



Cuckoo hashing. Johnson-Lindenstrass.

Hashing with two choices: max load $O(\log \log n)$.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert x: place in $h_1(x)$ or $h_2(x)$ if space.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*,*x*: place *y* in $h_i(y)$ where $j \neq i$ if space.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*,*x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long.

Hashing with two choices: max load O(loglog n).

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*,*x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table.

Hashing with two choices: max load O(loglog n).

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

 C_{ℓ} - event of cycle of length ℓ at a vertex.

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

 \mathcal{C}_{ℓ} - event of cycle of length ℓ at a vertex.

$$\Pr[C_{\ell}] \le {\binom{m}{\ell}} {\binom{n}{\ell}} {\binom{\ell}{n}}^{2(\ell)} \le {\left(\frac{e^2}{8}\right)}^{\ell}$$
(1)

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

 C_{ℓ} - event of cycle of length ℓ at a vertex.

$$\Pr[C_{\ell}] \le {\binom{m}{\ell}} {\binom{n}{\ell}} {\binom{\ell}{n}}^{2(\ell)} \le {\left(\frac{e^2}{8}\right)}^{\ell}$$
(1)

Probability that an insert hits a cycle of length $\ell \leq \frac{\ell}{n} \left(\frac{e^2}{8}\right)^{\ell}$

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

 C_{ℓ} - event of cycle of length ℓ at a vertex.

$$\Pr[C_{\ell}] \le {\binom{m}{\ell}} {\binom{n}{\ell}} {\binom{\ell}{n}}^{2(\ell)} \le {\binom{e^2}{8}}^{\ell}$$
(1)

Probability that an insert hits a cycle of length $\ell \leq \frac{\ell}{n} \left(\frac{e^2}{8}\right)^{\ell}$

Rehash every $\Omega(n)$ inserts (if $\leq n/8$ items in table.)

Hashing with two choices: max load $O(\log \log n)$.

Cuckoo hashing:

Array. Two hash functions h_1 , h_2 .

Insert *x*: place in $h_1(x)$ or $h_2(x)$ if space. Else bump elt *y* in $h_i(x)$ u.a.r. for $i \in [1,2]$. Bump *y*, *x*: place *y* in $h_j(y)$ where $j \neq i$ if space. Else bump *y'* in $h_j(y)$. And so on.

If go too long. Fail. Rehash entire hash table. Fails if cycle for insert.

 C_{ℓ} - event of cycle of length ℓ at a vertex.

$$\Pr[C_{\ell}] \le {\binom{m}{\ell}} {\binom{n}{\ell}} {\binom{\ell}{n}}^{2(\ell)} \le {\binom{e^2}{8}}^{\ell}$$
(1)

Probability that an insert hits a cycle of length $\ell \leq \frac{\ell}{n} \left(\frac{e^2}{8}\right)^{\ell}$

Rehash every $\Omega(n)$ inserts (if $\leq n/8$ items in table.) O(1) time on average.

Points: $x_1, \ldots, x_n \in \mathbb{R}^d$.

Points: $x_1, \ldots, x_n \in \mathbb{R}^d$. Random $k = \frac{c \log n}{\varepsilon^2}$ dimensional subspace.

Points: $x_1, ..., x_n \in \mathbb{R}^d$. Random $k = \frac{c \log n}{e^2}$ dimensional subspace. Claim: with probability $1 - \frac{1}{n^{c-2}}$,

$$(1-\varepsilon)\sqrt{\frac{k}{d}}|x_i-x_j| \leq |y_i-y_j| \leq (1+\varepsilon)\sqrt{\frac{k}{d}}|x_i-x_j|$$

Points: $x_1, \ldots, x_n \in \mathbb{R}^d$. Random $k = \frac{c \log n}{\epsilon^2}$ dimensional subspace. Claim: with probability $1 - \frac{1}{n^{c-2}}$,

$$(1-\varepsilon)\sqrt{\frac{k}{d}}|x_i-x_j| \leq |y_i-y_j| \leq (1+\varepsilon)\sqrt{\frac{k}{d}}|x_i-x_j|$$

"Projecting and scaling by $\sqrt{\frac{d}{k}}$ preserves all pairwise distances w/in factor of $1 \pm \varepsilon$."

