Math. J. Okayama Univ. **66** (2024), 1–30

EQUIVALENCE CLASSES OF DESSINS D'ENFANTS WITH TWO VERTICES

Madoka Horie

Abstract. Let N be a positive integer. For any positive integer $L \leq N$ and any positive divisor r of N, we enumerate the equivalence classes of dessins d'enfants with N edges, L faces and two vertices whose representatives have automorphism groups of order r. Further, for any non-negative integer h, we enumerate the equivalence classes of dessins with N edges, h faces of degree 2 with $h \leq N$, and two vertices whose representatives have automorphism group of order r. Our arguments are essentially based upon a natural one-to-one correspondence between the equivalence classes of all dessins with N edges and the equivalence classes of all pairs of permutations whose entries generate a transitive subgroup of the symmetric group of degree N.

1. Introduction

In [8], Grothendieck found an amazing relationship among finite coverings of the projective line which are unramified outside the points 0, 1 and ∞. From his point of view, such coverings can be understood by the corresponding dessins in terms of combinatorial or topological ways (see [24]). In this light, the enumeration of several kinds of dessins has been studied in many articles (cf. [4], [14]). In this paper, we aim to explicitly give some elementary formulas for the numbers of all equivalence classes of dessins d'enfants with two vertices with some prescribed structures. For dessins and their equivalence, we refer Girondo and González [7, Definition 4. 1].

Throughout this paper, we fix positive integers N, L and h with $h \leq L \leq N$. Let $(X, \beta^{-1}([0,1]))$ denote a dessin on a compact Riemann surface X with a Belyi function $\beta : X \longrightarrow \widehat{\mathbb{C}}$. We define an isomorphism f from a dessin $D = (X, \beta^{-1}([0,1]))$ to another dessin $D' = (X', \beta'^{-1}([0,1]))$ to be an orientation preserving homeomorphism such that $\beta' \circ f = \beta$ and it preserves the colors of vertices. If $D = D'$ as Riemann surfaces, we call f an automorphism of D. For a dessin D with N edges, we define a passport of D by $\mathrm{passport}(D) := [\lambda_0, \lambda_1, \lambda_\infty]$ with $\lambda_0, \lambda_1,$ and λ_∞ which are partitions of N (write $\lambda \vdash N$) satisfying λ_0 is the sequence of orders of all white points (multiplicities of β at all points of $\beta^{-1}(0)$), λ_1 is the sequence of orders of all black points (multiplicities of β at all points of $\beta^{-1}(1)$) and λ_∞ is the

Mathematics Subject Classification. Primary 14H57; Secondary 05A15, 20B30.

Key words and phrases. dessin d'enfants, symmetric group, combinatorics, Riemann surface.

sequence of multiplicities of β at all points of $\beta^{-1}(\infty)$. Note that the order of each face of a dessin is double of the multiplicity of β at the point in $\beta^{-1}(\infty)$ corresponding to the face.

Let $\mathfrak{D}(N)$ be the set of all equivalence classes of dessins with N edges. As a fact, for a given dessin with N edges and two vertices, its automorphism group (which is automatically isomorphic to a cyclic group) is of order N if and only if the dessin is regular, that is, the natural action of its automorphism group on its edges is transitive (for counting the equivalence classes of regular dessins with a prescribed automorphism group, see Jones [9, Section 3]). We define

$$\mathcal{D}_{\lambda,r} := \{D \in \mathfrak{D}(N) \mid \text{passport}(D) = [(N),(N),\lambda], |\text{Aut}(D)| = r\},$$

where $\lambda \vdash N$. Let $\mathbb{N}$ be the set of all positive integers. For each $m \in \mathbb{N}$, let D_m denote the set of all positive divisors of m and for each $r \in D_N$, let $D^*_{N,h,r} = \{n \in D_r \mid \ N/n \in D_h\}$. Now we introduce our main results.

Theorem 1.1. *For each $r \in D_N$, let $\mathfrak{D}_1(N,L,r)$ denote the set of all equivalence classes of dessins with N edges, L faces and two vertices whose representatives have automorphism group of order r. Then,*

$$|\mathfrak{D}_1(N,L,r)| = \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} |\mathcal{D}_{\lambda,r}| = \frac{r}{N}\sum_{n\in D_{N/r}} \mu\left(\frac{N}{nr}\right)\Psi_{N,L,n},$$

where μ denotes the Möbius function and $l(\lambda)$ is the number of parts of λ. The symbol $\Psi_{N,L,n}$ is defined in Section 2.1 (see the equation (2.1)).

Theorem 1.2. *For any $r \in D_N$, let $\mathfrak{D}_2(N,h,r)$ denote the set of all equivalence classes of dessins with N edges, h faces of degree 2 and two vertices whose representatives have the automorphism group of order r. Then, it holds*

$$|\mathfrak{D}_2(N,h,r)| = \sum_{\substack{\lambda\vdash N\\ m_1(\lambda)=h}} |\mathcal{D}_{\lambda,r}| = \frac{r}{N}\sum_{n\in D^*_{N,h,N/r}} \mu\left(\frac{N}{nr}\right)\Upsilon_{N,h,n},$$

where $m_1(\lambda)$ is the number of parts of λ which are equal to 1. The symbol $\Upsilon_{N,h,n}$ is defined in Section 2.1 (see the equation (2.4)).

We explain an idea for the computation. Define

$$\mathcal{D}'_{\lambda,r} := \{D \in \mathfrak{D}(N) \mid \text{passport}(D) = [(N),(N),\lambda], |\text{Aut}(D)| \in D_r\}.$$

It follows from $\mid \mathcal{D}'_{\lambda,r} \mid = \sum_{d|r} \mid \mathcal{D}_{\lambda,d} \mid$ and Möbius inversion formula, that

$$\mid \mathcal{D}_{\lambda,r} \mid = \sum_{d|r} \mu\left(\frac{r}{d}\right) \mid \mathcal{D}'_{\lambda,d} \mid .$$

From this, instead of studying $\mathcal{D}_{\lambda,r}$, we focus on $\mathcal{D}'_{\lambda,r}$ and get the formulas of main theorems based on the analysis of N-cycles belonging to the centralizer $C_{S_N}(\sigma_0^n)$ of σ_0^n in S_N, where $\sigma_0 = (1\ 2\ \ldots N) \in S_N$ and $n \in D_N$. This is a main idea of this article.

Remark 1. The set of all equivalence classes of dessins with N edges, L faces and two vertices is given by

$$\bigsqcup_{\lambda}\bigsqcup_{r}\mathcal{D}_{\lambda,r}.$$

Thus, its number is $\sum_{r\in D_N}|\mathfrak{D}_1(N,L,r)|$. Similarly, the number of all equivalence classes of dessins with N edges, h faces of degree 2 and two vertices is given by $\sum_{r\in D_N}|\mathfrak{D}_2(N,h,r)|$.

Example 1. We consider the case when N is an odd prime and $r = N$. For each positive integer t less than $N-1$, let X_t be the compact Riemann surface associate to the curve $x(x-1)^t = y^N$ and β_t be the Belyi function from X to $\widehat{\mathbb{C}}$: $\beta_t(x,y) = x$. Then the dessin $(X_t, \beta_t^{-1}([0,1]))$ has N edges, one face and two vertices whose automorphism group is cyclic to order r. By Theorem 1.1, $|\mathfrak{D}_1(N,1,N)| = N-2$. In fact, $N-2$ dessins $(X_t, \beta_t^{-1}([0,1]))$ exhaust all dessins in the question.

We define the genus of a dessin $(X, \mathcal{D})$ by the genus of the Riemann surface X. It follows that the genera of two dessins are equal if the dessins are equivalent.

Remark 2. As the Riemann-Hurwitz formula shows, the genus of a dessin with N edges, L faces and two vertices is $\frac{1}{2}(N-L)$ (cf. [7, Proposition 4.10]). Let N, L and r satisfy the same condition in Theorem 1.1. Then, $|\mathfrak{D}_1(N,L,r)|$ is, for each $r \in D_{2g+L}$, the number of equivalence classes of dessins of genus g with L faces and two vertices whose automorphism groups are of order r. Since $\frac{1}{2}(N-L)$ is an integer, in the case $L \not\equiv N \pmod 2$, obviously, $|\mathfrak{D}_1(N,L,r)| = 0$.

Remark 3. We consider immediate consequences of Theorem 1.2. If $h = N$, we get $|\mathfrak{D}_2(N,N,N)| = 1$ and $|\mathfrak{D}_2(N,N,r)| = 0$ for $r \neq N$. It corresponds to the fact that there exist only one equivalent class of permutation representation pair (defined in Section 2) satisfying Theorem 1.2. Those representative is given by $(\sigma_0, \sigma_0^{N-1})$ for $\sigma_0 = (1 \cdots N) \in S_N$. If a dessin of degree N have $N-1$ faces of degree 2, there exists Nth face of degree 2. Namely, $|\mathfrak{D}_2(N,N-1,r)| = 0$ for all $r \in D_N$. Moreover, if we consider for a permutation representation pair (σ_0, τ) such that $\tau\sigma_0$ fixes just $N-2$ numbers and have one transposition $(a\ b)$. In the cycle decomposition of τ, a and b are belong to different cycles. Since τ is not N-cycle, $|\mathfrak{D}_2(N,N-2,r)| = 0$ for all $r \in D_N$

Example 2. Using Mathematica 12 ([22]), we give tables for the formulas of $|\mathfrak{D}_1(N, L, r)|$ in Theorem 1.1 (Table 1) and $|\mathfrak{D}_2(N, h, r)|$ in Theorem 1.2 (Table 2). The program file is available at the author's homepage (https://sites.google.com/view/horiemathfile). Because of Remark 2 and Remark 3, we excluded the cases $L \not\equiv N \pmod 2$ for $|\mathfrak{D}_1(N, L, r)|$ and the cases $N \geq h \geq N-2$ for $|\mathfrak{D}_2(N, h, r)|$ from Table 1 and Table 2 respectively.

Table 1. Examples of Theorem 1.1

N	L	r	$\lvert\mathfrak{D}_1\rvert$	N	L	r	$\lvert\mathfrak{D}_1\rvert$	N	L	r	$\lvert\mathfrak{D}_1\rvert$
2	2	1	0	6	2	1	13	7	7	1	0
	2	2	1		2	2	1		7	7	1
3	1	1	0		2	3	1	8	2	1	378
	1	3	1		2	6	1		2	2	4
	3	1	0		4	1	5		2	4	1
	3	3	1		4	2	1		2	8	2
4	2	1	1		4	3	1		4	1	231
	2	2	0		4	6	0		4	2	0
	2	4	1		6	1	0		4	4	0
	4	1	0		6	2	0		4	8	1
	4	2	0		6	3	0		6	1	15
	4	4	1		6	6	1		6	2	1
5	1	1	1	7	1	1	25		6	4	1
	1	5	3		1	7	35		6	8	0
	3	1	3		3	1	67		8	1	0
	3	5	0		3	7	0		8	2	0
	5	1	0		5	1	10		8	4	0
	5	5	1		5	7	0		8	8	1

Example 3. For example, the case $N = 8$ and $h = 4$, $\sum_{r \in D_8} |\mathfrak{D}_2(8, 4, r)| = 10$. This is the number of all inequivalent dessins with 8 edges, 4 faces of degree 2 and two vertices. The permutation representation pairs corresponding to the 10 dessins are given by

$$(\sigma_0, (1\ 8\ 7\ 6\ 5\ 2\ 3\ 4)), (\sigma_0, (1\ 8\ 7\ 6\ 2\ 3\ 5\ 4)), (\sigma_0, (1\ 8\ 7\ 2\ 3\ 6\ 5\ 4)),$$
$$(\sigma_0, (1\ 8\ 2\ 3\ 7\ 6\ 5\ 4)), (\sigma_0, (1\ 8\ 7\ 6\ 2\ 4\ 3\ 5)), (\sigma_0, (1\ 8\ 7\ 2\ 5\ 4\ 3\ 6)),$$
$$(\sigma_0, (1\ 8\ 7\ 2\ 4\ 3\ 6\ 5)), (\sigma_0, (1\ 8\ 2\ 4\ 3\ 7\ 6\ 5)), (\sigma_0, (1\ 8\ 2\ 5\ 4\ 3\ 7\ 6)),$$
$$\text{and } (\sigma_0, (1\ 8\ 3\ 2\ 5\ 4\ 7\ 6)),$$

where $\sigma_0 = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)$. The above 10 dessins correspond to the data for degree 8 with *abc* triple $[a, b, c] = [8, 8, 2]$ in the notation of [12].

