LECTURE 12

→ FI, part IV.

- generalizations
- limitations
- non-automatizability

Fi – BIG PICTURE

↓

A WAY HOW TO REDUCE THE TASK

TO PROVE LENGTHS-OF-PROOFS

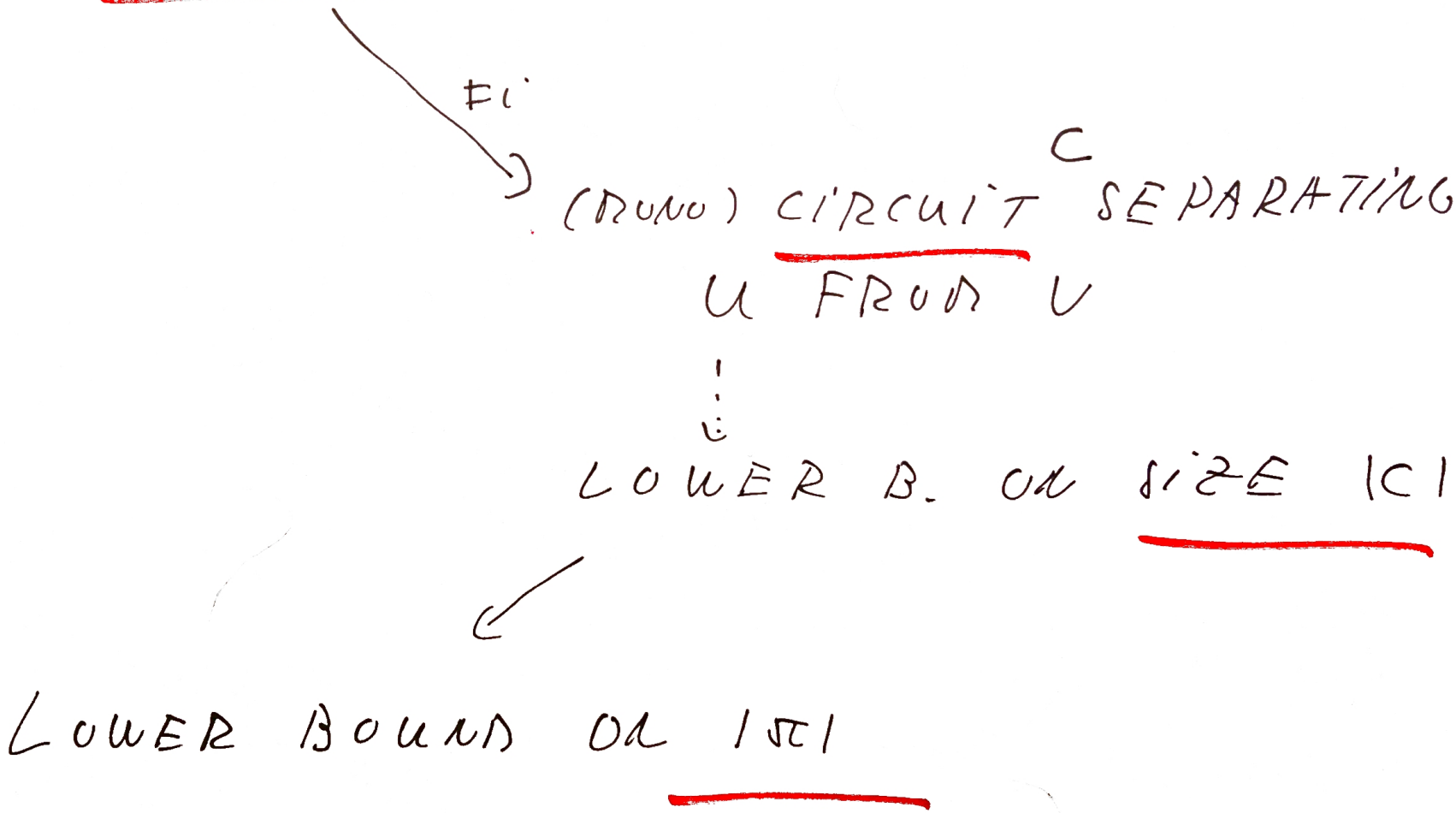
LOWER BOUNDS TO THE TASK

TO PROVE A LOWER BOUND

ON A COMPUTATIONAL MODEL

SPECIFIC APPROACH:

A REFUTATION π OF $U \cap V \neq \emptyset$



POSSIBLE GENERALIZATIONS

↓

"INTERPOLATE" BY ANOTHER COMPUTATIONAL MODEL ~~X~~

INSTEAD OF CIRCUITS

"FI BY X"

