APPENDIX

A CONSISTENCY PROOF FOR FORMAL NUMBER THEORY

The first consistency proof for first-order number theory S was given by Gentzen [1936, 1938b]. Since then, other proofs along similar lines have been given by Ackermann [1940], Lorenzen [1951], Schütte [1951, 1960], and Hlodovskii [1959]. As can be expected from Gödel's Second Theorem (cf. page 148), all these proofs use methods which apparently are not available in S. Our exposition will follow Schütte's proof [1951].

The consistency proof will apply to a system S_∞ which is much stronger than S. S_∞ is to have the same individual constant 0 and the same function letters $+, \cdot, '$ as S (cf. pp. 102–103), and the same predicate letter $=$. Thus, S and S_∞ have the same terms and, hence, the same atomic formulas (i.e., formulas $s = t$, where s and t are terms). However, the primitive propositional connectives of S_∞ will be $\vee$ and $\sim$, whereas S had $\supset$ and $\sim$ as its basic connectives. We define a wf of S_∞ to be an expression built up from the atomic formulas by a finite number of applications of the connectives $\vee$ and $\sim$ and of the quantifiers (x_i) $(i = 1, 2, \ldots)$. We let $\mathscr{A} \supset \mathscr{B}$ stand for $(\sim\mathscr{A}) \vee \mathscr{B}$; then any wf of S is an abbreviation of a wf of S_∞.

A closed atomic wf $s = t$ (i.e., an atomic wf containing no variables) is called *correct*, if, when we evaluate s and t according to the usual recursion equations for $+$ and $\cdot$, the same value is obtained for s and t; if different values are obtained, $s = t$ is said to be *incorrect*. Clearly, one can effectively determine whether a given closed atomic wf is correct or incorrect.

As *axioms* of S_∞ we take: (a) all correct closed atomic wfs; (b) negations of all incorrect closed atomic wfs. Thus, for example, $(0'')\cdot(0'') + 0'' = (0''')\cdot(0'')$ and $0' + 0'' \neq 0'\cdot 0''$ are axioms of S_∞.

S_∞ has the following rules of inference:

I. Weak Rules

(a) Exchange: $\dfrac{\mathscr{C} \vee \mathscr{A} \vee \mathscr{B} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{B} \vee \mathscr{A} \vee \mathscr{D}}$

(b) Consolidation: $\dfrac{\mathscr{A} \vee \mathscr{A} \vee \mathscr{D}}{\mathscr{A} \vee \mathscr{D}}$

II. Strong Rules

(a) Dilution: $\dfrac{\mathscr{D}}{\mathscr{A} \vee \mathscr{D}}$ (where $\mathscr{A}$ is any closed wf)

(b) DeMorgan: $\dfrac{\sim\mathscr{A} \vee \mathscr{D} \qquad \sim\mathscr{B} \vee \mathscr{D}}{\sim(\mathscr{A} \vee \mathscr{B}) \vee \mathscr{D}}$

(c) Negation: $\dfrac{\mathscr{A} \vee \mathscr{D}}{\sim\sim\mathscr{A} \vee \mathscr{D}}$

(d) Quantification: $\dfrac{\sim\mathscr{A}(t) \vee \mathscr{D}}{(\sim(x)\mathscr{A}(x)) \vee \mathscr{D}}$ (where t is a closed term)

(e) Infinite Induction: $\dfrac{\mathscr{A}(\overline{n}) \vee \mathscr{D} \quad \text{for all natural numbers n}}{((x)\mathscr{A}(x)) \vee \mathscr{D}}$

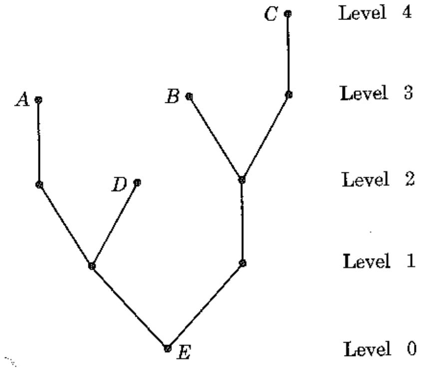
III. Cut: $\dfrac{\mathscr{C} \vee \mathscr{A} \qquad \sim\mathscr{A} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$

In all these rules, the wfs above the line are called *premisses*, and the wfs below the line, *conclusions*. The wfs denoted by $\mathscr{C}$ and $\mathscr{D}$ are called the *side* wfs of the rule; in every rule either or both side wfs may be absent—except that $\mathscr{D}$ must occur in a dilution (II(a)), and at least one of $\mathscr{C}$ and $\mathscr{D}$ in a cut (III). For example, $\dfrac{\mathscr{A} \qquad \sim\mathscr{A} \vee \mathscr{D}}{\mathscr{D}}$ is a cut, and $\dfrac{\sim\mathscr{A} \qquad \sim\mathscr{B}}{\sim(\mathscr{A} \vee \mathscr{B})}$ is an instance of DeMorgan's Rule, II(b). In any rule, the wfs which are not side wfs are called the *principal* wfs; these are the wfs denoted by $\mathscr{A}$ and $\mathscr{B}$ in the presentation above of the rules. The principal wf $\mathscr{A}$ of a cut is called the *cut wf*; the number of propositional connectives and quantifiers in $\sim\mathscr{A}$ is called the *degree* of the cut.

