ATOMIC FLOWS DO NOT FORM A PROOF SYSTEM

ANUPAM DAS

Abstract. We prove that, given certain cryptographic assumptions, atomic flows do not form a proof system when working with units.

We show that, when an atom and its dual appear in a tautology, each proof of that tautology can be polynomially transformed into one where each occurrence of the atom and its dual are introduced by an identity step.

Definition 1 (Trivial Weakenings)**.** If a tautology $\xi\{a^\epsilon\}$ has no occurrence of $\bar{a}$, and Φ is a proof of $\xi\{a^\epsilon\}$, we say that a^ϵ is a *trivial weakening* in Φ.

3.1. Supermix in Linear Deep Inference Systems.

Definition 2 (Supermix)**.** We define the supermix rule below:

$$\mathsf{sm}\,\frac{A \wedge \bigvee_i^n B_i}{A \vee \bigwedge_i^n B_i}$$

For the special case when $n = 1$, it coincides with the usual mix rule. Supermix is sound, and trivially derivable for $\{\mathsf{w}{\downarrow}, \mathsf{w}{\uparrow}\}$.

Proposition 3. *There is a derivation from* f *to* t *for* $\{\mathsf{m}\}$.

Proof.

$$= \dfrac{\dfrac{\dfrac{\mathsf{f}}{\mathsf{f} \wedge \mathsf{t}} \vee = \dfrac{\mathsf{f}}{\mathsf{f} \wedge \mathsf{t}}}{\mathsf{f} \vee \mathsf{t}}\,\mathsf{m}}{\mathsf{t}} \wedge = \dfrac{\mathsf{f} \vee \mathsf{t}}{\mathsf{t}}}{\mathsf{t}} =$$

□

Lemma 4. *There is a derivation from* $\bigvee_i^n B_i$ *to* $\mathsf{t} \vee \bigwedge_i^n B_i$ *for* $\{\mathsf{s}, \mathsf{m}\}$.

Proof. We proceed by induction on n.

Base Case: By Prop. 3 we have $\mathsf{m}\,\dfrac{\mathsf{f}}{\mathsf{t}} \vee B$.

Date: November 1, 2011.

Inductive Step: Suppose there are such derivations Φ_r for $r < n$. Define:

$$\Phi_n \quad \equiv \quad \mathsf{m}\,\dfrac{\mathsf{s}\,\dfrac{\mathsf{t} \vee \mathsf{t} \vee \bigvee_i B_i \quad (\Phi_{n-1}\,\|\,\{\mathsf{s},\mathsf{m}\})}{[\mathsf{t} \vee B_n] \wedge [\mathsf{t} \vee \mathsf{t} \vee \bigvee_i B_i]}}{[\mathsf{t} \vee B_n] \wedge [\mathsf{t} \vee \bigvee_i B_i]}$$

□

Theorem 5. *Supermix is derivable for* $\{\mathsf{s}, \mathsf{m}\}$.

Proof. Let Φ_n be the derivations constructed in Lemma 4.

$$\mathsf{s}\,\dfrac{A \wedge \mathsf{t} \vee \bigvee_i^n B_i \quad (\Phi_n\,\|\,\{\mathsf{s},\mathsf{m}\})}{A \wedge \mathsf{t} \vee \bigwedge_i^n B_i}$$

□

Remark 6. All derivations in this section have used only the logical rules, and so create no new vertices in an atomic flow. Their flows are just edges in parallel.

3.2. **Converting Non-Trivial Weakenings to Identities.**

Proposition 7. *Every* KS*-proof can be polynomially transformed into a unit-free proof with shape* $(\mathsf{w}\!\downarrow, \mathsf{ai}\!\downarrow, \{\mathsf{s}, \mathsf{m}\}, \mathsf{ac}\!\downarrow)$.

Lemma 8 (Atomic Weakening)**.** *In a unit-free system, weakening can be made atomic with only quadratic increase in proof size.*

Theorem 9. *There is a proof in* $\mathsf{KS} \setminus \{\mathsf{aw}\!\downarrow\}$ *of each expression* $\bigwedge_i [\mathsf{t} \vee A_i]$ *such that no atom occurs trivially.*

Proof. By Lemma 8 we can assume that each A_i is a disjunction of atoms. We first undergo a process of 'balancing' the formula; by this we mean we applying atomic contractions until there are equally many positive and negative occurrences of each atom. Suppose $A \wedge [B \vee a] \wedge [C \vee \bar{a}]$ is a formula in this form and consider the following derivation in $\mathsf{KS} \setminus \{\mathsf{aw}\!\downarrow\}$:

$$A \wedge \mathsf{m}\,\dfrac{\mathsf{sm}\,\dfrac{B \wedge C \wedge \mathsf{ai}\!\downarrow \dfrac{\mathsf{t}}{a \vee \bar{a}}}{(B \wedge C) \vee (a \wedge \bar{a})}}{[B \vee a] \wedge [C \vee \bar{a}]}$$

Observe that the premiss is $A \wedge B \wedge C$ which is also in this form but has strictly fewer atom occurrences. Therefore we can just repeat the above procedure, chaining the derivations together to obtain a proof. □

4. Identity Normal Form of a Proof

In this section we describe how to polynomially transform a KS-proof into one whose flow is in some way easy to generate, as we will see in the next section.

The following trick appears in Straßburger CITE in some variation.

Definition 10 (Balancing Trick)**.**

5. Main Result

5.1. **Automatisability and Feasible Interpolation.**

Definition 11 (Feasible Interpolation)**.**

Definition 12 (Automatisability)**.**

Theorem 13 (Impaglazzio)**.** *If a system is automatisable then it admits feasible interpolation.*

Theorem 14 (Bonet et al.)**.** *If integer factoring is hard for P/poly then LK does not admit feasible interpolation.*

Observation 15 (Jerabek)**.** KS *admits feasible interpolation just if LK does.*

Corollary 16. *If integer factoring is hard for P/poly then* KS *does not admit feasible interpolation, and hence is not automatisable.*

5.2. **Automatisability Algorithm From Polynomial-Time Correctness Criterion for Atomic Flows.**

6. Conclusions

6.1. **Flow Design.**

6.2. **Unit-Free Deep Inference.**

6.3. **The Linear Fragment of Propositional Logic.**