NOW ONE EXAMPLE, Chpt. 18 OFFERS A NUMBER OF OTHE EXAMPLES

LAST TIME : CP (CUTTING PLANES)

LINES : $\bar{a} \cdot \bar{p} + \bar{b} \cdot \bar{q} + \bar{c} \cdot \bar{r} \geq d$ (*)

COEFF's $\bar{a}, \bar{b}, \bar{c}, d \in \mathbb{Z}$

OF VAR's $\bar{p}, \bar{q}, \bar{r} \leq n^{O(1)}$ (cf. F1 SET-UP)

=

PLAYERS NEEDED TO SEND EACH OTHER VALUES OF PARTS OF THE SUM IN (*) THEY COULD EVALUATE (BINARY SEARCH)

ASSUMPTION :

$$-M \le \text{coeff's} \le M$$

$\Rightarrow$

$$-M \cdot n^{O(1)} \le \underbrace{\text{value of any part}} \le M \cdot n^{O(1)}$$

NEED UP TO $\log(M \cdot n^{O(1)}) =$

$= \log(M) + O(\log n)$ bits

TO SPECIFY

$\Rightarrow$ LOWER BOUNDS DEPEND ON M.

model X : MONO REAL CIRCUITS

GATES : COMPUTE UNARY/BINARY REAL NON-DECREASING ~~CONSTANTS~~ FUNCTIONS

INPUTS : STILL 0/1

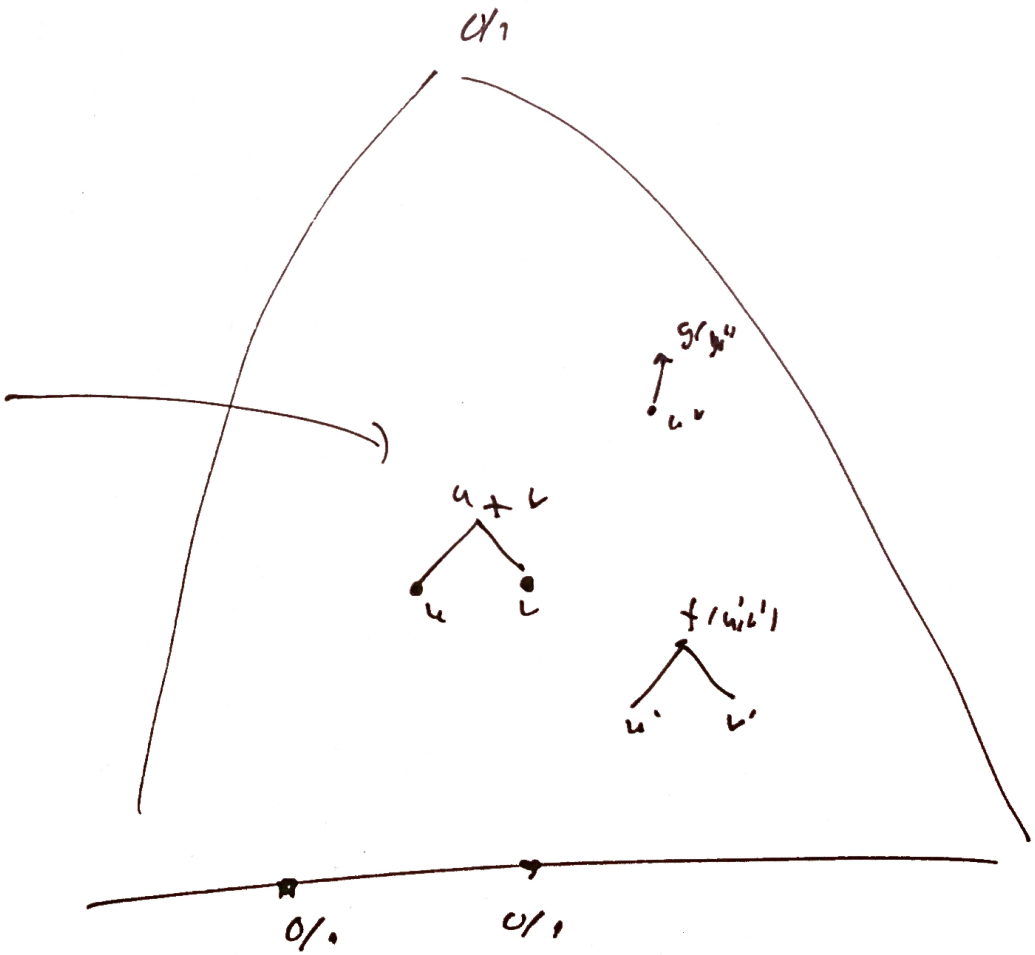
OUTPUT : STILL 0/1

REMARK : WE CONSIDER ONLY MONO CASE :

→ IN THE NON-MONO CASE IT CAN BE REMOVED BY ANOTHER PROOF (Sect. 17.1)

VALEUS
HERE
MAY BE

$\neq 0, 1$



OBSER.: NONO REAL C. COMPUTES NON BOOL. FUNCT.

