LECTURE 10

→ FI, part 2

(commun. complexity)

TODAY: BACKGROUND FROM COMMUNICATION COMPL.

Sec. 17.4

$U, V \subseteq \{0,1\}^n$, $I \neq \emptyset$

$R \subseteq U \times V \times I$

$\hookrightarrow$ $\boxed{\text{multifunction}}$ $\iff \forall (u,v) \in U \times V \; \exists i \in I \; R(u,v,i)$

abbr: "$R(u,v) = i$" ... i is one of possibly more values

MULTIFUNCTION

KARCHMER- WIGDERSON GAME

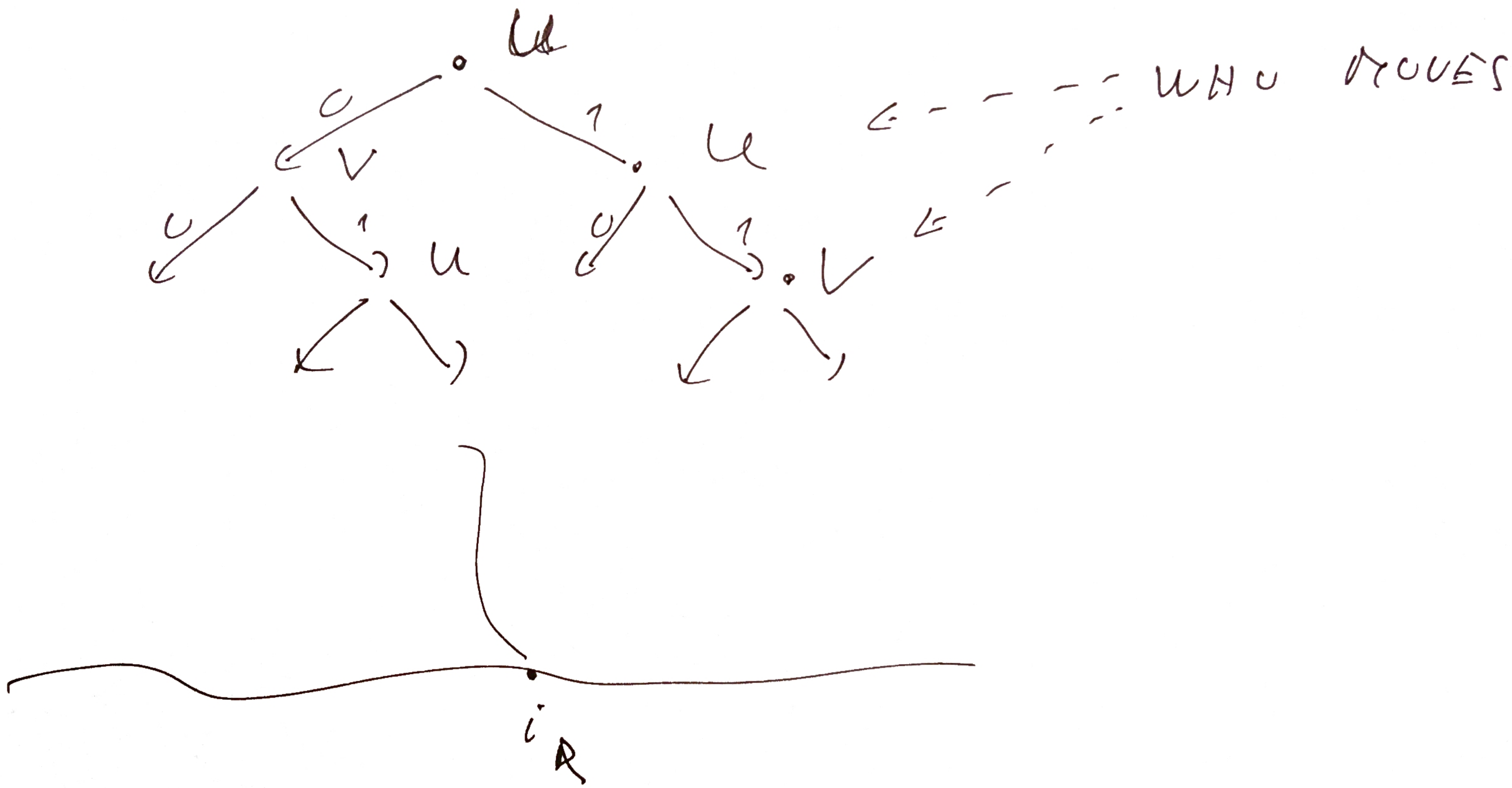
U-player : gets $u \in U$

V-player : gets $v \in V$

the TASK : FIND $i \in I$, $R(u,v) = i$

EXCHANGE BITS OF INFO

KW - PROTOCOL : LABELLED BINARY TREE



A VALID ANSWER

(I.E. : $R(u, v, i)$).

$\boxed{CC(R)} :=_{df}$ min depth of a KW-protocol solving the task

