Can. J. Math., Vol. XLI, No. 5, 1989, pp. 808–829

FINITE SPACES OF SIGNATURES

VICTORIA POWERS

Marshall's Spaces of Orderings are an abstract setting for the reduced theory of quadratic forms and Witt rings. A Space of Orderings consists of an abelian group of exponent 2 and a subset of the character group which satisfies certain axioms. The axioms are modeled on the case where the group is an ordered field modulo the sums of squares of the field and the subset of the character group is the set of orders on the field. There are other examples, arising from ordered semi-local rings [**4**, p. 321], ordered skew fields [**2**, p. 92], and planar ternary rings [**3**]. In [**4**], Marshall showed that a Space of Orderings in which the group is finite arises from an ordered field. In further papers Marshall used these abstract techniques to provide new, more elegant proofs of results known for ordered fields, and to prove theorems previously unknown in the field setting.

In [**1**], the reduced theory of higher level orders and Witt rings was developed, and Mulcahy's Spaces of Signatures [**7, 8, 9**] are an abstract setting for this higher level theory, just as Marshall's Spaces of Orderings are an abstract setting for the ordinary theory of reduced Witt rings. As in Marshall's theory, Spaces of Signatures are modeled on higher level ordered fields, and in addition there are examples rising from skew fields [**11**] and rings with many units [**6**]. In this paper we generalize Marshall's results on finite Spaces of Orderings by showing that a Space of Signatures in which the group is finite of 2-primary order arises from a preordered field.

I. Preliminaries. We use μ to denote the complex roots of unity. Let G be an abelian group of finite (even) exponent and let X be a nonempty subset of $G^* = \mathrm{Hom}(G, \mu)$. We give G^* the usual compact-open topology, where G and μ have the discrete topology. From [**7, 8**] we recall the definition of a Space of Signatures (SOS):

An m-dimensional form f (over (X, G)) is an m-tuple $\langle a_1, \ldots, a_m \rangle$, where each $a_i \in G$. We write $\dim f = m$. If $\sigma \in X$, then

$$\sum_{i=1}^{m} \sigma(a_i)$$

is *the value of* f at σ, denoted $\sigma(f)$. We allow the empty form $\langle\ \rangle$, with the convention that $\sigma(\langle\ \rangle) = 0$ for all $\sigma \in X$. If f and g are forms we say they are *equivalent* (over X), denoted $f \equiv g$, when $\sigma(f) = \sigma(g)$ for all $\sigma \in X$. If $f \equiv g$ and $\dim f = \dim g$ we say f and g are *isometric* (over X), denoted $f \approx g$. If $f = \langle a_1, \ldots, a_m \rangle$ and $g = \langle b_1, \ldots, b_n \rangle$, we define the sum of f and g, denoted

Received September 12, 1988.

$f \oplus g$, to be the form $\langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle$. We define the product of f and g to be the form $\langle a_i b_j \rangle$. For a nonempty form f and $a \in G$, a is *represented* by f if there is some form g such that $f \approx \langle a \rangle \oplus g$. The set of elements represented by f is denoted $D(f)$.

(X, G) is a Space of Signatures if the following axioms hold:

S_0: If $\sigma \in X$ then $\sigma^k \in X$ for all odd $k \in N$.

S_1: X is closed in G^*.

S_2: There exists $e \in G$ such that $\sigma(e) = -1$ for all $\sigma \in X$.

S_3: If $\sigma(x) = 1$ for all $\sigma \in X$, then $x = 1$.

S_4: If $z \in D(f \oplus g)$ where f and g are nonempty forms, then $z \in D(\langle x, y \rangle)$ for some $x \in D(f)$ and $y \in D(g)$.

S_5: If $\chi \in G^*$ and $D(\langle 1, x \rangle) \subset \ker \chi$ for all $x \in \ker \chi$, then $\chi \in X$.

We write -1 for the unique e of S_2. If (X, G) is only known to satisfy S_0, S_1, S_2, and S_3, then we say (X, G) is a *pre*-SOS. In the case where G has exponent a power of 2, S_5 follows from S_4 [**9**, 2.11], thus in this paper we can exclude S_5 since we will only look at SOS's whose group has exponent a power of 2.

The smallest SOS is denoted by C_2: G is the group of two elements and X consists of the character that sends -1 to -1. Generalizing this, we use C_s to denote the SOS where the group is cyclic of order 2^s, and X is all characters that send -1 to -1.

Given two SOS's (X_1, G_1) and (X_2, G_2), the *direct sum* of these is the SOS with

$$G = G_1 \times G_2 \text{ and } X = (X_1 \times 1) \cup (X_2 \times 1),$$

where $\cup$ denotes disjoint union. We say (X, G) is a *group extension* of (X', G') if G' imbeds in G and

$$X = \{\sigma \in G^* : \sigma|_{G'} \in X'\}.$$

For details and examples, see [**8**, §2]. A SOS is *constructable* if it is built up from C_2 by group extensions and direct sums. Constructable SOS's are realizable, i.e., they arise from preordered fields. For details, see [**10**].

We single out two special types of SOS's, *fans* and *quasifans*. Fans are SOS's where the X is as large as possible, more precisely, a SOS (X, G) is a fan if

$$X = \{\chi \in G^* | \chi(-1) = -1\}.$$

Thus, for any s, C_s is a fan. Fans are the simpliest SOS's, but are not as useful here as they are for Spaces of Orderings. A more important type of SOS is a quasifan: A trivial quasifan is C_s for some s, or $C_s \oplus C_t$ for some s, t. A SOS (X, G) is a quasifan if it is a group extension of a trivial quasifan. Quasifans are well understood, and play the role of "local objects" for SOS's. For details, see [**9**, §4].

A SOS is finite if X is finite (equivalently, if G is finite). The goal of this paper is to show that in the case where the order of G is a power of 2, finite SOS's are constructable, hence realizable. Our general approach is the same as Marshall's: we define an equivalence relation such that a finite SOS is the direct sum of its connected components, and each connected component is a group extension.

Definition 1.1. (i) If $\tau_1, \ldots, \tau_r \in G^*$, then let $S(\tau_1, \ldots, \tau_r)$ denote the subgroup of G^* generated by the τ_i's.

(ii) If $\tau_1, \ldots, \tau_r \in X$, we let $[\tau_1, \ldots, \tau_r]$ denote the subspace of (X, G) generated by the τ_i's, i.e., the group is $G/(\cap \ker \tau_i)$ and the set of signatures is $S(\tau_1, \ldots, \tau_r) \cap X$. For details, see [**9**, §2]. Note that $[\tau_1, \ldots, \tau_r]$ is again a SOS.

(iii) for g an element of a finite abelian group, $o(g)$ denotes the order of g.

We will use the following obvious facts frequently:

LEMMA 1.2. *Let G be an abelian group with order a power of* 2, *and let $g \in G$. Then for any $g \in G$ and odd $k, o(g) = o(g^k)$. Hence we have*

(i) For an odd integer m, there is some odd k such that $g^{mk} = g$.

(ii) Suppose $o(g^r) \leqq o(g^s)$. Then there is a k such that $g^r = g^{sk}$. Further, k is odd if and only if $o(g^r) = o(g^s)$.

Definition 1.3. (i) By S_2, X generates G^*, thus there exist $\sigma_1, \ldots, \sigma_n \in X$ such that $S(\sigma_1, \ldots \sigma_n) = G^*$, and no proper subset of $\{\sigma_1, \ldots, \sigma_n\}$ generates G^*. We call $\{\sigma_1, \ldots, \sigma_n\}$ a *minimal generating set* (MGS) for (X, G). Note that, by

$$S_2, \bigcap_{i=1}^{n} \ker \sigma_i = 1.$$

(ii) For a MGS $\{\sigma_1, \ldots, \sigma_n\}$, let

$$\Delta_i = \bigcap_{i \neq j} \ker \sigma_j.$$

Since $\cap \ker \sigma_i = 1, \Delta_i$ is cyclic and we fix a_i a generator of Δ_i. We call $\{a_i, \ldots, a_n\}$ a *dual set* for the MGS. Note that, unlike the case where G has exponent 2, the a_i's do not necessarily generate G.

(iii) Let S_i denote $S(\sigma_1, \ldots, \sigma_i, \ldots, \sigma_n)$. By Pontrayagin duality, $S_i^{\perp} = \Delta_i$.

LEMMA 1.4. *Fix $\{\sigma_1, \ldots, \sigma_n\}$ a* MGS *for (X, G).*

(i) *If k is an odd integer, then $\sigma_i^k \notin S_i$. Thus whenever $\Pi \sigma_i^{r_i} = 1$, each r_i is even.*

(ii) *$\sigma_i^k(a_i) = 1$ if and only if $\sigma_i^k \in S_i$. Thus $o(\sigma_i) = o(\sigma_i S_i)$ in G^*/S_i.*

(iii) *If* $\sigma_i(b) = \sigma_i(c)$ *for all* i*, then* $b = c$.

(iv) *If* $\{c_1, c_2, \ldots, c_n\}$ *are odd integers, then* $\{\sigma_1^{c_1}, \ldots, \sigma_n^{c_n}\}$ *is also a* MGS *for* (X, G).

Proof. (i) By [1.2(i)], there is an m such that $\sigma_i^{km} = \sigma_i$. Thus, if $\sigma_i^k \in S_i$, we would have $\sigma_i \in S_i$ which would contradict the minimality of the MGS.

(ii) If $\sigma_i^k(a_i) = 1$, then

$$\bigcap_{i \neq j} \ker \sigma_j \subset \ker \sigma_i^k.$$

Hence $\sigma_i^k \in S_i$.

(iii) If $\sigma_i(b) = \sigma_i(c)$ for all i, then $bc^{-1} \in \cap \ker \sigma_i = 1$.

(iv) follows from [1.2(i)] and S_i.

Proposition 1.5. *If* (X, G) *has a MGS of* n *elements, then* G *has exactly* 2^n *elements of order* 2. *In particular, the number of elements in a* MGS *for* (X, G) *is unique, called the rank of* (X, G).

Proof. Let $\{\sigma_1, \ldots, \sigma_n\}$ be a MGS for (X, G) and let $\{a_1, \ldots, a_n\}$ be a dual set. By [1.4], $\sigma_i(a_i) \neq 1$, hence there is a $c_i \in \Delta_i$ such that $\sigma_i(c_i) = -1$. We want to show that the c_i's form a basis for the socle (elements of order 2) of G, as a vector space over the field of two elements.

