EULER TOTIENT OF SUBFACTOR PLANAR ALGEBRAS

SÉBASTIEN PALCOUX

(Communicated by Adrian Ioana)

ABSTRACT. We extend Euler's totient function (from arithmetic) to any irreducible subfactor planar algebra, using the Möbius function of its biprojection lattice, as Hall did for the finite groups. We prove that if it is nonzero, then there is a minimal 2-box projection generating the identity biprojection. We explain a relation with a problem of K.S. Brown. As an application, we define the dual Euler totient of a finite group and we show that if it is nonzero, then the group admits a faithful irreducible complex representation. We also get an analogous result at depth 2, involving the central biprojection lattice.

1. INTRODUCTION

Any finite group G acts outerly on the hyperfinite II_1 factor R, and the group subfactor $(R \subseteq R \rtimes G)$, of index $|G|$, remembers the group [5]. Jones proved in [6] that the set of possible values for the index $|M : N|$ of a subfactor $(N \subseteq M)$ is

$$\{4\cos^2(\frac{\pi}{n}) \mid n \geq 3\} \sqcup [4, \infty].$$

By Galois correspondence [13], the lattice of intermediate subfactors of $(R \subseteq R \rtimes G)$ is isomorphic to the subgroup lattice of G. Moreover, Watatani [21] extended the finiteness of the subgroup lattice to any irreducible finite index subfactor. Then, the subfactor theory can be seen as an augmentation of the finite group theory, where the indices are not necessarily integers. The notion of subfactor planar algebra [8] is a diagrammatic axiomatization of the standard invariant of a finite index II_1 subfactor [7]. Bisch [2] proved that the intermediate subfactors are given by the biprojections (see Definition 3.1) in the 2-box space of the corresponding planar algebra. The recent results of Liu [12] on the biprojections are also crucial for this paper (see Section 3).

The usual Euler's totient function $\varphi(n)$ counts the number of positive integers up to n that are relatively prime to n. Let G be a finite group and let μ be the Möbius function (see Definition 4.1) of its subgroup lattice $\mathcal{L}(G)$. Hall proved in [4] that the Euler totient of G (defined below) is the cardinal of $\{g \in G \mid \langle g \rangle = G\}$.

$$\varphi(G) := \sum_{H \in \mathcal{L}(G)} \mu(H, G)|H|.$$

So if $\varphi(G)$ is nonzero, then G is cyclic, and $\varphi(C_n) = \varphi(n)$. This implication will be generalized in Section 5, as the author did with Ore's theorem in [15, 16]. Let $\mathcal{P}$ be an irreducible subfactor planar algebra and let μ be the Möbius function of its biprojection lattice $[e_1, \mathrm{id}]$. We use the notation of Definition 3.3. Let the Euler totient of $\mathcal{P}$ be

$$\varphi(\mathcal{P}) := \sum_{b \in [e_1, \mathrm{id}]} \mu(b, \mathrm{id})|b : e_1|.$$

Theorem 1.1. *If $\varphi(\mathcal{P})$ is nonzero, then $\mathcal{P}$ is w-cyclic (i.e., there is a minimal 2-box projection generating the identity biprojection).*

Then, for any finite group G, by considering $\mathcal{P}(R^G \subset R)$, we get that if the dual Euler totient

$$\hat{\varphi}(G) := \sum_{H \in \mathcal{L}(G)} \mu(1, H)|G : H|$$

is nonzero, then G has a faithful irreducible complex representation. It is a dual version of the initial implication. As a general application, we get a nontrivial upper bound for the minimal number of minimal central projections generating the identity biprojection. By applying this result to any finite group G, we deduce a nontrivial upper bound for the minimal number of irreducible components for a faithful complex representation of G. It involves the subgroup lattice and indices only. It is a link between combinatorics and representations in finite group theory. These results were not known to group theorists, and the author can provide a group theoretical translation of the proofs as he did in [17] for the dual Ore's theorem.

This path of research leads to (Section 6) a generalization of a problem of K.S. Brown (considered hard in [19]) and to a possible counterexample of Watatani's problem [21] on whether any finite lattice has a biprojection lattice representation.

We finally prove an additional result for the irreducible subfactor planar algebras of depth 2, involving the central biprojection lattice. The dual group case recovers a known result involving the normal subgroup lattice.

2. BASICS ON LATTICE THEORY

A *lattice* $(L, \wedge, \vee)$ is a poset L in which every two elements a, b have a unique supremum (or *join*) $a \vee b$ and a unique infimum (or *meet*) $a \wedge b$. Let G be a finite group. The set of subgroups $K \subseteq G$ forms a lattice, denoted by $\mathcal{L}(G)$, ordered by $\subseteq$, with $K_1 \vee K_2 = \langle K_1, K_2 \rangle$ and $K_1 \wedge K_2 = K_1 \cap K_2$. A *sublattice* of $(L, \wedge, \vee)$ is a subset $L' \subseteq L$ such that $(L', \wedge, \vee)$ is also a lattice. If $a, b \in L$ with $a \leq b$, then the *interval* $[a, b]$ is the sublattice $\{c \in L \mid a \leq c \leq b\}$. Any finite lattice is *bounded*, i.e., admits a minimum and a maximum, denoted by $\hat{0}$ and $\hat{1}$. The *atoms* are the minima of $L \setminus \{\hat{0}\}$. The *coatoms* are the maxima of $L \setminus \{\hat{1}\}$. Consider a finite lattice, b the join of its atoms, and t the meet of its coatoms; then let's call $[\hat{0}, b]$ and $[t, \hat{1}]$ its *bottom* and *top intervals*. A lattice is *distributive* if the join and meet operations distribute over each other.

