ORDINAL FACTORIZATION OF FINITE RELATIONS(1)

BY

C. C. CHANG

In this paper, we continue the work in [4] and [3] on ordinal multiplication of reflexive relations. In particular, we are concerned with the problem of unique factorization of a relation into indecomposable relations. A type α is called *indecomposable with respect to ordinal multiplication* (or simply, *indecomposable*) if $\alpha \neq 0$ and whenever $\alpha = \beta \cdot \gamma$, then either $\beta = 1$ or $\gamma = 1$. We let IT denote the class of indecomposable types. We define recursively the operation $\prod_{i \in n} \alpha_i$ by setting $\prod_{i \in 0} \alpha_i = 1$ and $\prod_{i \in p+1} \alpha_i = (\prod_{i \in p} \alpha_i) \cdot \alpha_p$. A type α has the strict unique factorization (SUF) property if whenever

$$\text{(A)} \qquad \alpha = \prod_{i \in n} \beta_i, \qquad \beta_i \in \text{IT for each } i \in n,$$

and

$$\text{(B)} \qquad \alpha = \prod_{j \in m} \gamma_j, \qquad \gamma_j \in \text{IT for each } j \in m,$$

then $m = n$ and $\beta_i = \gamma_i$ for each $i \in n$. A type α has the weak unique factorization (WUF) property if whenever (A) and (B) hold, then $m = n$ and there exists a permutation f of n such that $\beta_i = \gamma_{f(i)}$ for each $i \in n$. We shall see that there exist finite types which do not have the WUF property. After introducing the notion of a canonical factorization (CF), we shall prove that each finite type different from 0 and 1 has a unique CF. We shall also give characterizations of those finite types which have the SUF property as well as those finite types which have the WUF property(2).

The plan of the paper is as follows. We begin by proving a refinement theorem for ordinal products. This will require some extensions of results in [3]. We then prove some consequences of the refinement theorem when we progressively increase the restrictions to finite types. Among these results is a characterization of those finite types which form a permuting pair with

Received by the editors January 17, 1961.

(1) This paper contains results from one chapter of the author's doctoral thesis written under the direction of Professor Alfred Tarski at the University of California, Berkeley, in 1955. These results have mostly been summarized by the author in [2] at the Symposium on Lattice Theory held at Monterey, California in April, 1959. The author takes this opportunity to express his thanks to Professor Tarski for his guidance and encouragement during the writing of the thesis. The preparation of this paper was supported in part by the National Science Foundation grant G-6313, and in part by G-6693 and G-14006.

(2) The problem of developing a canonical form for the representation of an ordinal product was specifically stated as Problem 13 in [1, p. 37]. We have given a solution in the case of all finite types.

respect to ordinal multiplication. We conclude the paper with a complete solution of the factorization problem for finite types.

We assume thorough familiarity with the notation and contents of [3] and [4]. We call special attention to the introductory pages of [3] and we henceforth adopt the notation and conventions of that paper. For instance, by a relation or type we mean a reflexive relation or type. We let the Greek letters μ, ν (with appropriate subscripts) range over the class of all cardinals (finite and infinite) and, as in [3], we let μ^c and μ^s denote the cardinal and square type with cardinality μ. As in [4], we let the symbols $+^c$, $+^s$, and $+$ denote the respective operations of cardinal addition, square addition, and ordinal addition; the symbols $\sum^c$, $\sum^s$, and $\sum_{i,S}$ (S a simply ordering relation) shall denote the respective generalizations of the three additions. Also, we let the symbols CIT, SIT, and OIT denote the classes of types which are indecomposable under the respective modes of addition. As a consequence of the unique decomposition theorem [4, Appendix B], every type α has a unique representation as a sum of indecomposable types in each of the three modes of addition. To be more specific, every type α can be represented as a *cardinal sum*,

(C) $\alpha = \sum^c_{i\in\nu} \beta_i \cdot \nu_i^c$, where for each $i \in \nu$, $\beta_i \in$ CIT, $\beta_i \neq \beta_j$ if $i \neq j$, and $\nu \geqq 0$, $\nu_i > 0$ are cardinals,

as a *square sum*,

(D) $\alpha = \sum^s_{i\in\mu} \gamma_i \cdot \mu_i^s$, where for each $i \in \mu$, $\gamma_i \in$ SIT, $\gamma_i \neq \gamma_j$ if $i \neq j$, and $\mu \geqq 0$, $\mu_i > 0$ are cardinals,

or as an *ordered sum*,

(E) $\alpha = \sum_{i,S} \delta_i$, where for each $i \in F(S)$, $\delta_i \in$ OIT, and S is a simply ordering relation.

In each of the above cases, the representation is unique in their respective senses. If α is finite, the cardinals ν, ν_i in (C) and μ, μ_i in (D) as well as the relation S in (E) are all finite. More significantly, (E) can be written as

(F) $$\alpha = \sum_{i,T} \epsilon_i \cdot n_i^0,$$

where each n_i is an integer. We let CIT(α), SIT(α), and OIT(α) denote the sets of types which belong to CIT, SIT, and OIT, respectively, and which also occur in the corresponding decompositions (C), (D), and (E) of α. By the uniqueness of the decompositions, these sets are well-defined.

As was pointed out in [4], each one of the four operations, $+^c$, $+^s$, $+$, and $\cdot$ is a special case of the general sums of types β_i over a relation T, in symbols $\sum_{i,T}\beta_i$. From the associativity of this general sum, we see that the following (left) distributive laws hold:

$$\alpha\cdot\sum_{i\in\mu}^{c}\beta_i=\sum_{i\in\mu}^{c}\alpha\cdot\beta_i.$$

(G)
$$\alpha\cdot\sum_{i\in\mu}^{s}\beta_i=\sum_{i\in\mu}^{s}\alpha\cdot\beta_i.$$

$$\alpha\cdot\sum_{i,S}\beta_i=\sum_{i,S}\alpha\cdot\beta_i.$$

A moment's reflection will show that the corresponding right distributive laws will not hold. However, in the special cases $\alpha\in$CT and $\alpha\in$ST, we have also the following:

(H)
$$\text{If } \alpha\in\text{CT, then } \left(\sum_{i\in\mu}^{c}\beta_i\right)\cdot\alpha=\sum_{i\in\mu}^{c}(\beta_i\cdot\alpha).$$

$$\text{If } \alpha\in\text{ST, then } \left(\sum_{i\in\mu}^{s}\beta_i\right)\cdot\alpha=\sum_{i\in\mu}^{s}(\beta_i\cdot\alpha).$$

A type β is a *left (right) divisor* of α if there exists a type γ such that $\alpha=\beta\cdot\gamma(\alpha=\gamma\cdot\beta)$. Every type is a divisor of 0 and 1 is a divisor of any type. The property of being a left (or right) divisor is reflexive and transitive. It follows from [3, Theorem 19] that the set of left divisors of a finite type is simply ordered by the $<$ relation among types. From the previous discussion on distributivity, it follows that for each one of the three additions, if α is a left divisor of each summand, then α is a left divisor of the sum. In the special case that $\alpha\in$CT($\alpha\in$ST), if α is a right divisor of each summand, then α is a right divisor of the cardinal (square) sum.

Although ordinal multiplication is in general not commutative, there are special subsets of types among whose members ordinal multiplication is commutative. Examples of such sets are CT, ST and finite types of OT. We can verify quite easily that the classes CT, ST, and OT are each closed under ordinal multiplication and the taking of left or right divisors.

The first two lemmas are simple observations and will require no proof.

LEMMA 1. *Let* $\alpha\neq 0$.
(i) *If* $\alpha\notin$CIT, *then* $\alpha\in$SIT$\cap$OIT.
(ii) *If* $\alpha\notin$SIT, *then* $\alpha\in$CIT$\cap$OIT.
(iii) *If* $\alpha\notin$OIT, *then* $\alpha\in$CIT$\cap$SIT.

LEMMA 2. *Let* $\alpha \neq 1$ *and* $\beta \neq 0$.
(i) $\alpha \in \mathrm{CIT}$ *iff* $\beta \cdot \alpha \in \mathrm{CIT}$.
(ii) $\alpha \in \mathrm{SIT}$ *iff* $\beta \cdot \alpha \in \mathrm{SIT}$.
(iii) $\alpha \in \mathrm{OIT}$ *iff* $\beta \cdot \alpha \in \mathrm{OIT}$.

In terms of the defined notion of $\mathrm{CIT}(\alpha)$, we see that if $\alpha \neq 0$ then by conditions (C), (G), (H), and Lemmas 1 and 2, the following hold:

(J) $\alpha \in \mathrm{CT}$ if, and only if, $\mathrm{CIT}(\alpha) = \{1\}$.

(K) If $1 \in \mathrm{CIT}(\alpha)$, then $\mathrm{CIT}(\beta) \subset \mathrm{CIT}(\beta \cdot \alpha)$.

(L) If $\alpha \in \mathrm{CT}$, then $\mathrm{CIT}(\beta) = \mathrm{CIT}(\beta \cdot \alpha)$.

(M) If $1 \notin \mathrm{CIT}(\alpha)$ or if $\beta \in \mathrm{CIT}$, then $\mathrm{CIT}(\beta \cdot \alpha) = \{\beta \cdot \alpha_i;\ \alpha_i \in \mathrm{CIT}(\alpha)\}$.

(N) If β is finite, then $\alpha \in \mathrm{CT}$ iff $\mathrm{CIT}(\beta \cdot \alpha) = \mathrm{CIT}(\beta)$.

Each one of the conditions (J)–(N) remains true if we replace cardinal notions by square notions or ordinal notions.

The next lemma is a restatement of [3, Theorem 11 and Lemma 15].

LEMMA 3. *Let* $\alpha, \beta, \gamma, \delta$ *be types different from* 0. *If* $\alpha \cdot \delta = \beta \cdot \gamma$ *and* $\alpha \not< \beta$, *then there exist a relation* V *and, for each* $i \in F(V)$, *types* γ_i *and* δ_i *such that*
(i) $\gamma = \sum_{i,V} \gamma_i$ *and* $\delta = \sum_{i,V} \delta_i$,
(ii) *for each* $i \in F(V)$, $\alpha \cdot \delta_i = \beta \cdot \gamma_i$,
(iii) *for each* $i \in F(V)$, $\delta_i \in \mathrm{CT} \cup \mathrm{ST} \cup \mathrm{OT}$.

Proof. Excepting for a slight change of notation, the lemma follows from the indicated results.

Lemma 4 is an analog of [3, Lemma 5] and is another generalization of Euclid's Theorem.

LEMMA 4. *Let* p *and* q *be relatively prime positive integers.*
(i) *If* $p^c \cdot \alpha = q^c \cdot \beta$, *then there exists* γ *such that* $\alpha = q^c \cdot \gamma$ *and* $\beta = p^c \cdot \gamma$.
(ii) *If* $p^s \cdot \alpha = q^s \cdot \beta$, *then there exists* γ *such that* $\alpha = q^s \cdot \gamma$ *and* $\beta = p^s \cdot \gamma$.
(iii) *If* $p^0 \cdot \alpha = q^0 \cdot \beta$, *then there exists* γ *such that* $\alpha = q^0 \cdot \gamma$ *and* $\beta = p^0 \cdot \gamma$.

Proof. We shall first prove (i) and then give indications of the other proofs. Assume that $p^c \cdot \alpha = q^c \cdot \beta$, $p > q > 1$, and α, β different from 0. By Lemma 3, there exist a relation V and, for each $i \in F(V)$, types α_i and β_i such that

$$\alpha = \sum_{i,V} \alpha_i \quad \text{and} \quad \beta = \sum_{i,V} \beta_i, \tag{1}$$

$$\text{for each } i \in F(V),\ p^c \cdot \alpha_i = q^c \cdot \beta_i, \tag{2}$$

$$\text{for each } i \in F(V),\ \alpha_i \in \mathrm{CT} \cup \mathrm{ST} \cup \mathrm{OT}. \tag{3}$$

We first show that

(4) for each $i \in F(V)$, $\alpha_i \notin \mathrm{ST} \cup \mathrm{OT}$.

Assume that $\alpha_i \in \mathrm{ST}$. Representing both sides of (2) as square sums of types belonging to SIT, we see that since p^c, $q^c \in \mathrm{SIT}$

$$\mathrm{SIT}(p^c \cdot \alpha_i) = \{p^c\}$$

and

$$\mathrm{SIT}(q^c \cdot \beta_i) = \{q^c \cdot \gamma;\ \gamma \in \mathrm{SIT}(\beta_i)\}.$$

Since $\mathrm{SIT}(p^c \cdot \alpha_i) = \mathrm{SIT}(q^c \cdot \beta_i)$, it follows that $q \mid p$: a contradiction. Assume $\alpha_i \in \mathrm{OT}$. Representing both sides of (2) as ordinal sums of types belonging to OIT, we have

$$\mathrm{OIT}(p^c \cdot \alpha_i) = \{p^c\}$$

and

$$\mathrm{OIT}(q^c \cdot \beta_i) = \{q^c \cdot \gamma;\ \gamma \in \mathrm{OIT}(\beta_i)\}.$$

Thus again $q \mid p$ and a contradiction. Thus (4) is proved. From (2), (3), and (4), we obtain $\alpha_i \in \mathrm{CT}$. This implies $\beta_i \in \mathrm{CT}$ for each $i \in F(V)$. Using the commutativity of types in CT, and [3, Lemma 5], we have

(5) for each $i \in F(V)$, there exists a γ_i such that

$$\alpha_i = q^c \cdot \gamma_i \quad \text{and} \quad \beta_i = p^c \cdot \gamma_i.$$

Let $\gamma = \sum_{i,V} \gamma_i$. By the distributive law (G) and (5), we obtain the conclusion of (i).

The proof of (ii) is entirely analogous.

To prove (iii), we first eliminate the possibility that $\alpha_i \mathrm{CT} \cup \mathrm{ST}$. Thus for each $i \in F(V)$, $\alpha_i \in \mathrm{OT}$, $\beta_i \in \mathrm{OT}$, and $p^0 \cdot \alpha_i = q^0 \cdot \beta_i$. Using the discrete properties of p^0 and q^0, and remembering that in the proof of [3, Theorem 11] α_i and β_i are components of α and β under the equivalence relations H and K, we see that this implies $\alpha_i = q^0$ and $\beta_i = p^0$. Now $\gamma = \tau(V)$ is the required type such that $\alpha = q^0 \cdot \gamma$ and $\beta = p^0 \cdot \gamma$.