We still must define the notion of a proof in S_∞. Because of the Rule of Infinite Induction this is much more complicated than the notion of proof in S. A *G-tree* is defined to be a graph the points of which can be decomposed into disjoint "levels" as follows: At level 0, there is a single point, called the *terminal point*; each point at level i + 1 is connected by an edge to exactly one point at level i; each point P at level i is connected by edges to either zero, one, two, or denumerably many points at level i + 1 (these latter points at level i + 1 are called the *predecessors* of P); each point at level i is connected only to points at level i − 1 or i + 1; a point at level i not connected to any points at level i + 1 is called an *initial point*.

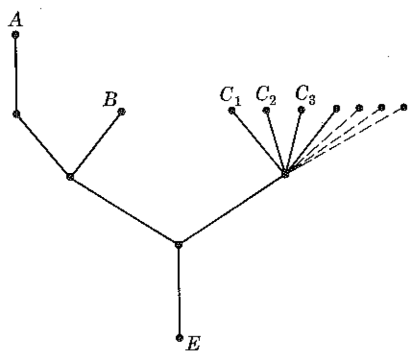
Examples of G-trees.

(1)



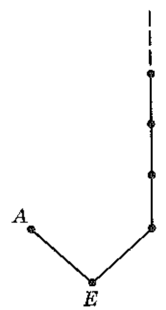
A, B, C, D, are initial points. E is the terminal point.

(2)



A, B, C_1, C_2, C_3, . . . are the initial points. E is the terminal point.

(3)



A is the only initial point.
E is the terminal point.

By a *proof-tree*, we mean an assignment of wfs of S_∞ to the points of a G-tree such that

(1) The wfs assigned to the initial points are axioms of S_∞;

(2) The wfs assigned to a non-initial point P and to the predecessors of P are, respectively, the conclusion and premisses of some rule of inference;

(3) There is a maximal degree of the cuts appearing in the proof-tree. This maximal degree is called the *degree* of the proof-tree. If there are no cuts, the degree is 0;

(4) There is an assignment of an ordinal number to each wf occurring in the proof-tree such that (a) the ordinal of the conclusion of a weak rule is the same as the ordinal of the premiss; (b) the ordinal of the conclusion of a strong rule or a cut is greater than the ordinals of the premisses.

The wf assigned to the terminal point of a proof-tree is called the *terminal wf*; the ordinal of the terminal wf is called the *ordinal* of the proof-tree. The proof-tree is said to be a *proof* of the terminal wf, and the *theorems* of S_∞ are defined to be the wfs which are terminal wfs of proof-trees. Notice that, since all axioms of S_∞ are closed wfs and the rules of inference take closed premisses into closed consequences, all theorems of S_∞ are closed wfs.

A *thread* in a proof-tree is a finite or denumerable sequence $\mathscr{A}_1, \mathscr{A}_2, \ldots$ of wfs starting with the terminal wf and such that each wf $\mathscr{A}_{i+1}$ is a predecessor of $\mathscr{A}_i$. Hence, the ordinals $\alpha_1, \alpha_2, \ldots$ assigned to the wfs in a thread do not increase, and they decrease at each application of a strong rule or a cut. Since there cannot exist a denumerably decreasing sequence of ordinals, it follows that only a finite number of applications of strong rules or cuts can be involved in a thread. Also, to a given wf, only a finite number of applications of weak rules are necessary. Hence, we can assume that there are only a finite number of consecutive applications of weak rules in any thread of a proof-tree. (Let us make this part of the definition of "proof-tree".) Then every thread of a proof-tree is finite.

If we restrict the class of ordinals which may be assigned to the wfs of a proof-tree, then this restricts the notion of a proof-tree, and, therefore, we obtain a (possibly) smaller set of theorems. If one uses various "constructive" segments of denumerable ordinals, then the systems so obtained and the methods used in the consistency proof below may be considered more or less "constructive".

EXERCISE

Prove that the associative rules $\dfrac{(\mathscr{C} \vee \mathscr{A}) \vee \mathscr{B}}{\mathscr{C} \vee (\mathscr{A} \vee \mathscr{B})}$ and $\dfrac{\mathscr{C} \vee (\mathscr{A} \vee \mathscr{B})}{(\mathscr{C} \vee \mathscr{A}) \vee \mathscr{B}}$ are derivable from the exchange rule, assuming association to the left. Hence, parentheses may be omitted from a disjunction.

LEMMA A-1. *Let $\mathscr{A}$ be a closed* wf *having* n *connectives and quantifiers. Then there is a proof of $\sim\mathscr{A} \vee \mathscr{A}$ of ordinal $\leqslant 2n + 1$ (in which no cut is used).*

PROOF. Induction on n.

(1) n = 0. Then $\mathscr{A}$ is a closed atomic wf. Hence, either $\mathscr{A}$ or $\sim\mathscr{A}$ is an axiom, because $\mathscr{A}$ is either correct or incorrect. Hence, by one application of the Dilution Rule, one of the following is a proof-tree.

$$\text{dilution}\ \dfrac{\mathscr{A}}{\sim\mathscr{A} \vee \mathscr{A}} \qquad \text{or} \qquad \dfrac{\dfrac{\sim\mathscr{A}}{\mathscr{A} \vee \sim\mathscr{A}}\ \text{dilution}}{\sim\mathscr{A} \vee \mathscr{A}}\ \text{exchange}$$

Hence, we can assign ordinals so that the proof of $\sim\mathscr{A} \vee \mathscr{A}$ has ordinal 1.

(2) Assume true for all k < n.

