

(I)  $Y \sim N(0, \beta I) \in \mathbb{R}^l$

$$D_{KL}(P_X \| P_Y) = \mathbb{E}_{X \sim P_X} \left[ -\log \left( \frac{P_Y}{P_X} \right) \right] = \mathbb{E}_{X \sim P_X} \left[ -\log \left( \frac{1}{P_X} \right) + \log P_Y \right] = -h(X) + \mathbb{E}_{X \sim P_X} [\log P_Y]$$

$$= -h(X) + \mathbb{E}_{X \sim P_X} \left[ \frac{l}{2} \log 2\pi\beta + \frac{1}{2\beta} \|X\|_2^2 \right] = -h(X) + \frac{l}{2} \log 2\pi\beta + \frac{1}{2\beta} \mathbb{E}[\|X\|_2^2]$$

(II) let  $\mathbb{E}[\|X\|_2^2] \leq t$  since from (I) we got:

$h(Y) = -D_{KL}(P_X \| P_X) + \frac{l}{2} \log(2\pi\beta) + \frac{1}{2\beta} \mathbb{E}[\|X\|_2^2]$ . In order to maximize  $h(Y)$ , one can increase  $\mathbb{E}[\|X\|_2^2]$  to its max, & also decrease  $D_{KL}(P_X \| P_X)$  since  $D_{KL} \geq 0$  its min = 0, therefore greedily thinking we will get

$\mathbb{E}[\|X\|_2^2] = t$ ,  $P_X = P_Y$  or  $D_{KL}(P_X \| P_X) = 0$  & therefore  $Y$  must take Normal distribution (its mean plays no role so let it be 0.)  $\Rightarrow Y \sim N(0, \beta I)$

$$\frac{\partial h(Y)}{\partial \beta} = \frac{l}{2} \log(2\pi\beta) + \frac{1}{2\beta} \frac{t}{t} = 0$$

$$\hookrightarrow \frac{+2\pi l}{4\pi\beta} + \frac{-t}{2\beta^2} = 0 \rightarrow \frac{t}{2\beta^2} = \frac{l}{2\beta} \rightarrow \beta^* = \frac{t}{l}$$

$$\text{thus: } h_{\max}(Y) = \frac{l}{2} \log(2\pi\beta) + \frac{t}{2\beta} = \frac{l}{2} \log\left(\frac{2\pi t}{l}\right) + \frac{l}{2} = \frac{l}{2} \log\left(\frac{2\pi t e}{l}\right)$$

(III) since  $I(X; Y) = h(X) - h(Y|X)$  & the fact that  $Y = AX + Z$ , we can deduce that  $h(Y|X) = h(Z)$ , therefore  $I(X; Y) = h(Y) - h(Z)$

Q.E.D. ■

130

✱  
 (I) We can see that the output of multiplication of two signed - permutation matrices  $A, B$  are always in  $\{0, \pm 1\}$ . So we must first prove that in each row & each column of  $C$ , there is only one nonzero element.

We know that each <sup>& column</sup> row of  $A$  is one of the  $\{\pm e_1, \pm e_2, \dots, \pm e_n\}$ , so when considering  $A b_i = \begin{bmatrix} a_{1i} & \dots & a_{ni} \end{bmatrix}^T b_i$ , there will be one and exactly one row of  $A$  (let it be  $a_k$ ) that  $a_k^T b_i \neq 0$ . And this will prove that each column of  $C$  can not be zero and it will be in the set  $\{\pm e_1, \dots, \pm e_n\}$ .

We can do the same thing for  $c_i^T B = a_i^T \begin{bmatrix} b_{i1} & \dots & b_{in} \end{bmatrix}$  and it will be suffice to prove it.