A distributive bounded lattice is called *Boolean* if any element b admits a unique *complement* $b^{\complement}$ (i.e., $b \wedge b^{\complement} = \hat{0}$ and $b \vee b^{\complement} = \hat{1}$). The subset lattice of $\{1, 2, \ldots, n\}$, with union and intersection, is called the Boolean lattice $\mathcal{B}_n$ of rank n. Any finite Boolean lattice is isomorphic to some $\mathcal{B}_n$.

Remark 2.1. A finite lattice is Boolean if and only if it is *uniquely atomistic*; i.e., every element can be written uniquely as a join of atoms. It follows that if $[a, b]$ and $[c, d]$ are intervals in a Boolean lattice, then

$$[a, b] \vee [c, d] := \{k \vee k' \mid k \in [a, b], k' \in [c, d]\}$$

is the interval $[a \vee c, b \vee d]$.

We refer to [20] for more details.

3. Subfactor planar algebras and biprojections

For the notions of subfactor, subfactor planar algebra, and basic properties, we refer to [7–9]. See also [14, Section 3] for a short introduction. Let $(N \subseteq M)$ be a finite index irreducible subfactor. The n-box spaces $\mathcal{P}_{n,+}$ and $\mathcal{P}_{n,-}$ of the planar algebra $\mathcal{P} = \mathcal{P}(N \subseteq M)$ are $N' \cap M_{n-1}$ and $M' \cap M_n$. Let $R(a)$ be the range projection of $a \in \mathcal{P}_{2,+}$. We define the relations $a \preceq b$ by $R(a) \leq R(b)$ and $a \sim b$ by $R(a) = R(b)$. Let $e_1 := e_N^M$ and id $:= e_M^M$ be the Jones and the identity projections in $\mathcal{P}_{2,+}$. Let tr be the normalized trace (i.e., $\mathrm{tr}(\mathrm{id}) = 1$). Then $\mathrm{tr}(e_1) = |M : N|^{-1} = \delta^{-2}$. Let $\mathcal{F} : \mathcal{P}_{2,\pm} \to \mathcal{P}_{2,\mp}$ be the Fourier transform (1-click or 90° rotation) and let $a * b = \mathcal{F}(\mathcal{F}^{-1}(a) \cdot \mathcal{F}^{-1}(b))$ be the coproduct of $a, b \in \mathcal{P}_{2,\pm}$. If a, b are positive, then so is $a * b$ by [12, Theorem 4.1].

Definition 3.1 ([12, Definition 2.14]). A *biprojection* is a nonzero projection $b \in \mathcal{P}_{2,\pm}$ with $\mathcal{F}(b)$ a multiple of a projection.

Note that $e_1 = e_N^M$ and id $= e_M^M$ are biprojections.

Theorem 3.2 ([2, p 212]). *A projection $b \in \mathcal{P}_{2,+}$ is a biprojection if and only if it is the Jones projection e_K^M of an intermediate subfactor $N \subseteq K \subseteq M$.*

Therefore, the set of biprojections is a lattice of the form $[e_1, \mathrm{id}]$.

Definition 3.3. Consider the intermediate subfactors $N \subseteq K_1 \subseteq K_2 \subseteq M$, and let $b_i \in [e_1, \mathrm{id}]$ be the biprojection $e_{K_i}^M$. We define $\mathcal{P}(b_1, b_2) := \mathcal{P}(K_1 \subseteq K_2)$ and

$$|b_2 : b_1| := \mathrm{tr}(b_2) / \mathrm{tr}(b_1) = |K_2 : K_1|.$$

Definition 3.4. Consider $a \in \mathcal{P}_{2,+}$ positive, and let p_n be the range projection of $\sum_{k=1}^{n} a^{*k}$. By finiteness, there exists N such that for all $m \geq N$, $p_m = p_N$, which is a biprojection [12, Lemma 4.14], denoted $\langle a \rangle$, called the *biprojection generated by a*. It is the smallest biprojection $b \succeq a$. For S a finite set of positive elements of $\mathcal{P}_{2,+}$, let $\langle S \rangle$ be $\langle \sum_{s \in S} s \rangle$.

Proposition 3.5 ([15]). *Let $p \in \mathcal{P}_{2,+}$ be a minimal central projection. Then, there exists $u \leq p$ a minimal projection such that $\langle u \rangle = \langle p \rangle$.*

Definition 3.6 ([15]). A planar algebra $\mathcal{P}$ is *weakly cyclic* (or *w-cyclic*) if it satisfies one of the following equivalent assertions:

- $\exists u \in \mathcal{P}_{2,+}$ a minimal projection such that $\langle u \rangle = \mathrm{id}$,
- $\exists p \in \mathcal{P}_{2,+}$ a minimal central projection such that $\langle p \rangle = \mathrm{id}$.

