On Quantum Certificates for Tautologies in Minimal Propositional Logic

Edward Hermann Haeusler[1]

Dept of Informatics
PUC-Rio

April 24, 2026

[1] Joint work with Robinson Callou, José Flávio C. Barros, Lorenzo Saraiva

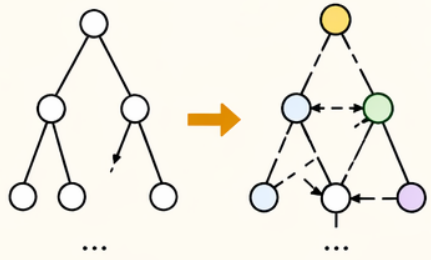
Dag-Like Derivability Structures

INFORMATION FLOW IN THE DLDS FRAMEWORK

WHY

proof compression, storing and validation

- Reduce redundancy in proofs
- Share subderivations and create overlap
- Store proofs in a compact form
- Enable efficient and scalable validation
- Create structure for efficient error detection

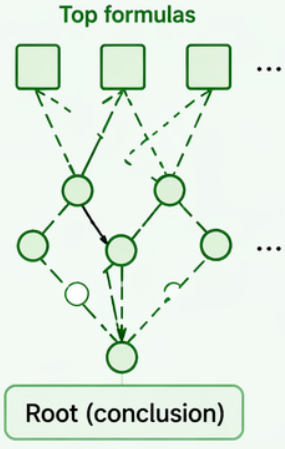


HOW

- Each admissible path is an input $\vec{x} = (i_1, i_2, \ldots, i_m)$
- Associated Boolean verifier:

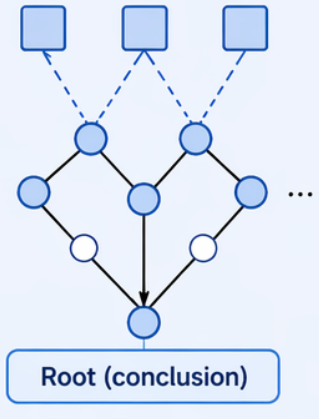
$$f_D(\vec{x}) = WF(D, \vec{x}) \wedge Closed(D, \vec{x})$$

- **WF**: checks local correctness of inference steps
- **Closed:** checks that all assumptions are discharged



WHAT

- DLDS: a compact (DAG) representation of the proof
- Selectors define local choices (branching points)
- Paths correspond to valid executions from leaves to the root
- Global sections (families of paths) are consistent and compatible across the structure

