17. Algebraic Proof of the Separation Theorem on Classical Propositional Calculus

By Tsutomu HOSOI

Mathematical Institute, University of Tokyo

(Comm. by Zyoiti SUETUNA, M.J.A., Feb. 12, 1966)

In our previous paper [2], it is shown that we can so axiomatize the classical predicate calculus that the separation theorem, mentioned below, holds on it:

Separation Theorem: *A classically provable formula can be proved by using at most the axioms for implication and those of the connectives which actually appear in the formula.*

An example of the propositional fragment of such axiom systems is:

1.1 $p \supset q \supset p$.

1.2 $(p \supset q \supset r) \supset (p \supset q) \supset (p \supset r)$.

1.3 $((p \supset q) \supset p) \supset p$.

1.4 $p \& q \supset p$ and $p \& q \supset q$.

1.5 $(p \supset q) \supset (p \supset r) \supset (p \supset q \& r)$.

1.6 $p \supset p \vee q$ and $q \supset p \vee q$.

1.7 $(p \supset r) \supset (q \supset r) \supset (p \vee q \supset r)$.

1.8 $(p \supset \sim q) \supset (q \supset \sim p)$.

1.9 $\sim p \supset p \supset q$.

The rules of inference are modus ponens and the rule of substitution for variables. We associate to the right and assume the convention that implication binds less strongly than other connectives. This system is classical, for we obtain from 1.3 the law of excluded middle by putting $p = r \vee \sim r$ and $q = r \& \sim r$.

In [2], we proved the separation theorem by using Gentzen's cut elimination theorem on the classical predicate calculus. And in this paper is given an algebraic proof of the theorem on the propositional calculus defined above. The algebraic proof of the theorem on the intuitionistic propositional calculus was given by Horn [1]. And his system is obtained from our system by deleting 1.3. He defined algebras called I, IN, ID, IC, IDN, ICN, ICD, or ICDN and reduced the proof of the theorem to the problem of embedding each algebra into an ICDN algebra. We will not give the details of Horn's paper but borrow some definitions and results from it, so see his paper for those.

Horn first embedded algebras without N into those with N, which was not so complicated. And then he treated the algebras without C, and finally the case of algebras without D, which was the most complicated. But the situation is quite different in the classical calculus, where the case of attaching D to algebras without D is easily treated since $\vee$ can be defined in terms of $\supset$. Only the case of attaching N required us some technics, owing perhaps to the fact that any algebra can be regarded as an ICDN algebra only if N is attached to it.

Our definition of algebras differs only in defining an I algebra. An I algebra must satisfy the following conditions.

2.1 If $1 \to x = 1$, then $x = 1$.

2.2 If $x \to y = y \to x = 1$, then $x = y$.

2.3 $x \to y \to x = 1$.

2.4 $(x \to y \to z) \to (x \to y) \to (x \to z) = 1$.

2.5 $((x \to y) \to x) \to x = 1$.

The last is the one added to Horn's definition.

Now we proceed to solve the embedding problem.

In an I algebra, we introduce a new function $+$ by $x + y = (x \to y) \to y$. Then the following identities hold.

3.1 $x + y = y + x$.

3.2 $x \to (x+y) = 1$ and $y \to (x+y) = 1$.

3.3 $(x \to z) \to (y \to z) \to ((x+y) \to z) = 1$.

The first is obtained as follows. By 2.5, $((x \to y) \to x) \leqq x$. Hence $((x \to y) \to y) \to ((y \to x) \to x) \geqq ((x \to y) \to y) \to ((y \to x) \to ((x \to y) \to x)) = (x \to y) \to ((x \to y) \to y) \to (y \to x) \to x = 1$. 3.2 is immediate from $x \to ((x \to y) \to y) = 1$ and from 3.1. And 3.3 is proved as follows. $(x \to z) \to (y \to z) \to (((x \to y) \to y) \to z) = (x \to z) \to ((x \to y) \to y) \to ((y \to z) \to z) = (x \to z) \to ((x \to y) \to y) \to ((z \to y) \to y) = (x \to z) \to (z \to y) \to (((x \to y) \to y) \to y) = (x \to z) \to (z \to y) \to ((y \to (x \to y)) \to (x \to y)) = (x \to z) \to (z \to y) \to (x \to y) = 1$.

4.1 **Lemma:** *Any* I (*or* IN, *or* IC, *or* ICN) *algebra* $\mathcal{A}$ *can be embedded in an* ID (*or* IDN, *or* ICD, *or* ICDN) *algebra* $\mathcal{B}$.

Proof. As $\mathcal{B}$ we take the same algebra $\mathcal{A}$. In $\mathcal{B}$ we define $x + y$ as above, and as the embedding mapping we take the identity mapping. Then the algebra $\mathcal{B}$ is easily seen to be the desired one.

4.2 **Lemma:** *Any* ID (*or* IDN) *algebra* $\mathcal{A}$ *can be embedded in an* ICD (*or* ICDN) *algebra* $\mathcal{B}$.

