# Lecture 4. Random Projections and Johnson-Lindenstrauss Lemma 

Yuan Yao<br>Hong Kong University of Science and Technology

March 11, 2020

## Outline

Recall: PCA and MDS

```
Random Projections
    Example: Human Genomics Diversity Project
    Johnson-Lindenstrauss Lemma
    Proofs
Applications of Random Projections
    Locality Sensitive Hashing
    Compressed Sensing
    Algorithms: BP, OMP, LASSO, Dantzig Selector, ISS, LBI etc.
    From Johnson-Lindenstrauss Lemma to RIP
```

Appendix: A Simple Version of Johnson-Lindenstrauss Lemma

## PCA and MDS

- Data matrix: $X=\left[x_{1}, \ldots, x_{n}\right] \in \mathbb{R}^{p \times n}$
- Centering: $Y=X H$, where $H=I-\frac{1}{n} \mathbf{1 1}^{T}$
- Singular Value Decomposition $Y=U S V^{T}, S=\operatorname{diag}\left(\sigma_{j}\right)$, $\sigma_{1} \geq \sigma_{2} \geq \ldots \geq \sigma_{\min (n, p)}$
- PCA is given by top- $k \operatorname{SVD}\left(S_{k}, U_{k}\right): U_{k}=\left(u_{1}, \ldots, u_{k}\right) \in \mathbb{R}^{p \times k}$, with embedding coordinates $U_{k} S_{k}$
- MDS is given by top- $k \operatorname{SVD}\left(S_{k}, V_{k}\right): V_{k}=\left(v_{1}, \ldots, v_{k}\right) \in \mathbb{R}^{n \times k}$, with embedding coordinates $V_{k} S_{k}$
- Kernel PCA (MDS): for $K \succeq 0, K_{c}=H K H^{T}, K_{c}=U \Lambda U^{T}$ gives MDS embedding $U_{k} \Lambda_{k}^{1 / 2} \in \mathbb{R}^{n \times k}$


## Computational Concerns: Big Data and High Dimensionality

- Big Data: $n$ is large
- Downsample for approximate PCA:

$$
\widehat{\Sigma}_{n^{\prime}}=\frac{1}{n^{\prime}} \sum_{i=1}^{n^{\prime}}\left(x_{i}-\widehat{\mu}_{n^{\prime}}\right)\left(x_{i}-\widehat{\mu}_{n^{\prime}}\right)^{T}, \quad \widehat{\Sigma}_{n^{\prime}}=U \Lambda U^{T}
$$

- Nyström Approximation for MDS: $V_{k}=\left(v_{1}, \ldots, v_{k}\right) \in \mathbb{R}^{n \times k}$ (we'll come to this in Manifold Learning - ISOMAP)
- High Dimensionality: $p$ is large
- Random Projections for PCA: $R X H=\tilde{U} \tilde{S} \tilde{V}^{T}$ with random matrix $R^{d \times p}$ (today): $\tilde{U}_{k}=\left(\tilde{u}_{1}, \ldots, \tilde{u}_{k}\right) \in \mathbb{R}^{d \times k}$
- Perturbation of MDS: $\tilde{V}_{k}=\left(\tilde{v}_{1}, \ldots, \tilde{v}_{k}\right) \in \mathbb{R}^{n \times k}$


## Outline

Recall: PCA and MDS
Random Projections
Example: Human Genomics Diversity Project
Johnson-Lindenstrauss Lemma
Proofs
Applications of Random Projections
Locality Sensitive Hashing
Compressed Sensing
Algorithms: BP, OMP, LASSO, Dantzig Selector, ISS, LBI etc.
From Johnson-Lindenstrauss Lemma to RIP
Appendix: A Simple Version of Johnson-Lindenstrauss Lemma

## Random Projections: Examples

- $R=\left[r_{1}, \cdots, r_{k}\right], r_{i} \sim U\left(S^{d-1}\right)$, e.g. $r_{i}=\left(a_{1}^{i}, \cdots, a_{d}^{i}\right) /\left\|a^{i}\right\|$ $a_{k}^{i} \sim N(0,1)$
- $R=A / \sqrt{k} \quad A_{i j} \sim N(0,1)$
- $R=A / \sqrt{k} \quad A_{i j}= \begin{cases}1 & p=1 / 2 \\ -1 & p=1 / 2\end{cases}$
- $R=A / \sqrt{k / s} \quad A_{i j}= \begin{cases}1 & p=1 /(2 s) \\ 0 & p=1-1 / s \\ -1 & p=1 /(2 s)\end{cases}$
where $s=1,2, \sqrt{D}, D / \log D$, etc.


## Example: Human Genomics Diversity Project

- Now consider a SNPs (Single Nucleid Polymorphisms) dataset in Human Genome Diversity Project (HGDP),
http://www.cephb.fr/en/hgdp_panel.php
- Data matrix of $n$-by- $p$ for $n=1,064$ individuals around the world and $p=644,258$ SNPs.
- Each entry in the matrix has $0,1,2$, and 9 , representing " $A A$ ", "AC", "CC", and "missing value", respectively.
- After removing 21 rows with all missing values, we are left with a matrix $X$ of size $1,043 \times 644,258$.


## Original MDS (PCA)

- Projection of 1,043 persons on the top-2 MDS (PCA) coordinates.
- Define

$$
K=H X X^{T} H=U \Lambda U^{T}, \quad H=I-\frac{1}{n} \mathbf{1 1}^{T}
$$

which is a positive semi-define matrix as centered Gram matrix whose eigenvalue decomposition is given by $U \Lambda U^{T}$.

- Take the first two eigenvectors $\sqrt{\lambda_{i}} u_{i}(i=1, \ldots, 2)$ as the projections of $n$ individuals.


## Figure: Original MDS (PCA)

Projection of 1,043 individuals on the top-2 MDS principal components, shows a continuous trajectory of human migration in history: human origins from Africa, then migrates to the Middle East, followed by one branch to Europe and another branch to Asia, finally spreading into America and Oceania.


## Random Projection MDS (PCA)

- To reduce the computational cost due to the high dimensionality $p=644,258$, we randomly select (without replacement) $\left\{n_{i}, i=1, \ldots, k\right\}$ from $1, \ldots, p$ with equal probability. Let $R \in \mathbb{R}^{k \times p}$ is a Bernoulli random matrix satisfying:

$$
R_{i j}= \begin{cases}1 / k & j=n_{i} \\ 0 & \text { otherwise }\end{cases}
$$

Now define

$$
\widetilde{K}=H\left(X R^{T}\right)\left(R X^{T}\right) H
$$

whose eigenvectors leads to new principal components of MDS.

