Short Proofs of Tautologies Using the Schema of Equivalence*

Matthias Baaz** Richard Zach***

Technische Universität Wien, Austria

Abstract. It is shown how the schema of equivalence can be used to obtain short proofs of tautologies A, where the depth of proofs is linear in the number of variables in A.

The schema of equivalence Eq

$$(A \Leftrightarrow B) \Rightarrow \big(C(A) \Leftrightarrow C(B)\big) \quad \text{Eq}$$

(A, B, C arbitrary formulas) is *the* propositional pendant of the schema of identity. It can be argued that, apart form the usual propositional tautologies and inference schemas which are given as axiomatizations of propositional logic (e.g., modus ponens, modus tollens, case distinction, chain rule), the schema of equivalence is also used extensively in mathematical reasoning. However, it seems that Eq has not been used or investigated in the proof theory of propositional logic to any significant extent. A related *rule*, which has been presented by SCHÜTTE [1960] (see Satz 2.9), is the following:

$$\frac{C(T) \quad C(F)}{C(A)}\ S$$

where A and C are formulas and T and F are the logical constants true and false, respectively. Using S, we can derive Eq uniformly for A, B, C in a constant number of steps:

(1) $T \Leftrightarrow T \Rightarrow \big(C(T) \Leftrightarrow C(T)\big)$

(2) $F \Leftrightarrow T \Rightarrow \big(C(F) \Leftrightarrow C(T)\big)$

(3) $A \Leftrightarrow T \Rightarrow \big(C(T) \Leftrightarrow C(T)\big)$ from (1), (2) by S

(4) $T \Leftrightarrow F \Rightarrow \big(C(T) \Leftrightarrow C(F)\big)$

(5) $F \Leftrightarrow F \Rightarrow \big(C(F) \Leftrightarrow C(F)\big)$

(6) $A \Leftrightarrow F \Rightarrow \big(C(A) \Leftrightarrow C(F)\big)$ from (4), (5) by S

(7) $A \Leftrightarrow B \Rightarrow \big(C(A) \Leftrightarrow C(B)\big)$ from (3), (6) by S

* to appear in *Computer Science Logic. Selected Papers from CSL'93*, LNCS, Springer, 1994

** Technische Universität Wien, Institut für Algebra und diskrete Mathematik E118.2, Wiedner Hauptstraße 8–10, A-1040 Wien, Austria, baaz@logic.tuwien.ac.at

*** Technische Universität Wien, Institut für Computersprachen E185.2, Resselgasse 3/1, A-1040 Wien, Austria, zach@logic.tuwien.ac.at

Eq can be used for the evaluation of complex propositional expressions in a bounded number of steps: Let P be some sound and complete Hilbert-style calculus for propositional classical logic (with an alphabet including T, F, $\Rightarrow$, $\vee$, $\Leftrightarrow$ as primitive or derived constants) consisting of a finite number of axiom schemata and rules (one of which is assumed to be the modus ponens). Let T_n be the set of tautologies in $\leq n$ variables, and let $\vdash^k$ denote derivability in depth $\leq k$ (w.l.o.g. proofs are assumed to be tree-like).

THEOREM *For all n the following holds:*

(1) there exists ϕ s.t. for all n and all $A \in T_n$ we have $P + \mathrm{EQ} \vdash^{\phi(n)} A$, where ϕ is a linear function and
(2) for all k there is an $A \in T_0$ s.t. $P \nvdash^k A$.

Proof. If $\Gamma = \{A_1, \ldots, A_m\}$, then $\bigwedge \Gamma \Rightarrow B$ denotes $(A_1 \Rightarrow (A_2 \Rightarrow \ldots (A_m \Rightarrow B)\ldots)$.

(1) First note that the k-times iterated schema of equivalence,

$$\bigwedge_{i=1}^{m} (A_i \Leftrightarrow B_i) \Rightarrow \big(C(A_1, \ldots, A_m) \Leftrightarrow C(B_1, \ldots, B_m)\big)$$

is derivable uniformly in $\leq \psi(m)$ steps from $P + \mathrm{Eq}$. Now we use induction on n:

$n = 0$: Let $\Gamma = \big\{ \Box_i(V_1, \ldots, V_{n_i}) \Leftrightarrow V \mid V_j, V \in \{T, F\} \big\}$ be all combinations representing the truth tables for the primitive connectives $\Box_i$. Furthermore, let Δ be an operator where ΔB is obtained from a formula B by replacing every subformula of the form $\Box_i(V_1, \ldots, V_{n_i})$ ($V_j \in \{T, F\}$) by its value $V \in \{T, F\}$. By Δ^j we denote the j-fold iteration of Δ: $\Delta^0 B \equiv B$ and $\Delta^{j+1} \equiv \Delta\Delta^j B$. (Here and in the following $\equiv$ denotes *syntactic* equality).