SPECIAL KW-FUNCTION : $U \cap V = \emptyset$

$KW[U,V] : (u,v) \longrightarrow$ any $i \in [n]$, $u_i \neq v_i$.

MONO VERSION : U closed upwards

$KW^m[U,V] : (u,v) \longrightarrow$ any $i \in [n]$, $u_i = 1, v_i = 0$

INDEED WELL-DEFINED

KW-THEOREM (Thm 17.4.1)

ASSUME $U \cap V = \emptyset$.

Then $CC(KW[U,V]) = \min\{ ldp(\varphi), \varphi$ separates U from $V \}$

$\therefore \varphi|U \equiv 1$

$\varphi|V \equiv 0$

Mono version: U CLOSED UPWARDS.

$\Downarrow$

$CC(KW^{m}[U,V]) = \min\{ ldp\, \varphi, \varphi \ldots$

$\ldots\ldots$

AND φ WITHOUT $\neg$.

FLAS (NEG. NORMAL FORM): $\neg$ in FRONT OF ATOMS ONLY

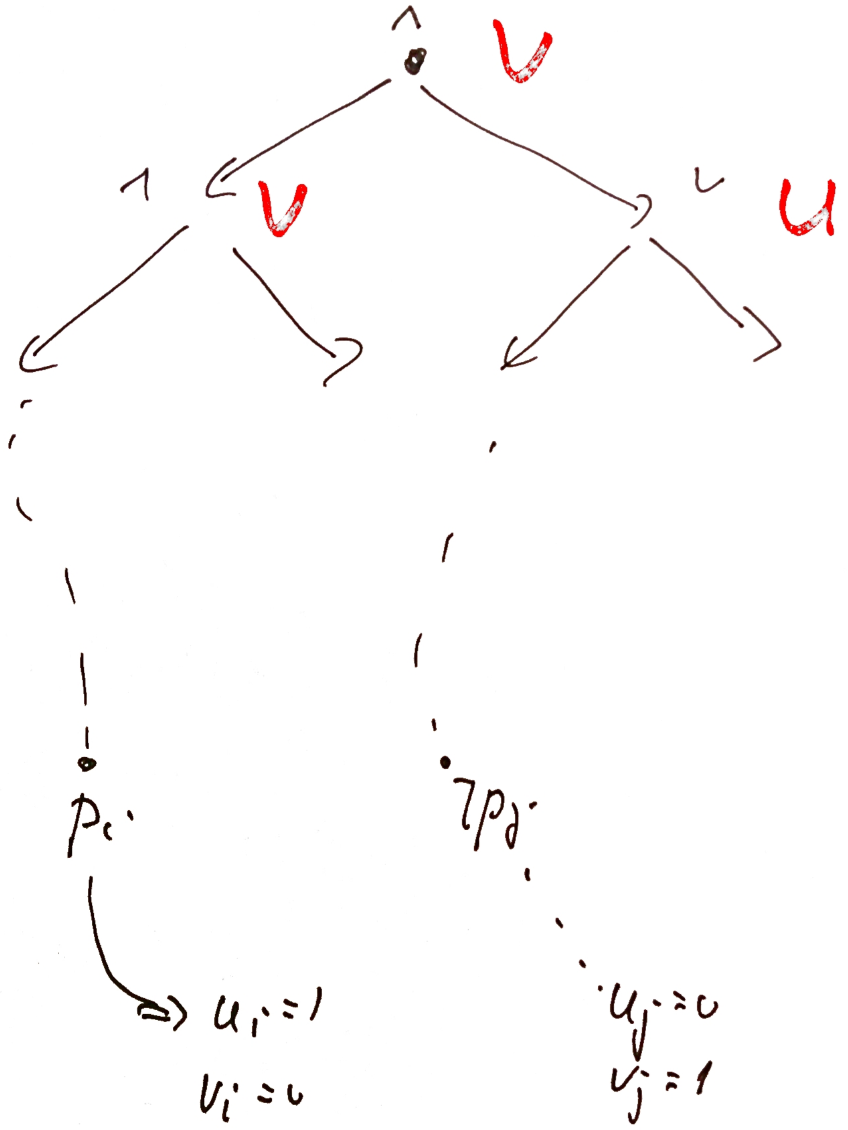
$\boxed{ldp(\varphi)}$: $ldp(\text{atom}, \neg\text{atoms}, \text{constants}) = 0$

