LECTURE 9

→ Feasible Interpolation, part 2.

FEASIBLE INTERPOLATION (abbr. FI)

- A METHOD HOW TO PROVE LOWER BOUNDS ON PROOF-SIZE
  - DOES NOT APPLY TO AC^0-F OR STRONGER BUT IT DOES APPLY TO THE WIDEST CLASS OF PROOF SYSTEMS - LOGICAL, ALGEBRAIC, GEOMETRIC, AD HOC ... - OF ALL METHODS

GENERAL SCHEME

- TRANSFORMS A PROOF INTO A COMPUTATIONAL DEVICE (USUALLY A CIRCUIT) SOLVING A SPECIFIC TASK
  - THEN USES LOWER BOUNDS FOR THAT DEVICE

LOGIC BACKGROUND : CRAIG'S INTERPOLATION THM.

ASSUME $\alpha(\bar{p},\bar{q}) \rightarrow \beta(\bar{p},\bar{r}) \in TAUT$,

WITH $\bar{p},\bar{q},\bar{r}$ DISJOINT TUPLES OF ATOMS

THEN $\exists$ FLA $\gamma(\bar{p})$ S.T.

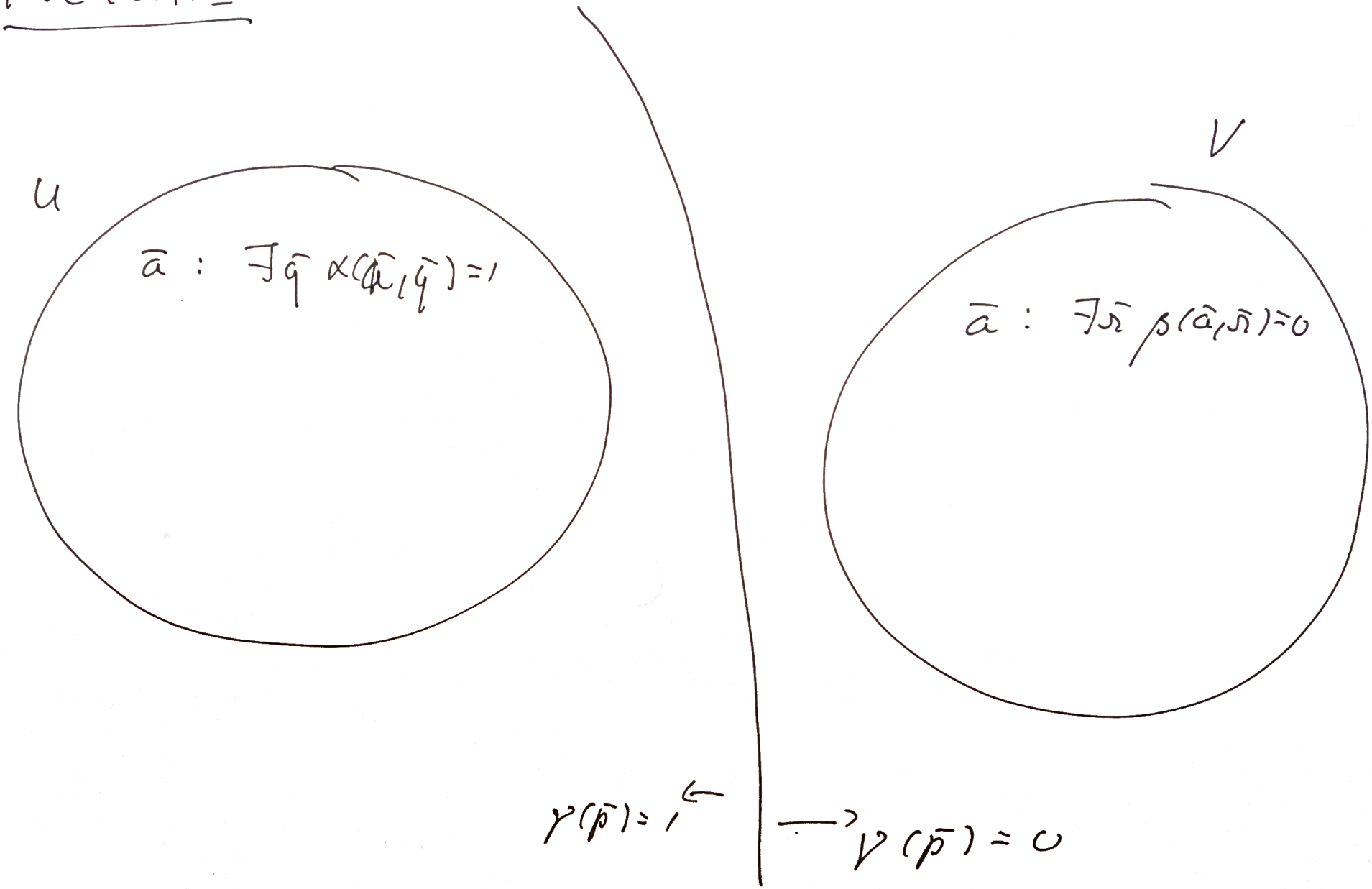
$$\alpha \rightarrow \gamma \quad \text{and} \quad \gamma \rightarrow \beta \quad \in TAUT$$

