ON THE CONTENT OF CLASSICAL PROPOSITIONAL PROOFS

Fabio Massaioli

Classe di Lettere e Filosofia, Scuola Normale Superiore, Pisa, Italy

SNS Logic Group Seminar – May 16th, 2023

THE PROBLEM OF PROOF IDENTITY

When are two proofs essentially the same?

but also

What is a proof? What does it mean to prove?

First explicit formulations by Kreisel (1965) and Prawitz (1971),
the latter together with the

Normalization Conjecture:

«Proofs are essentially the same proof if and only if they have the same normal form.»

THE PROBLEM OF PROOF IDENTITY

Now often known as *Hilbert's 24th problem*:

«Criteria of simplicity, or proof of the greatest simplicity of certain proofs. Develop a theory of the method of proof in mathematics in general. Under a given set of conditions there can be but one simplest proof. Quite generally, if there are two proofs for a theorem, you must keep going until you have derived each from the other, or until it becomes quite evident what variant conditions (and aids) have been used in the two proofs. Given two routes, it is not right to take either of these two or to look for a third; it is necessary to investigate the area lying between the two routes.»

THE PROBLEM OF PROOF IDENTITY

Our point of view:

What is the content of (syntactical) proofs? Which kind of information do they provide, and why does it count as evidence towards some proposition?

Methodology:

- find interesting equivalence relations on syntactical proof systems;
- find canonical representations of the equivalence classes, thus providing:
  - ◇ equational reasoning;
  - ◇ an account of the informational content of proofs.

The extensional approach fails:

set theoretic maps remember at most cardinality, forget structure.

THE PROBLEM OF PROOF IDENTITY

Proof system: a pair $\langle \mathbf{S}, \vdash_{\mathsf{S}} \rangle$

where

$$\vdash_{\mathsf{S}} \subseteq \mathbf{S} \times \mathcal{L}$$

such that

(i) decidable (correctness condition)

(ii) $P \vdash_{\mathsf{S}} A \implies A$ *valid* (soundness)

(iii) possibly the converse (completeness)

THE PROBLEM OF PROOF IDENTITY

Proof system: a pair $\langle \mathbf{S}, \vdash_{\mathsf{S}} \rangle$

where

$$\vdash_{\mathsf{S}} \subseteq \mathbf{S} \times \mathcal{L}$$

such that

(i) decidable (correctness condition)

(ii) $P \vdash_{\mathsf{S}} A \implies A$ *valid* (soundness)

(iii) possibly the converse (completeness)

Cook & Reckhow (1976), more recently Hughes (2006):

$\vdash_{\mathsf{S}}$ should be *decidable in polynomial time.*

NAMED FORMULAS & SEQUENTS

Idea: track atomic occurrences by assigning them unique names

$$\vdash (\underset{x}{\alpha} \wedge \underset{y}{\beta}) \vee \underset{z}{\alpha}, \underset{w}{\overline{\beta}}$$

Technically: *sharing-free* formulas on a countable set of names

$$\tau_1, \tau_2 ::= x \mid \tau_1 \vee \tau_2 \mid \tau_1 \wedge \tau_2 \qquad (x \in \mathcal{N},\ \tau_1, \tau_2 \textit{ share no names})$$

$$\overline{x} = x \qquad \overline{\tau_1 \vee \tau_2} = \overline{\tau_1} \wedge \overline{\tau_2} \qquad \overline{\tau_1 \wedge \tau_2} = \overline{\tau_1} \vee \overline{\tau_2}$$

Sequents: *sharing-free,* finite sets of formulas on names, plus an atom assignment

$$\Gamma = \langle \phi_\Gamma, \mathsf{at}_\Gamma \rangle \qquad \phi_\Gamma = \{\tau_1, \ldots, \tau_n\} \qquad \mathsf{at}_\Gamma : \mathsf{names}(\phi_\Gamma) \to \mathcal{A}$$

$$\Gamma, \Delta = \langle \phi_\Gamma \cup \phi_\Delta, \mathsf{at}_\Gamma \cup \mathsf{at}_\Delta \rangle \qquad \overline{\Gamma} = \langle \overline{\phi_\Gamma}, \overline{\mathsf{at}_\Gamma} \rangle \qquad A = \langle \{\tau\}, \mathsf{at}_A \rangle$$

GS4 ON NAMED SEQUENTS

Identities:

$$\frac{}{\vdash \Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}}\,\mathsf{ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, \overline{A}}{\vdash \Gamma}\,\mathsf{cut}$$

Logical rules:

$$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B}\,\vee \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B}\,\wedge$$

As a proof system:

$\langle \mathbf{ST}, \vdash_{\mathsf{GS4}} \rangle$ where $\mathbf{ST}$ is the set of all finite sequent-labeled binary trees, and
$P \vdash_{\mathsf{GS4}} \Gamma \iff P$ *with root* Γ *constructed by the rules above.*

ATOMIC COMMITMENTS

An interpretation of sequents (and formulas) as sets of sets of names:

$$\mathsf{AC}(\Gamma) \subseteq \mathscr{P}(\mathcal{N})$$

$\mathfrak{c} \in \mathsf{AC}(\Gamma)$ is a *commitment*
represents a disjunctive clause
in the *atomic occurrences* of Γ

satisfying the following equations:

$$\mathsf{AC}(\Gamma) = \{\, \mathsf{names}(\Gamma) \,\} \text{ for } \Gamma \text{ atomic} \qquad \textit{(comm-at)}$$

$$\mathsf{AC}(\Gamma, A \vee B) = \mathsf{AC}(\Gamma, A, B) \qquad \textit{(comm-or)}$$

$$\mathsf{AC}(\Gamma, A \wedge B) = \mathsf{AC}(\Gamma, A) \cup \mathsf{AC}(\Gamma, B) \qquad \textit{(comm-and)}$$

