Statistical privacy from hypercontractive diffusions

Dominic Dotterrer, Ph.D.

dominic.dotterrer@gs.com

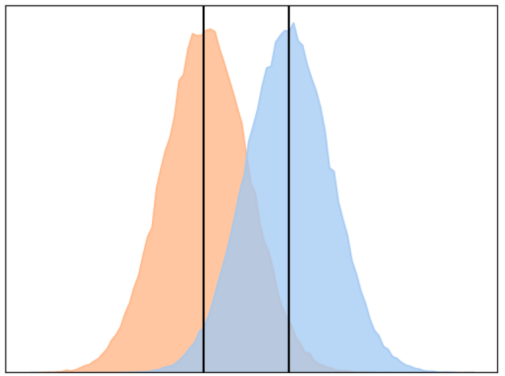
June 26, 2024

We are going to discuss two things:

1. We will formulate a statistical privacy problem.
2. We will describe an algorithm which uses the fundamental solutions of Fokker-Planck equations to address the privacy problem.

Refresher on differential privacy

- We draw a response, x, from a query, Q.
- By examining the query, we calculate how much a single respondent could hypothetically alter the query response by including their data. (the larger the sensitivity, the easier it is to detect the impact of the respondent).
- Now we add noise to the query response, $\tilde{x} = x + \delta$. The noise is calibrated so that the resulting distributions of responses are nearly statistically indistinguishable.



$$\frac{\mathbb{P}[\tilde{x} \in A \,|\, x = x_0]}{\mathbb{P}[\tilde{x} \in A \,|\, x = x_1]} < e^{\epsilon}$$

Or

$$\| \log \rho_0 - \log \rho_1 \|_\infty < \epsilon$$

[1] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy." Foundations and Trends in Theoretical Computer Science 9, no. 3–4 (2014): 211-407.

Knowledge of the query

In order to calibrate the noise, one needs full algorithmic knowledge of the query. What if it is proprietary?

Savings from native noise

Classical DP gives no considerations to the situation where Q is randomized. Noise inherent in the query does not lead to a savings of in the required added noise.

Sensitivity

DP can't address queries with hypothetically infinite sensitivity (such as mean, variance, quantiles, etc).

---

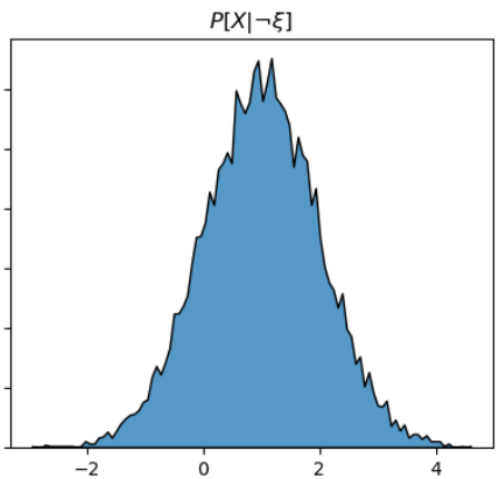
[2] Garfinkel, Simson L., John M. Abowd, and Sarah Powazek. "Issues encountered deploying differential privacy." In Proceedings of the 2018 Workshop on Privacy in the Electronic Society, pp. 133-137. 2018.

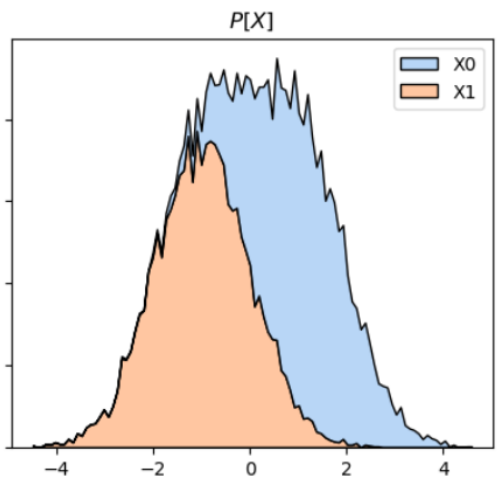
[3] Bambauer, Jane, Krishnamurty Muralidhar, and Rathindra Sarathy. "Fool's gold: an illustrated critique of differential privacy." Vand. J. Ent. Tech. L. 16 (2013): 701.