interpolant

REMARK:

THERE IS ALSO A FO-LOGIC VERSION.

PICTURE:



γ SEPARATES U FROM V

PROOF: DEFINE BOOL. FUNCTION $f : \{0,1\}^n \to \{0,1\}$ $(\bar{p} = p_1, \ldots, p_n)$

$$f(\bar{a}) = 1 \iff \bar{a} \in U \left(\iff \exists \bar{q}\ \alpha(\bar{a}\bar{q}) = 1 \iff \alpha(\bar{a}\bar{q}) \in SAT \right)$$

THEN TAKE A DNF FLA $\gamma(\bar{p})$ DEFINING

f :

$$\gamma(\bar{p}) = 1 \iff f(\bar{p}) = 1$$

[L 1.1.2] □

NOTE : γ HAS $|U|$ - many DISJUNCTS

SO MAY BE EXP - LARGE.

MODIFIED SET-UP : in $\alpha \to \beta$ VERSION β appears NEGATIVELY in THE DEF. of V, WHILE α is + in THE DEF. of U.

MORE "SYMMETRIC" SET-UP :

CLAUSES $A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q})$

CLAUSES $B_1(\bar{p},\bar{r}), \ldots, B_\ell(\bar{p},\bar{r})$

S.T. $\bar{a} \in U \iff \bigwedge_i A_i(\bar{a},\bar{q}) \in SAT$

$\bar{a} \in V \iff \bigwedge_j B_j(\bar{a},\bar{r}) \in SAT$

AND : $U \cap V = \emptyset \iff \langle A_1, \ldots, A_m, B_1, \ldots, B_\ell \rangle \in UNSAT.$

WHERE DO WE GET EXAMPLES?

$\hookrightarrow U, V \in NP$, $U \cap V = \emptyset$ [DISJOINT NP-PAIR]

BY THE NP-COMPL. OF CNF-SAT: $\forall n \geq 1$

- $\exists$ clauses $A_1(\bar{p}, \bar{q}), \ldots, A_m(\bar{p}, \bar{q})$,
  - $\bar{p} = (p_1, \ldots, p_r)$, $\bar{q} = (q_1, \ldots, q_s)$
  - $m, s \leq n^{O(1)}$
  - $\bar{a} \in U_n := U_n \cap \{0,1\}^* \iff \bigwedge_i A_i(\bar{a}, \bar{q}) \in SAT$

