NEW BEAUVILLE SURFACES, MODULI SPACES AND FINITE GROUPS

SHELLY GARION, MATTEO PENEGINI

Abstract. In this paper we construct new Beauville surfaces with group either $\mathrm{PSL}(2, p^e)$, or belonging to some other families of finite simple groups of Lie type of low Lie rank, or an alternating group, or a symmetric group, proving a conjecture of Bauer, Catanese and Grunewald. The proofs rely on probabilistic group theoretical results of Liebeck and Shalev, on classical results of Macbeath and on recent results of Marion. In addition, we give the asymptotic growth of the number of connected components of the moduli space of surfaces of general type corresponding to certain families of Beauville surfaces. We extend some of these results to the case of surfaces isogenous to a higher product.

1. Introduction

A *Beauville surface* S (over $\mathbb{C}$) is a particular kind of surface isogenous to a higher product of curves, i.e., $S = (C_1 \times C_2)/G$ is a quotient of a product of two smooth curves C_1, C_2 of genera at least two, modulo a free action of a finite group G, which acts faithfully on each curve. For Beauville surfaces the quotients C_i/G are isomorphic to $\mathbb{P}^1$ and both projections $C_i \to C_i/G \cong \mathbb{P}^1$ are coverings branched over three points. A Beauville surface is in particular a minimal surface of general type.

Beauville surfaces were introduced by F. Catanese in [Cat00], inspired by a construction of A. Beauville (see [B]). The two authors were interested in finding new examples of surfaces with $p_g = q = 0$ and of general type, which provide an interesting class of surfaces (see e.g. [BCG08]). As a matter of fact a Beauville surface has $q = 0$, but p_g can attain any non negative value. Since [Cat00] had appeared, many authors have been studying Beauville surfaces, see [BC, BCG05, BCG06, BCG08, FG, FGJ, FJ].

Nevertheless, many questions are still open in the study of such surfaces. For example, it is interesting to know which finite groups G can occur for some Beauville surfaces. Moreover, these surfaces are rigid, i.e., they have no nontrivial deformations. Hence they represent points in the moduli space of surfaces of general type. A natural question is whether we are able to estimate the number of these points. In this article we shall give partial answers to these questions using a group theoretical approach.

In the following subsections we shall present the notations, the known results and our main theorems. In Section 2 we shall present the geometrical background, and explain the link between geometry and group theory. In Section 3 one can find the proofs of the main results using group theory.

2000 *Mathematics Subject Classification.* 14J10,14J29,20D06,20H10,30F99.

1.1. **Groups of Beauville Surfaces.** Working out the definition of Beauville surfaces one sees that there is a pure group theoretical condition which characterizes the groups of Beauville surfaces: the existence of what in [BCG05] and [BCG06] is called a "Beauville structure".

Definition 1.1. *An* unmixed Beauville structure *for a finite group G is a quadruple $(x_1, y_1; x_2, y_2)$ of elements of G, which determines two triples $T_i := (x_i, y_i, z_i)$ $(i = 1, 2)$ of elements of G such that :*

(i) $x_i y_i z_i = 1$,

(ii) $\langle x_i, y_i \rangle = G$,

(iii) $\Sigma(T_1) \cap \Sigma(T_2) = \{1\}$, *where*

$$\Sigma(T_i) := \bigcup_{g \in G} \bigcup_{j=1}^{\infty} \{g x_i^j g^{-1}, g y_i^j g^{-1}, g z_i^j g^{-1}\}.$$

Moreover, $\tau_i := (\mathrm{ord}(x_i), \mathrm{ord}(y_i), \mathrm{ord}(z_i))$ is called the *type* of T_i, and a type which satisfies the condition:

$$\frac{1}{\mathrm{ord}(x_i)} + \frac{1}{\mathrm{ord}(y_i)} + \frac{1}{\mathrm{ord}(z_i)} < 1$$

is called *hyperbolic*.

A detailed explanation of this link between surfaces and finite groups will be given in Section 2.1, where we shall present a more general definition related to surfaces isogenous to a higher product.

Therefore, the question of which finite groups G admit an unmixed Beauville structure was raised. The following Theorem summarizes the known results.

Theorem 1.2. *The following groups admit an unmixed Beauville structure:*

(1) *The alternating groups A_n admit unmixed Beauville structures if and only if $n \geq 6$;*
(2) *The symmetric groups S_n admit unmixed Beauville structures if and only if $n \geq 5$;*
(3) *The groups* $\mathrm{SL}(2, p)$ *and* $\mathrm{PSL}(2, p)$ *for every prime $p \neq 2, 3, 5$;*
(4) *The Suzuki groups* $\mathrm{Sz}(2^p)$*, where p is an odd prime;*
(5) *A finite abelian group G admits an unmixed Beauville structure if and only if $G = (\mathbb{Z}/n\mathbb{Z})^2$ with $(n, 6) = 1$;*
(6) *For every prime p, there exists a $p-$group which admits an unmixed Beauville structure.*

Proof. Part (1) was proven in [BCG05], [BCG06] for n large enough, and it was later generalized in [FG]. Part (2) was proven for $n \geq 7$ in [BCG06], and it was later improved in [FG]. Parts (3), (4) and (5) appeared in [BCG05] (for part (5) see also [Cat00]). Part (6) is a consequence of (5) for $p \geq 5$, and the proof for $p = 2, 3$ appeared in [FGJ]. □

The question of which finite groups admit an unmixed Beauville structure is deeply related to the question of which finite groups are quotients of certain triangle groups, which was widely investigated (see [Co90] for a survey). Indeed, conditions *(i)* and *(ii)* of Definition 1.1 clearly imply that two certain triangle groups surject onto the finite group G. However, the question about Beauville structures is somewhat more delicate, due to condition *(iii)* of Definition 1.1.

The following Theorem regarding alternating groups, generalizing part (1) of Theorem 1.2, was conjectured by Bauer, Catanese and Grunewald in [BCG05, BCG06], who were inspired by the proof of Everitt [Ev] to Higman's Conjecture that every hyperbolic triangle group surjects to all but finitely many alternating groups.

Theorem 1.3. *Let $(r_1, s_1, t_1), (r_2, s_2, t_2)$ be two hyperbolic types. Then almost all alternating groups A_n admit an unmixed Beauville structure $(x_1, y_1; x_2, y_2)$ where $(x_1, y_1, (x_1y_1)^{-1})$ has type (r_1, s_1, t_1) and $(x_2, y_2, (x_2y_2)^{-1})$ has type (r_2, s_2, t_2).*

A similar Theorem also applies for symmetric groups.

Theorem 1.4. *Let $(r_1, s_1, t_1), (r_2, s_2, t_2)$ be two hyperbolic types, and assume that at least two of (r_1, s_1, t_1) are even and at least two of (r_2, s_2, t_2) are even. Then almost all symmetric groups S_n admit an unmixed Beauville structure $(x_1, y_1; x_2, y_2)$ where $(x_1, y_1, (x_1y_1)^{-1})$ has type (r_1, s_1, t_1) and $(x_2, y_2, (x_2y_2)^{-1})$ has type (r_2, s_2, t_2).*

The proofs of both Theorems are presented in Section 3.2, and are based on results of Liebeck and Shalev [LS04], who gave an alternative proof, based on probabilistic group theory, to Higman's Conjecture. We also provide similar Theorems for surfaces isogenous to a higher product not necessarily Beauville.

The following Theorem generalizes part (3) of Theorem 1.2.

Theorem 1.5. *Let p be a prime number, and assume that $q = p^e$ is at least 7. Then the group $\mathrm{PSL}(2, q)$ admits an unmixed Beauville structure.*

This Theorem is proved in Section 3.3. The proof is based on properties of the groups $\mathrm{PSL}(2, q)$ and on results of Macbeath [Ma].

Moreover, one can generalize the previous Theorem, as well as part (4) of Theorem 1.2, and prove similar results regarding some other families of finite simple groups of Lie type of low Lie rank, provided that their defining field is large enough.

Theorem 1.6. *The following finite simple groups of Lie type $G = G(q)$ admit an unmixed Beauville structure, provided that q is large enough.*

1. *Suzuki groups, $G = \mathrm{Sz}(q) = ^2B_2(q)$, where $q = 2^{2e+1}$;*
2. *Ree groups, $G = ^2G_2(q)$, where $q = 3^{2e+1}$;*
3. *$G = G_2(q)$, where $q = p^e$ for some prime number $p > 3$;*
4. *$G = ^3D_4(q)$, where $q = p^e$ for some prime number $p > 3$;*
5. *$G = \mathrm{PSL}(3, q)$, where $q = p^e$ for some prime p;*
6. *$G = \mathrm{PSU}(3, q)$, where $q = p^e$ for some prime p.*

This Theorem is proved in Section 3.4, and the proof is based on recent probabilistic group theoretical results of Marion [Mar3.09, Mar9.09], who investigated the possible surjection of certain triangle groups onto finite simple groups of Lie type of low Lie rank.

Another Conjecture of Bauer, Catanese and Grunewald [BCG05, BCG06] is that all finite simple non-abelian groups, except A_5, admit an unmixed Beauville structure. Indeed, Theorems 1.5 and 1.6 are a first step towards a possible proof of this Conjecture for all finite simple groups of Lie type (assuming that their defining field is large enough). Moreover, in the same direction of Theorems 1.3 and 1.4, and inspired by conjectures of Liebeck and Shalev [LS05] (see also Section 3.4.2), we propose the following Conjecture.

Conjecture 1.7. Let $(r_1, s_1, t_1), (r_2, s_2, t_2)$ be two hyperbolic types. If G is a finite simple classical group of Lie type of Lie rank large enough, then it admits an unmixed Beauville structure $(x_1, y_1; x_2, y_2)$, where $(x_1, y_1, (x_1y_1)^{-1})$ has type (r_1, s_1, t_1) and $(x_2, y_2, (x_2y_2)^{-1})$ has type (r_2, s_2, t_2).

Considering finite abelian groups, in Section 3.5, we generalize part (5) of Theorem 1.2 for surfaces isogenous to a higher product not necessarily Beauville having irregularity $q = 0$.

1.2. **Moduli Spaces.** By a celebrated Theorem of Gieseker (see [G]), once the two invariants of a minimal surface S of general type, K_S^2 and $\chi(S)$, are fixed, then there exists a quasiprojective moduli space $\mathcal{M}_{K_S^2,\chi(S)}$ of minimal smooth complex surfaces of general type with those invariants, and this space consists of a finite number of connected components. The union $\mathcal{M}$ over all admissible pairs of invariants (K^2, χ) of these spaces is called the *moduli space of surfaces of general type.*

In [Cat00], Catanese studied the moduli space of surfaces isogenous to a higher product of curves (see Theorem 4.14). As a result, one obtains that the moduli space of surfaces isogenous to a higher product with fixed invariants: a finite group G and types (τ_1, τ_2) (where the types $\tau_i := (g_i'|m_{i,1}, ..., m_{i,r_i})$, for $i = 1, 2$, are defined in 2.4 and in 2.5 for the special case of surfaces with irregularity $q = 0$), consists of a finite number of connected components of $\mathcal{M}$. We remark here that since Beauville surfaces are rigid, a Beauville surface yields an isolated point in the moduli space. A group theoretical method to count the number of these components was given in [BC], and it was used, for example, in [BC, BCG08, Po, P], to count the connected components of the moduli space of surfaces isogenous to a higher product with $\chi(S) = 1$. Using this method, that will be presented in Section 2.2, we deduce the following Theorems, in which we use the following standard notations.

Notation 1.8. *Denote:*
- $h(n) = O(g(n))$, *if* $h(n) \leq cg(n)$ *for some positive constant* c, *as* $n \to \infty$.
- $h(n) = \Omega(g(n))$, *if* $h(n) \geq cg(n)$ *for some positive constant* c, *as* $n \to \infty$.
- $h(n) = \Theta(g(n))$, *if* $c_1g(n) \leq h(n) \leq c_2g(n)$ *for some positive constants* c_1, c_2, *as* $n \to \infty$.

Theorem 1.9. *Let* $\tau_1 = (r_1, s_1, t_1)$ *and* $\tau_2 = (r_2, s_2, t_2)$ *be two hyperbolic types and let* $h(A_n, \tau_1, \tau_2)$ *be the number of Beauville surfaces with group* A_n *and with types* (τ_1, τ_2). *Then*

$$h(A_n, \tau_1, \tau_2) = \Omega(n^6).$$

Theorem 1.10. *Let* $\tau_1 = (r_1, s_1, t_1)$ *and* $\tau_2 = (r_2, s_2, t_2)$ *be two hyperbolic types, and assume that at least two of* (r_1, s_1, t_1) *are even and at least two of*

(r_2, s_2, t_2) are even, and let $h(S_n, \tau_1, \tau_2)$ be the number of Beauville surfaces with group S_n and with types (τ_1, τ_2). Then

$$h(S_n, \tau_1, \tau_2) = \Omega(n^6).$$

The proofs of both theorems are presented in Section 3.2, and are based on results of Liebeck and Shalev [LS04]. We also provide similar Theorems for surfaces isogenous to a higher product which are not necessarily Beauville.

Theorem 1.11. *Let τ_1 and τ_2 be two hyperbolic types, let p be an odd prime, and consider the group $\mathrm{PSL}(2,p)$. Let $h(\mathrm{PSL}(2,p), \tau_1, \tau_2)$ be the number of Beauville surfaces with group $\mathrm{PSL}(2,p)$ and with types (τ_1, τ_2). Then*

$$h(\mathrm{PSL}(2,p), \tau_1, \tau_2) = O(p^3).$$

The proof of this Theorem appears in Section 3.3.

Theorem 1.12. *Let $n \in \mathbb{N}$ s.t. $(n, 6) = 1$, let $G_n = (\mathbb{Z}/n\mathbb{Z})^2$, and let $\tau_n = (n, n, n)$. Let $h((\mathbb{Z}/n\mathbb{Z})^2, \tau_n, \tau_n)$ be the number of Beauville surfaces with group $(\mathbb{Z}/n\mathbb{Z})^2$ and with types (τ_n, τ_n). Then*

$$h((\mathbb{Z}/n\mathbb{Z})^2, \tau_n, \tau_n) = \Theta(n^4).$$

The proof of this Theorem appears in Section 3.5, where we also provide similar Theorem for surfaces isogenous to a higher product not necessarily Beauville.

In Section 2.3 we use the above Theorems to study the growth of the number of connected components as a function of χ, showing that it has a polynomial bound.

Remark 1.13. After completing this manuscript, it was brought to our attention that Fuertes and Jones [FJ], have independently and simultaneously constructed unmixed Beauville structures for the groups $\mathrm{PSL}(2, q)$, the Suzuki groups $G = \mathrm{Sz}(q) = {}^2B_2(q)$ and the Ree groups $G = {}^2G_2(q)$, thus proving some of our results appearing in Theorems 1.5 and 1.6. However, their constructions are of different type.

Acknowledgement. The authors would like to thank Ingrid Bauer, Fabrizio Catanese and Fritz Grunewald for suggesting the problems and for many useful discussions. We are grateful to Bob Guralnick, Martin Liebeck, Martin Kassabov, Aner Shalev, Boris Kunyavskii and Eugene Plotkin for interesting discussions. We would like to thank Claude Marion for referring us to his recent results.

The authors acknowledge the support of the DFG Forschergruppe 790 “Classification of algebraic surfaces and compact complex manifolds”. The first author acknowledges the support of the European Post-Doctoral Institute and the Max-Planck-Institute for Mathematics in Bonn.

2. From Geometry to Group Theory and Back

We shall denote by S a smooth irreducible complex projective surface of general type. We shall also use the standard notation in surface theory, hence we denote by $p_g := h^0(S, \Omega_S^2)$ the *geometric genus* of S, $q := h^0(S, \Omega_S^1)$ the *irregularity* of S, $\chi(S) = 1 + p_g - q$ the *holomorphic Euler-Poincaré characteristic*, $e(S)$ the *topological Euler number*, and K_S^2 the *self-intersection* *of the canonical divisor*. In this Section, C will always denote a smooth compact complex curve and $g(C)$ will be its *genus* (see e.g. [BHPV]).

2.1. **Ramification Structures.**

Definition 2.1. *A surface S is said to be* isogenous to a higher product of curves *if and only if, equivalently, either:*

(i) S admits a finite unramified covering, which is isomorphic to a product of curves of genera at least two;
(ii) S is a quotient $(C_1 \times C_2)/G$, where C_1 and C_2 are curves of genus at least two, and G is a finite group acting freely on $C_1 \times C_2$.

By Proposition 3.11 of [Cat00] the two properties (i) and (ii) are equivalent. In [Cat00] is also proven that any surface isogenous to a higher product has a unique minimal realization as a quotient $(C_1 \times C_2)/G$, where G is a finite group acting freely and with the property that no element acts trivially on one of the two factors C_i. From now on we shall work only with minimal realization.

We have two cases: the *mixed* case where the action of G exchanges the two factors (and then C_1 and C_2 are isomorphic), and the *unmixed* case where G acts diagonally on their product.

A surface S isogenous to a higher product is in particular a minimal surface of general type and it has

$$K_S^2 = 8\chi(S), \text{ or equivalently, } 4\chi(S) = e(S), \tag{1}$$

by Theorem 3.4 of [Cat00]. Moreover, by Serrano [S, Proposition 2.2],

$$q(S) = g(C_1/G) + g(C_2/G), \tag{2}$$

see also [Cat00] paragraph 3. Since [Cat00] had appeared, several authors studied surfaces isogenous to a higher product, and eventually they classified all of them in case $\chi(S) = 1$, see [BC, BCG08, CP, HP, Pi, Po, P, Z].