ATOMIC COMMITMENTS

Definition (Clique product). For all sets $S, T \subseteq \mathcal{P}(\mathcal{N})$ of commitments let

$$S \uplus T = \{X \cup Y \mid X \in S, Y \in T\}$$

Property. *The operator thus defined enjoys*

Commutativity:

$$S \uplus T = T \uplus S$$

Associativity:

$$(S \uplus T) \uplus U = S \uplus (T \uplus U)$$

Identity:

$$S \uplus \{\emptyset\} = S$$

Absorption:

$$S \uplus \emptyset = \emptyset$$

Distributivity over unions:

$$(S \cup T) \uplus U = (S \uplus U) \cup (T \uplus U)$$

ATOMIC COMMITMENTS

Definition. By induction on the sharing-free formulas on names:

$$\mathsf{AC}(x) = \{\,\{x\}\,\} \qquad \mathsf{AC}(\tau_1 \vee \tau_2) = \mathsf{AC}(\tau_1) \uplus \mathsf{AC}(\tau_2) \qquad \mathsf{AC}(\tau_1 \wedge \tau_2) = \mathsf{AC}(\tau_1) \cup \mathsf{AC}(\tau_2)$$

For any sequent Γ let

$$\mathsf{AC}(\Gamma) = \uplus_{\tau \in \phi_\Gamma} \mathsf{AC}(\tau)$$

Lemma. *The function* AC *satisfies the equations (comm-at), (comm-or), (comm-and), and additionally*

$$\mathsf{AC}(\Gamma, \Delta) = \mathsf{AC}(\Gamma) \uplus \mathsf{AC}(\Delta)$$

$$\mathsf{AC}(\Gamma) = \{\mathfrak{c} \cap \mathsf{names}(\Gamma) \mid \mathfrak{c} \in \mathsf{AC}(\Gamma, \Delta)\}$$

$$\mathsf{AC}(\Gamma) = \{\mathfrak{c} \setminus \mathsf{names}(\Delta) \mid \mathfrak{c} \in \mathsf{AC}(\Gamma, \Delta)\}$$

THE PROOF SYSTEM CG

Definition. *Commitment graphs* on a sequent Γ are

hypergraphs $G = \langle V_G, E_G \rangle$

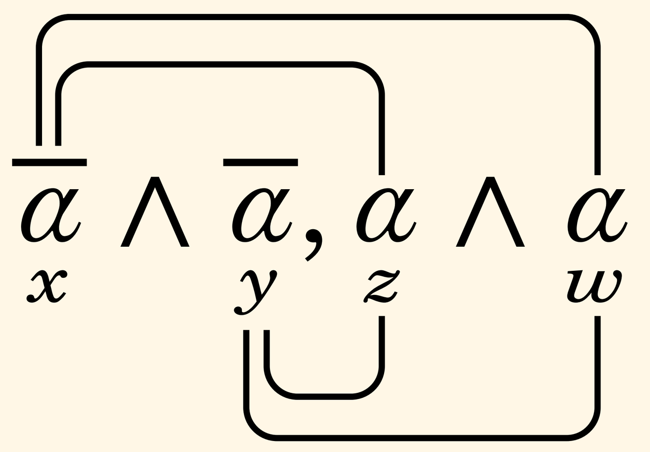
on the names of Γ, i.e.

– the *vertices* $V_G = \mathsf{names}(\Gamma)$ are the names of Γ;
– the *hyperedges* $E_G \subseteq \mathscr{P}(V_G)$ are *non-empty* sets of names of Γ;

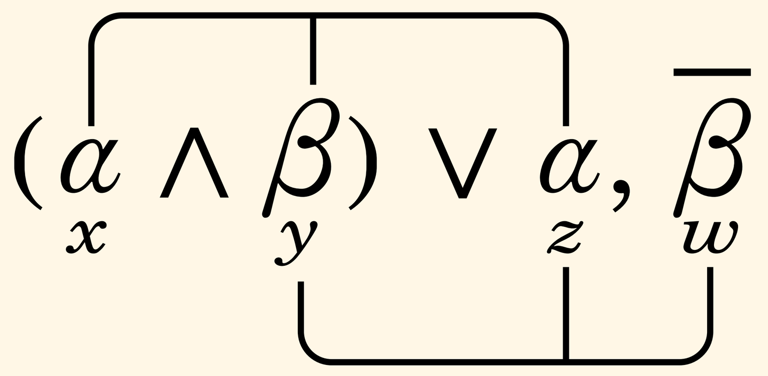
such that every edge is *maximal w.r.t. inclusion* within E_G,
that is we have for all $\mathfrak{c}, \mathfrak{d} \in E_G$

