Crossing Matrices and Thurston's Normal Form for Braids

J. Burillo M. Gutierrez S. Krstic Z. Nitecki

July 23, 2000

0 Introduction

Positive braids are those where all overcrossings are from left to right. By convention, the ii crossing number is always zero. The crossing matrix of b is an $n \times n$-matrix that codifies all the crossing numbers into a matrix. The purpose of this paper is to show the relation between this simple invariant and the canonical form of positive braids (as explained in [1] and [5]), with special emphasis on positive braids whose crossing numbers are ≤ 1. For example, it is possible to test whether a factorization $b = a_1 \cdots a_p$ of such a braid b is canonical because the crossing matrices of the factors must have a maximality property (Proposition 5.2). It is known [1, Thm. 2.6] that a positive braid of canonical length one is determined by its crossing matrix. We extend that result to positive braids of canonical length ≤ 2 and show that for canonical length ≥ 3 this is no longer true (Proposition 4.6 and Theorem 5.4). We give a characterization of all those matrices which are crossing matrices of a braid of length ≤ 2. This answers the question posed in [1, p. 496]. As an example, if every strand of a positive braid crosses *over* every other strand exactly once, this braid is the fundamental braid squared or the full twist braid (Example 5.5).

Another interesting result, in view of Garside's Lemma (Theorem 4 in [3]), is that the semi-group of pure positive braids is not finitely generated (Theorem 6.4).

Finally we characterize all matrices that are crossing matrices (Corollary 3.2). The characterization of the crossing matrices of positive braids remains an open problem.

A word about our notation; because braids, permutations and matrices all occur together we have decided to adhere to the following convention: permutations are always small Greek letters, braids are always small Latin letters (except that the notation α^+ denotes the braid induced by the permutation α), and matrices are always capital Latin letters. This has forced us to give up the notation Δ for the fundamental braid, which is used both in [1] and [3] (Thurston uses Ω in [5]), and instead we write d. The fundamental permutation $i \mapsto n+1-i$ is denoted δ and $\delta^+ = d$. We try to use related letters for related permutations, braids and matrices. Since we have mentioned one element of the braid group $\mathbf{B}_n$ and one of the symmetric group Σ_n, we call their identity elements d^0 and δ^0, respectively.

1 Definitions

Let n be a fixed integer ≥ 3. We will be concerned mainly with the braid group $\mathbf{B}_n$ (with elements $a, b, \ldots$) and the symmetric group Σ_n (with elements $\alpha, \beta, \ldots$). There is an obvious epimorphism $p : \mathbf{B}_n \to \Sigma_n$ and a section of p denoted by $\alpha \mapsto \alpha^+$ with image in the subsemigroup $\mathbf{B}_n^+$ of positive braids. For a permutation α, the braid α^+ is the simplest positive braid in $p^{-1}(\alpha)$ [1, p.484]. In order to insure that $p(ab) = p(a)p(b)$, for $a, b \in \mathbf{B}_n$, Σ_n must act on the right; consequently we write $i\pi$ for the image of the integer $i \in [1, n]$ under the permutation π. Many times expressions like $i\pi^{-1}$ appear as subindices or exponents and so we use the notation $\bar{x}$ for the inverse of x, where x is either in $\mathbf{B}_n$ or Σ_n. If G is a group with identity element e and $\leq$ is a partial order on G which is invariant under right translations, then the set $G^+ = \{g \in G \,|\, g \geq e\}$ is a subsemigroup of G. Conversely, if G^+ is a subsemigroup of G the definition $x \leq y$ if $yx^{-1} \in G^+$ defines an order preserved by right translation and whose positive elements are precisely G^+. For example, the integers have an order defined by the subsemigroup of non-negative integers, and $\mathbf{B}_n$ has an order defined by $\mathbf{B}_n^+$. Both these groups are lattices under this orders, [5, Corollary 9.3.7].More generally, we consider orders $\leq$ on groups G which are not necessarilty right invariant. We still write G^+ for the elements $\geq e$ and, if $x \leq y$, $[x, y]$ denotes the set $\{z \,|\, x \leq z \leq y\}$. For instance, we may define an ordering in Σ_n by $\alpha \leq \beta$ if $\alpha^+ \leq \beta^+$ in $\mathbf{B}_n$. see [5, Propositions 9.1.8 and 9.1.9]. The resulting order is a lattice and, if δ is given by $i\delta = n+1-i$, then δ is the largest permutation and we can identify Σ_n with $\Sigma_n^+ = [\delta^0, \delta^1]$. If $d = \delta^+$, the section $\alpha \mapsto \alpha^+$ is order preserving by definition, and its image is precisely $[d^0, d^1]$, see [1, Theorem 2.6]. Let $\mathcal{M}(n) = \mathcal{M}$ be the abelian group of $n \times n$-integral matrices with zero diagonal (with elements $A, B, \ldots$). We omit reference to n unless the context demands it. Given a matrix $M \in \mathcal{M}$, its ij entry (or *spot*) will be denoted M_{ij}. There is an action of Σ_n on $\mathcal{M}$ that makes this abelian group a Σ_n-module: if $M \in \mathcal{M}$ and $\pi \in \Sigma_n$ then $N = M^\pi$ satisfies $N_{ij} = M_{i\bar{\pi},j\bar{\pi}}$. The module $\mathcal{M}$ has a partial order: $A \leq B$ if and only if $A_{ij} \leq B_{ij}$ for all ij. In accordance to our conventions $\mathcal{M}^+$ is the subsemigroup of all positive $(\geq O)$ matrices in $\mathcal{M}$. The homomorphism p induces an action of $\mathbf{B}_n$ on $\mathcal{M}$, namely, $M^b = M^{p(b)}$, for $b \in \mathbf{B}_n$, $M \in \mathcal{M}$.

We denote by $\mathcal{S}(n) = \mathcal{S}$ the submodule of all symmetric matrices of $\mathcal{M}$. For $M \in \mathcal{M}$, $M^{\mathbf{u}}$ is the upper triangle of M, that is, $(M^{\mathbf{u}})_{ij} = M_{ij}$ if $i < j$ and $(M^{\mathbf{u}})_{ij} = 0$ otherwise. By $A^{\mathbf{t}}$ we mean the transpose of A.

Finally, let D be the upper triangular matrix with $D_{ij} = 1$ whenever $i < j$.

Definition 1.1 *The* **order reversal matrix** *of a permutation α is the matrix $R = R\alpha \in [O, D]$ given by $R_{ij} = 1$ if and only if $i < j$ and $i\alpha > j\alpha$.*

The map $\alpha \mapsto R\alpha$ is a derivation when R is viewed as the characteristic function of subsets of $[1, n] \times [1, n]$. See [5, 9.1.3] or formula (4) below. We say that a map $F : \mathbf{B}_n \to \mathcal{M}$ is a *derivation* if, for $a, b \in \mathbf{B}_n$, $F(ab) = F(a) + F(b)^{\bar{a}}$. Also notice that $D = R\delta$ and that $D - R\alpha = R\alpha\delta$ for all α. We use the notation $S\pi$ for the symmetric matrix $R\pi + R^{\mathbf{t}}\pi$. In particular, $S\delta = D + D^{\mathbf{t}}$ is called E.