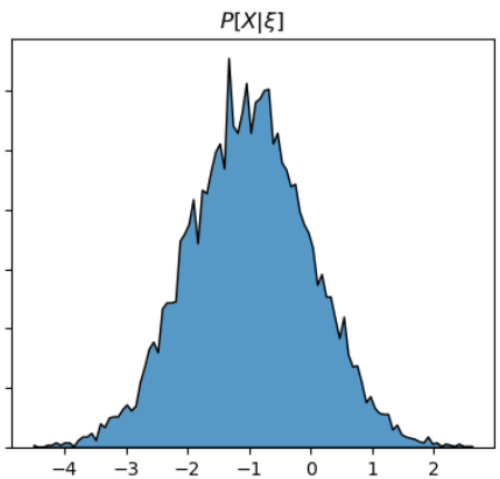
Reformulating this privacy problem

- We have a random variable, X, from which we would like to draw and report a sample $x \in X$.
- Reporting $x \in X$ could leak sensitive information. Namely, we have a sensitive event ξ and the associated conditional distributions:

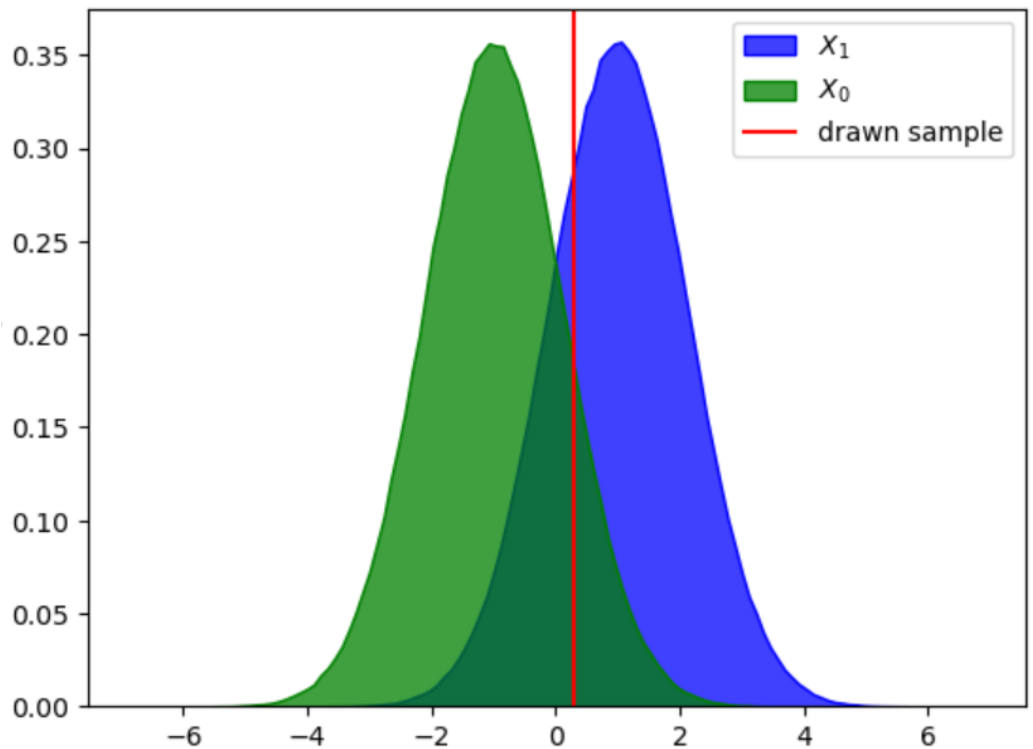
$$X_1 := P[X \mid \xi]$$
$$X_0 := P[X \mid \neg\xi]$$