$$\mathfrak{c} \subseteq \mathfrak{d} \implies \mathfrak{c} = \mathfrak{d}.$$

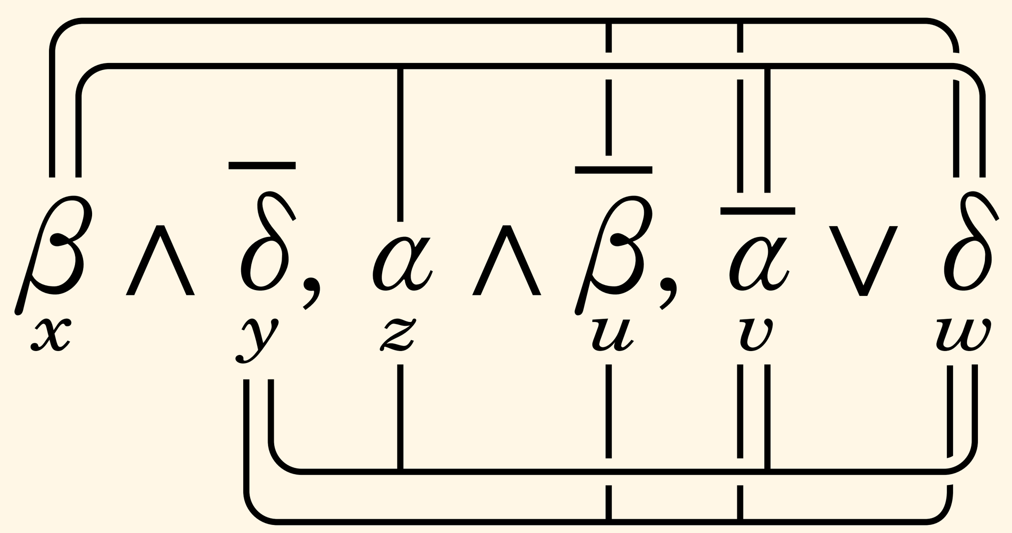
THE PROOF SYSTEM CG



$$\frac{\overparen{\overline{\alpha}_x, \alpha_z} \quad \overparen{\overline{\alpha}_x, \alpha_w} \quad \overparen{\overline{\alpha}_y, \alpha_z} \quad \overparen{\overline{\alpha}_y, \alpha_w}}{\overline{\alpha}_x \wedge \overline{\alpha}_y, \alpha_z \wedge \alpha_w}$$



$$\frac{\overparen{\alpha_x, \beta_y, \alpha_z} \quad \overparen{\beta_y, \alpha_z, \overline{\beta}_w}}{(\alpha_x \wedge \beta_y) \vee \alpha_z, \overline{\beta}_w}$$



$$\frac{\overparen{\beta_x, \alpha_z, \overline{\alpha}_v, \delta_w} \quad \overparen{\beta_x, \overline{\beta}_u, \overline{\alpha}_v, \delta_w} \quad \overparen{\overline{\delta}_y, \alpha_z, \overline{\alpha}_v, \delta_w} \quad \overparen{\overline{\delta}_y, \overline{\beta}_u, \overline{\alpha}_v, \delta_w}}{\beta_x \wedge \overline{\delta}_y, \alpha_z \wedge \overline{\beta}_u, \overline{\alpha}_v \vee \delta_w}$$

THE PROOF SYSTEM CG

Definition. The proof system CG is specified by the pair $\langle \mathbf{NG}, \vdash_{\mathsf{CG}} \rangle$ where

$\mathbf{NG}$ is the set of all *finite hypergraphs* on the set $\mathcal{N}$ of names, and

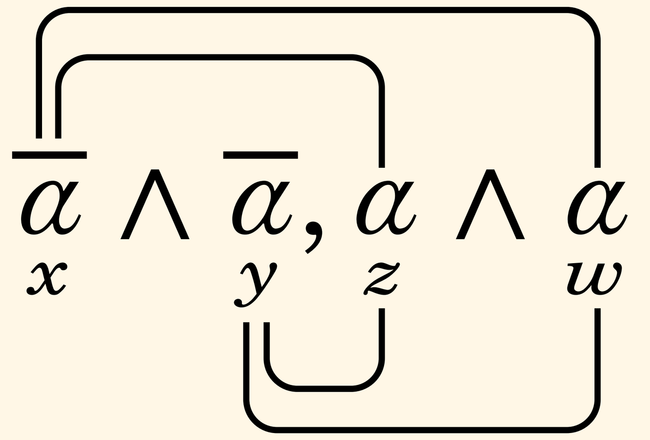
for all hypergraphs $G \in \mathbf{NG}$ and sequents Γ, $G \vdash_{\mathsf{CG}} \Gamma$ if and only if

(i) G is a commitment graph on Γ *(relevance)*

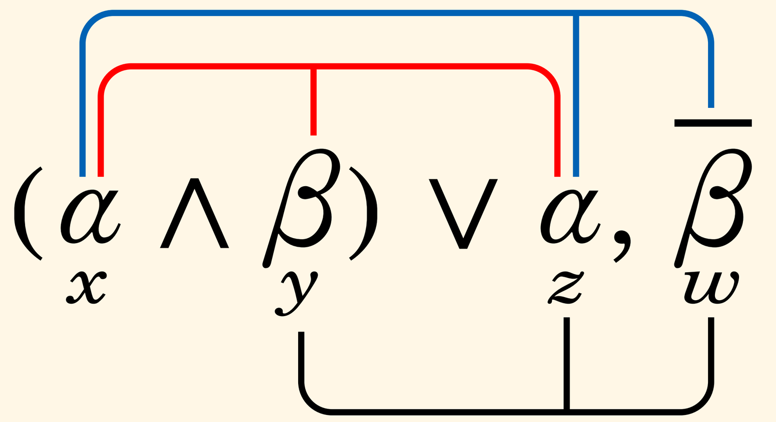
(ii) $\mathsf{AC}(\Gamma) \subseteq E_G$ *(adequacy)*
(each atomic commitment of Γ is an hyperedge of G)

(iii) for all $\mathfrak{c} \in E_G$ there are $x, y \in \mathfrak{c}$ such that $\Gamma[x] = \overline{\Gamma[y]}$ *(validity)*
(each commitment in G links at least one pair of dual atoms)