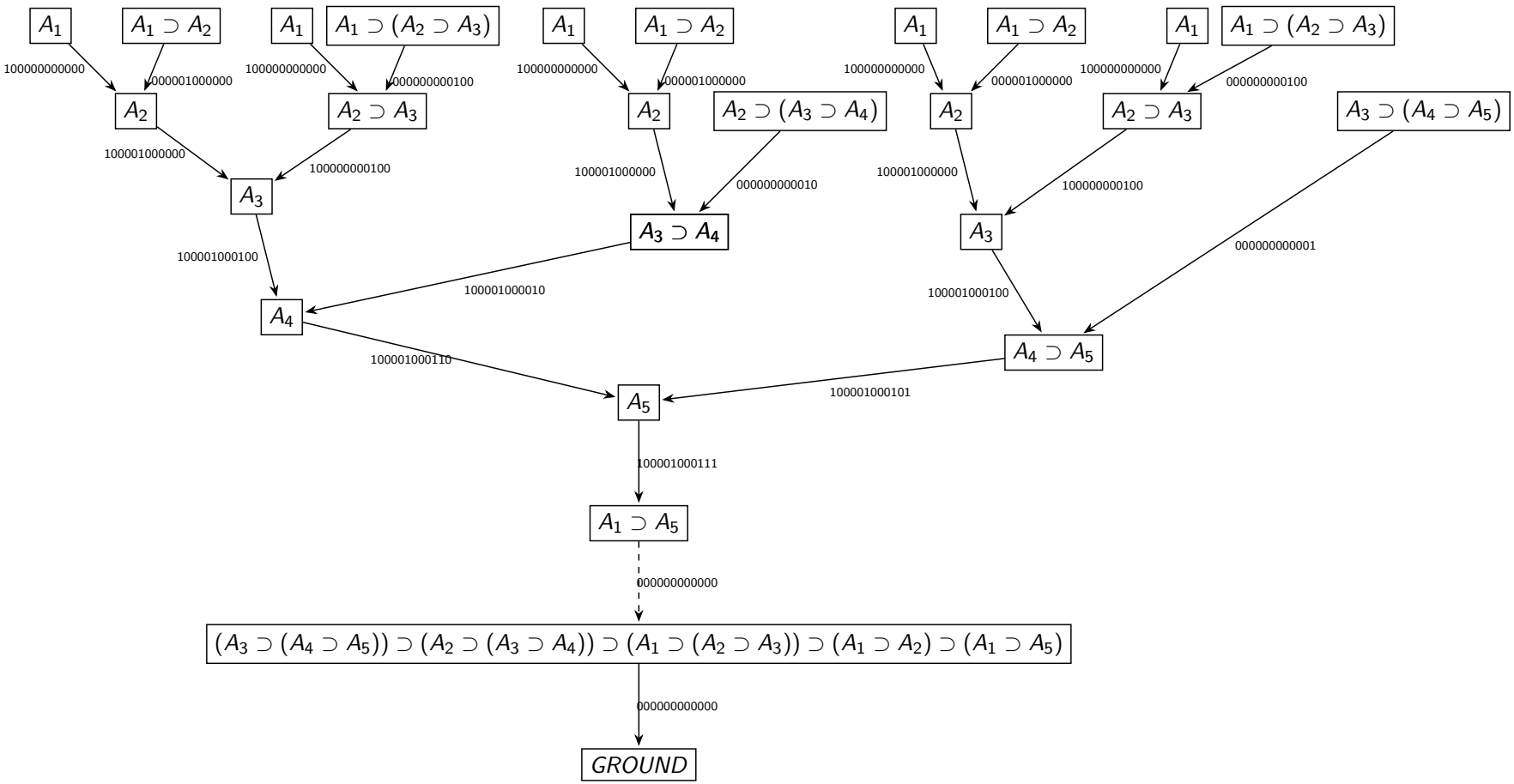


WHO

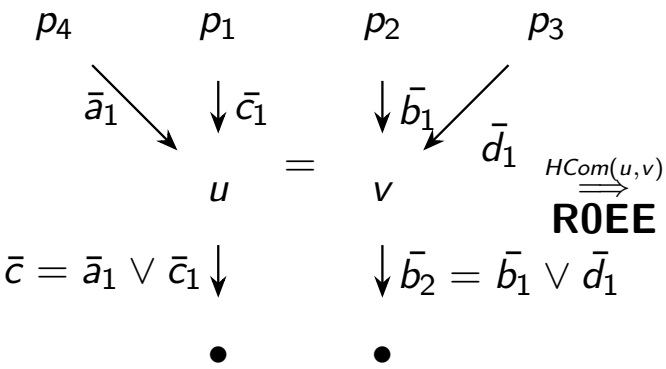
- Quantum algorithm (BBHT / Grover) queries the verifier
- Searches for invalid certificates (counterexamples)
- Complexity depends on the density of errors $\delta = \frac{M_0}{N}$
- Efficient detection when $\delta \geq \frac{1}{poly(m)}$

