Unconditional Differentially Private Mechanisms for Linear Queries

Aditya Bhaskara
Princeton University
bhaskara@cs.princeton.edu

Daniel Dadush
Georgia Institute of Technology
dndadush@gatech.edu

Ravishankar Krishnaswamy
Carnegie Mellon University
ravishan@cs.cmu.edu

Kunal Talwar
Microsoft Research SVC
kunal@microsoft.com

ABSTRACT

We investigate the problem of designing differentially private mechanisms for a set of d linear queries over a database, while adding as little error as possible. Hardt and Talwar [HT10] related this problem to geometric properties of a convex body defined by the set of queries and gave a $O(\log^3 d)$-approximation to the minimum ℓ_2^2 error, assuming a conjecture from convex geometry called the *Slicing* or *Hyperplane* conjecture. In this work we give a mechanism that works unconditionally, and also gives an improved $O(\log^2 d)$ approximation to the expected ℓ_2^2 error.

We remove the dependence on the Slicing conjecture by using a result of Klartag [Kla06] that shows that any convex body is close to one for which the conjecture holds; our main contribution is in making this result constructive by using recent techniques of Dadush, Peikert and Vempala [DPV10]. The improvement in approximation ratio relies on a stronger lower bound we derive on the optimum. This new lower bound goes beyond the packing argument that has traditionally been used in Differential Privacy and allows us to *add* the packing lower bounds obtained from orthogonal subspaces. We are able to achieve this via a *symmetrization* argument which argues that there always exists a near optimal differentially private mechanism which adds noise that is *independent of the input database!* We believe this result should be of independent interest, and also discuss some interesting consequences.

Categories and Subject Descriptors

F.0 [**Theory of Computation**]: General

General Terms

Algorithms, Theory

Keywords

Differential Privacy, Slicing conjecture

1. INTRODUCTION

Several organizations such as the census bureau and various corporations collect potentially sensitive data about individuals, e.g. the census records, health records, social network and search data, etc. Mining this data can help learn useful aggregate information about the population, e.g. the effectiveness of treatments, and social trends. At the same time, there are often ethical, legal or business reasons to ensure that the private information of individuals contributing to the database is not revealed. This has led to considerable interest in privacy preserving data analysis. Differential Privacy is recent privacy definition [DMNS06] that gives formal guarantees that the output of the mechanism does not compromise the privacy of individual contributing to the database even in the presence of auxiliary information. Differentially private mechanisms are randomized algorithms whose output distribution does not change significantly when one individual's data is added/removed. This is typically achieved by giving noisy answers to queries and for the answers to be useful, one would like to add as little noise as possible. Rather surprisingly, in many settings a large number of aggregate queries can be answered with a small amount of noise while maintaining differential privacy.

A lot of recent research has focused on understanding how little noise a differentially private mechanism can get away with. This work continues that line of research. We consider the question in the context of linear queries over databases represented as vectors in $\Re^n$. Two databases are considered neighboring if their ℓ_1 distance (or distance with respect to any other given norm) is at most 1. We represent a linear query by a $d \times n$ matrix F so that the correct answer on a database x is given by $Fx \in \Re^d$. A mechanism M_F outputs a vector $a \in \Re^d$.

Definition 1.1. *We say that M satisfies ε-differential privacy with respect to $|\cdot|$ if for any $x, x' \in \Re^n$, and for any measurable $S \subseteq \Re^d$,*

$$\frac{Pr[M(x) \in S]}{Pr[M(x') \in S]} \leq exp(\varepsilon|x - x'|)$$

Here $|\cdot|$ is an arbitrary norm on $\Re^n$. While our results hold for any norm, the ℓ_1 norm has the most applications in data analysis and we will present all results for this special case.

Error of the Mechanism. In this paper, we measure the quality of the mechanism by its worst case expected ℓ_2^2 error $err(M,F) \stackrel{def}{=} \sup_{x\in\Re^n} \mathbb{E}[\|M_F(x) - Fx\|_2^2]$ where the expectation is taken over the internal randomness of the mechanism. Denote by $err(F)$ the minimum of $err(M,F)$ over all ε-differentially private mechanisms F.

This setting was previously considered by Hardt and Talwar [HT10] who related the problem to geometric properties of a convex body defined by the queries.[1] They gave upper and lower bounds on the quantity $err(F)$, and showed that the two were within an $O(\log^3 d)$ factor of each other assuming a long-standing conjecture due to Bourgain known as the Slicing or the Hyperplane conjecture.

Our Results. In this work, we improve on this result in two ways. First, we give a new mechanism that gets near optimal error *unconditionally*, i.e., without reliance on the Slicing conjecture. We achieve this by combining techniques from the recent results of Klartag [Kla06] (which shows that any convex body is "close" to another that satisfies the hyperplane conjecture), and Dadush, Peikert and Vempala [DPV10] (which makes some of these results constructive). In addition, we note that Klartag's construction by itself does not suffice for us, and this forces us to suitably strengthen it to make it applicable in our setting.

Secondly, we improve the approximation ratio to $O(\log^2 d)$. This is done using a stronger lower bound on $err(F)$ that goes beyond the *packing argument*. Informally, nearly all previous lower bounds are shown by constructing a number of "close" databases, the answers for which are "far" from each other. We strengthen this approach by showing that packing-based lower bounds over orthogonal subspaces can be added together to get a stronger bound. This improvement relies on a symmetrization argument that shows that for differentially private mechanisms for linear queries of the form considered, it suffices to consider mechanisms that add *database-independent* noise. This fact should be of independent interest and we point out some other consequences later in section 1.

A Note about the Model

As in [HT10], our model uses ℓ_1 neighborhoods instead of the more traditional Hamming distance. Nevertheless, this model captures several settings. The most common example is linear queries over histograms, including contingency tables. These play an important role in statistics and their differentially private release has been studied previously by Barak et al. [BCD$^+$07] and Kasiviswanathan et al. [KRSU10]. Other examples include settings such as the work of McSherry and Mironov [MM09] where a natural transformation of the data converts a Hamming neighborhood to an ℓ_1 (or an ℓ_2) neighborhood. We refer the reader to [HT10] for further applications. Moreover, the fact that this definition of privacy assumes that the mechanism is defined for all $x \in \Re^n$ (as opposed to just $x \in \mathbb{Z}_+^n$), makes the upper bound results stronger and applicable in settings such as [MM09] where the stronger guarantee is needed. On the other hand, this also makes the lower bound weaker by allowing us to compete against a higher benchmark. But as shown in [HT10], for small enough ε, these lower bounds (over all ℓ_1) are not significantly higher than those defined over hamming distances. Moreover, all known mechanisms satisfy the stronger definitions we impose. Finally, recent work by De [De11] has shown that the lower bounds on $err(F)$ for certain specific F's shown in [HT10] can be extended to hold under the weaker definition as well. We leave open the question of whether for some F the two definitions lead to different error bounds.

We remark that a lot of previous work has looked at the question of the upper and lower bounding the worst case error over some family of functions, i.e. $\sup_{F\in\mathcal{F}} err(F)$. For example $\mathcal{F}$ may correspond to d sensitivity 1 queries [DN03, DMNS06] or low sensitivity queries coming from a concept class of low VC dimension [BLR08]. Such *absolute* guarantees on the error can be extremely useful and allow us to prove general results for large families of queries. However, for a specific query F at hand, they may be overly pessimistic when there is more structure in F. In some such cases, one can morph the query F to an F' so that the mechanism's answers on F' can be used to get a much lower error on F than would result by using the mechanism on F directly (see e.g. [BCD$^+$07] for a very specific F and [LHR$^+$10] for more general techniques).

The algorithmic problem of estimating $err(F)$ for a given F received attention first only in [HT10] (see also [GRS09]). Such *relative* guarantees may lead to mechanisms that add significantly less noise than the general case for specific F's of interest, and avoid the problem of optimizing the way in which a set of queries is asked as in [BCD$^+$07, LHR$^+$10]. Instead the relative guarantee directly ensures that the mechanism adds not much more error than the best possible rephrasing could have given. Thus designing mechanisms that give such a relative guarantee may be immensely valuable, and this is a promising avenue for research.

Open Problems

We leave open several natural questions. The algorithms in [HT10] and in this work involve sampling from convex bodies which can be done in polynomial but unreasonably large running time. While specific cases (such as when the relevant norm is ℓ_2 instead of ℓ_1 so that K is an ellipse) have simple and practical implementations, it is natural to demand practical algorithms for more general settings. Moreover, extending such results for more general queries (not just linear) would require new techniques.

Starting with the work of Blum, Ligett and Roth [BLR08], several recent works have given significantly better absolute bounds for large class of F's under the assumption that the vector x (in our notation) has small ℓ_1 norm. Such upper bounds are interesting and useful. The problem of getting relative guarantees on $err(F)$ given F and an upper bound on $|x|_1$ is a compelling one.

Finally our mechanism is non-interactive: it needs to know the whole query F in advance. Allowing online queries, where we get rows of F one at a time, leads to a natural question in online algorithms.

Related Work

Dwork et al. [DMNS06] showed the first general upper bound showing that any query can be released while adding noise proportional to the total *sensitivity* of the query. Nis-

[1] A minor technical difference is that they consider the ℓ_2 error instead of ℓ_2^2, but their results proceed by approximating the ℓ_2^2 error.

sim, Raskhodnikova and Smith [NRS07] showed that adding noise proportional to (a smoothed version of) the *local sensitivity* of the query suffices for guaranteeing differential privacy; this may be much smaller than the worst case sensitivity for non-linear queries. Lower bounds on the amount of noise needed for general low sensitivity queries have been shown in [DN03, DMT07, DY08, DMNS06, RHS07, HT10, De11]. Kasiviswathan et al. [KRSU10] showed upper and lower bounds for contingency table queries.

Blum, Ligett and Roth [BLR08] used learning theory techniques and the exponential mechanism [MT07] to allow answering a large number of queries of small VC dimension with error small compared to the number of individuals in the database. This line of work has been further extended and improved in terms of error bounds, efficiency, generality and interactivity in several subsequent works [DNR$^+$09, DRV10, RR10, HR10].

Ghosh, Roughgarden and Sundarajan [GRS09] showed that for a one dimensional counting query, the Laplacian mechanism is optimal in a very general utilitarian framework and Gupte and Sundararajan [GS10] extended this to risk averse agents. Brenner and Nissim [BN10] showed that such universally optimal private mechanisms do not exist for two counting queries or for a single non binary sum query. As mentioned above, Hardt and Talwar [HT10] considered relative guarantees for multi-dimensional queries, and their techniques also showed tight lower bounds for the class of low sensitivity linear queries. De [De11] unified and strengthened these bounds and showed stronger lower bounds for the class of non-linear low sensitivity queries.

Techniques

The key idea in the "K-norm" mechanism proposed by Hardt and Talwar [HT10] is to add noise *proportional* to the convex body $K = AB_1^n$, instead of independent Laplacian noise in each direction. The average noise (in ℓ_2^2) added in this mechanism then turns out to be roughly proportional to $\mathbb{E}_K \|x\|_2^2$. For convex bodies K that are in *approximately isotropic* position (to be defined soon), a well-studied conjecture in convex geometry (called the Slicing conjecture) says that this quantity is within a constant factor of the volume when scaled appropriately. Hardt and Talwar then prove a lower bound on the noise of an optimal mechanism in terms of the volume of K, thus concluding that the mechanism is nearly *optimum* in terms of the error if K is almost isotropic, assuming the Slicing conjecture.

There are two crucial deficiencies of the above mechanism. Firstly, they are only able to show constant-factor bounds in the error if the body K is nearly isotropic. If the body is far from isotropic, Hardt and Talwar propose a recursive mechanism and show that it is optimal up to a factor $O(\log^3 d)$. The main idea is that if K is not isotropic, we can find the *long* and *short* axes of K by computing its covariance matrix, and add noise to different extents along these axes (in particular, if there is only one dominant eigenvalue, this view lets us think about the problem as effectively being 1-dimensional). The two main issues which the [HT10] leave open are that of avoiding the dependence on the Hyperplane conjecture, and whether we can get improved approximation results.