$ldp(\varphi_1 \circ \varphi_2) = 1 + \max(ldp(\varphi_1), ldp(\varphi_2))$

LOGICAL DEPTH

PROOF: GIVEN SEPARATING φ USE IT AS A KW-PROTOCOL:

PLAYERS FIND ALWAYS A SUBFLA ψ: $\psi(u)=1$, $\psi(v)=0$



NO $\neg$s

$\Downarrow$

ONLY RESULTS

$u_i = 1 \wedge v_i = 0$

[= MONO VERSION]

GIVEN KW-PROTOCOL OF DEPTH t, CONSTRUCT

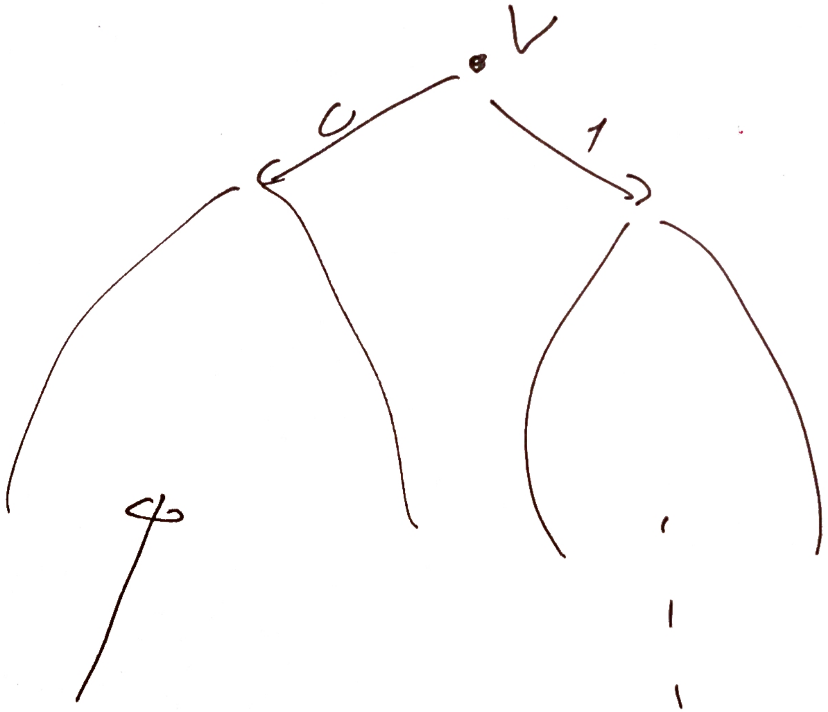
φ BY IND ON t

$t = 0$: EASY

$V_0 = \{v \mid V \text{ sends } 0\}$