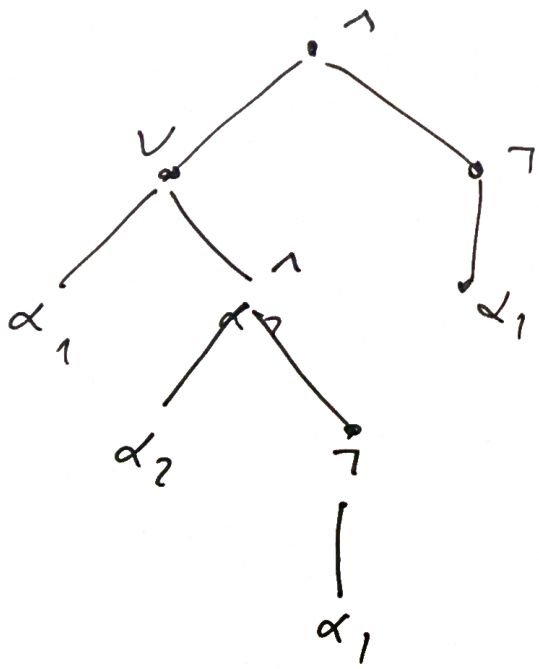
- ANALOGOUS: $B_1(\bar{r}, \bar{s}), \ldots, B_\ell(\bar{r}, \bar{s})$ FOR V
  $\bar{s} = (s_1, \ldots, s_t)$
  $\ell, t \leq n^{O(1)}$

SUMMARY : FI-SET-UP

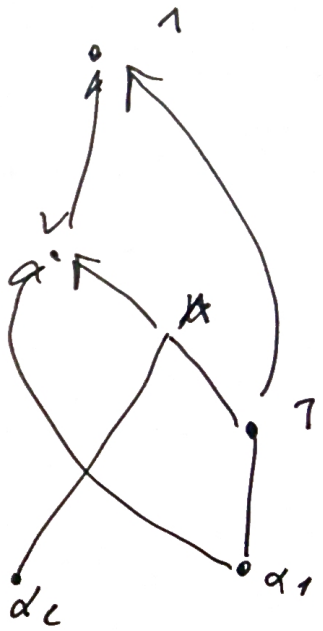
- $U \cap V = \emptyset$, U_n , V_n for $n \geq 1$
- $k, s, c \in \ldots, m, \ell \leq n^{O(1)}$
- $A_1(\bar{p}, \bar{q}), \ldots, A_m(\bar{p}, \bar{q})$ ---- U
- $B_1(\bar{p}, \bar{r}), \ldots, B_\ell(\bar{p}, \bar{r})$ ---- V
- THINK OF REFUTATIONS OF $A_1, \ldots, B_\ell$
- INTERPOLANT $I(\bar{p})$: $\bar{p} \in U \rightarrow I(\bar{p}) := 1$

  $\bar{p} \in V \rightarrow I(\bar{p}) = 0$

FCAS vs. CIRCUITS [Secs. 1.1. + 1.4]



TREE



DAG (= DIRECTED ACYCLIC GRAPH

[SUBFCAS MAY BE RE-USED]

CIRCUITS (= STRAIGHT LINE PROGRAMS)

- INPUTS: $x_1, \ldots, x_n$
- INSTRUCTIONS: $y_1, \ldots, y_t$

$y_i := \rightarrow$ ONE OF $x_1, \ldots, x_n$

$\neg y_{j_1}$, $j_1 < i$

$y_{j_1} \wedge y_{j_2}$, $j_1, j_2 < i$

$y_{j_1} \vee y_{j_2}$, $j_1, j_2 < i$

CAF:

$DEF_C(\bar{x}, \bar{s})$: THE SET OF CLAUSES DEFINING

[i.e. $\bar{s}$ is a valid comp. $\Leftrightarrow Def_C(\bar{a}, \bar{s}) = 1$]

on $\bar{a}$

OBSERVATION: ANY INTERPOLANT $I(\bar{p})$ OF

$$\underbrace{Def_C(\bar{p},\bar{q}), q_k}_{A's} \quad , \quad \underbrace{Def_C(\bar{p},\bar{r}), r_k}_{B's}$$

COMPUTES THE VALUE $C(\bar{b})$.