Our main technical tool for avoiding dependence on the Hyperplane conjecture is the result by Klartag [Kla06] on the existence of perturbations of convex bodies with a small *isotropic constant.* More formally, for any convex body $K \subseteq \mathbb{R}^d$, there exists a K' and a translate x_0 such that $(1-\varepsilon)(K'-x_0) \subseteq (K-x_0) \subseteq (K'-x_0)$, and $L_{K'} \leq \frac{c}{\sqrt{\varepsilon}}$ for some absolute constant c. Our idea is to sample the noise vector from this body K' instead of K: the fact that K' has a bounded isotropic constant lets us relate the error of our mechanism to the volume of K', and the fact that K' approximates K allows us to relate their volumes. While it is tempting to use this result to bypass the hyperplane conjecture, the issue now is that the body K' is not centered at the origin, and the average length of a random vector can be related to its volume only if the body is centered at the origin. On the other hand, if we translate K' to the origin, it only approximates $K - x_0$, and we have no control over the length of x_0. We circumvent this by using convolution based arguments to *symmetrize* the body K'. To convert this to an algorithm, we need constructive versions of all the above ideas. We refer the reader to Section 6 for more details about these issues and how we resolve them.

The improved approximation ratio, as mentioned derives primarily from a stronger lower bound. We first show using a novel symmetrization argument that for differentially private mechanisms for linear queries, one can assume that the distribution of $M(x) - Fx$ is independent of x; in other words, *oblivious noise* mechanism are close to optimal. This result, though simple, is of independent interest and should have other applications. As an example, Kasiviswanathan et al. [KRSU10] show lower bounds for differentially private mechanisms for contingency table queries, and somewhat stronger lower bounds for oblivious noise mechanisms. Our symmetrization result implies that their stronger lower bounds hold for all differentially private mechanisms.

2. PRELIMINARIES

We will write B_p^d to denote the unit ball of the p-norm in $\Re^d$. When $K \subseteq \Re^d$ is a centrally symmetric convex set, we write $\|\cdot\|_K$ for the (Minkowski) norm defined by K (i.e. $\|x\|_K = \inf\{r\colon x \in rK\}$). The ℓ_p-norms are denoted by $\|\cdot\|_p$, but we use $\|\cdot\|$ as a shorthand for the Euclidean norm $\|\cdot\|_2$. Given a function $F : \mathbb{R}^{d_1} \to \mathbb{R}^{d_2}$ and a set $K \subseteq \mathbb{R}^{d_1}$, FK denotes the set $\{F(x) : x \in K\}$. Finally, given a subspace V of $\mathbb{R}^d$, we denote by Π_V the *projection operator* onto the space V. Thus for a vector $u \in \mathbb{R}^d$, $\Pi_V(u)$ denotes the projection of u to the space V.

Throughout, c, C will denote absolute constants, and may vary from one occurrence to the next.

2.1 Convex Geometry

We review some elementary facts from convex geometry.

DEFINITION 2.1 (ISOTROPIC POSITION). *We say a convex body $K \subseteq \mathbb{R}^d$ is in* isotropic position *if its moment matrix is the identity $I_{d\times d}$. Recall that the moment matrix of K has entries $M_{i,j}$,*

$$M_{i,j} := \int_{\mathbb{R}^d} \mathbf{1}_K x_i x_j \, dx,$$

where $\mathbf{1}_K$ is the indicator function of the body K, and the integral is taken with the Lebesgue measure in $\mathbb{R}^d$. Furthermore, it is a simple fact that any $K \subseteq \mathbb{R}^d$ which is not contained in a $(d-1)$ dimensional subspace can be placed in isotropic position by using an invertible linear transformation.

Definition 2.2 (Isotropic constant). *Let K be a convex body in $\mathbb{R}^d$, and $M(K)$ be its moment (or covariance) matrix. The Isotropic constant is defined by*

$$L_K^{2d} = \frac{\det M(K)}{\mathsf{Vol}(K)^2},$$

where $\mathsf{Vol}(K)$ *denotes the d-dimensional volume.*

Note that the definition of isotropic constant is affine invariant. It is a fundamental property of a convex body, and a central conjecture in convex geometry is the so-called 'slicing' or 'hyperplane' conjecture, which says that $L_K \leq C$, for some absolute constant C (independent of the body and the dimension d). The conjecture derives its name from the connection to volumes of sections of convex bodies. The best known bounds for L_K in general are $c \leq L_K \leq Cd^{1/4}$.

We refer the reader to the early work by Milman and Pajor [MP89b], as well as the extensive survey of Giannopoulos [Gia03] for more facts regarding the isotropic constant. A final piece of notation we will use throughout is that of projections: for any convex body $K \subseteq \mathbb{R}^d$, and any subspace V of $\mathbb{R}^d$, we let $\Pi_V(K)$ denote the projection of K onto the subspace V.

3. THE IMPROVED MECHANISM

In this section, we present a modified version of the recursive mechanism of Hardt and Talwar [HT10]. The main change to the HT algorithm is in incorporating the constructive form of Klartag's result [Kla06], which shows that for any convex body K, there is a perturbation of K which has bounded isotropic constant.

The Perturb subroutine. The algorithm uses the procedure $\mathsf{Perturb}(K)$, which, given a convex body $K \subseteq \mathbb{R}^d$ returns a body $K' \subseteq \mathbb{R}^d$ with the following properties

1. $(1/2)K' \subseteq K \subseteq K'$, for an absolute constant c.
2. K' is centrally symmetric.
3. $L_{K'} < C$ for an absolute constant C.

When we say the procedure "returns" K', we mean that we can efficiently obtain uniform samples from K', and compute the moment matrix of K'. The exact subroutine for Perturb is presented in Section 5. A point to note here is that the procedure for sampling as well as that to compute the moment matrix will be *approximate* (i.e., the sample distribution will be "close to" uniform, and the matrix will be a good approximation to the moment matrix), but this is a technical matter and we do not go into the details at present.

We now present the procedure used to add noise, which we call noiseHT, to denote the fact that we use the convex perturbation K' instead of the original convex body K in the algorithm in [HT10]. [2]

The overall mechanism now, for an input database x, is to return $Fx + \mathsf{noiseHT}(K, F, d)$.

As promised before, our main improvements over [HT10] are (i) we avoid the dependence on the hyperplane conjecture, and (ii) we get an improved analysis for the approximation factor of the ℓ_2^2 error from $O(\log^3 d)$ to $O(\log^2 d)$.

[2] In the description, $\mathrm{Gamma}(k, \theta)(r)$ denotes the distribution $f(r) := r^{k-1} \frac{e^{-r/\theta}}{\Gamma(k)\theta^k}$ where $\Gamma(k) = \int e^{-r} r^{k-1} dr$ denotes the Gamma function.

procedure $\mathsf{noiseHT}(K, F, d)$
  // convex body K, query matrix F, dimension d
begin
1 Let $K' = \mathsf{Perturb}(K)$, and let $M(K')$ denote its moment matrix.
2 Let the eigenvalues of $M(K')$ (in non-increasing order) be $\lambda_1, \lambda_2, \ldots, \lambda_d$, and pick a corresponding orthonormal eigenbasis $u_1, \ldots u_d$.
3 Let $d' = \lfloor d/2 \rfloor$, and let $U = \mathrm{span}(u_1, \ldots, u_{d'})$ and $V = \mathrm{span}(u_{d'+1}, \ldots, u_d)$.
4 Sample $a \sim \mathrm{Uniform}(K')$ and $r \sim \mathrm{Gamma}(d+1, \varepsilon^{-1})$.
5 If $d = 1$, return ra. Otherwise return $\mathsf{noiseHT}(\Pi_U K, \Pi_U F, d') + \Pi_V(ra)$.
end

We now explain how our algorithm achieves these improvements.

Bypassing the Hyperplane Conjecture. Notice that if the algorithm uses K at all places instead of K', then it is exactly the algorithm presented in [HT10]. Indeed, sampling from K' instead of K in Step 4 is the crucial step in bypassing the hyperplane conjecture. The main computational issue here is in ensuring that we can efficiently sample from the body K'. We present these details in Sections 5 and 6.

Improved Error Analysis. The analysis of [HT10] proceeds by *charging* the expected squared error $\mathbb{E}[\|\Pi_V(ra)\|^2]$ to the quantity $f(d)\mathsf{Vol}_d(K)^{2/d}$, for an appropriate function $f(d)$. Thus the total squared error in the recursive process can then be bounded in terms of

$$f(d)\mathsf{Vol}_d(K)^{2/d} + f(d')\mathsf{Vol}_{d'}(\Pi_U K)^{2/d'} + \ldots \qquad (1)$$

The lower bound argument of [HT10] shows that each of these terms is a lower bound on the error of an ε-private mechanism, and this can be used to show that the total error is at most a $O(\log^3 d)$ factor of the error of any optimal ε-differentially private mechanism.

Our lower bound in Section 4 attempts to give an improvement in precisely such a scenario: if we have lower bound on the error in orthogonal subspaces, then we show that the sum of these quantities is also a lower bound on the overall error of any ε-differentially private mechanism. However, the difficulty in using this directly in the mechanism presented above is the following: In (1), the spaces onto which K is projected are not orthogonal to each other (in fact they are a sequence of spaces each *containing* the next).

While we can rectify this by using a more involved charging scheme (the complete details of which are presented in Section 7), we would be in much better shape if we can actually charge the error in each level of recursion to volume of the "discarded subspace" V, as this would ensure that the volumes we charge to are all mutually orthogonal. Unfortunately, this is not possible if the convex body is highly skewed: in this case $\Pi_V(K)$ (the projection of K onto V) has too small a volume to charge the error to. To fix this, we show that by carefully choosing the subspace V to project to, we can ensure that the volume of $\Pi_V(K)$ is large enough to charge the error to. Let us thus present a modified mechanism which, in addition to using the convex perturbation

K', also chooses the subspace V in a different way to greatly simplify the analysis.

As mentioned, we will also show the privacy and error analysis of the basic algorithm noiseHT in Section 7.

3.1 A Modified Mechanism

The mechanism follows the same basic outline: we come up with a $d/2$ dimensional subspace V, add noise first in this subspace, and recursively use this procedure to generate independent noise on $V^\perp$. However, while the HT mechanism chooses V to be the subspace spanned by the smallest $d/2$ eigenvectors of $M(K)$, the current mechanism chooses V more carefully. Intuitively, it picks a $d/2$ dimensional subspace V s.t. the projection of the moment ellipsoid $M(K')$ onto V is a sphere of appropriate radius.

```
procedure noiseNew(K, F, d)    // convex body K, query matrix F, dimension d
begin
1   Let K' = Perturb(K), and let M(K') denote its moment matrix.
2   Let V ← choose-subspace(M(K')), a procedure described below. Let V^⊥ denote the subspace orthogonal to V.
3   Sample a ~ Uniform(K') and r ~ Gamma(d + 1, ε^{-1}).^3
4   If d = 1, return ra. Otherwise return noiseNew(Π_{V^⊥} K, Π_{V^⊥} F, ⌊d/2⌋) + Π_V(ra).
end
```

As before, the overall mechanism given an input database x is to return $Fx+$ noiseNew(K, F, d). Let us now describe choose-subspace. The lemma following it shows that choose-subspace always finds the appropriate scalars.

```
procedure choose-subspace(M)    // d × d positive definite matrix M
begin
1   Let the eigenvalues of M (in non-increasing order) be λ_1, λ_2, ..., λ_d, and pick a corresponding orthonormal eigenbasis u_1, u_2, ..., u_d.
2   For i ∈ 1, ..., ⌈d/2⌉. If λ_{⌈d/2⌉} = λ_i, set v_i = u_i. Otherwise set v_i = a_i u_i + b_i u_{n−i+1}, for scalars a_i, b_i > 0 satisfying the relations ‖v_i‖ = 1 and v_i^t M v_i = λ_{⌈d/2⌉}.
3   Return V = span(v_1, ..., v_{⌈d/2⌉}).
end
```