2nd

So the multiplication of two signed-permutation matrices will be a signed-permutation matrix as its elements  $c_{ij} \in \{0, \pm 1\}$  & each row & column has exactly one non-zero element. Q.E.D. ■

(II) let  $x$  be  $k$ -sparse vector ( $\|x\|_0 = k$ ) &  $B \in \mathbb{R}^{n \times n}$  a Signed-Permutation Matrix. (2) (b) (i)

Since  $\forall i, \exists j: y_i = b_i^T x = \pm e_j^T x = \pm x_j$ , we can deduce that  $y = Bx$  has the exact elements with ~~different~~ the same absolute value & in a different order since a permutation-matrix was applied.

therefore,  $y = Bx$  and  $x$  have the exact number of zero elements.

therefore  $y = Bx$  is a  $k$ -sparse vector since  $\|x\|_0 = \|y\|_0 \leq k$ . Q.E.D

(III) Since each row of  $B$  is in the set  $\{\pm e_1, \dots, \pm e_n\}$ , then we have

$$b_i^T b_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases} \quad \text{so let } C = BB^T \rightarrow C_{ij} = b_i^T b_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

therefore we can see that  $BB^T = I$ , Q.E.D  $\rightarrow$  also  $B^T B = I$  for the same rationale. Q.E.D

(IV)  $\|x - x'\|_2^2 = (x - x')^T (x - x') = x^T x + x'^T x' - 2x^T x'$

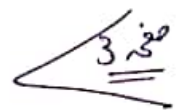
$$\|Bx - Bx'\|_2^2 = (Bx - Bx')^T (Bx - Bx') = x^T \underbrace{B^T B}_I x + x'^T \underbrace{B^T B}_I x' - 2x^T \underbrace{B^T B}_I x'$$

so  $\|x - x'\|_2^2 = \|Bx - Bx'\|_2^2 = x^T x + x'^T x' - 2x^T x'$  Q.E.D

$\hookrightarrow \|x - x'\|_2 = \|Bx - Bx'\|_2$

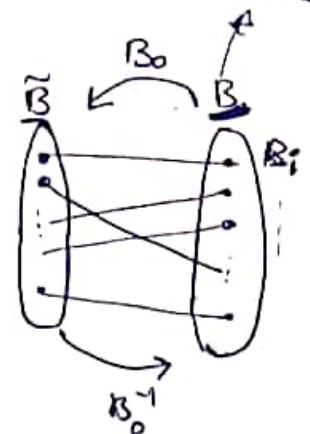
(V) Permutation Matrices  $\rightarrow n!$   
Signed-Permutation Matrices  $\rightarrow 2^n \times n!$

with  $\{0, \pm 1\}$  elements



the det of matrices

(VI) so in this graph which is depicted down below we can see that each  $B_{0i}$  will correspond to exactly one element of  $\tilde{B}$ , since  $B, B_0$  are full rank, they have inverse matrices, therefore  $\tilde{B}$  can correspond to only one  $B_{0i}$  via  $B_0^{-1}$ . Now since the distribution of  $B_0$ 's was Uniform over  $B_0$ , we can deduce that  $\tilde{B}$  will have Uniform distribution over its elements, since we have an injective transform from  $B_0$  to  $\tilde{B}$ .



Q.E.D

$$\frac{1}{|\tilde{B}|} = \int_{B_0} \mathbb{1}(\tilde{B}) = \int_{B_0} \mathbb{1}(B_0^{-1} \tilde{B}) = g_{\tilde{B}}(\tilde{B}) = \frac{1}{|B|}$$



Ⓐ In this  $B$  is a random matrix. It's obvious that  $E[b_{ij}] = 0$  for each element of  $B$ . Let  $Y = BX$ , then

$$Y_i = b_i^T X \Rightarrow E[Y_i] = E[b_i^T X] = E\left[\sum_{j=1}^d b_{ij} x_j\right] = \sum_{j=1}^d \underbrace{E[b_{ij}]}_0 x_j = 0$$

So  $\forall i, E[Y_i] = 0$  which leads to  $E[Y] = E[BX] = 0$ .