## Figure: Comparisons of Random Projected MDS with Original One



Figure: (Left) Projection of 1043 individuals on the top 2 MDS principal components. (Middle) MDS computed from 5,000 random columns. (Right) MDS computed from 100,000 random columns. Pictures are due to Qing Wang.

## Question

## How does the Random Projection work?

## General MDS

- Given pairwise distances $d_{i j}$ between $n$ sample points, MDS aims to find $Y:=\left[y_{i}\right]_{i=1}^{n} \in \mathbb{R}^{k \times n}$ such that the following sum of square is minimized,

$$
\begin{array}{ll}
\min _{Y=\left[y_{1}, \ldots, y_{n}\right]} & \sum_{i, j}\left(\left\|y_{i}-y_{j}\right\|^{2}-d_{i j}^{2}\right)^{2}  \tag{1}\\
\text { subject to } & \sum_{i=1}^{n} y_{i}=0
\end{array}
$$

i.e. the total distortion of distances is minimized.

## Metric MDS

- When $d_{i j}=\left\|x_{i}-x_{j}\right\|$ is exactly given by the distances of points in Euclidean space $x_{i} \in \mathbb{R}^{p}$, classical (metric) MDS defines a positive semidefinite kernel matrix $K=-\frac{1}{2} H D H$ where $D=\left(d_{i j}^{2}\right)$ and $H=I-\frac{1}{n} \mathbf{1 1}$. Then, the minimization (1) is equivalent to

$$
\begin{equation*}
\min _{Y \in \mathbb{R}^{k \times n}}\left\|Y^{T} Y-K\right\|_{F}^{2} \tag{2}
\end{equation*}
$$

i.e. the total distortion of distances is minimized by setting the column vectors of $Y$ as the eigenvectors corresponding to $k$ largest eigenvalues of $K$.

## MDS toward Minimal Total Distortion

- The main features of MDS are the following.
- MDS looks for Euclidean embedding of data whose total or average metric distortion are minimized.
- MDS embedding basis is adaptive to the data, e.g. as a function of data via spectral decomposition.
- Can we have a tighter control on metric distortions, e.g. uniform distortion control?


## Uniformly Almost-Isometry?

- What if a uniform control on metric distortion: there exists a $\epsilon \in(0,1)$, such that for every $(i, j)$ pair,

$$
(1-\epsilon) \leq \frac{\left\|y_{i}-y_{j}\right\|^{2}}{d_{i j}^{2}} \leq(1+\epsilon) ?
$$

It is a uniformly almost isometric embedding or a Lipschitz mapping from metric space $\mathcal{X}$ to $\mathcal{Y}$.

- An beautiful answer is given by Johnson-Lindenstrauss Lemma, if $\mathcal{X}$ is an Euclidean space (or more generally Hilbert space), that $\mathcal{Y}$ can be a subspace of dimension $k=O\left(\log n / \epsilon^{2}\right)$ via random projections to obtain an almost isometry with high probability.


## Johnson-Lindenstrauss Lemma

Theorem (Johnson-Lindenstrauss Lemma)
For any $0<\epsilon<1$ and any integer $n$, let $k$ be a positive integer such that

$$
k \geq(4+2 \alpha)\left(\epsilon^{2} / 2-\epsilon^{3} / 3\right)^{-1} \ln n, \quad \alpha>0 .
$$

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

$$
\begin{equation*}
(1-\epsilon)\|u-v\|^{2} \leq\|f(u)-f(v)\|^{2} \leq(1+\epsilon)\|u-v\|^{2} \tag{3}
\end{equation*}
$$

Such a $f$ in fact can be found in randomized polynomial time. In fact, inequalities (3) holds with probability at least $1-1 / n^{\alpha}$.

## Remark

- Almost isometry is achieved with a uniform metric distortion bound (Bi-Lipschitz bound), with high probability, rather than average metric distortion control;
- The mapping is universal, rather than being adaptive to the data.
- The theoretical basis of this method was given as a lemma by Johnson and Lindenstrauss (1984) in the study of a Lipschitz extension problem in Banach space.
- In 2001, Sanjoy Dasgupta and Anupam Gupta, gave a simple proof of this theorem using elementary probabilistic techniques in a four-page paper. Below we are going to present a brief proof of Johnson-Lindenstrauss Lemma based on the work of Sanjoy Dasgupta, Anupam Gupta, and Dimitris Achlioptas.


## Note

- The distributions of the following two events are identical: unit vector was randomly projected to $k$-subspace $\Longleftrightarrow$ random vector on $S^{d-1}$ fixed top- $k$ coordinates.

Based on this observation, we change our target from random $k$-dimensional projection to random vector on sphere $S^{d-1}$.

- Let $x_{i} \sim N(0,1)(i=1, \cdots, p)$, and $X=\left(x_{1}, \cdots, x_{p}\right)$, then $Y=X /\|x\| \in S^{p-1}$ is uniformly distributed.
- Fixing top- $k$ coordinates, we get $z=\left(x_{1}, \cdots, x_{k}, 0, \cdots, 0\right)^{T} /\|x\| \in \mathbb{R}^{p}$. Let $L=\|z\|^{2}$ and $\mu:=k / p$. Note that $\mathbf{E}\left\|\left(x_{1}, \cdots, x_{k}, 0, \cdots, 0\right)\right\|^{2}=k=\mu \cdot \mathbf{E}\|x\|^{2}$.
- The following lemma shows that $L$ is concentrated around $\mu$.


## Key Lemma

## Lemma

For any $k<p$, there hold
(a) if $\beta<1$ then
$\operatorname{Prob}[L \leq \beta \mu] \leq \beta^{k / 2}\left(1+\frac{(1-\beta) k}{p-k}\right)^{(p-k) / 2} \leq \exp \left(\frac{k}{2}(1-\beta+\ln \beta)\right)$
(b) if $\beta>1$ then
$\operatorname{Prob}[L \geq \beta \mu] \leq \beta^{k / 2}\left(1+\frac{(1-\beta) k}{p-k}\right)^{(p-k) / 2} \leq \exp \left(\frac{k}{2}(1-\beta+\ln \beta)\right)$
Here $\mu=k / p$.