Lemma 3.1. *Let M be a positive definite matrix, and let $\lambda_1, \dots, \lambda_n$ denote the eigenvalues of M in non-decreasing order. Then on input M, algorithm choose-subspace outputs a subspace $V \subseteq \mathbb{R}^n$ s.t.*

$$\forall x \in V,\ x^t M x = \lambda_{\lceil d/2 \rceil} \|x\|^2.$$

Proof: In order to help with the notation in the proof, we first make explicit the choice of the coefficients a_i, b_i referred to in the above procedure choose-subspace. For $i \in 1, \dots, \lceil n/2 \rceil - 1$, define

$$\beta_i = \frac{\lambda_{\lceil d/2 \rceil} - \lambda_{d-i+1}}{\lambda_i - \lambda_{d-i+1}}, \tag{2}$$

$$\alpha_i = \begin{cases} \frac{\beta_i - \sqrt{\beta_i(1-\beta_i)}}{2\beta_i - 1} & : \beta \neq 1/2 \\ 1/2 & : \text{otherwise} \end{cases}, \tag{3}$$

$$a_i = \frac{\alpha_i}{\sqrt{\alpha_i^2 + (1-\alpha_i)^2}}, b_i = \frac{1-\alpha_i}{\sqrt{\alpha_i^2 + (1-\alpha_i)^2}} \tag{4}$$

First, note that $0 \le \beta_i \le 1$ since $\lambda_i \ge \lambda_{\lceil d/2 \rceil} \ge \lambda_{d-i+1}$. A direct computation reveals the identity $\frac{\alpha_i^2}{\alpha_i^2 + (1-\alpha_i)^2} = \beta_i$. Now since the u_i's are orthonormal, we have that $\|v_i\|^2 = \|a_i u_i + b_i u_{d+1-i}\|^2 = a_i^2 + b_i^2 = \frac{\alpha_i^2}{\alpha_i^2 + (1-\alpha_i)^2} = 1$. Next, since the u_i's form an eigenbasis of M, we have that

$$\begin{aligned} v_i^t M v_i &= a_i^2 \lambda_i + b_i^2 \lambda_{d-i+1} & (5) \\ &= \frac{\alpha_i^2 \lambda_i}{\alpha_i^2 + (1-\alpha)^2} + \frac{(1-\alpha_i)^2 \lambda_{d-i+1}}{\alpha_i^2 + (1-\alpha_i)^2} & (6) \\ &= \beta_i \lambda_i + (1-\beta_i)\lambda_{d-i+1} = \lambda_{\lceil d/2 \rceil} & (7) \end{aligned}$$

Next, since the v_i's are generated by vectors in orthogonal eigenspaces of M, we have that $v_i^t M v_j = 0$ for distinct i, j. Then, for any $x \in V = \text{span}(v_1, \dots, v_{\lceil d/2 \rceil})$ we have that $x = \sum_{i=1}^{\lceil d/2 \rceil} (v_i^t x) v_i$ (since the v_i's are orthonormal), and hence

$$x^t M x = \sum_{i=1}^{\lceil d/2 \rceil} \lambda_{\lceil d/2 \rceil} (v_i^t x)^2 = \lambda_{\lceil d/2 \rceil} \|x\|^2 \text{ as needed.}$$

■

For a matrix $M \in \mathbb{R}^{d \times d}$ and a linear subspace V, $\dim(V) = k$, define $\det(M_V)$ as $\det(B^t M B)$, where $B = (b_1, \dots, b_k)$, and $b_1, \dots, b_k$ form an orthonormal basis for V (note that the definition does not depend on the choice of basis).

We now give lower bounds on projection volumes for convex bodies. This generalizes Proposition 7.1 of [HT10] to general projections (from projections onto eigenspaces).

Lemma 3.2. *Let $K \subseteq \mathbb{R}^d$ be a symmetric convex body with moment matrix M. Then for a linear subspace V, $\dim(V) = k$, we have that*

$$\mathsf{Vol}(\Pi_V(K))^{\frac{1}{k}} = \Omega\left(\sqrt{\frac{d}{k}} L_K^{-\frac{d}{k}} \det(M_V)^{\frac{1}{2k}}\right)$$

Proof: Let $E = \{x : xM^{-1}x \le 1\}$ denote the inertial ellipsoid of K. A standard computation reveals that

$$\begin{aligned} \mathsf{Vol}(\pi_V(\sqrt{d}E))^{\frac{1}{k}} &= \sqrt{d}\mathsf{Vol}(B_2^k)^{\frac{1}{k}} \det(M_V)^{\frac{1}{2k}} \\ &= \Theta\left(\sqrt{\frac{d}{k}} \det(M_V)^{\frac{1}{2k}}\right) \end{aligned}$$

For convex bodies $A, B \subseteq \mathbb{R}^d$, define $N(A, B) = \min\{|\Lambda| : A \subseteq \Lambda + B\}$, i.e. the minimum number of translates of B needed to cover A. For symmetric convex bodies, we have the classical inequality $N(A, B) \le 3^d \frac{\mathsf{Vol}(A)}{\mathsf{Vol}(A \cap B)}$. Therefore

$$N(2\sqrt{d}E, K) \le 3^d \frac{\mathsf{Vol}(2\sqrt{d}E)}{\mathsf{Vol}(2\sqrt{d}E \cap K)} \le C^d \frac{\det(M)^{\frac{1}{2}}}{\mathsf{Vol}(2\sqrt{d}E \cap K)}$$

Let X be distributed as uniform(K). By definition, we remember that $\mathbb{E}[XX^t] = M$. Then we have that

$$\frac{\mathsf{Vol}(2\sqrt{d}E \cap K)}{\mathsf{Vol}(K)} = 1 - \mathbb{P}[X^t M^{-1} X \geq 4d] \geq 1 - \frac{\mathbb{E}[X^t M^{-1} X]}{4d}$$
$$= 1 - \frac{d}{4d} = \frac{3}{4}$$

Therefore $N(2\sqrt{d}E, K) \leq C^d \frac{\det(M)^{\frac{1}{2}}}{\mathsf{Vol}(K)} \leq C^d L_K^d$. Hence

$$\mathsf{Vol}(\pi_V(K))^{\frac{1}{k}} \geq \mathsf{Vol}(\pi_V(\sqrt{d}E))^{\frac{1}{k}} N(\sqrt{d}E, K)^{-\frac{1}{k}}$$
$$= \Omega\left(\sqrt{\frac{d}{k}} L_K^{-\frac{d}{k}} \det(M_V)^{\frac{1}{2k}}\right)$$

as needed. ∎

We now upper bound the error produced by the mechanism on the subspace V, in terms of the volume of the projection. The fact that K' has a small isotropic constant will be important here.

Lemma 3.3. *Let $K', V \subseteq \mathbb{R}^d$, $r \sim$ uniform(K') and $a \sim$ Gamma$(d+1, \varepsilon^{-1})$ be as in step 4 of algorithm noise. Then*

$$\mathbb{E}[\|\Pi_V(ra)\|^2] = O\left(\frac{d^3}{\varepsilon^2} \mathsf{Vol}(\Pi_V(K))^{2/\lceil d/2 \rceil}\right)$$

Proof: Let $d' = \lceil d/2 \rceil$, and let $v_1, \dots, v_{d'}$ denote an orthonormal basis of V. By construction of V, we remember that $v_i^t M(K') v_i = \lambda_{d'} \|v_i\|^2 = \lambda_{d'}$ for $1 \leq i \leq d'$, where $\lambda_{d'}$ is the corresponding eigenvalue of $M(K')$. Now we have that

$$\mathbb{E}\left[\|\Pi_V(ra)\|^2\right] = \mathbb{E}\left[\sum_{i=1}^{d'} \langle v_i, ra \rangle^2\right] \tag{8}$$
$$= \mathbb{E}\left[a^2\right] \mathbb{E}\left[\sum_{i=1}^{d'} \langle v_i, r \rangle^2\right] \tag{9}$$
$$= \frac{(d+1)(d+2)}{\varepsilon^2} \sum_{i=1}^{d'} v_i^t M(K') v_i \tag{10}$$
$$= \frac{(d+1)(d+2)}{\varepsilon^2} \cdot (d' \lambda_{d'}) \tag{11}$$

We now need a lower bound on $\mathsf{Vol}_{d'}(\Pi_V(K))$. By construction, $K' \subseteq 2K$, thus $\mathsf{Vol}_{d'}(\Pi_V(K))^{\frac{1}{d'}} \geq \frac{1}{2} \mathsf{Vol}_{d'}(\Pi_V(K'))^{\frac{1}{d'}}$. Now by Lemma 3.2, we have that

$$\mathsf{Vol}_{d'}(\Pi_V(K'))^{\frac{1}{d'}} = \Omega\left(\sqrt{\frac{d}{d'}} L_{K'}^{-\frac{d}{d'}} \det(M(K')_V)^{\frac{1}{2d'}}\right) = \Omega(\lambda_{d'}^{\frac{1}{2}})$$

since $L_{K'} = O(1)$, $d \leq 2d'$. Thus combining the observations above, we have

$$\mathbb{E}[\|\Pi_V(ra)\|^2] = O\left(\frac{d^3}{\varepsilon^2} \mathsf{Vol}(\Pi_V(K))^{2/d'}\right).$$

This completes the proof. ∎

Using the above for each level of the recursion, we have the following corollary.

Corollary 3.4. *Let $V_1, \dots, V_r \subseteq \mathbb{R}^d$ denote the sequence of subspaces computed during the execution of* noise(K, F, d), *and let $d_1, \dots, d_r$ denote their corresponding dimensions. Then the V_i's are all mutually orthogonal, and the total squared error generated by the mechanism at most*

$$O\left(\frac{d^3}{\varepsilon^2} \sum_{i=1}^{k} \mathsf{Vol}_{d_i}(\Pi_{V_i}(K))^{\frac{2}{d_i}}\right).$$

We are now fully equipped to complete the analysis of the above mechanism.

3.2 Privacy Analysis

Since our algorithm is only a small modification (using K' instead of K), the privacy analysis almost carries through unchanged. Indeed, in Section 4 of [HT10], the authors show that for any convex body $L \subseteq \mathbb{R}^d$, the distribution $r \cdot u$, where $r \sim$ Gamma$(d+1, \varepsilon^{-1})$ and $u \sim$ Uniform(L) has p.d.f. at x proportional to $e^{-\varepsilon \|x\|_L}$. We use this at each level of the recursive procedure noiseNew in order to obtain our privacy guarantee.

Consider two databases x, x' with $\|x - x'\|_1 \leq 1$. Notice that different levels in our algorithm add noise along mutually orthogonal subspaces. Therefore, if the mechanism is ε-differentially private in each subspace, the *joint* distribution will be $\varepsilon \log d$ differentially private (this is well known, e.g., refer to [HT10]), which implies that our overall mechanism is $\varepsilon \log d$-differentially private.

To this end, consider some level of the recursion. For any y, the p.d.f value of $M(x)$ returning y is precisely $\frac{1}{Z} e^{-\varepsilon \|y - Fx\|_{K'}}$, for some normalization Z. Likewise, the p.d.f value of $M(x')$ returning y is $\frac{1}{Z} e^{-\varepsilon \|y - Fx'\|_{K'}}$ for the same Z. Thus the ratio of these p.d.f's is at most $e^{\varepsilon \|F(x - x')\|_{K'}}$, which is at most e^{ε}, because $F(x - x') \in FB_1^n = K \subseteq K'$. Thus for any y the probabilities are within a e^{ε} factor of each other, which implies ε-privacy at this level.

3.3 Error Analysis

The error analysis of our algorithm follows immediately from Corollary 3.4 and our (improved) lower bound in Theorem 4.2. Indeed, note that we get that the error of our mechanism is at most $O(1)$ times the lower bound stated in Theorem 4.2 when we use the collection of mutually orthogonal subspaces $\{V_i : 1 \leq i \leq r\}$. This immediately implies that our mechanism is $\varepsilon \log d$-differentially private with error being an $O(1)$-approximation to the optimal error w.r.t the ℓ_2^2 norm. To complete the proof, we simply set $\varepsilon' = \varepsilon / \log d$, and run our mechanism with ε' instead of ε (when choosing the random noise vector in step 3 at each level of recursion), to get an ε-differentially private mechanism that is an $O(\log^2 d)$-approximation w.r.t ℓ_2^2 error. This completes the analysis.

It remains to prove Theorem 4.2, and also show that the perturbed convex body (assumed at the beginning of the section) exists, and we can indeed sample efficiently from it. The following two sections address these issues.