Method 1:

Method 1: Pick unit v₁

Method 1: Pick unit v_1 ,

Method 1: Pick unit v_1 , v_2 orthogonal to v_1 ,

Method 1: Pick unit v_1 , v_2 orthogonal to v_1 , ...

```
Method 1:

Pick unit v_1,

v_2 orthogonal to v_1,

...

v_k orthogonal to previous vectors...
```

```
Method 1:

Pick unit v_1,

v_2 orthogonal to v_1,

...

v_k orthogonal to previous vectors...

Method 2:
```

```
Method 1:

Pick unit v_1,

v_2 orthogonal to v_1,

...

v_k orthogonal to previous vectors...

Method 2:

Choose k vectors v_1, \ldots, v_k
```

```
Method 1:

Pick unit v_1,

v_2 orthogonal to v_1,

...

v_k orthogonal to previous vectors...

Method 2:

Choose k vectors v_1, \ldots, v_k

Gram Schmidt orthonormalization of k \times d matrix where rows are v_i.
```

```
Method 1:

Pick unit v_1,

v_2 orthogonal to v_1,

...

v_k orthogonal to previous vectors...

Method 2:

Choose k vectors v_1, \ldots, v_k

Gram Schmidt orthonormalization of k \times d matrix where rows are v_i.

remove projection onto previous subspace.
```

Projections.

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

 $y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$ Projection: (y_1, \dots, y_k) .

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for *k* dimensions.

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal *U* - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for *k* dimensions.

```
Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k
```

Уi

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal *U* - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

 $y_i = \langle v_i | x \rangle$

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

 $y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle$

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

 $y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle$

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random *k*-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal *U* - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

 $y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle = \langle e_i | z \rangle$

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random k-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

$$y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle = \langle e_i | z \rangle$$

Inverse of U maps e_i to random vector v_i

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random k-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

$$y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle = \langle e_i | z \rangle$$

Inverse of U maps e_i to random vector v_i

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random k-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

$$y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle = \langle e_i | z \rangle$$

Inverse of U maps e_i to random vector v_i

z = Ux is uniformly distributed on *d* sphere for unit $x \in \mathbb{R}^d$.

Project *x* into subspace spanned by v_1, v_2, \cdots, v_k .

$$y_1 = x \cdot v_1, y_2 = x \cdot v_2, \cdots, y_k = x \cdot v_k$$

Projection: (y_1, \ldots, y_k) .

Have: Arbitrary vector, random k-dimensional subspace.

View As: Random vector, standard basis for k dimensions.

Orthogonal U - rotates v_1, \ldots, v_k onto e_1, \ldots, e_k

$$y_i = \langle v_i | x \rangle = \langle U v_i | U x \rangle = \langle e_i | U x \rangle = \langle e_i | z \rangle$$

Inverse of U maps e_i to random vector v_i

z = Ux is uniformly distributed on *d* sphere for unit $x \in \mathbb{R}^d$.

 y_i is *i*th coordinate of random vector *z*.

Random projection: first k coordinates of random unit vector, z_i .

Random projection: first *k* coordinates of random unit vector, z_i . $E[\sum_{i \in [d]} z_i^2] = 1.$

Random projection: first *k* coordinates of random unit vector, z_i . $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

 $E[\sum_{i\in[k]} z_i^2] = \frac{k}{d}.$

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

 $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$. Linearity of Expectation.

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

 $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$. Linearity of Expectation.

Expected length is $\sqrt{\frac{k}{d}}$.

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

$$E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$$
. Linearity of Expectation.

Expected length is $\sqrt{\frac{k}{d}}$.

Johnson-Lindenstrass: close to expectation.

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

$$E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$$
. Linearity of Expectation.

Expected length is $\sqrt{\frac{k}{d}}$.

Johnson-Lindenstrass: close to expectation. *k* is large enough \rightarrow

Random projection: first k coordinates of random unit vector, z_i .

 $E[\sum_{i \in [d]} z_i^2] = 1$. Linearity of Expectation.

By symmetry, each z_i is identically distributed.

$$E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$$
. Linearity of Expectation.

Expected length is $\sqrt{\frac{k}{d}}$.

Johnson-Lindenstrass: close to expectation. *k* is large enough \rightarrow

 $pprox (1\pm \varepsilon)\sqrt{rac{k}{d}}$ with decent probability.

z is uniformly random unit vector.

