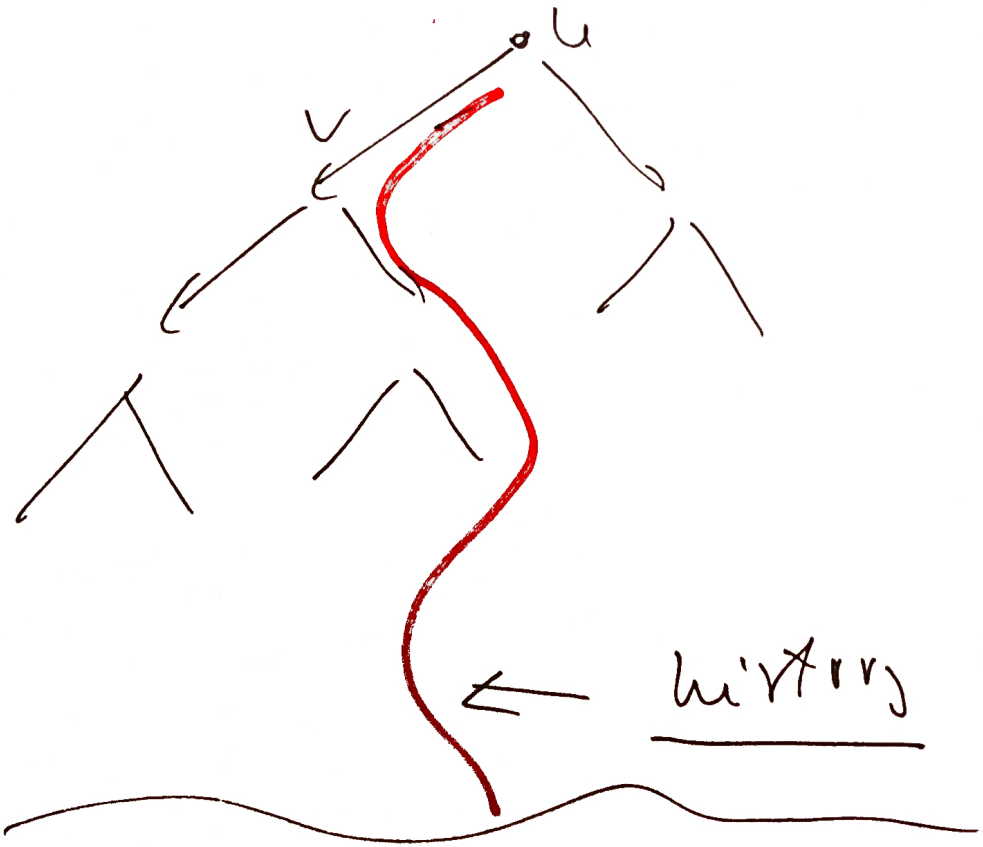
LECTURE 11.

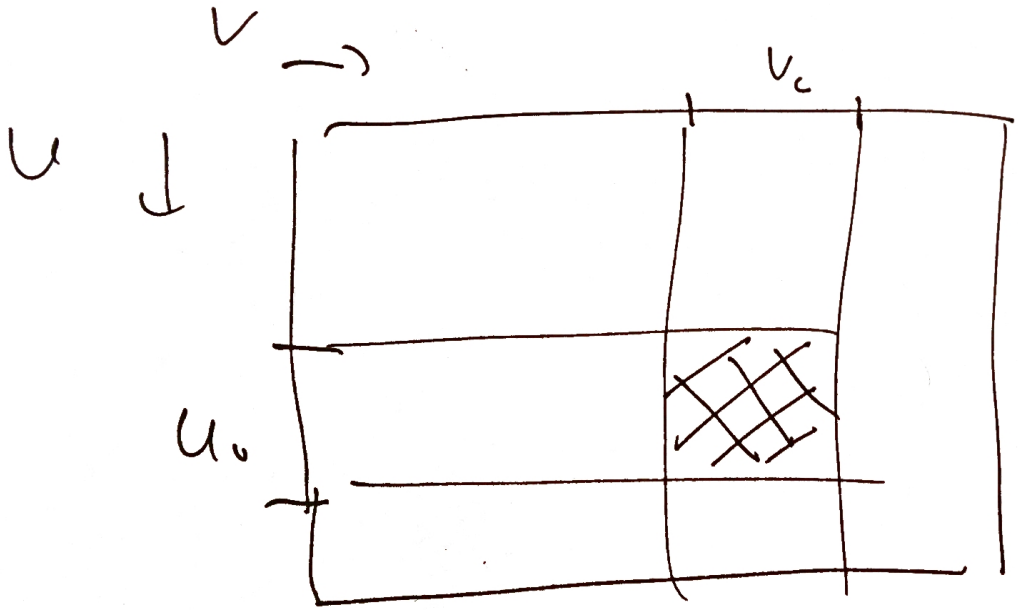
→ F1, part III.