4. A LOWER BOUND ON NOISE

Let $F : \mathbb{R}^n \to \mathbb{R}^d$ denote the query matrix (corresponding to the d linear queries in $\mathbb{R}^n$). As before, let $K = FB_1^n$ denote the convex set in $\mathbb{R}^d$ which is the image of the unit ball under the transformation F.

In [HT10], Hardt and Talwar show a lower bound on the error for *any ε-differentially private* mechanism in terms of the volume of K. Specifically, they show that

THEOREM 4.1. *Let F and K be as defined above, and let V denote any k-dimensional subspace of $\mathbb{R}^d$, and Π_V denote the orthogonal projection operator onto V, for some $1 \leq k \leq d$. Then every ε-differentially private mechanism M must satisfy*

$$\mathsf{err}(M, F) \geq \Omega\left(\frac{k^3}{\varepsilon^2}\ \mathsf{Vol}_k(\Pi_V(K))^{2/k}\right).$$

In the above theorem, the error term $\mathsf{err}(M, F)$ is defined as the maximum over x of the expected squared error added by the mechanism for database x. Formally, $\mathsf{err}(M, F) = \max_{x \in \mathbb{R}^n} \mathbb{E}[||M(x) - F(x)||^2]$.

In this section, we show a much stronger lower bound which is crucial in performing a tighter analysis of the recursive algorithm. Namely, if $V_1, V_2, \ldots, V_t$ are a collection of t mutually orthogonal subspaces of $\mathbb{R}^d$ of dimensions $k_1, k_2, \ldots k_t$ respectively, then every ε-differentially private mechanism must have expected squared error which is at least the *sum* of the respective bounds computed according to the above theorem. Formally,

THEOREM 4.2. *Let F and K be as defined above, and let $V_1, V_2, \ldots, V_t$ be a collection of t mutually orthogonal subspaces of $\mathbb{R}^d$ of dimensions $k_1, k_2, \ldots k_t$ respectively, then every ε-differentially private mechanism must satisfy*

$$\mathsf{err}(M, F) \geq \Omega\left(\sum_i \frac{k_i^3}{\varepsilon^2}\ \mathsf{Vol}_{k_i}(\Pi_{V_i}(K))^{2/k_i}\right).$$

The proof relies on the observation that the arguments of Hardt and Talwar [HT10] are essentially *local packing arguments*, which establish a lower bound on the squared error of the optimal mechanism, *when projected along subspace spanned by the operator* Π_V. This motivates us to argue that if V_1 and V_2 are orthogonal subspaces, then total squared error should be at least the sum of the two lower bounds! However, the primary hurdle towards establishing such an additive form is the following: the lower bound along the individual projections Π_{V_i} show that there exists an input database x_i for which the optimal mechanism adds a significant noise. But what if these x_i's are very different, i.e., the optimal mechanism somehow correlates the noise added and errs along different directions for different input databases?

In the following section, we show that such correlations do not help reduce error. Indeed, the following theorem shows that there is always a near optimal mechanism which adds noise *oblivious* of the input database, i.e., the noise distribution around each $x \in \mathbb{R}^n$ is the same.

4.1 Making the optimal mechanism oblivious

A crucial ingredient in the proof of Theorem 4.2 is the following lemma, which says that we can, without loss of generality, assume the noise to be *oblivious*. Formally, a mechanism M is said to have oblivious noise if the distribution of $M(x) - Fx$ is independent of x.

THEOREM 4.3. *Consider an ε-differentially private mechanism M which has an (worst-case) expected error of* $\mathsf{err}(M, F)$. *Then there is a 2ε-differentially private mechanism M' with oblivious noise, and* $\mathsf{err}(M', F) \leq \mathsf{err}(M, F)$.

Proof: We begin with some notation. Let $\rho(M, x, y)$ denote the probability density function of M returning y when the input database is x. Notice that we have $\int_y \rho(M, x, y) = 1$ by definition, for all $x \in \mathbb{R}^n$. Then, we can express the error of M with respect to the query system F as

$$\mathsf{err}(M, F) = \max_{x \in \mathbb{R}^n} \int_{y \in \mathbb{R}^n} \rho(M, x, y)\, ||Fx - y||_2^2\, dy \tag{12}$$

We can therefore replace the '$\max_{x \in \mathbb{R}^n}$' term with *any* probability density function f over $\mathbb{R}^n$ and still satisfy

$$\mathsf{err}(M, F) \geq \int_{x \in \mathbb{R}^n} f(x) \int_{y \in \mathbb{R}^n} \rho(M, x, y)\, ||Fx - y||_2^2\, dy\ dx \tag{13}$$

Now given an f, we define a new mechanism M_f as below. We later choose f appropriately so that M_f is differentially private.

```
mechanism M_f(F, x)   // query system F, input database x
begin
    Sample x' ∈ R^n according to the pdf f(x').
    Sample y' ∈ R^n according to the error probability ρ(M, x', y').
    Output y to be y := Fx + (y' − Fx').
end
```

Intuitively, the mechanism M_f does the following, regardless of the input database x: it samples a random x' according to distribution f, and adds noise according to what M would add on input x'. Clearly, since the noise added $y - Fx = y' - Fx'$ does not depend on the input x, this mechanism is oblivious.

The following lemma bounds the error of our mechanism M_f in terms of that of M, and the subsequent lemma shows that for a suitable choice of f, the mechanism M_f is 2ε-differentially private. These two lemmas would then complete the proof of Theorem 4.3.

LEMMA 4.4. *For any probability density function f, the expected squared error of the mechanism M_f (as defined above) is at most the expected squared error of M.*

Proof: Since the error is distributed exactly as $y' - Fx'$ (where x' is distributed according to f, and y' is distributed according to $\rho(M, x', y')$), we can express the expected squared error as $\mathsf{err}(M_f, F) =$

$$\int_{x' \in \mathbb{R}^n} f(x') \int_{y' \in \mathbb{R}^n} \rho(M, x', y')\, \left|\left|Fx' - y'\right|\right|_2^2 dy' dx' \tag{14}$$

But now the expression above is identical to the right hand side of (13), and so we get that $\mathsf{err}(M_f, F) \leq \mathsf{err}(M, F)$, which completes the proof. ■

LEMMA 4.5. *There exists a choice of f for which the mechanism M_f is 2ε-differentially private.*

Proof: We prove this by showing that, for all choices of x and z such that $||z - x||_1 \leq 1$, and for all $y \in \mathbb{R}^d$, the probability density functions of M_f outputting y on x and z differ by at most $e^{\pm 2\varepsilon}$. To this end, we first compute the values of $\rho(M_f, x, y)$ and $\rho(M_f, z, y)$, where $x, z \in \mathbb{R}^n$ such that $n = z - x \in B_1^n$ and $y \in \mathbb{R}^d$. Indeed, we have

$$\rho(M_f, x, y) = \int_{x' \in \mathbb{R}^n} f(x')\ \rho(M, x', y - Fx + Fx') dx' \tag{15}$$

The above expression comes out of the following probability calculation: for M_f to output y on input x, it has to sample some x' in Step 1 (which is distributed according to $f(\cdot)$), and then the mechanism M has to add noise vector y' which satisfies $y' - Fx' = y - Fx$ (see Step 3).

Likewise, we also get

$$\rho(M_f, z, y) = \int_{z' \in \mathbb{R}^n} f(z')\ \rho(M, z', y - Fz + Fz')dz'$$
$$= \int_{x' \in \mathbb{R}^n} f(x'+n)\ \rho(M, x'+n, y - Fz + Fx' + Fn)dx'$$
$$= \int_{x' \in \mathbb{R}^n} f(x'+n)\ \rho(M, x'+n, y - Fx + Fx')dx' \quad (16)$$

Above the first equality is by making the substitution $x' = z' - n$, and the second equality follows by noting that $x = z - n$, and so $Fx = Fz - Fn$. Now, since M is ε-differentially private, we know that $\rho(M, x'+n, y - Fx + Fx')$ is within a factor of $e^{\pm\varepsilon|n|_1}$ of the term $\rho(M, x', y - Fx + Fx')$ for every x'. Additionally, if f is also such that $f(x+n)$ and $f(x)$ are within a factor of $e^{\pm\varepsilon|n|_1}$ of each other, then we get that the expression in eq. (16) would be within $e^{\pm 2\varepsilon|n|_1}$ of the expression in eq. (15), which would imply that the mechanism M_f is 2ε-differentially private. A suitable choice for f to achieve this property is $f(x) \propto e^{-\varepsilon||x||_1}$ which is precisely the p.d.f of (a scaled variant of) the multi-dimensional Laplace distribution. This completes the proof. ■

As mentioned earlier, Lemmas 4.4 and 4.5 complete the proof of Theorem 4.3. ■

We note that the choice of f was crucial in the above proof. More näive choices such that f supported at a single point do not guarantee privacy: indeed the mechanism that always outputs zero is perfectly private, but would not stay private under the above transformation with f supported at a point.

We observe that this transformation works also for (ε, δ)-differentially private mechanisms, in which case it gives us an oblivious noise mechanism with $(2\varepsilon, e^{\varepsilon}\delta)$-differentially privacy. As alluded to in the introduction, Kasiviswanathan et al. [KRSU10] proved lower bounds for contingency table queries for (ε, δ)-differentially private mechanisms, and somewhat stronger bounds for oblivious noise (ε, δ)-differentially private mechanisms. A corollary of the above then is that the stronger lower bounds hold for arbitrary (ε, δ)-differentially private mechanisms.

It is now easy to prove theorem 4.2. From the above theorem, we can assume that M adds oblivious noise.

Proof of Theorem 4.2: Let $V_1, V_2, \ldots, V_t$ be a collection of t mutually orthogonal subspaces of $\mathbb{R}^d$ of dimensions $k_1, k_2, \ldots k_t$ respectively. Then we can apply Theorem 4.1 individually to each of the projections Π_{V_i} to get that the (squared) error is at least $\mathsf{err}_i := \Omega\left(\frac{k_i^3}{\varepsilon^2}\ \mathsf{Vol}_{k_i}(\Pi_{V_i}K)^{2/k_i}\right)$. In fact, the proof of the theorem in [HT10] implies that the expected value of the squared error *when projected along subspace* V_i is at least err_i. In other words, there exists some $x^{(i)} \in \mathbb{R}^n$ for which the expected (squared) error added by M when projected along V_i, is large. But now we can use Theorem 4.3 to infer that for *all points* $x \in \mathbb{R}^n$ (and in particular for the point $\vec{0} \in \mathbb{R}^n$), the expected square error when projected along V_i is at least err_i.

To complete the proof, we note that these projections are along mutually orthogonal subspaces, and therefore the total expected squared error for the point $\vec{0}$ is at least $\sum_i \mathsf{err}_i$. ■

5. CONSTRUCTING THE APPROXIMATE BODY K'

Recall (from the beginning of Section 3 where we define the Perturb subroutine) that our aim, given a convex body $K \subseteq \mathbb{R}^n$, is to come up with K' such that the Banach-Mazur distance $d_{BM}(K, K')$ is upper-bounded by a constant c_1, and further the isotropic constant $L_{K'} \le c_2$. Indeed, the recent powerful result of Klartag [Kla06] says that for any K, we can do this with $c_1 = (1+\varepsilon)$, and $c_2 = \frac{1}{\sqrt{\varepsilon}}$. We show in this section how to make the existential proof of [Kla06] constructive (and slightly strengthen it, as we require our body K' to be centrally symmetric for our mechanism). For clarity, we first recall that the Banach-Mazur distance between two convex bodies is defined as

$$d_{BM}(K_1, K_2) = \min_{a,b}\ \frac{b}{a}$$
$$\exists x_1, x_2 \quad \text{s.t. } a(K_1 - x_1) \subseteq (K_2 - x_2) \subseteq b(K_1 - x_1)$$

Before we discuss our modification to Klartag's procedure, let us first explain his proof techniques for obtaining such a perturbation K'. The rough outline is the following: given K, we first come up with a point $s \in \mathbb{R}^n$ by a probabilistic process (to be described shortly). Using this point s and the convex body K, we define a natural log-concave measure over points in $\mathbb{R}^n$, which we will denote f_s. The convex body K' can then be obtained in a deterministic way using this function f_s (corresponding to some kind of level sets w.r.t f_s). We now explain these steps in more detail. In addition to providing a complete exposition of his approach, this will also set up the notation we need.

