PROOF COMPLEXITY AS A COMPUTATIONAL LENS

RI

LECTURE 23

Recap: We are proving $\boxed{\text{size-space trade-offs}}$ for cutting planes

We have seen:

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

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

Given $z \in Z$, find $q \in Q$ such that $(z, q) \in S$

Fix $Z = \{0,1\}^m$

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

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

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

$$Ind(x,y) = (Ind(x_1,y_1), \ldots, Ind(x_m,y_m))$$

- 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)

Round-efficient communication protocol with small total communication for $lift_\ell(S)$
$\Rightarrow$ 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

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

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

$\boxed{\mathrm{Graph}_i(A_I)}$ $i \in I$
- Left vertices $[\ell]$
- Right vertices $[\ell]^{I \setminus \{i\}}$
- Edge $(x_{\{i\}}, x_{I \setminus \{i\}})$ if $x_{I \setminus \{i\}} \cdot x_i \in A_I$

"index-aware concatenation"

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

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

Average degree high enough if $\boxed{\geq \ell^{\lambda}}$ for $\lambda \approx 1-\varepsilon$ (to be specified later)

To restrict inputs in A or B on coordinate i to $U \subseteq [\ell]$ or $V \subseteq \{0,1\}^{\ell}$, respectively, denote

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

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

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

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

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

$$\boxed{\chi^b_{i,U}(B)} = \rho_{i,V^b(U)}(B)$$

EXAMPLE

$$I = [4] \quad \text{\# Boolean variables in } x$$
$$\ell = 5 \quad \text{lift length}$$
$$U = \{1, 4, 5\}$$

For

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

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

$$V^1(U) = \{ (\underline{1},0,0,\underline{1},\underline{1}), (\underline{1},0,1,\underline{1},\underline{1}), (\underline{1},1,0,\underline{1},\underline{1}), (\underline{1},1,1,\underline{1},\underline{1}) \}$$

For

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

$$x^1_{1,U} = \{ (\underline{1}00\underline{1}\underline{1}, 10111, 11000, 10000), (\underline{1}11\underline{1}\underline{1}, 11110, 11100, 11000) \}$$

$\boxed{\mathrm{eval}_{\Pi}(z)}$

Node $v \in \Pi$ have children v_b, $b \in \{0,1\}$, when bit b spoken

1 $A := [\ell]^m$, $B := \{0,1\}^{\ell m}$, $I := m$, $v := \mathrm{root}(\Pi)$

2 while $\boxed{v \text{ not a leaf}}$ do

3 $\quad Q := \emptyset$, $C_I := \pi_I(B)$

Bob's trimmed input set while waiting for future queries

4 $\quad$ while $\boxed{v \text{ node where Alice speaks}}$ do

5 $\quad\quad$ while $\boxed{\exists i \in I \text{ s.t. } \mathrm{AvgDeg}_i(\pi_I(A)) < \ell^{\lambda}}$ do

6 $\quad\quad\quad u_i := \mathrm{project}(A, C_I, I, i)$

7 $\quad\quad\quad A := \rho_{i,u_i}(A)$

$\quad\quad\quad C^0_{I\setminus\{i\}} := \pi_{I\setminus\{i\}}(\chi^0_{i,u_i}(C_I))$

$\quad\quad\quad C^1_{I\setminus\{i\}} := \pi_{I\setminus\{i\}}(\chi^1_{i,u_i}(C_I))$

$\quad\quad\quad C_{I\setminus\{i\}} := C^0_{I\setminus\{i\}} \cap C^1_{I\setminus\{i\}}$

$\quad\quad\quad I := I \setminus \{i\}$

$\quad\quad\quad Q := Q \cup \{i\}$

8 $\quad\quad b := \mathrm{argmax}\, |\pi_I(A \cap X^{v_b})|$

ALICE SPEAKS b

9 $\quad\quad A := \mathrm{prune}(A \cap X^{v_b}, I)$

$\quad\quad v := v_b$

10 $\quad\boxed{\text{Query coordinates in } Q \text{ to get string } z_Q \in \{0,1\}^{|Q|}}$