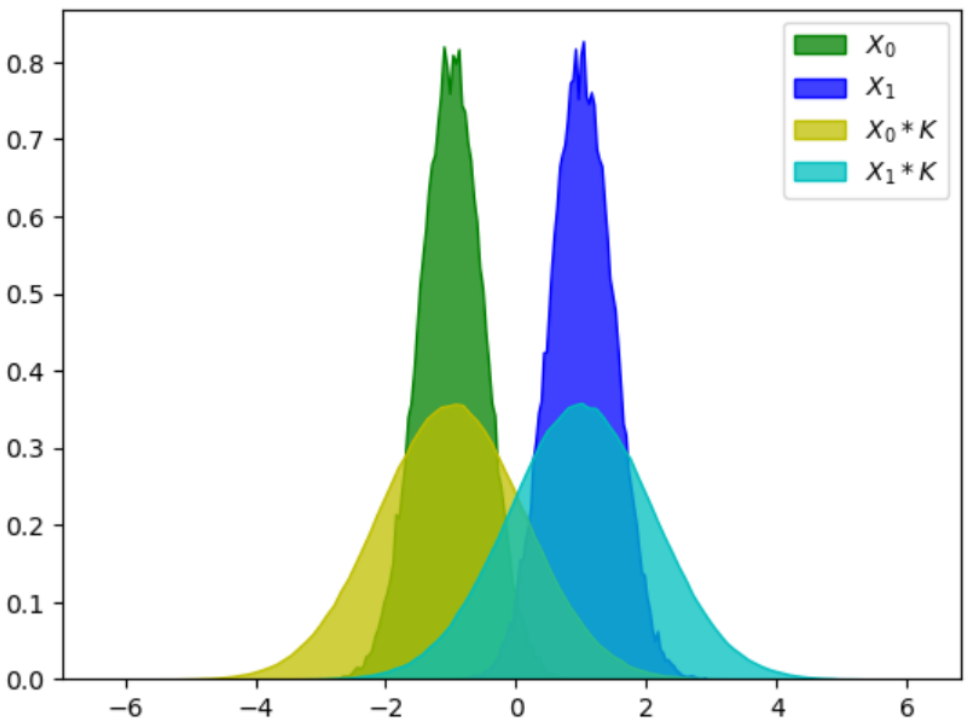
- We assume that our adversary has *full distributional knowledge of* X, X_0 *and* X_1 and therefore additionally $\mathbb{P}[\xi \mid x]$. The adversary has developed an unknown statistical test in which $\neg\xi$ is the null hypothesis.
- Our objective is to reduce the statistical power of the adversary's test while minimizing error.