5.1 An outline of Klartag's proof

The starting point in the proof of [Kla06] is the "equivalence" of convex bodies and log-concave distributions over $\mathbb{R}^n$. This has been studied earlier in different settings, see e.g., [BK05, KM05]. Indeed, much like convex bodies, it is possible to define an analog of the isotropic constant for such log-concave distributions as well. Suppose $f : \mathbb{R}^n \mapsto \mathbb{R}$ is log-concave (which means $\log f$ is concave over $\mathbb{R}^n$). Then the isotropic constant of f is defined by

$$L_f^{2d} = \det cov(f) \cdot \left(\frac{\sup_{\mathbb{R}^n} f(x)}{\int_{\mathbb{R}^n} f(x)dx}\right)^2 \quad (17)$$

Indeed, if f is the indicator function of a convex body K, i.e., $f(x) = 1$ iff $x \in K$ and 0 otherwise, then it is easy to see that $L_f = L_K$, where L_K is the the isotropic constant of K. Moreover, it is also possible to move in the other direction also, i.e., given an arbitrary log-concave function f, we can idenfity convex bodies K_f (associated with analogues of 'level sets' of f) with $L_f \approx L_{K_f}$.

Using the above intuition, the aim in [Kla06] is to come up with a log-concave distribution f supported on K (therefore we can also view it as a re-weighting of the uniform measure on K), with L_f being small. Given such a re-weighting, which is also 'not too unbalanced', it is possible to recover a K' with the properties we require. In particular, the following lemma formalizes this.

LEMMA 5.1. *(Lemma 2.8 of [Kla06]) Let $f : K \mapsto (0,\infty)$ be a log-concave re-weighting of a convex body K and let $x_0 = \int_z zf(z)dz$ denote its barycenter. Moreover, suppose for some $m > 1$, we have*

$$\sup_{x\in K} f(x) \le m^d \inf_{x\in K} f(x).$$

Then there exists a convex body T, s.t. $L_T = \Theta(L_f)$ (absolute constants), and further,

$$\frac{1}{m}(T - x_0) \subset K - x_0 \subset m(T - x_0).$$

Indeed, Klartag shows that we can find such an f with high probability by (i) sampling a random vector s from the polar of K, and (ii) setting $f(x) \propto e^{\langle s,x\rangle}$ if $x \in K$ and 0 otherwise. This is the crux of his paper, and he showed that such a (seemingly magical) re-weighting in fact works, by exploiting even more connections between log-concave functions and convex sets.

A crucial lemma about such exponential re-weightings is the following

LEMMA 5.2. *(Lemma 3.2 of [Kla06]) Let $f_s(x)$ be defined as described above, i.e., $f_s(x) = \frac{e^{\langle s,x\rangle}}{\int_{y\in K} e^{\langle s,y\rangle}dy} \cdot \mathbf{1}_K$. Then*

$$\int_{\mathbb{R}^n} \det cov(f_s)ds = \mathsf{Vol}(K).$$

The integral here is over the Lesbegue measure over $\mathbb{R}^n$.

This is a particular instantiation (setting φ to be the constant function 1) of the 'transportation map lemma' (Lemma 3.2), which is the heart of the proof of [Kla06]. Equipped with this lemma, the aim will be to find an s such that $\det cov(f_s) \approx \mathsf{Vol}(K)$, and f_s does not vary "much" over K (i.e., it is close to 1). This turns out to imply (using eq. (17)) that $L^{2d}_{f_s}$ is small, whereupon we can appeal to Lemma 5.1 to construct the body K'. A simple way to ensure that $f_s(x)$ does not vary much over K is to pick $s \in \varepsilon n K^*$, where K^* is the polar body of K. Formally, recall that $K^* = \{s : \langle x,s\rangle \le 1 \text{ for all } x \in K\}$. Thus the value of $f_s(x)$, which is proportional to $e^{\langle x,s\rangle}$ varies only by an $e^{\varepsilon n} \approx (1+\varepsilon)^n$ factor, which then enables us to use Lemma 5.1. Formally,

LEMMA 5.3. *(essentially Theorem 3.2 of [Kla06]) Suppose $s \sim \varepsilon n K^*$, is picked uniformly. Then*

$$\mathbb{E}\big[L^{2d}_{f_s}\big] \le \Big(\frac{C}{\sqrt{\varepsilon}}\Big)^d$$

for some absolute constant C.

Thus by Markov's inequality, we have that

$$\mathbb{P}_s\left[L^{2d}_{f_s} > \Big(\frac{2C}{\sqrt{\varepsilon}}\Big)^d\right] < \frac{1}{2^d} \tag{18}$$

Since we are interested in ε being a constant (say 1), we have that $L^2_{f_s} = O(1)$ except with probability exponentially small in d. This finishes the outline of the proof of [Kla06].

Note. The one technical detail here is that x_0 (the barycenter of f) is not 0, *even if the K we started with is centrally symmetric.*[4] However, for the purposes of our application, we really need the convex body K' to be centered as all our errors are measured with respect to the origin. If on the other hand, we translate K' to the origin, then we lose guarantees over K' approximating K (as it would only approximate $K - x_0$), and we have no control over the length of x_0.

Our approach to resolve this issue, is to make the function f centrally symmetric before applying Lemma 5.1 so that we obtain a centrally symmetric body K' which is also centered at the origin. To do this, we convolve the function f which Klartag defines, with *its mirror about* 0 and show that the convolved body also satisfies the structural properties that we required, and in addition, it is centered at the origin. Before going into the details of the convolution argument, we point out that another natural way to symmetrize K' is to consider K'' as being the convex hull of K' and $-K'$. While good bounds can be obtained on its volume, we do not know how to analyze its isotropic constant – in particular, it seems difficult to relate the uniform measure on K'' to that on K'. This turns out to be much easier for the convolution.

5.2 Symmetrization by Convolution

Let f_s be the log-concave function with support K as determined in the above step. For clarity, let us recall that $f_s(x) = \frac{e^{\langle s,x\rangle}}{\int_y e^{\langle s,y\rangle}}$, hence f_s it is easy to see that indeed a log-concave distribution. Now, let us define $f_{-s}(x) = \frac{e^{-\langle s,x\rangle}}{\int_y e^{-\langle s,y\rangle}}$, and define their *convolution* f to be

$$f(z) := (f_s * f_{-s})\ (z) = \int_x f_s(x) f_{-s}(z-x)dx \tag{19}$$

A basic property of a convolution is that

$$\int_{\mathbb{R}^n} f(z)\ dz = \Big(\int_{\mathbb{R}^n} f_s(z)\ dz\Big)\Big(\int_{\mathbb{R}^n} f_{-s}(z)\ dz\Big),$$

which implies that f is a probability density as well. A well-known fact (see Lemma 2.1 of Lovász and Simonovits [LS93] or [Din57]) is that log-concave distributions are closed under taking convolutions, which implies f is that log-concave as well.

From our definition of f_s, we also observe that $f_s(x) = f_{-s}(-x)$. Observe that convolution also has an interesting geometric view: we can view sampling from f as picking $u \sim f_s$, $v \sim f_{-s}$ and taking $x = u+v$, which is now precisely the same as picking $u, v \sim f_s$ independently, and setting $x = u - v$. Notice that this immediately implies that $f(z) = f(-z)$, i.e., f is centrally symmetric.

We now move on to showing that the convolved function f also has bounded isotropic constant. To this end, the following lemma establishes that the determinant of the covariance matrix of f is "close" to that of f_s.

LEMMA 5.4. *Given $f_s(x) \propto e^{\langle s,x\rangle}$, and $f := f_s * f_{-s}$, we have* $\det cov(f) = 2^d \det cov(f_s)$.

Proof: Now M_f denote the covariance matrix of f. Recall that f_s is not centered at the origin, and therefore let $\mu_i := \int_x f_s(x)x_i dx$. Now, since f is centered at the origin, the

[4] A perturbation which satisfies this condition was obtained earlier by Klartag [BK05], but that has weaker guarantees on the Banach-Mazur distance than those we seek.

(i, j)th entry of M_f is given by

$$\begin{aligned} M_f(i,j) &= \int_z f(z)\ z_i z_j\ dz \\ &= \int_{x,y} f_s(x) f_s(y)(x_i - y_i)(x_j - y_j)\ dxdy \\ &= \int_{x,y} f_s(x) f_s(y)[(x_i - \mu_i)(x_j - \mu_j) + \\ &\qquad (y_i - \mu_i)(y_j - \mu_j)] dxdy \quad \text{(cross terms vanish)} \\ &= 2\int_x f_s(x)(x_i - \mu_i)(x_j - \mu_j)\ dx = 2M_{f_s}(i,j) \end{aligned}$$

Notice that in the first step above, we have used the equivalence between (sampling $z \sim f$) and (sampling $x, y \sim f_s$ and then setting $z = x - y$). Therefore we have $M_f = 2M_{f_s}$, which implies the lemma statement. ■

Note that $\sup f = \sup_z f(z) = \sup_z \int_x f_s(x) f_{-s}(z-x)\ dx \leq (\sup f_s) \cdot \int_x f_s(x)\ dx \leq \sup f_s \leq e^{\varepsilon d}$. Thus the isotropic constant of f can be bounded as

$$\begin{aligned} L_f^{2d} &= \det cov(f) \cdot \Big(\frac{\sup f}{\int_z f(z)\ dz} \Big)^2 \\ &\leq 2^d \det cov(f_s)\ e^{2\varepsilon d} \leq C^d \cdot \det cov(f_s). \end{aligned}$$

To summarize, we have shown above that our convolved function defined as $f(z) = (f_s * f_{-s})(z) = \int_{y \in \mathbb{R}^d} f_s(y) f_{-s}(z-y)dy$ satisfies the following properties (where $f_s(x) = e^{\langle s,x \rangle}$ if $x \in K$ and 0 otherwise):

(i) **Support in** $2K$. Since f_s has support in K, the convolution has support in $K - K = 2K$ because K is centrally symmetric.

(ii) **Centrally Symmetric.** It is easy to see that $f(\cdot)$ is centrally symmetric, i.e., $f(-x) = f(x)$ for all x. In particular, this implies that the barycenter of f is the origin.

(iii) **Small Isotropic Constant.** We showed this by arguing that both the "volume of f" and the determinant of the covariance matrix are roughly similar to the corresponding values of f_s.

Furthermore, the function f has the following expression

$$f(z) = \frac{e^{-\langle s,z \rangle}}{M} \int_{y \in K \cap (K+z)} e^{2\langle s,y \rangle} dy \tag{20}$$

In the above expression M is some normalizing constant such that $\int_z f(z) = 1$. Given the above properties f satisfies, the eager reader might feel tempted to use Lemma 5.1 to obtain the convex body associated with this function f. However, we note that it lacks one crucial property required in the lemma statement, i.e., $\sup_{x \in 2K} f(x) \leq m^d \inf_{x \in 2K} f(x)$ (for useful applications of the lemma, we require m to be an absolute constant). This is because the points at the boundary of the convex body $2K$ have very little support in the convolution and their values could be highly disparate with the supremum value $f(0)$.

We resolve this issue by *truncating* f around the convex body $(1/2)K$, i.e., set $f(x) = 0$ for $x \notin (1/2)K$ (this is allowed, because we do not require f to be a probability distribution). We now show that it satisfies all the above-mentioned properties, in addition to bounded aspect-ratio.

(i) Support in $(1/2)K$.

(ii) Centrally Symmetric.