A special case of surfaces isogenous to a higher product is given by Beauville surfaces, which were also defined in [Cat00].

Definition 2.2. *A* Beauville surface *is a surface isogenous to a higher product $S = (C_1 \times C_2)/G$, which is rigid, i.e., it has no nontrivial deformation.*

Remark 2.3. Every Beauville surface of mixed type has an unramified double covering which is a Beauville surface of unmixed type.

The rigidity property of the Beauville surfaces is equivalent to the fact that $C_i/G \cong \mathbb{P}^1$ and that the projections $C_i \to C_i/G \cong \mathbb{P}^1$ are branched in three points, for $i = 1, 2$. Moreover, by Equation (2) one has $q(S) = 0$.

In the following we shall consider only the *unmixed* case.

From the above Remark one can see that studying Beauville surfaces (as well as surfaces isogenous to a higher product in general) is strictly linked to the study of branched covering of complex curves. We shall recall Riemann's existence theorem which translates the geometric problem of constructing branch covering into a group theoretical problem. We state it first in great generality.

Definition 2.4. *Let $g', m_1, \dots, m_r$ be positive integers. An* orbifold surface group *of type $(g' \mid m_1, \dots, m_r)$ is a group presented as follows:*

$$\Gamma(g' \mid m_1, \dots, m_r) := \langle a_1, b_1, \dots, a_{g'}, b_{g'}, x_1, \dots, x_r | \\ x_1^{m_1} = \dots = x_r^{m_r} = \prod_{k=1}^{g'} [a_k, b_k] x_1 \cdot \ldots \cdot x_r = 1 \rangle.$$

If $g' = 0$ it is called a polygonal group*, if $g' = 0$ and $r = 3$ it is called a* triangle group*.*

We remark that an orbifold surface group is in particular a *Fuchsian group* (see e.g. [Br] and [LS04]).

From the above definition, an orbifold surface group is the factor group of the fundamental group of the complement, in a complex curve C' of genus g', of a set of r points $\{p_1, \dots, p_r\}$, obtained by dividing modulo the normal subgroup generated by $\gamma_1^{m_1}, \dots, \gamma_r^{m_r}$, where, for each i, γ_i is a simple geometric loop winding once around p_i counterclockwise.

By Riemann's existence theorem, giving an action of a finite group G on a curve C of genus $g \geq 2$ is equivalent to giving:

(i) The quotient curve $C' := C/G$;
(ii) The branch points set $\{p_1, \dots, p_r\} \subset C'$;
(iii) An isomorphism of the quotient of the fundamental group $\pi_1(C' - \{p_1, \dots, p_r\})$ with $\Gamma := \Gamma(g' \mid m_1, \dots, m_r)$, such that the given generators of Γ are image elements of a standard basis of $\pi_1(C' - \{p_1, \dots, p_r\})$;
(iv) A surjective homomorphism:

$$\theta : \Gamma \longrightarrow G; \tag{3}$$

(v) For $1 \leq i \leq r$, $\theta(x_i)$ is an element of order m_i;
(vi) The Riemann-Hurwitz formula holds:

$$2g - 2 = |G| \left(2g' - 2 + \sum_{i=1}^{r} (1 - \frac{1}{m_i}) \right). \tag{4}$$

Now we restrict ourselves to the case where the quotient curve is isomorphic to $\mathbb{P}^1$. Conditions *(iv)* and *(v)* suggest the following definition.

Definition 2.5. *Let G be a finite group and $r \in \mathbb{N}$ with $r \geq 2$.*

- *An $r-$tuple $T = (x_1, \dots, x_r)$ of elements of G is called a* spherical $r-$system of generators *of G if $\langle x_1, \dots, x_r \rangle = G$ and $x_1 \cdot \ldots \cdot x_r = 1$.*
- *We say that T is of* type $\tau := (m_1, \dots, m_r)$ *if the orders of $(x_1, \dots, x_r)$ are respectively $(m_1, \dots, m_r)$.*
- *We say that T has an* unordered type τ *if the orders of $(x_1, \dots, x_r)$ are $(m_1, \dots, m_r)$ up to a permutation, namely, if there is a permutation $\pi \in S_r$ such that*

$$\mathrm{ord}(x_1) = m_{\pi(1)}, \dots, \mathrm{ord}(x_r) = m_{\pi(r)}.$$

- *We shall denote:*

$$\mathcal{S}(G, \tau) := \{\textit{spherical } r-\textit{systems for } G \textit{ of type } \tau\}.$$

- *Moreover, two spherical $r-$systems $T_1 = (x_1, \dots, x_{r_1})$ and $T_2 = (x_1, \dots, x_{r_2})$ are said to be* disjoint*, if:*

$$\Sigma(T_1) \bigcap \Sigma(T_2) = \{1\}, \tag{5}$$

where

$$\Sigma(T_i) := \bigcup_{g \in G} \bigcup_{j=0}^{\infty} \bigcup_{k=1}^{r_i} g \cdot x_{i,k}^j \cdot g^{-1}.$$

We obtain that the datum of a surface isogenous to a higher product of unmixed type $S = (C_1 \times C_2)/G$ with $q = 0$ is determined, once we look at the monodromy of each covering of $\mathbb{P}^1$, by the datum of a finite group G together with two respective disjoint spherical $r-$systems of generators $T_1 := (x_1, \dots, x_{r_1})$ and $T_2 := (x_1, \dots, x_{r_2})$, such that the types of the systems satisfy (4) with $g' = 0$ and respectively $g = g(C_i)$. The condition of being disjoint ensures that the action of G on the product of the two curves $C_1 \times C_2$ is free. We remark here that this can be specialized to $r_i = 3$, and therefore can be used to construct Beauville surfaces. This description suggests the following definition.

Definition 2.6. *An* unmixed ramification structure *of size (r_1, r_2) for a finite group G, is a pair (T_1, T_2) of tuples $T_1 := (x_1, \dots x_{r_1})$, $T_2 := (x_1, \dots x_{r_2})$ of elements of G, such that (T_1, T_2) is a disjoint pair of spherical r_i-system of generators of G.*

The definition of an *unmixed Beauville structure* given in the introduction is a special case of the above definition for $r_1 = r_2 = 3$. Therefore, the problem of finding Beauville surfaces of unmixed type is now translated into the problem of finding finite groups G which admit an unmixed Beauville structure.

Remark 2.7. Note that a group G and an unmixed ramification structure (or equivalently a Beauville structure) for it determine the main invariants of the surface S. Indeed, as a consequence of the Segre-Zeuthen formula one has:

$$e(S) = 4\frac{(g(C_1) - 1)(g(C_2) - 1)}{|G|}. \tag{6}$$

Hence, by (1) and (4) we obtain:

$$4\chi(S) = 4(1+p_g) = |G| \cdot \left(-2 + \sum_{k=1}^{r_1}(1 - \frac{1}{m_{1,k}})\right) \cdot \left(-2 + \sum_{k=1}^{r_2}(1 - \frac{1}{m_{2,k}})\right), \tag{7}$$

and so, in the Beauville case,

$$4\chi(S) = 4(1 + p_g) = |G|(1 - \mu_1)(1 - \mu_2),$$

where

$$\mu_i := \frac{1}{m_{1,i}} + \frac{1}{m_{2,i}} + \frac{1}{m_{3,i}}, \quad (i = 1, 2). \tag{8}$$

Now, it is left to verify that indeed $g(C_1) \geq 2$ and $g(C_2) \geq 2$. This follows from Equation (4) and from the following Lemma.

Lemma 2.8. *Let G be a finite, non trivial group with an unmixed ramification structure (T_1, T_2) of size (r_1, r_2), then*

$$\mathbb{Z} \ni \frac{|G|\big(-2 + \sum_{k=1}^{r_i}(1 - \frac{1}{m_{i,k}})\big)}{2} + 1 \geq 2, \text{ for } i = 1, 2. \tag{9}$$

The fact that the number in (9) is an integer follows from Riemann's existence theorem. We need to prove that this integer is at least 2, namely that $\sum_{k=1}^{r_i}(1 - \frac{1}{m_{i,k}}) > 2$ for $i = 1, 2$. We shall give two proofs for this fact, a geometric one and a group theoretic one, both are based on results of Bauer, Catanese and Grunewald.

Geometrical proof. Let $S = (C_1 \times C_2)/G$ be a surface isogenous to a product with $q(S) = 0$, notice first that without loss of generality $g(C_1) \neq 1$.

Indeed, suppose that $g(C_1) = 1$, then $S \to C_2/G \cong \mathbb{P}^1$ is an elliptic fibration with fibre isomorphic to C_1 or to a multiple of C_1. Since C_1 is an elliptic curve, the Segre-Zeuthen Theorem holds in the following form:

$$e(S) = 4\big(g(C_1) - 1\big)\big(g(C_2/G) - 1\big) = 0.$$

Since S is isogenous to a product $4\chi(S) = e(S) = 0$, but we have $\chi(S) = 1 + p_g - q = 1 + p_g > 0$. Hence $g(C_1) \neq 1$.

Second, suppose that S is a $\mathbb{P}^1$-bundle. Then S cannot be non-rational, because non-rational ruled surfaces have $q > 0$. Hence S must be rational. If S is rational then $p_g = 0$, and surfaces with $p_g = q = 0$ isogenous to a product were classified by Bauer-Catanese-Grunewald in [BCG08], and the only rational one is $S = \mathbb{P}^1 \times \mathbb{P}^1$, hence G is trivial and this case is also excluded. □

Group theoretical proof. If either $r_1 = 3$ or $r_2 = 3$, then the result follows from [BCG05, Proposition 3.2]. Indeed, if $r_i = 3$ (for $i = 1$ or 2) then the above inequality is equivalent to the condition that $\mu_i < 1$.

If $\mu > 1$ then the possible unordered types are

$$(2, 2, n)(n \in \mathbb{N}), \quad (2, 3, 3), \quad (2, 3, 4), \quad (2, 3, 5).$$

In the first case, $G \cong D_n$ is a dihedral group of order $2n$, and thus cannot admit an unmixed Beauville structure by [BCG05, Lemma 3.7]. Moreover, G cannot admit an unmixed ramification structure (T_1, T_2), where T_1 has an unordered type $(2, 2, n)$. Indeed, let C_n denote a maximal cyclic subgroup of D_n, then $D_n \setminus C_n$ contains at most two conjugacy classes, more precisely, it contains one if n is odd and two if n is even. If n is odd, since both T_1 and T_2 contain elements of $D_n \setminus C_n$, then $\Sigma_1 \cap \Sigma_2 \neq \{1\}$. If n is even, then T_1 necessarily contains two elements from two different conjugacy classes of $D_n \setminus C_n$, and T_2 always contains an element of $D_n \setminus C_n$, which again contradicts $\Sigma_1 \cap \Sigma_2 = \{1\}$.

In the other cases, one obtains the following isomorphisms of triangular groups

$$\Delta(2, 3, 3) \cong A_4, \quad \Delta(2, 3, 4) \cong S_4, \quad \Delta(2, 3, 5) \cong A_5,$$

and it is easy to check that these groups do not admit an unmixed Beauville structure (see also [BCG05, Proposition 3.6]). Moreover, these groups cannot admit an unmixed ramification structure (T_1, T_2), where T_1 has an unordered type $(2, 3, n)$ and $n = 3, 4, 5$. Indeed, in the groups A_4 and A_5, any two elements of the same order are either conjugate or one can be conjugated to some power of the other, in contradiction to $\Sigma_1 \cap \Sigma_2 = \{1\}$. For the group S_4, T_1 necessarily contains one 2-cycle, one 3-cycle and one 4-cycle, so the condition $\Sigma_1 \cap \Sigma_2 = \{1\}$ implies that T_2 can contain only elements which have exactly two 2-cycles, and these elements cannot generate S_4, yielding a contradiction.

If $\mu = 1$ then the possible unordered types are

$$(3,3,3), \quad (2,4,4), \quad (2,3,6),$$

and so G is a finite quotient of one of the wall-paper groups and cannot admit an unmixed Beauville structure by [BCG05, §6]. Moreover, the arguments in [BCG05, §6] show that, in fact, these groups cannot admit an unmixed ramification structure (T_1, T_2), where T_1 has an unordered type either $(3,3,3)$ or $(2,4,4)$ or $(2,3,6)$. For example, if G is a quotient of the triangle group $\Delta(3,3,3)$, and we denote by A the maximal normal abelian subgroup of G, then by [BCG05, Proposition 6.3], for any $g \in G \setminus A$ there exists some integer i s.t. g^i belongs to one of two fixed conjugacy classes C_1 and C_2. Moreover, T_1 necessarily contains two elements $g_1, g_2 \in G \setminus A$ such that $g_1^{i_1} \in C_1$ and $g_2^{i_2} \in C_2$ for some i_1, i_2. Since T_2 always contains an element of $G \setminus A$, this contradicts $\Sigma_1 \cap \Sigma_2 = \{1\}$.

For $r_1, r_2 \geq 4$ the above inequality holds, unless the type is $(2,2,2,2)$. In the latter case, G is a finite quotient of the wall-paper group

$$\begin{aligned}\Gamma &\cong \langle t_1, t_2, t_3, t_4 : t_1^2, t_2^2, t_3^2, t_4^2, t_1t_2t_3t_4 \rangle \cong \langle t_1, t_2, t_3 : t_1^2, t_2^2, t_3^2, (t_1t_2t_3)^2 \rangle \\ &\cong \langle t, r, s : [r,s], t^2, trtr, tsts \rangle,\end{aligned}$$

by setting $t_1 = rt$, $t_2 = ts$ and $t_3 = t$.

Hence, $\Gamma \cong \mathbb{Z}/2\mathbb{Z} \ltimes \mathbb{Z}^2$, and so all its finite quotients are of the form $G = \mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ for some $m, n \in \mathbb{N}$. We will show in Proposition 3.36 that these groups cannot admit an unmixed ramification structure of size $(4,4)$. In fact, the same argument also shows that these groups cannot admit an unmixed ramification structure (T_1, T_2), where T_1 has an unordered type $(2,2,2,2)$ (see Remark 3.37). $\square$

2.2. **Moduli Spaces.** Let S be an unmixed Beauville surface with group G and a pair of two disjoint spherical $3-$systems of generators of types (τ_1, τ_2). By (7) we have $\chi(S) = \chi(G, (\tau_1, \tau_2))$, and consequentially, by (1), $K_S^2 = K^2(G, (\tau_1, \tau_2)) = 8\chi(S)$. Moreover, by a theorem of Gieseker (see [G]), once K_S^2 and $\chi(S)$ are fixed, there exists a quasiprojective moduli space $\mathcal{M}_{K_S^2, \chi(S)}$ of minimal smooth complex surfaces of general type with these invariants.

Let us fix a group G and a pair of unmixed ramification types (τ_1, τ_2), and denote by $\mathcal{M}_{(G,(\tau_1,\tau_2))}$ the moduli space of isomorphism classes of Beauville surfaces admitting these data, then obviously it is a subset of the moduli space $\mathcal{M}_{K^2(G,(\tau_1,\tau_2)),\chi(G,(\tau_1,\tau_2))}$. Since the Beauville surfaces are rigid, by [Cat00] the space $\mathcal{M}_{(G,(\tau_1,\tau_2))}$ consists of a finite number of isolated points. Indeed, there is a group theoretical procedure to count these points, which is described in [BC].

Let us note that the study of the moduli space of Beauville surfaces is a particular case of the study of the moduli spaces of surfaces isogenous to a higher product. Indeed, we shall restrict here to the case of surfaces isogenous to a higher product with $q = 0$, the Beauville case will follow then clearly.

Definition 2.9. *The braid group of the sphere* $\mathbf{B}_r := \pi_0(Diff(\mathbb{P}^1 - \{p_1, \ldots, p_r\}))$ *operates on the epimorphism* θ *defined in* (3)*:*

$$\pi_1(\mathbb{P}^1 - \{p_1, \ldots, p_r\})/\langle \gamma^{m_1}, \ldots, \gamma^{m_r} \rangle \cong \Gamma := \Gamma(0 \mid m_1, \ldots, m_r) \xrightarrow{\theta} G.$$

Indeed, if $\sigma \in \mathbf{B}_r$ *then the operation is given by* $\theta \circ \sigma$*. The orbits of this action are called* Hurwitz equivalence classes *of the spherical systems of generators.*

Let (T_1, T_2) be a pair of disjoint spherical $r-$systems of generators of type (τ_1, τ_2), we call the pair (T_1, T_2) *unordered* if T_1 and T_2 have unordered types τ_1 and τ_2 respectively.

We shall denote by $\mathcal{U}(G; \tau_1, \tau_2)$ the set of all unordered pairs (T_1, T_2) of disjoint spherical $r-$systems of generators of type (τ_1, τ_2).

Theorem 2.10. [BC, Theorem 1.3]*. Let* S *be a surface isogenous to a higher product of unmixed type and with* $q = 0$*. Then to* S *we attach its finite group* G *(up to isomorphism) and the equivalence classes of an unordered pair of disjoint spherical systems of generators* (T_1, T_2) *of* G*, under the equivalence relation generated by:*

- *(i) Hurwitz equivalence for* T_1*;*
- *(ii) Hurwitz equivalence for* T_2*;*
- *(iii) Simultaneous conjugation for* T_1 *and* T_2*, i.e., for* $\phi \in \mathrm{Aut}(G)$ *we let* $\big(T_1 := (x_{1,1}, \ldots, x_{r_1,1}), \quad T_2 := (x_{1,2}, \ldots, x_{r_2,2})\big)$ *be equivalent to*

$$\big(\phi(T_1) := (\phi(x_{1,1}), \ldots, \phi(x_{r_1,1})), \quad \phi(T_2) := (\phi(x_{1,2}), \ldots, \phi(x_{r_2,2}))\big).$$

Then two surfaces S*,* S' *are deformation equivalent if and only if the corresponding equivalence classes of pairs of spherical generating systems of* G *are the same.*

Once we fix a finite group G and a pair of types (τ_1, τ_2) (of size (r_1,r_2)) of an unmixed ramification structure for G, counting the number of connected components of $\mathcal{M}_{(G,(\tau_1,\tau_2))}$ is then equivalent to the group theoretical problem of counting the number of classes of pairs of spherical systems of generators of G of type (τ_1, τ_2) under the equivalence relation given by the action of $\mathbf{B}_{r_1} \times \mathbf{B}_{r_2} \times \mathrm{Aut}(G)$. This leads to the following definition.