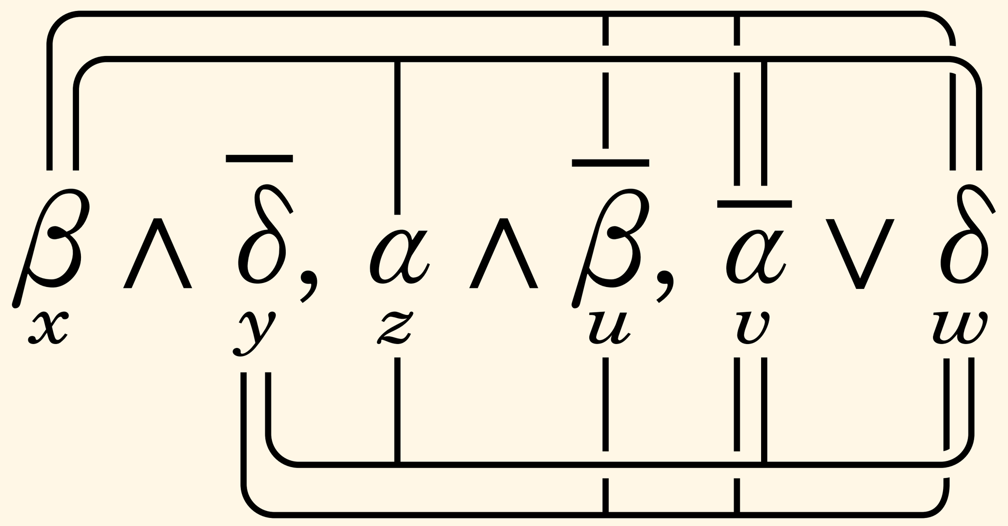
THE PROOF SYSTEM CG



$$\frac{\overbrace{\bar{\alpha}_x, \alpha_z} \quad \overbrace{\bar{\alpha}_x, \alpha_w} \quad \overbrace{\bar{\alpha}_y, \alpha_z} \quad \overbrace{\bar{\alpha}_y, \alpha_w}}{\bar{\alpha}_x \wedge \bar{\alpha}_y, \alpha_z \wedge \alpha_w}$$



$$\frac{\overbrace{\alpha_x, \beta_y, \alpha_z} \quad \overbrace{\beta_y, \alpha_z, \bar{\beta}_w}}{(\alpha_x \wedge \beta_y) \vee \alpha_z, \bar{\beta}_w} \qquad \overbrace{\alpha_x, \alpha_z, \bar{\beta}_w}^{?}$$



$$\frac{\overbrace{\beta_x, \alpha_z, \bar{\alpha}_v, \delta_w} \quad \overbrace{\beta_x, \bar{\beta}_u, \bar{\alpha}_v, \delta_w} \quad \overbrace{\bar{\delta}_y, \alpha_z, \bar{\alpha}_v, \delta_w} \quad \overbrace{\bar{\delta}_y, \bar{\beta}_u, \bar{\alpha}_v, \delta_w}}{\beta_x \wedge \bar{\delta}_y, \alpha_z \wedge \bar{\beta}_u, \bar{\alpha}_v \vee \delta_w}$$

THE PROOF SYSTEM CG

Lemma (Correctness-preserving operations). *The* CG*-correctness predicate is closed under the following rules:*

$$\frac{\Gamma \text{ atomic}}{\mathsf{CG}(\Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}) \vdash_{\mathsf{CG}} \Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}}\ \mathsf{ax} \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A, B}{G \vdash_{\mathsf{CG}} \Gamma, A \vee B}\ {\downarrow}\vee \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \vee B}{G \vdash_{\mathsf{CG}} \Gamma, A, B}\ {\uparrow}\vee$$

$$\frac{G \vdash_{\mathsf{CG}} \Gamma, A \quad H \vdash_{\mathsf{CG}} \Gamma, B}{G \sqcup H \vdash_{\mathsf{CG}} \Gamma, A \wedge B}\ {\downarrow}\wedge \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \wedge B}{G{\upharpoonright}_{\Gamma, A} \vdash_{\mathsf{CG}} \Gamma, A}\ {\uparrow}\wedge_{\mathsf{l}} \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \wedge B}{G{\upharpoonright}_{\Gamma, B} \vdash_{\mathsf{CG}} \Gamma, B}\ {\uparrow}\wedge_{\mathsf{r}}$$

THE PROOF SYSTEM CG

Lemma (Correctness-preserving operations). *The* CG*-correctness predicate is closed under the following rules:*

$$\frac{\Gamma \text{ atomic}}{\mathsf{CG}(\Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}) \vdash_{\mathsf{CG}} \Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}}\ \mathsf{ax} \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A, B}{G \vdash_{\mathsf{CG}} \Gamma, A \vee B}\ {\downarrow}\vee \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \vee B}{G \vdash_{\mathsf{CG}} \Gamma, A, B}\ {\uparrow}\vee$$

$$\frac{G \vdash_{\mathsf{CG}} \Gamma, A \quad H \vdash_{\mathsf{CG}} \Gamma, B}{G \sqcup H \vdash_{\mathsf{CG}} \Gamma, A \wedge B}\ {\downarrow}\wedge \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \wedge B}{G{\upharpoonright}_{\Gamma, A} \vdash_{\mathsf{CG}} \Gamma, A}\ {\uparrow}\wedge_{\mathsf{l}} \qquad \frac{G \vdash_{\mathsf{CG}} \Gamma, A \wedge B}{G{\upharpoonright}_{\Gamma, B} \vdash_{\mathsf{CG}} \Gamma, B}\ {\uparrow}\wedge_{\mathsf{r}}$$

where

$\mathsf{CG}(\Gamma) = \langle \mathsf{names}(\Gamma), \mathsf{AC}(\Gamma) \rangle$ is the graph formed from the atomic commitments of Γ;

$G \sqcup H = \langle V_G \cup V_H, E_G \cup E_H \rangle$ denotes hypergraph union;

$G{\upharpoonright}_{\Gamma} = \langle V_G \cap \mathsf{names}(\Gamma), \{\mathfrak{c} \in E_G \mid \mathfrak{c} \subseteq \mathsf{names}(\Gamma)\} \rangle$ denotes hypergraph restriction.

