ELSEVIER

Journal of Pure and Applied Algebra 108 (1996) 81–98

JOURNAL OF PURE AND APPLIED ALGEBRA

Braid group actions on left distributive structures, and well orderings in the braid groups

Richard Laver [1]

Mathematics Department, University of Colorado, Boulder, CO 80309, USA

Communicated by A. Blass; received 15 February 1994; revised 2 April 1995

0.

For $2 \leq N \leq \infty$ let B_N be the braid group on N strands; B_N, with generators $\sigma_1, \sigma_2, \ldots, \sigma_i, \ldots$ $(1 \leq i < N)$, is given by the relations $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ and $\sigma_i\sigma_j = \sigma_j\sigma_i$ $(j > i+1)$. Two basic group actions of B_N are as follows. B_N acts on the free group $(F, \circ)$ on generators $\{h_i : 0 \leq i < N\}$ by $(h_{i-1})^{\sigma_i} = h_{i-1} \circ h_i \circ h_{i-1}^{-1}$, $(h_i)^{\sigma_i} = h_{i-1}$, $(h_j)^{\sigma_i} = h_j$ for $j \neq i-1, i$, and $(u \circ v)^{\sigma_i} = (u)^{\sigma_i} \circ (v)^{\sigma_i}$ [1]. If $(G, \circ)$ is any group, B_N acts on G^N by $(\langle g_0, \ldots, g_{i-1}, g_i, \ldots, g_k, \ldots \rangle_{k<N})^{\sigma_i} = \langle g_0, \ldots, (g_{i-1} \circ g_i \circ g_{i-1}^{-1}), g_{i-1}, \ldots, g_k, \ldots \rangle_{k<N}$ (see [24, p. 157]).

More generally, the braid groups act, or partially act, in various ways on certain left distributive algebras and their direct powers. A left distributive algebra is a set with a binary operation on it satisfying the left distributive law $a(bc) = (ab)(ac)$ (for example, for a group $(G, \circ)$, the conjugation operation $gh = g \circ h \circ g^{-1}$ satisfies the left distribution law). Brieskorn [2] expressed a number of actions of B_N as generalizations of the second of the above examples: if $\mathscr{C}$ is an automorphic set (a left distributive algebra in which left multiplication by any element is bijective), then the condition $\langle c_0, \ldots, c_{i-1}, c_i, \ldots, c_k, \ldots \rangle^{\sigma_i} = \langle c_0, \ldots, (c_{i-1}c_i), c_{i-1}, \ldots, c_k, \ldots \rangle$ induces a group action of B_N on $\mathscr{C}^N$. See [2, 3, 16, 18, 27, 29] for some examples of this related to knots and braids.

For κ a cardinal, let $\mathscr{A}_\kappa$ be the free left distributive algebra on κ many generators. Then $\mathscr{A}_\kappa$ is not an automorphic set, but it does satisfy left cancellation, as follows. For $\mathscr{C}$ any left distributive algebra, $b, c \in \mathscr{C}$, define

$$b <_{\mathrm{L}} c \quad \Leftrightarrow \quad \text{for some } b_0, b_1, \ldots, b_n \in \mathscr{C},\ c = (((bb_0)b_1)\cdots b_{n-1})b_n\,.$$

Let $\mathscr{A} = \mathscr{A}_1$. Then $<_{\mathrm{L}}$ linearly orders $\mathscr{A}$ [4–6, 21]. It follows that $\mathscr{A}$ satisfies left cancellation. These and similar facts about the $\mathscr{A}_\kappa$'s $(\kappa > 1)$ are recalled in Section 1.

[1] Supported by NSF Grant DMS 9303217.

SSDI 0022-4049(95)00147-6

For $\mathscr{C}$ a left distributive algebra satisfying left cancellation, as noted by Dehornoy in [6], the action of B_N on $\mathscr{C}^N$ is still a partial group action. That is, for $\vec{c}$ in $\mathscr{C}^N$, the equation $\vec{d}^{\sigma_i} = \vec{c}$ has at most one solution, so $\vec{c}^{\sigma_i^{-1}}$ is unique when defined. Also needed to check that this action is well defined is a result of Garside [14] (see proof of Theorem 2.7 below). Write $\omega = \{0, 1, 2, \dots\}$. Dehornoy ([6, Theorem 7.6, Theorem 3.1 below]) proved, by means of the partial action of B_∞ on $\mathscr{A}^\omega$, that the linear ordering $<_{\mathrm{L}}$ on $\mathscr{A}$ induces a linear ordering $<$ on B_∞. For a combinatorial characterization of $<$, define, for $\alpha \in B_\infty$, ε the identity of B_∞, $\varepsilon < \alpha$ if and only if α can be represented as a nonempty braid word $w = \sigma_{i_1}^{\pm 1} \cdots \sigma_{i_n}^{\pm 1}$ such that the generator with least subscript appearing in w occurs only positively. Then for $\alpha, \beta \in B_\infty$, $\alpha < \beta$ holds if and only if $\varepsilon < \alpha^{-1}\beta$. So $i < j$ implies $\sigma_i > \sigma_j$ and, for example, $\sigma_i^{-1}\sigma_{i+1} < \varepsilon < \sigma_{i+1}^{-1}\sigma_i$.

Let B_N^+ be the set of positive braids in B_N-braids which can be represented by a word (possibly empty) in which the generators occur only positively. Thus Dehornoy's ordering extends the notion of positive braid: for $2 < N \leq \infty$, B_N^+ is a proper subset of $\{\alpha \in B_N : \varepsilon \leq \alpha\}$. The ordering is preserved under left translations; this yields, as remarked by Larue, a combinatorial proof that the braid groups are torsion free.

In this paper a result about a free left distributive version of Artin's group action is proved; this is then used to derive a result about $<$. Let $x_0, x_1, \dots, x_n, \dots$ be the generators of $\mathscr{A}_\omega$. Define $x_i^{\sigma_i} = x_{i-1}$, $x_{i-1}^{\sigma_i} = x_{i-1}x_i$, and $x_j^{\sigma_i} = x_j$ for $j \neq i-1, i$. This does not induce a partial action of B_∞ on $\mathscr{A}_\omega$ ($(x_0x_0)^{\sigma_1} = (x_1x_0)^{\sigma_1}$ for example). We define a subset of $\mathscr{A}_\omega$ – those members of $\mathscr{A}_\omega$ which can be expressed in "decreasing division form". Decreasing division form (*DDF*) is defined with the aid of a natural linear ordering $\prec$ on $\mathscr{A}_\omega$.

Theorem. *The action of the generators given above induces a partial group action of B_∞ on DDF. This action is order preserving, faithful, and for all $w \in DDF$ and $\alpha \in B_\infty^+$, $w \preceq w^\alpha$.*

To define *DDF*, as in the case of the normal forms of [21, 22], we will not work in $\mathscr{A}_\omega$ but in $\mathscr{P}_\omega$, the result of enlarging $\mathscr{A}_\omega$ to include a composition operation, and work with the *DDF* of that larger algebra.

Elrifai and Morton [12] define a partial ordering on B_∞: α is less than β in their sense if and only if there are γ and δ in B_∞^+, at least one of γ, δ different from ε, with $\beta = \gamma\alpha\delta$.

Theorem. *The ordering $<$ extends the ordering of Elrifai and Morton. For N finite, B_N^+ is well ordered under $<$.*

The parts of Section 1 needed for Sections 2 and 3 are Theorem 1.5 and basic properties of left distributive algebras (Proposition 1.1). Theorem 1.5 states the linear ordering on free left distributive algebras [4–7, 21, 22] in a general form. It is the version in [7] generalized to the $\mathscr{P}_\kappa$'s; it follows from Theorems 1.3 and 1.4. Theorem 1.3 was derived from large cardinals in [21], and without them in [6]; a short proof is given in [19]. A short account of parts of Theorem 1.4 may be found in, e.g., [9].

1.

We recall some facts from [4–7, 21, 22], and related results.

In a language with two binary operation symbols $\cdot$ and $\circ$, let, writing uv for $u\cdot v$, Σ be the set of laws $\{(a\circ b)\circ c = a\circ(b\circ c),\ (a\circ b)c = a(bc),\ a(b\circ c) = ab\circ ac,\ a\circ b = ab\circ a\}$. Then Σ implies the left distributive law $(a(bc) = (a\circ b)c = (ab\circ a)c = ab(ac))$.

Two models of Σ are $(G,\circ,\cdot)$ where G is a group, $\circ$ is the group operation and $\cdot$ is conjugacy, and, from set theory, $(\mathscr{E}_\lambda,\circ,\cdot)$, where for λ a limit ordinal $\mathscr{E}_\lambda$ is the set of nontrivial elementary embedding $j : (V_\lambda,\varepsilon) \to (V_\lambda,\varepsilon)$, $\circ$ is composition, and $j\cdot k = \bigcup_{\alpha<\lambda} j(k\cap V_\alpha)$. Let $\mathscr{P}_\kappa$, for κ a cardinal, be the free algebra satisfying Σ on generators $\{x_\alpha : \alpha < \kappa\}$, and let $\mathscr{P} = \mathscr{P}_1$.

Let A_κ (respectively, P_κ) be the set of terms in the variables $x_0, x_1, \ldots, x_\alpha, \ldots$ $(\alpha < \kappa)$ using the operation $\cdot$ (respectively, $\cdot$ and $\circ$). An example of such a term is $(x_2x_1)\circ(x_2(x_3\circ x_0))$. Then $\mathscr{A}_\kappa = A_\kappa/\equiv_{\mathscr{A}_\kappa}$ and $\mathscr{P}_\kappa = P_\kappa/\equiv_{\mathscr{P}_\kappa}$, where for $u,v\in A_\kappa$, $u\equiv_{\mathscr{A}_\kappa} v$ iff v is the result of repeated substitutions in u using the left distributive law, and $\equiv_{\mathscr{P}_\kappa}$ is similarly defined by substitutions using Σ.

Let $\mathscr{C}$ be an algebra satisfying Σ (or a left distributive algebra, in which case delete the parts of the following definitions involving $\circ$).

For $c_0, c_1, \ldots, c_n \in \mathscr{C}$, write $c_0c_1\cdots c_n$ for $(((c_0c_1)c_2)\cdots)c_n$ and write $c_0c_1\cdots c_{n-1}\circ c_n$ for $((((c_0c_1)c_2)\cdots)c_{n-1})\circ c_n$. Let $u = c_0c_1\cdots c_{n-1} * c_n$ mean that $u = c_0c_1\cdots c_n$ or $u = c_0c_1\cdots c_{n-1}\circ c_n$. Then for any $u\in\mathscr{P}_\kappa$, u can be written in the form $p_0p_1\cdots p_{n-1} * p_n$ where p_0 is a generator.

For $u,v\in\mathscr{C}$, say that u is a left component of v ($u <_{\mathrm{L}} v$) if there are $u_0,\ldots,u_n\in\mathscr{C}$ with $v = uu_0u_1\cdots u_{n-1} * u_n$. Then $<_{\mathrm{L}}$ is a transitive relation on $\mathscr{C}$.