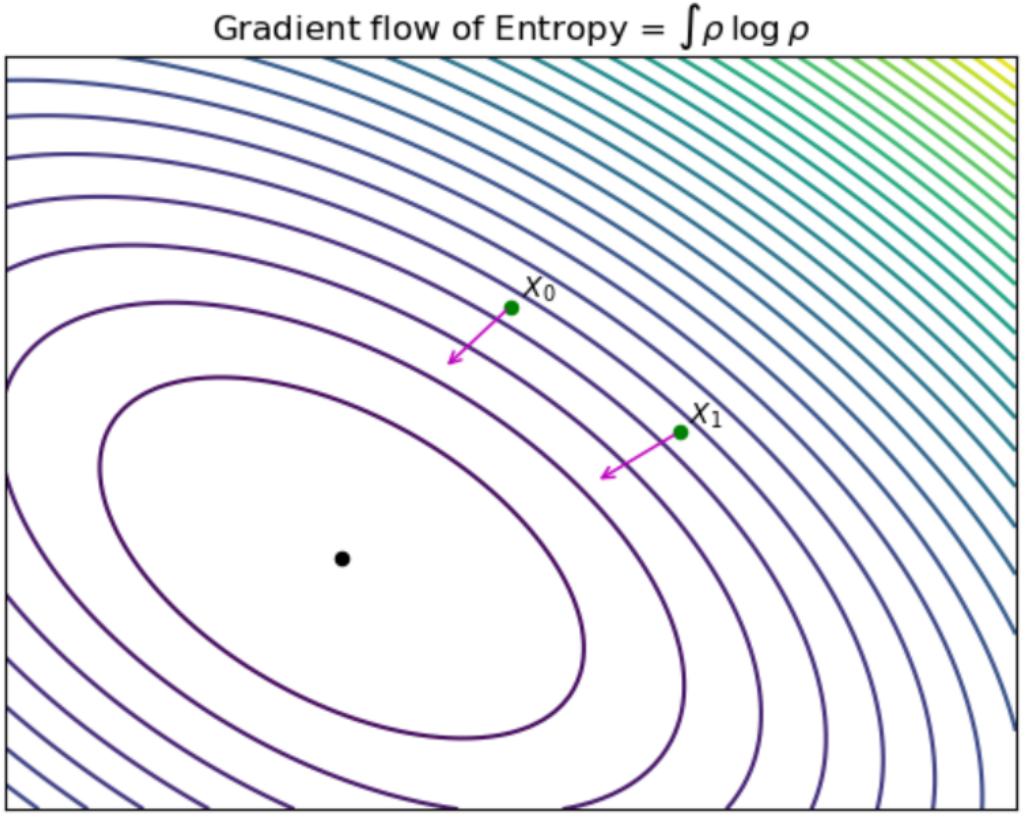


Thinking about the Gaussian mechanism

Adding Gaussian noise is the same as:

- Evolving the query response under Brownian motion for time τ.
- Evolving the conditional distributions under the heat equation
- Convolving the conditional distributions with a heat kernel, K.