PRF: $\bar{a} \in U \Rightarrow \exists$ comp. $\bar{s}$ of C on $\bar{a}$ ending

with $s_k = C(\bar{a}) = 1$

$$\Downarrow$$

$$I(\bar{a}) = 1$$

$\bar{a} \in V \Rightarrow \exists$ comp. $\bar{c}$ of C on $\bar{a}$ ending with $c_k := C(\bar{a}) = 0$

$$\Downarrow$$

$$I(\bar{a}) = 0 .$$

□

HENCE UNLESS

{ ANY CIRCUIT $C(\vec{p})$ CAN BE EQUIVALENTLY DEFINED BY FLA $\gamma(\vec{p})$, $|\gamma| \leq |C|^{O(1)}$, } UNLIKELY $NC = ?$ P/poly

NO INTERPOL. – FLA CAN BE BOUNDED BY poly IN THE SIZE OF THE INSTANCE.

⇓

RORAL: AID AT EXTRACTING INTERPOLANT AS CIRCUITS.

$$\sum_i |A_i| + \sum_j |B_j| \leq n^{O(1)}$$

OBSERVATION (D. RUNDICI)

UNLESS $NP \cap coNP \subseteq P/poly$ i.e. $\Rightarrow$ P-size circuits

~~DAG~~ INTERPOLATING CIRCUITS CANNOT BE IN GENERAL BOUNDED IN SIZE BY A POLY OF INSTANCE SIZE (i.e. poly(n)).

PRF: U_n ... A-clauses , when $U \in NP \cap coNP$ AND
V_n ... B-clauses $V := \{0,1\}^* - U$

$\Downarrow$

$I(\bar{p})$ COMPUTES $\bar{p} \in_? U_n$.

□

FI IDEA : DO NOT ESTIMATE $|I(\vec{p})|$

circuit size

IN TERMS OF n (i.e. the instance-size)

BUT IN TERMS OF $|\pi|$, WHERE

π IS A REFUTATION OF $\{A_1, \ldots, B_e\}$

REMARK: CLAUSES IN THE OBSERV. OR SLICE IS

HAVE SHORT REFUTATIONS IN R,

SO WE STILL AIM AT INTERPOLATING

CIRCUIT.

UNFORTUNATELY: NO NON-TRIVIAL CIRCUIT SIZE LOWER BOUNDS ARE KNOWN

$\Downarrow$

HENCE WE COULD, AT BEST, AID AT CONDITIONAL RESULT.

FORTUNATELY: STRONG LOWER BOUNDS ARE KNOWN FOR MONOTONE CIRCUIT

SO WE NEED "MONO-INTERPOLATION"

Thm (Lyndon - Thm 1.1.3)

ASSUME THE FI-SET-UP AND ASSUME THAT:

(*) { IN ALL p_i APPEAR IN ALL $A_1, \dots, A_n$ POSITIVELY (NO NEGATION)

THEN $I(\bar{p})$ CAN BE DEFINED BY 1-FREE (=ROOT) FORMULA (AND CIRCUIT)

- SAME PROOF — SEE Sec. 1.1
- (*) $\Rightarrow$ U closed upwards: $\left.\begin{matrix} \bar{a} \in U \\ \bar{a} \le \bar{b} \end{matrix}\right\} \Rightarrow \bar{b} \in U$
- ALTER-COND. TO (*): ALL p_i OCCUR ONLY NEGATIVELY IN ALL B_j

monotone FIXED-UP

↓

THE FIXED-UP

+ CONDITION (*)

⇕

U closed upwards.

WANT : EXTRACT MONOTONE INTERPOLATING CIRCUITS

DEF.