11 $\quad$ for $i \in Q$ in order

12 $\quad\quad B := \chi^{z_i}_{i,u_i}(B)$

13 $\quad$ while $\boxed{v \text{ node where Bob speaks}}$ do

14 $\quad\quad b := \mathrm{argmax}\, |\pi_I(B \cap Y^{v_b})|$

BOB SPEAKS b

15 $\quad\quad B := B \cap Y^{v_b}$

$\quad\quad v := v_b$

16 $\boxed{\text{return answer at leaf } v}$

Recall:

A_I is $\boxed{\text{THICK}}$ if for all $i \in I$

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

Throughout the protocol simulation, at every $v \in \Pi$ we will maintain that

$\boxed{A \subseteq \mathcal{X}^v \text{ is thick}}$

When Alice speaks a bit b and we move to v_b

$A \cap \mathcal{X}^{v_b}$ might no longer be thick

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

THICKNESS LEMMA

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

then the subset $A' \subseteq A$ returned by prune (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 $\boxed{\text{DENSITY LOSS}}$

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

We will take the Thickness Lemma on faith for now, and prove it when we have used it in the main simulation lemma

Recall also Bob's DENSITY LOSS

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

EVAL IV

When the protocol has leaked to much information about a coordinate i in Alice's input so that we need to issue a query, the project method restricts Alice's input to a set 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

LIFT LENGTH
$$\ell = m^{3+\varepsilon}$$
$$\gamma := \frac{1}{3+\varepsilon}$$
$$\ell^{\gamma} = (m^{3+\varepsilon})^{\gamma} = m$$

PROJECTION LEMMA

If $\boxed{\pi_I(A) \text{ is thick}}$

and $\boxed{\beta(C_I) \leq 2\,\ell^{\gamma}\log^2 \ell}$

then index set U returned by project(A, C_I, I, i) satisfies

(P1) $\pi_{I\setminus\{i\}}(\rho_{i,U}(A))$ is thick

(P2) $\alpha(\pi_{I\setminus\{i\}}(\rho_{i,U}(A)) \leq \alpha(\pi_I(A)) - \log \ell + \log \mathrm{AvgDeg}_i(\pi_I(A))$

(P3) For $b \in \{0,1\}$ let
$$\boxed{C^b_{I\setminus\{i\}}} := \pi_{I\setminus\{i\}}(\chi^b_{i,U}(C_I))$$
Then
$$\beta(C^0_{I\setminus\{i\}} \cap C^1_{I\setminus\{i\}}) \leq \beta(C_I) + 1$$

We take this lemma, too, on faith for now

Note that if $b = \arg\max\ \pi_I(A \cap X^{v_b})$, then
$$\boxed{\alpha(\pi_I(A \cap X^{v_b})) \leq \alpha(\pi_I(A)) + 1}$$

SIMULATION LEMMA

If deterministic communication protocol Π solves $Lift_\ell(S)$ for $\ell = m^{3+\varepsilon}$, $\varepsilon > 0$, using $\leq r$ rounds and total communication $\boxed{c < \frac{m}{2}(1-\lambda)\log \ell}$, 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 queries all variables is sufficient to "simulate" the communication protocol

Notation:

$\boxed{v}$ node in communication protocol Π

$\boxed{X^v}$ Alice's inputs consistent with communication up to v

$\boxed{Y^v}$ Bob's inputs — " —

$\boxed{R^v} := X^v \times Y^v$ (combinatorial rectangle)

Standard fact for deterministic communication:

R^v is exactly all consistent inputs at v

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

$\boxed{c_v^B}$ = # bits sent by Bob — " —

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

B — " — Bob

INVARIANTS MAINTAINED THROUGHOUT $eval_{\pi}(z)$

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

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

(I3) $\underbrace{m - |I|}_{\#\text{ queried coordinates}} \leq 2c_v^A / ((1-\lambda)\log \ell)$

(I4) $\beta(C_I) \leq \overbrace{m - |I|} + c_v^B$

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 $i \notin I$

$Ind(x_i, y_i) = z_i$ (returned by query to z)

Communication protocol has committed to z_i for all queried coordinates i

All invariants clearly true at start of algorithm.