LEMMA 5. *Let p, q be positive integers and $1 \notin \mathrm{CIT}(\epsilon)$. Then p^c is a left (right) divisor of $q^c +^c \epsilon$ if, and only if, $p \mid q$ and p^c is a left (right) divisor of ϵ.*

Proof. In the case that $p \mid q$ and p^c is a left (right) divisor of ϵ, clearly p^c will be a left (right) divisor of $q^c +^c \epsilon$. Assume that p^c is a left divisor of $q^c +^c \epsilon$, i.e., $p^c \cdot \gamma = q^c +^c \epsilon$ for some γ. We write $\gamma = \mu^c +^c \gamma'$ where $\mu^c \in \mathrm{CT}$ and $1 \notin \mathrm{CIT}(\gamma')$. Thus $p^c \cdot \gamma = p^c \cdot \mu^c +^c p^c \cdot \gamma'$. Since $p^c \cdot \mu^c \in \mathrm{CT}$ and $1 \notin \mathrm{CIT}(p^c \cdot \gamma')$, we have

(1) $$p^c \cdot \mu^c = q^c \quad \text{and} \quad p^c \cdot \gamma' = \epsilon.$$

Assume that p^c is a right divisor of $q^c +^c \epsilon$, i.e., $\gamma \cdot p^c = q^c +^c \epsilon$ for some γ. Again,

writing $\gamma=\mu^c+{}^c\gamma'$, we have $\gamma\cdot p^c=\mu^c\cdot p^c+{}^c\cdot\gamma'\cdot p^c$. Since $\mu^c\cdot p^c\in\mathrm{CT}$ and $1\notin\mathrm{CIT}(\gamma'\cdot p^c)$, we arrive at

$$\mu^c\cdot p^c = q^c \quad \text{and} \quad \gamma'\cdot p^c = \epsilon. \tag{2}$$

(1) and (2) prove the lemma.

LEMMA 6. *Let p, q be positive integers and $1\notin\mathrm{SIT}(\epsilon)$. Then p^e is a left (right) divisor of $q^e+{}^e\epsilon$ if, and only if, $p\mid q$ and p^e is a left (right) divisor of ϵ.*

Proof. Analogous to the proof of Lemma 5.

LEMMA 7. *Let α, β, γ be different from 0 and let β be finite. Assume that $\alpha\cdot p^c=\beta\cdot\gamma$ and p is the least positive integer q such that β is a left divisor of $\alpha\cdot q^c$. Then for each cardinal ν, β is a left divisor of $\alpha\cdot\nu^c$ if, and only if, p is a divisor of ν.*

Proof. Assume the hypothesis of the lemma. If p is a divisor of ν, then clearly β is a left divisor of $\alpha\cdot\nu^c$. Assume that $\beta\cdot\delta=\alpha\cdot\nu^c$ for some δ. If ν is infinite, then $\nu^c=p^c\cdot\nu^c$ and p divides ν. If ν is finite, let $r=(p,\nu)$ and for some m and n, $(m,n)=1$, $p=rm$, and $\nu=nr$. We have

$$\beta\cdot\delta\cdot m^c = \alpha\cdot\nu^c\cdot m^c = \alpha\cdot p^c\cdot n^c = \beta\cdot\gamma\cdot n^c.$$

Since β is finite, by [3, Theorem 1],

$$\delta\cdot m^c = \gamma\cdot n^c.$$

From [3, Lemma 5], there exists an ϵ such that

$$\delta = \epsilon\cdot n^c \quad \text{and} \quad \gamma = \epsilon\cdot m^c.$$

Hence,

$$\alpha\cdot r^c\cdot n^c = \alpha\cdot\nu^c = \beta\cdot\delta = \beta\cdot\epsilon\cdot n^c.$$

Cancelling n^c from the right [3, Lemma 4], we see that β is a left divisor of $\alpha\cdot r^c$. Thus $r=p$ and $p\mid\nu$.

LEMMA 8. *Let α, β, γ be different from 0 and let β be finite. Assume that $\alpha\cdot p^e=\beta\cdot\gamma$ and p is the least positive integer q such that β is a left divisor of $\alpha\cdot q^e$. Then for each cardinal ν, β is a left divisor of $\alpha\cdot\nu^e$ if, and only if, p is a divisor of ν.*

Proof. Analogous to the proof of Lemma 7.

LEMMA 9. *Let α, β, γ be different from 0 and let β be finite. Assume that $\alpha\cdot p^0=\beta\cdot\gamma$ and p is the least positive integer q such that β is a left divisor of $\alpha\cdot q^0$. Then for each positive integer n, β is a left divisor of $\alpha\cdot n^0$ if, and only if, p is a divisor of n.*

Proof. Analogous to the proof of Lemma 7. Notice that here we cannot conclude that p^0 is a left divisor of an arbitrary infinite order type.

LEMMA 10. *Let α, β, γ be different from 0 and let β be finite. Assume that β is not a left divisor of α. Then the following two conditions are equivalent:*

(i) *$\alpha \cdot p^e = \beta \cdot \gamma$ where p is the least positive integer q such that β is a left divisor of $\alpha \cdot q^e$.*

(ii) *There exist types α', ϵ and a positive integer q such that $(p, q) = 1$, $1 \notin \mathrm{CIT}(\epsilon)$ and*

$$\alpha = \alpha' \cdot (q^e +^e p^e \cdot \epsilon),$$
$$\beta = \alpha' \cdot p^e,$$
$$\gamma = q^e +^e \epsilon \cdot p^e.$$

Proof. Assume (i). We write $\gamma = q^e +^e \delta$ where $1 \notin \mathrm{CIT}(\delta)$ (q will prove to be a positive integer) and represent α, β, and δ as cardinal sums of indecomposable types as in (C):

$$\alpha = \sum_{i \in \nu}^{e} \alpha_i \cdot \nu_i^e. \tag{1}$$

$$\beta = \sum_{i \in \pi}^{e} \beta_i \cdot n_i^e. \tag{2}$$

$$\delta = \sum_{i \in \mu}^{e} \delta_i \cdot \mu_i^e, \qquad \delta_i \neq 1 \qquad \text{for each } i \in \mu. \tag{3}$$

From (1), we obtain

$$\mathrm{CIT}(\alpha \cdot p^e) = \mathrm{CIT}(\alpha) = \{\alpha_i;\ i \in \nu\}. \tag{4}$$

From (2), (3) and the distributive law (G), we obtain

$$\begin{aligned} \mathrm{CIT}(\beta \cdot \gamma) &= \{\beta \cdot \delta_i;\ i \in \mu\} \text{ if } q = 0 \\ &= \{\beta \cdot \delta_i;\ i \in \mu\} \cup \mathrm{CIT}(\beta) \text{ if } q \neq 0. \end{aligned} \tag{5}$$

Since β is finite, $\{\beta \cdot \delta_i;\ i \in \mu\} \cap \mathrm{CIT}(\beta) = 0$ and, by [3; Theorem 1], $\beta \cdot \delta_i \neq \beta \cdot \delta_j$ if $i \neq j$. From (1) and (4), we see that each type α_i is repeated $\nu_i^e \cdot p^e$ times. From (2), (3) and (5), we see that each type β_i is repeated $n_i^e \cdot q^e$ times, and each type $\beta \cdot \delta_i$ is repeated μ_i^e times. By the unicity of the representation, each μ_i is divisible by p and each $n_i \cdot q$ is divisible by p. Hence

$$\mu_i = \mu_i' \cdot p \text{ for some } \mu_i' \tag{6}$$

and

$$n_i \cdot q = n_i' \cdot p \text{ for some } n_i'. \tag{7}$$

Let $\epsilon = \sum^c_{i\in\mu} \delta_i \cdot (\mu_i')^c$. We deduce from (3), (6), and (H) that $1 \notin \mathrm{CIT}(\epsilon)$ and

$$\delta = \sum_{i\in\mu}^{c} \delta_i \cdot \mu_i^c = \sum_{i\in\mu}^{c} (\delta_i \cdot \mu_i'^c) \cdot p^c = \epsilon \cdot p^c.$$

Hence $\gamma = q^c +^c \epsilon \cdot p^c$. If $q=0$, then $\alpha \cdot p^c = \beta \cdot \gamma = \beta \cdot \epsilon \cdot p^c$. Cancelling p^c from the right, we have the contradiction that β is a left divisor of α. If q is infinite, then $q^c = q^c \cdot p^c$ and

$$\alpha \cdot p^c = \beta \cdot \gamma = \beta \cdot (q^c \cdot p^c +^c \epsilon \cdot p^c) = \beta \cdot (q^c +^c \epsilon) \cdot p^c.$$

We now reach the same contradiction after cancelling p^c from the right. Thus $q \neq 0$ and q is finite. Let $(p, q) = r$, $p = s \cdot r$, $q = t \cdot r$, and $(s, t) = 1$. Then

$$\alpha \cdot s^c \cdot r^c = \alpha \cdot p^c = \beta \cdot \gamma = \beta \cdot (t^c \cdot r^c +^c \epsilon \cdot s^c \cdot r^c) = \beta \cdot (t^c +^c \epsilon \cdot s^c) \cdot r^c.$$

Cancelling r^c from the right, we see that β is a left divisor of $\alpha \cdot s^c$. Since p is the least positive integer with such property, $p = s$ and $r = 1$. Thus $(p, q) = 1$. Going back now to condition (7), we see that each n_i is divisible by p, say $n_i = m_i \cdot p$ for some m_i. Let $\alpha' = \sum^c_{i\in n} \beta_i \cdot m_i^c$. Then by (2), $\beta = \alpha' \cdot p^c$ and, by (G) and (H),

$$\alpha \cdot p^c = \beta \cdot \gamma = \alpha' \cdot p^c \cdot (q^c +^c \epsilon \cdot p^c) = \alpha' \cdot (q^c +^c p^c \cdot \epsilon) \cdot p^c.$$

Cancelling p^c on the right we obtain $\alpha = \alpha' \cdot (q^c +^c p^c \cdot \epsilon)$. Thus (ii) has been proved.

Assume (ii). It is evident that (ii) implies the equality $\alpha \cdot p^c = \beta \cdot \gamma$. Assume that p does not satisfy the minimality condition. Let n be the least positive integer such that $\alpha \cdot n^c = \beta \cdot \gamma'$ for some γ'. By Lemma 7,

(8) $$p = n \cdot r \text{ for some } r,$$

and by what we have already proved,

(9) there exist types α'', ϵ' and a positive integer m such that $(n, m) = 1$, $1 \notin \mathrm{CIT}(\epsilon')$, and

$$\begin{aligned} q &= \alpha'' \cdot (m^c +^c n^c \cdot \epsilon'), \\ \beta &= \alpha'' \cdot n^c, \\ \gamma &= (m^c +^c \epsilon' \cdot n^c). \end{aligned}$$

Now, from (8) and (9) and the hypothesis,

$$\alpha'' \cdot n^c = \beta = \alpha' \cdot p^c = \alpha' \cdot r^c \cdot n^c.$$

Therefore, $\alpha'' = \alpha' \cdot r^c$ and

(10) $$\begin{aligned} \alpha' \cdot (q^c +^c p^c \cdot \epsilon) &= \alpha''(m^c + n^c \cdot \epsilon') = \alpha' \cdot r^c \cdot (m^c +^c n^c \cdot \epsilon') \\ &= \alpha' \cdot (r^c \cdot m^c +^c p^c \cdot \epsilon'). \end{aligned}$$

Since β is finite, α' is finite, and by [3, Theorem 1] we cancel α' from (10) on the left, leaving us the equality

$$q^c +^c p^c \cdot \epsilon = r^c \cdot m^c +^c p^c \cdot \epsilon'.$$

Using the uniqueness of the representation, $q^c = r^c \cdot m^c$. Since $(p, q) = 1$, we conclude by (8) that $r = 1$. Hence $p = n$ and (i) is proved.

LEMMA 11. *Let α, β, γ be different from 0 and let β be finite. Assume that β is not a left divisor of α. Then the following two conditions are equivalent:*

(i) *$\alpha \cdot p^s = \beta \cdot \gamma$ where p is the least positive integer q such that β is a left divisor of $\alpha \cdot q^s$.*

(ii) *There exist types α', ϵ and a positive integer q such that $(p, q) = 1$, $1 \notin \mathrm{SIT}(\epsilon)$, and*

$$\alpha = \alpha' \cdot (q^s +^s p^s \cdot \epsilon),$$

$$\beta = \alpha' \cdot p^s,$$

$$\gamma = q^s +^s \epsilon \cdot p^s.$$

Proof. Entirely analogous to the proof of Lemma 10.

LEMMA 12. *Let α, β, γ be different from 0 and let β be finite. Assume that β is not a left divisor of α. Then the following two conditions are equivalent:*

(i) *$\alpha \cdot p^0 = \beta \cdot \gamma$ where p is the least positive integer q such that β is a left divisor of $\alpha \cdot q^0$.*

(ii) *There exists a finite type ϵ and a positive integer q such that $(p, q) = 1$ and*

$$\alpha = \epsilon \cdot q^0,$$

$$\beta = \epsilon \cdot p^0,$$

$$\gamma = q^0.$$

Proof. Assume (i). By (E), we represent γ as an ordinal sum of types in OIT as follows:

$$\gamma = \sum_{i,S} \gamma_i \text{ where } S \text{ is a simply ordering relation.} \tag{1}$$

Using the refinement law for ordinal addition, we see that the equality $\alpha \cdot p^0 = \beta \cdot \gamma$ with $p \geqq 2$ leads to the following two cases:

(2) There exist simply ordering relations U and V such that

$$S = U + V \quad \text{and} \quad \alpha = \beta \cdot \sum_{i,U} \gamma_i.$$

(3) There exist simply ordering relations U and V and nonzero types β_1 and β_2 such that

$$S = U + 1 + V, \qquad \beta = \beta_1 + \beta_2,$$

$$\alpha = \left(\beta \cdot \sum_{i,U} \gamma_i\right) + \beta_1,$$

$$\alpha \cdot (p-1)^0 = \beta_2 + \beta \cdot \sum_{i,V} \gamma_i.$$

Condition (2) leads to the contradiction that β is a left divisor of α. Therefore, we assume (3) to hold. We shall prove:

(4) For some positive integer q, $\gamma = q^0$.