FACT : LOWER BOUND FOR DDNF CIRCUITS

SEPARATING $\text{CLIQUE}_{n,w}$ / $\text{COLOR}_{n,\zeta}$

APPLY FOR DDNF REAL CIRCUITS

AS WELL (ESS. SAME PROOF)

$2^{\Omega(n^{1/6})}$ for $w = n^{2/3}$, $\zeta = n^{1/3}$

THM. (PUDLÁK) : CP ADMIT NONU FI

BY NONU REAL CIRCUITS.

HENCE LOWER BOUND $2^{\Omega(n^{1/6})}$

TO THE NB. OF STEPS APPLIES (NO

REFERENCE TO R AS BEFORE).

□

WE LOOK AT HOW THE CONN.-COMPL.

APPROACH CAN BE MODIFIED.

REAL GAME

U-player : GETS $u \in U$

V-player : -"- $v \in V$

ONE ROUND:

- BOTH PLAYERS SEND A REAL (r_u and r_v, resp.) TO A REFEREE

- REF. ANNOUNCES 1 BIT:

  → 1, IF $r_u > r_v$

  → 0, IF $r_u \leq r_v$

PLAYERS DECIDE KNOWING u/v resp. PLUS THE HISTORY OF REFEREE'S ANNOUNCEMENTS $\in \{0,1\}^*$

$CC^{IR}(R)$:= REAL CC OF MULTIFUNCTION R
($R \subseteq U+V+I$)

LEMMA 18.2.1

IF U IS CLOSED UPWARDS THEN

$CC^{IR}(KW^m[U,V]) \leq$ MIN DEPTH OF A
MONO REAL CIRCUIT SEP. U/V

AND ALSO $\leq \log_{3/2}$ (SIZE OF MONO REAL FLA SEPAR. U/V)

ANALOGOUSLY AS BEFORE:

$\tilde{A}_1, \ldots, \tilde{B}_1, \ldots$ U/L, MONO FIXED-UP

CP-REFUT. of π $\perp$ WITH k STEPS

$\Downarrow$

MONO PROTOCOL separating U/L (i.e. computing $KW^m[U,V]$) $\leq_G$ OF SIZE $\leq k+n$, $CC^{IR} \leq T \leq \alpha/\log 4$)

$=$

IN ADDITION: π TREE-LIKE

$\Downarrow$

$\leq_G$ TREE-LIKE

$\Downarrow$

SEPARATING MONO

$\Downarrow$ REAL FLA

$CC^{IR}(KW^m[U,V]) \leq O(\log n)\cdot(\log 4)$.

REMARK (Cf. Thm. 18.2.3):

CC^{IR} CAN BE REDUCED TO

COMPLEXITY OF RANDOMIZED ORDINARY

KW-PROTOCOLS

⇓

YIELDS LOWER BOUNDS FOR TREE-LIKE CP ($= CP^*$)

FOR ANOTHER DUAL DISJOINT NP-PAIR

(↪ NOT CLIQUE/COLOR).

[18.2.4-6]

OTHER EX's OF PPS / MODELS (Chpt. 18 HAS MORE)

PC (POLY CALCULUS)

LS (Lovász – Schrijver)

→ NEXT SLIDE

OBDD

RCLIN), CP . .

LINES ... ∨ (lin. functions) ∨ ...

SPAN PROGRAMS

MONO LP-CIRCUITS

OR "NB. ON FOREHEAD COMM. COMPL. MODEL"

