J. Math. Soc. Japan
Vol. 17, No. 1, 1965

An algebraic formulation of cut-elimination theorem

By Satoko TITANI

(Received Aug. 22, 1964)

Gentzen [1] proved cut-elimination theorem in his formal system *LK* of the first order predicate calculus, saying that any provable sequent in *LK* is provable without cut rule in *LK*. Takeuti [5] extended Gentzen's *LK* to his *GLC* by generalization of inference rules from first to higher order predicate calculus. The cut-elimination theorem in *GLC* has not yet been proved; it was proved in [5] that it implies the consistency of classical analysis.

In this paper, we shall consider a formal system $\mathfrak{S}$ of simple type theory, as used by Schütte [4], but not containing the cut rule. It is easily seen that this system $\mathfrak{S}$ is equivalent to Takeuti's *GLC* or Schütte's system, from which cut rule is omitted. We shall represent this system $\mathfrak{S}$ as a 'quasi-Boolean algebra' and give an algebraic formulation of the cut-elimination theorem in $\mathfrak{S}$.

In § 1, we shall define 'quasi-Boolean algebra' B and prove four certain conditions in such algebra to be equivalent (Theorem 4). It will be noticed that the validity of (one of) these conditions in B, means that certain equivalence classes in B form a Boolean algebra in a natural way. In § 2, we shall give our system $\mathfrak{S}$, which will be represented as a quasi-Boolean algebra in § 3. Then it will be shown that any of the four conditions of Theorem 4 is equivalent to the cut-elimination theorem.

The author is grateful to Professor S. Iyanaga and Professor S. Maehara for their kind advice and guidance.

§ 1. Quasi-Boolean algebra.

We shall define an algebra called *quasi-Boolean algebra* and we shall introduce several concepts and prove some theorems in such algebras.

DEFINITION 1. We call a system X *quasi-ordered system*, when a relation $\leqq$ is defined in X and satisfies (P.1) and (P.2):

(P.1) For all x in X, $x \leqq x$.

(P.2) If $x \leqq y$ and $y \leqq z$, then $x \leqq z$.

We shall also sometimes write $x \geqq y$ to mean $y \leqq x$, $x \equiv y$ to mean that $x \leqq y$ and $x \geqq y$, and $x < y$ to mean that $x \leqq y$ but $x \not\equiv y$.

DEFINITION 2. We call a quasi-ordered system B *quasi-Boolean algebra*,

when binary operations $\cup$ and $\cap$ and unary operation $'$ are defined in B and satisfy (B.1)-(B.12):

(B.1) If $\alpha \in B$ and $\beta \in B$, then $\alpha \cup \beta \in B$ and $\alpha \cap \beta \in B$.

(B.2) $\alpha \leqq \alpha \cup \beta$ and $\beta \leqq \alpha \cup \beta$.

(B.3) If $\alpha \leqq \gamma$ and $\beta \leqq \gamma$, then $\alpha \cup \beta \leqq \gamma$.

(B.4) $\alpha \cap \beta \leqq \alpha$ and $\alpha \cap \beta \leqq \beta$.

(B.5) If $\gamma \leqq \alpha$ and $\gamma \leqq \beta$, then $\gamma \leqq \alpha \cap \beta$.

(B.6) $\alpha \cap (\beta \cup \gamma) \equiv (\alpha \cap \beta) \cup (\alpha \cap \gamma)$.

(B.7) If $\alpha < \beta$, then there is an element γ of B such that $\alpha \cup \gamma \not\equiv 1$ and $\beta \cup \gamma \equiv 1$.

(B.8) If $\alpha \in B$, then $\alpha' \in B$.

(B.9) $(\alpha \cup \beta)' \equiv \alpha' \cap \beta'$.

(B.10) $(\alpha \cap \beta)' \equiv \alpha' \cup \beta'$.

(B.11) $\alpha'' \equiv \alpha$.

(B.12) $\alpha \cup \alpha' \equiv 1$, where 1 is a special element of B.

DEFINITION 3. When a subset I of a quasi-Boolean algebra B satisfies the following conditions (I.1) and (I.2), we call I *ideal* of B.

(I.1) If $\alpha \in I$ and $\beta \in I$, then $\alpha \cup \beta \in I$.

(I.2) If $\alpha \in I$ and $\beta \leqq \alpha$, then $\beta \in I$.

DEFINITION 4. We say that an ideal I is *prime*, when if $\alpha \cap \beta \in I$ then $\alpha \in I$ or $\beta \in I$.

DEFINITION 5. We say that an ideal I is *regular*, when $\alpha \cap \alpha' \in I$ for any element α of B.

THEOREM 1. *Let S be a subset of B which has the following property (F):*

(F) For any finite number of elements $\alpha_1, \cdots, \alpha_n$ of S,

$$\alpha_1 \cup \cdots \cup \alpha_n \not\equiv 1 .$$

Then there is a maximal subset of B which contains S and has the property (F), and it is a maximal ideal of B.