## Proof of Johnstone-Lindenstrauss Lemma

- If $p \leq k$, the theorem is trivial.
- Otherwise take a random $k$-dimensional subspace $S$, and let $v_{i}^{\prime}$ be the projection of point $v_{i} \in V$ into $S$, then setting $L=\left\|v_{i}^{\prime}-v_{j}^{\prime}\right\|^{2}$ and $\mu=(k / p)\left\|v_{i}-v_{j}\right\|^{2}$ and applying Lemma 1(a), we get that

$$
\begin{aligned}
& \operatorname{Prob}[L \leq(1-\epsilon) \mu] \leq \exp \left(\frac{k}{2}(1-(1-\epsilon)+\ln (1-\epsilon))\right) \\
& \leq \exp \left(\frac{k}{2}\left(\epsilon-\left(\epsilon+\frac{\epsilon^{2}}{2}\right)\right)\right) \\
& \quad \text { by } \ln (1-x) \leq-x-x^{2} / 2 \text { for } 0 \leq x<1 \\
&= \exp \left(-\frac{k \epsilon^{2}}{4}\right) \leq \exp (-(2+\alpha) \ln n) \\
& \quad \text { for } k \geq 4(1+\alpha / 2)\left(\epsilon^{2} / 2\right)^{-1} \ln n \\
&= \frac{1}{n^{2+\alpha}}
\end{aligned}
$$

## Proof of Johnstone-Lindenstrauss Lemma (continued)

- Similarly, we can apply Lemma 1(b) to get

$$
\begin{aligned}
\operatorname{Prob}[L \geq(1+\epsilon) \mu] \leq & \exp \left(\frac{k}{2}(1-(1+\epsilon)+\ln (1+\epsilon))\right) \\
\leq & \exp \left(\frac{k}{2}\left(-\epsilon+\left(\epsilon-\frac{\epsilon^{2}}{2}+\frac{\epsilon^{3}}{3}\right)\right)\right), \\
& \quad \text { by } \ln (1+x) \leq x-x^{2} / 2+x^{3} / 3 \text { for } x \geq 0 \\
= & \exp \left(-\frac{k}{2}\left(\epsilon^{2} / 2-\epsilon^{3} / 3\right)\right) \leq \exp (-(2+\alpha) \ln n), \\
& \quad \text { for } k \geq 4(1+\alpha / 2)\left(\epsilon^{2} / 2-\epsilon^{3} / 3\right)^{-1} \ln n \\
= & \frac{1}{n^{2+\alpha}}
\end{aligned}
$$

## Proof of Johnstone-Lindenstrauss Lemma (continued)

- Now set the map $f(x)=\sqrt{\frac{d}{k}} x^{\prime}=\sqrt{\frac{d}{k}}\left(x_{1}, \ldots, x_{k}, 0, \ldots, 0\right)$. By the above calculations, for some fixed pair $i, j$, the probability that the distortion

$$
\frac{\left\|f\left(v_{i}\right)-f\left(v_{j}\right)\right\|^{2}}{\left\|v_{i}-v_{j}\right\|^{2}}
$$

does not lie in the range $[(1-\epsilon),(1+\epsilon)]$ is at most $\frac{2}{n^{(2+\alpha)}}$. Using the trivial union bound with $\binom{n}{2}$ pairs, the chance that some pair of points suffers a large distortion is at most:

$$
\binom{n}{2} \frac{2}{n^{(2+\alpha)}}=\frac{1}{n^{\alpha}}\left(1-\frac{1}{n}\right) \leq \frac{1}{n^{\alpha}}
$$

Hence $f$ has the desired properties with probability at least $1-\frac{1}{n^{\alpha}}$. This gives us a randomized polynomial time algorithm.

## Proof of Lemma 1

- For Lemma 1(a),

$$
\begin{aligned}
& \operatorname{Prob}(L \leq \beta \mu)=\operatorname{Prob}\left(\sum_{i=1}^{k} x_{i}^{2} \leq \beta \mu\left(\sum_{i=1}^{p} x_{i}^{2}\right)\right) \\
&=\operatorname{Prob}\left(\beta \mu \sum_{i=1}^{p} x_{i}^{2}-\sum_{i=1}^{k} x_{i}^{2} \geq 0\right) \\
&= \operatorname{Prob}\left[\exp \left(t \beta \mu \sum_{i=1}^{p} x_{i}^{2}-t \sum_{i=1}^{k} x_{i}^{2}\right) \geq 1\right], \quad(t>0) \\
& \leq \mathbf{E}\left[\exp \left(t \beta \mu \sum_{i=1}^{p} x_{i}^{2}-t \sum_{i=1}^{k} x_{i}^{2}\right)\right] \\
& \quad(\text { by Markov's inequality })
\end{aligned}
$$

## Proof of Lemma 1 (continued)

$$
\begin{aligned}
r . h . s . & =\Pi_{i=1}^{k} \mathbf{E} \exp \left(t(\beta \mu-1) x_{i}^{2}\right) \Pi_{i=k+1}^{p} \mathbf{E} \exp \left(t \beta \mu x_{i}^{2}\right) \\
& =\left(\mathbf{E} \exp \left(t(\beta \mu-1) x^{2}\right)\right)^{k}\left(\mathbf{E} \exp \left(t \beta \mu x^{2}\right)\right)^{p-k} \\
& =(1-2 t(\beta \mu-1))^{-k / 2}(1-2 t \beta \mu)^{-(p-k) / 2}=: g(t)
\end{aligned}
$$

where the last equation uses the fact that if $X \sim \mathcal{N}(0,1)$, then

$$
\mathbf{E}\left[e^{s X^{2}}\right]=\frac{1}{\sqrt{(1-2 s)}},
$$

for $-\infty<s<1 / 2$.

## Proof of Lemma 1 (continued)

- Now we will refer to last expression as $g(t)$.
- The last line of derivation gives us the additional constraints that $t \beta \mu \leq 1 / 2$ and $t(\beta \mu-1) \leq 1 / 2$, and so we have $0<t<1 /(2 \beta \mu)$.
- Now to minimize $g(t)$, which is equivalent to maximize

$$
h(t)=1 / g(t)=(1-2 t(\beta \mu-1))^{k / 2}(1-2 t \beta \mu)^{(p-k) / 2}
$$

in the interval $0<t<1 /(2 \beta \mu)$. Setting the derivative $h^{\prime}(t)=0$, we get the maximum is achieved at

$$
t_{0}=\frac{1-\beta}{2 \beta(p-\beta k)}
$$

Hence we have

$$
h\left(t_{0}\right)=\left(\frac{p-k}{p-k \beta}\right)^{(p-k) / 2}\left(\frac{1}{\beta}\right)^{k / 2}
$$

and this is exactly what we need.

- Similar derivation is for the proof of Lemma 1 (b).