Table 2. Examples of Theorem 1.2

N	h	r	$\lvert\mathfrak{D}_2\rvert$
3	0	1	0
	0	3	1
4	0	1	0
	0	2	0
	0	4	1
	1	1	1
	1	2	0
	1	4	0
5	0	1	1
	0	5	3
	1	1	1
	1	5	0
	2	1	2
	2	5	0
6	0	1	5
	0	2	1

N	h	r	$\lvert\mathfrak{D}_2\rvert$
6	0	3	1
	0	6	1
	1	1	8
	1	2	0
	1	3	0
	1	6	0
	2	1	2
	2	2	1
	2	3	0
	2	6	0
	3	1	3
	3	2	0
	3	3	1
	3	6	0
7	0	1	32
	0	7	5

N	h	r	$\lvert\mathfrak{D}_2\rvert$
7	1	1	36
	1	7	0
	2	1	24
	2	7	0
	3	1	5
	3	7	0
	4	1	5
	4	7	0
8	0	1	200
	0	2	5
	0	4	1
	0	8	3
	1	1	229
	1	2	0
	1	4	0
	1	8	0

N	h	r	$\lvert\mathfrak{D}_2\rvert$
8	2	1	124
	2	2	4
	2	4	0
	2	8	0
	3	1	56
	3	2	0
	3	4	0
	3	8	0
	4	1	8
	4	2	1
	4	4	1
	4	8	0
	5	1	7
	5	2	0
	5	4	0
	5	8	0

Remark 4. As a classical enumeration problem for coverings of Riemann surfaces, Hurwitz enumeration problem has been studied ([13], [16]) and especially, Mednykh gave a general formula ([16, Theorem 2.1]). Mednykh made use of the ramification type that is the matrix based on the numbers of ramified points of same order in the inverse image of each of every element of the ramification set. A Belyi function is a covering of $\widehat{\mathbb{C}}$ which is ramified at most three points. Our condition is more restrictive than Mednykh's one. In particular, we assumed that two of the three points are totally ramified and sum up all patterns of orders of third ramification point.

Remark 5. From the result of [15], the number of all equivalence classes of dessins with N edges and two vertices is the Stegall number ([20]):

$$\sum_{L=1}^{N} \sum_{r|N} \mathfrak{D}_1(N, L, r) = \frac{1}{N^2} \sum_{d|N} \varphi\left(\frac{N}{d}\right)^2 \left(\frac{N}{d}\right)^d d!.$$

We organize this paper as follows. In Section 2, we define symbols and recall some basic facts. In Section 3, we prepare some lemmas to prove main theorems. The proofs of Theorem 1 is given in Section 4. The proof of Theorem 2 is given in Section 5. Finally, we discuss some examples of our dessins in Section 6.

2. Notation and Basic facts

2.1. **Setting up Symbols.** First, we define the symbols $\varPsi_{N,L,n}$ and $\varUpsilon_{N,h,n}$ in Theorem 1.1 and Theorem 1.2. Let P_m denote the set of all prime divisors of a positive integer m. For each $n \in D_N$, we define

$$\varLambda^{(n)} = \varLambda^{(n)}(N, L) = \left\{ \lambda = (l_1, \dots, l_\nu) \;\middle|\; \begin{array}{l} \nu \in \mathbb{N}, l_1, \dots, l_\nu \in D_{N/n}, \\ l_1 \geq \cdots \geq l_\nu, \\ l_1 + \cdots + l_\nu = L \end{array} \right\}.$$

For each $\lambda = (l_1, \dots, l_\nu) \in \varLambda^{(n)}$ and $p \in P_{N/n}$, let $i_0(n, \lambda, p)$ denote the number of positive integers $j \leq \nu$ with $\gcd(l_j, p) = 1$, and $i(n, \lambda, p)$ the number of positive integers $j \leq \nu$ with $pl_j \mid N/n$, i.e., $pl_j \in D_{N/n}$. Obviously, $i_0(n, \lambda, p) \leq i(n, \lambda, p)$. We then define

$$A_{n,\lambda,p} = \left(1 - \frac{1}{p}\right)^{i(n,\lambda,p) - i_0(n,\lambda,p)} \left\{ \left(1 - \frac{1}{p}\right)^{i_0(n,\lambda,p)+1} - \left(-\frac{1}{p}\right)^{i_0(n,\lambda,p)+1} \right\}.$$

Note that if $i(n, \lambda, p) = 0$, $A_{n,\lambda,p} = 1$. We also define

$$\varDelta_\lambda = \prod_{j=1}^{\nu} l_j, \quad B_\lambda = \frac{\nu!}{\nu_1! \nu_2! \dots \nu_L! \, \varDelta_\lambda},$$

where for each positive integer $k \leq L$, ν_k is the number of all positive integers $j \leq \nu$ with $l_j = k$. For each positive integer $m \leq n$, we denote by $\varLambda_m^{(n)}$ the subset of $\varLambda^{(n)}$ consisting of all $\lambda = (l_1, \dots, l_\nu)$ with $\nu = m$. Using the elementary symmetric polynomial $\mathfrak{s}_m(\xi_1, \dots, \xi_n)$ of degree m in n variables $\xi_1, \dots, \xi_n$, we define

$$f_m^{(n)} = (1 - (-1)^m) \mathfrak{s}_m(1, 2, \dots, n) = \begin{cases} 2\mathfrak{s}_m(1, 2, \dots, n) & \text{if } 2 \nmid m, \\ 0 & \text{if } 2 \mid m. \end{cases}$$

For each $r \in D_N$ and $n \in D_{N/r}$, we define

$$\varPsi_{N,L,n} = \frac{N^n}{n^{n+1}(n+1)} \sum_{m=1}^{\min(n,L)} f_{n-m+1}^{(n)} \sum_{\lambda \in \varLambda_m^{(n)}} B_\lambda \prod_{p \in P_{N/n}} A_{n,\lambda,p}. \tag{2.1}$$

Next, for each $(j, n) \in \mathbb{N} \times \mathbb{N}$ with $j \leq n$, we put

$$\varSigma_j^{(n)} = \frac{n!}{(j-1)!} \left\{ \sum_{m=0}^{n-j-1} \frac{(-1)^m}{m! \, (j+m)(n-j-m)} \right\} + (-1)^{n-j} \binom{n-1}{j-1} - 1, \tag{2.2}$$

so that $\varSigma_n^{(n)} = 0$. We also put

$$\varSigma_0^{(n)} = (n-1)! - 1. \tag{2.3}$$

Note that $\varSigma_{n-1}^{(n)} = 0$ and $\varSigma_{n-2}^{(n)} = 0$ if $n \geq 2$. We define

(2.4)

$$\varUpsilon_{N,h,n} = \left\{ \sum_{m=hn/N}^{n-1} \binom{m}{hn/N} \frac{\varphi(N/n)N^{n-m-1}}{n^{n-m-1}} \left(\frac{N}{n}-1\right)^{m-hn/N} \left(\varSigma_m^{(n)} - \varSigma_{m+1}^{(n)}\right) \right\} + \binom{n}{hn/N} \left\{ \frac{\varphi(N/n)n}{N} \left(\left(\frac{N}{n}-1\right)^{n-hn/N} - (-1)^{n-hn/N} \right) + (-1)^{n-hn/N} \right\},$$

where φ stands for the Euler's totient function and we make a convention that $0^0 = 1$.

2.2. **Permutation Representation Pairs.** When two dessins are equivalent each other, they have the same numbers of vertices, edges and faces. Furthermore, for any integer $m > 0$, equivalent dessins have the same number of faces with degree $2m$. We define the degree of each face of a dessin as the number of edges of the dessin incident to the face (cf. Lando and Zvonkin [11, Definition 1.3.8]).

Let N be a fixed positive integer, and let S_N denote the symmetric group of degree N. A pair (σ, τ) in $S_N \times S_N$ of which σ and τ generate a transitive subgroup of S_N is called a permutation representation pair. Let $\mathcal{P}(N)$ denote the set of all permutation representation pairs. We say a permutation representation pair (σ, τ) is equivalent to a permutation representation pair (σ', τ'), if $(\sigma, \tau) = (\rho\sigma'\rho^{-1}, \rho\tau'\rho^{-1})$ for some $\rho \in S_N$. We denote by $\mathfrak{P}(N)$ the set of all equivalence classes of elements in $\mathcal{P}(N)$, and by $\mathfrak{D}(N)$ the set of equivalence classes of dessins with N edges. We introduce known facts for understanding equivalence classes of dessins as follows.

Proposition. *There is a one to one correspondence between $\mathfrak{D}(N)$ and $\mathfrak{P}(N)$ such that if $\mathfrak{c} \in \mathfrak{D}(N)$ corresponds to $(\sigma, \tau) \in \mathfrak{P}(N)$, then for any $m \in \mathbb{N}$,*

(i) *the number of white vertices of degree m in each dessin $\mathfrak{c}$ is equal to the number of m-cycles in the cycle decomposition of σ;*
(ii) *the number of black vertices of degree m in each dessin $\mathfrak{c}$ is equal to the number of m-cycles in the cycle decomposition of τ;*
(iii) *the number of faces of degree $2m$ in each dessin $\mathfrak{c}$ is equal to the number of m-cycles in the cycle decomposition of $\tau\sigma$;*
(iv) *the group* $\mathrm{Aut}(\mathfrak{c})$ *is isomorphic to the group*

$$C_{S_N}(\langle \sigma_0, \tau \rangle) := \{\sigma \in S_N \mid \sigma\tau' = \tau'\sigma \text{ for all } \tau' \in \langle \sigma_0, \tau \rangle\}.$$

In particular, the numbers of white vertices, black vertices and faces of the dessin $\mathfrak{c}$ are equal to the numbers of cycles in the cycle decompositions of σ, τ and $\tau\sigma$ respectively.

For the details of the proof of Proposition, see [7, Chapter 4] and [11, Chapters 1, 2].

Put

$$\sigma_0 = (1\ 2\ \ldots\ N) \in S_N.$$

By Proposition, the permutation representation pair of the dessin with N edges and two vertices is (σ_0, τ), where τ is an N-cycle. Since $C_{S_N}(\langle \sigma_0, \tau \rangle) \subset C_{S_N}(\sigma_0) = \langle \sigma_0 \rangle$, the automorphism group of any dessin with N edges and two vertices is a cyclic group of order dividing N. Take any positive divisor r of N. We shall give explicit expressions for statements of Theorem 1.1 and Theorem 1.2.

3. Key Lemmas

In this section, we introduce several preliminary results. Let $\mathcal{C}_N$ be the set of all N-cycles in S_N. For $\sigma, \tau \in S_N$, we define by passport(σ,τ) the passport of the dessin corresponding to the permutation representation pair (σ, τ). We define $\mathcal{C}_{\lambda,r}$, $\widetilde{\mathcal{C}}_{\lambda,r}$ and $\widetilde{\mathcal{C}}'_{\lambda,r}$ as follows.

$$\mathcal{C}_{\lambda,r} := \{\tau \in \mathcal{C}_N \mid \text{passport}(\sigma_0, \tau) = [(N), (N), \lambda], |C_{S_N}(\langle \sigma_0, \tau \rangle)| = r\},$$

$$\widetilde{\mathcal{C}}_{\lambda,r} := \{\tau \in \mathcal{C}_N \mid \text{passport}(\sigma_0, \tau) = [(N), (N), \lambda], [\langle \sigma_0 \rangle : C_{S_N}(\langle \sigma_0, \tau \rangle)] = r\}.$$

$$\widetilde{\mathcal{C}}'_{\lambda,r} := \{\tau \in \mathcal{C}_N \mid \text{passport}(\sigma_0, \tau) = [(N), (N), \lambda], [\langle \sigma_0 \rangle : C_{S_N}(\langle \sigma_0, \tau \rangle)] \in D_r\}.$$

The following lemma is a key of this article. In fact, the claims of Theorem 1.1 and Theorem 1.2 immediately follow from this lemma.