If $U=0$, then $\alpha=\beta_1$ and α is finite. Assume that for some $i\in F(V)$ $\gamma_i\neq 1$. Since $\beta\cdot\gamma_i\in \mathrm{OIT}(\beta\cdot\gamma)$, $\beta\cdot\gamma_i\in\mathrm{OIT}(\alpha\cdot p^0)=\mathrm{OIT}(\alpha)$. But $\kappa(\beta\cdot\gamma_i)>\kappa(\beta)>\kappa(\alpha)$ which is impossible. Thus for each $i\in F(V)$, $\gamma_i=1$, and since α is finite, (4) holds. Let us now assume that $U\neq 0$. Since β is finite, the last two equations of (3) lead to:

(5) There exist simply ordering relations U' and V' such that

$$U = 1 + U', \qquad V = 1 + V',$$

$$\alpha = \beta + \left(\beta \cdot \sum_{i,U'} \gamma_i\right) + \beta_1,$$

$$\alpha \cdot (p-1)^0 = \beta_2 + \beta + \sum_{i,V'} \gamma_i.$$

From the last two equations of (5), it follows immediately that

(6) $$\beta_1 + \beta_2 = \beta_2 + \beta_1.$$

Now, independently of the precise value of p, the last equation of (3) yields the following:

(7) there exist a simply ordering relation W and types β_3 and β_4 such that W is a final segment of V,

$$\beta = \beta_3 + \beta_4,$$

$$\alpha = \beta_4 + \beta \cdot \sum_{i,W} \gamma_i.$$

By the same reasoning that established condition (3), we can prove that $\beta_3\neq 0$ and $\beta_4\neq 0$, and, furthermore, $W\neq 0$. Using the next to the last equation of (3), namely,

$$\alpha = \beta \cdot \sum_{i,U} \gamma_i + \beta_1$$

and the last two equations of (7), we can establish (after a simple induction) that either

(8) there exists a positive integer n such that $\tau(U)=n^0$ and

$$\gamma_i = 1 \text{ for each } i \in F(U),$$

or else

(9) for each positive integer n there exists a nonzero simply ordering relation U_n such that

$$U_1 = U,$$
$$U_n = 1 + U_{n+1} + 1,$$
$$\sum_{i,U_n} \gamma_i = 1 + \left(\sum_{i,U_{n+1}} \gamma_i \right) + 1.$$

Let us consider condition (9) first. From the results and discussions in [4] (more specifically, [4, Postulate IV, p. 8] and [4, p. 71]) we see that (9) implies the statement that

(10) there exists a type γ' such that $\sum_{i,U} \gamma_i = \omega + \gamma' + \omega^*$.

Furthermore, from the discussion on [4, p. 26] and [4, Postulate II′] and condition (6) above, we see that

(11)
$$\begin{aligned} \beta\cdot\omega^* + \beta_1 &= (\beta_1 + \beta_2)\cdot\omega^* + \beta_1 \\ &= (\beta_2 + \beta_1)\cdot\omega^* = \beta\cdot\omega^*. \end{aligned}$$

Now, (3), (10), and (11) imply

$$\begin{aligned} \alpha = \beta\cdot \sum_{i,U} \gamma_i + \beta_1 &= \beta\cdot(\omega + \gamma' + \omega^*) + \beta_1 \\ &= \beta\cdot\omega + \beta\cdot\gamma' + \beta\cdot\omega^* + \beta_1 \\ &= \beta\cdot\omega + \beta\cdot\gamma' + \beta\cdot\omega^* \\ &= \beta\cdot \sum_{i,U} \gamma_i. \end{aligned}$$

This is of course a contradiction to the assumption that β is not a left divisor of α. Hence (9) fails and (8) must hold. From (8) it is easily seen that each type in OIT(α) must have cardinality at most $\kappa(\beta)$. So $\gamma_i=1$ for each $i\in F(S)$. Since (8) also implies that α is finite, we conclude that S is finite and (4) is now proved. Finally, if $(p, q)\neq 1$, then we can cancel their common factor r^0 on the right and violate the assumption (i). Thus $(p, q)=1$ and (ii) follows from [3, Lemma 5].

Assume (ii). It is clear that (ii) implies $\alpha\cdot p^0=\beta\cdot\gamma$. Suppose that n is the least positive integer such that $\alpha\cdot n^c=\beta\cdot\gamma'$ for some γ'. Then by Lemma 9,

(12) $$p = n\cdot r \text{ for some } r,$$

and, by what we have already proved,

(13) there exist a finite type ϵ' and a positive integer m such that $(m, n)=1$ and

$$\alpha = \epsilon' \cdot m^0, \qquad \beta = \epsilon' \cdot n^0, \qquad \gamma' = m^0.$$

Now, (12) and (13) yield the equation

$$\epsilon' \cdot n^0 = \beta = \epsilon \cdot p^0 = \epsilon \cdot r^0 \cdot n^0$$

which implies $\epsilon' = \epsilon \cdot r^0$. Thus $\epsilon \cdot q^0 = \alpha = \epsilon' \cdot m^0 = \epsilon \cdot r^0 \cdot m^0$. Cancelling ϵ on the left we have $q = r \cdot m$. Since $(p, q)=1$, we have $r=1$. (i) now has been proved.

We pause here to mention that, by a technique similar to (but easier than) the proof of (ii) from (i) in Lemma 12, it is now possible to establish the conjecture C.2 of [3, p. 180] in the affirmative. As was pointed out in [3, p. 181], all we have to show is that under the conditions $\alpha \not< \gamma$ and $\alpha \cdot \beta_i = \gamma \cdot \delta_i$ where $\beta_i = n^0$ for some positive integer n, we must either have $\gamma < \alpha$ or $\gamma = \alpha$. Suppose $\gamma \not< \alpha$, then by the type of reasoning used in the proof of Lemma 12 we first see that $\delta_i \in \mathrm{OT}$ and then we see that $\delta_i = n^0$. Thus, after cancelling n^0 on the right, we have $\alpha = \gamma$.

THEOREM 13 (THE REFINEMENT THEOREM). *Let $\alpha, \beta, \gamma, \delta$ be different from 0, $\alpha \not< \beta$, β and δ be finite, and $\alpha \cdot \delta = \beta \cdot \gamma$. Then one and only one of the following possibilities can hold.*

(I) *There exists an $\epsilon \neq 0$ such that $\alpha = \beta \cdot \epsilon$ and $\epsilon \cdot \delta = \gamma$.*

(II) *There exist positive integers p, q with $p \geqq 2$ and $(p, q)=1$, and types $\alpha' \neq 0$, $\gamma' \neq 0$, and ϵ such that $1 \notin \mathrm{CIT}(\epsilon)$, $\kappa(q^c +^c p^c \cdot \epsilon) > p$, and*

$$\alpha = \alpha' \cdot (q^c +^c p^c \cdot \epsilon),$$
$$\beta = \alpha' \cdot p^c,$$
$$\gamma = (q^c +^c \epsilon \cdot p^c) \cdot \gamma',$$
$$\delta = p^c \cdot \gamma'.$$

(III) *There exist positive integers p, q with $p \geqq 2$ and $(p, q)=1$, and types $\alpha' \neq 0$, $\gamma' \neq 0$, and ϵ such that $1 \notin \mathrm{SIT}(\epsilon)$, $\kappa(q^s +^s p^s \cdot \epsilon) > p$, and*

$$\alpha = \alpha' \cdot (q^s +^s p^s \cdot \epsilon),$$
$$\beta = \alpha' \cdot p^s,$$
$$\gamma = (q^s +^s \epsilon \cdot p^s) \cdot \gamma',$$
$$\delta = p^s \cdot \gamma'.$$

(IV) *There exist positive integers p, q with $p \geqq 2$ and $(p, q)=1$, and types $\gamma' \neq 0$, $\epsilon \neq 0$ such that ϵ is finite, $q > p$, and*

$$\alpha = \epsilon \cdot q^0,$$
$$\beta = \epsilon \cdot p^0,$$
$$\gamma = q^0 \cdot \gamma',$$
$$\delta = p^0 \gamma'.$$

Proof. From the hypotheses and Lemma 3, there exist a relation V and, for each $i \in F(V)$, types γ_i and δ_i such that $\gamma = \sum_{i,V} \gamma_i$, $\delta = \sum_{i,V} \delta_i$ and, for each $i \in F(V)$, $\alpha \cdot \delta_i = \beta \cdot \gamma_i$ and $\delta_i \in \mathrm{CT} \cup \mathrm{ST} \cup \mathrm{OT}$. If β is a left divisor of α, then (I) will follow trivially. So we now assume the negation of (I) and consider the following three possibilities:

(1) For some $i \in F(V)$, $\delta_i \in \mathrm{CT}$.

(2) For some $i \in F(V)$, $\delta_i \in \mathrm{ST}$.

(3) For some $i \in F(V)$, $\delta_i \in \mathrm{OT}$.

Since we have assumed that β is not a left divisor of α, in each of the three cases (1)–(3), δ_i must be the cardinal or square or order type of a positive integer greater than 1. Suppose condition (1) holds. If p is the least positive integer such that β is a left divisor of $\alpha \cdot p^c$, then by Lemma 10,

(4) there exist types α', ϵ and a positive integer q such that $(p, q) = 1$, $1 \notin \mathrm{CIT}(\epsilon)$, $\alpha = \alpha' \cdot (q^c +^c p^c \cdot \epsilon)$, and $\beta = \alpha' \cdot p^c$, and $\alpha \cdot p^c = \beta \cdot (q^c +^c \epsilon \cdot p^c)$.

From Lemma 7,

(5) $\delta_i = p^c \cdot n_i^c$ for some positive integer n_i.

Putting (4) and (5) together, we have

$$\beta \cdot \gamma_i = \alpha \cdot \delta_i = \alpha \cdot p^c \cdot n_i^c = \beta \cdot (q^c +^c \epsilon \cdot p^c) \cdot n_i^c.$$

Cancelling β on the left, we obtain $\gamma_i = (q^c +^c \epsilon \cdot p^c) \cdot n_i^c$. Summarizing our conclusions when (1) holds, we have

(6) there exist positive integers p, q, n_i with $p \geqq 2$ and $(p, q) = 1$, and types $\alpha' \neq 0$ and ϵ such that $1 \notin \mathrm{CIT}(\epsilon)$ and

$$\alpha = \alpha' \cdot (q^c +^c p^c \cdot \epsilon),$$
$$\beta = \alpha' \cdot p^c,$$
$$\gamma_i = (q^c +^c \epsilon \cdot p^c) \cdot n_i^c,$$
$$\delta_i = p^c \cdot n_i^c.$$

In case condition (2) holds, then in an entirely analogous manner we obtain

(7) there exist positive integers p, q, n_i with $p \geqq 2$ and $(p, q) = 1$, and types $\alpha' \neq 0$ and ϵ such that $1 \notin \mathrm{SIT}(\epsilon)$ and

$$\alpha = \alpha' \cdot (q^{\epsilon} + {}^{\epsilon}p^{\epsilon} \cdot \epsilon),$$
$$\beta = \alpha' \cdot p^{\epsilon},$$
$$\gamma_i = (q^{\epsilon} + {}^{\epsilon}\epsilon \cdot p^{\epsilon}) \cdot n_i^{\epsilon},$$
$$\delta_i = p^{\epsilon} \cdot n_i^{\epsilon}.$$

Again, in case condition (3) holds, we have by Lemmas 9 and 12,

(8) there exist positive integers p, q, n_i with $p \geqq 2$ and $(p, q) = 1$, and a finite type $\epsilon \neq 0$ such that

$$\alpha = \epsilon \cdot q^0,$$
$$\beta = \epsilon \cdot p^0,$$
$$\gamma = p^0 \cdot n_i^0,$$
$$\delta = q^0 \cdot n_i^0.$$

Using now the hypothesis that $\alpha \not< \beta$ again, we see that (6) and (7) imply

(9) $$\text{if } \epsilon = 0, \quad \text{then} \quad q > p.$$

(9) can be expressed by the inequalities $\kappa(q^{\epsilon} + {}^{\epsilon}p^{\epsilon} \cdot \epsilon) > p$ and $\kappa(q^{\epsilon} + {}^{\epsilon}p^{\epsilon} \cdot \epsilon) > p$. In a more straightforward manner, (8) implies that $q > p$. Thus, if (1) holds then $\alpha \notin \mathrm{CIT}$, if (2) holds then $\alpha \notin \mathrm{SIT}$, and if (3) holds then $\alpha \notin \mathrm{OIT}$. By Lemma 1, one and only one of the conditions (1)–(3) can hold. Therefore, either

(10) $$\text{for each } i \in F(V), \quad \delta_i \in \mathrm{CT},$$

(11) $$\text{for each } i \in F(V), \quad \delta_i \in \mathrm{ST},$$

or

(12) $$\text{for each } i \in F(V), \quad \delta_i \in \mathrm{OT}.$$

Assume that (10) holds. By (6), each $\delta_i = p^c \cdot n_i^c$ for some n_i. Let $\gamma' = \sum_{i,V} n_i^c$. We have

$$\delta = \sum_{i,V} \delta_i = \sum_{i,V} p^c \cdot n_i^c = p^c \cdot \gamma'$$

and

$$\gamma = \sum_{i,V} [(q^c + {}^c\epsilon \cdot p^c) \cdot n_i^c] = (q^c + {}^c\epsilon \cdot p^c) \cdot \gamma'.$$

These last two equations and (6) prove (II). In an analogous manner, (III) follows from (7) and (IV) follows from (8).

It now only remains to prove that each of the conditions (II), (III) and (IV) precludes the possibility of (I). Assume that (II) holds and also that $\alpha=\beta\cdot\beta'$ for some β'. Thus

$$\alpha'\cdot(q^c +^c p^c\cdot\epsilon) = \alpha = \alpha'\cdot p^c\cdot\beta'.$$

Cancelling α' (which is finite) on the left gives us

$$q^c +^c p^c\cdot\epsilon = p^c\cdot\beta'.$$

Since $1\notin\mathrm{CIT}(\epsilon)$, $1\notin\mathrm{CIT}(p^c\cdot\epsilon)$. Hence, by Lemma 5, $p\,|\,q$, which is a contradiction. Similarly the case (III) is handled by Lemma 6. Finally, due to the finiteness conditions, condition (IV) obviously implies the negation of (I).

The next few lemmas are essentially in the nature of corollaries to Theorem 13.

LEMMA 14. *Assume the hypotheses of Theorem* 13. *Then the following hold*:

(i) *If either* $\alpha\notin\mathrm{CIT}$, *or* $\beta\notin\mathrm{CIT}$, *or* $\gamma\in\mathrm{CT}$, *or* $\delta\in\mathrm{CT}$, *then only conditions* (I) *and* (II) *of Theorem* 13 *can hold.*

(ii) *If either* $\alpha\notin\mathrm{SIT}$, *or* $\beta\notin\mathrm{SIT}$, *or* $\gamma\in\mathrm{ST}$, *or* $\delta\in\mathrm{ST}$, *then only conditions* (I) *and* (III) *of Theorem* 13 *can hold.*

(iii) *If either* $\alpha\notin\mathrm{OIT}$, *or* $\beta\notin\mathrm{OIT}$, *or* $\gamma\in\mathrm{OT}$, *or* $\delta\in\mathrm{OT}$, *then only conditions* (I) *and* (IV) *of Theorem* 13 *can hold.*

(iv) *If either* α *or* β *has cardinality greater than* 1 *and belongs to* $\mathrm{CIT}\cap\mathrm{SIT}\cap\mathrm{OIT}$, *then only condition* (I) *of Theorem* 13 *can hold.*

Proof. By inspection of the conclusions of Theorem 13. In cases (i)–(iii), we can obviously eliminate the two undesirable conclusions. In case (iv), only conclusion (I) holds.