Case (i): $\mathscr{A}$ is $\mathscr{A}_1 \vee \mathscr{A}_2$. By inductive hypothesis, there are proofs of $\sim\mathscr{A}_1 \vee \mathscr{A}_1$ and $\sim\mathscr{A}_2 \vee \mathscr{A}_2$ of ordinals $\leqslant 2(n - 1) + 1 = 2n - 1$. By dilution, we obtain proofs of $\sim\mathscr{A}_1 \vee \mathscr{A}_1 \vee \mathscr{A}_2$ and $\sim\mathscr{A}_2 \vee \mathscr{A}_1 \vee \mathscr{A}_2$, respectively, of order 2n, and, by DeMorgan's Rule, a proof of $\sim(\mathscr{A}_1 \vee \mathscr{A}_2) \vee \mathscr{A}_1 \vee \mathscr{A}_2$ of ordinal 2n + 1.

Case (ii): $\mathscr{A}$ is $\sim\mathscr{B}$. Then, by inductive hypothesis, there is a proof of $\sim\mathscr{B} \vee \mathscr{B}$ of ordinal 2n − 1. By the Exchange Rule, we obtain a proof of $\mathscr{B} \vee \sim\mathscr{B}$ of ordinal 2n − 1, and then, applying the Negation Rule, we have a proof of $\sim\sim\mathscr{B} \vee \sim\mathscr{B}$, i.e., of $\sim\mathscr{A} \vee \mathscr{A}$, of ordinal $2n \leqslant 2n + 1$.

Case (iii): $\mathscr{A}$ is $(x)\mathscr{B}(x)$. By inductive hypothesis, for every natural number k, there is a proof of $\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k})$ of ordinal $\leqslant 2n - 1$. Then, by the Quantification Rule, for each k there is a proof of $(\sim(x)\mathscr{B}(x)) \vee \mathscr{B}(\overline{k})$ of ordinal $\leqslant 2n$ and, hence, by the Exchange Rule, a proof of $\mathscr{B}(\overline{k}) \vee \sim(x)\mathscr{B}(x)$ of ordinal $\leqslant 2n$. Finally, by an application of the Infinite Induction Rule, we obtain a proof of $((x)\mathscr{B}(x)) \vee \sim(x)\mathscr{B}(x)$ of ordinal $\leqslant 2n + 1$, and, by the Exchange Rule, a proof of $(\sim(x)\mathscr{B}(x)) \vee (x)\mathscr{B}(x)$ of ordinal $\leqslant 2n + 1$.

LEMMA A-2. *For any closed terms t and s, and any* wf *$\mathscr{A}(x)$ with x as its only free variable, the* wf *$s \neq t \vee \sim\mathscr{A}(s) \vee \mathscr{A}(t)$ is a theorem of S_∞ and is provable without applying the Cut Rule.*

PROOF. In general, if a closed wf $\mathscr{B}(t)$ is provable in S_∞, and s has the same value as t, then $\mathscr{B}(s)$ is also provable in S_∞. (Simply replace all occurrences of t which are "deductively connected" with the t in the terminal wf $\mathscr{B}(t)$ by s.) Now, if s has the same value $\overline{n}$ as t, then, since $\sim\mathscr{A}(\overline{n}) \vee \mathscr{A}(\overline{n})$ is provable, it follows by the previous remark that $\sim\mathscr{A}(s) \vee \mathscr{A}(t)$ is provable. Hence, by dilution, $s \neq t \vee \sim\mathscr{A}(s) \vee \mathscr{A}(t)$ is provable. If s and t have different values, $s = t$ is incorrect; hence, $s \neq t$ is an axiom. So, by dilution and exchange, $s \neq t \vee \sim\mathscr{A}(s) \vee \mathscr{A}(t)$ is a theorem.

LEMMA A-3, *Every closed* wf *which is a theorem of* S *is also a theorem of S_∞.*

PROOF. Let $\mathscr{A}$ be a closed wf which is a theorem of S. Clearly, every proof in S can be represented in the form of a finite proof-tree, where the initial wfs are axioms of S and the rules of inference are modus ponens and generalization. Let n be an ordinal assigned to such a proof-tree for $\mathscr{A}$.

If n = 0, then $\mathscr{A}$ is an axiom of S (cf. page 103).

(1) $\mathscr{A}$ is $\mathscr{B} \supset (\mathscr{C} \supset \mathscr{B})$, i.e., $\sim\mathscr{B} \vee (\sim\mathscr{C} \vee \mathscr{B})$. But, $\sim\mathscr{B} \vee \mathscr{B}$ is provable in S_∞ (Lemma A-1). Hence, so is $\sim\mathscr{B} \vee \sim\mathscr{C} \vee \mathscr{B}$ by a dilution and an exchange.

(2) $\mathscr{A}$ is $(\mathscr{B} \supset (\mathscr{C} \supset \mathscr{D}) \supset ((\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{B} \supset \mathscr{D}))$, i.e., $\sim(\sim\mathscr{B} \vee \sim\mathscr{C} \vee \mathscr{D}) \vee \sim(\sim\mathscr{B} \vee \mathscr{C}) \vee (\sim\mathscr{B} \vee \mathscr{D})$. By Lemma A-1, we have $\sim(\sim\mathscr{B} \vee \mathscr{C}) \vee \sim\mathscr{B} \vee \mathscr{C}$ and $(\sim\mathscr{B} \vee \sim\mathscr{C} \vee \mathscr{D}) \vee \sim(\sim\mathscr{B} \vee \sim\mathscr{C} \vee \mathscr{D})$. Then, by exchange, a cut (with $\mathscr{C}$ as cut formula), and consolidation, $\sim(\sim\mathscr{B} \vee \sim\mathscr{C} \vee \mathscr{D}) \vee \sim(\sim\mathscr{B} \vee \mathscr{C}) \vee \sim\mathscr{B} \vee \mathscr{D}$ is provable.