A pps P ADMITS FI iff $\exists f : \{0,1\}^* \to \{0,1\}^*$

S-T. :

if $M, L, A_1, \ldots, B_\ell$ OBEY THE FI SET-UP

AND π is a P-REFUT. OF $A_1, \ldots, B_\ell$

THEN:

(i) $f(\pi)$ is AN INTERPOLATING CIRCUIT

(ii) f has poly-growth : $|f(w)| \leq |w|^{O(1)}$

P ADMITS NONU FI ---- NONU FI SET-UP

//

$f(\pi)$ is A NONU CIRCUIT

OFTEN f (= MFI CONSTRUCTIONS) SATISFIES MORE:

(a) π is TREE-LIKE $\Rightarrow$ $f(\pi)$ is A FLA

(b) f is p-time computable

(c) f also produces P-proofs of "both implications $\alpha \to \gamma, \gamma \to \beta$", i.e. P-refs of $A_1, \ldots, A_m, I(\bar{p})=0$ and $B_1, \ldots, B_\ell, I(\bar{p})=1$

(d) $|f(\pi)| \le O(|\pi|)$ [LIN. SIZE]

LEMMA 17.12

ASSUME U, V IS A DISJOINT NP-PAIR, $A_1, \ldots, B_2$ OBEY THE FI SET-UP. LET P admits FI.

(1) IF EVERY CIRCUIT SEPARATING U_n from V_n MUST HAVE SIZE $\geq s(n)$ THEN ANY P-REF. ST OF $A_1, \ldots, B_2$ SATISFIES: $|\pi| \geq s(n)^{\Omega(1)}$.

(2) IF U IS CLOSED UPWARDS, $A_1, \ldots, B_2$ OBEY THE NONU FI SET-UP AND P ADMITS NONU FI $\Rightarrow$ ANY P-REF of $A_1, \ldots, B_2$ SATISFIES

$$|\pi| \geq s'(n)^{\Omega(1)}$$

WHERE $s'(n)$ IS THE MIN SIZE OF NONU SEPAR. CIRCUIT.

□

CONDITIONAL BOUNDS – EX'S

LEMMA 17.1.3: ASSUME P ADMITS FI AND $NP \not\subseteq P/poly$

THEN P IS NOT p-bounded.

PF: ASSUME P IS p-BOUNDED

$\Rightarrow NP = coNP = NP \cap coNP$

$NP \cap coNP \not\subseteq P/poly$

TAKE $U \in NP \cap coNP \setminus P/poly$

$\{A_1, \ldots, B_1\}$

EXPRESSING $U \to |U| = y$ ——FI——→ $\exists$ size $n^{O(1)}$ separating circuit

HAS p-size p-REF

□

$\subseteq NP$

UP = unambiguous NP $\Leftrightarrow$ unique witnesses

Ex: FACTORING $\in$ UP : i.e. $\{(n,i) \mid$ i^{th} bit of the canonical factoring of n is 1$\}$

HARD BIT OF A OWP :

Ex - RSA - PAIR

$U = \{u \mid RSA^{-1}(u)$ is ODD$\}$

$V =$ . . . . . is EVEN

$UP \neq P/poly \Rightarrow NP \neq P/poly \Rightarrow$ L. 17.1.3 WORKS

BUT THESE ARE VERY SPECIFIC WELL-TESTED PROBLEMS

BETH'S THM. (L 17.1.91)

ASSUME $U \in NP$, $A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q})$

DEFINE U_n IN THE SENSE OF THE FI SET-UP.

ASSUME P ADMITS FI.