We summarize some facts ($\mathscr{C}$ is still an arbitrary left distributive algebra or an algebra satisfying Σ).

Proposition 1.1. (i) *For $p\in\mathscr{P}_\kappa$ there is a unique α such that for some $p_0,\ldots,p_{i-1}\in\mathscr{P}_\kappa$, $p = x_\alpha p_0\cdots p_{i-2} * p_{i-1}$; write $x_\alpha = L(p)$.*

(ii) *For $a\in\mathscr{A}_\kappa$ there is a unique α and n such that for some $a_0,\ldots,a_{n-1}\in\mathscr{A}_\kappa$, $a = a_0(a_1(\cdots(a_{n-1}x_\alpha)))$; write $x_\alpha = R(a)$, $n = $ depth a.*

(iii) *For $w\in\mathscr{P}_\kappa$ there is a unique n such that for some $a_0,\ldots,a_n\in A_\kappa$, $w\equiv_{\mathscr{P}_\kappa} a_0\circ\cdots\circ a_n$.*

(iv) *If $a,b,c\in\mathscr{C}$, $b <_{\mathrm{L}} c$, then $ab <_{\mathrm{L}} a\circ b <_{\mathrm{L}} ac$.*

(v) *For $w\in P_\kappa$, let a cut of w be a $c\in P_\kappa$ gotten by truncating w at an occurrence of a variable in w. Thus the cut of $x_0x_1(x_2x_1\circ(x_1x_3\circ x_2))$ at the last occurrence of x_1 is $x_0x_1(x_2x_1\circ x_1)$. Then if c and d are cuts of w with c strictly to the left of d, then $c <_{\mathrm{L}} d$.*

Theorem 1.2 (Laver [21]). *For $a,b,a_0,\ldots,a_m,\ b_0,\ldots,b_m\in A_\kappa$*

(i) *$a_0\circ\cdots\circ a_m \equiv_{\mathscr{P}_\kappa} b_0\circ\cdots\circ b_m$ if and only if $a_0(a_1(\cdots(a_mx_\alpha)))\equiv_{\mathscr{A}_\kappa} b_0(b_1(\cdots(b_mx_\alpha)))$ for some/all generators x_α.*

(ii) *$a\equiv_{\mathscr{P}_\kappa} b$ if and only if $a\equiv_{\mathscr{A}_\kappa} b$.*

(iii) *$a <_{\mathrm{L}} b$ as members of $\mathscr{P}_\kappa$ if and only if $a <_{\mathrm{L}} b$ as members of A_κ.*

The proof in [21, Section 1], for $\kappa = 1$ works without change for arbitrary κ. By (ii), identify $\mathscr{A}_\kappa$ as a subalgebra of $\mathscr{P}_\kappa$ (restricted to $\cdot$). Write $\equiv$ for $\equiv_{\mathscr{P}_\kappa}, \equiv_{\mathscr{A}_\kappa}$.

Say that $\mathscr{C}$, a left distributive algebra or an algebra satisfying Σ, is irreflexive if for all $c \in \mathscr{C}$, $c \not<_{\mathrm{L}} c$. Common examples of left distributive algebras (such as groups under conjugation, vector spaces where $v \cdot w = tv + (1-t)w$ (t a fixed scalar)) are idempotent and thus not irreflexive.

Theorem 1.3 (Laver [21], Dehornoy [6] in ZFC). *For every cardinal κ, $\mathscr{A}_\kappa$ and $\mathscr{P}_\kappa$ are irreflexive.*

To prove this, note that if there exists an irreflexive left distributive algebra, then the $\mathscr{A}_\kappa$'s are irreflexive, and the $\mathscr{P}_\kappa$'s are easily seen to be irreflexive also (if $p \in \mathscr{P}_\kappa$, $p = pp_0 \cdots p_{n-1} * p_n$, and $x_\alpha = L(p_0)$, then $px_\alpha \in \mathscr{A}_\kappa$ and $px_\alpha <_{\mathrm{L}} px_\alpha$ would hold). In [21] it was shown that the algebras $\mathscr{E}_\lambda$ mentioned above are irreflexive, and, for $j \in \mathscr{E}_\lambda$, that the subalgebra of $\mathscr{E}_\lambda$ generated by j under $\cdot$ (respectively, under $\cdot$ and $\circ$) is isomorphic to $\mathscr{A}$ (respectively, $\mathscr{P}$). That there exists a λ with $\mathscr{E}_\lambda \neq \emptyset$ is a large cardinal axiom; nonempty $\mathscr{E}_\lambda$'s cannot be proved to exist in ZFC (some facts about the $\mathscr{E}_\lambda$'s appear in [8–11, 17, 21, 23, 25, 26, 28, 30]). Then Dehornoy [6] proved without using large cardinals that a certain left distributive algebra on the braid group is irreflexive, giving a proof of Theorem 1.3 in ZFC. Larue [19] has given a shorter proof of the irreflexivity of the algebra in [6].

For $\kappa = 1$, a stronger statement holds: $<_{\mathrm{L}}$ linearly orders $\mathscr{A}$ and $\mathscr{P}$. This was first proved in [21] (with the irreflexivity part coming via the large cardinal axiom). Dehornoy [4, 5] around the same time proved, independently and by a different method that for every $a, b \in \mathscr{A}$, $a \leq_{\mathrm{L}} b$ or $b \leq_{\mathrm{L}} a$ (from Theorem 1.4(iii) below). Thus he was only missing irreflexivity for the proof of the linear ordering. We summarize Dehornoy's method, and some applications of it using irreflexivity, in Theorem 1.4. We summarize the method of [21, 22] in Theorems 1.6 and 1.7. Either of these two methods, combined with the ZFC proof of Theorem 1.3 in [6], give a proof in ZFC that $<_{\mathrm{L}}$ linearly orders $\mathscr{A}$ and $\mathscr{P}$. This linear ordering is stated here in a general form in Theorem 1.5.

For $u, v \in A_\kappa$ write $u \to v$ to mean that v can be obtained from u by a sequence of substitutions, each of which replaces a subterm of the form $a(bc)$ by $(ab)(ac)$. Then $u \to v$ implies $u \equiv v$. Note that if $u_0u_1 \cdots u_m \to v$, then v is of the form $v_0v_1 \cdots v_n$, where for all $i \leq m$ there is a $j \leq n$ with $u_0u_1 \cdots u_i \equiv v_0v_1 \cdots v_j$.

Theorem 1.4 (Dehornoy [4–7]). (i) *$\mathscr{A}_\kappa$ is confluent, that is, if $a, b \in A_\kappa$ and $a \equiv b$, then for some $c \in A_\kappa$, $a \to c$ and $b \to c$.*
(ii) (*From* (i), *Theorem* 1.3, *and the remark preceding this theorem*) *For $w \in \mathscr{A}_\kappa$, $\{u \in \mathscr{A}_\kappa : u \leq_{\mathrm{L}} w\}$ is linearly ordered under $<_{\mathrm{L}}$.*
(iii) *If $a, b \in A$, then either $a, b \to c$ for some c, or for some $c = c_0c_1 \cdots c_n \in A$ with $n > 0$, either $a \to c_0$ and $b \to c$ or $b \to c_0$ and $a \to c$.*

The following remark about $\mathscr{P}_\kappa$ will be used below: if $t <_{\mathrm{L}} wx$ in $\mathscr{P}_\kappa$ and x is a generator then $t \leq_{\mathrm{L}} w$. Namely, for some generator y, $ty \leq_{\mathrm{L}} wx$, and $ty, wx \in \mathscr{A}_\kappa$. One has then that ty is a cut of some word for wx. The latter word, by induction on derivations, must be of the form $w_0(w_1(\cdots(w_n x)))$ where $w_0 \circ w_1 \circ \cdots w_n \equiv w$, from which it follows that $t \leq_{\mathrm{L}} w$.

For $p, q \in \mathscr{P}_\kappa$ say that p and q have a variable clash if there are $a_0, \ldots a_{n-1} \in A_\kappa$ ($n = 0$ allowed) and $x_\alpha \neq x_\beta$ with $a_0(a_1(\cdots(a_{n-1}x_\alpha))) \leq_{\mathrm{L}} p$ and $a_0(a_1(\cdots(a_{n-1}x_\beta))) \leq_{\mathrm{L}} q$. Note that $a_0(a_1(\cdots(a_{n-1}x_\alpha))) \leq_{\mathrm{L}} a_0(a_1(\cdots(a_{n-1}x_\beta)))$ cannot hold. Namely, they cannot be equivalent by Proposition 1.1 (ii), and if $a_0(a_1(\cdots(a_{n-1}x_\alpha))) <_{\mathrm{L}} a_0(a_1(\cdots(a_{n-1}x_\beta)))$, then by the above remark $a_0(a_1(\cdots(a_{n-1}x_\alpha))) \leq_{\mathrm{L}} a_0 \circ a_1 \circ \cdots \circ a_{n-1}$, which contradicts irreflexivity. It follows that if p and q have a variable clash then $p \leq_{\mathrm{L}} q$ cannot hold: by Theorem 1.4 (ii) one would have $a_0(a_1(\cdots(a_{n-1}x_\alpha)))$ $\leq_{\mathrm{L}}$-comparable with $a_0(a_1(\cdots(a_{n-1}x_\beta)))$.

If $\prec$ is a linear ordering of the generators, say that q dominates p (with respect to $\prec$) in a variable clash if there are a_i's, x_α, x_β as above with $x_\alpha \prec x_\beta$ (we say that the pair $\langle a_0(a_1(\cdots(a_{n-1}x_\alpha))), a_0(a_1(\cdots(a_{n-1}x_\beta)))\rangle$ witnesses $p \prec q$). Observe that if q dominates p in a variable clash, and $p \leq_{\mathrm{L}} p', q \leq_{\mathrm{l}} q'$, then q' dominates p' in a variable clash. Extend $\prec$ to a relation $\prec$ on $\mathscr{P}_\kappa$ by

$$p \prec q \Leftrightarrow p <_{\mathrm{L}} q \text{ or } q \text{ dominates } p \text{ in a variable clash.}$$

Dehornoy [7] derived from Theorems 1.3 and 1.4 that $\prec$ linearly orders $\mathscr{A}_\kappa$. We indicate the proof. To see, for example, that if $u, v \in \mathscr{A}_\kappa$, then either $u = v$, $u <_{\mathrm{L}} v$, $v <_{\mathrm{L}} u$ or u and v have a variable clash, let u and v be given by representatives (also called u and v) in A_κ. Let $\tilde{u}$ and $\tilde{v}$ be the members of A obtained from u and v by replacing all occurrences of variables by x_0. By the linearity of $<_{\mathrm{L}}$ on $\mathscr{A}$ we have, say, $\tilde{u} \leq_{\mathrm{L}} \tilde{v}$. By Theorem 1.4 there are $r_0, r_1, \ldots, r_n \in A$ with $\tilde{v} \longrightarrow r_0 r_1 \cdots r_n$ and $\tilde{u} \longrightarrow r_0 r_1 \cdots r_i$, where $i = 0$ or n. Applying the same substitutions to u and v yields $v \longrightarrow s_0 s_1 \cdots s_n$, $u \longrightarrow t_0 t_1 \cdots t_i$. If for all $\ell \leq i$, $s_\ell = t_\ell$, then $u \leq_{\mathrm{L}} v$ and we are done. Otherwise for some least ℓ, $s_\ell \neq t_\ell$ (but $\tilde{s}_\ell = \tilde{t}_\ell = r_\ell$). This implies, by Proposition 1.1(v) that there is a variable clash between p and q. A checking of cases then gives transitivity of $\prec$ on $\mathscr{A}_\kappa$, and the irreflexivity of $\prec$ on $\mathscr{A}_\kappa$ is derived from confluence as above using the irreflexivity of $<_{\mathrm{L}}$ on $\mathscr{A}$.

