

# Learning Noisy Parities

$$\{0,1\}^n$$

Unknown  $S \subseteq [n]$ ,  $w \in \{0,1\}^n$

First NOISELESS

Get several random

$$x \in \{0,1\}^n \text{ (uniformly)}$$

along with

$$f(x) = \bigoplus_{i \in S} x_i = \langle x, w \rangle \in \mathbb{F}_2$$

Find S.

with membership queries

ask for  $f(e_i)$

$$e_i = (0 \dots 0 \underset{i}{1} 0 \dots 0)$$

n queries

with random examples

If we get enough  $x$ 's so that  
span of these  $x$ 's =  $\mathbb{F}_2^n$

then can recover  $w$  from  
all the  $\langle w, x \rangle$   
(Gaussian elimination).

$$\textcircled{\ominus} \begin{matrix} \text{\#ex} \\ \nearrow \end{matrix} \begin{matrix} n \\ \left[ \begin{array}{c} \xrightarrow{x_1} \\ \xrightarrow{x_2} \\ \vdots \end{array} \right] \end{matrix} \begin{pmatrix} w \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \end{pmatrix}$$

want it to have rank  $n$ .

$$\begin{aligned} \underline{Q} \quad \Pr \left[ \begin{array}{c} \text{random } n \times n \text{ matrix} \\ \text{in } \mathbb{F}_2^n \text{ has rank } n \end{array} \right] \\ = \Pr \left[ \det(M) \neq 0 \right] \end{aligned}$$

Harsha: 0.51

Vishwas:  ~~$1/n$~~  0.5

Chaitanya:  $1 - \frac{n(n+1)}{2^{n+1}}$

Zach:  $1 - \frac{1}{2^n}$

Ahmed: 0.5.

---

$$\begin{aligned} P_n(\det(M) \neq 0) &= P_n\left[\forall i=1 \dots n, \right. \\ &\quad \left. \begin{array}{l} \text{ith column \# span} \\ \text{cols } 1 \dots i-1 \end{array} \right] \\ &= \left(1 - \frac{1}{2^n}\right) \left(1 - \frac{2}{2^n}\right) \left(1 - \frac{4}{2^n}\right) \\ &\quad \dots \left(1 - \frac{2^{i-1}}{2^n}\right) \dots \left(1 - \frac{2^{n-1}}{2^n}\right) \\ &\approx 0.36. \text{ (possibly)} \end{aligned}$$

---

$$P_n[x_1, \dots, x_m \text{ span dim} \leq n-1]$$

$$\approx P_n\left[\exists \text{ } n-1 \text{ dim subspace } W \text{ s.t. all } x_i \in W\right]$$

$$\leq \sum_{\substack{W \\ \dim(n-1)}} P_n[\text{all } x_i \in W]$$

$$\leq \left(\frac{1}{2^m}\right) \cdot (\#(n\text{-dim spaces}))$$

$$\leq \frac{2^n}{2^m}$$

Taking  $m = n + \omega(1)$  makes this  
 $P_n = o(1)$ .

### NOISY CASE

unknown  $w \in \{0,1\}^n$ .

Given many random examples

$x \in \{0,1\}^n$  and

$$\langle x, w \rangle + b \in \mathbb{F}_2$$

where  $b \in \{0,1\}$

with  $P_n[b=1] \leq \begin{cases} 0.01 \\ 0.49 \end{cases}$ .

How quickly can we find  $w$ ?

How many examples are needed?

## Coming up

1. Trivial  $2^n$  poly(n) time alg.
2. poly(n) examples suffice
3.  $O(2^n / \log n)$  time algorithm. (Blum-Kalai-Wasserman)  
+ examples

## Won't see

poly(n) examples +  $2^{n / \log \log n}$  time suffice (Lubashkevsky).

1 + 2:

Pick  $M = \text{poly}(n)$   
Get  $x_i$  and

$$y_i = \langle x_i, w \rangle + b_i \quad \text{for } i = 1, \dots, M.$$

For each  $v \in \{0, 1\}^n$

check  $N_v = (\# i \text{ s.t. } \langle x_i, v \rangle = y_i)$

Claim  $\exists$  exactly one  $v$  for which

this number  $N_v > (0.501) \cdot m$ .

Part 1 For  $v = w$   
w.h.p.  $N_w \geq 0.501 m$ .

Proof —  $N_w = m - (\# i \text{ st. } b_i = 1)$   
 $\geq m - 0.499m$  w.h.p.

Part 2 For  $v \neq w$ .  
 $P_n [N_v > 0.501 m] \ll \frac{1}{2^{2n}}$   
 $\hookrightarrow$  So  $P_n [\exists v \neq w \text{ st. } N_v > 0.501 m] <$   
 $\frac{2^n}{2^{2n}} = \frac{1}{2^n}$ .

