

# PUBLIC COMPLEXITY AS A COMPUTATIONAL LENS

RT

## LECTURE 23

Recap: We are prioritizing size-space trade-offs for cutting planes

We have seen:

- Short, space efficient representation of CNF formula  $F$  yields round-efficient protocol for  $\text{Search}(F)$  with small total communication
- Can define lifted CNF formulas  $\text{lift}_\ell(F)$  such that protocol for  $\text{Search}(\text{lift}_\ell(F))$  can also solve LIFTED SEARCH PROBLEM  $\text{lift}_\ell(\text{Search}(F))$

(TOTAL) SEARCH PROBLEM  $S \subseteq \mathbb{Z} \times Q$

Given  $z \in \mathbb{Z}$ , find  $q \in Q$  such that  $(z, q) \in S$   
Fix  $\mathbb{Z} = \{0, 1\}^m$

LIFTED SEARCH PROBLEM  $\text{lift}_\ell(S)$  for Alice & Bob

- Alice gets  $x \in \{0, 1\}^m$
- Bob gets  $y \in \{0, 1\}^{l \cdot m}$
- Find  $q$  such that  $(\text{Ind}(x, y), q) \in S$

$$\text{Ind}(x_i, y_i) = y_{i, x_i}$$

$$\text{Ind}(x, y) = (\text{Ind}(x_1, y_1), \dots, \text{Ind}(x_m, y_m))$$

- Have seen (claim that) there are pebbling formulas that cannot be solved by shallow parallel decision trees with small total # queries

Missing piece (to be added today)

R II

Round-efficient communication protocol  
with small total communication for lift(S)  
⇒ Shallow parallel decision tree with  
small total # queries for S

This SIMULATION THEOREM is needed for  
REAL COMMUNICATION to obtain trade-offs  
for general cutting planes

We do it for standard deterministic  
communication (which is enough to get  
trade-off results for resolution,  
polynomial calculus, and cutting planes  
with polynomially bounded coefficients).

### Proof idea

Simulate two-party communication protocol  
to extract decision tree

Problem: We don't know Alice's & Bob's inputs  
Try to send maximally uninformative messages  
back and forth. Keep track of subsets of  
possible inputs A & B consistent with communication  
so far. When protocol has leaked too  
much information about a coordinate  $i$ , let  
decision tree query  $i$ . Update A & B based on  
query result. Bound # parallel queries in terms  
of communication rounds and bits

$I \subseteq [m]$  set of non-queried indices

$S_I$  notational aid to specify that vectors  $\vec{s} \in S$  have coordinates in  $I$

$\pi_I(S)$  projects vectors in  $S$  to coordinates in  $I$  (and shrinks dimension)

$\text{Graph}_i(A_I) \quad i \in I$

- Left vertices  $[l]$

- Right vertices  $[l]^{I \setminus \{i\}}$

- Edge  $(x_{\ell, i}, x_{I \setminus \{i\}})$  if  $x_{I \setminus \{i\}} \cdot x_i \in A_I$

"index-aware concatenation"

$\text{AvgDeg}_i(A_I)$  = average non-zero right degree

$\text{MinDeg}_i(A_I)$  = minimum non-zero right degree

Average degree high enough if  $\geq l^2$  for  $l \approx 1 - \epsilon$   
(to be specified later)

To restrict inputs in  $A$  or  $B$  on coordinate  $i$

to  $U \subseteq [l]$  or  $V \subseteq \{0, 1\}^l$ , respectively, denote

$s_{i, U}(A) = \{x \in A \mid x_i \in U\}$

$s_{i, V}(B) = \{y \in B \mid y_i \in V\}$

The set of bitstrings that have bit  $b$  in all coordinates in  $U$  is denoted

$V^b(U) = \{w \in \{0, 1\}^l \mid \forall j \in U \quad w_j = b\}$

The restriction of inputs in  $B$  on coordinate  $i$  to songs that only have bit  $b$  in indices specified by  $U$  is denoted

$X_{i, U}^b(B) = s_{i, V^b(U)}(B)$

EXAMPLE

EVAL 1/2

$$I = [4]$$

# Boolean variables in z

$$l = 5$$

lift length

$$u = \{1, 4, 5\}$$

For

$$A_I = \{(1, 1, 1, 1), (2, 3, 4, 5), (3, 2, 1, 3), (4, 4, 4, 4), (1, 2, 3, 4), (2, 5, 5, 2), (3, 4, 5, 3), (5, 4, 3, 2)\}$$

$$S_{1, u}(A_I) = \{(1, 1, 1, 1), (4, 4, 4, 4), (1, 2, 3, 4), (5, 4, 3, 2)\}$$

$$V^1(u) = \left\{ \left( \frac{1}{-}, 0, 0, \frac{1}{-}, \frac{1}{-} \right), \left( \frac{1}{-}, 0, 1, \frac{1}{-}, \frac{1}{-} \right), \left( \frac{1}{-}, 1, 0, \frac{1}{-}, \frac{1}{-} \right), \left( \frac{1}{-}, 1, 1, \frac{1}{-}, \frac{1}{-} \right) \right\}$$