Definition 2.11. *Denote by* $h(G; \tau_1, \tau_2)$ *the number of* Hurwitz components*, namely the number of orbits of* $\mathcal{U}(G; \tau_1, \tau_2)$ *under the action of* $\mathbf{B}_{r_1} \times \mathbf{B}_{r_2} \times \mathrm{Aut}(G)$*, given by:*

$$(\gamma_1, \gamma_2, \phi) \cdot (T_1, T_2) := \big(\phi(\gamma_1(T_1)), \phi(\gamma_2(T_2))\big),$$

where $\gamma_1 \in \mathbf{B}_{r_1}$*,* $\gamma_2 \in \mathbf{B}_{r_2}$*,* $\phi \in \mathrm{Aut}(G)$ *and* $(T_1, T_2) \in \mathcal{U}(G; \tau_1, \tau_2)$*.*

In case of Beauville surfaces we define h as above substituting r_1 and r_2 with 3.

2.3. **Counting Points in the Moduli Space.** In this Section we shall make some remarks on the number of connected components of the moduli space corresponding to Beauville surfaces.

Let S be a smooth minimal surface of general type with $q(S) = 0$, and denote by $\mathcal{M}(S)$ the subvariety of $\mathcal{M}_{K_S^2,\chi(S)}$, corresponding to surfaces (orientedly) homeomorphic to S. We shall denote by $\mathcal{M}^0_{K_S^2,\chi(S)}$ the subspace of the moduli space corresponding to surfaces with $q = 0$.

Let $y := K_S^2$ and $x := \chi(\mathcal{O}_S)$, it is known that the number of connected components $\delta(y, x)$ of $\mathcal{M}^0_{y,x}$ is bounded from above by a function in y, indeed $\delta(y, x) \leq cy^{77y^2}$, where c is a positive constant (see e.g. [Cat92]). Hence we have that the number of components has an exponential upper bound in K^2.

There are also some results regarding the lower bound. In [Man], for example, a sequence X_n of simply connected surfaces of general type was constructed, such that a lower bound for the number of the connected components of $\mathcal{M}(X_n)$ was given.

Theorem 2.12. [Man, Theorem A]. *Denote by $y_n := K^2_{X_n}$ and by $x_n := \chi(\mathcal{O}_{X_n})$, then there exists a sequence X_n of simply connected surfaces of general type such that $x_n \to \infty$ as $n \to \infty$, and if $\delta(X_n)$ denotes the number of connected components of $\mathcal{M}(X_n)$, then*

$$\delta(X_n) \geq y_n^{\frac{1}{5} log y_n}.$$

We investigate the number of connected components $h(G_n; \tau_1, \tau_2)$ of $\mathcal{M}_{(G_n,(\tau_1,\tau_2))}$ for certain families of finite groups $\{G_n\}_n$.

If we restrict to the study of the moduli space of surfaces isogenous to a higher product with $q = 0$, we can only expect a polynomial growth in χ (and so in K^2) of the number of connected components.

Proposition 2.13. *Fix r_1 and r_2 in $\mathbb{N}$. Let $\{G_n\}_{n=1}^{\infty}$ be a family of finite groups, which admit an unmixed ramification structure of size (r_1, r_2). Let $\tau_{n,1} = (m_{n,1,1}, \ldots, m_{n,1,r_1})$ and $\tau_{n,2} = (m_{n,2,1}, \ldots, m_{n,2,r_2})$ be sequences of types $(\tau_{n,1}, \tau_{n,2})$ of unmixed ramification structures for G_n, and $\{X_n\}_{n=1}^{\infty}$ be the family of surfaces isogenous to higher product with $q = 0$ admitting the given data, then as $|G_n| \stackrel{n\to\infty}{\longrightarrow} \infty$:*

(i) $\chi(X_n) = \Theta(|G_n|)$.

(ii) $h(G_n; \tau_{n,1}, \tau_{n,2}) = O(\chi(X_n)^{r_1+r_2-2})$.

Proof. *(i)* Note that, for $i = 1, 2$,

$$\frac{1}{42} \leq -2 + \sum_{j=1}^{r_i}(1 - \frac{1}{m_{n,i,j}}) \leq r_i - 2.$$

Indeed, for $r_i = 3$, the minimal value for $(1 - \mu_i)$ is $1/42$. For $r_i = 4$, the minimal value for $\big(-2 + \sum_{j=1}^{r_i}(1 - \frac{1}{m_{n,i,j}})\big)$ is $1/6$, and when $r_i \geq 5$, this value is at least $1/2$.

Now, by Equation (7),

$$4\chi(X_n) = |G_n| \cdot \left(-2 + \sum_{j=1}^{r_1}(1 - \frac{1}{m_{n,1,j}})\right) \cdot \left(-2 + \sum_{j=1}^{r_2}(1 - \frac{1}{m_{n,2,j}})\right),$$

hence

$$\frac{|G_n|}{4\cdot 42^2} \leq \chi(X_n) \leq \frac{(r_1-2)(r_2-2)|G_n|}{4}.$$

(*ii*) For $i=1,2$, any spherical r_i-system of generators $T_{n,i}$ contains at most r_i-1 independent elements of G_n. Thus, the size of the set of all unordered pairs of type $(\tau_{n,1},\tau_{n,2})$ is bounded from above, by

$$|\mathcal{U}(G_n;\tau_{n,1},\tau_{n,2})| \leq |G_n|^{r_1+r_2-2},$$

and so, the number of connected components is bounded from above by

$$h(G_n;\tau_{n,1},\tau_{n,2}) \leq |G_n|^{r_1+r_2-2}.$$

Now, the result follows from (*i*).

□

By taking $r_1=r_3=3$ we get the following Corollary.

Corollary 2.14. *Let $\{G_n\}_{n=1}^{\infty}$ be a family of finite groups, which admit an unmixed Beauville structure. Let $\tau_{n,1}=(m_{n,1,1},m_{n,1,2},m_{n,1,3})$ and $\tau_{n,2}=(m_{n,2,1},m_{n,2,2},m_{n,2,3})$ be sequences of types $(\tau_{n,1},\tau_{n,2})$ of unmixed Beauville structures for G_n, and let $\{X_n\}_{n=1}^{\infty}$ be the family of Beauville surfaces admitting the given data, then as $|G_n| \stackrel{n\to\infty}{\longrightarrow} \infty$:*

(*i*) $\chi(X_n)=\Theta(|G_n|)$.
(*ii*) $h(G_n;\tau_{n,1},\tau_{n,2})=O(\chi(X_n)^4)$.

With the calculation done in this paper we can give a more accurate description of the asymptotic growth of h in case of Beauville surfaces and surfaces isogenous to a higher product with $q=0$, for certain families of finite groups.

Let us consider Beauville surfaces X_p with group $\mathrm{PSL}(2,p)$, where p is prime, as in Theorem 1.5, then by Proposition 2.13, as $p\to\infty$:

$$\chi(X_p)=\Theta(p^3),$$

while, by Theorem 1.11, if τ_1 and τ_2 are two hyperbolic types, we have

$$h(\mathrm{PSL}(2,p),\tau_1,\tau_2)=O(p^3).$$

We deduce the following Proposition, which improves the naive bound given in Corollary 2.14, for the case of $\mathrm{PSL}(2,p)$.

Proposition 2.15. *Let $\{X_p\}$ be the family of Beauville surfaces with group $\mathrm{PSL}(2,p)$, where p is prime. Then*

$$h(\mathrm{PSL}(2,p),\tau_1,\tau_2)=O(\chi(X_p)).$$

Consider now the family of Beauville surfaces X_p, where p is prime, admitting type $\tau_p=(p,p,p)$ and group $G_p:=(\mathbb{Z}/p\mathbb{Z})^2$, then by Proposition 2.13 we have as $p\to\infty$:

$$\chi(X_p)=\Theta(p^2),$$

while by Theorem 1.12,

$$h(G_p;\tau_p,\tau_p)=\Theta(p^4).$$

We deduce the following Proposition.

Proposition 2.16. *Let $\{X_p\}$ be the family of Beauville surfaces admitting type $\tau_p = (p,p,p)$ and group $G_p := (\mathbb{Z}/p\mathbb{Z})^2$, where p is prime. Then*

$$h(G_p;\tau_p,\tau_p) = \Theta(\chi^2(X_p)).$$

A similar result applies for surfaces isogenous to a higher product not necessarily Beauville with $q = 0$.

Consider the family of surfaces X_p, where p is prime, admitting type $\tau_p = (p,\dots,p)$ (p appears $(r+1)-$times) and group $G_p := (\mathbb{Z}/p\mathbb{Z})^r$, then by Proposition 2.13 we have as $p \to \infty$:

$$\chi(X_p) = \Theta(p^r),$$

while by Proposition 3.35,

$$h(G_p;\tau_p,\tau_p) = \Theta(p^{r^2}).$$

We deduce the following Proposition.

Proposition 2.17. *Let $\{X_p\}$ be the family of surfaces admitting type $\tau_p = (p,\dots,p)$ (p appears $(r+1)-$times) and group $G_p := (\mathbb{Z}/p\mathbb{Z})^r$, where p is prime. Then*

$$h(G_p;\tau_p,\tau_p) = \Theta(\chi^r(X_p)).$$

Therefore, there exist families of surfaces, such that the degree of the polynomial $h(G_p;\tau_p,\tau_p)$, in χ, can be arbitrarily large.

3. Finite Groups, Ramification Structures and Hurwitz Components

3.1. **Braid Group Actions.** Recall that the *braid group* $\mathbf{B}_r$ on r strands can be presented as

$$\mathbf{B}_r = \langle \sigma_1,\dots,\sigma_{r-1} | \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}, \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j| \geq 2\rangle.$$

The action of $\mathbf{B}_r$ on the set of spherical $r-$systems of generators for G of unordered type $\tau = (m_1,\dots,m_r)$, which was defined in 2.9, is given by

$$\sigma_i : (x_1,\dots,x_i,\dots,x_r) \to (x_1,\dots,x_{i-1},x_ix_{i+1}x_i^{-1},x_i,x_{i+2}\dots,x_r),$$

for $i = 1,\dots,r-1$.

There is also a natural action of $\mathrm{Aut}(G)$ given by

$$\phi(x_1,\dots,x_r) = (\phi(x_1),\dots,\phi(x_r)), \quad \phi \in \mathrm{Aut}(G).$$

Since the two actions of $\mathbf{B}_r$ and $\mathrm{Aut}(G)$ commute, one gets a double action of $\mathbf{B}_r \times \mathrm{Aut}(G)$ on the set of spherical $r-$systems of generators for G of an unordered type $\tau = (m_1,\dots,m_r)$.

Let $x \in G$ and denote by $C = x^{\mathrm{Aut}(G)}$ the $\mathrm{Aut}(G)-$equivalence class of x. Since all the elements in C have the same order, we may define $\mathrm{ord}(C) := \mathrm{ord}(x)$.

Let $\mathbf{C} = (C_1,\dots,C_r)$ be a set of $\mathrm{Aut}(G)$-equivalence classes. We say that $\mathbf{C}$ has *type* $\tau = (m_1,\dots,m_r)$ if $\mathrm{ord}(C_i) = m_i$ (for $i = 1,\dots,r$), and for every $1 \leq i \leq r$ there exists $x_i \in C_i$ such that $x_1 \cdot \dots \cdot x_r = 1$ and $\langle x_1,\dots,x_r\rangle = G$. $\mathbf{C}$ has an *unordered type* τ if the orders of $C_1,\dots,C_r$ are $m_1,\dots,m_r$ up to a permutation.

Observe that the action of $\mathbf{B}_r$ preserves the conjugacy classes, and hence the $\mathrm{Aut}(G)-$equivalence classes, of the elements in a spherical $r-$system of generators of G. Thus, in fact, $\mathbf{B}_r$ acts on $\mathbf{C} = (C_1, \dots, C_r)$, where $\mathbf{C}$ has an unordered type τ. The following Lemma easily follows.

Lemma 3.1. *Let τ_1 and τ_2 be two types, then*

$$h(G; \tau_1, \tau_2) \geq \#\{\mathbf{C}_i, \mathbf{D}_j : \mathbf{C}_i = (C_{i,1}, \dots, C_{i,r_1}) \textit{ and } \mathbf{D}_j = (D_{j,1}, \dots, D_{j,r_2}),$$
$$\textit{where } \mathbf{C}_i \textit{ and } \mathbf{D}_j \textit{ are of unordered types } \tau_1 \textit{ and } \tau_2 \textit{ respectively, and}$$
$$\{C_{i,k}\}_{i,k} \textit{ and } \{D_{j,l}\}_{j,l} \textit{ all belong to different } \mathrm{Aut}(G) - \textit{classes}\}.$$

In the special case of $\mathbf{B}_3$, the braid group on 3 strands, one can deduce a more accurate bound. Let $T = (x, y, (xy)^{-1})$ be a spherical $3-$system of generators for G, and let $C(T)$ be the $\mathrm{Aut}(G)-$equivalence class of T, namely

$$C(T) := \{(\phi(x), \phi(y), \phi(xy)^{-1}) : \phi \in \mathrm{Aut}(G)\}.$$

Define the *unordered* $\mathrm{Aut}(G)-$equivalence class of T by:

$$C^{un}(T) := C(x, y, (xy)^{-1}) \cup C(y, x, (yx)^{-1}) \cup C(x, (yx)^{-1}, y)$$
$$\cup\, C(y, (xy)^{-1}, x) \cup C((xy)^{-1}, x, y) \cup C((yx)^{-1}, y, x).$$

Lemma 3.2. *Let $T = (x, y, (xy)^{-1})$ be a spherical $3-$system of generators for G, then the action of $\mathbf{B}_3$ preserves $C^{un}(T)$.*

Proof. Let $(x, y, (xy)^{-1})$ be a spherical $3-$system for G, then the action of $\mathbf{B}_3 = \langle \sigma_1, \sigma_2 \rangle$ is given by:

$$\sigma_1 : (x, y, y^{-1}x^{-1}) \to (xyx^{-1}, x, y^{-1}x^{-1}) = x(y, x, x^{-1}y^{-1})x^{-1} \in C(y, x, (yx)^{-1}),$$

and

$$\sigma_2 : (x, y, y^{-1}x^{-1}) \to (x, yy^{-1}x^{-1}y^{-1}, y) = (x, x^{-1}y^{-1}, y) \in C(x, (yx)^{-1}, y).$$

□

Denote by $d = d(G; \tau)$ the number of orbits in the set of spherical $3-$systems of generators for G of unordered type τ, under the action of $\mathbf{B}_3 \times \mathrm{Aut}(G)$. This number can be effectively computed using the following Corollary, which follows immediately from Lemma 3.2.

Corollary 3.3.

$$d(G; \tau) = \#\{C^{un}(T) : T \in \mathcal{S}(G, \tau)\}.$$

Now, one can use $d(G; \tau)$ in order to bound the number of Hurwitz components.

Corollary 3.4. *Let τ_1 and τ_2 be two types, then*

$$\max\{d(G; \tau_1), d(G; \tau_2)\} \leq h(G; \tau_1, \tau_2) \leq d(G; \tau_1) \cdot d(G; \tau_2) \cdot |\mathrm{Aut}(G)|.$$

Proof. The left inequality is obvious. For the right inequality, let O_i (for $i = 1, 2$) be an orbit in the set of spherical $3-$systems of generators for G of unordered type τ_i under the action of $\mathbf{B}_3 \times \mathrm{Aut}(G)$, and note that there are $d(G; \tau_i)$ such orbits. Then, by the following Lemma 3.5, the product of O_1 and O_2 decomposes into at most $|\mathrm{Aut}(G)|$ orbits, under the diagonal action of $\mathrm{Aut}(G)$. □

The following is a well-known group theoretic Lemma. For the convenience of the reader we present here a short proof.

Lemma 3.5. *Let G be a finite group, and let H and K be two subgroups of G. Consider the diagonal action of G on the set $G/H \times G/K$. Then*

$$G/H \times G/K = \bigcup_{HgK \in H \backslash G/K} G/(H \cap gKg^{-1}),$$

hence, $G/H \times G/K$ decomposes into at most $|G|$ orbits.

Proof. Let $x \in G/H \times G/K =: D$, then $x = (g_1H, g_2K)$. The stabilizer of x is given by those $g \in G$ such that $gg_1H = g_1H$ and $gg_2K = g_2K$, hence $Stab(x) = g_1Hg_1^{-1} \cap g_2Hg_2^{-1}$.

The orbit of x is given by $G/Stab(x)$, choosing (H, g_3K) as a representative for x in the orbit, we have that $Gx = G/(H \cap g_3Kg_3^{-1})$ as a $G-$set. Hence, if $D = \cup_{i \in I} D_i$ is a decomposition of D into $G-$orbits, then for each D_i there is a $g_i \in G$ such that $D_i \cong G/(H \cap g_iKg_i^{-1})$ as a $G-$set. The index set I is determined by the sets of double cosets $H \setminus G/K$. Indeed the map $\phi : H \setminus G/K \to \{Orbits\ in\ D\}$ given by $HgK \mapsto G(H, gK)$ is well defined and bijective. $\square$

3.2. **Ramification Structures and Hurwitz Components for A_n and S_n.** In this Section we prove Theorems 1.3, 1.4, 1.9 and 1.10 regarding alternating and symmetric groups. The proofs are based on results of Liebeck and Shalev [LS04].