Proof.  
 $P_n \left[ \#(i \text{ st. } \langle x_i, v \rangle = \langle x_i, w \rangle + b_i) \right.$   
 $\left. > 0.501 m \right]$   
 $= P_n \left[ \#(i \text{ st. } \langle x_i, v-w \rangle = \underline{b_i}) \right.$   
 $\left. > 0.501 m \right]$   
 $= P_n \left[ m \text{ uniform coin tosses} \right.$   
 $\left. \text{give } > 0.501 m \text{ heads} \right]$

$$\leq e^{-\Omega(m)}$$

---

BKW plan

Find  $x^* \in \{0,1\}^m$

and many different subsets

$$U_1, U_2, \dots, U_\ell \subseteq [m]$$

$$\text{each } |U_j| \leq t$$

$$\text{s.t. } \sum_{i \in U_j} x_i = x^*$$

---

Then we get many noisy  
opinions about  $\langle x^*, w \rangle$   
and so we can get  $\langle x^*, w \rangle$   
exactly.

Need  $t$  small,  $\ell$  big.

---

Claim If  $b_1, b_2, \dots, b_t \in \{0,1\}$

with  $b_i$  all independent

$$\ln[b_i = 1] = \eta$$

then. 
$$P_n \left[ \bigoplus_{i=1}^t b_i = 1 \right] = \frac{1 - (1 - 2\eta)^t}{2}$$

Proof 
$$\sum_{\substack{J \subseteq [t] \\ |J| \text{ odd}}} \eta^{|J|} (1-\eta)^{t-|J|}$$

$$= \sum_{\substack{n \text{ odd} \\ n \leq t}} \binom{t}{n} \eta^n (1-\eta)^{t-n}$$

$$= \frac{(\eta + (1-\eta))^t - (\eta - (1-\eta))^t}{2}$$

If  $\eta = \frac{1-\epsilon}{2}$ , then noise for  
 sum of  $\sum_{i=1}^t b_i = \frac{1-\epsilon^t}{2}$ .

Suppose we could find for every  $x^t \in \{0, 1\}^n$   $l$  different ways

of summing up  $t$ -subsets of the  $x_i$  to  $x^*$ , then we get a noiseless evaluation of  $\langle x^*, w \rangle$  provided

$$l \gg \text{poly} \left( \frac{1}{(1-2\eta)^t} \right)^n$$

$\eta = 0.49 \Rightarrow$

$$l \gg 2^{\Omega(t)} \Rightarrow$$

BKW Given  $x_1, \dots, x_{2^{n/\log n}}$  uniformly random  
we can find  $\leq \frac{n}{\log n}$  vectors in time  $2^{O(n/\log n)}$  that sum up to any desired vector.

Noise prob goes from  $\underline{O(1)}$  to  $\frac{1}{2} - 2^{-n/\log n}$

Fact Given  $x_1, \dots, x_{2^{\sqrt{n}}}$  random vectors

for any  $x^* \in \{0,1\}^n$ ,  $\exists$  some subset  
of  $\leq \sqrt{n}$  of the  $x_i$  that sum up to  $x^*$ .

---

Don't know how to find this in time  $2^{o(n)}$

NICE QUESTION!

---

Take all the  $x_1, \dots, x_m$ .

Look at the first  $k$  bits  
of each of them.

This puts the  $x_i$  into  $2^k$   
buckets.  $S_1, S_2, \dots, S_{2^k}$ ,

For each  $j \in [2^k]$ , let  
 $z_j$  be some element of  $S_j$ .

Produce the vectors

$$T_j = \left\{ z_j + w \quad : \quad w \in S_j \setminus \{z_j\} \right\}$$

Elts of  $T_j$ :

- ① Independent
- ② First  $k$  bits  $= 0$ .
- ③ Last  $n-k$  bits uniform.
- ④ each elt is a sum of 2 of the  $x_i$ 's.

UTs are new examples

From  $m$  examples

we got  $m - 2^k$  new examples

each new example is a sum of two old examples, and is uniform conditioned on the first  $k$  bits being all 0.

Can repeat this  $\frac{n-1}{k}$  times to get,

From  $m$  examples,  $m - \frac{n-1}{k} \cdot 2^k$  examples whose first  $n-1$  bits are 0 and the last bit is uniform,

each new example is a sum of  
 $2^{n/k}$  original examples.

---

Want  $2^{n/k} = \frac{n}{\log n}$

$$\frac{n}{k} = \log n - \log \log n$$

$$k = \frac{n}{\log n - \log \log n}$$

$$\frac{n}{k} \approx \log n$$

$$k \approx \frac{n}{\log n}$$

---

Take  $m \gg \frac{n-1}{k} \cdot 2^k \approx 2^{O(n/\log n)}$

Then we get  $\frac{n}{\log n}$  original  
examples summing up to have  
first  $n-1$  bits 0.

---

So we express  $e_n$  as a sum of

$\frac{n}{\log n}$  vectors in time

$$\text{poly}\left(2^k \cdot \frac{n}{k}\right) = 2^{O(n/\log n)}$$