(3) $\mathscr{A}$ is $(\sim\mathscr{B} \supset \sim\mathscr{A}) \supset ((\sim\mathscr{B} \supset \mathscr{A}) \supset \mathscr{B}))$, i.e., $\sim(\sim\sim\mathscr{B} \vee \sim\mathscr{A}) \vee \sim(\sim\sim\mathscr{B} \vee \mathscr{A}) \vee \mathscr{B}$. Now, by Lemma A-1 we have $\sim\mathscr{B} \vee \mathscr{B}$, and then, by the Negation Rule, $\sim\sim\sim\mathscr{B} \vee \mathscr{B}$, and, by dilution and exchange,

(a) $\sim\sim\sim\mathscr{B} \vee \sim(\sim\sim\mathscr{B} \vee \mathscr{A}) \vee \mathscr{B}$.

Similarly, we obtain $\sim\sim\sim\mathscr{B} \vee \mathscr{B} \vee \sim\sim\mathscr{A}$ and $\sim\mathscr{A} \vee \mathscr{B} \vee \sim\sim\mathscr{A}$, and by DeMorgan's Rule, $\sim(\sim\sim\mathscr{B} \vee \mathscr{A}) \vee \mathscr{B} \vee \sim\sim\mathscr{A}$; then, by exchange,

(b) $\sim\sim\mathscr{A} \vee \sim(\sim\sim\mathscr{B} \vee \mathscr{A}) \vee \mathscr{B}$.
From (a) and (b), by DeMorgan's Rule, we have $\sim(\sim\sim\mathscr{B} \vee \sim\mathscr{A}) \vee \sim(\sim\sim\mathscr{B} \vee \mathscr{A}) \vee \mathscr{B}$.

(4) $\mathscr{A}$ is $(x)\mathscr{B}(x) \supset \mathscr{B}(t)$, i.e., $(\sim(x)\mathscr{B}(x)) \vee \mathscr{B}(t)$. Then, by Lemma A-1, we have $\sim\mathscr{B}(t) \vee \mathscr{B}(t)$; by the Quantification Rule, $(\sim(x)\mathscr{B}(x)) \vee \mathscr{B}(t)$.

(5) $\mathscr{A}$ is $(x)(\mathscr{B} \supset \mathscr{C}) \supset (\mathscr{B} \supset (x)\mathscr{C})$, where x is not free in $\mathscr{B}$, i.e., $\sim(x)(\sim\mathscr{B} \vee \mathscr{C}(x)) \vee \sim\mathscr{B} \vee (x)\mathscr{C}(x)$. Now, by Lemma A-1, for every natural number n, there is a proof of $\sim(\sim\mathscr{B} \vee \mathscr{C}(\overline{n})) \vee \sim\mathscr{B} \vee \mathscr{C}(\overline{n})$. (Note that the ordinals of these proofs are bounded by $2k + 1$, where k is the number of propositional connectives and quantifiers in $\sim\mathscr{B} \vee \mathscr{C}(x)$.)

Hence, by the Quantification Rule, for each n, there is a proof of

$$\sim(x)(\sim\mathscr{B} \vee \mathscr{C}(x)) \vee \sim\mathscr{B} \vee \mathscr{C}(\overline{n}) \quad (\text{of ordinal} \leqslant 2k + 2)$$

Hence, by exchange and infinite induction, there is a proof of

$$\sim(x)(\sim\mathscr{B} \vee \mathscr{C}(x)) \vee \sim\mathscr{B} \vee (x)\mathscr{C}(x) \quad (\text{of ordinal} \leqslant 2k + 3)$$

(S1) $\mathscr{A}$ is $t_1 = t_2 \supset (t_1 = t_3 \supset t_2 = t_3)$, i.e., $t_1 \neq t_2 \vee t_1 \neq t_3 \vee t_2 = t_3$. Apply Lemma A-2, with $x = t_3$ as $\mathscr{A}(x)$, t_1 as s, t_2 as t.

(S2) $\mathscr{A}$ is $t_1 = t_2 \supset (t_1)' = (t_2)'$, i.e., $t_1 \neq t_2 \vee (t_1)' = (t_2)'$. If t_1 and t_2 have the same value, then so do $(t_1)'$ and $(t_2)'$. Hence $(t_1)' = (t_2)'$ is correct and therefore an axiom. By dilution, we obtain $t_1 \neq t_2 \vee (t_1)' = (t_2)'$. If t_1 and t_2 have different values, $t_1 \neq t_2$ is an axiom; hence, by dilution and exchange, $t_1 \neq t_2 \vee (t_1)' = (t_2)'$ is provable.

(S3) $\mathscr{A}$ is $0 \neq t'$. 0 and t' have different values; hence, $0 \neq t'$ is an axiom.

(S4) $\mathscr{A}$ is $(t_1)' = (t_2)' \supset t_1 = t_2$, i.e., $(t_1)' \neq (t_2)' \vee t_1 = t_2$. (Exercise.)

(S5) $\mathscr{A}$ is $t + 0 = t$. $t + 0$ and t have the same values. Hence, $t + 0 = t$ is an axiom.

(S6)–(S8) follow similarly from the recursion equations for evaluating closed terms.