PROOF. Let $\mathfrak{P}$ be the class of all subsets which have the property (F) and contain S. Then $\mathfrak{P}$ is partially ordered by the relation of set inclusion, and it is an inductively ordered set. Hence there is a maximal element of $\mathfrak{P}$, by Zorn's lemma. Let M be the maximal element, and we shall prove that M is an ideal of B. (I.1) Suppose that $\alpha \in M$ and $\beta \in M$. Then for any finite number of elements $\gamma_1, \cdots, \gamma_n$ of M, we have $\alpha \cup \beta \cup \gamma_1 \cup \cdots \cup \gamma_n \not\equiv 1$, by hypothesis. That is to say, $\{\alpha \cup \beta\} \cup M$ has also the property (F). By maximality of M, we have $\alpha \cup \beta \in M$. (I.2) Suppose that $\alpha \in M$ and $\beta \leqq \alpha$. Then $\alpha \cup \gamma \not\equiv 1$ for any element γ of M. Hence $\beta \cup \gamma \not\equiv 1$ for any element γ of M, by $\beta \cup \gamma \leqq \alpha \cup \gamma$. That is to say, $\{\beta\} \cup M$ has the property (F). By maximality of M, we have $\beta \in M$.

Since ideal of B which differs from B has the property (F), M is a max-

imal ideal. q. e d.

THEOREM 2. *Any maximal ideal of B is a maximal subset which has the property (F).*

PROOF. A maximal ideal M of B has the property (F). By Theorem 1, there is a maximal subset M' of B which has the property (F) and contains M, and M' is a maximal ideal. Hence M' is M itself. q. e. d.

THEOREM 3. *Every maximal ideal of B is a prime ideal.*

PROOF. Let M be a maximal ideal and suppose that $\alpha \notin M$ and $\beta \notin M$. By Theorem 2, there are two elements γ and δ of M such that $\alpha \cup \gamma \equiv 1$ and $\beta \cup \delta \equiv 1$. Hence

$$(\alpha \cup \gamma) \cap (\beta \cup \delta) \equiv (\alpha \cap \beta) \cup (\alpha \cap \delta) \cup (\gamma \cap \beta) \cup (\gamma \cap \delta) \equiv 1 .$$

Since $(\alpha \cap \delta) \cup (\gamma \cap \beta) \cup (\gamma \cap \delta) \in M$, we have $\alpha \cap \beta \notin M$. q. e. d.

Now we shall prove:

THEOREM 4. *In a quasi-Boolean algebra B, the following four conditions are equivalent to each other.*

(I) *If $\alpha \equiv \beta$, then $\alpha' \equiv \beta'$.*

(II) *Any non-empty maximal ideal of B is a regular ideal.*

(III) *If S is a subset of B such that $\alpha_1 \cup \cdots \cup \alpha_n \not\equiv 1$ for any finite number of elements $\alpha_1, \cdots, \alpha_n$ of S (i. e. if S has the property (F)), then there is a regular maximal ideal which contains S.*

(IV) *If $\gamma \not\equiv 1$, then there is a regular maximal ideal which contains γ.*

LEMMA 1. *If $\alpha \equiv \beta$ implies $\alpha' \equiv \beta'$, then maximal ideal of B is regular.*

PROOF. Suppose that $\alpha \equiv \beta$ implies $\alpha' \equiv \beta'$. Then $(\alpha \cup \alpha')' \equiv (\beta \cup \beta')'$ for arbitrary two elements α and β of B. Hence $\alpha \cap \alpha' \leqq \beta$ for arbitrary two elements α and β by $\alpha \cap \alpha' \equiv \beta \cap \beta' \leqq \beta$. So any non-empty maximal ideal is regular. q. e. d.

LEMMA 2. *If all maximal ideals of B are regular, then for any subset S of B which has the property (F), there is a regular maximal ideal which contains S.*

PROOF. By Theorem 1, there is a maximal ideal which contains S. Since a maximal ideal of B is regular by hypothesis, there is a regular maximal ideal which contains S. q. e. d.

LEMMA 3. *If for any subset S of B which has the property (F), there is a regular maximal ideal containing S, then for any element γ of B such that $\gamma \not\equiv 1$, there is a regular maximal ideal containing γ.*

PROOF. This is clear if we take $\{\gamma\}$ instead of S.

LEMMA 4. *If for any γ such that $\gamma \not\equiv 1$, there is a regular maximal ideal containing γ, then $\alpha \equiv \beta$ implies $\alpha' \equiv \beta'$.*

PROOF. Suppose that $\alpha' \not\equiv \beta'$. Then either $\alpha' \cup \beta' > \alpha'$ or $\alpha' \cup \beta' > \beta'$ holds. We shall treat only the case $\alpha' \cup \beta' > \alpha'$. By (B.7), there is an element

γ of B such that $\alpha' \cup \beta' \cup \gamma \equiv 1$ and $\alpha' \cup \gamma \not\equiv 1$. So there is a regular maximal ideal M which contains $\alpha' \cup \gamma$ by the hypothesis. Then M contains α' and does not contain β' by $\alpha' \cup \gamma \cup \beta' \equiv 1$. Since M is regular and a maximal ideal is prime by Theorem 3, M contains either β or β'. Hence $\alpha \notin M$ by $\alpha' \in M$ and $\beta \in M$ by $\beta' \notin M$. That is to say, $\alpha \not\equiv \beta$. q. e. d.