Definition 1.2 *The* **crossing matrix** *of a braid is the derivation $C : \boldsymbol{B}_n \to \mathcal{M}$, characterized by the fact that $C(\alpha^+) = R\alpha$, for all $\alpha \in \Sigma_n$.*

Naturally, we must show that such a derivation exists. One way of seeing this is the following: let F be a free group of rank n and fix $\mathbf{a} = \{a_1, \ldots, a_n\}$, a basis of F. We consider the group $\mathbf{M} \subset \mathsf{Aut}\ F$ of automorphisms of the form $a_i \mapsto w_i a_i w_i^{-1}$ for $w_i \in F$, $1 \leq i \leq n$. These automorphisms are called basis-conjugating in [4], and a set of generators are the x_{ij} which map a_i to $a_j a_i a_j^{-1}$ and all other a_k to a_k. We only need to know that all the relators in the presentation of $\mathbf{M}$ found in [4] are commutators in the x_{ij}. Therefore, the abelianization of $\mathbf{M}$ is free abelian in the x_{ij}, $i \neq j$, and that group can be identified with $\mathcal{M}$. In addition, Σ_n can be considered as a subgroup of $\mathsf{Aut}\ F$ by letting $\pi \in \Sigma_n$ permute the elements of $\mathbf{a}$ in the obvious way. With that convention, $\bar{\pi} x_{ij} \pi = x_{i\pi, j\pi}$. Consequently, the abelianization of $\mathbf{M}$ as a Σ_n-group can be identified with the Σ_n-module $\mathcal{M}$. It is well-known (see, e.g. [2, Theorem 5.1, p. 25]) that the braid group embeds in $\mathsf{Aut}\ F$. This embedding is defined as follows: let $\tau_i \in \Sigma_n$ be the transposition of i and $i+1$. The τ_i, $1 \leq i \leq n-1$ are generators of Σ_n and the τ_i^+ are a set of generators of $\mathbf{B}_n$ (See [2, Theorem 1.5, p.8]). The embedding $\mathbf{B}_n \to \mathsf{Aut}\ F$ is given by $\tau_i^+ \mapsto x_{i,i+1}\tau_i$ and its image lies in the semidirect product $\mathbf{M} \times \Sigma_n \subset \mathsf{Aut}\ F$. Consequently the composition of this embedding with the projection $\mathbf{M} \times \Sigma_n \to \mathbf{M}$ is a map $P : \mathbf{B}_n \to \mathbf{M}$ satisfying $P(ab) = P(a)\bar{\pi}P(b)\pi$, where $\pi = p(a)$. The composition of P and the abelianization map $\mathbf{M} \to \mathcal{M}$ is precisely C. From here it is trivial to deduce that C has the desired properties.

Both $C : \mathbf{B}_n \to \mathcal{M}$ and $R : \Sigma_n \to \mathcal{M}$ are order preserving. As a result, $C([d^0, d^2]) \subset [O, E]$, and $\pi \leq \rho$ if and only if $R\pi \leq R\rho$; indeed, this is the definition of the order in Σ_n (see [5, 9.1.7]). Both Σ_n and $\mathbf{B}_n$ are lattices under the order; for example, $(\alpha \vee \beta)^+ = \alpha^+ \vee \beta^+$ for all $\alpha, \beta \in \Sigma_n$ and $\tau_i \vee \tau_{i+1} = \tau_i \tau_{i+1} \tau_i$ in Σ_n. Similarly, $\tau_i \vee \tau_j = \tau_i \tau_j$ if $|i - j| \geq 2$.

Definition 1.3 *A matrix A in $\mathcal{M}$ is said to be* $\mathbf{T}\nu$ *($\nu = 0, 1$) if whenever $1 \leq i < j < k \leq n$, then $A_{ij} = A_{jk} = \nu$ implies $A_{ik} = \nu$.*

Observe that these two properties of A depend only on its upper triangle $A^{\mathbf{u}}$. In general, T1 is used only for matrices in $[O, E]$ but T0 is used for more general matrices.

The image $R(\Sigma_n)$ of Σ_n under the map $R : \Sigma_n \to \mathcal{M}$ is precisely the set of all matrices in $[O, D]$ which are both T0 and T1. This result, and Definition 1.3, are due to Thurston [5, Lemma 9.1.6].

Definition 1.4 *The set $\mathcal{T}$ is the collection of all matrices in $\mathcal{M}$ of the form $A = T + R\alpha$, where $T \in \mathcal{S}$ and $\alpha \in \Sigma_n$.*

For $A \in \mathcal{T}$ the decomposition $T + R\alpha$ is determined by A because it is easy to check that the formula

$$i \mapsto i + \sum_j A_{ij} - \sum_k A_{ki} \tag{1}$$

defines a permutation α on $[1, n]$, and that $A = T + R\alpha$ for some $T \in \mathcal{S}$. For more details see §2.

Notation 1.5 *If $\mathcal{X} \subset \mathcal{M}$, then $\mathcal{X}^+$ is the intersection $\mathcal{X} \cap \mathcal{M}^+$, and $\mathcal{X}_0$ is the set of matrices of $\mathcal{X}$ which are T0.*

Thus we have sets such as $\mathcal{T}_0$ (the set of matrices in $\mathcal{T}$ which are T0), $\mathcal{S}_0^+$ (the positive, T0, symmetric matrices in $\mathcal{M}$), or $[O, D]_0$ (the set of T0 matrices $O \leq M \leq D$), etc.

Note that if $T + R\alpha \in \mathcal{T}^+$, then necessarily $T \in \mathcal{S}^+$.

When necessary for clarity, we write $C(b) = Tb + R\beta,\ p(b) = \beta$.

We define two commutative, associative operations in $[O, E]$, and two important constructions. The operations, union and intersection, are indeed union and intersection if one considers a matrix in $[O, E]$ as the characteristic function of a subset of $\{1, \ldots, n\} \times \{1, \ldots, n\}$. The two constructions, for matrices $A \in \mathcal{T}$, are A' and $A^{(1)}$. The first of these has a simple definition if $A \in \mathcal{S}$: $A'_{ij} = 1$ if and only if $A_{ij} \neq 0$, and $A'_{ij} = 0$ otherwise. The second construction, defined only on $\mathcal{T} \cap [O, E]$, adds to A ones on the spots where the condition T1 fails.

Definition 1.6

1. *If A and B are in $[O, E]$, then the* **intersection** *$A \cap B$ of A and B is defined by $(A \cap B)_{ij} = A_{ij} B_{ij}$, and the* **union** *$A \cup B$ is $A + B - A \cap B$. Two matrices in $[O, E]$ are disjoint if $A \cap B = O$. The notation $A \oplus B$ indicates the sum of disjoint matrices.*

2. *If $T \in \mathcal{S}^+$, T' is defined by $T'_{ij} = 1$ if and only if $T_{ij} \neq 0$, and $T'_{ij} = 0$ if $T_{ij} = 0$. In the general case, when $A \in \mathcal{T}$, $A = T + R\alpha$, A' is defined by $A' = (T' \cap S\alpha\delta) \oplus R\alpha$.*

3. *If $A \in \mathcal{T} \cap [O, E]$, define $A^{(1)}$ as follows: if for some $j \in [i + 1, k - 1]$ we have $A_{ij} = A_{jk} = 1$, then $A^{(1)}_{ik} = 1$; otherwise $A^{(1)}_{ik} = A_{ik}$.*

The property T0 is preserved under unions and T1 is preserved under intersections. If $A \in \mathcal{T} \cap [O, E]$, then $T \cap R\alpha = O$ and so $A = T \oplus R\alpha$. Basically, A' is obtained by replacing, in A, non-zero entries with 1, except when $T_{ij} \neq 0$ and $R\alpha_{ij} = 1$, in which case $A'_{ji} = 0$, $A'_{ij} = 1$. Notice that $A \in [O, E]$ is Tν if and only if A' is Tν. It is important to notice that, if $A = T + R\alpha$, A' is not, in general, equal to $T' + R\alpha$.

