ON A HIERARCHY OF FRAGMENTS OF INTUITIONISTIC PROPOSITIONAL LOGIC

by Jörg Hudelmaier

We consider a language of sequents of the form $c_1, \ldots, c_n \Rightarrow a$, where a is a propositional variable and the c_i are formulas of the form $a \to b$, $(a \wedge b) \to c$, or $(a \to b) \to c$, where a, b, and c are propositional variables. It is well known that to every sequent of intuitionistic propositional logic an equideducible sequent of this form may be found in polynomial time. Moreover by introducing new propositional variables in an obvious way we may restrict ourselves to sequents s where for all formulas $(a \wedge b) \to c$ resp. $(a \to b) \to c$ the propositional variable c occurs only once on the right hand side of an implication of s. For such sequents s we consider a relation R between pairs of propositional variables given by $(a,b) \in R$ iff s contains an implication $b \to a$ or $(c \to b) \to a$ or $(c \wedge b) \to a$ or $(b \wedge c) \to a$.We call sequents s for which this relation is well founded CD-sequents and we call C-variables in s all variables a which occur in formulas $(c \wedge b) \to a$ in s, D-variables all variables a which occur in at least two formulas $b \to a$ and $c \to a$ of s. By the above mentioned condition the sets of C- and D-variables are disjoint. Therefore we may define the Sturm number of a sequent s to be the maximal number of changes betwene C- and D-variables along the R-order associated with s.

Theorem 1: The set $D_n(C_n)$ of all provable(nonprovable) CD-sequents whose maximal variable is a D(C)-variable and whose Sturm number is $\leq n$, $n \geq 2$, is in the complexity class Σ_{n-1} of the polynomial hierarchy.

We consider the calculus LJ for intuitionistic propositional logic in the form consisting of axioms $M,a \Rightarrow a$ and rules

$$E\!\to \quad \frac{M, a \to b \Rightarrow a \qquad M, b \Rightarrow r}{M, a \to b \Rightarrow r}$$

$$E\!\to\!\wedge \quad \frac{M, (a \wedge b) \to c \Rightarrow a \qquad M, (a \wedge b) \to c \Rightarrow b \qquad M, c \Rightarrow r}{M, (a \wedge b) \to c \Rightarrow r}$$

$$E\!\to\to \quad \frac{M, a, (a \to b) \to c \Rightarrow b \qquad M, c \Rightarrow r}{M, (a \to b) \to c \Rightarrow r}$$

Due to the invertibility of the usual LJ-rules for introduction of $\wedge$ and $\to$ it is obvious that this calculus is complete for CD-sequents. Now we show:

Lemma: There is a transformation converting every LJ-deduction of a given CD-sequent into another deduction of the same sequent such that in the new deduction any rightmost premiss of an application of one of the rules is an axiom.

The proof of this lemma is immediate by using transformation steps leading from a deduction of, for instance

$$\dfrac{M,(a\to b)\to c,(u\wedge v)\to w \Rightarrow u \quad M,(a\to b)\to c,(u\wedge v)\to w \Rightarrow v \quad \dfrac{M,a,(a\to b)\to c,w \Rightarrow b \quad M,c,w \Rightarrow c}{M,(a\to b)\to c,w \Rightarrow c}}{M,(a\to b)\to c,(u\wedge v)\to w \Rightarrow c}$$

where the lower inference is a maximal inference not obeying the restriction on the right premiss to

$$\dfrac{\dfrac{M,a,(a\to b)\to c,(u\wedge v)\to w \Rightarrow u \quad M,a,(a\to b)\to c,(u\wedge v)\to w \Rightarrow v \quad M,a,(a\to b)\to c,w \Rightarrow b}{M,a,(a\to b)\to c,(u\wedge v)\to w \Rightarrow b} \quad M,c,(u\wedge v)\to w \Rightarrow c}{M,(a\to b)\to c,(u\wedge v)\to w \Rightarrow c}$$

This means that the calculus LJL which consists of the usual axioms and the rules

$$E\to \ \dfrac{M,a\to b \Rightarrow a}{M,a\to b \Rightarrow b}$$

$$E\to\wedge \ \dfrac{M,(a\wedge b)\to c \Rightarrow a \quad M,(a\wedge b)\to c \Rightarrow b}{M,(a\wedge b\ )\to c \Rightarrow c}$$

$$E\to\to \ \dfrac{M,a,(a\to b)\to c \Rightarrow b}{M,(a\to b\ )\to c \Rightarrow c}$$

is complete for CD-sequents. Moreover it is obvious that in an LJL-deduction of a CD-sequent the right hand sides of all premisses are smaller according to its R-ordering than the right hand side of its conclusion. Therefore we cannot use the same principal formula twice on any branch of a deduction. This means that the following calculus LJM is complete for CD-sequents: LJM has the usual axioms and the three rules