... MONO CIRCUITS + A TRICK

RANDOMIZED PROTOCOLS

LS .... LINEAR ARE

$f(p_1 q_1 r) \geq d$

$\therefore$ $\leq$ DEG 2 POLY OVER $\mathbb{R}$

NB. ONE FOREHEAD : INPUTS $= I_1 \cup I_2 \cup I_3$

3 PLAYERS : PLAYER 1 KNOWS INPUTS FROM $I_2 \cup I_3$

PL. 2 .... $I_1 \cup I_3$

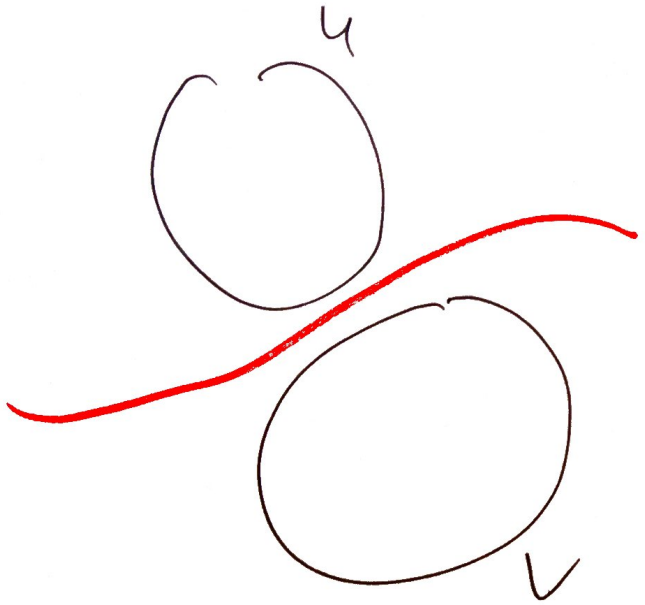
PL. 3 .... $I_1 \cup I_2$

I.E. : DOES NOT KNOW I_1

$\Rightarrow$ EACH MONOMIAL IS KNOWN TO ONE PLAYER

$\Rightarrow$ THEY CAN COOPERATIVELY EVALUATE f ....

LIMITATIONS : FI MEANS



HARD TO SEPARATE

$\Longrightarrow$ FI

$U \cap V \neq \phi$

HARD TO REFUTE.