For

$$B_I = \{(00000, 00000, 00000, 00000), (00001, 00011, 00111, 01111), (10011, 10111, 11000, 10000), (10101, 01010, 00000, 11111), (11111, 11110, 11100, 11000)\}$$

$$X_{1, u}^1 = \{(10011, 10111, 11000, 10000), (11111, 11110, 11100, 11000)\}$$

## eval<sub>Π</sub>(z)

Node  $v \in \Pi$  have children EVAL  $\Pi$   
 $v_0, v_1 \in \{0, 1\}$ , when 0/1 spoken

- 1  $A := [t]^m, B := \{0, 1\}^m, I := m, v := \text{root}(\Pi)$
- 2 while  $v$  not a leaf do
- 3  $Q := \emptyset, (C_I) := \Pi_I(B)$  Bob's mimmed, you sat  
while waiting for future queries
- 4 while  $v$  node where Alice speaks do
- 5 while  $\exists i \in I$  s.t.  $\text{AvgDeg}_i(\pi_I(A)) < l^2$  do
- 6  $u_i := \text{project}(A, C_I, I, i)$
- 7  $A := p_{i, u_i}(A)$   
 $C_{I \setminus \{i\}}^0 = \Pi_{I \setminus \{i\}}(x_{i, u_i}^0(C_I))$   
 $C_{I \setminus \{i\}}^1 = \Pi_{I \setminus \{i\}}(x_{i, u_i}^1(C_I))$   
 $C_{I \setminus \{i\}} := C_{I \setminus \{i\}}^0 \cap C_{I \setminus \{i\}}^1$   
 $I := I \setminus \{i\}$   
 $Q := Q \cup \{i\}$
- 8  $b := \text{argmax } |\pi_I(A \cap x^{v_b})|$  ALICE SPEAKS b
- 9  $A := \text{prune}(A \cap x^{v_b}, I)$   
 $v := v_b$
- 10 Query coordinates in  $Q$  to get string  $Z_Q \in \{0, 1\}^{|Q|}$
- 11 for  $i \in Q$  in order
- 12  $B := x_{i, u_i}^{Z_i}(B)$
- 13 while  $v$  node where Bob speaks do
- 14  $b := \text{argmax } |\pi_I(B \cap y^{v_b})|$  BOB SPEAKS b
- 15  $B := B \cap y^{v_b}$
- 16  $v := v_b$
- return answer at leaf  $v$

Recall:

EVAL III

$A_I$  is **THICK** if for all  $i \in I$

$$\text{MinDeg}_i(A_I) \geq \ell^{\mu} \quad (\text{where we set } \mu = \frac{2}{3})$$

Throughout the protocol simulation, at every  $V \in \Pi$  we will maintain that  $A \subseteq X^V$  is thick.

When Alice speaks a bit  $\delta$  and we move to  $V_\delta$

$A \cap X^{V_\delta}$  might no longer be thick

The **prime** method restores thickness and guarantees the following to be specified later

### THICKNESS LEMMA

If for all  $i \in I$   $\text{AvgDeg}_i(\pi_I(A)) \geq \ell^{\lambda}/4$ ,

then the subset  $A' \subseteq A$  returned by prime  $(A, I)$  satisfies

(T1)  $\pi_I(A')$  is thick

(T2) The density loss satisfies

$$\alpha(\pi_I(A')) \leq \alpha(\pi_I(A)) + 1$$

Recall that we defined Alice's **DENSITY LOSS**

$$\alpha(A_I) = -\log\left(\frac{|A_I|}{\ell^{|I|}}\right) = |I| \log \ell - \log |A_I|$$

We will take the Thickness lemma on faith for now, and prove it when we have used it in the main simulating lemma.  
Recall also Bob's **DENSITY LOSS**

$$\beta(B_I) = -\log\left(\frac{|B_I|}{2^{\ell^{|I|}}}\right) = |I| \ell - \log |B_I|$$

When the protocol has leaked too much

| EVAH IV

information about a coordinate in Alice's input so that we need to issue a query, the project method restricts Alice's input to a set  $\mathcal{U}$  such  $A$  is dense in the remaining coordinates also to be specified

We also want to make sure that Bob's input in this coordinate can handle query results both 0 and 1