For the second part we can check that each element  $b_{ij}$  does not lie on the main diagonal is not possible.

Let  $i \neq j \rightarrow C_{ij} = b_i^T X X^T b_j = \sum_{k=1}^d b_{ik} b_{jk} x_k$

$\triangleleft 4.30$

let  $C = E[BX X^T B^T]$

$B_0 B_0^T = I$

Since from Ⓐ we got that applying a matrix  $B$  to  $B$  will not change its distribution & expectation value since  $B_0$  is a full rank matrix. So by multiplying  $C$  from both sides by  $B_0$  we will get:

$$B_0 C B_0^T = B_0 E[BX X^T B^T] B_0^T = E\left[\underbrace{B_0 B}_{B_0 \sim \text{Unif}(\frac{1}{|B|})} X X^T \underbrace{B_0^T B^T}_{B^T}\right] = E\left[\tilde{B} X X^T \tilde{B}^T\right] = C$$

$\tilde{B} \sim \text{Unif}(\frac{1}{|B|})$

Since  $B_0^T = B_0^{-1}$  and  $B_0 C B_0^T = C \rightarrow B_0 C \underbrace{B_0^T B}_I = C B_0 \rightarrow C B_0 = B_0 C$

✓ Main Proof:

(\*) now will prove that for each  $C_{ij}$  where  $i \neq j$ ;  $C_{ij} = 0$ .

$$C_{ij} = b_i^T \underbrace{X X^T}_{(x_i x_j)} b_j = x_i x_j \times b_i^T b_j = x_i x_j \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases} = x_i^2$$

$b_i \rightarrow \text{row}$

now since there is symmetry we can tell that on the diagonals each  $x_i \in \{x_1, \dots, x_d\}$  has the same probability so the expected value of each  $C_{ii}$  will be:  $I = \tilde{e} \sim \text{Unif}(\{1, 2, \dots, d\})$

$$\left. \begin{aligned} E[C_{ii}] &= \frac{1}{d} \sum_{i=1}^d x_i^2 = \frac{1}{d} \|X\|_2^2 \\ i \neq j: E[C_{ij}] &= 0 \end{aligned} \right\} C = E[BX X^T B^T] = \alpha I$$

where  $\alpha = \frac{\|X\|_2^2}{d}$

Q.E.D ■

<< In this phase we used the method of a paper by Emmanuel J. Candès & Mark A. Rudelson : (2016)

Emmanuel J. Candès & Mark A. Rudelson :

How well can we estimate a sparse vector? if  $\|x\|_0 \leq k$  and  $\|x\|_2 \leq 1$

We can see that each  $x$  with  $k$ -sparsity lies into a sphere of radius 1 in  $d$ -dimensions. so now we will find  $f_X(x)$  where  $x$  can have up to ' $k$ ' nonzero elements. so let  $\tilde{x} = [\underbrace{1, 1, \dots, 1}_k, 0, \dots, 0]$  → so the first  $k$ -elements of  $B$  will matter

$$f_X(x) = P[X=x] = P[B\tilde{x}=x] = P[B\tilde{x} \text{ is in first } k \text{ columns of } B]$$

for the first  $k$  columns  $\rightarrow \frac{k!(l-k)! 2^{l-k}}{2^l \times l!}$   $\rightarrow$   $l-k$  element of  $B$  does not play a role so  $(l-k)! \times 2^{l-k}$  different matrices

$$f_X(x) = \frac{k!(l-k)!}{l!} \times 2^k = \frac{2^{-k}}{\binom{l}{k}} = \frac{1}{2^k \binom{l}{k}}$$

since we wanted to count the number of  $x$ 's into the sphere which is  $2^k \times \binom{l}{k} = |A|_{\ell_2}$   
Now we let  $\epsilon = 1/2$ .