Lemma 3.1. *We have the following identities:*

(i) $\mid \mathcal{C}_{\lambda,r} \mid = \dfrac{N}{r} \mid \mathcal{D}_{\lambda,r} \mid$

(ii) $\mid \mathcal{C}_{\lambda,r} \mid = \mid \widetilde{\mathcal{C}}_{\lambda,\frac{N}{r}} \mid$

(iii) $\mid \widetilde{\mathcal{C}}_{\lambda,r} \mid = \displaystyle\sum_{n|r} \mu\left(\frac{r}{n}\right) \mid \widetilde{\mathcal{C}}'_{\lambda,n} \mid .$

(iv) $\displaystyle\sum_{\substack{\lambda \vdash N \\ l(\lambda)=L}} \mid \widetilde{\mathcal{C}}'_{\lambda,r} \mid = \Psi_{N,L,n}.$

(v) $\displaystyle\sum_{\substack{\lambda \vdash N \\ m_1(\lambda)=h}} \mid \widetilde{\mathcal{C}}'_{\lambda,r} \mid = \Upsilon_{N,h,n}.$

Proof. Here we prove only (i), (ii) and (iii). (iv) and (v) will be handled in Section 4 and Section 5. Let $D \in \mathcal{D}_{\lambda,r}$. We can take some $\tau \in \mathcal{C}_{\lambda,r}$ corresponding to D under the identification between $\mathfrak{D}(N)$ and $\mathfrak{P}(N)$. Since $\mid \text{Aut}(D) \mid = \mid C_{S_N}(\langle \sigma_0, \tau \rangle) \mid = r$, we get

$$\text{Aut}(D) \simeq C_{S_N}(\langle \sigma_0, \tau \rangle) \simeq \langle \sigma_0 \rangle / \langle \sigma_0^r \rangle.$$

Therefore, N/r elements in $\mathcal{C}_{\lambda,r}$ corresponds to D and it yiels (i) So in $\mathcal{C}_{\lambda,r}$, each of all elements have N/r equivalent elements including itself. For (ii), since $\mid \langle\sigma_0\rangle \mid= N$ and $\mid C_{S_N}(\langle\sigma_0,\tau\rangle) \mid= r$, we get $[\langle\sigma_0\rangle : C_{S_N}(\langle\sigma_0,\tau\rangle)] = \frac{N}{r}$ For (iii), we have only to apply the Möbius inversion formula to $\mid \widetilde{\mathcal{C}}'_{\lambda,r} \mid= \sum_{d|r} \mid \widetilde{\mathcal{C}}_{\lambda,d} \mid$. □

If Lemma 3.1 is proved, the proofs of Theorem 1.1 and 1.2 are immediately completed. *Proof of Theorem 1.1 and Theorem 1.2.* From Lemma 3.1-(i), (ii), (iii) and (iv), we get Theorem 1.1 as follows.

$$D_1(N,L,r) = \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} \mid \mathcal{D}_{\lambda,r} \mid= \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} \frac{r}{N} \mid \mathcal{C}_{\lambda,r} \mid= \frac{r}{N} \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} \mid \widetilde{\mathcal{C}}_{\lambda,\frac{N}{r}} \mid$$

$$= \frac{r}{N} \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} \sum_{n\in D_{N/r}} \mu\left(\frac{N}{nr}\right) \mid \widetilde{\mathcal{C}}'_{\lambda,n} \mid= \frac{r}{N} \sum_{n\in D_{N/r}} \mu\left(\frac{N}{nr}\right) \sum_{\substack{\lambda\vdash N\\ l(\lambda)=L}} \mid \widetilde{\mathcal{C}}'_{\lambda,n} \mid$$

$$= \frac{r}{N} \sum_{n\in D_{N/r}} \mu\left(\frac{N}{nr}\right) \Psi_{N,L,n}.$$

Theorem 1.2 is similarly proved by using Lemma 3.1-(i),(ii),(iii) and (v). □

Before proving Lemma 3.1-(iv) and (v), we prepare some lemmas about cycles in S_N. Take $n \in D_N$. Let $E(N/n)$ denote the set of non-negative integers less than N/n, and $E(N/n)^\times$ the set of integers in $E(N/n)$ relatively prime to N/n. We note that $E(N/n)^\times \subset \mathbb{N}$ or $E(N/n)^\times = \{0\}$ according to whether $n < N$ or $n = N$. Given $m, u \in \mathbb{N}$ and m integers $a_1, \ldots, a_m$, we say that $a_1, \ldots, a_m$ are distinct modulo u when the residue classes of $a_1, \ldots, a_m$ modulo u are distinct.

Lemma 3.2. *Let $n \in D_N$. For an N-cycle τ in $C_{S_N}(\sigma_0^n)$ and a positive integer $a \leq N$, the n integers $\tau^0(a) = a, \ldots, \tau^{n-1}(a)$ are distinct modulo n, and $\tau^n(a) \equiv a + bn \pmod N$ with a unique $b \in E(N/n)^\times$.*

Proof. Note that an integer j satisfying $\tau^j(a) = a$ is divisible by N. If $\tau^k(a) = \tau^{k'}(a)+b'n$ with integers k, k' and b', then since $\tau^k(a) = \sigma_0^{b'n}\tau^{k'}(a) = \tau^{k'}\sigma_0^{b'n}(a)$, we obtain $\tau^{(k-k')N/n}(a) = \sigma_0^{b'nN/n}(a) = a$, so that $k \equiv k' \pmod n$. It therefore follows that $\tau^0(a), \ldots, \tau^{n-1}(a)$ are distinct modulo n and so are $\tau(a), \ldots, \tau^n(a)$. Hence we have $\tau^n(a) \equiv \tau^0(a) \pmod n$, i.e., $\tau^n(a) \equiv a + bn \pmod N$ with a unique $b \in E(N/n)$. As the latter congruence means $\tau^n(a) \equiv \sigma_0^{nb}(a) \pmod N$, we see that

$$\tau^{N/\gcd(b,N/n)}(a) = \tau^{n(N/n)/\gcd(b,N/n)}(a) = \sigma_0^{Nb/\gcd(b,N/n)}(a) = a.$$

Therefore b is relatively prime to N/n. □

Lemma 3.3. *Let $n \in D_N$ and $m \in \mathbb{N}$ with $m \leq n$. For each integer $b \in E(N/n)$, put $d_0 = \gcd(b, N/n)$ and $N_0 = mN/(d_0 n)$. Take m integers $1 < \alpha_1 < \cdots < \alpha_m < N$ which are distinct from each other modulo n. Then*

(i) *there exists a unique N_0-cycle ρ in $C_{S_N}(\sigma_0^{d_0 n})$ such that, for all positive integers $j < m$, $\rho(\alpha_j) = \alpha_{j+1}$ or equivalently $\rho^j(\alpha_1) = \alpha_{j+1}$ and that $\rho(\alpha_m)$ $(= \rho^m(\alpha_1)) \equiv \alpha_1 + bn \pmod N$;*

(ii) *the N_0-cycle ρ appears in the cycle decomposition of any permutation τ in $C_{S_N}(\sigma_0^{d_0 n})$ such that $\tau(\alpha_1) = \rho(\alpha_1), \ldots, \tau(\alpha_m) = \rho(\alpha_m)$.*

Proof. When j runs over the non-negative integers less than m, and u does over the non-negative integers less than $N/(d_0 n)$, the N_0 integers $\alpha_{j+1} + bnu$ are distinct from each other modulo N. Therefore, there exists a unique N_0-cycle ρ in S_N such that its N_0-cycle consists of N_0 numbers $\alpha_{j+1} + bnu$. Namely, $\rho^{j+mu}(\alpha_1) \equiv \alpha_{j+1} + bnu \pmod N$, i.e., $\rho^{j+mu}(\alpha_1) \equiv \sigma_0^{bnu}(\alpha_{j+1})$ $\pmod N$. Hence, in the case $j \neq m-1$,

$$\begin{aligned}
\sigma_0^{bn}\rho\left(\rho^{j+mu}(\alpha_1)\right) &= \sigma_0^{bn}\sigma_0^{bnu}(\alpha_{j+2}) \equiv \rho^{j+m(n+1)+1}(\alpha_1) \pmod N,\\
\rho\sigma_0^{bn}\left(\rho^{j+mu}(\alpha_1)\right) &= \rho\sigma_0^{bn}\sigma_0^{bnu}(\alpha_{j+1}) \equiv \rho^{j+m(n+1)+1}(\alpha_1) \pmod N.
\end{aligned}$$

Similarly, when $j = m-1$,

$$\begin{aligned}
\sigma_0^{bn}\rho\left(\rho^{m-1+mu}(\alpha_1)\right) &= \sigma_0^{bn}\sigma_0^{bn(u+1)}(\alpha_1) \equiv \rho^{m+m(u+1)}(\alpha_1) \pmod N,\\
\rho\sigma_0^{bn}\left(\rho^{m-1+mu}(\alpha_1)\right) &= \rho\sigma_0^{bn}\sigma_0^{bnu}(\alpha_m) \equiv \rho^{m+m(u+1)}(\alpha_1) \pmod N.
\end{aligned}$$

It follows from this that $\sigma_0^{bn}\rho$ coincides with $\rho\sigma_0^{bn}$ on $\{\alpha_1, \rho(\alpha_1), \ldots, \rho^{N_0-1}(\alpha_1)\}$. On the other hand, $\rho = (\alpha_1\ \rho(\alpha_1)\ \ldots\ \rho^{N_0-1}(\alpha_1))$ and $\sigma_0^{bn}(\alpha_1) = \rho^m(\alpha_1)$. Hence

$$\begin{aligned}
\sigma_0^{bn}\rho\sigma_0^{-bn} &= \left(\sigma_0^{bn}(\alpha_1)\ \sigma_0^{bn}\rho(\alpha_1)\ \ldots\ \sigma_0^{bn}\rho^{N_0-1}(\alpha_1)\right)\\
&= (\sigma_0^{bn}\left(\alpha_1)\ \rho\sigma_0^{bn}(\alpha_1)\ \ldots\ \rho^{N_0-1}\sigma_0^{bn}(\alpha_1)\right)\\
&= \left(\rho^m(\alpha_1)\ \rho^{m+1}(\alpha_1)\ \ldots\ \rho^{m+N_0-1}(\alpha_1)\right)\\
&= \rho.
\end{aligned}$$

This implies that ρ belongs to $C_{S_N}(\sigma_0^{d_0 n})$, since $d_0 n = \gcd(bn, N)$. Hence we have the first claim.

For (ii), let τ be a permutation in $C_{S_N}(\sigma_0^{d_0 n})$ such that $\tau(\alpha_{j+1}) = \rho(\alpha_{j+1})$ (for $j \in \{0, 1, \ldots, m-1\}$). Then, we have

$$\tau\left(\rho^{j+mu}(\alpha_1)\right) = \tau\sigma_0^{bnu}(\alpha_{j+1}) = \sigma_0^{bnu}\tau(\alpha_{j+1}) = \sigma_0^{bnu}\rho(\alpha_{j+1})$$

$$= \rho\sigma_0^{bnu}(\alpha_{j+1}) = \rho\left(\rho^{j+mu}(\alpha_1)\right),$$

Hence, the N_0-cycle ρ appears in the cycle decomposition of τ. Thus, the second claim is proved. □

We take any n-cycle $\boldsymbol{a} = (a_1\ a_2\ \ldots\ a_n)$ in S_n with $a_1 = 1$. Let

$$\sigma_{0,n} = (1\ 2\ \ldots\ n) \in S_n.$$

Then there exist a positive integer ν, ν positive integers $s_1, \ldots, s_\nu$ and ν injections

$$x_1 : \{1, 2, \ldots, s_1\} \to \{1, 2, \ldots, n\}, \quad \ldots, \quad x_\nu : \{1, 2, \ldots, s_\nu\} \to \{1, 2, \ldots, n\}$$

For a positive integer ν, we write the cycle decomposition of $\boldsymbol{a}\sigma_{0,n}$ in S_n in the following way:
(3.1)

$$(1\ a_2\ \ldots\ a_n)\sigma_{0,n} = \left(a_{x_1(1)}\ a_{x_1(2)}\ \ldots\ a_{x_1(s_1)}\right)\cdots\left(a_{x_\nu(1)}\ a_{x_\nu(2)}\ \ldots\ a_{x_\nu(s_\nu)}\right)$$

where $x_j(1) = \min\{x_j(1), x_j(2), \ldots, x_j(s_j)\}$ for $1 \le j \le \nu$. We may put

$$x_1(1) = 1, \quad \text{i.e.,} \quad a_{x_1(1)} = 1.$$

Take any n-tuple $\boldsymbol{u} = (u_1, u_2, \ldots, u_n) \in E(N/n)^n$ with $u_1 = 0$ and also take any $b \in E(N/n)^\times$. Applying Lemma 3.3 to $m = n$, $d_0 = 1$, $N_0 = N$ and $\alpha_j = a_j + u_j n$ for $1 \le j \le n$, we have an N-cycle $\rho = \rho_{a,\boldsymbol{u},b}$ in $C_{S_N}(\sigma_0^n)$ defined by

$$\begin{aligned}
&\rho(a_1 + u_1 n) = a_2 + u_2 n, \quad \ldots, \quad \rho(a_{n-1} + u_{n-1} n) = a_n + u_n n, \\
&\rho(a_n + u_n n) = a_1 + u_1 n + bn \equiv 1 + bn \pmod{N}.
\end{aligned}$$

Since $\rho(a_n + u_n n) \le N$ and $1 + bn \le N$, the last congruence becomes the equality

$$\rho(a_n + u_n n) = 1 + bn.$$

Note that $\rho = \sigma_0^b$ in the case $n = 1$.

For Lemma 3.4, we prepare some symbols below. For any positive integer $j \le \nu$, put

$$d_j = \gcd\left(\sum_{k=1}^{s_j}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) + b_j,\ \frac{N}{n}\right), \quad N_j = \frac{s_j N}{d_j n},$$

where $b_j = \begin{cases} b & (j = 1) \\ 0 & (j > 1) \end{cases}$ and for each $1 \le h \le s_j, \delta_j^{(k)} = \begin{cases} 1 & (a_{x_j(k)} = n) \\ 0 & (a_{x_j(k)} < n) \end{cases}$.

