ON THE LENGTHS OF PROOFS
IN THE PROPOSITIONAL CALCULUS

ROBERT A. RECKHOW

1976

a slight generalization of these systems (the Gentzen system for sets of clauses) is no less powerful than enumeration dags and regular resolution. This means that the two main families of systems in the neighbourhood of the double solid line, cut-free Gentzen systems and extension-free resolution-based systems, are interrelated, and probably have similar bounds on proof lengths.

5.3. FREGE SYSTEM SIMULATIONS

In this section various simulations between Frege systems are established. The most important results are in subsection 5.3.1., where it is shown that any two Frege systems can simulate each other. Subsection 5.3.2. introduces the idea of extended Frege systems, and shows how they simulate ordinary Frege systems and each other. The final subsection of this section is 5.3.3., where it is shown that s-Frege systems simulate extended Frege systems and each other.

5.3.1. Frege Systems without the Substitution Rule

Recall from subsection 4.2.1. that a Frege system is an implicationally complete system $\mathcal{F}=\langle\kappa,\mathcal{R}\rangle$, where κ is an adequate set of connectives and $\mathcal{R}$ is a finite set of sound rules of inference in the connectives κ.

The proof that any two Frege systems simulate each other will proceed in a series of easy stages. Paragraph 5.3.1.1. introduces the notion of "direct translation", and discusses some of the useful properties of direct translations. Paragraph 5.3.1.2. proves in a series of stages that if there are direct translations between the connectives of two Frege systems, then those systems simulate each other. Indirect translations and their properties are discussed in paragraph 5.3.1.3. Finally in paragraph 5.3.1.4. it is shown that two arbitrary Frege systems simulate each other.

5.3.1.1. Direct Translation

In order to compare Frege systems that operate on formulas with different sets of connectives, a way must be found to relate formulas with different connectives. At least three such methods are employed in this thesis, the first of which is called *direct translation*.

Let κ_1 and κ_2 be sets of connectives, and for $i=1,2$ let K_i be the set of formulas in the connectives $\kappa_i=\{*_i^1,\ldots,*_i^{k_i}\}$. For $1\le j\le k_i$, let $A_i^j=*_i^j(p_1,\ldots,p_n)$, where $n=n^{*_i^j}$. The formulas $\{A_i^j \mid 1\le j\le k_i\}$ are called the *primitive formulas* of κ_i. If $t:K_1\to K_2$ and $\sigma=\dfrac{B_1,\ldots,B_n}{q_1,\ldots,q_n}$ is a substitution in κ_1, then $t(\sigma)=\dfrac{t(B_1)\ldots t(B_n)}{q_1\ldots q_n}$ is a substitution in κ_2. The function $t:K_1\to K_2$ is called a *direct translation* from κ_1 to κ_2 if there exists a polynomial $p(n)$ such that for all formulas $B\in K_1$ and for all substitutions σ in κ_1,

1) $t(B)\sim B$,

2) $\ell t(B)\le p(\ell B)$, and

3) $t(B\sigma)=t(B)t(\sigma)$, provided that σ does not change the "distinguished" atom p_0. (The use of p_0 will become clear later.)

As an example, the first translations between $\{\neg,\vee\}$ and $\{\neg,\supset\}$ in paragraph 5.1.1.1. (not the ones that were *onto*) are examples of direct translations.

Property 3 places several restrictions on a direct translation t. The first of these is that for any atom p, $t(p)=p$. This is true because $p=p\frac{p}{p}$, so that by property 3, $t(p)=t(p\frac{p}{p})=t(p)\frac{t(p)}{p}$, which can only hold if either $t(p)=p$ or p does not occur in $t(p)$. Property 1 insures that this second alternative cannot occur. The second consequence of property 3 is that t is completely determined by $\{t(A^j_1)\mid 1\le j\le k_1\}$. That is, if $t(A^j_1)=t'(A^j_1)$ for $1\le j\le k_1$, then for every $B\in K_1$, $t(B)=t'(B)$. This fact is easily proved from property 3 by induction on the number of occurrences of connectives in B. Properties 2 and 3 also imply that for $1\le j\le k_1$ and for $1\le i\le n^{*^j_1}$, p_i occurs at most once in $t(A^j_1)$. To see that this is so, let $\sigma = \frac{A^j_1}{p_i}$, and let $B = (\dots(A^j_1\overbrace{\sigma)\dots)\sigma}^{n \text{ times}}$. Then $\ell B = (n+1)\ell A^j_1 - n\ell p_i$, since A^j_1 contains one occurrence of p_i. By property 3, $t(B)=(\dots(t(A^j_1)\overbrace{\sigma')\dots)\sigma'}^{n \text{ times}}$, where $\sigma' = \frac{t(A^j_1)}{p_i}$. If p_i occurs r times in $t(A^j_1)$, then p_i

occurs r^{n+1} times in $t(B)$, so that $\ell t(B) \geq r^{n+1}$. But by property 2, $\ell t(B) \leq p(\ell B) \leq p((n+1)\ell A_1^j - n\ell p_i) \leq p((n+1)\cdot c)$, where $c=\ell A_1^j$. This gives $r^{n+1} \leq p((n+1)\cdot c)$, which must be true for fixed p, r, and c, and for arbitrarily large n. This can only be true if $r \leq 1$.

This last consequence of property 3 has two further consequences. The first is that if p is any atom in B, then the number of occurrences of p in $t(B)$ is no greater than the number of occurrences of p in B. This is proven by induction on the number of occurrences of connectives in B. The second is that if $c = \max_{1 \leq j \leq k_1} \ell t(A_1^j)$, then for any formula $B \in K_1$, $\ell t(B) \leq c \cdot \ell B$. This is also proven by induction on the substructure of B. Therefore, property 2 in the definition of direct translation could be strengthened without any loss of generality to: 2') there is a constant c such that $\forall B \in K_1$, $\ell t(B) \leq c \cdot \ell B$.

The composition of two direct translations is a direct translation. That is, if t_1 is a direct translation from κ_1 to κ_2, and t_2 is a direct tranlsation from κ_2 to κ_3, then t_3 defined by $t_3(B) = t_2(t_1(B))$ is a direct translation from κ_1 to κ_3. This is true because $t_3(B)=t_2(t_1(B)) \sim t_1(B) \sim B$, $\ell t_3(B) = \ell t_2(t_1(B)) \leq c_2 \cdot \ell t_1(B) \leq c_2 \cdot c_1 \cdot \ell B$, and $t_3(B\sigma)=t_2(t_1(B\sigma))=t_2(t_1(B)t_1(\sigma))=t_2(t_1(B))t_2(t_1(\sigma))=t_3(B)t_3(\sigma)$.

There are several other properties of direct translations that will be used later. First is the obvious fact that if t is a direct translation from κ_1 to κ_2, and if $\kappa_1' \subseteq \kappa_1$, then the restriction of t to formulas in κ_1' is a direct translation from κ_1' to κ_2. Also, if t_1 is a direct translation from κ_1 to κ_3 and t_2 is a direct translation from κ_2 to κ_3, then t_1 and t_2 can be combined to give a direct translation from $\kappa_1 \cup \kappa_2$ to κ_3. Consequently, if there is a direct translation from κ_1 to κ_2, then there are direct translations both ways between $\kappa_1 \cup \kappa_2$ and κ_2.

Direct translations are very useful when they exist, but there is not always a direct translation from any one given set of connectives to any other. For example, there is no direct translation from $\{\neg, \vee, \equiv\}$ to $\{\neg, \vee\}$. The following development establishes one set of circumstances that guarantee the existence of a direct translation.

If κ is any adequate set of connectives (with no restriction on the arities of the connectives), then there exists a direct translation from $\kappa_0 = \{\mathsf{T}, \mathsf{F}, \neg, \vee, \subset, \supset, \&, |, \not\supset, \not\subset, \downarrow\}$ to κ. A careful and complete proof of this fact is rather tedious, so only a sketch will be given here. Since κ is adequate, there are a tautology T and an unsatisfiable formula F that can be expressed in terms of the connectives κ. Furthermore, T and F can be chosen so that the only atom in them is the "distinguished" atom p_0. These will serve as the direct translations of T and F respectively, and will also be used when needed to give constant truth values.