REMARK. We notice that while the conclusions of Theorem 13 are entirely symmetrical, due to the noncommutativity of ordinal multiplication the formulation of Lemma 14 is not symmetric.

LEMMA 15. *Let* γ, δ, ϵ *be different from* 0 *and let* δ *be finite. Assume that* $1\notin\mathrm{CIT}(\epsilon)$ *and* $p\geqq 2$ *and* $(p, q)=1$. *Then the following two conditions are equivalent.*

(i) $(q^c+^c\epsilon)\cdot\delta=p^c\cdot\gamma$.

(ii) *There exist types* $\gamma'\neq 0$, $\epsilon'\neq 0$ *such that* $1\notin\mathrm{CIT}(\epsilon')$,

$$\epsilon = p^c\cdot\epsilon',$$
$$\gamma = (q^c +^c \epsilon'\cdot p^c)\cdot\gamma',$$
$$\delta = p^c\cdot\gamma'.$$

Proof. Obviously (ii) implies (i). Assume (i). Since $\epsilon\neq 0$, $(q^c+^c\epsilon)\not< p^c$. Since $(p, q)=1$, by Lemma 5, p^c is not a left divisor of $(q^c+^c\epsilon)$. Therefore, by

Lemma 14 (i), there exist types $\alpha' \neq 0$, $\gamma' \neq 0$, $\epsilon' \neq 0$ and integers n and m satisfying condition (II) of Theorem 13. In particular,

$$(q^c +^c \epsilon) = \alpha' \cdot (m^c +^c n^c \cdot \epsilon'), \tag{1}$$

$$p^c = \alpha' \cdot n^c, \tag{2}$$

$$\gamma = (m^c +^c \epsilon' \cdot n^c) \cdot \gamma', \tag{3}$$

$$\delta = n^c \cdot \gamma'. \tag{4}$$

From (1) and (2) we see that α' divides q^c and α' divides p^c. Therefore since $(p, q) = 1$

$$\alpha' = 1, p = n, q = m, \text{ and } p^c \cdot \epsilon' = \epsilon. \tag{5}$$

(3), (4), and (5) yield the desired conclusions of (ii).

LEMMA 16. *Let γ, δ, ϵ be different from 0 and let δ be finite. Assume that $1 \notin \mathrm{SIT}(\epsilon)$ and $p \geqq 2$ and $(p, q) = 1$. Then the following two conditions are equivalent:*

(i) $(q^s +^s \epsilon) \cdot \delta = p^s \cdot \gamma$.

(ii) *There exist types $\gamma' \neq 0$, $\epsilon' \neq 0$ such that $1 \notin \mathrm{SIT}(\epsilon')$,*

$$\epsilon = p^s \cdot \epsilon',$$

$$\gamma = (q^s +^s \epsilon' \cdot p^s) \cdot \gamma',$$

$$\delta = p^s \cdot \gamma'.$$

Proof. Entirely analogous to the proof of Lemma 15.

LEMMA 17. *Let β, γ, δ be finite types different from 0, $p \geqq 2$, and $\kappa(\beta) \leqq p$. Then the following hold.*

(i) *If either $p^c \cdot \delta = \beta \cdot \gamma$ or $\delta \cdot p^c = \gamma \cdot \beta$, then $\beta \in \mathrm{CT}$.*

(ii) *If either $p^s \cdot \delta = \beta \cdot \gamma$ or $\delta \cdot p^s = \gamma \cdot \beta$, then $\beta \in \mathrm{ST}$.*

(iii) *If either $p^0 \cdot \delta = \beta \cdot \gamma$ or $\delta \cdot p^0 = \gamma \cdot \beta$, then $\beta \in \mathrm{OT}$.*

Proof. As usual, cases (i) and (ii) are so similar that we shall only prove (i). Assume $p^c \cdot \delta = \beta \cdot \gamma$. Since $\kappa(\beta) \leqq p$, certainly $p^c \not< \beta$. Therefore, by Lemma 14 (i), either β is a left divisor of p^c or $p^c = \alpha' \cdot (m^c +^c n^c \cdot \epsilon)$ and $\beta = \alpha' \cdot m^c$ for some appropriate α', m, n, and ϵ. We see clearly that in either case $\beta \in \mathrm{CT}$. Assume $\gamma \cdot \beta = \delta \cdot p^c$. Since $\kappa(\beta) \leqq p$ and all types involved are finite, we have $\kappa(\delta) \leqq \kappa(\gamma)$. Thus $\gamma \not< \delta$. By Lemma 14 (i) again, either β is a right divisor of p^c or $p^c = (m^c +^c \epsilon \cdot n^c) \cdot \gamma'$ and $\beta = m^c \cdot \gamma'$ for some appropriate γ', m, n, and ϵ. In either case we obtain $\beta \in \mathrm{CT}$. Cases (i) and (ii) have been proved.

To prove (iii), assume $p^0 \cdot \delta = \beta \cdot \gamma$. Then either β is a left divisor of p^0 or else p^0 and β are finite ordinal (right) multiples of some common type ϵ. Clearly, this implies $\beta \in \mathrm{OT}$. Assume $\delta \cdot p^0 = \gamma \cdot \beta$, then either β is a right divisor of p^0, or else p^0 and β are finite ordinal (left) multiples of some common type ϵ. Again, $\beta \in \mathrm{OT}$.

The next few lemmas are concerned with the commutativity of finite types. We shall rely heavily on the finiteness condition. In fact, most of our proofs are by induction. Lemmas 18 and 21 are the main lemmas leading to Theorem 22. As in most preliminary results involving mathematical induction, some of the following lemmas (Lemmas 19 and 20) are stated and proved in a stronger form than it appears necessary for their intended applications. However, this is apparently unavoidable.

LEMMA 18. *Let p, q be positive integers such that $p>q$, and let α be a finite type. Then the following hold.*

(i) $p^c\cdot\alpha\cdot q^c=q^c\cdot\alpha\cdot p^c$ *if and only if* $\alpha\in$CT.

(ii) $p^s\cdot\alpha\cdot q^s=q^s\cdot\alpha\cdot p^s$ *if and only if* $\alpha\in$ST.

(iii) $p^0\cdot\alpha\cdot q^0=q^0\cdot\alpha\cdot p^0$ *if and only if* $\alpha\in$OT.

Proof. We prove (i) by induction on the following statement:

(1) For each finite α, if $\kappa(\alpha)\leqq n$, and $p^c\cdot\alpha\cdot q^c=q^c\cdot\alpha\cdot p^c$, then $\alpha\in$CT.

The cases when $n=0$ or $n=1$ are trivial. Assume that (1) holds for n. Let α be such that

$$\kappa(\alpha) = n+1 \quad \text{and} \quad p^c\cdot\alpha\cdot q^c = q^c\cdot\alpha\cdot p^c. \tag{2}$$

If $\kappa(q^c\cdot\alpha)\leqq p$, then by Lemma 17, $q^c\cdot\alpha\in$CT and $\alpha\in$CT. Therefore, assume $\kappa(q^c\cdot\alpha)>p$ and, hence, $q^c\cdot\alpha\not<p^c$. By Lemma 14 (i), we see that either

$$q^c\cdot\alpha = p^c\cdot\epsilon \quad \text{and} \quad \epsilon\cdot p^c = \alpha\cdot q^c \text{ for some } \epsilon, \tag{3}$$

or else

$$\begin{aligned} q^c\cdot\alpha &= \alpha'\cdot(m^c +^c n^c\cdot\epsilon),\\ p^c &= \alpha'\cdot n^c,\\ \alpha\cdot q^c &= (m^c +^c \epsilon\cdot n^c)\cdot\gamma',\\ p^c &= n^c\cdot\gamma', \end{aligned} \tag{4}$$

for some appropriate α', γ', ϵ, m and n.

If (3) holds, then since $p>q$, we have $\kappa(\epsilon)<\kappa(\alpha)$ and

$$p^c\cdot\epsilon\cdot q^c = q^c\cdot\alpha\cdot q^c = q^c\cdot\epsilon\cdot p^c.$$

This together with the inductive hypothesis lead to the fact that $\epsilon\in$CT and, hence, $\alpha\in$CT. If (4) holds, then we see that $\alpha', \gamma'\in$CT, $\alpha'=\gamma'$, and

$$\alpha'\cdot m^c\cdot q^c +^c p^c\cdot\epsilon\cdot q^c = q^c\cdot\alpha\cdot q^c = q^c\cdot m^c\cdot\gamma' +^c q^c\cdot\epsilon\cdot p^c.$$

Since $\alpha'\cdot m^c\cdot q^c=q^c\cdot m^c\cdot\gamma'$, we cancel it on the left and obtain

$$p^c\cdot\epsilon\cdot q^c = q^c\cdot\epsilon\cdot p^c. \tag{5}$$

Clearly, $\kappa(p^c\cdot\epsilon\cdot q^c)\leqq\kappa(q^c\cdot\alpha\cdot q^c)$, and since $p>q$, $\kappa(\epsilon)<\kappa(\alpha)$. The inductive

hypothesis and (5) yield the conclusion $\epsilon \in CT$ and $\alpha \in CT$. Thus, (i) has been proved. The proofs of (ii) and (iii) are entirely analogous to the proof of (i).

Lemma 18 implies, of course, that any finite type which permutes with a finite type in CT or ST or OT must itself belong to the corresponding set of types.

LEMMA 19. *Let p, q, r be positive integers such that $p \geqq 2$ and $(p, q) = 1$. Then the following hold.*

(i) *There do not exist finite types $\delta \neq 0$ and $\epsilon \neq 0$, and a non-negative integer m such that $1 \notin \mathrm{CIT}(\delta)$, $1 \notin \mathrm{CIT}(\epsilon)$, and*

$$p^c \cdot (\delta \cdot q^c +^c [r^c +^c \delta \cdot (p^m)^c] \cdot p^c \cdot \epsilon) = (\epsilon \cdot r^c +^c [q^c +^c p^c \cdot \epsilon \cdot (p^m)^c] \cdot \delta) \cdot p^c.$$

(ii) *There do not exist finite types $\delta \neq 0$ and $\epsilon \neq 0$, and a non-negative integer m such that $1 \notin \mathrm{SIT}(\delta)$, $1 \notin \mathrm{SIT}(\epsilon)$, and*

$$p^s \cdot (\delta \cdot q^s +^s [r^s +^s \delta \cdot (p^m)^s] \cdot p^s \cdot \epsilon) = (\epsilon \cdot r^s +^s [q^s +^s p^s \cdot \epsilon \cdot (p^m)^s] \cdot \delta) \cdot p^s.$$

Proof. We prove (i) by contradiction. Suppose there exist finite types $\delta \neq 0$ and $\epsilon \neq 0$ such that the conclusion of (i) holds for some m. We may assume δ and ϵ are such that whenever δ' and ϵ' satisfy

$$\delta' \neq 0, \qquad \epsilon' \neq 0, \quad \text{and} \quad \kappa(\delta') + \kappa(\epsilon') < \kappa(\delta) + \kappa(\epsilon),$$

then for no m does (i) hold for δ' and ϵ'. We represent $\delta = \sum^c_{i \in s} \delta_i \cdot s_i^c$ and $\epsilon = \sum^c_{i \in t} \epsilon_i \cdot t_i^c$ as in (C). Thus $\mathrm{CIT}(\delta) = \{\delta_i; i \in s\}$ and $\mathrm{CIT}(\epsilon) = \{\epsilon_i; i \in t\}$. We see that $\delta_i \neq 1$ and $\epsilon_i \neq 1$. By inspection of the equation in (i), we obtain

$$\begin{aligned} &\mathrm{CIT}[p^c \cdot (\delta \cdot q^c +^c [r^c +^c \delta \cdot (p^m)^c] \cdot p^c \cdot \epsilon)] \\ &\qquad = \{p^c \cdot \delta_i; i \in s\} \cup \{p^c \cdot [r^c +^c \delta \cdot (p^m)^c] \cdot p^c \cdot \epsilon_i; i \in t\}, \end{aligned} \tag{1}$$

and

$$\begin{aligned} &\mathrm{CIT}[(\epsilon \cdot r^c +^c [q^c +^c p^c \cdot \epsilon \cdot (p^m)^c] \cdot \delta) \cdot p^c] \\ &\qquad = \{\epsilon_i; i \in t\} \cup \{(q^c +^c p^c \cdot \epsilon \cdot (p^m)^c] \cdot \delta_i; i \in s\}. \end{aligned} \tag{2}$$

Since every indecomposable type in the right-hand side of (1) is of the form $p^c \cdot \beta$ for some $\beta \in IT$, by the uniqueness of the decomposition, (1) and (2) imply

$$\text{for each } i \in t, \qquad \epsilon_i = p^c \cdot \epsilon_i' \text{ for some } \epsilon_i' \tag{3}$$

and

$$\text{for each } i \in s, \quad [q^c +^c p^c \cdot \epsilon \cdot (p^m)^c] \cdot \delta_i = p^c \cdot \gamma_i \text{ for some } \gamma_i. \tag{4}$$

Let $\epsilon' = \sum^c_{i \in t} \epsilon_i' \cdot t_i^c$. We easily see that (3) gives us

$$\epsilon = p^c \cdot \epsilon', \ \epsilon' \neq 0, \ 1 \notin \mathrm{CIT}(\epsilon'), \text{ and } \kappa(\epsilon') < \kappa(\epsilon). \tag{5}$$

Now, $1 \notin \mathrm{CIT}(p^c \cdot \epsilon \cdot (p^m)^c)$, hence by Lemma 15, (4) yields

(6) $\qquad$ for each $i \in s$, $\quad \delta_i = p^c \cdot \delta_i'$ for some δ_i'.

Let $\delta' = \sum_{i \in s}^c \delta_i' \cdot s_i^c$. (6) implies that

(7) $\qquad \delta = p^c \cdot \delta', \quad \delta' \neq 0, \quad 1 \notin \mathrm{CIT}(\delta'), \quad$ and $\quad \kappa(\delta') < \kappa(\delta)$.