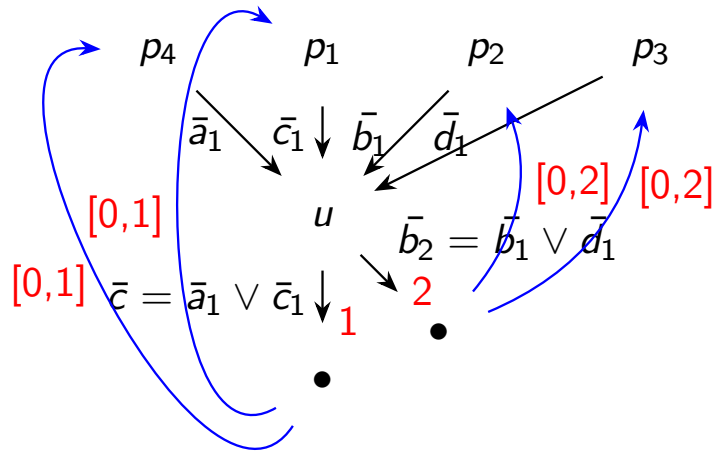
Finds errors with quantum advantage

A Natural Deduction Proof

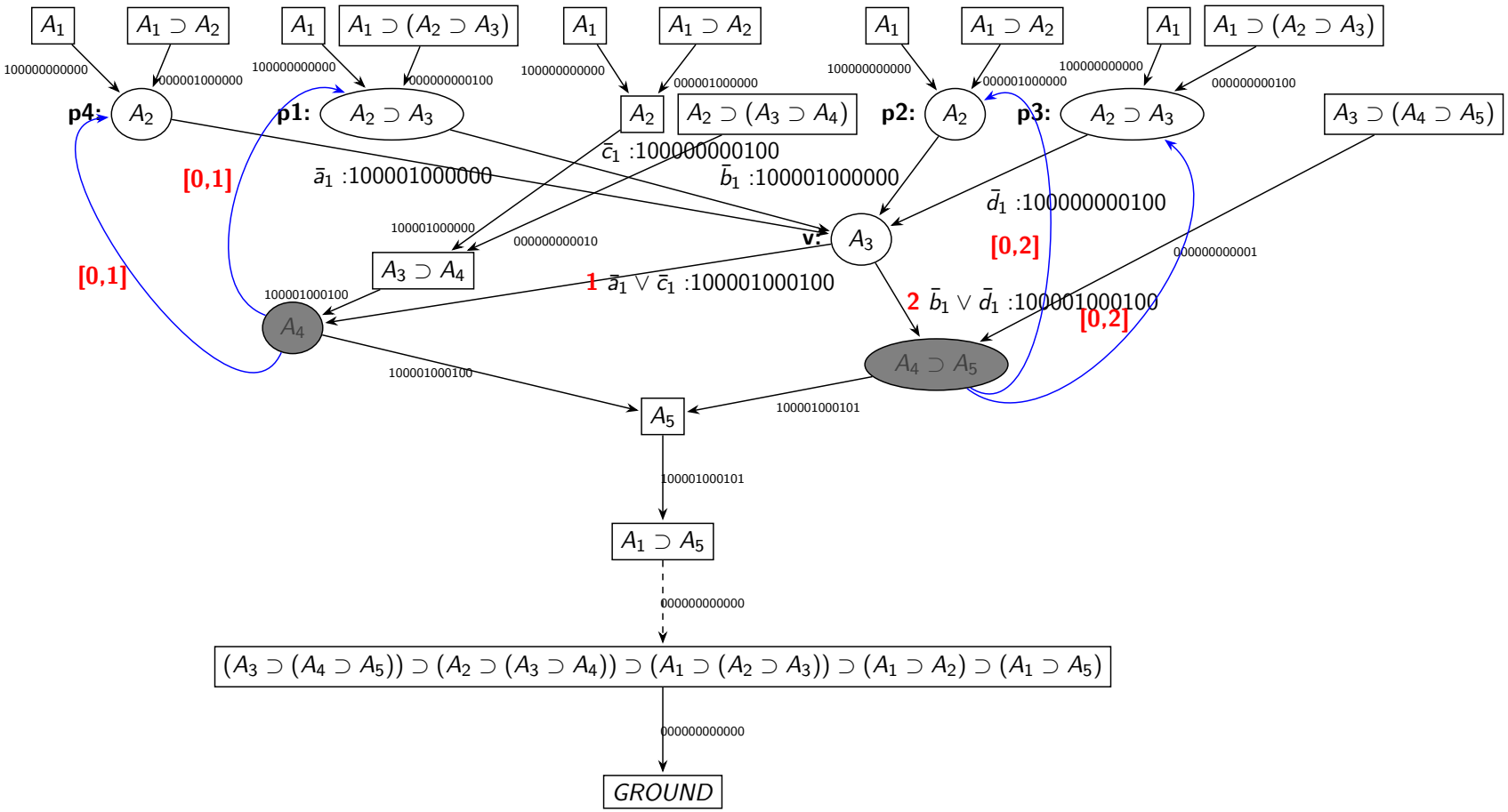


