The Trade-off between Privacy and Fidelity via Ehrhart Theory

Arun Padakandla, P. R. Kumar *Fellow, IEEE* and Wojciech Szpankowski *Fellow, IEEE*

Abstract

As an increasing amount of data is gathered nowadays and stored in databases, the question arises of how to protect the privacy of individual records in a database even while providing accurate answers to queries on the database. Differential Privacy (DP) has gained acceptance as a framework to quantify vulnerability of algorithms to privacy breaches. We consider the problem of how to sanitize an entire database via a DP mechanism, on which unlimited further querying is performed. While protecting privacy, it is important that the sanitized database still provide accurate responses to queries. The central contribution of this work is to characterize the amount of information preserved in an optimal DP database sanitizing mechanism (DSM). We precisely characterize the utility-privacy trade-off of mechanisms that sanitize databases in the asymptotic regime of large databases. We study this in an information-theoretic framework by modeling a generic distribution on the data, and a measure of fidelity between the histograms of the original and sanitized databases. We consider the popular $\mathbb{L}_1-$distortion metric, i.e., the total variation norm that leads to the formulation as a linear program (LP). This optimization problem is prohibitive in complexity with the number of constraints growing exponentially in the parameters of the problem. Leveraging tools from discrete geometry, analytic combinatorics, and duality theorems of optimization, we fully characterize the optimal solution in terms of a power series whose coefficients are the number of integer points on a multidimensional convex cross-polytope studied by Ehrhart in 1967. Employing Ehrhart theory, we determine a simple closed form computable expression for the asymptotic growth of the optimal privacy-fidelity trade-off to infinite precision. At the heart of the findings is a deep connection between the minimum expected distortion and a fundamental construct in Ehrhart theory - Ehrhart series of an integral convex polytope.

Index Terms

Differential Privacy, fidelity, distortion, information theory, linear programming optimization, Ehrhart theory, discrete geometry, dual LP, analytic combinatorics.

I. Introduction : Motivation, Contribution and Significance

Nowadays, fine grained and high-dimensional data containing information about their preferences/characteristics is being increasingly gathered from subjects. The data is stored in modern databases (DBs) that permit unrestrained and continuous querying. It is then mined for social, scientific, commercial and economic benefits. Dependencies discovered via such querying, among attributes previously not known to be related, can lead to significant scientific breakthroughs and/or commercial benefits. Due to their value, DBs are therefore being traded among corporations and governmental agencies to facilitate informed policy making. However, such trading of DBs containing private information, amongst untrusted agencies, and their unrestrained querying, results in catastrophic loss of subject privacy [1], [2].

To protect privacy, data needs to be somehow obfuscated, but the utility of the database for statistical inference degrades with increasing obfuscation. It has therefore become imperative to determine *what* to store in a DB so that it simultaneously 1) permits unrestrained querying and 2) provides acceptably accurate responses, even while 3) providing provable guarantees against privacy breaches. What is the precise utility-privacy trade-off, and what should be the mechanism by which the data is obfuscated? A precise information-theoretic study of the utility-privacy trade-off is the subject of this paper.

The need to quantify vulnerability of a DB sanitizing mechanism (DSM) to privacy violation has led to the notion of *differential privacy* (DP) [3], [4]. DP models a DSM, and more generally a query-response mechanism, as a randomized algorithm and quantifies the vulnerability of the latter via its sensitivity to individual records. Let $\underline{r}$ denote a DB, and $\mathcal{N}$ the set of all ordered pairs ($\underline{r}$, $\hat{\underline{r}}$) of DBs that differ in a single record. Consider a probabilistic mechanism, that when asked a certain query about a database $\underline{r}$, randomly outputs a response y with

This work was supported in part by NSF Center for Science of Information (CSoI) Grant CCF-0939370, NSF Grants CCF-1524312, ECCS-1646449, and CNS-1719384, NIH Grant 1U01CA198941-01, and USARO under Contract W911NF-15-1-0279.

a probability $\mathbb{W}(y|\underline{r})$. The random response can be regarded as adding noise to the answer of the query, though more randomization than mere addition is allowed. Such a mechanism M is $\theta-$DP for $\theta \in [0,1]$, if

$$\theta \leq \max_{(\underline{r},\hat{\underline{r}}) \in \mathcal{N}} \max_{y \in \mathcal{Y}} \frac{\mathbb{W}_M(y|\underline{r})}{\mathbb{W}_M(y|\hat{\underline{r}})} \leq \frac{1}{\theta}.$$

Larger values of θ correspond to less vulnerable mechanisms, but this increased protection is achieved at the cost of reduced accuracy of the query response. The key properties of DP - composition [5, Section 3.5] and post-processing [5, Proposition 2.1] - have motivated its adoption as a measure of privacy. In particular, the "post-processing" property states that querying a DB sanitized via $\theta-$DP DSM is, irrespective of the query and the querying mechanism, at least as robust as a $\theta-$DP mechanism. In other words, sanitizing a DB via a DP mechanism provides an impermeable firewall against privacy breaches.

This architecture has been referred to in the literature as *non-interactive* mechanisms. We reduce the case of persistent querying to the non-interactive case by considering how the *entire* database can be sanitized and exported. We address the following central questions that govern the same. Firstly, how does one quantify the amount of information preserved in a DB sanitizing mechanism (DSM)? Any such metric must be representative of the accuracy of responses provided to canonical DB queries. A higher accuracy of responses must be reflected by a larger amount of information preserved. Secondly, among all DSMs subject to a DP constraint $\theta \in (0,1)$, henceforth referred to as a $\theta-$DP DSM, which of them is optimal, and how much information is preserved?

Taking a cue from rate-distortion theory, we quantify the information preserved between the *information source* (original DB) and its *representation* (sanitized DBs) via a measure of *fidelity*. Most statistical, machine learning queries aim to glean at correlations across attributes. The quintessential object of interest is the histogram of the DB, referred to as *type* [6, Chap. 2], [7], [8]. We therefore characterize fidelity between the original and sanitized DBs via a distortion between their corresponding histograms. Measures of divergence between probability distributions such as total variation (TV), Kullbach-Leibler, Csiszár $f-$divergences [9], [10] serve as good choices for measure of distortion. Here we focus on the TV distance. Simple and yet popular, this choice provides us with an elegant case to present fundamental connections between DP and discrete geometry, combinatorics.

Adhering to the information-theoretic flavor, we focus on characterizing precisely the minimum expected distortion between histograms of the original and sanitized DBs, of an optimal $\theta-$DP DSM, in the asymptotic regime of large DBs. Section II contains a mathematical formulation of this problem. The latter reduces to a prohibitively complex optimization problem (Remark 2) with an exponential number of constraints. Seeking to identify the structure of the optimal mechanism, we consider the $\mathbb{L}_1$ or TV divergence measure, in which case the objective function is linear, thereby resulting in a linear program (LP). We are thus confronted with the task of identifying the limit of solutions to a sequence of LPs, each of which is subject to exponentially many constraints (Remark 2). One of our main contributions is a precise characterization of this limit, and hence the minimum expected $\mathbb{L}_1-$distortion of a $\theta-$DP DSM, in the limit of large DBs.

Our solution is built on the fundamental connections we discover between DP and *Ehrhart theory* [11]. Ehrhart theory concerns integer-point enumeration of polytopes. The counts of the number of integer points in the $t-$th dilation of a polytope (Fig. 2) - the *Ehrhart polynomial* of the polytope - and the associated generating function - the *Ehrhart series* of the polytope - are fundamental constructs in Ehrhart theory. As we describe below, they will play a central role in characterizing the limit we seek.

Our crucial first step of visualizing the LP through a graph paves the way to developing these connections with discrete geometry. In particular, we relate the objective and constraints of the LP with the distance distribution of vertices in this graph. This relationship enables us to glean the structure of an optimal solution to our LP. Identifying symmetry properties of the graph, we make the key observation that its distance distribution can be obtained via the Ehrhart polynomial of a suitably defined convex polytope. Leveraging these insights, we identify a sequence of truncated geometric $\theta-$DP mechanisms, which are indeed feasible solutions to the sequence of LPs. We characterize the limit of the corresponding sequence of expected $\mathbb{L}_1-$fidelities through a simple functional of the Ehrhart series of the above mentioned convex polytope, a significant finding. We then employ tools from analytic combinatorics and provide a simple computable closed form expression to the above functional, thereby further characterizing explicitly the limit of the sequence of expected $\mathbb{L}_1-$distortions.

The above mentioned expression is a limit of the objective values corresponding to a sequence of feasible solutions, and hence serves as an upper bound on the limit we seek. We leverage weak duality of LP to identify

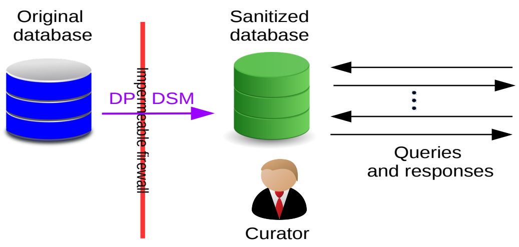


Figure 1. Differentially Private Database Sanitizing Mechanism. The original database is sanitized and then destroyed. All subsequent querying, unlimited in any way, is subsequently performed only on the *sanitized* database.

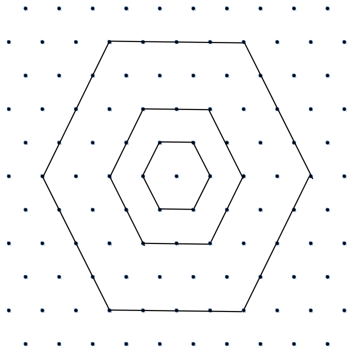


Figure 2. Counts of the number of integer points in the $t-$th dilation of a polytope. The dots represent integer points. There are 6, 12 and 24 integer points in the 1st, 2nd and 4th dilation of the innermost convex polytope.

a lower bound. Note that every feasible solution to the dual of the above LP evaluates to a lower bound on the minimum expected distortion. We therefore consider the sequence of dual LPs and identify a sequence of feasible solutions for the same. We prove that these feasible solutions evaluate to, in the limit, the same functional as obtained in the upper bound. This enables us to conclude that the Ehrhart series of the above mentioned convex integral polytope yields the minimum expected $\mathbb{L}_1-$distortion of a $\theta-$DP DSM, thereby establishing a connection between objects of fundamental interest in the two disciplines/areas.

In addition to proving that the sequence of truncated geometric mechanisms is optimal in the limit, the findings highlight a useful and interesting property analogous to universal optimality [12]. Given any distribution (pmf) on the set of records, we prove that this truncated geometric mechanism $\mathbb{W}^n(\cdot|\cdot)$ can be realized as a cascade of two mechanisms $\mathbb{U}^n(\cdot|\cdot), \mathbb{V}^n(\cdot|\cdot)$. See Figure 4. The first mechanism $\mathbb{U}^n(\cdot|\cdot)$ is a pure $\theta-$DP geometric mechanism that is invariant with the distribution on the set of records. The second mechanism $\mathbb{V}^n(\cdot|\cdot)$ is a truncation that is centered at the histogram corresponding to the distribution. The invariance of $\mathbb{U}^n(\cdot|\cdot)$ lends utility to this cascade mechanism. Specifically, a data gatherer who is oblivious to the true distribution on the set of records can sanitize the original DB through $\mathbb{U}^n(\cdot|\cdot)$ and generate an intermediate DB that is guaranteed to protect privacy while not compromising on utility. Indeed, any entity or enterprise with an accurate knowledge of the underlying distribution can post-process the intermediate database with the corresponding mechanism $\mathbb{V}^n(\cdot|\cdot)$ to obtain a DB with least distortion. In essence, this property permits distributed implementation of an optimal mechanism. This leads us to the notion of universal optimality [12]. Ghosh, Roughgarden and Sundararajan [12] have studied the particular setting of a count query, i.e., a database whose records can take one among two possibilities. They prove that the truncated geometric mechanism is universally optimal for any size of the database for a fairly general class of utility functions. Brenner and Nissim [13] prove that such universal optimal mechanisms do *not* exist if the records can take more than two possibilities. Our findings bring to light a relaxed notion of universal optimality that is useful, and which circumvents the impossibility results proven in [13]. Specifically, we seek optimality only for the family of multinomial distributions on the space of histograms. As the reader will note, this is sufficiently general. Secondly, we seek optimality in the limit of large databases. These two relaxations of universal optimality, both in the spirit of information theory, enable us prove positive existence results and are useful in the light of [13].

While DP [5] has been a subject of intense research, the problem of identifying optimal mechanisms and characterizing the privacy-fidelity trade-off in the expected sense has received much less attention. This, as we state in Remarks 2 and 3, is due to the complexity of the resulting optimization problem. Ghosh Roughgarden and Sundararajan [12] focus attention on a single count query and prove universal optimality of the geometric mechanism for a fairly general class of utility measures. It may be however noted that their finding only provides structural properties of an optimal mechanism leaving the precise characterization of an optimal mechanism and the maximum utility open. Our findings answer this question in the asymptotic limit of large databases, and moreover for a multi-dimensional count query. In our work, we provide a solution to the original optimization problem without resorting to relaxation or continuous extensions, in spite of its hardness. This is, in spirit similar to the work of Geng and Viswanath [14], [15], wherein staircase mechanisms [16] are proven to be the optimal noise adding mechanisms for a general class of convex utility functions, albeit in the minimax setting. Specifically, [15] employs functional analytic arguments to characterize the density function of an optimal noise adding mechanism.

Finally, we highlight certain additional aspects of our work. By considering an arbitrary distribution for entries in the DB, we enable a generic information theoretic study (Remark 1). Secondly, in our general formulation, a standard geometric mechanism is not optimal; in fact it is non-trivial to identify an optimal one (Remark 6). However, by identifying an optimal sequence of mechanisms we also design an efficient shaping of the geometric mechanism that renders it both feasible and optimal. Thirdly, we prove this sequence of mechanisms to be asymptotically universally optimal [12], thereby potentially supporting its adoption (Remark 7).

II. Preliminaries: Notation, Problem Statement

Notation will be introduced as and when necessary. A summary is provided in Table I in Appendix A.

Problem Formulation : Consider a DB with n *subjects*. Each subject is identified with a *record* which stores his or her preferences and/or characteristics. We let $\mathcal{R} = \{a_1, \cdots, a_K\}$ denote the set of possible records. K can be arbitrary, but will remain fixed throughout our study. We let $\underline{r} : = (r_1, \cdots, r_n) \in \mathcal{R}^n$ denote a generic DB with n records.

Example 1. Consider the DB in Fig. 3 containing records of $n = 6$ subjects. Each records contains 5 attributes - zip-code, ethnicity, income, health and average-monthly-expenditure. The database stores subject information with respect to 5 attributes - zipcode, ethnicity, income, health and average-monthly-expenditure. Let $\mathcal{A}_1 = \{47906, 47907, 77840, 77841\}, \mathcal{A}_2 = \{\text{asian}, \text{caucasian}, \text{hispanic}\}, \mathcal{A}_3 = \{50000, 55000, \cdots, 300000\}, \mathcal{A}_4 = \{\text{heart-ailment}, \text{no-heart-ailment}\}, \mathcal{A}_5 = \{500, 600, \cdots, 4000\}$ denote the preferences corresponding to the attributes. The set of records is $\mathcal{R} = \mathcal{A}_1 \times \cdots \mathcal{A}_5$, and $K = |\mathcal{R}| = 4 \cdot 3 \cdot 51 \cdot 2 \cdot 36 = 44064$.

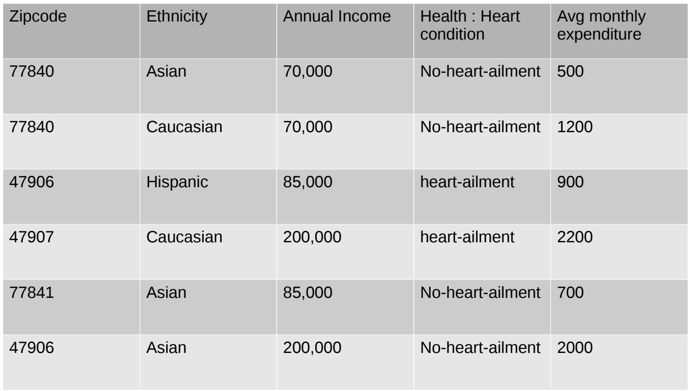
The *histogram* of a DB plays a key role in our study. For a DB $\underline{r} \in \mathcal{R}^n$ and a record $a_k \in \mathcal{R}$, we let $\mathtt{h}(\underline{r})_k = \sum_{i=1}^{n} \mathbb{1}_{\{r_i = a_k\}}$ denote the number of subjects with record a_k, and $\mathtt{h}(\underline{r}) : = (\mathtt{h}(\underline{r})_1, \cdots, \mathtt{h}(\underline{r})_K)$ denote the histogram corresponding to DB $\underline{r} \in \mathcal{R}^n$. Let

$$\mathcal{H}^n : = \{(h_1, \cdots, h_K) \in \mathbb{Z}^K : h_i \geq 0, \textstyle\sum_{k=1}^{K} h_k = n\} \tag{1}$$

denote the collection of histograms. When K is set to a particular value, we let $\mathcal{H}_K^n$ denote $\mathcal{H}^n$.

We measure fidelity between a pair of histograms through a distortion measure $\mathcal{F} : \mathcal{H}^n \times \mathcal{H}^n \to [0, \infty)$. Typical distortion measures include $\mathbb{L}_1, \mathbb{L}_2-$norms, divergence between probability distributions, such as Csiszár $f-$divergences [9], Wasserstein distance etc. For histograms $\underline{s}, \underline{t} \in \mathcal{H}^n$, $\mathcal{F}(\underline{s}, \underline{t})$ is a proxy for the useful information of $\underline{s}$ contained in $\underline{t}$ and vice versa.

In order to protect privacy, we employ a DP database *sanitizing mechanism* (DSM) to output a random sanitized DB. A DP mechanism is a randomized algorithm and we introduce the necessary notation. A mechanism (randomized algorithm) $M : \mathcal{A} \Rightarrow \mathcal{B}$ with set $\mathcal{A}$ of inputs and set $\mathcal{B}$ of outputs is a map $\mathbb{W}_M : \mathcal{A} \to \mathbb{P}(\mathcal{B})$ where $\mathbb{P}(\mathcal{B})$ is the set of probability distributions on $\mathcal{B}$. When input $a \in \mathcal{A}$, the mechanism M produces the output



Zipcode	Ethnicity	Annual Income	Health : Heart condition	Avg monthly expenditure
77840	Asian	70,000	No-heart-ailment	500
77840	Caucasian	70,000	No-heart-ailment	1200
47906	Hispanic	85,000	heart-ailment	900
47907	Caucasian	200,000	heart-ailment	2200
77841	Asian	85,000	No-heart-ailment	700
47906	Asian	200,000	No-heart-ailment	2000

Figure 3. The DB corresponding to Ex. 1.

$b \in \mathcal{B}$ with probability $\mathbb{W}_M(b|a)$. Since $M : \mathcal{A} \Rightarrow \mathcal{B}$ is uniquely characterized by the corresponding collection $(\mathbb{W}_M(\cdot|a) : a \in \mathcal{A}))$ of probability distributions, we refer to it either as $\mathbb{W}_M : \mathcal{A} \rightarrow \mathbb{P}(\mathcal{B})$ or $\mathbb{W}_M : \mathcal{A} \Rightarrow \mathcal{B}$.

A pair $\underline{r}, \underline{\hat{r}} \in \mathcal{R}^n$ of DBs is *neighboring* if $\underline{r}$ and $\underline{\hat{r}}$ differ in exactly one entry. Note that $\underline{r}, \underline{\hat{r}} \in \mathcal{R}^n$ are neighboring if and only if $|\mathtt{h}(\underline{r}) - \mathtt{h}(\underline{\hat{r}})|_1 = 2$. We also say a pair of histograms $\underline{h} \in \mathcal{H}^n$ and $\underline{\hat{h}} \in \mathcal{H}^n$ is neighboring if $|\underline{h} - \underline{\hat{h}}|_1 = 2$.

Definition 1. *Consider the space $\mathcal{R}^n$ of DBs with n subjects. A DSM, $M : \mathcal{R}^n \Rightarrow \mathcal{R}^n$ is $\theta-$DP ($0 < \theta < 1$) if for every pair of neighboring DBs $\underline{r}, \underline{\hat{r}}$ and every DB $\underline{s} \in \mathcal{R}^n$, we have $\theta \ \mathbb{W}_M(\underline{s}|\underline{r}) \leq \mathbb{W}_M(\underline{s}|\underline{\hat{r}}) \leq \theta^{-1} \ \mathbb{W}_M(\underline{s}|\underline{r})$.*

We formulate the problem of characterizing the minimum *expected* distortion of a $\theta-$DP DSM. Towards that end, we model a distribution on the space of DBs. For a record $a_k \in \mathcal{R}$, let $p(a_k) > 0$ denote the probability that a subject's record is a_k. The n records that make up the DB are independently and identically distributed with pmf $\underline{p} := (p(a_k) : a_k \in \mathcal{R})$. The probability of the gathered DB being $\underline{r} = (r_1, \cdots, r_n)$ is $\prod_{i=1}^n p(r_i)$ where r_i is the record of the i-th subject.