OBSERVATION USED IN THE PROOF OF Thm 17.4.3 (protocols => circuits) [on p. 369]:



CLAIM: THE SET OF $(u,v) \in U+V$ S.T. THE COMMUNICATION EVOLVES ACCORDING TO w IS A (COMBINATORIAL) RECTANGLE:

$$U_0 + V_0 \text{, SOME } U_0 \subseteq U, V_0 \subseteq V$$



PRE-CLAIM: ASSUME (u,v) and (u',v') YIELD HISTORY w. NOW CONSIDER PAIR (u, v'):

- AT THE START U-player SEES ONLY HIS u AND SENDS w_1 : HE SENT IT IN (u,v)

- THEN THE V-player SEES HER v' PLUS w_1 : SHE SAW THE SAME INFO IN PLAY (u',v'), SO SENDS ALSO w_2.

- ETC.

□

CONSIDER $X, Y \subseteq \{0,1\}^N$ (later: $N = u+s+\ell$)

THE SEMANTIC RULE ALLOWS TO INFER

$$\frac{X \quad Y}{Z}$$

IF $Z \supseteq X \cap Y$.

NOTATION: X, Y, Z REPRE SETS OF ASSIGNMENTS SATISFYING FLAS IN AN INFERENCE:

THEN: THE RULE $\Leftrightarrow$ SOUNDNESS OF THE

DEF.: A SEMANTIC DERIVATION OF C FROM $D_1, \ldots, D_n$ IS A SEQ.:

$$E_1, \ldots, E_k$$

S.T.

(1) EACH E_i IS EITHER $\in \{D_1, \ldots, D_n\}$

OR DERIVED

FROM EARLIER D_{j_1}, D_{j_2}, $j_1, j_2 < i$,

BY THE RULE

(2) $E_k = C$.

OBSERVATION : $D_1, \ldots, D_k \vdash C$

"CAN BE DERIVED"

$\Updownarrow$

$C \supseteq \bigcap_i D_i$

AND, IF SO, THE DERIVATION HAS $\leq k+1$ STEPS.

□

THIS LOOKS TRIVI BUT WHAT

IF WE RESTRICT ALL STEPS $\hat{E}_i$

TO SOME FAMILY $\mathcal{C}$ OF SETS?

DEF.: FOR $\mathcal{C} \subseteq \mathcal{P}(\{0,1\}^N)$, $E_1, \ldots, E_k$

IS AN $\mathcal{C}$-DERIVATION OFF

ALL $E_i \in \mathcal{C}$.

EX: $\mathcal{C} \rightleftarrows$ SETS DEFINABLE BY

CLAUSES IN N ATOMS

$\Downarrow$

SEMANTIC RESOLUTION.

FOR $D_1, \ldots, D_n, C \in \mathcal{K}$

WE CANNOT USE THE TRIVIAL DERIVATION

$D_1, D_2, D_1 \cap D_2, (D_1 \cap D_2) \cap D_3, \ldots$

MAYBE $\notin \mathcal{K}$

=

IT MAY NOT BE POSSIBLE TO $\mathcal{K}$-DERIVE

C

RECALL THE FIRST-UP (Lect. 9)

$U, V \subseteq \{0,1\}^n$, $U \cap V$

- A-clauses $A_1(\bar{p},\bar{q}), \ldots, A_m(\bar{p},\bar{q})$

  $\bar{p} = p_1, \ldots, p_n$, $\bar{q} = q_1, \ldots, q_s$

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

- B-clauses $B_1(\bar{p},\bar{r}), \ldots, B_t(\bar{p},\bar{r})$

  $\bar{r} = r_1, \ldots, r_\ell$

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

DONE IF U CLOSED UP IN p_i + IN A-CL'S.