MAIN RESULTS (PART I)

Corollary. *For all sequents* Γ,

$$\vdash_{\mathsf{CG}} \Gamma \iff \vdash_{\mathsf{GS4}} \Gamma$$

Theorem. *The system* CG *is sound and complete w.r.t. classical propositional validity.*

MAIN RESULTS (PART I)

Lemma. $\vdash_{\mathsf{CG}} \Gamma \implies \mathsf{CG}(\Gamma) \vdash_{\mathsf{CG}} \Gamma.$

Definition (Strict adequacy). Let $G \vdash_{\mathsf{CGs}} \Gamma$ if and only if $G \vdash_{\mathsf{CG}} \Gamma$ and $E_G = \mathsf{AC}(\Gamma)$.

MAIN RESULTS (PART I)

Lemma. $\vdash_{\mathsf{CG}} \Gamma \implies \mathsf{CG}(\Gamma) \vdash_{\mathsf{CG}} \Gamma$.

Definition (Strict adequacy). Let $G \vdash_{\mathsf{CGs}} \Gamma$ if and only if $G \vdash_{\mathsf{CG}} \Gamma$ and $E_G = \mathsf{AC}(\Gamma)$.

Property (Decomposition). *If* $G \vdash_{\mathsf{CGs}} \Gamma, A \wedge B$, *then*

$$G = (G{\upharpoonright}_{\Gamma,A}) \sqcup (G{\upharpoonright}_{\Gamma,B}).$$

Property (Uniqueness). *If* $G \vdash_{\mathsf{CGs}} \Gamma$ *and* $H \vdash_{\mathsf{CGs}} \Gamma$, *then* $G = H$.

MAIN RESULTS (PART I)

Lemma. $\vdash_{\mathsf{CG}} \Gamma \implies \mathsf{CG}(\Gamma) \vdash_{\mathsf{CG}} \Gamma$.

Definition (Strict adequacy). Let $G \vdash_{\mathsf{CGs}} \Gamma$ if and only if $G \vdash_{\mathsf{CG}} \Gamma$ and $E_G = \mathsf{AC}(\Gamma)$.

Property (Decomposition). *If $G \vdash_{\mathsf{CGs}} \Gamma, A \wedge B$, then*

$$G = (G\restriction_{\Gamma,A}) \sqcup (G\restriction_{\Gamma,B}).$$

Property (Uniqueness). *If $G \vdash_{\mathsf{CGs}} \Gamma$ and $H \vdash_{\mathsf{CGs}} \Gamma$, then $G = H$.*

Theorem. CG *(resp. CGs) is a proof system in the sense of Cook & Reckhow.*

THE PROOF SYSTEM WCG

Definition. *Witnessed commitment graphs* on a sequent Γ are

pairs $\mathbf{G} = \langle V_{\mathbf{G}}, \underset{\mathbf{G}}{\prec} \rangle$

with $\underset{\mathbf{G}}{\prec} \subseteq \mathscr{P}(V_{\mathbf{G}}) \times \mathscr{P}(V_{\mathbf{G}})$ a relation between subsets of $V_{\mathbf{G}}$

