Lecture \#19: Dimension Reduction, Johnson-Lindenstrauss, etc.
March 8, 2017
Lecturer: Anupam Gupta
Scribe: Anupam Gupta, Sidhanth Mohanty

Today we'll talk about dimensionality reduction, and some related topics in data streaming.

## 1 Dimension Reduction

Suppose we are given a set of $n$ points $\left\{x_{1}, x_{2}, \ldots, x_{n}\right\}$ in $\mathbb{R}^{D}$. How small can we make $D$ and still maintain the Euclidean distances between the points? Clearly, we can always make $D=n-1$, since any set of $n$ points lies on a $n-1$-dimensional subspace. And this is (existentially) tight: e.g., the case when $x_{2}-x_{1}, x_{3}-x_{1}, \ldots, x_{n}-x_{1}$ are all orthogonal vectors.

But what if we were OK with the distances being approximately preserved? There can only be $D$ orthogonal unit vectors in $\mathbb{R}^{D}$, there could be as many as $\exp \left(c \varepsilon^{2} D\right)$ unit vectors which are $\varepsilon$-orthogonal-i.e., whose mutual inner products all lie in $[-\varepsilon, \varepsilon]$. Near-orthogonality allows us to pack exponentially more vectors!
Put another way, note that

$$
\|\vec{a}-\vec{b}\|_{2}^{2}=\langle\vec{a}-\vec{b}, \vec{a}-\vec{b}\rangle=\langle\vec{a}, \vec{a}\rangle+\langle\vec{b}, \vec{b}\rangle-2\langle\vec{a}, \vec{b}\rangle=\|\vec{a}\|_{2}^{2}+\|\vec{b}\|_{2}^{2}-2\langle\vec{a}, \vec{b}\rangle .
$$

And hence the squared Euclidean distance between any pair of the points defined by these $\varepsilon$ orthogonal vectors falls in $2(1 \pm \varepsilon)$. So, if we wanted $n$ points exactly at unit (Euclidean) distance from each other, we would need $n-1$ dimensions. (Think of a triangle in 2 -dims.) But if we wanted to pack in $n$ points which were at distance $(1 \pm \varepsilon)$ from each other, we could pack them into

$$
O\left(\frac{\log n}{\varepsilon^{2}}\right)
$$

dimensions.
Now, we prove that we can pack exponentially many vectors in $D$ dimensions. Indeed, to see how $N=\exp \left(c \varepsilon^{2} D\right)$ vectors can be packed in $D$ dimensions, pick $N$ vectors uniformly at random and independently from $\left\{ \pm \frac{1}{\sqrt{D}}\right\}$ : the expected dot product of any two given vectors is 0 and the dot product is the sum of $D$ independent random variables that are either $-\frac{1}{D}$ or $\frac{1}{D}$ so we can say something about concentration.

For two random vectors $r_{1}$ and $r_{2}$, a calculation using Chernoff bounds tells us

$$
\begin{aligned}
\operatorname{Pr}\left[\left\langle r_{1}, r_{2}\right\rangle \geq \varepsilon\right] & \leq \exp \left(-\frac{2 \varepsilon^{2}}{\sum_{i=1}^{D}\left(\frac{2}{D}\right)^{2}}\right) \\
& =\exp \left(-\frac{1}{2} \varepsilon^{2} D\right)
\end{aligned}
$$

If we have $\exp \left(-0.1 \varepsilon^{2} D\right)$ vectors, then union bound across all pairs gives us a probability strictly less than 1 of any pair having a dot product greater than $\varepsilon$, completing the proof.

### 1.1 The Johnson Lindenstrauss lemma

The Johnson Lindenstrauss "flattening" lemma says that such a claim is true not just for equidistant points, but for any set of $n$ points in Euclidean space:

Lemma 19.1. Let $\varepsilon \in(0,1 / 2)$. Given any set of points $X=\left\{x_{1}, x_{2}, \ldots, x_{n}\right\}$ in $\mathbb{R}^{D}$, there exists a map $A: \mathbb{R}^{D} \rightarrow \mathbb{R}^{k}$ with $k=O\left(\varepsilon^{-2} \log n\right)$ such that

$$
1-\varepsilon \leq \frac{\left\|A\left(x_{i}\right)-A\left(x_{j}\right)\right\|_{2}^{2}}{\left\|x_{i}-x_{j}\right\|_{2}^{2}} \leq 1+\varepsilon .
$$