PUT : $N := n + s + \ell$

DEF.: A GAME DETERMINED BY SOME $A \subseteq \{0,1\}^\omega$

2 PLAYERS: $\forall$ & $\exists$

$\forall$: GETS $u \in U$ AND $q^u \in \{0,1\}^*$ S.T. $\bigwedge_i A_i(u, q^u)$

$\exists$: GETS $v \in V$ AND $r^v \in \{0,1\}^*$ ... $\bigwedge_j B_j(v, r^v)$

THEY ARE ASKED TO DECIDE SEVERAL

STATEMENTS ABOUT u, v, q^u, r^v:

(CONT'D)

(i) $(u, q^u, r^v) \in_? A$

(ii) $(v, q^u, r^v) \in_? A$

(iii) IF ANSWERS TO (i) & (ii) DIFFER,

FIND $(i \in [n])$: $u_i \neq v_i$.

CC(A) := min # of bits they need to exchange (in a KW-protocol) in THE WORST CASE SOLVING ANY (i), (ii), (iii).

NONO CASE : U CLOSED ↑

$\Pi CC_U(A) := \min T \geq CC(A)$ s.t. THEY CAN

SOLVE IN $\leq T$ STEPS OTHERWISE:

(a'v) IF $(u, q^u, r^v) \in A$, $(u, q^u, r^v) \notin A$ then

either : find $i \in [n]$, $u_i := 1$ & $v_i := 0$

or : decide $\exists u' \geq u$, $(u', q^u, r^v) \notin A$.

□ Def.

FINAL (?) TECHNICALITY:

FOR $A \subseteq \{0,1\}^{n+s}$ PUT

$$\tilde{A} \subseteq \{0,1\}^{N} := \{(a,b,c) \mid (a,b) \in A,\ c \in \{0,1\}^{\ell}\}$$

$|a|=n,\ |b|=s,\ |c|=\ell$

$$= A \times \{0,1\}^{\ell}$$

FOR $B \subseteq \{0,1\}^{n+\ell}$ PUT $\tilde{B} \subseteq \{0,1\}^{N}$:

$$\tilde{B} := \{(a,b,c) \mid |a|=n,\ |b|=s,\ |c|=\ell,$$
$$(a,c) \in B,\ b \in \{0,1\}^{s}\}.$$

THM. 17.5-1

ASSUME THE FIXED-UP, $A_1, \ldots, A_m \in \{0,1\}^{n+s}$, $B_1, \ldots, B_\ell \subseteq \{0,1\}^{n+t}$.

LET $\pi : D_1, \ldots, D_h = \psi$ BE A REFUTATION OF

$\hat{A_1}, \ldots, \hat{A_m}, \hat{B_1}, \ldots, \hat{B_\ell}$, S.T. FOR ALL D_i: $CC(D_i) \le T$.

THEN THERE $\exists$ PROTOCOL G FOR $KW[U,V]$

OF SIZE $\le k + 2n$ AND $CC \le T$.

HENCE (THM. 17.4.3) $\exists$ CIRCUIT $C(x_1, \ldots, x_n)$

SEPARATING U FROM V OF SIZE $|C| \le (k+2n)\, 2^{O(T)}$.

[NON-UNIFORM VERSION LATER.]

PRF : DEFINE $\mathcal{G} = (G, las, \delta, F)$ BY:

(1) G : HAS k INNER NODES (= NON-LEAVES)
CORRESP. TO STEPS IN π
AND ADDITIONAL $2k$ LEAVES

labelled (by las) by all $flos$: $u_i := 1 \wedge v_i := 0$
$u_i := 0 \wedge v_i := 1$

(2) $F(u,v) :\longrightarrow$ NODES D_j S.T. $(v, g^u, h^v) \notin D_j$

PLUS LEAVES WITH THE LABEL VALUE
FOR (u,v)

(3) STRATEGY $S(u_i, v_i, +1)$: AT $t := D_j$. DERIVED FROM

D_{i_1}, D_{i_2}, $i_1, i_2 < j$) :