HENCE TO SHOW THAT PPS P HAS NO (MONO) FI IT SUFFICES TO SHOW THAT $\exists$ p-SIZE P-REFUT'S OF

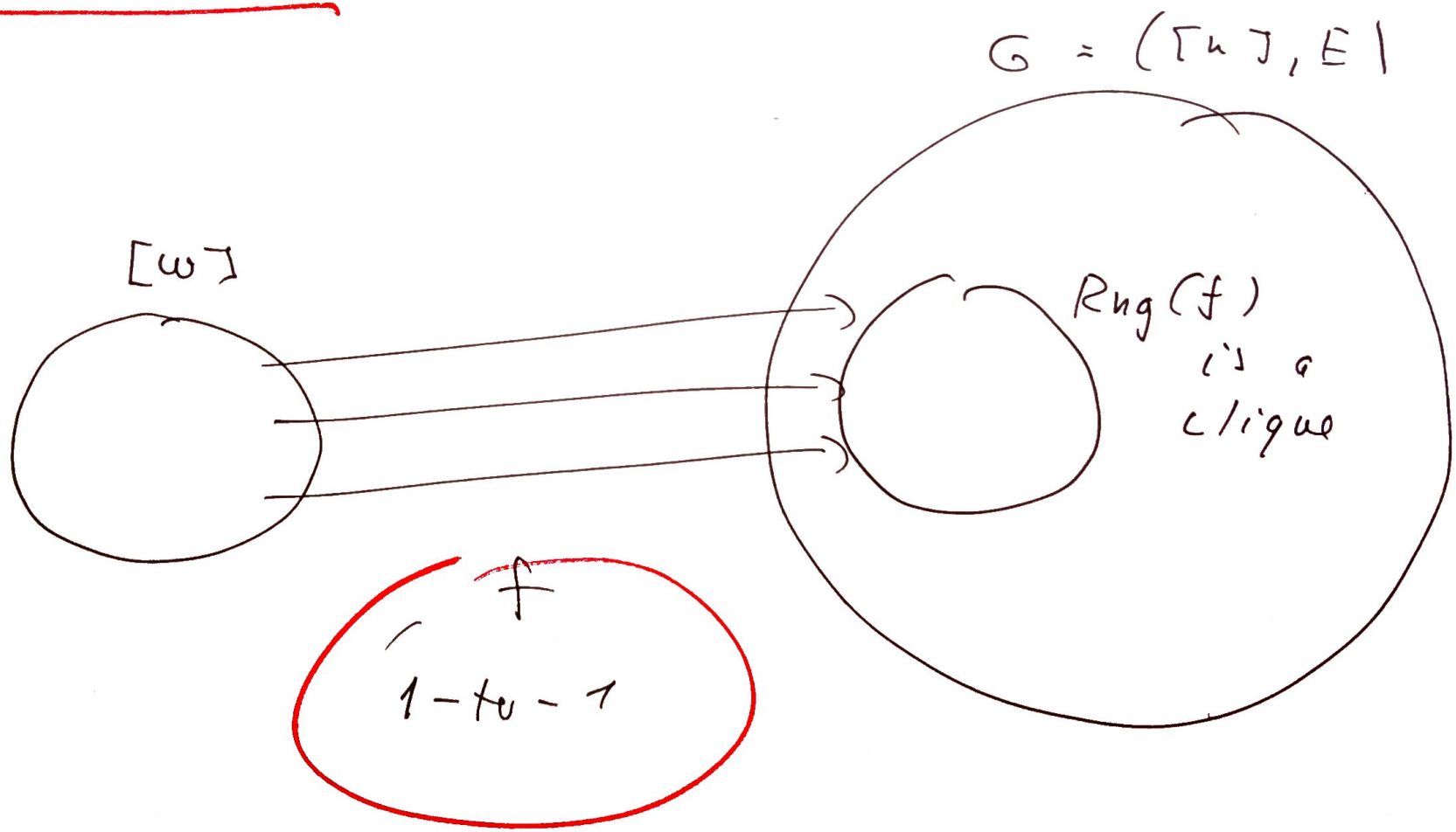
$$U \cap V \neq \emptyset$$

FOR ONE OF THE "HARD PAIR U/V"

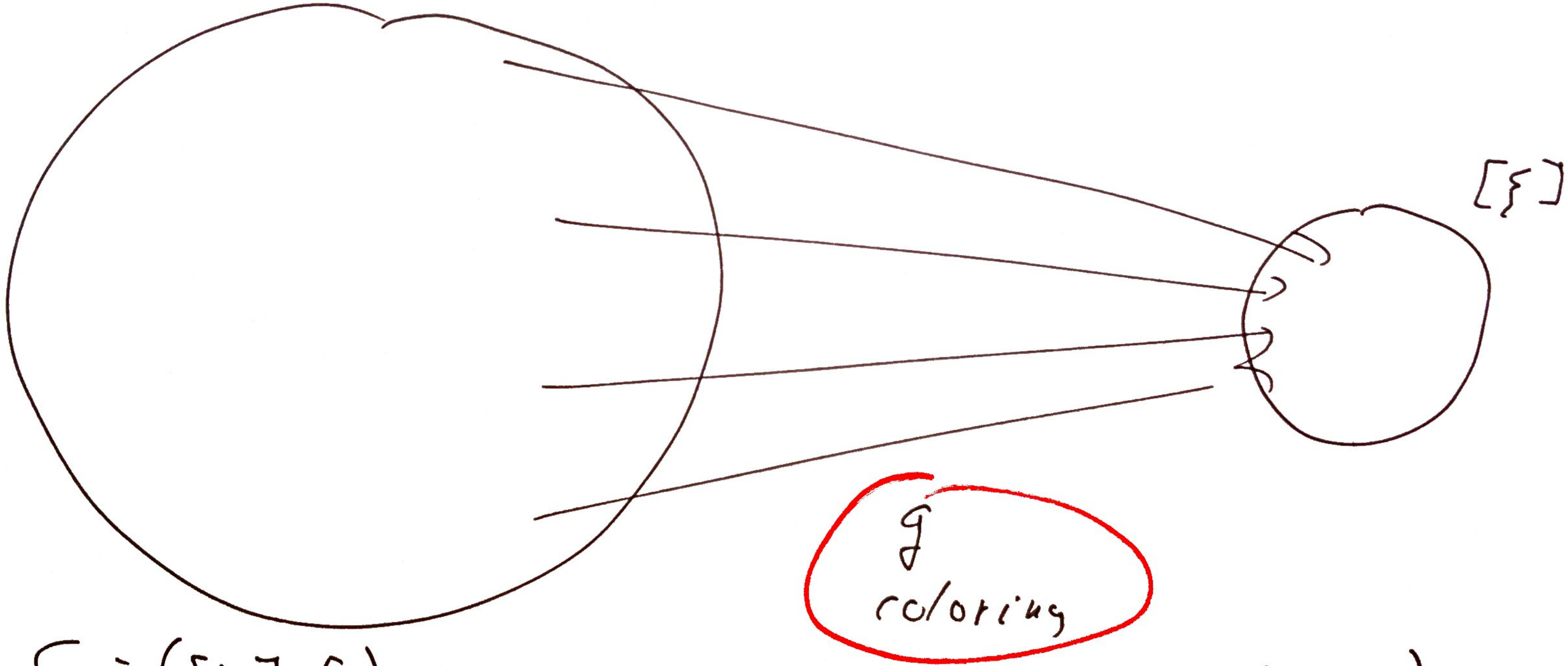
(MONO OR NON-MONO)

NONO CASE:

$CLIQUE_{n,w}$: G s.t.



$\text{COLOR}_{n,\xi}$: G s.t.



