceed $K + 1$. This is because, in an L-semi-chain, the shortest path connecting a node in the first level to a node in the last level has length at least $L - 1$, while in a K-dimensional differential graph, the shortest path between any two nodes has length at most K. Second, a $(K + 1)$-semi-chain does exist. A K-dimensional differential graph can be viewed as a combination of $|\Theta^{(k)}|$ copies of $(K - 1)$-dimensional differential graphs. Suppose $\hat{C}^K$ is the K-semi-chain in the $(K - 1)$-dimensional case. By duplicating $\hat{C}^K$ $|\Theta^{(k)}|$ times and shifting one copy upward by one level, we obtain a $(K+1)$-semi-chain $\hat{C}^{(K+1)}$ for the K-dimensional graph. Figure 4 illustrates this construction. Moreover, if $\hat{C}^K$ is strongly connected, then $\hat{C}^{(K+1)}$ remains strongly connected.

Proposition 1 is particularly useful when the dataset has low dimensionality, since in that case we do not need to consider overly complex semi-chains. In the two-dimensional

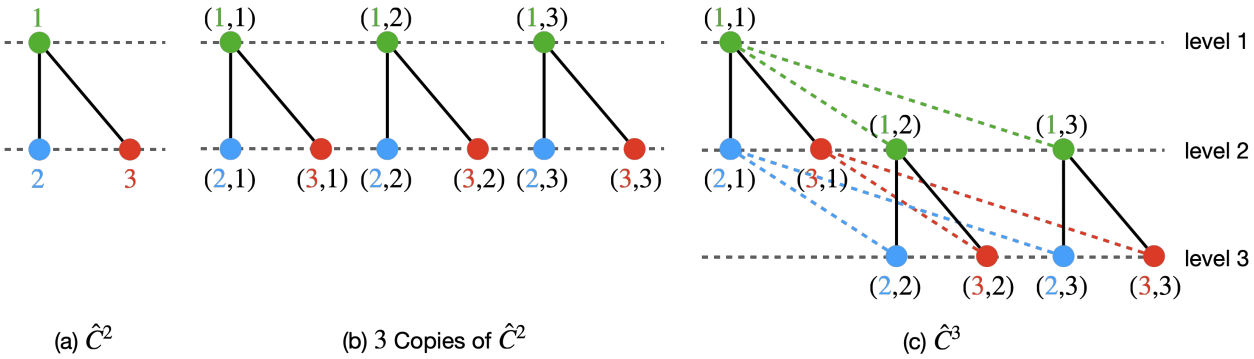


Figure 4: Illustration of Construction of $\hat{C}^3$ from $\hat{C}^2$

Note: In each panel, only the between-level edges are displayed. Panel (a) presents a 2-semi-chain $\hat{C}^2$ in the two-dimensional case where $\Theta = \{1, 2, 3\}$. To construct a 3-semi-chain in the three-dimensional case where $\Theta = \{1, 2, 3\}^2$, Panel (b) duplicates $\hat{C}^2$ three times, and Panel (c) shifts the first copy upward by one level. Since each $\hat{C}^2$ is connected, and after the shift, the nodes with the same value in the last dimension are linked with one another (shown as dashed lines in Panel (c)), the resulting $\hat{C}^3$ is strongly connected.

case, regardless of how many possible values each dimension takes, only 2-semi-chains exist. Therefore, to generate all extreme posteriors, the unfolding operation is unnecessary. However, when the dimensionality is high, even if each dimension contains only two possible values, more complex semi-chains may arise. In the next subsection, we will show that in this case, there exists only one pair of strongly connected 2-semi-chains.

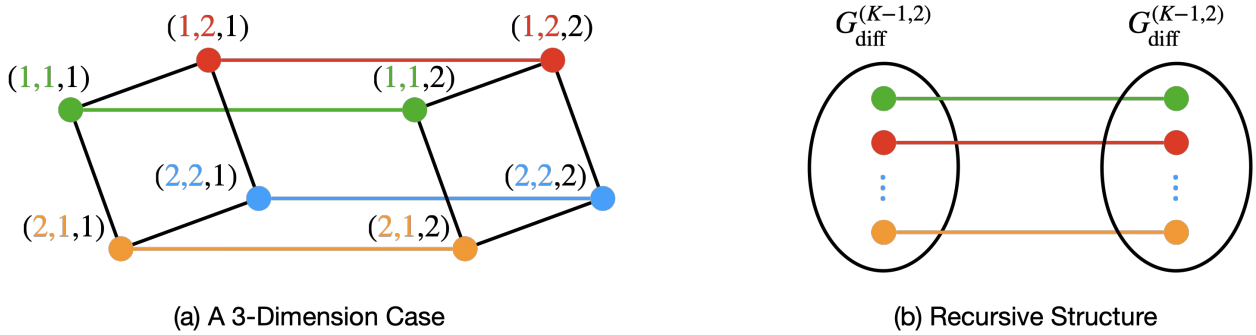
4.1 Binary Case

In this subsection, we focus on the binary case, where $\Theta = \{0, 1\}^K$. For convenience, we denote $\mathbf{G}_{\text{diff}}^{(K,2)}$ as the differential graph over $\{0, 1\}^K$.

In this setting, we can partition Θ according to the value of the last entry:

$$\Theta_{\theta^{(K)}=0} := \{\theta \in \Theta : \theta^{(K)} = 0\}, \quad \Theta_{\theta^{(K)}=1} := \{\theta \in \Theta : \theta^{(K)} = 1\}.$$

Then, we can define $\mathbf{G}_{\text{diff},a}^{(K,2)}$ as the subgraph of $\mathbf{G}_{\text{diff}}^{(K,2)}$ restricted to $\Theta_{\theta^{(K)}=a}$, for all $a \in \{0, 1\}$. Note that $\mathbf{G}_{\text{diff},a}^{(K,2)}$ has the same structure as $\mathbf{G}_{\text{diff}}^{(K-1,2)}$, for all $a \in \{1, 2\}$. Moreover, in $\mathbf{G}_{\text{diff}}^{(K,2)}$, aside from the edges in $\mathbf{G}_{\text{diff},0}^{(K,2)} \cup \mathbf{G}_{\text{diff},1}^{(K,2)}$, the remaining edges are between $\mathbf{G}_{\text{diff},0}^{(K,2)}$ and $\mathbf{G}_{\text{diff},1}^{(K,2)}$, connecting $(\theta^{(-K)}, 0)$ and $(\theta^{(-K)}, 1)$. Hence, $\mathbf{G}_{\text{diff}}^{(K,2)}$ can be constructed recursively by combining two copies of $\mathbf{G}_{\text{diff}}^{(K-1,2)}$ and adding edges between nodes that differ only in their last coordinate. Figure 5 illustrates this recursive structure.



(a) A 3-Dimension Case (b) Recursive Structure

Figure 5: Recursive Structure of the Differential Graph in the Binary Case

Let $C = (\Theta_l)_{l=1}^{L}$ be an L-semi-chain. The reverse semi-chain of C is the ordered partition $C^{\text{rev}} := (\Theta_{L-l+1})_{l=1}^{L}$, obtained by inverting the order of levels. Two semi-chains C and C' are said to be reverses of each other if $C' = C^{\text{rev}}$.

Proposition 2. *For any K-dimension differential graph in binary case, $\mathbf{G}_{\text{diff}}^{(K,2)}$, there exists a unique strongly connected 2-semi-chain up to reversal.*

When $K = 2$, the differential graph $\mathbf{G}_{\text{diff}}^{(2,2)}$ forms a cycle of four nodes. This case is illustrated in Figure 3, where we can easily observe that there exists a unique 2-semi-chain up to reversal. The key feature of this pair of 2-semi-chains is that all edges are between levels. Lemma 4 shows that this property guarantees the uniqueness of the 2-semi-chain up to reversal. Moreover, due to the recursive structure of $\mathbf{G}_{\text{diff}}^{(K,2)}$, this property is inherited from the K-dimensional case to the $(K+1)$-dimensional case.