$$E\to \ \dfrac{M, \Rightarrow a}{M,a\to b \Rightarrow b}$$

$$E\to\wedge \ \dfrac{M \Rightarrow a \quad M \Rightarrow b}{M,(a\wedge b\ )\to c \Rightarrow c}$$

$$E\to\to \ \dfrac{M,a \Rightarrow b}{M,(a\to b\ )\to c \Rightarrow c}$$

Now consider a given CD-sequent s of Sturm number n+1 whose maximal variable is a C-variable. Let A be the set of all C-variables of s which are greater than every D-variable. Then every LJM-deduction of s consists of branches made up of sequents s_1, ..., s_p, s_{p+1}, ...,s_{p+q}, where all the sequents s_{p+1}, ...,s_{p+q} have right hand sides from A and s_p is a sequent of smaller Sturm number than s. But since the a_i are C-variables, they only occur once as right hand sides of implications in s. Therefore

the sequents s_p, s_{p+1}, ...,s_{p+q}, areuniquely determined for every branch. Thus if s is not provable by LJM, then one of the s_p is not provable and a nondeterministic Turing machine may select one of them in polynomial time whose nonprovability may be established by an oracle for Σ_{n-1}-sets. Therefore the set of nonprovable sequents of this form is in Σ_n.
If the maximal variable of s is a D-variable and A is the set of all D-variables s which are greater than every C-variable, then all the deductions of s have an endpiece of the form s_p, s_{p+1}, ...,s_{p+q}, where all the sequents s_{p+1}, ...,s_{p+q} have right hand sides from A and s_p is a sequent of smaller Sturm number than s. Thus if s is provable than an appropriate endpiece is determined by a nondeterministic Turing machine in polynomial time and provability of the corresponding sequent s_p is established by an oracle for Σ_{n-1}-sets. Therefore the set of provable sequents of this form is in Σ_n.Thus in both cases the proposition holds.

Theorem 2:

a) The sets D_n are hard for Σ_{n-1}.

b) The union of all sets D_n is PSPACE-hard.

It suffices to show that we may reduce classical provability of the well known second order formulae $\exists X_1 \forall X_2 ... \forall X_{2n}\ F$, where F is in disjunctive normal form resp. $\exists X_1 \forall X_2 ... \exists X_{2n+1}\ G$ where G is in conjunctive normal form to the intuitionistic provability of sequents in D_{2n-1} resp. D_{2n}.
For this purpose we use three additional sets of propositional variables: one of these is just a dual X' = $\{x_i'\}$of the original set $X = \{x_i\}$ of variables and the other two are new sets $Y = \{y_i\}$ and $Z =\{z_i\}$. All four sets are pairwise disjoint. Then we associate to every second order formula $B = \exists x_{11}...x_{1l(1)} \forall x_{21}...x_{2l(2)}...\exists x_{r1}...x_{rl(r)}\,((p_{11}\vee...\vee p_{1m(1)})\wedge...\wedge(p_{n1}\vee ... \vee p_{nm(n)}))$ the sequent $\sigma(B) = q_{11}\to y_1, ..., q_{1m(1)}\to y_1, ..., q_{n1}\to y_n,...,q_{nm(n)}\to y_n,(y_1\wedge...\wedge y_n)\to z_{rl(r)},(x_{rl(r)}\to z_{rl(r)})\to z_{rl(r)-1},(x'_{rl(r)}\to z_{rl(r)})\to z_{rl(r)-1},...,(x_{r1}\to z_{r1})\to z_{r0},(x'_{r1}\to z_{r1})\to z_{r0},...,(x_{2l(2)}\to z_{2l(2)}\wedge x'_{2l(2)}\to z_{2l(2)})\to z_{2l(2)-1},...,(x_{21}\to z_{21}\wedge x'_{21}\to z_{21})\to z_{20},(x_{1l(1)}\to z_{1l(1)})\to z_{r1(r1-1},(x'_{r1(r1}\to z_{r1(r1)})\to z_{r1r1-1}, ...,(x_{11}\to z_{r11})\to z_{10} \Rightarrow z_{10}$, where q_{ij} is x if p_{ij} is x and q_{ij} is x' if p_{ij} is $\neg x$, and to every second order formula $B = \exists x_{11}...x_{1l(1)} \forall x_{21}...x_{2l(2)}...\forall x_{r1}...x_{rl(r)}\,((p_{11}\wedge...\wedge p_{1m(1)})\vee...\vee(p_{n1}\wedge ... \wedge p_{nm(n)}))$ we associate the sequent $\sigma(B) = (q_{11}\wedge...\wedge q_{1l(1)})\to y_1, ...,(q_{r1}\wedge...\wedge q_{rl(r)})\to y_r, y_1\to z_{rl(r)},...,y_r\to z_{rl(r)},(x_{r(r)}\to z_{rl(r)}\wedge x'_{r(r)}\to z_{rl(r)})\to z_{rl(r)-1}, ..., (x_{r1}\to z_{r1}\wedge x'_{r1}\to z_{r1})\to z_{r0},..., (\ x_{1l(1)}\to z_{1l(1)})\to z_{r1(r1-1},(x'_{r1(r1}\to z_{r1(r1)})\to z_{r1r1-1}, ...,(x_{11}\to z_{r11})\to z_{10} \Rightarrow z_{10}$, where the same condition on the q_{ij} holds as above. It is obvious that these sequents may be converted into CD-sequents by introduction of some new variables abbreviating certain subformulas.
Now it is evident that a formula B of one of these forms is provable in second order classical propositional logic iff there is a tree