An Horizontal Compression Rule

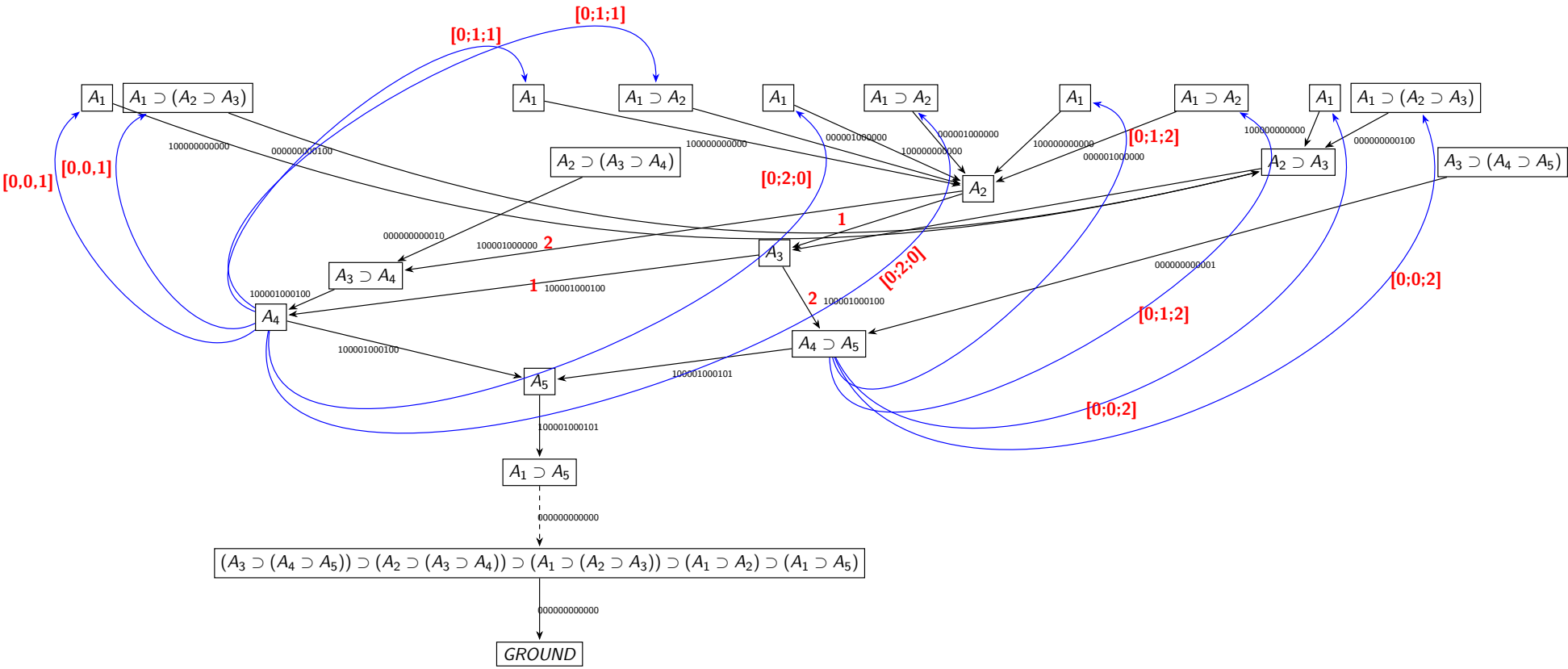




Horizontal Compression of the N.D. proof (I)