Proof. We can prove this lemma in the same way as Horn did his 8.5. It will be sufficient if only we add the case of 2.5 to the proof of Horn's 7.1. When A is a and B is b, $((A \to B) \to A) \to A = 1$ by 2.5. If A is a and B is $b \cup B'$, $((a \to b \cup B') \to a) \to a = ((a \to B') \cup (a \to b) \to a) \to a = ((a \to B') \to ((a \to b) \to a)) \to a \geqq ((a \to B') \to a) \to a = 1$. If A is $a \cup A'$, it is sufficient for us to prove $((a \cup A' \to B) \to a \cup A') \to a = 1$. But $((a \cup A' \to B) \to a \cup A') \to a = ((a \cup A' \to B) \to a) \cup ((a \cup A' \to B) \to A') \to a = ((a \to (A' \to B)) \to a) \cup ((A' \to (a \to B)) \to A') \to a \geqq a \cup A' \to a = 1$.

4.3 **Lemma:** *Any* ICD *algebra* $\mathcal{A}$ *can be embedded in an* ICDN *algebra* $\mathscr{B}$.

Proof. Case 1. If $\mathscr{A}$ has the smallest element 0, we take $\mathscr{A}$ as $\mathscr{B}$. And we define $\neg x$ by $x \to 0$. Then it is easily seen that $\mathscr{B}$ is an ICDN algebra. If we take the identity mapping as the embedding mapping, then the lemma is proved.

Case 2. If $\mathscr{A}$ has not the smallest element, we define $\mathscr{B}$ as the set $\mathscr{A} \cup \mathscr{A}'$, where $\mathscr{A}'$ is the set $\{x'; x \in \mathscr{A}\}$ (by x' we only mean a new symbol obtained by putting $'$ to x which is an element of $\mathscr{A}$). By the definition, $\mathscr{A}$ and $\mathscr{A}'$ are mutually disjoint. If $x, y \in \mathscr{A}$, then $x \to y$, xy, and $x+y$ are defined in $\mathscr{B}$ as the same as in $\mathscr{A}$. And also we define as follows.

$$
\begin{array}{lll}
x' \to y' = y \to x. & x \to y' = (xy)'. & x' \to y = x+y. \\
x'y' = y'x' = (x+y)'. & xy' = y'x = (x \to y)'. & \\
x'+y' = y'+x' = (xy)'. & x+y' = y'+x = y \to x. & \\
\neg x = x \to 1' \ (=x'). & \neg(x') = x' \to 1' \ (=x). &
\end{array}
$$

In $\mathscr{B}$, $1'$ is the smallest element, since $1' \to x = 1 + x = 1$ for any $x \in \mathscr{A}$ and $1' \to x' = x \to 1 = 1$ for any $x' \in \mathscr{A}'$.

Now we show that 2.5 holds for any elements x and y of $\mathscr{B}$. If $x, y \in \mathscr{A}$, then $((x \to y) \to x) \to x = 1$ by the definition. If $x = u' \in \mathscr{A}'$ $(u \in \mathscr{A})$ and $y \in \mathscr{A}$, then $((u' \to y) \to u') \to u' = ((u+y) \to u') \to u' = u \to (u+y)u = 1$. If $x \in \mathscr{A}$ and $y = u' \in \mathscr{A}'$ $(u \in \mathscr{A})$, then $((x \to u') \to x) \to x = ((xu)' \to x) \to x = (xu) + x \to x = 1$. If $x = u'$, $y = v' \in \mathscr{A}'$ $(u, v \in \mathscr{A})$, then $((u' \to v') \to u') \to u' = ((v \to u) \to u') \to u' = ((v \to u)u)' \to u' = u \to (v \to u)u = 1$. We can treat other axioms in the same way, and it is not so difficult but rather tedious, so we do not show the rests any more. So we know that $\mathscr{B}$ is a pseudo ICDN algebra.

Next we show that $\mathscr{B}$ is an ICDN algebra, that is, we prove that 2.2 holds in $\mathscr{B}$. If both x and y belong to $\mathscr{A}$ (or $\mathscr{A}'$), then 2.2 obviously holds by the definition. If $x = u' \in \mathscr{A}'$ and $y \in \mathscr{A}$, then $x \to y = u' \to y = u + y \in \mathscr{A}$ and $y \to u' = (yu)' \in \mathscr{A}'$. But $x \to y = y \to x$ by the hypothesis, so $u + y = (yu)' \in \mathscr{A} \cap \mathscr{A}'$, contrary to $\mathscr{A} \cap \mathscr{A}' = \phi$. So 2.2 holds vacuously. Hence $\mathscr{B}$ is an ICDN algebra. And as in the case 1, our lemma is proved by taking the identity mapping as the embedding mapping.

By the three lemmas proved above, our problem has been completely solved.

References

[1] A. Horn: The separation theorem of intuitionist propositional calculus. J. Symbolic Logic, **27**, 391-399 (1962).

[2] T. Hosoi: The separation theorem on the classical system. J. Fac. Sci., Univ. Tokyo, **12**, 223-230 (1966).