(iii) **Small Isotropic Constant.** Firstly, we observe that since we only set some $f(z)$ to 0, the determinant of the covariance matrix can only drop. Therefore, if we show that $\int_z f(z)dz$ does not drop significantly, that will establish that the isotropic constant does not change by too much (since $0 = \sup_z f(z)$ is also contained in $(1/2)K$, the supremum does not change due to truncation). To this end, the original "volume" is

$$\int_{z \in 2K} f(z) = \int_{v \in S_{d-1}} \int_{r=0}^{||v||_{2K}^{-1}} f(rv)\ Cr^{d-1} dr dv$$

since f is originally non-zero only inside $2K$. Now, the truncated volume is

$$\begin{aligned} \int_{z \in (1/2)K} f(z) &= \int_{v \in S_{d-1}} \int_{r=0}^{||v||_{(1/2)K}^{-1}} f(rv)\ Cr^{d-1} dr dv \\ &= \int_{v \in S_{d-1}} \int_{r=0}^{||v||_{2K}^{-1}/4} f(rv)\ Cr^{d-1} dr dv \\ &\geq \frac{1}{4^{d-1}} \int_{v \in S_{d-1}} \int_{r'=0}^{||v||_{2K}^{-1}} f(r'v/4)\ Cr'^{d-1} dr' dv \\ &\geq \frac{1}{8^{d-1}} \int_{v \in S_{d-1}} \int_{r'=0}^{||v||_{2K}^{-1}} f(r'v)\ Cr'^{d-1} dr' dv \end{aligned}$$

In the final inequality above, we have used the fact that $f(rx/4) \geq e^{-4\varepsilon d} f(rx)$ for any r, x such that $rx \in 2K$. This is true because of the following argument: from the expression in equation (20), we know that $f(rx)$ is $e^{-\langle s,rx \rangle}$ times an integral (of a non-negative function) over $K \cap (K + rx)$. Likewise $f(rx/4)$ is $e^{-\langle s,rx/4 \rangle}$ times an integral (of the same non-negative function) over $K \cap (K + rx/4)$. But now it is easy to see that $K \cap (K + rx) \subseteq K \cap (K + rx/4)$ using the convexity of K, and hence the latter integral is at least the former integral. Furthermore, since $s \in K^*$ and $rx, (rx/4) \in 2K$, we have that $e^{-\langle s,rx \rangle} \in [e^{-2\varepsilon d}, e^{2\varepsilon d}]$ as well as $e^{-\langle s,rx/4 \rangle} \in [e^{-2\varepsilon d}, e^{2\varepsilon d}]$. Therefore we have $e^{-\langle s,rx/4 \rangle} \geq e^{-4\varepsilon d} e^{-\langle s,rx \rangle}$. Multiplying these two bounds, we get that $f(rx/4) \geq e^{-4\varepsilon d} f(rx)$ for any r, x such that $rx \in 2K$.

(iv) **Supremum to Infimum Ratio.** Consider $z \in (1/2)K$. We now show that $f(z) \geq 4^{-d} f(0)$. To this end, note that $f(0) = \mathsf{Vol}(K)$, and $f(z) \geq e^{-2\varepsilon d} \mathsf{Vol}(K \cap (K+z))$ for $z \in (1/2)K$. But now, it is easy to verify that $K \cap (K+z) \supseteq z + (1/2)K$ and hence $\mathsf{Vol}(K \cap (K+z)) \geq 2^{-d} \mathsf{Vol}(K)$. Combining these two facts, we get that $f(z) \geq 4^{-d} f(0)$ for all $z \in (1/2)K$.

To summarize the steps discussed above, we now present (in the algorithm Perturb below) the procedure for constructing the centrally symmetric body K' which approximates (w.r.t the Banach-Mazur distance) the given centrally symmetric convex body K upto a factor of 2.

Theorem 5.5. *If K is any centrally symmetric convex body, then with probability at least $1 - 4^{-d}$, the convex body $K' = T$ generated above is (i) centrally symmetric, (ii) has bounded isotropic constant $L_{K'} = \Theta(1)$, and (iii) approximates K in the sense that $(1/2)K \subseteq K' \subseteq K$.*

```
procedure Perturb(K, d)     // convex body K, dimension d
begin
    Sample a random s ∼ εdK*, where
    K* = {x : ⟨x, y⟩ ≤ 1 ∀y ∈ K} is the polar of K.
    For any α, let f_α(x) = e^{⟨α,x⟩} if x ∈ K and 0.
    Define f(x) := (f_s ∗ f_{−s})(x) to be the convolution of
    f_s and f_{−s}.
    Truncate f(x) at (1/2)K, i.e., set f(x) = 0 if
    x ∉ (1/2)K.
    Use Lemma 5.1 on f and (1/2)K to obtain the
    resultant convex body K′ = T.
end
```

6. SAMPLING FROM AN ISOTROPIC PERTURBATION

We now shift our attention to the computational aspects of our algorithm, i.e., methods to efficiently sample from the different bodies we consider at the various steps of recursive algorithm noise.

6.1 Sampling from K'

Let us briefly review the steps of our algorithm where the body K' is involved: we need access to K' in the following senses:

1. Compute the moment matrix $M(K')$.
2. Sample $x \in \mathbb{R}^n$ with probability density proportional to $e^{-\varepsilon\|x\|_{K'}}$, which can be achieved by sampling $r \sim \text{Gamma}(d+1, \varepsilon^{-1})$ and $v \sim K'$ and setting $x = rv$.

Both of these can be done if we are able to sample from the body K' uniformly. Estimating $M(K')$ is done in the work of Dadush, et al. [DPV10]. In what follows, we give a way of sampling uniformly from the body K', which is a somewhat stronger requirement. To this end, we first give a (approximate) polynomial time membership oracle for the body K', and then use the grid-walk sampling techniques of [DFK91] (see, e.g., this survey by Vempala [Vem05] for more details). Also, we will restrict our attention to K being a centrally symmetric convex body.

To sample from K' we need (i) decent estimates of the size of K' which we know since K satisfies $rB_2^d \subseteq K \subseteq RB_2^d$ for polynomially bounded R/r, and (ii) a membership oracle. But first, to even determine the body K', we need to sample a random vector from the polar K^*. We discuss this issue in the next subsection, and then move on to constructing a membership oracle.

6.1.1 *Step 1: Sampling from the polar* K^*

In this section, we describe an efficient procedure to sample from the polar body

$$K^* = \{x : \langle x, y\rangle \le 1,\ \forall y \in K\}.$$

As mentioned earlier, this is the first step towards generating the approximator of K which satisfies the hyperplane conjecture. With this goal, let us first describe a simple membership testing oracle for the polar body, which we use as a subroutine for the sampling procedure. Indeed, because $y \in K$ and $K = FB_1^n$, we can write y as a convex combination of the columns of F and their negative vectors. That is, y lies in the convex hull of $\pm$ combinations of the columns of F. Therefore, membership in $K*$ is equivalent to

$$x \in K^* \Leftrightarrow |\langle x, f\rangle| \le 1 \ \text{ for all columns f of } F.$$

Indeed, x has inner product at most 1 with all columns and their negatives *if and only if* it has inner product at most 1 with any convex combination of them. Therefore, given an x, testing if $x \in K^*$ simply amounts to checking the inner product condition for each column f of the query matrix F, which can be done efficiently.

In order to use the grid-walk based sampling technique [DFK91], we require K^* to satisfy the following two properties:

(i) K^* has a membership oracle, and

(ii) K^* is bounded in the sense that $aB_2^d \subseteq K^* \subseteq bB_2^d$ where b/a has ratio $O(\text{poly}(d))$.

In our case, testing membership is easy, and furthermore, since we have the guarantee that $rB_2^d \subseteq K \subseteq RB_2^d$ for some R, r such that R/r has ratio $O(\text{poly}(d))$, we can use elementary properties of the polar body to infer that $(1/R)B_2^d \subseteq K^* \subseteq (1/r)B_2^d$, and therefore we can set $a = 1/R$ and $b = 1/r$ to get the desired bound for property (ii).

Using this, we can sample a random vector $s \sim \varepsilon dK^*$ and appeal to the results of Klartag [Kla06] [Section 4] to conclude that, with probability $1 - 4^{-d}$, the log-concave function $f_s(x) = e^{\langle s,x\rangle}$ for $x \in K$ (and 0 otherwise) has bounded isotropic constant. However, as mentioned earlier, the function is not centrally symmetric, and in fact, is not even centered at the origin. So before we can get a convex body from f_s, we next perform a convolution step in order to resolve these issues.

6.1.2 *Step 2: Membership Oracle for* K'

We now show how to obtain an approximate separation oracle for K'. Recall that we work with $g := f_{|(K/2)}$, i.e., the restriction of f to $K/2$, rescaled so as to give a distribution. Indeed, as we had explained in the previous section, the body K' is defined as the level sets of some appropriate function of g (à la [Bal]). Formally, Klartag defines the body K' (in the proof of Lemma 5.1) to be

$$K' = \left\{x \ : \ \int_r g(rx)r^d \, dr \ge \frac{g(0)}{d+1}\right\}.$$

THEOREM 6.1. *Let us fix $\rho > 0$. There exists a separation algorithm with the following guarantee: given x, if $x \in K'$, it always outputs YES, and if $x \notin K'\big(1 + \frac{\rho}{d}\big)$, it outputs NO w.p. at least $1 - \delta$. Further, the running time of the algorithm is at most poly$(n/\rho)\times$ polylog$(1/\delta)$.*

The idea of the proof is simple: first we consider an oracle to compute $g(y)/g(0)$ for a given y. We compute this to a factor $(1 \pm \frac{\rho}{d^2})$, w.p. $1 - 1/d^3$. Next, we observe that we can pick $O(d^2)$ discrete values for r, and compute the integral $\int_r (g(rx)/g(0))r^{d-1}dr$ at these values and estimate the integral.

Thus our first task is to estimate $g(y)/g(0)$, given y. Recall that

$$\frac{g(y)}{g(0)} = \frac{\int_{K\cap(K+y)} e^{\langle s,y\rangle} \, dy}{\int_K e^{\langle s,y\rangle} \, dy}, \qquad (21)$$

where s is the point in the polar picked in the definition of g. Because each of these terms is the integral of a log-concave function (namely $e^{\langle s,x\rangle}$) over a convex domain, we can use the machinery of Lovász and Vempala [LV06] to evaluate these. We state their result for completeness.

THEOREM 6.2. *Let f be a well-rounded log-concave function given by a sampling oracle. Given $\varepsilon, \delta > 0$, we can compute a number A such that with probability at least $1-\delta$,*

$$(1-\varepsilon)\int f \leq A \leq (1+\varepsilon)\int f$$

and the number of oracle calls is $O\left(\frac{n^4}{\varepsilon^2}\log^7\frac{n}{\varepsilon\delta}\right) = \widetilde{O}(n^4)$.

The well-roundedness of our f is easy to check – we omit the proof (this is also done in [DPV10]). We are now ready to evaluate the integral. Given x, for convenience let us define the integral of interest, $I(x) := \int_r (g(rx)/g(0))r^d\, dr$. First a couple of simple lemmas.

LEMMA 6.3. *If $\|x\|_K < 1/20$, $I(x) > \frac{1}{d+1}$.*

Proof: We note that if $y \in \frac{K}{2}$, then $\frac{K}{2} - y \subseteq K$, implying that $\frac{K}{2} \subseteq K + y$ (since K is symmetric). This implies that $\frac{K}{2} \subseteq K \cap (K+y)$. Thus for $y \in \frac{K}{2}$, we have

$$\frac{g(y)}{g(0)} \geq \frac{\int_{K/2} e^{\langle s,y\rangle}\, dy}{\int_K e^{\langle s,y\rangle}\, dy} \geq \frac{\inf_K e^{\langle s,y\rangle}}{\sup_K e^{\langle s,y\rangle}} \cdot \frac{\mathsf{Vol}(K/2)}{\mathsf{Vol}(K)} \geq \frac{e^{-2\varepsilon d}}{2^d}.$$

Since we pick $\varepsilon = 1/2$, we obtain a lower bound of $1/10^d$. Now consider $I(x)$: the value of $g(x)$ is non-zero as long as $rx \in \frac{K}{2}$, thus the r ranges to a value ≥ 10. Thus

$$I(x) \geq \int_{r=0}^{10} \frac{g(rx)}{g(x)} r^d\, dr \geq \frac{1}{10^d}\int_{r=0}^{10} r^d\, dr = \frac{10}{d+1}.$$

In the last step we used $\int_{r=0}^{a} r^d\, dr = \frac{a^{d+1}}{d+1}$. This proves the lemma. ■

LEMMA 6.4. *If $\|x\|_K > 4$, $I(x) < \frac{1}{d+1}$.*

Proof: For any y, we have $g(y) \leq e^{2\varepsilon d} < 3^d$ (even if we grossly over estimate the numerator integral). Thus $I(x) \leq \int_0^{1/8} g(y)r^d\, dr < \left(\frac{3}{8}\right)^d < \frac{1}{d+1}$. ■

Thus we know the "ball-park" of r which we need to integrate over. Next, we show why we can sample different values of r.