Suppose $b \in G$ has order 2. Then $\sigma_i(b) = \pm 1$ for all i. Define ϵ_i as follows: if $\sigma_i(b) = 1$, let $\epsilon_i = 0$ and if $\sigma_i(b) = -1$, let $\epsilon_i = 1$. Now set

$$c = \prod_{i=1}^{n} c_i^{\epsilon_i}.$$

Then, since $\sigma_i(b) = \sigma_i(c)$ for all i, by [1.4(iii)], $b = c$. Thus the c_i's span the socle of G.

Suppose $\Pi c_i^{\epsilon_i} = 1$ for some $\epsilon_i \in \{0, 1\}$. Then applying σ_i, we see that $(-1)^{\epsilon_i} = 1$ for all i, and hence $\epsilon_i = 0$ for all i. Thus the c_i's are independent and therefore form a basis for the socle of G. This implies that G has exactly 2^n elements of order 2.

Definition 1.6. Let $\{\sigma_1, \ldots, \sigma_n\}$ be a MGS for (X, G). The set $\{c_1, \ldots, c_n\}$ defined in the proof of [1.5] is called an S*-basis* for the MGS. Note that $\sigma_j(c_i) = 1$ if $i \neq j$, and $\sigma_i(c_i) = -1$.

Definition 1.7. Suppose $\{\sigma_1, \ldots, \sigma_n\}$ is a *MGS* for (X, G). We say σ_i is *strongly independent* if $\sigma_i^k \in S_i$ whenever $\sigma_i^k \neq 1$.

Lemma 1.8. *Suppose* $\{\sigma_1, \ldots, \sigma_n\}$ *is a* MGS *and* σ_i *is strongly independent. Then*

(i) $\sigma(a_i)$ *generates the image of* σ_i.

(ii) If $\alpha \in S_i$ *and* $\alpha \neq 1$, *then* $\ker \sigma_i \not\subset \ker \alpha$.

https://doi.org/10.4153/CJM-1989-037-3 Published online by Cambridge University Press

Proof. (i) is clear by [1.4(ii)].

(ii) If $\ker\sigma_i \subset \ker\alpha$, then $\alpha = \sigma_i^k$ for some integer k, and hence $\sigma_i^k \in S_i$, a contradiction.

LEMMA 1.9. *Suppose z_1, z_2, z_3, z_4 are elements of μ.*
(i) If $z_1 + z_2 = z_3 + z_4 \neq 0$, then, as sets, $\{z_1, z_2\} = \{z_3, z_4\}$.
(ii) If $z_1 \neq 1$ and $z_2 \neq 1$, then $1 + z_1 z_2 \neq z_1 + z_2$.

Proof. (i) is [**8**, 3.13], and (ii) follows easily from (i).

Definition 1.10. (i) Following [**8**], we say $x \in G$ is *rigid* if whenever $\langle 1, x\rangle \equiv \langle b, d\rangle, \{1, x\} = \{b, d\}$.

(ii) Suppose $Y \subset X$. We say $x \in G$ is Y*-rigid* if whenever $\langle 1, x\rangle \equiv \langle b, d\rangle$, then either $\sigma(b) = 1$ and $\sigma(d) = \sigma(x)$ for all $\sigma \in Y$, or $\sigma(b) = \sigma(x)$ and $\sigma(d) = 1$ for all $\sigma \in Y$.

Remarks 1.11. (i) Suppose x is Y-rigid, then x is $[Y]$-rigid.

(ii) If $x \in G$ and $\sigma \in X$ with $\sigma(x) \neq -1$, then $\sigma(\langle 1, x\rangle) \neq 0$. Hence, by $[1.9(i)], x$ is $\{\sigma\}$-rigid.

(iii) If x is $\{\sigma_1, \dots, \sigma_n\}$-rigid for some MGS $\{\sigma_1, \dots, \sigma_n\}$, then, by [1.4(iii)], x is rigid.

We make use of the following powerful theorem from [**8**], which gives a characterization of group extensions in terms of rigid elements:

THEOREM 1.12 [**8**, 5.5]. *Suppose there is some $x \in G$ such that both x and $-x$ are rigid. Then (X, G) is a group extension.*

Definition 1.13. Suppose $\{\sigma_1, \dots, \sigma_m\}$ is a subset of a fixed *MGS* for (X, G). We call a product

$$\prod_{i=1}^{m} \sigma_i^{r_i}$$

an *m-product* with respect to the given MGS. (We assume no product of a proper subset of $\{\sigma_i'^{r_i}\}$ is 1.)

The following proposition gives us a useful criterion for when a SOS is a direct sum:

PROPOSITION 1.14. *Suppose $\{\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m\}$ is a* MGS *for (X, G) such that whenever $\alpha\beta \in X$ with $\alpha \in S(\sigma_1, \dots, \sigma_n)$ and $\beta \in S(\tau_1, \dots, \tau_m)$, then either $\alpha = 1$ or $\beta = 1$. Then*

$$(X, G) = [\sigma_1, \dots, \sigma_n] \oplus [\tau_1, \dots, \tau_m].$$

Proof. Define

$$\Delta_1 = \bigcap_{i=1}^{n} \ker\sigma_i \text{ and } \Delta_2 = \bigcap_{i=1}^{m} \ker\tau_i.$$

Since, by assumption, $X = X_1 \dot\cup X_2$ where $X_1 = [\sigma_1, \dots, \sigma_n]$ and $X_2 = [\tau_1, \dots, \tau_m]$, we need only show that the canonical map

$$G \longrightarrow G/\Delta_1 \times G/\Delta_2$$

is an isomorphism. It is clear that $\Delta_1 \cap \Delta_2 = 1$ and hence the map is injective. To show the map is onto it is enough to show that

$$G^* \cong (G/\Delta_1)^* \times (G/\Delta_2)^*$$

since this would imply that $|G| = |G/\Delta||G/\sigma_2|$.

Any $\chi \in G^*$ can be written as $\chi = \sigma\tau$, where $\sigma \in S(\sigma_1, \dots, \sigma_n)$ and $\tau \in S(\tau_1, \dots, \tau_m)$. By our hypothesis, this decomposition is unique and thus we can map $\chi \longrightarrow (\sigma, \tau)$. This map is clearly an isomorphism, and we are done.

LEMMA 1.15. *Suppose* $\chi_1, \chi_2 \in G^* \setminus \{1\}$. *Then there is some* $x \in G$ *such that* $\chi_i(x) \neq 1, i = 1, 2$.

Proof. Since $\chi_i \neq 1$, there exist $x_1, x_2, \in G$ such that $\chi_i(x_i) \neq 1$. Then $x = x_1, x = x_2$ or $x = x_1x_2$ satisfies the lemma.

The following lemma has the flavor of Marshall's "Basic Lemma" [**4**, 3.1].

LEMMA 1.16. *Suppose* $\{\sigma_1, \dots, \sigma_n\}$ *is a* MGS *for* (X, G), $\{a_1, \dots, a_n\}$ *is a dual set, and* $\{c_1, \dots, c_n\}$ *is an* S*-basis. Further suppose* X *contains* $\sigma = \sigma_1\alpha\sigma_n^t$ *where* $\alpha \in S(\sigma_2, \dots, \sigma_{n-1})$ *and* t *is even, and there is some* $a \in \ker\sigma_1 \cap \dots \cap \ker\sigma_{n-1}$ *such that* $\sigma_n^t(a) \neq 1$. *Let* f *be the form* $\langle 1, c_1c_2 \dots c_{n-1}, c_2c_3 \dots c_{n-1}a\rangle$. *Then for any* $x \in G$ *such that* $\sigma_1(x) \neq 1$ *and* $\sigma_n(x) \neq 1$, f *cannot represent* x.

Proof. Let g be the form $\langle c_1c_2 \dots c_{n-1}, c_2c_3 \dots c_{n-1}a\rangle$. Suppose f represents x, then by Axiom S_4, there is $y \in G$ such that g represents y and $\langle 1, y\rangle$ represents x.

Suppose $\langle c_1, a\rangle \equiv \langle b, d\rangle$. By [1.9(i)], since $\sigma_j(\langle c_1, a\rangle) = 2$ for $j = 2, \dots, n-1$, we must have $\sigma_j(b) = \sigma_j(d) = 1$ for $j = 2, \dots, n-1$. Since t is even, $\sigma_n(a) \neq -1$, and so

$$\sigma_n(\langle c_1, a\rangle) \neq 0.$$

Thus, by [1.9(1)], wlog we can assume $\sigma_n(b) = 1$ and $\sigma_n(d) = \sigma_n(a)$. Since $\sigma_1(\langle b, d\rangle) = \sigma_1(\langle c_1, a\rangle) = 0, \sigma_1(d) = -\sigma_1(b)$. Then

$$\sigma(\langle b, d\rangle) = \sigma_1(b) - \sigma_1(b)\sigma_n^t(a),$$

while

$$\sigma(\langle c_1, a\rangle) = -1 + \sigma_n^t(a).$$

Hence $\sigma_1(b) = -1$, and so $b = c_1$ and $d = a$.

We have shown that $\langle c_1, a\rangle$ represents only c_1 and a, and therefore $g = c_2c_3 \dots c_{n-1}\langle c_1, a\rangle$ represents only $r = c_1c_2 \dots c_{n-1}$ and $s = c_2c_3 \dots c_{n-1}a$. Thus y must be r or s. But since $\sigma_n(\langle 1, r\rangle) = 2$ and $\sigma_n(x) \neq 1$, by [1.9(i)] $\langle 1, r\rangle$ cannot represent x. Similarly, since $\sigma_1(\langle 1, s\rangle) = 2, \langle 1, s\rangle$ cannot represent x. Thus y cannot be r or s, a contradiction. Hence f cannot represent x.

2. Spaces of small rank. In this section we will show that if rank $(X, G) \leqq 3$, then (X, G) is constructable. By [1.14], we know that if (X, G) is not a direct sum, then X does not "break up" into a disjoint union of smaller pieces. We will use this fact to find $x \in G$ such that $\pm x$ is rigid in the case where (X, G) is not a direct sum proving, by [1.12], that (X, G) is a group extension.

Remarks 2.1. The only SOS that is both a direct sum and a group extension is $C_2 \oplus C_2$, by [**7**.4.8(ii)]. By [**9**, 3.7], any SOS of rank 1 is a fan and hence is constructable.