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim: $\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

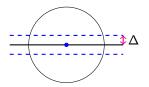
Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

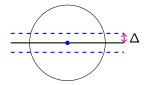


z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

 $|z_1| \ge \Delta$ if

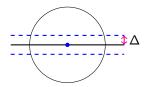


z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere.

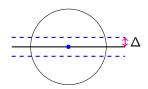


z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

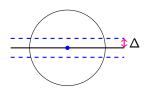


z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .

 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

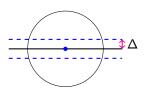


Area of caps

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

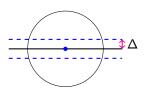
Area of caps

 \leq S.A. of sphere of radius $\sqrt{1-\Delta^2}$

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

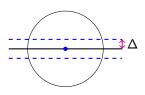
Area of caps

 \leq S.A. of sphere of radius $\sqrt{1-\Delta^2} \propto r^d = (1-\Delta^2)^{d/2}$

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

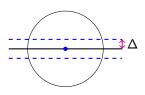
Area of caps \leq S.A. of sphere of radius $\sqrt{1 - \Delta^2}$ $\propto r^d = (1 - \Delta^2)^{d/2}$ $\propto (1 - \frac{t^2}{d})^{d/2}$

Concentration Bounds.

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap".

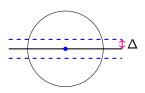
Area of caps \leq S.A. of sphere of radius $\sqrt{1 - \Delta^2}$ $\propto r^d = (1 - \Delta^2)^{d/2}$ $\propto (1 - \frac{t^2}{d})^{d/2} \approx e^{\frac{-t^2}{2}}$

Concentration Bounds.

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



$$\begin{split} |z_1| \geq \Delta \text{ if } \\ z \geq \Delta \text{ from equator of sphere.} \\ \text{Point on "Δ-spherical cap".} \end{split}$$

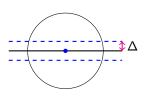
Area of caps \leq S.A. of sphere of radius $\sqrt{1-\Delta^2}$ $\propto r^d = (1-\Delta^2)^{d/2}$ $\propto (1-\frac{t^2}{d})^{d/2} \approx e^{\frac{-t^2}{2}}$ Constant of \propto is unit sphere area.

Concentration Bounds.

z is uniformly random unit vector. Random point on the unit sphere. $E[\sum_{i \in [k]} z_i^2] = \frac{k}{d}$.

Claim:
$$\Pr[|z_1| > \frac{t}{\sqrt{d}}] \le e^{-t^2/2}$$

Sphere view: surface "far" from equator defined by e_1 .



 $|z_1| \ge \Delta$ if $z \ge \Delta$ from equator of sphere. Point on " Δ -spherical cap". Area of caps

 $\leq \text{S.A. of sphere of radius } \sqrt{1 - \Delta^2} \\ \propto r^d = (1 - \Delta^2)^{d/2} \\ \propto \left(1 - \frac{t^2}{d}\right)^{d/2} \approx e^{\frac{-t^2}{2}} \\ \text{Constant of } \propto \text{ is unit sphere area.}$

 $\Pr[\text{any } z_i^2 > (2\log d)E[z_i^2]] \text{ is small}.$

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small.

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small.

Total Length?

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small.

Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$.

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t$] $\leq e^{-t^2 d/2}$

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2 d/2}$

Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, k = \frac{c \log n}{\varepsilon^2}$.

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t$] $\leq e^{-t^2 d/2}$

Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, k = \frac{c \log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right|\right]$$

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t$] $\leq e^{-t^2 d/2}$

Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, k = \frac{c \log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right]$$

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t$] $\leq e^{-t^2 d/2}$

Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c \log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k}$$

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr $\left[\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t \right] \le e^{-t^2 d/2}$

Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c \log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{Z_1^2 + Z_2^2 + \dots + Z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$. Pr[$\left|\sqrt{z_1^2 + z_2^2 + \cdots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}$] $\leq e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$. Pr[$\left|\sqrt{z_1^2 + z_2^2 + \cdots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}$] $\leq e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector.

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$. Pr[$\left|\sqrt{z_1^2 + z_2^2 + \cdots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}$] $\leq e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit.

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr $\left[\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right] > t \right] \le e^{-t^2 d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{c^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit. Projection fails to preserve $|x_i - x_i|$

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit. Projection fails to preserve $|x_i - x_j|$

with probability $\leq \frac{1}{n^c}$

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2 d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{Z_1^2 + Z_2^2 + \dots + Z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit.