Remark 1. We do not assume any restriction on $\underline{p}$, allowing a generic information theoretic study, as we further elaborate below by showing that the problem can be mapped into the class of histograms. In particular, since we do not assume p_k factorizes across attribute fields, as for example a uniform distribution would, the model permits arbitrary correlation across attributes.

The *expected distortion* of a DSM $(\mathbb{W}_M(\cdot|\underline{r}) : \underline{r} \in \mathcal{R}^n)$ is defined as

$$D^n(\mathbb{W}_M, \underline{p}, \mathcal{F}) := \mathbb{E}_M \left\{ \mathcal{F}(\mathtt{h}(\underline{R}), \mathtt{h}(\underline{S})) \right\} := \sum_{\underline{r} \in \mathcal{R}^n} \sum_{\underline{s} \in \mathcal{R}^n} \prod_{i=1}^n p(r_i) \mathbb{W}_M(\underline{s}|\underline{r}) \mathcal{F}(\mathtt{h}(\underline{r}), \mathtt{h}(\underline{s})).$$

We now provide a formulation of the problem: We seek to characterize

$$D_K^*(\theta, \underline{p}, \mathcal{F}) := \lim_{n \to \infty} D_*^n(\theta, \underline{p}, \mathcal{F}), \text{ where } D_*^n(\theta, \underline{p}, \mathcal{F}) \overset{(a)}{:=} \min_{\substack{\mathbb{W}(\cdot|\cdot) \text{is a} \\ \theta-\text{DP DSM}}} D^n(\mathbb{W}, \underline{p}, \mathcal{F}). \tag{2}$$

$D_*^n(\theta, \underline{p}, \mathcal{F})$ is the minimum expected distortion corresponding to a DB with n records. Characterizing $D_K^*(\theta, \underline{p}, \mathcal{F})$ precisely, as well as a sequence of optimal mechanisms is the main goal of the study.

III. Main Results : Precise characterization of $D_K^*(\theta, \underline{p}, |\cdot|_1)$ and Essential Universal Optimality

First, we provide a simpler equivalent formulation of problem (2) with an exponentially smaller number of decision variables. As we will note, even this simplified formulation is quite involved.

Equivalent formulation of $D_*^n(\theta, \underline{p}, \mathcal{F})$ via sufficiency of histogram sanitization: Viewing the DB through its histogram enables us to simplify (2)(a). We make two observations. (i) The distortion between the original and sanitized DBs is a function only of their histograms, and (ii) the DP constraints are related only through the histograms of the DBs. These observations enable us to restrict attention to mechanisms that identically randomize DBs with the same histogram. For such a mechanism M, we have $(\mathbb{W}_M(\underline{s}|\underline{r}) : \underline{s} \in \mathcal{R}^n) = (\mathbb{W}_M(\underline{s}|\underline{\tilde{r}}) : \underline{s} \in \mathcal{R}^n)$ whenever $\mathtt{h}(\underline{r}) = \mathtt{h}(\underline{\tilde{r}})$. In Appendix B, we prove that this restriction does *not* entail any loss in optimality. The first observation enables us to go further. It lets us conclude that the expected distortion of a mechanism does not depend on how it distributes the probability among DBs with the same histogram. Formally, the expected distortions of two DSMs $M, \tilde{M}$ are identical if $\sum_{\underline{s} \in \mathcal{R}^n : \mathtt{h}(\underline{s}) = \underline{h}} \mathbb{W}_M(\underline{s}|\underline{r}) = \sum_{\underline{s} \in \mathcal{R}^n : \mathtt{h}(\underline{s}) = \underline{h}} \mathbb{W}_{\tilde{M}}(\underline{s}|\underline{r})$ for all $\underline{h} \in \mathcal{H}^n$ and for all $\underline{r} \in \mathcal{R}^n$. These enable us to shift our viewpoint from DB sanitization to *histogram sanitization.* We define a $\theta-$DP histogram sanitizing mechanism (HSM) as follows:

Definition 2. *A pair $\underline{h}, \underline{\hat{h}} \in \mathcal{H}^n$ of histograms is neighboring if $|\underline{h} - \underline{\hat{h}}|_1 = 2$. A histogram sanitizing mechanism (HSM) $M : \mathcal{H}^n \Rightarrow \mathcal{H}^n$ is $\theta-$DP ($0 < \theta < 1$) if for every pair $\underline{h}, \underline{\hat{h}} \in \mathcal{H}^n$ of neighboring histograms and every histogram $\underline{g} \in \mathcal{H}^n$, we have $\theta \ \mathbb{W}_M(\underline{g}|\underline{h}) \leq \mathbb{W}_M(\underline{g}|\underline{\hat{h}}) \leq \theta^{-1} \ \mathbb{W}_M(\underline{g}|\underline{h})$.*

We now describe our problem (2) from the histogram sanitization viewpoint. A random DB $\underline{R} \in \mathcal{R}^n$ is chosen with distribution as modeled earlier. Its histogram $\mathtt{h}(\underline{R})$ is input to a HSM $M : \mathcal{H}^n \Rightarrow \mathcal{H}^n$. Let $\underline{G} \in \mathcal{H}^n$ denote the random output histogram. Any DB $\underline{S} \in \mathcal{R}^n$, whose histogram $\mathtt{h}(\underline{S}) = \underline{G}$ can be considered as the sanitized DB. Our goal is to find a $\theta-$DP HSM M that minimizes

$$\mathbb{E}_M\{\mathcal{F}(\mathtt{h}(\underline{R}), \mathtt{h}(\underline{S}))\} = \mathbb{E}_M\{\mathcal{F}(\mathtt{h}(\underline{R}), \underline{G})\} = \sum_{\underline{h}\in\mathcal{H}^n}\sum_{\underline{g}\in\mathcal{H}^n} P(\mathtt{h}(\underline{R}) = \underline{h})\mathbb{W}_M(\underline{g}|\underline{h})\mathcal{F}(\underline{g}, \underline{h}).$$

We note that the distribution $P(\mathtt{h}(\underline{R}) = \underline{h})$ of the random histogram is given by $P(\underline{R} = \underline{r}) = \prod_{i=1}^n p(r_i) = \prod_{k=1}^K p(a_k)^{\mathtt{h}(\underline{r})_k}$. Henceforth, we let $p_k : = p(a_k)$ and $\underline{p}^{\underline{h}} : = \prod_{k=1}^K p_k^{h_k}$. With these, we have $P(\underline{R} = \underline{r}) = \underline{p}^{\mathtt{h}(\underline{r})}$. This leads to

$$P(\mathtt{h}(\underline{R}) = \underline{h}) = \sum_{\underline{r}\in\mathcal{R}^n:\mathtt{h}(\underline{r})=\underline{h}} P(\underline{R} = \underline{r}) = \sum_{\underline{r}\in\mathcal{R}^n:\mathtt{h}(\underline{r})=\underline{h}} \underline{p}^{\mathtt{h}(\underline{r})} = \binom{n}{\underline{h}}\underline{p}^{\underline{h}}, \tag{3}$$

where (3) follows from the fact that the number of DBs whose histogram is $\underline{h} \in \mathcal{H}^n$ is the multinomial coefficient $\binom{n}{\underline{h}} : = \binom{n}{h_1 \cdots h_K}$. We note that the multinomial distribution (3) with a generic distribution $\underline{p}$ on the set of records is indeed the most generic distribution on the space of histograms. Throughout, we make no assumption on $\underline{p}$, resulting in a fairly generic study.

Equation (3) lets us explicitly state our equivalent simplified problem as follows. Given a privacy budget $\theta > 0$, our goal is to characterize $D_K^*(\theta, \underline{p}, \mathcal{F}) : = \lim_{n\to\infty} D_*^n(\theta, \underline{p}, \mathcal{F})$, where

$$\begin{array}{rcll}
D_*^n(\theta, \underline{p}, \mathcal{F}) & := & \min\limits_{\mathbb{W}(\cdot|\cdot)} D^n(\mathbb{W}, \underline{p}, \mathcal{F}), & \text{with } D^n(\mathbb{W}, \underline{p}, \mathcal{F}) : = \sum\limits_{\underline{h}\in\mathcal{H}^n}\sum\limits_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}}\underline{p}^{\underline{h}}\mathbb{W}(\underline{g}|\underline{h})\mathcal{F}(\underline{h}, \underline{g}), \\
\text{subject to} & & \mathbb{W}(\underline{g}|\underline{h}) \geq 0 & \text{for every pair } (\underline{g}, \underline{h}) \in \mathcal{H}^n \times \mathcal{H}^n, \\
 & & \sum\limits_{\underline{g}\in\mathcal{H}^n} \mathbb{W}(\underline{g}|\underline{h}) \overset{(a)}{=} 1 & \text{for every } \underline{h} \in \mathcal{H}^n, \\
 & & \mathbb{W}(\underline{g}|\underline{h}) - \theta\ \mathbb{W}(\underline{g}|\underline{\hat{h}}) \overset{(b)}{\geq} 0 & \text{for every pair of histograms } (\underline{h}, \underline{\hat{h}}) \in \mathcal{H}^n \times \mathcal{H}^n \\
 & & & \text{for which } |\underline{h} - \underline{\hat{h}}|_1 = 2 \text{ and every } \underline{g} \in \mathcal{H}^n.
\end{array} \tag{4}$$

In going from (2) to (4), we have replaced the collection $(\mathbb{W}(\underline{s}|\underline{r}) : \mathtt{h}(\underline{s}) = \underline{h})$ by a single decision variable $\mathbb{W}(\underline{h}|\mathtt{h}(\underline{r}))$ and set $\mathbb{W}(\cdot|\underline{r}) = \mathbb{W}(\cdot|\underline{\tilde{r}})$ whenever $\mathtt{h}(\underline{r}) = \mathtt{h}(\underline{\tilde{r}})$. Constraints (4) and (2) are specified by $|\mathcal{H}^n|^2 = \binom{n+K-1}{K-1}^2 \sim (n+1)^{2K}$ and K^{2n} decision variables, respectively. With K fixed, the former is exponentially smaller. This simplification is not a result of any assumption. $D_*^n(\theta, \underline{p}, \mathcal{F})$ defined in (4) and (2)(a) are proven to be equal in Appendix B.

Remark 2. The optimization problem (4) has $(n+1)^{2K}$ decision variables. For every choice $(\underline{h}, \underline{\hat{h}})$ of neighboring histograms and every $\underline{g} \in \mathcal{H}^n$, the LP imposes two types of constraints. There are $\mathcal{O}(k^2|\mathcal{H}^n|^2) = \mathcal{O}(k^2(n+1)^{2(k-1)})$ constraints[1] of the form (4)(b). For any practical values of K and n, it is intractable to obtain a solution via computation. In fact, we are unaware of a solution of this LP even for the case $K = 2$. While [12] proves the optimal mechanism can be achieved by a post-processing remapping of the geometric mechanism, for any user preference an optimal mechanism and the corresponding utility remain unknown.

Notwithstanding this difficulty, one can obtain a precise characterization of $D_K^*(\theta, \underline{p}, \mathcal{F})$ by leveraging rich tools from discrete geometry and LP theory.

Statement of the Main Result : We restate our problem in the context of the $\mathbb{L}_1-$distance measure. We aim to characterize $D_K^*(\theta, \underline{p}, |\cdot|_1) : = \lim_{n\to\infty} D_*^n(\theta, \underline{p}, |\cdot|_1)$, where

$$\begin{gathered}
D_*^n(\theta, \underline{p}, |\cdot|_1) : = \min D^n(\mathbb{W}, \underline{p}, |\cdot|_1) \text{ subject to the constraints in (4), where} \\
D^n(\mathbb{W}, \underline{p}, |\cdot|_1) : = \sum_{\underline{h}\in\mathcal{H}^n}\sum_{\underline{g}\in\mathcal{H}^n}\binom{n}{\underline{h}}\underline{p}^{\underline{h}}\mathbb{W}(\underline{g}|\underline{h})|\underline{h} - \underline{g}|_1.
\end{gathered} \tag{5}$$

Since we restrict attention to $|\cdot|_1$, we let $D_*^n(\theta, \underline{p})$ and $D_K^*(\theta, \underline{p})$ denote $D_*^n(\theta, \underline{p}, |\cdot|_1)$ and $D_K^*(\theta, \underline{p}, |\cdot|_1)$ in the sequel. Theorem 1 is our main result and provides a simple computable closed form expression for $D_K^*(\theta, \underline{p})$. In

[1] For every $\underline{h} \in \mathcal{H}^n$ except those for which one or more of the coordinates are 0, we have $|\{\underline{\hat{t}} \in \mathcal{H}^n : |\underline{h} - \underline{\hat{t}}|_1 = 2\}| = k(k-1)$. Also, $|\mathcal{H}^n| = \binom{n+k-1}{k-1} \sim (n+1)^{k-1}$ [7, Lemma II.1], [6, Chap 2, Lemma1].

particular, we provide three characterizations of $D^*_K(\theta,\underline{p})$. The first one expresses $D^*_K(\theta,\underline{p})$ in terms of the Ehrhart series of a suitably defined convex polytope, thereby establishing connection between DP and Ehrhart theory. The second employs simple combinatorial arguments to characterize the resulting power series explicitly. The third exploits analytic combinatorial techniques to express this power series in terms of a *hyper-geometric series*. The latter encapsulates the entire information from a power series and provides a computable expression. The result also shows that the limiting minimum distortion is not dependent on $\underline{p}$.

Theorem 1. *(a) The minimum expected $\mathbb{L}_1-$distortion of a $\theta-$DP HSM is given by*

$$D^*_K(\theta,\underline{p}) = \frac{2\theta}{\mathrm{Ehr}_{\mathcal{P}}(\theta)}\frac{d\mathrm{Ehr}_{\mathcal{P}}(\theta)}{d\theta} - \frac{2\theta}{1-\theta}, \text{ where } \mathrm{Ehr}_{\mathcal{P}}(\mathrm{z}) := 1 + \sum_{\mathrm{d}=1}^{\infty} \mathrm{L}_{\mathcal{P}}(\mathrm{d})\mathrm{z}^{\mathrm{d}} \tag{6}$$

is the Ehrhart series of the cross-polytope whose $d-th$ dilation is given by

$$\mathcal{P}_d = \{(x_1,\cdots,x_K) \in \mathbb{R}^K : \textstyle\sum_{k=1}^K x_k = 0, \sum_{k=1}^K |x_k| \le 2d\}, \tag{7}$$

and $L_{\mathcal{P}}(d)$ is the number of points in $\mathcal{P}_d$ with integer co-ordinates. $D^*_K(\theta,\underline{p})$ does not depend on $\underline{p}$ and hence does not depend on the multinomial distribution. (b) We have

$$\mathrm{Ehr}_{\mathcal{P}}(\theta) = \frac{1}{1-\theta} + \sum_{\mathrm{d}=1}^{\infty}\left\{\sum_{\mathrm{r}=1}^{\mathrm{K}-1}\binom{\mathrm{K}}{\mathrm{r}}\binom{\mathrm{d}+\mathrm{r}-1}{\mathrm{r}-1}\binom{\mathrm{d}-1}{\mathrm{K}-\mathrm{r}-1}\right\}\frac{\theta^{\mathrm{d}}}{1-\theta}, \text{ and} \tag{8}$$

(c)

$$D^*_K(\theta,\underline{p}) = 2\theta\left\{\frac{K-1}{1-\theta} + \frac{S'_{K-1}(\theta)}{S_{K-1}(\theta)}\right\}, \text{ where } S_{K-1}(\theta) = \sum_{j=0}^{K-1}\theta^j\left[\binom{K-1}{j}\right]^2 \tag{9}$$

with $S'_{K-1}(\theta) := \frac{d}{d\theta}S_{K-1}(\theta)$. An optimal HSM is obtained as a truncation of a geometric mechanism $\mathbb{W}^*(\underline{g}|\underline{h}) = (1-\theta)^{-1}\mathrm{Ehr}_{\mathcal{P}}(\theta)^{-1}\theta^{\frac{|\underline{\mathrm{g}}-\underline{\mathrm{h}}|_1}{2}}$, where $\mathrm{Ehr}_{\mathcal{P}}(\theta)$ is defined in (8).

Below, we express $D^*_K(\theta,\underline{p})$ in terms of another important construct in analysis - the *Legendre polynomial*. We note that $S_{K-1}(\theta) = (1-\theta)^{K-1}L_{K-1}(\frac{1+\theta}{1-\theta})$ [17, Pg. 86, Prob. 85], where $L_n(x) := \frac{1}{2^n n!}\frac{d^n}{dx^n}(x^2-1)^n$ is the Legendre polynomial of degree n defined in [18, Pg. 147, Prob. 219]. This leads to the following important characterization.

Corollary 1. *The minimum expected $\mathbb{L}_1-$distortion of a $\theta-$DP HSM is given by*

$$D^*_K(\theta,\underline{p}) = K\left\{\frac{1+\theta}{1-\theta} + \frac{L_K(y)}{L_{K-1}(y)}\right\}, \text{ where } y = \frac{1+\theta}{1-\theta}. \tag{10}$$

In particular for $K=2$, the limit $D^*_2(\theta,\underline{p}) = \lim_{n\to\infty} D^n_*(\theta,\underline{p}) = \frac{4\theta}{1-\theta^2}$.

The proof is based on the identity $S_{K-1}(\theta) = (1-\theta)^{K-1}L_{K-1}(y)$ and the recurrence relation $(1-y^2)L'_{K-1}(y) = KyL_{K-1}(y) - KL_K(y)$. We provide the details in Appendix C.

Remark 3. We emphasize that (9) and (10) provide an *exact computable closed form expression* for $D^*_K(\theta,\underline{p})$. Owing to the complexity of the resulting optimization problem, study of the privacy-distortion trade-off for the *expected* distortion, which is the common object of interest in information theory, is very limited. While a lot more is known in the minimax setting, most of these results are only up to an order. The reader will note that the tools we employ in proving Thm. 1 are also applicable for the minimax setting. A similar analysis can throw more light on the latter setting. In the interest of brevity, we reserve this for future work.

Remark 4. One may recover problem formulations studied in [12], [19], among others, by an appropriate choice of the distortion measure $\mathcal{F}(\cdot,\cdot)$ in (4). In particular Ghosh, Roughgarden and Sundararajan [12] study the $K=2$ case for a fairly generic distortion measure, and prove structural properties of an optimal mechanism. While these hold for each n, they do not pin down an optimal mechanism, leaving $D^*_2(\theta,\underline{p})$ unknown. On the one hand, [20] studies a min-max problem setting. Secondly, their continuous extension results in a larger constraint set, lending the lower bounds developed therein invalid for the original discrete problem setting.

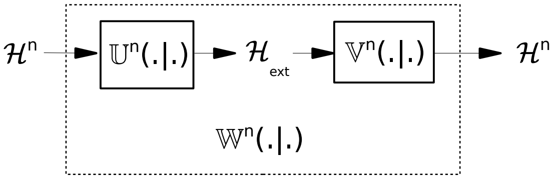


Figure 4. $\mathbb{W}^n(\cdot|\cdot)$ realized as a cascade mechanism.

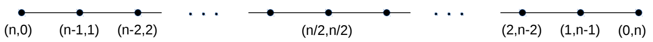


Figure 5. Privacy-constraint graph for $K = 2$ and general n. The vertices are labeled by the corresponding histogram. Two vertices are connected by an edge if their corresponding histograms are at an $\mathbb{L}_1-$distance 2.

A striking aspect of (6) is the invariance of $D^*_K(\theta, \underline{p})$ with $\underline{p}$ as noted above. Why is this true? For large n, $\binom{n}{\underline{h}}\underline{p}^{\underline{h}}$ approximates a pmf that is 'relatively flat' [21] on the set of histograms within an $\mathbb{L}_1-$ball of radius $\mathcal{O}(\sqrt{n})$ centered at $(np_1, \cdots, np_K)$. This radius being sub-linear, for any $\underline{p}$ with positive entries, the $\mathbb{L}_1-$ball that contains most of the mass is eventually supported on the set of histograms. Since we are concerned only in the eventual limit, the effect of $\underline{p}$ is only a shift of the center of this $\mathbb{L}_1-$ball containing a 'relatively flat' pmf. This leads us to the following question. Can we design a sequence $\mathbb{W}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n : n \in \mathbb{N}$ of mechanisms that is in the limit optimal, where each $\mathbb{W}^n$ can be realized as a cascade of $\mathbb{U}^n : \mathcal{H}^n \Rightarrow \mathcal{Y}$ and $\mathbb{V}^n : \mathcal{Y} \Rightarrow \mathcal{H}^n$, where $\mathbb{U}^n$ is $\theta-$DP and is invariant with $\underline{p}$? As the informed reader will recognize, this is related to the notion of universal optimality [12]. We define the related notion of essential universal optimality.