3.2.1. *Theoretical Background – Higman's Conjecture and a Theorem of Liebeck and Shalev on Fuchsian groups.* Conder [Co80] (following Higman) proved that sufficiently large alternating groups are in fact *Hurwitz groups*, namely they are quotients of the Hurwitz triangle group $\Delta(2, 3, 7)$, using the method of coset diagrams. In fact, Higman had already conjectured in the late 1960s that every hyperbolic triangle group, and more generally – every Fuchsian group, surjects to all but finitely many alternating groups.

This conjecture was proved by Everitt [Ev] using the method of coset diagrams, and later Liebeck and Shalev [LS04] gave an alternative proof based on probabilistic group theory. In fact, they proved a more explicit and general result, which is presented below.

Note that the results of Liebeck and Shalev are applicable to any Fuchsian group Γ, however, we shall use them only for the case of orbifold surface groups $\Gamma = \Gamma(g' \mid m_1, \ldots, m_r)$ (see Definition 2.4) that satisfy the inequality

$$2g' - 2 + \sum_{i=1}^{r} (1 - \frac{1}{m_i}) > 0. \tag{10}$$

Definition 3.6. *Let $C_i = g_i^{S_n}$ $(1 \leq i \leq r)$ be conjugacy classes in S_n, and let m_i be the order of g_i. Define* $\mathrm{sgn}(C_i) = \mathrm{sgn}(g_i)$*, and write $\mathbf{C} = (C_1, \ldots, C_r)$. Define*

$$\mathrm{Hom}_{\mathbf{C}}(\Gamma, S_n) = \{\phi \in \mathrm{Hom}(\Gamma, S_n) : \phi(x_i) \in C_i \ for\ 1 \leq i \leq r\}.$$

Definition 3.7. *Conjugacy classes in S_n of cycle-shape (m^k), where $n = mk$, namely, containing k cycles of length m each, are called* homogeneous.

A conjugacy class having cycle-shape $(m^k, 1^f)$*, namely, containing* k *cycles of length* m *each and* f *fixed points, with* f *bounded, is called* almost homogeneous.

Theorem 3.8. [LS04, Theorem 1.9]. *Let* Γ *be a Fuchsian group, and let* C_i $(1 \leq i \leq r)$ *be conjugacy classes in* S_n *with cycle-shapes* $(m_i^{k_i}, 1^{f_i})$*, where* $f_i < f$ *for some constant* f *and* $\prod_{i=1}^{r} \operatorname{sgn}(C_i) = 1$*. Set* $\mathbf{C} = (C_1, \ldots, C_r)$*. Then the probability that a random homomorphism in* $\operatorname{Hom}_{\mathbf{C}}(\Gamma, S_n)$ *has image containing* A_n *tends to* 1 *as* $n \to \infty$*.*

Applying this when Γ is the triangle group $\Delta(m_1, m_2, m_3)$ demonstrates that three elements, with product 1, from almost homogeneous classes C_1, C_2, C_3 of orders m_1, m_2, m_3, randomly generate A_n or S_n, provided $1/m_1 + 1/m_2 + 1/m_3 < 1$. In particular, when $(m_1, m_2, m_3) = (2, 3, 7)$, this gives random $(2, 3, 7)$ generation of A_n.

Using Theorem 3.8, Liebeck and Shalev deduced the following Corollary regarding S_n.

Corollary 3.9. [LS04, Theorem 1.10]. *Let* $\Gamma = \Gamma(-|m_1, \ldots, m_r)$ *be a polygonal group which satisfies the above inequality* (10)*, and assume that at least two of* $m_1, \ldots, m_r$ *are even. Then* Γ *surjects to all but finitely many symmetric groups* S_n*.*

3.2.2. *Ramification Structures of* A_n *and* S_n*.*

Proof of Theorem 1.3. Assume that (r_1, s_1, t_1) and (r_2, s_2, t_2) are two hyperbolic types and that n is large enough. By the following Algorithm 3.10, we choose six almost homogeneous conjugacy classes in S_n, C_{r_1}, C_{s_1}, C_{t_1}, C_{r_2}, C_{s_2}, C_{t_2}, of orders r_1, s_1, t_1, r_2, s_2, t_2 respectively, such that they contain only even permutations, and they all have different numbers of fixed points.

By Theorem 3.8, the probability that three random elements (x_1, y_1, z_1) (equivalently (x_2, y_2, z_2)) whose product is 1, taken from the almost homogeneous conjugacy classes $(C_{r_1}, C_{s_1}, C_{t_1})$ (equivalently $(C_{r_2}, C_{s_2}, C_{t_2})$) will generate A_n, tends to 1 as $n \to \infty$.

This implies that if n is large enough, one can find six elements x_1, y_1, z_1, x_2, y_2, z_2 in A_n of orders r_1, s_1, t_1, r_2, s_2, t_2 respectively satisfying the following properties.

- $x_1 \in C_{r_1}$, $y_1 \in C_{s_1}$, $z_1 \in C_{t_1}$, $x_2 \in C_{r_2}$, $y_2 \in C_{s_2}$, $z_2 \in C_{t_2}$.
- $x_1 y_1 z_1 = x_2 y_2 z_2 = 1$ and $\langle x_1, y_1 \rangle = \langle x_2, y_2 \rangle = A_n$.
- For any choice of integers $l_{x_1}, l_{y_1}, l_{z_1}, l_{x_2}, l_{y_2}, l_{z_2}$, if the six elements $x_1^{l_{x_1}}$, $y_1^{l_{y_1}}$, $z_1^{l_{z_1}}$, $x_2^{l_{x_2}}$, $y_2^{l_{y_2}}$, $z_2^{l_{z_2}}$ are not trivial, then they all belong to different conjugacy classes in S_n, and hence $\Sigma(x_1, y_1, z_1) \bigcap \Sigma(x_2, y_2, z_2) = \{1_{A_n}\}$.

Therefore, if n is large enough, the quadruple $(x_1, y_1; x_2, y_2)$ is an unmixed Beauville structure for A_n, where (x_1, y_1, z_1) has type (r_1, s_1, t_1) and (x_2, y_2, z_2) has type (r_2, s_2, t_2). □

Algorithm 3.10. *Choosing six almost homogeneous conjugacy classes* C_{r_1}, C_{s_1}, C_{t_1}, C_{r_2}, C_{s_2}, C_{t_2} *in* S_n*, of orders* $r_1, s_1, t_1, r_2, s_2, t_2$ *respectively, such that they contain only even permutations, and they all have different numbers of fixed points.*

Step 1: Sorting $r_1, s_1, t_1, r_2, s_2, t_2$.

Let $m_6 \leq \cdots \leq m_1$ be the sorted sequence whose elements are exactly $r_1, s_1, t_1, r_2, s_2, t_2$. Since n can be as large as we want, we may assume that $n > 100m_1$.

Step 2: Choosing even integers k'_i $(1 \leq i \leq 6)$.

For $1 \leq i \leq 6$, let

$$k'_i = \begin{cases} \lfloor n/m_i \rfloor & \text{if it is even,} \\ \lfloor n/m_i \rfloor - 1 & \text{otherwise.} \end{cases}$$

Observe that for $1 \leq i \leq 6$,

$$k'_i m_i \leq n \leq (k'_i + 2)m_i.$$

Step 3: Choosing even integers k_i $(1 \leq i \leq 6)$ s.t. for every $1 \leq i \neq j \leq 6$, $k_i m_i \neq k_j m_j$.

It may happen that for some $i \neq j$, $k'_i m_i = k'_j m_j$. Therefore, for every i we will choose from the set $\{k'_i - 2l : 0 \leq l \leq 5\}$ a proper integer $k_i = k'_i - 2l$ (for some l), s.t. for every $1 \leq i \neq j \leq 6$, $k_i m_i \neq k_j m_j$. Note that by our assumption, the integers k_i $(1 \leq i \leq 6)$ are positive.

Step 4: Defining the conjugacy classes C_i $(1 \leq i \leq 6)$.

Assume that n is large enough and let C_i $(1 \leq i \leq 6)$ be conjugacy classes in S_n with cycle shapes

$$(m_i^{k_i}, 1^{f_i}), \text{ where } f_i = n - k_i m_i.$$

Observe that the conjugacy classes C_i $(1 \leq i \leq 6)$ satisfy the following properties:

(i) For every $1 \leq i \leq 6$, $\text{sgn}(C_i) = 1$, since C_i contains an even number of cycles (as the k_i-s are even).

(ii) For every $1 \leq i \leq 6$, $f_i = n - k_i m_i \leq (k'_i + 2)m_i - (k'_i - 10)m_i = 12m_i \leq 12m_1$, and hence it is bounded independently of n.

(iii) For every $1 \leq i \neq j \leq 6$, $f_i \neq f_j$, since $k_i m_i \neq k_j m_j$.

(iv) Let $c_i \in C_i$ be some element, then any non-trivial power $c_i^{l_i}$ has exactly f_i fixed points.

(v) By *(iii)* and *(iv)*, for any $1 \leq i \neq j \leq 6$ and any two integers l_i, l_j, if the powers $c_i^{l_i}$ and $c_j^{l_j}$ are not trivial, then they belong to different conjugacy classes in S_n.

Step 5: Defining the conjugacy classes $C_{r_1}, C_{s_1}, C_{t_1}, C_{r_2}, C_{s_2}, C_{t_2}$.

Let $k_{r_1}, k_{s_1}, k_{t_1}, k_{r_2}, k_{s_2}, k_{t_2}$ (respectively $f_{r_1}, f_{s_1}, f_{t_1}, f_{r_2}, f_{s_2}, f_{t_2}$) be the elements of the set $\{k_1, \ldots, k_6\}$ (respectively $\{f_1, \ldots, f_6\}$), ordered by the same correspondence between $\{r_1, s_1, t_1, r_2, s_2, t_2\}$ and $\{m_1, \ldots, m_6\}$.

Now, $C_{r_1}, C_{s_1}, C_{t_1}, C_{r_2}, C_{s_2}, C_{t_2}$ are the six conjugacy classes in S_n with cycle-shapes $(r_1^{k_{r_1}}, 1^{f_{r_1}})$, $(s_1^{k_{s_1}}, 1^{f_{s_1}})$, $(t_1^{k_{t_1}}, 1^{f_{t_1}})$, $(r_2^{k_{r_2}}, 1^{f_{r_2}})$, $(s_2^{k_{s_2}}, 1^{f_{s_2}})$, $(t_2^{k_{t_2}}, 1^{f_{t_2}})$ respectively.

In a similar way, we prove Theorem 1.4 regarding the symmetric groups.

Proof of Theorem 1.4. Assume that (r_1, s_1, t_1) and (r_2, s_2, t_2) are two hyperbolic types, such that at least two of (r_1, s_1, t_1) are even and at least two of (r_2, s_2, t_2) are even, and that n is large enough. By slightly modifying Algorithm 3.10, we may choose six almost homogeneous conjugacy classes C_{r_1}, C_{s_1}, C_{t_1}, C_{r_2}, C_{s_2}, C_{t_2} in S_n, of orders r_1, s_1, t_1, r_2, s_2, t_2 respectively, such that two classes of $C_{r_1}, C_{s_1}, C_{t_1}$ and two classes of $C_{r_2}, C_{s_2}, C_{t_2}$ contain only odd permutations, and all these classes have different numbers of fixed points.

By Theorem 3.8 and Corollary 3.9, the probability that three random elements (x_1, y_1, z_1) (equivalently (x_2, y_2, z_2)) whose product is 1, taken from the almost homogeneous conjugacy classes $(C_{r_1}, C_{s_1}, C_{t_1})$ (equivalently $(C_{r_2}, C_{s_2}, C_{t_2})$) will generate S_n, tends to 1 as $n \to \infty$.

Therefore, if n is large enough, there exists a quadruple $(x_1, y_1; x_2, y_2)$ which is an unmixed Beauville structure for S_n, where (x_1, y_1, z_1) has type (r_1, s_1, t_1) and (x_2, y_2, z_2) has type (r_2, s_2, t_2). □

Moreover, since Theorem 3.8 and Corollary 3.9 apply to any polygonal group, one can modify Algorithm 3.10 and deduce the following Corollaries.

Corollary 3.11. *Let $\tau_1 = (m_{1,1}, \ldots, m_{1,r_1})$ and $\tau_2 = (m_{1,1}, \ldots, m_{1,r_2})$ be two sets of natural numbers such that $m_{k,i} \geq 2$ and $\sum_{i=1}^{r_k}(1 - 1/m_{k,i}) > 2$ for $k = 1, 2$. Then, almost all alternating groups A_n admit an unmixed ramification structure of type (τ_1, τ_2).*

Corollary 3.12. *Let $\tau_1 = (m_{1,1}, \ldots, m_{1,r_1})$ and $\tau_2 = (m_{1,1}, \ldots, m_{1,r_2})$ be two sets of natural numbers such that $m_{k,i} \geq 2$, at least two of $(m_{k,1}, \ldots, m_{k,r_k})$ are even and $\sum_{i=1}^{r_k}(1-1/m_{k,i}) > 2$, for $k = 1, 2$. Then, almost all symmetric groups S_n admit an unmixed ramification structure of type (τ_1, τ_2).*

3.2.3. *Hurwitz Components of A_n and S_n.*

Proof of 1.9. Let $\tau_1 = (r_1, s_1, t_1)$ and $\tau_2 = (r_2, s_2, t_2)$ be two hyperbolic types, let $k \in \mathbb{N}$ be an arbitrary integer, and assume that n is large enough. By slightly modifying Algorithm 3.10, we may actually choose $6k$ almost homogeneous conjugacy classes in S_n,

$$\{C_{r_1,i}, C_{s_1,i}, C_{t_1,i}, C_{r_2,i}, C_{s_2,i}, C_{t_2,i}\}_{i=1}^{k},$$

which contain even permutations, such that every six classes have orders $r_1, s_1, t_1, r_2, s_2, t_2$ respectively, and all the $6k$ conjugacy classes have different numbers of fixed points.

Hence, if n is large enough, there are $6k$ different S_n-conjugacy classes in A_n, and moreover, for each $1 \leq i_1, i_2, i_3, j_1, j_2, j_3 \leq k$, $(C_{r_1,i_1}, C_{s_1,i_2}, C_{t_1,i_3})$ has type τ_1 and $(C_{r_2,j_1}, C_{s_2,j_2}, C_{t_2,j_3})$ has type τ_2, by Theorem 1.3.

From Lemma 3.1, since $S_n = \mathrm{Aut}(A_n)$ (for $n > 6$), we deduce that if n is large enough, then $h(A_n; \tau_1, \tau_2) \geq k^6$. Now, k can be arbitrarily large, therefore,

$$h(A_n; \tau_1, \tau_2) \overset{n\to\infty}{\longrightarrow} \infty.$$

Moreover, as the number of different almost homogeneous conjugacy classes in S_n of some certain order grows linearly in n, the proof actually shows that $h = \Omega(n^6)$. □

Similarly, we can show that if $\tau_1 = (r_1, s_1, t_1)$ and $\tau_2 = (r_2, s_2, t_2)$ are two hyperbolic types, such that at least two of (r_1, s_1, t_1) are even and at least two of (r_2, s_2, t_2) are even, then

$$h(S_n; \tau_1, \tau_2) \overset{n\to\infty}{\longrightarrow} \infty,$$

and moreover, $h = \Omega(n^6)$, thus proving Theorem 1.10.

In addition, using similar techniques, we can deduce the following Corollaries.

Corollary 3.13. *Let $\tau_1 = (m_{1,1}, \dots, m_{1,r_1})$ and $\tau_2 = (m_{1,1}, \dots, m_{1,r_2})$ be two sets of natural numbers such that $m_{k,i} \geq 2$ and $\sum_{i=1}^{r_k}(1-1/m_{k,i}) > 2$ for $k = 1, 2$. Then, $h(A_n; \tau_1, \tau_2)$ grows at least polynomially (of degree $r_1 + r_2$) in n.*

Corollary 3.14. *Let $\tau_1 = (m_{1,1}, \dots, m_{1,r_1})$ and $\tau_2 = (m_{1,1}, \dots, m_{1,r_2})$ be two sets of natural numbers such that $m_{k,i} \geq 2$, at least two of $(m_{k,1}, \dots, m_{k,r_k})$ are even and $\sum_{i=1}^{r_k}(1 - 1/m_{k,i}) > 2$, for $k = 1, 2$. Then, $h(S_n; \tau_1, \tau_2)$ grows at least polynomially (of degree $r_1 + r_2$) in n.*

3.3. **Beauville Structures and Hurwitz Components for** $\mathrm{PSL}(2, p^e)$**.** In this section we prove Theorems 1.5 and 1.11. The proofs are based on well-known properties of $\mathrm{PSL}(2, p^e)$ (see for example [Di, Go, Su]) and on results of Macbeath [Ma].

3.3.1. *Theoretical Background I – Properties of* $\mathrm{PSL}(2, p^e)$. Let $q = p^e$, where p is a prime number and $e \geq 1$. Recall that $\mathrm{GL}(2, q)$ is the group of invertible 2×2 matrices over the finite field with q elements, which we denote by $\mathbb{F}_q$, and $\mathrm{SL}(2, q)$ is the subgroup of $\mathrm{GL}(2, q)$ comprising the matrices with determinant 1. Then $\mathrm{PGL}(2, q)$ and $\mathrm{PSL}(2, q)$ are the quotients of $\mathrm{GL}(2, q)$ and $\mathrm{SL}(2, q)$ by their respective centers.