Projection fails to preserve $|x_i - x_j|$

with probability $\leq \frac{1}{n^c}$

Scaled vector length also preserved.

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]$] is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left|\sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}}\right| > t$] $\leq e^{-t^2 d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}, \ k = \frac{c\log n}{\varepsilon^2}$.

$$\Pr\left[\left|\sqrt{Z_1^2 + Z_2^2 + \dots + Z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit.

Projection fails to preserve $|x_i - x_j|$

with probability $\leq \frac{1}{n^c}$

Scaled vector length also preserved.

 $\leq n^2$ pairs

Argued Pr[any $z_i^2 > (2 \log d) E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr[$\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t] \le e^{-t^2 d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}$, $k = \frac{c \log n}{c^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit.

Projection fails to preserve $|x_i - x_j|$

with probability $\leq \frac{1}{n^c}$

Scaled vector length also preserved.

 $\leq n^2$ pairs plus union bound

Argued Pr[any $z_i^2 > (2\log d)E[z_i^2]]$ is small. Total Length? $z = \sqrt{z_1^2 + z_2^2 + \cdots + z_k^2}$. Pr $\left[\left| \sqrt{(z_1^2 + z_2^2 + \cdots + z_k^2)} - \sqrt{\frac{k}{d}} \right| > t \right] \le e^{-t^2 d/2}$ Substituting $t = \varepsilon \sqrt{\frac{k}{d}}$, $k = \frac{c\log n}{c^2}$.

$$\Pr\left[\left|\sqrt{z_1^2 + z_2^2 + \dots + z_k^2} - \sqrt{\frac{k}{d}}\right| > \varepsilon \sqrt{\frac{k}{d}}\right] \le e^{-\varepsilon^2 k} = e^{-c\log n} = \frac{1}{n^c}$$

Johnson-Lindenstraus: For *n* points, $x_1, ..., x_n$, all distances preserved to within $1 \pm \varepsilon$ under $\sqrt{\frac{k}{d}}$ -scaled projection above.

View one pair $x_i - x_j$ as vector. Scale to unit.

Projection fails to preserve $|x_i - x_j|$

with probability $\leq \frac{1}{n^c}$

Scaled vector length also preserved.

 $\leq n^2$ pairs plus union bound \rightarrow prob any pair fails to be preserved with $\leq \frac{1}{n^{c-2}}$.

Find nearby points in high dimensional space.

Find nearby points in high dimensional space. Points could be images!

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary. Find close points to *x*:

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary.

Find close points to x:

Check grid cell and neighboring grid cells.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary.

Find close points to x:

Check grid cell and neighboring grid cells.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary.

Find close points to x:

Check grid cell and neighboring grid cells.

Project high dimensional points into low dimensions.

Find nearby points in high dimensional space. Points could be images!

Hash function $h(\cdot)$ s.t. $h(x_i) = h(x_j)$ if $d(x_i, x_j) \le \delta$.

Low dimensions: grid cells give \sqrt{d} -approximation. Not quite a solution. Why?

Close to grid boundary.

Find close points to x:

Check grid cell and neighboring grid cells.

Project high dimensional points into low dimensions.

Use grid hash function.

Implementing Johnson-Lindenstraus

Random vectors

Implementing Johnson-Lindenstraus

Random vectors have many bits

Implementing Johnson-Lindenstraus

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$$
$$E[C_l^2] =$$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

Coordinate for bit vector b.

 $C_{l} = \frac{1}{\sqrt{d}} \sum_{i} b_{i} z_{i}$ $E[C_{l}^{2}] = E[\frac{1}{d} \sum_{i,j} b_{i} b_{j} z_{i} z_{j}]$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_{l} = \frac{1}{\sqrt{d}} \sum_{i} b_{i} z_{i}$$
$$E[C_{l}^{2}] = E[\frac{1}{d} \sum_{i,j} b_{i} b_{j} z_{i} z_{j}] = \frac{1}{d} \sum_{i,j} E[b_{i} b_{j}] z_{i} z_{j} = \frac{1}{d} \sum_{i} z_{i}^{2}$$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_{l} = \frac{1}{\sqrt{d}} \sum_{i} b_{i} z_{i}$$
$$E[C_{l}^{2}] = E[\frac{1}{d} \sum_{i,j} b_{i} b_{j} z_{i} z_{j}] = \frac{1}{d} \sum_{i,j} E[b_{i} b_{j}] z_{i} z_{j} = \frac{1}{d} \sum_{i} z_{i}^{2} = \frac{1}{d}$$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_{l} = \frac{1}{\sqrt{d}} \sum_{i} b_{i} z_{i}$$
$$E[C_{l}^{2}] = E[\frac{1}{d} \sum_{i,j} b_{i} b_{j} z_{i} z_{j}] = \frac{1}{d} \sum_{i,j} E[b_{i} b_{j}] z_{i} z_{j} = \frac{1}{d} \sum_{i} z_{i}^{2} = \frac{1}{d}$$