Lemma 4. *For any graph on Θ, suppose there exists a strongly connected 2-semi-chain with no within-level edges. Then this 2-semi-chain is unique up to reversal.*

Proof. Let (A, B) be the strongly connected 2-semi-chain with no within-level edges, shown in Figure 6(a). Take any other 2-semi-chain (C, D), shown in Figure 6(b). Denote

$$A_1 := C \cap A, \quad B_1 := C \cap B, \quad A_2 := D \cap A, \quad B_2 := D \cap B.$$

Since (C, D) is different from (A, B), $A_1 \cup B_2 \neq \emptyset$, $A_2 \cup B_1 \neq \emptyset$.

Since (A, B) has no within-level edges, there are no edges between A_1 and A_2, nor between B_1 and B_2. Therefore, in the original graph, the edges from $A_1 \cup B_2$ to $A_2 \cup B_1$ are either be from A_1 to B_1 or from B_2 to A_2. But these edges are within-level with respect to (C, D). Hence, (C, D) cannot be strongly connected. Thus, the only strongly

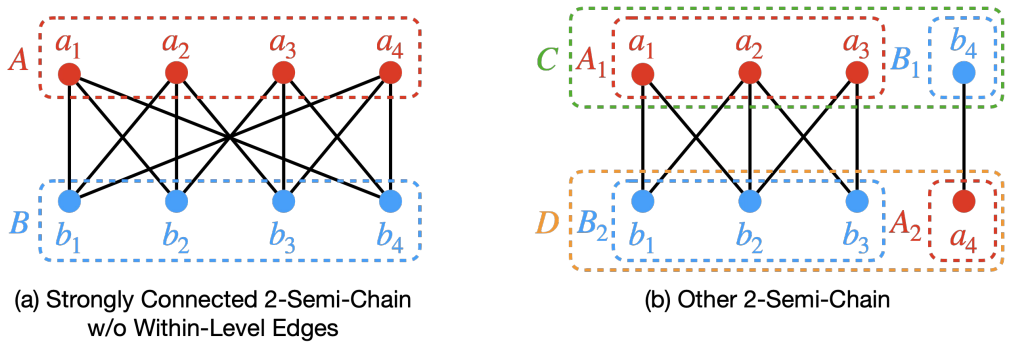


Figure 6: Illustration of Uniqueness in Lemma 4

connected 2-semi-chains are (A, B) and its reverse (B, A), i.e. the 2-semi-chain is unique up to reversal. □

The construction of this pair of 2-semi-chains is straightforward. Starting from any node assigned to one level, all its neighboring nodes are placed in the opposite level, and this process continues recursively. Proposition 2 then implies that, in the binary differential privacy case, all extreme posteriors can be generated solely through unfolding.

4.2 Two-Dimension Case

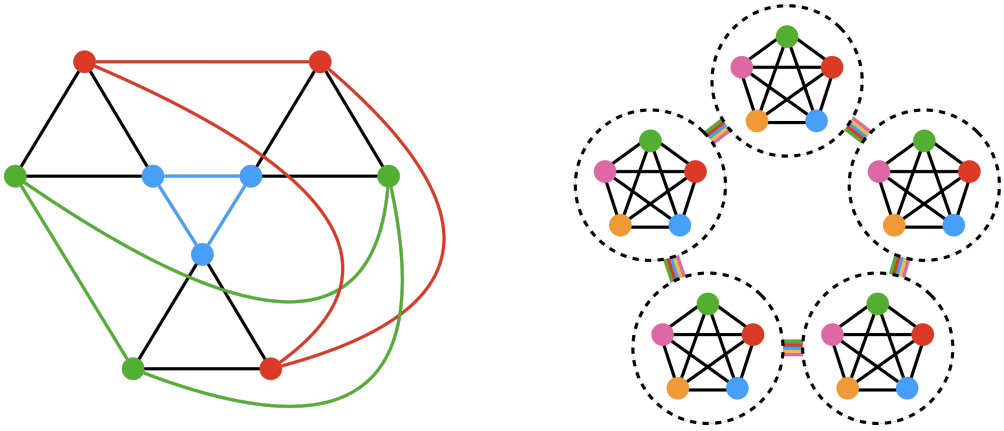
In the two-dimensional case, only 2-semi-chains exist, and they can be generated from spanning trees of the graph. However, different spanning trees may yield the same 2-semi-chain. In this subsection, we further analyze the structural properties of 2-semi-chains in the two-dimensional case and propose a more efficient algorithm to generate all strongly connected 2-semi-chains without duplication.

Consider a two-dimensional dataset $\Theta = X \times Y$, where $X = \{x_1, \ldots, x_{n_1}\}$ and $Y = \{y_1, \ldots, y_{n_2}\}$ for some $n_1, n_2 \geq 2$. For each $\hat{x} \in X$ and $\hat{y} \in Y$, define the equivalence classes For each $\hat{x} \in X$ and $\hat{y} \in Y$, define

$$[\hat{x}] := \{(\hat{x}, y) : y \in Y\}, \quad [\hat{y}] := \{(x, \hat{y}) : x \in X\},$$

as the equivalent classes. By the definition of differential privacy, for any pair $(\theta_i, \theta_j) \in \Theta^2$, $(\theta_i, \theta_j) \in E$ if and only if there exists $\hat{x} \in X$ or $\hat{y} \in Y$ such that $\theta_i, \theta_j \in [\hat{x}]$ or $[\hat{y}]$.

Let $\mathbf{G}^2_{\text{diff}}$ be the differential graph in two dimensions. If we partition the nodes according to $[x]$-equivalent classes, then: (i) for each $\hat{x} \in X$, the subgraph restricted to $[\hat{x}]$ is a complete graph; (ii) for each $\hat{y} \in Y$, the class $[\hat{y}]$ intersects every $[x]$-equivalent class at exactly one



(a) Differential Graph with $\Theta = \{1,2,3\}^2$ (a) Abstract Structure

Figure 7: Structure of the Differential Graph in the Two Dimension

point and these points are connected with each other. Figure 7 provides illustrative examples.

Given a 2-semi-chain of $\mathbf{G}^2_{\text{diff}}$, it can be partitioned into n_1 components according to the $[x]$-equivalence classes. Each $[x]$-equivalence class corresponds to a *division pattern* of Y, which divides the points in that class into two levels based on their y-coordinate values.

Let $\mathcal{D}$ denote the collection of division patterns of Y, which includes all ordered partitions of Y, as well as $(\emptyset, Y)$ and $(Y, \emptyset)$, representing the cases where all points in Y are assigned to a single level. For an equivalence class $[\hat{x}]$, we say that $[\hat{x}]$ in a 2-semi-chain follows the division pattern $\hat{d} = (Y_1, Y_2) \in \mathcal{D}$ if

$$[\hat{x}]_l = \{(\hat{x}, y) : y \in Y_l\}, \quad \text{for all } l \in \{1, 2\},$$

where $[\hat{x}]_l$ denotes the subset of $[\hat{x}]$ assigned to l-level in the 2-semi-chain.

Hence, to construct a 2-semi-chain: (i) select n_1 division patterns, and (ii) assign these division patterns to $[x]$-equivalence classes. For a division pattern $d = (Y_1, Y_2)$, if $Y_1 = \emptyset$ or $Y_2 = \emptyset$, we say d is undivided; otherwise, d is divided. To ensure that the 2-semi-chain is strongly connected, there exists at least one divided division pattern. Then, we can distinguish the following three categories of strongly connected 2-semi-chains (Figure 8): (Category I) no $[x]$-equivalent class is undivided; (Category II) exactly one level contains an undivided $[x]$-equivalent class; (Category III) both levels contain undivided $[x]$-equivalent classes.