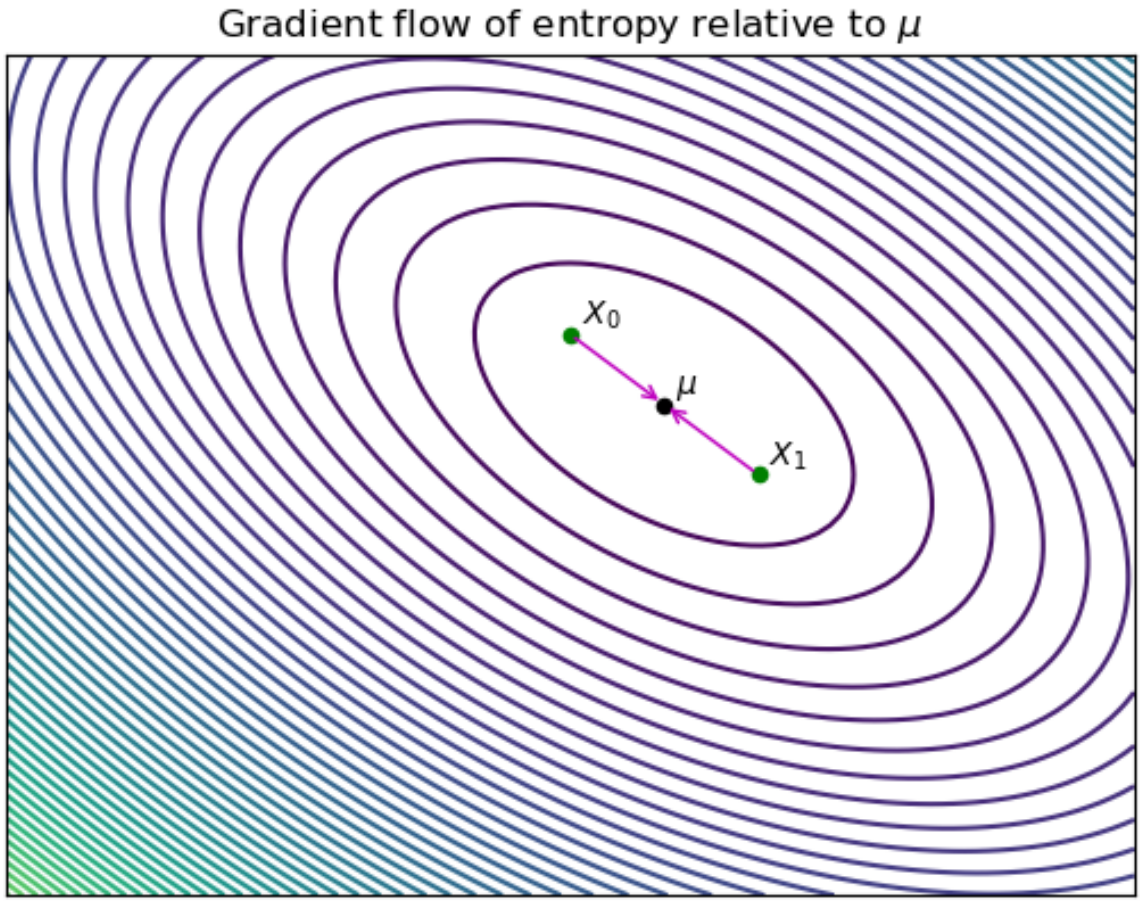


Heat flow is the gradient descent of entropy.

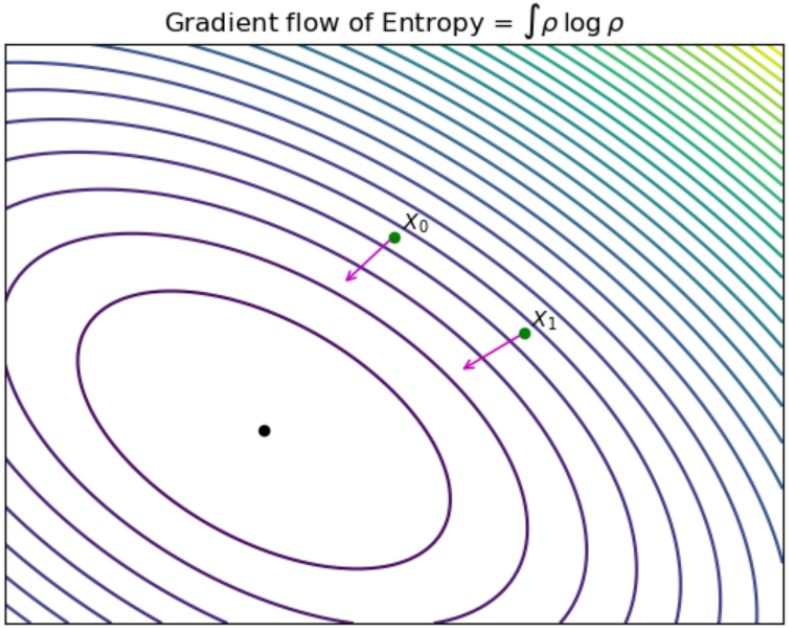
We flow the two conditional distributions for enough time that they become "close" in the sense that

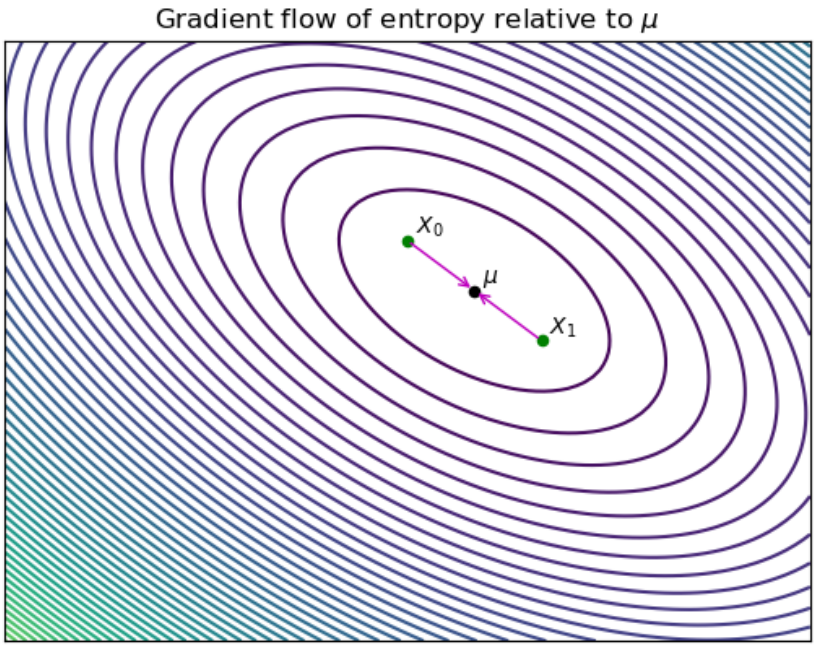
$$\| \log \rho_0 - \log \rho_1 \|_\infty \leq \epsilon$$

