## Problem definition

$\triangleright$ Covariate vectors: $x_{1}, x_{2}, \ldots, x_{n} \in \mathbb{R}^{d}$
$\triangleright$ Responses: $\boldsymbol{y}_{1}, \boldsymbol{y}_{2}, \ldots, y_{n} \in \mathbb{R}$
$\triangleright$ Model:

$$
\boldsymbol{y}_{\boldsymbol{i}}=\overline{\boldsymbol{w}}^{\top} \boldsymbol{x}_{\overline{\boldsymbol{\pi}}(i)}+\varepsilon_{i}, \quad i \in[n]
$$

$\triangleright$ Unknown linear function: $\overline{\boldsymbol{w}} \in \mathbb{R}^{d}$
$\triangleright$ Unknown permutation: $\bar{\pi} \in S_{n}$
$\triangle$ Measurement errors: $\varepsilon_{1}, \varepsilon_{2}, \ldots, \varepsilon_{n} \in \mathbb{R}$
e.g., $\left(\varepsilon_{i}\right)_{i=1}^{n}$ iid from $\left.\mathrm{N}\left(0, \sigma^{2}\right)\right)$

## Examples

## Multi-view geometry


$\triangleright$ Unknown correspondence between keypoints

$\triangleright$ Observe the entire emission spectrum at once

## Strong NP-hardness

## Definition 1 (Permuted Linear System)

 Given $X \in \mathbb{Z}^{n \times d}, \boldsymbol{Y} \in \mathbb{Q}^{n}$, decide if there exists a vector $\boldsymbol{w} \in \mathbb{Q}^{d}$ and a permutation $\pi \in S_{n}$ such that $\boldsymbol{X} \boldsymbol{w}=\boldsymbol{Y}_{\boldsymbol{\pi}}$Proposition 1.Permuted Linear System is strongly NP-complete by a reduction from 3-Partition.

Approximation guarantee for least-squares
Definition 2 (Least-squares recovery)
Given $\left(\boldsymbol{x}_{i}\right)_{i=1}^{n}$ and $\left(\boldsymbol{y}_{i}\right)_{i=1}^{n}$ from $\mathbb{R}$, find

$$
\left(\hat{w}_{m l e}, \hat{\pi}_{m l e}\right):=\underset{w \in \mathbb{R}, \pi \in S_{n}}{\arg \min } \sum_{i=1}^{n}\left(y_{i}-w x_{\pi(i)}\right)^{2}
$$

Theorem 1. There is an algorithm that given any inputs $\left(x_{i}\right)_{i=1}^{n},\left(y_{i}\right)_{i=1}^{n}$, and $\epsilon \in(0,1)$, returns a
$(1+\epsilon)$-approximate solution to the least squares problem in time $(n / \epsilon)^{O(k)}+\operatorname{poly}(n, d)$, where
$k=\operatorname{dim}\left(\operatorname{span}\left(x_{i}\right)_{i=1}^{n}\right)$.

## Approximation algorithm

This uses the following coreset result for linear systems: Proposition 2 (Boutsidis, Drineas, Magdon-Ismail) Given a matrix $A \in \mathbb{R}^{n \times k}$, there exists a weighted subset of $4 \boldsymbol{k}$ rows determined by a matrix $S \in \mathbb{R}^{4 k \times n}$ such that for any $\boldsymbol{b}$, every minimizer of the subsampled linear system

$$
w^{\prime} \in \arg \min _{w}\|S(A w-b)\|_{2}^{2}
$$

also satisfies

$$
\left\|A w^{\prime}-b\right\|_{2}^{2} \leq c
$$

for $\boldsymbol{c}=\boldsymbol{O}(\boldsymbol{n} / \boldsymbol{k})$. Morever, there exists an efficient algorithm which returns a matrix $S$ in time poly $(n, k)$.