LEMMA 2.2. *Suppose $\{\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m\} \subset X$, and X contains $\gamma = \alpha\beta$ where $\alpha \in S(\sigma_1, \dots, \sigma_n)$ and $\beta \in S(\tau_1, \dots, \tau_m)$. Given $x \in G$ such that x is $\{\sigma_1, \dots, \sigma_n\}$-rigid and $\{\tau_1, \dots, \tau_m\}$-rigid, $\alpha(x) \neq 1$ and $\beta(x) \neq 1$. Then x is $\{\sigma_1, \dots, \sigma_n, \tau_1, \dots, \tau_m\}$- rigid.*

Proof. Suppose $\langle 1, x\rangle \equiv \langle b, d\rangle$ for $b, d \in G$. Then, since x is $\{\sigma_1, \dots, \sigma_n\}$-rigid, interchanging b and d if necessary, we can assume $\sigma_1(b) = 1$ and $\sigma_i(d) = \sigma_i(x)$ for $i = 1, \dots, n$. Hence $\alpha(b) = 1$ and $\alpha(d) = \alpha(x)$. Since x is $\{\tau_1, \dots, \tau_m\}$-rigid, either $\tau_i(b) = 1$ for $i = 1, \dots, m$ or $\tau_i(x) = \tau_i(x)$ for $i = 1, \dots, m$. If the latter case occurs, then we have

$$\gamma(\langle b, d\rangle) = \alpha(x) + \beta(x),$$

while

$$\gamma(\langle 1, x\rangle) = 1 + \alpha(x)\beta(x) \neq \alpha(x) + \beta(x)$$

by [1.9(ii)], a contradiction. Hence we must have $\tau_i(b) = 1$ for $i = 1, \dots, m$ and thus $b = 1$. Therefore, x is rigid.

COROLLARY 2.3 *Suppose $\{\sigma_1, \sigma_2\} \subset X$, and there is an even integer s such that $\sigma_1^s \neq 1$ and $\sigma_1^s\sigma_2 \in X$. If $x \in G$ such that $\sigma_1^s(x) \neq 1$, then $\pm x$ are $\{\sigma_1, \sigma_2\}$-rigid.*

Proof. Since s is even, $\sigma_1(x) \neq \pm 1$, hence by [1.11(ii)], $\pm x$ are $\{\sigma_1\}$-rigid. If $\sigma_2(x) \neq 1, x$ is $\{\sigma_1, \sigma_2\}$-rigid by [2.2]. If $\sigma_2(x) = 1$, then by [1.9(i)], $\sigma_2(b) = \sigma_2(d) = 1$ whenever $\langle 1, x\rangle \equiv \langle b, d\rangle$ and hence x is $\{\sigma_1, \sigma_2\}$-rigid. A similar proof works for $-x$.

We begin with the classification of small SOS's by showing that a rank 2 SOS is a group extension or a direct sum.

THEOREM 2.4. *Let (X,G) be a* SOS *of rank* 2 *and let $\{\sigma_1,\sigma_2\}$ be a* MGS. *Suppose $(X,G) \neq C_2 \oplus C_2$. Then (X,G) is a group extension if and only if X contains a* 2*-product. (See* [1.13] *for the definition of m-products.) Furthermore, any* SOS *of rank* 2 *is a direct sum or a group extension.*

Proof. If X doesn't contain a 2-product, then by [1.14] (X,G) is a direct sum and since $(X,G) \neq C_2 \oplus C_2$, by the remark above (X,G) cannot be a group extension. Thus if (X,G) is a group extension, X must contain a 2-product.

Since X contains a 2-product, renumbering if necessary and taking an odd power of the 2-product, we can assume $\sigma_1^s\sigma_2 \in X$ for some even s. Then, by [2.3], there is an $x \in G$ such that $\pm x$ are rigid, and so (X,G) is a group extension by [1.12].

The classification of rank 3 SOS's is much more complicated than the rank 2 case. We will break it up into several different cases. For the rest of this section we fix a rank 3 SOS, a MGS $\{\sigma_1,\sigma_2,\sigma_3\}$, a dual set $\{a_1,a_2,a_3\}$, and an S-basis $\{c_1,c_2,c_3\}$.

PROPOSITION 2.5. *Suppose $[\sigma_1,\sigma_2]$ is a group extension and X contains a* 3*-product. Then (X,G) is a group extension.*

Proof. As in [2.4], we can assume $\sigma_1^s\sigma_2 \in X$ for some even s with $\sigma_1^s \neq 1$. By assumption, there is a 3-product $\gamma\sigma_3^t \in X$, where $\gamma \in S(\sigma_1,\sigma_2)$ with $\gamma \neq 1$ and $\sigma_3^t \neq 1$.

Case 1. Suppose t is odd. By [1.4(iv)], we can replace σ_3 by σ_3^t and thus we can assume $\tau = \gamma\sigma_3$. By [1.15], there is some $x \in G$ such that $\gamma(x) \neq 1$ and $\sigma_1^s(x) \neq 1$. Then, by [2.3], $\pm x$ are $\{\sigma_1,\sigma_2\}$-rigid. If $\sigma_3(x) = 1$, then $\sigma_3(b) = \sigma_3(d) = 1$ whenever $\langle 1,x\rangle \equiv \langle b,d\rangle$, by [1.9(i)], and hence x is rigid. If $\sigma_3(x) \neq 1$, then x is rigid by [2.2]. A similar proof shows $-x$ is rigid.

Case 2. Suppose σ_3 is not strongly independent. Then we have $\sigma_1^u\sigma_2^v\sigma_3^w = 1$ for some integers u,v, and w with $\sigma_3^w \neq 1$. By [1.4(i)], w is even and so $\sigma_3^{1-w} = \sigma_1^u\sigma_2^v\sigma_3 \in X$. Hence we are done by Case 1.

Case 3. Suppose σ_3 is strongly independent and $\alpha\sigma_3^w \in X$ where $\alpha \in S(\sigma_1,\sigma_2), \sigma_3^w \neq 1, \alpha \neq \gamma$, and $\alpha \neq 1$. By [1.8] and [1.15], there exists $y \in \ker\sigma_3$ such that $\sigma_1^s(y) \neq 1$ and $\gamma\alpha^{-1}(y) \neq 1$. Let $x = ya_3$, then, since σ_3 is strongly independent, $\sigma_3^t(x)$ and $\sigma_3^w(x)$ are not 1. Since $\alpha(x) \neq \gamma(x)$, one of these is not 1, hence by [2.2] and [2.3], x is rigid. Since t and w are even $\alpha(-x) \neq \gamma(-x)$. Thus a similar proof shows that $-x$ is rigid.

Case 4. If cases 1, 2 and 3 don't hold, then $\tau = \sigma_1^u\sigma_2^v\sigma_3^t$ with σ_3 strongly independent and t even. Since case 1 doesn't hold, the only 3-products in X are of the form $\sigma_1^u\sigma_2^v\sigma_3^k$, where k is even. Since case 3 doesn't hold, the only 2-products in X are in $[\sigma_1,\sigma_2]$ and, since $\tau^3 \in X$, we must have $(\sigma_1^u\sigma_2^v)^3 = \sigma_1^u\sigma_2^v$ and hence $(\sigma_1^u\sigma_2^v)^2 = 1$.

Suppose u is odd and v is even. By [1.8], we can find $y \in \ker\sigma_3$ such that $\sigma_2^v(y) = -1$. Since $(\sigma_1^u\sigma_2^v)^2 = 1$, choosing $x = y$ or $x = c_1y$ we have $\sigma_1^u(x) = \sigma_2^v(x) = -1$ and $\sigma_3(x) = 1$.

Let f be the form $\langle 1, c_1c_2, c_2a_3\rangle$ and let g be the form $\langle xa_3, c_1c_2, c_2\rangle$. An easy check shows that $\sigma(f) = \sigma(g)$ for all $\sigma \in [\sigma_1, \sigma_2]$, and any 1-product. The only other elements of X are of the form $\sigma = \sigma_1^u\sigma_2^v\sigma_3^k$, and an easy check shows in this case $\sigma(f) = \sigma(g)$. Thus $f \equiv g$, but by [1.16], f cannot represent xa_3, a contradiction.

If u is even and v is odd, then there is some $y \in \ker\sigma_3$ such that $\sigma_1^u(y) = -1$, and thus, as above, we have x such that $\sigma_1^u(x) = \sigma_2^v(x) = -1$. Let $f = \langle 1, c_1c_2, c_1a_3\rangle$ and $g = \langle xa_3, c_1c_2, c_1\rangle$ and use the same argument as before to get a contradiction. Therefore this case cannot occur.

LEMMA 2.6. *Suppose that X contains $\sigma_1^r\sigma_2^s\sigma_3^t$ where r, s, and t are all odd. Then (X, G) is a quasifan.*

Proof. Since r, s, and t are odd, by [1.4(iv)] we can replace $\{\sigma_1, \sigma_2, \sigma_3\}$ by $\{\sigma_1^r, \sigma_2^s, \sigma_3^t\}$. Thus we can assume $r = s = t = 1$. For $x \in G$, let Y_x be $\{\sigma \in X : \sigma(x) \neq 1\}$. By [**8**, 3.10] and [**9**, 4.5], if $Y_x^\perp$ is cyclic for every x of order 2 in $G \setminus \{-1\}$, then (X, G) is a quasifan. From the proof of [1.5] we know that the elements of order 2 in G are of the form $\prod c_i^{\epsilon_i}$ where $\epsilon_i \in \{0, 1\}$. For $x = c_1, Y_x$ contains σ_2 and σ_3, hence c_1 is the only element of order 2 $Y_x^\perp$ contains, and thus $Y_x^\perp$ is cyclic. A similar argument works for $x = c_2$ or c_3. For $x = c_1c_2, Y_x$ contains σ_3 and $\sigma_1\sigma_2\sigma_3$, hence $Y_x^\perp$ is cyclic. A similar argument works for c_1c_3 and c_2c_3, and we are done.

In the next few lemmas we take care of the case where X contains a 3-product with two even exponents. We start with the case where the MGS is strongly independent.