2 Order Reversal Matrices.

We give here some basic properties of the order reversal matrices. First, it is clearly necessary that $R\pi$ be T0 and T1 (See [5, 9.1.6]). Conversely, if a matrix $A \in [O, D]$ is T0 and T1, then Formula (1) defines a permutation α for which $R\alpha = A$. To give the reader an idea of the proof of this assertion, let $\theta = \theta_A$ be the function $[1, n] \to \mathbf{Z}$ defined by (1). If $A \in [O, D]$ the image of θ clearly lies in $[1, n]$. We show that if $i < k$ and $A_{ik} = 1$ then $i\theta > k\theta$. Property T0 alone gives that $i + \sum_{j=i}^{k} A_{ij} > k - \sum_{j=i}^{k} A_{jk}$ because, for each j between i and k, at least one of A_{ij} or A_{jk} must be one. Then T1 alone implies that $\sum_{j=k+1}^{n} A_{ij} - \sum_{j=1}^{i-1} A_{ji} \geq \sum_{j=k+1}^{n} A_{kj} - \sum_{j=1}^{i-1} A_{jk}$ because, e.g., for each $j \in [k+1, n]$ with $A_{kj} = 1$ we have the corresponding $A_{ij} = 1$ by T1. The two inequalities put together give the desired result. A similar calculation gives that if $A_{ik} = 0$, then $i\theta < k\theta$. In particular, θ is one-to-one, and therefore, a permutation whose reversal matrix is A.

Let $\tau_i \in \Sigma_n$ be the transposition of i and $i + 1$, $1 \leq i \leq n - 1$.

Definition 2.1 *The* **initial set** $I(\pi)$ *of a permutation* π *is the set of indices* $i \in [1, n-1]$ *for which* $\pi^+ = \tau_i^+ \rho^+$*, where* ρ *is some element in* Σ_n*. The* **final set** $F(\pi)$ *of* π *is the initial set of* π^{-1}*.*

Equivalently, $I(\pi)$ is the set of indices i for which $R\pi_{i,i+1} = 1$ (See [1, Prop. 2.4]).

Definition 2.2 *A pair* ij*,* $i < j$ *is called a* **final spot** *for* π *if* $|i\pi - j\pi| = 1$*.*

For any permutation $\pi \in \Sigma_n$, and for each $k \in [1, n-1]$, there is a final spot with $i\pi = k,\ j\pi = k + 1$, if $R\pi_{ij} = 0$ or $i\pi = k + 1,\ j\pi = k$, if $R\pi_{ij} = 1$. We will call these spots **trivial** or **non-trivial final spots** of π, respectively. Then the final set of π is the set of indices k for which ij is a non-trivial final spot with $k = j\pi$.

Definition 2.3 *Suppose that* $A \in \mathcal{T} \cap [O, E]$*,* $A = T \oplus R\alpha$*, and that* $C \leq D$*;*

1. *If* $C \leq A$*,* π *is a* **maximal** *(resp.* **minimal***)* **permutation** *in* $[C, A]$ *if* $R\pi \in [C, A]$ *and if* $C \leq R\rho \leq A$ *implies* $\rho \leq \pi$ *(resp.* $\rho \geq \pi$*).*

2. *We say that* $B \in [O, D]$ *is an* **intermediate matrix** *of* A *if* $T^{\boldsymbol{u}} \leq B \leq A$*. If* $B = R\pi$*, we say that* π *is an* **intermediate permutation** *of* A*.*

3. *An intermediate permutation* π *of* A *is* **maximal** *(resp.* **minimal***) if it is maximal (resp. minimal) in* $[T^{\boldsymbol{u}}, A]$*.*

We collect some basic properties of final spots in the following

Lemma 2.4 *If $\pi \in \Sigma_n$,*

1. *A spot ij of $R\pi$ is final if and only if the matrix U defined by $U_{ij} = 1 - R\pi_{ij}$, and $U_{kl} = R\pi_{kl}$, otherwise, is the order reversal matrix of $R\pi\tau$, where τ is the transposition of $i\pi$ and $j\pi$.*

2. *For $A \in \mathcal{T}^+$, a permutation π with $R\pi \leq A$ is maximal if and only if $A_{ij} = 0$ for all trivial final spots of π.*

To prove a result on minimal permutations we need a result for $A = O + R\delta = D$ (cf. Definition 1.6):

Lemma 2.5 *If $B \in [O, D]_0$ then $B^{(1)} \in [O, D]_0$.*

Proof:

Assume throughout that $i < j < k$; say $B_{ij} = B_{jk} = 1$ and $B_{ik} = 0$, as above. Assume that for some intermediate l, $i < l < k$ (necessarily $\neq j$), $B_{il} = B_{lk} = 0$; we will show that either $B^{(1)}_{il}$ or $B^{(1)}_{lk}$ equals 1. This will complete the proof.

Case 1. $i < l < j$: Since B is T0 and $B_{ij} = 1$, necessarily $B_{lj} = 1$, but $B_{jk} = 1$ so $B^{(1)}_{lk} = 1$.

Case 2. $j < l < k$: This time $B_{jl} = 1$, but $B_{ij} = 1$ and hence $B^{(1)}_{il} = 1$.

□

Corollary 2.6 *If $B \in [O, D]_0$ there exists a minimal π in $[B, D]$.*

Proof:

Define by induction $B^{(0)} = B$ and $B^{(i+1)} = (B^{(i)})^{(1)}$. By Lemma 2.5, we have an increasing chain of T0 matrices $O \leq B^{(0)} \leq B^{(1)} \leq \cdots \leq D$ and, by construction, $B^{(s)} = B^{(s+1)}$ if and only if $B^{(s)}$ is T1. Since the chain must stabilize, $B^{(s)}$ is both T0 and T1 for some s and so $B^{(s)} = R\pi$, for some π. Clearly $R\pi$ is minimal. □

Definition 2.7 *The matrix $R\pi$ obtained in Corollary 2.6 is called* $\sup B$.

When $B = R\alpha \cup R\beta$ then $\sup B = R(\alpha \vee \beta)$ in the sense of Thurston [5].

Remark 2.8 *The involution $A \mapsto D - A$ is a "complementation" in $[O, D]$ exchanging unions with intersections, and T0 matrices with T1 matrices. Thus, it is possible to view Corollary 2.6 as a result on the $A^{[s]} = D - (D - A)^{(s)}$ claiming that, given a T1 matrix $O \geq A \geq D$, then $A \geq A^{[1]} \geq A^{[2]} \geq \cdots \geq O$ is a decreasing sequence of T1 matrices which stabilizes precisely when $A^{[s]}$ is a T0 matrix. This matrix is called* $\inf A$ *and* $\inf R\alpha \cap R\beta = R(\alpha \wedge \beta)$. *As a curiosity, we mention that, if t_i and t_j are two standard generators of $\boldsymbol{B}_n$ then $t_i \vee t_j$ coincides with the braid $t_i * t_j$ defined in [1, § 2].*

We close with the following observations:

Lemma 2.9 *Assume that $A \in [O, D]$ and that $\pi \in \Sigma_n$.*

1. *If $A \leq R\pi$ then A^π is lower triangular.*

2. *If $A \cap R\pi = O$, then A^π is upper triangular.*

3. *If A is a T1 matrix, then A^π is a T1 matrix.*

Proof:

To prove (1) we observe that, if $i < j$ and $R\pi_{ij} = 1$, then the ij entry of A is sent by π to $A_{i\pi,j\pi}$ which is in the lower triangle because $i\pi > j\pi$. If $A_{ij} \leq R\pi_{ij}$, all non-trivial entries of A end up in the lower triangle of A^π. The proof of (2) is equally simple.