Algorithm 1 Approximation algorithm
input Covariate matrix $X=\left[x_{1}\left|x_{2}\right| \cdots \mid x_{n}\right]^{\top} \in \mathbb{R}^{n \times k}$. response vector $\boldsymbol{y}=\left(\boldsymbol{y}_{1}, \boldsymbol{y}_{2}, \ldots, \boldsymbol{y}_{n}\right)^{\top} \in \mathbb{R}^{n}$; approximation parameter $\epsilon \in(0,1)$
1: Compute the matrix $S \in \mathbb{R}^{r \times n}$ from input matrix $X$
2: Let $\mathcal{B}$ be the set of all permutations of $\boldsymbol{y}$
3: Let $c:=1+4(1+\sqrt{n /(4 k)})^{2}$.
4: for each $b \in \mathcal{B}$ do
5: Compute $\tilde{\boldsymbol{w}}_{b} \in \arg \min _{w \in \mathbb{R}^{k}} \|[\| \mathbf{0}] S(X \boldsymbol{w}-b)_{2}^{2}$, and let $r_{b}:=\min _{\Pi \in \mathcal{P}_{n}} \|[\| \mathbf{0}] \boldsymbol{X} \tilde{\boldsymbol{w}}_{b}-\Pi^{\top} \boldsymbol{y}_{2}^{2}$
6: Construct a $\sqrt{\epsilon \boldsymbol{r}_{b} / \boldsymbol{c}}$-net $\mathcal{N}_{b}$ for the Euclidean ball of radius $\sqrt{\boldsymbol{c r _ { b }}}$ around $\tilde{\boldsymbol{w}}_{b}$, so that for each $v \in \mathbb{R}^{k}$ with $\|[\| 0] v-\tilde{\boldsymbol{w}}_{b 2} \leq \sqrt{\boldsymbol{c r _ { b }}}$, there exists $\boldsymbol{v}^{\prime} \in \mathcal{N}_{b}$ such that $\|[\| 0] v-v^{\prime}{ }_{2} \leq \sqrt{\epsilon r_{b} / c}$.
7: end for
8. return

$$
\hat{\boldsymbol{w}} \in \underset{\boldsymbol{w} \in \bigcup_{b \in \mathcal{B}} \mathcal{N}_{b}}{\arg \min } \min _{\Pi \in \mathcal{P}_{n}}\left\|\boldsymbol{X} \boldsymbol{w}-\boldsymbol{\Pi}^{\top} \boldsymbol{y}\right\|_{2}^{2}
$$

and
$\hat{\Pi} \in \underset{\Pi \in \mathcal{P}}{\arg \min }\left\|\boldsymbol{X} \hat{\boldsymbol{w}}-\Pi^{\top} \boldsymbol{y}\right\|_{2}^{2}$
$\Pi \in \mathcal{P}_{n}$

Polynomial time recovery in the random setting
Theorem 2. Fix any $\overline{\boldsymbol{w}} \in \mathbb{R}^{d}$ and $\overline{\boldsymbol{\pi}} \in \boldsymbol{S}_{n}$, and assume $n \geq \boldsymbol{d}$. Suppose $\left(x_{i}\right)_{i=0}^{n}$ are drawn iid from $\mathbf{N}\left(0, I_{d}\right)$, and $\left(\boldsymbol{y}_{i}\right)_{i=0}^{n}$ satisfy

$$
y_{0}=\overline{\boldsymbol{w}}^{\top} x_{0} ; \quad y_{i}=\overline{\boldsymbol{w}}^{\top} \boldsymbol{x}_{\bar{\pi}(i)}, \quad i \in[n]
$$

There is an algorithm that, given inputs $\left(x_{i}\right)_{i=0}^{n}$ and $\left(\boldsymbol{y}_{i}\right)_{i=0}^{n}$, returns $\overline{\boldsymbol{\pi}}$ and $\overline{\boldsymbol{w}}$ with high probability.

## Reduction to (random) subset sum

Given $d+1$ measurements and one correspondence $y_{0}=\overline{\boldsymbol{w}}^{T} \boldsymbol{x}_{0}$, for orthogonal $\left(x_{i}\right)_{i=0}^{n}$, can write:

$$
\begin{aligned}
y_{0} & =\sum_{j=1}^{d}\left(\bar{w}^{\top} x_{j}\right)\left(x_{j}^{\top} x_{0}\right)=\sum_{j=1}^{d} y_{\bar{\pi}^{-1}(j)}\left(x_{j}^{\top} x_{0}\right) \\
& =\sum_{i=1}^{d} \sum_{j=1}^{d} \mathbb{1}\{\bar{\pi}(i)=j\} \cdot \underbrace{y_{i}\left(x_{j}^{\top} x_{0}\right)}_{c_{i, j}}
\end{aligned}
$$