Now $A \in T_0$ contains no variables, only T, F. Let $r(A)$ be the minimal number s.t. $\Delta^{r(A)} A \equiv T$. We use *Yukami's Trick* (from YUKAMI [1984]): The two formulas

$$\bigwedge \Gamma \Rightarrow \big[\big(A \Leftrightarrow \underbrace{\big(\Delta^1 A \Leftrightarrow \cdots (\Delta^{r(A)-1} A \Leftrightarrow \overbrace{\Delta^{r(A)} A}^{T})\ldots\big)}_{B}\big) \Leftrightarrow$$

$$\Leftrightarrow \underbrace{\big(\Delta^1 A \Leftrightarrow (\Delta^2 A \Leftrightarrow \cdots (\overbrace{\Delta^{r(A)} A}^{T} \Leftrightarrow \overbrace{\Delta^{r(A)+1} A}^{T})\ldots\big)}_{C}\big]$$

and

$$\big((T \Leftrightarrow T) \Leftrightarrow T\big) \Rightarrow \big[\overbrace{\big(\Delta^1 A \Leftrightarrow (\Delta^2 A \Leftrightarrow \cdots (\Delta^{r(A)-1} A \Leftrightarrow (T \Leftrightarrow T))\ldots\big)}^{C} \Leftrightarrow$$

$$\Leftrightarrow \underbrace{\big(\Delta^1 A \Leftrightarrow (\Delta^2 A \Leftrightarrow \cdots (\Delta^{r(A)-1} A \Leftrightarrow T)\ldots\big)}_{B}\big]$$

are instances of the (iterated) schema of equivalence, thus derivable independent of A from $P + \mathrm{Eq}$. Since both Γ and $\big(T \Leftrightarrow T\big) \Leftrightarrow T\big)$ are tautologies, they can be derived

in a constant number of steps independent of A. Hence, $P + \mathrm{Eq} \vdash^c \big((A \Leftrightarrow B) \Leftrightarrow B\big)$ and consequently also $P + \mathrm{Eq} \vdash^{c'} A$.

$n > 0$: Let $A(X) \in T_n$ contain exactly n distinct variables. The following formulas

$$(X \Leftrightarrow T) \Rightarrow \big(A(X) \Leftrightarrow A(T)\big)$$
$$(X \Leftrightarrow F) \Rightarrow \big(A(X) \Leftrightarrow A(F)\big)$$

are instances of Eq. By induction hypothesis, both $A(T)$ and $A(F)$ are derivable in $\phi(n-1)$ steps from $P + \mathrm{Eq}$. Hence we have

$$P + \mathrm{Eq} \vdash^{\phi(n-1)+d} (X \Leftrightarrow T) \Rightarrow A(X)$$
$$P + \mathrm{Eq} \vdash^{\phi(n-1)+d} (X \Leftrightarrow F) \Rightarrow A(X)$$

and consequently $P + \mathrm{Eq} \vdash^{\phi(n-1)+d'} A(X)$. (Note that the law of excluded middle $(X \Leftrightarrow T) \vee (X \Leftrightarrow F)$ is derivable.) Since d' (and d) do not depend on either $A(X)$ or n, ϕ is linear.

(2) Note that there are only finitely many proof descriptions (or proof skeletons, see KRAJÍČEK and PUDLÁK [1988]) of bounded depth. Every proof description can be realized by a most general proof: Write all axioms with different variables, apply the rules in the description and unify. So, for every k, there is a sequence of formulas $A_1, \ldots, A_{h(k)}$ s.t.

(1) $P \vdash^k A_i$ for $1 \leq i \leq h(k)$ and
(2) if $P \vdash^k A$, then $A = A_i\sigma$ for some A_i and substitution σ.

If all tautologies of the form $\big(T \Leftrightarrow (T \Leftrightarrow (T \Leftrightarrow \cdots (T \Leftrightarrow T)\ldots)\big)$ were provable in bounded depth, then $\big(T \Leftrightarrow (T \Leftrightarrow (T \Leftrightarrow \cdots (T \Leftrightarrow X)\ldots)\big)$ would also be provable, which is absurd. □

Three questions regarding the strength of these results remain open: In the induction step of the proof, the law of the excluded middle was used essentially. Can the result also be obtained without this? Does the result hold for intuitionistic propositional calculus? Furthermore, does the *rule* of equivalence

$$\frac{A \Leftrightarrow B}{C(A) \Leftrightarrow C(B)}$$

suffice for the results to hold? Lastly, do the results hold uniformly for *all* tautologies, not only for those with a fixed number of variables?

References

KRAJÍČEK, J. and P. PUDLÁK.
[1988] The number of proof lines and the size of proofs in first order logic. *Arch. Math. Logic*, **27**, 69–84.

SCHÜTTE, K.
[1960] *Beweistheorie*. Springer, Berlin.

YUKAMI, T.
[1984] Some results on speed-up. *Ann. Japan Assoc. Philos. Sci.*, **6**, 195–205.