Further, we make a convention that

$$x_j(s_j + 1) = x_j(1), \quad u_0 = u_n.$$

Applying Lemma 3.3 to $m = s_j$, $b \in E(N/n)^\times$, $d_0 = d_j$, $N_0 = N_j$, $\alpha_1 = a_{x_j(1)}$ and $\alpha_{k'} = a_{x_j(k')} + \sum_{k=1}^{k'-1}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n$ for $1 < k' \leq s_j$, let π_j denote the N_j-cycle in $C_{S_N}(\sigma_0^{d_j n})$ such that

$$\pi_j^{k'}\left(a_{x_j(1)}\right) = a_{x_j(k'+1)} + \sum_{k=1}^{k'}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n$$

and that

$$\pi_j^{s_j}\left(a_{x_j(1)}\right) \equiv a_{x_j(1)} + \sum_{k=1}^{s_j}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n + b_j n \pmod{N}.$$

Lemma 3.4. *All disjoint cycles in the cycle decomposition of $\rho\sigma_0 = \rho_{\boldsymbol{a},\boldsymbol{u},b}\sigma_0$ are given by*

$$\sigma_0^{in}\pi_j\sigma_0^{-in} \quad (0 \leq i \leq d_\nu - 1, 1 \leq j \leq \nu).$$

Proof. Let $j \in \{1, 2, \ldots, \nu\}$. If $k \in \{1, 2, \ldots, s_j\}$, then $\sigma_{0,n} = (1\ 2\ \ldots\ n)$ sends $a_{x_j(k)}$ to $a_{x_j(k)} + 1 - \delta_j^{(k)} n$, $(a_{x_j(1)}\ a_{x_j(2)} \ldots a_{x_j(s_j)})$ sends $a_{x_j(k)}$ to $a_{x_j(k+1)}$. Therefore, by (—refW), $a = (a_1\ a_2\ \ldots\ a_n)$ must send $a_{x_j(k)} + 1 - \delta_j^{(k)} n$ to $a_{x_j(k+1)}$. Applying a^{-1}, we have $a_{x_j(k+1)} = a_{x_j(k)} + 1 - \delta_j^{(k)} n$. Hence,

$$a_{x_j(k)} + 1 = a_{x_j(k+1)-1} + \delta_j^{(k)} n,$$

where we put $a_0 = a_n$ so that

$$a_{x_1(s_1)} + 1 = a_n + \delta_1^{(s_1)} n.$$

For the sake of convenience, we extend the domain of each $\sigma \in S_N$ to $\mathbb{Z}$ by the rule that $\sigma(m) = \sigma(m')$ for every $(m, m') \in \mathbb{Z} \times \{1, 2, \ldots, N\}$ with $m \equiv m'$ (mod N). Then any $a, a' \in \mathbb{Z}$ and any $u \in D_{N/n}$ satisfy $a + a'un \equiv \sigma_0^{a'un}(a)$ (mod N), which yields

$$\tau(a + a'un) \equiv \tau(a) + a'un \pmod{N}$$

for any $\tau \in C_{S_N}(\sigma_0^{un})$, because $\tau(a + a'un) = \tau\sigma_0^{a'un}(a) = \sigma_0^{a'un}\tau(a)$. Obviously $\rho\sigma_0$ belongs to $C_{S_N}(\sigma_0^n)$ and, unless $j = 1$, $\{x_j(1), x_j(2), \ldots, x_j(s_j)\}$ does not contain 1. Therefore, for each $k' \in \{1, 2, \ldots, s_j\}$,

$$\rho\sigma_0\left(a_{x_j(k')} + \sum_{k=1}^{k'-1}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n\right)$$

$$\equiv \rho\left(a_{x_j(k')} + 1\right) + \sum_{k=1}^{k'-1}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n$$

$$\equiv \rho\left(a_{x_j(k'+1)-1}\right) + \delta_j^{(k')} n + \sum_{k=1}^{k'-1}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n \pmod N,$$

whence, by the definition of ρ,

$$\rho\sigma_0\left(a_{x_j(k')} + \sum_{k=1}^{k'-1}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n\right)$$
$$\equiv \begin{cases} a_{x_j(k'+1)} + \sum_{k=1}^{k'}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n \pmod N & \text{if } k' < s_j, \\ a_{x_j(1)} + \sum_{k=1}^{s_j}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n + b_j n \pmod N & \text{if } k' = s_j. \end{cases}$$

Thus

$$(\rho\sigma_0)^{k'}(a_{x_j(1)}) \equiv a_{x_j(k'+1)} + \sum_{k=1}^{k'}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n \pmod N \quad \text{for } k' < s_j,$$

$$(\rho\sigma_0)^{s_j}(a_{x_j(1)}) \equiv a_{x_j(1)} + \sum_{k=1}^{s_j}\left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) n + b_j n \pmod N.$$

The definition of π_j therefore implies that π_j appears in the cycle decomposition of $\rho\sigma_0$. Since $\sigma_0^n(\rho\sigma_0)\sigma_0^{-n} = \rho\sigma_0$, it follows that the N_j-cycles $\sigma_0^{in}\pi_j\sigma_0^{-in}$, $i \in \{1, 2, \ldots, d_j - 1\}$, also appear in the cycle decomposition of $\rho\sigma_0$. Furthermore, for each positive integer $k \le N_j$, the definitions of π_j and d_j together with Lemma 3.3 yield

$$\pi_j^k\left(a_{x_j(1)}\right) - a_{x_j(1)} \equiv 0 \pmod{d_j n} \quad \text{or} \quad \pi_j^k\left(a_{x_j(1)}\right) - a_{x_j(1)} \not\equiv 0 \pmod n$$

according to whether $s_j \mid k$ or $s_j \nmid k$; while, for each non-negative integer $i < d_j$,

$$\sigma_0^{in}\pi_j\sigma_0^{-in} = \left(\sigma_0^{in}\left(a_{x_j(1)}\right)\ \sigma_0^{in}\pi_j\left(a_{x_j(1)}\right)\ \ldots\ \sigma_0^{in}\pi_j^{N_j-1}\left(a_{x_j(1)}\right)\right),$$
$$\sigma_0^{in}\left(a_{x_j(1)}\right) - a_{x_j(1)} \equiv in \pmod{d_j n}.$$

Hence the N_j-cycles $\sigma_0^{in}\pi_j\sigma_0^{-in}$, $i \in \{0, 1, \ldots, d_j - 1\}$, are distinct. Given a positive integer $j' \leq \nu$ other than j, any of the above N_j-cycles differs as well from any $\sigma_0^{in}\pi_{j'}\sigma_0^{-in}$, $i \in \{0, 1, \ldots, d_{j'} - 1\}$. Indeed, for each quartet (k, i, k', i') of non-negative integers with $k < N_j$, $i < d_j$, $k' < N_{j'}$ and $i' < d_{j'}$,

$$\sigma_0^{in}\pi_j^k\left(a_{x_j(1)}\right) \equiv \pi_j^k\left(a_{x_j(1)}\right) \not\equiv \pi_{j'}^{k'}\left(a_{x_{j'}(1)}\right) \equiv \sigma_0^{i'n}\pi_{j'}^{k'}\left(a_{x_{j'}(1)}\right) \pmod{n}.$$

We thus find that π_j, $\sigma_0^n\pi_j\sigma_0^{-n}$, $\ldots$, $\sigma_0^{(d_j-1)n}\pi_j\sigma^{-(d_j-1)n}$ for all $j \in \{1, 2, \ldots, \nu\}$ are disjoint cycles in the cycle decomposition of $\rho\sigma_0$. The proof of the lemma is now completed since $\displaystyle\sum_{j=1}^{\nu} d_jN_j = \frac{N}{n}\sum_{j=1}^{\nu} s_j = N$. □

For readers convenience, we give an example for Lemma 3.4.

Example 4. For $N = 8$ and $n = 4$, let 4-cycle $\boldsymbol{a} = (1\ 3\ 4\ 2)$, n-tuple $\boldsymbol{u} = (0, 1, 0, 1) \in E(2)^4$ and $b = 1 \in E(2)^\times$. From Lemma 3.3, we get $\rho = (1\ 7\ 4\ 6\ 5\ 3\ 8\ 2)$. Since $\rho\sigma_0 = (1)(2\ 8\ 7)(5)(6\ 4\ 3)$, $\nu = 2$ and $d_\nu = 2$, the claim of Lemma 3.4 is

$$\{(1), (2\ 8\ 7), (5), (6\ 4\ 3)\} = \{\sigma_0^{4i}\pi_j\sigma_0^{-4i}(0 \leq i \leq 1, 1 \leq j \leq 2)\}.$$

Actually, for π_1, with $s_1 = 1$,

$$\begin{aligned}\pi_1(a_{x_1(1)}) &= \pi_1(1)\\ &\equiv a_{x_1(1)} + 4(u_{x_1(2)} - u_{x_1(2)-1} + \delta_1^{(1)}) + 4b_1 \pmod{8}.\\ &= 1 + 4 + 4 \equiv 1 \pmod{8}.\end{aligned}$$

Moreover,

$$\pi_2(a_{x_2(1)}) = \pi_2(3) = a_{x_2(2)} + 4(u_{x_2(2)} - u_{x_2(2)-1} + \delta_2^{(1)}) = 2 + 4 = 6$$

$$\pi_2^2(3) = a_{x_2(3)} + 4\sum_{k=1}^{2}(u_{x_2(+1)} - u_{x_2(k+1)-1} + \delta_2^{(k)}) = 4 + 0 = 4$$

and $\pi_2^3(3) = 3$. Namely, π_1 and $\sigma_0^4\pi_1\sigma_0^{-4}$ are both identities of S_8, $\pi_2 = (3\ 6\ 4)$ and $\sigma_0^4\pi_2\sigma_0^{-4} = (2\ 8\ 7)$.

4. Proof of Lemma 3.1-(iv)

Let λ be any partition in $\Lambda_\nu^{(n)}$. Assume that λ is given by $L = l_1 + \cdots + l_\nu$ with a decreasing sequence $l_1 \geq \cdots \geq l_\nu$ of ν integers in $D_{N/n}$. For each positive integer $j \leq \nu$ and each $p \in P_{N/n}$, we denote by $l_{j,p}$ the p-part of l_j, i.e., the highest power of p dividing l_j. In addition to the lemmas in the preceding section, we prove one more lemma for the proof of Lemma 3.1-(iv). To state it, we set $\boldsymbol{d} = (d_1, \dots, d_\nu)$ in $D^{\nu}_{N/n}$.

Lemma 4.1. *Let α be any permutation in S_ν. Then the number of all $(\boldsymbol{u}, b) \in E(N/n)^{n-1} \times E(N/n)^\times$ with $\boldsymbol{d} = (l_{\alpha(1)}, \dots, l_{\alpha(\nu)})$ is equal to*

$$\frac{N^n}{n^n \Delta_\lambda} \prod_{p \in P_{N/n}} A_{n,\lambda,p}.$$

Proof. We write W for the set of all $(w_1, \dots, w_{\nu+1}) \in E(N/n)^{\nu+1}$ satisfying

$$\gcd(w_1, N/n) = l_{\alpha(1)}, \dots, \gcd(w_\nu, N/n) = l_{\alpha(\nu)}, \quad \gcd(w_{\nu+1}, N/n) = 1,$$
$$\sum_{j=1}^{\nu+1} w_j \equiv 1 \pmod{N/n}.$$

Let us prove

$$|W| = \frac{N^\nu}{n^\nu \Delta_\lambda} \prod_{p \in P_{N/n}} A_{n,\lambda,p}. \tag{4.1}$$

Take $p \in P_{N/n}$ and let $e(p) := \mathrm{ord}_p(N/n)$. We denote by W_p the set of $(\nu+1)$-tuples $(w'_1, \dots, w'_{\nu+1})$ of non-negative integers less than $p^{e(p)}$ with

$$l_{\alpha(1),p} \mid w'_1, \dots, l_{\alpha(\nu),p} \mid w'_\nu, \quad \sum_{j=1}^{\nu+1} w'_j \equiv 1 \pmod{p^{e(p)}}.$$