Note that the target dimension $k$ is independent of the original dimension $D$, and depends only on the number of points $n$ and the accuracy parameter $\varepsilon$.
It is easy to see that we need at least $\Omega\left(\frac{1}{\varepsilon} \log n\right)$ using a packing argument. Noga Alon showed a lower bound of $\Omega\left(\frac{\log n}{\varepsilon^{2} \log 1 / \varepsilon}\right)$. Larsen and Nelson showed that any linear dimensionality reduction scheme must require $\Omega\left(\varepsilon^{-2} \log n\right)$ dimensions for some data sets. And recently they showed the tight and matching lower bound of $\Omega\left(\frac{\log n}{\varepsilon^{2}}\right)$ dimensions for any dimensionality reduction scheme from $n$ dimensions that preserves pairwise distances.

### 1.2 The construction

The JL lemma is pretty surprising, but the construction of the map is perhaps even more surprising: it is a super-simple random construction. Let $M$ be a $k \times D$ matrix, such that every entry of $M$ is filled with an i.i.d. draw from a standard normal $N(0,1)$ distribution (a.k.a. the "Gaussian" distribution). For $x \in \mathbb{R}^{D}$, define

$$
A(x)=\frac{1}{\sqrt{k}} M x
$$

That's it. You hit the vector $x$ with a Gaussian matrix $M$, and scale it down by $\sqrt{k}$. That's the map $A$. Note that it is a linear map: $A(x)+A(y)=A(x+y)$. So suppose we could show the following lemma:

Lemma 19.2. [Distributional Johnson-Lindenstrauss] Let $\varepsilon \in(0,1 / 2)$. If $A$ is constructed as above with $k=c \varepsilon^{-2} \log \delta^{-1}$, and $x \in \mathbb{R}^{D}$ is a unit vector, then

$$
\operatorname{Pr}\left[\|A(x)\|_{2}^{2} \in 1 \pm \varepsilon\right] \geq 1-\delta .
$$

Then we'd get a proof of Lemma 19.1. Indeed, set $\delta=1 / n^{2}$, and hence $k=O\left(\varepsilon^{-2} \log n\right)$. Now for each $x_{i}, x_{j} \in X$ we get that the squared length of $x_{i}-x_{j}$ is maintained to within $1 \pm \varepsilon$ with probability at least $1-1 / n^{2}$. By a union bound, all $\binom{n}{2}$ pairs of distances in $\binom{X}{2}$ are maintained with probability at least $1-\binom{n}{2} \frac{1}{n^{2}} \geq 1 / 2$. This proves Lemma 19.1.
A few comments about this construction:

- The above proof shows not only the existence of a good map, we also get that a random map as above works with constant probability! In other words, a Monte-Carlo randomized algorithm for dimension reduction. (Since we can efficiently check that the distances are preserved to within the prescribed bounds, we can convert this into a Las Vegas algorithm.) Or we can also get deterministic algorithms: see here.
- The algorithm (at least the Monte Carlo version) does not even look at the set of points $X$ : it works for any set $X$ with high probability. Hence, we can pick this map $A$ before the points in $X$ arrive.


### 1.3 Some properties of Gaussians

We'll be using basic facts about Gaussians, let's just recall them. The probability density function for the Gaussian $N\left(\mu, \sigma^{2}\right)$ is

$$
f(x)=\frac{1}{\sqrt{2 \pi} \sigma} e^{\frac{(x-\mu)^{2}}{2 \sigma^{2}}} .
$$

We also use the following; the proof just needs some elbow grease.
Proposition 19.3. If $G_{1} \sim N\left(\mu_{1}, \sigma_{1}^{2}\right)$ and $G_{2} \sim N\left(\mu_{2}, \sigma_{2}^{2}\right)$ are independent, then for $c \in \mathbb{R}$,

$$
\begin{gather*}
c G_{1} \sim N\left(c \mu_{1}, c^{2} \sigma_{1}^{2}\right)  \tag{19.1}\\
G_{1}+G_{2} \sim N\left(\mu_{1}+\mu_{2}, \sigma_{1}^{2}+\sigma_{2}^{2}\right) . \tag{19.2}
\end{gather*}
$$