(S9) $\mathscr{A}$ is $\mathscr{B}(0) \supset ((x)(\mathscr{B}(x) \supset \mathscr{B}(x')) \supset (x)\mathscr{B}(x))$, i.e.,

$$\sim\mathscr{B}(0) \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee (x)\mathscr{B}(x)$$

(1) Clearly, by Lemma A-1, exchange and dilution,

$\sim\mathscr{B}(0) \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(0)$ is provable.

(2) For $k \geqslant 0$, let us prove by induction that the following wf is provable:

$\sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \ldots \vee \sim(\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k}')) \vee \mathscr{B}(\overline{k}')$.

(a) For $k = 0$; $\vdash_{S_\infty} \sim\sim\mathscr{B}(0) \vee \sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})$ by Lemma A-1, dilution, and exchange; similarly, $\vdash_{S_\infty} \sim\mathscr{B}(\overline{1}) \vee \sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})$. Hence, by DeMorgan's Rule, $\vdash_{S_\infty} \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})$, and, by exchange,

$$\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \mathscr{B}(\overline{1})$$

(b) Assume for k:

$$\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \ldots \vee \sim(\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k}')) \vee \mathscr{B}(\overline{k}')$$

Hence, by exchange, negation, and dilution,

$$\vdash_{S_\infty} \sim\sim\mathscr{B}(\overline{k}') \vee \sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \ldots \vee \sim(\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k}')) \vee \mathscr{B}(\overline{k}'')$$

Also, by Lemma A-1 for $\mathscr{B}(\overline{k}'')$, dilution and exchange,

$$\vdash_{S_\infty} \sim\mathscr{B}(\overline{k}'') \vee \sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \ldots \vee \sim(\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k}')) \vee \mathscr{B}(\overline{k}''),$$

Hence, by DeMorgan's Rule,

$$\vdash_{S_\infty} \sim(\sim\mathscr{B}(\overline{k}') \vee \mathscr{B}(\overline{k}'')) \vee \sim\mathscr{B}(0) \vee \sim(\sim\mathscr{B}(0) \vee \mathscr{B}(\overline{1})) \vee \ldots \vee \sim(\sim\mathscr{B}(\overline{k}) \vee \mathscr{B}(\overline{k}')) \vee \mathscr{B}(\overline{k}''))$$

and, by exchange, the result follows for $k + 1$.

Now, applying the exchange and quantification rules k times to the result of (2), we have, for each $k \geqslant 0$,

$$\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(x)(\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \ldots \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(\overline{k}')$$

and, by consolidation, $\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(\overline{k}')$. Hence, together with (1), we have, for all $k \geqslant 0$,

$$\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee \mathscr{B}(\overline{k})$$

Then, by infinite induction,

$$\vdash_{S_\infty} \sim\mathscr{B}(0) \vee \sim(x)(\sim\mathscr{B}(x) \vee \mathscr{B}(x')) \vee (x)\mathscr{B}(x)$$

Thus, all the closed axioms of S are provable in S_∞. We assume now that $n > 0$. Then, (i) $\mathscr{A}$ may arise by modus ponens from $\mathscr{B}$ and $\mathscr{B} \supset \mathscr{A}$, where $\mathscr{B}$ and $\mathscr{B} \supset \mathscr{A}$ have smaller ordinals in the proof-tree. We may assume that $\mathscr{B}$ contains no free variables, since we can replace any such free variables by 0 in $\mathscr{B}$ and its predecessors in the proof-tree.

Hence, by inductive hypothesis, $\vdash_{S_\infty} \mathscr{B}$ and $\vdash_{S_\infty} \mathscr{B} \supset \mathscr{A}$, i.e., $\vdash_{S_\infty} \sim\mathscr{B} \vee \mathscr{A}$. Hence, by a cut, we obtain $\vdash_{S_\infty} \mathscr{A}$. The other possibility (ii) is that $\mathscr{A}$ is $(x)\mathscr{B}(x)$ and comes by generalization from $\mathscr{B}(x)$. Now, in the proof-tree, working backwards from $\mathscr{B}(x)$, replace the appropriate free occurrences of x by $\bar{n}$. We then obtain a proof of $\mathscr{B}(\bar{n})$, of the same ordinal. This holds for all n; by inductive hypothesis, $\vdash_{S_\infty} \mathscr{B}(\bar{n})$ for all n. Hence, by infinite induction, $\vdash_{S_\infty} (x)\mathscr{B}(x)$, i.e., $\vdash_{S_\infty} \mathscr{A}$.

COROLLARY A-4. *If* S_∞ *is consistent*, S *is consistent.*

PROOF. If S is inconsistent, then $\vdash_S 0 \neq 0$. Hence, by Lemma A-3, $\vdash_{S_\infty} 0 \neq 0$. But, $\vdash_{S_\infty} 0 = 0$, since $0 = 0$ is correct. For any wf $\mathscr{A}$ of S_∞, we would have, by dilution, $\vdash_{S_\infty} 0 \neq 0 \vee \mathscr{A}$, and, together with $\vdash_{S_\infty} 0 = 0$, by a cut, $\vdash_{S_\infty} \mathscr{A}$. Thus, any wf of S_∞ is provable; so, S_∞ is inconsistent.

By Corollary A-4, to prove the consistency of S it suffices to show the consistency of S_∞.