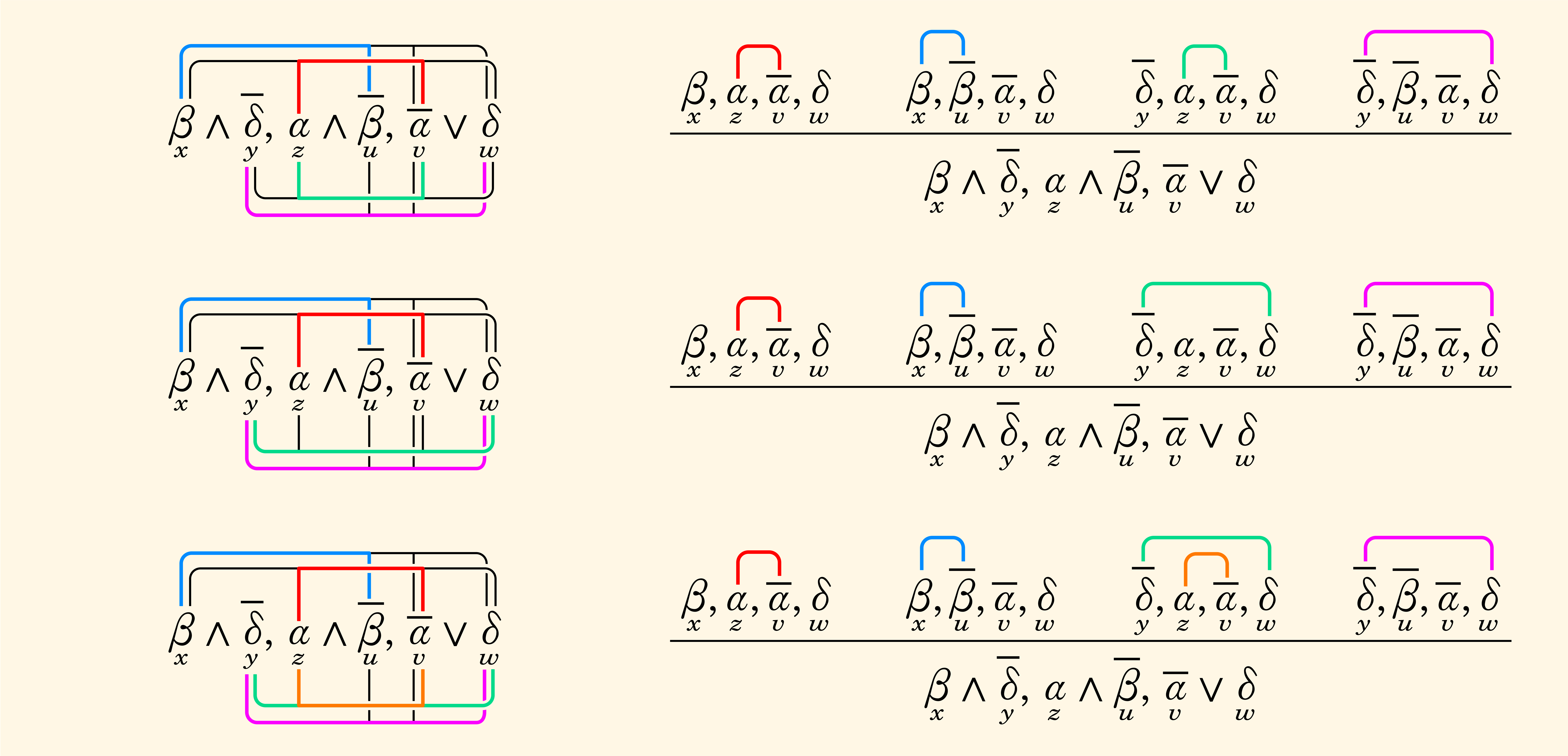
such that

- $\langle V_{\mathbf{G}}, E_{\mathbf{G}} \rangle$ is a commitment graph on Γ;
- for each commitment $\mathfrak{c} \in E_{\mathbf{G}}$, $\langle \mathfrak{c}, W_{\mathbf{G}}(\mathfrak{c}) \rangle$ is a simple graph;

where

- $E_{\mathbf{G}} = \{\mathfrak{c} \mid \exists \mathfrak{w}.\, \mathfrak{c} \underset{\mathbf{G}}{\prec} \mathfrak{w}\}$ is the set of all *commitments* in $\mathbf{G}$;
- $W_{\mathbf{G}}(\mathfrak{c}) = \{\mathfrak{w} \mid \mathfrak{c} \underset{\mathbf{G}}{\prec} \mathfrak{w}\}$ is the set of all *witnesses* associated to a commitment $\mathfrak{c}$ in $\mathbf{G}$.

THE PROOF SYSTEM WCG



THE PROOF SYSTEM WCG

Definition. The proof system WCG is specified by the pair $\langle \mathbf{WNG}, \vdash_{\mathsf{WCG}} \rangle$ where

$\mathbf{WNG}$ is the set of all *finite witnessed graphs* on the set $\mathcal{N}$ of names, and

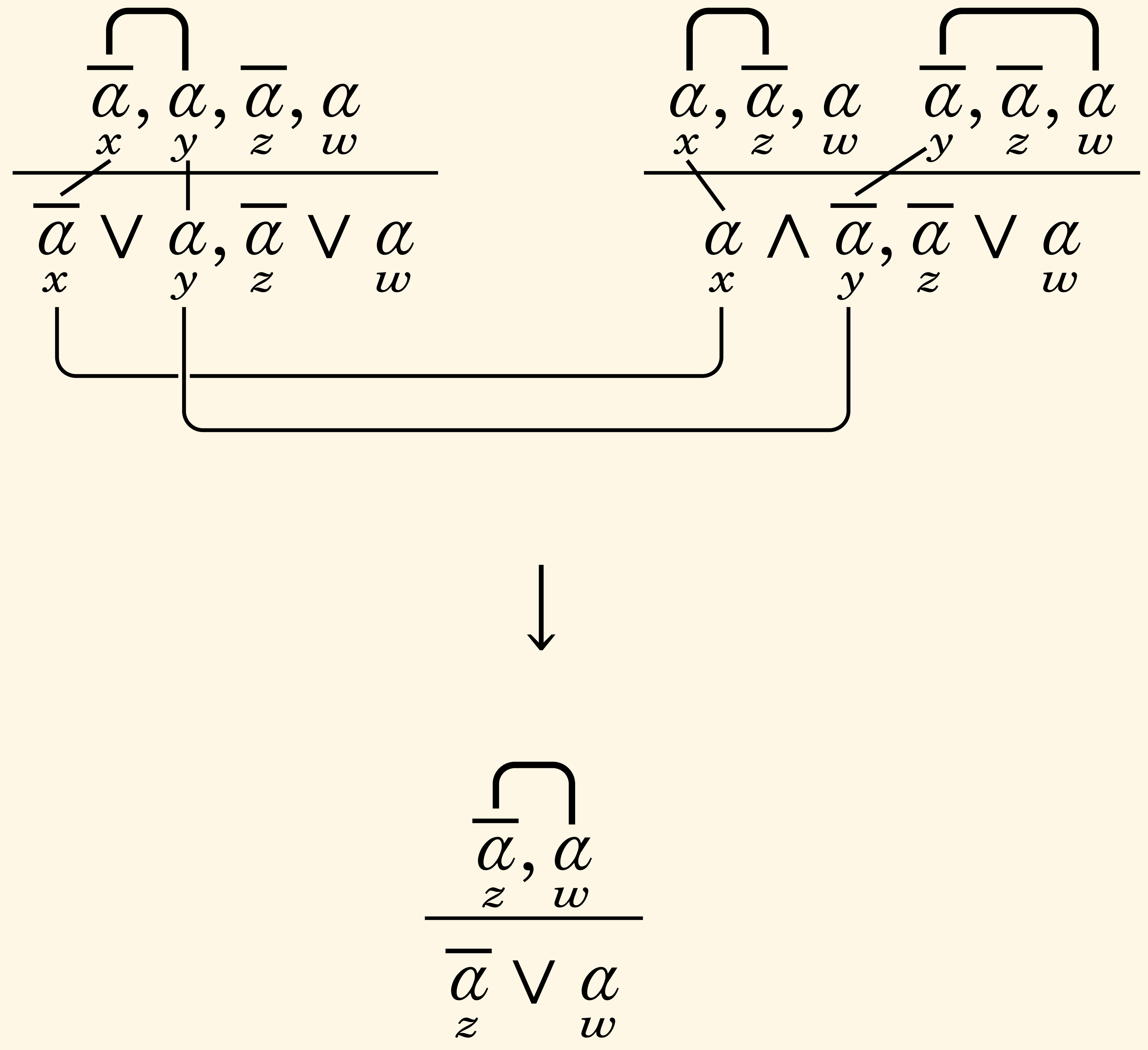
for all hypergraphs $\mathbf{G} \in \mathbf{WNG}$ and sequents Γ, $\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma$ if and only if