LEMMA 2.7. *Suppose $\sigma = \sigma_1^r\sigma_2^s\sigma_3^t \in X$ for some integers r, s, and t, where s is even. Given $x \in G$ such that $\sigma_3(x) = 1, \sigma_1(x) \neq -1, \sigma_1^r(x) \neq 1$ and $\sigma_2^s(x) \neq 1$. Then x is rigid.*

Proof. Suppose $\langle 1, x\rangle \equiv \langle b, d\rangle$ for some $b, d \in G$. Since $\sigma_i(x) \neq -1$ for each i, by [1.11(ii)], x is $\{\sigma_i\}$-rigid for $i = 1, 2, 3$ and so if $b \in \{1, x\}$,

$$\sigma(b) \in \{\sigma_1^r(x), \sigma_2^s(x)\}.$$

Then

$$\sigma(\langle b, d\rangle) = \sigma_1^r(x) + \sigma_2^s(x),$$

but

$$\sigma(\langle 1, x\rangle) = 1 + \sigma_1^r\sigma_2^s(x) \neq \sigma_1^r(x) + \sigma_2^s(x)$$

by [1.9(ii)], a contradiction. Hence $b \in \{1, x\}$ and so x is rigid.

LEMMA 2.8. *Suppose each σ_i is strongly independent, and there are even integers $\{r, s, k, m\}$ such that $o(\sigma_1^k) > 2, o(\sigma_2^s) > 2, \sigma_1^r \neq 1, \sigma_2^m \neq 1$, and X*

contains $\sigma_1^k\sigma_2^m\sigma_3$ and $\sigma_1^r\sigma_2^s\sigma_3$. (These do not have to be distinct.) Then (X,G) is a group extension.

Proof. Let $x = a_1a_2$, then by [2.7] x is rigid. Suppose $\langle 1,-x\rangle \equiv \langle b,d\rangle$ for $b,d \in G$. Then, by [1.11(ii)], we can assume

$$\sigma_1(b) = 1, \sigma_1(d) = -\sigma_1(x) \text{ and } \{\sigma_2(b),\sigma_2(d)\} = \{1,-\sigma_2(x)\}.$$

Since $\sigma_3(\langle b,d\rangle) = \sigma_3(\langle 1,-x\rangle) = 0$, we have $\sigma_3(d) = -\sigma_3(b)$.

Suppose $\sigma_2(b) = -\sigma_2(x)$ and $\sigma_2(d) = 1$, then

$$\sigma_1^k\sigma_2^m\sigma_3(\langle b,d\rangle) = \sigma_3(b) - \sigma_3(b)\sigma_1^k(x).$$

Then, since

$$\sigma_1^k\sigma_2^m\sigma_3(\langle 1,-x\rangle) = 1 + \sigma_1^k(x) \neq 0,$$

$\sigma_3(b) = -1$ and $\sigma_3(d) = 1$. But then

$$\sigma_1^r\sigma_2^s\sigma_3(\langle b,d\rangle) \neq \sigma_1^r\sigma_2^s\sigma_3(\langle 1,-x\rangle),$$

a contradiction. Hence $\sigma_2(x) = 1$ and $\sigma_2(d) = -(x)$. Then

$$\sigma_1^k\sigma_2^m\sigma_3(\langle b,d\rangle) = \sigma_3(b) + \sigma_3(b)\sigma_1^k(x)$$

and hence $\sigma_3(b) = 1$. Thus $b = 1$ and so $-x$ is rigid. Therefore, by [1.12], (X,G) is a group extension.

LEMMA 2.9. *Suppose each σ_i is strongly independent and there are even integers $\{k,m,r,s\}$ such that X contains the 3-products $\sigma_1^k\sigma_2^m\sigma_3$ and $\sigma_1^r\sigma_2\sigma_3^s$. Then (X,G) is a group extension.*

Proof. Let $x = a_1c_2$. Suppose $\langle 1,x\rangle \equiv \langle b,d\rangle$, then by [1.9(i)], $\sigma_3(b) = \sigma_3(d) = 1$. Since $o(\sigma_1) > 2$ and σ_1 is strongly independent, by [1.8] $\sigma_1(x) \neq \pm 1$. Thus, by [1.11(ii)], we can assume $\sigma_1(b) = 1$ and $\sigma_1(d) = \sigma_1(a_1)$. Since $\sigma_2(\langle 1,x\rangle) = 0, \sigma_2(d) = -\sigma_2(b)$. Then

$$\sigma_1^r\sigma_2\sigma_3^s(\langle 1,x\rangle) = 1 - \sigma_1^r(a_1) \neq 0$$

while

$$\sigma_1^r\sigma_2\sigma_3^s(\langle b,d\rangle) = \sigma_2(b) - \sigma_2(b)\sigma_1^r(a_1).$$

Thus $\sigma_2(b) = 1$ and hence $b = 1$. Therefore x is rigid.

Note that $-x = c_1a_1c_3$, and hence a similar argument as above, using $\sigma_1^k\sigma_2^m\sigma_3$, shows that $-x$ is rigid. Therefore, by [1.12], (X,G) is a group extension.

Proposition 2.10. *Suppose each σ_i is strongly independent and X contains a 3-product. Then (X,G) is a group extension.*

Proof. Since all elements of X send -1 to -1, renumbering and taking an odd power if necessary, we can assume $\sigma_1^r\sigma_2^s\sigma_3 \in X$ where $\sigma_1^r \neq 1, \sigma_2^s \neq 1$. If r, s are odd, we are done by [2.6]. Assume one is even, then they both are even.

Let f be the form $\langle 1, c_1c_3, c_1a_2\rangle$ and let g be the form $\langle a_1a_2c_3, c_1a_1, c_1\rangle$. Then by [1.16], f cannot represent $a_1a_2c_3$ hence $f \not\cong g$, and so there is some $\tau \in X$ such that $\tau(f) \neq \tau(g)$. An easy check shows that τ is not a 1-product, and if τ is a 2-product we are done by [2.5]. Thus we can assume τ is a 3-product, say $\tau = \sigma_1^k\sigma_2^l\sigma_3^m$. If the exponent are odd, we are done by [2.6]. If $\{k, m\}$ are both even or $\{l, m\}$ are both even, we are done by [2.9].

Suppose none of the above hold, then $\{k, l\}$ are even. Since $\tau(f) \neq \tau(g)$, an easy check shows that $o(\sigma_1^k) > 2$. If $o(\sigma_2^l) > 2$ we are done by [2.8]. If $o(\sigma_1^l) = 2$, then repeat the argument with the forms $\langle 1, c_2c_3, c_2a_1\rangle$ and $\langle a_1a_2c_3, c_2a_2, c_2\rangle$, and use [2.5], [2.6], [2.7], or [2.8].

Now we look at the case where the MGS is not strongly independent.

Lemma 2.11. *Suppose there are integers r_i such that $\prod \sigma_i^{r_i} = 1$. Further, suppose there are no relations among any two of the σ_i's. Then*

(i) The order of $\sigma_i^{r_i}$ is constant over all i.

(ii) For $i \neq j$, there is an $x \in G$ such that $\sigma_i^{r_i}(x) = \sigma_j^{r_j}(x) = -1$ and $\sigma_k(x) = 1$, where $k = \{1,2,3\} \setminus \{i,j\}$.

Proof. (i) Suppose $(\sigma_i^{r_i})^m \neq 1$ and $(\sigma_j^{r_j})^m = 1$ for some m. Then

$$\left(\prod \sigma_k^{r_k}\right)^m = 1,$$

which gives us a shorter relation among the σ_i's, a contradiction.

(ii) If $\ker\sigma_k \subset \ker\sigma_i^{r_i}$, then we would have a relation among $\{\sigma_k, \sigma_i\}$, a contradiction. Hence there is an $x \in \ker\sigma_k$ such that $\sigma_i^{r_i}(x) = -1$. Since

$$\prod \sigma_i^{r_i}(x) = 1,$$

we must have $\sigma_j^{r_j}(x) = -1$.

Lemma 2.12. *Given the hypotheses and notation of* [2.11]. *Suppose $o(\sigma_j(a_j)) = r_j$ for each j. Then for each $i \neq j$, and any $\{z, q\} \subset \mathbf{C}$ with $z^{r_i} = q^{r_j} = -1$, there exists $x \in G$ such that $\sigma_i(x) = z, \sigma_j(x) = q$ and $\sigma_k(x) = 1$, where $k = \{1,2,3\} \setminus \{i,j\}$.*

Proof. Replacing σ_i's by odd powers if necessary, we can assume each r_i is a power of 2. By [1.8] and [1.15], there exists $y \in \ker\sigma_k$ such that $\sigma_i^{r_i}(y) = \sigma_j^{r_j}(y) = -1$. Then, by [1.1], there exists odd m such that $\sigma_i(y^m) = z$. Then

$$o(\sigma_j^{r_j}(y^m) = o(q),$$

and since $o(a_i) = r_i$, we have

$$\sigma_j(a_j^u y_m) = q \text{ for some } u.$$

Thus $a_j^u y^m$ satisfies the lemma.

PROPOSITION 2.13. *Suppose*

$$\prod_{i=1}^{e} \sigma_i^{r_i} = 1 \textit{ for some } r_i,$$

where each $\sigma_i^{r_i} \neq 1$. *Then* (X, G) *is a group extension.*

Proof. If X contains a 2-product, then we are done by [2. 5], so assume that X contains no 2-products. Hence, by [2. 12], $o(\sigma_i^{r_i})$ is constant over i.

Suppose $o(\sigma_i^{r_i}) > 2$. Fix z, a complex square root of -1, then by [2. 11], there exists $x \in G$ such that $\sigma_i^{r_i}(x) = z$ for $i = 1, 2$. Hence $\sigma_3^{r_3}(x) = -1$. Using an argument similar to that in the proof of [2. 8], we can show that $\pm x$ are rigid, and we are done.

Now suppose $o(\sigma_j^{r_j}) = 2$ for all j and there is no relation as in the first case, then the relation given must be the only one. Hence, by [1.4(ii)], $o(\sigma_j(a_j)) = r_j$. Fix complex numbers z_i such that $z_i^{r_i} = -1$, then by [2. 12], there exist $x_i \in G$ such that $\sigma_i(x_i) = 1$ and $\sigma_j(x_i) = z_j$ if $j \neq i$.

Let f be the form $\langle 1, c_1c_2, c_1x_1 \rangle$ and let g be the form $\langle c_2x_2, c_1x_3, c_1 \rangle$. As in [1. 16], we can easily show that f cannot represent c_2x_2 and thus there is some $\tau \in X$ such that $\tau(f) \neq \tau(g)$. An easy check shows that τ is not a 1-product and we assumed X contains no 2-products, hence τ is a 3-product. Hence

$$\tau = \prod_{i=1}^{3} \tau_i^{s_i}$$

for some s_i's, and by [1.4(i)], $\sigma_i^{s_i} \notin S_i$ for each i. Thus $\sigma_i^{s_i}(x_i) \neq 1$ for each i.