LEMMA A-5. *The rules of DeMorgan, negation, and infinite induction are invertible, i.e., from a proof of a wf which is a consequence of some premisses by one of these rules one can obtain a proof of the premisses (and the ordinal and degree of such a proof are no higher than the ordinal and degree of the original proof).*

PROOF

(1) DeMorgan. $\mathscr{A}$ is $\sim(\mathscr{B} \vee \mathscr{E}) \vee \mathscr{D}$. Take a proof of $\mathscr{A}$. Take all those subformulas $\sim(\mathscr{B} \vee \mathscr{E})$ of wfs of the proof-tree obtained by starting with $\sim(\mathscr{B} \vee \mathscr{E})$ in $\mathscr{A}$ and working back up the proof-tree. This process continues through all applications of weak rules and through all strong rules in which $\sim(\mathscr{B} \vee \mathscr{E})$ is part of a side wf. It can end only at dilutions $\dfrac{\mathscr{F}}{\sim(\mathscr{B} \vee \mathscr{E}) \vee \mathscr{F}}$ or applications of DeMorgan's Rule: $\dfrac{\sim\mathscr{B} \vee \mathscr{F} \quad \sim\mathscr{E} \vee \mathscr{F}}{\sim(\mathscr{B} \vee \mathscr{E}) \vee \mathscr{F}}$. The set of all occurrences of $\sim(\mathscr{B} \vee \mathscr{E})$ obtained by this process is called the *history* of $\sim(\mathscr{B} \vee \mathscr{E})$. Let us replace all occurrences of $\sim(\mathscr{B} \vee \mathscr{E})$ in its history by $\sim\mathscr{B}$. Then we still have a proof-tree (after unnecessary formulas are erased), and the terminal wf is $\sim\mathscr{B} \vee \mathscr{D}$. Similarly, if we replace $\sim(\mathscr{B} \vee \mathscr{E})$ by $\sim\mathscr{E}$ we obtain a proof of $\sim\mathscr{E} \vee \mathscr{D}$.

(2) Negation. $\mathscr{A}$ is $\sim\sim\mathscr{B} \vee \mathscr{D}$. Define the history of $\sim\sim\mathscr{B}$ as was done for $\sim(\mathscr{B} \vee \mathscr{E})$ in (1); replace all occurrences of $\sim\sim\mathscr{B}$ in its history by $\mathscr{B}$; the result is a proof of $\mathscr{B} \vee \mathscr{D}$.

(3) Infinite Induction. $\mathscr{A}$ is $((x)\mathscr{B}(x)) \vee \mathscr{D}$. Define the history of $(x)\mathscr{B}(x)$ as in (1); replace $(x)\mathscr{B}(x)$ in its history by $\mathscr{B}(\bar{n})$ (and if one of the initial occurrences in its history appears as the consequence of an infinite induction, erase the tree above all the premisses except the one involving $\bar{n}$); we then obtain a proof of $\mathscr{B}(\bar{n}) \vee \mathscr{D}$.

LEMMA A-6 (Schütte [1951]: Reduktionssatz). *Given a proof of* $\mathscr{A}$ *in* S_∞ *of positive degree m and ordinal* α, *there is a proof of* $\mathscr{A}$ *in* S_∞ *of lower degree and ordinal* 2^α (cf. page 178).

PROOF. By transfinite induction on the ordinal α of the given proof of $\mathscr{A}$. $\alpha = 0$: this proof can contain no cuts and, hence, has degree 0. Assume the theorem proved for all ordinals $< \alpha$. Starting from the terminal wf $\mathscr{A}$, find the first application of a non-weak rule, i.e., of a strong rule or a cut. If it is a strong rule, each premiss has ordinal $\alpha_i < \alpha$. By inductive hypothesis, for these premisses, there are proof-trees of lower degree and ordinal 2^{α_i}. Substitute these proof-trees for the proof-trees above the premisses in the original proof. We thus obtain a new proof for $\mathscr{A}$ except that the ordinal of $\mathscr{A}$ should be taken to be 2^α, which is greater than every 2^{α_i} (cf. Proposition 4.30(9)).

The remaining case is that of a cut.

$$\frac{\mathscr{C} \vee \mathscr{B} \quad \sim\mathscr{B} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$$

If the ordinals of $\mathscr{C} \vee \mathscr{B}$ and $\sim\mathscr{B} \vee \mathscr{D}$ are α_1, α_2, then, by inductive hypothesis, we can replace the proof-trees above them so that the degrees are reduced and the ordinals are 2^{α_1}, 2^{α_2}, respectively. We shall distinguish various cases according to the form of the cut formula $\mathscr{B}$.

(a) $\mathscr{B}$ is an atomic wf. Either $\mathscr{B}$ or $\sim\mathscr{B}$ must be an axiom. Let $\mathscr{K}$ be the non-axiom of $\mathscr{B}$ and $\sim\mathscr{B}$. By inductive hypothesis, the proof-tree above the premiss containing $\mathscr{K}$ can be replaced by a proof-tree with lower degree having ordinal 2^{α_i} (i = 1 or 2). In this new proof-tree, consider the history of $\mathscr{K}$ (as defined in the proof of Lemma A-5). The initial wfs in this history can arise only by dilutions. So, if we erase all occurrences of $\mathscr{K}$ in this history, we obtain a proof-tree for $\mathscr{C}$ or for $\mathscr{D}$ of ordinal 2^{α_i}; then, by a dilution, we obtain $\mathscr{C} \vee \mathscr{D}$, of ordinal 2^α. The degree of the new proof-tree is less than m.