## Outline

```
Recall: PCA and MDS
Random Projections
    Example: Human Genomics Diversity Project
    Johnson-Lindenstrauss Lemma
    Proofs
```

Applications of Random Projections
Locality Sensitive Hashing
Compressed Sensing
Algorithms: BP, OMP, LASSO, Dantzig Selector, ISS, LBI etc.
From Johnson-Lindenstrauss Lemma to RIP
Appendix: A Simple Version of Johnson-Lindenstrauss Lemma

Applications of Random Projections

## Locality Sensitive Hashing (LSH)

- (M.S. Charikar 2002) A locality sensitive hashing scheme is a distribution on a family $\mathcal{F}$ of hash functions operating on a collection of objects, such that for two objects $x, y$

$$
\underset{h \in \mathcal{F}}{\operatorname{Prob}}[h(x)=h(y)]=\operatorname{sim}(x, y)
$$

where $\operatorname{sim}(x, y) \in[0,1]$ is some similarity function defined on the collection of objects.

- Such a scheme leads to efficient (sub-linear) algorithms for approximate nearest neighbor search and clustering.


## LSH via Random Projections

- (Goemans and Williamson (1995); Charikar (2002)) Given a collection of vectors in $R^{d}$, we consider the family of hash functions defined as follows: We choose a random vector $\vec{r}$ from the $d$-dimensional Gaussian distribution (i.e. each coordinate is drawn the 1-dimensional Gaussian distribution). Corresponding to this vector $\vec{r}$, we define a hash function $h_{\vec{r}}$ as follows:

$$
h_{\vec{r}}(\vec{u})=\operatorname{sign}(\vec{r} \cdot \vec{u})= \begin{cases}1 & \text { if } \vec{r} \cdot \vec{u} \geq 0 \\ -1 & \text { if } \vec{r} \cdot \vec{u}<0\end{cases}
$$

Then for vectors $\vec{u}$ and $\vec{v}$

$$
\operatorname{Pr}\left[h_{\vec{r}}(\vec{u})=h_{\vec{r}}(\vec{v})\right]=1-\frac{\theta(\vec{u}, \vec{v})}{\pi}
$$

## Compressed Sensing

- Compressive sensing can be traced back to 1950s in signal processing in geography. Its modern version appeared in LASSO (Tibshirani, 1996) and Basis Pursuit (Chen-Donoho-Saunders, 1998), and achieved a highly noticeable status after 2005 due to the work by Candes and Tao et al.
- The basic problem of compressive sensing can be expressed by the following under-determined linear algebra problem. Assume that a signal $x^{*} \in \mathbb{R}^{p}$ is sparse with respect to some basis (measurement matrix) $A \in \mathbb{R}^{n \times p}$ or $A \in \mathbb{R}^{n \times p}$ where $n<p$, given measurement $b=A x^{*}=A x^{*} \in \mathbb{R}^{n}$, how can one recover $x^{*}$ by solving the linear equation system

$$
\begin{equation*}
A x=b ? \tag{4}
\end{equation*}
$$

## Sparsity

- As $n<p$, it is an under-determined problem, whence without further constraint, the problem does not have an unique solution. To overcome this issue, one popular assumption is that the signal $x^{*}$ is sparse, namely the number of nonzero components $\left\|x^{*}\right\|_{0}:=\#\left\{x_{i}^{*} \neq 0: 1 \leq i \leq p\right\}$ is small compared to the total dimensionality $p$. Figure below gives an illustration of such sparse linear equation problem.


Figure: Illustration of Compressive Sensing (CS). A is a rectangular matrix with more columns than rows. The dark elements represent nonzero elements while the light ones are zeroes. The signal vector $x^{*}$, although high dimensional, is sparse.

## $P_{0}$

Without loss of generality, we assume each column of design matrix $A=\left[A_{1}, \ldots, A_{p}\right]$ has being standardized, that is, $\left\|A_{j}\right\|_{2}=1$, $j=1, \ldots, p$.

- With such a sparse assumption above, a simple idea is to find the sparsest solution satisfying the measurement equation:

$$
\begin{array}{lcl}
\left(P_{0}\right) & \min & \|x\|_{0}  \tag{5}\\
& \text { s.t. } & A x=b .
\end{array}
$$

- This is an NP-hard combinatorial optimization problem.


## A Greedy Algorithm: Orthogonal Matching Pursuit

Input $A, b$.
Output $x$.
initialization: $r_{0}=b, x_{0}=0, S_{0}=\emptyset$.
repeat if $\left\|r_{t}\right\|_{2}>\varepsilon$,

1. $j_{t}=\arg \max _{1 \leq j \leq p}\left|\left\langle A_{j}, r_{t-1}\right\rangle\right|$.
2. $S_{t}=S_{t-1} \cup j_{t}$.
3. $x_{t}=\arg \min _{x \in \mathbb{R}^{p}}\left\|b-A_{S_{t}} x\right\|$.
4. $r_{t}=b-A x_{t}$.
return $x^{t}$.

- Stephane Mallat and Zhifeng Zhang (1993), choose the column of maximal correlation with residue, as the steepest descent in residue.
- Joel Tropp (2004) shows that OMP recovers $x^{*}$ under the Incoherence condition; Tony Cai and Lie Wang (2011) extended it to noisy cases.


## Basis Pursuit (BP): $P_{1}$

- A convex relaxation of (5) is called Basis Pursuit (Chen-Donoho-Saunders, 1998),

$$
\begin{align*}
\left(P_{1}\right) & \min  \tag{6}\\
& \|x\|_{1}:=\sum\left|x_{i}\right| \\
\text { s.t. } & A x=b .
\end{align*}
$$

This is a tractable linear programming problem.

- Now a natural problem arises, under what conditions the linear programming problem $\left(P_{1}\right)$ has the solution exactly solves $\left(P_{0}\right)$, i.e. exactly recovers the sparse signal $x^{*}$ ?
- Donoho and Huo (2001) proposed Incoherence condition; Joel Tropp (2004) shows that BP recovers $x^{*}$ under the Incoherence condition.


## Illustration

Figure shows different projections of a sparse vector $x^{*}$ under $l_{0}, l_{1}$ and $l_{2}$, from which one can see in some cases the convex relaxation (6) does recover the sparse signal solution in (5).


Figure: Comparison between different projections. Left: projection of $x^{*}$ under $\|\cdot\|_{0}$; middle: projection under $\|\cdot\|_{1}$ which favors sparse solution; right: projection under Euclidean distance.

## Basis Pursuit De-Noising (BPDN)

- When measurement noise exists, i.e. $b=A x^{*}+\varepsilon$ with bound $\|\varepsilon\|_{2}$, the following Basis Pursuit De-Noising (BPDN) are used instead

$$
\begin{array}{ccl}
(B P D N) & \min & \|x\|_{1}  \tag{7}\\
& \text { s.t. } & \|A x-b\|_{2} \leq \epsilon .
\end{array}
$$

It's a convex quadratic programming problem.