4. EULER TOTIENT

We define a notion of Euler totient on the irreducible subfactor planar algebras as an extension of the usual Euler's totient function on the positive integers.

Definition 4.1. The *Möbius function* μ of a finite poset P is defined inductively as follows. For $a, b \in P$ with $a \leq b$,

$$\mu(a, b) := \begin{cases} 1 & \text{if } a = b, \\ -\sum_{c \in (a,b]} \mu(c, b) & \text{otherwise.} \end{cases}$$

The following result can be seen as a Boolean representation for the Möbius function of a finite lattice.

Theorem 4.2 (Crosscut theorem). *Let L be a finite lattice and let $a_1, \ldots, a_n$ be its coatoms. Consider the (order-reversing) map $m : \mathcal{B}_n \to L$ such that*

$$m(I) = \begin{cases} \hat{1} & \text{if } I = \emptyset, \\ \bigwedge_{i \in I} a_i & \text{otherwise.} \end{cases}$$

Then for any $a \in L$,

$$\mu(a, \hat{1}) = \sum_{I \in m^{-1}(\{a\})} (-1)^{|I|}.$$

Proof. It is a reformulation of [20, Corollary 3.9.4] on $[a, \hat{1}]$ with its coatoms. $\square$

Definition 4.3. Let $\mathcal{P}$ be an irreducible subfactor planar algebra with biprojection lattice $[e_1, \text{id}]$ and Möbius function μ. For any $b_1, b_2 \in [e_1, \text{id}]$ with $b_1 \leq b_2$, consider

$$\varphi(b_1, b_2) := \sum_{b \in [b_1, b_2]} \mu(b, b_2) |b : b_1|.$$

The *Euler totient* of $\mathcal{P}$ is $\varphi(\mathcal{P}) := \varphi(e_1, \text{id})$.

Remark 4.4. Let $\hat{\mathcal{P}}$ be the dual subfactor planar algebra of $\mathcal{P}$. Then

$$\varphi(\mathcal{P}) = \sum_{b \in [e_1, \text{id}]} \mu(b, \text{id}) |b : e_1| \qquad \text{and} \qquad \varphi(\hat{\mathcal{P}}) = \sum_{b \in [e_1, \text{id}]} \mu(e_1, b) |\text{id} : b|,$$

because the biprojection lattice of $\hat{\mathcal{P}}$ is the reverse of that of $\mathcal{P}$.

Lemma 4.5 ([4]). *The Euler totient of a finite group G,*

$$\varphi(G) := \sum_{H \in \mathcal{L}(G)} \mu(H, G) |H|,$$

is the cardinal of $\{g \in G \mid \langle g \rangle = G\}$.

Proof. By Theorem 4.2 with its map $m : \mathcal{B}_n \to \mathcal{L}(G)$,

$$\varphi(G) = \sum_{H \in \mathcal{L}(G)} \sum_{\alpha \in m^{-1}(\{H\})} (-1)^{|\alpha|} |H| = \sum_{\alpha \in \mathcal{B}_n} (-1)^{|\alpha|} |m(\alpha)|.$$

Then, by the inclusion-exclusion principle, $\varphi(G) = |G \setminus \bigcup_i m(\{i\})|$. $\square$

Corollary 4.6. *A finite group G is cyclic if and only if $\varphi(G)$ is nonzero.*

Proof. If G is cyclic, then $G = C_n$ for some positive integer n, and $\varphi(G) = \varphi(n) \neq 0$. Conversely, if $\varphi(G) \neq 0$, then G is cyclic by Lemma 4.5. $\square$

Note that $\varphi(\mathcal{P}(R \subseteq R \rtimes G)) = \varphi(G)$ and $\varphi(C_n) = \varphi(n)$, the usual Euler's totient function of n. Thus, we can see $\mathcal{P} \mapsto \varphi(\mathcal{P})$ as an extension from the positive integers to the irreducible subfactor planar algebras. The following proposition extends the usual formula that if $n = \prod_i p_i^{n_i}$ is the prime factorization of n, then

$$\varphi(n) = \prod_i p_i^{n_i - 1} \cdot \prod_i (p_i - 1).$$

Proposition 4.7. *Let* $[t, \mathrm{id}]$ *be the top interval of* $[e_1, \mathrm{id}]$. *Then*

$$\varphi(\mathcal{P}) = |t : e_1| \cdot \varphi(t, \mathrm{id}).$$

Proof. If $b \notin [t, \mathrm{id}]$, then $\mu(b, \mathrm{id}) = 0$ by Theorem 4.2 because $m^{-1}(\{b\}) = \emptyset$. Next if $b \in [t, \mathrm{id}]$, then $|b : e_1| = |b : t| \cdot |t : e_1|$, since the index is multiplicative [6]. □

5. Main result

In this section, we generalize one way of Corollary 4.6 by the following theorem. We will see later with Remark 7.12 that the converse is false in general.