Let $J_p := \{j \in \mathbb{N} \mid 1 \le j \le \nu, l_{\alpha(j),p} < p^{e(p)}\}$, $I_p := \{j \in J_p \mid l_{\alpha(j),p} = 1\}$ and $W^{(p)} := \{(w'_1, \dots, w'_{\nu+1}) \in W_p \mid p l_{\alpha(j),p} \nmid w'_j \ (j \in J_p \setminus I_p)\}$. Clearly

$$|J_p| = i(n, \lambda, p) \ge |I_p| = i_0(n, \lambda, p).$$

When any multiple w_j of $l_{\alpha(j),p}$ for each $j \in \{1, 2, \dots, \nu\}$ are given, there exists a unique non-negative integer $w_{\nu+1} < p^{e(p)}$ satisfying $\sum_{j=1}^{\nu+1} w_j \equiv 1 \pmod{p^{e(p)}}$. Therefore,

$$|W_p| = \prod_{j=1}^{\nu} \frac{p^{e(p)}}{l_{j,p}} = \frac{p^{\nu e(p)}}{\prod_{j=1}^{\nu} l_{j,p}}$$

and consequently,

$$\left| W^{(p)} \right| = |W_p| \left(1 - \frac{1}{p}\right)^{|J_p \setminus I_p|} = \frac{p^{\nu e(p)}}{\prod_{j=1}^{\nu} l_{j,p}} \left(1 - \frac{1}{p}\right)^{i(n,\lambda,p) - i_0(n,\lambda,p)}. \tag{4.2}$$

We set $I'_p = I_p \cup \{\nu+1\}$. For each $j \in I'_p$, let

$$W^{(p)}_j := \{(w'_1, \dots, w'_{\nu+1}) \in W^{(p)} \mid p \in D_{w'_j}\}.$$

Let I range over the non-empty subsets of I'_p. Then we naturally have

$$\left| W^{(p)} \setminus \bigcup_{j\in I'_p} W_j^{(p)} \right| = |W^{(p)}| + \sum_I (-1)^{|I|} \left| \bigcap_{j\in I} W_j^{(p)} \right|$$

and, unless $I = I'_p$, an argument similar to the one verifying (4.2) yields

$$\left| \bigcap_{j\in I} W_j^{(p)} \right| = \frac{|W^{(p)}|}{p^{|I|}}$$

(with any element of $I'_p \setminus I$ taken instead of the subscript $\nu+1$). Since $\bigcap_{j\in I'_p} W_j^{(p)} = \emptyset$, it follows from the above that

$$\begin{aligned} \left| W^{(p)} \setminus \bigcup_{j\in I'_p} W_j^{(p)} \right| &= \left|W^{(p)}\right| \left(\sum_{k=0}^{|I'_p|} \binom{|I'_p|}{k} \left(-\frac{1}{p}\right)^k - \left(-\frac{1}{p}\right)^{|I'_p|} \right) \\ &= \left|W^{(p)}\right| \left(\left(1-\frac{1}{p}\right)^{i_0(\lambda,p)+1} - \left(-\frac{1}{p}\right)^{i_0(\lambda,p)+1} \right). \end{aligned}$$

Hence, by (4.2),

$$\left| W^{(p)} \setminus \bigcup_{j\in I_p} W_j^{(p)} \right| = \frac{p^{\nu e(p)} A_{n,\lambda,p}}{\prod_{j=1}^{\nu} l_{j,p}}.$$

On the other hand, $W^{(p)} \setminus \bigcup_{j\in I'_p} W_j^{(p)}$ is none other than the set of $(\nu+1)$-tuples $(w'_1, \dots, w'_{\nu+1})$ of non-negative integers less than $p^{e(p)}$ for which

$$\gcd\left(w'_1, p^{e(p)}\right) = l_{\alpha(1),p}, \quad \dots, \quad \gcd\left(w'_\nu, p^{e(p)}\right) = l_{\alpha(\nu),p}, \quad p \nmid w'_{\nu+1},$$
$$\sum_{j=1}^{\nu+1} w'_j \equiv 1 \pmod{p^{e(p)}}.$$

This fact implies that

$$|W| = \prod_{p\in P_{N/n}} \left| W^{(p)} \setminus \bigcup_{j\in I'_p} W_j^{(p)} \right|,$$

because a $(\nu+1)$-tuple $(w_1, \dots, w_{\nu+1})$ in $E(N/n)^{\nu+1}$ belongs to W if and only if

$$\gcd\left(w^*_{1,p}, p^{e(p)}\right) = l_{\alpha(1),p}, \quad \dots, \quad \gcd\left(w^*_{\nu,p}, p^{e(p)}\right) = l_{\alpha(\nu),p}, \quad p \nmid w^*_{\nu+1,p},$$

$$\sum_{j=1}^{\nu+1} w^*_{j,p} \equiv 1 \pmod{p^{e(p)}},$$

with p running through $P_{N/n}$, where $w^*_{1,p}, \ldots, w^*_{\nu+1,p}$ denote respectively the minimal non-negative residues of $w_1, \ldots, w_{\nu+1}$ modulo $p^{e(p)}$. Thus (4.1) is proved.

Next, put $u_1 = 0$ as before and let $(u_2, \ldots, u_n)$ run through $E(N/n)^{n-1}$. For each pair (j, k) of positive integers with $j \le \nu$ and $k \le s_j$, we take the integer $w_j^{(k)}$ in $E(N/n)$ satisfying

$$w_j^{(k)} \equiv u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)} \pmod{N/n}.$$

All $u_{x_j(k+1)} - u_{x_j(k+1)-1}$ for $(j,k) \ne (1, s_1)$ can be arranged into the sequence $u_2 - u_1, \ldots, u_n - u_{n-1}$, so that the correspondence

$$(u_2, \ldots, u_n) \mapsto \left(w_1^{(1)}, \ldots, w_1^{(s_1-1)}, w_2^{(1)}, \ldots, w_2^{(s_2)}, \ldots, w_\nu^{(1)}, \ldots, w_\nu^{(s_\nu)}\right)$$

defines a permutation on $E(N/n)^{n-1}$. For each positive integer $j \le \nu$, take the integer $\widetilde{w}_j$ in $E(N/n)$ satisfying

$$\widetilde{w}_j \equiv \sum_{k=1}^{s_j} w_j^{(k)} + b_j \pmod{N/n}.$$

Since

$$\begin{aligned}\sum_{j=1}^{\nu} \widetilde{w}_j - b &\equiv \sum_{j=1}^{\nu}\sum_{k=1}^{s_j} \left(u_{x_j(k+1)} - u_{x_j(k+1)-1} + \delta_j^{(k)}\right) + \sum_{j=1}^{\nu} b_j - b \\ &\equiv \sum_{j=1}^{n} (u_j - u_{j-1}) + 1 \equiv 1 \pmod{N/n},\end{aligned}$$

we have $(d_1, \ldots, d_\nu) = (l_{\alpha(1)}, \ldots, l_{\alpha(\nu)})$ if and only if $(\widetilde{w}_1, \ldots, \widetilde{w}_\nu, \tilde{b})$ belongs to W where $\tilde{b}$ denotes the minimal non-negative residue of $-b$ modulo N/n. Furthermore

$$w_2^{(s_2)} \equiv \widetilde{w}_2 - \sum_{k=1}^{s_2-1} w_2^{(k)} \pmod{N/n},$$

$$\ldots,$$

$$w_\nu^{(s_\nu)} \equiv \widetilde{w}_\nu - \sum_{k=1}^{s_\nu-1} w_\nu^{(k)} \pmod{N/n}.$$

Thus, the correspondence

$$(u_2, \ldots, u_n, b) \mapsto \left(\widetilde{w}_1, \ldots, \widetilde{w}_\nu, \tilde{b}, w_1^{(1)}, \ldots, w_1^{(s_1-1)}, \ldots, w_\nu^{(1)}, \ldots, w_\nu^{(s_\nu-1)}\right)$$

induces a bijection from the set of $(\boldsymbol{u}, b)$ with $\boldsymbol{d} = (l_{\alpha(1)}, \ldots, l_{\alpha(\nu)})$ to the direct product $W \times E(N/n)^{n-\nu}$. Therefore, by (4.1), the number in question of the lemma is $|W| \left(\dfrac{N}{n}\right)^{n-\nu} = \dfrac{N^n}{n^n \Delta_\lambda} \prod_{p \in P_{N/n}} A_{n,\lambda,p}$. □

We are now ready to prove Lemma3.1-(iv).

Proof of Lemma 3.1-(iv). Denote by Π_n the direct product of the set of n-cycles in S_n and $E(N/n)^{n-1} \times E(N/n)^\times$. We let $\boldsymbol{a} = (1\ a_2\ \ldots\ a_n)$ range over all n-cycles in S_n, $\boldsymbol{u} = (u_2, \ldots, u_n)$ over all $(n-1)$-tuples in $E(N/n)^{n-1}$, and b over all integers in $E(N/n)^\times$. In view of Lemma 3.2, a map from the set of N-cycles in $C_{S_N}(\sigma_0^n)$ to Π_n can be defined by sending each N-cycle τ in $C_{S_N}(\sigma_0^n)$ to

$$\left((1\ a'_2\ \ldots\ a'_n), \frac{\tau(1) - a'_2}{n}, \ldots, \frac{\tau^{n-1}(1) - a'_n}{n}, \frac{\tau^n(1) - 1}{n}\right),$$

where a'_j denotes, for each integer j with $2 \leq j < n$, the minimal positive residue of $\tau^{j-1}(1)$ modulo n. Furthermore Lemma 3.3 for the case $(m, d) = (n, 1)$ shows that this map is a bijection. In other words, the correspondence

$$((1\ a_2\ \ldots\ a_n), u_2, \ldots, u_n, b) \mapsto \rho = \rho_{\boldsymbol{a},\boldsymbol{u},b}$$

defines a bijection from Π_n to the set of all N-cycles in $C_{S_N}(\sigma_0^n)$. Let m range over the positive integers not exceeding n. Let R_m denote the set of $\boldsymbol{a}$ with $\nu = m$, i.e., the set of $(1\ a_2\ \ldots\ a_n)$ for which the cycle decomposition (3) of $(1\ a_2\ \ldots\ a_n)\sigma_{0,n}$ in S_n contains just m cycles. Since

$$\left|\left\{\left(l_{\alpha(1)}, \ldots, l_{\alpha(\nu)}\right)\ ;\ \alpha \in S_\nu\right\}\right| = \frac{\nu!}{\nu_1! \nu_2! \cdots \nu_L!} = B_\lambda \Delta_\lambda,$$

we then see from Lemma 4.1 that, for each $\boldsymbol{a} \in R_m$ and any $\lambda \in \Lambda_m^{(n)}$ given by $L = l_1 + \cdots + l_m$ with a decreasing sequence $l_1 \geq \cdots \geq l_m$ of m integers in $D_{N/n}$, the number of $(\boldsymbol{u}, b)$ with $\nu = m$ and with $(d_1, \ldots, d_m) = (l_{\alpha(1)}, \ldots, l_{\alpha(m)})$ for some $\alpha \in S_m$ is equal to

$$\frac{N^n B_\lambda}{n^n} \prod_{p \in P_{N/n}} A_{n,\lambda,p}.$$

However, by Lemma 3.4, the number of cycles in the cycle decomposition of $\rho\sigma_0$ coincides with $\sum_{j=1}^{\nu} d_j$. Therefore, for each $\boldsymbol{a} \in R_m$, the number of $\rho = \rho_{\boldsymbol{a},\boldsymbol{u},b}$ such that the cycle decomposition of $\rho\sigma_0$ contains exactly L cycles, namely the number of ρ belonging to T, is equal to

$$\frac{N^n}{n^n} \sum_{\lambda \in \Lambda_m^{(n)}} B_\lambda \prod_{p \in P_{N/n}} A_{n,\lambda,p}.$$

Further $\Lambda_m^{(n)} = \emptyset$ if $m > L$. We thus obtain

$$\sum_{\lambda \vdash N, l(\lambda)=L} |\, \widetilde{\mathcal{C}}'_{\lambda,r} \,| = \sum_{m=1}^{\min(n,L)} \frac{|R_m| N^n}{n^n} \sum_{\lambda \in \Lambda_m^{(n)}} B_\lambda \prod_{p \in P_{N/n}} A_{n,\lambda,p}.$$

On the other hand, Theorem 1 of Zagier [23] together with [23, Application 3] shows that $|R_m|/(n-1)!$ equals $(1+(-1)^{n-m})/(n+1)!$ times the coefficient of ξ^m in the polynomial $\xi(\xi+1)\cdots(\xi+n)$ in a variable ξ:

$$|R_m| = \frac{1+(-1)^{n-m}}{n(n+1)} \mathfrak{s}_{n-m+1}(1,2,\ldots,n) = \frac{f_{n-m+1}^{(n)}}{n(n+1)}$$

(cf. also [11, A.2]). Hence Lemma 3.1-(iv) is proved. □

5. Proof of Lemma 3.1-(v)

To prove Lemma 3.1-(v), we need several preliminary results. Take any $n \in \mathbb{N}$. We do not assume n to divide N at first.