- Similarly, Jiang-Yao-Liu-Guibas (2012) considers $\ell_{\infty}$-noise:

$$
\begin{array}{cl}
\min & \|x\|_{1} \\
\text { s.t. } & \|A x-b\|_{\infty} \leq \epsilon .
\end{array}
$$

This is a linear programming problem.

## LASSO

Least Absolute Shrinkage and Selection Operator (LASSO) (Tibshirani, 1996) solves the following problem for noisy measurement:

$$
\begin{equation*}
(L A S S O) \min _{x \in \mathbb{R}^{p}}\|A x-b\|_{2}^{2}+\lambda\|x\|_{1} \tag{8}
\end{equation*}
$$

- A convex quadratic programming problem.
- Yu-Zhao (2006), Lin-Yuan (2007), Wainwright (2009) show the model selection consistency (support recovery of $x^{*}$ ) of LASSO under the Irrepresentable condition.


## Dantzig Selector

The Dantzig Selector (Candes and Tao (2007)) is proposed to deal with noisy measurement $b=A x^{*}+\epsilon$ :

$$
\begin{array}{cl}
\min & \|x\|_{1}  \tag{9}\\
\text { s.t. } & \left\|A^{T}(A x-b)\right\|_{\infty} \leq \lambda
\end{array}
$$

- A linear programming problem, more scalable than convex quadratic programming (LASSO) for large scale problems.
- Bickel, Ritov, Tsybakov (2009) show that Dantzig Selector and LASSO share similar statistical properties.


## Differential Inclusion: Inverse Scaled Spaces (ISS)

Differential inclusion:

$$
\begin{align*}
& \dot{\rho}_{t}=\frac{1}{n} A^{T}\left(b-A x_{t}\right),  \tag{10a}\\
& \rho_{t} \in \partial\left\|x_{t}\right\|_{1} . \tag{10b}
\end{align*}
$$

starting at $t=0$ and $\rho_{0}=\beta_{0}=0$.

- Replace $\frac{\rho}{t}$ in KKT condition of LASSO by $\frac{\mathrm{d} \rho}{\mathrm{d} t}$,

$$
\frac{\rho_{t}}{t}=\frac{1}{n} A^{T}\left(b-A x_{t}\right), \quad t=\frac{1}{\lambda}
$$

to achieve unbiased estimator $\hat{x}_{t}$ when it is sign-consistent.

## Differential Inclusion: Inverse Scaled Spaces (ISS) (more)

- Burger-Gilboa-Osher-Xu (2006) (in image recovery it recovers the objects in an inverse-scale order as $t$ increases (larger objects appear in $x_{t}$ first))
- Osher-Ruan-Xiong-Yao-Yin (2016) shows that its solution is a debiasing regularization path, achieving model selection consistency under nearly the same conditions of LASSO.
- Note: if $\hat{x}_{\tau}$ is sign consistent $\operatorname{sign}\left(\hat{x}_{\tau}\right)=\boldsymbol{\operatorname { s i g n }}\left(x^{*}\right)$, then $\hat{x}_{\tau}=x^{*}+\left(A^{T} A\right)^{-1} A^{T} \varepsilon$ which is unbiased.
- However for LASSO, if $\hat{x}_{\lambda}$ is sign consistent $\boldsymbol{\operatorname { s i g n }}\left(\hat{x}_{\lambda}\right)=\boldsymbol{\operatorname { s i g n }}\left(x^{*}\right)$, then $\hat{x}_{\lambda}=x^{*}+\lambda\left(A^{T} A\right)^{-1} \operatorname{sign}\left(x^{*}\right)+\left(A^{T} A\right)^{-1} A^{T} \varepsilon$ which is biased.


## Example: Regularization Paths of LASSO vs. ISS




Figure: Diabetes data (Efron et al.'04) and regularization paths are different, yet bearing similarities on the order of parameters being nonzero

## Linearized Bregman Iterations

A damped dynamics below has a continuous solution $x_{t}$ that converges to the piecewise-constant solution of (10) as $\kappa \rightarrow \infty$.

$$
\begin{align*}
\dot{\rho}_{t}+\frac{\dot{x}_{t}}{\kappa} & =-\nabla_{x} \ell\left(x_{t}\right),  \tag{11a}\\
\rho_{t} & \in \partial \Omega\left(x_{t}\right), \tag{11b}
\end{align*}
$$

Its Euler forward discretization gives the Linearized Bregman Iterations (LBI, Osher-Burger-Goldfarb-Xu-Yin 2005) as

$$
\begin{align*}
& z_{k+1}=z_{k}-\alpha \nabla_{x} \ell\left(x_{k}\right)  \tag{12a}\\
& x_{k+1}=\kappa \cdot \operatorname{prox}_{\Omega}\left(z_{k+1}\right) \tag{12b}
\end{align*}
$$

where $z_{k+1}=\rho_{k+1}+\frac{x_{k+1}}{\kappa}$, the initial choice $z_{0}=x_{0}=0$ (or small Gaussian), parameters $\kappa>0, \alpha>0, \nu>0$, and the proximal map associated with a convex function $\Omega$ is defined by

$$
\operatorname{prox}_{\Omega}(z)=\arg \min _{x} \frac{1}{2}\|z-x\|^{2}+\Omega(x)
$$

## Uniform Recovery Conditions

- Under which conditions we can recover arbitrary $k$-sparse $x^{*} \in \mathbb{R}^{p}$ by those algorithms, for $k=\left|\operatorname{supp}\left(x^{*}\right)\right| \ll n<p$ ?
- Now we turn to several conditions presented in literature, under which the algorithms above can recover $x^{*}$. Below $A_{S}$ denotes the columns of $A$ corresponding to the indices in $S=\operatorname{supp}\left(x^{*}\right) ; A^{*}$ denotes the conjugate of matrix $A$, which is $A^{T}$ if $A$ is real.


## Uniform Recovery Conditions: a) Uniqueness

a) Uniqueness. The following condition ensures the uniqueness of $k$-sparse $x^{*}$ satisfying $b=A x^{*}$ :

$$
A_{S}^{*} A_{S} \geq r I, \quad \text { for some } r>0,
$$

without which one may have more than one $k$-sparse solutions in solving $b=A_{S} x$.