When q is even, then one can identify $\mathrm{PSL}(2, q)$ with $\mathrm{SL}(2, q)$ and also with $\mathrm{PGL}(2, q)$, and so its order is $q(q-1)(q+1)$. When q is odd, the orders of $\mathrm{PGL}(2, q)$ and $\mathrm{PSL}(2, q)$ are $q(q-1)(q+1)$ and $\frac{1}{2}q(q-1)(q+1)$ respectively, and therefore we can identify $\mathrm{PSL}(2, q)$ with a normal subgroup of index 2 in $\mathrm{PGL}(2, q)$. Also recall that $\mathrm{PSL}(2, q)$ is simple for $q \neq 2, 3$.

One can classify the elements of $\mathrm{PSL}(2, q)$ according to the possible Jordan forms of their pre-images in $\mathrm{SL}(2, q)$. The following table lists the three types of elements, according to whether the characteristic polynomial $P(\lambda) := \lambda^2 - \alpha\lambda + 1$ of the matrix $A \in \mathrm{SL}(2, q)$ (where α is the trace of A) has 0, 1 or 2 distinct roots in $\mathbb{F}_q$.

element type	roots of $P(\lambda)$	canonical form in $\mathrm{SL}(2, \overline{\mathbb{F}_q})$	order	conjugacy classes
unipotent	1 root	$\begin{pmatrix} \pm 1 & 1 \\ 0 & \pm 1 \end{pmatrix}$ $\alpha = \pm 2$	p	two conjugacy classes in $\mathrm{PSL}(2, q)$, which unite in $\mathrm{PGL}(2, q)$
split	2 roots	$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ where $a \in \mathbb{F}_q^*$ and $a + a^{-1} = \alpha$	divides $\frac{1}{d}(q-1)$ $d = 1$ for q even $d = 2$ for q odd	for each α: one conjugacy class in $\mathrm{PSL}(2, q)$
non-split	no roots	$\begin{pmatrix} a & 0 \\ 0 & a^q \end{pmatrix}$ where $a \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ $a^{q+1} = 1$ and $a + a^q = \alpha$	divides $\frac{1}{d}(q+1)$ $d = 1$ for q even $d = 2$ for q odd	for each α: one conjugacy class in $\mathrm{PSL}(2, q)$

The subgroups of $\mathrm{PSL}(2,q)$ are well-known (see [Di, Su]), and fall into the following three classes.

Class I: The small triangle subgroups.

These are the *finite* triangle groups $\Delta = \Delta(l,m,n)$, which can occur if and only if $1/l + 1/m + 1/n > 1$.

This inequality holds only for the following triples:

- $(2,2,n)$: Δ is a dihedral subgroup of order $2n$.
- $(2,3,3)$: $\Delta \cong A_4$.
- $(2,3,4)$: $\Delta \cong S_4$.
- $(2,3,5)$: $\Delta \cong A_5$.

Moreover, if at least two of l,m and n are equal to 2 or if $2 \leq l,m,n \leq 5$, then a subgroup of $\mathrm{PSL}(2,q)$ which is generated by three elements t,u and $v=(tu)^{-1}$, of orders l,m and n respectively, may be a small triangle group (for a detailed list of such triples see [Ma, §8]).

Class II: Structural subgroups.

Let $\mathcal{B}$ be a subgroup of $\mathrm{PSL}(2,q)$ defined by the images of the matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\},$$

and let $\mathcal{C}$ be a subgroup of $\mathrm{PSL}(2,\overline{\mathbb{F}_q})$ defined by the images of the matrices

$$\left\{ \begin{pmatrix} t & 0 \\ 0 & t^q \end{pmatrix} : t \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q, t^{q+1} = 1 \right\}.$$

Any subgroup of $\mathrm{PSL}(2,q)$ which can be conjugated (in $\mathrm{PSL}(2,\overline{\mathbb{F}_q})$) to a subgroup of either $\mathcal{B}$ or $\mathcal{C}$ is called a *structural subgroup* of $\mathrm{PSL}(2,q)$.

Class III: Subfield subgroups.

If $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_q$, then $\mathrm{PSL}(2,p^r)$ is a subgroup of $\mathrm{PSL}(2,q)$. If the quadratic extension $\mathbb{F}_{p^{2r}}$ is also a subfield of $\mathbb{F}_q$, then $\mathrm{PGL}(2,p^r)$ is a subgroup of $\mathrm{PSL}(2,q)$. These groups, as well as any other subgroup of $\mathrm{PSL}(2,q)$ which is isomorphic to any one of them, will be referred to as *subfield subgroups* of $\mathrm{PSL}(2,q)$.

We note that all subgroups isomorphic to $\mathrm{PSL}(2,p^r)$ (or to $\mathrm{PGL}(2,p^r)$) are conjugate in $\mathrm{PGL}(2,q)$ and belong to at most two $\mathrm{PSL}(2,q)-$conjugacy classes.

3.3.2. *Theoretical Background II – Generation Theorems of Macbeath.* Let $(\alpha,\beta,\gamma) \in \mathbb{F}_q^3$, and denote

$$E(\alpha,\beta,\gamma) := \{A,B,C \in \mathrm{SL}(2,q) : ABC = I, \mathrm{tr}A = \alpha, \mathrm{tr}B = \beta, \mathrm{tr}C = \gamma\}.$$

Since all elements in $\mathrm{PSL}(2,q)$ whose pre-images in $\mathrm{SL}(2,q)$ have the same trace are conjugate in $\mathrm{PGL}(2,q)$, all of them have the same order in $\mathrm{PSL}(2,q)$. Therefore, we may denote by $\mathcal{O}rd(\alpha)$ the order in $\mathrm{PSL}(2,q)$ of the image of a matrix $A \in \mathrm{SL}(2,q)$ whose trace equals α, and denote, for an integer l,

$$\mathcal{T}_l = \{\alpha \in \mathbb{F}_q : \mathcal{O}rd(\alpha) = l\}.$$

Note that if q is odd then $\alpha \in \mathcal{T}_l$ if and only if $-\alpha \in \mathcal{T}_l$.

Now, one can easily compute the size of $\mathcal{T}_l$ for any integer l.

Lemma 3.15. *Let $q = 2^e$, then in* $\mathrm{PSL}(2,q) = \mathrm{SL}(2,q)$*,*

(*i*) $\mathcal{T}_2 = \{0\}$ *and so* $|\mathcal{T}_2| = 1$.
(*ii*) *If* $r \geq 3$ *and* $r \mid (q \pm 1)$ *then* $|\mathcal{T}_r| = \frac{\phi(r)}{2}$, *where* ϕ *is the Euler function.*
(*iii*) *For other values of* r, $|\mathcal{T}_r| = 0$.

Lemma 3.16. *Let* p *be an odd prime and let* $q = p^e$. *Then in* $\mathrm{PSL}(2, q)$,
(*i*) $\mathcal{T}_p = \{\pm 2\}$ *and so* $|\mathcal{T}_p| = 2$.
(*ii*) $\mathcal{T}_2 = \{0\}$ *and so* $|\mathcal{T}_2| = 1$.
(*iii*) *If* $r \geq 3$ *and* $r \mid \frac{q \pm 1}{2}$ *then* $|\mathcal{T}_r| = \phi(r)$, *where* ϕ *is the Euler function.*
(*iv*) *For other values of* r, $|\mathcal{T}_r| = 0$.

Remark 3.17. For example, $|\mathcal{T}_3| = 1$ if q is even and 2 if q is odd. Moreover, $\mathcal{T}_3 = \{1\}$ if $q = 2^e$, $\mathcal{T}_3 = \{\pm 1\}$ if $p \geq 5$, and $\mathcal{T}_3 = \{\pm 1\} = \{\pm 2\}$ for $p = 3$.

These two Lemmas are immediate, but for the convenience of the reader we shall present a proof of part *(iii)* of Lemma 3.16.

Proof of Lemma 3.16 (iii). Let λ be a primitive root of unity of order $2r$ in $\mathbb{F}_q$ (resp. in $\mathbb{F}_{q^2}$), then there are $2\phi(r)$ diagonal split (resp. non-split) matrices whose images in $\mathrm{PSL}(2, q)$ have exact order r, parameterized by $\{\pm\lambda^i : 1 \leq i \leq 2r, (i, 2r) = 1\}$, if r is odd, or by $\{\pm\lambda^i : 1 \leq i \leq r, (i, 2r) = 1\}$, if r is even.

Hence, there are exactly $\phi(r)$ different traces of split (resp. non-split) elements of order r, given as $\{\pm\alpha_1, \dots, \pm\alpha_\psi\}$, where $\psi = \frac{\phi(r)}{2}$. □

The importance of considering the sets of traces $\mathcal{T}_l$ and the set $E(\alpha, \beta, \gamma)$ is due to the following Theorems of Macbeath [Ma].

Theorem 3.18. [Ma, Theorem 1]. *$E(\alpha, \beta, \gamma)$ is not empty for any $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$.*

Definition 3.19. *Let $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$. We say that (α, β, γ) is* singular *if*

$$\alpha^2 + \beta^2 + \gamma^2 - \alpha\beta\gamma = 4.$$

Let $l = \mathcal{O}rd(\alpha)$, $m = \mathcal{O}rd(\beta)$ and $n = \mathcal{O}rd(\gamma)$. We say that (α, β, γ) is small *if at least two of l, m, n are equal to 2 or if $2 \leq l, m, n \leq 5$.*

Theorem 3.20. [Ma, Theorem 2]. *$(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is singular if and only if for $(A, B, C) \in E(\alpha, \beta, \gamma)$, the group generated by the images of A and B is a structural subgroup of* $\mathrm{PSL}(2, q)$.

Theorem 3.21. [Ma, Theorem 4]. *If $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is neither singular nor small, then for any $(A, B, C) \in E(\alpha, \beta, \gamma)$, the group generated by the images of A and B is a subfield subgroup of* $\mathrm{PSL}(2, q)$.

Theorem 3.22. [Ma, Theorem 3]. *If q is odd and $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is non-singular, then the image of $E(\alpha, \beta, \gamma)$ contains two* $\mathrm{PSL}(2, q)-$*conjugacy classes, and one* $\mathrm{PGL}(2, q)-$*conjugacy class.*

If q is even and $(\alpha, \beta, \gamma) \in \mathbb{F}_q^3$ is non-singular, then $E(\alpha, \beta, \gamma)$ contains one $\mathrm{PSL}(2, q)-$*conjugacy class.*

Recall that (A_1, B_1, C_1) and (A_2, B_2, C_2) are $\mathrm{PSL}(2, q)-$*conjugate* if there exists some $G \in \mathrm{PSL}(2, q)$ such that

$$GA_1G^{-1} = A_2 \text{ and } GB_1G^{-1} = B_2.$$

Note that this will immediately imply that $GC_1G^{-1} = GB_1^{-1}A_1^{-1}G^{-1} = B_2^{-1}A_2^{-1} = C_2$.

Macbeath [Ma] used these generation theorems of $\mathrm{PSL}(2,q)$ to prove that $\mathrm{PSL}(2,q)$ can be generated by two elements one of which is an involution. Moreover, he classified all the values of q for which $\mathrm{PSL}(2,q)$ is a *Hurwitz group*, namely a quotient of the Hurwitz triangle group $\Delta(2,3,7)$.

3.3.3. *Beauville Structures of* $\mathrm{PSL}(2,p^e)$.

Proof of 1.5. It is known by [BCG05, Proposition 3.6] (and can be easily verified by computer calculations) that $\mathrm{PSL}(2,2)\cong S_3$, $\mathrm{PSL}(2,3)\cong A_4$ and $\mathrm{PSL}(2,4)\cong\mathrm{PSL}(2,5)\cong A_5$ do not admit an unmixed Beauville structure.

Case $q=p^e$ odd.

Let $q\geq 13$ be an odd prime power, then we will construct an unmixed Beauville structure for $\mathrm{PSL}(2,q)$, $(A_1,B_1;A_2,B_2)$, of type (τ_1,τ_2), where

$$\tau_1=\left(\frac{q-1}{2},\frac{q-1}{2},\frac{q-1}{2}\right) \text{ and } \tau_2=\left(\frac{q+1}{2},\frac{q+1}{2},\frac{q+1}{2}\right).$$

Let $r=\frac{q-1}{2}$ (respectively $r=\frac{q+1}{2}$), and note that $r>5$. Let α be a trace of some diagonal split (respectively non-split) element $A\in\mathrm{SL}(2,q)$ whose image in $\mathrm{PSL}(2,q)$ has exact order r, and note that $\alpha\neq 0,\pm1,\pm2$, since A is neither of orders 2 or 3 nor unipotent (see Lemma 3.16 and Remark 3.17).

Observe that (α,α,α) is a non-singular triple. Indeed, the equality $3\alpha^2-\alpha^3=4$ is equivalent to $(\alpha-2)^2(\alpha+1)=0$, but the latter is not possible.

By Theorem 3.18, $E(\alpha,\alpha,\alpha)\neq\emptyset$, and since (α,α,α) is not singular nor small, for $(A,B,C)\in E(\alpha,\alpha,\alpha)$, one has $A\neq\pm B$, and moreover, the image of the subgroup $\langle A,B\rangle$ is a subfield subgroup of $\mathrm{PSL}(2,q)$, by Theorem 3.21. However, since the order of A is exactly $\frac{q-1}{2}$ (respectively $\frac{q+1}{2}$) then the image of the subgroup $\langle A,B\rangle$ is exactly $\mathrm{PSL}(2,q)$.

Observe that $\frac{q-1}{2}$ and $\frac{q+1}{2}$ are relatively prime. Hence, if $A_1,A_2\in\mathrm{PSL}(2,q)$ have orders $\frac{q-1}{2}$ and $\frac{q+1}{2}$ respectively, then every two non-trivial powers A_1^i and A_2^j have different orders, thus

$$\{g_1A_1^ig_1^{-1}\}_{g_1,i}\cap\{g_2A_2^jg_2^{-1}\}_{g_2,j}=\{1\},$$

implying that $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$, as needed.

For smaller values of q, a computer calculation (using MAGMA) shows that $\mathrm{PSL}(2,7)$ admits an unmixed Beauville structure of type $((4,4,4),(7,7,7))$, $\mathrm{PSL}(2,9)\cong A_6$ admits an unmixed Beauville structure of type $((4,4,4),(5,5,5))$, and $\mathrm{PSL}(2,11)$ admits an unmixed Beauville structure of type $((5,5,5),(6,6,6))$.

Case $q=2^e$ even.

Let $q\geq 8$ be an even prime power, then we will construct an unmixed Beauville structure for $\mathrm{PSL}(2,q)$, $(A_1,B_1;A_2,B_2)$, of type (τ_1,τ_2), where

$$\tau_1=(q-1,q-1,q-1) \text{ and } \tau_2=(q+1,q+1,q+1).$$

Let $r=q-1$ (respectively $r=q+1$), and note that $r>5$. Let α be a trace of some diagonal split (respectively non-split) element $A\in\mathrm{PSL}(2,q)=\mathrm{SL}(2,q)$ of exact order r, and note that $\alpha\neq 0,1$, since A is neither unipotent nor of order 3 (see Lemma 3.15 and Remark 3.17).

Observe that (α,α,α) is a non-singular triple. Indeed, the equality $\alpha^2+\alpha^2+\alpha^2-\alpha^3=4$ is equivalent (in characteristic 2) to $\alpha^2+\alpha^3=\alpha^2(\alpha+1)=0$, but the latter is not possible.

By Theorem 3.18, $E(\alpha,\alpha,\alpha)\neq\emptyset$, and since (α,α,α) is not singular nor small, for $(A,B,C)\in E(\alpha,\alpha,\alpha)$, one has $A\neq B$, and moreover, the subgroup $\langle A,B\rangle$ is a subfield subgroup of $\mathrm{PSL}(2,q)$, by Theorem 3.21. However, since the order of A is exactly $q-1$ (respectively $q+1$), then $\langle A,B\rangle=\mathrm{PSL}(2,q)$.

Observe that $q-1$ and $q+1$ are relatively prime (since both of them are odd). Hence, if $A_1,A_2\in\mathrm{PSL}(2,q)$ have orders $q-1$ and $q+1$ respectively, then every two non-trivial powers A_1^i and A_2^j have different orders, thus

$$\{g_1A_1^ig_1^{-1}\}_{g_1,i}\cap\{g_2A_2^jg_2^{-1}\}_{g_2,j}=\{1\},$$

implying that $\Sigma(A_1,B_1,C_1)\cap\Sigma(A_2,B_2,C_2)=\{1\}$, as needed. □

Remark 3.23. Note that in the case of $\mathrm{PSL}(2,q)$, unlike the case of alternating and symmetric groups, the possible types of the Beauville structures depend on $q=p^e$. Namely, one cannot fix a hyperbolic type (r,s,t) and hope that almost all groups $G=\mathrm{PSL}(2,q)$ with $lcm(r,s,t)$ dividing $|G|$, will be quotient of $\Delta(r,s,t)$.

Indeed, Macbeath [Ma, Theorem 8] proved that $\mathrm{PSL}(2,p^e)$ is a *Hurwitz group*, namely a quotient of $\Delta(2,3,7)$ if either $e=1$ and $p=0,\pm1 \pmod 7$, or $e=3$ and $p=\pm2,\pm3 \pmod 7$.

Recently, Marion [Mar09] showed that this phenomenon occurs in general for any prime hyperbolic type. Namely, he showed that if (p_1,p_2,p_3) is a hyperbolic triple of primes and p is a prime number, then there exists a unique integer e such that $\mathrm{PSL}(2,p^e)$ is a quotient of the triangle group $\Delta(p_1,p_2,p_3)$.