Lemma 5.1. *If $j \in \mathbb{N}$ and $j \leq n$, then*

$$\sum_{m=j}^{n} (-1)^m \binom{m-1}{j-1} \binom{n}{m} = (-1)^j.$$

Proof. This can be shown by induction on n, with j fixed. □

In S_n, we put $\sigma_{0,n} = (1\ 2\ \ldots\ n)$ as before (without assuming $n \mid N$). When $I \subseteq \{1,2,\ldots,n\}$, let $Z_I^{(n)}$ denote the set of all n-cycles $\boldsymbol{a} \in S_n \setminus \{\sigma_{0,n}^{-1}\}$ such that $\boldsymbol{a}\sigma_{0,n}(a) = a$ for all $a \in I$. For each non-negative integer $m \leq n$, we denote by $\mathcal{F}_m^{(n)}$ the family of subsets of $\{1,2,\ldots,n\}$ with cardinality m, and by $Y_m^{(n)}$ the union of $Z_I^{(n)}$ for all $I \in \mathcal{F}_m^{(n)}$.

Lemma 5.2. *For any $j \in \mathbb{N}$ with $j \leq n$,*

$$\left| Y_j^{(n)} \right| = \sum_{m=0}^{n-j-1} (-1)^m \binom{j+m-1}{j-1} \sum_{I \in \mathcal{F}_{j+m}^{(n)}} \left| Z_I^{(n)} \right|.$$

Proof. Since $Z_{\{1,2,\ldots,n\}}^{(n)} = \emptyset$, we may assume $j < n$. For each $\boldsymbol{a} \in Y_j^{(n)}$, let $J_{\boldsymbol{a}}$ denote the set of positive integers $a \leq n$ with $\boldsymbol{a}\sigma_{0,n}(a) = a$. Noting that $\boldsymbol{a} \neq \sigma_{0,n}^{-1}$, we then have $j \leq |J_{\boldsymbol{a}}| \leq n-1$, i.e., $0 \leq |J_{\boldsymbol{a}}| - j \leq n-j-1$. When any non-negative integer $m \leq n-j-1$ and any $\boldsymbol{a} \in Y_j^{(n)}$ are given, the number of $I \in \mathcal{F}_{j+m}^{(n)}$ satisfying $Z_I^{(n)} \ni \boldsymbol{a}$, i.e., $J_{\boldsymbol{a}} \supseteq I$ is none other than $\binom{|J_{\boldsymbol{a}}|}{j+m}$, which equals 0 in the case $m > |J_{\boldsymbol{a}}| - j$. Therefore

$$\begin{aligned}
&\sum_{m=0}^{n-j-1} (-1)^m \binom{j+m-1}{j-1} \sum_{I \in \mathcal{F}_{j+m}^{(n)}} \left| Z_I^{(n)} \right| \\
&= \sum_{m=0}^{n-j-1} (-1)^m \binom{j+m-1}{j-1} \sum_{I \in \mathcal{F}_{j+m}^{(n)}} \sum_{\boldsymbol{a} \in Z_I^{(n)}} 1 \\
&= \sum_{m=0}^{n-j-1} (-1)^m \binom{j+m-1}{j-1} \sum_{\boldsymbol{a} \in Y_j^{(n)}} \binom{|J_{\boldsymbol{a}}|}{j+m} \\
&= \sum_{\boldsymbol{a} \in Y_j^{(n)}} \sum_{m=0}^{|J_{\boldsymbol{a}}|-j} (-1)^m \binom{j+m-1}{j-1} \binom{|J_{\boldsymbol{a}}|}{j+m},
\end{aligned}$$

and here, by Lemma 5.1,

$$\sum_{m=0}^{|J_{\boldsymbol{a}}|-j} (-1)^m \binom{j+m-1}{j-1} \binom{|J_{\boldsymbol{a}}|}{j+m} = \sum_{m'=j}^{|J_{\boldsymbol{a}}|} (-1)^{m'-j} \binom{m'-1}{j-1} \binom{|J_{\boldsymbol{a}}|}{m'} = 1.$$

Thus the present lemma is proved. □

Lemma 5.3. *Let* $I \subseteq \{1, 2, \ldots, n\}$ *and* $|I| < n$. *Then*

$$\left| Z_I^{(n)} \right| = (n - |I| - 1)! - 1.$$

Proof. The lemma certainly holds in the case $I = \emptyset$, since $Z_\emptyset^{(n)}$ is the set of all n-cycles in $S_n \setminus \{\sigma_{0,n}^{-1}\}$. Let us consider the case $I \neq \emptyset$ from now on. We put $Z_0 = Z_I^{(n)} \cup \{\sigma_{0,n}^{-1}\}$ to prove $|Z_0| = (n - |I| - 1)!$. As is easily seen, there exist a positive integer m and m non-empty subsets $I_1, \ldots, I_m$ of I such that I is the disjoint union of $I_1, \ldots, I_m$ and that, for each positive integer $u \leq m$, a unique $a_u \in I_u$ satisfies

$$I_u = \left\{ a_u, \sigma_{0,n}(a_u), \ldots, \sigma_{0,n}^{|I_u|-1}(a_u) \right\}, \ \sigma_{0,n}^{-1}(a_u) \notin I, \ \sigma_{0,n}^{|I_u|}(a_u) \notin I.$$

Hence, by the definition of $Z_I^{(n)}$, Z_0 is the set of n-cycles $\boldsymbol{a}$ in S_n such that, for all positive integers $u \leq m$,

$$\begin{aligned}
&\boldsymbol{a}\left(\sigma_{0,n}^{|I_u|}(a_u)\right) = \sigma_{0,n}^{|I_u|-1}(a_u), \ \boldsymbol{a}\left(\sigma_{0,n}^{|I_u|-1}(a_u)\right) \\
&= \sigma_{0,n}^{|I_u|-2}(a_u), \ \ldots, \ \boldsymbol{a}(\sigma_{0,n}(a_u)) = a_u.
\end{aligned}$$

Since $\{\sigma_{0,n}^{-1}(a_1), \ldots, \sigma_{0,n}^{-1}(a_m)\} \cap I = \emptyset$, all $\boldsymbol{a} \in Z_0$ satisfy $\{\boldsymbol{a}(a_1), \ldots, \boldsymbol{a}(a_m)\} \cap I = \emptyset$. We also note that $\sigma_{0,n}^{|I_1|}(a_1)$, $\ldots$, $\sigma_{0,n}^{|I_m|}(a_m)$ are distinct.

Now let $\bar{I} = \{1, 2, \ldots, n\} \setminus I$. We denote by Z' the set of all $(n-|I|)$-cycles in the symmetric group on $\bar{I}$. If $\boldsymbol{a} \in Z_0$, let us define a permutation $\bar{\boldsymbol{a}}$ on $\bar{I}$ by the following rule:

$$\begin{aligned} &\bar{\boldsymbol{a}}\left(\sigma_{0,n}^{|I_u|}(a_u)\right) = \boldsymbol{a}(a_u) \quad \text{for } u \in \{1, 2, \ldots, m\}, \\ &\bar{\boldsymbol{a}}(a') = \boldsymbol{a}(a') \qquad\qquad \text{for } a' \in \bar{I} \setminus \left\{\sigma_{0,n}^{|I_1|}(a_1), \ldots, \sigma_{0,n}^{|I_m|}(a_m)\right\}. \end{aligned}$$

We then find without difficulty that $\bar{\boldsymbol{a}}$ belongs to Z' and that the map $\boldsymbol{a} \mapsto \bar{\boldsymbol{a}}$ of Z_0 into Z' is a bijection $Z_0 \to Z'$. Hence $|Z_0| = |Z'| = (n - |I| - 1)!$. □

Lemma 5.4. *For any $j \in \mathbb{N} \cup \{0\}$ with $j < n$, the number of n-cycles $\boldsymbol{a}$ in S_n such that $\boldsymbol{a}\sigma_{0,n}$ fixes exactly j elements of $\{1, 2, \ldots, n\}$ is equal to $\Sigma_j^{(n)} - \Sigma_{j+1}^{(n)}$.*

Proof. As $\Sigma_n^{(n)} = 0$, it suffices to prove that $\Sigma_j^{(n)}$ is the number of n-cycles $\boldsymbol{a} \in S_n \setminus \{\sigma_{0,n}^{-1}\}$ for which $\boldsymbol{a}\sigma_{0.n}$ fixes at least j elements of $\{1, 2, \ldots, n\}$: $|Y_j^{(n)}| = \Sigma_j^{(n)}$. In the case $j = 0$, this immediately follows from Lemma 5.3 and the definition (equation (2.3)). We next assume $j > 0$. In view of Lemmas 5.2 and 5.3, we have

$$\begin{aligned} \left|Y_j^{(n)}\right| &= \sum_{m=0}^{n-j-1} (-1)^m \binom{j+m-1}{j-1} \binom{n}{j+m} ((n-j-m-1)! - 1) \\ &= \sum_{m=0}^{n-j-1} \frac{(-1)^m n!}{(j-1)!\, m!\, (j+m)(n-j-m)} - \sum_{m'=j}^{n-1} (-1)^{m'-j} \binom{m'-1}{j-1} \binom{n}{m'}. \end{aligned}$$

Therefore, with the definition (1), Lemma 5.1 yields

$$\left|Y_j^{(n)}\right| = \Sigma_j^{(n)} + 1 - (-1)^j \sum_{m'=j}^{n} (-1)^{m'} \binom{m'-1}{j-1} \binom{n}{m'} = \Sigma_j^{(n)}.$$

□

Now let us return to the situation of Lemma 3.4, in which $n \mid N$. Fixing any $b \in E(N/n)^\times$ and letting $\boldsymbol{u} = (u_2, \ldots, u_n)$ range over all $(n-1)$-tuples in $E(N/n)^{n-1}$, we define

$$U = \left\{ \boldsymbol{u} = (u_2, \ldots, u_n) \in E(N/n)^{n-1} \;\middle|\; \sum_{\substack{1 \le j \le \nu \\ N_j = 1}} d_j = h \right\}.$$

We put $n' = n - hn/N$, so that $n' \in \mathbb{N} \cup \{0\}$ in the case $N/n \mid h$.

Lemma 5.5. *Let* $t = |\{j \in \mathbb{N} \mid j \leq \nu, s_j = 1\}|$. *Then*

$$|U| = \begin{cases} 0 & \text{if } N/n \nmid h \text{ or if } t < hn/N, \\ \binom{t}{hn/N} \dfrac{N^{n-t-1}}{n^{n-t-1}} \left(\dfrac{N}{n} - 1\right)^{t-hn/N} & \text{if } N/n \mid h,\ hn/N \leq t < n, \\ \binom{n}{hn/N} \left(\dfrac{n}{N}\left(\left(\dfrac{N}{n} - 1\right)^{n'} - (-1)^{n'}\right) + \delta_b\right) & \text{if } N/n \mid h,\ t = n; \end{cases}$$

Here δ_b *denotes* $(-1)^{n'}$ *or* 0 *according to whether* $b = N/n - 1$ *or not.*

Proof. Let $I_0 = \{j \in \mathbb{N} \mid j \leq \nu, s_j = 1\}$.For each $j \in \{1, 2, \ldots, \nu\}$, as follows from the definition of N_j, the condition $N_j = 1$ is equivalent to the condition that $s_j = 1$ and that $d_j = N/n$. Hence, by Lemma 3.4,

$$h = |\{j \in I_0 \mid d_j = N/n\}| \frac{N}{n} \leq \frac{tN}{n}$$

in the case $\boldsymbol{u} \in U$. This shows that $U = \emptyset$ if $N/n \nmid h$ or $t < hn/N$.