By Lemmas 1-4, Theorem 4 is proved.

Now let $\tilde{B}$ be the set of equivalence classes by the relation $\equiv$, and let $\tilde{\alpha}$ be the class containing α. Then the operations $\cup$ and $\cap$ in $\tilde{B}$ can be defined by the following;

$$\tilde{\alpha} \cup \tilde{\beta} = \widetilde{\alpha \cup \beta},$$

$$\tilde{\alpha} \cap \tilde{\beta} = \widetilde{\alpha \cap \beta}.$$

Indeed, if $\alpha_1 \equiv \alpha_2$ and $\beta_1 \equiv \beta_2$, then $\alpha_1 \cup \beta_1 \geqq \alpha_2$ and $\alpha_1 \cup \beta_1 \geqq \beta_2$ by (B.2). So $\alpha_1 \cup \beta_1 \geqq \alpha_2 \cup \beta_2$ by (B.3). Similarly, $\alpha_2 \cup \beta_2 \geqq \alpha_1 \cup \beta_1$. Hence $\alpha_1 \cup \beta_1 \equiv \alpha_2 \cup \beta_2$. $\alpha_1 \cap \beta_1 \equiv \alpha_2 \cap \beta_2$ is also proved similarly. If the condition (I) of Theorem 4 holds, operation $'$ in $\tilde{B}$ can be defined by $(\tilde{\alpha})' = \tilde{\alpha}'$. Then it is obvious by (B.1)—(B.6) and (B.8)—(B.12), that $\tilde{B}$, with the above defined operations $\cup$, $\cap$ and $'$, is a Boolean algebra.

The conditions (I)—(IV) of Theorem 4 do not always hold in quasi-Boolean algebra. In the following we shall give an example of quasi-Boolean algebra in which the conditions (I)—(IV) do not hold.

EXAMPLE. Let N be the set of all natural numbers. Let $\mathfrak{M}$ be a set of all mappings from N to $\{0, 1/2, 1\}$. For each element α of $\mathfrak{M}$, let $|\alpha|$ be a subset $\{i \mid i \in N \text{ and } \alpha(i) \geqq 1/2\}$ of N. For elements α and β of $\mathfrak{M}$, let $\alpha \leqq \beta$ mean that $|\alpha|$ is contained in $|\beta|$. Then $\mathfrak{M}$ is a quasi-ordered system. We define operations $\cup$, $\cap$ and $'$ in $\mathfrak{M}$ by the following expressions.

$(\alpha \cup \beta)(i) = \max\{\alpha(i), \beta(i)\}$,

$(\alpha \cap \beta)(i) = \min\{\alpha(i), \beta(i)\}$,

$(\alpha')(i) = 1 - \alpha(i)$, where 1 is a mapping which maps all i in N to 1.

Then $\mathfrak{M}$ is a quasi-Boolean algebra.

PROOF. We shall show $|\alpha \cup \beta| = |\alpha| \cup |\beta|$ and $|\alpha \cap \beta| = |\alpha| \cap |\beta|$ previously.

$$\begin{aligned} |\alpha \cup \beta| &= \{i \mid (\alpha \cup \beta)(i) \geqq 1/2\} \\ &= \{i \mid \max\{\alpha(i), \beta(i)\} \geqq 1/2\} \\ &= \{i \mid \alpha(i) \geqq 1/2 \text{ or } \beta(i) \geqq 1/2\} \\ &= |\alpha| \cup |\beta|, \\ |\alpha \cap \beta| &= \{i \mid (\alpha \cap \beta)(i) \geqq 1/2\} \\ &= \{i \mid \min\{\alpha(i), \beta(i)\} \geqq 1/2\} \end{aligned}$$

$$= \{i \mid \alpha(i) \geqq 1/2 \text{ and } \beta(i) \geqq 1/2\}$$
$$= |\alpha| \cap |\beta| .$$

(B.1) is obvious by the definition of $\mathfrak{M}$. (B.2) Since $|\alpha| \subset |\alpha| \cup |\beta| = |\alpha \cup \beta|$ and $|\beta| \subset |\alpha| \cup |\beta| = |\alpha \cup \beta|$, we have $\alpha \leqq \alpha \cup \beta$ and $\beta \leqq \alpha \cup \beta$. (B.3) Assume $\alpha \leqq \gamma$ and $\beta \leqq \gamma$. Then $|\alpha| \subset |\gamma|$ and $|\beta| \subset |\gamma|$. Since $|\alpha \cup \beta| = |\alpha| \cup |\beta| \subset |\gamma|$, we have $\alpha \cup \beta \leqq \gamma$. (B.4) Since $|\alpha \cap \beta| = |\alpha| \cap |\beta| \subset |\alpha|$ and $|\alpha \cap \beta| = |\alpha| \cap |\beta| \subset |\beta|$, we have $\alpha \cap \beta \leqq \alpha$ and $\alpha \cap \beta \leqq \beta$. (B.5) Assume $\gamma \leqq \alpha$ and $\gamma \leqq \beta$. Then $|\gamma| \subset |\alpha|$ and $|\gamma| \subset |\beta|$ by the definition. Since $|\gamma| \subset |\alpha| \cap |\beta| = |\alpha \cap \beta|$, we have $\gamma \leqq \alpha \cap \beta$. (B.6) $\alpha \cap (\beta \cup \gamma) \equiv (\alpha \cap \beta) \cup (\alpha \cap \gamma)$ holds by the following:

$$|\alpha \cap (\beta \cup \gamma)| = |\alpha| \cap (|\beta| \cup |\gamma|) = (|\alpha| \cap |\beta|) \cup (|\alpha| \cap |\gamma|)$$
$$= |(\alpha \cap \beta) \cup (\alpha \cap \gamma)| .$$