$G = ([n], E)$

$((i,j) \in E \rightarrow g(i) \neq g(j))$

OBSERVATION: IF $G \in CLIQUE_{4,\omega} \cap COLOR_{4,\chi}$ AND MAPS f, g WITNESS IT THEN:

$$g \circ f : [\omega] \longrightarrow [\chi]$$

IS 1-TO-1.

PRF.: $Rng(f)$ IS A CLIQUE (=ALL EDGES) AND HENCE ALL ITS VERTICES HAVE TO GET A DIFFERENT COLOR BY g.

□

WITH THE PARAMETERS $\omega := n^{2/3}$, $\xi := n^{1/3}$

THIS VIOLATES THE

WEAK PHP: $WPHP(\xi^2, \xi)$ for $h := g \circ f$.

FACT (Corr. 11.4.5): DNF-P AND SO ALSO AC^0-F AND F AND ... STRONGER ... PROOF

$WPHP(m^2, m)$ IN SIZE $m^{O(\log m)}$.

17

COROLLARY: THESE (AND STRONGER) PPS' DO NOT ADMIT DOUBLE FI.

NON-TRIVIAL CASE: RSA-PAIR [Sec. 17.2]

RSA: $N := p \cdot q$

$$RSA : x \in [N] \longrightarrow y := x^{e} \bmod N \in [N]$$

1-to-1

e ← PUBLIC KEY

$U := \{ y \in [N] \mid RSA^{-1}(y) \text{ is ODD} \}$

$V := \{ y \in [N] \mid RSA^{-1}(y) \text{ is EVEN} \}$.

THINK OF $N \subseteq \{0,1\}^n$ FOR $n = \lceil \log_2 N \rceil$, SO $U, V \subseteq \{0,1\}^n$.

FACT : SEPARATING U/V IS AS HARD AS (INVERTING) BREAKING RSA.

I. E. :

RSA SECURE AGAINST p-SIZE CIRCUITS $\Rightarrow$ U/V CANNOT BE SEPARATED BY p-SIZE CIRCUITS

[this is a known fact in crypto]

USING THE SAME ENCODING AS IN NP-COMPL. OF SAT WE CAN ENCODE $(x, y \in \{0,1\}^4)$:

$$RSA(x) = y$$

$$\Downarrow$$

PROP. CNF FLA $\varphi(x, y, z)$

S.T. $\forall u, v \in \{0,1\}^4$:

$$RSA(u) = v \iff \varphi(u, v, z) \in SAT$$

THM.: ER (= EXTENDED R) HAS P-SIZE REFUTATIONS OF:

$$\varphi(x,y,z) \wedge \varphi(x',y,z') \wedge x \neq x'$$

I.E. IT PROVES SHORTLY THAT RSA is 1-to-1.

□

[Sec. 18.7]

COROLLARY (Thm. IV. 7.2)

ER HAS SHORT REFUTATIONS OF ~~THE~~ $U \cap V \neq \emptyset$ FOR THE RSA-PAIR.

HENCE, ASSUMING THE SECURITY OF RSA, ER DOES NOT ADMIT F_1. □

FACT: SIMILAR RESULTS ARE KNOWN FOR F AND EVEN LOW DEPTH F_d, USING OTHER CRYPTO-HYPOTHESES (e.g. SECURITY OF DIFFIE-HELLMAN)

CAN WE INTERPRET THE FAILURE OF F_i FOR P AS SOME "POSITIVE" STATEMENT?

YES

[Sec. 17.3]

DEFINITION: PPS P IS AUTOMATIZABLE

IFF $\exists$ DETER. ALG. $\mathcal{A}$ S.T.

$\forall$ UNSAT SET OF CLAUSES C:

$\mathcal{A}$ FINDS A P-REFUT. OF C

IN TIME POLY $(S_P(C))$

MIN SIZE OF A P-REFUT. OF C

BECAUSE TIME $\geq$ SIZE OF $\mathcal{A}$ IN P THIS IS OPTIMAL UP TO poly. ☐

LEMMA 17.3.1 ASSUME P SATISFIES THE PROPERTY

(*): IF C HAS A SIZE s P-REFUT. AND

C' IS OBTAINED FROM C BY SUBSTITUTING

O/1 FOR SOME VAR'S THEN C' HAS

A SIZE $\leq O(s)$ P-REFUT.

THEN:

P IS AUTOMATIZABLE

$\Rightarrow$

P ADMITS FI

PRF: $\mathcal{C}$ IN FI SET-UP:

$$A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q}), B_1(\bar{p},\bar{r}), \ldots, B_\ell(\bar{p},\bar{r})$$

ASSUME $\mathcal{C}$ HAS A SIZE s ρ-REFUT.