$$
\begin{array}{cccc}
 & x_{11}/x_{11}' & & \\
 & ... & & \\
 & x_{1l(1)}/x_{1l(1)}' & & \\
 & & & \\
x_{21} & & x_{21}' & \\
 & & & \\
x_{22} & x_{22}' & x_{22} & x_{22}' \\
 & & & \\
x_{r1}/x_{r1}' & x_{r1}/x_{r1}' & x_{r1}/x_{r1}' & x_{r1}/x_{r1}' \\
... & ... & ... & ... \\
x_{rl(r)}/x_{rl(r)}' & x_{rl(r)}/x_{rl(r)}' & x_{rl(r)}/x_{rl(r)}' & x_{rl(r)}/x_{rl(r)}'
\end{array}
$$

where $x/$ is either x or $\neg x$ such that for every branch b of this tree $b \to F$ resp. $b \to G$ is provable in classical first order propositional logic.
But since neither b nor F nor G do contain any complex negated formulas, these implications are provable in the ordinary classical calculus iff they are provable in a calculus without negation rules augmented with additional axioms $M, a, \neg a \Rightarrow N$ and $M \Rightarrow a, \neg a, N$. Moreover for the formulas $b \to F$ resp. $b \to G$ the first kind of these axioms is superfluous since a branch b cannot contain a variable and its negation at the same time. Therefore a straightforward induction on the lengths of deductions shows that the formulas $b \to F$ resp. $b \to G$ are provable iff the formulas $b' \to F'$ resp. $b' \to G'$ are provable, where b', F' and G' result from b, F, and G by replacing all formulas $\neg a$ by a new dual variable a'. (For the axioms $b', a \Rightarrow a, F'$ are still axioms and the axioms $b' \Rightarrow a, a', F'$ are also axioms, because b' either contains a or a'.)
This shows that a formula B is provable iff there is a tree of the above form where this time x/x' is either x or x', such that for all branches b' of this tree the formula $b' \to F'$ resp. $b' \to G'$ is provable in first order classical propositional logic.
Now on the other hand it is obvious that $\sigma(B)$ is provable in intuitionistic propositional logic using the calculus LJM iff for this tree and for all its branches b' the sequent $b', q_{11} \to y_1, \ldots, q_{1m(1)} \to y_1, \ldots, q_{n1} \to y_n, \ldots, q_{nm(n)} \to y_n, (y_1 \wedge \ldots \wedge y_n) \to z_{rl(r)} \Rightarrow z_{rl(r)}$ resp. $b', (q_{11} \wedge \ldots \wedge q_{1l(1)}) \to y_1, \ldots, (q_{r1} \wedge \ldots \wedge q_{rl(r)}) \to y_r\, y_1 \to z_{rl(r)}, \ldots, y_r \to z_{rl(r)} \Rightarrow z_{rl(r)}$ is provable. But these sequents are equideducible with $b' \Rightarrow (q_{11} \vee \ldots \vee q_{1l(1)}) \wedge \ldots \wedge (q_{r1} \vee \ldots \vee q_{rl(r)})$ resp. $b' \Rightarrow (q_{11} \wedge \ldots \wedge q_{1l(1)}) \vee \ldots \vee (q_{r1} \wedge \ldots \wedge q_{rl(r)})$. These sequents in turn do not contain any negation sign, hence they are provable in intuitionistic logic iff they are provable in classical logic.

Corollary: To every intuitionistic sequent s there is a normal form $N(s)$ such that $N(s)$ is a CD-sequent and $N(s)$ is provable in intuitionistic propositional logic iff s is provable. Moreover $N(s)$ may be obtained in polynomial time.