Theorem 5.1. *An irreducible subfactor planar algebra* $\mathcal{P}$ *is w-cyclic if its Euler totient* $\varphi(\mathcal{P})$ *is nonzero.*

Proof. Let $p_1, \ldots, p_r$ be the minimal central projections of $\mathcal{P}_{2,+}$. Consider the sum

$$S(i) := \sum_{b \in [e_1, \mathrm{id}]} \mu(b, \mathrm{id}) \, \mathrm{tr}(bp_i).$$

By Theorem 4.2 with its map $m : \mathcal{B}_n \to [e_1, \mathrm{id}]$,

$$S(i) = \sum_{b \in [e_1, \mathrm{id}]} \sum_{\beta \in m^{-1}(\{b\})} (-1)^{|\beta|} \, \mathrm{tr}(bp_i) = \sum_{\beta \in \mathcal{B}_n} (-1)^{|\beta|} \, \mathrm{tr}(m(\beta)p_i).$$

Recall that the map m is order-reversing and the image of the atoms of $\mathcal{B}_n$ are the coatoms of $[e_1, \mathrm{id}]$; let's call these latter ones $b_1, \ldots, b_n$. Let A_i be the set of atoms α of $\mathcal{B}_n$ satisfying $p_i \leq m(\alpha)$, and let B_i be the set of atoms not in A_i. Let α_i (resp. β_i) be the join of all the elements of A_i (resp. B_i).

Claim. For $\alpha \in \mathcal{B}_n$, $p_i \leq m(\alpha) \Leftrightarrow \alpha \in [\alpha_i, \hat{1}]$.

Proof. Just observe that $p_i \leq \bigwedge_{j \in \alpha} b_j$ if and only if $\forall j \in \alpha, \ p_i \leq b_j$. □

Now by Remark 2.1, we have

$$\mathcal{B}_n = [\emptyset, \alpha_i] \vee [\emptyset, \beta_i] = \bigsqcup_{\alpha \in [\emptyset, \alpha_i]} \alpha \vee [\emptyset, \beta_i].$$

Consider the following sum:

$$T(i) := \sum_{\beta \in [\emptyset, \beta_i]} (-1)^{|\beta|} \, \mathrm{tr}(m(\beta)p_i).$$

For any $\alpha \in [\emptyset, \alpha_i]$ and $\beta \in [\emptyset, \beta_i]$, we have $(-1)^{|\alpha \vee \beta|} = (-1)^{|\alpha|}(-1)^{|\beta|}$ and

$$m(\alpha \vee \beta)p_i = m(\alpha)p_i \wedge m(\beta)p_i = m(\beta)p_i.$$

So we get that

$$S(i) = \sum_{\alpha \in [\emptyset, \alpha_i]} (-1)^{|\alpha|} T(i) = T(i) \cdot (1 - 1)^{|A_i|}.$$

Claim. The planar algebra $\mathcal{P}$ is w-cyclic if and only if $\exists i$ with $|A_i| = 0$.

Proof. It is w-cyclic if and only if $\exists i$ with $\langle p_i \rangle = \mathrm{id}$, if and only if for any coatom $b \in [e_1, \mathrm{id}]$, $p_i \not\le b$, and if and only if $|A_i| = 0$. □

If $\mathcal{P}$ is not w-cyclic, then $\forall i$ $|A_i| \ne 0$, so $S(i) = 0$; but $|b : e_1| = \mathrm{tr}(b)/\mathrm{tr}(e_1)$, $\mathrm{tr}(b) = \sum_i \mathrm{tr}(bp_i)$, and $\mathrm{tr}(e_1) = \delta^{-2}$, so $\varphi(e_1, \mathrm{id}) = \delta^2 \sum_{i=1}^r S(i) = 0$. □

It is a double generalization of [1, Theorem 3.10] from groups to subfactors and from Boolean lattice to any lattice. It is also a purely combinatorial criterion for a subfactor planar algebra to be w-cyclic.

6. Generalization of a problem of K.S. Brown

We will explain how this path of research leads to a generalization of a problem of K.S. Brown in finite group theory and to a possible counterexample of the problem of Watatani on representing any finite lattice as a biprojection lattice.

Proposition 6.1. *Assume that every biprojection is central. Then*

$$\varphi(\mathcal{P}) = \delta^2 \sum_{\langle p_i \rangle = \mathrm{id}} \mathrm{tr}(p_i)$$

with $p_1, \ldots, p_r$ the minimal central projections of $\mathcal{P}_{2,+}$.

Proof. First of all, $|b : e_1| = \mathrm{tr}(b)/\mathrm{tr}(e_1)$ and $\mathrm{tr}(e_1) = \delta^{-2}$, so

$$\varphi(\mathcal{P}) = \delta^2 \sum_{b \in [e_1, \mathrm{id}]} \mu(b, \mathrm{id}) \, \mathrm{tr}(b).$$

By Theorem 4.2 with its map $m : \mathcal{B}_n \to [e_1, \mathrm{id}]$,

$$\varphi(\mathcal{P}) = \delta^2 \sum_{\beta \in \mathcal{B}_n} (-1)^{|\beta|} \, \mathrm{tr}(m(\beta)),$$

but every biprojection is central, so by the inclusion-exclusion principle

$$\varphi(\mathcal{P}) = \delta^2[\mathrm{tr}(\mathrm{id}) - \mathrm{tr}(R[\sum_{i=1}^n m(\{i\})])] = \delta^2 \sum_{\langle p_i \rangle = \mathrm{id}} \mathrm{tr}(p_i). \qquad \square$$