### 1.4 The proof

Now, on to the proof of Lemma 19.2. Here's the main idea. Imagine that the vector we're considering is just the elementary unit vector $e_{1}=(1,0, \ldots, 0)$. Then $M e_{1}$ is just a vector with independent and identical Gaussian values, and we're interested in its length - the sum of squares of these Gaussians. Let us analyze the expected value of the length of this random vector. Entry $i$ in this random vector $\left(M e_{1}\right)_{i}$ is distributed as $\frac{1}{\sqrt{k}} N(0,1)$.
Thus, the expected value of the length is given by

$$
\mathbf{E}\left[\sum_{i=1}^{k}\left(M e_{1}\right)_{i}^{2}\right]=\sum_{i=1}^{k} \mathbf{E}\left[\left(M e_{1}\right)_{i}^{2}\right] \sum_{i=1}^{k} \frac{1}{k}=1
$$

Since the expectation is 1 , the heart is in the right place!
If these were bounded r.v.s, we'd be done - but they are not. However, their tails are very small, so things should work out: they are pretty much bounded.

So, if we take a sum of a bunch of such random variables (actually of their squares), it should behave pretty much like its mean (which is $\propto k$ ), because of a Chernoff-like argument. And so the expected length is close to $\sqrt{k}$, which explains the division by $\sqrt{k}$.
Of course this is very vague and imprecise. In fact, while the Laplace distribution with distribution $f(x) \propto e^{-\lambda|x|}$ for $x \in \mathbb{R}$ also has pretty thin tails-"exponential tails", this won't work the same, even if you squint as hard as you like. It turns out you need "sub-Gaussian tails". So we just need to make all this precise, and remove the assumption that the vector was just $e_{1}$. That's what the rest of the formal proof does: it has a few steps, but each of them is fairly elementary.

### 1.5 The proof, this time for real

Recall that we want to argue about the squared length of $A(x) \in \mathbb{R}^{k}$. To start off, observe that each coordinate of the vector $M x$ behaves like

$$
Y \sim\left\langle G_{1}, G_{2}, \ldots, G_{D}\right\rangle \cdot x=\sum x_{i} G_{i}
$$

where the $G_{i}$ 's are i.i.d. $N(0,1)$ r.v.s. But then Proposition 19.3 tells us that $Y \sim N\left(0, x_{1}^{2}+x_{2}^{2}+\right.$ $\left.\ldots+x_{D}^{2}\right)$. And since $x$ is a unit length vector, this is $N(0,1)$. So, each of the $k$ coordinates of $M x$ behaves just like an independent Gaussian!

### 1.5.1 The Expectation

What is the squared length of $A(x)=\frac{1}{\sqrt{k}} M x$, then? It is

$$
Z:=\sum_{i=1}^{k} \frac{1}{k} \cdot G_{i}^{2}
$$

where each $G_{i} \sim N(0,1)$, independent of the others. And since $\mathbf{E}\left[G_{i}^{2}\right]=\operatorname{Var}\left(G_{i}\right)+\mathbf{E}\left[G_{i}\right]^{2}=1$, we get $\mathbf{E}[Z]=1$.

### 1.5.2 Concentration about the Mean

Now to show that $Z$ does not deviate too much from 1 . And $Z$ is the sum of a bunch of independent and identical random variables. If only the $G_{i}$ 's were all bounded, we could have used a Chernoff bound and be done. But these are not bounded, so this is finally where we'll need to do a little work. ${ }^{1}$ So let's start down the ye olde Chernoff path, for the upper tail, say:

$$
\begin{equation*}
\operatorname{Pr}[Z \geq 1+\varepsilon] \leq \operatorname{Pr}\left[e^{t k Z} \geq e^{t k(1+\varepsilon)}\right] \leq \mathbf{E}\left[e^{t k Z}\right] / e^{t k(1+\varepsilon)}=\prod_{i}\left(\mathbf{E}\left[e^{t G_{i}^{2}}\right] / e^{t(1+\varepsilon)}\right) \tag{19.3}
\end{equation*}
$$

for every $t>0$. And what is $\mathbf{E}\left[e^{t G^{2}}\right]$ for $G \sim N(0,1)$ ? Let's calculate it:

$$
\begin{equation*}
\frac{1}{\sqrt{2 \pi}} \int_{g \in \mathbb{R}} e^{t g^{2}} e^{-g^{2} / 2} d g=\frac{1}{\sqrt{2 \pi}} \int_{z \in \mathbb{R}} e^{-z^{2} / 2} \frac{d z}{\sqrt{1-2 t}}=\frac{1}{\sqrt{1-2 t}} \tag{19.4}
\end{equation*}
$$

for $t<1 / 2$. So our current bound on the upper tail is that for all $t \in(0,1 / 2)$ we have

$$
\operatorname{Pr}[Z \geq(1+\varepsilon)] \leq\left(\frac{1}{e^{t(1+\varepsilon)} \sqrt{1-2 t}}\right)^{k}
$$

Let's just focus on part of this expression:

$$
\begin{align*}
\left(\frac{1}{e^{t} \sqrt{1-2 t}}\right) & \left.=\exp \left(-t-\frac{1}{2} \log (1-2 t)\right)\right)  \tag{19.5}\\
& =\exp \left((2 t)^{2} / 4+(2 t)^{3} / 6+\cdots\right) \leq \exp \left(t^{2}\left(1+2 t+2 t^{2}+\cdots\right)\right)  \tag{19.6}\\
& =\exp \left(t^{2} /(1-2 t)\right)
\end{align*}
$$

Plugging this back, we get

$$
\begin{aligned}
\operatorname{Pr}[Z \geq(1+\varepsilon)] & \leq\left(\frac{1}{e^{t(1+\varepsilon)} \sqrt{1-2 t}}\right)^{k} \\
& \leq \exp \left(k t^{2} /(1-2 t)-k t \varepsilon\right) \leq e^{-k \varepsilon^{2} / 8}
\end{aligned}
$$

if we set $t=\varepsilon / 4$ and use the fact that $1-2 t \geq 1 / 2$ for $\varepsilon \leq 1 / 2$. (Note: this setting of $t$ also satisfies $t \in(0,1 / 2)$, which we needed from our previous calculations.)
Almost done: let's take stock of the situation. We observed that $\|A(x)\|_{2}^{2}$ was distributed like an average of squares of Gaussians, and by a Chernoff-like calculation we proved that

$$
\operatorname{Pr}\left[\|A(x)\|_{2}^{2}>1+\varepsilon\right] \leq \exp \left(-k \varepsilon^{2} / 8\right) \leq \delta / 2
$$

[^0]for $k=\frac{8}{\varepsilon^{2}} \ln \frac{2}{\delta}$. A similar calculation bounds the lower tail, and finishes the proof of Lemma 19.2.
Citations: The JL Lemma was first proved in this paper of Bill Johnson and Joram Lindenstrauss. There have been several proofs after theirs, usually trying to tighten their results, or simplify the algorithm/proof (see citations in some of the newer papers): the proof follows some combinations of the proofs in this STOC '98 paper of Piotr Indyk and Rajeev Motwani, and this paper by Sanjoy Dasgupta and Anupam Gupta.

## 2 Using Random Signs instead of Gaussians

While Gaussians have all kinds of nice properties, they are real-valued distributions and hence require attention to precision. How about populating $A$ with draws from other, simpler distributions? How about setting each $M_{i j} \in_{R}\{-1,+1\}$, and letting $A=\frac{1}{\sqrt{k}} M$ ? (A random sign is also called a Rademacher random variables, the name Bernoulli being already taken for a random bit in $\{0,1\}$.) Now, we want to study the properties of

$$
\begin{equation*}
Z:=\sum_{i=1}^{k}\left(\sum_{j=1}^{D} A_{i j} \cdot x_{j}\right)^{2} \tag{19.7}
\end{equation*}
$$

To keep subscripts to a minimum, consider the inner sum for index $i$, which looks like

$$
\begin{equation*}
Y_{i}:=\left(\sum_{j} R_{j} \cdot x_{j}\right) \tag{19.8}
\end{equation*}
$$

each $R_{j}$ being an independent Rademacher variable.