(B.7) Assume $\alpha < \beta$. Let γ be a mapping defined in the following:

$$\gamma(i) = \begin{cases} 1, & \text{if } \beta(i) = 0, \\ 0, & \text{if } \beta(i) \geqq 1/2 . \end{cases}$$

Then $\alpha \cup \gamma \not\equiv 1$ and $\beta \cup \gamma \equiv 1$. Hence there is an element γ of B such that $\alpha \cup \gamma \not\equiv 1$ and $\beta \cup \gamma \equiv 1$. (B.8) is obvious by the definition. (B.9) $(\alpha \cup \beta)' \equiv \alpha' \cap \beta'$ holds by the following:

$$|(\alpha \cup \beta)'| = \{i \mid 1 - (\alpha \cup \beta)(i) \geqq 1/2\}$$
$$= \{i \mid 1 - \max\{\alpha(i), \beta(i)\} \geqq 1/2\}$$
$$= \{i \mid \min\{1-\alpha(i), 1-\beta(i)\} \geqq 1/2\}$$
$$= |\alpha' \cap \beta'| .$$

(B.10) $(\alpha \cap \beta)' \equiv \alpha' \cup \beta'$ holds similarly to (B.9). (B.11) $\alpha'' \equiv \alpha$ is obvious by the definition. (B.12) $\alpha \cup \alpha' \equiv 1$ holds by the following:

$$|\alpha \cup \alpha'| = \{i \mid \max\{\alpha(i), 1-\alpha(i)\} \geqq 1/2\} = N .$$

By the above, $\mathfrak{M}$ is a quasi-Boolean algebra. q. e. d.

Now we take an element α of $\mathfrak{M}$ such that $\alpha(i) = 1/2$ for any element i of N. Then $\alpha \equiv 1$ and $\alpha' \not\equiv 1'$, because

$$|\alpha'| = \{i \mid 1 - \alpha(i) \geqq 1/2\} = N \quad \text{and} \quad |1'| = \phi .$$

So (I) of Theorem 4 does not hold.

§ 2. A formal system of simple type theory.

We shall introduce a formal system $\mathfrak{S}$ of simple type theory which is obtained from LK by generalization of inference rules from first to higher order predicate calculus, and addition of rules for λ-symbol, but by omitting the cut rule.

1. Inductive definition of *types.*

1.1. 0 and 1 are types.

1.2. If $\tau_1, \cdots, \tau_n$ are types, then $(\tau_1, \cdots, \tau_n)$ is a type.

2. Primitive symbols.

2.1. Free and bound variables of each type:

$a_1^\tau, a_2^\tau, \cdots$ for free variables of type τ,

$x_1^\tau, x_2^\tau, \cdots$ for bound variables of type τ.

Sometimes we omit the upper index.

2.2. An arbitrary number of constants of certain types.

2.3. An arbitrary number of function symbols with certain argument place.

2.4. Logical symbols: $\neg$, $\vee$, $\wedge$, $\exists$, $\forall$, λ, $\in$.

2.5. Parentheses and comma.

3. Inductive definition of *expressions.*

3.1. Every free variable of type τ and every constant of type τ are expressions of type τ.

3.2. If φ is a function symbol with n argument places and $e_1, \cdots, e_n$ are expressions of type 0, then $\varphi(e_1, \cdots, e_n)$ is an expression of type 0.

3.3. If $e_1, \cdots, e_n$ are expressions of type $\tau_1, \cdots, \tau_n$ and e is an expression of type $(\tau_1, \cdots, \tau_n)$, then $(e_1, \cdots, e_n \in e)$ is an expression of type 1.

3.4. If A is an expression of type 1, then $\neg A$ is an expression of type 1.

3.5. If A and B are expressions of type 1, then $(A \vee B)$ and $(A \wedge B)$ are expressions of type 1. (Instead of $(A \vee B)$ and $(A \wedge B)$, we write also $A \vee B$ and $A \wedge B$ when there can be no misunderstanding.)

3.6. If x^τ is a bound variable which does not occur in an expression $A(a^\tau)$ of type 1, then $\exists x^\tau A(x^\tau)$ and $\forall x^\tau A(x^\tau)$ are expressions of type 1.

3.7. If $x_1^{\tau_1}, \cdots, x_n^{\tau_n}$ are different bound variables which do not occur in an expression $A(a_1^{\tau_1}, \cdots, a_n^{\tau_n})$ of type 1, then $\lambda x_1^{\tau_1}, \cdots, x_n^{\tau_n} A(x_1^{\tau_1}, \cdots, x_n^{\tau_n})$ is an expression of type $(\tau_1, \cdots, \tau_n)$.