We will check that $\prec$ also linearly orders $\mathscr{P}_\kappa$. This may be proved by deriving (in the manner of Theorem 1.4(i)) a confluence result for $\mathscr{P}_\kappa$ (if $p, q \in P_\kappa$, $p \equiv q$, then for some $r \in P_\kappa$, $p, q \longrightarrow r$, where in the definition of $\longrightarrow$, the rules $(a \circ b) \circ c \leftrightarrow a \circ (b \circ c)$, $(a \circ b)c \leftrightarrow a(bc)$, $a(b \circ c) \longrightarrow (ab \circ ac)$, $a \circ b \longrightarrow ab \circ a$ are allowed) and applying it together with Theorem 1.3. A shorter proof is to derive the result from the linearity of $\prec$ on $\mathscr{A}_\kappa$.

Theorem 1.5. *Given a linear ordering $\prec$ on $\{x_\alpha : \alpha < \kappa\}$, extend it to a relation $\prec$ on $\mathscr{P}_\kappa$ as above. Then $\prec$ linearly orders $\mathscr{P}_\kappa$, extends $<_{\mathrm{L}}$, and if $p, q, r \in \mathscr{P}_\kappa$ with $q \prec r$, then $pq \prec p \circ q \prec pr$ (whence $pq = pr \Leftrightarrow q = r$, $pq \prec pr \Leftrightarrow q \prec r$).*

Proof. Let $\mathscr{A}'_\kappa$ be the free left distributive algebra with generators $\{x_\alpha : \alpha < \kappa\} \cup \{x\}$, where x is a new variable, and let $\prec$ on $\mathscr{A}'_\kappa$ be defined as above from the given ordering on $\{x_\alpha : \alpha < \kappa\}$ together with $x \prec x_\alpha$ (all α).

Lemma 1. *$v \prec w$ in $\mathscr{P}_\kappa \Leftrightarrow wx$ dominates vx in a variable clash in $\mathscr{A}'_\kappa$.*

Proof. Let $v = a_0 \circ \cdots \circ a_n$ with each $a_i \in \mathscr{A}_\kappa$.

($\Rightarrow$) If $v <_{\mathrm{L}} w$, then $w = vv_0 \cdots v_{n-1} * v_n$ for some $v_0, \ldots, v_n \in \mathscr{P}_\kappa$, and, letting $x_\alpha = L(v_0)$, $vx = a_0(a_1(\cdots a_n x))$ and $a_0(a_1(\cdots(a_n x_\alpha))) <_{\mathrm{L}} wx$, and if w dominates v in a variable clash, then wx so dominates vx.

($\Leftarrow$) Suppose for variables $z \prec r$ from $\{x_\alpha : \alpha < \kappa\} \cup \{x\}$ that $s = b_0(b_1(\cdots(b_n z))) \leq_{\mathrm{L}} vx$, $t = b_0(b_1(\cdots(b_n r))) \leq_{\mathrm{L}} wx$.

Then $b_0 \circ b_1 \circ \cdots \circ b_n \leq_{\mathrm{L}} v$; moreover, since $x \prec r$, $t \neq wx$ so $t \leq_{\mathrm{L}} w$. Thus if $s \leq_{\mathrm{L}} v$, s and t witness that $v \prec w$. The other case is where $s = vx$, whence $v = b_0 \circ \cdots \circ b_n <_{\mathrm{L}} b_0(b_1(\cdots(b_n r))) = t \leq_{\mathrm{L}} w$, giving $v \prec w$. □

Lemma 2. *If u, v, w in $\mathscr{P}_\kappa$, $u \prec v \prec w$, then $u \prec w$.*

Proof. By Lemma 1 we have $\langle a_0(a_1(\cdots(a_n j))), a_0(a_1(\cdots(a_n k)))\rangle$ witnessing $ux \prec vx$, and $\langle b_0(b_1(\cdots(b_m \ell))),\ b_0(b_1(\cdots(b_m t)))\rangle$ witnessing $vx \prec wx$. Since x does not occur in u or v, the a_i's, b_i's belong to $\mathscr{A}_\kappa$. To show wx dominates ux in a variable clash, write $\vec{a} = a_0 \circ \cdots \circ a_n$, $\vec{b} = b_0 \circ \cdots \circ b_m$. Since both $\vec{a}k$, $\vec{b}\ell \leq_{\mathrm{L}} vx$, by Theorem 1.4(ii) $\vec{a}k$ and $\vec{b}\ell$ are $\leq_{\mathrm{L}}$-comparable.

Case 1: $\vec{a}k = \vec{b}\ell$. Then $\vec{a} = \vec{b}$ and $\langle \vec{a}j, \vec{a}t\rangle$ witnesses $ux \prec wx$.

Case 2: $\vec{a}k <_{\mathrm{L}} \vec{b}\ell$. Then $\vec{a}k \leq_{\mathrm{L}} \vec{b}$. Thus $\vec{a}k <_{\mathrm{L}} \vec{b}t \leq_{\mathrm{L}} wx$, so $\langle \vec{a}j, \vec{a}k\rangle$ witnesses $ux \prec wx$.

Case 3: $\vec{b}\ell <_{\mathrm{L}} \vec{a}k$. Then similarly $\vec{b}\ell \leq_{\mathrm{L}} \vec{a} <_{\mathrm{L}} \vec{a}j \leq_{\mathrm{L}} ux$, and $\langle \vec{b}\ell, \vec{b}t\rangle$ witnesses $ux \prec wx$. □

Lemma 3. *For $v, w \in \mathscr{P}_\kappa$ exactly one of $v \prec w$, $v = w$, $w \prec v$ holds.*

Proof. By the linearity of $\prec$ on $\mathscr{A}'_\kappa$ either $vx = wx$ or, say, $vx \prec wx$. If $vx = wx$, then $v = w$. If $vx \prec wx$, then either $vx <_{\mathrm{L}} wx$ or wx dominates vx in a variable clash. Since $vx <_{\mathrm{L}} wx$ cannot hold – it implies $vx \leq_{\mathrm{L}} w$ but x does not occur in w – assume $\langle \vec{a}k, \vec{a}\ell\rangle$ witnesses $vx \prec wx$. Since $\ell \neq x$, $\vec{a}\ell \leq_{\mathrm{L}} w$, so if $\vec{a}k \leq_{\mathrm{L}} v$, then $\langle \vec{a}k, \vec{a}\ell\rangle$ witnesses $v \prec w$. The other case is $\vec{a}k = vx$, whence $v = \vec{a} <_{\mathrm{L}} \vec{a}\ell \leq_{\mathrm{L}} w$, so $v <_{\mathrm{L}} w$.

Finally, $\prec$ is irreflexive on $\mathscr{P}_\kappa$: for $p \in \mathscr{P}_\kappa$, $p \not\prec p$ since $px \not\prec px$ in $\mathscr{A}'_\kappa$. Thus at most one of $v \prec w$, $v = w$, $w \prec v$ holds.

This proves the linearity of $\prec$, and the other statements in the theorem are immediate from that and the definition of the ordering. □

The division form of [21, 22] is a way to determine, for $u, v \in \mathscr{P}$, which of $u <_{\mathrm{L}} v$, $u = v$, $v <_{\mathrm{L}} u$ holds, by a type of lexicographic comparison. The remarks about it (from here through the end of this section) are included for completeness and for comparison with the next section, which is a self-contained version of division forms for the case of $\mathscr{P}_\omega$.

Define, for $p \in \mathscr{P}$, a p-normal term to be a product expressed in the form $p_0 p_1 \cdots p_{n-1} * p_n$, where $p_0 = p$, $p_{i+2} \leq_{\mathrm{L}} p_0 p_1 \cdots p_i$ for all i, and if $* = \circ$ and $n \geq 2$ then $p_n <_{\mathrm{L}} p_0 p_1 \cdots p_{n-2}$.

Theorem 1.6 (Laver [21, 22]). (i) *For all $p, u \in \mathscr{P}$, if $p \leq_{\mathrm{L}} u$ then u is representable uniquely as a p-normal term $p_0 \cdots p_{n-1} * p_n$.*
(ii) *Moreover, let (T, ℓ) be the rooted, $\mathscr{P}$-labeled tree such that ℓ (root of T) $= u$, such that $\ell(t) \leq_{\mathrm{L}} p$ implies t is a maximal node of T, and such that $p <_{\mathrm{L}} \ell(t)$ implies, letting $p_0 \cdots p_{n-1} * p_n$ be the p-normal term equalling $\ell(t)$, t's immediate successors are $t_0, \ldots, t_n$ with $\ell(t_i) = p_i$. Then T is finite.*

The uniqueness part relies on irreflexivity. The term for u given by part (ii) (in a language with a symbol for each $q \leq_{\mathrm{L}} p$) is called the p-division form of u.

For $p, q \in \mathscr{P}$ define the (nonnegative) iterates $I_n(p,q)$ of $\langle p, q\rangle$ by $I_0(p,q) = q$, $I_1(p,q) = p$, $I_{k+2}(p,q) = I_{k+1}(p,q) I_k(p,q)$. Writing $I_n(p,q) = I_n$, then $I_{n+1} \circ I_n = p \circ q$ by iterating the law $a \circ b = ab \circ a$.

If $p, u \in \mathscr{P}$, define the p-associated sequence $S_p(u) = S(u)$ of u as follows. If $u \leq_{\mathrm{L}} p$, $S(u) = \langle u \rangle$. If the p-normal product equalling u is $u_0 u_1, \ldots u_n$ (so $u_0 = p$), then $S(u) = \langle u_0, u_1, \ldots, u_n \rangle$. If the p-normal product for u is $u_0 u_1 \cdots u_{n-1} \circ u_n$, then $S(u)$ is the infinite sequence $\langle u_0, u_1, \ldots, u_i, \ldots \rangle$, where for $i > n$, $u_i = u_0 u_1 \cdots u_{i-2}$. That is, for $i \geq n$, $u_i = I_{i-n}(u_0 u_1 \cdots u_{n-1}, u_n)$.