(a) $(u_i, q^u, r^v) \notin D_j$ =>

$S(u_i, v_i, D_j) :=$ / D_{i_1}, $(v_i, q^u, r^v) \notin D_{i_1}$

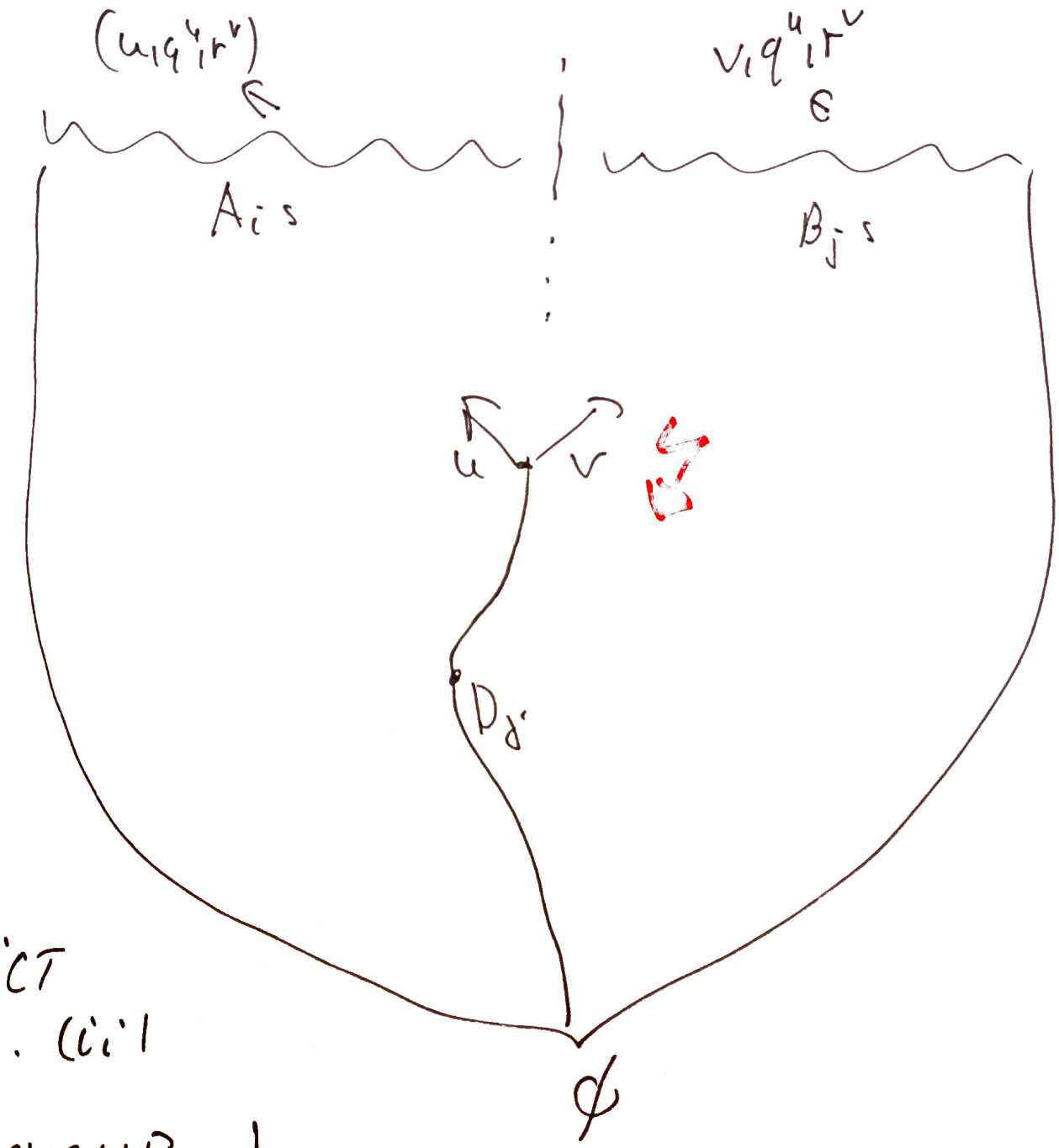
\ D_{i_2}, $(v_i, q^u, r^v) \in D_{i_1}$ (so $\notin D_{i_2}$).

(b) $(u_i, q^u, r^v) \in D_j$ => THE PLAYERS FIND C-TASK (i, i')

$i' \in [n]$, $u_{i'} \neq v_{i'}$, AND

$S(u_i, v_i, D_j) :=$ THE LEAF CORRESP. TO THIS i'

13.



A CONFLICT
(i) vs. (ii)

MUST OCCUR !

17

THM 17.5.1 – NONU VERSION

ADDITIONAL HYPOTHESIS:

- $(u, q^u) \in \bigcap_{j \le u} A_j \;\wedge\; u \le u' \Rightarrow (u', q^{u'}) \in \bigcap_{j \le u'} A_j$.

AND $\boxed{DCC_u(D_i) \le T}$, ALL D_i.

THEN: (a) NONU PROTOCOL $\mathcal{C}$ FOR $KU^m[u,u']$

EXISTS OF SIZE $\le k+u$, $CC \le T$

(b) AND NONU SEPARATING CIRCUIT C

OF SIZE $|C| \le (k+u) \cdot 2^{O(T)}$.