A truth function (or a connective) f is called *monotone* if $\tau_1 \leq \tau_2$ implies $f(\tau_1) \leq f(\tau_2)$, where $\mathsf{T} \leq \mathsf{T}$, $\mathsf{F} \leq \mathsf{F}$, $\mathsf{F} \leq \mathsf{T}$, and $\tau_1 \leq \tau_2$ if and only if $\forall j\ \tau_1(j) \leq \tau_2(j)$ ($\tau_1(j)$ is the j^{th} component of the n-tuple of truth values τ_1). It is easy to show that the composition of monotone functions is monotone, and that there exist truth functions that are not monotone. Then, since κ is adequate, κ must contain a non-monotone connective. From this connective and the formulas T and F, a direct translation for $\neg p$ can be constructed.

A truth function (or a connective) f is called *even* if f can be represented by a formula in the connectives $\{\mathsf{T}, \mathsf{F}, \neg, \equiv, \not\equiv\}$, and it is *odd* if it is not even. It is easy to show by induction on the representing formula that the number of T entries in the truth table for an even function is even. Note that the eight odd binary connectives are all in κ_0. Again, it can be shown that the composition of even functions is even, and that there are truth functions that are not even, so that κ must contain an odd connective $*$. It can then be shown that $*$ along with T and F can be used to give a direct translation of one of the eight odd binary connectives. Since each of the eight odd binary connectives can be represented in terms of each of the others plus $\neg$, direct translations for the other seven odd binary connectives can also be obtained.

Although the existence of direct translations from κ_0 to any adequate set of connectives κ is interesting for its own sake, there are several important consequences of this fact as well. The first of these is that if t is a direct translation from κ_1 to κ_2 and if κ_2 is adequate, then there is a direct translation t' from κ_1 to κ_2 such that $\forall B \in K_1$, $\forall p_i$ occurring in

B (except p_0), the number of occurrences of p_i in $t'(B)$ equals the number of occurrences of p_i in B, and $\ell t'(B) \geq \ell B$. If κ_1 contains some connective $*$ that does not depend on all of its arguments, then $t(*(p_1,\ldots,p_{n^*}))$ may not contain all of $\{p_1,\ldots,p_{n^*}\}$. The translation t' puts back those dropped atoms without changing the truth function represented. This is done by using translations of formulas in κ_0. For example, if $t(*(p_1,\ldots,p_{n^*}))$ contains all of the atoms of $\{p_1,\ldots,p_{n^*}\}$ except p_i, then $t'(*(p_1,\ldots,p_{n^*}))$ could be the direct translation of $(t(*(p_1,\ldots,p_{n^*}))\&(p_i \vee \top))$. In this way it can be insured that no occurrences of atoms are lost and that lengths of formulas are never decreased by direct translations.

The final property of direct translations is that if κ_2 is adequate, and t is a direct translation from κ_1 to κ_2, then there is a direct translation t' from κ_1 to κ_2 that is one-to-one. The trick here is to use translations of formulas in κ_0 to attach a unique "tag" to the translation of each primitive formula of κ_1, so that the translation may be uniquely reversed. Suppose $T_1,\ldots,T_{k_1}$ are distinct tautologies in the connectives κ_2 built up using the distinguished atom p_0. Then for each $*_1^i \in \kappa_1$, let $t'(*_1^i(\vec{p}))$ be the direct translation (from $\kappa_0 \cup \kappa_2$ to κ_2) of $(t(*_1^i(\vec{p}))\&T_i)$. Since these "tags" are distinct, it can now be proven by induction on the substructure of B_1 and B_2, that if $t'(B_1)=t'(B_2)$ then $B_1=B_2$. Note that this construction does not conflict with the previous one, so that if κ_2 is adequate and t is a direct translation from κ_1 to κ_2, it may be assumed without loss of generality that there is a constant c such that all of the following hold:

1) $t(B)\sim B$
2) $\ell B\leq\ell t(B)\leq c\cdot\ell B$
3) $t(B\sigma)=t(B)t(\sigma)$, provided σ does not substitute for p_0, and
4) $B'\neq B \Rightarrow t(B')\neq t(B)$.

5.3.1.2. Frege Systems and Direct Translations

In order for one Frege system to simulate another, a way must be found to extend the ideas of translation of formulas from the previous paragraph to the translation of inferences. The example in paragraph 5.1.1.1. showed how this can be done in one particular example, and this paragraph shows how it is done in general.

The method used here is a bit different from the method that was used to show simulations between Mendelson's and Shoenfield's systems. This method applies to any pair of Frege systems $F_1=<\kappa_1,\mathcal{R}_1>$ and $F_2=<\kappa_2,\mathcal{R}_2>$ for which there are direct translations t_1 from κ_1 to κ_2 and t_2 from κ_2 to κ_1. To show that F_2 simulates F_1, tautologies in κ_2 must be translated into κ_1 (*via* t_2), and derivations in system F_1 must be translated into derivations in system F_2 (*via* some function h) in such a way that for any tautology A in the connectives κ_2, and for any derivation D of $t_2(A)$ in system F_1, $h(D,A)$ is a derivation of A in system F_2. The derivation $h(D,A)$ is constructed in two parts. The first is a translation of derivation D that gives a derivation of $t_1(t_2(A))$, and the second is a derivation of A from $t_1(t_2(A))$. The construction of the first part is described in lemma 5.3.1.2.a., and the second part is in lemmas 5.3.1.2.b.-d. These lemmas are tied together in theorem 5.3.1.2.e., the main result of this paragraph.

LEMMA 5.3.1.2.a.

If $I_1=\langle\kappa_1,\mathcal{R}_1\rangle$ is an inference system, $F_2=\langle\kappa_2,\mathcal{R}_2\rangle$ is a Frege system, and t is a direct translation from κ_1 to κ_2, then there are constants a_1 and a_2 such that whenever $\Gamma\vdash_{I_1}A$ *via* D, there is a derivation D' such that:

1) $t(\Gamma)\vdash_{F_2} t(A)$ *via* D',

2) $\ell^s D' \le a_1\cdot\ell^s D$, and

3) $\ell D' \le a_2\cdot(\ell D+\ell\Gamma)\cdot d(D)$.

Proof

Let $\mathcal{R}_1 = \{R_1=\Delta_1\to B_1,\ldots,R_k=\Delta_k\to B_k\}$. Since the rules of $\mathcal{R}_1$ are sound, $\Delta_i\models B_i$, and since $t(B)\sim B$, $t(\Delta_i)\models t(B_i)$, for $1\le i\le k$. Then, since F_2 is implicationally complete, there are derivations D^i such that $t(\Delta_i)\vdash_{F_2}t(B_i)$ *via* D^i, for $1\le i\le k$.

Let $a_1 = \max_{1\le i\le k}\ell^s D^i$, $a_3 = \max_{1\le i\le k}\ell D^i$, and $a_4 = \max_{1\le i\le k}\ell^a D^i$.

Also, let a_5 be a constant such that $\ell t(B)\le a_5\cdot\ell B$. The required derivation D' is constructed from D by replacing each formula C in D by a derivation D_C, where $t(\Delta^C)\vdash_{F_2}t(C)$ *via* D_C, and Δ^C

is the set of formulas from which C is inferred in D. In particular, suppose that C is inferred from Δ^C by substitution σ^C in rule R_{i_C}. Then, $\Delta^C=\Delta_{i_C}\sigma^C$ and $C=B_{i_C}\sigma^C$, and $D_C=D^{i_C}t(\sigma^C)$ is a derivation of $t(B_{i_C})t(\sigma^C)=t(B_{i_C}\sigma^C)=t(C)$ from $t(\Delta_{i_C})t(\sigma^C)=t(\Delta_{i_C}\sigma^C)=t(\Delta^C)$. If D' is constructed in this way, then $t(\Gamma)\vdash_{F_2}t(A)$ *via* D'. Also, $\ell^s D'=\sum_{C\in D}\ell^s D_C$, and $\ell D'=\sum_{C\in D}\ell D_C$. But $\ell^s D_C=\ell^s D^{i_C}\leq a_1$, so that $\ell^s D'\leq\sum_{C\in D}a_1=a_1\cdot\ell^s D$. Since σ^C need not specify a substitution for any atom not in $\Delta_{i_C}\cup\{B_{i_C}\}$, $\ell\sigma^C\leq\ell\Delta^C+\ell C$. Then, $\ell D_C=\ell D^{i_C}t(\sigma^C)\leq\ell D^{i_C}+\ell^a D^{i_C}\cdot\ell t(\sigma^C)\leq a_3+a_4\cdot a_5\cdot(\ell\Delta^C+\ell C)\leq\frac{a_2}{2}\cdot(\ell\Delta^C+\ell C)$, where $\frac{a_2}{2}=a_3+a_4\cdot a_5$. This gives $\ell D'=\sum_{C\in D}\ell D_C\leq\sum_{C\in D}\frac{a_2}{2}\cdot(\ell\Delta^C+\ell C)=\frac{a_2}{2}\cdot\sum_{C\in D\cup\Gamma}k^C\ell C$, where k^C is one greater than the number of formulas in D of which C is an immediate ancestor. Then, since $k^C\leq d(D)+1$,

$$\ell D'\leq\frac{a_2}{2}\cdot\sum_{C\in D\cup\Gamma}(d(D)+1)\cdot\ell C=\frac{a_2}{2}\cdot(d(D)+1)\cdot\sum_{C\in D\cup\Gamma}\ell C=$$

$$\frac{a_2}{2}\cdot(d(D)+1)\cdot(\ell D+\ell\Gamma)\leq a_2\cdot d(D)\cdot(\ell D+\ell\Gamma).$$

⊠5.3.1.2.a.