Theorem 1.7 (Laver [21, 22]). *For $p, u, v \in \mathscr{P}$, $u <_{\mathrm{L}} v$ if and only if $S_p(u)$ is lexicographically less than $S_p(v)$.*

ptThat is, $S_p(u)$ is a proper initial segment of $S_p(v)$, or $S_p(u)$ and $S_p(v)$ differ at some first coordinate i and $u_i <_{\mathrm{L}} v_i$. To derive that $<_{\mathrm{L}}$ linearly orders $\mathscr{P}$, let p be the generator x_0 of $\mathscr{P}$. For $u, v \in \mathscr{P}$, whether or not $u <_{\mathrm{L}} v$ is decided by comparing $S(u)$ and $S(v)$, and then if $S(u)$ and $S(v)$ first differ at coordinates u_i, v_i, comparing $S(u_i)$ and $S(v_i)$, etc. One can check that this procedure ends in a finite number of steps.

If $u = p_0 p_1 \cdots p_{n-1} * p_n$ is a p_0-normal term, then it is seen that for each $i < n$, p_{i+1} is the $<_{\mathrm{L}}$ greatest member q of $\mathscr{P}$ with $p_0 \cdots p_i q \leq_{\mathrm{L}} u$ (see e.g. Lemma 2.1(i) below). Theorem 1.6(i) thus implies that a type of division algorithm for $\mathscr{P}$ terminates in a finite number of steps. Namely, if $u <_{\mathrm{L}} v$ let u_0 be greatest with $uu_0 \leq_{\mathrm{L}} v$, and if $uu_0, u \circ u_0 \neq v$ let u_1 be greatest with $uu_0u_1 \leq_{\mathrm{L}} v$, etc. Then for some n, $v = uu_0u_1 \cdots u_n$ or $v = uu_0u_1 \cdots u_{n-1} \circ u_n$.

2.

From here on, $\prec$ is the linear ordering on $\mathscr{P}_\omega$ induced by the ordering $x_0 \succ x_1 \succ x_2 \succ \cdots \succ x_n \succ \cdots$, as in Theorem 1.5.

For $p \in \mathscr{P}_\omega$, a p-normal term in $\mathscr{P}_\omega$ is a term of the form $p_0 p_1 \cdots p_{n-1} * p_n$, where

$$p_0 = p,\ p_{i+2} \preceq p_0 p_1 \cdots p_i \text{ for all } i \le n-2, \text{ and}$$
$$\text{if } * = \circ \text{ and } n \ge 2,\ p_n \prec p_0 p_1 \cdots p_{n-2}$$

A normal term is an x_i-normal term for x_i a generator. We will blur the distinction, when no confusion should arise, between such terms and the members of $\mathscr{P}_\omega$ they represent.

For a p_0-normal term $p_0 p_1 \cdots p_{n-1} * p_n$, define its associated sequence $S(p_0 p_1 \cdots p_{n-1} * p_n)$ to be $\langle p_0, p_1, \ldots, p_n\rangle$ if $* = \cdot$, and if $* = \circ$, to be the infinite sequence $\langle p_0, p_1, \ldots, p_i, \ldots\rangle$ where for all $i > n$, $p_i = p_0 p_1 \cdots p_{i-2}$. If $\langle p_0, p_1, \ldots, p_i\rangle$ is an initial segment of $S(p_0 \cdots p_{n-1} * p_n)$, then $p_0 p_1 \cdots p_i \preceq p_0 p_1 \cdots p_{n-1} * p_n$; in the case $* = \circ$ and $i \ge n$ this follows from $i + 1 - n$ applications of the $a \circ b = ab \circ a$ law.

We have that for any initial segment $\langle p_0, \ldots, p_i\rangle$ of an associated sequence, $p_0 \cdots p_i$ is a p_0-normal term. Note that for $p_0 \in \mathscr{P}$, distinct p_0-normal terms cannot have the same associated sequence: if the sequence is finite, this is immediate, and if it is infinite, say $\langle p_0, p_1, \ldots, p_i \cdots\rangle$, then it equals $S(p_0 p_1 \cdots p_{n-1} \circ p_n)$ where either $n = 1$ or there is an i with $p_i \prec p_0 p_1 \cdots p_{i-2}$ and n is the greatest such i.

If $p_0 \cdots p_{n-1} * p_n$, $q_0 \cdots q_{m-1} * q_m$ are p_0-normal terms (so $p_0 = q_0$) define $p_0 \cdots p_{n-1} * p_n <_{\text{Lex}} q_0 \cdots q_{m-1} * q_m$ if either $S(p_0 \cdots p_{n-1} * p_n)$ is a proper initial segment of $S(q_0 \cdots q_{m-1} * q_m)$ or there is an i with p_i, q_i coordinates of $S(p_0 \cdots p_{n-1} * p_n)$, $S(q_0 \cdots q_{m-1} * q_m)$, respectively, such that $p_j = q_j$ $(j < i)$ and $p_i \prec q_i$.

Lemma 2.1. (i) *If* $p = p_0 \cdots p_{n-1} * p_n$ *is a* p_0*-normal term,* $0 < j \le n$, *and* $p_j \prec q_j$, *then* $p \prec p_0 \cdots p_{j-1} q_j$.
(ii) *If* $p = p_0 \cdots p_{n-1} * p_n$ *and* $q = q_0 \cdots q_{m-1} * q_m$ *are* p_0*-normal terms* (*so* $p_0 = q_0$), *then*

$$p \prec q \Leftrightarrow S(p) <_{\text{Lex}} S(q).$$

Proof. (i) Let $S(p) = \langle p_0, p_1, \ldots\rangle$, finite or infinite. Write $p_i = q_i$ $(i < j)$. We are done if for some r, $p_0 \cdots p_r$ is dominated by $q_0 \cdots q_j$ in a variable clash, so assume that it does not happen. Then in particular $p_j <_{\text{L}} q_j$. We claim that

$$\text{for all } i \ge j, \quad p_0 \cdots p_{i-1} \circ p_i <_{\text{L}} q_0 q_1 \cdots q_j.$$

For the case $i = j$ use $p_j <_{\text{L}} q_j$ and $p_0 \cdots p_{j-1} = q_0 \cdots q_{j-1}$. Suppose $i \ge j$ and the claim is true for i. Then $q_0 \cdots q_j = (p_0 \cdots p_{i-1} \circ p_i) r_0 \cdots r_{t-1} * r_t \ge_{\text{L}} (p_0 \cdots p_{i-1} \circ p_i) r_0 = p_0 \cdots p_{i-1}(p_i r_0) = p_0 \cdots p_i (p_0 \cdots p_{i-1} r_0)$. We have $p_{i+1} \preceq p_0 \cdots p_{i-1}$.

Case 1: p_{i+1} dominated by $p_0 \cdots p_{i-1}$ in a variable clash. Then, as we are assuming cannot happen, $p_0 \cdots p_i p_{i+1}$ is dominated by $p_0 \cdots p_i (p_0 \cdots p_{i-1})$, whence by $q_0 \cdots q_j$, in a variable clash.

Case 2: $p_{i+1} = p_0 \cdots p_{i-1}$. Then $q_0 \cdots q_j \ge_{\text{L}} p_0 \cdots p_i (p_0 \cdots p_{i-1} r_0) = (p_0 \cdots p_i \circ p_{i+1}) r_0 >_{\text{L}} p_0 \cdots p_i \circ p_{i+1}$.

Case 3: $p_{i+1} <_{\mathrm{L}} p_0 \cdots p_{i-1}$. Then $q_0 \cdots q_j >_{\mathrm{L}} p_0 \cdots p_i(p_{i+1}s)$ (for some s) $>_{\mathrm{L}} p_0 \cdots p_i \circ p_{i+1}$.

The claim suffices for part (i) of the lemma, as there is an $i \geq j$ such that $p = p_0 \cdots p_{i-1} * p_i <_{\mathrm{L}} q_0 \cdots q_j$.

(ii) ($\Leftarrow$) Let $S(p) = \langle p_0, p_1, \ldots \rangle$, $S(q) = \langle q_0, q_1, \ldots \rangle$, with $p_0 = q_0$. If $S(p)$ is a proper initial segment of $S(q)$, then $S(p) = \langle p_0, p_1, \ldots, p_\ell \rangle$, $S(q) = \langle p_0, p_1, \ldots, p_\ell, q_{\ell+1} \ldots \rangle$ and $p = p_0 \cdots p_\ell <_{\mathrm{L}} p_0 \cdots p_\ell q_{\ell+1} \leq_{\mathrm{L}} q$. So assume for some least j with $0 < j \leq n$ that $p_j \prec q_j$. Then we are done by part (i).

($\Rightarrow$) Since different normal terms p and q have different associated sequences, $S(p) = S(q)$ implies $p = q$. So we are done by the ($\Leftarrow$) direction and linearity of $\prec$. □

Call a p_0-normal term $p_0 \cdots p_{n-1} * p_n$ normal if p_0 is an x_i.

In the language of $\cdot$ and $\circ$ with a constant symbol for each x_i, define the notion of a division-form term (with respect to $\prec$) inductively as follows: For $n \geq 0$, $p_0 p_1 \cdots p_{n-1} * p_n$ is a division form term iff p_0 is an x_i, $p_1, \ldots, p_n$ are division form terms, and $p_0 p_1 \cdots p_{n-1} * p_n$ is normal. Let $DF = \{p \in \mathscr{P}_\omega : p$ has a representation as a division form term$\}$. By Lemma 2.1 the representation is unique. If $p, q \in DF$, then by Lemma 2.1 the question whether $p \prec q$, $p = q$ or $q \prec p$ is determined by a lexicographic comparison of the division form terms representing p and q.

We define the notion of "decreasing division form" mentioned in the introduction. *DDF* consists of those members p of *DF* such that every component ab or $a \circ b$ of the *DF* term representing p satisfies $b \prec a$. Equivalently, call a normal term $p_0 \cdots p_{n-1} * p_n$ decreasing normal if, in the definition of normal, additionally $p_1 \prec p_0$, and define a *DDF* term as in the preceding paragraph, replacing "normal" by "decreasing normal". So a *DDF* term is either an x_i or a term of the form $p_0 p_1 \cdots p_{n-1} * p_n$ for some $n > 0$, where p_0 is an x_i, $p_1 \prec p_0$, $p_{i+2} \preceq p_0 \cdots p_i$, $p_n \prec p_0 \cdots p_{n-2}$ if $n \geq 2$ and $* = \circ$, and each p_i is a *DDF* term. Then $DDF = \{p \in \mathscr{P}_\omega : p$ has a representation as a decreasing division form term$\}$.