LEMMA 6.5. *Let $x \in K$, and $y = (1+\theta)x$, for some $\theta > 0$. Then we have*

$$1 \leq \frac{g(x)}{g(y)} \leq e^{O(\theta)d}$$

Proof: The involves a computation using the expression (21), and integrating using polar coordinates (roughly, as in the 'truncating' argument earlier). We defer the proof to a full version of the paper. ■

Thus given an x, the above lemmas show that the range for r to be considered in the integration is $\left(\frac{1}{20\|x\|_K}, \frac{4}{\|x\|_K}\right)$, which can be computed because we can find $\|x\|_K$ accurately. Further, we showed that if r, r' are within a multiplicative $(1+1/d^2)$ factor, the integrand is equal up to a small multiplicative factor. Thus we can discretize the integral into a sum of $O(d^2)$ terms and evaluate each one using Theorem 6.2.

It can now be verified that if we need an "accuracy" of $\frac{\rho}{d}$ with probability $(1-\delta)$, the number of samples is at most poly$(n/\rho)\cdot$ polylog$(1/\delta)$. This completes the proof of Theorem 6.1. ■

6.2 Approximate oracle for K' suffices

Hardt and Talwar [HT10] define a β-weak separation oracle for a convex body K as one that always answers YES for $x \in K$ and NO for $x \notin (1+\beta)K$. Along similar lines, we can define a randomized β-approximate separation oracle as one that outputs YES with probability $(1-\delta)$ for $x \in K$ and NO with probability $(1-\delta)$ for $x \notin (1+\beta)K$. The arguments above show that one can implement a randomized β-weak separation oracle for K' in time polynomial in $\frac{1}{\beta}$ and $\log\frac{1}{\delta}$. The results in [HT10] show that such an oracle is sufficient to define a distribution that satisfies ε-differential privacy, and which has an error distribution close to the ideal mechanism that can sample exactly from K'. Thus we can in polynomial time get a differentially private mechanism with the claimed error bound.

7. ANALYSIS OF ALGORITHM PERTURBHT

The privacy analysis is identical to that given in Section 3.1. So we only focus on analyzing the total error of the mechanism. To this end, we begin with some basic lemmas concerning a single recursive call of the above function, both of which are proved in [HT10] (and follow from [MP89a])

LEMMA 7.1 (PROPOSITION 7.7 IN [HT10]). *Let K' be a convex body in $\mathbb{R}^d$, and $M(K')$ be its moment matrix. Suppose $M(K')$ has eigenvalues $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_d$, and let u_i be the corresponding eigenvectors. Then for any $S \subseteq [d]$, if $\mathcal{S}$ is the space $\mathsf{span}\{\cup_{i\in S} u_i\}$ and $\Pi_{\mathcal{S}}$ denotes the projection operator onto $\mathcal{S}$, we have*

$$\mathsf{Vol}(\Pi_{\mathcal{S}}K')^{1/|S|} \geq \left(\frac{C}{L_{K'}}\right)^{\frac{d-|S|}{|S|}} \cdot \left(\prod_{i\in S}\lambda_i\right)^{\frac{1}{(2d)}}$$

LEMMA 7.2 (LEMMA 7.9 IN [HT10]). *Let K' be the convex body computed in Step 1 of the algorithm* noise. *Then the expected value $E[||\Pi_V a||^2]$ of the squared error added in Step 5 is at most $O(d^3/\varepsilon^2)\sum_{i=d/2}^{d}\lambda_i$, where V and λ_i's are as defined in Steps 2 and 3 of the algorithm.*

Note. Both the above lemmas are stated in [HT10] for the body $K = FB_1^n$, but the proof holds for any convex body and in particular for K'.

Roadmap. We are now ready to present our analysis. It categorizes each level of the recursion as either a *stopping level* or a *continuation level*. The intuition behind these levels is extremely simple: informally, we say that a level is a stopping level if the volume of the bodies $\Pi_U K$ and $\Pi_V K$ are comparable (where Π_U and Π_V are the projections to the higher $d/2$ and lower $d/2$ eigenvectors respectively). On the other hand, we call a level a continuation level if $\Pi_U K$ has much larger volume than $\Pi_V K$. The analysis proceeds by breaking up the recursion into blocks of levels, where each block is a block of continuation levels sandwiched by two successive stopping levels. In each such block, we will charge the total error in *all* the continuation levels, to the volume of the lower subspace $\Pi_V K$ in the latter stopping level (and this is where we use the definition of the stopping level). Since we recurse on the upper subspace for the next block, it becomes easy to identify *mutually orthogonal* subspaces to charge our total error, which puts us in shape to apply Theorem 4.2. The next two subsections carry out this argument in more detail.

7.1 A continuation level

Consider a level of the recursion in which we have the body K, K', dimension d, λ_i, u_i, U, and V as defined in the various steps of the algorithm. Now we define a level to be a *continuation level* if

$$\mathsf{Vol}(\Pi_U K')^{\frac{1}{(d/2)}} > 8 \cdot \mathsf{Vol}(K')^{\frac{1}{d}} \quad (22)$$

The following lemma bounds the total error of our algorithm by the volume of K when projected to the subspace U.

LEMMA 7.3. *There is an absolute constant C_1 such that the following holds: Suppose that the algorithm has an unaccounted (squared) error at most $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K)^{\frac{2}{d}}$ at the beginning of a continuation level of the recursive algorithm* perturbHT*. Then the total unaccounted error at the beginning of the next recursive call is at most*

$$C_1 \cdot ((d/2)^3/\varepsilon^2)\mathsf{Vol}(\Pi_U K)^{\frac{2}{(d/2)}}) \leq C_1 \cdot (\tilde{d}^3/\varepsilon^2)\mathsf{Vol}(\tilde{K})^{\frac{1}{d}},$$

where $\tilde{K} = \Pi_U K$ and $\tilde{d} = d/2$ are the input parameters for the next recursive call.

Proof: By assumption the total unaccounted (squared) error at the beginning of this level is $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K)^{\frac{2}{d}}$. Since $K \subseteq K'$ (by definition in Step 1 of the algorithm),this is at most $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K')^{\frac{2}{d}}$. Now, we can use the definition of a continuation level to bound this quantity by $(C_1/64)\left(d^3/\varepsilon^2\right)\mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}}$.

Furthermore, the total squared error which our mechanism adds at this level is bounded by $C_2 \cdot (d^2/\varepsilon^2)\sum_{i=d/2}^{d}\lambda_i \leq C_2 \cdot (d^3/\varepsilon^2)\lambda_{d/2}$ for some constant C_2 from Lemma 7.2. We can express this in terms of the volume by using the following relationship.

$$\mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}} \geq \left(\frac{C}{L_{K'}}\right)^2 \left(\prod_{i=1}^{d/2}\lambda_i\right)^{2/d)} \geq \left(\frac{C}{L_{K'}}\right)^2 \lambda_{d/2}$$

The first inequality above used Lemma 7.1 and the second inequality follows because the λ_i's are non-increasing. Therefore we can bound the (squared) error incurred in this level by $C_2\left(d^3/\varepsilon^2\right)(L_{K'}/C)^2\,\mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}}$. Finally, adding the unaccounted error with the error incurred at this level, we get the total error at the beginning of the next level is at most

$$8 \left(\frac{C_2 \cdot L_{K'}^2}{C^2} + \frac{C_1}{64}\right)\left(\frac{(d/2)^3}{\varepsilon^2}\right)\mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}}$$
$$\leq C_1\left(\frac{(d/2)^3}{\varepsilon^2}\right)\mathsf{Vol}(\Pi_U K)^{\frac{2}{(d/2)}}$$

Again, in the inequality above we used the fact that $\Pi_U K' \subseteq \Pi_U(2K)$ and hence $\mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}} \leq 4\mathsf{Vol}(\Pi_U K)^{\frac{2}{(d/2)}}$. Also in order to satisfy the inequality, we set our parameters such that $32\left(\frac{C_2 \cdot L_{K'}^2}{C^2} + \frac{C_1}{64}\right) \leq C_1$, i.e., $C_1 \geq 64 C_2 L_{K'}^2/C^2$. Since $L_{K'}$ is $\Theta(1)$ (because K' satisfies the hyperplane conjecture), and C_2 and C are constants determined in Lemmas 7.2 and 7.1 respectively, we can set C_1 to be a constant. Thus we have showed that the desired invariant on the total error is satisfied at a continuation level, which completes the proof. ∎

7.2 A stopping level

Again consider a level of the recursion in which we have the bodies K, K', dimension d, λ_i, u_i, U, and V as defined in the various steps of the algorithm. We say that this level is a *stopping level* if

$$\mathsf{Vol}(\Pi_U K')^{\frac{1}{(d/2)}} \leq 8 \cdot \mathsf{Vol}(K')^{\frac{1}{d}} \quad (23)$$

In this case, we now show that the volumes of K' and $\Pi_V K'$ are roughly identical, and as a consequence, unlike the continuation step where we "charge" the error to the top projection $\Pi_U K$, we can actually charge the total error to the bottom projection $\Pi_V K$. Our analysis then breaks up the levels of recursion into blocks, where each block is a series of continuation levels followed by a stopping level.

LEMMA 7.4. *There is an absolute constant B such that the following holds: In every stopping level of the recursive procedure, we have $\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}} \geq B \cdot \left(\prod_{i=1}^{d/2}\lambda_i\right)^{\frac{1}{(d/2)}}$, and therefore $\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}} \geq \sqrt{B} \cdot \left(\prod_{i=1}^{d}\lambda_i\right)^{\frac{1}{d}}$.*

Proof: We begin by comparing the higher eigenvalues and the lower eigenvalues of K based on the guarantee of equation (23). Indeed, we have

$$\begin{aligned}\left(\prod_{i=1}^{d/2}\lambda_i\right)^{\frac{1}{(d/2)}} &\leq \left(\frac{L_{K'}}{C}\right)^2 \mathsf{Vol}(\Pi_U K')^{\frac{2}{(d/2)}} \\ &\leq 8\left(\frac{L_{K'}}{C}\right)^2 \mathsf{Vol}(K')^{\frac{2}{d}} \\ &= \frac{8}{L_{K'}^2}\left(\frac{L_{K'}}{C}\right)^2\left(\prod_{i=1}^{d}\lambda_i\right)^{\frac{1}{d}}\end{aligned}$$

Above, the first inequality follows from Lemma 7.1, the second inequality from equation (23), and the final equality from the definition of the isotropic constant $L_{K'}$. It is now easy to see that for a suitable choice of B, say, $B = C^4/64$, the above inequality implies the first inequality of the lemma statement. The second inequality easily follows by multiplying both sides by $\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}}$. We complete the proof by noting that C is a constant from Lemma 7.1. ∎

Now the following lemma "charges" the total unaccounted error of our algorithm to the volume of K's projection on the lower subspace V. Note that, since our algorithm recurses only on $U = V^{\perp}$, all the subspaces we charge our error to *are mutually orthogonal.*

LEMMA 7.5. *Suppose that the unaccounted (squared) error at the beginning of a stopping level of algorithm* perturbHT *is at most $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K)^{\frac{2}{d}}$. Then the total error (unaccounted error plus the error incurred in this recursion) is at most $O(d^3/\varepsilon^2)\mathsf{Vol}(\Pi_V K)^{\frac{2}{(d/2)}}$.*

Proof: By assumption the total unaccounted (squared) error at the beginning of this level is $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K)^{\frac{2}{d}}$. Since$K \subseteq K'$ (by definition in Step 1 of the algorithm), this is at most $C_1 \cdot (d^3/\varepsilon^2)\mathsf{Vol}(K')^{\frac{2}{d}}$.