$V_1 = \{v \mid V \text{ sends } 1\}$

$t > 0$



$d_p \leq t-1$ protocol

FOR U/V_0

$d_p \leq t-1$

FOR U/V_1

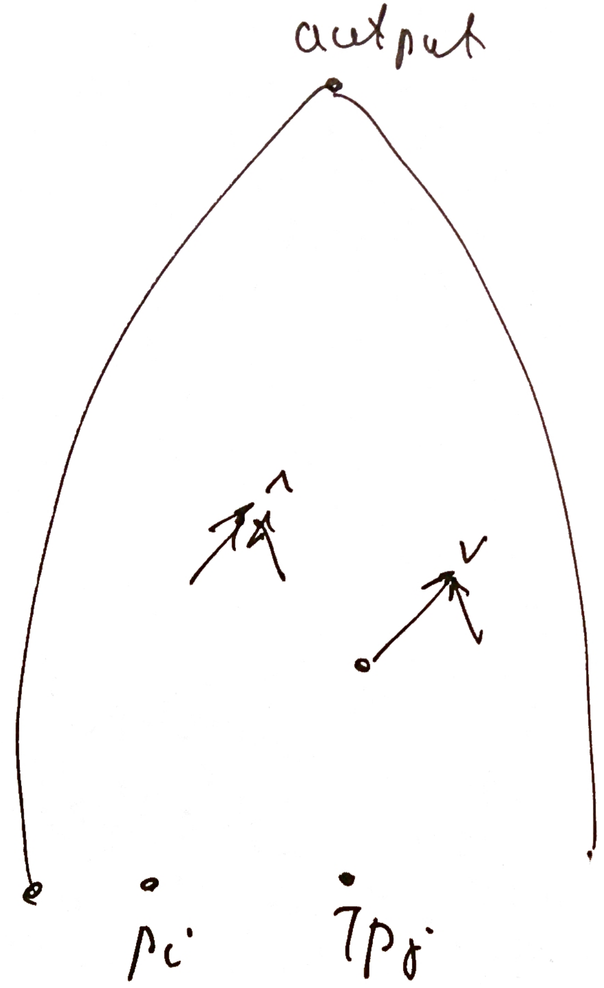
$\therefore$ IND. HYPO: FLAS φ_0, φ_1 $\Rightarrow$

$\varphi_0 \wedge \varphi_1$ works for U/V

$\square$

ASSUME WE HAVE A SEPARATING CIRCUIT C

C:



$\Downarrow$

DAG-LIKE PROTOCOL:

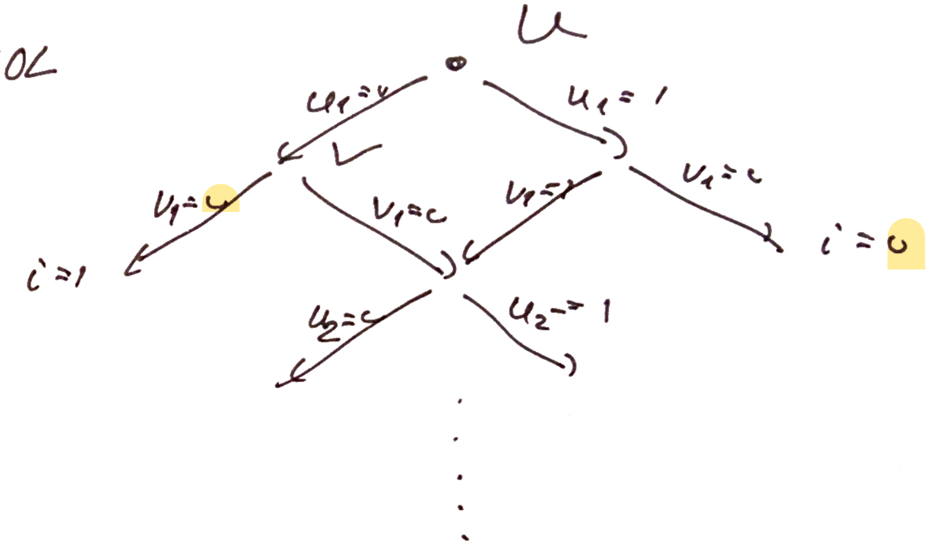
PLAYERS GO TO SUBCIRCUIT D : $D(u)=1$, $D(v)=0$

⋮

LOOKS MORE EFFICIENT.