Similarly define *p-DF* and *p-DDF* for $p \in \mathscr{P}_\omega$ as follows. We want the *p-DF*, *p-DDF* terms r to have first coordinate p if $p \leq_{\mathrm{L}} r$; otherwise the first coordinate will be an x_i. So define, for $q \in \mathscr{P}_\omega$, a normal term for q with respect to p to be either a p-normal term $q = pp_1 \cdots p_{n-1} * p_n$, or a normal term $q = x_i u_1 \cdots u_{m-1} * u_m$ where $p \not\leq_{\mathrm{L}} q$. Then the notion of a p-division form (*p-DF*) term, in the language with constant symbols for the variables and a constant symbol for p, is obtained hereditarily from the notion of a normal term for q with respect to p, in the same way that the notion of a *DF*-term is obtained from the notion of a normal term. Let $p\text{-}DF = \{q : q$ has a representation as a *p-DF* term$\}$. Similarly define a decreasing normal term for q with respect to p, a p-decreasing division form (*p-DDF*) term, and *p-DDF*. Then if p is an x_n, $p\text{-}DF = DF$, $p\text{-}DDF = DDF$.

So there are two types of sequences used in building up *p-DF* terms. The next lemma expresses how to lexicographically compare two such terms $u = u_0 u_1 \cdots u_{n-1} * u_n$ and $v = v_0 v_1 \cdots v_{m-1} * v_m$ to determine whether $u \prec v$.

Lemma 2.2. (i) *If* $u_0 = v_0$, *then* $u \prec v$ *is determined as in Lemma* 2.1.
(ii) *If* $u_0 = x_n$, $v_0 = x_m$ $(n \neq m)$, *then* $u \prec v$ *if and only if* $n > m$.
(iii) *If* $u_0 = x_n$, $v_0 = p$, *and* $x_n \neq p$ (*whence* $u \not\geq_{\mathrm{L}} p$), *then* $u \prec v$ *if and only if* $u \prec p$.

Proof. (i) and (ii) are immediate. For (iii), if $u \prec p$, then since $u \not\geq_{\mathrm{L}} p$, p dominates u in a variable clash, thus v dominates u in a variable clash, so $u \prec v$.

For $p \in \mathscr{P}_\omega$, define $\mathrm{Var}(p) = \{x_n : x_n \text{ occurs in } p\}$.

Lemma 2.3. (i) *If* $p \in DDF$, $L(p) = x_n$, *then* $\mathrm{Var}(p) \subset \{x_m : m \geq n\}$.
(ii) *If* $p \in DDF$, $x_m \succ p$, *then* $\mathrm{Var}(p) \subset \{x_k : k > m\}$.
(iii) *If* $q \in p$-*DDF*, *then every proper subterm of the p-DDF term representing* q *is* $\prec q$.

Proof. We have that (i) implies (ii), since for $L(p) = x_n$ we must have $n > m$.

(i) is proved by induction on *DDF* terms; suppose (i) is true for all subterms of $p = p_0 p_1 \cdots p_{i-1} * p_i$, where $p_0 = x_n$. Since $x_n \succ p_1$, $x_n \succ L(p_1)$, and since for $i \geq 2$, $p_i \preceq p_0 \cdots p_{i-2}$, $L(p_i) \preceq x_n$; done by induction.

For (iii) (by induction on *p-DDF* terms) if $n > 0$ and $q = p_0 p_1 \cdots p_{n-1} * p_n$, then $p_0 p_1 \cdots p_{n-1} \prec q$, and if $n = 1$, then $p_n \prec p_0 \prec q$, and if $n > 1$, then $p_n \preceq p_0 \cdots p_{n-2} \prec q$. □

Theorem 2.4. *Suppose* $a, b \in \{x_n : n < \omega\}$, $a \succ b$. *Then if* $p \in DDF$, *then* $p \in (a \circ b) - DDF$.

Proof. The method is similar to those in [21, 22]. Let $|q|$ (respectively $|q|^{a\circ b}$) be the *DDF*-term (respectively, the $a \circ b$-*DDF* term) representing q, if one exists. Recall that an $a \circ b$-*DDF* term $p_0 p_1 \cdots p_{i-1} * p_i$ is either a decreasing $(a \circ b)$-normal term (so $p_0 = (a \circ b)$) or a decreasing normal term (so p_0 is an x_j), where in the latter case, $x_j p_1 \cdots p_{i-1} * p_i \not\geq_{\mathrm{L}} a \circ b$. Technically speaking, $a \circ b$ is either a normal-*DDF* term of length 2 or an $(a \circ b)$-*DDF* term of length 1; no problems will arise by identifying these two terms.

If $p = p_0 \cdots p_n$ and q are $(a \circ b)$-*DDF* terms define $q \ll p$ if either $n = 0$ and $q \prec p_0$, or $n > 0$ and $q \preceq p_0 \cdots p_{n-1}$.

Lemma 1. *If* p, q *are* $(a \circ b)$-*DDF terms, then* $q \ll p$ *iff the term* pq *is an* $(a \circ b)$-*DDF term. Moreover,* $q \ll p$ *implies* $pq \gg p$ *and* $|p \circ q|^{a\circ b}$ *exists.*

Proof. If p is the $(a \circ b)$-normal term $(a \circ b) p_1 \cdots p_{n-1} p_n$, then clearly $|pq|^{a\circ b} = pq \gg p$. Writing $q = p_{n+1}$, we have that $|(p \circ q)|^{a\circ b} = (a \circ b) p_1 \cdots p_{i-1} \circ p_i$, where $i \leq n + 1$ is greatest such that $p_i \prec (a \circ b) p_1 \cdots p_{i-2}$ ($i = 1$ if no i satisfies that condition).

If $p = x_k q_1 \cdots q_n$ the same statements obtain, where it is checked that in exactly the case $x_k = q_0 = a$, $q_1 = b$, $q_i = q_0 \cdots q_{i-2}$ for $2 \leq i \leq n+1$, $q_{n+1} = q$, that $|p \circ q|^{a \circ b} = a \circ b$; otherwise $|p \circ q|^{a \circ b} \not\geq_{\mathrm{L}} a \circ b$. This proves the lemma. $\square$

Definition. For $p, q \in (a \circ b)$-*DDF* define a relation $p \sqsupset q$, by induction first on the $(a \circ b)$-*DDF* term for p, then on the $(a \circ b)$-*DDF* term for q ($p \sqsupset q$ will guarantee that $|pq|^{a \circ b}$ and $|p \circ q|^{a \circ b}$ exist).

(a) If $p = a \circ b$ or p is an x_i, then $p \sqsupset q$ if and only if $p \succ q$.

(b) If $p = p_0 p_1 \cdots p_n$ for $n > 0$, then $p \sqsupset q$ if and only if either $q \ll p$, or $q = p_0 \cdots p_{n-1} r_n \cdots r_{k-1} * r_k$ (possibly $k = n$), where $p_n \sqsupset r_n$ and $p_n \circ r_n \ll p_0 \cdots p_{n-1}$.

(c) If $p = p_0 p_1 \cdots p_{n-1} \circ p_n$, then $p \sqsupset q$ if and only if $p_n \sqsupset q$ and $p_n \circ q \ll p_0 \cdots p_{n-1}$.

Lemma 2. *For* $p, q, s \in (a \circ b)$-*DDF*

(i) $q \ll p$ *implies* $p \sqsupset q$.

(ii) $p \sqsupset q$ *implies* $p \succ q$.

(iii) $p \sqsupset q \succeq s$ *implies* $p \sqsupset s$.

Proof. (i) is by definition. (ii) and (iii) are proved by induction on p. For (ii), in the second clause of part (b) of the definition of $p \sqsupset q$, $p_n \succ r_n$ holds by induction. And in part (c) of the definition $p_n \succ q$ holds by induction and $p \succ p_n$ holds by Lemma 2.3(iii). And for (iii), in the second part of clause (b), if $s = p_0 \cdots p_{n-1} s_n s_{n+1} \cdots s_{t-1} * s_t$ with $s_n \prec r_n$, then by induction $p_n \sqsupset s_n$, and $p_n \circ s_n \prec p_n \circ r_n \ll p_0 \cdots p_{n-1}$. $\square$

Lemma 3. *If* $p, q \in (a \circ b)$-*DDF*, $p \sqsupset q$, *then* $|pq|^{a \circ b}$, $|p \circ q|^{a \circ b}$ *exist and* $pq \sqsupset p$.

Proof. (*By induction first on* p, *then on* q)

Case 1: $p = (a \circ b)$ or p is an x_k. This is by definition, as in Lemma 1.

Case 2: $p = u_0 \cdots u_n$. Then if $q \ll p$, we are done as in Lemma 1. So assume $q = u_0 \cdots u_{n-1} v_n \cdots v_{k-1} * v_k$, as in part (ii) of the definition of $\sqsupset$. Suppose $k > n$. Since $u_n \sqsupset v_n$, by the induction hypothesis on p, $|u_n \circ v_n|^{a \circ b}$ exists, and for each v_i, $v_i \prec q$ by Lemma 2.3(iii), so $p \sqsupset v_i$ by Lemma 2, so $|pv_i|^{a \circ b}$ exists by the induction hypothesis on q. Thus

$$|pq|^{a \circ b} = u_0 \cdots u_{n-1} |u_n \circ v_n|^{a \circ b} v_{n+1} |pv_{n+2}|^{a \circ b} \cdots |pv_{k-1}|^{a \circ b} * |pv_k|^{a \circ b}$$

with, in the case $* = \circ$, $pv_k \prec p(u_0 u_1 \cdots v_n \cdots v_{k-2}) = u_0 u_1 \cdots u_{k-1}(u_n \circ v_n) v_{n+1}(pv_{n+2}) \cdots (pv_{k-2})$ by the second part of Theorem 1.5. If $* = \cdot$, $|pq|^{a \circ b} \sqsupset p$ is clear. If $* = \circ$, we have $pv_k \sqsupset p$ by the induction hypothesis on p and $pv_k \circ p = p \circ v_k \ll u_0 \cdots u_{n-1}(u_n \circ v_n) v_{n+1}(pv_{n+2}) \cdots (pv_{k-1})$, by the last clause of Theorem 1.5. Finally when $* = \circ$, $|p \circ q|^{a \circ b} = |pq \circ p|^{a \circ b} = u_0 u_1 \cdots u_{n-1} |u_n \circ v_n|^{a \circ b} \cdots |pv_{k-1}|^{a \circ b} \circ |p \circ v_k|^{a \circ b}$, and if $* = \cdot$, $p \prec u_0 \cdots u_{n-1}(u_n \circ v_n) \cdots (pv_{k-1})$, so $|p \circ q|^{a \circ b} = |pq|^{a \circ b} \circ p$. The case $k = n$ is similarly checked.