As was pointed out in the example of paragraph 5.1.1.1., a result like lemma 5.3.1.2.a. is not enough to insure that system F_2 can simulate system I_1, because t need not be onto.

In that example, it was possible to make t onto, but in general this may not be possible. The following three lemmas give an alternative way of solving this problem. The method used is to "undo" the translation t by means of another translation and further inferences in system F_2. These further inferences are described in lemmas 5.3.1.2.b. and 5.3.1.2.c., and their use in conjunction with a translation from κ_2 to κ_1 is described in lemma 5.3.1.2.d.

LEMMA 5.3.1.2.b.

If κ is adequate and t' is a direct translation from κ to κ, then there are an inference system $I\langle\kappa,\mathcal{R}\rangle$ and constants b_1 and b_2 such that for every formula A in the connectives κ there are derivations D_1 and D_2 such that:

1) $A \vdash_I t'(A)$ *via* D_1,

2) $t'(A) \vdash_I A$ *via* D_2, and for $i=1,2$,

3) $\ell^s D_i \leq b_1 \cdot \ell^c A$,

4) $\ell D_i \leq b_2 \cdot \ell^c A \cdot \ell A$, and

5) $d(D_i)=1$.

Proof

Since κ is adequate, there is a formula $\hat{E}(p,q)$ in the connectives κ such that $\hat{E}(p,q) \sim (p \equiv q)$. Let $b_3 = \ell\hat{E}(p,q)$ $b_4 = \ell^a \hat{E}(p,q)$, and let b_5 be the constant such that $\ell t'(A) \leq b_5 \cdot \ell A$. For each connective $\star \in \kappa$, let $A^{\star} = \star(p_1,\ldots,p_{n^{\star}})$ (*e.g.* $A^{\vee} = (p_1 \vee p_2)$, $A^{\equiv} = (p_1 \equiv p_2)$, $A^{\neg} = \neg p_1$, *etc.*), and let $B^{\star} = t'(A^{\star})$. $\mathcal{R}$ will contain the rules

1) $\to\hat{E}(p,p)$,

2) $\{\hat{E}(p,q),p\}\to q$,

3) $\{\hat{E}(p,q),q\}\to p$, and

4) for each connective $*$:
$$\{\hat{E}(p_1,q_1),\ldots,\hat{E}(p_{n^*},q_{n^*})\}\to\hat{E}(A^*,B^*\tfrac{q_1\ldots q_{n^*}}{p_1\ldots p_{n^*}}).$$

Since $\hat{E}$ represents equivalence and $t'(A)\sim A$, these rules are clearly sound, so that $I=<\kappa,\mathcal{R}>$ is an inference system. For any formula A in the connectives κ, let D^A be a derivation of $\hat{E}(A,t'(A))$ in the system I, defined inductively as follows: 1) if A is an atom p, then D^A is $\hat{E}(p,p)$, by rule 1, and 2) if A is $*(B_1,\ldots,B_{n^*})$, then D^A is $D^{B_1}\ldots D^{B_{n^*}}\hat{E}(A,t'(A))$, the last formula of which follows according to rule 4^* under the substitution $\sigma = \dfrac{B_1\ldots B_{n^*}t'(B_1)\ldots t'(B_{n^*})}{p_1\ldots p_{n^*}\quad q_1\ldots q_{n^*}}$. Note that $\ell^s D^A=\ell^a A+\ell^c A$, $d(D^A)=1$, and for each formula $B=\hat{E}(C,t'(C))\in D^A$, $\ell B\le\ell\hat{E}(p,q)+\ell^a\hat{E}(p,q)\cdot(\ell C+\ell t'(C))\le b_3+b_4(\ell A+b_5\ell A)\le b_6\ell A$, where $b_6=b_3+b_4(1+b_5)$. Let k be the maximum arity of any connective in κ, so that $\ell^a A\le k\ell^c A$. This implies that $\ell^s D^A\le(k+1)\ell^c A$. Finally, let D_1 be $D^A t'(A)$ (which follows by rule 2) and let D_2 be $D^A A$ (which follows by rule 3). Then, $A\vdash_I t'(A)$ *via* D_1, $t'(A)\vdash_I A$ *via* D_2, and for $i=1,2$, $\ell^s D_i\le 1+\ell^s D^A\le 1+(k+1)\cdot\ell^c A\le b_1\cdot\ell^c A$, where $b_1=k+2$,

$\ell D_i \le \ell^s D_i \cdot$(length of longest formula in D_i) $\le b_1 \cdot \ell^c A \cdot b_6 \cdot \ell A$

$= b_2 \cdot \ell^c A \cdot \ell A$, where $b_2 = b_1 \cdot b_6$, and $d(D_i)=1$. ⊠5.3.1.2.b.

LEMMA 5.3.1.2.c.

If $F=\langle\kappa,\mathcal{R}\rangle$ is a Frege system, and t' is a direct translation from κ to κ, then there are constants c_1 and c_2 such that for every formula A in the connectives κ there are derivations D_1' and D_2' such that:

1) $A \vdash_F t'(A)$ *via* D_1'

2) $t'(A) \vdash_F A$ *via* D_2', and for $i=1,2$

3) $\ell^s D_i' \le c_1 \cdot \ell^c A$, and

4) $\ell D_i' \le c_2 \cdot \ell^c A \cdot \ell A$.

Proof

Since κ is adequate, lemma 5.3.1.2.b. applies, so let I, b_1, b_2, A, D_1, and D_2 be as stated in that lemma. By lemma 5.3.1.2.a., with $I_1=I$, $F_2=F$, and t the identity function, there are derivations D_1' and D_2' such that:

1) $A \vdash_F t'(A)$ *via* D_1',

2) $t'(A) \vdash_F A$ *via* D_2', and for $i=1,2$,

3) $\ell^s D_i' \le a_1 \cdot \ell^s D_i \le a_1 \cdot b_1 \cdot \ell^c A \le c_1 \cdot \ell^c A$, where $c_1 = a_1 \cdot b_1$, and

4) $$\ell D_i' \le a_2 \cdot \left(\ell D_i + \begin{Bmatrix} \ell A \text{ if } i=1 \\ \ell t'(A) \text{ if } i=2 \end{Bmatrix}\right) \cdot d(D_i)$$
$$\le a_2 \cdot 2 \cdot \ell D_i \cdot 1$$
$$\le 2 \cdot a_2 \cdot b_2 \cdot \ell^c A \cdot \ell A$$
$$\le c_2 \cdot \ell^c A \cdot \ell A, \text{ where } c_2 = 2 \cdot a_2 \cdot b_2.$$ ⊠5.3.1.2.c.

LEMMA 5.3.1.2.d.

If $I=\langle\kappa_1,\mathcal{R}_1\rangle$ is an inference system, $F=\langle\kappa_2,\mathcal{R}_2\rangle$ is a Frege system, t_1 is a direct translation from κ_1 to κ_2, and t_2 is a direct translation from κ_2 to κ_1, then there are constants e_1 and e_2 such that whenever $t_2(\Gamma)\vdash_I t_2(A_0)$ *via* D there is a derivation D'' such that:

1) $\Gamma\vdash_F A_0$ *via* D''

2) $\ell^s D''\leq e_1\cdot(\ell^s D+\ell^c\Gamma+\ell^c A_0)$, and

3) $\ell D''\leq e_2\cdot[(\ell D+\ell\Gamma)\cdot d(D)+\ell^c\Gamma\cdot\ell\Gamma+\ell^c A_0\cdot\ell A_0]$.