$$
\begin{aligned}
\mathbf{E}\left[Y_{i}^{2}\right] & =\mathbf{E}\left[\left(\sum_{j} R_{j} x_{j}\right)\left(\sum_{l} R_{l} x_{l}\right)\right] \\
& =\mathbf{E}\left[\sum_{j} R_{j}^{2} x_{j}^{2}+\sum_{j \neq l} R_{j} R_{l} x_{j} x_{l}\right] \\
& =\sum_{j} \mathbf{E}\left[R_{j}^{2}\right] x_{j}^{2}+\sum_{j \neq l} \mathbf{E}\left[R_{j} R_{l}\right] x_{j} x_{l}=\sum_{j} x_{j}^{2}
\end{aligned}
$$

if the $R_{j}$ 's are pairwise independent, since $R_{j}^{2}=1$ and $\mathbf{E}\left[R_{j} R_{l}\right]=\mathbf{E}\left[R_{j}\right] \mathbf{E}\left[R_{l}\right]=0$ by independence. Plugging this into (19.7) and recalling that $A_{i j} \in\left\{-\frac{1}{\sqrt{k}},+\frac{1}{\sqrt{k}}\right\}$, we get

$$
\begin{equation*}
\mathbf{E}[Z]=\sum_{i=1}^{k} \frac{1}{k} \mathbf{E}\left[Y_{i}^{2}\right]=\sum_{i=1}^{k} \frac{1}{k} \sum_{j} x_{j}^{2}=\|x\|_{2}^{2} \tag{19.9}
\end{equation*}
$$

Just what we like! Now we just need to show that $\operatorname{Pr}\left[Z \in(1 \pm \varepsilon)\|x\|_{2}^{2}\right] \geq 1-\delta$ as long as $k=\Omega\left(\varepsilon^{-2} \log \delta^{-1}\right)$.

### 2.1 Concentration Around the Mean via Subgaussian-ness

Let's look over the proof in Section 1.5.2, and see what properties of Gaussians we used. We used that for $t \in(0,1 / 2)$,
$(\star) \mathbf{E}\left[e^{t G^{2}}\right] \leq \frac{1}{\sqrt{1-2 t}}$
but the rest of the Chernoff-like proof of Section 1.5 did not use any other facts about Gaussians. We can prove ( $\star$ ) for Rademacher random variables using explicit calculations, but instead let's give a useful abstraction:

Definition 19.4. A random variable $V$ is said to be subgaussian with parameter $c$ if for all real $s$, we have $\mathbf{E}\left[e^{s V}\right] \leq e^{c s^{2}}$.
(You can define subgaussian-ness alternatively as satisfying $\operatorname{Pr}[|V|>v] \leq C e^{-c v^{2}}$ for suitable constants $c, C$; these notes by Roman Vershynin show the two definitions are equivalent for symmetric distributions.) Here are some useful facts:

Fact 19.5. The following facts hold:
(i) (Gaussian) For $G \sim N(0,1)$, then $\mathbf{E}\left[e^{s G}\right]=e^{s^{2} / 2}$; i.e., it is $1 / 2$-subgaussian.
(ii) (Rademacher) A Rademacher random variable is $1 / 2$-subgaussian.
(iii) (Sums) If $V_{i}$ 's are independent and $c_{i}$-subgaussian, and $x$ is some vector, then $V=\sum_{i} x_{i} V_{i}$ is also $\sum_{i} c_{i} x_{i}^{2}$-subgaussian.

Proof. The first fact about Gaussians is a simple calcuation:

$$
\mathbf{E}\left[e^{s G}\right]=\frac{1}{\sqrt{2 \pi}} \int_{x \in \mathbb{R}} e^{s x} e^{-\frac{x^{2}}{2}} d x=\frac{1}{\sqrt{2 \pi}} e^{s^{2} / 2} \int_{x \in \mathbb{R}} e^{-\frac{(x-s)^{2}}{2}} d x=e^{s^{2} / 2} .
$$

(Good - it's heartening to know that a Gaussian is also subgaussian!)
For the second fact, observe that:

$$
\mathbf{E}\left[e^{s R}\right]=\frac{e^{s}+e^{-s}}{2}=\cosh s=1+\frac{s^{2}}{2!}+\frac{s^{4}}{4!}+\cdots \leq e^{s^{2} / 2}
$$