Instead of flowing toward the uniform distribution, why not flow to something closer?



Relative Entropy





Example: Ornstein-Uhlenbeck process

Generator

$$\frac{\partial}{\partial t} f = \Delta f + x \cdot \nabla f$$

Potential / Hamiltonian

$$h(x) = \frac{\|x\|^2}{2}$$

Stationary distribution

$$\mu = \frac{1}{Z} e^{-\frac{\|x\|^2}{2}} dx$$

---

[4] Uhlenbeck, George E., and Leonard S. Ornstein. "On the theory of the Brownian motion." Physical review 36, no. 5 (1930): 823.

[5] Iglehart, Donald L. "Limit theorems for the multi-urn Ehrenfest model." The Annals of Mathematical Statistics 39, no. 3 (1968): 864-876.

Generator

$$\frac{\partial}{\partial t} f = \Delta f + \nabla h \cdot \nabla f$$

Stationary distribution

$$\mu = \frac{1}{Z} e^{-h(x)} dx$$

Entropy functional

$$\mathcal{E}_\mu(\nu) = \int \log\left(\frac{d\nu}{d\mu}\right) \, d\nu$$

Stochastic processes have a notion of curvature (the "carré du champ").

Let K_t be the semigroup generated by $\Delta + \nabla h$ and assume $Ric_g + \nabla^2 h \geq \kappa$, then:

- $|\nabla K_t f|(x) \leq e^{-\kappa t} K_t |\nabla f|(x) \quad \forall f \in C^\infty$ and x
- $d_2^W(\mu K_t, \nu K_t) < e^{-\kappa t} d_2^W(\mu, \nu) \quad \forall \mu, \nu$ and $t > 0$

  where d_2^W is the Wasserstein optimal transport metric.

---

[6] Bakry, Dominique, and Michel Émery. "Diffusions hypercontractives." In Séminaire de Probabilités XIX 1983/84: Proceedings, pp. 177-206.

[7] Lott, John. "Some Geometric Calculations on Wasserstein Space." Commun. Math. Phys 277 (2008): 423-437.

[8] Lott, John, and Cédric Villani. "Ricci curvature for metric-measure spaces via optimal transport." Annals of Mathematics (2009): 903-991.

[9] Otto, Felix. "The geometry of dissipative evolution equations: the porous medium equation." (2001): 101-174.

[10] von Renesse, Max-K., and Karl-Theodor Sturm. "Transport inequalities, gradient estimates, entropy and Ricci curvature." Communications on pure and applied mathematics 58, no. 7 (2005): 923-940.

Lemma

$$\| \log(K_t\rho_0) - \log(K_t\rho_1)\|_\infty < B \cdot d_2^W(K_t\rho_0, K_t\rho_1)$$

where B depends on the support of X.$\square$

So therefore, if $\nabla^2 h \geq \kappa$,

$$\| \log(K_t\rho_0) - \log(K_t\rho_1)\|_\infty < Be^{-\kappa t} d_2^W(\rho_0, \rho_1).$$

and we can select

$$t > -\frac{1}{\kappa} \log\left(\frac{\epsilon}{B \cdot d_2^W(\rho_0, \rho_1)}\right)$$

What reference measure should we use?