Proof

Let e_3 be a constant such that $\ell t_2(A)\leq e_3\cdot\ell A$. Then, by lemma 5.3.1.2.a., there is a derivation D', where

1) $t_1(t_2(\Gamma))\vdash_F t_1(t_2(A_0))$ *via* D',

2) $\ell^s D'\leq a_1\cdot\ell^s D$, and

3) $\ell D'\leq a_2\cdot(\ell D+\ell t_2(\Gamma))\cdot d(D)\leq a_2\cdot e_3\cdot(\ell D+\ell\Gamma)\cdot d(D)$.

Let $\Gamma=\{A_1,\ldots,A_k\}$. Then, since $t_1\circ t_2$ is a direct translation from κ_2 to κ_2, by lemma 5.3.1.2.c. there are derivations $D_0,D_1,\ldots,D_k$ such that

1) $t_1(t_2(A_0))\vdash_F A_0$ *via* D_0,

2) $A_i\vdash_F t_1(t_2(A_i))$ *via* D_i $(1\leq i\leq k)$,

3) $\ell^s D_i\leq c_1\cdot\ell^c A_i$ $(0\leq i\leq k)$, *and*

4) $\ell D_i\leq c_2\cdot\ell^c A_i\cdot\ell A_i$.

Then, if $D''=D_1\ldots D_k D' D_0$, $\Gamma\vdash_F A$ *via* D''. Also,

$\ell^s D''\leq c_1\cdot\ell^c A_1+\ldots+c_1\cdot\ell^c A_k+a_1\cdot\ell^s D+c_1\cdot\ell^c A_0\leq e_1\cdot(\ell^c\Gamma+\ell^s D+\ell^c A_0)$, where $e_1=c_1+a_1$, and

$$\ell D'' \leq c_2\cdot\ell^c A_1\cdot\ell A_1+\ldots+c_2\cdot\ell^c A_k\cdot\ell A_k+a_2\cdot e_3\cdot(\ell D+\ell\Gamma)\cdot d(D)+c_2\cdot\ell^c A_0\cdot\ell A_0$$

$$\leq e_2\cdot[(\ell D+\ell\Gamma)\cdot d(D)+\ell^c\Gamma\cdot\ell\Gamma+\ell^c A_0\cdot\ell A_0],$$ where $e_2=c_2+a_2\cdot e_3$.

⊠5.3.1.2.d.

The groundwork has now been laid so that the main result of this section can be proved.

THEOREM 5.3.1.2.e.

If $F_1=\langle\kappa_1,\mathcal{R}_1\rangle$ and $F_2=\langle\kappa_2,\mathcal{R}_2\rangle$ are Frege systems, t_1 is a direct translation from κ_1 to κ_2, and t_2 is a direct translation from κ_2 to κ_1, then F_2 p-simulates F_1. Furthermore, if F_1 is polynomial-bounded by a polynomial of degree r, then F_2 is polynomial-bounded by a polynomial of degree no more than $2r$.

Proof

Let $g=t_2$, and let $h(D,A)=D''$ if $\vdash_{F_1} t_2(A)$ *via* D, (where D'' is the derivation described by lemma 5.3.1.2.d.), and if it is not true that $\vdash_{F_1} t_2(A)$ *via* D, then let $h(D,A)=0$. By lemma 5.3.1.2.d. (with Γ empty), $\vdash_{F_2} A$ *via* $h(D,A)$, and $\ell h(D,A) \leq e_2\cdot(\ell D+\ell A)^2$. Also, $F_2(h(D,A))=A$ whenever $F_1(D)=t_2(A)$. Thus, system F_2 simulates F_1. Also, note that $g\in\mathcal{PT}$, and a close look at the proof of lemmas 5.3.1.2.a-d. shows that $h\in\mathcal{PT}$ also. Therefore F_2 p-simulates F_1. ⊠5.3.1.2.e.

Theorem 5.3.1.2.e. leads immediately to the following corollary.

COROLLARY 5.3.1.2.f.

Let C be any class of adequate sets of connectives such that there exist direct translations between any two sets in C. Then, any two Frege systems with connective sets from C can p-simulate each other.

Examples of such classes C are:

1) all adequate subsets of $\kappa_0=\{T,F,\neg,\vee,\subset,\supset,\&,|,\not\supset,\not\subset,\downarrow\}$,
2) all adequate subsets of $\kappa_0\cup\{\equiv,\not\equiv\}$ that contain either $\equiv$ or $\not\equiv$, and
3) all adequate subsets of $\kappa_0\cup\kappa$ that include κ as a subset (where κ is any set of connectives).

5.3.1.3. Indirect Translation

Direct translations between certain pairs of adequate sets of connectives do not exist. For example, there is no direct translation from $\{\neg,\vee,\equiv\}$ to $\{\neg,\vee\}$. In particular, there is no formula in the connectives $\{\neg,\vee\}$ that both is equivalent to $(p\equiv q)$ and contains only one occurrence of each of p and q. Therefore, the requirements for direct translations are too strict, and one of them must be dropped. The first two requirements are essential, and dropping the third requires giving up a great deal of convenience in working with these translations.

Let κ_1 and κ_2 be sets of connectives, and let K_1 and K_2 be the corresponding sets of formulas. A function $t:K_1\rightarrow K_2$ is called an *indirect translation* from κ_1 to κ_2 if there is a polynomial $p(n)$ such that for all formulas $B\in K_1$,

1) $t(B) \sim B$, and

2) $\ell t(B) \leq p(\ell B)$.

Note: For the indirect translations considered in this thesis, the condition $t \in \mathcal{PF}$ is also satisfied.

All direct translations are also indirect translations, and it was Spira who first showed the existence of an indirect translation between sets of connectives where no direct translation is possible [Spira 1971]. Spira's method may be extended to show the existence of indirect translations from any set of connectives to any adequate set of connectives. But since direct translations exist from κ_0 to any adequate set of connectives, the indirect translations of interest are those translations from other sets of connectives to κ_0.

Let κ be an arbitrary set of connectives, let K be the set of all formulas in the connectives κ, and let k be the maximum arity of connectives in κ. Thus, K is a set of trees whose maximum branching degree is k. A particular indirect translation from κ to $\kappa_1 = \{\top, \mathrm{F}, \neg, \vee, \&\}$ will be described here and used throughout this and the following paragraph.

Let A be any formula in K. If no atoms occur in A or if A contains one atom occurrence, then let $t(A)$ be either T, F, p, or $\neg p$, whichever is equivalent to A. If A contains $n>1$ occurrences of atoms, then let C be the subformula of A that contains nearest to $\frac{1}{2}n$ occurrences of atoms. (Ties are resolved according to some arbitrary set of rules such as: if A has a subformula of size $\frac{1}{2}n+x$ and another of size $\frac{1}{2}n-x$, choose the one of size $\frac{1}{2}n+x$; and if A has several subformulas of size s, choose the leftmost.) The number of occurrences of atoms in C must be between $\frac{n}{k+1}$ and $\frac{k\cdot n}{k+1}$. This is true because if D is a subtree of A with more than $\frac{k\cdot n}{k+1}$ occurrences of atoms, then since the degree of the root of D is at most k, one of the subtrees of D must contain more than $\frac{n}{k+1}$ occurrences of atoms.

Let B be the formula with one occurrence of the new atom p such that $A=B\frac{C}{p}$. Then, not counting p, the number of occurrences of atoms in B is also between $\frac{n}{k+1}$ and $\frac{k\cdot n}{k+1}$. Note that $A\sim((B\frac{\mathrm{I}}{p}\&C)\vee(B\frac{\mathrm{E}}{p}\&\neg C))$, and let $t(A)=((t(B\frac{\mathrm{I}}{p})\&t(C))\vee(t(B\frac{\mathrm{E}}{p})\&\neg t(C))$.

It is clear from this construction that $t(A)\sim A$. To show that there is a polynomial p such that $\ell t(A)\leq p(\ell A)$, let $f(n)=\max\{\ell^a t(B)\mid \ell^a B\leq n\}$. Clearly, $f(1)=1$, and f is nondecreasing. For $n>1$, it is certainly true that $f(n)\leq 4f(\frac{k\cdot n}{k+1})$, which leads to the solution $f(n)\leq n^{\frac{2}{\log_2\frac{k+1}{k}}}\leq n^{2k}$. This last inequality holds because of the following lemma.

LEMMA 5.3.1.3.a.