PRF – NONC:

→ ONLY n LEAVES ⇒ $u_i := 1 + u_{i-n}$, $i \in [n]$

→ $F(u,v)$: DEFINED AS BEFORE

→ $S(u,v,t)$: MORE SUBTLE

IN THE 2nd CASE OF THE EARLIER DEF. OF $S(u,v,t)$ PLAYERS MOVE DIFFERENTLY:

CONT'D

THE PLAYERS SOLVE TASK (ii) INSTEAD OF (iii):

↳ EITHER FIND i : $u_1 = 1 \wedge v_i = 0$, AND $S(u,v,D_j)$ IS THAT LEAF

↳ OR $\exists u' \Sigma u$: $(u', q^u, r^v) \notin D_{j_{i-1}}$, AND DEFINE $S(u,v,D_j)$ AS IN CASE 1 BEFORE

↳ D_{i_1}, $(u, q^u, r^v) \notin D_{i_1}$

↳ D_{i_2}, $(u, q^u, r^v) \in D_{i_1}$.

MONOTONICITY HYP. $\Rightarrow (u, q^u) \in \bigcap_j A_j$, SO S WELL-DEFINED.

□.

COROLLARY 17.5.2 LET P BE A PPS OPERATING IN STEPS DERIVED BY BINARY INFERENCE RULES. PUT

$\mathcal{X}_P :=$ SETS DEFINABLE BY LINES IN P-PROOFS

ASSUME: $\Pi CC_n(A) \leq n^{o(1)}$, call $A \in \mathcal{X}_P$ (I ASSUME THE NOAC FI' SET-UP). LET $\xi = n^{1/3}$, $w = n^{2/3}$.

THEN EVERY $\mathcal{X}_P$-REFUTATION OF THE DISJOINTNESS OF $CLIQUE_{n,w}$ and $COLOR_{n,\xi}$ MUST HAVE $\geq 2^{\Omega(n^{1/6})}$ STEPS.

HENCE ALSO ALL P-REF'S OF MUST HAVE $\geq 2^{\Omega(n^{1/6})}$ STEPS.

□

• $n^{o(1)} \leq n^{\varepsilon}$, call $\varepsilon > 0$ for $n >> 1$.

$n^{o(1)}$ .... A FUNCTION $f(n)$ S.T.

"LITTLE o OF 1"

$\forall \varepsilon > 0 \quad \forall n >> 1 :$

$f(n) \leq n^{\varepsilon}$.

THINK ABOUT: $n^{\text{infinitesimal}}$

PRF : $\mathcal{C}_P$ SEMANTIC REF.

17.5.1 ⇔ MONO PROTOCOL G, size $\leq k+n$, $cc \leq T$ ($n^{O(1)}$)

⇔

MONO SEPARATIN CIRCUIT C, $|C| \leq (k+n)2^{O(T)}$

$\leq 2^{n^{O(1)}} \cdot k$

LOWER BOUND FOR : $\geq 2^{\Omega(n^{1/6})}$

RAZBOROV

→ ALON-BOPPANA

⇔

$k \geq 2^{\Omega(n^{1/6})}$

EX. 1 : $\mathcal{K}_R$:= SETS DEFINED BY CLAUSES

(IN ATOMS $\bar{p}, \bar{q}, \bar{r}$)

R - REFUT. OF $A_1, \ldots, B_j$

$\Downarrow$

SEMANTIC $\mathcal{K}_R$ - REFUT. OF $\tilde{A_1}, \ldots, \tilde{B_1}, \ldots$ CLAUSE

$\Downarrow$

THE THM. APPLIES

A CLAUSE:

$$(\ldots p_i \vee \ldots \neg p_j \vee \ldots) \wedge (\ldots \bar{q}\text{-literals} \ldots) \vee (\bar{r}\text{-literals})$$