Definition 3. A sequence $\mathbb{W}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n : n \in \mathbb{N}$ of $\theta-$DP HSMs are *essentially universally optimal* (Ess-Univ-Opt) if for each $n \in \mathbb{N}$, $\mathbb{W}^n$ can be realized as a cascade $\mathbb{U}^n : \mathcal{H}^n \to \mathcal{H}^n_{\text{ext}}$, $\mathbb{V}^n : \mathcal{H}^n_{\text{ext}} \to \mathcal{H}^n$, i.e. (see Figure 4), $\mathbb{W}^n(\underline{g}|\underline{h}) = \sum_{\underline{b} \in \mathcal{H}^n_{\text{ext}}} \mathbb{U}^n(\underline{b}|\underline{h})\mathbb{V}^n(\underline{g}|\underline{b})$ for every $\underline{g}, \underline{h} \in \mathcal{H}^n$, where $\mathcal{H}^n_{\text{ext}}$ is any (not necessarily finite) set, such that (i) $\lim_{n\to\infty} D^n(\mathbb{W}^n, \underline{p}) = D^*_K(\theta, \underline{p})$ for every pmf $\underline{p}$ on a set of K elements, and (ii) $\mathbb{U}^n : \mathcal{H}^n \to \mathcal{H}^n_{\text{ext}}$ is $\theta-$DP and invariant with $\underline{p}$.

Remark 5. Ess-Univ-Opt is a *relaxed/weaker* form of universal optimality [12] in two respects. Firstly, we *restrict* the class of pmfs on histograms to *multinomial* pmfs. Indeed, our definition of $D^n_*(\theta, \underline{p})$ in (5) is wrt $\binom{n}{\underline{h}}\underline{p}^{\underline{h}}$. Secondly, we only ask for *asymptotic* optimality of the sequence of mechanisms. This relaxed notion is of interest for the following reasons. Firstly, we operate with large databases. For sufficiently large n the distortion of an Ess-Univ-Opt sequence of mechanisms might be sufficiently close to the true optimum for that n. Secondly, as the reader will note, it suffices to consider multinomial pmfs on $\mathcal{H}^n$. In the light of non-existence of 'strict' universally optimal mechanisms [13], it is worth pursuing this relaxed notion.

As mentioned in [12], the existence of Ess-Univ-Opt is noteworthy. The proof of our main result will bring to light a sequence of Ess-Univ-Opt mechanisms.

Theorem 2. *Ess-Univ-Opt mechanisms for histogram sanitization wrt $\mathbb{L}_1-$distortion exist.*

The proof of Thm. 2 follows from the proof of Thm. 1 wherein a sequence of truncated geometric mechanisms are proven to be Ess-Univ-Opt. The following section details the proof of Theorem 1.

IV. Analysis and Proofs

The proof of Theorem 1 involves two parts - establishing the upper bound and the lower bound. The lower bound is via the weak duality theorem and is detailed in Section IV-B. The upper bound leverages tools from Ehrhart theory and is provided in Section IV-A. Before we provide a proof of the upper bound, we introduce the necessary constructs from Ehrhart theory and describe how and why they are related to $D^*_K(\theta, \underline{p})$ and the LP (5) studied here. The following description serves as a road map of the proof.

$D^*_K(\theta, \underline{p})$ is the limit of solutions to a sequence of LPs (5). These LPs are involved. We begin with the privacy-constraint (PC) graph [13] which greatly aids in visualization and naturally leads us into Ehrhart theory. Consider a graph $G = (V, E)$ with vertex set $V = \mathcal{H}^n$ and an edge set $E = \left\{(\underline{h}, \hat{\underline{h}}) \in \mathcal{H}^n \times \mathcal{H}^n : |\underline{h} - \hat{\underline{h}}|_1 = 2\right\}$. Figures 5, 6 provide the PC graph for $(K = 2, n)$, $(K = 3, n = 5)$ respectively. For every vertex $\underline{h} \in V$, visualize the sub-collection $(\mathbb{W}(\underline{g}|\underline{h}) : \underline{g} \in \mathcal{H}^n)$ of decision variables as a function of V, i.e., as values lying on V, corresponding to $\underline{h} \in V$ (See Fig. 7). The values $(\mathbb{W}(\underline{g}|\underline{h}) : \underline{g} \in \mathcal{H}^n)$ and $(\mathbb{W}(\underline{g}|\hat{\underline{h}}) : \underline{g} \in \mathcal{H}^n)$ corresponding to two neighboring

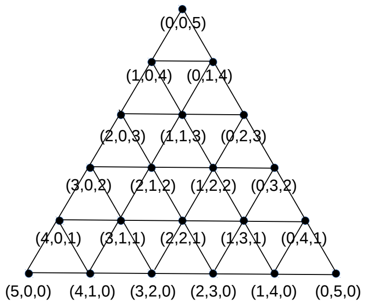


Figure 6. Privacy-constraint graph for $k = 3$, $n = 5$.

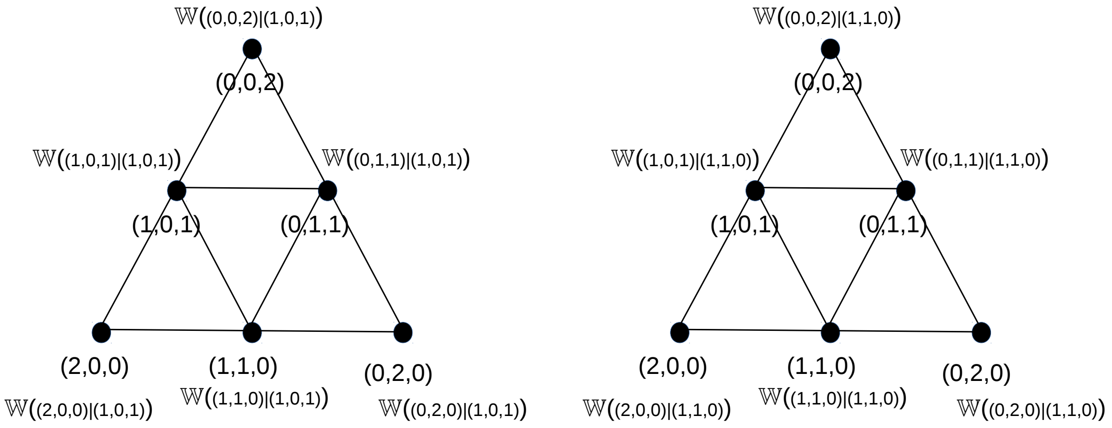

$\mathbb{W}$((0,0,2)|(1,0,1))
(0,0,2)
$\mathbb{W}$((1,0,1)|(1,0,1))
$\mathbb{W}$((0,1,1)|(1,0,1))
(1,0,1)
(0,1,1)
(2,0,0)
(1,1,0)
(0,2,0)
$\mathbb{W}$((2,0,0)|(1,0,1))
$\mathbb{W}$((1,1,0)|(1,0,1))
$\mathbb{W}$((0,2,0)|(1,0,1))
$\mathbb{W}$((0,0,2)|(1,1,0))
(0,0,2)
$\mathbb{W}$((1,0,1)|(1,1,0))
$\mathbb{W}$((0,1,1)|(1,1,0))
(1,0,1)
(0,1,1)
(2,0,0)
(1,1,0)
(0,2,0)
$\mathbb{W}$((2,0,0)|(1,1,0))
$\mathbb{W}$((1,1,0)|(1,1,0))
$\mathbb{W}$((0,2,0)|(1,1,0))

Figure 7. The PC graphs for $K = 3, N = 2$ are depicted. The decision variables $(\mathbb{W}(\underline{g}|(1,0,1)) : \underline{g} \in \mathcal{H}_3^2)$ are associated with the nodes of the graph on the left. On the right, the decision variables $(\mathbb{W}(\underline{g}|(1,1,0)) : \underline{g} \in \mathcal{H}_3^2)$ are associated with the nodes of the graph. Since $(1,1,0)$ and $(1,0,1)$ are neighbors, at every node, the two values have to be within θ and $\frac{1}{\theta}$ of each other.

vertices $\underline{h}, \hat{\underline{h}}$ have to be within θ and $\frac{1}{\theta}$ of each other everywhere, i.e., at every $\underline{g}$ (see Fig. 7). In addition, the values corresponding to any node must be non-negative and sum to 1. The PC graph also provides a visualization of the objective function. $|\underline{g}-\underline{h}|_1$ is exactly twice $d_G(\underline{g},\underline{h})$ (proof in Lemma 3(ii), Appendix D). Two useful consequences follow. Firstly, the values corresponding to a node, say $\underline{h}$, that are equidistant from $\underline{h}$, are multiplied by identical coefficients in the objective function. Formally, $\binom{n}{\underline{h}}|\tilde{\underline{g}} - \underline{h}|_1 = \binom{n}{\underline{h}}|\underline{g} - \underline{h}|_1$ iff $d_G(\tilde{\underline{g}},\underline{h}) = d_G(\underline{g},\underline{h})$. Here and henceforth, $d_G(v_1, v_2)$ denotes the length of a shortest path from $v_1 \in V$ to $v_2 \in V$ in graph $G = (V, E)$. Secondly, coefficients associated with the values increase with their distance from $\underline{h}$. Formally, if $d_G(\tilde{\underline{g}},\underline{h}) > d_G(\underline{g},\underline{h})$, then $\binom{n}{\underline{h}}|\tilde{\underline{g}} - \underline{h}|_1 > \binom{n}{\underline{h}}|\underline{g} - \underline{h}|_1$. These observations let us restate our objective function (5) as

$$D^n(\mathbb{W},\underline{p}) \overset{(a)}{=} \sum_{\underline{h}\in\mathcal{H}^n}\sum_{d=1}^{n}\sum_{\substack{\underline{g}\in\mathcal{H}^n:\\ |\underline{g}-\underline{h}|_1=2d}} \binom{n}{\underline{h}}\underline{p}^{\underline{h}}\mathbb{W}(\underline{g}|\underline{h})2d = \sum_{\underline{h}\in\mathcal{H}^n}\binom{n}{\underline{h}}\underline{p}^{\underline{h}}\sum_{d=1}^{n} 2d \sum_{\substack{\underline{g}\in\mathcal{H}^n:\\ d_G(\underline{g},\underline{h})=d}} \mathbb{W}(\underline{g}|\underline{h}). \tag{11}$$

In arriving at (11)(a), we used the fact that for any $\underline{g},\underline{h} \in \mathcal{H}^n$, we have $|\underline{g}-\underline{h}|_1$ is an even integer and at most $2n$. This is proven in Lemma 3(i), Appendix D. Consider a HSM $M : \mathcal{H}^n \Rightarrow \mathcal{H}^n$ for which $\mathbb{W}(\underline{g}|\underline{h}) = f(\underline{h}, |\underline{g}-\underline{h}|_1)$ is a function only of the distance between the vertices. In the sequel, we will prove this sub-collection contains a mechanism that is optimal in the limit $n \to \infty$. For such a HSM, (11) reduces to

$$D^n(\mathbb{W},\underline{p}) = \sum_{\underline{h}\in\mathcal{H}^n}\binom{n}{\underline{h}}\underline{p}^{\underline{h}}\sum_{d=1}^{n} 2dN_d(\underline{h})f(\underline{h},2d), \text{ where } N_d(\underline{h}) = \left|\left\{\underline{g} \in \mathcal{H}^n : d_G(\underline{g},\underline{h}) = d\right\}\right| \tag{12}$$

is the number of vertices at graph distance d from $\underline{h}$. To evaluate the RHS of $D^n(\mathbb{W},\underline{p})$ above, we will need to characterize the sum $\sum_{d=1}^{n} dN_d(\underline{h})f(\underline{h},d)$. Let us consider the sequence $N_1(\underline{h}), N_2(\underline{h}), \cdots, N_n(\underline{h})$ which may be regarded as the distance distribution of the vertex $\underline{h} \in V = \mathcal{H}^n$. Consider Fig. 8 and two sequences $(N_d(\underline{h}) : d = 1, 2, \cdots)$ and $(N_d(\tilde{\underline{h}}) : d = 1, 2, \cdots)$ for any pair $\underline{h}, \tilde{\underline{h}} \in V$ within the dotted circle. These sequences agree on the initial few terms, henceforth referred to as the *head*, and disagree in a few subsequent terms due to the presence of the boundary. As the boundary recedes (i.e., $n \to \infty$), the first term of disagreement recedes, and the head elongates. Alternatively stated, the heads of the sequences $(N_d(\underline{h}) : d = 1, 2, \cdots)$ for $\underline{h}$ within the dotted circle become invariant with $\underline{h}$. Formally, there exists a distance $r \in \mathbb{N}$ such that, for every $\underline{h}$ in the dotted circle, $N_d(\underline{h}) \to N_d$ for all $d = 1, 2, \cdots, r-1$. Moreover $r \to \infty$ as the boundary recedes, i.e., $n \to \infty$. We characterize N_d by considering $\underline{c} := n\underline{p}$. Observe that

$$N_d(\underline{c}) = \left| \left\{ \underline{g} \in \mathcal{H}^n : d_G(\underline{g}, \underline{c}) = d \right\} \right| = \left| \left\{ \underline{z} \in \mathbb{Z}^K : \underline{c} + \underline{z} \in \mathcal{H}^n, |\underline{z}|_1 = 2d \right\} \right|$$

$$= |\{\underline{z} \in \mathbb{Z}^K \colon c_i + z_i \geq 0, \sum_{i=1}^{K} c_i + z_i = n, |\underline{z}|_1 = 2d\}| = |\{\underline{z} \in \mathbb{Z}^K \colon z_i \geq -np_i, \sum_{i=1}^{K} z_i = 0, |\underline{z}|_1 = 2d\}|.$$

As $n \to \infty$, the lower bound on z_i vanishes (becomes redundant), and we have

$$N_d(\underline{c}) \to N_d := \left| \{\underline{z} \in \mathbb{Z}^k : \textstyle\sum_{k=1}^{K} z_k = 0, |\underline{z}|_1 = 2d\} \right|. \tag{13}$$

N_d is the number of *integer* points on the *face* of the *integral convex polytope*

$$\mathcal{P}_d = \{(x_1, \cdots, x_K) \in \mathbb{R}^K : \textstyle\sum_{k=1}^{K} x_k = 0, \sum_{k=1}^{K} |x_k| \leq 2d\}. \tag{14}$$

Indeed, if $L_{\mathcal{P}}(d) := |\mathbb{Z}^K \cap \mathcal{P}_d|$, then $N_d = L_{\mathcal{P}}(d) - L_{\mathcal{P}}(d-1)$.[2] Notice that $L_{\mathcal{P}}(d)$ is the number of integral points in the $d-$th dilation of the integral convex polytope $\mathcal{P} := \mathcal{P}_1$. $L_{\mathcal{P}}(d)$ and its generating function play a central role in this paper. Ehrhart theory concerns the enumeration of integer points in a integral convex polytope and the objects associated with these counts. We present the foundational results in Ehrhart theory that we will have opportunity to use. The reader is referred to [11] for a beautiful exposition of Ehrhart theory.

A convex $l-$polytope is a convex polytope of dimension l. A convex $l-$polytope whose vertices have integral co-ordinates is an integral convex $l-$polytope. $L_{\mathcal{P}}(d)$ is the number of integral points in the $d-$th dilation of the integral convex $l-$polytope (Fig. 2). Our pursuit of $L_{\mathcal{P}}(d)$ and the associated objects is aided by the following fundamental theorem of Ehrhart. Ehrhart's theorem states that if $\mathcal{P}$ is an integral convex $l-$polytope, then $L_{\mathcal{P}}(d)$ is a polynomial in d of degree l. We refer to $L_{\mathcal{P}}(d)$ as *Ehrhart's polynomial*. We will identify N_d, and hence $L_{\mathcal{P}}(d)$, precisely in our proof. As evidenced by (6), we will have opportunity to study the generating function of the counts $L_{\mathcal{P}}(d) : d \in \mathbb{N}$. We refer to the formal power series

$$\mathrm{Ehr}_{\mathcal{P}}(\mathrm{z}) = 1 + \textstyle\sum_{\mathrm{d}=1}^{\infty} \mathrm{L}_{\mathcal{P}}(\mathrm{d})\mathrm{z}^{\mathrm{d}} \text{ as the } \textit{Ehrhart series} \text{ of } \mathcal{P}, \text{ and let } \mathscr{E}_{\mathcal{P},\mathrm{f}}(\mathrm{z}) := (1-\mathrm{z})\mathrm{Ehr}(\mathrm{z}). \tag{15}$$

Since $N_d = L_{\mathcal{P}}(d) - L_{\mathcal{P}}(d-1)$, we have $\mathscr{E}_{\mathcal{P},f}(\theta) = (1-\theta)\mathrm{Ehr}_{\mathcal{P}}(\theta) = 1 + \sum_{\mathrm{d}=1}^{\infty} \mathrm{N_d}\theta^{\mathrm{d}}$.

Having introduced the tools, we now sketch the main elements of the proof. In this section, we first argue that the RHS of (6) is an upper bound on $D_K^*(\theta, \underline{p})$.

A. Upper bound

Suppose one were to consider the popular Laplace/geometric/staircase mechanism $\mathscr{G} : \mathcal{H}^n \Rightarrow \mathcal{H}^n$ and characterize its distortion. In that case,

$$\mathbb{W}_{\mathscr{G}}(\underline{g}|\underline{h}) \propto \theta^{\frac{|\underline{g}-\underline{h}|_1}{2}} \text{ and hence } \mathbb{W}_{\mathscr{G}}(\underline{g}|\underline{h}) = \frac{\theta^{d_G(\underline{g},\underline{h})}}{E_{\underline{h}}(\theta)}, \text{ where } E_{\underline{h}}(\theta) = 1 + \sum_{d=1}^{n} N_d(\underline{h})\theta^d \tag{16}$$

is a normalizing constant chosen to ensure $\sum_{\underline{g} \in \mathcal{H}^n} \mathbb{W}_{\mathscr{G}}(\underline{g}|\underline{h}) = 1$. It will be apparent that $\mathbb{W}_{\mathscr{G}}(\cdot|\underline{h})$ is $\theta-$DP only if $E_{\underline{h}}(\theta)$ is invariant with $\underline{h}$. For any (finite) $n \in \mathbb{N}$ this is not true, leading to obstacles in defining a feasible $\theta-$DP HSM analog to the geometric mechanism. We overcome this by considering a cascade mechanism. See Figure 4. $\mathbb{U}^n$ is analogous to the geometric mechanism $\mathbb{W}_{\mathcal{G}}$ and outputs a 'histogram' in an 'extended set of histograms'. This

[2] If $(x_1, \cdots, x_K) \in \mathbb{Z}^K$ and $\sum_{k=1}^{K} x_k = 0$, then $\sum_{k=1}^{K} |x_k|$ is an even integer. This follows in a straightforward manner from Lemma 3(i), Appendix D. Therefore, if $(x_1, \cdots, x_K) \in \mathbb{Z}^K \cap \mathcal{P}_d$ and $\sum_{k=1}^{K} |x_k| < 2d$, then $\sum_{k=1}^{K} |x_k| \leq 2(d-1)$.