For (3) it will be convenient to put $\rho = \bar{\pi}$ and show that $B = A^{\bar{\rho}}$ is T1. Let i, k be integers in $[1, n]$. If $i < j < k$, then $B_{ij} = B_{jk} = 1$ implies that $A_{i\rho,j\rho} = A_{j\rho,k\rho} = 1$. Since $A \in [O, D]$ then necessarily $i\rho < j\rho < k\rho$ and so $1 = A_{i\rho,k\rho} = B_{ik}$. □

3 Crossing Matrices.

In Definition 2.1, $\tau_i \in \Sigma_n$ is the transposition $(i, i+1)$. Let $t_i = \tau_i^+$; the standard presentation for the group $\mathbf{B}_n$ (see [2, Thm 1.5]) is

$$\langle t_1, \ldots, t_{n-1} \,:\, t_i \vee t_j = t_j \vee t_i, \quad i, j \in [1, n-1] \rangle.$$

The matrix $C(t_i)$, therefore, has a 1 in spot $i, i+1$ and zeros elsewhere. Using the fact that C is a derivation, it is easy to conclude that $C(t_i^{-1})$ has -1 in the $i+1, i$ spot, and zero elsewhere.

Lemma 3.1 *If $A = C(b)$ then A_{ij} equals the number of times the i^{th} strand of b crosses from left to right* over *the j^{th} strand minus the number of times that the i^{th} strand crosses from right to left* over *the j^{th} strand.*

Proof:

This is clear if $b = t_i^\epsilon$, $\epsilon = \pm 1$. We proceed by induction on the word length of b as a word in the generators. If $C(b)$ satisfies the equality of the lemma, then, if $\beta = p(b)$, $C(bt_i^\epsilon) = C(b) + C(t_i^\epsilon)^{\bar{\beta}}$ is obtained from $C(b)$ by adding a 1 to the $i\bar{\beta}, (i+1)\bar{\beta}$ spot (if $\epsilon = 1$) or a -1 to the $(i+1)\bar{\beta}, i\bar{\beta}$ spot (if $\epsilon = -1$). This means that $C(bt_i^\epsilon)$ satisfies the lemma. □

A consequence of this Lemma is that, if b is a positive braid, its crossing matrix lies in $[O, E]$ precisely when each strand crosses over another strand at most once.

The group of pure (colored) braids is $\mathbf{P}_n = \ker p$ and it has a presentation with generators $a_{ij} = w_{ij} t_i^2 w_{ij}^{-1}$, where $w_{i,i+1} = e$ and $w_{ij} = t_{j-1} \dots t_{i+1}$ if $i < j, j \neq i+1$.

See [2, Lemma 4.2]. According to our conventions $\mathbf{P}_n^+ = \mathbf{P}_n \cap \mathbf{B}_n^+$. From Figure 11 in [2, p. 21] we conclude that $C(a_{ij})$ is a symmetric matrix with 1 in the ij and ji spots, and zero elsewhere.

Corollary 3.2 *For all $n \geq 3$ we have,*

1. $C(\boldsymbol{P}_n) = \mathcal{S}$, *and*

2. $C(\boldsymbol{B}_n) = \mathcal{T}$.

Proof:

We begin by remarking that $C|\mathbf{P}_n$ is a homomorphism $\mathbf{P}_n \to \mathcal{S}$. Since the $C(a_{ij})$ generate $\mathcal{S}$, it follows that C maps $\mathbf{P}_n$ onto $\mathcal{S}$. If $T + R\beta$ lies in $\mathcal{T}$ then, since $T \in \mathcal{S}$, there exists a pure braid a such that $C(a) = T$. Therefore $C(a\beta^+) = T + R\beta$. □

A much more complicated task is to find $C(\mathbf{B}_n^+)$ and $C(\mathbf{P}_n^+)$.

Remark 3.3 *If b is a positive braid $b = t_{i_1} \dots t_{i_q}$, we define its reverse $\mathrm{rev}\, b$ as $\mathrm{rev}\, b = t_{i_q} \dots t_{i_1}$. See [3, page 236]. The set $\{b_{ij}\} \subset \boldsymbol{P}_n^+$ given by $b_{ij} = w_{ij} t_i^2 \,\mathrm{rev}\, w_{ij}$, is also a set of generators of $\boldsymbol{P}_n$. However, it is* **not** *true that the b_{ij} are semi-group generators of $\boldsymbol{P}_n^+$. See Theorem 6.4 below.*

Definition 3.4 *A matrix $A \in \mathcal{T}^+$ is called* **realizable** *if $A = C(a)$ for some $a \in \boldsymbol{B}_n^+$.*

It is clear that $C(\mathbf{B}_n^+) \subset \mathcal{T}_0^+$ because if strands i and k cross in a positive braid a, then the j strand, for $i < j < k$, must exit the triangle formed by strands i and k and the top of the braid. Example 6.5 below shows that this inclusion is strict. For our next observation we remind the reader (cf. Definition 1.6) that if $A \in \mathcal{T}_0^+$, then $A' \in \mathcal{T}_0^+$.

Lemma 3.5 *For $A \in \mathcal{T}_0^+$, if A' is a realizable matrix, so is A.*

Proof:

Suppose that $A' = C(a')$, that $B = A - A'$, and that ij is a non-trivial spot of A', $i < j$. Factor $a' = bt_kc$, where $b, c \in \mathbf{B}_n^+$, $p(b) = \beta$, $k = i\beta$. Now replace t_k by $t_k^{2B_{ij}+1}$. Do this for every ij; the result is a braid a with $C(a) = A$. □

Notice that we do not claim the converse. This Lemma shows that the realization problem must be solved first in $\mathcal{T}_0^+ \cap [O, E]$.

Definition 3.6 *If $A \in \mathcal{T}^+$ and $R\beta \leq A$, define $\beta \backslash A$ to be the matrix $(A - R\beta)^\beta$.*

With this definition, if $a = \beta^+ c$ and $A = C(a)$, then $\beta \backslash A = C(c)$.

Lemma 3.7 *If $A \in \mathcal{T}^+$ and $R\beta \leq A$, then $\beta \backslash A \in \mathcal{T}^+$.*

We postpone the proof until after Corollary 4.2.

4 Matrices in $[O, E]$.

Throughout this section $A = T + R\alpha \geq 0$; if also $A \leq E$, then $A = T \oplus R\alpha$.

Lemma 4.1 *Suppose that $a \in \boldsymbol{B}_n^+$ has crossing matrix $A = T \oplus R\alpha \leq E$ and that $\beta \in \Sigma_n$. If $C(a\beta^+) \leq E$ then*

$$T \cap S\alpha\beta = O, \tag{2}$$

and

$$C(a\beta^+) = (T \oplus S\alpha \cap S\alpha\beta\delta) \oplus R\alpha\beta. \tag{3}$$

Proof:

Write $C(a\beta^+) = U \oplus R\alpha\beta$. We compare the ij entries of T, $R\alpha$, U and $R\alpha\beta$ distinguishing three cases:

Case 1. The strands do not cross in a. Then $R\alpha\beta_{ij} = 1$ if and only if they cross in β^+, and the other three matrices are zero at ij.