Using (5) and (7), we rewrite the left-hand side of the equation in (i) as follows:

$$
\begin{aligned}
& p^c \cdot (\delta \cdot q^c +^c [r^c +^c \delta \cdot (p^m)^c] \cdot p^c \cdot \epsilon) \\
&\quad = p^c \cdot (p^c \cdot \delta' \cdot q^c +^c [r^c +^c p^c \cdot \delta' \cdot (p^m)^c] \cdot p^c \cdot p^c \cdot \epsilon') \\
&\quad = p^c \cdot (p^c \cdot \delta' \cdot q^c +^c p^c \cdot [r^c +^c \delta' \cdot (p^{m+1})^c] \cdot p^c \cdot \epsilon') \\
&\quad = p^c \cdot p^c \cdot (\delta' \cdot q^c +^c [r^c +^c \delta' \cdot (p^{m+1})^c] \cdot p^c \cdot \epsilon').
\end{aligned} \tag{8}
$$

Similarly, the right-hand side of the equation in (i) can be transformed.

$$
\begin{aligned}
& (\epsilon \cdot r^c +^c [q^c +^c p^c \cdot \epsilon \cdot (p^m)^c] \cdot \delta) \cdot p^c \\
&\quad = (p^c \cdot \epsilon' \cdot r^c +^c [q^c +^c p^c \cdot p^c \cdot \epsilon' \cdot (p^m)^c] \cdot p^c \cdot \delta') \cdot p^c \\
&\quad = (p^c \cdot \epsilon' \cdot r^c +^c p^c \cdot [q^c +^c p^c \cdot \epsilon' \cdot (p^{m+1})^c] \cdot \delta') \cdot p^c \\
&\quad = p^c \cdot (\epsilon' \cdot r^c +^c [q^c +^c p^c \cdot \epsilon' \cdot (p^{m+1})^c] \cdot \delta') \cdot p^c.
\end{aligned} \tag{9}
$$

Equating now the last line of (8) with the last line of (9), and cancelling p^c on the left we obtain

$$
\begin{aligned}
& p^c \cdot (\delta' \cdot q^c +^c [r^c +^c \delta' \cdot (p^{m+1})^c] \cdot p^c \cdot \epsilon') \\
&\qquad = (\epsilon' \cdot r^c +^c [q^c +^c p^c \cdot \epsilon' \cdot (p^{m+1})^c] \cdot \delta') p^c.
\end{aligned} \tag{10}
$$

(10) implies that (i) holds for δ', ϵ' and $(m+1)$ when $\kappa(\delta') + \kappa(\epsilon') < \kappa(\delta) + \kappa(\epsilon)$. This is a contradiction to the minimality conditions satisfied by δ and ϵ. Hence (i) has been proved. The proof for (ii) is entirely analogous to the proof of (i).

LEMMA 20. *Let p, q be positive integers such that $p \geqq 2$ and $(p, q) = 1$, and let ϵ be a finite type different from 0. Then the following hold.*

(i) *If $1 \notin \mathrm{CIT}(\epsilon)$, then there do not exist a finite type $\delta \neq 0$ and a non-negative integer m such that $1 \notin \mathrm{CIT}(\delta)$ and*

$$(p^{m+1})^c \cdot \delta \cdot (q^c +^c \epsilon) = (q^c +^c \epsilon) \cdot (p^m)^c \cdot \delta \cdot p^c.$$

(ii) *If $1 \notin \mathrm{SIT}(\epsilon)$, then there do not exist a finite type $\delta \neq 0$ and a non-negative integer m such that $1 \notin \mathrm{SIT}(\delta)$ and*

$$(p^{m+1})^s \cdot \delta \cdot (q^s +^s \epsilon) = (q^s +^s \epsilon) \cdot (p^m)^s \cdot \delta \cdot p^s.$$

Proof. We prove (i) by contradiction. Suppose there exists a finite type δ such that the conclusion of (i) holds for some m. We may assume that δ is such that whenever δ' satisfy

$$\delta' \neq 0, \quad 1 \notin \mathrm{CIT}(\delta'), \quad \text{and} \quad \kappa(\delta') < \kappa(\delta),$$

then for no m does (i) hold for δ'. We represent $\delta = \sum^c_{i\in s} \delta_i \cdot s^c_i$ and $\epsilon = \sum^c_{i\in t} \epsilon_i \cdot t^c_i$ as in (C). By inspection of the equation in (i), we obtain

(1) $$\mathrm{CIT}((p^{m+1})^c \cdot \delta \cdot (q^c +^c \epsilon)) = \{(p^{m+1})^c \cdot \delta_i;\ i \in s\} \cup \{(p^{m+1})^c \cdot \delta \cdot \epsilon_i;\ i \in t\}$$

and

(2) $$\mathrm{CIT}((q^c +^c \epsilon) \cdot (p^m)^c \cdot \delta \cdot p^c) = \{(q^c +^c \epsilon) \cdot (p^m)^c \cdot \delta_i;\ i \in s\}.$$

Since the left-hand sides of (1) and (2) are equal, we have

(3) for each $i \in s$, there exists a β_i such that

$$(q^c +^c \epsilon) \cdot (p^m)^c \cdot \delta_i = (p^{m+1})^c \cdot \beta_i.$$

Since $(p^{m+1}, q) = 1$, by Lemma 15 and (3), we have

(4) for each $i \in s$, $(p^m)^c \cdot \delta_i = (p^{m+1})^c \cdot \delta'_i$ for some δ'_i.

Let $\delta' = \sum^c_{i\in s} \delta'_i \cdot s^c_i$. Cancelling $(p^m)^c$ on the left in (4), we have

$$\delta = p^c \cdot \delta', \quad \delta' \neq 0, \quad 1 \notin \mathrm{CIT}(\delta'), \quad \text{and} \quad \kappa(\delta') < \kappa(\delta).$$

Substituting $p^c \cdot \delta'$ for δ in the equation in (i), we obtain

$$(p^{m+2})^c \cdot \delta' \cdot (q^c +^c \epsilon) = (q^c +^c \epsilon) \cdot (p^{m+1})^c \cdot \delta' \cdot p^c.$$

This implies that (i) holds for δ' and $(m+1)$ where $\kappa(\delta') < \kappa(\delta)$, which is a contradiction to the way δ was picked. Hence (i) is proved. The proof for (ii) is entirely analogous to the proof of (i).

LEMMA 21. *Let p, q be positive integers such that $p \geqq 2$ and $(p, q) = 1$, and let ϵ be a finite type different from 0. Then the following hold.*

(i) *If $1 \notin \mathrm{CIT}(\epsilon)$, then there does not exist a finite type $\gamma \neq 0$ such that $p^c \cdot \gamma \cdot (q^c +^c p^c \cdot \epsilon) = (q^c +^c p^c \cdot \epsilon) \cdot \gamma \cdot p^c$.*

(ii) *If $1 \notin \mathrm{SIT}(\epsilon)$, then there does not exist a finite type $\gamma \neq 0$ such that $p^s \cdot \gamma \cdot (q^s +^s p^s \cdot \epsilon) = (q^s +^s p^s \cdot \epsilon) \cdot \gamma \cdot p^s$.*

Proof. We prove (i) by contradiction. Suppose there exists a finite type $\gamma \neq 0$ satisfying the equation of (i). We represent $\gamma = r^c +^c \delta$ where $1 \notin \mathrm{CIT}(\delta)$. If $\delta = 0$, then we would have the equation $p^c \cdot r^c \cdot q^c +^c p^c \cdot r^c \cdot p^c \cdot \epsilon = q^c \cdot r^c \cdot p^c +^c p^c \cdot \epsilon \cdot r^c \cdot p^c$. From this, we obtain

$$p^c \cdot r^c \cdot p^c \cdot \epsilon = p^c \cdot \epsilon \cdot r^c \cdot p^c.$$

Cancelling p^c on the left, we see that ϵ permutes with $(p \cdot r)^c$. Hence, by Lemma 18 (i), $\epsilon \in \mathrm{CT}$, which is a contradiction. Therefore, we assume $\delta \neq 0$. If $r = 0$, then we have the equation

$$p^c \cdot \delta \cdot (q^c +^c p^c \cdot \epsilon) = (q^c +^c p^c \cdot \epsilon) \cdot \delta \cdot p^c,$$

which is impossible by Lemma 20 (i), with $m=0$. Therefore, $\delta \neq 0$ and $r \neq 0$. After multiplying out the equation in (i) and cancelling the term $(p \cdot r \cdot q)^c$, we obtain the equation

$$p^c \cdot (\delta \cdot q^c +^c [r^c +^c \delta] \cdot p^c \cdot \epsilon) = (\epsilon \cdot r^c +^c [q^c +^c p^c \cdot \epsilon] \cdot \delta) \cdot p^c,$$

which is impossible by Lemma 19 (i), with $m=0$. Thus in each case we have reached a contradiction and (i) is proved. The proof for (ii) is entirely analogous to the proof of (i).

THEOREM 22. *Let α and β be finite types different from* 0 *and* 1, *and let n be a positive integer. Then $\alpha^n \cdot \beta = \beta \cdot \alpha^n$ if, and only if, one of the following four conditions holds*:

(i) $\alpha \in$ CT *and* $\beta \in$ CT.
(ii) $\alpha \in$ ST *and* $\beta \in$ ST.
(iii) $\alpha \in$ OT *and* $\beta \in$ OT.
(iv) $\alpha = \gamma^p$ *and* $\beta = \gamma^q$ *for some type* γ *and integers* p *and* q.

Proof. It is clear that each one of the four conditions (i)–(iv) will imply $\alpha \cdot \beta = \beta \cdot \alpha$ and hence $\alpha^n \cdot \beta = \beta \cdot \alpha^n$. We complete the proof in the other direction by establishing the following statement by induction.

(1) If α and β are finite types different from 0 and $\kappa(\alpha^n \cdot \beta) \leqq m$, then one of the conditions (i)–(iv) holds.

The cases where $m=0$ and $m=1$ are trivial. Assume (1) holds for m. Let α and β be finite types such that $\kappa(\alpha^n \cdot \beta) \leqq m+1$ and

$$\alpha \cdot (\alpha^{n-1} \cdot \beta) = \beta \cdot \alpha^n. \tag{2}$$

We now apply Theorem 13 to the equation of (2) and consider the following nine possible cases.

CASE 1. $\kappa(\alpha) = \kappa(\beta)$. In this case, by [3, Corollary 20], $\alpha = \beta$ and clearly condition (iv) is satisfied.

CASE 2. $\kappa(\alpha) > \kappa(\beta)$. By Theorem 13 we divide this into four subcases.

CASE 2a. $\alpha = \beta \cdot \epsilon$ for some type ϵ. Since $\kappa(\beta) \geqq 2$, we see that $\kappa(\epsilon) < \kappa(\alpha)$. Now (2) implies

$$(\beta \cdot \epsilon)^n \cdot \beta = \beta \cdot (\beta \cdot \epsilon)^n.$$

Using the associative law, we can write the above as

$$\beta \cdot (\epsilon \cdot \beta)^n = \beta \cdot (\beta \cdot \epsilon)^n.$$

Cancelling β on the left yields the equation

$$(\epsilon \cdot \beta)^n = (\beta \cdot \epsilon)^n. \tag{3}$$

Applying [3, Corollary 3] to (3), we see that $\epsilon \cdot \beta = \beta \cdot \epsilon$. The commutativity of ϵ and β implies that $\epsilon^n \cdot \beta = \beta \cdot \epsilon^n$. Since $\kappa(\epsilon^n \cdot \beta) < \kappa(\alpha^n \cdot \beta)$, by the inductive

hypothesis we conclude that one of the conditions (i)–(iv) holds for ϵ and β. It is now immediate that the same condition will hold for α and β.

CASE 2b. For some appropriate α', ϵ, p and q,

$$\alpha = \alpha' \cdot (q^c +^c p^c \cdot \epsilon) \quad \text{and} \quad \beta = \alpha' \cdot p^c. \tag{4}$$

Equations (2) and (4) give

$$\alpha' \cdot (q^c +^c p^c \cdot \epsilon) \cdot \alpha^{n-1} \cdot \alpha' \cdot p^c = \alpha' \cdot p^c \cdot \alpha^{n-1} \cdot \alpha' \cdot (q^c +^c p^c \cdot \epsilon).$$

Cancelling α' on the left and applying Lemma 21 (i) with $\gamma = \alpha^{n-1} \cdot \alpha'$, we see that ϵ must be 0. Hence

$$q^c \cdot (\alpha^{n-1} \cdot \alpha') \cdot p^c = p^c \cdot (\alpha^{n-1} \cdot \alpha') \cdot q^c$$

and, by Lemma 18 (i), $\alpha^{n-1} \cdot \alpha' \in \mathrm{CT}$. This leads to the conclusion (i) that $\alpha, \beta \in \mathrm{CT}$.

CASE 2c. For some appropriate α', ϵ, p and q,

$$\alpha = \alpha' \cdot (q^s +^s p^s \cdot \epsilon) \quad \text{and} \quad \beta = \alpha' \cdot p^s.$$

The argument here is exactly the same as in Case 2b, except for using Lemmas 18 (ii) and 21 (ii). This will lead to the conclusion (ii).

CASE 2d. For some appropriate ϵ, p, and q,

$$\alpha = \epsilon \cdot q^0 \quad \text{and} \quad \beta = \epsilon \cdot p^0. \tag{5}$$

Equations (2) and (5) give

$$\epsilon \cdot q^0 \cdot \alpha^{n-1} \cdot \epsilon \cdot p^0 = \epsilon \cdot p^0 \cdot \alpha^{n-1} \cdot \epsilon \cdot q^0.$$

Cancelling ϵ on the left, and applying Lemma 18 (iii), we see that $\alpha^{n-1} \cdot \epsilon \in \mathrm{OT}$. This leads to the conclusion (iii).

CASE 3. $\kappa(\beta) < \kappa(\alpha)$. By Theorem 13, we also divide this case into four subcases.

CASE 3a. $\beta = \alpha \cdot \epsilon$ for some type ϵ. Since $\kappa(\alpha) \geqq 2$, we have $\kappa(\epsilon) < \kappa(\beta)$. Equation (2) implies,

$$\alpha^n \cdot \alpha \cdot \epsilon = \alpha \cdot \epsilon \cdot \alpha^n.$$

Cancelling α on the left, we obtain $\alpha^n \cdot \epsilon = \epsilon \cdot \alpha^n$. Since $\kappa(\alpha^n \cdot \epsilon) < \kappa(\alpha^n \cdot \beta)$, by inductive hypothesis one of the conditions (i)–(iv) holds for α and ϵ. This of course implies that one of the conditions (i)–(iv) holds for α and β.