(b) $\mathscr{B}$ is $\sim\mathscr{E}$: $\dfrac{\mathscr{C} \vee \sim\mathscr{E} \quad \sim\sim\mathscr{E} \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$

There is a proof-tree for $\sim\sim\mathscr{E} \vee \mathscr{D}$ of degree $<$m and ordinal 2^{α_2}. By Lemma A-5, there is a proof-tree for $\mathscr{E} \vee \mathscr{D}$ of degree $<$m and ordinal 2^{α_2}. There is also, by inductive hypothesis, a proof-tree for $\mathscr{C} \vee \sim\mathscr{E}$ of degree $<$m and ordinal 2^{α_1}. Now, construct

$$\begin{array}{ccc} \text{Exchange}\ \dfrac{\begin{array}{c}\vdots\\ \mathscr{E} \vee \mathscr{D}\end{array}}{\mathscr{D} \vee \mathscr{E}} & & \dfrac{\begin{array}{c}\vdots\\ \mathscr{C} \vee \sim\mathscr{E}\end{array}}{\sim\mathscr{E} \vee \mathscr{C}}\ \text{Exchange} \\ & \text{Cut} & \\ & \dfrac{\mathscr{D} \vee \mathscr{C}}{\mathscr{C} \vee \mathscr{D}}\ \text{Exchange} & \end{array}$$

The degree of the indicated cut is the degree of $\sim\mathscr{E}$ which is one less than the degree of $\sim\sim\mathscr{E}$, which, in turn, is $\leqslant$m. The ordinal of $\mathscr{D} \vee \mathscr{C}$ can be taken to be 2^{α}. Hence, we have a proof of lower degree and ordinal 2^{α}.

(c) $\mathscr{B}$ is $\mathscr{E} \vee \mathscr{F}$: $\dfrac{\mathscr{C} \vee \mathscr{E} \vee \mathscr{F} \quad \sim(\mathscr{E} \vee \mathscr{F}) \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$

There is a proof-tree for $\sim(\mathscr{E} \vee \mathscr{F}) \vee \mathscr{D}$ of lower degree and ordinal 2^{α_2}. Hence, by Lemma A-5, there are proof-trees for $\sim\mathscr{E} \vee \mathscr{D}$ and $\sim\mathscr{F} \vee \mathscr{D}$ of degree $<$m and ordinal 2^{α_2}. There is also a proof-tree for $\mathscr{C} \vee \mathscr{E} \vee \mathscr{F}$ of degree $<$m and ordinal 2^{α_1}. Construct:

$$\begin{array}{lccc} & \vdots & \vdots & \\ & \mathscr{C} \vee \mathscr{E} \vee \mathscr{F} & \sim\mathscr{F} \vee \mathscr{D} & \\ \text{Cut} & & & \\ & \mathscr{C} \vee \mathscr{E} \vee \mathscr{D} & & \\ \text{Exchange} & & & \vdots \\ & \mathscr{C} \vee \mathscr{D} \vee \mathscr{E} & & \sim\mathscr{E} \vee \mathscr{D} \\ \text{Cut} & & & \\ & & \mathscr{C} \vee \mathscr{D} \vee \mathscr{D} & \\ \text{Consolidation} & & & \\ & & \mathscr{C} \vee \mathscr{D} & \end{array}$$

The cuts indicated have degrees $<$m; hence, the new proof-tree has degree $<$m; the ordinal of $\mathscr{C} \vee \mathscr{E} \vee \mathscr{D}$ can be taken as $2^{\max(\alpha_1, \alpha_2)} +_0 1$, and then the ordinal of $\mathscr{C} \vee \mathscr{D} \vee \mathscr{D}$ and $\mathscr{C} \vee \mathscr{D}$ as 2^{α}.

(d) $\mathscr{B}$ is $(x)\mathscr{E}$: $\dfrac{\mathscr{C} \vee (x)\mathscr{E} \quad (\sim(x)\mathscr{E}) \vee \mathscr{D}}{\mathscr{C} \vee \mathscr{D}}$

By inductive hypothesis, the proof-tree above $\mathscr{C} \vee (x)\mathscr{E}$ can be replaced by one with smaller degree and ordinal 2^{α_1}. By Lemma A-5 and the remark at the beginning of the proof of Lemma A-2, we can obtain proofs of $\mathscr{C} \vee \mathscr{E}(t)$ of degree $<$m and ordinal 2^{α}, for any closed term t. Now, the proof-tree above the right-hand formula $(\sim(x)\mathscr{E}) \vee \mathscr{D}$ can be replaced, by inductive hypothesis, by one with smaller degree and ordinal 2^{α_2}. The history of $\sim(x)\mathscr{E}$ in this proof terminates above either at dilutions or as principal wfs in applications of the Quantification Rule:

$$\begin{array}{c} \sim\mathscr{E}(t_i) \vee \mathscr{G}_i \\ \\ (\sim(x)\mathscr{E}) \vee \mathscr{G}_1 \end{array}$$

Replace every such application by the cut

$$\begin{array}{ccc} \mathscr{C} \vee \mathscr{E}(t_i) & & (\sim\mathscr{E}(t_i)) \vee \mathscr{G}_1 \\ \\ & \mathscr{C} \vee \mathscr{G}_i & \end{array}$$