Renumbering and replacing τ by an odd power of τ if necessary, we can assume $\tau = \sigma_1^k \sigma_2^m \sigma_3$ where $\sigma_1^k(a_1) \neq 1$ and $\sigma_2^m(a_2) \neq 1$. Let x_3 be as above. If $\sigma_1^k\sigma_2^m(x_3) = 1$, let $x = a_1x_3$ and if $\sigma_1^k\sigma_2^m(x_3) \neq 1$, let $x = x_3$. Then, since $\sigma_1^{r_1}(a_1) = 1$ by [1.4(ii)], we have $\sigma_3(x) = 1, \sigma_1^{r_1}(x) = \sigma_2^{r_2}(x) = -1$ and $\sigma_1^k\sigma_2^m(x) = 1$. Also, since $\sigma_1^k \notin S_1$ and $\sigma_1^{r_1} \in S_1, o(\sigma_1^{r_1}) < o(\sigma_1^k)$ and so $\sigma_1(x) \neq \pm 1$. Similarly, $\sigma_2(x) \neq \pm 1$. Using τ and an argument similar to that in the proof of [2. 8], we can show that $\pm x$ are rigid. Therefore, (X, G) is a group extension.

Finally we have the main theorem of this section:

THEOREM 2.14. *Any* SOS *of rank* 3 *is a group extension or a direct sum. Therefore, any* SOS *of rank* $\leqq 3$ *is constructable, and hence realizable.*

Proof. Assume (X, G) is not a direct sum. Suppose X contains a 3-product, then if the MGS is strongly independent, by [2. 10], (X, G) is a group extension.

If some σ_i is not strongly independent, then we have a relation among 2 or 3 of $\{\sigma_1, \sigma_2, \sigma_3\}$. If there is a relation among 3, then by [2. 13] we are done. If there is a relation among 2, then X contains a 2-product and we are done by [2. 5].

Suppose (X, G) does not contain a 3-product. Since (X, G) is not a direct sum, by [1. 14], renumbering if necessary X must contain two 2-products $\sigma_1^r\sigma_2^s$ and $\sigma_2^t\sigma_3^u$. If t is even, then u must be odd and as in case 1 of [2. 5] we can find x such that $\pm x$ are rigid. A similar argument works if s is even. If t and s are both odd, taking odd powers we have $\tau = \sigma_1^k\sigma_2$ and $\sigma_2\sigma_3^m$ in X. Clearly $\{\sigma_1, \sigma_3, \tau\}$ is a MGS, and

$$\sigma_2\sigma_3^m = \sigma_1^{-k}\tau\sigma_3^m \in X.$$

Hence X contains a 3-product and we are done.

COROLLARY 2.15. *If rank $X = 3$ and X contains a 3-product, then X is a group extension.*

3. The connected case. We define an equivalence relation on SOS's such that the group extensions are precisely the connected SOS's. It will take most of the work of this section to show that the relation is in fact an equivalence relation.

Definition 3.1. We define $\sim$ on X as follows: If $(X, G) = C_2$ or $C_2 \oplus C_2$, then $\sigma \sim \tau$ for all $\sigma, \tau \in X$. For all other $X, \sigma \sim \tau$ if there is some $\gamma \in X$ such that $\gamma \notin \{\sigma^{-1}, \tau^{-1}\}$ and $\sigma\tau\gamma \in X$.

LEMMA 3.2 *For any $\sigma \in X$ and odd $k, \sigma \sim \sigma^k$. In particular, $\sim$ is reflexive.*

Proof. We can assume (X, G) is not C_2 or $C_2 \oplus C_2$. Then $|X| > 2$, so there is some $\tau \in X$ such that $\tau \neq \sigma$. If $\sigma^2 = 1$, then $\sigma\sigma\tau = \tau \in X$, and thus $\sigma \sim \sigma = \sigma^k$. Suppose $\sigma^2 \neq 1$, then $\sigma^{-1} \neq \sigma$. If $\sigma^k \neq \sigma^{-1}$, we have $\sigma\sigma^k\sigma = \sigma^{k+2}$ and so $\sigma \sim \sigma^k$. If $\sigma^k = \sigma^{-1}$, since $|X| > 2$, there is some $\tau \in X$ such that $\tau \notin \{\sigma, \sigma^{-1}\}$. Then $\sigma\sigma^k\tau = \tau \in X$ and we are done.

LEMMA 3.3. *Suppose rank $(X, G) \leqq 3$ and $\{\sigma_1, \ldots, \sigma_n\}$ is a MGS such that $\sigma_1 \sim \sigma_i$ for all i. Then (X, G) is a group extension.*

Proof. If X has rank 3 and contains a 3-product then we are done by [2.15], so assume not. By assumption there is some $\alpha \notin \{\sigma_1^{-1}, \sigma_2^{-1}\}$ such that $\sigma_1\sigma_2\alpha \in X$. If X has rank 2 we are done by [2.4]. Suppose X has rank 3, since X contains no 3- products we get a 2-product $\sigma_1^r\sigma_2^s \in X$. Similarly, we have $\sigma_1^u\sigma_3^v \in X$, and then by [2.14] we are done.

Definition 3.4. (cf. [**8**, 5. 1]). Let (X, G) be a SOS. The *translation group of* X is

$$\{\alpha \in G^* : \alpha X \subset X\},$$

https://doi.org/10.4153/CJM-1989-037-3 Published online by Cambridge University Press

and is denoted gr(X). For $\alpha \in G^*$, define X_α to be

$$\{\sigma \in X : \alpha^k \sigma \in X \text{ for all } k\}.$$

LEMMA 3.5. (i) $\mathrm{gr}(X) = \{\alpha \in G^* : X_\alpha = X\}$.

(ii) *If* $\alpha^2 = 1$, *then* $X_\alpha = \{\sigma \in X : \alpha\sigma \in X\}$, *and* $\sigma \in X_\alpha$ *if and only if* $\sigma^k \in X_\alpha$ *for all odd* k *if and only if* $\sigma^k \in X_\alpha$ *for some odd* k.

(iii) *If* $X_\alpha \neq \emptyset$, *then* $(X_\alpha, G/X_\alpha^\perp)$ *is a subspace.*

(iv) *If* $\alpha^2 = 1$ *and* $\{\sigma_1, \ldots, \sigma_n\} \subset X_\alpha$, *then* $[\sigma_1, \ldots, \sigma_n] \subset X_\alpha$.

Proof. (i) is proven by an easy induction argument, since if $\alpha X = X$, then

$$\alpha^k X = \alpha^{k-1}(\alpha X) \subset \alpha^{k-1} X.$$

(ii) is easy, and (iii) and (iv) follow from [**8**, 5.4] and [**8**, 5.5].

PROPOSITION 3.6. *A SOS* (X, G) *is a group extension if and only if* $\mathrm{gr}(X) = \{1\}$. *Hence if* $\alpha \neq 1$, *then* X_α *is a group extension.*

Proof. This follows from [**8**], 5.4] and [**8**], 5.5].

PROPOSITION 3.7. *Suppose* $o(\alpha) = 2$. *Then for any* $x \in G$ *such that* $\alpha(x) = -1, \pm x$ *is* X_α*-rigid.*

Proof. Since $\alpha(-x) = \alpha(x)$, it is enough to show that x is rigid. Note that if $\sigma(x) = 1$ for all $\sigma \in X_\alpha$, then x is trivially X_α-rigid, so assume $\sigma(x) \neq 1$ for some $\sigma \in X_\alpha$. Suppose $\langle 1, x\rangle \equiv \langle b, d\rangle$, we first show that

$$\{\alpha(b), \alpha(d)\} = \{1, -1\}.$$

If $\sigma(x) \neq \pm 1$, then by [1. 10] interchanging b and d if necessary, we can assume $\sigma(b) = 1$ and $\sigma(d) = \sigma(x)$. By assumption, $\alpha\sigma \in X$, hence we have

$$\sigma\alpha(\langle 1, x\rangle) = \sigma\alpha(\langle b, d\rangle).$$

Thus

$$\alpha(b) + \alpha(d)\sigma(x) = 1 - \sigma(x) \neq 0,$$

hence by [1.9(i)], $\alpha(b) = 1$ and $\alpha(d) = -1$. If $\sigma(x) = -1$, then we have $\sigma\alpha(x) = 1$, hence $\sigma\alpha(b) = \sigma\alpha(d) = 1$. Since $\alpha(b) = \pm 1$, we must have $\sigma(b) = \pm 1$. Because $\sigma(\langle 1, x\rangle) = 0, \sigma(d) = -\sigma(b)$ and therefore $\alpha(d) = -\alpha(b)$, proving

$$\{\alpha(b), \alpha(d)\} = \{1, -1\}.$$

By the above, interchanging b and d if necessary, can assume $\alpha(b) = 1$ and $\alpha(d) = -1$. We will show that $\sigma(b) = 1$ for all $\sigma \in X_\alpha$, which will clearly imply x is X_α-rigid. If $\sigma(x) = 1$, then by [1.9(i)] $\sigma(b) = 1$. If $\sigma(x) \neq \pm 1$, then by [1.11]

$$\{\sigma(b), \sigma(d)\} = \{1, \sigma(x)\}.$$

Suppose $\sigma(b) = \sigma(x)$, then $\sigma\alpha(b) = \sigma(x)$, while

$$\sigma\alpha(\langle 1, x\rangle) = 1 - \sigma(x) \neq 0,$$

which is a contradiction of [1.9]. Hence $\sigma(b) = 1$. Finally, if $\sigma(x) = -1$, then $\sigma\alpha(x) = 1$ and so $\sigma(b) = \sigma\alpha(b) = 1$.

Our goal is to show that a connected SOS is a group extension. We will do this by showing that $gr(X) \neq \{1\}$. Thus we need to take a closer look at the subspaces X_α.

PROPOSITION 3.8. *Suppose $o(\alpha) = o(\beta) = 2$ and $X_\alpha \cap X_\beta \cap X_{\alpha\beta} \neq \emptyset$, and $\sigma \in X_\alpha \setminus X_\beta$. Then $\sigma \notin X_{\alpha\beta}$.*

Proof. Assume $\sigma_1 \in X_\alpha \cap X_\beta \cap X_{\alpha\beta}$, and $\sigma\alpha\beta \in X$. Then, since $\{\sigma_1, \sigma_1\alpha, \sigma\alpha\} \subset X_\beta$, by [3.5(iv)], $[\sigma_1, \sigma_1\alpha, \sigma\alpha] \subset X_\beta$. But this implies

$$\sigma = (\sigma_1^{-1})(\sigma_1\alpha)(\sigma\alpha) \in X_\beta,$$

a contradiction. Hence $\sigma\alpha\beta \notin X$ and so $\sigma \notin X_{\alpha\beta}$.