Category I. Since the subgraph on each $[x]$-equivalent class is complete, when an $[x]$-equivalent class is divided, all inner nodes are connected with each other through between-

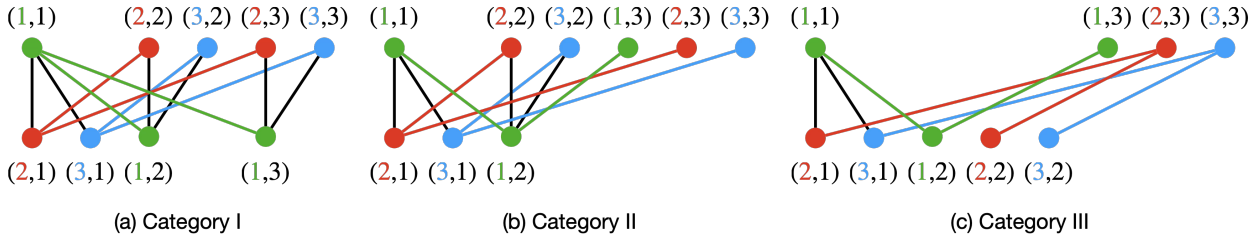


Figure 8: Illustration of the Three Categories of 2-Semi-Chains when $\Theta = \{1, 2, 3\}^2$

level edges. In category I, as long as all equivalent classes are not partitioned in the same way, the 2-semi-chain are strongly connected: If there are two equivalent classes $[\hat{x}_1]$ and $[\hat{x}_2]$ that follow different patterns, then from $[\hat{x}_1]$ to $[\hat{x}_2]$ there exists at least one pair of nodes with the same y connected by between-level edges. For the remaining $[x]$-equivalent classes, the division pattern must differ from both $[\hat{x}_1]$ and $[\hat{x}_2]$. Hence, the resulting 2-semi-chain is strongly connected.

Category II. Since only one level contains an undivided $[x]$-equivalent class, the nodes in this class are connected only via within-level edges, as illustrated in Figure 8(b). Therefore, to ensure that these nodes are connected by between-level edges, the opposite level must contain, for each $y \in Y$, at least one node in $[y]$.

Category III. There is one divided equivalent class $[\hat{x}_1]$, and the first and second levels contain undivided equivalent classes $[\hat{x}_2]$ and $[\hat{x}_3]$, respectively. As illustrated in Figure 8(c), each node in $[\hat{x}_1] \cup [\hat{x}_2] \cup [\hat{x}_3]$ is connected to the others through between-level edges. More importantly, for all $y \in Y$, each level contains at least one node in $[y]$. Hence, for the remaining $[x]$-equivalent classes, any division pattern can be chosen to maintain a strongly connected 2-semi-chain.

For a sequence of division patterns, $d = (d_{t_1}, \ldots, d_{t_{n_1}})$, if it can generate a strongly connected 2-semi-chain, we say d is strongly connected division sequence. To construct an algorithm to generate all strongly connected division sequence, at first, we need code a number of different division pattern,

$$\mathcal{D} = \{d_1, \ldots, d_{2^{n_2}-2}, d_{2^{n_2}-1}, d_{2^{n_2}}\},$$

where $d_{2^{n_2}-1} = (Y, \emptyset)$, $d_{2^{n_2}} = (\emptyset, Y)$ and others corresponds to different ordered partition of Y. We say that $d = (d_{t_1}, \ldots, d_{t_{n_1}})$ is increasing if $t_1 \leq t_2 \leq \ldots \leq t_{n_1}$. We need only to generate all increasing, strongly connected division sequences, then applying these division patterns to $[x]$-equivalent classes according to arbitrary permutation, we can generate all

strongly connected 2-semi-chains.

Proposition 3. *Algorithm 1 generates all increasing, strongly connected sequences of division patterns for two-dimensional differential privacy, ensuring no duplication.*

Algorithm 1: Construction of Increasing, Strongly Connected Division Sequences

Input: Integers n_1, n_2; set Y; and the collection of division patterns $\mathcal{D}$.
Output: Set $\mathcal{L}$ of all increasing, strongly connected division sequences
Initialize $t_0 \leftarrow 1$, $\mathcal{L} \leftarrow \emptyset$;
Function `Enumerate`$(z, t_{z-1}, (t_1, \ldots, t_{z-1}))$**:**
  for $t_z \in [t_{z-1}, 2^{n_2} - 2]$ **do**
    [Category I] **if** $z = n_1$ **and** $\left|\{t_1, \ldots, t_{n_1}\}\right| \geq 2$ **then**
      Add $(d_{t_1}, \ldots, d_{t_{n_1}})$ to $\mathcal{L}$;
    [Category II] **for** $l \in \{1, 2\}$ **do**
      if $Y \subseteq \bigcup_{z'=1}^{z} d_{t_{z'}}[l]$ *(for $d = (Y_1, Y_2)$, $d[l] = Y_l$)* **then**
        Add $(d_{t_1}, \ldots, d_{t_z}, \underbrace{d_{2^{n_2}+l-2}, \ldots, d_{2^{n_2}+l-2}}_{n_1 - z})$ to $\mathcal{L}$;
    [Category III] **if** $z \leq n_1 - 2$ **then**
      for $n' \in [1, n_1 - z - 1]$ **do**
        Add $(d_{t_1}, \ldots, d_{t_z}, \underbrace{d_{2^{n_2}-1}, \ldots, d_{2^{n_2}-1}}_{n'}, \underbrace{d_{2^{n_2}}, \ldots, d_{2^{n_2}}}_{n_1 - n' - z})$ to $\mathcal{L}$;
    if $z < n_1$ **then**
      `Enumerate`$(z + 1, t_z, (t_1, \ldots, t_z))$;

`Enumerate`$(1, t_0, ())$;

The logic of Algorithm 1 is as follows. Begin by choosing d_{t_1} from the set of division patterns, then append d_{t_2} with $t_2 \geq t_1$, and continue inductively with nondecreasing indices. Each time a new pattern is added, check whether the remaining positions can be filled by undivided patterns to produce a valid sequence in Category II or Category III; if so, output the corresponding sequence. Figure 9 gives an example of running the algorithm.

5 Discussion and Future Work

This paper characterizes the set of all feasible distributions subject to graph-based inferential privacy by establishing a connection between extreme posteriors and strongly connected semi-chains. We show that every extreme posterior can be generated by enumerating all