## Uniform Recovery Conditions: b) Incoherence

b) Incoherence. Donoho-Huo (2001) shows the following sufficient condition

$$
\mu(A):=\max _{i \neq j}\left|\left\langle A_{i}, A_{j}\right\rangle\right|<\frac{1}{2 k-1},
$$

for sparse recovery by BP, which is later improved by Elad-Bruckstein (2001) to be

$$
\mu(A)<\frac{\sqrt{2}-\frac{1}{2}}{k} .
$$

This condition is numerically verifiable, so the simplest condition.

## Uniform Recovery Conditions: c) Irrepresentable

c) Irrepresentable condition. It is also called the Exact Recovery Condition (ERC) by Joel Tropp (2004), which shows that under the following condition

$$
M=:\left\|A_{S^{c}}^{*} A_{S}\left(A_{S}^{*} A_{S}\right)^{-1}\right\|_{\infty}<1
$$

both OMP and BP recover $x^{*}$.

- This condition is unverifiable since the true support set $S$ is unknown.
- "Irrepresentable" is due to Yu and Zhao (2006) for proving LASSO's model selection consistency under noise, based on the fact that the regression coefficients of $A_{j} \sim A_{S} \beta+\varepsilon$ for $j \in S^{c}$, are the row vectors of $A_{S^{c}}^{*} A_{S}\left(A_{S}^{*} A_{S}\right)^{-1}$, suggesting that columns of $A_{S}$ can not be linearly represented by columns of $A_{S^{c}}$.


## Incoherence vs. Irrepresentable

- Tropp (2004) also shows that Incoherence condition is strictly stronger than the Irrepresentable condition in the following sense:

$$
\begin{equation*}
\mu<\frac{1}{2 k-1} \Rightarrow M \leq \frac{k \mu}{1-(k-1) \mu}<1 . \tag{13}
\end{equation*}
$$

- On the other hand, Tony Cai et al. $(2009,2011)$ shows that the Irrepresentable and the Incoherence condition are both tight in the sense that if it fails, there exists data $A, x^{*}$, and $b$ such that sparse recovery is not possible.


## Uniform Recovery Conditions: d) Restricted Isometry Property

d) Restricted-Isometry-Property (RIP) For all $k$-sparse $x \in \mathbb{R}^{p}$,

$$
\exists \delta_{k} \in(0,1) \text {, s.t. }
$$

$$
\left(1-\delta_{k}\right)\|x\|_{2}^{2} \leq\|A x\|_{2}^{2} \leq\left(1+\delta_{k}\right)\|x\|_{2}^{2} .
$$

- This is the most popular condition by Candes-Romberg-Tao (2006).
- Although RIP is not easy to be verified, Johnson-Lindestrauss Lemma says some suitable random matrices will satisfy RIP with high probability.


## Restricted Isometry Property for Uniform Exact Recovery

Candes (2008) shows that under RIP, uniqueness of $P_{0}$ and $P_{1}$ can be guaranteed for all $k$-sparse signals, often called uniform exact recovery.

Theorem
The following holds for all $k$-sparse $x^{*}$ satisfying $A x^{*}=b$.

- If $\delta_{2 k}<1$, then problem $P_{0}$ has a unique solution $x^{*}$;
- If $\delta_{2 k}<\sqrt{2}-1$, then the solution of $P_{1}(\mathrm{BP})$ has a unique solution $x^{*}$, i.e. recovers the original sparse signal $x^{*}$.


## Restricted Isometry Property for Stable Noisy Recovery

Under noisy measurement $b=A x^{*}+\varepsilon$, Candes (2008) also shows that RIP leads to stable recovery of the true sparse signal $x^{*}$ using BPDN.
Theorem
Suppose that $\|\varepsilon\|_{2} \leq \epsilon$. If $\delta_{2 k}<\sqrt{2}-1$, then

$$
\left\|\hat{x}-x^{*}\right\|_{2} \leq C_{1} k^{-1 / 2} \sigma_{k}^{1}\left(x^{*}\right)+C_{2} \epsilon,
$$

where $\hat{x}$ is the solution of BPDN and

$$
\sigma_{k}^{1}\left(x^{*}\right)=\min _{\operatorname{supp}(y) \leq k}\left\|x^{*}-y\right\|_{1}
$$

is the best $k$-term approximation error in $l_{1}$ of $x^{*}$.

## $\mathrm{JL} \Rightarrow \mathrm{RIP}$

- Johnson-Lindenstrauss Lemma ensures RIP with high probability.
- Baraniuk, Davenport, DeVore, and Wakin (2008) show that in the proof of Johnson-Lindenstrauss Lemma, one essentially establishes that a random matrix $A \in \mathbb{R}^{n \times p}$ with each element i.i.d. sampled according to some distribution satisfying certain bounded moment conditions, has $\|A x\|_{2}^{2}$ concentrated around its mean $\mathbf{E}\|A x\|_{2}^{2}=\|x\|_{2}^{2}$ (see Appendix), i.e.

$$
\begin{equation*}
\operatorname{Prob}\left(\left|\|A x\|_{2}^{2}-\|x\|_{2}^{2}\right| \geq \epsilon\|x\|_{2}^{2}\right) \leq 2 e^{-n c_{0}(\epsilon)} \tag{14}
\end{equation*}
$$

With this one can establish a bound on the action of $A$ on $k$-sparse $x$ by an union bound via covering numbers of $k$-sparse signals.

## JL $\Rightarrow$ RIP: Key Lemma

## Lemma

Let $A \in \mathbb{R}^{n \times p}$ be a random matrix satisfying the concentration inequality (14). Then for any $\delta \in(0,1)$ and any set all $T$ with $|T|=k<n$, the following holds

$$
\begin{equation*}
(1-\delta)\|x\|_{2} \leq\|A x\|_{2} \leq(1+\delta)\|x\|_{2} \tag{15}
\end{equation*}
$$

for all $x$ whose support is contained in $T$, with probability at least

$$
\begin{equation*}
1-2\left(\frac{12}{\delta}\right)^{k} e^{-c_{0}(\delta / 2) n} \tag{16}
\end{equation*}
$$

## Proof of Lemma

It suffices to prove the results when $\|x\|_{2}=1$ as $A$ is linear.