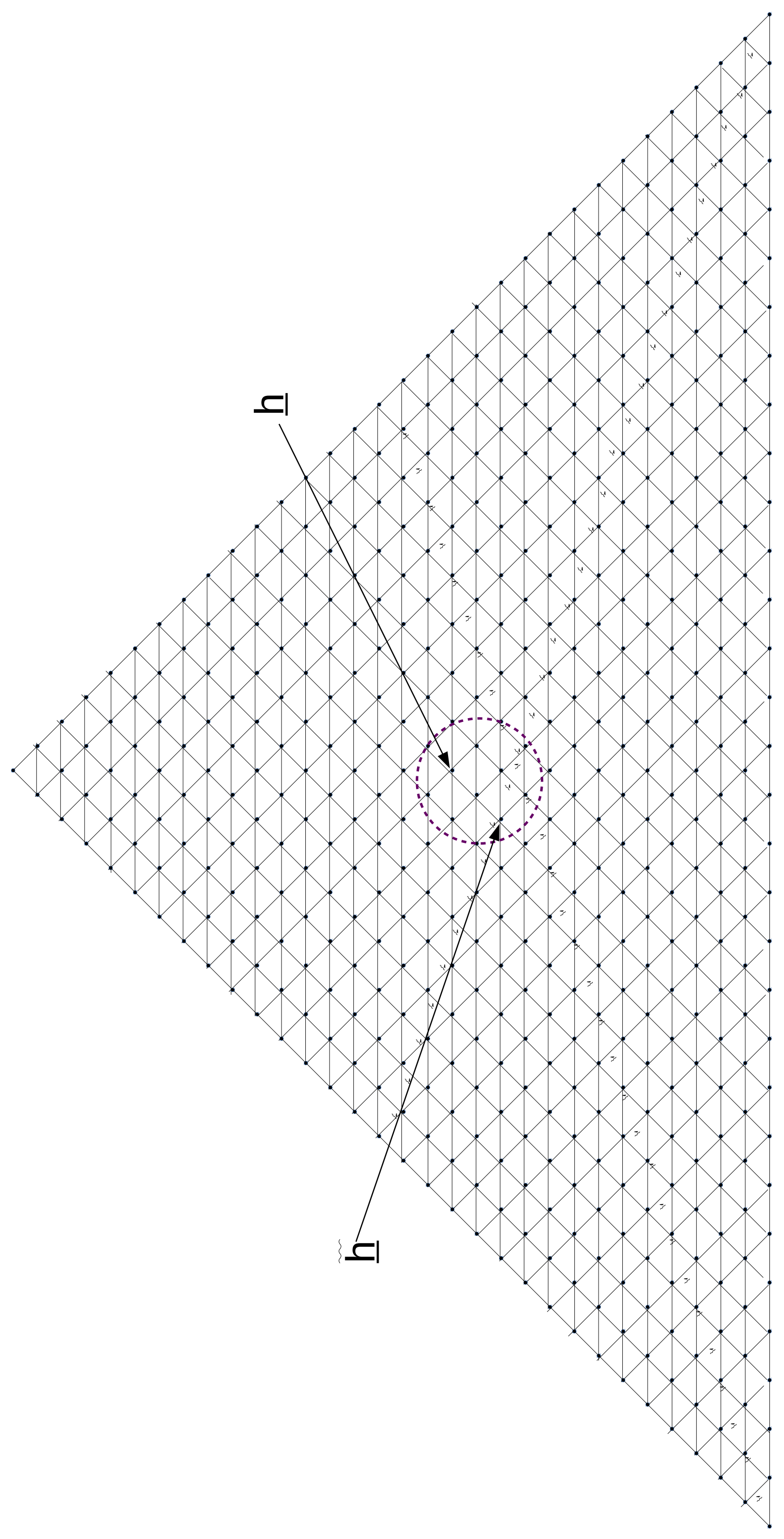


Figure 8. The dotted circle within which the distance distribution of nodes is considered.

overcomes the issue of $E_{\underline{h}}(\theta)$ being variant with $\underline{h}$. An 'extended histogram' is then remapped back to a histogram $\underline{h} \in \mathcal{H}^n$ via the truncation mechanism $\mathbb{V}^n$. $\mathbb{V}^n(\cdot|\cdot)$ is so chosen such that effective expected $\mathbb{L}_1-$distortion does not increase, in the limit. Reserving these elements to the proof, we put forth a heuristic limiting argument that explains the effective distortion of the cascade mechanism in Figure 4. As $n \to \infty$, we noted that $N_d(\underline{h}) \to N_d$ and becomes invariant with $\underline{h}$, and hence it is plausible that (i) $E_{\underline{h}}(\theta) \to \mathscr{E}_{\mathcal{P},f}(\theta)$, where $\mathscr{E}_{\mathcal{P},f}(\theta) : = 1+\sum_{d=1}^{\infty} N_d\theta^d = (1-\theta)\mathrm{Ehr}_{\mathcal{P}}$, and (ii) $\mathbb{W}_{\mathscr{G}}(\underline{g}|\underline{h}) \to (\mathscr{E}_{\mathcal{P},f}(\theta))^{-1}\theta^{d_G(\underline{g},\underline{h})}$. We substitute this in the RHS of (11), to obtain

$$
\begin{aligned}
\lim_{n\to\infty} D^n(\mathbb{W}_{\mathscr{G}}, \underline{p}) &= \lim_{n\to\infty} \sum_{\underline{h}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \sum_{d\geq 1} 2d \sum_{\substack{\underline{g}\in\mathcal{H}^n: \\ d_G(\underline{g},\underline{h})=d}} \frac{\theta^{d_G(\underline{g},\underline{h})}}{\mathscr{E}_{\mathcal{P},f}(\theta)} \\
&= \lim_{n\to\infty} \sum_{\underline{h}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \sum_{d\geq 1} \frac{2dN_d\theta^d}{\mathscr{E}_{\mathcal{P},f}(\theta)} = \lim_{n\to\infty} \sum_{\underline{h}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \lim_{n\to\infty} \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta}, \qquad (17) \\
&= \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \frac{2\theta}{\mathrm{Ehr}_{\mathcal{P}}(\theta)} \frac{d\mathrm{Ehr}_{\mathcal{P}}(\theta)}{d\theta} - \frac{2\theta}{1-\theta}, \qquad (18)
\end{aligned}
$$

and the latter quantity is invariant with n, enabling us conclude that

$$
\lim_{n\to\infty} D^n(\mathbb{W}_{\mathscr{G}}, \underline{p}) = \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \frac{2\theta}{\mathrm{Ehr}_{\mathcal{P}}(\theta)} \frac{d\mathrm{Ehr}_{\mathcal{P}}(\theta)}{d\theta} - \frac{2\theta}{1-\theta}. \qquad (19)
$$

In arriving at (17), we used the fact that $\frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \sum_{d\geq 1} dN_d\theta^{d-1}$, and in arriving at (18) we used $\mathscr{E}_{\mathcal{P},f}(\theta) : = 1 + \sum_{d=1}^{\infty} N_d\theta^d = (1-\theta)\mathrm{Ehr}_{\mathcal{P}}$. These informal arguments provide a heuristic explanation for (6) and leaves certain interesting and non-trivial elements, that are addressed in Section IV-A.

Remark 6. We side-stepped the question of identifying a $\theta-$DP mechanism for any $n \in \mathbb{N}$. Characterizing a (truncated) geometric $\theta-$DP mechanism for a general K is non-trivial owing to the presence of multiple boundary vertices, the involved geometry of the PC graph, and lack of an expression for the 'tail' sum.[3] It is also worth noting that the often used technique of enlarging the output space to be continuous followed by a heuristic map does not permit a precise performance characterization. Moreover, as we note in the following proof, we are required to shape the geometric mechanism appropriately to minimize expected distortion.

Next, we show (8). Towards that end, we characterize N_d explicitly. We recognize that an explicit characterization for N_d or $L_{\mathcal{P}}(d)$ will enable us express the power series in (19). In general, characterizing the Ehrhart polynomial of a convex polytope is involved (see [11]). However, in our case we are able to characterize N_d for the cross-polytope $\mathcal{P}_d$ in (7). Recall $N_d = |\mathcal{S}_d|$, where

$$
\mathcal{S}_d : = \mathbb{Z}^K \cap \mathcal{P}_d = \left\{ (x_1, \cdots, x_K) \in \mathbb{Z}^K : \sum_{k=1}^{K} x_k = 0, \sum_{k=1}^{K} |x_k| \leq 2d \right\}.
$$

$\mathcal{S}_d$ can be partitioned into *disjoint* sets based on the coordinates (in set $A_{|P|}$ below) corresponding to its non-negative indices. Let

$$
\begin{aligned}
A_n \quad &: = \quad \left\{ (a_1, \cdots, a_n) \in \mathbb{Z}^n : a_i \geq 0, \sum_{i=1}^{n} a_i = d \right\}, \\
B_m \quad &= \quad \left\{ (b_1, \cdots, b_m) \in \mathbb{Z}^m : b_j < 0, \; -\sum_{j=1}^{m} b_i = d \right\} = \left\{ (b_1, \cdots, b_m) \in \mathbb{Z}^m : b_j > 0 \sum_{j=1}^{m} b_i = d \right\}.
\end{aligned}
$$

[3] The reader is encouraged to construct, via a truncation or otherwise, a $\theta-$DP mechanism analogous to the geometric mechanism, for the case of $K = 3$ and $n = 5$ depicted in Fig. 6, to recognize the non-triviality.

It can be verified that,

$$\mathcal{S}_d = \bigcup_{P\subseteq[K]} A_{|P|} \times B_{K-|P|} = \bigcup_{P\subseteq[K]} A_{K-|P|} \times B_{|P|}.$$

We can now compute $|A_{|P|}|$ and $|B_{|P|}|$. Since

$$\begin{aligned} |A_n| = \binom{d+n-1}{n-1}, |B_m| = \binom{d-1}{m-1}, \text{ we have } N_d &= \sum_{r=1}^{K-1} \binom{K}{r}\binom{d+r-1}{r-1}\binom{d-1}{K-r-1} \\ &= \sum_{r=1}^{K-1} \binom{K}{r}\binom{d+K-r-1}{K-r-1}\binom{d-1}{r-1}, \end{aligned}$$

where the running variable r denotes the cardinality of the (running set) $P \subseteq [K]$. An alternate count can be obtained by explicitly considering the set of zero coordinates. Suppose $0 \leq z \leq K-1$ denotes the number of $0-$coordinates, and p the number of positive co-ordinates, then, for $d \geq 1$, it can be verified that

$$\mathcal{S}_d \;=\; \bigcup_{\substack{Z\subseteq[K]:|Z|\\ \leq K-2}} \; \bigcup_{\substack{P\subseteq[K]\setminus Z:\\ 1\leq|P|\\ \leq K-Z-1}} B_{|P|} \times B_{K-|P|-|Z|}, \text{ and hence } N_d = \sum_{z=0}^{K-2}\sum_{p=1}^{K-z-1} \binom{K}{z}\binom{K-z}{p}\binom{d-1}{p-1}\binom{d-1}{K-z-p-1}.$$

So, we conclude

$$\begin{aligned} \mathscr{E}_{\mathcal{P},f}(\theta) &= 1 + \sum_{d=1}^{\infty}\left\{\sum_{r=1}^{K-1}\binom{K}{r}\binom{d+r-1}{r-1}\binom{d-1}{K-r-1}\right\}\theta^d \qquad (20) \\ &= 1 + \sum_{d=1}^{\infty}\left\{\sum_{r=1}^{K-1}\binom{K}{r}\binom{d+K-r-1}{K-r-1}\binom{d-1}{r-1}\right\}\theta^d \\ &= 1 + \sum_{d=1}^{\infty}\left\{\sum_{z=0}^{K-2}\sum_{p=1}^{K-z-1}\binom{K}{z}\binom{K-z}{p}\binom{d-1}{p-1}\binom{d-1}{K-z-p-1}\right\}\theta^d. \end{aligned}$$

Finally, we show (9). We refer to [22, Eqn (3.8)] for an alternate characterization for N_d. It may be verified that points on the root lattice A_{K-1} at fractional height d in [22] correspond to vertices on the face of $\mathcal{P}_d$ in (14). [22] also refers to these vertices as being at a distance d or d bonds away. From [22, Eqn (3.8)], we have

$$\begin{aligned} N_d &= \sum_{r=1}^{K-1}\binom{K}{r}\binom{d+r-1}{r-1}\binom{d-1}{K-r-1} = \sum_{j=0}^{K-1}\left[\binom{K-1}{j}\right]^2\binom{d+K-j-2}{K-2} \\ &= \sum_{j=0}^{K-1}\left[\binom{K-1}{j}\right]^2\binom{d+K-j-2}{d-j}. \qquad (21) \end{aligned}$$

We now use RHS of (21) to conclude

$$\begin{aligned} \mathscr{E}_{\mathcal{P},f}(\theta) = 1 + \sum_{d\geq1}\theta^d\left\{\sum_{j=1}^{K-1}\binom{K}{j}\binom{d+j-1}{j-1}\binom{d-1}{K-j-1}\right\} &= \sum_{l\geq0}\theta^l\left\{\sum_{j=0}^{k-1}\binom{l-j+K-2}{l-j}\left[\binom{K-1}{j}\right]^2\right\} \\ = \sum_{l\geq0}\binom{l+K-2}{l}\left\{\sum_{j=0}^{K-1}\left[\binom{K-1}{j}\right]^2\theta^{j+l}\right\} &= \frac{\sum_{j=0}^{K-1}\left[\binom{K-1}{j}\right]^2\theta^j}{(1-\theta)^{K-1}} = \frac{S_{K-1}(\theta)}{(1-\theta)^{K-1}}. \qquad (22) \end{aligned}$$

Substituting (22) in (19), we obtain (9).

We identify a sequence of upper bounds $D_n^u(\theta) \geq D_*^n(\theta, \underline{p}) : n \in \mathbb{N}$ and characterize the corresponding limit $\lim_{n\to\infty} D_n^u(\theta)$ to obtain an upper bound on $D_K^*(\theta, \underline{p})$. For this, we identify a sequence $\mathbb{W}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n : n \in \mathbb{N}$ of $\theta-$DP HSMs and let $D_n^u(\theta) := D(\mathbb{W}^n, \underline{p})$.

In view of Remark 6, we propose $\mathbb{W}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n$ as a cascade of mechanisms $\mathbb{U}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n_{\text{ext}}$ and $\mathbb{V}^n : \mathcal{H}^n_{\text{ext}} \Rightarrow \mathcal{H}^n$. See Figure 4. $\mathbb{U}^n$ is a geometric mechanism and outputs 'histograms' from an 'enlarged set of histograms'. This overcomes technical obstacles mentioned in Remark 6. $\mathbb{V}^n$ takes as input only the output of $\mathbb{U}^n$, and remaps $\mathcal{H}^n_{\text{ext}}$ to $\mathcal{H}^n$. More importantly, it shapes the joint distribution to minimize the expected distortion. Since a geometric mechanism is, in general, optimal in most DP settings, and $\mathbb{V}^n$ is carefully shaped, we obtain a reasonably good sequence $\mathbb{W}^n$ of mechanisms that is, in the limit, optimal.

In establishing the upper bound, we first specify mechanisms $\mathbb{U}^n$, $\mathbb{V}^n$ and characterize the distortion $D(\mathbb{U}^n)$ of $\mathbb{U}^n$. Next, we relate $D(\mathbb{W}^n, \underline{p})(= D^u_n(\theta))$ to $D(\mathbb{U}^n)$ and thereby characterize the former as an upper bound.

We take a clue from (16) and Remark 6. The normalizing terms $E_{\underline{h}}(\theta)$, $E_{\underline{\tilde{h}}}(\theta)$ differ because the tails of the sequences $N_d(\underline{h}) : d \geq 1$ and $N_d(\underline{\tilde{h}}) : d \geq 1$ differ. The latter is due to the presence of the boundary of $\mathcal{H}^n$ (or the PC graph). We enlarge $\mathcal{H}^n$ to eliminate the boundary. This we do by getting rid of the non-negativity constraint in (1). The enlarged 'set of histograms' is therefore $\mathcal{H}^n_{\text{ext}} := \{(h_1, \cdots, h_K) \in \mathbb{Z}^K : \sum_{k=1}^K h_k = n\}$. $\mathcal{H}^n_{\text{ext}}$ is isomorphic to $\{\underline{z} \in \mathbb{Z}^K : \sum_{k=1}^K z_k = 0\}$ and

$$N_d := \left| \{\underline{z} \in \mathbb{Z}^k : \sum_{k=1}^K z_k = 0, |\underline{z}|_1 = 2d\} \right|, \tag{23}$$

defined identical to (13), is the number of 'extended histograms' at an $\mathbb{L}_1$ distance of $2d$ from *any* element in $\mathcal{H}^n_{\text{ext}}$. N_d being invariant with $\underline{h}$, we define a $\theta-$DP mechanism $\mathbb{U}^n : \mathcal{H}^n \Rightarrow \mathcal{H}^n_{\text{ext}}$ analogous to the geometric mechanism in (16) as

$$\mathbb{U}^n(\underline{g}|\underline{h}) = \left(\mathscr{E}_{\mathcal{P},f}(\theta)\right)^{-1} \theta^{\frac{|\underline{g}-\underline{h}|_1}{2}}, \tag{24}$$

where $\mathcal{P}$ is the convex polytope whose $d^{th}-$dilation is

$$\mathcal{P}_d = \{(x_1, \cdots, x_K) \in \mathbb{R}^K : \sum_{k=1}^K x_k = 0, \sum_{k=1}^K |x_k| \leq 2d\}.$$

In order to prove $\mathbb{W}^n$ is $\theta-$DP, it suffices to prove $\mathbb{U}^n$ is $\theta-$DP. Indeed, by the post-processing theorem of DP, so long as $\mathbb{V}^n : \mathcal{H}^n_{\text{ext}} \Rightarrow \mathcal{H}^n$ takes only the output of $\mathbb{U}^n$ as input, the cascade mechanism $\mathbb{W}^n$ is $\theta-$DP. It is straightforward to prove that $\mathbb{U}^n$ is $\theta-$DP, and the steps are provided in Appendix F.

Before we identify $\mathbb{V}^n(\cdot|\cdot)$, let us characterize the distortion of $\mathbb{U}^n$. Let

$$D(\mathbb{U}^n) := \sum_{\underline{h} \in \mathcal{H}^n} \sum_{\underline{g} \in \mathcal{H}^n_{\text{ext}}} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} |\mathbb{U}^n(\underline{g}|\underline{h})\underline{g} - \underline{h}|_1 \tag{25}$$

denote the distortion of $\mathbb{U}^n$. From (24), (25), we have

$$\begin{aligned} D(\mathbb{U}^n) &= \sum_{\underline{h} \in \mathcal{H}^n} \sum_{\underline{g} \in \mathcal{H}^n_{\text{ext}}} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{U}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 = \sum_{\underline{h} \in \mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \sum_{\underline{g} \in \mathcal{H}^n_{\text{ext}}} \frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)} \theta^{\frac{|\underline{g}-\underline{h}|_1}{2}} |\underline{g} - \underline{h}|_1 \\ &= \sum_{\underline{h} \in \mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)} \sum_{d \geq 1} \sum_{\substack{\underline{g} \in \mathcal{H}^n_{\text{ext}} \\ |\underline{g}-\underline{h}|_1 = 2d}} 2d\theta^d = \sum_{\underline{h} \in \mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)} \sum_{d \geq 1} 2dN_d\theta^d \\ &= \sum_{\underline{h} \in \mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta}, \end{aligned} \tag{26}$$

where (26) follows from steps identical to those that lead to (18).

The choice of $\mathbb{V}^n$ is based on the fact that the DBs whose histograms differ widely from the mean histogram $n\underline{p}$ contribute an exponentially (in n) small amount to the expected value. $\mathbb{V}^n$ maps the histogram outside the $\mathbb{L}_1-$ball of radius $Rn^{\frac{2}{3}}$ centered at $n\underline{p}$ to the histogram $n\underline{p}$. The histograms within radius $Rn^{\frac{2}{3}}$ of $n\underline{p}$ remain unchanged. Formally, let

$$\mathbb{V}^n(\underline{g}|\underline{h}) = 1 \text{ if } \underline{g} = \underline{h}, |\underline{h} - n\underline{p}|_1 \leq Rn^{\frac{2}{3}}, \quad \mathbb{V}^n(\underline{g}|\underline{h}) = 1 \text{ if } \underline{g} = n\underline{p}, |\underline{h} - n\underline{p}|_1 > Rn^{\frac{2}{3}},$$

and $\mathbb{V}^n(\underline{g}|\underline{h}) = 0$ otherwise. For completeness, we also note $\mathbb{W}^n(\underline{g}|\underline{h}) = \sum_{\underline{b} \in \mathcal{H}^n_{\text{ext}}} \mathbb{V}^n(\underline{g}|\underline{b})\mathbb{U}^n(\underline{b}|\underline{h})$.

Does $\mathbb{V}^n$ output a histogram in $\mathcal{H}^n$? The output of $\mathbb{V}^n$ is contained within a $\mathbb{L}_1-$ball of radius $\alpha_n = Rn^{\frac{2}{3}}$ centered at $n\underline{p} \in \mathcal{H}^n$. The boundary of $\mathcal{H}^n$ is at a $\mathbb{L}_1-$distance of at least $\beta_n = \min_{k=1,\cdots,K} np_k$ from $n\underline{p} \in \mathcal{H}^n$. Since $p_k > 0$ for all $k \in [K]$, as $n \to \infty$, $\alpha_n \leq \beta_n$, and the range of $\mathbb{V}^n$ is contained within $\mathcal{H}^n$. The output of mechanism $\mathbb{V}^n$ is indeed a histogram. We provide a formal proof below.