REMARK. $A(a^\tau)$ denotes an expression containing a^τ in certain distinguished places. The notation may be related to one place, no place, or several places in the expression. $A(x^\tau)$ denotes the result of substituting x^τ for a^τ in the distinguished places of $A(a^\tau)$. In the same way $A(a_1, \cdots, a_n)$ denotes an expression containing distinct variables $a_1, \cdots, a_n$ in certain distinguished places, and $A(x_1, \cdots, x_n)$ or $A(e_1, \cdots, e_n)$ denotes the result of substituting $x_1, \cdots, x_n$ or $e_1, \cdots, e_n$ respectively for $a_1, \cdots, a_n$ in the distinguished places of $A(a_1, \cdots, a_n)$.

Specially we call an expression of type 1 *formula.*

4. Sequent.

A *sequent* is a formal expression of the form

$$A_1, \cdots, A_m \rightarrow B_1, \cdots, B_n,$$

where $m, n \geqq 0$ and $A_1, \cdots, A_m, B_1, \cdots, B_n$ are arbitrary formulas.

5. Rules of inference.

5.1. Logical rules of inference.

Introduction of	in succeedent.	in antecedent.
$\vee$:	$\dfrac{\Gamma \rightarrow \Theta, A}{\Gamma \rightarrow \Theta, A \vee B}, \quad \dfrac{\Gamma \rightarrow \Theta, B}{\Gamma \rightarrow \Theta, A \vee B}.$	$\dfrac{A, \Gamma \rightarrow \Theta \quad B, \Gamma \rightarrow \Theta}{A \vee B, \Gamma \rightarrow \Theta}.$
$\wedge$:	$\dfrac{\Gamma \rightarrow \Theta, A \quad \Gamma \rightarrow \Theta, B}{\Gamma \rightarrow \Theta, A \wedge B}.$	$\dfrac{A, \Gamma \rightarrow \Theta}{A \wedge B, \Gamma \rightarrow \Theta}, \quad \dfrac{B, \Gamma \rightarrow \Theta}{A \wedge B, \Gamma \rightarrow \Theta}.$
$\neg$:	$\dfrac{A, \Gamma \rightarrow \Theta}{\Gamma \rightarrow \Theta, \neg A}.$	$\dfrac{\Gamma \rightarrow \Theta, A}{\neg A, \Gamma \rightarrow \Theta}.$
$\exists$:	$\dfrac{\Gamma \rightarrow \Theta, A(e^\tau)}{\Gamma \rightarrow \Theta, \exists x^\tau A(x^\tau)}.$	$\dfrac{A(a^\tau), \Gamma \rightarrow \Theta}{\exists x^\tau A(x^\tau), \Gamma \rightarrow \Theta}.$
$\forall$:	$\dfrac{\Gamma \rightarrow \Theta, A(a^\tau)}{\Gamma \rightarrow \Theta, \forall x^\tau A(x^\tau)}.$	$\dfrac{A(e^\tau), \Gamma \rightarrow \Theta}{\forall x^\tau A(x^\tau), \Gamma \rightarrow \Theta}.$
$\in$:	$\dfrac{\Gamma \rightarrow \Theta, A(e_1, \cdots, e_n)}{\Gamma \rightarrow \Theta, e_1, \cdots, e_n \in \lambda x_1, \cdots, x_n A(x_1, \cdots, x_n)}.$	
		$\dfrac{A(e_1, \cdots, e_n), \Gamma \rightarrow \Theta}{e_1, \cdots, e_n \in \lambda x_1, \cdots, x_n A(x_1, \cdots, x_n), \Gamma \rightarrow \Theta}.$

5.2. Structural rules of inference.

	in succeedent.	in antecedent.
Thinning	$\dfrac{\Gamma \rightarrow \Theta}{\Gamma \rightarrow \Theta, C}.$	$\dfrac{\Gamma \rightarrow \Theta}{C, \Gamma \rightarrow \Theta}.$
Contraction	$\dfrac{\Gamma \rightarrow \Theta, C, C}{\Gamma \rightarrow \Theta, C}.$	$\dfrac{C, C, \Gamma \rightarrow \Theta}{C, \Gamma \rightarrow \Theta}.$
Interchange	$\dfrac{\Gamma \rightarrow \Theta, C, D, \Lambda}{\Gamma \rightarrow \Theta, D, C, \Lambda}.$	$\dfrac{\Gamma, C, D, \Delta \rightarrow \Theta}{\Gamma, D, C, \Delta \rightarrow \Theta}.$

Stipulation: A, B, C, D are arbitrary formulas; $\Gamma, \Delta, \Theta, \Lambda$ are finite sequences of zero or more formulas; a^τ is a free variable; $e^\tau, e_1, \cdots, e_n$ are expressions; $x^\tau, x_1, \cdots, x_n$ are bound variables; $A(a^\tau)$, $A(e^\tau)$, $A(e_1, \cdots, e_n)$, $\exists x^\tau A(x^\tau)$, and $\forall x^\tau A(x^\tau)$ are formulas of such form.

Restrictions on variables: The free variable denoted by a^τ in the above shemata of the logical rules will never occur in the conclusion of the concerned rules.