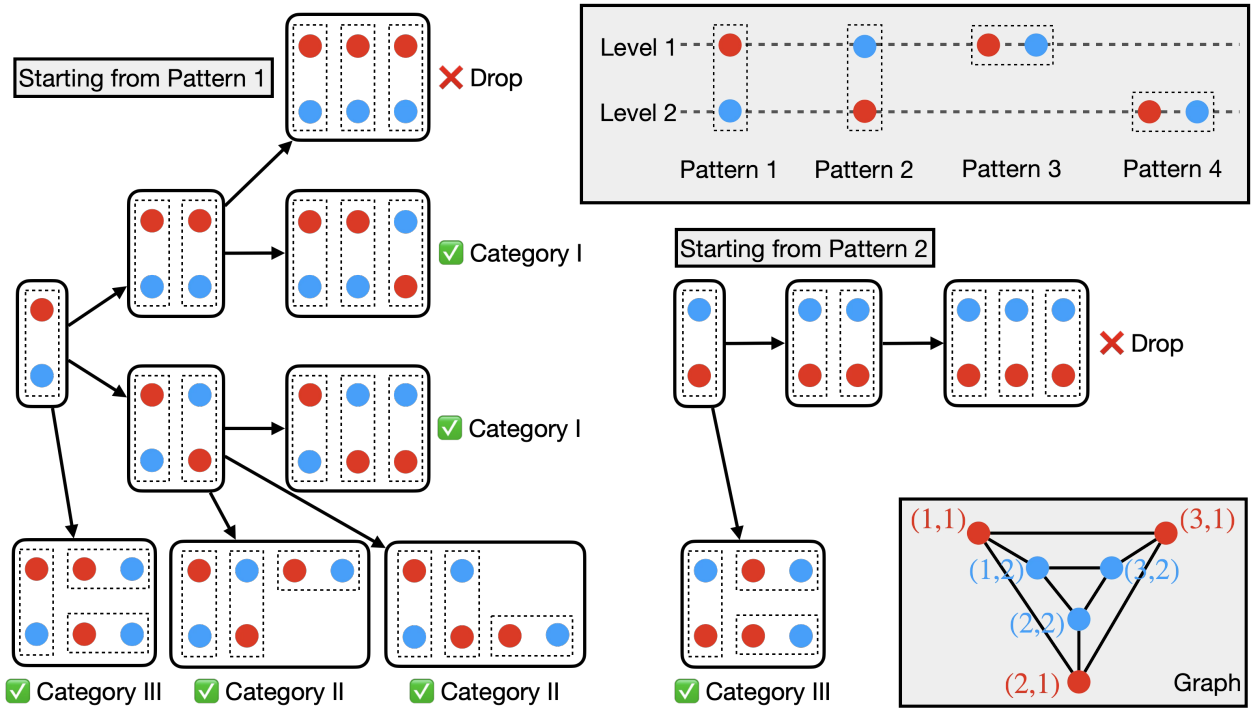


Figure 9: Illustration of Algorithm for $X = \{1, 2, 3\}$ and $Y = \{1, 2\}$

strongly connected 2-semi-chains and subsequently applying the unfolding operation. For differential privacy, when each dimension of the dataset is binary, there exists a unique strongly connected 2-semi-chain up to reversal. In the two-dimensional case, only 2-semi-chains exist, and we propose an efficient algorithm to generate all strongly connected 2-semi-chains without duplication.

When the underlying data structure becomes more complex, the number of extreme posteriors, and hence the number of Blackwell-undominated privacy-preserving signals, grows rapidly. Determining which of these signals attains the optimum in a specific decision problem remains an open question. Future research will explore applications of the theoretical framework developed in this paper to such problems, including optimal information design under privacy constraints.

In addition, the microfoundations of privacy concepts warrant further investigation. Understanding how individuals or institutions perceive and trade off privacy in strategic settings could guide the selection of appropriate graph structures. More broadly, extending the characterization of the Blackwell frontier to other privacy notions beyond graph-based or differential privacy remains an important avenue for future work.

References

Abowd, J. M. (2018). The us census bureau adopts differential privacy. In *Proceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining*, pp. 2867–2867.

Abowd, J. M. and I. M. Schmutte (2019, January). An Economic Analysis of Privacy Protection and Statistical Accuracy as Social Choices. *American Economic Review 109*(1), 171–202.

Bazaraa, M. S., J. J. Jarvis, and H. D. Sherali (2011). *Linear programming and network flows*. John Wiley & Sons.

Blackwell, D. (1953). Equivalent comparisons of experiments. *The annals of mathematical statistics*, 265–272.

Bogachev, V. I. (2007). *Measure theory*. Springer.

Concas, A., L. Reichel, G. Rodriguez, and Y. Zhang (2021). Chained graphs and some applications. *Applied Network Science 6*(1), 39.

Diestel, R. (2025). *Graph theory*, Volume 173. Springer Nature.

Dwork, C., F. McSherry, K. Nissim, and A. Smith (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of cryptography conference*, pp. 265–284. Springer.

Ghosh, A. and R. Kleinberg (2016). Inferential privacy guarantees for differentially private mechanisms. *arXiv preprint arXiv:1603.01508*.

He, K., F. Sandomirskiy, and O. Tamuz (2021). Private private information. *arXiv preprint arXiv:2112.14356*.

Kamenica, E. and M. Gentzkow (2011, October). Bayesian Persuasion. *American Economic Review 101*(6), 2590–2615.

Kifer, D. and A. Machanavajjhala (2014). Pufferfish: A framework for mathematical privacy definitions. *ACM Transactions on Database Systems (TODS) 39*(1), 1–36.

Pan, Y., Z. S. Wu, H. Xu, and S. Zheng (2025). Differentially private bayesian persuasion. In *Proceedings of the ACM on Web Conference 2025*, pp. 1425–1440.

Schmutte, I. M. and N. Yoder (2022). Information design for differential privacy. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, pp. 1142–1143.

Simon, B. (2011). *Convexity: an analytic viewpoint*, Volume 187. Cambridge University Press.

Strack, P. and K. H. Yang (2024). Privacy-preserving signals. *Econometrica 92*(6), 1907–1938.

Strack, P. and K. H. Yang (2025). Non-discriminatory personalized pricing. *arXiv preprint arXiv:2506.20925*.

Wang, S., S. Zheng, Z. Lin, G. Fanti, and Z. S. Wu (2025). Inferentially-private private information. In *Proceedings of the ACM on Web Conference 2025*, pp. 2579–2595.

Xu, Z. and W. Zhao (2025). Privacy-constrained signal. *Working Paper*.

A Proofs

Proof of Lemma 1

Let $\mathcal{M}$ be a compact convex subset of $\Delta(\Theta)$, where Θ with its σ-algebra is a standard Borel space. To ensure the analysis is non-trivial, we assume that $\mu_0 \in \mathcal{M} \setminus \operatorname{ext} \mathcal{M}$.

In this subsection, we prove Lemma 1 for this more general $\mathcal{M}$.

Proof of Lemma 1. We first show (ii): A signal $\pi \in \overline{\Pi}_{\mathcal{M}}$ if and only if $\langle \pi \rangle (\operatorname{ext} \mathcal{M}) = 1$. "If". Suppose there exists another $\pi' \in \Pi_{\mathcal{M}}$ such that $\pi \prec \pi'$, then there exists a nondegenerate dilation $K : \Delta(\Theta) \to \Delta(\Delta(\Theta))$ such that for almost every $\mu \in \operatorname{supp}(\langle \pi \rangle)$,

$$\mu = \int_{\Delta(\Theta)} \nu K(d\nu|\mu).$$

This means that for almost every $\mu \in \operatorname{supp}(\langle \pi \rangle)$, it can be expressed by linear combination of $\nu \in \operatorname{supp}(\langle \pi' \rangle)$. Since K is nondegenerate, there exists a positive measure subset $A \subseteq \operatorname{supp}(\langle \pi \rangle)$ such that $K(\mu|\mu) < 1$ for any $\mu \in A$. Hence, there is a positive measure subset A such that $\mu \notin \operatorname{ext} \mathcal{M}$ for any $\mu \in E$, which is contradicted with $\langle \pi \rangle (\operatorname{ext} \mathcal{M}) = 1$.

"Only if". We construct a dilation from $\mathcal{M}$ to $\Delta(\operatorname{ext}\mathcal{M})$. Since $\Theta \subseteq \mathbb{R}^n$, $\Delta(\Theta)$ embeds into a locally convex space and endowed with the topology of weak convergence is metrizable. $\mathcal{M}$ is a compact convex subset of $\Delta(\Theta)$, which is also metrizable. By Choquet's Theorem (Theorem 10.7, p.168, Simon (2011)), for any $\mu \in \mathcal{M}$, the set

$$\Gamma(\mu) := \left\{ P_\mu \in \Delta(\operatorname{ext}\mathcal{M}) : \mu = \int \nu dP_\mu(\nu) \right\}$$

is nonempty. Moreover, $\Gamma(\mu)$ is closed in the weak-* topology. Define the barycenter map $B : \Delta(\mathcal{M}) \to \mathcal{M}$ by $B(P_\mu) = \int \nu dP_\mu = \mu$. By Simon (2011), Theorem 9.1 (p.136), the map B is continuous. Consequently, for any open set $U \subseteq \Delta(\operatorname{ext}\mathcal{M})$, $\Gamma^{-1}(U) = \{\mu \in \mathcal{M} : B^{-1}(\mu) \cap U \neq \emptyset\} = B(U)$, which is an open set. Therefore, by the Kuratowski–Ryll-Nardzewski measurable selection theorem (Theorem 6.9.3, p.36, Vol. II, Bogachev (2007)), there exists a measurable selection $P^*_\mu : \mathcal{M} \to \Delta(\operatorname{ext}\mathcal{M})$ such that $\mu = \int \nu dP^*_\mu(\nu)$ Hence, the map $D : \mu \mapsto P^*_\mu$ defines a dilation. If $\langle \pi \rangle (\operatorname{ext}\mathcal{M}) \neq 1$, then D is nondegenerate, which implies $\pi \notin \overline{\Pi}_{\mathcal{M}}$.