We recall $\mathbb{V}^n : \mathcal{H}^n_{\text{ext}} \to \mathcal{H}^n$ is defined as

$$\mathbb{V}^n(\underline{g}|\underline{h}) = \begin{cases} 1 & \text{if } \underline{g} = \underline{h}, |\underline{h} - n\underline{p}|_1 \leq Rn^{\frac{2}{3}} \\ 1 & \text{if } \underline{g} = n\underline{p}, |\underline{h} - n\underline{p}|_1 > Rn^{\frac{2}{3}}, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and } \mathbb{W}^n(\underline{g}|\underline{h}) = \sum_{\underline{b}\in\mathcal{H}^n} \mathbb{V}^n(\underline{g}|\underline{b})\mathbb{U}^n(\underline{b}|\underline{h}),$$

where $R > 0$ is any constant invariant with n. Since $\mathbb{V}^n$ is a deterministic map, it can also be defined through the map $f_{\mathbb{V}^n} : \mathcal{H}^n_{\text{ext}} \Rightarrow \mathcal{H}^n$ where

$$f_{\mathbb{V}^n}(\underline{h}) = \begin{cases} \underline{h} & \text{if } |\underline{h} - n\underline{p}|_1 \leq Rn^{\frac{2}{3}} \\ n\underline{p} & \text{otherwise, i.e., } |\underline{h} - n\underline{p}|_1 > Rn^{\frac{2}{3}}, \end{cases} \quad \text{and } \mathbb{V}^n(\underline{g}|\underline{h}) = \mathbb{1}_{\{\underline{g}=f_{\mathbb{V}^n}(\underline{h})\}},$$

where $R > 0$ is a constant, invariant with n. Let us analyze what 'extended histograms' are within the range of $f_{\mathbb{V}^n}$. $\underline{h} \in \mathcal{H}^n_{\text{ext}}$ falls in the range of $f_{\mathbb{V}^n}$, or in other words, is output by mechanism $\mathbb{V}^n$ only if $|\underline{h} - n\underline{p}| \leq Rn^{\frac{2}{3}}$, which is true only if $|h_k - np_k| \leq Rn^{\frac{2}{3}}$. The latter is equivalent to $np_k - Rn^{\frac{2}{3}} \leq h_k \leq np_k + Rn^{\frac{2}{3}}$ for every $k \in [K]$. Observe that, since we assumed $p_k > 0$ for all $k \in [K]$, the lower bound $np_k - Rn^{\frac{2}{3}} > 0$ for any $R > 0$ and sufficiently large n. For sufficiently large n, $\mathbb{V}^n$ outputs an extended histogram whose coordinates are non-negative. From (1), and the definition $\mathcal{H}^n_{\text{ext}}$, the output of $\mathbb{V}^n$ is indeed a histogram from $\mathcal{H}^n$. Observe that, since we assumed $p_k > 0$ for all $k = 1, 2 \cdots, K$, we have $np_i - Rn^{\frac{2}{3}} > 0$ for any R and sufficiently large n. Hence, for sufficiently large n, the output of mechanism $\mathbb{V}^n$ is indeed a histogram.

We now prove that $\lim_{n\to\infty} D(\mathbb{W}^n, \underline{p}) \leq \lim_{n\to\infty} D(\mathbb{U}^n)$. We describe the arguments before we provide the mathematical steps. Let $D_{\underline{h}}(\mathbb{W}^n) = \sum_{\underline{g}\in\mathcal{H}^n} \mathbb{W}^n(\underline{g}|\underline{h})|\underline{g} - \underline{h}|_1$, $D_{\underline{h}}(\mathbb{U}^n) = \sum_{\underline{g}\in\mathcal{H}^n_{\text{ext}}} \mathbb{U}^n(\underline{g}|\underline{h})|\underline{g} - \underline{h}|_1$ denote (unweighted) contributions of $\underline{h}$ to $D(\mathbb{W}^n, \underline{p})$ and $D(\mathbb{U}^n)$ respectively. Refer to Fig. 9. Let $B(\frac{1}{2})$ and $B(1)$ be the $\mathbb{L}_1-$balls centered at $n\underline{p}$ of radii $\frac{R}{2}n^{\frac{2}{3}}$ and $Rn^{\frac{2}{3}}$ respectively. Let $B^c(1) := \mathcal{H}^n_{\text{ext}} \setminus B(1)$. For each $\underline{h} \in B(\frac{1}{2})$, the mechanism $\mathbb{V}^n$ has the effect of decreasing $\underline{h}$'s contribution. In other words, for any $\underline{h} \in B(\frac{1}{2})$, $D_{\underline{h}}(\mathbb{W}^n) \leq D_{\underline{h}}(\mathbb{U}^n)$. This is because (i) $\mathbb{V}^n$ transfers mass placed on $\tilde{g} \in B^c(1)$ - an element farther from $n\underline{p}$ - to $n\underline{p}$, and (ii) $\mathbb{V}^n$ does not alter the mass placed on elements $\underline{g} \in B(1)$ (other than $n\underline{p}$).[4] What about for $\underline{h} \in B^c(\frac{1}{2})$? The weights $\binom{n}{\underline{h}}\underline{p}^{\underline{h}}$ associated with these elements, when summed up, contribute an exponentially small amount. Formally, $\sum_{\underline{h}\in B^c(\frac{1}{2})} \binom{n}{\underline{h}}\underline{p}^{\underline{h}} \leq \exp\{-n\alpha\}$ for some $\alpha > 0$. Since $|\underline{g} - \underline{h}|_1 \leq 2n$ whenever $\underline{h}, \underline{g}\ in\mathcal{H}^n$, we have $D(\mathbb{W}^n, \underline{h}) \leq 2n\exp\{-\alpha n\}$ and hence $\sum_{\underline{h}\in B^c(\frac{1}{2})} \binom{n}{\underline{h}}\underline{p}^{\underline{h}} D(\mathbb{W}^n, \underline{h}) \to 0$ as $n \to 0$. We flesh out these details in Appendix G.

From (26), (18) it suffices to characterize either the Ehrhart series $\text{Ehr}_{\mathcal{P}}(\theta)$ or $\mathscr{E}_{\mathcal{P},f}(\theta)$, of $\mathcal{P} = \mathcal{P}_1$, where $\mathcal{P}_d$ is the polytope characterized in (14). From (22), we conclude

$$D^*_K(\theta, \underline{p}) \leq \frac{2\theta}{\mathscr{E}_{\mathcal{P},f}(\theta)} \frac{d\mathscr{E}_{\mathcal{P},f}(\theta)}{d\theta} = \mathscr{D}_K(\theta) : = 2\theta \left\{ \frac{K-1}{1-\theta} + \frac{S'_{K-1}(\theta)}{S_{K-1}(\theta)} \right\}. \tag{27}$$

Remark 7. Observe that $\mathbb{U}^n$ is invariant with $\underline{p}$, and $\mathbb{V}^n$ is a remapping mechanism that depends on $\underline{p}$ and reduces the expected distortion for histograms of high probability. In order to prove Theorem 2, it suffices to prove the lower bound, i.e., the reverse inequality in (27).

B. Lower Bound

Our proof of the lower bound is via the weak duality theorem. The weak duality theorem states that every feasible solution to the dual LP evaluates to a lower bound on the primal optimal. The reader is referred to Appendix E for precise statement of the WDT in the context of our problem. Consider the dual of the LP in (5). If we can identify a dual feasible solution whose objective value evaluates to C^n_* and $\lim_{n\to\infty} C^n_* = \mathscr{D}_K(\theta)$ defined in (27), then we would have proved Theorem 1. This is our approach. Towards, this end we begin by identifying the dual of the LP in (5).

[4] This is made precise in the sequence of steps (53) - (55) below.

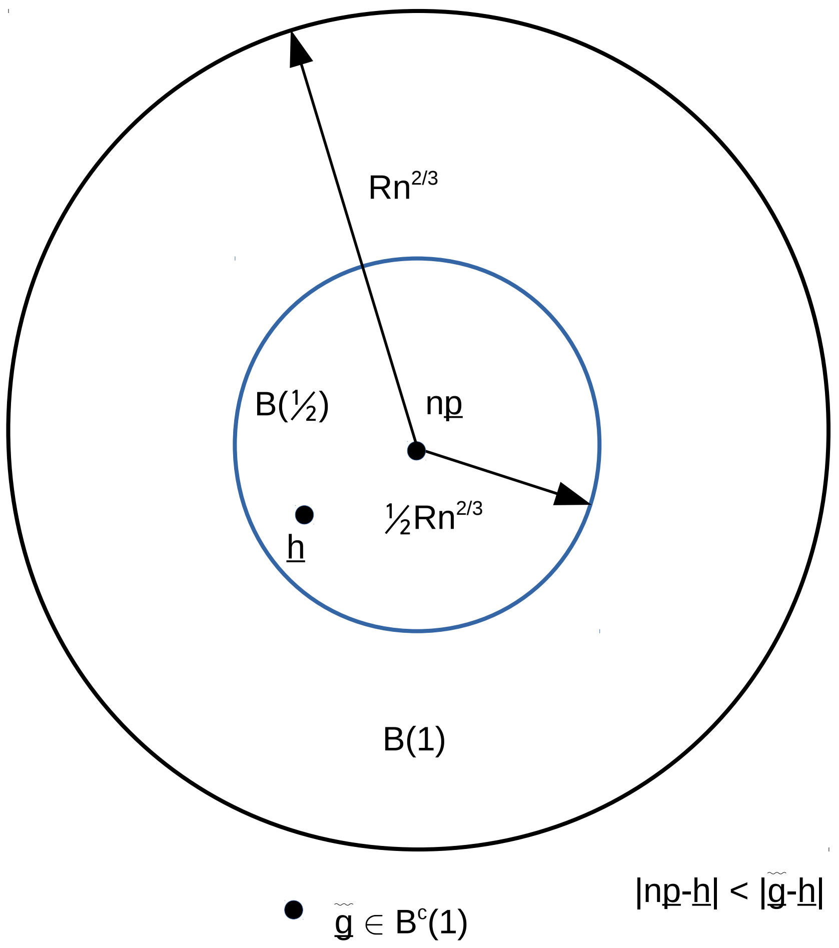


Figure 9.

Associated to each DP constraint (4(b)), we have a non-negative dual variable $\lambda_{\underline{g}|(\underline{h},\hat{\underline{h}})}$. Note that $\lambda_{\underline{g}|(\underline{h},\hat{\underline{h}})}$ and $\lambda_{\underline{g}|(\hat{\underline{h}},\underline{h})}$ are distinct dual variables. Associated to each sum constraint (4) we have a free dual variable $\mu_{\underline{h}}$. It can be verified that the dual of (5) is

$$S_*^n(\theta) := \max \sum_{\underline{h}\in\mathcal{H}^n} \mu_{\underline{h}} \text{ subject to (i) } \mu_{\underline{h}} \leq \binom{n}{\underline{h}} \underline{p}^{\underline{h}} |\underline{h}-\underline{g}|_1 + \theta \sum_{\hat{\underline{h}}\in\mathcal{N}(\underline{h})} \lambda_{\underline{g}|(\hat{\underline{h}},\underline{h})} - \sum_{\tilde{\underline{h}}\in\mathcal{N}(\underline{h})} \lambda_{\underline{g}|(\underline{h},\tilde{\underline{h}})} \text{ for } (\underline{h},\underline{g}) \in \mathcal{H}^n \times \mathcal{H}^n \text{ and (ii) } \lambda_{\underline{g}|(\hat{\underline{h}},\underline{h})} \geq 0 \text{ for } \underline{g} \in \mathcal{H}^n \text{ and } (\hat{\underline{h}},\underline{h}) \in \mathcal{H}^n \times \mathcal{H}^n \text{ satisfying } |\underline{h}-\hat{\underline{h}}|_1 = 2, \tag{28}$$

where $\mathcal{N}(\underline{h}) := \{\hat{\underline{h}} \in \mathcal{H}^n : |\underline{h}-\hat{\underline{h}}|_1 = 2\}$ is the set of neighbors of $\underline{h} \in \mathcal{H}^n$. We let $C^n(\underline{\lambda},\underline{\mu}) = \sum_{\underline{h}\in\mathcal{H}^n} \mu_{\underline{h}}$ denote the objective value corresponding to a feasible solution $\underline{\lambda},\underline{\mu}$, where $\underline{\lambda}$ and $\underline{\mu}$ represent the aggregate of $\lambda_{\underline{g}|(\hat{\underline{h}},\underline{h})}$ and $\mu_{\underline{h}}$ variables respectively.

The reader will note that each constraint in the primal LP (4) has translated to a variable in the dual LP (28) and vice versa. We therefore have at least $\mathcal{O}(k^2|\mathcal{H}^n|^2) = \mathcal{O}(k^2(n+1)^{2(k-1)})$ variables (Remark 2). In order to describe the methodology behind the assignment of dual variables and the evaluation of its objective value, we first focus on the $K = 2$ case. For this case, we provide a complete solution, i.e., identify a pair of primal and dual feasible solutions that satisfy complementary slackness conditions. This enables us to glean the structure of an optimal dual feasible solution. We leverage this structure in providing an assignment for the general K case. Specifically, we provide an interpretation of the dual feasible assignment via shadow prices (Appendix I) which naturally leads us to the assignment for the general K case.

The $K = 2$ **case**: We identify the histogram $(i, n-i) \in \mathcal{H}_2^n$ with just its first co-ordinate. We also let $\mathbb{W}(n-j|i)$ denote $\mathbb{W}((n-j,j)|(i,n-i))$, $\lambda_{j|(i-1,i)}$ denote $\lambda_{(j,n-j)|((i-1,n-i+1),(i,n-i))}$, and so on. With this notational simplification, we state below the primal and dual LPs for $K = 2$.

$$\begin{array}{llc|llc}
 & \text{Primal LP} & & & \text{Dual LP} & \\
\min & \displaystyle\sum_{i=0}^{n}\sum_{j=0}^{n} \mathscr{C}_i^n \mathbb{W}(j|i) 2|j-i| & & \max & \displaystyle\sum_{i=0}^{n} \mu_i & \\
\text{subject to} & \mathbb{W}(j|i) \geq 0, \text{ for all } 0 \leq i, j \leq n & & \text{subject to} & \mu_i \leq \mathscr{C}_i^n 2|j-i| & \\
 & & & & +\theta\lambda_{j|(i-1,i)} + \theta\lambda_{j|(i+1,i)} & \\
 & & & & -\lambda_{j|(i,i-1)} - \lambda_{j|(i,i+1)} & \\
 & \sum_{j=0}^{n} \mathbb{W}(j|i) = 1 \text{ for all } 0 \leq i \leq n & & & \mu_i \text{ is free,} & \\
 & \mathbb{W}(j|i-1) - \theta\mathbb{W}(j|i) \geq 0 \text{ for all } i, j & & & \lambda_{j|(i-1,i)} \geq 0, \text{ for every } i, j & \\
 & \mathbb{W}(j|i+1) - \theta\mathbb{W}(j|i) \geq 0 \text{ for all } i, j, & & & \lambda_{j|(i+1,i)} \geq 0 \text{ for every } i, j, &
\end{array} \tag{29}$$

where $\mathscr{C}_i^n = \binom{n}{i} p_1^i (1-p_1)^{n-i}$. We have suppressed dependence of $\mathscr{C}_i^n$ on p_1. Furthermore, we let $p = p_1$ and $p_2 = 1 - p$. We provide a complete solution, i.e., primal and dual feasible solutions that satisfy complementary slackness conditions. Recall that from complementary slackness, we are required to prove that (i) either the primal constraint is tight or the corresponding dual variable is 0, and (ii) either the primal variable is 0 or the dual constraint is tight. For ease of verification, we have stated variables and constraints that are duals of each other on the same row of (29).

Let us begin with a primal feasible solution. Let $f_i = \sum_{j=0}^{i} 2\mathscr{C}_j^n \theta^{i-j}$, $b_i = \sum_{k=i}^{n} 2\mathscr{C}_k^n \theta^{k-i}$, and[5]

$$A_n := \min\left\{ i \in [0,n] : \begin{array}{c} f_{k-1} - \theta b_k \geq 0 \\ \text{for every } k \geq i \end{array} \right\}, B_n := \max\left\{ i \in [0,n] : \begin{array}{c} b_{k+1} - \theta f_k \geq 0 \\ \text{for every } k \leq i \end{array} \right\}. \tag{30}$$

$A_n - 1$ and $B_n + 1$ will represent the left and right ends of a truncated geometric mechanism which we prove is optimal. In Appendix H, we prove that $A_n < np_1 < B_n$. We use the same in the following assignment. Consider the truncated geometric mechanisms that are folded at $A_n - 1$ on the left and $B_n + 1$ on the right. Specifically, let $\mathbb{U}^n : \mathcal{H}_2^n \Rightarrow \mathcal{H}_{\text{ext}}^n$ and $\mathbb{V}^n : \mathcal{H}_{\text{ext}}^n \Rightarrow \mathcal{H}_2^n$, where $\mathcal{H}_{\text{ext}}^n := \{(i, n-i) : i \in \mathbb{Z}\}$. As stated earlier, we refer to $(i, n-i) \in \mathcal{H}_{\text{ext}}^n$ by its first co-ordinate i. Let

$$\mathbb{U}^n(k|i) = \theta^{|k-i|}\frac{1-\theta}{1+\theta} \text{ for } k \in \mathbb{Z}, i \in [0,n], \quad \mathbb{V}^n(j|i) = \begin{cases} 1 & \text{if } j = i, j \in [A_n - 1, B_n + 1] \\ 1 & \text{if } i \leq A_n - 1, j = A_n - 1 \\ 1 & \text{if } i \geq B_n + 1, j = B_n + 1 \\ 0 & \text{otherwise,} \end{cases} \tag{31}$$

and $\mathbb{W}^n(j|i) = \sum_{k\in\mathbb{Z}} \mathbb{U}^n(k|i)\mathbb{V}^n(j|k)$. It can be verified that

$$\mathbb{W}^n(j|i) = \begin{cases} \theta^{|j-i|}\frac{1-\theta}{1+\theta} & i \in [0,n], j \in [A_n, B_n] \\ \frac{\theta^{|j-i|}}{1+\theta} & j = B_n + 1, i \leq j \\ & \text{or } j = A_n - 1, i \geq j \\ 0 & j \notin [A_n - 1, B_n + 1], \end{cases} \quad \mathbb{W}(j|i) = \begin{cases} 1 - \frac{\theta^{A_n - i}}{1+\theta} & i < A_n - 1, j = A_n - 1 \\ 1 - \frac{\theta^{i-B_n}}{1+\theta} & i > B_n + 1, j = B_n + 1 \\ 0 & \text{otherwise.} \end{cases} \tag{32}$$

It can be easily verified that the above assignment satisfies the constraints in (4). This can be done in either of two ways. The first is just by the fact that $\mathbb{U}^n$ being $\theta-$DP implies $\mathbb{W}^n$ is $\theta-$DP. The second is by verifying that $\mathbb{W}^n$ as assigned in (32) satisfies (4a) and (4b). We leave this to the reader.

What are the complementary slackness conditions with regard to the above primal feasible assignment? We make the following observations with regard to the above assignment. Firstly,

$$\mathbb{W}^n(j|i-1) - \theta\mathbb{W}^n(j|i) > 0 \text{ if } j \leq i-1 \text{ and } \mathbb{W}^n(j|i+1) - \theta\mathbb{W}^n(j|i) > 0 \text{ if } j \geq i+1. \tag{33}$$

Secondly,

$$\theta < \frac{\mathbb{W}(A_n - 1|i)}{\mathbb{W}(A_n - 1|i-1)} < \frac{1}{\theta} \text{ if } i \leq A_n \text{ and similarly } \theta < \frac{\mathbb{W}(B_n + 1|i+1)}{\mathbb{W}(B_n + 1|i)} < \frac{1}{\theta} \text{ if } i \geq B_n + 1.$$

[5] We assume, without loss of generality that $p_1 \leq \frac{1}{2}$

Moreover, for $j \in [A_n - 1, B_n + 1]$, we have $\mathbb{W}^n(j|i) > 0$ and hence the corresponding constraints have to be met with equality in the dual LP. Specifically, our dual feasible assignment must satisfy

$$\mu_i = 2\mathscr{C}_i^n|j-i| + \theta\lambda_{j|(i-1,i)} + \theta\lambda_{j|(i+1,i)} - \lambda_{j|(i,i-1)} - \lambda_{j|(i,i+1)} \text{ for } j \in [A_n - 1, B_n + 1]. \tag{34}$$

We now provide a feasible assignment for the dual variables. Let $\lambda_{A_n-1|(i-1,i)} = 0$ for $i \leq A_n - 1$ and $\lambda_{B_n+1|(i+1,i)} = 0$ for $i \geq B_n + 1$. Let $\lambda_{j|(i-1,i)} = 0$ if $j \leq i - 1$ and $\lambda_{j|(i+1,i)} = 0$ if $j \geq i + 1$.[6] With this, the reader can verify that we have handled the last three rows of (29). We are only left to provide an assignment for the rest of the dual variables that satisfy (34). For $i \in \{1, \cdots, A_n - 1\}$ and $j \in \{i, \cdots, A_n - 1\}$, set $\lambda_{j|(i-1,i)} := 0$.

$$\text{For } i \in \{1, \cdots, A_n - 1\} \text{ and } j \in \{A_n - 1, \cdots, n\}, \text{ set } \lambda_{j|(i-1,i)} := [j - (A_n - 1)]f_{i-1}. \tag{35}$$

$$\text{For } i \in [A_n, n] \text{ and } j \in [i, n], \text{ set } \lambda_{j|(i-1,i)} := \tfrac{f_{i-1} - \theta b_i}{1-\theta^2} + (j-i)f_{i-1}. \tag{36}$$

$$\text{For } i \in [B_n + 1, n-1] \text{ and } j \in [B_n + 1, i], \text{ set } \lambda_{j|(i+1,i)} := 0.$$

$$\text{For } i \in [B_n + 1, n-1] \text{ and } j \in [0, B_n + 1], \text{ set } \lambda_{j|(i+1,i)} := [(B_n + 1) - j]b_{i+1}.$$

$$\text{For } i \in [0, B_n] \text{ and } j \in [0, i], \text{ set } \lambda_{j|(i+1,i)} := \tfrac{b_{i+1} - \theta f_i}{1-\theta^2} + (i-j)b_{i+1}. \text{ For } i < A_n - 1, \text{ set} \tag{37}$$

$$\mu_i = 2\mathscr{C}_i^n|(A_n - 1) - i|, \text{ and } i > B_n + 1, \text{ set } \mu_i = 2\mathscr{C}_i^n|i - (B_n + 1)| \tag{38}$$

$$\text{For } i \in [A_n - 1, B_n + 1], \text{ set } \mu_i := f_i + b_i - \tfrac{4}{(1-\theta^2)}\mathscr{C}_i^n \tag{39}$$

$$\text{For } i \in [A_n - 1, B_n + 1] \text{ verify } \mu_i = \theta(f_{i-1} + b_{i+1}) - \tfrac{4\theta^2}{(1-\theta^2)}\mathscr{C}_i^n. \tag{40}$$

The above assignment is indeed non-trivial. We refer the reader to Appendix I for an interpretation of the above assignment via shadow prices. This interpretation will prove very valuable in arriving at the dual variable assignment for the general K case in (49). We will now use the above assignment to verify (34).