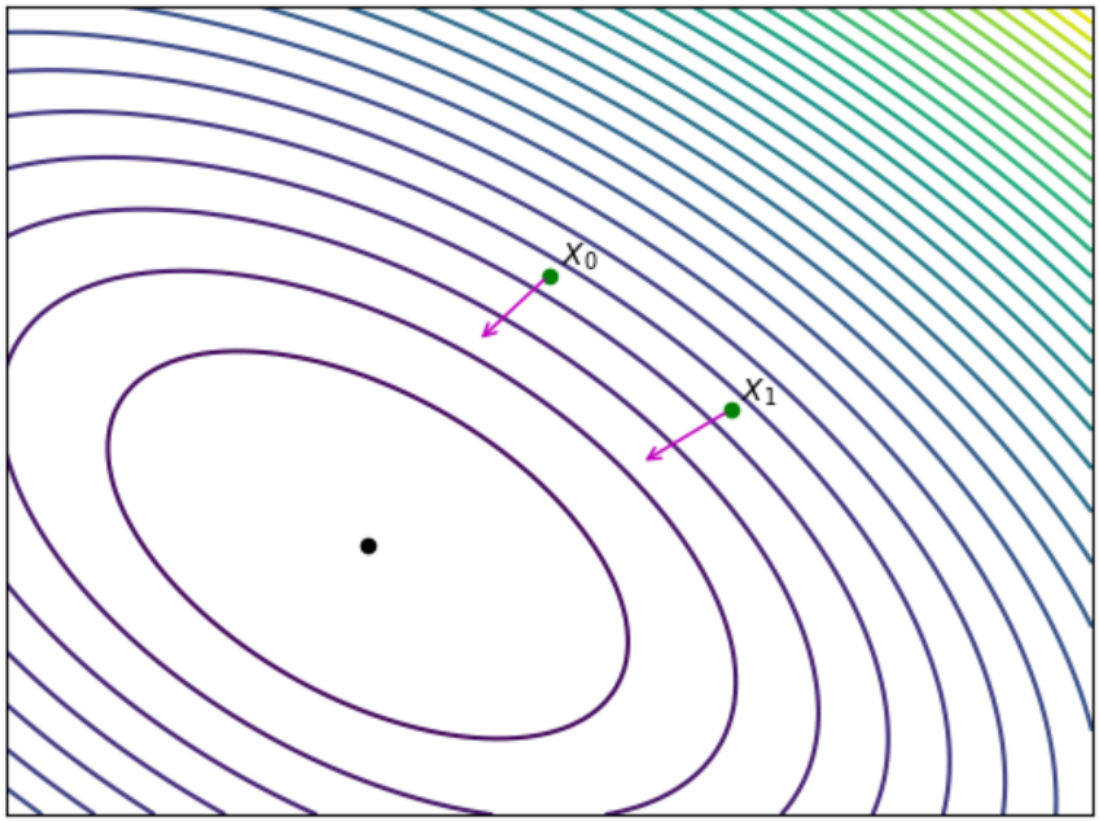
We would like to use the noise kernel

$$K_t = e^{-tL}$$

where

$$L = \Delta + \nabla h$$

How do we select the Hamiltonian, h?



In addition to rapid convergence, we also want small gradients.

We can formulate a optimization problem for h:

Definition

Let K_t be the kernel for semigroup generated by $L = \Delta + \nabla h$.

Let U be a positive, convex function.

We seek to minimize the cost function:

$$E(h) = \int U(|u - v|) dK_{t,u}(v) dX(u)$$

Subject to the constraint that $\| \log (K_t * \rho_0) - \log (K_t * \rho_1) \| < \epsilon$