PROPOSITION 3.9. *(cf. [**4**, 4.4]). Suppose α and β are elements of G^* of exact order 2. If $X_\alpha \cap X_\beta \cap X_{\alpha\beta} \neq \emptyset$, then $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$.*

Proof. Suppose not, then there exists $\sigma_1 \in X_\alpha \cap X_\beta \cap X_{\alpha\beta}, \sigma_2 \in X_\alpha \setminus X_\beta$ and $\sigma_3 \in X_\beta \setminus X_\alpha$. Replace X by the subspace of X generated by $\{\sigma_1\alpha, \sigma_1^{-1}\beta, \sigma_2, \sigma_2^{-1}\alpha, \sigma_3\}$. Note that

$$\sigma_1 = (\sigma_1\alpha)(\sigma_2)(\sigma_2^{-1}\alpha) \text{ and } \sigma_1\alpha\beta = (\sigma_1^{-1}\beta)^{-1}(\sigma_2)(\sigma_2^{-1}\alpha)$$

are both in X. Also note that

$$\sigma_2\beta = (\sigma_1\alpha)(\sigma_1^{-1}\beta)(\sigma_2\alpha) \text{ and } \sigma_3\alpha = (\sigma_3)(\sigma_2)(\sigma_2^{-1}\alpha)$$

are both in G^*.

We first show that X is a group extension. Pick $x \in G$ such that $\alpha(x) \neq 1$ and $\beta(x) \neq 1$. We will show $\pm x$ are rigid, and clearly it is enough to show x is rigid, since $\alpha(-x) = \alpha(x)$ and $\beta(-x) = \beta(x)$. By [3.7], x is X_α-rigid and X_β-rigid.

Suppose $\langle 1, x\rangle \equiv \langle b, d\rangle$ for some $b, d \in G$, then we can assume $\sigma(b) = 1$ and $\sigma(d) = \sigma(x)$ for all $\sigma \in X_\alpha$. If $\sigma_1(x) \neq 1$, then $\sigma_1(d) \neq 1$. Since $\sigma_1 \in X_\beta$ and x is X_β-rigid, we then must have $\sigma(b) = 1$ for all $\sigma \in X_\beta$. Hence $\sigma(b) = 1$ for all

$\sigma \in X$ and so $b = 1$. Therefore, x is rigid. If $\sigma_1(x) = 1$, then $\sigma_1\alpha(x) \neq 1$. Since $\sigma_1\alpha \in X_\beta$, replace σ_1 by $\sigma_1\alpha$ and use the same argument to show that x is rigid.

By [1.12], X is a group extension. We can assume X is a group extension of some SOS (X', G') which is not a group extension. For $\sigma \in X$, let $\bar{\sigma}$ denote σ restricted to G'. If $\bar{\alpha} \neq 1$ and $\bar{\beta} \neq 1$, the same argument as for X shows that X' is a group extension, but we assumed not. Hence we have either $\bar{\alpha} = 1$ or $\bar{\beta} = 1$. If $\bar{\alpha} = 1$, then $\bar{\sigma}_3\bar{\alpha} = \bar{\sigma}_3 \in X'$ and so, by the definition of group extension, $\sigma_3\alpha \in X$, a contradiction. Similarly, if $\bar{\beta} = 1$, then $\sigma_2\beta \in X$, a contradiction. Therefore we must have $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$.

LEMMA 3.10. (*cf.* [**4**, 4.6]). *Suppose $o(\alpha) = o(\beta) = 2$ and $|X_\alpha \cap X_\beta| \geq 2$. Then there is some $\gamma \in G^*$ such that $o(\gamma) = 2$ and $X_\alpha, X_\beta \subset X_\gamma$.*

Proof. If $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$, we are done, so assume not.

Case 1. Suppose $\sigma \in X_\alpha \cap X_\beta$ such that $o(\sigma) > 2$. Then pick r such that σ^r has exact order 2, and let $\gamma = \sigma^r$. Since r is even, clearly

$$\sigma \in X_\alpha \cap X_\gamma \cap X_{\alpha\gamma}.$$

Then, by [3.9], $X_\alpha \subset X_\gamma$ or $X_\gamma \subset X_\alpha$.

Suppose $X_\gamma \subset X_\alpha$. Then $\sigma\beta \in X_\gamma \subset X_\alpha$, and hence

$$\sigma \in X_\alpha \cap X_\beta \cap X_{\alpha\beta}.$$

But then, by [3.9], $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$, and we assumed not. Thus we must have $X_\alpha \subset X_\gamma$. A similar proof shows that $X_\beta \subset X_\gamma$, and we are done.

Case 2. Suppose all elements of $X_\alpha \cap X_\beta$ have order 2, then by assumption there is $\sigma_1, \sigma_2 \in X_\alpha \cap X_\beta$ such that $\sigma_1 \neq \sigma_2$. Let $\gamma = \sigma_1\sigma_2$, then

$$\sigma_1 \in X_\alpha \cap X_\gamma \cap X_{\alpha\gamma}.$$

The proof is now the same as in case 1.

PROPOSITION 3.11. *Suppose $\sigma_1, \sigma_2 \in X$ such that $\sigma_2 \notin [\sigma_1]$ and $\sigma_1 \sim \sigma_2$. Then there is some $\gamma \in G^*$ with $o(\gamma) = 2$ such that $\sigma_1, \sigma_2 \in X_\gamma$.*

Proof. It is clear that we need only show that $\sigma_1, \sigma_2 \in X_\delta$ for some $\delta \in G^*$ such that $\delta \neq 1$. By definition we have $\sigma_3 \in X$ such that $\sigma_3 \notin \{\sigma_1^{-1}, \sigma_2^{-1}\}$ and $\sigma_1\sigma_2\sigma_3 \in X$. By [3.5(i)] and [3.6] it is enough to show $[\sigma_1, \sigma_2, \sigma_3]$ is a group extension. If rank $[\sigma_1, \sigma_2, \sigma_3] = 3$, we are done by [2.6].

Assume rank $[\sigma_1, \sigma_2, \sigma_3] = 2$, then we can assume $\{\sigma_1, \sigma_2\}$ is a MGS, and so we have $\sigma_3 = \sigma_1^r\sigma_2^s$ for some r, s. If $\sigma_1^{r+1} = 1$, then $\sigma_3 = \sigma_1^{-1}\sigma_2^s$ and so $\sigma_2^s \neq 1$. Then, by [2.4], we are done. A similar argument works if $\sigma_2^{s+1} = 1$. If $\sigma_1^{r+1} \neq 1$ and $\sigma_2^{s+1} \neq 1$, we have $\sigma_1\sigma_2\sigma_3 = \sigma_1^{r+1}\sigma_2^{s+1} \in X$ and again we are done by [2.4].

We now come to one of the main theorems of this section:

THEOREM 3.12. (cf. [**4**, 4.7]). *Suppose (X,G) is connected, then there is some $\gamma \in G^*$ of exact order 2 such that $X = X_\gamma$. Hence, by [3.7], X is a group extension.*

Proof. The case where X has rank 1 is trivial, thus we assume rank $X \geq 2$. If all elements of X have order 2, then (X,G) is a Space of Orderings and we are done by Marshall's work [**4**], thus we assume X contains an element of order greater than 2. Pick $\sigma_1 \in X$ such that σ_1 has maximal possible order, then $\sigma_1^2 \neq 1$. Pick $\sigma_2 \in X$ such that $\sigma_2 \notin [\sigma_1]$. By hypothesis, $\sigma_1 \sim \sigma_2$, hence by [3.11] there is some γ of exact order 2 such that $\sigma_1, \sigma_2 \in X_\gamma$. Pick $\alpha \in G^*$ such that $\sigma_1 \in X_\alpha$ and $|X_\alpha|$ is maximal. Then, since σ_1 has maximal order and $|X_\alpha| \geq |X_\gamma|$, rank $X_\alpha \geq 2$.

Suppose $X_\alpha \neq X$, then pick $\tau \in X \setminus X_\alpha$. By assumption $\tau \sim \sigma_1$ and so, by [3.11] there is some β such that $\tau, \sigma_1 \in X_\beta$. Since $\sigma_1^2 \neq 1, |X_\alpha \cap X_\beta| \geq 2$, hence by [3.10] there is some γ of exact order 2 such that $X_\alpha \subset X_\gamma$ and $X_\beta \subset X_\gamma$. But this contradicts the maximality of $|X_\alpha|$, since $\tau \in X_\gamma \setminus X_\alpha$. Thus we must have $X_\alpha = X$.

It remains only to prove the transitivity of $\sim$. Unlike the case where $G^2 = 1$, we must do a substantial amount of extra work to prove transitivity.

LEMMA 3.13. *Suppose $\sigma_1, \sigma_2 \in X_\alpha$ where $o(\alpha) = 2$ and $|X_\alpha| \geq 3$. Then $\sigma_1 \sim \sigma_2$.*

Proof. If $\sigma_2 \in [\sigma_1]$, then we are done by [3.2], so assume not. Assume $\sigma_2 \neq \sigma_1\alpha$, then $\sigma_1^{-1}\alpha \neq \sigma_2^{-1}$ and, by assumption, $\sigma_1^{-1} \neq \sigma_2^{-1}$. We have

$$\sigma_1\sigma_2(\sigma_1^{-1}\alpha) = \sigma_2\alpha \in X,$$

hence $\sigma_1 \sim \sigma_2$.

Suppose $\sigma_2 = \sigma_1\alpha$. If $o(\sigma_1) = 2$, then pick $\sigma_3 \in X_\alpha$ such that $\sigma_3 \notin \{\sigma_1^{-1}, \sigma_2^{-1}\}$. Then

$$\sigma_1\sigma_2\sigma_3 = \sigma_3\alpha \in X,$$

hence $\sigma_1 \sim \sigma_2$. If $o(\sigma_1) > 2$, then $\sigma_1 \notin \{\sigma_1^{-1}, \sigma_2^{-1}\}$ and we have

$$\sigma_1\sigma_2\sigma_1 = \sigma_1^3\alpha \in X,$$

hence $\sigma_1 \sim \sigma_2$.