For (i): A signal is ex post privacy-preserving if and only if it is Blackwell-dominated by some signal in $\overline{\Pi}_{\mathcal{M}}$. The "if" direction is immediate from the convexity of $\mathcal{M}$. The "only if" direction follows by the same argument used for the "only if" part of (ii). □

Proof of Theorem 1

Proof of Lemma 2. "Only if". By the definition, $\mu \in \mathcal{M}^\varepsilon_{\mathbf{G}}$ if

$$e^{-\varepsilon} \frac{\mu(\theta_j)}{\mu_0(\theta_j)} \leq \frac{\mu(\theta_i)}{\mu_0(\theta_i)} \leq e^{\varepsilon} \frac{\mu(\theta_j)}{\mu_0(\theta_j)}, \quad \forall (\theta_i, \theta_j) \in \mathbf{G}, \tag{6}$$

which can be expressed as

$$\frac{\mu(\theta_j)}{\mu_0(\theta_j)} = e^{w_{ij}\varepsilon} \frac{\mu(\theta_i)}{\mu_0(\theta_i)}, \text{ and } w_{ij} \in [-1, 1], \quad \forall (\theta_i, \theta_j) \in \mathbf{G}.$$

Since $\mathbf{G}$ is connected, for any $(\theta_{j_1}, \theta_{j_r}) \in \Theta^2$, there is a path in $\mathbf{G}$, $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_r}$, such that

$$\frac{\mu(\theta_{j_1})}{\mu_0(\theta_{j_1})} = e^{\sum_{r'=1}^{r-1} w_{j_{r'} j_{r'+1}} \varepsilon} \frac{\mu(\theta_{j_r})}{\mu_0(\theta_{j_r})}.$$

If there is a $\theta_i \in \Theta$ such that $\mu(\theta_i) = 0$ then $\mu(\theta_j) = 0$ for all $\theta_j \in \Theta$ which contradicts that $\mu \in \Delta(\Theta)$. Therefore, $\delta_j = \ln \mu(\theta_j) - \ln \mu_0(\theta_j)$ is well-defined for all $\theta_j \in \Theta$. $\mu \in \mathcal{M}^\varepsilon_{\mathbf{G}}$ implies

(2) is valid and (3) holds. Moreover, it is obvious that (4) $w_{ij}\varepsilon = \delta_i - \delta_j = -w_{ji}\varepsilon$ and (5) $w_{j_1 j_r}\varepsilon = \delta_{j_r} - \delta_{j_1} = \sum_{r'=1}^{r-1}(\delta_{j_{r'+1}} - \delta_{j_{r'}}) = \sum_{r'=1}^{r-1} w_{j_{r'} j_{r'+1}}\varepsilon$.

"If". Suppose $\mathbf{W}$ satisfies these conditions. Consider a sequence $w_{j_1 j_2}, w_{j_2 j_3}, \ldots, w_{j_{J-1} j_J}$. The following J independent linear constraints determine a unique $\hat{\mu}$:

$$\frac{\mu(\theta_{j_{r+1}})}{\mu_0(\theta_{j_{r+1}})} - e^{w_{j_r j_{r+1}}\varepsilon}\frac{\mu(\theta_{j_r})}{\mu_0(\theta_{j_r})} = 0, \quad \forall r \in \{1, \ldots, J-1\}, \tag{7}$$

$$\sum_{j=1}^{N} \mu(\theta_j) = 1, \tag{8}$$

If there exists $\theta_j \in \Theta$ such that $\hat{\mu}(\theta_j) \leq 0$, then (7) will induces that $\hat{\mu}(\theta) \leq 0$ for all $\theta \in \Theta$, which contradicts with (8). Thus, (7) can be rewritten as (2) and $\hat{\mu} \in \Delta(\Theta)$. Denote $\hat{\mathbf{W}}$ be the matrix induce by $\hat{\mu}$ which satisfies (4), (5) and $\hat{w}_{j_r j_{r+1}} = w_{j_r j_{r+1}}$ for all $r \in \{1, \ldots, J-1\}$. Given the values of $w_{j_1 j_2}, w_{j_2 j_3}, \ldots, w_{j_{J-1} j_J}$, all other entries of $\mathbf{W}$ are endogenously and uniquely determined by (4) and (5). Therefore, $\hat{\mathbf{W}} = \mathbf{W}$, then $\mathbf{W}$ can be obtained by $\hat{\mu}$. Moreover, since $\hat{\mathbf{W}} = \mathbf{W}$ satisfies (3), $\hat{\mu} \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$. □

Proof of Lemma 3. By the definition, $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ if and only if (6) (which induces $\mu(\theta_j) > 0$ for all $\theta_j \in \Theta$) and (8). Since $\mu \in \mathbb{R}^J$, $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ is an extreme point of $\mathcal{M}^{\varepsilon}_{\mathbf{G}}$ if and only if a total of J constraints are binding in (6) and (8) (Theorem 3.1, pp.102, Bazaraa et al. (2011)). Because (8) is always binding, it remains to identify $J-1$ binding constraints from (6). For each pair of constraints in (6), $e^{-\varepsilon}\frac{\mu(\theta_j)}{\mu_0(\theta_j)} \leq \frac{\mu(\theta_i)}{\mu_0(\theta_i)} \leq e^{\varepsilon}\frac{\mu(\theta_j)}{\mu_0(\theta_j)}$, it corresponds to $w_{ij} = -w_{ji} \in [-1, 1]$ and the two inequalities cannot be binding simultaneously. Hence, finding $J-1$ independent binding constraints in (6) is equivalent to identifying $J-1$ independent $w_{ij} = \pm 1$ in $\mathbf{G}$.

Now, we show that identifying $J-1$ independent $w_{ij} = \pm 1$ for some $(\theta_i, \theta_j) \in \mathbf{G}$ is equivalent to find a spanning tree $\mathbf{T}$ of $\mathbf{G}$ such that $w_{ij} = \pm 1$ for every $(\theta_i, \theta_j) \in \mathbf{T}$.

"If". For a tree $\mathbf{T}$, by Lemma 2, the collection of $\mathcal{W}_{\mathbf{T}} := \{w_{ij} : (\theta_i, \theta_j) \in \mathbf{T} \text{ and } i < j\}$ is not independent if and only there exists some $\hat{w} \in \mathcal{W}_{\mathbf{T}}$ that can be expressed as a linear combination of the others through the equations in (4) and (5). By construction of $\mathcal{W}_{\mathbf{T}}$, the constraints in (4) do not apply. Moreover, since $\mathbf{T}$ is acyclic, (5) does not apply either. Thus, $\mathcal{W}_{\mathbf{T}}$ is independent. Because $\mathbf{T}$ has $J-1$ edges, we have $|\mathcal{W}_{\mathbf{T}}| = J-1$. Hence, $\mathcal{W}_{\mathbf{T}}$ identifies $J-1$ independent constraints $w_{ij} = \pm 1$ for $(\theta_i, \theta_j) \in \mathbf{T}$.

"Only if". Suppose no such spanning tree exists. Assume there are $J-1$ pairs of constraints $w_{ij} = \pm 1 = -w_{ji}$ for some $(\theta_i, \theta_j) \in \mathbf{G}$; otherwise, it is trivial. Consider any subgraph with $J-1$ edges such that $w_{ij} = \pm 1$ for every edge. Such a subgraph necessarily

contains a cycle. By (5), within this cycle one weight can be written as a linear combination of the others. Hence, the cycle reduces the number of independent constraints, so the subgraph yields at most $J-2$ independent weights. □

Lemma 5. *Suppose* $\mathbf{W}$ *corresponds to some* $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$. *If* $\mu \in \operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}$, *then* $w_{ij} \in \{\pm 1, 0\}$ *for every* $(\theta_i, \theta_j) \in \mathbf{G}$.

