Paper Summary: Probabilistic Encryption

Eli Rosenthal Will Kochanski

1 Introduction

In the paper "An Elementary Proof of a Theorem of Johnson and Lindenstrauss" ???ref Dasgupta and Gupta reprove a major dimensionality reduction result of Johnson and Lindenstrauss (???year). Their approach is interesting for the simplicity of its presentation and use of relatively elementary probabilistic techniques.
Dimensionality reduction is an important tool in data analysis on a large scale, but can be unintuitive due to the large number of dimensions in which these transformations apply and are useful. The main insight of this paper is to first analyse the problem at high level making use of rotational invariance, so that the probabilistic analysis can be performed in a much simplier setting.

2 Dimensionality Reduction

In data analysis we often want to produce summary information to describe a large data set. A natural extension of this is to ask whether we can find a smaller repesentation of our data which preserves the overall structure. In many cases our data can be represented as a set of points, V in some high dimensional euclidean space $\mathbb{R}^d$.
A common problem in data analysis is to produce summary information to describe a large data set in a smaller form.
– Dimension reduction vs summary information.
– what a dimension reduction would look like – what kinds of properties we might be interested in preserving – the role of randomness (i.e. avoiding selecting features, ease of use, streaming computation)

3 The Johnson Lindenstrauss Theorem

Theorem 1. *For any $0 \leq \epsilon \leq 1$, and any integer n, let k be a positive integer such that*

$$k \geq 4(\epsilon^2/2 - \epsilon^3/3)^{-1} \ln n$$

Then for any set of n points $V \subseteq \mathbb{R}^d$, there exists a map $f : \mathbb{R}^d \to R^k$ such that for all $u, v \in V$

$$(1-\epsilon)\|u-v\|^2 \leq \|f(u) - f(v)\|^2 \leq (1+\epsilon)\|u-v\|^2$$

Furthermore, this map can be found in randomized polynomial time.

– Statement of the theorem – Contextualization of variables – Intution, when projected length is tightly concentrated around mean
– Intuition for a random projection – rotational invariance, linear scaling, allows us to analyse a random vector.

3.1 Sampling from the Unit Sphere

– Why it might be difficult – first attempt using polar coordinates
– Key realization: We can impose constraints *after* sampling – all we need is a rotationally symmetric distribution – Enter gaussians, why do they work. – Other key advantage: Now each component is i.i.d – Makes projection very easy to reason about.

4 Large Deviation Bounds

– Remains to analyse the result of the projetion – Probabilistic method, low failure for each distance, take union bound, repeat until success to get – randomized algorithms
??? how much detail into math do we want to give?
Dimensionality reduction is an important - why we care about DR - in particular, this version is pretty cool
- rotational invariance of the joint distribution, - how do we go about vvv - sampling from a smooth surface - are gaussians always the answer? showing why the gaussian stuff is rotationally invariant
- talking about chernoff bounds

References

[1] S. GOLDWASSER AND S. MITECALI (1984), "Probabilistic Encryption", in *Journal of Computer and System Sciences*, vol. 28(2), pp. 270-299