### PROJECTION LEMMA

If  $\Pi_I(A)$  is thick

and  $\beta(C_I) \leq 2\ell^\delta \log^2 \ell$

then index set  $\mathcal{U}$  returned by

project ( $A, C_I, I, i$ ) satisfies

(P1)  $\Pi_{I \setminus \{i\}}(g_{i,u}(A))$  is thick

(P2)  $\alpha(\Pi_{I \setminus \{i\}}(g_{i,u}(\pi))) \leq \alpha(\Pi_I(A)) - \log \ell$   
+  $\log \text{AvgDeg}_i(\Pi_I(A))$

(P3) For  $b \in \{0, 1\}$  let

$$C_{I \setminus \{i\}}^b := \Pi_{I \setminus \{i\}}(x_{i,u}^b(C_I))$$

Then

$$\beta(C_{I \setminus \{i\}}^0 \cap C_{I \setminus \{i\}}^1) \leq \beta(C_I) + 1$$

We take this lemma, too, on faith for now  
Note that if  $b = \arg \max \Pi_I(A \cap X^{v_b})$ , then

$$\alpha(\Pi_I(A \cap X^{v_b})) \leq \alpha(\Pi_I(A)) + 1$$

SIMULATION LEMMA

If deterministic communication protocol  $\Pi$  solves  $\text{Liffo}(S)$  for  $\ell = m^{3+\epsilon}$ ,  $\epsilon > 0$ , using  $\leq r$  rounds and total communication

$c \leq \frac{m}{2} (1-\lambda) \log \ell$ , then eval $_{\Pi}(z)$  encodes a parallel decision tree that has depth  $\leq r$  and total query complexity  $\leq \frac{2c}{(1-\lambda) \log \ell}$

Remark: If  $c$  is larger, then  $c > m$ , and a parallel decision tree of depth 1 that guesses all variables is sufficient to "simulate" the communication protocol

Notation:

$v$  node in communication protocol  $\Pi$

$x^v$  Alice's inputs consistent with communication up to  $v$

$y^v$  Bob's inputs — || —

$R^v := x^v \times y^v$  (combinatorial rectangle)

Standard fact for deterministic communication:

$R^v$  is exactly all consistent inputs at  $v$

$c_v^A = \# \text{ bits sent by Alice up to node } v$

$c_v^B = \# \text{ bits sent by Bob } - || -$

$A$  is "cleaned-up" subset of possible inputs for Alice

$B$  — || —

Bob

# INVARIANTS MAINTAINED THROUGHOUT eval<sub>II</sub>(z)

(I1)  $\pi_I(A)$  is thick

(I2)  $A \times B \subseteq R^V$

(I3)  $m - |I| \leq 2c_V^A / ((1-\lambda) \log l)$   
# quenched coordinates

(I4)  $\beta(C_I) \leq m - |I| + c_V^B$

ADDITIONAL INVARIANTS AT BEGINNING OF ROUND for Alice or Bob

(I5)  $\beta(\pi_I(B)) \leq m - |I| + c_V^B$

(I6) For all  $(x, y) \in A \times B$  and all  $i \notin I$   
 $\text{Ind}(x_i, y_i) = z_i$   
(returned by query to  $\mathcal{Z}$ )

All invariants clearly true at start of algorithm.

Invariant (I1)  $A$  modified only at lines 7 & 9.

At line 7  $\pi_I(A)$  is thick by assumption.

(in lemma statement)

Also by assumption  $c_V^A + c_V^B \leq c \leq m \log l = l^\delta \log l$

(I3) & (I4) say that

$$\begin{aligned}
 \beta(C_I) &\leq m - |I| + c_V^B \\
 &\leq \frac{2c_V^A}{(1-\lambda) \log l} + c_V^B \\
 &\leq c_V^A + c_V^B \\
 &\leq l^\delta \log l
 \end{aligned}$$

Hence conditions in Projection Lemma  
satisfied (with some margin - the tech  
lemmas are stated as needed for real communication)

Hence  $\pi_I(A)$  remains thick

At line 9 we need to verify that conditions  
for Thickness Lemma hold.

Since we have exited the while loop at lines 5-7

$$\text{AvgDeg}_i(\pi_I(A)) \geq \ell^2$$

Recall that in general

$$\begin{aligned} \text{AvgDeg}_i(A_I) &= \frac{\#\text{edges in Graph}_i(A_I)}{\#\text{non-isolated right vertices in Graph}_i(A_I)} \\ &= \frac{|A_I|}{|\pi_{I \setminus \{i\}}(A_I)|} \end{aligned}$$

Hence, we have

$$\begin{aligned} \text{AvgDeg}_i(\pi_I(A \cap X^{v_6})) &= \frac{|\pi_I(A \cap X^{v_6})|}{|\pi_{I \setminus \{i\}}(A \cap X^{v_6})|} \geq \\ &\geq \frac{\frac{1}{2} |\pi_I(A)|}{|\pi_{I \setminus \{i\}}(A)|} = \\ &= \frac{1}{2} \text{AvgDeg}_i(\pi_I(A)) \geq \frac{\ell^2}{2} \end{aligned}$$