Proof of Lemma 5. Suppose $\mu \in \operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}$, then according to Lemma 3, there exists a spanning tree $\mathbf{T}$ such that $w_{ij} = \pm 1$ for all $(\theta_i, \theta_j) \in \mathbf{T}$. For any other $(\theta_{i'}, \theta_{j'}) \in \mathbf{G} \setminus \mathbf{T}$, there exists a path from $\theta_{i'}$ to $\theta_{j'}$ in $\mathbf{T}$. Thus, $w_{i'j'}$ is determined by the sum of the weights along this path. Since for any $(\theta_i, \theta_j) \in \mathbf{T}$, $w_{ij} = \pm 1$, then $w_{i'j'} \in \{\pm 1, 0\}$. □

Lemma 6. *For any* L*-semi-chain* $C = (\Theta_l)_{l=1}^{L}$, $L \geq 2$, *the matrix* $\mathbf{W}$ *satisfying*

$$w_{ij} = \begin{cases} 1 & \text{if there exists } l \in \{1, \ldots, L-1\} \text{ such that } \theta_i \in \Theta_l, \theta_j \in \Theta_{l+1} \\ 0 & \text{if there exists } l \in \{1, \ldots, L\} \text{ such that } \theta_i, \theta_j \in \Theta_l \end{cases}.$$

can correspond to some $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$.

Proof of Lemma 6. The remaining entries of $\mathbf{W}$ are determined by (4) and (5). Since constraints (3) and (4) are automatically satisfied, it remains to show that constraint (5) is also satisfied. In particular, for any cycle in the graph $\mathbf{G}$, $\theta_{j_1}, \theta_{j_2}, \ldots, \theta_{j_r}, \theta_{j_{r+1}=\theta_{j_1}}$, $\sum_{r'=1}^{r} w_{j'_r j_{r'+1}} = 0$.

Consider an arbitrary cycle. Its edges can be divided into two types: (i) Within-level edges. The sum of their weights is always zero by construction. (ii) Between-level edges. These edges induce a cycle in the partition graph, where partitions $\{\Theta_l\}_{l=1}^{L}$ are vertices and a pair of vertices are linked if and only if they are adjacent levels. Thus, the partition graph is a line from top to bottom. To form a cycle in this line graph, every downward step must eventually be matched by a upward step. Since the weight w of an edge from l-th level Θ_l to $(l-1)$-th level Θ_{l+1} is the negative of the weight of the reverse edge (from $(l-1)$-th level to l-th level), the total weight of edges between levels cancels out to zero. Accordingly, in any cycle, the total weight is 0. □

Proof of Theorem 1. "If". Due to Lemma 6, such $\mathbf{W}$ can correspond to some $\mu \in \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ and therefore satisfy (3), (4), (5). The strong connectedness of C implies that the subgraph post deleting all within-level edges is connected. Note that if θ_i and θ_j are linked in the subgraph, then $w_{ij} = \pm 1$. The finite connected subgraph always has at least one spanning tree $\mathbf{T}$

(Theorem 1.5.1, pp.14, Diestel 2025), such that any pair $(\theta_i, \theta_j) \in \mathbf{T}$, $w_{ij} = \pm 1$. Lemma 3 implies that $\mu \in \operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}$.

"Only if". Suppose $\mu \in \operatorname{ext} \mathcal{M}^{\varepsilon}_{\mathbf{G}}$ and let $\mathbf{W}$ be the corresponding matrix, satisfying (3), (4), (5). By Lemma 3, there exists a spanning tree $\mathbf{T}$ such that $w_{ij} = \pm 1$ whenever $(\theta_i, \theta_j) \in \mathbf{T}$. Begin with an arbitrary root node θ_i and place it in some level. For each neighbor $\theta_j \in N(\theta_i)$, if $w_{ij} = 1$ then assign θ_j to the level immediately above θ_1; if $w_{ij} = -1$, assign θ_j to the level immediately below θ_i. Proceed inductively: for any newly assigned node, allocate its neighbors according to the same rule. Since T is a spanning tree, each node is assigned exactly once, and this procedure yields a well-defined ordered partition $(\Theta_l)_{l=1}^{L}$.

Now consider any $\theta_i \in \Theta_l$ and $\theta_j \in \Theta_{l'}$. There is a path $(\theta_{i_k})_0^n$ in $\mathbf{T}$, with $\theta_{i_0} = \theta_i$, $\theta_{i_n} = \theta_j$. Regarding the path, it is required that, if $\theta_{i_k} \in \Theta_l$, then $\theta_{i_{k+1}} \in \Theta_{l-1} \cup \Theta_{l+1}$, and $w_{i_k i_{k+1}} = 1(-1)$ if $\theta_{i_{k+1}} \in \Theta_{l+1}(\theta_{i_{k+1}} \in \Theta_{l-1})$. Constraint (5) then implies that

$$w_{ij} = w_{i_0 i_n} = \sum_{k=0}^{n-1} w_{i_k i_{k+1}} = l' - l$$

If $l = l'$, then $w_{ij} = 0$, and if $l' - l = 1$, then $w_{ij} = 1$. Therefore, $\mathbf{W}$ satisfies the conditions stated in the Theorem. Besides, if $|l - l'| \geq 2$, then $(\theta_i, \theta_j) \notin \mathbf{G}$, otherwise constraint (3) will be violated. Therefore, the ordered partition $(\Theta_l)_{l=1}^{L}$ forms a semi-chain. Finally, since the spanning tree is contained in the subgraph post deleting links within same partitions, the semi-chain is strongly connected.

□

Proof of Theorem 2

Definition 9. *Let $C^L = (\Theta_l)_{l=1}^{L}$ be an L-semi-chain for some $L \geq 3$.*

1. *The ordered partition $(\Theta_2, \Theta_1 \cup \Theta_3, (\Theta_l)_{i=4}^{L})$ is called an downward folding of C^L.*
2. *The ordered partition $((\Theta_l)_{l=1}^{L-3}, \Theta_{L-2} \cup \Theta_L, \Theta_{L-1})$ is called an upward folding of C^L.*
3. *The L_--semi-chain C^{L_-}, for some $2 \leq L_- < L$, is obtained from C^L by successive downward (resp. upward) folding if there exists a sequence $C^{L_-}, C^{L_-+1}, \ldots, C^L$ such that each $C^{L'}$ is an downward (resp. upward) folding of $C^{L'+1}$, for all $L' \in \{L_-, \ldots, L-1\}$.*

It is clear that the downward (or upward) folding of an L-semi-chain with $L \geq 3$ is a semi-chain, and this folding is unique.

Lemma 7. *Given an L-semi-chain C^L for some $L \geq 3$, C^{L-1} is obtained from C^L by downward (or upward) folding. C^L is strongly connected if and only if C^{L-1} is strongly connected.*

Proof of Lemma 7. W.l.o.g., we restrict attention to downward folding. Let $C^L = (\Theta_l)_{l=1}^L$, then $C^{L-1} = (\Theta_2, \Theta_1 \cup \Theta_3, (\Theta_l)_{l=4}^L)$. Suppose C^L is strongly connected. After folding Θ_1 into Θ_3, the only modification is that the signs of the edges between Θ_1 and Θ_2 are reversed. Importantly, no between-level edge is converted into a within-level edge. Hence, every path that certifies strong connectivity in C^L remains valid in C^{L-1}. Therefore, C^{L-1} is strongly connected. Conversely, suppose C^{L-1} is strongly connected. When unfolding by placing Θ_1 back into the first level, by the definition of C^L, Θ_1 is adjacent only to Θ_2 and has no edges to $\Theta_3 \cup \Theta_4$. Thus, reinstating Θ_1 does not create any within-level edges and preserves all existing between-level edges. Consequently, strong connectivity of C^{L-1} implies strong connectivity of C^L. □

Lemma 8. *C^{L+1} is an upward (resp. downward) unfolding of C^L if and only if C^L is the downward (resp. upward) folding of C^{L+1}.*