Recall $\mathscr{C}_i^n = \binom{n}{i}p^i(1-p)^{n-i}$. We first prove that for any $i < A_n - 1$, $j \in [A_n - 1, B_n + 1]$,

$$\begin{array}{c}\binom{n}{i}p^i(1-p)^{n-i}2|j-i| + \theta\lambda_{j|(i-1,i)} \\ +\theta\lambda_{j|(i+1,i)} - \lambda_{j|(i,i+1)} - \lambda_{j|(i,i-1)}\end{array} = \binom{n}{i}p^i(1-p)^{n-i}2|(A_n - 1) - i|. \tag{41}$$

Towards that end, note that $\lambda_{j|(i+1,i)} = \lambda_{j|(i,i-1)} = 0$ for the considered values for i, j. Substituting $\lambda_{j|(i-1,i)} = [j - (A_n - 1)]f_{i-1}$ from (35), we have $\theta\lambda_{j|(i-1,i)} - \lambda_{j|(i,i+1)} = [j - (A_n - 1)](\theta f_{i-1} - f_i) = -[j - (A_n - 1)]\binom{n}{i}2p^i(1-p)^{n-i}$, and we therefore have (41). From the assignment (37), (38), we conclude validity of (34) for $i < A_n - 1$. Before we continue, we note that

$$f_i = \theta f_{i-1} + \binom{n}{i}2p^i(1-p)^{n-i}, \quad \text{and} \quad b_i = \theta b_{i+1} + \binom{n}{i}2p^i(1-p)^{n-i}. \tag{42}$$

We now consider upper bounds on μ_i for the range $i \in [A - 1, B + 1], j \in [i + 1, n]$. Substituting (36), (37) and using (42), one can verify that

$$\begin{aligned} \begin{array}{l}\binom{n}{i}p^i(1-p)^{n-i}2|j-i| \\ \\ +\theta\lambda_{j|(i-1,i)} - \lambda_{j|(i,i+1)}\end{array} &= \binom{n}{i}p^i(1-p)^{n-i}2|j-i| + \frac{\theta f_{i-1} - f_i - \theta^2 b_i + \theta b_{i+1}}{1-\theta^2} \\ &\quad +(j-i)(\theta f_{i-1} - f_i) + f_i \\ &= f_i + b_i - \frac{4}{(1-\theta^2)}\binom{n}{i}p^i(1-p)^{n-i}. \end{aligned} \tag{43}$$

Similarly, for $i \in [A - 1, B + 1], j \in [0, i - 1]$, one can substitute (36), (37) and use (42) to establish

$$\begin{aligned} \begin{array}{l}\binom{n}{i}p^i(1-p)^{n-i}2|j-i| \\ \\ +\theta\lambda_{j|(i+1,i)} - \lambda_{j|(i,i-1)}\end{array} &= \binom{n}{i}p^i(1-p)^{n-i}2|j-i| + \frac{\theta b_{i+1} - \theta^2 f_i - b_i + \theta f_{i-1}}{1-\theta^2} \\ &\quad +(i-j)(\theta b_{i+1} - b_i) + b_i \\ &= f_i + b_i - \frac{4}{(1-\theta^2)}\binom{n}{i}p^i(1-p)^{n-i}. \end{aligned} \tag{44}$$

[6] For the general K, we will assign $\lambda_{\underline{g}|(\underline{\hat{h}},\underline{h})} = 0$ if $|\underline{g} - \underline{\hat{h}}|_1 \leq |\underline{g} - \underline{h}|_1$. Note that this simple observation halves the number of decision variables.

Suppose $i \in [A-1, B+1]$ and $j = i$; the upper bound on μ_i is

$$\begin{aligned} \theta\lambda_{i|(i-1,i)} + \theta\lambda_{i|(i+1,i)} &= \frac{\theta f_{i-1} - \theta^2 b_i + \theta b_{i+1} - \theta^2 f_i}{1-\theta^2} \\ &= \theta f_{i-1} + \theta b_{i+1} - \frac{4\theta^2}{(1-\theta^2)}\binom{n}{i} p^i (1-p)^{n-i}. \end{aligned} \tag{45}$$

The expressions in (43), (44) and (45) being equal to the assignment (39) for μ_i in the range $i \in [A-1, B+1]$, we conclude validity of (34). We are left to prove validity of (34) for $i \geq B_n + 1$. This is similar to (41). Substituting (38), one can verify that

$$\begin{array}{c} \binom{n}{i}p^i(1-p)^{n-i}2|j-i| + \theta\lambda_{j|(i-1,i)} \\ +\theta\lambda_{j|(i+1,i)} - \lambda_{j|(i,i+1)} - \lambda_{j|(i,i-1)} \end{array} = \binom{n}{i}p^i(1-p)^{n-i}2|i-(B_n+1)|. \tag{46}$$

From the assignment for μ_i in (38) for $i > B_n+1$, we have the validity of (34) for $i > B_n+1$. We have thus proved the validity of (34) for all values of i and $j \in [A_n-1, B_n+1]$. The non-negativity of $\lambda_{j|(i-1,i)}$ and $\lambda_{j|(i+1,i)}$ follows from (i) definition of A_n, B_n, and (ii) non-negativity of f_i, b_i. We have thus proved that the above assignments are valid primal and feasible assignments and satisfy complementary slackness conditions. We only need to evaluate the objective of one of these values and prove that it tends to $\frac{4\theta}{1-\theta^2}$ in the limit $n \to \infty$.

It is easier to evaluate the objective value of the above feasible dual assignment. Substituting (39), (38), we have

$$\begin{aligned} C^n(\underline{\lambda}, \underline{\mu}) = \sum_{i=0}^{n} \mu_i = \sum_{i=A_n-1}^{B_n+1} (f_i + b_i) + \sum_{i<A_n-1} \binom{n}{i} p^i(1-p)^{n-i} 2|A_n - 1 - i| \\ + \sum_{i>B_n+1} \binom{n}{i} p^i (1-p)^{n-i} 2|i - B_n - 1| - \frac{4}{(1-\theta^2)} \sum_{A_n-1}^{B_n+1} \mathscr{C}_i^n \\ \geq \sum_{i=0}^{n}(f_i+b_i) - \frac{4}{(1-\theta^2)} - \sum_{i=0}^{A_n-2}(f_i+b_i) - \sum_{i=B_n+2}^{n}(f_i+b_i). \end{aligned}$$

We focus on the first term above:

$$\begin{aligned} \sum_{i=0}^{n}(f_i+b_i) &= 2\sum_{i=0}^{n}\sum_{j=0}^{i}\binom{n}{j}p^j(1-p)^{n-j}\theta^{i-j} + 2\sum_{i=0}^{n}\sum_{k=i}^{n}\binom{n}{k}p^k(1-p)^{n-k}\theta^{k-i} \\ &= 2\sum_{j=0}^{n}\sum_{i=j}^{n}\binom{n}{j}p^j(1-p)^{n-j}\theta^{i-j} + 2\sum_{k=0}^{n}\sum_{i=0}^{k}\binom{n}{k}p^k(1-p)^{n-k}\theta^{k-i} \\ &= 2\sum_{j=0}^{n}\binom{n}{j}p^j(1-p)^{n-j}\frac{1-\theta^{n-j+1}}{1-\theta} + 2\sum_{k=0}^{n}\binom{n}{k}p^k(1-p)^{n-k}\frac{1-\theta^{k+1}}{1-\theta} \\ &= \frac{4}{1-\theta} - \frac{2\theta^{n+1}}{1-\theta}\mathbb{E}\{\theta^{-X_n}\} - \frac{2\theta}{1-\theta}\mathbb{E}\{\theta^{X_n}\}, \end{aligned}$$

where X_n is a Bernoulli RV with parameters n, p. Since $\mathbb{E}\left\{\theta^{X_n}\right\} \cong (p\theta + (1-p))^n \underset{n\to\infty}{\to} 0$, we[7] have $\lim_{n\to\infty}\sum_{i=0}^{n}(f_i+b_i) = \frac{4}{1-\theta}$. We therefore have

$$\lim_{n\to\infty} C^n(\underline{\lambda},\underline{\mu}) \geq \frac{4\theta}{1-\theta^2} - \lim_{n\to\infty}\sum_{i=0}^{A_n-2}(f_i+b_i) - \lim_{n\to\infty}\sum_{i=B_n+2}^{n}(f_i+b_i) = \frac{4\theta}{1-\theta^2}. \tag{47}$$

In arriving at (47), we have used $np - A_n = B_n - np = O(\sqrt{n})$ and standard results in concentration of binomial probabilities. This concludes the proof for the case $K = 2$. A step-by-step proof of (47) is provided in [23].

We now leverage the shadow price interpretation provided in Appendix I to provide an assignment for general K. The proof of feasibility of the following assignment follows from arguments analogous to those presented in Eqns. (41) - (45) for the $K = 2$ case.

[7] Recall that $\theta \in (0, 1)$.

Refer to Appendix D for definition of the PC graph G and its properties. For $\underline{a} \in \mathcal{H}^n$, let $\mathcal{N}(\underline{a}) := \{\underline{\hat{a}} \in \mathcal{H}^n : |\underline{a} - \underline{\hat{a}}|_1 = 2\}$ be the set of neighbors of $\underline{a}$. For $\underline{a}, \underline{b} \in \mathcal{H}^n$, let

$$\mathcal{F}(\underline{b}, \underline{a}) := \{\underline{\tilde{a}} \in \mathcal{N}(\underline{a}) : |\underline{b} - \underline{\tilde{a}}|_1 > |\underline{b} - \underline{a}|_1\}, \mathcal{C}(\underline{b}, \underline{a}) := \{\underline{\tilde{a}} \in \mathcal{N}(\underline{a}) : |\underline{b} - \underline{\tilde{a}}|_1 < |\underline{b} - \underline{a}|_1\}$$
$$\text{and } \mathcal{E}(\underline{b}, \underline{a}) := \{\underline{\tilde{a}} \in \mathcal{N}(\underline{a}) : |\underline{b} - \underline{\tilde{a}}|_1 = |\underline{b} - \underline{a}|_1\}$$

be the set of histograms farther to, closer to, and at equidistant from $\underline{b}$ than $\underline{a}$ respectively. Recall that $2d_G(\underline{a}, \underline{b}) = |\underline{a} - \underline{b}|_1$ (Lemma 3). Complementary slackness conditions imply

$$\lambda_{\underline{g}|(\underline{h}, \underline{\hat{h}})} = 0 \text{ whenever } |\underline{g} - \underline{\hat{h}}|_1 > |\underline{g} - \underline{h}|_1. \tag{48}$$

When $|\underline{g} - \underline{\hat{h}}|_1 < |\underline{g} - \underline{h}|_1$, let

$$\lambda_{\underline{g}|(\underline{h}, \underline{\hat{h}})} = \frac{\displaystyle\sum_{\underline{a} \in \mathcal{C}(\underline{h}, \underline{\hat{h}})} \binom{n}{\underline{a}} \underline{p}^{\underline{a}}\ 2\ \theta^{d_G(\underline{a}, \underline{h})} - \theta \sum_{\underline{b} \in \mathcal{C}(\underline{\hat{h}}, \underline{h})} \binom{n}{\underline{b}} \underline{p}^{\underline{b}}\ 2\ \theta^{d_G(\underline{\hat{h}}, \underline{b})}}{1 + |\mathcal{C}(\underline{h}, \underline{\hat{h}})|\theta^2 - (K(K-1))\theta^2 + \theta|\mathcal{E}(\underline{h}, \underline{\hat{h}})|} + |\underline{g} - \underline{h}|_1 \sum_{\underline{a} \in \mathcal{C}(\underline{h}, \underline{\hat{h}})} \binom{n}{\underline{a}} \underline{p}^{\underline{a}}\ \theta^{d_G(\underline{a}, \underline{h})} \tag{49}$$

$$\mu_{\underline{g}} = \frac{\displaystyle\theta \sum_{\underline{h} \in \mathcal{N}(\underline{g})} \left\{ \sum_{\underline{a} \in \mathcal{C}(\underline{h}, \underline{g})} \binom{n}{\underline{a}} \underline{p}^{\underline{a}}\ 2\ \theta^{d_G(\underline{a}, \underline{h})} - \theta \sum_{\underline{b} \in \mathcal{C}(\underline{g}, \underline{h})} \binom{n}{\underline{b}} \underline{p}^{\underline{b}}\ 2\ \theta^{d_G(\underline{h}, \underline{b})} \right\}}{1 + |\mathcal{C}(\underline{h}, \underline{\hat{h}})|\theta^2 - (K(K-1))\theta^2 + \theta|\mathcal{E}(\underline{h}, \underline{\hat{h}})|}. \tag{50}$$

Having provided the above assignments, the natural question that arises is whether these are feasible for (28), and if yes, what do they evaluate to? A couple of remarks are in order. The first term in (49) is negative if $\underline{g} = \underline{\hat{h}}$, $|\underline{\hat{h}} - n\underline{p}| > |\underline{h} - n\underline{p}| + 2$ and $|\underline{\hat{h}} - n\underline{p}| > \Theta(\sqrt{n})$. This is the case analogous to (35). Therein, note that when $i \in [A, B]$, the assignment is (36). In fact, the fraction in (49) is analogous to the fraction in (36). The reader will recognize $\mathcal{E}(\underline{h}, \underline{\hat{h}}) = 0$ and $\mathcal{C}(\underline{h}, \underline{\hat{h}}) = \mathcal{F}(\underline{h}, \underline{\hat{h}}) = 1$. The first term in the numerator of the fraction in (49) is analogous to f_{i-1} in (36). The rest of the terms can also be related to the assignment in (35) - (39). The above assignment is a slightly simplified version, in the sense that the variables corresponding to non-active constraints have been ignored. Appendix I provides a clear interpretation for the above assignment for $K = 2$. An analogous argument to our thorough description for the $K = 2$ case, its feasibility and the evaluation of its objective value completes the proof.

V. Concluding Remarks

Our work is aimed at initiating a systematic information theoretic study of the fundamental trade-off between the utility lost and the privacy preserved in any data obfuscation mechanism. It is addressed in the information theoretic spirit by characterizing the expected fidelity in the asymptotic regime of large databases. In this work, we have adopted DP as the framework to quantify the vulnerability of the obfuscated data to privacy breaches. Our measure of utility - the $\mathbb{L}_1-$distance measure between the histograms - is simple and yet provides us with an ideal setting to put forth the connections between DP, Ehrhart theory, analytic combinatorics and linear programming.

Going further, one may ask questions at two different levels. At a technical level, it would be interesting to build on the following questions and provide suitable answers. Can one derive simple closed form computable expressions characterizing the utility-privacy trade-off for other pertinent distortion measures? What would be the optimal sanitizing mechanisms? We conjecture that such a study will involve enumerating integer points on the intersection of convex polytopes.

At a more strategic level, we deem it necessary to ask the following question. Given that we require certain utility and accuracy from our data mining algorithms, can we provide the stringent guarantees sought by DP for sanitizing databases or responding to individual queries? Our work proves that the minimal distortion (9) scales linearly with the dimensionality of the database, even if the number of records grows unbounded. Given the fine-grained and high-dimensional nature of our databases, is this adequate? Why are we not able to exploit the presence of a large number of records in our sanitization? The answer lies in the fact that DP is attempting to be robust against an adversary that knows $n - 1$ records perfectly. As the number of records grow, the *fraction* of entries that the adversary knows *increases* to 1. Indeed, this is a conservative model. Since the adversary's 'power' is increasing with the size of the DB, a DP mechanism is unable to exploit the presence of a large number of records to 'minimize the necessary randomization'. In other words, it is unable to hide one subject's record in the pool of all records without the help of randomization. We therefore conclude by asking the questions: Is a very low utility the inevitable price to pay for provable guarantees on privacy for large databases that DP promises? or, can we provide a more realistic framework to quantify privacy and vulnerability of query-response mechanisms?

Appendix A
Summary of Notation

Symbol	Meaning
$\mathbb{Z}, \mathbb{N}, \mathbb{R}$	Sets of integers, natural and real numbers
$[a, b]$	For $a, b \in \mathbb{Z}$, we let $[a, b] : = \{a, a+1, \cdots, b\}$
$[n]$	For $n \in \mathbb{N}$, we let $[n] = [1, n]$.
$M : \mathcal{A} \Rightarrow \mathcal{B}$	A randomized algorithm, referred to herein as a mechanism, with set $\mathcal{A}$ of inputs and set $\mathcal{B}$ of outputs.
$\mathbb{W}_M(b\|a)$	Probability that mechanism M produces[8] output $b \in \mathcal{B}$ when input with $a \in \mathcal{A}$.
$\mathbb{W}_M : \mathcal{A} \to \mathbb{P}(\mathcal{B})$ or $\mathbb{W}_M : \mathcal{A} \Rightarrow \mathcal{B}$	Alternate notations for mechanism $M : \mathcal{A} \Rightarrow \mathcal{B}$. $\mathbb{P}(\mathcal{B})$ is the set of probability distributions on $\mathcal{B}$
$d_G(v_1, v_2)$	Length of a shortest path from $v_1 \in V$ to $v_2 \in V$ in graph $G = (V, E)$
$\binom{n}{\underline{h}}$	When $\sum_{k=1}^{K} h_k = n$, we let $\binom{n}{\underline{h}} = \binom{n}{h_1 \cdots h_K}$.
Uppercase letters	Random variables and (generic) parameters that remain fixed throughout.
Calligraphic letters	Represent finite sets Examples : $\mathcal{A}, \mathcal{R}$

Table I
Description of symbols used in the article

Appendix B
It suffices to focus on mechanisms that are a function only of the histogram of the database

In our search for an optimal database sanitizing mechanism, we prove here that we may restrict attention to mechanisms that satisfy $\mathbb{W}(\underline{a}|\underline{b}) = \mathbb{W}(\underline{a}|\tilde{\underline{b}})$ whenever $\mathtt{h}(\underline{b}) = \mathtt{h}(\tilde{\underline{b}})$.