(and again there is some margin)

It follows that the Thickness Lemma guarantees thickness

## Invariant (I2)

$A$  and  $B$  never increase

The node  $v \in \Pi$  changes at lines 9 and 15

In both cases we make sure for new  $\sqrt{b}$  that  $A \subseteq X^{\sqrt{b}}$  and  $B \subseteq Y^{\sqrt{b}}$ , respectively

## Invariant (I3)

Show that

$$\alpha(\Pi_I(A)) \leq 2C_V^A - (m - |I|)(1-\lambda) \log l \quad (3)$$

and use  $\alpha(\cdot) \geq 0$  by definition

At beginning  $\alpha(\Pi_I(A)) = 0$

Want to show

- (a) Alice sends bit  $\Rightarrow$  density loss increase at most 2
- (b) Query issued  $\Rightarrow$  density loss decrease  $(1-\lambda) \log l$

$A, I, C_V^A$  only modified at lines 7 & 9

Line 7 Projection lemma says that when  $|I|$  decreases by 1, then density loss changes according to (P2) by

$$-\log l + \log \text{AvgDeg}_i(\Pi_I(A))$$

$$\leq -\log l + \log l'$$

$$\leq -(1-\lambda) \log l$$

Line 8 chooses  $b$  s.t.  $\alpha(\Pi_I(A \cap X^{\sqrt{b}})) \leq \alpha(\Pi_I(A)) + 1$

Line 9 Thickness lemma (T2) says further density loss of  $\leq +1$  from previous

This shows that (3) holds.

### Invariant (I<sup>4</sup>)

$C_I$  is updated at lines 3 & 7

At line 3, (I<sup>4</sup>) is implied by (I<sup>5</sup>).

At line 7, we have already argued that the Projection Lemma applies. Then (P3) says that

$$\beta(C_{I \setminus E_S}) \leq \beta(C_I) + 1$$

so density loss  $\leq \# \text{ coordinates queried}$

### Invariant (I<sup>5</sup>)

Holds at beginning of round. Needs to be restored at end of round

If Bob speaks,  $B$  is updated at line 15

By choice of bits spoken by Bob

$$\left| \pi_I(B \cap Y^B) \right| \text{ increases by } \leq 1$$

since

$$\left| \pi_I(B \cap Y^B) \right| \geq \frac{1}{2} \left| \pi_I(B) \right|$$

If Alice speaks  $B$  is updated at line 12

Invariant I<sup>4</sup> says that corresponding property holds for  $C_I$

Suppose  $Q = \{i_1, i_2, \dots, i_{|Q|}\}$

$$\text{Let } I_0 = Q \cup I$$

$$I_j = (Q \cup I) \setminus \{i_1, \dots, i_j\}$$

$$I_{|Q|} = I$$

EVTC X

Let update of  $B$  on line 12  
be

$$B_0 = B$$

$$B_j = \chi_{i,j,u_j}^{z_i} (B_{j-1})$$

Then by construction computed earlier  
on line 7

$$\pi_{I_j}(B_j) \supseteq C_{I_j}$$

and (I5) follows from (I4).

### Invariant 6

Recall that  $A$  &  $B$  never increase

We only need to consider when  $I$  shrinks,  
which happens at line 7

When  $i$  removed from  $I$ , Invariant 6  
is false for  $i$

At line 12 before Bob speaks

$A$  has been restricted to only contain indices  $U_i$   
for coordinate  $i$

$B$  is now restricted so that in all positions  
 $x_i \in U_i$  for  $y \in B$  it holds that  $y_{i,x_i} = z_i$

This is what  $\chi_{i,u_i}^{z_i}(B)$  ensures  
(the return)

After this  $\text{Ind}(x_i, y_i) = z_i$

for all  $(x, y) \in A \times B$

This shows that Invariants (I1)-(I6)  
hold as claimed.

When  $\text{eval}_T(z)$  reaches a leaf, there have been  $\leq r$  rounds of queries, at most once after every time Alice is finished speaking.

[ $\# \text{rounds} = \# \text{times both parties get to speak}$ ]

By Invariant I3, total # queries

$$m - |I| \leq 2 c^A / ((1-\lambda) \log t) \\ \leq 2 c / ((1-\lambda) \log t)$$

We also need to prove that for any  $z \in \{0,1\}^m$  the answer from the decision tree is  $\text{eval}_T(z) = g$  such that  $(z, g) \in S$

Argue this by showing that  $\exists (x,y) \in A \times B$  such that  $\text{Ind}(x,y) = z$ .

Since protocol  $T$  computes  $g$  such that  $(\text{Ind}(x,y), g) \in S$

this means that decision tree gives correct answer

The proof is essentially a special case of the Projection Lemma, so we skip it in the interest of time. 

Now we need to provide details on prune and project