Case 3: $p = u_0 \cdots u_{k-1} \circ u_k$. Then $|u_k q|^{a\circ b}$ and $|u_k \circ q|^{a\circ b}$ exist by induction, $u_k \circ q \ll u_0 \cdots u_{k-1}$, so $|pq|^{a\circ b} = u_0 \cdots u_{k-1}|u_k q|^{a\circ b}$. For $|pq|^{a\circ b} \sqsupset p$ we have $|u_k q|^{a\circ b} \sqsupset u_k$ by induction and $u_k q \circ u_k = u_k \circ q \ll u_0 \cdots u_{k-1}$, as desired, and $|p \circ q|^{a\circ b} = u_0 \cdots u_{k-1} \circ |u_k \circ q|^{a\circ b}$, with similar verifications. □

Lemma 4. *Suppose $u \in DDF$ and $a \succ u$. Then $|au|^{a\circ b}$ exists and $|au|^{a\circ b} \sqsupset a$.*

Proof. (*By induction on u*). If u' is a component of u, then $u \succ u'$ by Lemma 2.3(iii), so $a \succ u'$ and the lemma is true for a and u'. We check the main case $u = b\ell_0 \cdots \ell_{t-1} \circ \ell_t$. Then $|au|^{a\circ b} = (a\circ b)\ell_0|a\ell_1|^{a\circ b} \cdots |a\ell_{t-1}|^{a\circ b} \circ |a\ell_t|^{a\circ b}$, an $(a\circ b)$-normal term, each $|a\ell_i|^{a\circ b}$ existing by induction. To see $|au|^{a\circ b} \sqsupset a$, we have $|a\ell_t|^{a\circ b} \sqsupset a$ by induction and $a\ell_t \circ a = a \circ \ell_t \preceq a(b\ell_0 \cdots \ell_{t-1}) = (a \circ b)\ell_0(a\ell_1)\cdots(a\ell_{t-2})$, as desired. □

For the theorem, we show by induction on DDF-terms p that $|p|^{a\circ b}$ exists. If $L(p) \neq a$, i.e., $p = x_n u_0 \cdots u_{m-1} * u_m$ with $x_n \neq a$, then by induction $|p|^{a\circ b} = x_n|u_0|^{a\circ b} \cdots |u_{m-1}|^{a\circ b} * |u_m|^{a\circ b}$. Similarly if $p = au_0 \cdots u_{m-1} * u_m$ but u_0 is not of the form $bv_0 \cdots v_{k-1} * v_k$ for some $k \geq 0$, we are done by induction. And $|a(bv_0 \cdots v_k)c_0 \cdots c_{r-1} * c_r|^{a\circ b} = (a\circ b)|v_0|^{a\circ b}|av_1|^{a\circ b} \cdots |av_k|^{a\circ b}|c_0|^{a\circ b} \cdots |c_{r-1}|^{a\circ b} * |c_r|^{a\circ b}$. So we are left with the cases where p has one of the forms $a * (b \circ u)$, $a(b \circ u)c_0 \cdots c_{k-1} * c_k$, $a * (bu_0 \cdots u_{n-1} \circ u_n)$, $a(bu_0 \cdots u_{n-1} \circ u_n)c_0 \cdots c_{k-1} * c_k$. We look at the cases requiring the lemmas and leave the others to the reader.

For $p = a(b \circ u)c_0 \cdots c_{k-1} * c_k$, we have $|a(b \circ u)|^{a\circ b} = (a \circ b)|u|^{a\circ b} \circ ab$. We claim $((a \circ b)|u|^{a\circ b} \circ ab) \sqsupset c_0$. Since $c_0 \preceq a$ it suffices by Lemma 2(ii) to show $((a \circ b)|u|^{a\circ b} \circ ab) \sqsupset a$. We have $ab \sqsupset a$ and $ab \circ a = a \circ b \ll (a \circ b)|u|^{a\circ b}$, as desired. Thus $|a(b \circ u)|^{a\circ b} \sqsupset c_0$ so by Lemma 3 $|a(b \circ u)c_0|^{a\circ b}$ exists and is $\sqsupset a(b \circ u) \succeq c_1$. Iterating Lemma 2(ii) and Lemma 3 k times in this manner yields that $|p|^{a\circ b}$ exists.

For $p = a(bu_0 \cdots u_{n-1} \circ u_n)c_0 \cdots c_{k-1} * c_k$, we have $r = a(bu_0 \cdots u_{n-1} \circ u_n) = (a \circ b)u_0(au_1)\cdots(au_{n-1}) \circ (au_n)$ and claim that $|r|^{a\circ b} \sqsupset c_0$. By Lemma 3, $|au_n|^{a\circ b} \sqsupset a \succeq c_0$, so $|au_n|^{a\circ b} \sqsupset c_0$ and $au_n \circ c_0 \preceq au_n \circ a = a \circ u_n \preceq a(bu_0 \cdots u_{n-2}) = (a \circ b)u_0(au_1)\cdots(au_{n-2})$. This proves the claim and finishes the theorem by iterating Lemmas 2(ii) and 3 as in the previous case. □

For $i = 1, 2, \ldots,$ σ_i the ith generator of B_∞, define

$$(x_{i-1})^{\sigma_i} = x_{i-1}x_i, \qquad (x_i)^{\sigma_i} = x_{i-1},$$
$$(x_k)^{\sigma_i} = x_k \quad (k \neq i-1, i).$$

Then because the x_i's are free generators of $\mathscr{P}_\omega$, this map extends to a map $u \to u^{\sigma_i}$ from $\mathscr{P}_\omega$ to $\mathscr{P}_\omega$.

Theorem 2.5. *For $p, q \in DDF$, $i = 1, 2, \ldots$*

(i) $p \prec q \Leftrightarrow p^{\sigma_i} \prec q^{\sigma_i}$.

(ii) $p \preceq p^{\sigma_i}$.

Proof. Let $a = x_{i-1}$, $b = x_i$, so $(a \circ b)^{\sigma_i} = a \circ b$. By Theorem 2.4, it suffices to prove (i) and (ii) for all $p, q \in (a \circ b)$-*DDF*.

For (i) we show by induction on $p \in (a \circ b)$-*DDF* that for all $q \in (a \circ b)$-*DDF*, $p \prec q \Rightarrow p^{\sigma_i} \prec q^{\sigma_i}$ (the ($\Leftarrow$) direction then follows by linearity of $\prec$).

Let p be $p_0 p_1 \cdots p_{n-1} * p_n$ in $(a \circ b)$-*DDF*, where p_0 is either $a \circ b$, some generator e different from a and b, b, or a, and $p^{\sigma_i} = p_0^{\sigma_i} p_1^{\sigma_i} \cdots p_{n-1}^{\sigma_i} * p_n^{\sigma_i}$ is a $p_0^{\sigma_i}$-decreasing normal sequence by the induction hypothesis.

Now suppose $p \prec q_0 \cdots q_{k-1} * q_k$, the $a \circ b$-*DDF* term for q; to show $p^{\sigma_i} \prec q^{\sigma_i}$. If $p_0 = q_0$, let $j \le n$ be least such that $p_j \prec$ the jth member q_j of q's associated sequence. Then $p_\ell^{\sigma_i} = q_\ell^{\sigma_i}$, $\ell < j$, and $p_j^{\sigma_i} \prec q_j^{\sigma_i}$ by induction, so by Lemma 2.1(i) $p^{\sigma_i} \prec q^{\sigma_i}$.

So assume $p_0 \ne q_0$. We check the cases $p_0 = b$ and q_0 is a or $a \circ b$, $p_0 = a$ and $q_0 = a \circ b$; the other cases are either impossible or are cases where p^{σ_i} is dominated by q^{σ_i} in a variable clash. In the $p_0 = b$ case (with $n \ge 1$), $p_1 \prec p_0$ so $L(p_1)$ is a generator $c \prec b$, and we are done by a variable clash here as well.

We claim that if $p_0 = a$, then $p \prec p^{\sigma_i} \prec a \circ b$, which will prove the last case $p_0 = a$, $q_0 = a \circ b$. Note that $p_1 \preceq b$ lest $a \circ b <_{\mathrm{L}} p$. Thus $p^{\sigma_i} = abp_1^{\sigma_i} \cdots p_{n-1}^{\sigma_i} * p_n^{\sigma_i}$ is, by that fact and the induction hypothesis, an a-decreasing normal term (i.e., of length $n+2$). Since $p_0 = a$ the condition $n = 1$, $p_1 = b$ and $* = \circ$ is disallowed, whence Lemma 2.1(i) gives $p^{\sigma_i} \prec a \circ b$. To show $p \prec p^{\sigma_i}$, we have $L(p_1) \preceq b$. If $L(p_1) \prec b$, then we are done by a variable clash. If $L(p_1) = b$, then $p_1 = b$ (otherwise $p_1 = bs_0 \cdots s_{n-1} * s_n$ and $a \circ b \le_{\mathrm{L}} p$). Then

$$p = abp_2 p_3 \cdots p_{n-1} * p_n,$$

$$p^{\sigma_i} = abap_2^{\sigma_i} p_3^{\sigma_i} \cdots p_{n-1}^{\sigma_i} * p_n^{\sigma_i},$$

Let $v_0 = a$, $v_1 = b$, $v_{j+2} = v_0 v_1 \cdots v_j$, so for $j > 1$, $v_j = I_{j-1}(a,b)$. Then by induction on j, $(v_0 \cdots v_j)^{\sigma_i} = v_0 \cdots v_{j+1}$. If for every $j \le n$, $p_j = v_j$, then $* \ne \circ$ (lest $p = a \circ b$), so $p = v_0 \cdots v_n \prec v_0 \cdots v_n v_{n+1} = p^{\sigma_i}$. Finally, if for some least j, $p_j \prec v_j$ (note $j \ge 2$), then $p^{\sigma_i} \ge_{\mathrm{L}} (p_0 \cdots p_{j-1})^{\sigma_i} = (v_0 \cdots v_{j-1})^{\sigma_i} = v_0 \cdots v_{j-1} v_j$, which is $\succ p$ by Lemma 2.1(i). This proves (i).

For (ii), we prove $p \preceq p^{\sigma_i}$ by induction on $p \in (a \circ b)$-*DDF*. Writing p as in part (i), if $p_0 = a \circ b$ or p_0 is a generator different from a and b, $p \preceq p^{\sigma_i}$ by the induction hypothesis and Lemma 2.1(i). If $p_0 = b$, then p^{σ_i} dominates p in a variable clash, and for the case $p_0 = a$, $p \prec p^{\sigma_i}$ was proved in part (i). □

Theorem 2.6. *If $p \in DDF$, then for all $i \ge 1$, $(p)^{\sigma_i} \in DDF$.*

Proof. First note that the definitions and lemmas about $(a \circ b)$-*DDF* in Theorem 2.4 apply to the simpler situation of *DDF* as well. Namely, for $p \in DDF$ write $|p|$ for the *DDF* representation of p, and let, for $p, q \in DDF$, $q \ll p$ if either p is an x_k and $q \prec p$ or $|p| = p_0 p_1 \cdots p_n$ for some $n > 0$ and $q \preceq p_0 \cdots p_{n-1}$ and let $p \sqsupset q$

$(p, q \in DDF)$ hold if one of the following holds:
(i) $p \gg q$.
(ii) $|p| = p_0 p_1 \cdots p_n$, $|q| = p_0 p_1 \cdots p_{n-1} q_n \cdots q_{k-1} * q_k$, with $p_n \sqsupset q_n$ and $(p_n \circ q_n) \ll p_0 \cdots p_{n-1}$.
(iii) $|p| = p_0 p_1 \cdots p_{n-1} \circ p_n$, $p_n \sqsupset q$, $p_n \circ q \ll p_0 p_1 \cdots p_{n-1}$.
Then, as before, if $p, q, s \in DDF$, $p \sqsupset q \succ s$, then $p \sqsupset s$, and $p \sqsupset q$ implies that pq, $p \circ q \in DDF$ and $pq \sqsupset p$.