$\boxed{\text{Invariant (I1)}}$ A modified only at lines 7 & 9.

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

Also by assumption (in lemma statement) $c_v^A + c_v^B \leq c \leq m \log \ell = \ell^\delta \log \ell$

(I3) & (I4) say that

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

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
$\mathrm{AvgDeg}_i(\pi_I(A)) \geq \ell^\lambda$

Recall that in general

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

Hence, we have

$$\mathrm{AvgDeg}_i(\pi_I(A \cap X^{v_t})) = \frac{|\pi_I(A \cap X^{v_t})|}{|\pi_{I\setminus\{i\}}(A \cap X^{v_t})|} \geq$$

$$\geq \frac{\frac{1}{2}\,\pi_I(A)|}{|\pi_{I\setminus\{i\}}(A)|} =$$

$$= \frac{1}{2}\,\mathrm{AvgDeg}_i(\pi_I(A)) \geq \frac{\ell^\lambda}{2}$$

(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 v_b
that $A \subseteq X^{v_b}$ and $B \subseteq Y^{v_b}$, respectively

Invariant (I3)

Show that

$$\alpha(\Pi_I(A)) \leq 2\, c_v^A - (m - |I|)(1-\lambda)\log \ell \quad (3)$$

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 $(1-\lambda)\log \ell$

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

$$-\log \ell + \log \mathrm{AvgDeg}_i(\Pi_I(A))$$

$$\leq -\log \ell + \log \ell^{\lambda}$$

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

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

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

This shows that (3) holds.

Invariant (I4)

C_I is updated at lines 3 & 7

At line 3, (I4) is implied by (I5).

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

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

so density loss $\leq$ # coordinates queried

Invariant (I5)

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

<u>If Bob speaks</u>, B is updated at line 15

By choice of bits b spoken by Bob

$$\beta\left(\Pi_I\left(B \cap Y^{v_b}\right)\right) \text{ increases by } \leq 1$$

since

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

<u>If Alice speaks</u> B is updated at line 12

Invariant I4 says that corresponding property holds for C_I

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

Let
$$I_0 = Q \cup I$$
$$I_j = (Q \cup I) \setminus \{i_1, \ldots, i_j\}$$
$$I_{|Q|} = I$$

Let updates of B on line 12 be

$$B_0 = B$$
$$B_j = \chi^{z_{i_j}}_{i_j, u_{i_j}}(B_{j-1})$$

Then by construction

$$\Pi_{I_j}(B_j) \supseteq C_{I_j}$$ computed earlier on line 7

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 (the restriction) $\chi^{z_i}_{i,u_i}(B)$ ensures

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

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

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

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

[# rounds = # times both parties get to speak]

By Invariant I3, total # queries

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

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

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

Since protocol Π computes q such that $(\mathrm{Ind}(x,y), q) \in S$ 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. $\blacksquare$

Now we need to provide details on prune and project

$\boxed{\text{prune}(A, I)}$

$A_I := \pi_I(A)$

while $\boxed{\exists i \text{ such that } \mathrm{MinDeg}_i(A_I) < \ell^{\mu}}$ do

$x_{I \setminus \{i\}} :=$ right vertex in $\mathrm{Graph}_i(A_I)$ of degree $< \ell^{\mu}$

$A_I := \{ x_I \in A_I \mid \pi_{I \setminus \{i\}}(x_I) \neq x_{I \setminus \{i\}} \}$

return $\{ x \in A \mid \pi_I(x) \in A_I \}$

---

prune returns a set A' s.t. $\pi_I(A')$ is thick by definition.