Random vectors have many bits

Use random bit vectors: $\{-1, +1\}^d$ instead.

Almost orthogonal.

Project z.

$$C_{l} = \frac{1}{\sqrt{d}} \sum_{i} b_{i} z_{i}$$

$$E[C_{l}^{2}] = E[\frac{1}{d} \sum_{i,j} b_{i} b_{j} z_{i} z_{j}] = \frac{1}{d} \sum_{i,j} E[b_{i} b_{j}] z_{i} z_{j} = \frac{1}{d} \sum_{i} z_{i}^{2} = \frac{1}{d}$$

$$E[\sum_{i} C_{l}^{2}] = \frac{k}{d}$$

Project onto [-1,+1] vectors.

Project onto [-1,+1] vectors. $E[C] = E[\sum_{l} C_{l}^{2}] = \frac{k}{d}$

Project onto [-1,+1] vectors. $E[C] = E[\sum_{l} C_{l}^{2}] = \frac{k}{d}$ Concentration?

Project onto [-1,+1] vectors. $E[C] = E[\sum_{l} C_{l}^{2}] = \frac{k}{d}$ Concentration?

$$\Pr\left[|\boldsymbol{C} - \frac{k}{d}| \ge \varepsilon \frac{k}{d}\right] \le \boldsymbol{e}^{-\varepsilon^2 k}$$

Project onto $\left[-1,+1\right]$ vectors.

$$E[C] = E[\sum_{l} C_{l}^{2}] = \frac{k}{d}$$

Concentration?

$$\Pr\left[|C-\frac{k}{d}| \ge \varepsilon \frac{k}{d}\right] \le e^{-\varepsilon^2 k}$$

Choose $k = \frac{c \log n}{\varepsilon^2}$.

Project onto [-1, +1] vectors.

$$E[C] = E[\sum_{l} C_{l}^{2}] = \frac{k}{d}$$

Concentration?

$$\Pr\left[|C-\frac{k}{d}| \ge \varepsilon \frac{k}{d}\right] \le e^{-\varepsilon^2 k}$$

Choose $k = \frac{c \log n}{\epsilon^2}$. \rightarrow failure probability $\leq 1/n^c$.

$$\Pr\left[|C - \frac{k}{d}| \ge \varepsilon \frac{k}{d}\right] \le e^{-\varepsilon^2 k}$$

$$\Pr\left[|C - \frac{k}{d}| \ge \varepsilon \frac{k}{d}\right] \le e^{-\varepsilon^2 k}$$

Variance of C^2 ?

$$\Pr\left[|C - \frac{k}{d}| \ge \varepsilon \frac{k}{d}
ight] \le e^{-\varepsilon^2 k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$

$$\Pr\left[|C - \frac{k}{d}| \ge \varepsilon \frac{k}{d}
ight] \le e^{-\varepsilon^2 k}$$

Variance of *C*²? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2)$

$$\Pr\left[|C-rac{k}{d}|\geq arepsilonrac{k}{d}
ight]\leq e^{-arepsilon^2k}$$

Variance of *C*²? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2$

$$\Pr\left[|C-rac{k}{d}|\geq arepsilonrac{k}{d}
ight]\leq e^{-arepsilon^2k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) \left(\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2\right) \le \left(\frac{k}{d^2}\right) 2\left(\sum_i z_i^2\right)^2 \le \frac{2k}{d^2}.$

$$\Pr\left[|C-rac{k}{d}|\geq arepsilonrac{k}{d}
ight]\leq e^{-arepsilon^2k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}$. Roughly normal (gaussian):

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian): Density $\propto e^{-t^2/2}$ for *t* std deviations away.