Lemma. *If $p \in DDF$, $p \prec x_k x_{k+1}$, then $p \sqsubset x_k x_{k+1}$.*

Proof. If $p \preceq x_k$, then $p \ll x_k x_{k+1}$. The other case is $p = x_k r_0 \cdots r_{n-1} * r_n$, with $r_0 \prec x_{k+1}$; then $r_0 \sqsubset x_{k+1}$ and $(x_{k+1} \circ r_0) \ll x_k$. □

Fix i in the theorem, and let $a = x_{i-1}$, $b = x_i$.

We prove by induction on $p \in DDF$ that $(p)^{\sigma_i} \in DDF$. If p is an x_k we are done, so let $|p| = p_0 p_1 \cdots p_{n-1} * p_n$, for $n > 0$. If p_0 is any variable other than a, then by the induction hypothesis and Theorem 2.5(i), $|p^{\sigma_i}| = |p_0^{\sigma_i}| \cdots |p_{n-1}^{\sigma_i}| * |p_n^{\sigma_i}|$.

So suppose $p_0 = a$, then

$$(p)^{\sigma_i} = ab(p_1)^{\sigma_i} \cdots (p_{n-1})^{\sigma_i} * (p_n)^{\sigma_i} \qquad (*)$$

where by Theorem 2.5(i) the sequence $(ab)(p_1)^{\sigma_i} \cdots (p_{n-1})^{\sigma_i} * (p_n)^{\sigma_i}$ is (ab)-decreasing normal. We have $L(p_1) \preceq b$; if $L(p_1) \prec b$, then by Lemma 2.3(ii), $(p_1)^{\sigma_i} \prec a$ so the sequence $(*)$ is a-decreasing normal, as desired.

So assume $p_1 = bt_1 \cdots t_{m-1} * t_m$, then $|p_1^{\sigma_i}| = a|t_1^{\sigma_i}| \cdots |t_{m-1}^{\sigma_i}| * |t_m^{\sigma_i}|$. Since $t_1 \prec b$, Lemma 2.3(ii) gives $t_1^{\sigma_i} \prec b$, whence $p_1^{\sigma_i} \prec ab$. By the lemma, then, $ab \sqsupset (p_1)^{\sigma_i}$.

Thus the statement which immediately preceeds the lemma may be iterated n times on the expression $(*)$, to obtain that $p^{\sigma_i} \in DDF$. □

Theorem 2.7. *The maps $u \to u^{\sigma_i}$, restricted to DDF, induce a partial group action of B_∞ on DDF.*

Proof. We have that $x_k^{\sigma_i \sigma_{i+1} \sigma_i}$ and $x_k^{\sigma_{i+1} \sigma_i \sigma_{i+1}}$ equal

$x_k(x_{k+1}x_{k+2})$	$(k = i-1)$
$x_{k-1}x_k$	$(k = i)$
x_{k-2}	$(k = i+1)$
x_k	(otherwise)

and for $j > i+1$, $x_k^{\sigma_i \sigma_j}$ and $x_k^{\sigma_j \sigma_i}$ are

$x_k^{\sigma_i}$	$(k = i-1, i)$
$x_k^{\sigma_j}$	$(k = j-1, j)$
x_k	(otherwise)

By Theorem 2.5(i) the maps $u \to u^{\sigma_i^{-1}}$, restricted to DDF, are one-to-one. Let w be a braid word $\sigma_{i_0}^{\pm 1} \sigma_{i_1}^{\pm 1} \cdots \sigma_{i_m}^{\pm 1}$. Define the domain of w to be the set of $d \in$

DDF such that for each $j \leq m$, $(((d)^{\sigma_{i_0}^{\pm 1}})^{\sigma_{i_1}^{\pm 1}} \cdots)^{\sigma_{i_j}^{\pm 1}}$ exists and lies in DDF. And for $d \in$ domain w write $d^w = (((d)^{\sigma_{i_0}^{\pm 1}}) \cdots)^{\sigma_{i_m}^{\pm 1}}$. We need to check that if w and w' are equivalent braid words, $d \in \mathit{domain}\, w \cap \mathit{domain}\, w'$, then $d^w = d^{w'}$. It suffices to show there is a derivation of the equivalence of w and w', with $d \in \operatorname{dom} w''$ for every intermediate word w'' in the derivation. This follows from Garside [14]. Namely, let $w \xrightarrow{*} v$ mean that v can be obtained from w via applications of the rewriting rules $\sigma_i^{-1}\sigma_i \xrightarrow{*} \emptyset$, $\sigma_i\sigma_i^{-1} \xleftrightarrow{*} \emptyset$, $\sigma_i\sigma_j \xleftrightarrow{*} \sigma_j\sigma_i$ $(i > j+1)$, and $\sigma_i\sigma_{i+1}\sigma_i \xleftrightarrow{*} \sigma_{i+1}\sigma_i\sigma_{i+1}$. Note that, by Theorems 2.5(i) and 2.6, if $w \xrightarrow{*} v$, then domain $w \subseteq$ domain v. So it suffices to show that if w and w' are equivalent, then there is a v with $w \xrightarrow{*} v$, $w' \xrightarrow{*} v$. Garside defines $\Delta_n = \sigma_1(\sigma_2\sigma_1)(\sigma_3\sigma_2\sigma_1)\cdots(\sigma_{n-1}\cdots\sigma_3\sigma_2\sigma_1)$, and shows for $i < n$ that $\sigma_i\Delta_n \xleftrightarrow{*} \Delta_n\sigma_{n-i}$, $\sigma_i^{-1}\Delta_n \xrightarrow{*} \Delta_n\sigma_{n-i}^{-1}$, and $\sigma_i \xrightarrow{*} \Delta_n c$ for some negative braid word c (i.e., a word in $\{\sigma_m^{-1} : 1 \leq m < n\}$). He then derives that for w equivalent to w' there is a v (of the form dc, d a positive word, c a negative word) with $w \xrightarrow{*} v$, $w' \xrightarrow{*} v$, as desired. □

3.

We recall the definitions [6] of the linear ordering $<$ on B_∞. Let $\mathscr{C}$ be a left distributive (or Σ) algebra. Let $\mathscr{C}^\omega$ be the set of sequences $\vec{c} = \langle c_0, c_1, \ldots, c_n, \ldots\rangle$ from $\mathscr{C}$. Then the action of a braid generator on $\mathscr{C}^\omega$,

$$\langle c_0, \ldots, c_{i-1}, c_i, \ldots, c_n, \ldots\rangle^{\sigma_i} = \langle c_0, \ldots, c_{i-1}c_i, c_{i-1}, \ldots, c_n, \ldots\rangle$$

extends, when $\mathscr{C}$ satisfies left cancellation, to a partial action of B_∞ on $\mathscr{C}^\omega$ (again, Garside's result is used in seeing that $\vec{c}^\alpha$, when defined, is unique). We use the same notation $\vec{c}^\alpha, p^\alpha$ for this action and the one defined in the last section; since they are on different sets, no confusion should arise.

Define for $\vec{c}, \vec{d} \in \mathscr{C}^\omega$, $\vec{c} <_{\text{Lex}} \vec{d}$ if there is an i with $c_i \neq d_i$, and for the least such i, $c_i <_{\text{L}} d_i$.

Theorem 3.1 (Dehornoy [6]). *Let $\mathscr{C}$ be an $\mathscr{A}_\kappa$ or $\mathscr{P}_\kappa$.*

(i) *For any $\alpha_0, \ldots, \alpha_n \in B_\infty$ there is a $\vec{c} \in \mathscr{C}^\omega$ such that for all $i \leq n$, $(\vec{c})^{\alpha_i}$ exists.*

(ii) *Define $\alpha < \beta \Leftrightarrow$ for some/any $\vec{c}$ such that $\vec{c}^\alpha$ and $\vec{c}^\beta$ exist, $\vec{c}^\alpha <_{\text{Lex}} \vec{c}^\beta$; then $<$ is a linear ordering on B_∞ (which is independent of $\mathscr{C}$).*

(iii) *$<$ is the unique linear ordering on B_∞ such that for all $\alpha, \beta, \gamma \in B_\infty$, $\beta < \gamma \Leftrightarrow \alpha\beta < \alpha\gamma$, and such that $\sigma_i\alpha > \beta$ if α and β are in the algebra generated by $\{\sigma_j : j > i\}$.*

(iv) *$\beta < \gamma \Leftrightarrow \beta^{-1}\gamma > \varepsilon$, where $\alpha > \varepsilon \Leftrightarrow \alpha$ can be expressed by a braid word in which the generator with least subscript occurs only positively.*

Part (iv) is implicit in the construction in [6, Lemma 7.1].

We will work with the case $\mathscr{C} = \mathscr{P}_\omega$. Let $\vec{x} = \langle x_0, x_1, \ldots, x_n, \ldots\rangle$ be the sequence of generators of $\mathscr{P}_\omega$. For $\alpha \in B_\infty$, $\vec{p} \in (\mathscr{P}_\omega)^\omega$ such that $(\vec{p})^\alpha$ exists, let $((\vec{p})^\alpha)_k$ be the kth coordinate of $(\vec{p})^\alpha$. Let Rev : $B_\infty \to B_\infty$ be the reversing antiautomorphism: $\mathrm{Rev}(\sigma_i^{\pm 1}) = \sigma_i^{\pm 1}$, $\mathrm{Rev}(\beta\gamma) = (\mathrm{Rev}\,\gamma)(\mathrm{Rev}\,\beta)$.

The following was also noted, for the case of the action of B_∞ on the free group under conjugation, in Larue [19].