Interestingly, this situation is different for other families of groups of Lie type of low Lie rank (under the assumption that (p_1,p_2,p_3) are not too small), as was shown in recent results of Marion [Mar3.09, Mar9.09], which are detailed in Theorem 3.26 below.

3.3.4. *Hurwitz Components of* $\mathrm{PSL}(2,p)$. In order to estimate the number of Hurwitz components for $\mathrm{PSL}(2,p)$, we would first like to estimate the number $d(\mathrm{PSL}(2,q);\tau)$ for certain types τ, see Corollaries 3.3 and 3.4.

Recall that when p is an odd prime, the automorphisms of $\mathrm{PSL}(2,p)$ are exactly conjugations by elements of $\mathrm{PGL}(2,p)$, thus by Corollary 3.3, Theorem 3.21 and Theorem 3.22, we obtain the following.

Lemma 3.24. *Let $2\le l\le m\le n$ and assume that $m>2$ and $n>5$. Then*

$$d(\mathrm{PSL}(2,p);(l,m,n))=\#\big\{(\pm\alpha,\pm\beta,\pm\gamma):\\ \alpha\in\mathcal{T}_l,\beta\in\mathcal{T}_m,\gamma\in\mathcal{T}_n,\ \text{and } \alpha^2+\beta^2+\gamma^2-\alpha\beta\gamma\neq4\big\}.$$

Corollary 3.25. *Let $p\ge5$ be an odd prime, then in* $\mathrm{PSL}(2,p)$,

(*i*) $d(\mathrm{PSL}(2,p);(2,3,p))=1$.
(*ii*) *If $r\ge7$ and $r\mid\frac{p\pm1}{2}$ then* $d(\mathrm{PSL}(2,p);(2,3,r))=\frac{\phi(r)}{2}$.
(*iii*) $d(\mathrm{PSL}(2,p);(p,p,p))=1$.

(*iv*) *If* $r \geq 7$ *and* $r \mid \frac{p\pm1}{2}$ *then*

$$d(\mathrm{PSL}(2,p);(r,r,r)) = \frac{\psi(\psi+1)(\psi+2)}{6},$$

where $\psi = \frac{\phi(r)}{2}$.

(*v*) *If* $2 < l < m < n$ *such that* $n > 5$ *and* l, m, n *all divide* $\frac{p\pm1}{2}$, *then*

$$d(\mathrm{PSL}(2,p);(l,m,n)) = \frac{\phi(l)\phi(m)\phi(n)}{8}.$$

(*vi*) *If* $2 \leq l \leq m \leq n$ *such that* $m > 2$ *and* $n > 5$ *then*

$$d(\mathrm{PSL}(2,p);(l,m,n)) \leq \frac{\phi(l)\phi(m)\phi(n)}{8}.$$

Proof. The proof is based on Lemma 3.16 and Lemma 3.24.

(*i*) The orders $(2,3,p)$ correspond to the traces $(0,\pm1,\pm2)$.

(*ii*) The orders $(2,3,r)$ correspond to the traces $(0,\pm1,\pm\gamma)$, with $\mathcal{O}rd(\gamma) = r$. We need to verify that this triple is non-singular. Indeed, $0^2 + 1^2 + \gamma^2 - 0 = 4$ is equivalent to $\gamma^2 = 3$, and $\gamma^2 = 3$ if and only if $\mathcal{O}rd(\gamma) = 6$, a contradiction.

Here is an explanation of the last statement. Let μ be a primitive root of unity of order 12 (in $\mathbb{F}_p$ or in $\mathbb{F}_{p^2}$), and observe that there are exactly four such roots: $\pm\mu$ and $\pm\mu^{-1}$. Hence the trace of a split (or non-split) element of order 6 (in $\mathrm{PSL}(2,p)$) equals $\pm\gamma = \pm(\mu+\mu^{-1})$. Now, $\gamma^2 = \mu^2 + \mu^{-2} + 2 = -\rho - \rho^2 + 2 = 1 + 2 = 3$, as ρ is a third root of unity.

(*iii*) The orders (p,p,p) correspond to the traces $(-2,-2,2)$ (see [Ma, Theorem 7]).

(*iv*) The orders (r,r,r) correspond to the traces $(\pm\alpha_i,\pm\alpha_j,\pm\alpha_k)$ for $1 \leq i \leq j \leq k \leq \psi$. If $\alpha_i^2 + \alpha_j^2 + \alpha_k^2 - \alpha_i\alpha_j\alpha_k = 4$, then $\alpha_i^2 + \alpha_j^2 + \alpha_k^2 - \alpha_i\alpha_j\alpha_k \neq 4$, hence, if necessary, we may replace $(\alpha_i,\alpha_j,\alpha_k)$ by $(-\alpha_i,-\alpha_j,-\alpha_k)$, to get a non-singular triple. Therefore,

$$d(\mathrm{PSL}(2,p);(r,r,r)) = \binom{\psi}{3} + 2\binom{\psi}{2} + \psi = \frac{\psi(\psi+1)(\psi+2)}{6}.$$

(*v*) The orders (l,m,n) correspond to the traces (α,β,γ) where $\mathcal{O}rd(\alpha) = l$, $\mathcal{O}rd(\beta) = m$, $\mathcal{O}rd(\gamma) = n$, and $\alpha,\beta,\gamma \neq 0$. Now, we may replace (α,β,γ) by $(-\alpha,-\beta,-\gamma)$, to get a non-singular triple, if necessary.

(*vi*) This follows from the previous calculations.

□

Proof of Theorem 1.11. Let p be an odd prime, and let $\tau_1 = (l_1,m_1,n_1)$ and $\tau_2 = (l_2,m_2,n_2)$ be two hyperbolic types. By Corollary 3.25, for $i = 1,2$, $d(\mathrm{PSL}(2,p);(l_i,m_i,n_i))$ is maximal when l_i, m_i and n_i are three different integers dividing $\frac{p\pm1}{2}$, and hence is at most $\frac{\phi(l_i)\phi(m_i)\phi(n_i)}{8}$.

Recall that the automorphism group of $\mathrm{PSL}(2,p)$ is isomorphic to $\mathrm{PGL}(2,p)$. Define the following constant

$$c := \frac{\phi(l_1)\phi(m_1)\phi(n_1)\phi(l_2)\phi(m_2)\phi(n_2)}{64},$$

then, by Corollary 3.4,

$$h(G;\tau_1,\tau_2) \le d(G;\tau_1)\cdot d(G;\tau_2)\cdot |\mathrm{Aut}(G)| \le c\cdot p(p-1)(p+1) = O(p^3).$$

□

3.4. **Beauville Structures for Other Finite Simple Groups of Lie Type.** In this section we prove Theorem 1.6 regarding certain families of finite simple groups of Lie type of low Lie rank. The proof is based on recent results of Marion [Mar3.09, Mar9.09]. Moreover, we discuss some Conjectures on finite simple groups of Lie type in general.

3.4.1. *Beauville Structures for Finite Simple Groups of Low Lie Rank.*
Theorem 3.26. [Mar3.09, Theorems 1,2,4] *and* [Mar9.09, Theorem 1]. *Let G be one of the finite simple groups of Lie type listed below, and let (p_1,p_2,p_3) be a hyperbolic tripe of primes $p_1 \le p_2 \le p_3$, such that $lcm(p_1,p_2,p_3)$ divides $|G|$, which, moreover, satisfy the conditions given bellow.*

1. *Suzuki groups, $G = {}^2B_2(q)$, where $q = 2^{2e+1}$;*
2. *Ree groups, $G = {}^2G_2(q)$, where $q = 3^{2e+1}$;*
3. *$G = G_2(q)$, where $q = p^e$ for some prime number $p > 3$, and $(p_1,p_2,p_3) \notin \{(2,5,5),(3,3,5),(3,5,5),(5,5,5)\}$;*
4. *$G = {}^3D_4(q)$, where $q = p^e$ for some prime number $p > 3$, and (p_1,p_2,p_3) are distinct primes, s.t. $\{p_1,p_2\} \ne \{2,3\}$;*
5. *$G = \mathrm{PSL}(3,q)$, where $q = p^e$ for some prime p, and (p_1,p_2,p_3) are odd primes;*
6. *$G = \mathrm{PSU}(3,q)$, where $q = p^e$ for some prime p, and (p_1,p_2,p_3) are odd primes.*

Then, if $\phi \in \mathrm{Hom}(\Delta,G)$ is a randomly chosen homomorphism from the triangle group $\Delta = \Delta(p_1,p_2,p_3)$ to G, then

$$\lim_{q\to\infty} Prob\{\phi \text{ is surjective }\} = 1.$$

Now we have all the ingredients needed for the proof of Theorem 1.6.

Proof of Theorem 1.6.

(1) Let $G = {}^2B_2(q)$, where $q = 2^{2e+1}$, then
$$|G| = q^2(q^2+1)(q-1).$$
Since $q^2+1 \equiv 0 \pmod 5$, there are at least two prime numbers, 5 and some $r > 5$, which divide $|G|$. If q is large enough, then, by Theorem 3.26, the two triangle groups, $\Delta(5,5,5)$ and $\Delta(r,r,r)$, surject onto G, and hence G admits a Beauville structure of type $((5,5,5),(r,r,r))$.

(2) Let $G = {}^2G_2(q)$, where $q = 3^{2e+1}$, then
$$|G| = q^3(q-1)(q^3+1).$$
Since $q^3+1 \equiv 0 \pmod 7$, there are at least two odd prime numbers, 7 and some r ($7 \ne r > 3$), which divide $|G|$. If q is large enough, then, by Theorem 3.26, the two triangle groups, $\Delta(7,7,7)$ and $\Delta(r,r,r)$, surject onto G, and hence G admits a Beauville structure of type $((7,7,7),(r,r,r))$.

(3) Let $G = G_2(q)$, where $q = p^e$ for some prime number $p > 3$, then

$$|G| = q^6(q-1)^2(q+1)^2(q^2-q+1)(q^2+q+1),$$

(which is a factorization into irreducible polynomials), and so there are at least two distinct prime numbers, $r, s \geq 7$, which divide $|G|$. If q is large enough, then, by Theorem 3.26, the two triangle groups, $\Delta(r,r,r)$ and $\Delta(s,s,s)$, surject onto G, and hence G admits a Beauville structure of type $((s,s,s),(r,r,r))$.

(4) Let $G = {}^3D_4(q)$, where $q = p^e$ for some prime number $p > 3$, then

$$|G| = q^{12}(q-1)^2(q+1)^2(q^2-q+1)^2(q^2+q+1)^2(q^4-q^2+1),$$

(which is a factorization into irreducible polynomials), and so there are at least six distinct primes, $p_1 = 2, p_2 = 3, p_3, p_4, p_5, p_6$, which divide $|G|$. If q is large enough, then, by Theorem 3.26, the two triangle groups, $\Delta(2,p_3,p_5)$ and $\Delta(3,p_4,p_6)$, surject onto G, and hence G admits a Beauville structure of type $((2,p_3,p_5),(3,p_4,p_6))$.

(5) Let $G = \mathrm{PSL}(3,q)$ (resp. $G = \mathrm{PSU}(3,q)$), where $q = p^e$ for some prime p, then

$$|G| = \frac{1}{d}q^3(q-1)^2(q+1)(q^2+q+1),$$

(resp. $|G| = \frac{1}{d}q^3(q-1)(q+1)^2(q^2-q+1)$), where $d = 1$ or 3.

Hence, there are at least two distinct odd prime numbers, greater than 3, r and s, which divide $|G|$. If q is large enough, then, by Theorem 3.26, the two triangle groups, $\Delta(r,r,r)$ and $\Delta(s,s,s)$, surject onto G, and hence G admits a Beauville structure of type $((s,s,s),(r,r,r))$.

□

3.4.2. *Conjectures on Finite Simple Classical Groups of Lie Type.* Liebeck and Shalev raised the following Conjecture in [LS05] regarding finite simple classical groups of Lie type.

Conjecture 3.27 (Liebeck-Shalev)**.** For any Fuchsian group Γ there is an integer $f(\Gamma)$, such that if G is a finite simple classical group of Lie rank at least $f(\Gamma)$, then the probability that a randomly chosen homomorphism from Γ to G is an epimorphism tends to 1 as $|G| \to \infty$.

If this Conjecture holds, it immediately implies that any finite simple classical group G of Lie rank large enough admits an unmixed Beauville structure. Indeed, let s and t be two distinct primes greater than 3, then the triangle groups $\Delta(s,s,s)$ and $\Delta(t,t,t)$ will surject onto G, if G is of Lie rank large enough, yielding a Beauville structure of type $((s,s,s),(t,t,t))$ for G.

Moreover, this Conjecture inspired us to formulate Conjecture 1.7.

3.5. **Ramification Structures and Hurwitz Components for Abelian groups and their extensions.** In this Section we generalize previous results regarding abelian groups and their extensions, which appeared in [BCG05], and prove Theorem 1.12.

3.5.1. *Ramification Structures of Abelian Groups.* The following Theorem generalizes [BCG05, Theorem 3.4] in case G abelian and S is isogeneous to a higher product (not necessarily Beauville).

From now on we use the additive notation for abelian groups.

Theorem 3.28. *Let G be an abelian group, given as*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z},$$

where $n_1 \mid \cdots \mid n_t$. For a prime p, denote by $l_i(p)$ the largest power of p which divides n_i (for $1 \le i \le t$).

Let $r_1, r_2 \ge 3$, then G admits an unmixed ramification structure of size (r_1, r_2) if and only if the following conditions hold:

- $r_1, r_2 \ge t+1$;
- $n_t = n_{t-1}$;
- *If* $l_{t-1}(3) > l_{t-2}(3)$ *then* $r_1, r_2 \ge 4$;
- $l_{t-1}(2) = l_{t-2}(2)$;
- *If* $l_{t-2}(2) > l_{t-3}(2)$ *then* $r_1, r_2 \ge 5$ *and* r_1, r_2 *are not both odd.*

Proof. Let $(x_1, \ldots, x_{r_1}; y_1, \ldots, y_{r_2})$ be an unmixed ramification structure of size (r_1, r_2). Set

$$\Sigma_1 := \Sigma(x_1, \ldots, x_{r_1}) := \{i_1x_1, \ldots, i_{r_1}x_{r_1} : i_1, \ldots i_{r_1} \in \mathbb{Z}\},$$

and

$$\Sigma_2 := \Sigma(y_1, \ldots, y_{r_2}) := \{j_1y_1, \ldots, j_{r_2}y_{r_2} : j_1, \ldots j_{r_2} \in \mathbb{Z}\},$$

and recall that $\Sigma_1 \cap \Sigma_2 = \{0\}$.

Consider the primary decomposition of G,

$$G = \bigoplus_{p \in \{\text{Primes}\}} G_p,$$

and observe that since G is generated by $\min\{r_1, r_2\} - 1$ elements, so is any G_p (which is a characteristic subgroup of G).

Therefore, G_p can be written as

$$G_p \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k_{t-1}}\mathbb{Z} \times \mathbb{Z}/p^{k_t}\mathbb{Z},$$

where $k_1 \le \cdots \le k_{t-1} \le k_t$ and $1 \le t \le \min\{r_1, r_2\} - 1$.

Denote $H_p := p^{k_t-1}G_p$, and observe that H_p is an elementary abelian group of rank at most t.

Step 1. Let $x_1 = (x_{1,p}) \in \bigoplus_{p \in \{\text{Primes}\}} G_p$ and let

$$\Sigma_{1,p} := \Sigma(x_{1,p}, \ldots, x_{r_1,p}) := \{l_1x_{1,p}, \ldots, l_{r_1}x_{r_1,p} : l_1, \ldots l_{r_1} \in \mathbb{Z}\},$$

be the set of multiples of $(x_{1,p}, \ldots, x_{r_1,p})$, then by the Chinese Remainder Theorem, $x_{1,p}$ is a multiple of x_1, and hence $\Sigma_1 \supseteq \Sigma_{1,p}$.

Step 2. G_p is not cyclic.

Otherwise, if $G_p \cong \mathbb{Z}/p^k\mathbb{Z}$, then $H_p = p^{k-1}G_p \cong \mathbb{Z}/p\mathbb{Z}$. Since $\Sigma_{1,p}$ contains a generator of G_p, it also contains a non-trivial element of H_p and so $\Sigma_{1,p} \supseteq H_p$. Thus $\Sigma_1 \supseteq H_p$, and similarly $\Sigma_2 \supseteq H_p$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{0\}$.

Step 3. $k_t = k_{t-1}$, namely $G_p \cong \mathbb{Z}/p^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k_{t-1}}\mathbb{Z} \times \mathbb{Z}/p^{k_{t-1}}\mathbb{Z}$, where $k_1 \le \cdots \le k_{t-1}$ and $2 \le t \le \min\{r_1, r_2\} - 1$.

Otherwise, if $k_t \neq k_{t-1}$, then $H_p = p^{k_t-1}G_p \cong \mathbb{Z}/p\mathbb{Z}$. As in Step 2, $\Sigma_{1,p}$ contains a generator of G_p, and so it also contains a non-trivial element of H_p. Thus $\Sigma_{1,p} \supseteq H_p$, and similarly $\Sigma_{2,p} \supseteq H_p$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{0\}$.

Step 4. $p = 2$ or 3.

The extra conditions for $p = 2$ and 3 are due to dimensional reasons.

- Let $p = 2$ and assume that $k_{t-1} > k_{t-2}$. In this case, $H_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$ contains only three non-trivial vectors. However, $|H_2 \cap \Sigma_{1,2}| \geq 2$ and $|H_2 \cap \Sigma_{2,2}| \geq 2$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{0\}$.
- Let $p = 2$ and assume that $k_{t-1} = k_{t-2} > k_{t-3}$. In this case, $H_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$ contains only seven non-trivial vectors.