Proof of Lemma 8. Let $C^{L+1} = (\Theta_l)_{l=1}^L$ and $C^L = (\hat{\Theta}_l)_{l=1}^L$. Suppose C^{L+1} is an upward unfolding of C^L. Then there exists a partition $\{\hat{\Theta}_2^1, \hat{\Theta}_2^2\}$ such that $\Theta_1 = \hat{\Theta}_2^1$ and $\Theta_3 = \hat{\Theta}_2^2$. Then, by merging Θ_1 back into Θ_3, we recover C^L. Conversely, suppose C^L is obtained from C^{L+1} by downward folding. Then $\hat{\Theta}_2 = \Theta_1 \cup \Theta_3$. By the definition of C^{L+1}, there is no edge from Θ_1 to $\Theta_3 \cup (\hat{\Theta}_3 = \Theta_4)$. Hence, C^{L+1} can be obtained from C^L by dividing $\hat{\Theta}_2$ into Θ_1 and Θ_3, and then assigning Θ_1 as the new first level. □

Proof of Theorem 2. Through recursion, it is easy to show that an ordered partition $(\Theta_l)_{l=1}^L$ obtained from a 2-semi-chain by successive upward unfolding is a semi-chain. For any C^L, there exists a sequence of decreasing-level semi-chain $C^{L-1}, C^{L-2}, \ldots, C^2$, where each $C^{L'}$ is obtained from $C^{L'+1}$ by downward folding. By Lemma 8, it follows that C^L can be obtained by successive upward unfolding starting from C^2. Moreover, by Lemma 7, C^L is strongly connected if and only if the C^2 from which it is generated is strongly connected. □

Proof of Proposition 1

Lemma 9. *For the differential graph* $\mathbf{G}_{\text{diff}}$ *in* K*-dimension case, there exists a strongly connected* $(K+1)$*-semi-chain.*

Proof of Lemma 9. The proof is based on mathematical induction and constructive methods. Some notations are introduced beforehand. Within this proof, denote $\Theta^{[m]} := \prod_{k=1}^{m} \Theta^{(k)}$ the set of m-dimensional states, with a typical element $\theta^{[m]} = (\theta^{(l)})_{l=1}^{m}$.

Case $K = 1$. Clearly, choosing any single point in Θ as the first level and placing the remaining points in the second level yields a 2-semi-chain. Moreover, since when $K = 1$, $\mathbf{G}_{\text{diff}}$ is complete, this 2-semi-chain is strongly connected.

Suppose for $K = m - 1$, there exists a strongly connected m-semi-chain, denoted by $C^m = (\Theta_l^{[m-1]})_{l=1}^{m}$. For $K = m$, fix $\hat{\theta}^{(m)} \in \Theta^{(m)}$ and construct $C^{m+1} = (\Theta_l^{[m]})_{l=1}^{m+1}$ as follows:

$$\Theta_1^{[m]} = \left\{ (\theta^{[m-1]}, \hat{\theta}^{(m)}) : \theta^{[m-1]} \in \Theta_1^{[m-1]} \right\},$$

$$\Theta_l^{[m]} = \left\{ (\theta^{[m-1]}, \hat{\theta}^{(m)}) : \theta^{[m-1]} \in \Theta_l^{[m-1]} \right\} \bigcup \left\{ (\theta^{[m-1]}, \theta^{(m)}) : \theta^{[m-1]} \in \Theta_{l-1}^{[m-1]}, \theta^{(m)} \neq \hat{\theta}^{(m)} \right\}, \forall l \in \{2, \cdots, m\}$$

$$\Theta_{m+1}^{[m]} = \left\{ (\theta^{[m-1]}, \theta^{(m)}) : \theta^{[m-1]} \in \Theta_m^{[m-1]}, \theta^{(m)} \neq \hat{\theta}^{(m)} \right\}$$

Fix some $\tilde{\theta}^{(m)} \in \Theta^{(m)}$, denote

$$C_{\tilde{\theta}^{(m)}}^{m+1} := \left\{ \Theta_l^{[m]} \cap \{\theta^{[m]} : \theta^{(m)} = \tilde{\theta}^{(m)}\} \right\}$$

the ordered partition restricting to nodes with m-th coordinate $\tilde{\theta}^{(m)}$. By construction, we have that

$$\begin{cases} (\theta^{[m-1]}, \theta^{(m)}) \in \Theta_{l+1}^{[m]} & \iff \theta^{[m-1]} \in \Theta_l^{[m-1]} \quad \text{if } \theta^{(m)} \neq \hat{\theta}^{(m)} \\ (\theta^{[m-1]}, \hat{\theta}^{(m)}) \in \Theta_l^{[m]} & \iff \theta^{[m-1]} \in \Theta_l^{[m-1]} \end{cases}$$

In this sense, $C_{\tilde{\theta}^{(m)}}^{m+1}$ (for the subgraph of G, formed by nodes with m-th coordinate $\tilde{\theta}^{(m)}$) is of same structure as C^m, for any $\tilde{\theta}^{(m)} \in \Theta^{(m)}$. Therefore, the edge between a pair with fixed m-th coordinate is either within same level or between adjacent levels, since C^m is a semi-chain. On the other hand, the edge between a pair with different m-th coordinates (and therefore same first $m-1$ coordinate) is either within same level (if both m-th coordinates differs from $\hat{\theta}^{(m)}$) or between adjacent levels (if one of the m-th coordinates is $\hat{\theta}^{(m)}$). Accordingly, the ordered partition C^{m+1} is an $(m+1)$-semi-chain.

It remains to prove the strong connectivity of C^{m+1}. On one hand, $C_{\tilde{\theta}^{(m)}}^{m+1}$ inherits the

strong connectivity from C^m. On the other hand, there is an edge between $(\theta^{[m-1]}, \theta^{(m)})$ and $(\theta^{[m-1]}, \theta^{\hat{(m)}})$, which is between adjacent levels. Accordingly, C^{m+1} is strongly connected.

□

Proof of Proposition 1. "If". By Lemma 9, a strongly connected $(K+1)$-semi-chain exists. By Lemma 7, successive downward folding of this strongly connected $(K+1)$-semi-chain generates a strongly connected L-semi-chain for any $L \leq K$.

"Only if". Suppose there exists an L-semi-chain. Then the shortest path connecting a node in the first level to a node in the last level must have length at least $L-1$. However, for any two points in Θ, they can differ in at most K dimensions, so, by the definition of $\mathbf{G}_{\text{diff}}$, the shortest path connecting them has length at most K. Therefore, the maximum possible length of a semi-chain is $K+1$. □

Proof of Proposition 2

Lemma 10. *Suppose $\mathbf{G}_{\text{diff}}^{(K-1,2)}$ has a strongly connected 2-semi-chain (A, B) in which there is no within-level edges. Then, $((A,0) \cup (B,1), (B,0) \cup (A,1))$ is a 2-semi-chain with no within-level edges of $\mathbf{G}_{\text{diff}}^{(K,2)}$, where $(A,0) := \{(\theta^{(-K)}, 0) : \theta^{(-K)} \in A\}$ and similarly for others.*

Proof. First, since (A, B) is an ordered partition of $\{0,1\}^{n-1}$, $((A,0) \cup (B,1), (B,0) \cup (A,1))$ is an ordered partition of $\{0,1\}^n$. Moreover, any 2-ordered partition is 2-semi-chain.

Strong connectivity: By the strong connectivity of (A, B), any pair of nodes in $(A,0) \cup (B,0)$ is connected by a between-level path (i.e., a path along within-level edges), and the same holds for $(A,1) \cup (B,1)$. For any $(\theta_i^{(-K)}, 0) \in (A,0)$ and $(\theta_j^{(-K)}, 1) \in (A,1) \cup (B,1)$, there is a within-level path from $(\theta_i^{(-K)}, 0)$ to $(\theta_i^{(-K)}, 1)$, and since $(\theta_i^{(-K)}, 1) \in (A,1)$, it has a between-level path to $(\theta_j^{(-K)}, 1)$. Hence $(\theta_i^{(-K)}, 0)$ and $(\theta_j^{(-K)}, 1)$ are connected via a path consisting entirely of between-level edges. Thus, every node in $(A,0)$ is connected via between-level edges with any other node, and by the same reasoning the result holds for $(A,1)$, $(B,0)$ and $(B,1)$. Consequently, $((A,0) \cup (B,1), (B,0) \cup (A,1))$ is a strongly connected.