$$A = \left\{ x \mid x = \frac{1}{\sqrt{k}} (x_1, \dots, x_k), \forall i, x_i \in \{0, 1\}, \|x\|_2 = 1 \right\}$$

let  $N_\epsilon(P)$  denote the number of points with distance at most  $\epsilon$  with respect to  $P$ . now if we sum all the points in  $A$ , we will ensure that this number exceeds  $|A|$ . thus (let us assume that the points are positioned minimally.)

$$\sum_{P \in A} N_\epsilon(P) \geq |A|$$

$$|B| = P(A, \|\cdot\|_2, \epsilon = \frac{1}{2}) \quad B \subseteq A$$

$$P(A, \|\cdot\|_2, \epsilon) \times \overline{N_\epsilon(P)} \geq |A| \Rightarrow P(A, \|\cdot\|_2, \epsilon) \geq \frac{|A|}{|\overline{N_\epsilon(P)}|}$$

$$\text{ince } \overline{N_\epsilon} = \{ \hat{x} \mid \hat{x} \in A, \|\hat{x} - x\|_2^2 \leq \epsilon \} \subseteq \{ x \mid x \in A, \frac{1}{k} \|x - \hat{x}\|_2 \leq \epsilon \} \leftarrow P$$

what we did was to use the inequality to manipulate norm<sup>2</sup> to norm<sup>1</sup>.

لرفته براینکه این  $\ell_2$  به  $\ell_1$   
را بعد از این تبدیل، افق را باز بزرگ

مفهوم

$$\text{Let } \mathcal{U} = \left\{ u \in \left\{ 0, +\frac{1}{\sqrt{k}}, -\frac{1}{\sqrt{k}} \right\}^d, \|u\|_0 = k \right\}, |\mathcal{U}| = \binom{d}{k} 2^k$$

$\forall u, u' \in \mathcal{U}; \frac{1}{k} \|u' - u\|_0 \leq \|u' - u\|_2^2$  & thus if  $\|x' - x\|_2^2 \leq \varepsilon = \frac{1}{2}$ , then  $\|x' - x\|_0 \leq \frac{k}{2}$ . from this we observe that for any fixed  $x \in \mathcal{U}$

$$\left| \left\{ u' \in \mathcal{U} : \|x' - u\|_2^2 \leq \varepsilon \right\} \right| \leq \left| \left\{ u' \in \mathcal{U} : \|x' - x\|_0 \leq \frac{k}{2} \right\} \right| \leq \binom{d}{k/2} 3^{k/2}$$

suppose we wanted to construct  $\mathcal{X}$  by picking elements of  $\mathcal{U}$  at random. when adding the  $j^{\text{th}}$  point point to  $\mathcal{X}$  (denote by  $x_j$ ); the probability that  $x_j$  violates  $\forall x_i, x_j \in \mathcal{X} \|x_i - x_j\|_2^2 \geq \varepsilon$  is bounded by:

each element is either  $+\frac{1}{\sqrt{k}}$  or  $-\frac{1}{\sqrt{k}}$

$$\frac{(j-1) \binom{d}{k/2} 3^{k/2}}{\binom{d}{k} 2^k} \rightarrow \text{by union bound}$$

$$P_i \leq \frac{|X|^2}{2} \frac{\binom{d}{k/2} 3^{k/2}}{\binom{d}{k} 2^k}$$

$$\text{so we get } \mathcal{P}(X, \|\cdot\|_2, \varepsilon) \geq \frac{|X|}{|N_\varepsilon|}$$