IF π IS A P-REFUT. OF:

$$A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q}), q_1, A_1(\bar{p},\overline{\bar{q}}), \ldots, A_m(\bar{p},\overline{\bar{q}}), \overline{\pi q_1}$$

$\Rightarrow$ $\exists$ circuit $C(\bar{p})$ OF SIZE $|\pi|^{O(1)}$ COMPUTING

q_1:

$$\bigwedge_i A_i(\bar{p},\bar{q}) \Rightarrow (q_1 \equiv C(\bar{p}))$$

PROOF: APPLY CRAIG'S INTERPOLATION.

$$\left(\bigwedge_i A_i(\bar{p},\bar{q}) \cdot q_1\right) \to \gamma(\bar{p})$$

$$\gamma(\bar{p}) \to \left(\bigwedge_i A_i(\bar{p},\bar{r}) \to r_1\right)$$

□

(EX.) $\bigwedge_i A_i(\bar{p},\bar{q}) \rightleftharpoons \bar{q}$ is the CANONICAL FACTORIZATION OF $\bar{p}$

[WILL ELABORATE ON THIS LATER]

COROLLARIES (17.1.5-6)

ASSUME THAT

EITHER NO P-SIZE CIRCUIT COMPUTES FACTORIZ.

OR " " DECIDES RSA.

THEN NO PPS P THAT ADMITS f_1

IS P-BOUNDED.

PROF:

P-BOUNDED $\Rightarrow$ SHORT P-REF'S + f_1

SMALL CIRCUIT

□

WE WANT UNCONDITIONAL LOWER BOUNDS

↙

THIS REQUIRES

(i) ESTABLISH NONU FI FOR P

(ii) TO HAVE DISJOINT NP-PAIR U/L

WITH U CLOSED UPWARD

THAT IS (UNCOND.) ~~HARD~~ IMPOSSIBLE

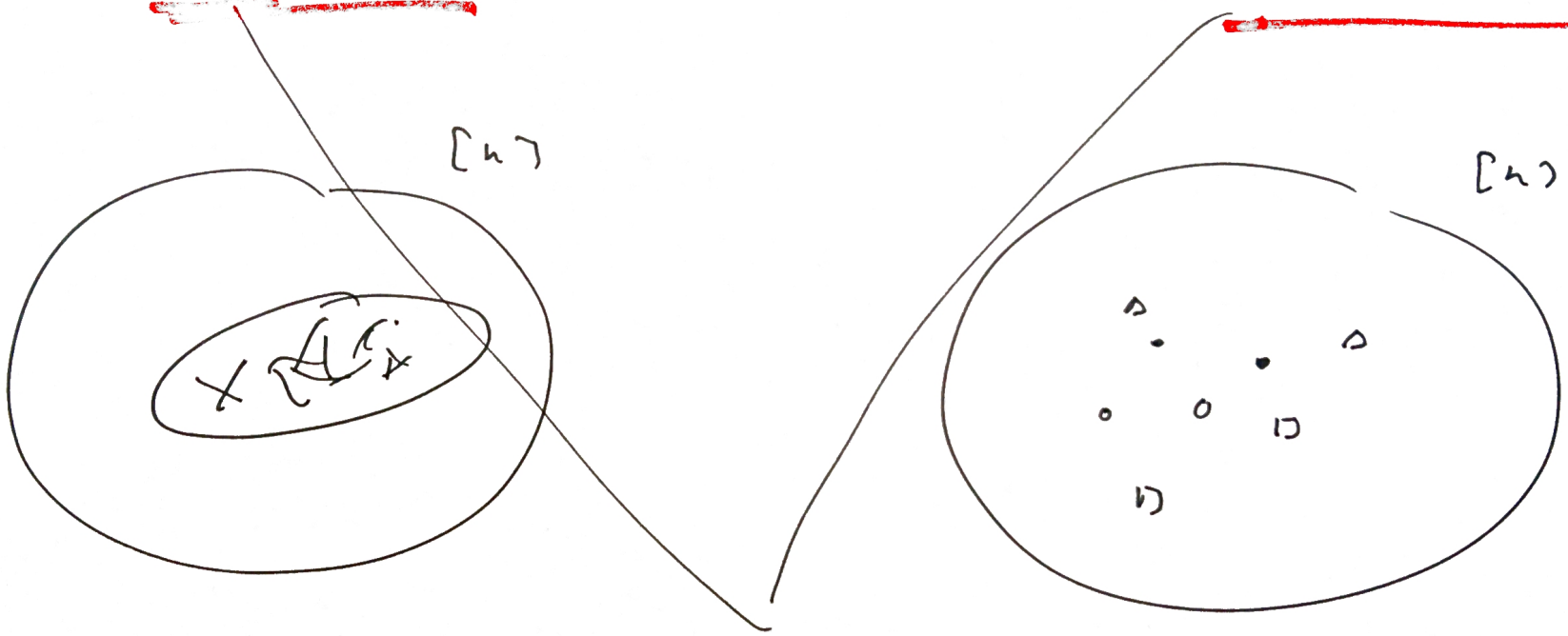
TO SEPARATE BY POLY-SIZE

MONO CIRCUITS.

ITEM BOUND PAIR

U: graphs with large clique

V: graphs colorable by a small nb. of colors



(i) large > small

then $U \cap V = \emptyset$

~~$\Gamma_{n,\omega}$~~: CLIQUE$_{n,\omega}$

- graphs on $[n]$ having clique of size $\geq \omega$

- $\underbrace{A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q})}$, $\bar{p}$: $\binom{\omega}{2}$-tuple