Finally,

$$
\mathbf{E}\left[e^{s V}\right]=\mathbf{E}\left[e^{\sum_{i}\left(s x_{i}\right) V_{i}}\right]=\prod_{i} \mathbf{E}\left[e^{s x_{i} V_{i}}\right] \leq \prod_{i} e^{c_{i}\left(s x_{i}\right)^{2}}=e^{c s^{2} \sum_{i} x_{i}^{2}}=e^{s^{2} \sum_{i} c_{i} x_{i}^{2}}
$$

The inequality in the middle uses the definition of subgaussian-ness.
Lemma 19.6. If $V$ is subgaussian with parameter $c$, then $E\left[e^{s V^{2}}\right] \leq \frac{1}{\sqrt{1-4 c s}}$ for $s>0$.
Proof. Well, suppose $G \sim N(0,1)$ is an independent Gaussian, then

$$
E_{V}\left[e^{s V^{2}}\right]=E_{G, V}\left[e^{\sqrt{2 s} V G}\right]
$$

by the calculation we just did for Gaussians. (Note that we've just introduced a Gaussian into the mix, without any provocation! But it will all work out.) Let just rewrite that

$$
E_{G, V}\left[e^{\sqrt{2 s} V G}\right]=E_{G}\left[E_{V}\left[e^{(\sqrt{2 s} G) V}\right]\right] .
$$

Using the $c$-subgaussian behavior of $V$ we bound this by

$$
E_{G}\left[e^{c(\sqrt{2 s}|G|)^{2}}\right]=E_{G}\left[e^{2 c s G^{2}}\right] .
$$

Finally, the calculation (19.4) gives this to be $\frac{1}{\sqrt{1-4 c s}}$.

Excellent. Note that $Y_{i}$ is a weighted sum of Rademachers (as defined in (19.8)); by Fact 19.8(ii) and (iii), each $R_{i}$ 's are $1 / 2$-subgaussian, so $Y_{i}=\sum_{i} x_{i} R_{i}$ is too. And hence $E\left[e^{t Y_{i}^{2}}\right] \leq \frac{1}{\sqrt{1-2 t}}$ for $\{-1,+1\}$-random variables as well. And now doing the same calculations as for the Gaussian case, from Section 1.5.2, we get that the Rademacher matrix also has the JL property!
Note that the Rademacher JL matrix $A$ now just requires us to pick $k D=O\left(D \varepsilon^{-2} \log \delta^{-1}\right)$ random bits (instead of $k D$ random Gaussians); also, there are fewer precision issues to worry about. One can consider other distributions to stick into the matrix $A$-all you need to show is that $Z$ has the right mean, and that the entries are subgaussian. ${ }^{2}$

Analogous to subgaussian distributions, we also explore subexponential distributions a bit.
Definition 19.7. A random variable $W$ is said to be subexponential with parameter $\nu$ if for all real $s$, we have $\mathbf{E}\left[e^{t(W-\mathbf{E} W)}\right] \leq e^{\frac{\nu^{2} t^{2}}{2}}$ for $|t| \leq \frac{C}{\nu}$ for an absolute constant $C$.
(An equivalent definition is $\operatorname{Pr}[W-\mathbf{E} W \geq \lambda] \leq c_{1} e^{-c_{2} \lambda}$ for some suitable constants $c_{1}, c_{2}$.)
Fact 19.8. The following facts about subexponential random variables hold:
(i) The exponential distribution is subexponential.
(ii) If $X$ is drawn from a subgaussian distribution, then the distribution of $X^{2}$ is necessarily subexponential.
(iii) The sum of subexponential random variables is a subexponential random variable.

In the proof of 19.2 , if we pick entries of $A$ from a Gaussian, then each $(A x)_{i}^{2}$ is distributed according to a subexponential distribution and the distribution of $\|A x\|_{2}^{2}$ is also subexponential.
On a final note, we call a distribution $\mathcal{D}$ over $k \times n$ matrices a distributional JL family if 19.2 is true when $A$ is drawn from $\mathcal{D}$.

Citations: The scheme of using Rademacher matrices instead of Gaussian matrices for JL was first proposed in this paper by Dimitris Achlioptas. The idea of extending it to subgaussian distributions appears in this paper of Indyk and Naor, and this paper of Matousek. The paper of Klartag and Mendelson generalizes this even further.