WANT: SIZE $s^{O(1)}$ SEPARATING CIRCUIT.

Algorithm $\mathcal{B}$: GIVEN $\bar{u} \in \{0,1\}^*$

(1) RUN $\mathcal{A}$ (= AUTOMATIZING ALG.)

ON:

$$B_1(\bar{u},\bar{r}), \ldots, B_\ell(\bar{u},\bar{r}).$$

FOR:

s^{c+1} time, where:

$\mathcal{A}$ runs in time s^c.

CLAIM IF $\mathcal{A}$ OUTPUTS A P-REFUT,

$\mathcal{B}$ OUTPUTS 1.

OTHERWISE $\mathcal{B}$ OUTPUTS 0.

CLAIM: $\mathcal{B}$ SEPARATES U_ℓ / U_ℓ AND IS P-TIME.

↳ : IF IT WERE THAT $U_\ell \not\equiv U_\ell$ WE ~~could substitute~~

COULD SUBSTITUTE INTO THE ORIG. C

$\bar{q} :=$ SOME WITNESSES $\bar{q}^u$ FOR $U_\ell \not\equiv U_\ell$.

BY (*) THIS NEW C' HAS SIZE $< |x|$

REFUTATION. BUT ALL $A_i(U_{|y|}^{q_i})$ ARE TRUE

SO THIS IS A REFUT. OF

$$B_1(u,\vec{s}), \ldots, B_\ell(u,\vec{s}) \qquad (\#)$$

||

$\mathcal{A}$ OUGHT TO FIND SOME P-REF. OF (#) IN

TIME $(O(s))^c$ (n^c is time of $\mathcal{A}$).

$\leq s^{c+1}$ FOR $s >> 0$.

SO:

$u \in U \longrightarrow \mathcal{A}$ finds it $\longrightarrow B$ outputs 1

$u \in V \longrightarrow$ (#) IS SAT SO B CANNOT FIND A REF. $\longrightarrow B$ outputs 0.

CLAIM

TO CONCLUDE THE PROOF REPLACE $\mathcal{B}$ BY

A CIRCUIT D: $\mathcal{B}$ p-time $\Rightarrow$ D p-size

[SAVAGE's THM.]

$\square_L$.

Will-Will:

- $P \neq NP \cap coNP$ $\longrightarrow$ WE GET (CONDITIONAL) PROOF-SIZE LOWER BOUNDS
- $P = NP \cap coNP$ $\longrightarrow$ WE GET TIME LOWER BOUND FOR P-PROOF SEARCH ALG'S.

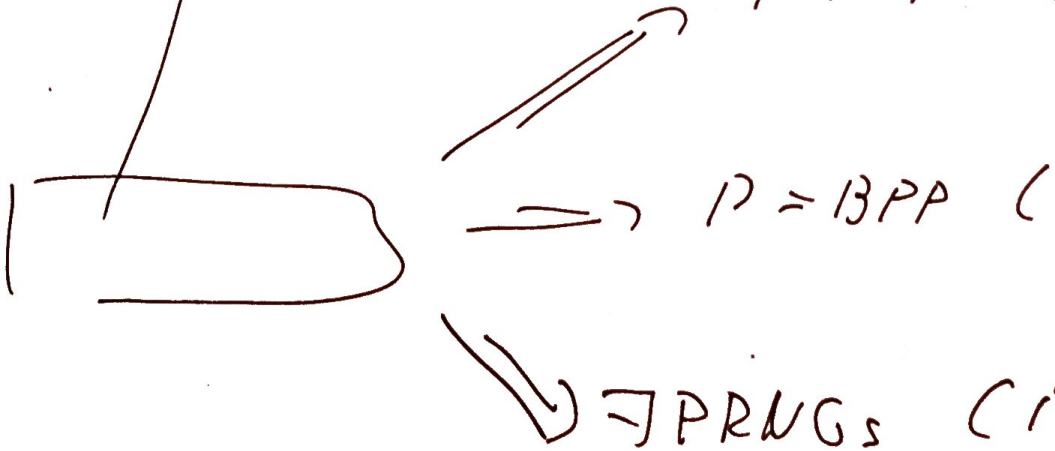
FUTURE OF FI? ONE SHOULD TRY TO GENERALIZE

THE BIG PIC:

COMPUTATIONAL HARDNESS ⟹ PROOF-COMPLEXITY HARDNESS

AND CONSIDER FI AS AL INSTANCE OF THIS PRINCIPLE.