For integers $k\geq 2$, $(k+1)^k\geq 2k^k$.

Proof

By the binomial theorem,

$$
\begin{aligned}
(k+1)^k &= \sum_{i=0}^{k} \binom{k}{i} k^i \\
&= \binom{k}{k} k^k + \binom{k}{k-1} k^{k-1} + \sum_{i=0}^{k-2} \binom{k}{i} k^i \\
&= 1 \cdot k^k + k \cdot k^{k-1} + \sum_{i=0}^{k-2} \binom{k}{i} k^i \\
&= 2k^k + \sum_{i=0}^{k-2} \binom{k}{i} k^i \\
&\geq 2k^k
\end{aligned}
$$

∎5.3.1.3.a.

From this it can be concluded that $\frac{k+1}{k} \geq 2^{\frac{1}{k}}$, so that $log_2 \frac{k+1}{k} \geq \frac{1}{k}$, which implies that $\frac{2}{log_2 \frac{k+1}{k}} \leq 2k$. For $k=2$, this gives an upper bound on $f(n)$ of n^4. Pratt [Pratt 1974] has shown by a more careful analysis that $f(n)$ is in fact $O(n^{log_3 10})$, or about $O(n^{2.095})$, which nearly equals Khrapchenko's lower bound of n^2 [Khrapchenko 1971]. Pratt's analysis is specific to the case $k=2$, but a similar analysis for $k>2$ would probably yield upper bounds nearer to n^k. Finally, since $\ell t(B)$ is bounded by some constant times $\ell^a t(B) \cdot \ell B$, the bound (admittedly very loose) $\ell t(B) \leq c \cdot (\ell B)^{2k+1}$ is obtained.

5.3.1.4. Frege Systems and Indirect Translations

Let $\kappa_0=\{T,F,\neg,\vee,\subset,\supset,\&,|,\not\supset,\not\subset,\downarrow\}$, $\kappa_1=\{T,F,\neg,\vee,\&\}$, let κ be an arbitrary adequate set of connectives, and let $\hat{\kappa}=\kappa\cup\kappa_1$. Let k be the maximum arity of connectives in $\hat{\kappa}$. By corollary 5.3.1.2.f. all Frege systems in the connectives $\hat{\kappa}$ and κ can p-simulate each other. Thus, in order to show that any two Frege systems can p-simulate each other, it is sufficient to show a Frege system with the connectives κ_1 and another system with the connectives $\hat{\kappa}$ that p-simulate each other.

Let $F=\langle\kappa,\mathcal{R}\rangle$ be a Frege system, and let $\hat{F}=\langle\hat{\kappa},\hat{\mathcal{R}}\rangle$ be the Frege system obtained from F by the addition of sufficient new rules to make $\hat{F}$ implicationally complete. See, for example, the proof of lemma 5.3.1.2.b. Let t be the indirect translation from $\hat{\kappa}$ to κ_1 as described in paragraph 5.3.1.3. A Frege system $F_1=\langle\kappa_1,\mathcal{R}_1\rangle$ can be obtained from Shoenfield's system for $\{\neg,\vee\}$ with the addition of rules for $\{T,F,\&\}$ as in the proof of lemma 5.3.1.2.b. Also, let $F_0=\langle\kappa_0,\mathcal{R}_0\rangle$ be an arbitrary Frege system in connectives κ_0. Finally, let $\hat{E}(p,q)$ and $\hat{I}(r,s)$ be formulas in the connectives κ_1 such that $\hat{E}(p,q)\sim(p\equiv q)$ and $\hat{I}(r,s)\sim(r\supset s)$. For example, $\hat{E}(p,q)$ could be $((p\&q)\vee(\neg p\&\neg q))$, and $\hat{I}(r,s)$ could be $(\neg r\vee s)$. The notation defined here will be used throughout paragraph 5.3.1.4.

Lemmas 5.3.1.4.a-d. will show how $\hat{F}$ p-simulates F_1.

LEMMA 5.3.1.4.a.

There are an inference system $I=\langle\hat{\kappa},\tilde{\mathcal{R}}\rangle$ and constants a_1 and a_2 such that for every formula A in the connectives $\hat{\kappa}$, there are derivations D_1 and D_2 such that:

1) $A \vdash_I t(A)$ *via* D_1,

2) $t(A) \vdash_I A$ *via* D_2, and for i=1,2,

3) $\ell^s D_i \le a_1 \cdot (\ell A)^{3k}$,

4) $\ell D_i \le a_2 \cdot (\ell A)^{5k+1}$,

5) $d(D_i) = 1$.

Proof

Let $\tilde{\mathcal{R}}$ contain the following rules:

1) $\to \hat{E}(p,p)$,

2) $\hat{E}(p,q), \hat{E}(q,r) \to \hat{E}(p,r)$,

3) $\hat{E}(p,q) \to \hat{E}(\neg p, \neg q)$,

4) $\hat{E}(p,q), p \to q$,

5) $\hat{E}(p,q), q \to p$,

6) $\hat{E}(p,q), \hat{I}(p,r) \to \hat{I}(q,r)$,

7) $\to \hat{I}(p, \hat{E}(q,q))$,

8) $\to \hat{I}(p, \hat{E}(\mathsf{T},p))$,

9) $\to \hat{I}(\neg p, \hat{E}(\mathsf{F},p))$,

10) $\hat{I}(p,\hat{E}(q,r)), \hat{E}(q,s) \to \hat{I}(p,\hat{E}(s,r))$,

11) $\hat{I}(p,\hat{E}(q,r)), \hat{I}(\neg p,\hat{E}(s,r)) \to \hat{E}(r,((q\&p)\vee(s\&\neg p)))$,

and for each connective $*\in\hat{R}$, $\tilde{\mathcal{R}}$ contains the rules:

12) for each $1\le i\le n^*$, and for each $\vec{u}\in\{\mathsf{T},\mathsf{F}\}^{i-1}$ and $\vec{v}\in\{\mathsf{T},\mathsf{F}\}^{n-i}$,

$\to \hat{E}(*(\vec{u},p_i,\vec{v}), t(*(\vec{u},p_i,\vec{v})))$, and

13) $\hat{I}(p,\hat{E}(q_1,r_1)),\dots,\hat{I}(p,\hat{E}(q_{n^*},r_{n^*})) \to \hat{I}(p,\hat{E}(*(\vec{q}),*(\vec{r})))$.

All of these rules are sound, so that I is in fact an inference system.

Derivations D_1 and D_2 both are built from a derivation D, where $\vdash_I \hat{E}(A,t(A))$ *via* D. In fact, each is only one step longer than D, D_1 using rule 4, and D_2 using rule 5. Derivation D is constructed recursively on the number of occurrences of atoms in A.

If A contains no atoms or one occurrence of an atom, then rules 1, 2, 3, and 12 can be used to derive $\hat{E}(A,t(A))$ in a number of steps bounded by twice the number of occurrences of connectives in A plus one.

If A contains more than one occurrence of an atom and $t(A)$ is $((t(B\frac{T}{p})\&t(C))\vee(t(B\frac{F}{p})\&\neg t(C))$, assume inductively that D^0, D^+, and D^- are derivations of $\hat{E}(C,t(C))$, $\hat{E}(B\frac{T}{p},t(B\frac{T}{p}))$, and $\hat{E}(B\frac{F}{p},t(B\frac{F}{p}))$, respectively. If there were derivations D^{++} of $\hat{I}(p,\hat{E}(B\frac{T}{p},B))$ and D^{--} of $\hat{I}(\neg p,\hat{E}(B\frac{F}{p},B))$, then $D^{++}\frac{C}{p}$ would be a derivation of $\hat{I}(C,\hat{E}(B\frac{T}{p},A))$, and $D^{--}\frac{C}{p}$ would be a derivation of $\hat{I}(\neg C,E(B\frac{F}{p},A))$. Applying rules 6 and 3 to each of these formulas plus $\hat{E}(C,t(C))$, gives $\hat{I}(t(C),\hat{E}(B\frac{T}{p},A))$ and $\hat{I}(\neg t(C),\hat{E}(B\frac{F}{p},A))$ in 3 steps. Two applications of rule 10 give $\hat{I}(t(C),\hat{E}(t(B\frac{T}{p}),A))$ and $\hat{I}(\neg t(C),\hat{E}(t(B\frac{F}{p}),A))$, and one application of rule 11 yields $\hat{E}(A,((t(B\frac{T}{p})\&t(C))\vee(t(B\frac{F}{p})\&\neg t(C))))=\hat{E}(A,t(A))$, as desired. The total number of steps in this derivation is six plus the number of steps in $D^0D^0D^+D^-D^{++}\frac{C}{p}D^{--}\frac{C}{p}$. Derivations D^0, D^+, and D^- are derived inductively, and derivations D^{++} and D^{--} are constructed, using rules 7, 8, 9, and 13, by induction on the number of occurrences of connectives in B, the total number of steps being bounded by some constant c times that number of connectives.