We need to show $\alpha(\pi_I(A')) \leq \alpha(\pi_I(A)) + 1$

Equivalent to

$$\boxed{|\pi_I(A')| \geq |\pi_I(A)|/2}$$

TIME TO INTRODUCE MAGIC NUMBERS

Recall
$$\boxed{\begin{aligned} \ell &= m^{3+\varepsilon} \\ \gamma &:= \frac{1}{3+\varepsilon} \end{aligned}}$$

Choose $\delta, \lambda, \mu \in (0,1)$ such that

$$\boxed{\begin{aligned} \lambda - \gamma &> \mu &\quad (a) \\ \mu + \delta - 1 &> \gamma &\quad (b) \\ \gamma + \delta &< 1 &\quad (c) \end{aligned}}$$

Fix $\xi > 0$ such that $\gamma = \frac{1}{3} - 2\xi$

Can set

$$\lambda = 1 - \xi$$
$$\mu = 2/3$$
$$\delta = 2/3$$

By definition, # right vertices of positive degree

$$\boxed{\frac{|\pi_I(A)|}{\mathrm{AvgDeg}_i(\pi_I(A))}}$$

Write $A'_I = \pi_I(A')$ for brevity

$\mathrm{Graph}_i(A'_I)$ is subgraph of $\mathrm{Graph}_i(\pi_I(A))$, so at most that many right vertices of positive degree there as well.

Upper-bounds # iterations for coordinate i, since every iteration removes non-isolated right vertex

iterations per coordinate

$$\leq \frac{|\pi_I(A)|}{\mathrm{AvgDeg}_i(\pi_I(A))} \leq \boxed{\frac{|\pi_I(A)|}{\ell^\lambda/2}}$$

[since while loop at 5 exited]

Summed over all coordinates # iterations

$$\leq 2\,|I|\,\frac{|\pi_I(A)|}{\ell^\lambda} \leq \boxed{2\,\ell^{\gamma-\lambda}\,|\pi_I(A)|}$$

$\boxed{|I| \leq m = \ell^\gamma}$

Each iteration removes $< \ell^\mu$ elements from A'_I

Total # removal

$$\leq \boxed{2\,\ell^{\gamma+\mu-\lambda}}\,|\pi_I(A)| \leq (*)$$

By (a) we have $\gamma+\mu-\lambda < 0$, so for m $(=\ell^\gamma)$ large enough we get

$$(*) \leq |\pi_I(A)|/2$$

which proves the Thickness Lemma $\square$

$\boxed{\text{project}(A, C_I, I, i)}$

pick $\mathcal{U} \subseteq [\ell]$ such that $|\mathcal{U}| = \ell^{\delta}$ uniformly at random

$C^0 := \pi_{I \setminus \{i\}}(\chi^0_{i,\mathcal{U}}(C_I))$

$C^1 := \pi_{I \setminus \{i\}}(\chi^1_{i,\mathcal{U}}(C_I))$

$C^* := C^0 \cap C^1$

if $\left(\boxed{\beta(C^*) \leq \beta(C_I) + 1} \right.$

and $\left(\boxed{\pi_{I \setminus \{i\}}(\rho_{i,\mathcal{U}}(A)) = \pi_{I \setminus \{i\}}(A)} \right) \Big)$

return $\mathcal{U}$

else

return project(A, C_I, I, i)

To prove the Projection Lemma, we just pick $\mathcal{U} \subseteq [\ell]$ of size ℓ^{δ} and argue that a.a.s. this $\mathcal{U}$ satisfies (P1) – (P3)

This boils down to two claims

CLAIM A

If $\pi_I(A)$ is thick, then

$$\boxed{\pi_{I \setminus \{i\}}(\rho_{i,\mathcal{U}}(A)) = \pi_{I \setminus \{i\}}(A)}$$

with probability $1 - o(1)$ over randomly sampled $\mathcal{U} \subseteq [\ell]$, $|\mathcal{U}| = \ell^{\delta}$