It follows that the converse of Theorem 5.1 is true if every biprojection is central. If moreover they form a Boolean lattice, then by [15, Theorem 4.26], $\mathcal{P}$ is w-cyclic, so $\varphi(\mathcal{P})$ is nonzero, and without assuming the biprojections to be central, $\mathcal{P}$ is still w-cyclic by [16, Theorem 5.9], and $\varphi(\mathcal{P})$ is suspected to still be nonzero:

Conjecture 6.2. *If $[e_1, \mathrm{id}]$ is Boolean, then $\varphi(\mathcal{P})$ is nonzero.*

Remark 6.3. If $[e_1, \mathrm{id}]$ is Boolean of rank $n + 1$, we wonder whether $\varphi(\mathcal{P}) \ge \phi^n$, with ϕ the golden ratio. If this lower bound is correct, then it is optimal as realized by the tensor product $\mathcal{TLJ}(\sqrt{2}) \otimes \mathcal{TLJ}(\phi)^{\otimes n}$, thanks to [15, Theorem 4.8].

By Theorem 5.1, a proof of Conjecture 6.2 would be stronger than [16]. This conjecture can be seen as the Boolean restriction of the following planar algebraic generalization of a problem of K.S. Brown (considered hard in [19]):

Conjecture 6.4. *Let $\mathcal{P}$ be an irreducible subfactor planar algebra. Then its Euler characteristic (defined below) is nonzero:*

$$\chi(\mathcal{P}) := - \sum_{b \in [e_1, \mathrm{id}]} \mu(b, \mathrm{id}) | \, \mathrm{id} : b |.$$

Gaschütz proved the usual Brown's problem, i.e., for $\mathcal{P}(R \subseteq R \rtimes G)$, if G is solvable.

It is an extension of Conjecture 6.2 because by Remark 4.4, $\chi(\mathcal{P}) = \pm\varphi(\hat{\mathcal{P}})$ if $[e_1, \mathrm{id}]$ is Boolean (of rank n), because then $\mu(e_1, b) = (-1)^n \mu(b, \mathrm{id})$. This last equality holds more generally for any Eulerian lattice, which is a graded lattice such that $\mu(a, b) = (-1)^{|b|-|a|}$ for $a \leq b$, with $a \mapsto |a|$ the rank function. This leads us to:

Conjecture 6.5. *If $[e_1, \mathrm{id}]$ is Eulerian, then $\varphi(\mathcal{P})$ is nonzero, and so $\mathcal{P}$ is w-cyclic.*

The last part of Conjecture 6.5, deduced from the first together with Theorem 5.1, would provide an extension of Ore's theorem [16, Theorem 5.9] from top Boolean to top Eulerian lattices (notation: a lattice is called top X if its top interval is X). Note that the face lattice of any convex polytope is Eulerian [20, Proposition 3.8.9].

Proposition 6.6. *An Eulerian subgroup lattice (of a finite group) is Boolean.*

*Proof.* If $\mathcal{L}(G)$ is Eulerian, then $\mu(1, G) = \pm 1$, but [11, Théorème 3.1] states that

$$\mu(1, G) \in \frac{|G|}{|G : G'|_0} \mathbb{Z}$$

with G' the commutator subgroup of G and $|G : G'|_0$ the square-free part of $|G : G'|$. Then $|G| = |G : G'|_0$, and so $G' = 1$. It follows that G is abelian with $|G|$ square-free, so G is cyclic of square-free order and $\mathcal{L}(G)$ is Boolean. $\square$

It is unknown whether Proposition 6.6 extends to any interval. This leads us to:

Question 6.7. Is there an irreducible subfactor planar algebra with a non-Boolean Eulerian biprojection lattice?

It is unknown whether any finite lattice admits a biprojection lattice representation [21, 22], even in the group-subgroup case, so the smallest non-Boolean Eulerian lattice (the face lattice of the square polytope below) could be a counterexample.
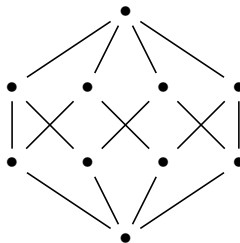
7. APPLICATIONS

We will deduce a nontrivial upper bound from Theorem 5.1 providing a link between combinatorics and representations in finite group theory by translating.

Definition 7.1. The *Euler totient* of an interval of finite groups $[H, G]$ is

$$\varphi(H, G) := \sum_{K \in [H,G]} \mu(K, G)|K : H|.$$

Note that $\varphi(\mathcal{P}(R \rtimes H \subseteq R \rtimes G)) = \varphi(H, G)$.

Corollary 7.2. *There is $g \in G$ with $\langle Hg \rangle = G$ if and only if $\varphi(H, G)$ is nonzero.*

Proof. By Proposition 6.1 or directly, let $M_1, \ldots, M_n$ be the coatoms of $[H, G]$. Then, as for the proof of Lemma 4.5,

$$|H|\varphi(H, G) = |G \setminus \bigcup M_i|,$$

so that $\varphi(H, G)$ is the cardinal of $\{Hg \mid g \in G \text{ and } \langle Hg \rangle = G\}$. $\square$

Corollary 7.3. *The minimal cardinal for a generating set of a finite group G is the minimal length ℓ for an ordered chain of subgroups*

$$\{e\} = H_0 < H_1 < \cdots < H_\ell = G$$

such that $\varphi(H_i, H_{i+1})$ is nonzero.