Case 2. The strands cross once in a. Then $T_{ij} = 0$, $R\alpha_{ij} = 1$, and precisely one of $R\alpha\beta_{ij}$ or U_{ij} equals 1 (depending on whether or not they cross in β^+).

Case 3. The strands cross twice in a. Then they cannot cross in β^+, so $T_{ij} = U_{ij} = 1$ and $R\alpha_{ij} = R\alpha\beta_{ij} = 0$.

By inspection, T_{ij} and $S\alpha\beta_{ij}$ agree only when they are both zero. This proves (2). Once more, inspection shows that $T = 0$, $U = 1$ occurs precisely when $R\alpha = 1$ and $R\alpha\beta = 0$ or, equivalently, $R\alpha\beta\delta = 1$. This proves (3). □

It is geometrically obvious, and it follows from Lemma 2.9, that $C(\alpha^+\beta^+)$ is always $\leq E$. Consequently an important special case of (3) is

$$C(\alpha^+\beta^+) = R\alpha \oplus (R\beta)^{\bar{\alpha}} = (S\alpha \cap S\alpha\beta\delta) \oplus R\alpha\beta. \tag{4}$$

This formula shows that the map $R : \Sigma_n \to \mathcal{M}/\mathcal{S}$ is a derivation. An induction gives,

Corollary 4.2 *If $a = \alpha_1^+ \cdots \alpha_p^+$ has crossing matrix $A = Ta \oplus R\alpha \leq E$, ($\alpha = p(a) = \alpha_1 \cdots \alpha_p$) then*

$$Ta = \bigoplus_{i=1}^{p-1} (S\alpha_1 \cdots \alpha_i \cap S\alpha_1 \cdots \alpha_{i+1}\delta).$$

We now give the promised proof of 3.7:

Proof of Lemma 3.7:

By the properties of A' mentioned after Definition 1.6, it clearly suffices to prove the case $A \leq E$. Assume then that $A = T \oplus R\alpha$. Then $S\beta \cap S\alpha\delta \leq T$ and we can write $A = (T - S\beta \cap S\alpha\delta) \oplus ((S\beta \cap S\alpha\delta) \oplus R\alpha)$ and, by Lemma 4.1, $R\beta \oplus (R\bar{\beta}\alpha)^{\bar{\beta}} = (S\beta \cap S\alpha\delta) \oplus R\alpha$. This shows that $\beta \backslash A = (T - S\beta \cap S\alpha\delta)^{\beta} \oplus R\bar{\beta}\alpha$. □

For general $A \in \mathcal{T}^+$ we have,

$$\beta\backslash(T + R\alpha) = (T - S\beta \cap S\alpha\delta)^{\beta} + R\bar{\beta}\alpha. \tag{5}$$

A consequence of this and Corollary 4.2 is the formula

$$\alpha_p\backslash\cdots\backslash\alpha_1\backslash A = O;$$

this formula is true even if A does not lie in $[O, E]$.

By Definition 2.3, a permutation π is intermediate to A if $R\pi$ lies in $[T^{\mathbf{u}}, A]$. We want to study braids of the form $\beta^+\gamma^+$. For that we need the following

Lemma 4.3 *If $A = T + R\alpha \in \mathcal{T}_0 \cap [O, E]$ admits an intermediate permutation π, then (i) T must be a T1 matrix and (ii) $\pi\backslash A = R\bar{\pi}\alpha$.*

PROOF:
Assume that for some $i < j < k$ we have $T_{ij} = T_{jk} = 1$ but that $T_{ik} = 0$. Since $R\pi = T^{\mathbf{u}} \oplus R\pi \cap R\alpha$ is T1, it follows that $R\pi_{ik} = R\alpha_{ik} = 1$ so by the T0 property for $R\alpha$ either $R\alpha_{ij}$ or $R\alpha_{jk}$ must be 1. Say $R\alpha_{ij} = 1$; then $A_{ij} = T_{ij} + R\alpha_{ij} = 2$, contradicting $A \leq E$. This proves (i). By (5) $\pi\backslash A = (A - R\pi)^{\pi} = ((T - T^{\mathbf{u}}) \oplus R\pi\delta \cap R\alpha)^{\pi} = U + R\bar{\pi}\alpha$ for some $U \in \mathcal{S}$, and the third of these matrices is upper triangular by Lemma 2.9 2. It follows that $U = O$. □

Recall from Definition 2.1 the concepts of initial and final set.

Proposition 4.4 *Assume that $A \in \mathcal{T}_0 \cap [O, E]$ and that $R\pi \in [O, A]$.*

1. *If π is maximal in $[O, A]$, then*

$$I(\bar{\pi}\alpha) \subset F(\pi). \tag{6}$$

2. *If π is an intermediate permutation, then π is maximal in A if and only if (6) holds.*

Proof:

If $J \subset [1, n-1]$ we denote its complement by J'.

To prove the first statement we show $F'(\pi) \subset I'(\bar{\pi}\alpha)$. If $i \notin F(\pi)$, let $j = i\bar{\pi},\;\; k = (i+1)\bar{\pi}$. Then $j < k$ and jk is a trivial final spot of $R\pi$. If $R\pi$ is maximal then $A_{jk} = 0$ for otherwise $R\pi < R\pi\tau_i \leq A$ contradicting maximality by Lemma 2.4. Let $B = \pi \backslash A = T \oplus R\bar{\pi}\alpha$ for some $T \in \mathcal{S}$. Then $B_{i,i+1} = A_{jk} = 0$ so that $R(\bar{\pi}\alpha)_{i,i+1} = 0$ and $i \notin I(\bar{\pi}\alpha)$.

For the second statement, if jk is a trivial final spot of $R\pi$ then $j\pi \notin I(\bar{\pi}\alpha)$ by (6) so that $R\alpha_{j,k} = A_{j,k} = 0$ and $R\pi$ must be maximal by Lemma 2.4. □

The following definition can be found in [1, § 2].

Definition 4.5 *A braid $b \in \boldsymbol{B}_n^+$ has a* **canonical decomposition** $b = \alpha_1^+ \cdots \alpha_p^+$*, if, for $i = 1, \ldots, p-1$, the $\alpha_i \in \Sigma_n$ and $I(\alpha_{i+1}) \subset F(\alpha_i)$. The integer p is the* **canonical length** *of b.*

Compare with formula (6). Say $q \leq p$ is the largest integer with $\alpha_q = \delta$ ($q = 0$ if all $\alpha_i \neq \delta$). Then $[1, n-1] = I(\delta) = I(\alpha_q) \subset F(\alpha_{q-1})$. Consequently [1, Lemma 2.7] $\alpha_{q-1} = \delta$ and, by induction, $\alpha_1 = \cdots = \alpha_q = \delta$; in that case $b \in [d^q, d^p]$.

Assume that B is intermediate in $A = T \oplus R\alpha \in \mathcal{T} \cap [O, E]$. Under the hypothesis that T is T1, $B - T$ is T1 if and only if the conditions $B_{ij} = B_{jk} = 1,\; B_{ik} = 0$ imply that precisely one of T_{ij} and T_{jk} must be 0. If we alter the requirements on T, we obtain a slightly different condition which we call, for the purposes of the next lemma, Condition A1:

The matrix B is **A1** if (i) B is an intermediate matrix of A and (ii) for all $i < j < k$, $B_{ij} = B_{jk} = 1$ and $B_{ik} = 0$ implies that both $T_{ij} = T_{jk} = 0$.