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

$$\sigma = \frac{\sqrt{2k}}{d},$$

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) \left(\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2\right) \le \left(\frac{k}{d^2}\right) 2\left(\sum_i z_i^2\right)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

$$\sigma = rac{\sqrt{2k}}{d}, t = rac{arepsilon rac{k}{d}}{rac{\sqrt{2k}}{d}}$$

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

$$\sigma = rac{\sqrt{2k}}{d}, \ t = rac{arepsilon rac{k}{d}}{rac{\sqrt{2k}}{d}} = arepsilon \sqrt{k}/\sqrt{2}$$

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

So, assuming normality

$$\sigma = rac{\sqrt{2k}}{d}, \ t = rac{arepsilon rac{k}{d}}{rac{\sqrt{2k}}{\sqrt{2}}} = arepsilon \sqrt{k}/\sqrt{2}.$$

Probability of failure roughly $\leq e^{-t^2/2}$

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) (\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2) \le \left(\frac{k}{d^2}\right) 2(\sum_i z_i^2)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

So, assuming normality

$$\sigma = rac{\sqrt{2k}}{d}, \ t = rac{arepsilon rac{k}{d}}{rac{\sqrt{2k}}{\sqrt{2}}} = arepsilon \sqrt{k}/\sqrt{2}.$$

Probability of failure roughly $\leq e^{-t^2/2}$ $\rightarrow e^{\epsilon^2 k/4}$

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) \left(\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2\right) \le \left(\frac{k}{d^2}\right) 2\left(\sum_i z_i^2\right)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

So, assuming normality

$$\sigma = rac{\sqrt{2k}}{d}, \ t = rac{arepsilon rac{k}{d}}{rac{\sqrt{2k}}{\sqrt{2k}}} = arepsilon \sqrt{k}/\sqrt{2}.$$

Probability of failure roughly $\leq e^{-t^2/2}$ $\rightarrow e^{\epsilon^2 k/4}$

"Roughly normal."

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) \left(\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2\right) \le \left(\frac{k}{d^2}\right) 2\left(\sum_i z_i^2\right)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

So, assuming normality

$$\sigma = \frac{\sqrt{2k}}{d}, t = \frac{\varepsilon \frac{k}{d}}{\frac{\sqrt{2k}}{d}} = \varepsilon \sqrt{k} / \sqrt{2}.$$

Probability of failure roughly $\leq e^{-t^2/2}$ $\rightarrow e^{\varepsilon^2 k/4}$

"Roughly normal." Chernoff, Berry-Esseen, Central Limit Theorems.

$$\Pr\left[|C-\frac{k}{d}|\geq \varepsilon\frac{k}{d}
ight]\leq e^{-arepsilon^{2}k}$$

Variance of C^2 ? Recall $C_l = \frac{1}{\sqrt{d}} \sum_i b_i z_i$ $Var(C) \le \left(\frac{k}{d^2}\right) \left(\sum_i z_i^4 + 4\sum_{i,j} z_i^2 z_j^2\right) \le \left(\frac{k}{d^2}\right) 2\left(\sum_i z_i^2\right)^2 \le \frac{2k}{d^2}.$

Roughly normal (gaussian):

Density $\propto e^{-t^2/2}$ for *t* std deviations away.

So, assuming normality

$$\sigma = \frac{\sqrt{2k}}{d}, t = \frac{\varepsilon \frac{k}{d}}{\frac{\sqrt{2k}}{d}} = \varepsilon \sqrt{k} / \sqrt{2}.$$

Probability of failure roughly $\leq e^{-t^2/2}$ $\rightarrow e^{\varepsilon^2 k/4}$

"Roughly normal." Chernoff, Berry-Esseen, Central Limit Theorems.



Cuckoo hashing.

Cuckoo hashing.

Two hash functions.



Cuckoo hashing.

Two hash functions. Few cycles in random sparse graph.

Cuckoo hashing.

Two hash functions. Few cycles in random sparse graph. Chaining works!

Cuckoo hashing.

Two hash functions. Few cycles in random sparse graph. Chaining works!

Johnson-Lindenstrass.

Cuckoo hashing.

Two hash functions. Few cycles in random sparse graph. Chaining works!

Johnson-Lindenstrass.

 $O(\log n)$ dimensions give good approximation of distances.