Proof. A subset $\{g_1, \ldots, g_n\}$ is generating iff there is an ordered chain of subgroups

$$\{e\} = K_0 < K_1 < \cdots < K_n = G$$

with $K_{i+1} = \langle K_i, g_{i+1} \rangle = \langle K_i g_{i+1} \rangle$, iff $\varphi(K_i, K_{i+1})$ is nonzero by Corollary 7.2. $\square$

So, the minimal cardinal for a generating set of a finite group G depends only on the subgroup lattice and indices (known to [4]). We will generalize Corollary 7.3 by a nontrivial upper bound. Let $\mathcal{P}$ be an irreducible subfactor planar algebra.

Lemma 7.4 ([15]). *Let $b_1 < b_2$ be biprojections. If $\mathcal{P}(b_1, b_2)$ is w-cyclic, then there is a minimal projection $u \in \mathcal{P}_{2,+}$ such that $b_2 = \langle b_1, u \rangle$.*

Theorem 7.5. *The minimal number r of minimal projections generating the identity biprojection (i.e., $\langle u_1, \ldots, u_r \rangle = \mathrm{id}$) is at most the minimal length ℓ for an ordered chain of biprojections*

$$e_1 = b_0 < b_1 < \cdots < b_\ell = \mathrm{id}$$

such that $\varphi(b_i, b_{i+1})$ is nonzero.

Proof. Consider a chain as above. By Theorem 5.1, $\mathcal{P}(b_i, b_{i+1})$ is w-cyclic, so by Lemma 7.4, there is a minimal projection $u_{i+1} \in \mathcal{P}_{2,+}$ such that $b_{i+1} = \langle b_i, u_{i+1} \rangle$. It follows that $\langle u_1, \ldots, u_\ell \rangle = \mathrm{id}$. $\square$

We deduce weak dual versions of Corollaries 7.2, 4.6, and 7.3, giving the link between combinatorics and representation theory:

Definition 7.6. The *dual Euler totient* of the interval $[H, G]$ is

$$\hat{\varphi}(H, G) := \sum_{K \in [H,G]} \mu(H, K)|G : K|.$$

Note that $\varphi(\mathcal{P}(R^G \subseteq R^H)) = \hat{\varphi}(H, G)$.

Definition 7.7. Let W be a representation of a group G, K a subgroup of G, and X a subspace of W. Let the *fixed-point subspace* be

$$W^K := \{w \in W \mid kw = w \ , \forall k \in K\}$$

and the *pointwise stabilizer subgroup* be

$$G_{(X)} := \{g \in G \mid gx = x \ , \forall x \in X\}.$$

Definition 7.8. An interval of finite group $[H, G]$ is said to be *linearly primitive* if there is an irreducible complex representation V of G with $G_{(V^H)} = H$.

Theorem 7.9 ([15])**.** *The planar algebra $\mathcal{P}(R^G \subseteq R^H)$ is w-cyclic if and only if the interval of finite groups $[H, G]$ is linearly primitive.*

Corollary 7.10. *If the dual Euler totient $\hat{\varphi}(H, G)$ is nonzero, then the interval of finite groups $[H, G]$ is linearly primitive.*

Proof. Apply Theorem 5.1 to $\mathcal{P}(R^G \subseteq R^H)$ and then Theorem 7.9.   □

In particular, let the dual Euler totient of G be $\hat{\varphi}(G) := \hat{\varphi}(1, G)$. Then:

Corollary 7.11. *A finite group G admits a faithful irreducible complex representation if its dual Euler totient $\hat{\varphi}(G)$ is nonzero.*

Proof. It follows from Corollary 7.10 because $G_{(V)} = \ker(\pi_V)$.   □

It is a purely combinatorial criterion for a finite group to have an irreducible faithful complex representation.

Remark 7.12. The converse is false. The modular maximal-cyclic group $M_4(2)$ (of order 16) has a faithful irreducible complex representation, whereas $\hat{\varphi}(M_4(2)) = 0$. This is not surprising because according to Proposition 4.7, $\varphi(e_1, \mathrm{id}) \neq 0$ if and only if $\varphi(t, \mathrm{id}) \neq 0$ with $[t, \mathrm{id}]$ the top interval of $[e_1, \mathrm{id}]$, and the bottom interval of $[1, M_4(2)]$ is $[1, C_2^2]$. Even if we assume that $[1, G]$ is its own bottom interval, the converse is still false: there are exactly two counterexamples of index ≤ 100, given by $G = D_8 \rtimes C_2^2$ or $D_8 \rtimes S_3$ (of order 64 and 96 respectively).

Theorem 7.13 ([3, §226])**.** *A complex representation V of a finite group G is faithful if and only if for any irreducible complex representation W there is an integer n such that $W \preceq V^{\otimes n}$.*

Corollary 7.14. *The minimal number of irreducible components for a faithful complex representation of G is at most the minimal length ℓ for an ordered chain of subgroups*

$$\{e\} = H_0 < H_1 < \cdots < H_\ell = G$$

such that $\hat{\varphi}(H_i, H_{i+1})$ is nonzero.