We do not require that T be T1 in this definition, but this is in fact automatic in most of the applications in view of Lemma 4.3.

Lemma 4.6 *Assume that $A = T \oplus R\alpha \in \mathcal{T}_0 \cap [O, E]$ admits an intermediate matrix B which is A1. Then* $\sup B \leq A$.

Proof:

We will show that under the hypothesis, $B^{(1)}$ is A1. By induction it will follow that all $B^{(s)}$ are A1, and in particular $\sup B$ is an intermediate matrix. The condition on B means that if $B_{ij} = B_{jk} = 1,\; B_{ik} = 0$, then necessarily $R\alpha_{ij} = R\alpha_{jk} = 1$ and, since $R\alpha$ is T1, $R\alpha_{ik} = 1 = A_{ik}$; this spot can be adjoined to B to obtain $B^{(1)} \leq A$. To check that $B^{(1)}$ is A1, assume that the

ij and jk spots of $B^{(1)}$ are non-trivial and that $B^{(1)}_{ik} = 0$. Clearly, we may assume that at least one of ij and jk is a trivial spot of B, for otherwise $T_{ij} = T_{jk} = 0$ by hypothesis because $B \leq B^{(1)}$ implies that $B_{ik} = 0$.

Case 1. Assume, for example, that $B_{ij} = 1$ and $T_{jk} = B_{jk} = 0$. Then, for some intermediate $j < l < k$, $B_{jl} = B_{lk} = 1$. If $B_{il} = 0$ the hypothesis on B implies that $T_{ij} = T_{jl} = 0$, and we are done. If $B_{il} = 1$, then this and $B_{lk} = 1$ imply $B^{(1)}_{ik} = 1$, contradicting our assumption.

Case 2. If both $B_{ij} = B_{jk} = 0$, then clearly the same is true of the matrix T.

□

As a consequence we have,

Proposition 4.7 *A matrix $A \in \mathcal{T}_0 \cap [O, E]$ is the crossing matrix of a positive braid of canonical length ≤ 2 if, and only if, A admits intermediate permutations π. If π and ρ are any two such intermediate permutations, then so is $\pi \vee \rho$. Consequently there is a unique maximal intermediate permutation μ and A determines the braid $\mu^+(\bar{\mu}\alpha)^+$ of canonical length ≤ 2, and the map $C : [d^0, d^2] \to \mathcal{T}_0 \cap [O, E]$ is one-to-one.*

Proof:

The first statement follows immediately from Lemma 4.3 and Proposition 4.4. For the rest of this Proposition, we must show that $B = R\pi \cup R\rho$ is A1. Assume, therefore, that, for $i < j < k$, $B_{ij} = B_{jk} = 1$ and that $B_{ik} = 0$. By Lemma 4.3, T is a T1 matrix; therefore at least one of the spots ij or jk of T must be trivial. Say $T_{ij} = 0$; then either $R\pi$ or $R\rho$ must be non-trivial at the ij spot. Assume $R\pi_{ij} = 1$. If $T_{jk} = 1 = R\pi_{jk}$, then $R\pi_{ik} = B_{ik} = 1$ contradicting our assumption. Therefore $T_{jk} = 0$ as well.

By Lemma 4.6, it follows that $\sup B \leq A$; thus $\pi \vee \rho$ is an intermediate permutation. There are only finitely many intermediate permutations π_ι; consequently, there is a maximal such permutation $\mu = \bigvee_\iota \pi_\iota$. By Lemma 4.3, $\mu\backslash A = R(\bar{\mu}\alpha)$ and $A = C(\mu^+(\bar{\mu}\alpha)^+)$. □

Another corollary of Formula (4) is

Corollary 4.8 *If $\alpha, \beta \in \Sigma_n$, the following are equivalent:*

1. $\alpha \leq \beta$,

2. $R\alpha \oplus (R\bar{\alpha}\beta)^{\bar{\alpha}} = R\beta$*, and*

3. $\alpha^+(\bar{\alpha}\beta)^+ = \beta^+$*.*

Proof:

If $\alpha \leq \beta$ then $\alpha\backslash R\beta = T \oplus R\bar{\alpha}\beta$ by formaula (5). On the other hand $(R\beta - R\alpha)^\alpha$ is upper triangular by Lemma 2.9 2. Thus $T = O$. This proves 2.

If 2 holds $C(\alpha^+(\bar{\alpha}\beta)^+) = R\alpha \oplus (R\bar{\alpha}\beta)^{\bar{\alpha}} = R\beta = C(\beta^+)$. All braids involved are of canonical length ≤ 2. Therefore they are equal, and 3 is proved.

Clearly 3 implies $C(\alpha^+) \leq C(\beta^+)$, that is, $\alpha \leq \beta$. □

5 Canonical Decompositions and Crossing Matrices.

We want to generalize partially Proposition 4.4 2. We start with the following

Lemma 5.1 *Assume that* $b = \beta^+\gamma^+$ *is the canonical decomposition of* b*, that* a *is a positive braid with* $p(a) = \alpha$*, and that* $C(ab) \leq E$*. Then* $I(\gamma) \subset F(\alpha\beta)$ *and the matrix* $R\alpha\beta$ *is maximal in* $S\alpha\beta + R\alpha\beta\gamma$*.*

Proof:

By canonicity, if $k \in I(\gamma)$, then $k \in F(\beta)$. In matrix terms, this says that, if $i' = (k+1)\bar{\beta}$ and $j' = k\bar{\beta}$, then $R\beta_{i'j'} = 1$. Now, if $i\alpha = i'$, $j\alpha = j'$, then strands i and j cross precisely once in $a\beta^+$, so $R\alpha\beta_{ij} = 1$. For second statement, from Proposition 4.4 and formula (4), $R\alpha\beta$ is maximal in $M = S\alpha\beta \cap S\alpha\beta\gamma\delta \oplus R\alpha\beta\gamma$. Since $M \leq N = S\alpha\beta + R\alpha\beta\gamma$ and M and N have the same trivial spots in the upper triangle, the maximality of $R\alpha\beta$ in N follows from Lemma 2.4 2. □

The following partial generalization of Proposition 4.4 follows from Lemma 5.1 by induction:

Proposition 5.2 *Suppose that* a *has canonical decomposition* $\alpha_1^+ \cdots \alpha_p^+$ *and that it has crossing matrix* $\leq E$*. Then, for* $1 \leq i \leq p-1$, $R\alpha_1 \cdots \alpha_i$ *is maximal in* $S\alpha_1 \cdots \alpha_i + R\alpha_1 \cdots \alpha_{i+1}$*.*

In general, the matrix $S\alpha_1 \cdots \alpha_i + R\alpha_1 \cdots \alpha_{i+1} \notin [O, E]$ but it is easily computed. However, the hypothesis that the crossing matrix be in $[O, E]$ is crucial here as the example $a = t_1^3$ shows; $\tau_1^+\tau_1^+\tau_1^+$ is the canonical factorization of a but $R\tau_1^2 = O$ is not maximal in $S\tau_1^2 + R\tau_1^3 = R\tau_1$.