By the definition of the isotropic constant $L_{K'}$, we have $L_{K'}^2\mathsf{Vol}(K')^{\frac{2}{d}} = \left(\prod_{i=1}^{d}\lambda_i\right)^{\frac{1}{d}}$. Thus we can bound the total unaccounted squared error by $(C_1/L_{K'}^2)(d^3/\varepsilon^2)\left(\prod_{i=1}^{d}\lambda_i\right)^{\frac{1}{d}}$. But now we may appeal to Lemma 7.4 and relate the product of all eigenvalues to only those of the lower $d/2$ eigenvalues. Indeed using the lemma, we can bound the total unaccounted error by $\frac{C_1}{\sqrt{B}\cdot L_{K'}^2}(d^3/\varepsilon^2)\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}}$.

In addition to this, the total squared error which our mechanism adds at this level can be bounded by

$$C_2\cdot(d^2/\varepsilon^2)\sum_{i=d/2}^{d}\lambda_i \leq C_2\cdot(d^3/\varepsilon^2)\lambda_{d/2} \leq C_2\cdot(d^3/\varepsilon^2)\left(\prod_{i=1}^{d/2}\lambda_i\right)^{\frac{1}{(d/2)}},$$

for some constant C_2 from Lemma 7.2. Again we can bound this in terms of the lower eigenvalues using Lemma 7.4 and get that this error is at most $(C_2/B)(d^3/\varepsilon^2)\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}}$. Finally we add the above two errors and then use Lemma 7.1, to get that the total error is at most

$$\left(\frac{C_2}{B}+\frac{C_1}{\sqrt{B}}\right)\left(\frac{d^3}{\varepsilon^2}\right)\left(\prod_{i=d/2}^{d}\lambda_i\right)^{\frac{1}{(d/2)}} \leq \left(\frac{C_2}{B}+\frac{C_1}{\sqrt{B}}\right)\left(\frac{L_{K'}}{C}\right)^2\left(\frac{d^3}{\varepsilon^2}\right)\mathsf{Vol}(\Pi_V K')^{\frac{2}{(d/2)}} \qquad (24)$$

Note that B, C, C_1, C_2, and $L_{K'}$ are all constants. Moreover $\mathsf{Vol}(\Pi_V K')^{\frac{2}{(d/2)}} \leq 4\mathsf{Vol}(\Pi_V K)^{\frac{2}{(d/2)}}$ since $\Pi_V K' \subseteq \Pi_V(2K)$, completing the proof. ■

7.3 Putting things together

We are now fully equipped to jointly analyze the two levels and apply our strengthened lower bound of Theorem 4.2. To this end, let K_i denote the convex body considered by the i^{th} recursive call of noise. Also let $\mathcal{S}_i$ be the subspace of $\mathbb{R}^d$ which K_i lies in, and d_i be its dimension. Formally we have $K_0 = K$, $\mathcal{S}_0 = \mathbb{R}^d$, and $d_0 = d$. Note that by construction, $\mathcal{S}_i$ and $\mathcal{S}_{i'}$ are orthogonal for $i \neq i'$.

Analyzing Blocks. Let $0 \leq i_1 \leq i_2 \leq i_m$ denote the levels in the recursive procedure when a *stopping level* was executed. We now bound the error incurred in total by all the levels in each block $(i_l, i_{l+1}]$ for $0 \leq l < m$. To this end, consider an block $(i_l, i_{l+1}]$ for some $0 \leq l < m$.

By definition, we have that each of the levels $i_l+1, i_l+2\ldots, i_{l+1}-1$ are continuation levels. Therefore, we can repeatedly apply Lemma 7.3, with an initial value of unaccounted error set to 0 for the first application of the Lemma and inductively passing on the error accrued in all previous levels to the next level. We can then conclude that the *total unaccounted squared error* incurred by our algorithm coming out of level $i_{l+1}-1$ (which is equal to the sum of the squared errors incurred at each of the levels $i_l+1, i_l+2, \ldots, i_{l+1}-1$) is at most $C_3\frac{(d_{i_{l+1}})^3}{\varepsilon^2}\cdot\mathsf{Vol}(K_{i_{l+1}})^{2/d_{i_{l+1}}}$ for some constant C_3.

But now, since the level i_{l+1} is a stopping level, we can apply Lemma 7.5 and conclude that the error incurred in this level (along with the unaccounted error defined above) is upper bounded by $O(d_{i_{l+1}}^3/\varepsilon^2)\mathsf{Vol}(\Pi_{V_{i_{l+1}}}(K))^{\frac{2}{d_{i_{l+1}}/2}}$.

Finally, to complete the proof, notice that, since we recurse on the subspace $U_{i_{l+1}} = V_{i_{l+1}}^{\perp}$, the set of subspaces we charge our error to are mutually orthogonal. We can hence apply Theorem 4.2 and conclude that the total squared error of our algorithm is at most a constant factor of our lower bound on the optimal squared error. But since our algorithm is only $\varepsilon\log d$ differentially private, we have to set $\varepsilon' = \varepsilon/(\log d)$, and this would blow up our ℓ_2^2 error approximation by a factor of $O(\log^2 d)$.

8. REFERENCES

[Bal] Keith M. Ball. Logarithmically concave functions and sections of convex sets in Rn. *Studia Mathematica*, 1988:69–84.

[BCD+07] Boaz Barak, Kamalika Chaudhuri, Cynthia Dwork, Satyen Kale, Frank McSherry, and Kunal Talwar. Privacy, accuracy, and consistency too: a holistic solution to contingency table release. In *Proc. 26th PODS*, pages 273–282. ACM, 2007.

[BK05] B. and Klartag. An isomorphic version of the slicing problem. *Journal of Functional Analysis*, 218(2):372 – 394, 2005.

[BLR08] Avrim Blum, Katrina Ligett, and Aaron Roth. A learning theory approach to non-interactive database privacy. In *STOC '08: Proceedings of the 40th annual ACM symposium on Theory of computing*, pages 609–618, New York, NY, USA, 2008. ACM.

[BN10] Hai Brenner and Kobbi Nissim. Impossibility of differentially private universally optimal mechanisms. In *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, FOCS '10, pages 71–80, Washington, DC, USA, 2010. IEEE Computer Society.

[De11] Anindya De. Lower bounds in differential privacy. *CoRR*, abs/1107.2183, 2011.

[DFK91] Martin E. Dyer, Alan M. Frieze, and Ravi Kannan. A random polynomial time algorithm for approximating the volume of convex bodies. *J. ACM*, 38(1):1–17, 1991.

[Din57] Alexander Dinghas. Über eine Klasse superadditiver Mengenfunktionale von Brunn-Minkowski-Lusternikschem Typus. *Math. Z.*, 68:111–125, 1957.

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Proc. 3rd TCC*, pages 265–284. Springer, 2006.

[DMT07] Cynthia Dwork, Frank McSherry, and Kunal Talwar. The price of privacy and the limits of LP decoding. In *Proc. 39th STOC*, pages 85–94. ACM, 2007.

[DN03] Irit Dinur and Kobbi Nissim. Revealing information while preserving privacy. In *Proc. 22nd PODS*, pages 202–210. ACM, 2003.

[DNR+09] Cynthia Dwork, Moni Naor, Omer Reingold, Guy N. Rothblum, and Salil Vadhan. On the complexity of differentially private data release: efficient algorithms and hardness results. In *Proceedings of the 41st annual ACM symposium* *on Theory of computing*, STOC '09, pages 381–390, New York, NY, USA, 2009. ACM.

[DPV10] Daniel Dadush, Chris Peikert, and Santosh Vempala. Enumerative algorithms for the shortest and closest lattice vector problems in any norm via m-ellipsoid coverings. *CoRR*, abs/1011.5666, 2010.

[DRV10] Cynthia Dwork, Guy N. Rothblum, and Salil Vadhan. Boosting and differential privacy. In *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, FOCS '10, pages 51–60, Washington, DC, USA, 2010. IEEE Computer Society.

[DY08] Cynthia Dwork and Sergey Yekhanin. New efficient attacks on statistical disclosure control mechanisms. In *Proc.* 28*th CRYPTO*, pages 469–480. Springer, 2008.

[Gia03] Apostolos Giannopoulos. Notes on isotropic convex bodies. , 2003.

[GRS09] Arpita Ghosh, Tim Roughgarden, and Mukund Sundararajan. Universally utility-maximizing privacy mechanisms. In *STOC*, pages 351–360, 2009.

[GS10] Mangesh Gupte and Mukund Sundararajan. Universally optimal privacy mechanisms for minimax agents. In *Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, PODS '10, pages 135–146, New York, NY, USA, 2010. ACM.

[HR10] Moritz Hardt and Guy N. Rothblum. A multiplicative weights mechanism for privacy-preserving data analysis. In *Proceedings of the 2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, FOCS '10, pages 61–70, Washington, DC, USA, 2010. IEEE Computer Society.

[HT10] Moritz Hardt and Kunal Talwar. On the geometry of differential privacy. In *Proceedings of the 42nd ACM symposium on Theory of computing*, STOC '10, pages 705–714, New York, NY, USA, 2010. ACM.

[Kla06] B. Klartag. On convex perturbations with a bounded isotropic constant. *Geometric And Functional Analysis*, 16:1274–1290, 2006. 10.1007/s00039-006-0588-1.

[KM05] Bo'az Klartag and Vitali Milman. Geometry of log-concave functions and measures. *Geom. Dedicata*, 170:169–182, 2005.

[KRSU10] Shiva Prasad Kasiviswanathan, Mark Rudelson, Adam Smith, and Jonathan Ullman. The price of privately releasing contingency tables and the spectra of random matrices with correlated rows. In *Proceedings of the 42nd ACM symposium on Theory of computing*, STOC '10, pages 775–784, New York, NY, USA, 2010. ACM.

[LHR$^+$10] Chao Li, Michael Hay, Vibhor Rastogi, Gerome Miklau, and Andrew McGregor. Optimizing linear counting queries under differential privacy. In *Proceedings of the twenty-ninth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, PODS '10, pages 123–134, New York, NY, USA, 2010. ACM.

[LS93] László Lovász and Miklós Simonovits. Random walks in a convex body and an improved volume algorithm. *Random Struct. Algorithms*, 4(4):359–412, 1993.

[LV06] László Lovász and Santosh Vempala. Simulated annealing in convex bodies and an $^*(^4)$ volume algorithm. *J. Comput. Syst. Sci.*, 72(2):392–417, 2006.

[MM09] Frank McSherry and Ilya Mironov. Differentially private recommender systems: building privacy into the net. In *Proc.* 15*th KDD*, pages 627–636. ACM, 2009.

[MP89a] V. Milman and A. Pajor. Isotropic position and inertia ellipsoids and zonoids of the unit ball of a normed n-dimensional space. *Geometric Aspects of Functional Analysis*, 1376:64–104, 1989.

[MP89b] V.D. Milman and A. Pajor. Isotropic position and inertia ellipsoids and zonoids of the unit ball of a normed n-dimensional space. *Geometric Aspects of Functional Analysis*, 1376:64–104, 1989.

[MT07] Frank McSherry and Kunal Talwar. Mechanism design via differential privacy. In *Proc.* 48*th FOCS*, pages 94–103. IEEE, 2007.

[NRS07] Kobbi Nissim, Sofya Raskhodnikova, and Adam Smith. Smooth sensitivity and sampling in private data analysis. In *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, pages 75–84, New York, NY, USA, 2007. ACM.

[RHS07] Vibhor Rastogi, Sungho Hong, and Dan Suciu. The boundary between privacy and utility in data publishing. In Christoph Koch, Johannes Gehrke, Minos N. Garofalakis, Divesh Srivastava, Karl Aberer, Anand Deshpande, Daniela Florescu, Chee Yong Chan, Venkatesh Ganti, Carl-Christian Kanne, Wolfgang Klas, and Erich J. Neuhold, editors, *VLDB*, pages 531–542. ACM, 2007.

[RR10] Aaron Roth and Tim Roughgarden. Interactive privacy via the median mechanism. In *Proceedings of the 42nd ACM symposium on Theory of computing*, STOC '10, pages 765–774, New York, NY, USA, 2010. ACM.

[Vem05] Santosh Vempala. Geometric random walks: a survey. *MSRI Volume on Combinatorial and Computational Geometry*, 52:577–616, 2005.