(i) $\mathbf{G}$ is a witnessed commitment graph on Γ *(relevance)*

(ii) $E_G = \mathsf{AC}(\Gamma)$ *(strict adequacy)*
(the atomic commitment of Γ are those in $\mathbf{G}$)

(iii) if $\mathfrak{c} \underset{\mathbf{G}}{\prec} \{x, y\}$ then $\Gamma[x] = \overline{\Gamma[y]}$ *(reliability)*
(witnesses link dual atoms)

CUT-ELIMINATION FOR WCG



CUT-ELIMINATION FOR WCG

Definition (Relativized witnessing). Let $\mathbf{G}$ be a witnessed commitment graph, $I \subseteq \mathcal{N}$ an arbitrary set of names.

Write $\mathfrak{c} \underset{\mathbf{G} \setminus I}{\prec} \mathfrak{w}$ iff there is $\mathfrak{d} \underset{\mathbf{G}}{\prec} \mathfrak{w}$ such that $\mathfrak{c} = \mathfrak{d} \setminus I$.

CUT-ELIMINATION FOR WCG

Definition (Alternating path). Let $\mathbf{G}, \mathbf{H}$ be any two witnessed commitment graphs, $I \subseteq \mathcal{N}$ an arbitrary set of names.

An *alternating path witnessing* $\mathfrak{c}$ *between* $\mathbf{G}$ *and* $\mathbf{H}$ *through the interface* I is

a sequence $x_1, \dots, x_n \in V_{\mathbf{G}} \cup V_{\mathbf{H}}$ of *pairwise distinct* vertices of $\mathbf{G}, \mathbf{H}$

such that

(i) $x_2, \dots, x_{n-1} \in I$ (all internal vertices belong to the interface), and

(ii) *either* $\mathfrak{c} \underset{\mathbf{G} \setminus I}{\prec} \mathfrak{w}_i$ for all odd i and $\mathfrak{c} \underset{\mathbf{H} \setminus I}{\prec} \mathfrak{w}_i$ for all even i,
or $\mathfrak{c} \underset{\mathbf{G} \setminus I}{\prec} \mathfrak{w}_i$ for all even i and $\mathfrak{c} \underset{\mathbf{H} \setminus I}{\prec} \mathfrak{w}_i$ for all odd i,

where $\mathfrak{w}_i = \{x_i, x_{i+1}\}$ for all $1 \leq i < n$.

We say that an alternating path is *complete* iff $x_1, x_n \notin I$,
i.e. if its endpoints lie outside the interface.

CUT-ELIMINATION FOR WCG

Definition (Composition of WCGs). Let $\mathbf{G}, \mathbf{H}$ be any two witnessed commitment graphs, $I \subseteq \mathcal{N}$ an arbitrary set of names.

Define the *composite of* $\mathbf{G}$ *and* $\mathbf{H}$ *on the interface* I as the WCG

$$\mathbf{G} \odot_I \mathbf{H} = \langle V, \prec \rangle$$

where

$V = (V_{\mathbf{G}} \cup V_{\mathbf{H}}) \setminus I$, and

$\mathfrak{c} \prec \{x, y\}$ iff there is an *alternating path* $x_1, \ldots, x_n$ *witnessing* $\mathfrak{c}$ *between* $\mathbf{G}$ *and* $\mathbf{H}$ *through the interface* I such that $x_1 = x$ and $x_n = y$.

CUT-ELIMINATION FOR WCG

Theorem (Hauptsatz). *The* WCG*-correctness predicate is closed under composition:*

$$\dfrac{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, A \qquad \mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, \overline{A}}{\mathbf{G} \odot_A \mathbf{H} \vdash_{\mathsf{WCG}} \Gamma}\,\mathsf{cut}$$

Proof sketch. By induction on the complexity of the conclusion Γ.

$$\dfrac{\dfrac{\dfrac{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma', B \vee C, A}{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma', B, C, A}\,\uparrow\vee \qquad \dfrac{\mathbf{H} \vdash_{\mathsf{WCG}} \Gamma', B \vee C, \overline{A}}{\mathbf{H} \vdash_{\mathsf{WCG}} \Gamma', B, C, \overline{A}}\,\uparrow\vee}{\mathbf{G} \odot_A \mathbf{H} \vdash_{\mathsf{WCG}} \Gamma', B, C}\,\mathsf{cut}}{\mathbf{G} \odot_A \mathbf{H} \vdash_{\mathsf{WCG}} \Gamma', B \vee C}\,\downarrow\vee$$

CUT-ELIMINATION FOR WCG

Theorem (Hauptsatz). *The* WCG*-correctness predicate is closed under composition:*

$$\frac{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, A \quad \mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, \overline{A}}{\mathbf{G} \odot_A \mathbf{H} \vdash_{\mathsf{WCG}} \Gamma} \text{cut}$$