Suppose next that $N/n \mid h$ and $t \geq hn/N$. For each $k \in \{1, 2, \ldots, n\}$, let u_k^* denote the integer in $E(N/n)$ such that $u_k^* \equiv u_k - u_{k-1} \pmod{N/n}$. In particular, $u_1^* \equiv -u_n \pmod{N/n}$. Set

$$I^* = \left\{ j \in I_0 \mid u^*_{x_j(1)} \equiv -\delta_j^{(1)} - b_j \pmod{N/n} \right\},$$

and let $\mathcal{F}$ be the family of all subsets of I_0 with cardinality hn/N. Obviously

$$|\mathcal{F}| = \binom{t}{hn/N} = \binom{t}{t - hn/N}.$$

Given any $j \in I_0$, we see from the definition of d_j that $d_j = N/n$ if and only if $u^*_{x_j(1)} \equiv -\delta_j^{(1)} - b_j \pmod{N/n}$. Therefore, by Lemma 3.4, the three conditions

$$\boldsymbol{u} \in U, \quad I^* \in \mathcal{F}, \quad \left| \left\{ j \in I_0 \mid u^*_{x_j(1)} \not\equiv -\delta_j^{(1)} - b_j \pmod{N/n} \right\} \right| = t - \frac{hn}{N}$$

are equivalent. On the other hand, when we assume $t < n$ with taking a positive integer $k' \leq n$ outside the set $\{x_j(1)\,;\ j \in I_0\}$ of cardinality t, the correspondence $\boldsymbol{u} \mapsto (u_1^*, \ldots, u^*_{k'-1}, u^*_{k'+1}, \ldots, u_n^*)$ defines a permutation on $E(N/n)^{n-1}$. Thus, in the case $t < n$,

$$|U| = \left(\frac{N}{n}\right)^{n-1-t} |\mathcal{F}| \left(\frac{N}{n} - 1\right)^{t-hn/N} = \binom{t}{hn/N} \frac{N^{n-t-1}}{n^{n-t-1}} \left(\frac{N}{n} - 1\right)^{t-hn/N}.$$

We now suppose that $N/n \mid h$ and $t = n$. Let I be any set in $\mathcal{F}$, namely any subset of $I_0 = \{1, 2, \ldots, n\}$ with cardinality hn/N. Let U' denote the set of $\boldsymbol{u} \in E(N/n)^{n-1}$ satisfying $I^* \supseteq I$. We put $\bar{I} = I_0 \setminus I = \{1, 2, \ldots, n\} \setminus I$, and so $n' = |\bar{I}|$. Let us consider the case where $h < N$, i.e., $n' > 0$. As there exists a positive integer k in $\bar{I}$ and the correspondence $\boldsymbol{u} \mapsto (u_1^*, \ldots, u_{k-1}^*, u_{k+1}^*, \ldots, u_n^*)$ defines a permutation on $E(N/n)^{n-1}$, it follows that

$$|U'| = \left(\frac{N}{n}\right)^{n-1-hn/N} = \left(\frac{N}{n}\right)^{n'-1}.$$

For each $j \in \bar{I}$, let U'_j denote the set of $\boldsymbol{u} \in U'$ with $u^*_{x_j(1)} \equiv -\delta_j^{(1)} - b_j \pmod{N/n}$. Clearly $U' \setminus \bigcup_{j \in \bar{I}} U'_j$ is the set of all $\boldsymbol{u} \in E(N/n)^{n-1}$ satisfying $I^* = I$. Let I' vary over the non-empty subsets of $\bar{I}$. Then

$$\left| U' \setminus \bigcup_{j \in \bar{I}} U'_j \right| = |U'| + \sum_{I'} (-1)^{|I'|} \left| \bigcap_{j \in I'} U'_j \right|.$$

In the case $I' \neq \bar{I}$, the permutation on $E(N/n)^{n-1}$ defined for any $k \in \bar{I} \setminus I'$ by the correspondence $\boldsymbol{u} \mapsto (u_1^*, \ldots, u_{k-1}^*, u_{k+1}^*, \ldots, u_n^*)$ causes us to have

$$\left| \bigcap_{j \in I'} U'_j \right| = \left(\frac{N}{n}\right)^{n'-1-|I'|}.$$

Furthermore

$$(5.1) \quad \sum_{j=1}^{n} u^*_{x_j(1)} = \sum_{j=1}^{n} u_j^* \equiv 0 \pmod{N/n}, \quad \sum_{j=1}^{n} \left(-\delta_j^{(1)} - b_j\right) = -1 - b.$$

Therefore, when $-1-b \not\equiv 0 \pmod{N/n}$, i.e., $b \neq N/n-1$, we have $\bigcap_{j \in \bar{I}} U'_j = \emptyset$, so that

$$\begin{aligned} \left| U' \setminus \bigcup_{j \in \bar{I}} U'_j \right| &= \left(\frac{N}{n}\right)^{n'-1} + \sum_{I' \neq \bar{I}} (-1)^{|I'|} \left(\frac{N}{n}\right)^{n'-1-|I'|} \\ &= \sum_{k=0}^{n'} \binom{n'}{k} (-1)^k \left(\frac{N}{n}\right)^{n'-1-k} - (-1)^{n'} \left(\frac{N}{n}\right)^{-1} \\ &= \frac{n}{N} \left(\left(\frac{N}{n} - 1\right)^{n'} - (-1)^{n'} \right). \end{aligned}$$

When $b = N/n - 1$, it follows for any $j_0 \in \bar{I}$ that

$$\bigcap_{j\in\bar{I}} U'_j = \bigcap_{j\in\bar{I}\setminus\{j_0\}} U'_j \quad \text{or} \quad \bigcap_{j\in\bar{I}} U'_j = U'_{j_0} = U'$$

according to whether $n' > 1$ or $n' = 1$; hence

$$\begin{aligned}\left| U' \setminus \bigcup_{j\in\bar{I}} U'_j \right| &= \sum_{k=0}^{n'} \binom{n'}{k} (-1)^k \left(\frac{N}{n}\right)^{n'-1-k} - (-1)^{n'} \left(\frac{N}{n}\right)^{-1} - (-1)^{n'-1} \\ &= \frac{n}{N}\left(\left(\frac{N}{n} - 1\right)^{n'} - (-1)^{n'}\right) + (-1)^{n'}.\end{aligned}$$

Thus we find that the number of $\boldsymbol{u} \in E(N/n)^{n-1}$ with $I^* = I$ is equal to

$$\frac{n}{N}\left(\left(\frac{N}{n} - 1\right)^{n'} - (-1)^{n'}\right) + \delta_b.$$

This fact yields

$$|U| = \binom{n}{hn/N}\left(\frac{n}{N}\left(\left(\frac{N}{n} - 1\right)^{n'} - (-1)^{n'}\right) + \delta_b\right).$$

Finally, in the case where $h = N$, i.e., $n' = 0$, since $\mathcal{F}$ consists only of $\{1, 2, \ldots, n\}$ and (8) still holds, we easily obtain $|U| = \delta_b$, the same equality as the above. □

By means of Lemmas 5.4 and 5.5, we can prove Lemma 3.1-(v) as follows.

Proof of Lemma 3.1-(v). Let $n \in D^*$. As in the proof of Lemma 3.1-(iv), let $\boldsymbol{a}$ range over all n-cycles in S_n, $\boldsymbol{u}$ over all $(n-1)$-tuples in $E(N/n)^{n-1}$, and b over all integers in $E(N/n)^\times$. Further, as in Lemma 5.5, let t denote the number of $j \in \{1, 2, \ldots, \nu\}$ with $s_j = 1$. We take any integer m satisfying $hn/N \leq m < n$. By Lemma 5.4, the number of $\boldsymbol{a}$ with $t = m$ is equal to $\Sigma_m^{(n)} - \Sigma_{m+1}^{(n)}$ because the condition $t = m$ means that $\boldsymbol{a}\sigma_{0,n}$ fixes exactly m elements of $\{1, 2, \ldots, n\}$. In addition, $t = n$ if and only if $\boldsymbol{a} = \sigma_{0,n}^{-1}$. Lemma 5.5 therefore shows that

$$\begin{aligned}&\sum_{\lambda\vdash N, m_1(\lambda)=h} |\, \widetilde{\mathcal{C}}'_{\lambda,r} \,| \\ &= \sum_{m=hn/N}^{n-1} \left(\Sigma_m^{(n)} - \Sigma_{m+1}^{(n)}\right) \varphi(N/n) \binom{m}{hn/N} \frac{N^{n-m-1}}{n^{n-m-1}} \left(\frac{N}{n} - 1\right)^{m-hn/N}\end{aligned}$$

$$+\binom{n}{hn/N}\left(\frac{n}{N}\left(\left(\frac{N}{n}-1\right)^{n-hn/N}-(-1)^{n-hn/N}\right)+(-1)^{n-hn/N}\right)$$
$$+(\varphi(N/n)-1)\binom{n}{hn/N}\left(\frac{n}{N}\left(\left(\frac{N}{n}-1\right)^{n-hn/N}-(-1)^{n-hn/N}\right)\right)$$
$$= \Upsilon_{N,h,n}.$$

□

6. Appendix

A purpose in this appendix is to discuss about Belyi maps for our dessins with $2 \leq N \leq 6$. According to Table 1, there are

$$\overbrace{1}^{N=2}+\overbrace{2}^{N=3}+\overbrace{3}^{N=4}+\overbrace{8}^{N=5}+\overbrace{24}^{N=6}=\overbrace{14}^{2\leq N\leq 5}+\overbrace{24}^{N=6}=38$$

such dessins. In a general setting, several authors have computed a Belyi map for each of given dessin passports as in [2], [6], [18],[17] and [1]. In particular, the database [12] based on the algorithm given in [17] is considerably useful. However, Birch's excellent computation in [2, p.40-44] is already good enough to cover the above 14 dessins for $2 \leq N \leq 5$ with [6, Proposition 9], [1] supplementary. However, it would be convenient for readers to explain how to obtain Belyi maps for our dessins. For $N = 6$, it seems difficult to compute all dessins in question by using Mathematica v.12 as far as we carried out. Instead, we rely on the database [12].

Recall our notation that a dessin passport $[(N),(N),\lambda]$ in $\mathfrak{D}_{\lambda,r}$ means the corresponding Riemann surface X and the associated Belyi map $\beta : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ satisfy the following properties that

(1) β is totally ramified with the ramification degree (index) N at each point in the fiber at 0 or 1. In particular, $|\beta^{-1}(\{0,1\})| = 2$;
(2) The length L of the partition λ (of N) is the length of the cyclic decomposition of $\sigma_\infty = (\sigma_0\sigma_1)^{-1}$;
(3) $|\mathrm{Aut}(X,D)| = r$.

Let us remark that if $L = N$, then σ_∞ is trivial and $|\beta^{-1}(\{\infty\})| = N$. Hence, β is split completely at ∞. On the other hands, if $L = 1$, then $|\beta^{-1}\{(\infty\})| = 1$ and hence, β is totally ramified at ∞. In this appendix, we denote by $\mathrm{Aut}(X,D) = \mathrm{Aut}(X,D,\beta)$ the group of automorphisms of X which preserve β and the colors of the dessin D on X drawn by β. The latter assumption forces the automorphisms to fix $\beta^{-1}(\{0,1\})$ pointwisely.

6.1. **The case when $N = L = r$.** In this case, the genus of the dessin is zero. A Belyi map is simply given by $\beta : X = \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}),\ z \mapsto$

$\dfrac{z^N}{z^N-1}$. Clearly, $\mathrm{Aut}(X,D,\beta)$ is generated by $\alpha_N : X \longrightarrow X,\ z \mapsto \zeta_N z$ where ζ_N is a primitive N-th root of unity. Notice that $\beta^{-1}(\{0,1\}) = \{0,\infty\}$ and it is fixed pointwisely by α_N.

This examples cover five dessins among our 38 dessins.

6.2. **The case when** $(N,L,r) = (3,1,3)$**.** In this case, the genus of X is one, hence it is an elliptic curve over some number field. From Type [3,3,3] in [2, p.42], after a slight modification, we see $X : y(1-y) = x^3$. One can easily find the Belyi map which is given by

$$\beta : X \longrightarrow \mathbb{P}^1(\mathbb{C}),\ (x,y) \mapsto y.$$

We remark that the automorphism $X \longrightarrow X,\ (x,y) \mapsto (x,1-y)$ actually preserves β but not fix pointwisely the colors $\beta^{-1}(\{0,1\}) = \{(0,0),(0,1)\}$ of the dessin. On the other hands, one can easily check that $\mathrm{Aut}(X,D,\beta)$ is generated by $E \longrightarrow E,\ (x,y) \mapsto (\zeta_3 x, y)$.

6.3. **The case when** $(N,L,r) = (4,2,1)$**.** In this case, the genus of X is one. From Type [4,4,31] in [2, p.42], we see $X : y^2 = 4(2x+9)(x^2+2x+9)$ and β is the composition of $X \longrightarrow \mathbb{P}^1(\mathbb{C}),\ (x,y) \mapsto x^2+4x+18+y$ and $\gamma : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}),\ z \mapsto \dfrac{z}{z-1}$. Notice that Birch's notation respects the passport (the ramification datum) at $0,\infty,1$ in this order while our notation is one at $0,1,\infty$. The automorphism γ plays a role to switch $1,\infty$ but preserve 0. It is easy to see that $\mathrm{Aut}(X)$ is generated by the (non-trivial) translation maps and an involution $\iota : X \longrightarrow X,\ (x,y) \mapsto (x,-y)$. Thus, any non-trivial element of $\mathrm{Aut}(X)$ does not preserve β. Therefore, $\mathrm{Aut}(X,D,\beta)$ is trivial.

6.4. **The case when** $(N,L,r) = (4,2,4)$**.** In this case, the genus of X is one. From Type [4,4,22] in [2, p.42], after a slight modification, we see $X : y(1-y) = x^4$ and $\beta : X \longrightarrow \mathbb{P}^1(\mathbb{C}),\ (x,y) \mapsto y$. As in the case $(N,L,r) = (3,1,3)$, the automorphism $X \longrightarrow X,\ (x,y) \mapsto (x,1-y)$ actually preserves β but not fix pointwisely the colors $\beta^{-1}(\{0,1\}) = \{(0,0),(0,1)\}$ of the dessin. On the other hands, one can easily check that $\mathrm{Aut}(X,D,\beta)$ is generated by $E \longrightarrow E,\ (x,y) \mapsto (\zeta_4 x, y)$.