$$\begin{aligned} \frac{|N_\varepsilon|}{|X|} &\leq \frac{\binom{d}{k/2} 3^{k/2}}{\binom{d}{k} 2^k} = \left(\frac{3}{4}\right)^{k/2} \frac{\binom{d}{k/2}}{\binom{d}{k}} = \left(\frac{3}{4}\right)^{k/2} \frac{k! (d-k)!}{\left(\frac{k}{2}\right)! \left(d - \frac{k}{2}\right)!} = \left(\frac{3}{4}\right)^{k/2} \times \prod_{i=1}^{\lfloor \frac{k/2}{2} \rfloor} \frac{\lfloor \frac{k/2}{2} \rfloor + i}{d - k + i} \\ &\leq \left(\frac{3}{4}\right)^{k/2} \left(\frac{k/2 + k/2}{d - k + \frac{k}{2}}\right)^{k/2} = \left(\frac{3}{4}\right)^{k/2} \left(\frac{d}{k} - \frac{1}{2}\right)^{k/2} \end{aligned}$$

$$\& \text{ since } k \leq \frac{d}{2} \rightarrow 2k \leq d \xrightarrow{+2d} 4d - 2k \geq 3d$$

$$\mathcal{P}(X, \|\cdot\|_2, \varepsilon) \geq \left(\frac{4d - 2k}{3k}\right)^{k/2} \geq \left(\frac{3d}{8k}\right)^{k/2} \geq \left(\frac{d}{k}\right)^{k/2}$$

6.150

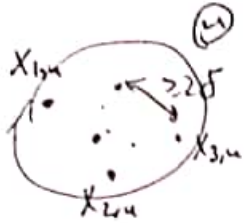
$$\text{finally } \Rightarrow \boxed{\mathcal{P}(X, \|\cdot\|_2, \varepsilon) \geq \left(\frac{d}{k}\right)^{k/2}} \quad \text{Q.E.D.}$$



$$\varepsilon = \min_{\hat{x}(y)} \max_{x \in S_n^d} \mathbb{E}[\|\hat{x} - x\|^2] \quad \text{for a given } U=u: \quad \hat{x} = \hat{x} \quad : (19)$$

here we have observed  $Y|U$  & estimated  $x$ . Furthermore, instead of one  $\varepsilon$ -packing set, we have  $|U|$   $\varepsilon$ -packing sets from our parametric set (1).

let  $T_u = \{x_{1,u}, \dots, x_{m,u}\}$  be the points such that they have at least  $2\delta$  distance



let us consider only this case, we know from Fano's inequality that

$$\varepsilon \geq \delta^2 \mathbb{E}_{U \sim \pi_u} [\mathbb{P}[J \neq \hat{J}]] \stackrel{\text{by}}{\geq} \delta^2 \left( 1 - \frac{\mathbb{I}(J; Y|U) + \log 2}{\log M} \right) \quad U=u$$

$$\text{thus:} \Rightarrow \varepsilon \geq \delta^2 \mathbb{E}_{U \sim \pi_u} \left[ 1 - \frac{\mathbb{I}(J; Y|U) + \log 2}{\log M} \right] \stackrel{\text{line 1}}{=} \delta^2 \left( 1 - \frac{\mathbb{E}_{U \sim \pi_u} [\mathbb{I}(J; Y|U) + \log 2]}{\log M} \right)$$

$$\Rightarrow \varepsilon \geq \delta^2 \left( 1 - \frac{\mathbb{I}(J; Y|U) + \log 2}{\log M} \right) \quad (*)$$

since by strong DPI we have  $\mathbb{I}(J; Y|U) \leq \mathbb{I}(X; Y)$ , from (\*) we can deduce that:

$$\varepsilon \geq \delta^2 \left( 1 - \frac{\mathbb{I}(X; Y) + \log 2}{\log M} \right) \quad \underline{\underline{\text{Q.E.D.}}} \quad \blacksquare$$

$$(*) \quad \mathbb{E}_{\pi_u} [\mathbb{I}(J; Y|U=u)] = \mathbb{I}(J; Y|U) \leq \mathbb{I}(X; Y)$$

$$\Phi(\delta) = \delta^2$$

→ انبؤ من سؤلك  
مستحيل



Let we observed  $E = \min_{\hat{f}(Y)} \max_X \mathbb{E}[\|X - \hat{f}(Y)\|_2^2]$ , : (3.5) '6