Replace all occurrences in the history of $\sim(x)\mathscr{E}(x)$ by $\mathscr{C}$. The result is still a proof-tree, and the terminal wf is $\mathscr{C} \vee \mathscr{D}$. The proof-tree has degree $<$m, since the degree of $\sim\mathscr{E}(t_i)$ is less than the degree of $\sim(x)\mathscr{E}$. Replace each old ordinal β of the proof-tree by $2^{\alpha_1} +_0 \beta$. If β was the ordinal of the premiss $\sim\mathscr{E}(t) \vee \mathscr{G}_i$ of an eliminated Quantification Rule application above, and if γ was the ordinal of the conclusion $(\sim(x)\mathscr{E}) \vee \mathscr{G}_i$, then, in the new cut introduced, $\mathscr{C} \vee \mathscr{E}(t)$ has ordinal 2^{α_1}, $\sim\mathscr{E}(t_i) \vee \mathscr{G}_i$ has ordinal $2^{\alpha_1} +_0 \beta$, and the conclusion $\mathscr{C} \vee \mathscr{G}_i$ has ordinal $2^{\alpha_1} +_0 \gamma > \max(2^{\alpha_1}, 2^{\alpha_1} +_0 \beta)$. At all other places, the ordinal of the conclusion is still greater than the ordinal of the premisses, since $\delta <_0 \mu$ implies $2^{\alpha_1} +_0 \delta <_0 2^{\alpha_1} +_0 \mu$. Finally, the right-hand premiss $(\sim(x)\mathscr{E}) \vee \mathscr{D}$ (originally of ordinal α_2) goes over into $\mathscr{C} \vee \mathscr{D}$ with ordinal $2^{\alpha_1} +_0 2^{\alpha_2} \leqslant 2^{\max(\alpha_1, \alpha_2)} +_0 2^{\max(\alpha_1, \alpha_2)} = 2^{\max(\alpha_1, \alpha_2)} \times_0 2 = 2^{\max(\alpha_1, \alpha_2) +_0 1} \leqslant 2^{\alpha}$. If this is $<_0 2^{\alpha}$, the ordinal of $\mathscr{C} \vee \mathscr{D}$ can be raised to 2^{α}.

COROLLARY A-7. *Every proof of $\mathscr{A}$ of ordinal α and degree m can be replaced by a proof of $\mathscr{A}$ of ordinal* $2^{2^{\cdot^{\cdot^{\cdot^{2^{(2^{\alpha})}}}}}}$ *and degree* 0 (*i.e., a cut-free proof*).

PROPOSITION A-8. S_∞ *is consistent.*

PROOF. Consider any wf $\mathscr{A}$ of the form $(0 \neq 0) \vee (0 \neq 0) \vee \ldots \vee (0 \neq 0)$. If there is a proof of $\mathscr{A}$, then by Corollary A-7, there is a cut-free proof of $\mathscr{A}$. By inspection of the rules of inference, $\mathscr{A}$ can be derived only from other wfs of the same form: $(0 \neq 0) \vee \ldots \vee (0 \neq 0)$. Hence, the axioms of the proof would have to be of this form. But there are no axioms of this form; hence, $\mathscr{A}$ is unprovable. Therefore, S_∞ is consistent.

EXERCISE

If no restriction is placed upon the class of ordinals which can be attached to proofs: (1) S_∞ is ω-consistent (Hint: Corollary A-7, Proposition A-8, and the Rule of Infinite Induction). (2) Every closed wf of S_∞ which is true for the standard model is provable. Hence, S_∞ would be complete.

To reduce the non-constructive aspect of the consistency proof, one can restrict the class of ordinals which can be assigned to wfs of a proof-tree. Consider the set of ordinals $\{\omega, \omega^\omega, \omega^{\omega^\omega}, \ldots\}$ (defined inductively by: $\gamma_0 = \omega, \gamma_{n+1} = \omega^{\gamma_n}$). Let us denote the least upper bound of this set by ε_0. If we use only ordinals $<_0 \varepsilon_0$, then all the proofs given above still go through (for, if $\delta <_0 \varepsilon_0$, then $2^\delta <_0 \varepsilon_0$). In addition, the ordinals $<_0 \varepsilon_0$ can be written down in a certain standard "polynomial" notation: (i) the ordinals $<_0 \omega^\omega$ can be written in the form

$$(\omega^{k_1} \times_0 n_1) +_0 (\omega^{k_2} \times_0 n_2) +_0 \ldots +_0 (\omega^{k_l} \times_0 n_l)$$

where $k_1, k_2, \ldots, k_l$ is a decreasing sequence of finite ordinals, and $n_1, n_2, \ldots, n_l$ are finite ordinals; (ii) the ordinals between ω^ω and ω^{ω^ω} can be written in the form $(\omega^{\alpha_1} \times_0 n_1) +_0 (\omega^{\alpha_2} \times_0 n_2) +_0 \ldots +_0 (\omega^{\alpha_l} \times_0 n_l)$ where $\alpha_1, \alpha_2, \ldots, \alpha_l$ is a decreasing sequence of ordinals $<_0 \omega^\omega$ and $n_1, n_2, \ldots, n_l$ are finite ordinals, etc. (cf. Bachmann [1955], III; Gentzen [1938b]).

The chief non-constructive aspect of the consistency proof was the use of transfinite induction in the proof of Lemma A-6. The principle of transfinite induction up to a given ordinal has been formalized and studied by Gentzen [1943] and Schütte [1951, 1960]; as was to be expected, transfinite induction up to ε_0, is not derivable in S. Whether

or not certain concepts and assumptions (such as denumerable ordinals and transfinite induction up to ε_0) should really be considered "constructive" seems ultimately to be a subjective matter. For further details and discussion, in addition to the references already given, cf. Hilbert-Bernays [1939], Rosser [1937], Müller [1961], and Shoenfield [1959].