Let $f(n)$ be an upper bound on the number of steps in the derivation D over all formulas A of length no greater than n. Then $f(1)=1$, and for $n>1$, $f(n)\leq 6+4\cdot f(\frac{k\cdot n}{k+1})+2\cdot c\cdot n$. Using lemma 5.3.1.3.a., it can be shown that $f(n)\leq 2\cdot c\cdot n^{3k}$. Finally, note that each formula in D has length bounded by some constant d times $\ell t(A)$, so that $\ell^s D\leq 2\cdot c\cdot(\ell A)^{3k}$, and $\ell D\leq 2\cdot c\cdot d\cdot(\ell A)^{5k+1}$. Each formula in the entire derivation is used only once, so $d(D)=1$.

☒5.3.1.4.a.

Lemma 5.3.1.4.a. leads immediately to the following lemma.

LEMMA 5.3.1.4.b.

There is a Frege system $\tilde{F}=<\mathcal{K},\ddot{\mathbb{R}}>$ and there are constants b_1 and b_2 such that whenever $t(\Delta)\vdash_{F_1} t(A)$ *via* D_1 there is a derivation D_2 such that: (Note - Δ is any set of formulas in $\hat{K}$.)

1) $\Delta\vdash_{\tilde{F}} A$ *via* D_2,

2) $\ell^s D_2\leq b_1\cdot(\ell^s D_1+(\ell\Delta)^{3k}+(\ell A)^{3k})$, and

3) $\ell D_2\leq b_2\cdot(\ell D_1+(\ell\Delta)^{5k+1}+(\ell A)^{5k+1})$.

Proof

Let $\ddot{\mathcal{R}}=\mathcal{R}_1\cup\tilde{\mathcal{R}}$, where $\tilde{\mathcal{R}}$ is the set of rules from lemma 5.3.1.4.a. If $\Delta=\{B^1,\ldots,B^m\}$, then by lemma 5.3.1.4.a., there are derivations $D^1,\ldots,D^m$ such that for $1\le i\le m$

1) $B^i \vdash_{\tilde{F}} t(B^i)$ *via* D^i,

2) $\ell^s D^i \le a_1\cdot(\ell B^i)^{3k}$, and

3) $\ell D^i \le a_2\cdot(\ell B^i)^{5k+1}$.

Also, there is a derivation D^0 such that

$t(A) \vdash_{\tilde{F}} A$ *via* D^0, $\ell^s D^0 \le a_1\cdot(\ell A)^{3k}$, and $\ell D^0 \le a_2\cdot(\ell A)^{5k+1}$.

Since D_1 is already a derivation in the system $\tilde{F}$, the desired derivation D_2 is just $D^1\ldots D^m D_1 D^0$, and the lemma follows, with $b_1=a_1$ and $b_2=a_2$. ☒5.3.1.4.b.

LEMMA 5.3.1.4.c.

System $\tilde{F}$ of lemma 5.3.1.4.b. p-simulates system F_1.

Proof

Let $g(A)=t(A)$, and let $h(D_1,A)=D_2$, if $\vdash_{F_1} t(A)$ *via* D_1, where D_2 is the derivation whose existence is guaranteed by lemma 5.3.1.4.b. (where Δ is empty); and if it is not true that $\vdash_{F_1} t(A)$ *via* D_1, then let $h(D_1,A)=0$. By lemma 5.3.1.4.b., $\ell h(D_1,A) \le b_2(\ell D_1+(\ell A)^{5k+1}) = q(\ell D_1,\ell A)$, and $\tilde{F}(h(D_1,A))=A$ whenever $F_1(D_1)=g(A)$. Also, $\ell g(A)\le c\cdot(\ell A)^{2k+1}$, and $g,h\in\mathcal{PF}$. Therefore $\tilde{F}$ p-simulates F_1. ☒5.3.1.4.c.

Since p-simulation is transitive, lemma 5.3.1.4.c. and theorem 5.3.1.2.e. can be combined to give the following.

LEMMA 5.3.1.4.d.

Every Frege system F p-simulates F_1 and F_0.

That is, the adequate sets of connectives of arity no greater than two which do not include $\equiv$ or $\not\equiv$ form a "core", and any Frege system whose connectives are one of these "core" sets can be p-simulated by any other Frege system. What remains to be shown is that these "core" systems can p-simulate the others.

The proof that F_1 p-simulates $\hat{F}$ will be similar to the development in paragraph 5.3.1.2., but since there may be no direct translation from $\mathcal{R}$ to κ_1, some new arguments will be needed. In particular, the analog of lemma 5.3.1.2.a. will have to work when t is an indirect translation, rather than a direct one. The analog for indirect translation of lemma 5.3.1.2.b. has already been established by lemma 5.3.1.4.a. The proof of the analog of lemma 5.3.1.2.a. is rather involved, and will be built up by a series of stages.

LEMMA 5.3.1.4.e.

There is an inference system $I=<\kappa_1,\mathcal{R}'>$ and there are constants e_1 and e_2 such that for any formula A in the connectives $\mathcal{R}$ and for any subformula E of A and formula G (with one occurrence of q) such that $G\frac{E}{q}=A$, there is a derivation D such that

1) $\vdash_I \hat{E}(t(A),((t(G\frac{\mathrm{I}}{q})\&t(E))\vee(t(G\frac{\mathrm{E}}{q})\&\neg t(E))))$ via D,

2) $\ell^{s}D \leq e_1\cdot(\ell A)^{4k}$,

3) $\ell D \leq e_2 \cdot (\ell A)^{6k+1}$, and

4) $d(D)=1$.

Proof

The idea of the proof is to recursively build a derivation D of $\hat{E}(t(A),((t(G\frac{\mathrm{T}}{q})\&t(E))\vee(t(G\frac{\mathrm{F}}{q})\&\neg t(E))))$. Clearly, if A contains no more than a certain small finite number n_0 of occurrences of atoms, then if I contains a rule for each of the finite number of possible cases, the required derivation can consist of a single step.

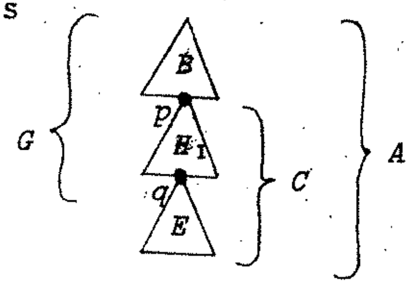
Let the number of occurrences of atoms in A be $n>n_0$, and let C be that subformula of A such that $A=B\frac{C}{p}$ and $t(A)=((t(B\frac{\mathrm{T}}{p})\&t(C))\vee(t(B\frac{\mathrm{F}}{p})\&\neg t(C)))$. If $C=E$ and $G=B\frac{q}{p}$, then the required derivation is the single-step instance of the rule $\hat{E}(p,p)$. Otherwise, there are three possible cases:

1) E is a subtree (subformula) of C, or

2) C is a subtree of E, or

3) C and E are disjoint subtrees of A.

In case 1), C can be written as $H_1\frac{E}{q}$, and G can be written as $B\frac{H_1}{p}$. Pictorially, this is



Let D^1, D^2, and D^3 be the following three derivations (derived recursively):

$\vdash_I \hat{E}(t(C),((t(H_1\frac{I}{q})\&t(E))\vee(t(H_1\frac{E}{q})\&\neg t(E))))$ *via* D^1,

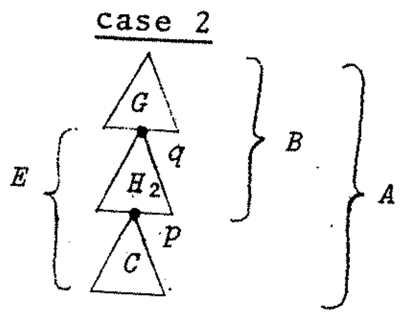
$\vdash_I \hat{E}(t(G\frac{I}{q}),((t(B\frac{I}{p})\&t(H_1\frac{I}{q}))\vee(t(B\frac{E}{p})\&\neg t(H_1\frac{I}{q}))))$ *via* D^2, and

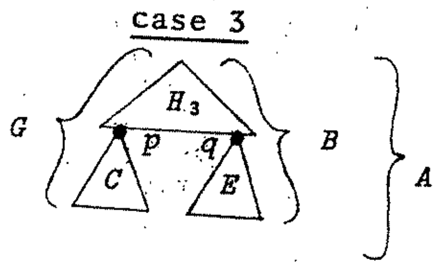
$\vdash_I \hat{E}(t(G\frac{E}{q}),((t(B\frac{I}{p})\&t(H_1\frac{E}{q}))\vee(t(B\frac{E}{p})\&\neg t(H_1\frac{E}{q}))))$ *via* D^3.