  If $r_1 = 4$ then $\Sigma_{1,2}$ contains four different vectors which generate H_2, whose sum is zero, say $\{e_1, e_2, e_3, e_1 + e_2 + e_3\}$. Now, the other three vectors in H_2 are necessarily $\{e_1 + e_2, e_1 + e_3, e_2 + e_3\}$, which are linearly dependent, and so cannot generate $H_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$.

  When r_1 is odd, $\Sigma_{1,2}$ contains four different vectors from H_2. Indeed, a sum $x_1 + \cdots + x_{r_1}$ of some vectors v, u, w over $\mathbb{Z}/2\mathbb{Z}$ (i.e. $x_i \in \{v, u, w\}$), where r_1 is odd, cannot be equal to 0, unless v, u and w are linearly dependent, and so cannot generate $H_2 \cong (\mathbb{Z}/2\mathbb{Z})^3$. Thus, if r_1 is odd, then $|H_2 \cap \Sigma_{1,2}| \geq 4$, and similarly, if r_2 is odd, then $|H_2 \cap \Sigma_{2,2}| \geq 4$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{0\}$.
- Let $p = 3$ and assume that $k_{t-1} > k_{t-2}$. In this case, $H_3 \cong (\mathbb{Z}/3\mathbb{Z})^2$ contains only eight non-trivial vectors. If $r_1 = 3$ then $\Sigma_{1,3}$ contains three different vectors, which generate H_3, whose sum is zero, say $\{e_1, e_2, 2e_1 + 2e_2\}$, as well as their multiples $\{2e_1, 2e_2, e_1 + e_2\}$. Now, the other two vectors in H_2 are necessarily $\{e_1 + 2e_2, 2e_1 + e_2\}$, which are linearly dependent, and so cannot generate $H_3 \cong (\mathbb{Z}/3\mathbb{Z})^2$.

Step 5. Now, let $p \geq 5$ and assume that $G_p = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k_{t-1}}\mathbb{Z} \times \mathbb{Z}/p^{k_{t-1}}\mathbb{Z}$, where $k_1 \leq \cdots \leq k_{t-1}$ and $2 \leq t \leq \min\{r_1, r_2\} - 1$. We will choose appropriate vectors for $\Sigma_{1,p}$ and $\Sigma_{2,p}$.

Assume that (a, b, c, d) satisfy the condition in Equation (11) below, and let

$$\begin{array}{rlrl}
x_{1,p} &= (1, 0, \dots, 0, 1, 0) & y_{1,p} &= (1, 0, \dots, 0, a, b) \\
x_{2,p} &= (0, 1, 0, \dots, 0, 0, 1) & y_{2,p} &= (0, 1, 0, \dots, 0, c, d) \\
x_{3,p} &= (0, 0, 1, 0, \dots, 0, -1, 0) & y_{3,p} &= (0, 0, 1, 0, \dots, 0, -a, -b) \\
x_{4,p} &= (0, 0, 0, 1, 0 \dots, 0, 0, -1) & y_{4,p} &= (0, 0, 0, 1, 0, \dots, 0, -c, -d) \\
&\vdots & &\vdots \\
x_{t-2,p} &= (0, \dots, 0, 1, *, *) & y_{t-2,p} &= (0, \dots, 0, 1, *, *) \\
x_{t-1,p} &= (0, \dots, 0, 0, *, *) & y_{t-1,p} &= (0, \dots, 0, 0, *, *) \\
x_{t,p} &= (0, \dots, 0, 0, *, *) & y_{t,p} &= (0, \dots, 0, 0, *, *) \\
&\vdots & &\vdots \\
x_{r_1,p} &= (-1, \dots, -1, -1, -1) & y_{r_2,p} &= (-1, \dots, -1, -a-c, -b-d)
\end{array}$$

where the elements marked with $(*,*)$ in $x_{t-2,p}$ (and after) are chosen from $\{(0,\pm1),(\pm1,0),\pm(1,1)\}$ such that $(x_{1,p},x_{2,p},\dots,x_{t,p})$ are independent and the sum $x_{1,p}+\cdots+x_{r_1,p}=0$. Similarly, the elements marked with $(*,*)$ in $y_{t-2,p}$ (and after) are chosen from $\{\pm(a,b),\pm(c,d),\pm(a+c,b+d)\}$, such that $(y_{1,p},y_{2,p},\dots,y_{t,p})$ are independent and $y_{1,p}+\cdots+y_{r_1,p}=0$.

Since $\langle x_{1,p},\dots,x_{r_1,p}\rangle=G_p=\langle y_{1,p},\dots,y_{r_2,p}\rangle$, we deduce that $(x_{1,p},\dots,x_{r_1,p})$ form a spherical r_1-system of generators for G_p and that $(y_{1,p},\dots,y_{r_2,p})$ form a spherical r_2-system of generators for G_p. Moreover, for every $1\le i\le r_1$, $1\le j\le r_2$, and $k,l\in\mathbb{Z}$, if the vectors $kx_{i,p}$ and $ly_{j,p}$ are not trivial, then they are linearity independent. Hence, $\Sigma_{1,p}\cap\Sigma_{2,p}=\{0\}$, as needed.

When $p=2$ or 3 it suffices to construct unmixed ramification structures for the elementary abelian groups in characteristic 2 and 3. These yield an unmixed ramification structure for any choice of H_2 (resp. H_3), which induces an appropriate structure for any G_2 (resp. G_3), by completing the generating vectors of H_2 (resp. H_3) to generating vectors of G_2 (resp. G_3), essentially in the same way of $p\ge5$. These constructions are described in the following Lemmas 3.29 and 3.30.

Now, recall that by using the primary decomposition of G, it was enough to check the conditions on each primary component G_p, thus G admits an unmixed ramification structure of size (r_1,r_2) as needed. □

Lemma 3.29. *Let $G=(\mathbb{Z}/2\mathbb{Z})^t$.*

If $t\ge4$ then G always admits an unmixed ramification structure of size (r_1,r_2), for any $r_1,r_2\ge t+1$.

If $t=3$ then G admits an unmixed ramification structure of size (r_1,r_2), if and only if $r_1,r_2\ge5$ and r_1, r_2 are not both odd.

Proof. It is enough to show the existence of structures satisfying the above conditions, as in Step 4 of Theorem 3.28 we proved that they are necessary.

Let $t\ge4$. It is enough to construct such a structure for the cases

$$r_1=t+1=r_2,\quad r_1=t+2=r_2\quad\text{and}\quad r_1=t+1,r_2=t+2.$$

Indeed, if for some value of r, $\{v_1,\dots,v_r\}$ is a set of r vectors, that generate $G=(\mathbb{Z}/2\mathbb{Z})^t$ and whose sum is zero, then so is also the set of $r+2$ vectors $\{v_1,\dots,v_r,v_r,v_r\}$. In this way, one can construct any set of size $r+2k$ (for any $k\in\mathbb{N}$).

Now, we can construct the following unmixed ramification structure, where $r_1=t+1=r_2$:

$$\begin{aligned}
x_1&=(1,0,\dots,0) & y_1&=(1,1,0,\dots,0)\\
x_2&=(0,1,0,\dots,0) & y_2&=(0,1,1,0,\dots,0)\\
&\vdots & &\vdots\\
x_{t-1}&=(0,\dots,1,0) & y_{t-1}&=(0,\dots,0,1,1)\\
x_t&=(0,\dots,0,1) & y_t&=(1,1,1,0\dots,0)\\
x_{t+1}&=(1,1,\dots,1,1) & y_{t+1}&=(0,1,1,0\dots,0,1)
\end{aligned}$$

We can construct the following unmixed ramification structure, where $r_1 = t+2 = r_2$:

$$\begin{aligned} x_1 &= (1,0,\ldots,0) & y_1 &= (1,1,0,\ldots,0) \\ x_2 &= (0,1,0,\ldots,0) & y_2 &= (0,1,1,0,\ldots,0) \\ &\vdots & &\vdots \\ x_{t-1} &= (0,\ldots,0,1,0) & y_{t-1} &= (0,\ldots,0,1,1) \\ x_t &= (0,\ldots,0,0,1) & y_t &= (1,1,1,0\ldots,0) \\ x_{t+1} &= (0,\ldots,0,1,0) & y_{t+1} &= (1,1,1,0\ldots,0) \\ x_{t+2} &= (1,\ldots,1,0,1) & y_{t+2} &= (1,0,\ldots,0,1) \end{aligned}$$

By taking the $t+1$ vectors $\{x_1,\ldots,x_{t+1}\}$ from the first structure, and the $t+2$ vectors $\{y_1,\ldots,y_{t+2}\}$ from the second structure, one obtains an unmixed ramification structure with $r_1 = t+1$ and $r_2 = t+2$.

Where $t = 3$, we can construct the following structure with $r_1 = r_2 = 6$:

$$\Sigma_1 = \{(1,0,0),(1,1,0),(1,1,1),(1,0,0),(1,1,0),(1,1,1)\},$$
$$\Sigma_2 = \{(0,0,1),(0,1,1),(1,0,1),(0,0,1),(0,1,1),(1,0,1)\},$$

and so, we can construct any structure for which $r_1, r_2 \geq 6$ are even.

We can also construct the following structure with $r_1 = 5$ and $r_2 = 6$:

$$\Sigma_1 = \{(1,0,0),(0,1,0),(1,1,0),(1,0,1),(1,0,1)\},$$
$$\Sigma_2 = \{(0,0,1),(0,1,1),(1,1,1),(0,0,1),(0,1,1),(1,1,1)\},$$

and so, we can construct any structure for which $r_1 \geq 5$ is odd and $r_2 \geq 6$ is even, and vice versa. □

Lemma 3.30. *Let $G = (\mathbb{Z}/3\mathbb{Z})^t$.*

If $t \geq 3$ then G always admits an unmixed ramification structure of size (r_1, r_2), for any $r_1, r_2 \geq t+1$.

If $t = 2$ then G admits an unmixed ramification structure of size (r_1, r_2), if and only if $r_1, r_2 \geq 4$.

Proof. It is enough to show the existence of structures satisfying the above conditions, as in Step 4 of Theorem 3.28 we proved that they are necessary.

Note that it is enough to construct such a structure for the minimal possible values of r_1 and r_2. Indeed, if for some value of r, $\{v_1,\ldots,v_r\}$ is a set of r vectors, that generate $G = (\mathbb{Z}/3\mathbb{Z})^t$ and whose sum is zero, then one can also construct the following sets, which have the same properties:

- $\{v_1,\ldots,v_{r-1},v_r,v_r,v_r,v_r\}$ of size $r+3$ (and so any set of size $r+3k$).
- $\{v_1,\ldots,v_{r-1},2v_r,2v_r\}$ of size $r+1$ (and so any set of size $r+3k+1$).
- $\{v_1,\ldots,v_{r-1},v_r,v_r,2v_r\}$ of size $r+2$ (and so any set of size $r+3k+2$).

Now, if $t \geq 3$, we can construct the following unmixed ramification structure, where $r_1 = r_2 = t+1$:

$$\begin{aligned} x_1 &= (1,0,\dots,0) & y_1 &= (1,2,0,\dots,0) \\ x_2 &= (0,1,0,\dots,0) & y_2 &= (0,1,2,0,\dots,0) \\ &\vdots & &\vdots \\ x_{t-1} &= (0,\dots,1,0) & y_{t-1} &= (0,\dots,0,1,2) \\ x_t &= (0,\dots,0,1) & y_t &= (1,\dots,1,1,2) \\ x_{t+1} &= (2,2,\dots,2,2) & y_{t+1} &= (1,2,\dots,2,2) \end{aligned}$$

And when $t = 2$, we can construct the following structure, with $r_1, r_2 = 4$:

$$\begin{aligned} \Sigma_1 &= \{(1,0),(0,1),(2,0),(0,2)\}, \\ \Sigma_2 &= \{(1,2),(1,1),(2,1),(2,2)\}. \end{aligned}$$

$\square$

Lemma 3.31. *Let $p \geq 5$ be a prime number and $U := (\mathbb{Z}/p\mathbb{Z})^*$, the number N of quadruples $(a,b,c,d) \in U$ such that:*

$$a-b,\ a+c,\ c-d,\ b+d,\ a+c-b-d,\ ad-bc \in U \tag{11}$$

is $N = (p-1)(p-2)(p-3)(p-4)$.

Proof. The number N equals $p-1$ times the number of solutions that we get for $a = 1$. Now, $b \neq 0, 1$, so there are $p-2$ possibilities for b. The conditions $c \neq 0, -1$ and $d \neq 0, -b$ imply $(p-2)^2$ possibilities for the pair (c,d). From this number we need to subtract the number of solutions for $c = d$, $d = 1-b+c$ and $d = bc$, which are $p-2$, $p-2$ and $p-4$ respectively. We deduce that there are $(p-2)^2 - [(p-2)+(p-2)+(p-4)] = (p-3)(p-4)$ possibilities for the pair (c,d). Hence $N = (p-1)(p-2)(p-3)(p-4)$. $\square$

We remark that this Lemma corrects the calculation given in [BCG05, Theorem 3.4].

3.5.2. *Hurwitz Components in Case $(\mathbb{Z}/n\mathbb{Z})^2$.* Observe that for $G = (\mathbb{Z}/n\mathbb{Z})^2$ there is only one type of a spherical $3-$system of generators, which is $\tau = (n,n,n)$. Also note that $\mathrm{Aut}(G) \cong \mathrm{GL}(2,n)$.

The following Lemmas give a more precise estimation of the number of Hurwitz components in case $G = (\mathbb{Z}/n\mathbb{Z})^2$, which generalizes Remark 3.5 in [BCG05].

Lemma 3.32. *Let $p \geq 5$ be a prime. The number $h = h(G;\tau,\tau)$, where $\tau = (p,p,p)$, of Hurwitz components for $G = (\mathbb{Z}/p\mathbb{Z})^2$ satisfies*

$$N_p/36 \leq h \leq N_p/6,$$

where $N_p = (p-1)(p-2)(p-3)(p-4)$.

Proof. Let $(x_1,x_2;y_1,y_2)$ be an unmixed Beauville structure for G. Since x_1, x_2 are generators of G, they are a basis, and without loss of generality x_1, x_2 are the standard basis $x_1 = (1,0)$, $x_2 = (0,1)$. Now, let $y_1 = (a,b)$, $y_2 = (c,d)$, then the condition $\Sigma_1 \cap \Sigma_2 = \{0\}$ means that any pair of the six vectors yield a basis of G, implying that a,b,c,d must satisfy the conditions given in Equation (11).

Moreover, the N_p pairs $\big((1,0),(0,1);(a,b),(c,d)\big)$, where a,b,c,d satisfy (11), are exactly the representatives for the $\mathrm{Aut}(G)-$orbits in the set $\mathcal{U}(G;\tau,\tau)$.

Now, one should consider the action of $B_3 \times B_3$ on $\mathcal{U}(G;\tau,\tau)$, which is equivalent to the action of $S_3 \times S_3$, since G is abelian. The action of S_3 on the second component is obvious (there are 6 permutations), and the action of S_3 on the first component can be translated to an equivalent $\mathrm{Aut}(G)-$action, given by multiplication in one of the six matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$

yielding an equivalent representative.

Therefore, the action of S_3 on the second component yields orbits of length 6, and the action of S_3 on the first component connects them together, and gives orbits of sizes from 6 to 36, which implies the desired result. □

Corollary 3.33. *Let $p \geq 5$ be a prime. The number $h = h(G;\tau,\tau)$, where $\tau = (p^k, p^k, p^k)$, of Hurwitz components for $G = (\mathbb{Z}/p^k\mathbb{Z})^2$ satisfies*

$$N_{p^k}/36 \leq h \leq N_{p^k}/6,$$

where $N_{p^k} = p^{4k-4}(p-1)(p-2)(p-3)(p-4)$.

Proof. In this case, the number N_{p^k} of $\mathrm{Aut}(G)-$orbits in the set $\mathcal{U}(G;\tau,\tau)$ is exactly p^{4k-4} times N_p, and the proof is the same as in the previous Lemma 3.32. □

Corollary 3.34. *Let n be an integer s.t. $(n,6) = 1$. The number $h = h(G;\tau,\tau)$, where $\tau = (n,n,n)$, of Hurwitz components for $G = (\mathbb{Z}/n\mathbb{Z})^2$, where $n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$, satisfies*

$$N_n/36 \leq h \leq N_n/6,$$

where $N_n = \prod_{i=1}^{t} p_i^{4k_i-4}(p_i-1)(p_i-2)(p_i-3)(p_i-4)$.

Proof. By the Chinese Remainder Theorem, the number N_n of $\mathrm{Aut}(G)-$orbits in the set $\mathcal{U}(G;\tau,\tau)$ can be computed using Corollary 3.33, and the proof is now the same as in Lemma 3.32. □

Since $N_n = \Theta(n^4)$, this completes the proof of Theorem 1.12.

3.5.3. *Hurwitz Components in Case G Abelian and S not Beauville.* Fix an integer r, let $p > 5$ be a prime number, and let $G = (\mathbb{Z}/p\mathbb{Z})^r$, then by Theorem 3.28, G admits an unmixed ramification structure of type (τ_1, τ_2) where $\tau_1 = \tau_2 = \tau = (p, \ldots, p)$ (p appears $(r+1)-$times) and $r_1 = r_2 = r+1$.