Lemma 3.2. *If $\alpha \in B_\infty^+$, then for all k, $((\vec{x})^\alpha)_k = (x_k)^{\mathrm{Rev}\,\alpha}$.*

Proof. The lemma holds if α is a σ_i. Suppose $\alpha = \beta\sigma_i$ where $\beta \in B_\infty^+$ and the lemma holds for β. Then $(\vec{x})^\alpha = ((\vec{x})^\beta)^{\sigma_i} = \langle x_0^{\mathrm{Rev}\,\beta}, x_1^{\mathrm{Rev}\,\beta}, \ldots\rangle^{\sigma_i} = \langle x_0^{\mathrm{Rev}\,\beta}, \ldots, x_{i-2}^{\mathrm{Rev}\,\beta}, x_{i-1}^{\mathrm{Rev}\,\beta} x_i^{\mathrm{Rev}\,\beta}, x_{i-1}^{\mathrm{Rev}\,\beta}, x_{i+1}^{\mathrm{Rev}\,\beta}, \ldots\rangle$. If $n \neq i-1, i$, then $x_n^{\mathrm{Rev}\,\beta} = x_n^{\sigma_i \mathrm{Rev}\,\beta} = x_n^{\mathrm{Rev}\,\alpha}$, and $x_{i-1}^{\mathrm{Rev}\,\beta} x_i^{\mathrm{Rev}\,\beta} = (x_{i-1}x_i)^{\mathrm{Rev}\,\beta} = x_{i-1}^{\sigma_i \mathrm{Rev}\,\beta} = x_{i-1}^{\mathrm{Rev}\,\alpha}$. Finally, $x_{i-1}^{\mathrm{Rev}\,\beta} = x_i^{\sigma_i \mathrm{Rev}\,\beta} = x_i^{\mathrm{Rev}\,\alpha}$. $\square$

The proof works for any $\alpha \in B_\infty$ such that $(\vec{x})^\alpha$ exists, but this improvement is vacuous by the following result due to Larue.

Theorem 3.3 (Larue [20]). *For $2 \le N \le \infty$, $\alpha \in B_N$, $\langle x_i : i < N\rangle$ the sequence of generators of $\mathscr{P}_N$, $\langle x_i : i < N\rangle^\alpha$ exists if and only if $\alpha \in B_N^+$.*

The faithfulness of the action of B_∞ on $(\mathscr{C})^\omega$ follows from Theorem 3.1(i) and (ii). We derive the faithfulness of the action of B_∞ on DDF.

Theorem 3.4. *If $\alpha, \beta \in B_\infty$, $\alpha \neq \beta$, then for some $d \in DDF$, $d^\alpha \neq d^\beta$.*

Proof. We have $\mathrm{Rev}\,\alpha \neq \mathrm{Rev}\,\beta$. Let m be such that $\alpha, \beta \in B_m$. Let $\Delta = \Delta_m (= \mathrm{Rev}\,\Delta_m$ [14]). Then pick n sufficiently large so that $\mathrm{Rev}\,\alpha \cdot \Delta^n$, $\mathrm{Rev}\,\beta \cdot \Delta^n \in B_m^+$. Namely [14], for each $i < m$, Δ can be written as $\sigma_i \cdot \gamma$ for some $\gamma \in B_m^+$. That, together with $\sigma_\ell \Delta = \Delta \sigma_{m-\ell}$ $(1 \le \ell \le m-1)$, gives the existence of such an n. Then by Theorem 3.1(ii), $(\vec{x})^{\mathrm{Rev}\,\alpha \cdot \Delta^n} \neq (\vec{x})^{\mathrm{Rev}\,\beta \cdot \Delta^n}$. So by Lemma 3.2 there is an i with $x_i^{\Delta^n \cdot \alpha} \neq x_i^{\Delta^n \cdot \beta}$. Take $d = x_i^{\Delta^n}$ (a member of DDF by Theorem 2.6). $\square$

Theorem 3.5. *If $\alpha \in B_\infty$, $\beta \in B_\infty^+$, $\beta \neq \varepsilon$, then $\beta\alpha > \alpha$.*

Proof. It suffices to show that for all i, $\sigma_i\alpha > \alpha$. First we show it when $\alpha \in B_\infty^+$. By Theorem 3.1(ii) there is a least k with $u = ((\vec{x})^\alpha)_k \neq ((\vec{x})^{\sigma_i \alpha})_k = v$, and either $u <_{\mathrm{L}} v$ or $v <_{\mathrm{L}} u$; we want to show the former, it will suffice to show $u \preceq v$. We have $u = (x_k)^{\mathrm{Rev}\,\alpha}$, $v = (x_k)^{\mathrm{Rev}\,\alpha \cdot \sigma_i}$ by Lemma 3.2. By applications of Theorem 2.6, $x_k^{\mathrm{Rev}\,\alpha} \in DDF$. So $u \preceq v$ by Theorem 2.5(ii), giving the theorem when $\alpha \in B_\infty^+$.

For $\alpha \in B_\infty$, pick, as in Theorem 3.4, m and n, with $m > i$, such that for $\Delta = \Delta_m$ we have $\Delta^n\alpha \in B_\infty^+$. It suffices by Theorem 3.1(iii) to show that $\Delta^n\sigma_i\alpha > \Delta^n\alpha$. Assuming without loss of generality that n is even, then $\Delta^n\sigma_i\alpha = \sigma_i\Delta^n\alpha$, and we are done by the first part of the theorem. $\square$

For $\beta, \alpha \in B_\infty^+$ say that β is a proper subsequence of α if $\alpha = \delta_0\delta_1\cdots\delta_n$ for some sequence of generators δ_i and for some $0 \le i_0 < \cdots < i_\ell \le n$ with $\ell < n$, $\beta = \delta_{i_0}\delta_{i_1}\cdots\delta_{i_\ell}$.

Corollary 3.6. *If $\beta, \alpha \in B_\infty^+$, β a proper subsequence of α, then $\beta < \alpha$.*

Proof. (*By Theorems* 3.5 *and* 3.1(iii), *by induction on the unique n such that α is the product of n many generators.*). Since $\varepsilon < \sigma_i$, the atomic case holds. If β is an initial segment of α, we are done. So suppose for some least r that $i_r > r$. Then $\delta_{i_r} \cdots \delta_{i_l} \leq \delta_{r+1}\delta_{r+2} \cdots \delta_n$ (by induction) $< \delta_r\delta_{r+1} \cdots \delta_n$ (Theorem 3.5). Multiplying on the left by $\delta_0 \cdots \delta_{r-1}$ gives $\beta < \alpha$. □

By Theorem 3.5 the linear ordering $<$ extends the partial ordering on B_∞ used by Elrifai and Morton in [12] (they defined $\beta < \alpha \leftrightarrow$ for some $\gamma, \delta \in B_\infty^+$ with at least one of γ, δ different from ε, $\alpha = \gamma\beta\delta$).

Corollary 3.7. *For N finite, B_N^+ is well ordered under $<$.*

Proof. Else there would be a sequence $\alpha_0 > \alpha_1 > \cdots > \alpha_n > \cdots$ with $\alpha_j = \delta_{j,0}\delta_{j,1} \cdots \delta_{j,n_j}$, each $\delta_{j,m} \in \{\sigma_1, \ldots, \sigma_{N-1}\}$. Applying (a special case of) Higman's theorem [15], there exist $j < k$ with $\delta_{j,0} \cdots \delta_{j,n_j}$ a subsequence of $\delta_{k,0} \cdots \delta_{k,n_k}$, contradicting Corollary 3.6. □

Burckel [3] has recently given a tree representation for the members of B_N^+, showing that the ordinal of B_N^+ is $\omega^{\omega^{N-2}}$.

Theorems 3.1(ii), 3.3, and Corollary 3.7 imply the following result.

Corollary 3.8. *For $2 \leq N < \infty$, $\langle x_i : i < N \rangle$ the sequence of generators of $\mathscr{P}_N$, $\{\langle x_i : i < N \rangle^\alpha : \alpha \in B_N$ and $\langle x_i : i < N \rangle^\alpha$exists$\}$ is well ordered under $<_{\text{Lex}}$.*

References

[1] E. Artin, Theorie der Zöpfe, Abh. Math. Sem. Univ. Hamburg 4 (1925), 47–72.

[2] E. Brieskorn, Automorphic sets and braids and singularities, in: Braids, ed., Contemporary Math, Vol. 78, (American Math. Soc., 1988) 45–117.

[3] S. Burckel, Thesis, Université de Caen, 1994.

[4] P. Dehornoy, Free distributive groupoids, J. Pure Appl. Algebra 61 (1989) 123–146.

[5] P. Dehornoy, Sur la structure des gerbes libres, Comptes-rendu de l'Acad. des Sciences de Paris 309-I (1989) 143–148.

[6] P. Dehornoy, Braid groups and left distributive structures, Trans. Amer. Math. Soc. 345 (1994) 115–150.

[7] P. Dehornoy, A canonical ordering for free left distributive magmas, Proc. Amer. Math. Soc. 122 (1994) 31–36.

[8] R. Dougherty, Critical points in an algebra of elementary embeddings, Ann. Pure Appl. Logic 65 (1993) 211–241.

[9] R. Dougherty and T. Jech, Finite left distributive algebras and embedding algebras, Adv. Math.

[10] A. Drapal, Homomorphisms of primitive left distributive groupoids, Comm. Algebra 22-7 (1994) 2579–2592.

[11] A. Drapal, Persistence of cyclic left distributive algebras, J. Pure. Appl. Algebra 105 (1995) 137–165.

[12] E.A. Elrifai and H.R. Morton, Algorithms for positive braids, Quart. J. Math. Oxford 45 (2) (1994) 479–497.

[13] R. Fenn and C. Rourke, Racks and links in codimension 2, J. Knot Theory and its ramifications (1992) 343–406.
[14] F.A. Garside, The braid group and other groups, Quart. J. Math. Oxford 20 (2) (1969) 235–254.
[15] G. Higman, Ordering by divisibility in abstract algebras, Proc. London Math. Soc. 2 (1952) 326–336.
[16] D. Joyce, A classifying invariant of knots: the knot quandle, J. Pure Appl. Algebra 23 (1982) 37–65.
[17] A. Kanamori, The Higher Infinite: Large Cardinals in Set Theory from Their Beginnings (Springer, Berlin 1994).
[18] L. Kauffman, Knots and Physics (World Scientific, Singapore, 1991) Chapter 1–13.
[19] D. Larue, Braid words and irreflexivity, Algebra Universalis 31 (1994) 104–112.
[20] D. Larue, Thesis, University of Colorado, 1994.
[21] R. Laver, The left distributive law and the freeness of an algebra of elementary embeddings, Adv. Math. 91 (1992) 209–231.
[22] R. Laver, A division algorithm for the free left distributive algebra, Proc. Helsinki 1990 ASL meeting (Springer, Berlin, 1993) 155–162.
[23] R. Laver, On the algebra of elementary embeddings of a rank into itself, Adv. Math. 110 (1995) 334–346
[24] R.C. Lyndon and P.E. Schupp, Combinatorial Group Theory (Springer, New York, 1977) 157.
[25] D.A. Martin, Infinite games, Proc. International Congress of Mathematicians, Helsinki, 1978, 73–116.
[26] D.A. Martin, Woodin's proof of PD, handwritten notes, 1985.
[27] S. Matveev, Distributive groupoids in knot theory, Math. USSR-Sb. (1982) 73–83.
[28] J. Steel, On the well-foundedness of the Mitchell order, J. Symbolic Logic. 58 (1993) 931–940.
[29] M. Takesaki, Abstractions of symmetric functions, Tohuku Math. J. 49 (1943) 143–207 (Japanese); Math. Reviews 9, p. 8.
[30] F. Wehrung, Gerbes primitives, CRAS Paris 313 (1991) 357–362.