6. Proof.

As *formal proofs* we use only ones *in tree form*, each of which has one lowermost sequent—the endsequent—and some uppermost sequents of the form

$$D \to D,$$

where D is an arbitrary formula.

A *proof* of a sequent is a formal proof which has the sequent as the endsequent. A sequent is said to be *provable*, if there exists a proof of the sequent.

For sequents $P_1, \cdots, P_m, Q_1, \cdots, Q_n$, let

$$\frac{P_1, \cdots, P_m}{Q_1, \cdots, Q_n}$$

mean that if $P_1, \cdots, P_m$ are provable, then $Q_1, \cdots, Q_n$ are also provable. Using this notation, the cut-elimination theorem is expressed as follows:

$$\frac{\Gamma \to \Theta, D \quad D, \Delta \to \Lambda}{\Gamma, \Delta \to \Theta, \Lambda,}$$

for arbitrary finite sequences $\Gamma, \Delta, \Theta, \Lambda$ of zero or more formulas and an arbitrary formula D.

7. THEOREM 5.

7.1. $$\frac{\Gamma \to \Theta, A \vee B}{\Gamma \to \Theta, A, B.}$$

7.2. $$\frac{A \vee B, \Gamma \to \Theta}{A, \Gamma \to \Theta,} \qquad \frac{A \vee B, \Gamma \to \Theta}{B, \Gamma \to \Theta.}$$

7.3. $$\frac{\Gamma \to \Theta, A \wedge B}{\Gamma \to \Theta, A,} \qquad \frac{\Gamma \to \Theta, A \wedge B}{\Gamma \to \Theta, B.}$$

7.4. $$\frac{A \wedge B, \Gamma \to \Theta}{A, B, \Gamma \to \Theta.}$$

7.5. $$\frac{\Gamma \to \Theta, \neg A}{A, \Gamma \to \Theta.}$$

7.6. $$\frac{\neg A, \Gamma \to \Theta}{\Gamma \to \Theta, A.}$$

We shall define '*provable with order n*', inductively.

1) Every sequent of the form $D \to D$ is provable with order 0.

2) If the premises of an inference $\to \wedge$ or $\vee \to$[1] are provable with order n_1 and n_2, then the conclusion is provable with order $\max(n_1, n_2)+1$.

3) If the premise of the other inference is provable with order n, then the conclusion is provable with order $n+1$.

When a sequent is provable with order n and is not provable with order $< n$, we say that *order* of the sequent is n.

PROOF OF 7.1. Supposing that a sequent

1) See Kleene [3], p. 443.

$$\Gamma \to \Theta_1, A \vee B, \Theta_2, \cdots, \Theta_n, A \vee B, \Theta_{n+1} \qquad (P)$$

is provable, where $A \vee B$ does not occur in $\Theta_1, \cdots, \Theta_{n+1}$, we shall prove that the sequent

$$\Gamma \to \Theta_1, \cdots, \Theta_n A, B, \Theta_{n+1} \qquad (Q)$$

is provable by mathematical induction on the order of the sequent (P).

Case 1. Let the sequent (P) be provable with order 0. Then (P) is $A \vee B \to A \vee B$, and then (Q) is $A \vee B \to A, B$. Hence (Q) is provable by the following figure.

$$\dfrac{\dfrac{A \to A}{A \to A, B} \quad \dfrac{B \to B}{B \to A, B}}{A \vee B \to A, B}.$$

Case 2. Let the last inference of the proof of the sequent (P) be $\to \vee$ with respect to $A \vee B$, i.e.

$$\dfrac{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A \text{ (or } B)}{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A \vee B}.$$

If $n=1$, (Q) is provable by thinning (or, thinning and interchange). If $n>1$, the following figure shows that (Q) is provable.

$$\dfrac{\dfrac{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A}{\Gamma \to \Theta_1, \cdots, \Theta_{n-1}, A, B, \Theta_n, A}}{\Gamma \to \Theta_1, \cdots, \Theta_{n-1}, \Theta_n, A, B}$$

by hypothesis of induction

Case 3. Let the last inference in the proof of the sequent (P) be not $\to \vee$ with respect to $A \vee B$. If the last inference has one premise, it is of the form

$$\dfrac{\Gamma' \to \Theta'_1, A \vee B, \cdots, \Theta'_m, A \vee B, \Theta'_{m+1}}{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A \vee B, \Theta_{n+1}}. \qquad (*)$$

Then the following figure shows that (Q) is provable.

$$\dfrac{\dfrac{\Gamma' \to \Theta'_1, A \vee B, \cdots, \Theta'_m, A \vee B, \Theta'_{m+1}}{\Gamma' \to \Theta'_1, \cdots, \Theta'_m, A, B, \Theta'_{m+1}}}{\Gamma \to \Theta_1, \cdots, \Theta_n, A, B, \Theta_{n+1}}$$

by the hypothesis of induction
by the same inference rule as (*) or by several structural rules of inference.

When the last inference in the proof of the sequent (P) has two premises (i.e. when the last inference is $\vee \to$ or $\to \wedge$), (Q) can be proved in the same way as the above.