CLAIM B

For $b \in \{0,1\}$ let $C^b := \Pi_{I \setminus \{i\}}(\mathcal{X}^b_{i,u}(C_I))$
and let $C^* := C^0 \cap C^1$

If $\beta(C_I) \leq 2\ell^\delta \log \ell$, then

$$\boxed{\beta(C^*) \leq \beta(C_I) + 1}$$

with probability $1 - o(1)$ over random $U \subseteq [\ell]$, $|U| = \ell^\delta$

If we accept these claims, then we can prove the Projection Lemma:

By the union bound, there is a set U satisfying both $\underbrace{\text{Claim A and}}_{\text{conditions in}}$ Claim B

Fix such an U.

Claim B yields property (P3)

Recall that min degree and thickness can only increase under projection

$$\boxed{\forall j \in I \setminus \{i\} \quad MinDeg_j(\Pi_{I \setminus \{i\}}(A)) \geq MinDeg_j(\Pi_I(A))}$$

$\Pi_I(A)$ is thick by assumption.

Hence $\Pi_{I \setminus \{i\}}(A)$ is also thick

And if $\Pi_{I \setminus \{i\}}(\rho_{i,u}(A)) = \Pi_{I \setminus \{i\}}(A)$ as in Claim A

then property (P1) follows.

By plugging in the definitions, we verified last lecture that

$$\boxed{\alpha(\pi_{I\setminus\{i\}}(A)) = \alpha(\pi_I(A)) - \log \ell + \log \mathrm{AvgDeg}_i(\pi_I(A))}$$

The equality

$$\underline{\pi_{I\setminus\{i\}}(\rho_{i,\mathcal{U}}(A))} = \pi_{I\setminus\{i\}}(A)$$

Proof of Projection Lemma

now yields property (P2) $\blacksquare$

Claim B is technically complicated, and we are running out of time and energy. Let us take it on faith (a big ask!) and instead do Claim A.

<u>Proof of Claim A</u>

Equality

$$\boxed{\pi_{I\setminus\{i\}}(\rho_{i,\mathcal{U}}(A)) = \pi_{I\setminus\{i\}}(A)}$$

holds if <u>every right vertex</u> of $\mathrm{Graph}_i(\pi_I(A))$ of positive degree has an <u>edge into $\mathcal{U}$</u>

$\mathrm{MinDeg}_i(\pi_I(A)) \geq \ell^{\mu}$ by thickness

$|\mathcal{U}| = \ell^{\delta}$

For fixed right vertex $R = x_{I\setminus\{i\}}$

$$\Pr_{\mathcal{U}}\left[R \text{ has no neighbours in } \mathcal{U}\right] \leq$$

$$\leq \boxed{\frac{\binom{\ell - |N_i(R)|}{\ell^{\delta}}}{\binom{\ell}{\ell^{\delta}}}} \leq$$

If $n \le m$ then

$$\binom{n}{k} \Big/ \binom{m}{k} \le \left(\frac{n}{m}\right)^k$$

$$\le \binom{\ell - \ell^{\mu}}{\ell^{\delta}} \Big/ \binom{\ell}{\ell^{\delta}}$$

$$\le \left(\frac{\ell - \ell^{\mu}}{\ell}\right)^{\ell^{\delta}} = \left(1 - \ell^{\mu - 1}\right)^{\ell^{\delta}}$$

$$\le \exp\left(-\ell^{\mu+\delta-1}\right)$$

Taking a union bound over all right vertices, the probability that some vertex fails to have a neighbour in U is at most

$$\ell^{|I|-1} \cdot \exp\left(-\ell^{\mu+\delta-1}\right) <$$

$$< \exp\left(|I| \log \ell - \ell^{\mu+\delta-1}\right)$$

$$\le \exp\left(\ell^{\delta} \log \ell - \ell^{\mu+\delta-1}\right)$$

$$= o(1)$$

$$\boxed{\mu + \delta - 1 > \gamma \quad (6)}$$

and Claim A follows ∎