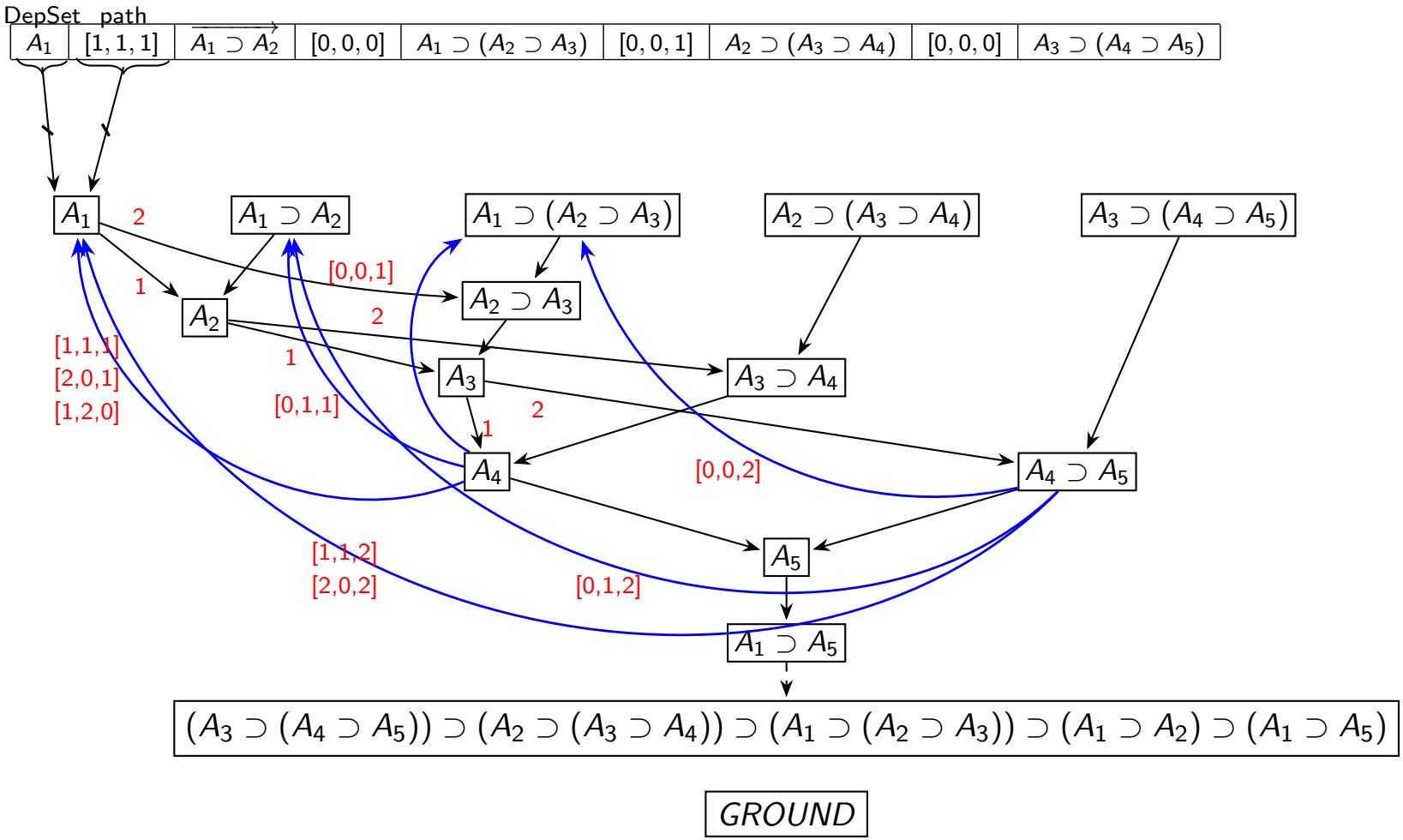


Horizontal Compression of the ND Proof (II)



Many Different Paths in the Same Compressed DLDS (Dag-Like Deriv. Struc.)