The desired conclusion of the derivation D is inferred from these three equivalences by an instance of the sound inference rule R_1:

$$\hat{E}(r,((v\&u)\vee(w\&\neg u))),\hat{E}(s,((p\&v)\vee(q\&\neg v))),\hat{E}(t,((p\&w)\vee(q\&\neg w)))$$
$$\rightarrow \hat{E}(((p\&r)\vee(q\&\neg r)),((s\&u)\vee(t\&\neg u))).$$

Cases 2 and 3 pictorially are:


case 2


case 3

Case 2 is similar to case 1, and gives rise to three recursively derived derivations, from which the conclusion of D can be inferred by an instance of rule R_2:

$$\hat{E}(u,((x\&r)\vee(y\&\neg r))),\hat{E}(p,(s\&x)\vee(t\&\neg x))),\hat{E}(q,((s\&y)\vee(t\&\neg y)))$$
$$\rightarrow \hat{E}(((p\&r)\vee(q\&\neg r)),((s\&u)\vee(t\&\neg u))).$$

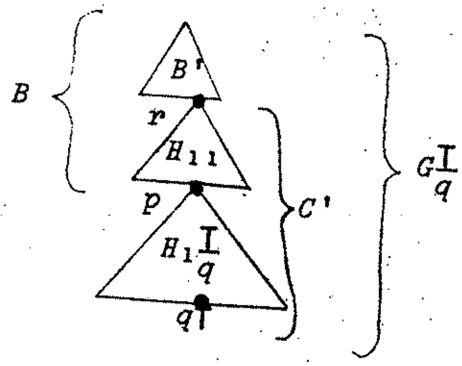
Case 3 gives rise to four recrusively derived derivations, from which the conclusion of D can be derived by an instance of rule R_3:

$$\hat{E}(p,((v\&u)\vee(w\&\neg u))),\hat{E}(q,((x\&u)\vee(y\&\neg u))),\hat{E}(s,((v\&r)\vee(x\&\neg r))),$$
$$\hat{E}(t,((w\&r)\vee(y\&\neg r))) \rightarrow \hat{E}(((p\&r)\vee(q\&\neg r)),((s\&u)\vee(t\&\neg u))).$$

Therefore, the inference system I must contain rules R_1, R_2, and R_3, rules for each of the cases when $n \le n_0$, and the rules $\to\hat{E}(p,p)$. Each formula in D is bounded in length by some constant $c \cdot \ell t(A)$, and $d(D)=1$, by this construction.

To show a polynomial upper bound on the number of steps of D, it is necessary to consider two levels of recursion at once. Let $f(n)=\max\{\ell^s D \mid \ell^a A \le n$, and D is constructed by this method$\}$. Then, f is nondecreasing, and if $n_0=1$, then $f(1)=1$. For $n \ge 2$ it is necessary to consider a second level of recursion. This involves an analysis of a total of nine cases, one of which will be analyzed here as an example.

If case 1 holds, then $\ell^s D^1 \le f(\frac{k \cdot n}{k+1})$, because the number of occurrences of atoms in C must be between $\frac{n}{k+1}$ and $\frac{k \cdot n}{k+1}$, by virtue of the fact that t is the indirect translation. The number of occurrences of atoms in $G\frac{\mathsf{T}}{q}$ and $G\frac{\mathsf{F}}{q}$, however, may be as large as $n-1$, so a second level of recursion must be considered for them. Since the formulas involved in derivations D^2 and D^3 are the same except for the interchanges of some T's and F's, they will have the same length. Consider D^2, and assume that case 1 again holds, so that $t(G\frac{\mathsf{T}}{q})=((t(B'\frac{\mathsf{T}}{r})\,\&\,t(C'))\vee(t(B'\frac{\mathsf{F}}{r})\,\&\,\neg t(C')))$, where $H_1\frac{\mathsf{T}}{q}$ is a subtree of C'. Pictorially, this is



Recursively, this calls for three derivations D^{21}, D^{22}, and D^{23}, where

$\vdash_I \hat{E}(t(C'),((t(H_{11}\frac{\mathrm{I}}{p})\&t(H_1\frac{\mathrm{I}}{q}))\vee(t(H_{11}\frac{\mathrm{E}}{p})\&\neg t(H_1\frac{\mathrm{I}}{q})))$ *via* D^{21},

$\vdash_I \hat{E}(t(B\frac{\mathrm{I}}{p}),((t(B'\frac{\mathrm{I}}{r})\&t(H_{11}\frac{\mathrm{I}}{p}))\vee(t(B'\frac{\mathrm{E}}{r})\&\neg t(H_{11}\frac{\mathrm{I}}{p})))$ *via* D^{22}, and

$\vdash_I \hat{E}(t(B\frac{\mathrm{E}}{p}),((t(B'\frac{\mathrm{I}}{r})\&t(H_{11}\frac{\mathrm{E}}{p}))\vee(t(B'\frac{\mathrm{E}}{r})\&\neg t(H_{11}\frac{\mathrm{E}}{p})))$ *via* D^{23}.

But now let n' be the number of occurrences of atoms in $G\frac{\mathrm{I}}{q}$. Then, since C' is chosen by the t function, the number of occurrences of atoms in C' is between $\frac{n'}{k+1}$ and $\frac{k\cdot n'}{k+1}$, and since $n'<n$, this is less than $\frac{k\cdot n}{k+1}$. Similarly, the number of occurrences of atoms in $B\frac{\mathrm{I}}{p}$ and $B\frac{\mathrm{E}}{p}$ is between $\frac{n}{k+1}$ and $\frac{k\cdot n}{k+1}$, so that the number of steps in each of D^{21}, D^{22}, and D^{23} is no greater than $f(\frac{k\cdot n}{k+1})$. This implies that

$\ell^s D \leq 1+f(\frac{k\cdot n}{k+1})+2(1+3f(\frac{k\cdot n}{k+1})) = 3+7f(\frac{k\cdot n}{k+1})$, for this one case 1.1. The analysis for the other eight cases is similar, the worst case being case 3.3 which gives

$$\ell^s D \leq 1+2f(\frac{k\cdot n}{k+1})+2(1+4f(\frac{k\cdot n}{k+1})) = 3+10f(\frac{k\cdot n}{k+1}).$$

Therefore, any function g satisfying

$$g(1)\geq 1, \text{ and}$$

$$g(n) \geq 3+10g(\tfrac{k}{k+1}n) \qquad (n\geq 2)$$

gives an upper bound for $f(n)$. One such function is $g(n)=n^{4k}$, since $1^{4k}=1\geq 1$, and for $n\geq 2$,

$$\begin{aligned} 3+10\cdot(\tfrac{k}{k+1}n)^{4k} &= [\tfrac{3}{n^{4k}}+10\cdot(\tfrac{k}{k+1})^{4k}]\cdot n^{4k} \\ &\leq [\tfrac{3}{2^4}+10\cdot((\tfrac{k}{k+1})^{k})^{4}]\cdot n^{4k} \\ &\leq [\tfrac{3}{16}+10\cdot(\tfrac{1}{2})^{4}]\cdot n^{4k} \qquad \text{(lemma 5.3.1.3.a.)} \\ &\leq [\tfrac{13}{16}]n^{4k} \\ &\leq n^{4k}. \end{aligned}$$

Therefore, $\ell^{s}D\leq(\ell A)^{4k}$, so that $\ell D \leq c\cdot\ell t(A)\cdot\ell^{s}D \leq c\cdot(\ell A)^{6k+1}$.

☒5.3.1.4.e.

LEMMA 5.3.1.4.f.

Lemma 5.3.1.4.e. still holds, even if the inference system I is replaced by Frege system F_1.

Proof

This is an immediate consequence of lemma 5.3.1.2.a., where the direct translation from κ_1 to κ_1 is the identity function.