Fast $J$-L: Do we really need to plug in non-zero values into every entry of the matrix $A$ ? What if most of $A$ is filled with zeroes? The first problem is that if $x$ is a very sparse vector, then $A x$ might be zero with high probability? Achlioptas showed that having a random two-thirds of the entries of $A$ being zero still works fine: the paper of Nir Ailon and Bernard Chazelle showed that if you first hit $x$ with a suitable matrix $P$ which caused $P x$ to be "well-spread-out" whp, and then $\|A P x\| \approx\|x\|$ would still hold for a much sparser $A$. Moreover, this $P$ requires much less randomless, and furthermore, the computations can be done faster too! There has been much work on fast and sparse versions of JL: see, e.g., this SODA 11 paper of Ailon and Edo Liberty, and this arxiv preprint by Daniel Kane and Jelani Nelson. Jelani Nelson also has some notes on the Fast JL Transform.

## 3 Compressive Sensing

In an attempt to build a better machine to take MRI scans, we decrease the number of sensors. Then, instead of the signal $x$ we intended to obtain from the machine, we only have a small number

[^1]of measurements of this signal. Can we hope to recover $x$ from the measurements we made if we make sparsity assumptions on $x$ ? We use the term $r$-sparse signal for a vector with at most $r$ nonzero entries.

Formally, $x$ is a $n$-dimensional vector, and a measurement of $x$ with respect to a vector $a$ is a real number given by $\langle x, a\rangle$. And the question we want to answer is how to reconstruct $x$ with $r$ nonzero entries satisfying $A x=b$ if we are given $k \times n$ matrix $A$ and $n$ dimensional vector $b$.
Unfortunately, it turns out that the problem as formulated is NP-hard: but this is only assuming $A$ and $b$ are contrived by an adversary. Our setting is a bit different. $x$ is some $r$-sparse signal out there that we want to determine. We have a handle over $A$ and can choose it to be any matrix we like, and we are provided with appropriate $b=A x$, from which we attempt to reconstruct $x$.

Consider the following similar looking problem called the basis pursuit (BP) problem: minimize $\|x\|_{1}$ subject to $A x=b$. This problem can be formulated as a linear problem as follows, and hence can be efficiently solved.
Introduce $n$ new variables $y_{1}, y_{2}, \ldots, y_{n}$ under the constraints

$$
\begin{array}{r}
-y_{i} \leq x_{i} \leq y_{i} \\
A x=b
\end{array}
$$

and objective $\min \sum_{i} y_{i}$.
Definition 19.9. We call a matrix $A$ as BP-exact if for all $b=A x$ such that $x^{*}$ is an $r$-sparse solution, $x^{*}$ is also the unique solution to basis pursuit.

Theorem 19.10. [Donoho, Candes-Tao] If we pick $A \in \mathbb{R}^{k \times D}$ from a distributional JL family with $k \geq \Omega\left(r \log \left(\frac{D}{r}\right)\right)$, then with high probability $A$ is BP-exact.

We note that the $r \log \left(\frac{D}{r}\right)$ comes from $\log \binom{D}{r} \approx \log \left(\frac{D}{r}\right)^{r}=r \log \left(\frac{D}{r}\right)$.
The last ingredient that one would use to show 19.10 is the Restricted Isometry Property (RIP) of such a matrix $A$.

Definition 19.11. A matrix $A$ is $(t, \varepsilon)$-RIP if for all unit vectors $x$ with $\|x\|_{0} \leq t$, we have $\|A x\|_{2}^{2} \in[1 \pm \varepsilon]$.

Citations: See Chapter 4 of Ankur Moitra's book for more on compressed sensing, sparse recovery and basis pursuit. 19.10 comes from this paper by Emmanuel Candes and Terry Tao.


[^0]:    ${ }^{1}$ Note: we could take the easy way out, observe that the squares of Gaussians are chi-squared r.v.s, the sum of $k$ of them is chi-squared with $k$ degrees of freedom, and the internets conveniently has tail bounds for these things. But we digress.

[^1]:    ${ }^{2}$ If the $E\left[e^{t G^{2}}\right] \leq \frac{1}{\sqrt{1-a t}}$ for $a \neq 2$, you will need to redo the proof from Section 1.5.2 since the linear terms in (19.5) don't cancel any more to give (19.6). See, e.g., Indyk and Naor or Matousek for details.

