## Fast JL Transform

Hu Fu @SHUFE October 2022

## Picture So Far

- Recall: JL-transform multiplies $\mathbf{x} \in \mathbb{R}^{d}$ with a $t \times d$ matrix with i.i.d. standard Gaussian entries
- AMS emulates JL-transform with a matrix with $\{0,1\}$ entries, each row generated by a 4 -wise independent hash function
- This suggests that the matrix in JL-transform may be made simpler
- Achlioptas (2003) gave a transform with matrix entries from $\{-1,0,1\}$, about $2 / 3$ of them being 0
- Count-Sketch in fact approximately preserves $\ell_{2}$ norm (see homework)
- Recall we had pairwise independent hash functions $h:[d] \rightarrow[w]$ and $g:[d] \rightarrow\{ \pm 1\}$.
- The operation of Count-Sketch can be seen as multiplying $\mathbf{x}$ first with a $d \times d$ diagonal matrix $D$ with random entries from $\{ \pm 1\}$, and then by a $w \times d$ matrix $M$ with $M_{h(i), i}=g(i)$ and all other entries 0 .


## Making JL-transform Faster

- The original JL-transform takes time $\Omega(t d)$ to multiply the matrix with $\mathbf{x}$
. $t=O\left(\log \left(\frac{1}{\delta}\right) \epsilon^{-2}\right)$ if we would like to preserve the norm w.p. $1-\delta$
- Can we be faster asymptotically?
- Two approaches:
- Sparse JL-Transforms: construct matrices satisfying the JL-property with few nonzero entries
- Fast JL-Transforms: construct matrices satisfying the JL-property with structural properties which allow faster matrix multiplication [Ailon \& Chazelle, 2006]


## First Attempt

- If we try with a $\{0,1\}$ matrix, what happens if we sample, for each entry, just one coordinate of $\mathbf{x}$ ?
- Consider $t \times d$ matrix $S$, where in each row a uniformly random entry is 1 , and all other entries are 0 .

$$
\mathbb{E}\left[(S \mathbf{x})_{i}^{2}\right]=\sum_{j=1}^{d} \frac{x_{j}^{2}}{d} \Rightarrow \mathbb{E}\left[\left\|\sqrt{\frac{d}{t}} S \mathbf{x}\right\|_{2}^{2}\right]=\|\mathbf{x}\|_{2}^{2}
$$

- How well does $\|S \mathbf{x}\|_{2}^{2}$ concentrate around its expectation?
- In the worst case, $\mathbf{x}$ has only one non-zero entry, then $t$ needs to be $\Theta(d)$ for us to see that entry
. Generally, this doesn't work well when $\frac{\|\mathbf{x}\|_{\infty}}{\|\mathbf{x}\|_{2}} \approx 1$


## Rotating $\mathbf{x}$

- The ratio $\frac{\|\mathbf{x}\|_{\infty}}{\|\mathbf{x}\|_{2}}$ depends heavily on the bases in which we represent $\mathbf{x}$
- E.g., the ratio is 1 for $(1,0, \cdots, 0)$, but is only $1 / \sqrt{d}$ if we rotate it to $(1 / \sqrt{d}, \cdots, 1 / \sqrt{d})$
- The ratio is close to 1 if $\mathbf{x}$ "aligns well" with the axes, i.e., standard basis
- Idea: first rotate $\mathbf{x}$ randomly - equivalent to multiplying it by a random orthogonal matrix $M$


## Walsh-Hadamard Matrix

Def. A Hadamard matrix is an orthogonal $d \times d$ matrix with all entries from $\{1 / \sqrt{d},-1 / \sqrt{d}\}$.
Example. $H_{2}=\left(\begin{array}{cc}1 & 1 \\ 1 & -1\end{array}\right) / \sqrt{2}$
Welsh-Hadamard Matrices. $H_{d}=\left(\begin{array}{cc}H_{d / 2} & H_{d / 2} \\ H_{d / 2} & -H_{d / 2}\end{array}\right) / \sqrt{2}$