Proposition 3.35. *Fix an integer $r \geq 2$, then the number $h = h(G;\tau,\tau)$ of Hurwitz components for $G = (\mathbb{Z}/p\mathbb{Z})^r$ and $\tau = (p,\ldots,p)$ (p appears $(r+1)-$times) satisfies, as $p \to \infty$,*

$$h = \Theta(p^{r^2}).$$

Proof. Let $(x_1,\ldots,x_{r+1}; y_1,\ldots,y_{r+1})$ be an unmixed ramification structure for G. Since $x_1,\ldots,x_{r+1}$ generate G, they are a basis, and without loss of generality they are of the form given in Step 5 of Theorem 3.28. However, for $y_1,\ldots,y_{r+1}$ one can take any appropriate set of $r+1$ vectors in $(\mathbb{Z}/p\mathbb{Z})^r$, which admit an unmixed ramification structure, and so each proper choice of $(y_1, \dots, y_{r+1})$ corresponds to exactly one $\mathrm{Aut}(G)-$orbit in the set $\mathcal{U}(G;\tau,\tau)$.

Therefore, one can choose any invertible $(r-2)\times(r-2)$ matrix for

$$\begin{pmatrix} y_{1,1} & \cdots & y_{1,r-2} \\ & \vdots & \\ y_{r-2,1} & \cdots & y_{r-2,r-2} \end{pmatrix},$$

choose any vector of length $r-2$ for $(y_{r-1,1}, \dots, y_{r-1,r-2})$, and similarly for $(y_{r,1}, \dots, y_{r,r-2})$. Moreover, for $1 \le i \le r-2$, one can choose for $(y_{i,r-1}, y_{i,r})$ any vector from the set $S := \{(a,b) \in \mathbb{F}_p^2 : a \neq 0, b \neq 0, a \neq b\}$. Observe that $|S| = (p-1)(p-2)$.

Now, one has to make sure that y_{r-1} is not a linear combination of $y_1, \dots, y_{r-2}$, by choosing $(y_{r-1,r-1}, y_{r-1,r})$ appropriately from S, and so there are at least $(p-1)(p-2)-1 = p^2-3p+1$ possibilities for this pair. Moreover, one should choose $(y_{r,r-1}, y_{r,r})$ appropriately from S, such that y_r is not some linear combination of $y_1, \dots, y_{r-1}$, and that $(y_{r+1,r-1}, y_{r+1,r}) \in S$, and so the number of possibilities to the pair $(y_{r,r-1}, y_{r,r})$ is at least $(p-3)(p-5) = p^2-8p+15$.

The condition that the pairs $(y_{i,r-1}, y_{i,r}) \in S$ for $1 \le i \le r+1$ is needed to guarantee that for any $k,l \in \mathbb{Z}$ and $1 \le i,j \le r+1$, if the vectors kx_i and ly_j are not trivial, then they are linearity independent, and so $\Sigma_1 \cap \Sigma_2 = \{0\}$, as needed.

Hence, the number of $\mathrm{Aut}(G)-$orbits in the set $\mathcal{U}(G;\tau,\tau)$ is bounded from below by

$$\begin{aligned} &|\mathrm{GL}((r-2),p)|p^{2(r-2)}\big((p-1)(p-2)\big)^{r-2}(p^2-3p+1)(p^2-8p+15) \\ &= \Theta\big(p^{(r-2)^2+2(r-2)+2(r-2)+2+2}\big) = \Theta\big(p^{r^2}\big). \end{aligned}$$

It is clear that the number of orbits is bounded from above by

$$|\mathrm{GL}(r,p)| = \Theta(p^{r^2}).$$

Now, the action of $B_{r+1} \times B_{r+1}$ on the $\mathrm{Aut}(G)-$orbits of $\mathcal{U}(G;\tau,\tau)$, is equivalent to the action of $S_{r+1} \times S_{r+1}$, since G is abelian, and so yields orbits of sizes between $(r+1)!$ and $((r+1)!)^2$. This has no effect on the above asymptotic, however, since r is fixed. $\square$

3.5.4. *Extensions of Abelian Groups.* The following Proposition generalizes the result in [BCG05, Lemma 3.7], that dihedral groups do not admit unmixed Beauville structures, and is needed for the proof of Lemma 2.8.

Proposition 3.36. *For any $n, m \in \mathbb{N}$, the finite group*

$$G = \mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$$

does not admit an unmixed ramification structure of size $(4,4)$.

Proof. Observe that G can be presented by

$$G = \langle t, r, s : t^2, r^m, s^n, [r,s], tsts, trtr \rangle,$$

and so any element in G can be written uniquely as $t^\epsilon r^i s^j$ for $\epsilon \in \{0,1\}$, $1 \le i \le m$, $1 \le j \le n$.

Conjugation of some element $tr^i s^j$ by r^{-1} yields $r^{-1}tr^i s^j r = ttr^{-1}tr^i s^j r = trr^i r s^j = tr^{i+2}s^j$, and similarly conjugation by s^{-1} yields $tr^i s^{j+2}$. Hence, $tr^i s^j$ can be conjugated to $tr^{i+2k}s^{j+2l}$ for any k, l.

Let $A \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ be the maximal normal abelian subgroup in G, then $G \setminus A$ contains at most four conjugacy classes, represented by t, tr, ts, trs. In fact, it contains one conjugacy class if both m, n are odd, two conjugacy classes if one of m, n is odd and the other is even, and four if both m, n are even.

Since any spherical 4−system of generators of G must contain an element of $G \setminus A$, the condition that $\Sigma_1 \cap \Sigma_2 = \{1\}$ immediately implies that m, n cannot both be odd.

Assume now that m is even and n is odd, and consider the following map

$$G \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^2, \text{ defined by } (t^\epsilon r^i s^j) \mapsto \big(\epsilon, i(\text{mod } 2)\big).$$

Note that for any j and any odd i, one has that

$$(r^i s^j)^{nm/2} = (r^{m/2})^{ni}(s^n)^{mj/2} = r^{m/2} =: u \neq 1.$$

If $T = (t^{\epsilon_1}r^{i_1}s^{j_1}, t^{\epsilon_2}r^{i_2}s^{j_2}, t^{\epsilon_3}r^{i_3}s^{j_3}, t^{\epsilon_4}r^{i_4}s^{j_4})$ is a spherical 4−system of generators of G, then $\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 \equiv 0 \pmod 2$, $i_1 + i_2 + i_3 + i_4 \equiv 0 \pmod 2$, and the images of the elements in T generate $(\mathbb{Z}/2\mathbb{Z})^2$. Hence, the image in $(\mathbb{Z}/2\mathbb{Z})^2$ of such a spherical 4−system of generators can be (up to a permutation) only one of

(i) $\{(1,1),(1,0),(0,1),(0,0)\}$,
(ii) $\{(1,1),(1,1),(1,0),(1,0)\}$,
(iii) $\{(1,1),(1,1),(0,1),(0,1)\}$,
(iv) $\{(1,0),(1,0),(0,1),(0,1)\}$.

Therefore, for any two spherical 4-systems T_1 and T_2 one can find $x \in T_1$ and $y \in T_2$ such that either

- $x, y \in G \setminus A$ are conjugate; or
- $x, y \in A$ and $x^{mn/2} = u = y^{mn/2}$;

a contradiction to $\Sigma_1 \cap \Sigma_2 = \{1\}$.

If both m and n are even, write $m = 2^\mu m'$ and $n = 2^\nu n'$, where m', n' are odd. Without loss of generality, we may assume that $\mu \geq \nu$.

Consider the following map

$$G \twoheadrightarrow (\mathbb{Z}/2\mathbb{Z})^3, \text{ defined by } (t^\epsilon r^i s^j) \mapsto \big(\epsilon, i(\text{mod } 2), j(\text{mod } 2)\big).$$

If $\mu > \nu$ and if i is odd then

$$(r^i s^j)^{2^{\mu-1}m'n'} = (r^{2^{\mu-1}m'})^{in'}(s^{2^{\mu-1}n'})^{jm'} = r^{m/2} := u \neq 1,$$

and if $\mu = \nu$ then

$$(r^i s^j)^{2^{\mu-1}m'n'} = \begin{cases} r^{m/2} := u \neq 1, & \text{if } i \text{ is odd and } j \text{ is even;} \\ s^{n/2} := v \neq 1, & \text{if } i \text{ is even and } j \text{ is odd;} \\ r^{m/2}s^{n/2} := w \neq 1, & \text{if } i, j \text{ are odd.} \end{cases}$$

If $T = (t^{\epsilon_1}r^{i_1}s^{j_1}, t^{\epsilon_2}r^{i_2}s^{j_2}, t^{\epsilon_3}r^{i_3}s^{j_3}, t^{\epsilon_4}r^{i_4}s^{j_4})$ is a spherical 4−system of generators of G, then $\epsilon_1 + \epsilon_2 + \epsilon_3 + \epsilon_4 \equiv 0 \pmod 2$, $i_1 + i_2 + i_3 + i_4 \equiv 0 \pmod 2$, $j_1 + j_2 + j_3 + j_4 \equiv 0 \pmod 2$ and the images of the elements in T generate $(\mathbb{Z}/2\mathbb{Z})^3$. Hence, the image in $(\mathbb{Z}/2\mathbb{Z})^3$ of such a spherical $4-$system of generators can be (up to a permutation) only one of

(i) $\{(1,1,1),(1,0,0),(0,1,0),(0,0,1)\}$,
(ii) $\{(1,1,0),(1,0,1),(0,1,0),(0,0,1)\}$,
(iii) $\{(1,1,0),(1,0,0),(0,1,1),(0,0,1)\}$,
(iv) $\{(1,1,1),(1,0,1),(0,1,1),(0,0,1)\}$,
(v) $\{(1,0,1),(1,0,0),(0,1,1),(0,1,0)\}$,
(vi) $\{(1,1,1),(1,1,0),(0,1,1),(0,1,0)\}$,
(vii) $\{(1,1,1),(1,1,0),(1,0,1),(1,0,0)\}$.

Therefore, for any two spherical 4-systems T_1 and T_2 one can find $x \in T_1$ and $y \in T_2$ such that either

- $x, y \in G \setminus A$ are conjugate; or
- $x, y \in A$ and $x^{2^{\mu-1}m'n'} = u = y^{2^{\mu-1}m'n'}$; or
- $x, y \in A$ and $x^{2^{\mu-1}m'n'} = v = y^{2^{\mu-1}m'n'}$;

a contradiction to $\Sigma_1 \cap \Sigma_2 = \{1\}$. □

Remark 3.37. In fact, the same argument also shows that the finite group $G = \mathbb{Z}/2\mathbb{Z} \ltimes (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$ $(m, n \in \mathbb{Z})$ cannot admit an unmixed ramification structure (T_1, T_2), where T_1 has type $(2,2,2,2)$.

Indeed, $G \setminus A$ contains at most four conjugacy classes, more precisely, it contains one conjugacy class if both m, n are odd, two conjugacy classes if one of m, n is odd and the other is even, and four if both m, n are even.

Since any spherical system of generators of G must contain an element of $G \setminus A$, the condition that $\Sigma_1 \cap \Sigma_2 = \{1\}$ immediately implies that m, n cannot both be odd.

If m is even and n is odd, then the above argument shows that the image in $(\mathbb{Z}/2\mathbb{Z})^2$ of any spherical system of generators contains at least two of $(1,1),(1,0),(0,1)$, and hence one can find $x \in T_1$ and $y \in T_2$ such that either $x, y \in G \setminus A$ are conjugate, or $x, y \in A$ and $x^{mn/2} = y^{mn/2}$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{1\}$.

If m is even and n is even, then the elements of order two in G are exactly $tr^i s^j$ $(1 \le i \le m,\ 1 \le j \le n)$, $u = r^{m/2}$, $v = s^{n/2}$ and $w = r^{m/2}s^{n/2}$. The above argument shows that T_1 either contains four elements from four different conjugacy classes of $G \setminus A$, or two elements from two different conjugacy classes of $G \setminus A$ and two different elements of $\{u, v, w\}$. Since T_2 is also a spherical system of generators, then one can find $x \in T_1$ and $y \in T_2$ such that either $x, y \in G \setminus A$ are conjugate, or $y^i = x \in \{u, v, w\}$, a contradiction to $\Sigma_1 \cap \Sigma_2 = \{1\}$.

References

[BHPV] W.P. Barth, K. Hulek, C.A.M. Peters, A. Van de Ven, *Compact complex surfaces.* Second edition. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], **4**. Springer-Verlag, Berlin, 2004.

[BC] I. Bauer, F. Catanese, *Some new surfaces with* $p_g = q = 0$. Proceeding of the Fano Conference. Torino (2002), 123–142.

[BCG05] I. Bauer, F. Catanese, F. Grunewald, *Beauville surfaces without real structures.* In: Geometric methods in algebra and number theory, Progr. Math., vol **235**, Birkhäuser Boston, (2005), 1–42.

[BCG06] I. Bauer, F. Catanese, F. Grunewald, *Chebycheff and Belyi polynomials, dessins d'enfants, Beauville surfaces and group theory.* Mediterr. J. Math. **3, no.2**, (2006), 121–146.

[BCG08] I. Bauer, F. Catanese, F. Grunewald, *The classification of surfaces with* $p_g = q = 0$ *isogenous to a product.* Pure Appl. Math. Q., **4**, no. 2, part1, (2008), 547–586.

[B] A. Beauville, *Surfaces Algébriques Complex.* Astérisque **54**, Paris (1978).

[Br] T. Breuer, *Characters and Automorphism Group of Compact Riemann Surfaces.* London Math. Soc., Lecture Notes Series **280**. Cambridge University Press, (2000).

[CP] G. Carnovale, F. Polizzi, *The classification of surfaces with* $p_g = q = 1$ *isogenous to a product of curves*, Adv. Geom. **9** (2009), 233–256.

[Cat84] F. Catanese, *On the moduli spaces of surfaces of general type.* J. Diff. Geo. **19**, (1984), 483–515.

[Cat92] F. Catanese, *Chow varieties, Hilbert schemes and moduli spaces of surfaces of general type.* J. Algebraic Geom. **1** (1992), no. 4, 561–595

[Cat00] F. Catanese, *Fibred surfaces, varieties isogenous to a product and related moduli spaces.* Amer. J. Math. **122**, (2000), 1–44.

[Co80] M.D.E. Conder, *Generators for alternating and symmetric groups*, J. London Math. Soc. **22** (1980) 75–86.

[Co90] M.D.E. Conder, *Hurwitz groups: a brief survey*, Bull. Amer. Math. Soc. **23** (1990) 359-370.

[Di] L. E. Dickson. *Linear groups with an exposition of the Galois field theory* (Teubner, 1901).

[Ev] B. Everitt, *Alternating quotients of Fuchsian groups*, J. Algebra **223** (2000) 457–476.

[FG] Y. Fuertes, G. González-Diez, *On Beauville structures on the groups* S_n *and* A_n, preprint.

[FGJ] Y. Fuertes, G. González-Diez, A. Jaikin-Zapirain, *On Beauville surfaces*, preprint.

[FJ] Y. Fuertes, G. Jones, *Beauville surfaces and finite groups*, preprint availiable at arXiv:0910.5489.

[G] D. Gieseker, *Global moduli for surfaces of general type.* Invent. Math **43** no. 3, (1977), 233–282.

[Go] D. Gorenstein, *Finite groups*, Chelsea Publishing Co., New York, 1980.

[HP] C. Hacon, R. Pardini, *Surfaces with* $p_g = q = 3$. Trans. Amer. Math. Soc. **354**, (2002), 2631-2638.

[LS04] M.W. Liebeck, A. Shalev, *Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks.* J. Algebra **276** (2004) 552–601.

[LS05] M.W. Liebeck, A. Shalev, *Fuchsian groups, finite simple groups and representation varieties.* Invent. Math. **159** (2005), no. 2, 317–367.

[Ma] A. M. Macbeath, *Generators of the linear fractional groups*, Number Theory (Proc. Sympos. Pure Math., Vol. XII, Houston, Tex., 1967), Amer. Math. Soc., Providence, R.I. (1969) 14–32.

[Man] M. Manetti, *Iterated double covers and connected components of moduli spaces.* Topology **36**, (1997), 745–764.

[Mar09] C. Marion, *Triangle groups and* $\mathrm{PSL}_2(q)$, J. Group Theory **12** (2009), 689-708

[Mar3.09] C. Marion, *Triangle generation of finite exceptional groups of low rank*, preprint.

[Mar9.09] C. Marion, *Random and deterministic triangle generation of three-dimentional classical groups I*, preprint.

[P] M. Penegini, *The classification of isotrivial fibred surfaces vith* $p_g = q = 2$. With an appendix of S. Rollenske, preprint availiable at arXiv:0904.1352.

[Pi] G.P. Pirola, *Surfaces with* $p_g = q = 3$. Manuscripta Math. **108** no. 2, (2002), 163–170.

[Po] F. Polizzi, *On surfaces of general type with* $p_g = q = 1$ *isogenous to a product of curves.* Comm. Algebra **36** no. 6, (2008), 2023–2053.

[S] F. Serrano, *Isotrivial fibred surfaces.* Annali di Matematica. pura e applicata, Vol. **CLXXI**, (1996), 63–81.

[Su] M. Suzuki, *Group Theory I*, Springer-Verlag, Berlin, 1982.

[Z] F. Zucconi, *Surfaces with* $p_g = q = 2$ *and an irrational pencil.* Canad. J. Math. Vol. **55**, (2003), 649–672.

Shelly Garion, Max-Planck-Institute for Mathematics, D-53111 Bonn, Germany
E-mail address: shellyg@mpim-bonn.mpg.de

Matteo Penegini, Lehrstuhl Mathematik VIII, Universität Bayreuth, NWII, D-95440 Bayreuth, Germany
E-mail address: matteo.penegini@uni-bayreuth.de