No within-level edge: $\mathbf{G}_{\text{diff}}^{(K,2)}$ can be divided into two $\mathbf{G}_{\text{diff}}^{(K-1,2)}$. The edges of $\mathbf{G}_{\text{diff}}^{(K,2)}$ within the same $\mathbf{G}_{\text{diff}}^{(K-1,2)}$ are between-level and other edges connecting $\theta = (\theta^{(-K)}, 0)$ and $\theta' = (\theta^{(-K)}, 1)$ are also between-level, since $(A,0)$, $(B,1)$ are in the first level while $(A,1)$ and $(B,0)$ are in the second level. □

Proof of Proposition 2. When $K = 1$, there are only two points in $\Theta = \{0, 1\}$. Hence, the unique (up to reversal) strongly connected 2-semi-chain is $(\{0\}, \{1\})$ which satisfies the assumption in Lemma 4. Hence, since the transitivity in Lemma 10 and uniqueness in Lemma 4, for any K, there is a unique strongly connected 2-semi-chain. □

Proof of Proposition 3

Lemma 11. *For any strongly connected 2-semi-chain of $\mathbf{G}^2_{\text{diff}}$, there exists at least one $\hat{x} \in X$ such that $[\hat{x}]$ is divided.*

Proof of Lemma 11. Suppose for any $\hat{x} \in X$, every $\theta \in [\hat{x}]$ is in the same level. Then, given $\hat{x}$, for any $y, y' \in Y$, edge $((\hat{x}, y), (\hat{x}, y'))$ is within-level. Suppose there is a path between (x_1, y_1) and (x_2, y_2), then there must exist $x' \in X$ such that edge $((x', y_1), (x', y_2))$ is in this path. Therefore, there does not exist a path from (x_1, y_1) to (x_2, y_2) without a within-level edge. It contradicts with strong connectivity. □

Lemma 12. *After allocating any number of divided $[x]$, the induced sub-2-semi-chain is strongly connected if and only if there is at least two $[x]$, the division pattern are different.*

Proof. "Only if". Suppose there is only one division pattern, then the edges in the same $[\hat{y}]$ are within-level. Hence $(x_1, \hat{y})$ and $(x_2, \hat{y})$ are not connected by a between-level path.

"If". Assume $[x_1]$ and $[x_2]$ have different division methods. First, since $[x_1]$ and $[x_2]$ are divided and subgraph on the them are complete, the nodes within the same equivalent class are connected by a between-level path. Second, since the division methods are different, there is a $\hat{y} \in Y$ such that $(x_1, \hat{y})$ and $(x_2, \hat{y})$ are in the different level. Then, $(x_1, \hat{y})$ and $(x_2, \hat{y})$ are connected by a between-level path. Therefore, the sub-2-semi-chain restricted on $[x_1]$ and $[x_2]$ are strongly connected. Furthermore, for the sequential divided $[x_l]$, its division method must be different with one of $[x_1]$ and $[x_2]$. Since the same reason, the sub-2-semi-chain restricted on these divided $[x]$ are strongly connected. □

Lemma 13. *A 2-semi-chain with m divided $[x]$-equivalent classes and $n_1 - m$ undivided ones in the first (resp. second) level is strongly connected if and only if, after allocating the m divided $[x]$, for every $y \in Y$, there exists $\hat{\theta}_y$ in the second (resp. first) level such that $\hat{\theta}_y \in [y]$, and all these nodes $\{\hat{\theta}_y\}_{y \in Y}$ are connected by a between-level path.*

Proof of Lemma 13. "If". Suppose after allocating all divided $[x]$, in second level, for each $\hat{y} \in Y$, there is $\theta_{\hat{y}} \in [\hat{y}]$. Then, there are at least two divided $[x]$ with different division pattern

and according to Lemma 12, these divided $[x]$ are strongly connected. Furthermore, since for each point in the rest undivided $[x]$ in the first level, it connects with the corresponding $\hat{\theta}_y$ in the second level, the 2-semi-chain is strongly connected.

"Only if". Suppose in the second level, there is no point in $[\hat{y}]$. Then, for $[x_{m+1}]$ which is totally allocated in the first level, $(x_{m+1}, \hat{y})$ only have edges with nodes in $[x_{m+1}] \cup [\hat{y}]$ which are all within the first level. Hence, 2-semi-chain is not strongly connected. □

Lemma 14. *Any 2-semi-chain contains one divided $[\hat{x}_1]$, one undivided $[\hat{x}_2]$ in the first level, one undivided $[\hat{x}_3]$ in the second level, then it is strongly connected.*

Proof of Lemma 14. Since $[\hat{x}_1]$ is divided and subgraph on $[\hat{x}_1]$ is complete, all nodes in $[\hat{x}_1]$ are connected by a between-level path. Let $([\hat{x}_1]_1, [\hat{x}_1]_2)$ be the partition of $[\hat{x}_1]$. Denote $Y_1 := \{y \in Y : (\hat{x}_1, y) \in [\hat{x}_1]_1\}$ and $Y_2 := \{y \in Y : (\hat{x}_1, y) \in [\hat{x}_1]_2\}$.

Since the whole $[\hat{x}_2]$ is allocated in the first level, for any $y \in Y_2$, $(\hat{x}_2, y)$ is connected with $(\hat{x}_1, y)$ by a between-level path. Furthermore, for any $y' \neq y \in Y$, $(\hat{x}_1, y)$ is connected with $(\hat{x}_1, y')$ by a between-level path. Then, the nodes in $[\hat{x}_1] \cup ([\hat{x}_2] \cap Y_2)$ are connected with each other via a between-level path. For $[\hat{x}_3]$, the nodes in $[\hat{x}_3] \cap Y_1$ and $[\hat{x}_3] \cap Y_2$ are connected to the corresponding nodes in $[\hat{x}_1] \cap Y_1$ and $[\hat{x}_2] \cap Y_2$ via a between-level path, respectively. Additionally, the nodes in $[\hat{x}_2] \cap Y_1$ are connected to the nodes in $[\hat{x}_3] \cap Y_1$ via a between-level path. Therefore, the sub-2-semi-chain restricted to $[\hat{x}_1] \cup [\hat{x}_2] \cup [\hat{x}_3]$ is strongly connected.

Moreover, in both levels of this sub-2-semi-chain, for any $y \in Y$, there is $\hat{\theta}_y \in [y]$. Therefore, no matter whether divide the rest $[x]$-equivalent classes or not and what division patterns, the 2-semi-chain are strongly connected. □

Proof of Proposition 3. Assume the sequence of division patterns contains m divided $[x]$-equivalent class and $n_1 - m$ undivided $[x]$-equivalent class. Given $m \leq n_1$, the algorithm generates all sequences $\{d_{t_1}, \ldots, d_{t_m}\}$ with $1 \leq t_1 \leq \cdots \leq t_m \leq 2^{n_2} - 2$ (recall that $\{d_3, \ldots, d_{2^{n_2}}\}$ are the set of the ordered partitions of Y, $d_{2^{n_2}-1} = (Y, \emptyset)$ and $d_{2^{n_2}} = (\emptyset, Y)$). By Lemma 12, the first part of Algorithm 1 generates all strongly connected sequences of division patterns in Category I. By Lemma 13, the second part generates those in Category II. Finally, by Lemma 14, the third part generates those in Category III. Moreover, since the algorithm enumerates all sequences $(d_{t_1}, \ldots, d_{t_m})$ with $1 \leq t_1 \leq \cdots \leq t_m \leq 2^{n_2} - 2$ without repetition, no duplicated sequence of division patterns is produced.

□