A recursive construction

Claim. $H_{d}$ is a Hadamard matrix

Proof. By induction, each entry of $H_{d / 2}$ is in $\{ \pm 1 / \sqrt{d / 2}\}$, so each entry of $H_{d}$ is in $\{ \pm 1 / \sqrt{d}\}$.
$H_{d}^{\top} H_{d}=\left(\begin{array}{cc}H_{d / 2}^{\top} & H_{d / 2}^{\top} \\ H_{d / 2}^{\top} & -H_{d / 2}^{\top}\end{array}\right)\left(\begin{array}{cc}H_{d / 2} & H_{d / 2} \\ H_{d / 2} & -H_{d / 2}\end{array}\right) / 2=\left(\begin{array}{cc}2 H_{d / 2}^{\top} H_{d / 2} & 0 \\ 0 & 2 H_{d / 2}^{\top} H_{d / 2}\end{array}\right) / 2=I$

## Walsh-Hadamard Matrix

Def. A Hadamard matrix is an orthogonal $d \times d$ matrix with all entries from $\{1 / \sqrt{d},-1 / \sqrt{d}\}$.
Example. $H_{2}=\left(\begin{array}{cc}1 & 1 \\ 1 & -1\end{array}\right) / \sqrt{2}$
Welsh-Hadamard Matrices. $H_{d}=\left(\begin{array}{cc}H_{d / 2} & H_{d / 2} \\ H_{d / 2} & -H_{d / 2}\end{array}\right) / \sqrt{2}$

A recursive
construction

Claim. $H_{d}$ is a Hadamard matrix

Claim. The product $H_{d} \mathbf{x}$ can be computed in time $O(d \log d)$. similar to Fast Fourier Transform

## Randomized Hadamard Matrix

- Of course a "good" vector $\mathbf{x}$ can become a "bad" $H_{d} \mathbf{x}$.
- We need to introduce randomness to $H_{d}$
- The -1 in $H_{2}$ may as well be elsewhere
- Let $D$ be a $d \times d$ diagonal matrix with diagonal entries randomly sampled from $\{-1,1\}$
- $H_{d} D$ is still Hadamard: $\left(H_{d} D\right)^{\top} H_{d} D=D^{\top} H_{d}^{\top} H_{d} D=I$.
- Write $H=H_{d}$ henceforth

Thm. For nonzero $\mathbf{x} \in \mathbb{R}^{d}$, let $\mathbf{y}=H D \mathbf{x}$, then $\mathbb{P}\left[\frac{\|\mathbf{y}\|_{\infty}}{\|\mathbf{y}\|_{2}} \geq \sqrt{\frac{2 \ln (4 d / \delta)}{d}}\right] \leq \frac{\delta}{2}$.

Thm. For nonzero $\mathbf{x} \in \mathbb{R}^{d}$, let $\mathbf{y}=H D \mathbf{x}$, then $\mathbb{P}\left[\frac{\|\mathbf{y}\|_{\infty}}{\|\mathbf{y}\|_{2}} \geq \sqrt{\frac{2 \ln (4 d / \delta)}{d}}\right] \leq \frac{\delta}{2}$.
Proof. Without loss of generality, assume $\|x\|_{2}=1$. Then $\|y\|_{2}=\|H D x\|_{2}=1$ as well.
To bound $\|\mathrm{y}\|_{\infty}$, note that for each $i, y_{i}$ has the same distribution as $\sum_{j} D_{j} x_{j}$ where $D_{j}$ 's are i.i.d. Rademacher variables. If we let $z_{j}:=D_{j} x_{j}$, then $\mathbb{E}\left[z_{j}\right]=0$. Chernoff bound does not apply...

Thm. (Hoeffding's Bound) If $X_{1}, \cdots, X_{n}$ are independent random variables where $X_{i} \in\left[a_{i}, b_{i}\right]$. Let $X=\sum X_{i}$.
Then $\mathbb{P}(|X-\mathbb{E}[X]| \geq s) \leq 2 \exp \left(-\frac{2 s^{2}}{\sum_{i}\left(b_{i}-a_{i}\right)^{2}}\right)$.
Proof idea similar to Chernoff bound. Use the following bound on $\mathbb{E}\left[e^{\lambda X_{i}}\right]$ :
Lemma. (Hoeffiding's Lemma) If random variable $X$ is in $\left[a_{i}, b_{i}\right]$, then $\mathbb{E}\left[e^{\lambda(X-\mathbb{E}[X])}\right] \leq \exp \left(\frac{\lambda^{2}(b-a)^{2}}{8}\right)$.