U ... decides on u
U ... $-i$ $-v$ } 1 BIT

U-player decides = 1 BIT

V-player decides = 1 BIT

SOLVING (i) or (ii) : 2 BITS

SOLVING (iii) : i.e. A CONFLICT IN THE $\bar{p}$-PART

‖

PLAYER ~~THE~~ WHO CLAIMS THAT IT IS

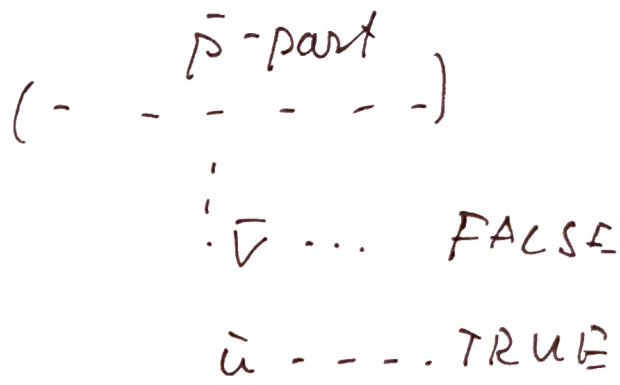
TRUE SENDS $\log n$ BITS TO

IDENTIFY SOME ~~THE~~ TRUE LITERAL : THE u_i or $\neg u_i$

$\pm p_i$

$CC(\text{A CLAUSE}) \leq \log n$

MONO CASE HAVING A CONFLICT IN THE $\bar{p}$-PART:



U-PLAYER CAN DECIDE ON HIS OWN IF

$\exists u' \geq u$, u' ... MAKES IT FALSE = 1 BIT

IF NOT $\Rightarrow$ NECESSARILY TO MAKE IT FALSE WE HAVE TO CHANGE SOME $u_i = 1$ to $u'_i = 0$

$u_i = 1 \wedge u'_i = 0$

U-player needs $\log n$ BITS TO IDENTIFY i

$D^{cc}_u(A\,cl.) \leq \log n$

COR.: ANY R-REFUT. OF $CLIQUE_{n,n^{2/3}} \cup COLOR_{n,n^{1/3}}$

NEEDS $\geq 2^{\Omega(n^{1/6})}$ STEPS. $=$

EX.2: $\mathcal{X}_{LIN}$: SETS DEFINED BY LINEAR EQ'S OVER $\mathbb{F}_2$.

$\Uparrow$

LEC (= LIN. EQUATIONAL CALCULUS)

$$\bar{a}\cdot\bar{p} + \underbrace{\bar{b}\cdot\bar{q}}_{q^u\text{-deltas}} + \bar{c}\cdot\bar{r} = d \qquad , \; \bar{a},\bar{b},\bar{c},d \in \mathbb{F}_q + \bar{r} \in \mathbb{F}_q$$

$\bar{u}/\bar{v}$ determ.: 1 BIT

q^u-deltas: 1 BIT

1 BIT

CONFLICT : USE BINARY SEARCH TO FIND $i : u_i \neq v_i$: $2\log u$ BITS

$$CC(\text{lin. eq.}) \leq 2\cdot\log u$$

NON CASES : ANALOGOUSLY ADAPTED

$$NCC_u(\text{lin. equ.}) \leq 2\log u$$

EX.3 : $\mathcal{C}_{CP}$: SETS DEFINED BY INTEGER LIN. INEQUALITIES

↖ CUTTING PLANES

$$\bar{a}\cdot\bar{p} + \bar{b}\cdot\bar{q} + \bar{c}\cdot\bar{s} \geq d, \quad \bar{a},\bar{b},\bar{c},d \in \mathbb{Z}$$

ASSUME: $-\Pi \leq$ all coeff's $a,b,c,d \leq \Pi$, some $\Pi \in \mathbb{Z}^{2n}$.

↓

Values of any part $\in [-\Pi\cdot n^{O(1)}, \Pi\cdot n^{O(1)}]$

↓

needs $(\log \Pi + O(\log n))$ BITS

TO IDENTIFY

log n rounds

of BINARY SEARCH

$CC(\text{INT. LIN. INEQS.}) \leq (O(\log n)\times\log \Pi)$

$(\log n)$.

29.

A SIMILAR BOUND FOR $RCC_d \leq (\log n)(O(\log n) + \log R)$.

$\Downarrow$ (FIP FOR SEMANTIC DER)
+ (FROM PROTOCOLS TO CIRCUITS)

$\exists$ mono circuit $C(t_{1,1}, \ldots, t_{n,n})$

SEPARATING $CLIQUE_{n,n^{2/3}}$ FROM $COLOR_{n,n^{1/3}}$

OF SIZE

$$|C| \leq (k+n) \cdot (n \cdot n^{O(1)})^{\log n}$$

$\downarrow$ CONT'D

↓ USING THE CIRCUIT LOWER BOUND

k (= the nb. of PROOF STEPS)

$$k \geq \frac{2^{\Omega(n^{1/6})}}{\Pi^{\log n}} \geq 2^{\Omega(n^{1/6})}$$

IF $\Pi \leq 2^{n^{o(1)}}$

↑ A CP-LOWER-BOUND

(WILL REMOVE Π NEXT TIME). //