Lemma 2. *Given a privacy constraint $\theta > 0$, there exists a mechanism $(\mathbb{W}(\cdot|\underline{a}) : \underline{a} \in \mathcal{R}^n)$ such that (i) $\mathbb{W}(\cdot|\underline{a}) = \mathbb{W}(\cdot|\tilde{\underline{a}})$ whenever $\mathtt{h}(\underline{a}) = \mathtt{h}(\tilde{\underline{a}})$, (ii) $\frac{\mathbb{W}(\underline{b}|\underline{a})}{\mathbb{W}(\underline{b}|\tilde{\underline{a}})} \in [\theta, \frac{1}{\theta}]$ for every pair $\underline{a}, \hat{\underline{a}}$ of neighboring databases and every database $\underline{b}$, and (iii) $D^n(\mathbb{W}) \leq D^n(\mathbb{U})$ for every sanitizing mechanism $\mathbb{U}$ that is $\theta-$DP.*

Proof. We prove the following statement. Given any $\theta-$DP database sanitizing mechanism $(\mathbb{U}(|\cdot|\underline{a}) : \underline{a} \in \mathcal{R}^n)$, there exists a $\theta-$DP sanitizing mechanism $(\mathbb{W}(\cdot|\underline{a}) : \underline{a} \in \mathcal{R}^n)$ that satisfies (i) and (ii) in the theorem statement and $D^n(\mathbb{W}) \leq D^n(\mathbb{U})$. Towards that end, define

$$\underline{c}_{\underline{g}}^* \in \arg_{\underline{d}:h(\underline{d})=\underline{g}} \min \sum_{\underline{b} \in \mathcal{R}^n} \mathcal{F}(\mathtt{h}(\underline{b}), \mathtt{h}(\underline{d}))\mathbb{U}(\underline{b}|\underline{d}) \text{ and let } \mathbb{W}(\underline{a}|\underline{b}) = \mathbb{U}(\underline{a}|\underline{c}_{h(\underline{b})}^*) \text{ for all } \underline{a} \in \mathcal{R}^n, \underline{b} \in \mathcal{R}^n.$$

Suppose $h(\underline{b}) = h(\tilde{\underline{b}})$, then $\mathbb{W}(\underline{a}|\underline{b}) = \mathbb{U}(\underline{a}|\underline{c}_{h(\underline{b})}^*) = \mathbb{U}(\underline{a}|\underline{c}_{h(\tilde{\underline{b}})}^*) = \mathbb{W}(\underline{a}|\tilde{\underline{b}})$. Suppose $\underline{b}$ and $\hat{\underline{b}}$ are neighboring databases, then $|h(\underline{b}) - h(\hat{\underline{b}})| = 2$. Since $c_{h(\underline{b})}^*$ and $c_{h(\hat{\underline{b}})}^*$ are neighboring and $\mathbb{U}$ is $\theta-$DP, we have

$$\frac{\mathbb{W}(\underline{a}|\underline{b})}{\mathbb{W}(\underline{a}|\hat{\underline{b}})} = \frac{\mathbb{U}(\underline{a}|c_{h(\underline{b})}^*)}{\mathbb{U}(\underline{a}|c_{h(\hat{\underline{b}})}^*)} \in [\theta, \frac{1}{\theta}] \text{ for all } \underline{a} \in \mathcal{R}^n.$$

Lastly, we study $D^n(\mathbb{W})$:

$$\begin{aligned} D^n(\mathbb{W}) &= \sum_{\underline{a} \in \mathcal{R}^n} \sum_{\underline{b} \in \mathcal{R}^n} p(\underline{a})\mathbb{W}(\underline{b}|\underline{a})\mathcal{F}(\mathtt{h}(\underline{a}), \mathtt{h}(\underline{b})) = \sum_{\underline{g} \in \mathcal{H}^n} \sum_{\substack{\underline{a} \in \mathcal{R}^n: \\ \mathtt{h}(\underline{a}) = \underline{g}}} p(\underline{a}) \sum_{\underline{b} \in \mathcal{R}^n} \mathbb{W}(\underline{b}|\underline{a})\mathcal{F}(\mathtt{h}(\underline{a}), \mathtt{h}(\underline{b})) \\ &= \sum_{\underline{g} \in \mathcal{H}^n} \sum_{\substack{\underline{a} \in \mathcal{R}^n: \\ \mathtt{h}(\underline{a}) = \underline{g}}} p(\underline{a}) \sum_{\underline{b} \in \mathcal{R}^n} \mathbb{U}(\underline{b}|c_{\mathtt{h}(\underline{a})}^*)\mathcal{F}(\mathtt{h}(\underline{a}), \mathtt{h}(\underline{b})) \leq \sum_{\underline{g} \in \mathcal{H}^n} \sum_{\substack{\underline{a} \in \mathcal{R}^n: \\ \mathtt{h}(\underline{a}) = \underline{g}}} p(\underline{a}) \sum_{\underline{b} \in \mathcal{R}^n} \mathbb{U}(\underline{b}|\underline{a})\mathcal{F}(\mathtt{h}(\underline{a}), \mathtt{h}(\underline{b})) = D^n(\mathbb{U}) \end{aligned}$$

Suppose $\mathbb{U} : \mathcal{R}^n \to \mathcal{R}^n$ and $\mathbb{V} : \mathcal{R}^n \to \mathcal{R}^n$ are DSMs such that

$$\sum_{\substack{\underline{a}\in\mathcal{R}^n:\\ \mathtt{h}(\underline{a})=\underline{h}}} \mathbb{U}(\underline{a}|\underline{b}) = \sum_{\substack{\underline{c}\in\mathcal{R}^n:\\ \mathtt{h}(\underline{a})=\underline{h}}} \mathbb{V}(\underline{c}|\underline{b}) \quad \forall \underline{h}\in\mathcal{H}^n, \forall \underline{b}\in\mathcal{R}^n, \text{ then}$$

$$\begin{aligned} D^n(\mathbb{U}) &= \sum_{\underline{a}\in\mathcal{R}^n}\sum_{\underline{b}\in\mathcal{R}^n} p(\underline{a})\mathbb{U}(\underline{b}|\underline{a})\mathcal{F}(\mathtt{h}(\underline{b}),\mathtt{h}(\underline{a})) = \sum_{\underline{a}\in\mathcal{R}^n}\sum_{\underline{h}\in\mathcal{H}^n}\sum_{\substack{\underline{b}\in\mathcal{R}^n:\\ \mathtt{h}(\underline{b})=\underline{h}}} p(\underline{a})\mathbb{U}(\underline{b}|\underline{a})\mathcal{F}(\underline{h},\mathtt{h}(\underline{a})) \\ &= \sum_{\underline{a}\in\mathcal{R}^n}\sum_{\underline{h}\in\mathcal{H}^n} p(\underline{a})\mathcal{F}(\underline{h},\mathtt{h}(\underline{a}))\sum_{\substack{\underline{b}\in\mathcal{R}^n:\\ \mathtt{h}(\underline{b})=\underline{h}}}\mathbb{U}(\underline{b}|\underline{a}) = \sum_{\underline{a}\in\mathcal{R}^n}\sum_{\underline{h}\in\mathcal{H}^n} p(\underline{a})\mathcal{F}(\underline{h},\mathtt{h}(\underline{a}))\sum_{\substack{\underline{b}\in\mathcal{R}^n:\\ \mathtt{h}(\underline{b})=\underline{h}}}\mathbb{V}(\underline{b}|\underline{a}) \\ &= D^n(\mathbb{V}). \end{aligned}$$

The above discussion narrows our search to histogram sanitizing mechanisms $\mathbb{W} : \mathcal{H}^n \to \mathcal{H}^n$. The prior distribution on $\mathcal{H}^n$ is given by (3). Our goal, is therefore to only identify a $\theta-$DP HSM that minimizes

$$D^n(\mathbb{W}) = \sum_{\underline{h}\in\mathcal{H}^n}\sum_{\underline{g}\in\mathcal{H}^n}\binom{n}{\underline{h}}\underline{p}^{\underline{h}}\mathbb{W}(\underline{g}|\underline{h})\mathcal{F}(\underline{g},\underline{h}).$$

■

Appendix C
Proof of Corollary 1

We let $y = \frac{1+\theta}{1-\theta}$ and note $\frac{dy}{d\theta} = \frac{2}{(1-\theta)^2}$. Observe that

$$\begin{aligned} \frac{S'_{K-1}(\theta)}{S_{K-1}(\theta)} &= \frac{1}{(1-\theta)^{K-1}L_{K-1}(y)}\frac{d}{d\theta}\left\{(1-\theta)^{K-1}L_{K-1}(y)\right\} = \frac{-(K-1)}{(1-\theta)} + \frac{(1-\theta)^{K-1}\frac{dL_{K-1}(y)}{d\theta}}{(1-\theta)^{K-1}L_{K-1}(y)} \\ &= \frac{-(K-1)}{(1-\theta)} + \frac{\frac{dL_{K-1}(y)}{dy}\frac{2}{(1-\theta)^2}}{L_{K-1}(y)} = \frac{-(K-1)}{(1-\theta)} + \frac{L'_{K-1}(y)\frac{2}{(1-\theta)^2}}{L_{K-1}(y)}. \end{aligned} \tag{51}$$

We now utilize the recurrence relations $(1-y^2)L'_n(y) = nL_{n-1}(y) - nyL_n(y)$ for every $n \geq 2$ and $(m+1)L_{m+1}(y) - (2m+1)yL_m(y) + mL_{m-1}(y) = 0$ for every $m \geq 1$. Substituting $n = K-1$ and $m = K-1$ in these relations, we conclude $(1-y^2)L'_{K-1}(y) = KyL_{K-1}(y) - KL_K(y)$, and hence $\frac{L'_{K-1}(y)}{L_{K-1}(y)} = \frac{Ky}{(1-y^2)} - \frac{K}{(1-y^2)}\frac{L_K(y)}{L_{K-1}(y)}$. Substituting this in (51), one can verify

$$2\theta\left\{\frac{K-1}{1-\theta} + \frac{S'_{K-1}(\theta)}{S_{K-1}(\theta)}\right\} = 2\theta\left\{\frac{-K}{\theta}\left(\frac{1+\theta}{1-\theta}\right) + \frac{K}{2\theta}\frac{L_K(y)}{L_{K-1}(y)}\right\} = K\left\{\frac{L_K(y)}{L_{K-1}(y)} + \frac{1+\theta}{1-\theta}\right\},$$

and this concludes the proof.

Appendix D
Properties of Privacy-Constraint Graph and $\mathcal{H}^n$

We list and prove some simple properties of the set of histograms $\mathcal{H}^n$ and the PC graph involved in our study.

Lemma 3. *Consider the set $\mathcal{H}^n_K$ of histograms defined in (1) and the PC graph $G = (V, E)$, wherein $V = \mathcal{H}^n_K$ and $E = \left\{(\underline{h}, \hat{\underline{h}}) \in \mathcal{H}^n \times \mathcal{H}^n : |\underline{h} - \hat{\underline{h}}|_1 = 2\right\}$. The following are true (i) For any $\underline{g}, \underline{h} \in \mathcal{H}^n$, $|\underline{g} - \underline{h}|_1$ is an even integer and at most $2n$. (ii) $2d_G(\underline{g}, \underline{h}) = |\underline{g} - \underline{h}|_1$.*

Proof. (i) For any $\underline{g}, \underline{h} \in \mathcal{H}^n$, we have $\sum_{k=1}^K g_k = \sum_{k=1}^K h_k = n$, and hence for any subset $S \subseteq [K]$, we have $\sum_{i\in S}(g_i - h_i) = \sum_{j\in[K]\setminus S}(h_j - g_j)$. Note that

$$|\underline{g} - \underline{h}|_1 = \sum_{i=1}^n |g_i - h_i| = \sum_{i:g_i\geq h_i}(g_i - h_i) + \sum_{j:h_j>g_j}(h_j - g_j) = 2\sum_{i:g_i\geq h_i}(g_i - h_i),$$

which is an even integer. Moreover $\sum_{i:g_i\geq h_i}(g_i-h_i)\leq\sum_{i=1}^{K}g_i=n$, and hence $|\underline{g}-\underline{h}|_1\leq 2n$.

(ii) We prove this by induction on K. When $K=1$, we have $\mathcal{H}_1^n=\{(n)\}$, and the statement is true. When $K=2$, we note that $|(n-i,i)-(n-j,j)|_1=2|i-j|$ and the nodes $(n-i,i),(n-j,j)$ are indeed $|i-j|$ hops apart (Fig. 5). Hence $|i-j|=d_G((n-i,i),(n-j,j))$ and the statement is true. We assume the truth of this statement for $K=1,\cdots,L-1$ and any n. Suppose $K=L$ and let $\underline{g},\underline{h}\in\mathcal{H}_L^n$. If for some coordinate i, we have $g_i=h_i$, then, let $\tilde{\underline{g}}:=(g_j:j\neq i)$ and $\tilde{\underline{h}}:=(h_j:j\neq i)$. We have $\tilde{\underline{g}},\tilde{\underline{h}}\in\mathcal{H}_{L-1}^{n-g_i}$. By our induction hypothesis, we have $2d_{\tilde{G}}(\tilde{\underline{g}},\tilde{\underline{h}})=|\tilde{\underline{g}}-\tilde{\underline{h}}|=|\underline{g}-\underline{h}|$, where $\tilde{G}$ is the PC graph corresponding to $\mathcal{H}_{L-1}^{n-g_i}$. It can now be verified that a shortest path from $\underline{g}$ to $\underline{h}$ on G corresponds to a shortest path between $\tilde{\underline{g}}$ to $\tilde{\underline{h}}$ in $\tilde{G}$ and hence $d_{\tilde{G}}(\tilde{\underline{g}},\tilde{\underline{h}})=d_G(\underline{g},\underline{h})$. In fact, observe that the graph induced on the set of vertices on a horizontal line in Fig. 6 is isomorphic to the graph in Fig. 5 for an appropriate choice of n. Let us now consider the alternate case where $\underline{g},\underline{h}\in\mathcal{H}_L^n$ are such that for *no* co-ordinate i do we have $g_i=h_i$. Without loss of generality, assume $a=g_1-h_1>0$. Let $i_1,\cdots,i_R\in[2,L]$ be coordinates such that $h_{i_r}>g_{i_r}$ for $r\in[1,R]$ and $\sum_{r=1}^{R}(h_{i_r}-g_{i_r})\geq a$. The existence of coordinates $i_1,\cdots,i_R$ can be easily proved by using the fact that $\underline{g},\underline{h}\in\mathcal{H}_L^n$. Now, let $b_1,\cdots b_R>0$ be integers such that $h_{i_r}-g_{i_r}\geq b_r>0$ for $r\in[R]$ and $\sum_{r=1}^{R}b_{i_r}=a$. Now consider $\underline{f}\in\mathcal{H}_L^n$ such that $f_1=g_1-a$, $f_{i_r}=g_{i_r}+b_r$ and $f_j=g_j$ if $j\notin\{1,i_1,\cdots,i_R\}$. It can now be verified, by using the induction hypothesis on $\underline{f},\underline{h}$, that $d_G(\underline{g},\underline{h})=d_G(\underline{g},\underline{f})+d_G(\underline{f},\underline{h})$, $2d_G(\underline{g},\underline{f})=|\underline{g}-\underline{f}|_1$, $2d_G(\underline{f},\underline{h})=|\underline{f}-\underline{h}|_1$, and $|\underline{g}-\underline{f}|_1+|\underline{f}-\underline{h}|_1=|\underline{g}-\underline{h}|_1$, thereby proving the statement for $K=L$. ■

APPENDIX E
THE WEAK DUALITY THEOREM OF LP

We refer the reader to [24] for a description of the dual linear program. Following the same notation, we state WDT below.

Weak Duality Theorem : Consider the following primal and dual LP problems. Let $\mathbf{A}$ be a matrix with rows $\mathbf{a}_i'$ and columns $\mathbf{A}_j$.

	Primal LP			Dual LP	
Minimize	$\mathbf{c}'\mathbf{x}$		Maximize	$\mathbf{p}'\mathbf{b}$	
subject to	$\mathbf{a}_i'\mathbf{x}\geq\mathbf{b}_i$	$i\in M_1$	subject to	$p_i\geq 0$	$i\in M_1$
	$\mathbf{a}_i'\mathbf{x}=\mathbf{b}_i$	$i\in M_3$		p_i free	$i\in M_3$
	$x_j\geq 0$	$j\in N_1,$		$\mathbf{p}'\mathbf{A}_j\leq c_j$	$j\in N_1.$

If $\mathbf{x}$ and $\mathbf{p}$ are feasible solutions to the primal and dual problems respectively, then $\mathbf{p}'\mathbf{b}\leq\mathbf{c}'\mathbf{x}$.

APPENDIX F
MECHANISM $\mathbb{U}:\mathcal{H}^n\Rightarrow\mathcal{H}^n_{\text{EXT}}$ IS A $\theta-$DP MECHANISM

Recall, $\mathbb{U}:\mathcal{H}^n\Rightarrow\mathcal{H}^n_{\text{ext}}$ is specified in (24), and we let

$$\mathscr{E}_{\mathcal{P},f}(\theta)=(1-\theta)\mathrm{Ehr}_{\mathcal{P}}(\theta)=1+\sum_{\mathrm{d}=1}^{\infty}\mathrm{N_d}\theta^{\mathrm{d}}. \tag{52}$$

Clearly, $\mathbb{U}^n(\underline{g}|\underline{h})\geq 0$. We note that

$$\begin{aligned}\sum_{\underline{g}\in\mathcal{H}^n_{\text{ext}}}\mathbb{U}^n(\underline{g}|\underline{h}) &= \frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)}\sum_{\underline{g}\in\mathcal{H}^n_{\text{ext}}}\theta^{\frac{|\underline{g}-\underline{h}|_1}{2}}=\frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)}\sum_{d=0}^{\infty}\sum_{\substack{\underline{g}\in\mathcal{H}^n_{\text{ext}}:\\|\underline{g}-\underline{h}|_1=2d}}\theta^{\frac{|\underline{g}-\underline{h}|_1}{2}}=\frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)}\sum_{d=0}^{\infty}\sum_{\substack{\underline{g}\in\mathcal{H}^n_{\text{ext}}:\\|\underline{g}-\underline{h}|_1=2d}}\theta^d\\ &= \frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)}\sum_{d=0}^{\infty}N_d\theta^d=\frac{1}{\mathscr{E}_{\mathcal{P},f}(\theta)}\left(1+\sum_{d=1}^{\infty}N_d\theta^d\right)=1.\end{aligned}$$

Lastly, suppose $\underline{h}\in\mathcal{H}^n$ and $\tilde{\underline{h}}\in\mathcal{H}^n$ are a pair of neighboring histograms,

$$\mathbb{U}^n(\underline{g}|\underline{h})/\mathbb{U}^n(\underline{g}|\tilde{\underline{h}})=\theta^{\frac{|\underline{g}-\underline{h}|_1}{2}}/\theta^{\frac{|\underline{g}-\tilde{\underline{h}}|_1}{2}}=\theta^{\frac{\left(|\underline{g}-\underline{h}|_1-|\underline{g}-\tilde{\underline{h}}|_1\right)}{2}}.$$

By the triangle inequality, $-2=-|\underline{h}-\tilde{\underline{h}}|_1\leq|\underline{g}-\tilde{\underline{h}}|_1-|\underline{g}-\underline{h}|_1\leq|\underline{h}-\tilde{\underline{h}}|_1=2$, and we wee that the above ratio is in $[\theta,\frac{1}{\theta}]$. $\mathbb{U}^n$ is therefore a $\theta-$DP mechanism.

Appendix G
For n sufficiently large, $D^n_{\mathcal{H}}(\mathbb{W}^n) \leq D(\mathbb{U}^n)$

Here we prove that the expected distortion of $\mathbb{W}^n$ is, in the limit, at most that of $\mathbb{U}^n$, i.e., $\lim_{n\to\infty} D(\mathbb{W}^n, \underline{p}) \leq \lim_{n\to\infty} D(\mathbb{U}^n)$. Towards this end, we let $B(\delta, \underline{h}) := \left\{\underline{g} \in \mathcal{H}^n : |\underline{g} - \underline{h}|_1 \leq \delta\right\}$ and $B^c(\delta, \underline{h}) := \mathcal{H}^n \setminus B(\delta, \underline{h})$ its complement. We abbreviate $B(\frac{1}{2}) = B(\frac{R}{2}n^{\frac{2}{3}}, n\underline{p})$, $B^c(\frac{1}{2}) = B^c(\frac{R}{2}n^{\frac{2}{3}}, n\underline{p})$, $B(1) = B(Rn^{\frac{2}{3}}, n\underline{p})$, $B^c(1) = B^c(Rn^{\frac{2}{3}}, n\underline{p})$. Observe that

$$\begin{aligned}
D(\mathbb{W}^n, \underline{p}) &= \sum_{\underline{h}\in\mathcal{H}^n} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \\
&= \sum_{\underline{h}\in B(\frac{1}{2})} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 + \sum_{\underline{h}\in B^c(\frac{1}{2})} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \\
&\leq \sum_{\underline{h}\in B(\frac{1}{2})} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 + \sum_{\underline{h}\in B^c(\frac{1}{2})} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) 2n \\
&\leq \sum_{\underline{h}\in B(\frac{1}{2})} \sum_{\underline{g}\in\mathcal{H}^n} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 + 2n \sum_{\underline{h}\in B^c(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}}.
\end{aligned}$$

It can be easily shown that $\sum_{\underline{h}\in B^c(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \leq \exp\{-n\alpha\}$, and hence the second term above can be made arbitrarily small by choosing n large enough. We henceforth focus on the first term above which is given by

$$\begin{aligned}
&\sum_{\underline{h}\in B(\frac{1}{2})} \sum_{\underline{g}\in B(1)} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 + \sum_{\underline{h}\in B(\frac{1}{2})} \sum_{\underline{g}\in B^c(1)} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \\
&= \sum_{\underline{h}\in B(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \left(|n\underline{p} - \underline{h}|_1 \mathbb{W}^n(n\underline{p}|\underline{h}) + \sum_{\underline{g}\in B(1)\setminus\{n\underline{p}\}} \mathbb{W}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \right) \qquad (53) \\
&= \sum_{\underline{h}\in B(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \left(|n\underline{p} - \underline{h}|_1 [\mathbb{U}^n(n\underline{p}|\underline{h}) + \sum_{\underline{\tilde{g}}\in B^c(1)} \mathbb{U}^n(\underline{\tilde{g}}|\underline{h})] + \sum_{\underline{g}\in B(1)\setminus\{n\underline{p}\}} \mathbb{U}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \right) \qquad (54) \\
&\leq \sum_{\underline{h}\in B(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \left(|n\underline{p} - \underline{h}|_1 \mathbb{U}^n(n\underline{p}|\underline{h}) + \sum_{\underline{\tilde{g}}\in B^c(1)} |\underline{\tilde{g}} - \underline{h}|_1 \mathbb{U}^n(\underline{\tilde{g}}|\underline{h}) + \sum_{\underline{g}\in B(1)\setminus\{n\underline{p}\}} \mathbb{U}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \right) \qquad (55) \\
&\leq \sum_{\underline{h}\in B(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \left(|n\underline{p} - \underline{h}|_1 \mathbb{U}^n(n\underline{p}|\underline{h}) + \sum_{\underline{\tilde{g}}\in B^c(1)} |\underline{\tilde{g}} - \underline{h}|_1 \mathbb{U}^n(\underline{\tilde{g}}|\underline{h}) + \sum_{\underline{g}\in B(1)\setminus\{n\underline{p}\}} \mathbb{U}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \right) \\
&= \sum_{\underline{h}\in B(\frac{1}{2})} \binom{n}{\underline{h}} \underline{p}^{\underline{h}} \sum_{\underline{g}\in\mathcal{H}^n} \mathbb{U}^n(\underline{g}|\underline{h}) |\underline{g} - \underline{h}|_1 \leq D(\mathbb{U}^n),
\end{aligned}$$

where (i) (53) follows from $\mathbb{W}^n(\underline{\tilde{g}}|\underline{h}) = 0$ for $\underline{\tilde{g}} \in B^c(1)$ implying[9] that the second term is zero, (ii) (54) follows from the definition of $\mathbb{W}^n$ in terms of $\mathbb{U}^n$, (iii) (55) is true since, for every $\underline{h} \in B(\frac{1}{2})$ and every $\underline{\tilde{g}} \in B^c(1)$, $|n\underline{p} - \underline{h}|_1 \leq \frac{R}{2}n^{\frac{2}{3}} \leq Rn^{\frac{2}{3}} \leq |\underline{\tilde{g}} - \underline{h}|_1$.