Thm. For nonzero $\mathbf{x} \in \mathbb{R}^{d}$, let $\mathbf{y}=H D \mathbf{x}$, then $\mathbb{P}\left[\frac{\|\mathbf{y}\|_{\infty}}{\|\mathbf{y}\|_{2}} \geq \sqrt{\frac{2 \ln (4 d / \delta)}{d}}\right] \leq \frac{\delta}{2}$.
Proof. Without loss of generality, assume $\|\mathrm{x}\|_{2}=1$. Then $\|\mathrm{y}\|_{2}=\|H D \mathbf{x}\|_{2}=1$ as well. To bound $\|\mathrm{y}\|_{\infty}$, note that for each $i, y_{i}$ has the same distribution as $\sum D_{j} x_{j}$ where $D_{j}$ 's are i.i.d. Rademacher variables. If we let $z_{j}:=D_{j} x_{j}$, then $\mathbb{E}\left[z_{j}\right]=0$. Chernoff bound does not apply since $z_{j} \in\left[-x_{j} / \sqrt{d}, x_{j} / \sqrt{d}\right]$ To apply Hoeffding's bound, note that $\sum 4 x_{j}^{2} / d^{2}=4 / d$.

$$
\mathbb{P}\left[\left|z_{j}\right| \geq \sqrt{\frac{2 \ln (4 d / \delta)}{d}}\right] \leq 2 \exp \left(-\frac{d}{2} \frac{2 \ln (4 d / \delta)}{d}\right)=2 \cdot \frac{\delta}{4 d}=\frac{\delta}{2 d}
$$

The theorem follows from a union bound over $z_{j}$ 's.
Thm. (Hoeffding's Bound) If $X_{1}, \cdots, X_{n}$ are independent random variables where $X_{i} \in\left[a_{i}, b_{i}\right]$. Let $X=\sum X_{i}$.
Then $\mathbb{P}(|X-\mathbb{E}[X]| \geq s) \leq 2 \exp \left(-\frac{2 s^{2}}{\sum_{i}\left(b_{i}-a_{i}\right)^{2}}\right)$.

## The Dieces meran

. For any $\mathbf{x} \in \mathbb{R}^{d}$ with $\|\mathbf{x}\|=1, \mathbb{P}\left[\left\|\sqrt{\frac{d}{t}} S H D \mathbf{x}\right\| \in[1-\epsilon, 1+\epsilon]\right]=$ ?

- $D \in\{-1,0,1\}^{d \times d}$ : diagonal matrix with Rademacher entries
- $H \in\{-1 / \sqrt{d}, 1 / \sqrt{d}\}^{d \times d}$ : Walsh Hadamard matrix
- $S \in\{0,1\}^{I \times d}$ : Sampling matrix, with exactly one 1 in each row
- $\|H D \mathbf{x}\|_{2}=1$. With probability $\geq 1-\frac{\delta}{2},\|H D \mathbf{x}\|_{\infty} \leq \sqrt{\frac{2 \ln (4 d / \delta)}{d}}$
. Let $\mathbf{z}:=S H D \mathbf{x}$. Then each $\mathbb{E}\left[z_{i}^{2}\right]=\frac{1}{d}, \mathbb{E}\left[\|\mathbf{z}\|_{2}^{2}\right]=\frac{t}{d}$. With probability $\geq 1-\frac{\delta}{2}, z_{i}^{2} \leq \frac{2 \ln (4 d / \delta)}{d}$.
Claim. If $z_{i}^{2} \leq \frac{2 \ln (4 d / \delta)}{d}$, for $t=\frac{2 \ln ^{2}(4 d / \delta) \ln (4 / \delta)}{\epsilon^{2}}, \mathbb{P}\left[\left\|\sqrt{\frac{d}{t}} S z\right\|_{2}^{2} \notin[1-\epsilon, 1+\epsilon]\right] \leq \frac{\delta}{2}$


## Fast JL-Transform

Thm. For any $\mathbf{x} \in \mathbb{R}^{d}$ with $\|\mathbf{x}\|=1$, for $t \geq \frac{2 \ln ^{2}(4 d / \delta) \ln (4 / \delta)}{\epsilon^{2}}$,
$\mathbb{P}\left[\left\|\sqrt{\frac{d}{t}} S H D \mathbf{x}\right\| \in[1-\epsilon, 1+\epsilon]\right] \geq 1-\delta$.

- $D \in\{-1,0,1\}^{d \times d}$ : diagonal matrix with Rademacher entries
- $H \in\{-1 / \sqrt{d}, 1 / \sqrt{d}\}^{d \times d}$ : Walsh Hadamard matrix
- $S \in\{0,1\}^{1 \times d}$ : Sampling matrix, with exactly one 1 in each row