☒5.3.1.4.f.

Lemmas 5.3.1.4.e. and 5.3.1.4.f. form the crucial link in the simulation of system $\hat{P}$ by system F_1. Now the simulation may proceed by analogy with the proof of lemma 5.3.1.2.a., with indirect translation here playing the rôle that direct translation played there.

LEMMA 5.3.1.4.g.

There are constants g_1 and g_2 such that whenever $\Gamma \vdash_{\hat{F}} A$ *via* D there is a derivation D' such that:

1) $t(\Gamma) \vdash_{F_1} t(A)$ *via* D',

2) $\ell^s D' \leq g_1 \cdot (\ell\Gamma + \ell D)^{4k+1} \cdot d(D)$, and

3) $\ell D' \leq g_2 \cdot (\ell\Gamma + \ell D)^{6k+2} \cdot d(D)$.

Proof

The proof proceeds analogously to lemma 5.3.1.2.a. For each formula B in D, derivation D' has the formula $t(B)$. For each inference rule $R_i \in \hat{\mathcal{R}}$, where $R_i = \Delta_i \to B_i$, let D^i be a derivation in system F_1 such that $t(\Delta_i) \vdash_{F_1} t(B_i)$ *via* D^i. Now suppose that B is inferred from $\hat{\Delta}$ in D by substitution σ in rule R_i. Then, $B = B_i\sigma$, $\hat{\Delta} = \Delta_i\sigma$, and each formula in $\hat{\Delta}$ either is a hypothesis of D or appears in D before B. Let $D^B = D^i t(\sigma)$, so that $t(\Delta_i)t(\sigma) \vdash_{F_1} t(B_i)t(\sigma)$ *via* D^B. Unlike the case in lemma 5.3.1.2.a., insertion of D^B in place of B is not sufficient to make D' the desired derivation. This is because t is an indirect (rather than a direct) translation, so that $t(B_i)t(\sigma)$ is not necessarily the same formula as $t(B_i\sigma)$. In fact, what must be done is that $t(B_i\sigma)$ must be derived from $t(B_i)t(\sigma)$, and for each $C_j \in \Delta_i$, $t(C_j)t(\sigma)$ must be derived from $t(C_j\sigma)$.

This is where lemmas 5.3.1.4.e. and 5.3.1.4.f. come in. Remember that since $\hat{F}$ has only a finite number of finite rules of inference, B_i (and each $C_j \in \Delta_i$) is one of a finite number of formulas for which these derivations must be constructed. Only the substitution σ is allowed to vary arbitrarily. To derive $t(B_i\sigma)$ from $t(B_i)t(\sigma)$, a derivation of $\hat{E}(t(B_i\sigma),t(B_i)t(\sigma))$ is constructed by recursion on the number of occurrences of atoms in B_i. Consider first the case where B_i contains no occurrences of atoms. In this case $B_i\sigma=B_i$ and $t(B_i)t(\sigma)=t(B_i)=t(B_i\sigma)$, so that the desired derivation is just an instance of the standard derivation of the tautology $\hat{E}(p,p)$.

Suppose that B_i contains at least one occurrence of the atom p, r is a new atom, and σ substitutes C for p. Then, there is a formula $\tilde{B}_i$ with one occurrence of r such that $B_i=\tilde{B}_i\frac{p}{r}$, and $B_i\sigma=\tilde{B}_i\sigma\frac{C}{r}$. By lemma 5.3.1.4.f., let D^0 be a derivation of $\hat{E}(t(B_i\sigma),((t(\tilde{B}_i\sigma\frac{\mathrm{T}}{r})\&t(C))\vee(t(\tilde{B}_i\sigma\frac{\mathrm{F}}{r})\&\neg t(C))))$. Since $\tilde{B}_i\frac{\mathrm{T}}{r}$ and $\tilde{B}_i\frac{\mathrm{F}}{r}$ contain one less occurrence of atoms than B_i, assume as inductive hypothesis that there exist derivations D^+ and D^- of $\hat{E}(t(\tilde{B}_i\frac{\mathrm{T}}{r}\sigma),t(\tilde{B}_i\frac{\mathrm{T}}{r})t(\sigma))$ and $\hat{E}(t(\tilde{B}_i\frac{\mathrm{F}}{r}\sigma),t(\tilde{B}_i\frac{\mathrm{F}}{r})t(\sigma))$, respectively. From these three equivalences (noting that $\tilde{B}_i\sigma\frac{\mathrm{T}}{r} = \tilde{B}_i\frac{\mathrm{T}}{r}\sigma$), $\hat{E}(t(B_i\sigma),((t(\tilde{B}_i\frac{\mathrm{T}}{r})t(\sigma)\&t(C))\vee(t(\tilde{B}_i\frac{\mathrm{F}}{r})t(\sigma)\&\neg t(C))))$ can be derived in a fixed number of steps. (In effect, equals have been substituted for equals.) But this last equivalence is the same as $\hat{E}(t(B_i\sigma),((t(\widetilde{B}_i\frac{T}{r})\&p)\vee(t(\widetilde{B}_i\frac{F}{r})\&\neg p))t(\sigma))$. Applying lemma 5.3.1.4.f. again, let D'' be a derivation of $\hat{E}(t(B_i),((t(\widetilde{B}_i\frac{T}{r})\&p)\vee(t(\widetilde{B}_i\frac{F}{r})\&\neg p)))$, so that $D''t(\sigma)$ is a derivation of $\hat{E}(t(B_i)t(\sigma),((t(\widetilde{B}_i\frac{T}{r})\&p)\vee(t(\widetilde{B}_i\frac{F}{r})\&\neg p))t(\sigma))$. These last two equivalences lead to a derivation of $\hat{E}(t(B_i\sigma),t(B_i)t(\sigma))$ in a constant number of steps.

To analyze the length of this derivation, first observe that every formula in it is bounded in length by some constant c times $\ell t(B_i\sigma)$. Then, note that the number of steps in D'' is fixed because B_i is fixed, and that the number of recursion steps in derivations D^+ and D^- is also fixed, since at each level of recursion the formula into which σ is being substituted has one less occurrence of atoms than at the previous level, and again since B_i is fixed. Thus, the total number of steps in this entire derivation is bounded by some constant d times the number of steps in D^0. By lemma 5.3.1.4.f., this quantity is bounded above by $d\cdot e_1\cdot(\ell B_i\sigma)^{4k}$.

Putting this derivation together with similar derivations for $C_j\sigma$ for each $C_j\in\Delta_i$, and with D^B, gives a derivation D_B of $t(B)=t(B_i\sigma)$ from $t(\Delta_i\sigma)=t(\hat{\Delta})$, such that there are constants (independent of σ) g_1 and g_2 such that $\ell^s D_B \leq g_1\cdot(\ell\hat{\Delta}+\ell B)^{4k}$ and $\ell D_B \leq g_2\cdot(\ell\Delta+\ell B)^{6k+1}$. Putting together these derivations D_B

for each formula B in D gives the derivation D' such that

$$t(\Gamma) \vdash_{F_1} t(A) \; via \; D',$$

$$\ell^{s}D' \leq g_1 \cdot (\ell\Gamma + \ell D)^{4k+1} \cdot d(D), \text{ and}$$

$$\ell D' \leq g_2 \cdot (\ell\Gamma + \ell D)^{6k+2} \cdot d(D).$$

⊠5.3.1.4.g.

Lemmas 5.3.1.4.g. and 5.3.1.4.a. can be combined to give the following.

LEMMA 5.3.1.4.h.

Frege system F_1 p-simulates $\hat{F}$.

Proof

Since $\kappa_1 \subseteq \hat{\kappa}$, g is the identity function. The function h is built using the constructions in lemmas 5.3.1.4.g. and 5.3.1.4.a. If $\vdash_{\hat{F}} A$ *via* D, then $h(D,A)$ is $D'D_2$, where D' is the derivation (in system F_1) of $t(A)$ constructed by lemma 5.3.1.4.g. and D_2 is the derivation of A from $t(A)$ constructed by lemma 5.3.1.4.a. It is a routine matter to verify that $g,h \in \mathcal{PF}$ and that $F_1(h(D,A))=A$ whenever $\hat{F}(D)=g(A)$. ⊠5.3.1.4.h.

Combining this result with lemma 5.3.1.4.d. and the transitivity of p-simulation, the main theorem of this section is immediate.

THEOREM 5.3.1.4.i.

Any two Frege systems p-simulate each other.