CASE 3b. For some appropriate β', ϵ, p and q,

$$\beta = \beta' \cdot (q^c +^c p^c \cdot \epsilon) \quad \text{and} \quad \alpha = \beta' \cdot p^c. \tag{6}$$

By essentially the same argument we used in Case 2b, we see that letting $\gamma = \alpha^{n-1} \cdot \beta'$, we obtain from (2) and (6),

$$p^c \cdot \gamma \cdot (q^c +^c \mathrm{p}^c \cdot \epsilon) = (q^c +^c \mathrm{p}^c \cdot \epsilon) \cdot \gamma \cdot p^c.$$

Applying Lemma 21 (i), we see that ϵ must be 0. Hence,

$$p^c \cdot \gamma \cdot q^c = q^c \cdot \gamma \cdot p^c.$$

By Lemma 18 (i), $\gamma = \alpha^{n-1} \cdot \beta' \in \mathrm{CT}$. This leads to the conclusion (i) that $\alpha, \beta \in \mathrm{CT}$.

CASE 3c. For some appropriate β', ϵ, p and q,

$$\beta = \beta' \cdot (q^s +^s \mathrm{p}^s \cdot \epsilon) \quad \text{and} \quad \alpha = \beta' \cdot p^s.$$

The argument is exactly the same as in Case 3b, except for using Lemmas 18 (ii) and 21 (ii). This will lead to the conclusion (ii).

CASE 3d. For some appropriate ϵ, p and q,

$$\beta = \epsilon \cdot q^0 \quad \text{and} \quad \alpha = \epsilon \cdot p^0. \tag{7}$$

Since (5) and (7) are exactly the same, using the same argument for Case 2d will lead us to the conclusion (iii).

Next follow some corollaries of Theorem 22.

COROLLARY 23. *Let α and β be finite types different from* 0 *and* 1. *Then $\alpha \cdot \beta = \beta \cdot \alpha$ if and only if one of the following four conditions holds*:

(i) $\alpha \in \mathrm{CT}$ *and* $\beta \in \mathrm{CT}$.

(ii) $\alpha \in \mathrm{ST}$ *and* $\beta \in \mathrm{ST}$.

(iii) $\alpha \in \mathrm{OT}$ *and* $\beta \in \mathrm{OT}$.

(iv) $\alpha = \gamma^p$ *and* $\beta = \gamma^q$ *for some type* γ *and integers* p *and* q.

COROLLARY 24. *Let α and β be finite types different from* 0 *and* 1, *and let n and m be positive integers. Then $\alpha^n \cdot \beta^m = \beta^m \cdot \alpha^n$ if and only if $\alpha \cdot \beta = \beta \cdot \alpha$.*

Proof. It is clear that $\alpha \cdot \beta = \beta \cdot \alpha$ implies $\alpha^n \cdot \beta^m = \beta^m \cdot \alpha^n$. On the other hand, if $\alpha^n \cdot \beta^m = \beta^m \cdot \alpha^n$, then α and β^m will satisfy conditions (i)–(iv) of Theorem 22. From this, we deduce that $\alpha \cdot \beta^m = \beta^m \cdot \alpha$. Applying Theorem 22 once more, we have $\alpha \cdot \beta = \beta \cdot \alpha$.

COROLLARY 25. *Let α, β, γ be finite types and let α be different from* 0 *and* 1. *If $\alpha \cdot \beta = \beta \cdot \alpha$ and $\alpha \cdot \gamma = \gamma \cdot \alpha$, then $\beta \cdot \gamma = \gamma \cdot \beta$.*

Proof. Clearly, if either β or γ is equal to 0 or 1, then the conclusion holds. Therefore, assume β and γ are different from 0 and 1. Applying Corollary 23 to the equations $\alpha \cdot \beta = \beta \cdot \alpha$ and $\alpha \cdot \gamma = \gamma \cdot \alpha$, we see that one of the following possibilities holds:

(i) $\alpha, \beta, \gamma \in \mathrm{CT}$.

(ii) $\alpha, \beta, \gamma \in \mathrm{ST}$.

(iii) $\alpha, \beta, \gamma \in \mathrm{OT}$.

(iv) There exist types ϵ and δ, and integers p, q, m and n such that

$$\alpha = \epsilon^p \quad \text{and} \quad \beta = \epsilon^q,$$

$$\alpha = \delta^m \quad \text{and} \quad \gamma = \delta^n.$$

Conditions (i)–(iii) lead trivially to the conclusion $\beta\cdot\gamma=\gamma\cdot\beta$. In case (iv) holds, we see that

$$\epsilon^p\cdot\delta^m = \delta^m\cdot\epsilon^p.$$

Therefore, by Corollary 24, $\epsilon\cdot\delta=\delta\cdot\epsilon$. This implies $\beta\cdot\gamma=\gamma\cdot\beta$.

Corollary 25 has an interesting consequence. Let the binary relation E be defined on the set X of finite types different from 0 and 1 as follows:

$$E(\alpha, \beta) \text{ if and only if } \alpha\cdot\beta = \beta\cdot\alpha.$$

Then, it is clearly seen that E is a reflexive and symmetric relation. By Corollary 25, E is also a transitive relation. Therefore E is an equivalence relation on the set X of finite types different from 0 and 1. The following are clearly among the equivalence classes of X/E:

$$X_1 = \mathrm{CT}\cap X.$$
$$X_2 = \mathrm{ST}\cap X.$$
$$X_3 = \mathrm{OT}\cap X.$$

Let us now consider the set Y of all indecomposable finite types which are not in CT$\cup$ST$\cup$OT, i.e., $Y=[(\mathrm{X}-\mathrm{CT}\cup\mathrm{ST}\cup\mathrm{OT})\cap\mathrm{IT}]$. By Corollary 23, it follows that no two distinct elements of Y can be in the same equivalence class. In fact, for $\alpha\in Y$,

$$\alpha/E = \{\alpha^n;\ n \text{ a positive integer}\},$$

and if $\alpha, \beta\in Y$, $\alpha\neq\beta$, then $\alpha/E\cap\beta/E=0$. It turns out that, in general, all the E equivalence classes of the set $Z=X-(\mathrm{CT}\cup\mathrm{ST}\cup\mathrm{OT})$ can be described as follows. Let W denote the set of finite types β different from 0 and 1, and such that β admits no nontrivial roots; i.e.,

$$W = \{\beta;\ \beta \text{ finite}, \beta\neq 0, \beta\neq 1, \text{ for no } \gamma \text{ and } n>1 \text{ does } \beta=\gamma^n\}.$$

We assert that for each $\alpha\in Z$, $\alpha/E=\{\beta^n;\ n \text{ a positive integer}\}$ for some $\beta\in W$. The proof is easy.

Our next lemma is a generalization of Euclid's Theorem to exponentiation of finite types.

LEMMA 26. *Let α and β be finite types different from* 0 *and* 1, *and let p, q be positive integers such that $(p, q)=1$. Assume that $\alpha^p=\beta^q$. Then there exists a type γ such that*

$$\alpha = \gamma^q \quad \textit{and} \quad \beta = \gamma^p.$$

Proof. From the hypothesis and Corollaries 23 and 24, it follows that either

(1) $$\alpha, \beta \in \mathrm{CT}\cup\mathrm{ST}\cup\mathrm{OT}, \text{ or}$$

(2) there exist δ, m, n, such that $\alpha = \delta^m$ and $\beta = \delta^n$.

In case (1), the conclusion follows from the corresponding lemma on the multiplication of natural numbers. In case (2), we obtain

$$\delta^{m\cdot p} = \delta^{n\cdot q}$$

and, since δ is finite, $m\cdot p = n\cdot q$. Since $(p, q) = 1$, there exists an r such that $m = r\cdot q$ and $n = r\cdot p$. Letting $\gamma = \delta^r$, we see immediately that $\alpha = \gamma^q$ and $\beta = \gamma^p$.

Before we embark on our discussion of the factorization problem, we need one more crucial lemma.

LEMMA 27. *Let ϵ be a finite type and let p, q be positive integers such that $p \geqq 2$ and $(p, q) = 1$. Then the following hold:*

(i) *If $1 \notin \mathrm{CIT}(\epsilon)$, then $q^c +^c p^c\cdot\epsilon \in \mathrm{IT}$ if and only if $q^c +^c \epsilon\cdot p^c \in \mathrm{IT}$.*

(ii) *If $1 \notin \mathrm{SIT}(\epsilon)$, then $q^s +^s p^s\cdot\epsilon \in \mathrm{IT}$ if and only if $q^s +^s \epsilon\cdot p^s \in \mathrm{IT}$.*

Proof. To prove (i), we first assume that $q^c +^c p^c\cdot\epsilon \in \mathrm{IT}$. If $\epsilon = 0$, then clearly q is a prime. Therefore, assume $\epsilon \neq 0$. Suppose that

(1) for some α and β, $q^c +^c \epsilon\cdot p^c = \alpha\cdot\beta$.

Multiplying the equation in (1) by p^c on the left and rearranging we have

(2) $$(q^c +^c p^c\cdot\epsilon)\cdot p^c = p^c\cdot\alpha\cdot\beta.$$

Since all types are finite, we have either

(3) $$p^c\cdot\alpha \not< (q^c +^c p^c\cdot\epsilon)$$

or else

(4) $$(q^c +^c p^c\cdot\epsilon) \not< p^c\cdot\alpha.$$

We assume (3) first. Applying Lemma 14 (i) to (2), we obtain the following two cases:

(5) For some ϵ', $p^c\cdot\alpha = (q^c +^c p^c\cdot\epsilon)\cdot\epsilon'$ and $\epsilon'\cdot\beta = p^c$.

(6) For some appropriate α' and $m \geqq 2$, $(q^c +^c p^c\cdot\epsilon) = \alpha'\cdot m^c$.

Condition (5) gives $\epsilon' \in \mathrm{CT}$ and $p^c\cdot\alpha = (q^c\cdot\epsilon' +^c p^c\cdot\epsilon\cdot\epsilon')$. Since $1 \notin \mathrm{CIT}(p^c\cdot\epsilon\cdot\epsilon')$, by Lemma 5 p^c is a left divisor of $q^c\cdot\epsilon'$. Since $(p, q) = 1$, p^c is a divisor of ϵ'. On the other hand, (5) also implies that ϵ' is a divisor of p^c. Therefore $p^c = \epsilon'$ and $\beta = 1$. Condition (6) leads to the contradiction that $q^c +^c p^c\cdot\epsilon = m^c$. Let us now consider (4). Since $(p, q) = 1$, $p^c\cdot\alpha$ cannot be a left divisor of $(q^c +^c p^c\cdot\epsilon)$. Thus only one case remains and that is for some appropriate α', ϵ', γ', m and n,

$$\begin{aligned}(q^c +^c p^c\cdot\epsilon) &= \alpha'\cdot(m^c +^c n^c\cdot\epsilon'),\\ p^c\cdot\alpha &= \alpha'\cdot p'^c,\\ p^c &= p'^c\cdot\gamma'.\end{aligned}$$

Since $\kappa(m^c +^c n^c \cdot \epsilon') \geqq 2, \alpha' = 1$. Thus $p \mid p'$ and $p' \mid p$. Therefore $p = p'$ and $\alpha = 1$.

We see that the assumption (1) leads to $\alpha = 1$ or $\beta = 1$. Hence $q^c +^c \epsilon \cdot p^c \in$ IT. The proofs of the other direction of (i) as well as the equivalence of (ii) are entirely analogous to the proof already given.

Let us begin the discussion of the factorization problem by first giving an example of a finite type α which does not have the WUF property. Let $\alpha = (1 +^c 2^c \cdot 2^0) \cdot 2^c$. We readily see that

$$\alpha = (1 +^c 2^c \cdot 2^0) \cdot 2^c = 2^c \cdot (1 +^c 2^0 \cdot 2^c).$$

Since 2 is a prime and $\kappa(1 +^c 2^c \cdot 2^0) = \kappa(1 +^c 2^0 \cdot 2^c) = 5$, each type occurring in the factorization of α is indecomposable. It is also clear that $1 +^c 2^c \cdot 2^0 \neq 1 +^c 2^0 \cdot 2^c$. Thus, α does not have the WUF property. In an entirely similar manner, we see that $\beta = (1 +^s 2^s \cdot 2^0) \cdot 2^s = 2^s \cdot (1 +^s 2^0 \cdot 2^s)$ is another example of a finite type which does not have the WUF property. It turns out that essentially these two examples illustrate the general situation concerning finite types which do not possess the WUF property. Examples of types which have the WUF property but not the SUF property are, for instance, n^c, n^s and n^0 where n is not a prime. Again, essentially, these examples illustrate the general situation of finite types which have the WUF property but not the SUF property.

It is interesting to notice here that of the two finite examples we gave in the preceding paragraph, one is a partially ordering type and the other is a connected type. Referring the reader to the survey presented in [2], it is known that there are also finite p.o.r. which do not satisfy the unique decomposition theorem for cardinal multiplication. It is not known, however, whether there are finite connected relations not satisfying the unique decomposition theorem for cardinal multiplication.

As these examples illustrate, the types of the form $q^c +^c p^c \cdot \epsilon$ and $q^s +^s p^s \cdot \epsilon$ together with their associated types of the form $q^c +^c \epsilon \cdot p^c$ and $q^s +^s \epsilon \cdot p^s$ will play an important role in our subsequent discussion. For this purpose, we introduce some special notation to single out types of the above form. For each positive integer p, we let

$$\mathfrak{L}^c p = \{q^c +^c p^c \cdot \epsilon;\ q \text{ an integer, } \epsilon \text{ finite, } \epsilon \neq 0 \text{ and } 1 \notin \mathrm{CIT}(\epsilon)\}.$$

$$\mathfrak{L}^s p = \{q^s +^s p^s \cdot \epsilon;\ q \text{ an integer, } \epsilon \text{ finite, } \epsilon \neq 0 \text{ and } 1 \notin \mathrm{SIT}(\epsilon)\}.$$

In a similar manner, we let the associated types be singled out by:

$$\mathfrak{R}^c p = \{q^c +^c \epsilon \cdot p^c;\ q \text{ an integer, } \epsilon \text{ finite, } \epsilon \neq 0 \text{ and } 1 \notin \mathrm{CIT}(\epsilon)\}.$$

$$\mathfrak{R}^s p = \{q^s +^s \epsilon \cdot p^s;\ q \text{ an integer, } \epsilon \text{ finite, } \epsilon \neq 0 \text{ and } 1 \notin \mathrm{SIT}(\epsilon)\}.$$

Some very simple properties of these sets of finite types can be given. For instance, by the unique decomposition of a type into cardinal or square sums of types of CIT or SIT, we see that if a type α belongs to, say, $\mathfrak{L}^c p$, then the

q and the ϵ are uniquely determined. That is to say if $\alpha = q^c + {}^c p^c \cdot \epsilon$ and $\alpha = r^c + {}^c p^c \cdot \epsilon'$, then $q = r$ and $\epsilon = \epsilon'$. A type α may belong to more than one set of the form $\mathfrak{L}^c p$. However, from Lemma 4 (i), we see that $\alpha \in \mathfrak{L}^c p \cap \mathfrak{L}^c q$ if and only if $\alpha \in \mathfrak{L}^c r$, where r is the l.c.m. of p and q. A similar remark can be made with respect to the sets $\mathfrak{R}^c p$ and $\mathfrak{R}^c q$ (here we should cite [3, Lemma 5]). Of course, as in many previous results, these remarks apply equally well to sets with the superscript small s.