COROLLARY 3.14. *Suppose $Y \subset X$ such that Y is a group extension, $Y \neq C_2 \oplus C_2$, and $\sigma, \gamma \in Y$. Then $\sigma \sim \tau$ in X.*

Proof. By [3.6], $Y = Y_\alpha$ for some $\alpha \neq 1$. Since $Y \neq C_2 \oplus C_2, |Y| > 2$. Hence, by [3.13], $\sigma \sim \tau$ in Y, and therefore in X.

LEMMA 3.15. *Suppose $\alpha \neq 1, \beta \neq 1$, and there exists $\sigma_1 \in X_\alpha \cap X_\beta$, $\sigma_2 \in X_\alpha$, and $\sigma_3 \in X_\beta$. If $\sigma_2\alpha \sim \sigma_3$ or $\sigma_3\beta \sim \sigma_2$, then $\sigma_2 \sim \sigma_3$.*

Proof. Note that, by [3.6] and [3.14], if $\sigma_2 \in X_\beta$ or $\sigma_3 \in X_\alpha$, then $\sigma_2 \sim \sigma_3$. Hence the lemma is true if $\sigma_1 \in [\sigma_2], \sigma_2 \in [\sigma_3]$, or $\sigma_1 \in [\sigma_3]$, so assume none of these hold. If $o(\sigma_1) > 2$, then

$$|X_\alpha \cap X_\beta| \geq 2$$

and so, by [3.10], $X_\alpha \subset X_\beta$ or $X_\beta \subset X_\alpha$, and we are done by the first observation. Thus we can assume $o(\sigma_1) = 2$. Assume one of $\{o(\sigma_2), o(\sigma_3)\}$ is greater than 2, since if not we are done by Marshall's work [**4**, 4.5].

Suppose $\sigma_2\alpha \sim \sigma_3$, then by [3.11], $\sigma_2\alpha, \sigma_3 \in X_\gamma$ for some γ with $o(\gamma) = 2$. Assume $o(\sigma_2) > 2$, then $o(\sigma_2\alpha) > 2$. Since $\sigma_2\alpha \in X_\alpha \cap X_\gamma$, by [3.10], either $X_\alpha \subset X_\gamma$ or $X_\gamma \subset X_\alpha$. If $X_\gamma \subset X_\alpha$, then $\sigma_3 \in X_\alpha$. If $X_\alpha \subset X_\gamma$, then $\sigma_2, \sigma_3 \in X_\gamma$, and we are done by [3.6] and [3.14].

Now assume $o(\sigma_2) = 2$, then by assumption $o(\sigma_3) > 2$. Hence, as above, $X_\beta \subset X_\gamma$ or $X_\gamma \subset X_\beta$. If $X_\gamma \subset X_\beta$, then $\sigma_2\alpha \in X_\beta$ and so $\sigma_2\alpha, \sigma_1 \in X_\beta$. Thus

$$|X_\alpha \cap X_\beta| \geqq 2$$

and so, as above, we are done. If $X_\beta \subset X_\gamma$, then $\sigma_1, \sigma_2\alpha \subset X_\alpha \cap X_\gamma$, and so by [3.10], $X_\alpha \subset X_\gamma$ or $X_\gamma \subset X_\alpha$ and proceed as above.

A similar proof works for the case of $\sigma_3\beta \sim \sigma_2$.

PROPOSITION 3.16. *Suppose $o(\alpha) = o(\beta) = 2, \sigma_1 \in X_\alpha \cap X_\beta, \sigma_2 \in X_\alpha$, and $\sigma_3 \in X_\beta$. Suppose X contains an element of one of the following forms: (a) $\sigma_2^s\sigma_3^t\gamma$ where $\sigma_2^s \neq 1, \sigma_3^t \neq 1$, and $\gamma \in \{1, \alpha, \beta\}$, (b) $\sigma_1^r\sigma_2^s\sigma_3^t\gamma$, where r is odd, $\sigma_2^s \neq 1, \sigma_3^t \neq 1$, and $\gamma \in \{1, \alpha, \beta\}$, or (c) $\sigma_1^r\sigma_2^s\sigma_3^t\alpha\beta$, where r, s and t are odd. Then $\sigma_2 \sim \sigma_3$.*

Proof. Assume X contains σ of type (a). If $\sigma = \sigma_2^s\sigma_3^t$, then $Y = [\sigma_2, \sigma_3]$ is a group extension by [2.4] and we are done by [3.14]. Suppose $\sigma = \sigma_2^s\sigma_3^t\alpha$. If s is odd, then $\sigma_2\alpha \sim \sigma_3$ since $[\sigma_2\alpha, \sigma_3]$ is a group extension. Hence, by [3.15], $\sigma_2 \sim \sigma_3$. If s is even,

$$\sigma_2^s\sigma_3^t\alpha = (\sigma_2\alpha)(\sigma_2^{s-1})\sigma_3^t$$

and hence $\sigma_2\alpha \sim \sigma_3$. Thus $\sigma_2 \sim \sigma_3$ by [3.15]. A similar argument works if $\sigma = \sigma_2^s\sigma_3^t\beta$. If

$$\sigma = \sigma_2^s\sigma_3^t\alpha\beta,$$

then σ can be written as either

$$(\sigma_2\alpha)^s(\sigma_3\beta)(\sigma_3)^{t-1} \text{ or } (\sigma_2\alpha)(\sigma_2)^{s-1}(\sigma_3\beta)^t.$$

Hence either $\sigma_2 \sim \sigma_3\beta$ or $\sigma_2\alpha \sim \sigma_3$, and we are done by [3.15].

Assume X contains σ of type (b). Since r is odd, $[\sigma_1\gamma, \sigma_2, \sigma_3]$ contains a 3-product and thus is a group extension by [2.15]. Hence $\sigma_2 \sim \sigma_3$ by [3.14].

Assume X contains σ of type (c). Then, by [2.15], $[\sigma_1\alpha, \sigma_2, \sigma_3\beta]$ is a group extension, and we are done by [3.14] and [3.15].

THEOREM 3.17. *$\sim$ is an equivalence relation.*

Proof. by [3.2], $\sim$ is reflexive, and it is clearly symmetric, thus we need only show that it is transitive. Suppose $\sigma_1 \sim \sigma_2$ and $\sigma_1 \sim \sigma_3$, then we want to show $\sigma_2 \sim \sigma_3$. By [3.11], these exists α and β of exact order 2 such that $\sigma_1, \sigma_2 \in X_\alpha$ and $\sigma_1, \sigma_3 \in X_\beta$. If $o(\sigma_1) > 2$, then, by [3.10], $X_\alpha, X_\beta \subset X_\gamma$ for some γ where $o(\gamma) = 1$. Hence, by [3.6] and [3.14], $\sigma_2 \sim \sigma_3$. Thus we assume $o(\sigma_1) = 2$. If $\sigma_2 \in X_\beta$ or $\sigma_3 \in X_\alpha$, then we are done by [3.6] and [3.14]. If $\sigma_2 \in X_{\alpha\beta}$, then $\sigma_2\alpha, \sigma_3 \in X_\beta$. Hence $\sigma_2\alpha \sim \sigma_3$ and so $\sigma_2 \sim \sigma_3$ by [3.15]. By a similar argument, we are done if $\sigma_3 \in X_{\alpha\beta}$.

Replace X by the subspace of X generated by

$$S = \{\sigma_1\alpha, \sigma_1\beta, \sigma_2, \sigma_2^{-1}\alpha, \sigma_3\}.$$

Note that $\sigma_1\alpha \sim \sigma$ for all $\sigma \in S$, thus if rank $X \leqq 3$ we are done by [3.3] and [3.14]. Hence we can assume rank $X \geq 4$.

Case 1. Suppose rank $X = 5$. For ease exposition, set $\tau_1 = \sigma_1\alpha, \tau_2 = \sigma_1\beta, \tau_3 = \sigma_2, \tau_4 = \sigma_2^{-1}\alpha$, and $\tau_5 = \sigma_3$. Then $\{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5\}$ is a MGS for X. Let $\{a_1, \ldots, a_5\}$ be a dual basis and $\{c_1, \ldots, c_5\}$ be an S-basis. Since $o(\tau_1) = o(\tau_2) = 2, a_1 = c_1$ and $a_2 = c_2$. Note that X contains $\sigma_1 = \tau_1\tau_3\tau_4$ and $\sigma_3\beta = \tau_1\tau_2\tau_3\tau_4\tau_5$.

Let $f = \langle 1, c_2c_3c_4c_5, c_1c_2c_3c_5\rangle$ and $g = \langle c_1c_2c_4c_5, c_2c_3, c_3c_5\rangle$. Renumbering, we can apply [1.16] (with $\sigma = \tau_1\tau_3\tau_4, d = c_1$, and $x = c_1c_2c_4c_5$). Thus there is some $\tau \in X$ such that $\tau(f) \neq \tau(g)$. Suppose

$$\tau = \prod_{i=1}^{5} \tau_i^{r_i}.$$

An easy check shows that if only one r_i is odd, then $\tau(f) = \tau(g)$, hence there must be at least 3 odd r_i's. This means τ is a 3-, 4-, or 5-product.

Suppose τ is a 3-product, then $\tau = \tau_i^r\tau_j^s\tau_k^t$ where r, s and t are odd. Since $\tau(f) \neq \tau(g)$, an easy check shows that $\{i, j, k\}$ is not $\{1, 3, 4\}$, $\{1, 2, 3\}$, $\{2, 3, 4\}$, or $\{3, 4, 5\}$. Let us look at the remaining 5 possibilities for $\{i, j, k\}$. If $\tau = \tau_1\tau_2\tau_4^r$, then $\sigma_2 \in X_\beta$, and we're done. If $\tau = \tau_1\tau_2\tau_5^r$, then $\sigma_3 \in X_{\alpha\beta}$ and we're done. If $\tau = \tau_1\tau_3^r\tau_5^s$, then $[\tau_1, \tau_3, \tau_5]$ is a group extension by [2.15] and contains σ_2 and σ_3, and thus we are done by [3.14]. A similar proof works for $\tau = \tau_2\tau_3^t\tau_5^s$. If $\tau = \tau_1\tau_4^r\tau_5^s$ or $\tau = \tau_2\tau_4^r\tau_5^s$, we are done by [3.16].