Appendix H
Characterization of A_n, B_n defined in (30)

A_n on the left and B_n on the right constitute the boundaries of the support of the truncated geometric mechanism. It is instructive to study A_n, B_n for different distributions $\mathscr{C}^n_i$. Suppose one replaces $\mathscr{C}^n_i$ by $\frac{1}{n+1}$ - the uniform pmf on the set of histograms $\mathcal{H}^n_2$, then simple calculation shows that $A_n \leq \mathcal{N}_\theta := \min\{i \in \mathbb{N} : \theta^i < 1 - \theta\}$ and

[9] Note that the range of $f_{\mathbb{V}^n}$ is $B(1)$.

$B_n \geq n - \mathcal{N}_\theta$. Since this will provide us with important intuition, we first proceed with these steps. We recall the definitions for ease of reference:

$$f_i := 2\sum_{j=0}^{i} \mathscr{C}_j^n \theta^{i-j}, \quad b_i := 2\sum_{k=i}^{n} \mathscr{C}_k^n \theta^{k-i},$$

$$A_n := \min \left\{ i \in [0,n] : \begin{array}{c} f_{k-1} - \theta b_k \geq 0 \\ \text{for every } k \geq i \end{array} \right\}, B_n := \max \left\{ i \in [0,n] : \begin{array}{c} b_{k+1} - \theta f_k \geq 0 \\ \text{for every } k \leq i \end{array} \right\}. \tag{56}$$

Since we are interested in $f_{i-1} - \theta b_i$ and $b_{i+1} - \theta f_i$, we will ignore the multiplier 2 in the definitions of f_i and b_i. We work out a simple case to understand the core problem. Let us begin with the case $\mathcal{C}_i^n = \frac{1}{n+1}$ for $i \in [0,n]$. It can be verified that

$$\begin{aligned} f_{i-1} - \theta b_i &= \frac{1}{n+1}\left[\theta^{i-1} + \theta^{i-2} + \cdots + \theta + 1 - \theta\left(1 + \theta + \theta^2 + \cdots + \theta^{n-i}\right)\right] \\ &= \frac{1}{n+1}\left[\frac{1-\theta^i}{1-\theta} - \theta\left(\frac{1-\theta^{n-i+1}}{1-\theta}\right)\right] = \frac{1}{n+1}\left[1 - \frac{\theta^i - \theta^{n-i+2}}{1-\theta}\right] \\ &\geq \frac{1}{n+1}\left[1 - \frac{\theta^i}{1-\theta}\right]. \end{aligned}$$

Clearly, $A_n < \min\{i : \theta^i < 1-\theta\}$. A similar sequence of steps leads one to conclude that $B_n > \max\{i : \theta^{n-i} < 1-\theta\}$. We observe $A_n = \mathcal{O}(1)$ and $n - B_n = \mathcal{O}(1)$. Our characterization for A_n and B_n for $\mathscr{C}_i^n = \binom{n}{i} p^i (1-p)^{n-i}$ is based on the above intuition. The key property of the binomial pmf, that it is near-uniform in the window $[np - \mathcal{O}(\sqrt{n}), np + \mathcal{O}(\sqrt{n})]$ is employed. Specifically, note that for sufficiently large n

$$\max\left\{\frac{\mathscr{C}_{np}^n}{\mathscr{C}_{np-x}^n}, \frac{\mathscr{C}_{np}^n}{\mathscr{C}_{np+x}^n}\right\} \leq 2\exp\{\frac{x^2}{2np(1-p)}\}, \tag{57}$$

where (57) follows from [21, Eqn. 106].[10] For $x \sim \sqrt{\frac{n}{(\log n)^4}}$, the above ratio shrinks as $\frac{1}{n^4}$. Note that $\binom{n}{np}$ scales as $\frac{1}{\sqrt{n}}$. We can use this to bound the ratio between the largest and the smallest binomial probability masses in the range $[np - \sqrt{\frac{n}{(\log n)^4}}, np + \sqrt{\frac{n}{(\log n)^4}}]$, and we can use the same sequence of steps used above. It can be proved that $np - A_n = \mathcal{O}(\sqrt{\frac{n}{(\log n)^4}})$ and $B_n - np = \mathcal{O}(\sqrt{\frac{n}{(\log n)^4}})$. The reader may refer to [23] for a detailed proof of these claims.

Appendix I
Interpretation of dual variable assignments via shadow prices

We provide an interpretation for the assignments of the dual variables in Eq. (35)-(39) via shadow prices. Assignment (36) for $j = i$ can be interpreted via mechanism $\hat{\mathbb{W}}(\cdot|\cdot)$ defined as $\hat{\mathbb{W}}(k|j) = \mathbb{W}(k|j) + d\mathbb{W}(k|j)$, where $\mathbb{W}(\cdot|\cdot)$ is the truncated geometric mechanism defined in (32) and

$$d\mathbb{W}(k|j) = \begin{cases} 0 & \text{if } k \neq (i-1), \text{ and } k \neq i, \\ -\epsilon\theta^{|j-(i-1)|} & \text{if } k = (i-1), \\ +\epsilon\theta^{|j-(i-1)|} & \text{if } k = i. \end{cases} \tag{58}$$

It is straightforward to verify that $\hat{\mathbb{W}}$ satisfies all the constraints of a $\theta-$DP mechanism (just as $\mathbb{W}$), and more importantly, $\hat{\mathbb{W}}(i|i-1) - \theta\hat{\mathbb{W}}(i|i) = \epsilon(1-\theta^2)$. In fact, except for this constraint, $\mathbb{W}$ and $\hat{\mathbb{W}}$ are identical wrt all other constraints. $\mathbb{W}$ and $\hat{\mathbb{W}}$ are identical vertices in their corresponding feasible regions, with the only difference being that $\hat{\mathbb{W}}$ satisfies the constraint $\hat{\mathbb{W}}(i|i-1) - \theta\hat{\mathbb{W}}(i|i) \geq \epsilon(1-\theta^2)$. Moreover, it can be verified that $D_{\mathcal{H}}^n(\hat{\mathbb{W}}) - D_{\mathcal{H}}^n(\mathbb{W}) = \epsilon(f_{i-1} - \theta b_i)$. Recognize that

$$\lim_{\epsilon \to 0} \frac{D_{\mathcal{H}}^n(\hat{\mathbb{W}}) - D_{\mathcal{H}}^n(\mathbb{W})}{\hat{\mathbb{W}}(i|i-1) - \theta\hat{\mathbb{W}}(i|i)} = \lim_{\epsilon \to 0} \frac{D^n(d\mathbb{W})}{\hat{\mathbb{W}}(i|i-1) - \theta\hat{\mathbb{W}}(i|i)} = \lim_{\epsilon \to 0} \frac{\epsilon(f_{i-1} - \theta b_i)}{\epsilon(1-\theta^2)} = \lambda_{i|(i-1,i)}.$$

[10] Note that $\mathscr{C}_i^n = \binom{n}{i} 2^{-nH(X)} \left(\frac{p}{1-p}\right)^{i-np}$.

These are indeed the shadow prices that we alluded to. We continue and discuss the interpretation for the rest of the variables. Consider assignment (36) for $j > i$. Consider $\hat{\mathbb{W}}(\cdot|\cdot)$ defined as $\hat{\mathbb{W}}(a|b) = \mathbb{W}(a|b) + d\mathbb{W}(a|b)$, where $\mathbb{W}(\cdot|\cdot)$ is the truncated geometric mechanism defined in (32), and $d\mathbb{W}$ is now defined as

$$d\mathbb{W}(a|b) = \begin{cases} 0 & \text{if } a \neq (i-1), \text{ and } a \neq i, \text{ and } a \neq j \\ -\epsilon\theta^{|b-(i-1)|} & \text{if } a = (i-1), \\ +\epsilon\theta^{|b-(i-1)|} & \text{if } a = i, b \geq i \\ +\epsilon\theta^{|b-(i-1)|+2} & \text{if } a = i, b \leq i-1 \\ +\epsilon(\theta^{|b-(i-1)|} - \theta^{|b-(i-1)|+2}) & \text{if } a = j, b \leq i-1 \\ 0 & \text{if } a = j, b \geq i. \end{cases} \tag{59}$$

As earlier, it is straightforward to verify that $\hat{\mathbb{W}}$ satisfies all the constraints of a $\theta-$DP mechanism (just as $\mathbb{W}$), and more importantly, $\hat{\mathbb{W}}(j|i-1) - \theta\hat{\mathbb{W}}(j|i) = \epsilon(1-\theta^2)$. In fact, except for this constraint, $\mathbb{W}$ and $\hat{\mathbb{W}}$ are identical wrt all other constraints. Moreover, it can be verified that $D^n_{\mathcal{H}}(\hat{\mathbb{W}}) - D^n_{\mathcal{H}}(\mathbb{W}) = \epsilon(f_{i-1} - \theta b_i)$. Recognize that

$$\begin{aligned} \lim_{\epsilon\to 0} \frac{D^n_{\mathcal{H}}(\hat{\mathbb{W}}) - D^n_{\mathcal{H}}(\mathbb{W})}{\hat{\mathbb{W}}(j|i-1) - \theta\hat{\mathbb{W}}(j|i)} &= \lim_{\epsilon\to 0} \frac{D^n(d\mathbb{W})}{\hat{\mathbb{W}}(j|i-1) - \theta\hat{\mathbb{W}}(j|i)} \\ &= \lim_{\epsilon\to 0} \frac{\epsilon(\theta^2 f_{i-1} + (j-i+1)(1-\theta^2)f_{i-1} - \theta b_i)}{\epsilon(1-\theta^2)} = \lambda_{j|(i-1,i)}. \end{aligned}$$

Now consider (37) with $j = i$. Analogous to (58), consider

$$d\mathbb{W}(k|j) = \begin{cases} 0 & \text{if } k \neq (i+1), \text{ and } k \neq i, \\ -\epsilon\theta^{|j-(i+1)|} & \text{if } k = (i+1), \\ +\epsilon\theta^{|j-(i+1)|} & \text{if } k = i. \end{cases} \tag{60}$$

Following the same arguments as above, it can be verified by straightforward substitutions that

$$\lim_{\epsilon\to 0} \frac{D^n_{\mathcal{H}}(\hat{\mathbb{W}}) - D^n_{\mathcal{H}}(\mathbb{W})}{\hat{\mathbb{W}}(i|i+1) - \theta\hat{\mathbb{W}}(i|i)} = \lim_{\epsilon\to 0} \frac{D^n(d\mathbb{W})}{\hat{\mathbb{W}}(i|i+1) - \theta\hat{\mathbb{W}}(i|i)} = \lim_{\epsilon\to 0} \frac{\epsilon(b_{i+1} - \theta f_i)}{\epsilon(1-\theta^2)} = \lambda_{i|(i+1,i)},$$

where, as before, $\hat{\mathbb{W}}(\cdot|\cdot)$ defined as $\hat{\mathbb{W}}(k|j) = \mathbb{W}(k|j) + d\mathbb{W}(k|j)$, and $\mathbb{W}(\cdot|\cdot)$ is the truncated geometric mechanism. Similarly, for $j < i$ we can verify the assignment in (37) through the following. Define mechanism $\hat{\mathbb{W}}(\cdot|\cdot) = \mathbb{W}(k|j) + d\mathbb{W}(k|j)$, where $\mathbb{W}(\cdot|\cdot)$ is the truncated geometric mechanism defined in (32), and

$$d\mathbb{W}(a|b) = \begin{cases} 0 & \text{if } a \neq (i+1), \text{ and } a \neq i, \text{ and } a \neq j \\ -\epsilon\theta^{|b-(i+1)|} & \text{if } a = (i+1), \\ +\epsilon\theta^{|b-(i+1)|} & \text{if } a = i, b \geq i \\ +\epsilon\theta^{|b-(i+1)|+2} & \text{if } a = i, b \geq i+1 \\ +\epsilon(\theta^{|b-(i+1)|} - \theta^{|b-(i+1)|+2}) & \text{if } a = j, b \geq i+1 \\ 0 & \text{if } a = j, b \leq i. \end{cases} \tag{61}$$

Following the same arguments as above, it can be verified by straightforward substitutions that

$$\begin{aligned} \lim_{\epsilon\to 0} \frac{D^n_{\mathcal{H}}(\hat{\mathbb{W}}) - D^n_{\mathcal{H}}(\mathbb{W})}{\hat{\mathbb{W}}(j|i+1) - \theta\hat{\mathbb{W}}(j|i)} &= \lim_{\epsilon\to 0} \frac{D^n(d\mathbb{W})}{\hat{\mathbb{W}}(j|i+1) - \theta\hat{\mathbb{W}}(j|i)} \\ &= \lim_{\epsilon\to 0} \frac{\epsilon(\theta^2 b_{i+1} + (i+1-j)(1-\theta^2)b_{i+1} - \theta f_i)}{\epsilon(1-\theta^2)} = \lambda_{j|(i+1,i)}, \end{aligned}$$

where, as before, $\hat{\mathbb{W}}(\cdot|\cdot)$ defined as $\hat{\mathbb{W}}(k|j) = \mathbb{W}(k|j) + d\mathbb{W}(k|j)$, and $\mathbb{W}(\cdot|\cdot)$ is the truncated geometric mechanism. Finally, we explain the assignment for μ_i in the range $[A-1, B+1]$. Consider $\hat{\mathbb{W}}(b|a) = \mathbb{W}(b|a) + d\mathbb{W}(b|a)$ where $\mathbb{W}$ is the truncated Geometric mechanism as before, and

$$d\mathbb{W}(a|b) = \begin{cases} 0 & \text{if } a \neq (i-1), \text{ and } a \neq i, \text{ and } a \neq (i+1) \\ -\epsilon\theta^{|b-(i-1)|+1} & \text{if } a = (i-1), \\ -\epsilon\theta^{|b-(i+1)|+1} & \text{if } a = i+1, \\ +\epsilon\theta^{|b-(i-1)|+1} + \epsilon\theta^{|b-(i+1)|+1} & \text{if } a = i, b \neq i \\ +\epsilon(1+\theta^2) & \text{if } a = i, b = i \end{cases} \tag{62}$$

The following can be verified easily : $\sum_{j=0}^{n} \hat{\mathbb{W}}(j|i) = 1 + \epsilon - \epsilon\theta^2$. $\hat{\mathbb{W}}$ and $\mathbb{W}$ are identical with respect to the set of DP constraints they satisfy, and

$$\begin{aligned} \lim_{\epsilon \to 0} \frac{D^n_{\mathcal{H}}(\hat{\mathbb{W}}) - D^n_{\mathcal{H}}(\mathbb{W})}{\sum_{j=0}^{n} \hat{\mathbb{W}}(j|i) - 1} &= \lim_{\epsilon \to 0} \frac{D^n(d\mathbb{W})}{\sum_{j=0}^{n} \hat{\mathbb{W}}(j|i) - 1} \\ &= \lim_{\epsilon \to 0} \frac{\epsilon[\theta(1-\theta^2)(f_{i-1} + b_{i+1}) - 4\theta^2 \binom{n}{i} p^i (1-p)^{n-i}]}{\epsilon(1-\theta^2)} = \mu_i . \end{aligned}$$

The key import of the above interpretation is the relationship between the assignments (58)-(62). (59) can be obtained from (58) by just shifting mass from i to j. Similarly, (61) can be obtained from (60) by just shifting mass from i to j. This provides an alternate proof of feasibility of this dual variable assignment. Also note that the assignment (62) is obtained as θ times the assignment (58) summed to θ times the assignment (60). The feasibility of this assignment is now an immediate consequence of these relationships. This shadow price interpretation is the basis for (49), whose feasibility follows immediately from the geometry of the constraints.

References

[1] L. Sweeney, "Weaving technology and policy together to maintain confidentiality," *The Journal of Law, Medicine & Ethics*, vol. 25, no. 2-3, pp. 98–110, 1997. [Online]. Available: http://dx.doi.org/10.1111/j.1748-720X.1997.tb01885.x

[2] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, ser. SP '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 111–125. [Online]. Available: http://dx.doi.org/10.1109/SP.2008.33

[3] C. Dwork, "Differential privacy," in *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ser. ICALP'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–12.

[4] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proceedings of the Third Conference on Theory of Cryptography*, ser. TCC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 265–284.

[5] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Found. Trends Theor. Comput. Sci.*, vol. 9, pp. 211–407, Aug. 2014. [Online]. Available: http://dx.doi.org/10.1561/0400000042

[6] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge Univ. Press, 2011.

[7] I. Csiszár, "The method of types [information theory]," *IEEE Trans. on Info. Th.*, vol. 44, no. 6, pp. 2505–2523, Oct 1998.

[8] Y. Baryshnikov, J. J. Duda, and W. Szpankowski, "Types of markov fields and tilings," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4361–4375, Aug 2016.

[9] I. Csiszár, "Information-type measures of difference of probability distributions and indirect observations," *Studia Scientiarum Mathematicarum Hungarica*, vol. 2, pp. 299–318, 1967.

[10] ——, "Information Measures: A Critical Survey," in *Transactions of the Seventh Prague Conference on Information Theory, Statistical Decision Functions, Random Processes*. Dordrecht: D. Riedel, 1978, pp. 73–86.

[11] M. Beck and S. Robins, *Computing the Continuous Discretely : Integer-Point Enumeration in Polyhedra*, 2nd ed. Springer, 2015.

[12] A. Ghosh, T. Roughgarden, and M. Sundararajan, "Universally utility-maximizing privacy mechanisms," *SIAM Journal on Computing*, vol. 41, no. 6, pp. 1673–1693, 2012. [Online]. Available: http://dx.doi.org/10.1137/09076828X

[13] H. Brenner and K. Nissim, "Impossibility of differentially private universally optimal mechanisms," in *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, ser. FOCS '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 71–80. [Online]. Available: http://dx.doi.org/10.1109/FOCS.2010.13

[14] Q. Geng and P. Viswanath, "Optimal noise adding mechanisms for approximate differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 952–969, Feb 2016.

[15] ——, "The optimal noise-adding mechanism in differential privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 2, pp. 925–951, Feb 2016.

[16] Q. Geng, P. Kairouz, S. Oh, and P. Viswanath, "The staircase mechanism in differential privacy," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1176–1184, Oct 2015.

[17] G. Pólya and G. Szeg o, *Problems and Theorems in Analysis*. Springer, 1976, vol. 2.

[18] ——, *Problems and Theorems in Analysis*. Springer, 1976, vol. 1.

[19] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 9, pp. 5018–5029, Sept 2016.

[20] M. Hardt and K. Talwar, "On the geometry of differential privacy," in *Proceedings of the Forty-second ACM Symposium on Theory of Computing*, ser. STOC '10. New York, NY, USA: ACM, 2010, pp. 705–714.

[21] W. Szpankowski and S. Verdu, "Minimum expected length of fixed-to-variable lossless compression without prefix constraints," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4017–4025, July 2011.

[22] J. H. Conway and N. J. A. Sloane, "Low–dimensional lattices. vii. coordination sequences," *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 453, no. 1966, pp. 2369–2389, 1997. [Online]. Available: http://rspa.royalsocietypublishing.org/content/453/1966/2369

[23] A. Padakandla, P. R. Kumar, and W. Szpankowski, "The Trade-off between Privacy and Fidelity via Ehrhart Theory," available at https://www.cs.purdue.edu/homes/arunpr/preprints/UtilityPrivacy.pdf.

[24] D. Bertsimas and J. Tsitsiklis, *Introduction to Linear Optimization*, 1st ed. Athena Scientific, 1997.