For p, q both greater than or equal to two, there exists no type α which belongs to $\mathfrak{L}^c p$ and $\mathfrak{L}^s q$. This can be seen as follows: Suppose $\alpha = m^c + {}^c p^c \cdot \epsilon$ and $\alpha = n^s + {}^s q^s \cdot \epsilon'$ where $1 \notin \mathrm{CIT}(\epsilon)$ and $1 \notin \mathrm{SIT}(\epsilon')$. If both $m \neq 0$ and $n \neq 0$, then $\alpha \notin \mathrm{CIT}$ and $\alpha \notin \mathrm{SIT}$, which is impossible by Lemma 1. Therefore, assume either $m = 0$ or $n = 0$. Suppose $m = 0$. Then $p^c \cdot \epsilon = n^s + {}^s q^s \cdot \epsilon'$. If $n \neq 0$, then $1 \in \mathrm{SIT}(\alpha)$ but clearly $1 \notin \mathrm{SIT}(p^c \cdot \epsilon)$. Hence, both m and n are 0. Thus, $p^c \cdot \epsilon = q^s \cdot \epsilon'$. Suppose that $p \leqq q$, then by Lemma 17, $p^c \in \mathrm{ST}$ which is impossible. So we have shown that if $p, q \leqq 2$, $\mathfrak{L}^c p \cap \mathfrak{L}^s q = 0$. Similarly, $\mathfrak{R}^c p \cap \mathfrak{R}^s q = 0$. In general, $\mathfrak{L}^c p \cap \mathfrak{R}^c q \neq 0$, $\mathfrak{L}^c p \cap \mathfrak{R}^s q \neq 0$, $\mathfrak{L}^s p \cap \mathfrak{R}^s q \neq 0$, and $\mathfrak{L}^s p \cap \mathfrak{R}^c q \neq 0$.

Finally, we note that under the condition $(p, q) = 1$, $\alpha \in \mathfrak{L}^c p \cap \mathfrak{R}^c q$ if and only if for some r and type $\epsilon \neq 0$, $1 \notin \mathrm{CIT}(\epsilon)$, $\alpha = r^c + {}^c p^c \cdot \epsilon \cdot q^c$. In one direction this is trivial, so let us assume $\alpha = r^c + {}^c p^c \cdot \epsilon_1$, where $1 \notin \mathrm{CIT}(\epsilon_1)$ and $\alpha = r^c + {}^c \epsilon_2 \cdot q^c$ where $1 \notin \mathrm{CIT}(\epsilon_2)$. It now follows that $p^c \cdot \epsilon_1 = \epsilon_2 \cdot q^c$. If either $p = 1$ or $q = 1$, then clearly the conclusion holds. So let us assume $p, q \geqq 2$. By Lemma 17, $\kappa(\epsilon_1) > q$ and $\kappa(\epsilon_2) > p$. Applying Lemma 14 (i), we have either

$$\epsilon_2 = p^c \cdot \epsilon \quad \text{and} \quad \epsilon_1 = \epsilon \cdot q^c \text{ for some } \epsilon,$$

or

$$\epsilon_2 = \alpha' \cdot (m^c + {}^c n^c \cdot \epsilon), \quad p^c = \alpha' \cdot n^c,$$
$$\epsilon_1 = (m^c + {}^c \epsilon \cdot n^c) \cdot \gamma', \quad q^c = n^c \cdot \gamma', \quad \text{for some appropriate } \alpha', \gamma', \epsilon, m, n.$$

The first possibility of course leads to the desired conclusion. In the second possibility, we note that since $(p, q) = 1$, $n = 1$, $p^c = \alpha'$, $q^c = \gamma'$. Thus, $\epsilon_2 = p^c \cdot (m^c + {}^c \epsilon)$ and $\epsilon_1 = (m^c + {}^c \epsilon) \cdot q^c$. Since $1 \notin \mathrm{CIT}(\epsilon_1)$ and $1 \notin \mathrm{CIT}(\epsilon_2)$, we must have $m = 0$, which again leads to $\alpha = r^c + {}^c p^c \cdot \epsilon \cdot q^c$. By exactly the same type of argument we may establish a similar remark for $\mathfrak{L}^s p \cap \mathfrak{R}^s q$. As for the sets $\mathfrak{L}^c p \cap \mathfrak{R}^s q$ and $\mathfrak{L}^s p \cap \mathfrak{R}^c q$, we simply state that if $(p, q) = 1$, then $\alpha \in \mathfrak{L}^c p \cap \mathfrak{R}^s q$ if and only if $\alpha = p^c \cdot \epsilon \cdot q^s$ for some $\epsilon \neq 0$ such that $1 \notin \mathrm{CIT}(\epsilon)$ and $1 \notin \mathrm{SIT}(\epsilon)$. A similar remark holds for $\mathfrak{L}^s p \cap \mathfrak{R}^c q$.

In order to be specific when we pass from a type $q^c + {}^c p^c \cdot \epsilon$ to the type $q^c + {}^c \epsilon \cdot p^c$, we introduce, for each positive integer p, the following functions:

For $\alpha \in \mathfrak{L}^c p$,

$F^c p(\alpha) = q^c + {}^c \epsilon \cdot p^c$ when q^c and ϵ are the unique integer and type such that $\alpha = q^c + {}^c p^c \cdot \epsilon$.

For $\alpha \in \mathfrak{L}^s p$,

$F^s p(\alpha) = q^s +^s \epsilon \cdot p^s$ where q^s and ϵ are the unique integer and type such that $\alpha = q^s +^s p^s \cdot \epsilon$.

We see without difficulty that the domain of $F^c p$ is $\mathfrak{L}^c p$, the domain of $F^s p$ is $\mathfrak{L}^s p$, the range of $F^c p$ is $\mathfrak{R}^c p$, and the range of $F^s p$ is $\mathfrak{R}^s p$. We can also show that $F^c p$ and $F^s p$ are one-to-one functions.

Let $\mathfrak{F}$ be the set of all finite sequences of finite types different from 0 and 1. For our purposes, we represent a finite sequence of types α_i and of length n as follows:

$$\langle \alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1} \rangle.$$

In order to discuss the *canonical factorization* of a finite type, we introduce a function $\mathfrak{CF}$ whose domain is $\mathfrak{F}$ and whose range is included in $\mathfrak{F}$. The intuitive meaning of $\mathfrak{CF}$ is as follows. Suppose we are given an element of $\mathfrak{F}$, say

$$\langle \alpha_0, \alpha_1, \cdots, \alpha_{n-1} \rangle.$$

We shall first move (in a definite manner) each factor α_i belonging to CT$\cup$ST$\cup$OT as far to the left as possible. Next, we shall permute any group of adjacent factors which all belong to CT or ST or OT in their natural increasing order from left to right. Of course, by the examples we have already mentioned, the resulting sequence $\langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$ may not have exactly the same elements as the sequence $\langle \alpha_0, \alpha_1, \cdots, \alpha_{n-1} \rangle$; however, we shall do this without changing the product $\prod_{i \in n} \alpha_i$. That is, at the end of the process $\prod_{i \in n} \alpha_i = \prod_{i \in n} \beta_i$.

We define the function $\mathfrak{CF}$ by induction on the length n of a sequence. It turns out that $\mathfrak{CF}$ will map sequences of length n into sequences of the same length.

If $\alpha = \langle \alpha_0 \rangle$ is a one-termed sequence, we let $\mathfrak{CF}(\alpha) = \alpha$. Assume that $\mathfrak{CF}(\alpha)$ is defined for each $\alpha \in \mathfrak{F}$ of length n. Let $\alpha = \langle \alpha_0, \alpha_1, \cdots, \alpha_n \rangle$, and let $\mathfrak{CF}(\langle \alpha_0, \alpha_1, \cdots, \alpha_{n-1} \rangle) = \langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$. We divide the definition of $\mathfrak{CF}(\alpha)$ into four parts.

CASE 1. $\alpha_n \notin$ CT$\cup$ST$\cup$OT. In this case,

$$\mathfrak{CF}(\alpha) = \langle \beta_0, \beta_1, \cdots, \beta_{n-1}, \alpha_n \rangle.$$

CASE 2. $\alpha_n \in$ CT. Let $\alpha_n = p^e$ where $p \geqq 2$. Let h be the least integer m satisfying the following three conditions:

(2i) $$m \leqq n - 1.$$

(2ii) $$\text{If } m < n - 1, \quad \text{then} \quad \beta_{m+1} \in \mathfrak{L}^c p.$$

(2iii) For each r such that $m + 1 < r \leqq n - 1$, either $\beta_r \in$ CT or $\beta_r \in \mathfrak{L}^c p$.

Let k be the least integer m satisfying:

(2iv) $$m \leqq h.$$

(2v) For each r such that $m < r \leqq h$, $\beta_r = (p_r)^c$ for some $p_r > p$.

We let $\mathfrak{CF}(\alpha) = \langle \gamma_0, \gamma_1, \cdots, \gamma_n \rangle$ where

$$\gamma_r = \beta_r \quad \text{for } 0 \leqq r \leqq k,$$

$$\gamma_{k+1} = p^c,$$

$$\gamma_{r+1} = \begin{cases} \beta_r & \text{if } k < r \leqq n-1 \text{ and } \beta_r \in \mathrm{CT}, \\ F^c p(\beta_r) & \text{if } k < r \leqq n-1 \text{ and } \beta_r \in \mathfrak{L}^c p. \end{cases}$$

CASE 3. $\alpha_n \in \mathrm{ST}$. Let $\alpha_n = p^s$ where $p \geqq 2$. Let h be the least integer m satisfying the following three conditions:

(3i) $$m \leqq n-1.$$

(3ii) $$\text{If } m < n-1, \quad \text{then} \quad \beta_{m+1} \in \mathfrak{L}^s p.$$

(3iii) For each r such that $m+1 < r \leqq n-1$, either $\beta_r \in \mathrm{ST}$ or $\beta_r \in \mathfrak{L}^s p$.

Let k be the least integer m satisfying:

(3iv) $$m \leqq h.$$

(3v) for each r such that $m < r \leqq h$, $\beta_r = (p_r)^s$ for some $p_r > p$.

We let $\mathfrak{CF}(\alpha) = \langle \gamma_0, \gamma_1, \cdots, \gamma_n \rangle$ where

$$\gamma_r = \beta_r \quad \text{for } 0 \leqq r \leqq k,$$

$$\gamma_{k+1} = p^s,$$

$$\gamma_{r+1} = \begin{cases} \beta_r & \text{if } k < r \leqq n-1 \text{ and } \beta_r \in \mathrm{ST}, \\ F^s p(\beta_r) & \text{if } k \leqq n-1 \text{ and } \beta_r \in \mathfrak{L}Sp. \end{cases}$$

CASE 4. $\alpha_n \in \mathrm{OT}$. Let $\alpha_n = p^0$ when $p \geqq 2$. Let k be the least integer m satisfying:

(4i) $$m \leqq n-1.$$

(4ii) For each r such that $m < r \leqq n-1$, $\beta_r = (p_r)^0$ for some $p_r > p$.

We let $\mathfrak{CF}(\alpha) = \langle \gamma_0, \gamma_1, \cdots, \gamma_n \rangle$ where

$$\gamma_r = \beta_r \quad \text{for } 0 \leqq r \leqq k,$$

$$\gamma_{k+1} = p^0,$$

$$\gamma_{r+1} = \beta_r \quad \text{for } k < r \leqq n-1.$$

Perhaps at this point it is best to give an illustration of how the $\mathfrak{CF}$ function operates. Suppose we are given the sequence,

$$\langle 2^c, 1 +^c 12^c \cdot 2^s, 4^c, 3^c, 2^s, 6^c, 7^0, 2^0, 5^s +^s 6^s \cdot 2^0, 3^s, 3^s, 2^s \rangle.$$

Let us write down successively the values of $\mathfrak{CF}$ of the initial segments. In some cases where the outcome is evident, we shall skip several steps at once.

$\langle 2^c \rangle$,

$\langle 2^c, 1 +^c 12^c \cdot 2^s \rangle$,

$\langle 2^c, 4^c, 1 +^c 3^c \cdot 2^s \cdot 4^c \rangle$,

$\langle 2^c, 3^c, 4^c, 1 +^c 2^s \cdot 12^c \rangle$,

$\langle 2^c, 3^c, 4^c, 1 +^c 2^s \cdot 12^c, 2^s, 6^c, 2^0, 7^0, 5^s +^s 6^s \cdot 2^0 \rangle$,

$\langle 2^c, 3^c, 4^c, 1 +^c 2^s \cdot 12^c, 2^s, 6^c, 2^0, 7^0, 3^s, 5^s +^s 2^s \cdot 2^0 \cdot 3^s, 3^s \rangle$,

$\langle \cdots, 7^0, 2^s, 3^s, (5^s +^s 2^0 \cdot 6^s), 3^s \rangle$.

The last line is the result. Notice that $1 +^c 2^s \cdot 12^c$ and 2^s cannot be interchanged because $1 +^c 2^s \cdot 12^c$ cannot be written in the form $q^s +^s 2^s \cdot \epsilon$. Also 3^s cannot be interchanged with either $5^s +^s 2^s \cdot 2^0$ or $5^s +^s 2^0 \cdot 2^s$, because neither of these types can be written in the form $(q^s +^s 3^s \cdot \epsilon)$.

The example may give the erroneous impression that every type can be written in one of the above forms. This is not the case of course. In addition, we should also point out that some factors may repeat and they may stand adjacent to each other.

Some simple properties of the function $\mathfrak{CF}$ are stated in the next lemma.

LEMMA 28. *Let* $\mathfrak{CF}(\langle \alpha_0, \alpha_1, \cdots, \alpha_{n-1} \rangle) = \langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$. *The following hold*:

(i) *For each* $i \in n$, *either* $\beta_i = \alpha_j$ *for some* $j \in n$, *or* $\beta_i = F^c k(\alpha_j)$ *for some* k *and* $j \in n$, *or* $\beta_i = F^s k(\alpha_j)$ *for some* k *and* $j \in n$.