NOTE



A SIMPLE TO STATE OPEN PROBLEM

ASSUME F (= FREGE PPS, e.g.) PROVES IN SIZE s

$$\alpha \vee \beta$$

WHERE α, β HAVE NO ATOM IN COMMON.

IS THERE THEN NECESSARILY A SIZE

$$\leq \text{poly}(s)$$

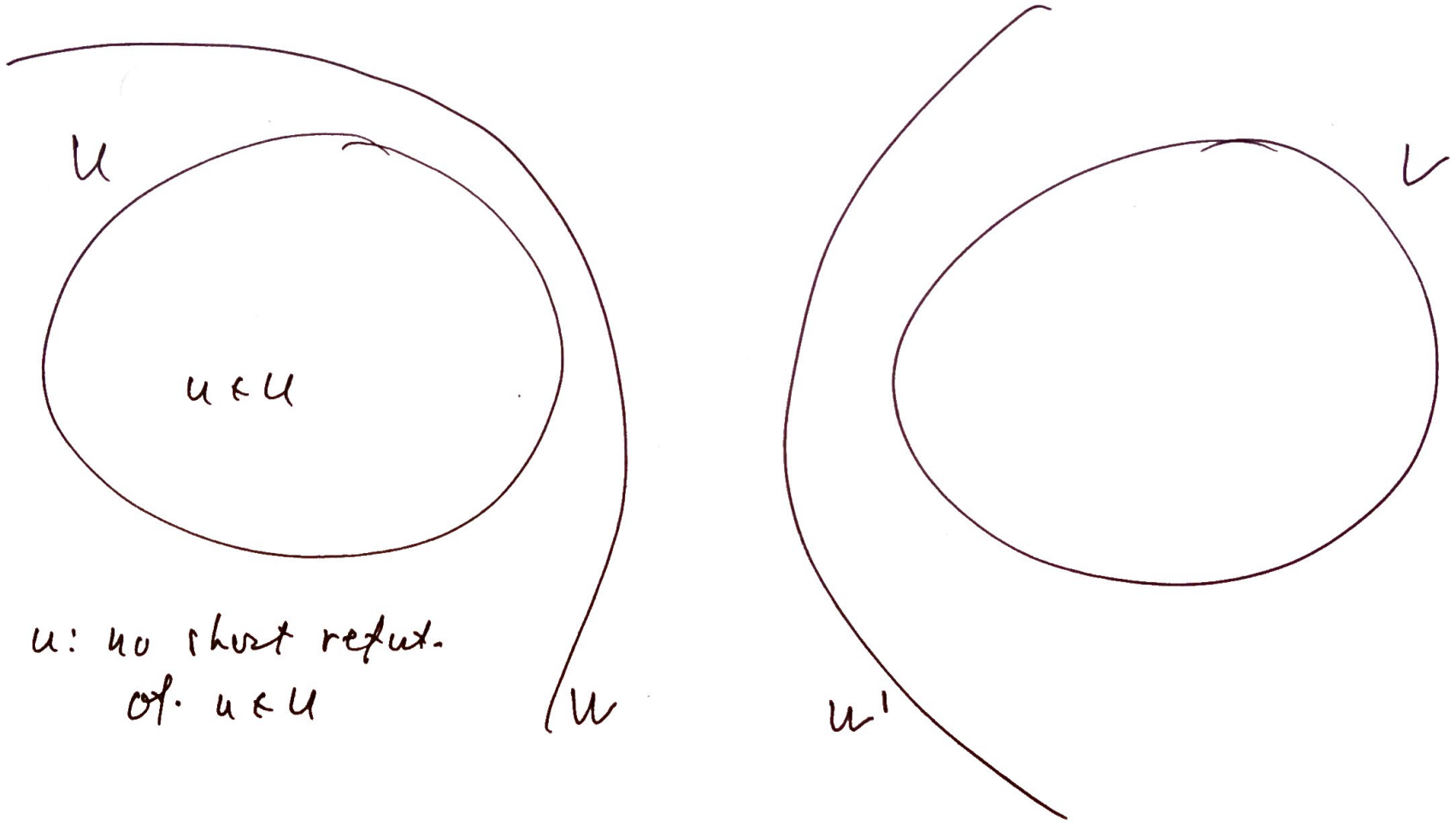
F-proof of α OR β ?

OBSERVATIONS: (i) $\alpha \vee \beta$ TAUT $\Rightarrow$ SUBST. FALSIFYING ASSIGN. TO TURN $\alpha \vee \beta$ INTO OR β i.e. β.

(ii) AT LEAST ONE IS TAUT AND HENCE PROVABLE.

FI-STYLE PICTURE

U/V ENP



$u \notin U \vee u \notin V$