Proof sketch. By induction on the complexity of the conclusion Γ.

$$\dfrac{\dfrac{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma', B \wedge C, A}{\mathbf{G}{\upharpoonright}_{\Gamma', B, A} \vdash_{\mathsf{WCG}} \Gamma', B, A} {\uparrow}\wedge_{\mathsf{l}} \quad \dfrac{\mathbf{H} \vdash_{\mathsf{WCG}} \Gamma', B \wedge C, \overline{A}}{\mathbf{H}{\upharpoonright}_{\Gamma', B, \overline{A}} \vdash_{\mathsf{WCG}} \Gamma', B, \overline{A}} {\uparrow}\wedge_{\mathsf{l}}}{\dfrac{(\mathbf{G}{\upharpoonright}_{\Gamma', B, A}) \odot_A (\mathbf{H}{\upharpoonright}_{\Gamma', B, \overline{A}}) \vdash_{\mathsf{WCG}} \Gamma', B}{(\mathbf{G} \odot_A \mathbf{H}){\upharpoonright}_{\Gamma', B} \vdash_{\mathsf{WCG}} \Gamma', B} =} \text{cut}$$

CUT-ELIMINATION FOR WCG

Theorem (Hauptsatz). *The* WCG*-correctness predicate is closed under composition:*

$$\frac{\mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, A \quad \mathbf{G} \vdash_{\mathsf{WCG}} \Gamma, \overline{A}}{\mathbf{G} \odot_A \mathbf{H} \vdash_{\mathsf{WCG}} \Gamma}\,\mathsf{cut}$$

Proof sketch. By induction on the complexity of the conclusion Γ.

For atomic Γ, construct a complete alternating path
and prove reliability (hard).

WITNESSED GS4

Identities:

$$\frac{}{x, y \vdash \Gamma, \underset{x}{\overline{\alpha}}, \underset{y}{\alpha}}\ \text{w-ax} \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, \overline{A}}{\vdash \Gamma}\ \text{cut}$$

Structural rules:

$$\frac{\vdash \Gamma \quad \vdash \Gamma}{\vdash \Gamma}\ \sqcup$$

Logical rules:

$$\frac{\vdash \Gamma, A, B}{\vdash \Gamma, A \vee B}\ \vee \qquad \frac{\vdash \Gamma, A \quad \vdash \Gamma, B}{\vdash \Gamma, A \wedge B}\ \wedge$$

MAIN RESULTS (PART II)

Theorem. *There is a cut-elimination procedure for* WGS4 *that preserves the interpretation of* WGS4 *derivations as* WCG *proofs.*

Proof sketch. By induction on the height of the derivation. Permute all logical rules below cuts until they are reduced to atomic contexts, then compute the composition in WCG and reconstruct a WGS4 derivation using axioms and superpositions.

Theorem. *Interpretation in* WCG *identifies* WGS4 *derivations up to*

(i) arbitrary permutations of logical rules;
(ii) commutativity, associativity and idempotency of superpositions;
(iii) cut-elimination.

RELATED WORK

WCG and its composition algorithm are strongly related with Andrews' system of refutations by matings (Andrews 1976, 1980), as well as with Lamarche & Straßburger's system of classical proof-nets (Lamarche & Straßburger 2005, Straßburger 2011), known as $\mathbb{B}$*-nets*.

In contrast with WCG, $\mathbb{B}$*-nets*

– fail to be a proof system in the sense of Cook & Reckhow;

– are not invariant under any known cut-elimination procedure, either for WGS4 or for more traditional formulations of classical sequent calculus;

– are sequentializable in multiplicative sequent calculus but not in WGS4 (permutations of conjunction rules are not identities).

The theory of proof equivalence induced by $\mathbb{B}$*-nets* is *incomparable* with the one induced by WCG.

FUTURE WORK

WCG can interpret multiplicative style sequent calculi:
which proofs are identical under this interpretation?

Relationship with known cut-elimination procedures?

Complete cut-reduction procedure?

The composition algorithms tracks information attached to witness edges:

What about proper axioms / provability in theories?

What about extra-logical reasoning?

REFERENCES

Andrews, P. B., *Refutations by Matings*. IEEE Trans. Comput. **25**(8), 801–807 (1976)

Andrews, P. B., *Transforming matings into natural deduction proofs*. In: Bibel, W. and Kowalski, R. (eds.) 5th Conference on Automated Deduction, pp. 281–292. Springer Berlin Heidelberg (1980)

Cook, S. A. and Reckhow, R. A., *The relative efficiency of propositional proof systems.* The Journal of Symbolic Logic **44**(1), 36–50 (1979)

Hughes, D. J., *A minimal sequent calculus free of structural rules.* Annals of Pure and Applied Logic **161**(10), 1244–1253 (2010)

Hughes, D. J., *Proofs without Syntax*. Annals of Mathematics **164**(3), 1065–1079 (2006)

Hughes, D. J., *Towards Hilbert's 24th Problem: Combinatorial Proof Invariants*. Electronic Notes in Theoretical Computer Science **165**, 37–63 (2006)

Lamarche, F. and Straßburger, L., *Naming Proofs in Classical Propositional Logic*. In: Urzyczyn, P. (ed.) Typed Lambda Calculi and Applications, pp. 246–261. Springer Berlin Heidelberg (2005)

Straßburger, L., *Towards a Theory of Proofs of Classical Logic*. Université Pairs Diderot – Paris VII (2011)

Pulcini, G., *A note on cut-elimination for classical propositional logic.* Archive for Mathematical Logic **61**(3), 555–565 (2022)