Hence, the proof of

$$\dfrac{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A \vee B, \Theta_{n+1}}{\Gamma \to \Theta_1, \cdots, \Theta_n, A, B, \Theta_{n+1}}$$

is completed. Specially, in the case Θ_{n+1} is empty, we have

$$\dfrac{\dfrac{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A \vee B}{\Gamma \to \Theta_1, \cdots, \Theta_n, A, B}}{\Gamma \to \Theta_1, A \vee B, \cdots, \Theta_n, A, B}.$$

Hence, for any finite sequences Γ and Θ of formulas,

$$\dfrac{\Gamma \to \Theta, A \vee B}{\Gamma \to \Theta, A, B,}$$ q. e. d.

7.2.—7.6. are proved in the same way as 7.1.

§ 3. An algebraic representation of cut-elimination theorem.

We shall show first that formulas of our formal system form a quasi-Boolean algebra.

THEOREM 6. *Let $\mathfrak{S}$ be a set of all formulas of the formal system of simple type theory defined in* § 2. *When A and B are formulas, let $A \leqq B$ mean that*

$$\dfrac{\Gamma \to \Theta, A}{\Gamma \to \Theta, B}$$

for any finite sequences Γ and Θ of formulas. Then $\mathfrak{S}$ is a quasi-Boolean algebra on operations $\vee$, $\wedge$ and $\supset$, where 1 *is an arbitrarily fixed provable formula.*

PROOF.

(B.1): If $A \in \mathfrak{S}$ and $B \in \mathfrak{S}$, then $A \vee B \in \mathfrak{S}$ and $A \wedge B \in \mathfrak{S}$. It is trivial by the definition of formula.

(B.2): $A \leqq A \vee B$ and $B \leqq A \vee B$. Clear by the inference rule $\to \vee$.

(B.3): If $A \leqq C$ and $B \leqq C$, then $A \vee B \leqq C$. Proved by the following figure.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \to \Theta, A \vee B}{\Gamma \to \Theta, A, B}\ \text{by 7.1. in § 2}}{\Gamma \to \Theta, A, C}\ \text{by } B \leqq C}{\dfrac{\Gamma \to \Theta, C, A}{\Gamma \to \Theta, C, C}\ \text{by } A \leqq C}}{\Gamma \to \Theta, C}.$$

(B.4): $A \wedge B \leqq A$ and $A \wedge B \leqq B$. Clear by 7.3. in § 2.

(B.5): If $C \leqq A$ and $C \leqq B$, then $C \leqq A \wedge B$. Proved by the following figure.

$$\dfrac{\dfrac{\Gamma \to \Theta, C}{\Gamma \to \Theta, A \quad \Gamma \to \Theta, B}\ \text{by } C \leqq A \text{ and } C \leqq B}{\Gamma \to \Theta, A \wedge B}.$$

(B.6): $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$. $A \wedge (B \vee C) \geqq (A \wedge B) \vee (A \wedge C)$ holds by (B.2)—(B.4), and $A \wedge (B \vee C) \leqq (A \wedge B) \vee (A \wedge C)$ is shown by the

following figure.

$$\begin{array}{c} \Gamma\to\Theta,\ A\wedge(B\vee C) \\ \hline\hline \Gamma\to\Theta,\ A \qquad\qquad \Gamma\to\Theta,\ B\vee C \\ \hline\hline \Gamma\to\Theta,\ A \qquad \Gamma\to\Theta,\ B,\ A \qquad \Gamma\to\Theta,\ B,\ C \\ \hline \Gamma\to\Theta,\ A,\ A\wedge C \qquad\qquad \Gamma\to\Theta,\ B,\ A\wedge C \\ \hline\hline \Gamma\to\Theta,\ A\wedge B,\ A\wedge C \\ \hline \Gamma\to\Theta,\ (A\wedge B)\vee(A\wedge C)\,. \end{array} \qquad \begin{array}{l} \text{by 7.3. in § 2} \\ \text{by 7.1. in § 2} \end{array}$$

(B.7): If $A<B$, then there is a formula C in $\mathfrak{S}$ such that $A\vee C\not\equiv 1$ and $B\vee C\equiv 1$. Suppose that $A<B$. Then there are sequences Γ, Θ of formulas such that $\Gamma\to\Theta, B$ is provable and $\Gamma\to\Theta, A$ is not provable. Let Γ be $\{D_1, \cdots, D_m\}$ and let Θ be $\{E_1, \cdots, E_n\}$. Then $\to\neg D_1\vee\cdots\vee\neg D_m\vee E_1\vee\cdots\vee E_n\vee B$ is provable and $\to\neg D_1\vee\cdots\vee\neg D_m\vee E_1\vee\cdots\vee E_n\vee A$ is not provable. So if we denote the formula $\neg D_1\vee\cdots\vee\neg D_m\vee E_1\vee\cdots\vee E_n$ by C, we have $A\vee C\not\equiv 1$ and $B\vee C\equiv 1$. Hence there is a formula C in $\mathfrak{S}$ such that $A\vee C\not\equiv 1$ and $B\vee C\equiv 1$.

(B.8): If $A\in\mathfrak{S}$, then $\neg A\in\mathfrak{S}$. Clear by the definition of formula.