Now suppose τ is a 4-product, then it has 3 odd exponents and 1 even exponents. If $\tau = \tau_1\tau_2\tau_i^r\tau_j^s$, then we are done by [3.16]. If $\tau = \tau_1\tau_3^r\tau_4^s\tau_5^t$, then, since

https://doi.org/10.4153/CJM-1989-037-3 Published online by Cambridge University Press

$\tau(f) \neq \tau(g)$, we must have t odd and we are done by [3.16]. A similar proof works for $\tau = \tau_2\tau_3^r\tau_4^s\tau_5^t$.

Finally, suppose τ is a 5-product. Since $\tau(f) \neq \tau(g), \tau$ must have at least one even exponent, and hence it has exactly 2 even exponents. Since $o(\tau_1) = o(\tau_2) = 2$, the exponents of τ_1 and τ_2 are 1. Then τ is either of the form $\sigma_2^r\sigma_3^s\alpha^k\beta, \sigma_3^s\alpha\beta$, or $\sigma_2^r\alpha^k\beta$. If $\tau = \sigma_3^s\alpha\beta$, then $\sigma_3\beta \in X_\alpha$ and so $\sigma_3\beta \sim \sigma_2$. Hence $\sigma_2 \sim \sigma_3$ by [3.15]. A similar proof works if $\tau = \sigma_2^r\alpha\beta$. If $\tau = \sigma_2^r\sigma_3^s\alpha^k\beta$, then $\sigma_2 \sim \sigma_3$ by [3.16].

Case 2. Suppose $\alpha = \sigma_2^k$ for some (necessarily even) k. Then clearly $\{\sigma_1, \sigma_1\beta, \sigma_2, \sigma_3\}$ is a MGS for X. Since σ_1 and $\sigma_1\beta$ have order 2 they must be strongly independent. For ease of exposition, let $\tau_1 = \sigma_1, \tau_2 = \sigma_1\beta, \tau_3 = \sigma_3$ and $\tau_4 = \sigma_2$. Pick a dual basis $\{a_1, \ldots, a_4\}$ and an S-basis $\{c_1, \ldots, c_4\}$. Note X contains $\tau_1\tau_2\tau_4$, and $\tau_1\tau_4^k$.

Let $f = \langle 1, c_2c_3c_4, c_1c_2c_3\rangle$ and let $g = \langle c_1c_2c_4, c_2c_3, c_3\rangle$. By [1.16], there is some $\tau \in X$ such that $\tau(f) \neq \tau(g)$. An easy check shows that

$$\tau = \prod_{i=1}^{4} \tau_i^{r_i}$$

has more than one odd exponent, and hence has exactly 3 odd exponents.

Suppose τ is a 3-product, then since $\tau(f) \neq \tau(g), \tau \notin [\tau_1, \tau_2, \tau_4]$. If $\tau = \tau_1\tau_2\tau_3^r$, then $\sigma_2 \in X_\beta$. If $\tau = \tau_1\tau_3^r\tau_4^s$, or if $\tau = \tau_2\tau_3^r\tau_4^2$, then we are done by [3.16].

Finally, suppose τ is a 4-product, then $\tau = \tau_1\tau_2\tau_3^r\tau_4^s = \sigma_2^r\sigma_3^s\beta$ and we are done by [3.16].

Case 3. Suppose $\alpha \notin [\sigma_2]$ and rank $X = 4$. We let $\tau_1 = \sigma_1\alpha, \tau_2 = \sigma_1\beta, \tau_3 = \sigma_2, \tau_4 = \sigma_2^{-1}\alpha$, and $\tau_5 = \sigma_3$. One of these must be in the span of the others, hence we have a relation

$$\prod_{i=1}^{5} \tau_i^{r_i} = 1$$

where at least two of the r_i's are odd. We consider separately the cases where both τ_1 and τ_2 are in this relation, only τ_1 is in the relation, and only τ_2 is in the relation.

Suppose we have $\tau_1\tau_2\tau_3^r\tau_4^s\tau_5^t = 1$. If s is odd, then this gives us

$$\sigma_2^s = \sigma_2^r\sigma_3^t\beta \in X.$$

If $\sigma_2^r \neq 1$ and $\sigma_3^t \neq 1$, then we are done by [3.16]. If $\sigma_3^t \neq 1$ or $\sigma_2^r \neq 1$, then $\sigma_2 \in X_\beta$. If s is even, then we have

$$\sigma_3 = (\sigma_2)^{r-s}(\sigma_3)^{t-1}\alpha\beta \in X,$$

hence either $\sigma_2 \in X_{\alpha\beta}, \sigma_3 \in X_{\alpha\beta}$, or we are done by [3.16].

Suppose we have $\tau_1\tau_3^r\tau_4^s\tau_5^t = 1$. If $\tau_5^t = 1$, then this means

$$\tau_1 = (\sigma_2)^{r-s}\sigma_3^t\alpha^m \in X$$

where $(\sigma_2)^{r-s} \neq 1$, and we're done by [3.16]. If $\tau_5^t = 1$, then $r-s$ must be odd, and we have

$$\sigma_1 = (\sigma_2)^{r-s}\alpha^m.$$

Since $\sigma_1 \in X_\beta$, this implies either $\sigma_2 \in X_\beta$ or $\sigma_2 \in X_{\alpha\beta}$.

Finally, suppose $\tau_3^r\tau_4^s\tau_5^t = 1$. If $\tau_5^t = 1$, then $\alpha = (\sigma_2)^{r-s}$, but we assumed not. Hence we have

$$\sigma_2 = \sigma_2^k\sigma_3^t\alpha^m \in X$$

where $\sigma_2^k \neq 1$ and $\sigma_3^t \neq 1$, and we are done by [3.16].

4. Classification of finite spaces of signatures. We now know that $\sim$ defines an equivalence relation, and that each connected component of (X, G) is a group extension. Thus to show that (X, G) is constructable, we need to show that it is the direct sum of its connected components. We use the following application of the Representation Theorem, which is a special case of [**5**, 3.4]. The author is grateful to Marshall for suggesting the use of this theorem in this case.

PROPOSITION 4.1. *Suppose $(X_1, G_1), (X_2, G_2), \ldots, (X_n, G_n)$ are the connected components of (X, G), where*

$$G_i = G\Big/\Big(\bigcap_{\sigma\in X_i}\ker\sigma\Big).$$

Then $(X, G) = \oplus(X_i, G_i)$, the direct sum of its connected components.

Proof. Given $a \in G$, we define $\hat{a} : X \longrightarrow \mu$ by $\hat{a}(\sigma) = \sigma(a)$. Then for a form $\rho = \langle a_1, \ldots, a_n\rangle$, we define $\hat{\rho} : X \longrightarrow C$ by $\hat{\rho} = \sum \hat{a}_i$.

If X is connected the result is trivial, so we assume not. Since $\sim$ is an equivalence relation, X is the disjoint union of the X_i's. Hence it is enough to show that the cannonical map $\phi : G \longrightarrow \prod G_i$ is an isomorphism. It is clearly injective, thus we must show it is onto.

For each i, fix $a_i \in G_i$. Define $f : X \longrightarrow \mu$ by $f(\sigma) = \sigma(a_i)$ for $\sigma \in X_i$. We want to show that f is represented by a form ρ over X. By the Representation theorem [**9**, 5.8], it is enough to prove it for the case where X is a quasifan.

If X is a group extension, then, by [3.5(i)] and [3.6], X is connected and we assumed not. Thus X is not a group extension and so, since X is a quasifan, (X, G) is the direct sum of two fans. But fans are connected, hence X has two connected components and we have $\phi : G \longrightarrow G_1 \times G_2$ is an isomorphism. Hence there is some $a \in G$ such that $\phi(a) = (a_1, a_2)$ and then clearly $f = \hat{a}$. Therefore f is represented by a form over X.

Since f is represented over all quasifans, $f = \hat{\rho}$ for some form ρ over X. Note that f is a unit since the function defined using a_i^{-1} instead of a_i is an inverse for f. Then, by [**5**, 2.3], $f = \hat{a}$ for some $a \in G$. Hence $\phi(a) = (a_1, a_2, \ldots, a_n)$ and therefore ϕ is onto.

We finally come to the main result of this paper:

THEOREM 4.2. *Suppose* (X, G) *is a* SOS *with* G *finite of* 2*-primary order. Then* (X, G) *is constructable, hence there is a field* K *and a preorder* $T \subset K$ *such that* $(X_T, \dot{K}/\dot{T}) = (X, G)$.

Proof. By [**10**, 3.5], we are done if we show that (X, G) is constructable, i.e., built up from C_2 by group extensions and direct sums. We proceed by induction on $|G|$.

If $|G| = 2$, then $(X, G) = C_2$. If $|G| = 4$, then $(X, G) = C_2 \oplus C_2$, or $(X, G) = C_4$, both of which are constructable. Hence we assume $|G| > 4$.

If (X, G) is connected, then by [3. 12] it is a group extension of some SOS (X', G'). By definition of group extension, $|G'| < |G|$, hence by induction (X', G') is constructable. Therefore, (X, G) is constructable.

If (X, G) is not connected, then by [4. 1], (X, G) is the direct sum of its connected components. Since there is more than one component, each one is smaller than (X, G) and hence by induction is constructable. Therefore (X, G) is constructable.

REFERENCES

1. E. Becker and A. Rosenberg, *Reduced forms and reduced Witt rings of higher level*, J. Algebra *92* (1985), 477–503.

2. T. Craven, *Witt rings and orderings of skew fields*, J. Algebra *77* (1982), 74–96.

3. F. Kalhoff, *Spaces of orderings and Witt rings of planar ternary rings*, J. Pure Appl. Math., to appear.

4. M. Marshall, *Classification of finite spaces of orderings*, Can. J. Math *31* (1979), 320–330.

5. M. Marshall and C. Mulcahy, *The Witt ring of a space of signatures.* Preprint.

6. M. Marshall and L. Walter, *Signatures of higher level on rings with many units.* Preprint.

7. C. Mulcahy, *Spaces of signatures*, Ph.D. thesis, Cornell University (1985).

8. ——— *An abstract approach to higher level forms and rigidity*, Comm. Algebra *16* (1988), 577–612.

9. ——— *The representation theorem for spaces of signatures*, J. Algebra *3* (1988), 105–122.

10. V. Powers, *Characterizing reduced Witt rings of higher level*, Pac. J. Math. *128* (1987), 333–347.

11. ——— *Higher level reduced Witt rings of skew fields*, Math. Zeit. *198* (1988), 545–554.

Emory University,
Atlanta, Georgia