Proof. Consider a chain as above. By Corollary 7.5 applied to $\mathcal{P}(R^G \subseteq R)$, we have $\langle u_1, \ldots, u_\ell \rangle = \mathrm{id}$, with u_i a minimal projection. Let p_i be the central support of u_i. Then $\langle p_1 + \cdots + p_\ell \rangle = \mathrm{id}$. But the coproduct of two minimal central projections is given by the tensor product of the associated irreducible representations of G [16, Corollary 7.5]. So by Definition 3.4 and Theorem 7.13, the representation $V_1 \oplus \cdots \oplus V_\ell$ (with V_i the irreducible complex representation $\mathrm{im}(p_i)$) is faithful.   □

Note that Corollary 7.14 extends to any finite dimensional Kac algebra as for [16, Remark 6.14]. It can also be improved by taking for H_0 any core-free subgroup of H_1 (instead of just $\{e\}$), thanks to [16, Lemma 6.13]. In particular:

Corollary 7.15. *A finite group G admits a faithful irreducible complex representation if there is a core-free subgroup $H < G$ with $\hat{\varphi}(H, G)$ nonzero.*

This criterion is more efficient than Corollary 7.11 (consider for example G simple), but it is no more purely combinatorial.

Question 7.16. Is the converse of Corollary 7.15 true?

8. ADDITIONAL RESULT FOR DEPTH 2

We can prove an additional result in the depth 2 case (involving the central biprojection lattice) coming from the fact that the irreducible depth 2 subfactor planar algebras correspond to the Kac algebras [10]. Note that the group subfactors are depth 2, since the group algebras are examples of Kac algebras.

Theorem 8.1 (Splitting, [10, p 39]). *Let $\mathcal{P}$ be an irreducible depth 2 subfactor planar algebra. Any element $x \in \mathcal{P}_{2,+}$ splits as follows:*
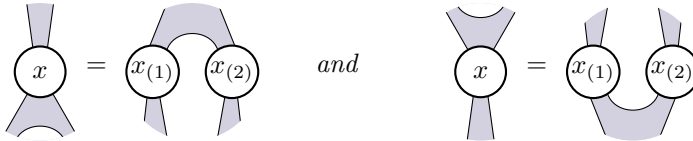
Note that $\Delta(x) = x_{(1)} \otimes x_{(2)}$ is the sumless Sweedler notation for the comultiplication of the corresponding Kac algebra.

Corollary 8.2. *If $a, b \in \mathcal{P}_{2,+}$ are central, then so is the coproduct $a * b$.*

Proof. This diagrammatic proof by splitting is due to Vijay Kodiyalam:

$$(a * b) \cdot x = \cdots = x \cdot (a * b).$$

$\square$
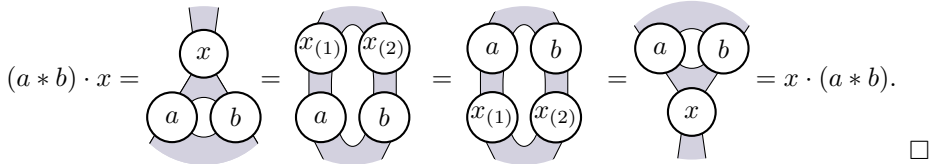
Corollary 8.3. *The set of central biprojections is a sublattice of $[e_1, \mathrm{id}]$.*

Proof. Let b_1, b_2 be central biprojections. Then $b_1 \wedge b_2$ is central, and $b_1 \vee b_2$ is the range projection of $(b_1 * b_2)^{*k}$ for k large enough and so is central by Corollary 8.2. $\square$

Let $\mathcal{C}$ be the central biprojection lattice and let $\mu_{\mathcal{C}}$ be its Möbius function. Let the central Euler totient of $\mathcal{P}$ be

$$\varphi_{\mathcal{C}}(\mathcal{P}) := \sum_{b \in \mathcal{C}} \mu_{\mathcal{C}}(b, \mathrm{id}) |b : e_1|.$$

Theorem 8.4. *Let $p_1, \ldots, p_r$ be the minimal central projections of $\mathcal{P}_{2,+}$. Then*

$$\varphi_{\mathcal{C}}(\mathcal{P}) = \delta^2 \sum_{\langle p_i \rangle = \mathrm{id}} \mathrm{tr}(p_i).$$

Proof. By Corollary 8.2, a central projection generates a central biprojection. The rest of the proof is identical to that of Proposition 6.1. □

Corollary 8.5. *Let $\mathcal{P}$ be an irreducible subfactor planar algebra of depth 2. Then $\mathcal{P}$ is w-cyclic if and only if $\varphi_{\mathcal{C}}(\mathcal{P})$ is nonzero.*

Remark 8.6. The last three results extend to any irreducible subfactor planar algebra in which any central projection generates a central biprojection.