$\triangleright\left\{c_{i, j}\right\}$ and $y_{0}$ define a subset sum problem whose solution recovers the underlying correspondence.
$\triangleright$ In general $\left(x_{i}\right)_{i=0}^{n}$ are close to orthogonal; use the Moore-Penrose pseudoinverse.
$\triangleright$ The one given correspondence can be brute-forced, creating $d+1$ subset sum instances of which only one has a solution

## Solving random subset-sum instances

## Proposition 3 (Lagarias and Odlyzko).

Random instances of subset sum are efficiently solvable when the $\boldsymbol{c}_{i, j}$ 's are independently and uniformly distributed over a large enough subinterval of $\mathbb{Z}$.
This relies on the following inequality which lower bounds the closeness to the target sum of incorrect solutions. Lemma 1. For any vector ( $z_{i, j}$ ) which is not the correct correspondence

$$
\left|y_{0}-\sum_{i, j} z_{i, j} c_{i, j}\right| \geq \frac{1}{2^{\text {poly }(d)}}\|\bar{w}\|_{2}
$$

$\triangleright$ We show this bound holds under other distributions satisfying general anticoncentration bounds and even if the $\boldsymbol{c}_{i, j}$ 's are not independent

## Reduction to shortest vector problem

Definition 3 (Shortest vector problem).
Given a lattice basis $\mathbf{B} \subset \mathbb{R}^{d}$, output a lattice vector
$\mathrm{B} z \in \Lambda \mathrm{~B}$ where

$$
z=\underset{z \in \mathbb{Z}-\{0\}}{\arg \min }\|\mathrm{B} z\|_{2}^{2}
$$

Lemma 2 (LLL Lattice Basis Reduction)
There is an efficient approximation algorithm for solving the Shortest Vector Problem with
$\triangleright$ Approximation factor: $2^{d / 2}$
$\triangleright$ Running time: poly $(d, \log \lambda(B))$
Algorithm 2 Lattice algorithm for subset sum
input Source numbers $\left\{c_{i}\right\}_{i \in \mathcal{I}} \subset \mathbb{R}$; target sum $t \in \mathbb{R}$; lattice parameter $\boldsymbol{\beta}>\mathbf{0}$
1: Construct lattice basis $B \in \mathbb{R}^{(|\mathcal{I}|+2) \times(|\mathcal{I}|+1)}$ where

$$
B:=\left[\begin{array}{c}
\boldsymbol{I}|\mathcal{I}|+1 \\
\boldsymbol{\beta t} \mid-\boldsymbol{\beta} c_{i}: i \in \mathcal{I}
\end{array}\right] \in \mathbb{R}^{(|\mathcal{I}|+2) \times(|\mathcal{I}|+1)}
$$

2: Run LLL Lattice Basis Reduction to find non-zero lattice vector $v$ of length at most $2^{|\mathcal{I}| / 2} \cdot \lambda_{1}(B)$.

Information-theoretic lower bounds on SNR
Definition 4 (Random measurement setting) Observe

$$
y_{i}=\bar{w}^{T} x_{\bar{\pi}(i)}+\epsilon_{i}
$$

where
$\triangleright \epsilon_{i} \stackrel{i i d}{\sim} \mathcal{N}\left(0, \sigma^{2}\right)$ is the measurement noise
$\triangleright \boldsymbol{x}_{i} \stackrel{i i d}{\sim} \mathcal{N}\left(0, \boldsymbol{I}_{\boldsymbol{d}}\right)$ are the covariates
Definition 5 (SNR).
The signal-to-noise ratio for this model is $\|\bar{w}\|_{2}^{2} / \sigma^{2}$
Theorem 3.In the random measurement setting, if for some constant $C$

$$
S N R \leq C \cdot \min \left\{\frac{d}{\log \log n}, 1\right\}
$$

then for every estimator $\hat{\boldsymbol{w}}$, there exists a $\overline{\boldsymbol{w}} \in \mathbb{R}^{d}$ such that

$$
\mathbb{E}\left[\|\hat{w}-\bar{w}\|_{2}\right] \geq \frac{1}{24}\|\bar{w}\|_{2}
$$

$\triangleright$ Recall that standard linear regression satisfies the bound $\mathbb{E}\left[\| w_{m l e}-\bar{w}\right] \leq C \sigma \sqrt{d / n}$
$\triangleright$ In the low SNR regime, more measurements makes the problem more difficult