HOWEVER, THERE IS NO ANALOG FOR THE KW-THM

EX: THE DAG-LIKE PROTOCOL



FINDS i, $u_i \neq v_i$,

FOR ANY PAIR

$u \neq v$.

I.E. IT HAS NOTHING

TO DO WITH

SEPARATIONS OF

SETS

SIZE ~ 5n

$\Rightarrow$ $\boxed{\text{MORAL}}$: DAG-PROTOCOLS NEED TO BE MORE SUBTLE

<u>(LONG) DEF.:</u> A <u>PROTOCOL</u> IS A 4-TUPLE

$$\mathfrak{G} = (G, lab, S, F)$$

WHERE:

(i) $\boxed{G}$ IS A DAG WITH ONE SOURCE (= indeg 0 node) DENOTED $\emptyset$

(ii) $\boxed{lab}$ IS A LABELLING OF LEAVES (= outdeg 0 nodes) BY: (a) $u_i = 1,\ v_i = 0$

OR (b) $u_i = 0,\ v_i = 1$

$\boxed{\text{MONO PROTOCOLS}}$: ONLY labels (a)

↓ CONT'D

(iii) $\boxed{S} : U \times V \times T_0 \longrightarrow G$: STRATEGY

NON-LEAVES OF G

$(u, v, x) \longrightarrow$ some node y that can be reached by a (directed) edge from x

(iv) $\boxed{F(u,v)} \subseteq G$, for all (u,v) : CONSISTENCY CONDITION

(a) $\phi \in F(u,v)$

(b) $x \in F(u,v) \Rightarrow S(u,v,x) \in F(u,v)$

(c) $y \in F(u,v)$ A LEAF $\Rightarrow$ $lab(y)$ is VALID FOR (u,v).

$\downarrow$ CONT'D

SIZE s of $\mathbb{G}$ $:= |G|$

CC ϵ of $\mathbb{G}$ $:=$ CC OF COMPUTING $S(u,v,t)_t$ ~~ANY t~~ AND ~~x~~ $t \in F(u,v)$, ANY t

COMM. COMPL.

$\square$ end of the def.

SUMMARY: $\mathbb{G} = (G, lab, S, F)$

UNDERLYING GRAPH

GIVES ANSWERS AT LEAVES

STRATEGY HOW TO MOVE IN G

IDENTIFIES NODES WHICH LEAD ~~...~~ – VIA S – TO A VALID ANSWER

$|S|$ size

$|\epsilon$ CC$|$

EX: C : SEPARATING CIRCUIT AS A PROTOCOL

G : THE GRAPH OF C , SOURCE = THE OUTPUT GATE

EDGES: FROM A GATE TO ITS FEEDING GATES

LEAVES : INPUTS x_i OR $\neg x_i$.

S : GO TO (LEFT-MOST) SUBCIRCUIT D : $D(u)=1 \wedge D(v)=0$

$F(u,v) :=$ subcircuit D s.t.

lab : input $x_i \longrightarrow$ lab $= (u_i = 1 \wedge v_i = 0)$

$\neg x_i \longrightarrow \; = (u_i = 0 \wedge v_i = 1)$

ONLY THIS HAPPENS WITH MONO C $\Longrightarrow$ MONO PROTOCOL

$S = |C|$

$t = 2$

__Thm (17.4.3)__ $\mathcal{U} \cap \mathcal{V} = \emptyset$, $\mathcal{G}$ a SIZE s AND

CC ϵ ~~ERR~~ PROTOCOL FOR $KW[\mathcal{U}, \mathcal{V}]$.

THEN $\exists$ SEPARATING CIRCUIT C S.T.

(*) $$\boxed{|C| \leq s \cdot 2^{O(\epsilon)}}.$$

IF $\mathcal{U}$ IS CLOSED UPWARDS AND $\mathcal{G}$ IS MONO THEN C IS MONO TOO, OF SIZE (*).

__PRF__: TRICKY IND ARGUMENT, ~1 PAGE THOUGH. READ IT IN THE BOOK TO SEE WHAT IS GOING ON.