$E$  is bounded by  $\delta^2 \left(1 - \frac{I(X;Y) + \log 2}{\log M}\right)$ . In previous parts we found that: (we use the things we did in Assouad method)

$$\begin{cases} I(X;Y) = h(Y) - h(Z) \\ M \geq \left(\frac{d}{k}\right)^{k/2} \end{cases} \quad \begin{cases} \text{Serving max}\{h(Y)\} = Y \sim \mathcal{N}(0, \frac{d}{\epsilon} I) \\ \mathbb{E}\|T\|_2^2 \leq t \end{cases}$$

So we wish to minimize the R.H.S. by maximizing  $I(X;Y)$  which is done when  $h(Y)$  is maximized  $\rightarrow Y \sim \mathcal{N}(0, \beta I)$ .

$$\mathbb{E}[\|Y\|_2^2] = \mathbb{E}[\|AX + Z\|_2^2] = \mathbb{E}[X^T A^T A X + 2X^T A Z + Z^T Z] \quad \mathbb{E}Z = 0$$

since  $\mathbb{E}[Z^T Z] = n\sigma^2 \rightarrow \mathbb{E}[\|Y\|_2^2] \leq n\sigma^2 + \mathbb{E}[X^T A^T A X]$

$$\mathbb{E}[\|Y\|_2^2] \leq n\sigma^2 + (\mathbb{E}\|X\|_2^2) \sigma_{\max}^2(A^T A) \leq n\sigma^2 + (\mathbb{E}\|X\|_2^2) \|A\|_F^2$$

$$\Leftrightarrow \mathbb{E}[\|Y\|_2^2] \leq n\sigma^2 + 8\delta^2 \|V\|_2^2 \|A\|_F^2 = n\sigma^2 + 8\delta^2 \|A\|_F^2$$

the main part  $\Rightarrow I(X;Y) = h(Y) - h(Z) \leq \frac{n}{2} \log\left(\frac{2\pi t e}{n}\right) - \frac{n}{2} \log(2\pi\sigma^2 e)$  < 3.5.10

$$\Rightarrow I(X;Y) \leq \frac{n}{2} \log\left(\frac{t}{n\sigma^2}\right) = \frac{n}{2} \log\left(1 + \frac{8\delta^2 \|A\|_F^2}{n\sigma^2}\right) \quad \frac{\log(1+x) \leq x}{\text{if } x > 0}$$

$$\Rightarrow I(X;Y) \leq \frac{n}{2} \left(\frac{8\delta^2 \|A\|_F^2}{n\sigma^2}\right) = \frac{4\delta^2 \|A\|_F^2}{\sigma^2} \quad (*)$$

now plugging (\*) into the main assertion from 4<sup>th</sup> phase implies that  $\xrightarrow{\text{dumb log 2}}$

$$E \geq \delta^2 \left(1 - \frac{I(X;Y) + \log 2}{\log M}\right) \geq \delta^2 \left(1 - \frac{2}{k \log\left(\frac{d}{k}\right)} \left(\frac{4\delta^2 \|A\|_F^2}{\sigma^2}\right)\right)$$

let  $= \frac{1}{2}$



$$\frac{1}{2} = 1 - \frac{2}{k \log\left(\frac{d}{k}\right)} \left( \frac{4\delta^2 \|A\|_F^2}{\sigma^2} \right)$$

$$C = o(1)$$

$$\hookrightarrow 4\delta^2 \|A\|_F^2 = 4k \log\left(\frac{d}{k}\right) \rightarrow \delta^2 = \frac{k \log\left(\frac{d}{k}\right) \sigma^2 \times C}{\|A\|_F^2}$$

$$\boxed{E \geq \delta^2 \times \frac{1}{2} = \frac{C k \log\left(\frac{d}{k}\right) \sigma^2}{\|A\|_F^2}}$$

Q.E.D 

منه