(B.9): $\neg(A\vee B)\equiv\neg A\wedge\neg B$. Clear by the following two figures.

$$\begin{array}{c} \Gamma\to\Theta,\ \neg(A\vee B) \\ \hline\hline A\vee B,\ \Gamma\to\Theta \\ \hline\hline A,\ \Gamma\to\Theta \qquad B,\ \Gamma\to\Theta \\ \hline \Gamma\to\Theta,\ \neg A \qquad \Gamma\to\Theta,\ \neg B \\ \hline \Gamma\to\Theta,\ \neg A\wedge\neg B\,. \end{array} \qquad \begin{array}{l} \text{by 7.5. in § 2} \\ \text{by 7.2. in § 2} \end{array}$$

$$\begin{array}{c} \Gamma\to\Theta,\ \neg A\wedge\neg B \\ \hline\hline \Gamma\to\Theta,\ \neg A \qquad \Gamma\to\Theta,\ \neg B \\ \hline\hline A,\ \Gamma\to\Theta \qquad B,\ \Gamma\to\Theta \\ \hline A\vee B,\ \Gamma\to\Theta \\ \hline \Gamma\to\Theta,\ \neg(A\vee B)\,. \end{array} \qquad \begin{array}{l} \text{by 7.3. in § 2} \\ \text{by 7.5. in § 2} \end{array}$$

(B.10): $\neg(A\wedge B)\equiv\neg A\vee\neg B$. Proved similarly to (B.9).

(B.11): $\neg\neg A\equiv A$. $A\leqq\neg\neg A$ is clear by inference rules. $\neg\neg A\leqq A$ is clear by 7.5. and 7.6. in § 2.

(B.12): $A\vee\neg A\equiv 1$. Clear by the fact that $\to A\vee\neg A$ is provable.

THEOREM 7. *For any formula C and sequences $\Gamma, \Delta, \Theta, \Lambda$ of formulas,*

$$\frac{\Gamma\to\Theta,\ C \qquad C,\ \Delta\to\Lambda}{\Gamma,\ \Delta\to\Theta,\ \Lambda} \qquad (\textit{cut-elimination theorem})$$

holds if and only if $A\equiv B$ implies $\neg A\equiv\neg B$ for any formulas A and B.

PROOF. Suppose that

$$\frac{\Gamma\to\Theta,\ C \qquad C,\ \Delta\to\Lambda}{\Gamma,\ \Delta\to\Theta,\ \Lambda}$$

holds for any formula C and sequences $\Gamma, \Delta, \Theta, \Lambda$ of formulas. Then $A \leqq B$ implies $\neg B \leqq \neg A$ as shown by the following figure.

$$\dfrac{\dfrac{\dfrac{A \to A}{A \to B}\ \text{by } A \leqq B \qquad \dfrac{\Gamma \to \Theta, \neg B}{B, \Gamma \to \Theta}\ \text{by 7.5. in § 2}}{A, \Gamma \to \Theta}\ \text{by hypothesis}}{\Gamma \to \Theta, \neg A.}$$

Similarly, $B \leqq A$ implies $\neg A \leqq \neg B$. Hence $A \equiv B$ implies $\neg A \equiv \neg B$.

Inversely, suppose that $A \equiv B$ implies $\neg A \equiv \neg B$ for any formulas A and B. Then $C \wedge \neg C \leqq F$ for any formulas C and F, because

$$C \wedge \neg C \equiv \neg(C \vee \neg C) \equiv \neg(F \vee \neg F) \equiv F \wedge \neg F \leqq F.$$

Now let $\Gamma \to \Theta, C$ and $C, \Delta \to \Lambda$ be provable, where it does not happen that all of sequences $\Gamma, \Delta, \Theta, \Lambda$ are empty, since our formal system is consistent[2]. Let F be a formula contained in Θ or Λ, or a negation of a formula contained in Γ or Δ. Then the following figure shows that $\Gamma, \Delta \to \Theta, \Lambda$ is provable.

$$\dfrac{\dfrac{\dfrac{\dfrac{\Gamma \to \Theta, C \qquad \dfrac{C, \Delta \to \Lambda}{\Delta \to \Lambda, \neg C}}{\Gamma, \Delta \to \Theta, \Lambda, C \wedge \neg C}}{\Gamma, \Delta \to \Theta, \Lambda, F}\ \text{by } C \wedge \neg C \leqq F}{\Gamma, \Delta \to \Theta, \Lambda,}$$

q. e. d.

The condition that $A \equiv B$ implies $\neg A \equiv \neg B$ is the condition (I) of Theorem 4. Hence Theorem 4 shows that conditions (I)—(IV) are algebraic representations of the cut-elimination theorem.

References

[1] G. Gentzen, Untersuchungen über das logische Schliessen, Math. Z., **39** (1935), 176-210, 405-431.

[2] G. Gentzen, Die Widerspruchsfreiheit der Stufenlogik, Math. Z., **41** (1936), 357-366.

[3] S. C. Kleene, Introduction to metamathematics, Amsterdam-Groningen, 1952.

[4] K. Schütte, Sintactical and semantical properties of simple type theory, J. Symbolic logic, **25** (1960), 305-326.

[5] G. Takeuti, On a generalized logic calculus, Japan. J. Math., **23** (1935), 39-96.

2) This can be proved in the almost same way as in Gentzen [2].