- Let $X_{T}:=\left\{x: \operatorname{supp}(x)=T,\|x\|_{2}=1\right\}$. We first choose $Q_{T}$, a $\delta / 4$-cover of $X_{T}$, such that for every $x \in X_{T}$ there exists $q \in Q_{T}$ satisfying $\|q-x\|_{2} \leq \delta / 4$. Since $X_{T}$ has dimension at most $k$, it is well-known from covering numbers that the capacity $\#\left(Q_{T}\right) \leq(12 / \delta)^{k}$.
- Now we are going to apply the union bound of (14) to the set $Q_{T}$ with $\epsilon=\delta / 2$. For each $q \in Q_{T}$, with probability at most $2 e^{-c_{0}(\delta / 2) n}, \mid A q\left\|_{2}^{2}-\right\| q\left\|_{2}^{2} \geq \delta / 2\right\| q \|_{2}^{2}$. Hence for all $q \in Q_{T}$, the same bound holds with probability at most

$$
2 \#\left(Q_{T}\right) e^{-c_{0}(\delta / 2) n} \leq 2\left(\frac{12}{\delta}\right)^{k} e^{-c_{0}(\delta / 2) n}
$$

## Proof Lemma (continued)

- Now we define $\alpha$ to be the smallest constant such that

$$
\|A x\|_{2} \leq(1+\alpha)\|x\|_{2}, \quad \text { for all } x \in X_{T}
$$

We can show that $\alpha \leq \delta$ with the same probability.

- For this, pick up a $q \in Q_{T}$ such that $\|q-x\|_{2} \leq \delta / 4$, whence by the triangle inequality

$$
\|A x\|_{2} \leq\|A q\|_{2}+\|A(x-q)\|_{2} \leq 1+\delta / 2+(1+\alpha) \delta / 4
$$

This implies that $\alpha \leq \delta / 2+(1+\alpha) \delta / 4$, whence $\alpha \leq 3 \delta / 4 /(1-\delta / 4) \leq \delta$. This gives the upper bound. The lower bound also follows this since

$$
\|A x\|_{2} \geq\|A q\|_{2}-\|A(x-q)\|_{2} \geq 1-\delta / 2-(1+\delta) \delta / 4 \geq 1-\delta
$$

which completes the proof.

## RIP Theorem

- With this lemma, note that there are at most $\binom{p}{k}$ subspaces of $k$-sparse, an union bound leads to the following result for RIP.
Theorem
Let $A \in \mathbb{R}^{n \times p}$ be a random matrix satisfying the concentration inequality (14) and $\delta \in(0,1)$. There exists $c_{1}, c_{2}>0$ such that if

$$
k \leq c_{1} \frac{n}{\log (p / k)}
$$

the following RIP holds for all $k$-sparse $x$,

$$
\left(1-\delta_{k}\right)\|x\|_{2}^{2} \leq\|A x\|_{2}^{2} \leq\left(1+\delta_{k}\right)\|x\|_{2}^{2}
$$

with probability at least $1-2 e^{-c_{2} n}$.

## Proof of RIP Theorem

## Proof.

For each of $k$-sparse signal $\left(X_{T}\right)$, RIP fails with probability at most

$$
2\left(\frac{12}{\delta}\right)^{k} e^{-c_{0}(\delta / 2) n}
$$

There are $\binom{p}{k} \leq(e p / k)^{k}$ such subspaces. Hence, RIP fails with probability at most

$$
2\left(\frac{e p}{k}\right)^{k}\left(\frac{12}{\delta}\right)^{2} e^{-c_{0}(\delta / 2) n}=2 e^{-c_{0}(\delta / 2) n+k[\log (e p / k)+\log (12 / \delta)]}
$$

Thus for a fixed $c_{1}>0$, whenever $k \leq c_{1} n / \log (p / k)$, the exponent above will be $\leq-c_{2} n$ provided that

$$
c_{2} \leq c_{0}(\delta / 2)-c_{1}(1+(1+\log (12 / \delta)) / \log (p / k)
$$

Note that one can always choose $c_{2}>0$ if $c_{1}>0$ is small enough.

## Summary

The following results are about mean estimation under noise:

- Johnson-Lindenstrauss Lemma tells: random projections give a universal basis to achieve uniformly almost isometric embedding, using $O\left(\varepsilon^{-2} \log n\right)$ number of projections
- Various Applications
- Dimensionality reduction: PCA or MDS
- Locality Sensitive Hashing: clustering, nearest neighbor search, etc.
- Compressed Sensing: random design satisfying Restricted Isometry Property with high probability


## Outline

```
Recall: PCA and MDS
Random Projections
    Example: Human Genomics Diversity Project
    Johnson-Lindenstrauss Lemma
    Proofs
Applications of Random Projections
    Locality Sensitive Hashing
    Compressed Sensing
    Algorithms: BP, OMP, LASSO, Dantzig Selector, ISS, LBI etc.
    From Johnson-Lindenstrauss Lemma to RIP
```

Appendix: A Simple Version of Johnson-Lindenstrauss Lemma

## A Simple Version of Johnson-Lindenstrauss Lemma

Theorem (Simplified Johnson-Lindenstrauss Lemma)
Let $A=\left[A_{i j}\right]^{k \times d}$ where $A_{i j} \sim \mathcal{N}(0,1)$ and $R=A / \sqrt{k}$. For any $0<\epsilon<1$ and any positive integer $k$, the following holds for all $0 \neq x \in \mathbb{R}^{d}$,

$$
\begin{equation*}
(1-\epsilon) \leq \frac{\|R x\|^{2}}{\|x\|^{2}} \leq(1+\epsilon), \tag{17}
\end{equation*}
$$

or for all $x \neq y \in \mathbb{R}^{d}$,

$$
\begin{equation*}
1-\epsilon \leq \frac{\|R x-R y\|^{2}}{\|x-y\|^{2}} \leq 1+\epsilon \tag{18}
\end{equation*}
$$

with probability at least $1-2 \exp \left(-\frac{k \varepsilon^{2}}{4}(1-2 \varepsilon / 3)\right)$.

## Remark

- This version of JL-Lemma is essentially used in the derivation of RIP in compressed sensing.
- Extension to sub-Gaussian distributions with bounded moment conditions can be found in Joseph Salmon's lecture notes.
- Given $n$ sample points $x_{i} \in V$. If we let

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

then

$$
\mathbb{P}\left(\|R u\|^{2} \geq 1+\varepsilon\right) \leq \exp (-(2+\alpha) \log n)=\left(\frac{1}{n}\right)^{2+\alpha}
$$

a union of $\binom{n}{2}$ probabilistic bounds gives the full JL-Lemma.

## A Basic Lemma

## Lemma

Let $X \sim \mathcal{N}(0,1)$.
(a) For all $t \in(-\infty, 1 / 2)$,

$$
\mathbf{E}\left(e^{t X^{2}}\right)=\frac{1}{1-2 t} .
$$

Proof.
(a) follows from Gaussian integral.