(ii) *For each* $i \in n$, $\mathfrak{CF}(\langle \beta_0, \beta_1, \cdots, \beta_i \rangle) = \langle \beta_0, \beta_1, \cdots, \beta_i \rangle$.

(iii) $\prod_{i \in n} \alpha_i = \prod_{i \in n} \beta_i$.

(iv) *If* $\alpha_i \in \mathrm{IT}$ *for each* $i \in n$, *then* $\beta_i \in \mathrm{IT}$ *for each* $i \in n$.

Proof. Conditions (i), (ii) and (iii) are proved by induction on n. We shall not present their proofs. We only point out that the given precise definition of $\mathfrak{CF}$ is sufficient for the proof of each case. While admittedly the details are sometimes long and messy, we do not see any difficulties. Condition (iv) is proved by Lemma 27 and (i).

A *factorization* of a finite type β different from 0 and 1 is a sequence $\langle \alpha_0, \cdots, \alpha_{n-1} \rangle$ of types $\alpha_i \in \mathrm{IT}$ such that $\beta = \prod_{i \in n} \alpha_i$. A *canonical factorization* of a finite type β different from 0 and 1 is a sequence $\langle \alpha_0, \cdots, \alpha_{n-1} \rangle$ of types $\alpha_i \in \mathrm{IT}$ such that $\beta = \prod_{i \in n} \alpha_i$ and $\langle \alpha_0, \cdots, \alpha_{n-1} \rangle$ is in the range of the function $\mathfrak{CF}$. It is evident that every finite type β different from 0 and 1 has at least one factorization; furthermore, by applying $\mathfrak{CF}$ to this factoriza-

tion of β, we obtain at least one canonical factorization of β of the same length. We prove in the next theorem that the CF is unique.

THEOREM 29. *Every finite type different from* 0 *and* 1 *has a unique canonical factorization.*

Proof. It is clear that corresponding to each finite type β there exists a finite upper bound to the lengths of the factorizations of β. We establish the theorem by proving the following statement by induction on n.

(1) For each finite type β different from 0 and 1, if n is the largest number m such that β has a factorization of length m, then β has a unique canonical factorization.

The case $n=1$ is trivial. Assume that (1) holds for some $n \geqq 1$. Let

(2) $\langle \beta_0, \beta_1, \cdots, \beta_n \rangle$ be a canonical factorization of β, such that n is at the maximum.

Let

(3) $\langle \alpha_0, \alpha_1, \cdots, \alpha_m \rangle$ be any canonical factorization of β.

Notice that $m \leqq n$. Let $\gamma = \prod_{i \in n} \beta_i$ and $\delta = \prod_{i \in m} \alpha_i$ so that

$$\delta \cdot \alpha_m = \gamma \cdot \beta_n. \tag{4}$$

Since the maximum of the lengths of factorizations of γ and δ must both be less or equal to n, by the inductive hypothesis,

(5) $\langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$ is the unique CF of γ,

and

(6) $\langle \alpha_0, \alpha_1, \cdots, \alpha_{m-1} \rangle$ is the unique CF of δ.

We shall now prove

$$\kappa(\gamma) = \kappa(\delta). \tag{7}$$

Assume that

$$\kappa(\gamma) < \kappa(\delta), \tag{8}$$

and we shall derive a contradiction.

Applying Theorem 13 to (4), we obtain four cases. We shall treat them in turn.

CASE 1. There exists an $\epsilon \neq 0$ such that $\delta = \gamma \cdot \epsilon$ and $\epsilon \cdot \alpha_m = \beta_n$. Since $\kappa(\gamma) < \kappa(\delta)$, we have $\kappa(\epsilon) > 1$. This implies that $\beta_n \notin \mathrm{IT}$ which is a contradiction.

CASE 2. There exist positive integers p, q with $p \geqq 2$ and $(p, q) = 1$, and types $\alpha' \neq 0$, $\gamma' \neq 0$ and ϵ such that $1 \notin \mathrm{CIT}(\epsilon)$, $\kappa(q^c +^c p^c \cdot \epsilon) > p$, and

$$\begin{aligned} \delta &= \alpha' \cdot (q^c +^c p^c \cdot \epsilon), \\ \gamma &= \alpha' \cdot p^c, \\ \beta_n &= (q^c +^c \epsilon \cdot p^c) \cdot \gamma', \\ \alpha_m &= p^c \cdot \gamma'. \end{aligned}$$

Since $p \geqq 2$, we see immediately that $\gamma' = 1$. We now distinguish two subcases.

CASE 2a. $\epsilon = 0$. In this case, $\alpha_m = p^c$, $\beta_n = q^c$, $q > p$, and $(p, q) = 1$. Clearly the maximum length of factorizations of α' is at most n. Hence, by the inductive hypothesis, let

(9) $\langle \gamma_0, \gamma_1, \cdots, \gamma_r \rangle$ be the unique CF of α'.

Since $\delta = \alpha' \cdot q^c$ and $\gamma = \alpha' \cdot p^c$, we see that the CF of δ and γ given in (6) and (5) are obtained from the CF of α' given in (9) by adding q^c and p^c, respectively, at the extreme right and manipulate according to the rules of the function $\mathfrak{CF}$.

Let us begin with the sequence

$$\langle \gamma_0, \gamma_1, \cdots, \gamma_r, q^c \rangle$$

and turn it into the sequence

$$\langle \alpha_0, \alpha_1, \cdots, \alpha_{m-1} \rangle$$

by the given rules. If

(10) $$\alpha_{m-1} \neq q^c,$$

then either

(11) $$\gamma_r = k^c \text{ for some } k > q,$$

or else

(12) $$\gamma_r \in \mathfrak{L}^c q.$$

Suppose (11) holds. Then, since $k > q > p$, in obtaining the sequence

$$\langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$$

from the sequence

$$\langle \gamma_0, \gamma_1, \cdots, \gamma_r, p^c \rangle,$$

we see that $\beta_{n-1} = k^c$. But this means that the sequence

$$\langle \beta_0, \beta_1, \cdots, \beta_n \rangle = \langle \beta_0, \beta_1, \cdots, k^c, q^c \rangle$$

cannot be a CF of β, contradicting (2). Suppose (12) holds. We consider the following two more subcases. Either

(13) $$\gamma_r \in \mathfrak{L}^c p,$$

or else

(14) $$\gamma_r \notin \mathfrak{L}^c p.$$

Suppose (13) holds. Then $\beta_{n-1} = F^c p(\gamma_r)$. Since $(p, q) = 1$, by our previous discussion of $\mathfrak{L}^c p \cap \mathfrak{L}^c q$, we see that (12) and (13) imply $\beta_{n-1} \in \mathfrak{L}^c q$. Thus the sequence

$$\langle \beta_0, \beta_1, \cdots, \beta_n \rangle = \langle \beta_0, \beta_1, \cdots, \beta_{n-1}, q^c \rangle$$

cannot be a CF of β, contradicting (2). Suppose (14) holds. Then, since $\gamma_r \notin \mathrm{CT}$, $\beta_{n-1} = p^c$ and $\beta_{n-2} = \gamma_r$. Again the sequence

$$\langle \beta_0, \beta_1, \cdots, \beta_n \rangle = \langle \beta_0, \cdots, \gamma_r, p^c, q^c \rangle$$

cannot be a CF of β, as by (12) q^c can be pushed to the left. This again contradicts (2). Therefore (12) cannot hold. Since neither (11) nor (12) can hold, (10) cannot hold. Hence

(15) $$\alpha_{m-1} = q^c.$$

(15) implies that the sequence

$$\langle \alpha_0, \alpha_1, \cdots, \alpha_m \rangle = \langle \alpha_0, \alpha_1, \cdots, q^c, p^c \rangle$$

is not a CF of β, contradicting (3). So, Case 2a leads to a contradiction.

CASE 2b. $\epsilon \neq 0$. Again, let (9) hold. In this case, the sequence

$$\langle \gamma_0, \gamma_1, \cdots, \gamma_r, (q^c +^c p^c \cdot \epsilon) \rangle$$

is a CF of δ. Therefore, by (6), $\alpha_{m-1} = (q^c +^c p^c \cdot \epsilon)$. But $\alpha_m = p^c$, therefore the sequence

$$\langle \alpha_0, \cdots, \alpha_m \rangle = \langle \alpha_0, \cdots, q^c +^c p^c \cdot \epsilon, p^c \rangle$$

cannot be a CF of β, contradicting (3). Case 2b also leads to a contradiction.

CASE 3. This case can be treated in an entirely analogous manner as Case 2. We only note that everywhere cardinal notions are replaced by square notions.

CASE 4. There exist positive integers p, q with $p \geqq 2$ and $(p, q) = 1$, and types $\gamma' \neq 0$ and $\epsilon \neq 0$ such that $q > p$ and

$$\begin{aligned} \delta &= \epsilon \cdot q^0, \\ \gamma &= \epsilon \cdot p^0, \\ \beta_n &= q^0 \cdot \gamma', \\ \alpha_m &= p^0 \cdot \gamma'. \end{aligned}$$

It is evident that $\gamma' = 1$. Therefore, $\beta_n = q^0$ and $\alpha_m = p^0$. By the inductive hypothesis, let

(16) $\langle \gamma_0, \gamma_1, \cdots, \gamma_r \rangle$ be the unique CF of ϵ.

In going from the sequence

$$\langle \gamma_0, \gamma_1, \cdots, \gamma_r, q^0 \rangle$$

to the CF

$$\langle \alpha_0, \cdots, \alpha_{m-1} \rangle$$

of δ, we note that if $\alpha_{m-1} \neq q^0$, then $\gamma_r = k^0$ for some $k > q$, and $\alpha_{m-1} = k^0$. This implies that the sequence

$$\langle \alpha_0, \cdots, \alpha_{m-1}, \alpha_m \rangle = \langle \alpha_0, \cdots, k^0, p^0 \rangle$$

cannot be a CF of β, contradicting (3). If $\alpha_{m-1} = q^0$, then the sequence

$$\langle \alpha_0, \alpha_1, \cdots, \alpha_{m-1}, \alpha_m \rangle = \langle \alpha_0, \cdots, q^0, p^0 \rangle$$

cannot be a CF of β, contradicting (3). Thus Case 4 leads to a contradiction.

Since each case leads to a contradiction, we see that (8) fails. In an entirely analogous manner, we can show that the inequality $\kappa(\delta) < \kappa(\gamma)$ must also fail. Thus, (7) must hold. Now, from (4) and [3, Corollary 20], we obtain

(17) $$\gamma = \delta \quad \text{and} \quad \beta_n = \alpha_m.$$

The inductive hypothesis and (17) yield the desired conclusion that the sequences in (5) and (6) must be the same, and hence, $n = m$ and $\alpha_i = \beta_i$ for each $i \in n$. The theorem is proved.

A simple consequence of Theorem 29 and Lemma 28 is that every factorization of a finite type β different from 0 and 1 has a constant length.

THEOREM 30. *Let β be a finite type different from 0 and 1. Then β has the strict unique factorization property if and only if there exists a factorization $\langle \beta_0, \cdots, \beta_{n-1} \rangle$ of β such that the following are satisfied:*

(i) *No two distinct (prime) cardinal, square, or order types shall stand adjacent to each other.*

(ii) *No cardinal type p^c (square type p^s) shall stand immediately to the right of a type γ where $\gamma \in \mathfrak{L}^c p (\gamma \in \mathfrak{L}^s p)$.*

(iii) *No cardinal type p^c (square type p^s) shall stand immediately to the left of a type γ where $\gamma \in \mathfrak{R}^c p (\gamma \in \mathfrak{R}^s p)$.*

Proof. Assume that β has the SUF property. Let $\langle \beta_0, \cdots, \beta_{n-1} \rangle$ be the canonical factorization of β. If $\langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$ does not satisfy either (i), (ii), or (iii), then by a very simple reshuffling of the factors, we can obtain another factorization of β different from $\langle \beta_0, \beta_1, \cdots, \beta_{n-1} \rangle$.

On the other hand, assume that a factorization $\langle \beta_0, \cdots, \beta_{n-1} \rangle$ of β satisfies (i)–(iii). Then, since it already satisfies (i) and (ii),

$$\mathfrak{CF}(\langle\beta_0, \cdots, \beta_{n-1}\rangle) = \langle\beta_0, \cdots \beta_{n-1}\rangle.$$

Therefore, $\langle\beta_0, \cdots, \beta_{n-1}\rangle$ is the canonical factorization of β. Let $\langle\gamma_0, \cdots, \gamma_{n-1}\rangle$ be another factorization of β. Suppose that

$$\langle\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\rangle \neq \langle\beta_0, \cdots, \beta_{n-1}\rangle.$$

Since

$$\mathfrak{CF}(\langle\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\rangle) = \langle\beta_0, \cdots, \beta_{n-1}\rangle,$$

it follows that $\langle\gamma_0, \gamma_1, \cdots, \gamma_{n-1}\rangle$ violates either (i) or (ii). Since $\langle\beta_0, \cdots, \beta_{n-1}\rangle$ satisfies (i), we see that $\langle\gamma_0, \cdots, \gamma_{n-1}\rangle$ must violate (ii). Hence, by the definition of the function $\mathfrak{CF}$, $\langle\beta_0, \cdots, \beta_{n-1}\rangle$ must violate (iii). This is a contradiction. Thus β has the SUF property.

THEOREM 31. *Let β be a finite type different from* 0 *and* 1. *Then β has the weak unique factorization property if and only if every factorization $\langle\beta_0, \cdots, \beta_{n-1}\rangle$ of β satisfies* (ii) *and* (iii) *of Theorem* 30.

Proof. The proof of Theorem 31 is quite similar to the proof of Theorem 30. We shall not present the proof here.

Notice that while divisors (left or right) of types with the SUF or WUF property have the corresponding properties, the same cannot be said of their products.

REFERENCES

1. G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloquium Publications, vol. 25, rev. ed., 1948.

2. C. C. Chang, *Cardinal and ordinal multiplication of relation types*, Proceedings of Symposia in Pure Mathematics, vol. 2, American Mathematical Society, 1961, pp. 123–128.

3. C. C. Chang and Anne C. Morel, *Some cancellation theorems for ordinal products of relations*, Duke Math. J. vol. 27 (1960) 171–182.

4. A. Tarski, *Ordinal algebras*, Amsterdam, North-Holland Publishing Co., 1956.

UNIVERSITY OF CALIFORNIA,
LOS ANGELES, CALIFORNIA