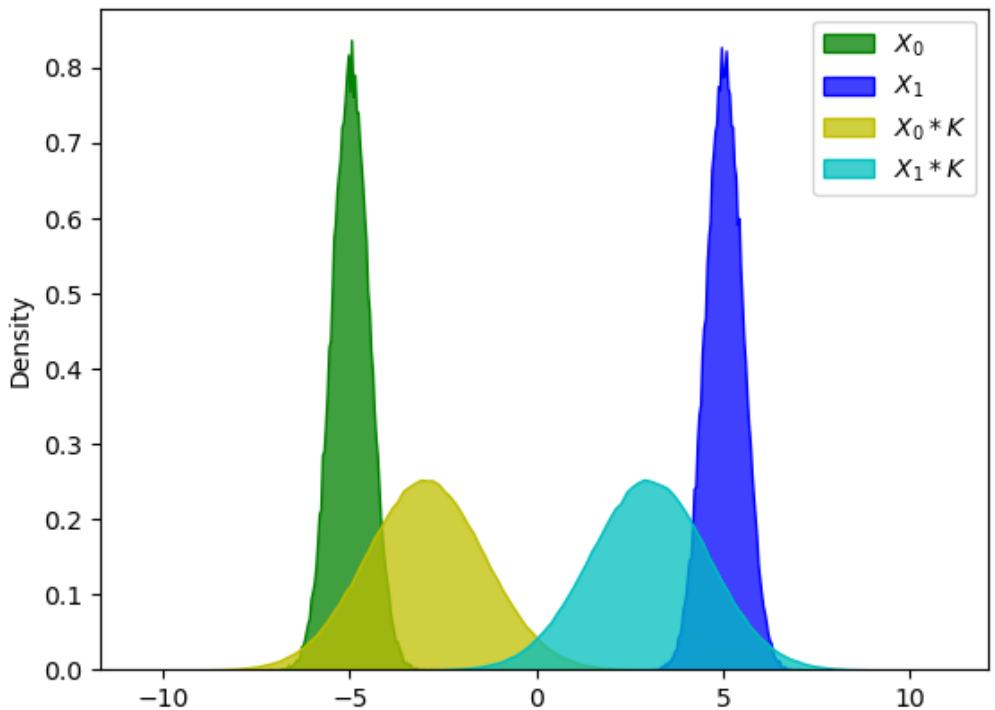
Recall: Ornstein-Uhlenbeck Process

- $h(x) = \frac{\|x\|^2}{2}$
- $\frac{\partial}{\partial t} f = \Delta f + x \cdot \nabla f$
- $\mu = \frac{1}{Z} e^{-\frac{\|x\|^2}{2}}$
- Notice that when x is large, the convection (drift) term dominates the diffusion term.
- Therefore, for query responses drawn far from zero will be assigned a large, biased noise sample.

Balancing diffusion and convection

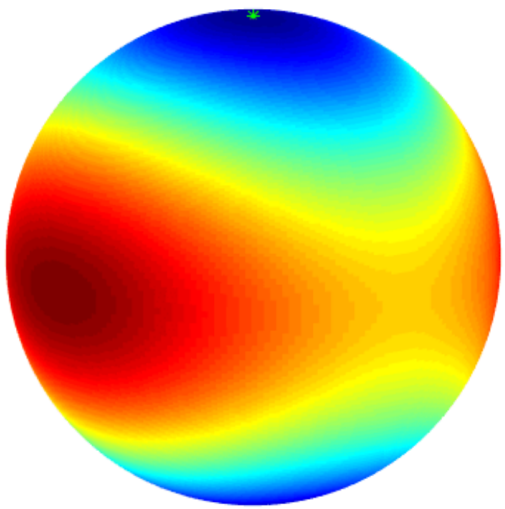
When X_0 and X_1 are "far away," the event ξ is harder to privatize.

- We must decrease the convexity, κ so that convection doesn't dominate the error. (Remember that the limit as $\kappa \to 0$ is the Gaussian mechanism)
- Decreasing convexity means increasing the evolution time, t, which means higher variance noise.



Hypercontractivity properties come from the lower bound

$$Ric_g + \nabla^2 h \geq \kappa$$



In the specific scenario that X takes values on a N-dimensional sphere (e.g. normalized time series, normalized model parameters) we get hypercontractivity for free ($Ric_g = (N-1)\mathcal{I}$).

Questions?

Thank You