$\bar{q}$: each atom

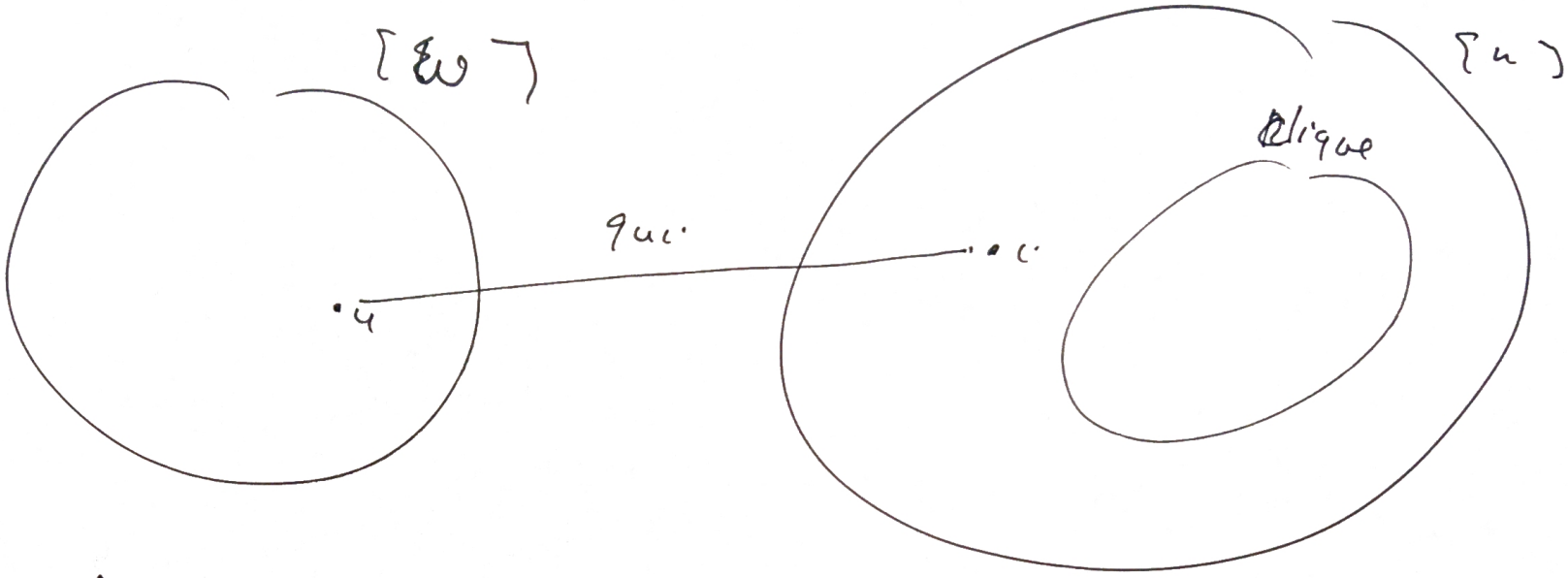
FORMALIZE THAT $\bar{q}$ is

a GRAPH OF A

1-to-1 MAP

$$[\{\}] \longrightarrow \subseteq [n]$$

ONTO A CLIQUE



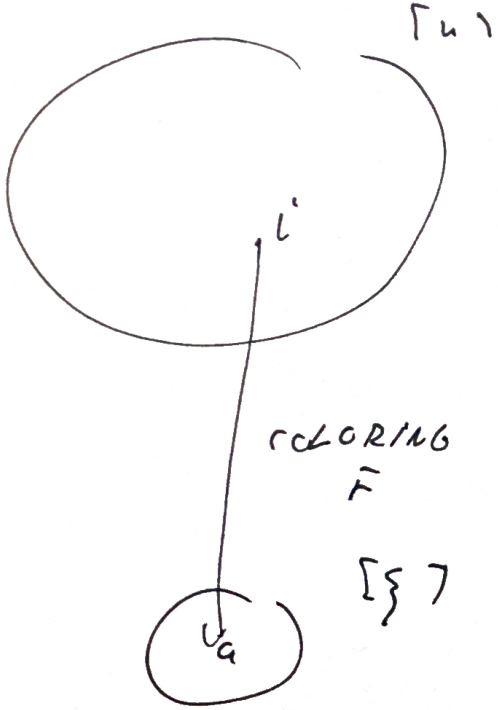
p_{ij} : for $\{i,j\} \subseteq [n]$

q_{ui} : $u \in [\omega]$, $i \in [n]$

A-clauses:

- $\bigvee_i q_{ui}$, all u
- $\neg q_{ui} \vee \neg q_{uj}$, all u, $i \neq j$
- $\neg q_{ui} \vee \neg q_{vi}$, all $u \neq v$, i
- $\neg q_{ui} \vee \neg q_{vj} \vee p_{ij}$, all $u \neq v$, i,j.

$COLOR_{n,5}$: graphs 5-colorable



B-clauses: p_{ij}

x_{ia} , $i \in [n]$, $a \in [5]$

- $\bigvee_a x_{ia}$, all i

- $\neg x_{ia} \vee \neg x_{ib}$, all i, $a \neq b$

- $\neg x_{ia} \vee \neg x_{ja} \vee \neg p_{ij}$, all $i \neq j$, a

[Sec. 13.5]

OBSERVATION: For $n \geq \omega \geq \xi \geq 1$,

~~FOR~~ $\mathrm{CLIQUE}_{n,\omega} \to \mathrm{COLOR}_{n,\xi} = 4$.

$\mathrm{CLIQUE}_{n,\omega}$ → CLOSED UPWARDS

$\mathrm{COLOR}_{n,\xi}$ → IN FACT: CLOSED DOWNWARDS

PRF:

→ vertices in a clique have to get different colours

→ adding edges cannot remove a clique

→ removing edges cannot destroy a coloring

THM (RAZBOROV, as improved by ALON & BOPPANA)

For $n \geq \omega > \xi \geq 3$ and $\omega \cdot \sqrt{\xi} \leq n/(\delta \log n)$

ANY MONO CIRCUIT SEPARATING CLIQUE$_{n,\omega}$ FROM COLOR$_{n,\xi}$ MUST HAVE THE SIZE

$$S^+(n) \geq 2^{\Omega(\sqrt{\xi})}.$$

□

Ex.-parameters: $\omega = n^{2/3}$, $\xi = n^{1/3}$

$$\Rightarrow \text{l.bound} \geq 2^{\Omega(n^{1/6})}.$$

[Thm 13.5.3]