## Proof of JL Lemma

Let us denote $x \in \mathbb{R}^{d}, u=\frac{x}{\|x\|}$ and $Y_{i}$ the column values of the output, i.e $Y_{i}=(R u)_{i}=\sum_{j=1}^{d} R_{i, j} u_{j}$. Then,

$$
\begin{aligned}
\mathbb{E}\left(Y_{i}\right) & =\mathbb{E}\left(\sum_{j=1}^{d} R_{i, j} u_{j}\right)=\sum_{j=1}^{d} \mathbb{E}\left(R_{i, j} u_{j}\right)=\sum_{j=1}^{d} u_{j} \mathbb{E}\left(R_{i, j}\right)=0 \\
\operatorname{Var}\left(Y_{i}\right) & =\operatorname{Var}\left(\sum_{j=1}^{d} R_{i, j} u_{j}\right)=\mathbb{E}\left(\sum_{j=1}^{d} R_{i, j} u_{j}\right)^{2}=\sum_{j=1}^{d} \operatorname{Var}\left(R_{i, j} u_{j}\right) \\
& =\sum_{j=1}^{d} u_{j}^{2} \operatorname{Var}\left(R_{i, j}\right)=\frac{1}{k}
\end{aligned}
$$

## Proof of JL Lemma (continued)

(Upper). Defining $Z_{i}=\sqrt{k} Y_{i} \sim \mathcal{N}(0,1)$, one can state the following bound:

$$
\begin{aligned}
\mathbb{P}\left(\|R u\|^{2} \geq 1+\varepsilon\right) & =\mathbb{P}\left(\sum_{i=1}^{k}\left(\left(\sqrt{k} Y_{i}\right)^{2}-1\right) \geq \varepsilon k\right) \\
& =\mathbb{P}\left(\sum_{i=1}^{k}\left(Z_{i}^{2}-1\right) \geq \varepsilon k\right) \\
& \leq e^{-t \varepsilon k} \prod_{i=1}^{k} \mathbf{E} \exp \left(t\left(Z_{i}^{2}-1\right)\right), \quad \text { (Markov Ineq.) } \\
& =e^{-t k(1+\varepsilon)}\left[\mathbf{E} e^{t Z^{2}}\right]^{k} \\
& =e^{-t k(1+\varepsilon)}(1-2 t)^{-k / 2}=: g(t) \quad \text { (Lemma (a)) }
\end{aligned}
$$

## Proof of JL Lemma (continued)

Let

$$
h(t):=1 / g(t)=e^{t k(1+\varepsilon)}(1-2 t)^{k / 2} .
$$

Hence $\min _{t} g(t)$ is equivalent to $\max _{t} h(t)$. Taking derivative of $h(t)$,

$$
\begin{aligned}
& \left.0=\left.h^{\prime}(t)\right|_{t^{*}}=k(1+\varepsilon) e^{t k(1+\varepsilon)}(1-2 t)^{k / 2}-k e^{t k(1+\varepsilon)}(1-2 t)^{k / 2-1}\right)\left.\right|_{t^{*}} \\
& =k e^{t^{*} k(1+\varepsilon)}\left(1-2 t^{*}\right)^{k / 2-1}\left[(1+\varepsilon)\left(1-2 t^{*}\right)-1\right] \\
& \Rightarrow t^{*}=\frac{1}{2}-\frac{1}{2(1+\varepsilon)} \\
& \Rightarrow g\left(t^{*}\right)=e^{-t^{*} k(1+\varepsilon)}\left(1-2 t^{*}\right)^{-k / 2}=e^{-k \varepsilon / 2}(1+\varepsilon)^{k / 2} \\
& =\exp \left(-\frac{k \varepsilon}{2}+\frac{k}{2} \ln (1+\varepsilon)\right) \\
& \quad \leq \exp \left(-\frac{k \varepsilon}{2}+\frac{k}{2}\left(\varepsilon-\frac{\varepsilon^{2}}{2}+\frac{\varepsilon^{3}}{3}\right)\right), \quad u \operatorname{sing} \ln (1+x) \leq x-\frac{x^{2}}{2}+\frac{x^{3}}{3} \\
& \quad=\exp \left(-\frac{k \varepsilon^{2}}{4}+\frac{k \varepsilon^{3}}{6}\right), \quad \varepsilon \in(0,1)
\end{aligned}
$$

## Proof of JL Lemma (continued)

(Lower) . Similarly

$$
\begin{aligned}
\mathbb{P}\left(\|R u\|^{2} \leq 1-\varepsilon\right) & =\mathbb{P}\left(\sum_{i=1}^{k}\left(1-\left(\sqrt{k} Y_{i}\right)^{2}\right) \geq \varepsilon k\right) \\
& =\mathbb{P}\left(\sum_{i=1}^{k}\left(1-Z_{i}^{2}\right) \geq \varepsilon k\right) \\
& \leq e^{-t \varepsilon k} \prod_{i=1}^{k} \mathbf{E} \exp \left(t\left(1-Z_{i}^{2}\right)\right), \quad \text { (Markov Ineq.) } \\
& =e^{t k(1-\varepsilon)}\left[\mathbf{E} e^{-t Z^{2}}\right]^{k} \\
& =e^{t k(1-\varepsilon)}(1+2 t)^{-k / 2}=: g(t) \quad \text { (Lemma (a)) }
\end{aligned}
$$

## Proof of JL Lemma (continued)

Let

$$
h(t):=1 / g(t)=e^{t k(\varepsilon-1)}(1+2 t)^{k / 2}
$$

Taking derivative of $h(t)$,

$$
\begin{aligned}
& \left.0=\left.h^{\prime}(t)\right|_{t^{*}}=k(\varepsilon-1) e^{t k(\varepsilon-1)}(1+2 t)^{k / 2}+k e^{t k(\varepsilon-1)}(1+2 t)^{k / 2-1}\right)\left.\right|_{t^{*}} \\
& =k e^{t^{*} k(\varepsilon-1)}\left(1+2 t^{*}\right)^{k / 2-1}\left[(\varepsilon-1)\left(1+2 t^{*}\right)+1\right] \\
& \Rightarrow t^{*}=\frac{1}{2(1-\varepsilon)}-\frac{1}{2} \\
& \Rightarrow g\left(t^{*}\right)=e^{t^{*} k(1-\varepsilon)}\left(1+2 t^{*}\right)^{-k / 2}=e^{k \varepsilon / 2}(1-\varepsilon)^{k / 2} \\
& = \\
& \quad \exp \left(\frac{k \varepsilon}{2}+\frac{k}{2} \ln (1-\varepsilon)\right) \\
&
\end{aligned}
$$

Appendix: A Simple Version of Johnson-Lindenstrauss Lemma