Proposition 5.3 *Suppose that $A \leq E$ is realizable. Let $a = \beta^+\gamma^+$ be the canonical decomposition of a braid of canonical length 2 and $b = \pi^+ r$, $r \in \boldsymbol{B}_n^+$, another braid, not necessarily in canonical form, with $C(a) = C(b) = A$. Then $\pi \leq \beta$.*

PROOF:
Before the proof, we make the general remark that if $R\beta_{il} = 0$ and $A_{il} = 1$, then strands i and l of a must cross in γ^+ and consequently A_{li} must be trivial since i and l cannot cross and recross in γ^+. Also, the equality of the crossing matrices implies that i and l must cross in b only once. For the proof we argue by contradiction. Assume that there exists a pair (i, l), with $i < l$, for which $R\pi_{il} = 1$ and $R\beta_{il} = 0$ and, among all such pairs, choose one for which $l\beta - i\beta$ is minimal. First notice that necessarily $R\gamma_{i\beta, l\beta} = 1$ and consequently, $l\beta - i\beta \neq 1$, or equivalently, that strands i and l cannot be adjacent at the end of β^+ because, in that case, $i\beta$ would be in $I(\gamma)$ but not in $F(\beta)$ and this contradicts the canonicity of the factorization $a = \beta^+\gamma^+$. Therefore there exists at least one index j with $i\beta < j\beta < l\beta$.

Second, we observe that $j \notin [i, l]$ because this would imply that $R\beta_{ij} = R\beta_{jl} = 0$ and, since either $R\pi_{ij}$ or $R\pi_{jl}$ must be 1, then one of the pairs (i, j) or (j, l) contradicts the minimality assumption on (i, l). Assume, for instance, that $j < i$, the case $j > l$ being completely symmetric. From all j satisfying these properties ($j < i$, $i\beta < j\beta < l\beta$), choose one for which $j\beta$ is largest, or equivalently, one for which the j strand is closest to the l strand at the end of β^+. By our general remark, strands i and l may not cross in r and the j strand must cross the i strand in $\pi^+ r$. If j crosses i before i crosses l, then j must also cross l, for otherwise j must recross i in π^+, and that is impossible in a permutation braid. If j crosses i after i crosses l, then j must also cross l since i and l never recross. Either way, j crosses l in b and so j must also cross l in a, and it must do so in γ^+. The conclusion is that $l\beta - j\beta > 1$ because if this difference is 1, in the same way as before, we obtain a contradiction to the canonicity of the factorization $a = \beta^+\gamma^+$. Consequently, there exists a k such that $i\beta < j\beta < k\beta < l\beta$, $k\beta = j\beta + 1$, and, by the maximality condition imposed on j, necessarily $l < k$.

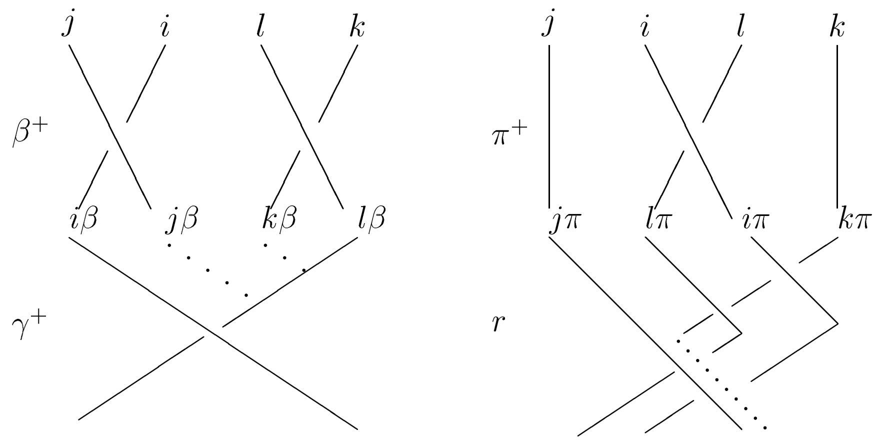

Figure 1: Proposition 5.3

In the braid $\pi^+ r$ strands j and k must both cross i and l and, as before, they must do so in r because, if they crossed in π^+, the minimality of the pair (i, l) would be violated. Also, strands j and k must never cross because, if they did, this would again violate the canonicity of the factorization of a. But the only way in which j and k cross both i and l in r, without crossing each other, is if one

of j and k crosses both i and l twice (see figure 1) and this is impossible because in $\beta^+\gamma^+$, j crosses l once and k crosses i only once, namely, in γ^+. This contradiction completes the proof. □

Theorem 5.4 *If $A \leq E$ is realizable by a braid of canonical length 2, then it cannot be realized by any braid of canonical length ≥ 3. In particular the braid a is in $[d^0, d^2]$ if and only if $C(a) \leq E$ and $C(a)$ admits an intermediate order reversal matrix in $[Ta^{\boldsymbol{u}}, C(a)]$.*

Proof:

By Proposition 4.7, it suffices to show: if A admits an intermediate π, then no braid of canonical length ≥ 3 realizes it. We reason by contradiction; choose a counter-example $A = C(\alpha_1^+ \cdots \alpha_p^+) = C(\beta^+\gamma^+)$, with minimal $p \geq 3$. Then Proposition 5.3 shows that $\alpha_1 \leq \beta$, and so, by Corollary 4.8, $\alpha_1^+(\bar{\alpha}_1\beta)^+ = \beta^+$. Thus $\alpha_1 \backslash A = C(\alpha_2^+ \cdots \alpha_p^+) = C((\bar{\alpha}_1\beta)^+\gamma^+)$ realizes a braid of canonical length ≤ 2. By the minimality of p, it follows that $\alpha_2^+ \cdots \alpha_p^+ = (\bar{\alpha}_1\beta)^+\gamma^+$ and so that $p-1 \leq 2$. If $p \leq 2$ we are done; if $p = 3$, then $C(\alpha_2^+\alpha_3^+) = C((\bar{\alpha}_1\beta)^+\gamma^+)$ and Proposition 4.6 imply that $\alpha_2^+\alpha_3^+ = (\bar{\alpha}_1\beta)^+\gamma^+$. Consequently $\alpha_1^+\alpha_2^+\alpha_3^+ = \beta^+\gamma^+$. This is a contradiction. □

Example 5.5 *Uniqueness fails for braids of canonical length ≥ 3.*

If $a = t_1^2 t_2^2$ and $b = t_2^2 t_1^2$, then a and b have canonical length three (for instance, $a = (\tau_1)^+(\tau_1\tau_2)^+\tau_2^+)$, and $C(a) = C(b) \in [O, E]$. Thus, the injectivity of C does not extend beyond canonical length two. It is also important to remark that, while $C([d^0, d^2]) \subset [O, E]$, there are braids of large canonical length whose crossing matrices lie in $[O, E]$. For example, the braid $t_1^2 \cdots t_{n-1}^2$ has canonical length $n+1$ and its crossing matrix consists of ones in the spots $i, i+1$ and $i+1, i$, $i = 1, \ldots, n-1$ and zeros everywhere else. On the other hand observe that the equation $C(x) = E$ in $\mathbf{B}_n^+$ has a unique solution, namely, $x = d^2$, because E is realizable by $x = d^2$ and by Theorem 5.4, no other positive braid can realize E.