The rest is only translation. Let G be a finite group, let $\mathcal{N}(G)$ be its normal subgroup lattice. and let $\mu_{\mathcal{N}}$ be the Möbius function of $\mathcal{N}(G)$. Let the dual normal Euler totient be

$$\hat{\varphi}_{\mathcal{N}}(G) := \sum_{H \in \mathcal{N}(G)} \mu_{\mathcal{N}}(1, H)|G : H|.$$

Corollary 8.7. *A finite group G has a faithful irreducible complex representation if and only if $\hat{\varphi}_{\mathcal{N}}(G)$ is nonzero.*

Proof. Apply Corollary 8.5 on $\mathcal{P}(R^G \subseteq R)$ or Theorem 8.4 with $V_i = \text{im}(p_i)$; then

$$\hat{\varphi}_{\mathcal{N}}(G) = \sum_{V_i \text{ faithful}} \dim(V_i)^2.$$

□

The above equality can be proved directly from the content of page 97 in [18].

Acknowledgments

References

[1] Mamta Balodi and Sebastien Palcoux, *On Boolean intervals of finite groups*, J. Combin. Theory Ser. A **157** (2018), 49–69, DOI 10.1016/j.jcta.2018.02.004. MR3780407

[2] Dietmar Bisch, *A note on intermediate subfactors*, Pacific J. Math. **163** (1994), no. 2, 201–216. MR1262294

[3] W. Burnside, *Theory of groups of finite order*, 2d ed, Dover Publications, Inc., New York, 1955. MR0069818

[4] Philip Hall, *The Eulerian functions of a group*, Q. J. Math., Oxf. Ser. **7** (1936), 134–151.

[5] Vaughan F. R. Jones, *Actions of finite groups on the hyperfinite type* II_1 *factor*, Mem. Amer. Math. Soc. **28** (1980), no. 237, v+70, DOI 10.1090/memo/0237. MR587749

[6] V. F. R. Jones, *Index for subfactors*, Invent. Math. **72** (1983), no. 1, 1–25, DOI 10.1007/BF01389127. MR696688

[7] V. Jones and V. S. Sunder, *Introduction to subfactors*, London Mathematical Society Lecture Note Series, vol. 234, Cambridge University Press, Cambridge, 1997. MR1473221

[8] Vaughan F. R. Jones, *Planar algebras, I* (1999), 122 pp., available at `arXiv:math/9909027`. to appear in New Zealand J. of Math.

[9] Vijay Kodiyalam and V. S. Sunder, *On Jones' planar algebras*, J. Knot Theory Ramifications **13** (2004), no. 2, 219–247, DOI 10.1142/S021821650400310X. MR2047470

[10] Vijay Kodiyalam, Zeph Landau, and V. S. Sunder, *The planar algebra associated to a Kac algebra*, Proc. Indian Acad. Sci. Math. Sci. **113** (2003), no. 1, 15–51, DOI 10.1007/BF02829677. Functional analysis (Kolkata, 2001). MR1971553

[11] Charles Kratzer and Jacques Thévenaz, *Fonction de Möbius d'un groupe fini et anneau de Burnside* (French), Comment. Math. Helv. **59** (1984), no. 3, 425–438, DOI 10.1007/BF02566359. MR761806

[12] Zhengwei Liu, *Exchange relation planar algebras of small rank*, Trans. Amer. Math. Soc. **368** (2016), no. 12, 8303–8348, DOI 10.1090/tran/6582. MR3551573

[13] Masahiro Nakamura and Zirô Takeda, *On the fundamental theorem of the Galois theory for finite factors*, Proc. Japan Acad. **36** (1960), 313–318. MR0123926

[14] Sebastien Palcoux, *Ore's theorem for cyclic subfactor planar algebras and applications*, 50 pp., available at `arXiv:1505.06649v10`.

[15] Sebastien Palcoux, *Ore's theorem on cyclic subfactor planar algebras and beyond*, Pacific J. Math. **292** (2018), no. 1, 203–221, DOI 10.2140/pjm.2018.292.203. MR3708264

[16] Sebastien Palcoux, *Ore's theorem on subfactor planar algebras*, 14 pp., available at `arXiv: 1704.00745`. Under review.

[17] Sebastien Palcoux, *Dual Ore's theorem on distributive intervals of finite groups*, J. Algebra **505** (2018), 279–287, DOI 10.1016/j.jalgebra.2018.03.017. MR3789914

[18] P. P. Pálfy, *On faithful irreducible representations of finite groups*, Studia Sci. Math. Hungar. **14** (1979), no. 1-3, 95–98 (1982). MR645518

[19] John Shareshian and Russ Woodroofe, *Order complexes of coset posets of finite groups are not contractible*, Adv. Math. **291** (2016), 758–773, DOI 10.1016/j.aim.2015.10.018. MR3459029

[20] Richard P. Stanley, *Enumerative combinatorics. Volume 1*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 49, Cambridge University Press, Cambridge, 2012. MR2868112

[21] Yasuo Watatani, *Lattices of intermediate subfactors*, J. Funct. Anal. **140** (1996), no. 2, 312–334, DOI 10.1006/jfan.1996.0110. MR1409040

[22] Feng Xu, *On representing some lattices as lattices of intermediate subfactors of finite index*, Adv. Math. **220** (2009), no. 5, 1317–1356, DOI 10.1016/j.aim.2008.11.006. MR2493615

INSTITUTE OF MATHEMATICAL SCIENCES, CHENNAI, INDIA

Current address: Harish-Chandra Research Institute, Allahabad, Uttar Pradesh, 211019 India

Email address: `sebastienpalcoux@gmail.com`