DLDS with Leaf Compression



From DLDS to poly-Kernel + Input-Paths

- A compressed DLDS induces many admissible paths from the top formulas to the root.
- Each path is determined by a sequence of local selector choices.

$$x = (i_1, i_2, \ldots, i_m)$$

- We move from a graph view to an input view:
- A (local) path is an input from a top-formula for verification;
- A global path is a product of all compatible local paths.

For every admissible input-path $\vec{x}$

$\overline{f_{D(\Pi)}}(\vec{x}) = \vec{y}$, *iff*, $DepSet(\Pi|\vec{x}) = Set(\vec{y})$

Proved in Lean4

Boolean Verification

- Each admissible global path x defines m local verification traces;
- We associate to the DLDS a Boolean verifier;

$$f_D(\vec{x}) \equiv WF(D, \vec{x}) \wedge Closed(D, \vec{x})$$

- $WF(D, \vec{x})$: local correctness of inference steps
- $Closed(D, \vec{x})$: all assumptions are discharged

$$D \text{ is valid} \iff \forall \vec{x}\, f_D(x) = 1$$

PUC RIO

Global Sections = Families of Paths

- Each selector = local branching choice
- Each path = sequence of choices from a leaf to the root

Global section

- assigns a choice to every selector
- induces one path per top formula
- all paths are mutually consistent

Global section = consistent family of paths

Horizontal Compression and Local-to-Global Structure

Before compression

- tree-like derivation
- no overlap between branches
- local choices are independent

After horizontal compression

- DAG with shared subderivations
- overlapping contexts appear
- paths must agree on overlaps

Compression creates the geometry of overlap

From Compression to Sheaf Structure

$$S = \text{set of branching points of the DLDS}$$

$$Dom(s) = \text{admissible choices at selector } s$$

Base category

$$\mathcal{C}_D = (\mathcal{P}(S), \subseteq)$$

the poset category of subsets of S, ordered by inclusion.

Presheaf of local assignments

$$E : \mathcal{C}_D^{op} \to \mathbf{Set}, \qquad E(U) = \prod_{s \in U} Dom(s)$$

Restrictions

$$\rho_U^V : E(V) \to E(U) \quad \text{for } U \subseteq V,$$

given by projection.

Compatibility

$$\sigma_U|_{U \cap V} = \sigma_V|_{U \cap V}$$

Global sections

$$\Gamma(E_D) = \text{compatible families of paths}$$

Key Insight

Horizontal compression creates overlaps; global executions arise as glued local assignments.

Semantic Entropy and Detection of Invalid Paths

Semantic entropy

$$H_{\text{sem}}(D) = \prod_{s \in S} \log_2 |Dom(s)| = \left(\sum_{s \in S} \log_2 |Dom(s)| - \log_2 |\Gamma(E_D)| \right)$$

Meaning

- measures number of valid executions
- small entropy $\Rightarrow$ few valid paths

Total assignments

$$N = \left| \prod_{s \in S} Dom(s) \right|$$

Invalid fraction

$$\delta = 1 - \frac{2^{H_{\text{sem}}(D)}}{N}$$

Key Intuition

Low entropy $\Rightarrow$ few valid paths $\Rightarrow$ many invalid assignments $\Rightarrow$ quantum search finds errors quickly

Quantum Consequence

- Let N be the total number of verifier inputs.
- Let M_0 be the number of invalid certificates.
- Define the density of counterexamples:

$$\delta = \frac{M_0}{N}$$

- Large semantic entropy implies many invalid certificates:

$$M_0 \geq 2^{H_{\mathrm{sem}}(D)}$$

- If $\delta \geq 1/\mathrm{poly}(m)$, amplitude amplification (BBHT/Grover) detects a bad certificate in polynomial time.

Main Theorem

Theorem. If

$$H_{\mathrm{sem}}(D) \geq m^2 \log m - C \log m$$

for some constant $C > 0$, then

$$\delta \geq \frac{1}{\mathrm{poly}(m)}.$$

Hence:

- invalid certificates occupy an inverse-polynomial fraction of the search space;
- a quantum algorithm can detect one in polynomial time;
- the oracle itself is implementable by a polynomial-size circuit.