6 Pure Braids.

The kernel of the homomorphism $p : \mathbf{B}_n \to \Sigma_n$ is $\mathbf{P}_n$. It is important to remark here that $\mathbf{B}_n^+$ is a semi-group whose presentation (as a semi-group) is identical to the presentation of $\mathbf{B}_n$ (as a group). This fact is known as the Garside Lemma (see [3] and [5, 9.2.5]); however, it is **not true** that the semi-group $\mathbf{P}_n^+$ admits the presentation of $\mathbf{P}_n$ given in [2, Lemma 4.2, p. 20]; clearly, the generators a_{ij} do not lie in $\mathbf{P}_n^+$. Even if we modify these generators to the b_{ij} defined in § 3, which do lie in $\mathbf{P}_n^+$, the resulting set is not a semi-group generating set. For example, the braid $t_1 t_2^2 t_1 = b_{12} b_{13} b_{23}^{-1}$. We have already established that, if $b \in \mathbf{P}_n^+$, then $C(b) \in \mathcal{S}_0^+$. Naturally, if $A \in \mathcal{S}_0^+ \cap [O, E]$ is also T1, then $A = S\pi$ for some $\pi \in \Sigma_n$ and A is realized only by $b = \pi^+\bar{\pi}^+$, because $\pi^+\bar{\pi}^+$ is the canonical factorization of b. See Proposition 4.6.

Lemma 6.1 *Any matrix in $\mathcal{S}_0^+$ is of the form $\bigcup_{i=1}^p S\alpha_i$, for finitely many $\alpha_i \in \Sigma_n$.*

Proof:

We use the following simple construction. Suppose that $U \in [O, D]_0$, and that $1 \leq i < n$. Then $Z_i U$ is the matrix V defined by

1. $V_{hk} = 0$ if $h < i$;

2. $V_{ik} = U_{ik}$, and

3. if $i < j < k$, then $V_{jk} = 1$ if and only if $U_{ik} = 1$ and $U_{ij} = 0$.

It is easy to show that $Z_i U \leq U$ and that $Z_i U$ is both T0 and T1 and thus, of the form $R\alpha_i$. Clearly, then, $U = \bigcup R\alpha_i$, and $U + U^{\mathbf{t}} = \bigcup S\alpha_i$. □

Lemma 6.2 *Unions of one or two matrices of the form $S\pi$ are realizable.*

Proof:

We have already shown that $S\pi = C(\pi^+\bar{\pi}^+)$. Unions of the form $S\alpha \cup S\beta$ are also realizable because $S\alpha \cup S\beta = C(\alpha^+(\bar{\alpha}\beta)^+(\bar{\beta})^+)$, by Corollary 4.2. □

Lemmas 6.1 and 6.2 lead us to conjecture that $C(\mathbf{P}_n^+) = \mathcal{S}_0^+$.

Lemma 6.3 *For $n = 3$, $C(\boldsymbol{P}_3^+) = \mathcal{S}(3)_0^+$ and $C(\boldsymbol{B}_3^+) = \mathcal{T}(3)_0^+$.*

Proof:

For $n = 3$ there are eight symmetric matrices in $[O, E]$, and only one of them, which we will call A, is not T0 and it is defined by $A_{13} = A_{31} = 1$, and otherwise $A_{ij} = 0$. Of the remaining seven, six are of the form $S\pi$, $\pi \in \Sigma_3$, and the seventh is $S\tau_1 \cup S\tau_2$, which is realizable by Lemma 6.2. By Lemma 3.5, all symmetric positive and T0 3×3 matrices are realizable. For the second assertion notice that, for $n = 3$, the only matrices of $\mathcal{T}(3)_0^+ \cap [O, E]$ not in $(\mathcal{S}(3)_0^+ + R(\Sigma_3)) \cap [O, E]$ are the $A + R\tau_i$, $i = 1, 2$, which are realized by $t_1 t_2^2$ and $t_2 t_1^2$, respectively. Again Lemma 3.5 proves the assertion. □

Theorem 6.4 *For $n \geq 3$, the semi-group $\boldsymbol{P}_n^+$ is not finitely generated.*

Proof:

We first treat the case $n = 3$.

Observe first that $\mathcal{S}(3)_0^+$ is not a finitely generated (additive) semi-group, for if $T^1, \ldots, T^q$ is a finite set of matrices in $\mathcal{S}(3)_0^+$ and N is the maximum of the $T_{1,3}^i$, then the symmetric matrix T with $T_{12} = T_{23} = 1$ and $T_{13} = 2N + 1$

is not a linear positive combination of the T^i. Indeed, if $T = \sum n_i T^i$, then $\sum n_i T^i_{13} = 2N + 1$ implies that $\sum n_i \geq 3$. Since, for each i either T^i_{12} or T^i_{23} is non trivial, it follows that one of the sums $\sum n_i T^i_{12}$ or $\sum n_i T^i_{23}$ is ≥ 2. Thus, no finite set of T^j can generate $\mathcal{S}(3)^+_0$.

To see that $\mathbf{P}^+_3$ is not finitely generated, note that $C : \mathbf{P}^+_3 \to \mathcal{S}(3)^+_0$ is a semi-group epimorphism and therefore, that a finite set of generators of $\mathbf{P}^+_3$ would give a finite set of generators of $\mathcal{S}(3)^+_0$.

Finally, to prove the general case, note that for $n > 3$ we have a natural embedding $\mathbf{B}^+_3 \subset \mathbf{B}^+_n$ obtained by viewing $\mathbf{B}^+_3$ as the subsemi-group of $\mathbf{B}^+_n$ generated by t_1 and t_2. This embedding preserves pure braids. By Garside's Lemma any product $b_1, \ldots, b_q$ of braids in $\mathbf{B}^+_n$ which lies in $\mathbf{B}^+_3$ must have each factor b_i in $\mathbf{B}^+_3$. Thus, any set of generators of $\mathbf{P}_n \cap \mathbf{B}^+_n$ must include a set of generators for the positive braids in $\mathbf{P}_3$. □

Unfortunately, we have been unable to generalize Lemma 6.3 for $n \geq 4$. We conjecture that $C(\mathbf{P}^+_n) = \mathcal{S}^+_0$, but the assertion that $C(\mathbf{B}^+_n) = \mathcal{T}^+_0$ is false already when $n = 4$.

Example 6.5 *The following matrices lie in $\mathcal{T}^+_0$ but are not realizable:*

$$G = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad K = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

If a matrix A is realizable, then there exists at least one $i \in [1, n-1]$ with $R\tau_i \leq A$ and $\tau_i \backslash A \in \mathcal{T}_0$. To see this, assume that $A = C(b)$, $b \in \mathbf{B}^+_n$. Then $b = t_i c$ for some i and some positive braid c. Thus $\tau_i \backslash A = C(c)$ and so, in particular, it is T0. This fails in the case of G and K.

If $A = T + R\alpha$ is realizable, T is not necessarily T0. For example, change spots 13 and 31 to zeros in either G or K above. The results are realizable (by $t_3 t_2^2 t_1 \in \mathbf{B}_4$ and $t_3 t_2 t_4^2 t_3 \in \mathbf{B}_5$, respectively) but their corresponding symmetric matrices are not T0.

References

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

[2] V.L. Hansen, Braids and Coverings, London Mathematical Society Student Texts 18.(Cambridge University Press, 1989).

[3] F.A. Garside, *The braid group and other groups. Quart. J. Math. Oxford* (2)**20**(1969) 235–254.

[4] J. McCool, *On basis-conjugating automorphisms of free groups*, Can. J. *Math.* **38**(1986) 1525–1529.

[5] W. Thurston, *Braid groups. in* D. Epstein *et al.*, Word Processing in Groups (Jones and Bartlett, 1992) 181–209.