6.5. **The case when** $(N,L,r) = (5,3,1)$**.** In this case, we have three dessins and each of them is of genus one. Two dessins among all can be read off from Type [5,5,311] in [2, p.43] and the remaining dessin is from Type [5,5,221] in [2, p.43]. The Belyi map for each case is given by $\beta = \gamma \circ J$ where J is the Birch's Belyi map and γ is defined in Section 6.3. All curves are non-CM elliptic curves and as in $(N,L,r) = (4,2,1)$, we can easily check the triviality of $\mathrm{Aut}(X,D,\beta)$.

6.6. **The case when** $(N, L, r) = (5, 1, 5)$**.** In this case, we have three dessins and each of them is of genus two. This has been already mentioned at line -6 to the bottom line in page 380 of [6]. From Type [5,5,5] in [2, p.43], we see $X : y(1-y) = x^5$ and $\beta : X \longrightarrow \mathbb{P}^1(\mathbb{C}),\ (x, y) \mapsto y$. Let us consider three automorphisms $\sigma_i : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C}),\ i = 0, 1, 2$ defined by

$$\sigma_0 = \mathrm{id},\ \sigma_1(z) = \frac{1}{1-z},\ \sigma_2 = \frac{z}{z-1}.$$

It is easy to check that σ_1, σ_2 can not be liftable to any automorphism of X (notice that in either case of $(N, L, r) = (3, 1, 3)$ or $(4, 2, 4)$, σ_1, σ_2 can lift to some automorphism of X). Notice that $\mathrm{Aut}(X, D, \beta)$ is generated by $(x, y) \mapsto (\zeta_5 x, y)$. Therefore, $(X, \sigma_i \circ \beta),\ i = 0, 1, 2$ give three dessins as desired.

We explain how to find an explicit equation for each of X and β. Since X is of genus two, it is defined by $y^2 = f(x)$ where $f(x)$ is a polynomial of degree 5 or 6. At this point, there is no clear reason, but to start the computation, suppose $f(x)$ is of degree 5 which is the case when the point P_∞ at infinity is a Weierstrass point on X (the case of degree 6 will be handled later). Since our Belyi map β is totally ramified at infinity and it is of degree 5, β belongs to the Riemann-Roch space $L(5P_\infty) = \langle 1, x, x^2, y\rangle$. We write $\beta = \beta(x, y) = b_0 + b_1 x + b_2 x^2 + cy$ and $f(x) = x^5 + a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$. Since $L(4P_\infty) = \langle 1, x, x^2\rangle$, $c \neq 0$. Hence we may assume $c = 1$. The point in each fiber at 0 or 1 has valency five. Therefore, for $t = 0, 1$, we first solve $\beta(x, y) = t$ in y and then substitute it into $f(x) - y^2$ to formulate

$$f(x) - (b_0 + b_1 x + b_2 x^2)^2 = k_1 (x - d_1)^5,\ f(x) - (1 - b_0 - b_1 x - b_2 x^2)^2 = k_2 (x - d_2)^5.$$

By using Mathematica version 12.1, we can easily solve the system of the equations for

$$a_0, a_1, a_2, a_3, a_4, b_0, b_0, b_1, b_2, k_1, k_2, d_1, d_2.$$

As a result, we would find the above equation after a change of variables.

6.7. **The case when** $(N, L, r) = (5, 1, 1)$**.** In this case, the genus of X is two. It is defined by $y^2 = f(x)$ where $f(x)$ is of degree 6 and there are two points, say $P_\pm$, at infinity. Fuertes and Mednykh found an explicit equation for X in [6, Proposition 9]. They used an interpretation of X in terms of the quotient of the complex upper half plane $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ by some Fuchsian group. A different approach using only Riemann-Roch spaces as above is given in [1, p.14] and it yields

$$X : y^2 = x^6 + 3x^5 + \frac{29}{4}x^4 + \frac{19}{2}x^3 + \frac{29}{4}x^2 + 3x + 1$$

and

$$\beta = x^5 + \frac{5}{2}x^4 + 5x^3 + 5x^2 + \frac{5}{2}x + 1 + (1 + x + x^2)y.$$

By using Magma calculator [3], one can check that $\mathrm{Aut}(X)$ is generated by the hyperelliptic involution, $(x, y) \mapsto (1/x, y/x^3)$, and $(x, y) \mapsto (\zeta_3 x, y)$. The triviality of $\mathrm{Aut}(X, D, \beta)$ follows from this. By using the transformation $(x, y) \mapsto \Big(\frac{\zeta_3 x + 1}{x - \zeta_3}, \frac{\sqrt{5}y}{2(x - \zeta_3)^3}\Big)$, we get the equation of Fuertes and Mednykh, that is defined by $y^2 = x^6 + \frac{118}{5}x^3 + 1$. Birch also gave an explicit form for X with $J = \beta$ which is isomorphic over $\mathbb{Q}$ to one defined above.

As a small remark, those curves have the same Igusa invariants

$$I_2 = \frac{5963102065799}{2560000},\ I_4 = \frac{72224783519}{1638400},\ I_6 := \frac{22783969823}{6553600}$$

(see [21] for Igusa invariants of curves (or Riemann surfaces) of genus two).

Let us sketch a computation to find X and β out because Adrianov-Shabat's explanation is kind of sketchy. We write $f(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. If $a_0 = 0$, after a change of variables, the point at infinity becomes a Weierstrass point. We have already considered this case. Therefore, after shifting the variable x, we may further assume $a_0 = 1$. Let $P_\pm$ are two points at infinity. Put $P_\infty := P_+$ and suppose β belongs to the Riemann-Roch space $L(5P_\infty)$ but not to $L(4P_\infty)$. We first consider the Riemann-Roch spaces $L(5P_\infty) \subset L(5(P_+ + P_-)) = \langle 1, x, x^2, x^3, x^4, x^5, y, xy, x^2y\rangle$ and write

$$\beta = \beta(x, y) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5 + (c_0 + c_1x + c_2x^2)y.$$

The above condition on β is equivalent to $\mathrm{ord}_{1/x}(\beta(1/x, \sqrt{f(1/x)}/x^3)) = 5$ where the square root is chose so that the Taylor series of $\sqrt{f(1/x)}$ at P_∞ takes the form $\sqrt{f(1/x)} = 1 + \cdots \in \mathbb{C}[[1/x]]$. Thus, i-th coefficient of $\beta(1/x, \sqrt{f(1/x)}/x^3)$ in $1/x$ is zero if $i \le 4$. Solving the system of equations in this condition, we can write $b_1, \ldots, b_5$ in terms of $a_1, \ldots, a_5, c_0, c_1, c_2$ (8 variables). On the other hand, the ramification index of β at a point in each fiber at 0 or 1 is five. Therefore, for $t = 0, 1$, we solve $\beta(x, y) = t$ in y and then substitute it into $f(x) - y^2$. We observe that there is an elimination of the terms of higher degree so that $\{f(x)-y^2\}(c_0+c_1x+c_2x^2)^2$ is (generically) of degree 5 by construction. Now we formulate

$$\{f(x) - y^2\}(c_0 + c_1x + c_2x^2)^2 = k_1(x - d_1)^5,$$
$$\{f(x) - y^2\}(c_0 + c_1x + c_2x^2)^2 = k_2(x - d_2)^5$$

and they yields an algebraic system of the equations for

$$a_0, \ldots, a_5, b_0, c_0, c_1, c_2, k_1, k_2, d_1, d_2 \text{ (14 variables).}$$

Successively eliminating variables, we would have a desired form as in [1].

6.8. **The case when $N = 6$.** In this case, we rely on [12] as mentioned. Henceforth, we follow the notation there. The case when $[N, L, r] = [6, 6, 6]$ corresponds to $[a, b, c] = [6, 6, 1]$. The case $[N, L] = [6, 4]$ corresponds to the labels of the ramification types $[[6], [6], \text{four cycles}]$ with total $1 + 1 + 5 = 7$ dessins.

The case $[N, L] = [6, 2]$ corresponds to the labels of the ramification types $[[6], [6], \text{two cycles}]$ with total $13 + 1 + 1 + 1 = 16$ dessins. Thus, we can read off 24 dessings and also Belyi maps from [12].

Acknowledgements

The author is grateful to Professor Takuya Yamauchi for his insightful comments and specific suggestions. She would like to thank Professor Hiroshi Tsunogai for useful discussions. She also thank the referee for carefully reading the article and fruitful suggestions.

References

[1] N. M. Adrianov and G. B. Shabat, Calculating Complete Lists of Belyi Pairs, Mathematics 2022, 10(2), 258; https://doi.org/10.3390/math10020258.
[2] B. Birch, Noncongruence subgroups, covers and drawings. The Grothendieck theory of dessins d'enfants (Luminy, 1993), 25–46, London Math. Soc. Lecture Note Ser., 200, Cambridge Univ. Press, Cambridge, 1994.
[3] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235-265, 1997. Computational algebra and number theory (London, 1993).
[4] M. A. Deryagina and A. D. Mednyh, On the enumeration of circular maps with given number of edges, Siberian Math. J., Vol. 54, No. 4, 624–639, (2013).
[5] B. Dubrovin, D. Yang and D. Zagier, Classical Hurwitz Number and related combinatorics, Moscow Mathematical Journal, Vol. 17, No. 4, 601–633 (2017). (DOI: 10.17323/1609-4514-2017-17-4-601-633)
[6] Y. Fuertes and A. Mednykh, Genus 2 semi-regular coverings with lifting symmetries. Glasg. Math. J. 50 (2008), no. 3, 379–394.
[7] E. Girondo and G. González-Diez, *Introduction to Compact Riemann Surfaces and Dessins D'enfants*, London Math. Soc. Student Texts, vol. 79, Cambridge University Press, Cambridge, 2012.
[8] A. Grothendieck, Esquisse d'un programme. In *Geometric Galois Action, vol.1*, London Math. Soc. Lecture Note Ser., vol. 242, Cambridge University Press, Cambridge, 1997, pp. 5-48 (English translation, pp. 243-284).
[9] G. A. Jones, Regular dessins with a given automorphism group (2014), Contemporary Mathematics. vol. 629, 245–260 (2014).

[10] G. A. Jones and M. Streit, Galois groups, monodromy groups and cartographic groups. In *Geometric Galois Action, vol.2*, London Math. Soc. Lecture Note Ser., vol. 243, Cambridge University Press, Cambridge, 1997, pp. 25-65.

[11] S. K. Lando and A. K. Zvonkin, *Graphs on Surfaces and their Applications*, Encyclopedia of Mathematical Sciences, vol. 141, Springer-Verlag, Berlin, 2004.

[12] The LMFDB Collaboration, Belyi maps database, available at `https://beta.lmfdb.org/Belyi/`.

[13] A. D. Mednykh, Nonequivalent coverings of Riemann surfaces with a given ramification type. Sib. Mat. Zh. vol.25 (1984) 120–142. [Trans. Amer. Math. Soc. **107** (1963), 320–346; MR0148900].

[14] A. D. Mednykh and R. Nedela, Recent progress in enumeration of hypermaps, Journal of Mathematical Sciences, Vol. 226, No. 5, (2017). (DOI: 10.1007/s10958-017-3555-5)

[15] W. O. J. Moser, A (modest) generalization of the theorems of Wilson and Fermat, Canad. Math. Bull. Vol.33(2), 1990(pp253–256).

[16] S. Monni, J. S. Song and Y. S. Song, The Hurwitz enumeration problem of branched covers and Hodge integrals, J. Geom. Phys. 50, No.1–4, 223–256 (2004).

[17] M. Musty, S. Schiavone, J. Sijsling, Jeroen, and J. Voight, A database of Belyi maps. Proceedings of the Thirteenth Algorithmic Number Theory Symposium, 375–392, Open Book Ser., 2, Math. Sci. Publ., Berkeley, CA, 2019.

[18] J. Sijsling and J. Voight, On computing Belyi maps. Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, 73–131, Publ. Math. Besançon Algèbre Théorie Nr., 2014/1, Presses Univ. Franche-Comté, Besancon, 2014.

[19] J. Silverman, The arithmetic of elliptic curves. Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp.

[20] J. E. Steggall, On the number of patterns which can be derived from certain elements. Messenger of Mathematics, 32 (1907), 56-61.

[21] M. Streng, Computing Igusa class polynomials. Math. Comp. 83 (2014), no. 285, 275–309.

[22] Wolfram Research, Inc., Mathematica, Wolfram Research, Inc., Ver. 12.0.0.0, `https://www.wolfram.com/mathematica`.

[23] D. Zagier, On the distribution of the number of cycles of elements in symmetric groups, Nieuw Arc. Wiskd. IV Ser., **13**, 489-495 (1995).

[24] L. Zapponi, What is a dessin d'enfant?, Notice of the AMS, Vol. 50, No. 7, pp788–789 (2003).

Madoka Horie
Graduate School of Science
Tohoku University
Sendai 980-8575,Japan
e-mail address: horiemaaa@gmail.com

(*Received February 7, 2022*)
(*Accepted October 8, 2023*)