Entropy controls detectability.

PUC RIO

Conclusion

- **Proof-theoretic view:** compression creates hidden selector freedom
- **Geometric view:** entropy is logarithmic global-section multiplicity
- **Quantum view:** enough hidden multiplicity yields efficient detection

Verification = global consistency of local choices.

Thank you

Questions?

PUC
RIO

Compression vs Explosion: An application to Non-Hamiltonian graphs certificates

- Naive non-Hamiltonian proofs:

  size up to m^m

- DLDS:

  polynomial size

$\Rightarrow$ Exponential behavior compressed into a polynomial structure

- Before compression:
  - independent branches
  - many separate elimination traces
- After compression:
  - shared traces π_i
  - overlapping subderivations
  - same structure reused many times

$\Rightarrow$ Exponentially many paths flow through few traces

PUC RIO

Error Amplification and Density

- Global inputs:

$$N = \prod_{s \in S} |Dom(s)|$$

- Only few assignments are globally consistent

$\Rightarrow$ High semantic entropy:

$$H_{\text{sem}}(D)$$

- Repetition of top-formulas:
  - many paths share the same trace π_i
- If an error occurs on π_i:
  - it propagates to many inputs

$\Rightarrow$ Large set of invalid certificates

$\Rightarrow$ Inverse-polynomial density:

$$\delta \geq \frac{1}{\text{poly}(m)}$$

PUC RIO

Polynomial Repetition of Top-Formulas

Lemma (Pigeonhole on subformulas)

Let Π be a natural deduction proof whose conclusion has at most m subformulas.
Let T be the number of top-formulas of Π.
Then there exists a top-formula i such that

$$\mathrm{mult}(i) \;\geq\; \left\lceil \frac{T}{m} \right\rceil .$$

In particular, if $T \geq m^2$, then

$$\mathrm{mult}(i) \;\geq\; m.$$

Interpretation

One formula i is repeated polynomially many times as a top-formula.

PUC RIO

Why this matters for DLDS

Proof idea

- Every top-formula is a subformula of the conclusion $\Rightarrow$ at most m distinct possibilities.
- The T occurrences are distributed among $\leq m$ formulas.
- By pigeonhole:

$$\mathrm{mult}(i) \;\geq\; \left\lceil \frac{T}{m} \right\rceil .$$

Connection to DLDS and BBHT

- A repeated top-formula i induces many elimination branches.
- After horizontal compression, these collapse into a shared trace π_i.
- This trace is reused across many local paths.
- If a dependency error occurs on π_i, it propagates to many inputs.
- If the number of induced inputs is $\geq N/\mathrm{poly}(m)$, then $\delta \geq 1/\mathrm{poly}(m)$ and BBHT applies.

PUC RIO

From Entropy to Density (No Extra Hypothesis)

Entropy controls density of errors
Let $N = \prod_{s \in S} |Dom(s)|$ be the total number of verifier inputs and

$$H_{\mathrm{sem}}(D) = \sum_{s \in S} \log_2 |Dom(s)| - \log_2 |\Gamma(E_D)|.$$

Then the number of invalid inputs satisfies

$$M_0 \;\geq\; N - |\Gamma(E_D)| \;\geq\; N - 2^{H_{\mathrm{sem}}(D)}.$$

Hence

$$\delta \;=\; \frac{M_0}{N} \;\geq\; 1 - \frac{2^{H_{\mathrm{sem}}(D)}}{N}.$$

Consequence
If

$$H_{\mathrm{sem}}(D) \;\geq\; m^2 \log m - C \log m,$$

then

$$\delta \;\geq\; \frac{1}{\mathrm{poly}(m)}.$$

Combined with propagation via the shared trace π_i:

- errors are structurally propagated;
- entropy guarantees many invalid inputs.

Therefore BBHT detects an invalid certificate in polynomial time.

PUC RIO