Counting Belyi pairs over finite fields

George Shabat

Abstract Alexander Grothendieck's theory of *dessins d'enfants* relates *Belyi pairs* over $\overline{\mathbb{Q}}$ with certain graphs on compact oriented surfaces; the present paper is aimed at the extension of this correspondence. We introduce two closely related categories of Belyi pairs over arbitrary algebraically closed fields, in particular over the algebraic closures $\overline{\mathbb{F}_p}$ of finite fields. The lack of the analogs of graphs on surfaces over $\overline{\mathbb{F}_p}$ promotes the development of other tools that are introduced and discussed. The problem of counting Belyi pairs of bounded complexity is posed and illustrated by some examples; the application of powerful methods of counting dessins d'enfants together with the concept of *bad primes* is emphasized. The relations with geometry of the moduli spaces of curves is briefly mentioned.

Introduction

The hidden relations between seemingly different objects cause the increasing interest of mathematicians, especially since the middle of twentieth century, when it became possible to understand these relations in categorical terms. The recent explosions of activity in topological recursion, *Langlands program* (e.g., [8]), *monstrous moonshine* (e.g., [9]) provide some obvious examples.

Alexander Grothendieck's theory of *dessins d'enfants* (see [12], [24] and [17]) demonstrates yet another mixture of combinatorial topology, arithmetic geometry and group theory. In its original form it relates *Belyi pairs* (to be defined soon) over $\overline{\mathbb{Q}}$ with certain graphs on compact oriented surfaces. The concept of Belyi pair is automatically extended to the case of arbitrary algebraically closed fields, in particular they can be defined over the fields

George Shabat
Russian State University for the Humanities, Miusskaya sq. 6, Moscow, GSP-3, 125993, Russia, e-mail: george@shabat.gmail.com

$\overline{\mathbb{F}_p}$, the algebraic closures of finite fields; the lack of the analogs of graphs on surfaces over $\overline{\mathbb{F}_p}$ promotes the development of other tools that will be introduced and discussed in the present paper.

The objects of the categories that we are going to consider are definable by finite amounts of information; hence the task of counting objects of bounded complexity arises naturally. The theory is in its infancy and therefore the consideration of some simple examples will prevail over the general theorems.

The paper is based on the author's talk at the Creswick conference in the December 2016; the author is indebted to the organizers of this conference for the stimulating atmosphere in this wonderful place. The special thanks go to P. Norbury for clarifying the matters that we are going to discuss in the last section.

The paper is supported in part by the Simons foundation.

1 Belyi pairs

We shall work over ground fields $\Bbbk$, assuming forever that they are algebraically closed,

$$\overline{\Bbbk} = \Bbbk.$$

The smaller fields $\Bbbk_0$ will be considered as well, such that $\Bbbk = \overline{\Bbbk_0}$; the typical cases are $\Bbbk_0 = \mathbb{Q}$ and $\Bbbk_0 = \mathbb{F}_p$ for a prime p. The intermediate fields $\mathbb{K}$,

$$\Bbbk_0 \subset \mathbb{K} \subset \Bbbk$$

with $[\mathbb{K} : \Bbbk_0] < \infty$, will also be in the game; typically, these $\mathbb{K}$'s will be fields of *algebraic numbers* and *finite fields* $\mathbb{F}_q = \mathbb{F}_{p^r}$.

By a *curve* we always mean a *complete curve* over $\Bbbk$; it would be nice to assume that our curves are *irreducible* and *smooth* as well, however, in the cases of *bad reduction* (at least one of) these properties is lost.

For a smooth irreducible curve $\mathbf{X}$ we identify a rational function $f \in \Bbbk(\mathbf{X})$ with a *regular* map $f : \mathbf{X} \to \mathbf{P}_1(\Bbbk)$ to the projective line.

For the rest of the paper we assume that these maps are *separable*, or, equivalently, that the field extensions $\Bbbk(\mathbf{X}) \supset \Bbbk(f)$ are separable, not like $\mathbb{F}_p(\sqrt[p]{x}) \supset \mathbb{F}_p(x)$.

A non-constant $f \in \Bbbk(\mathbf{X}) \setminus \Bbbk$ defines a *surjective* map $f : \mathbf{X} \to \mathbf{P}_1(\Bbbk)$, and for *almost* all $c \in \mathbf{P}_1(\Bbbk)$ – that is, except finitely many c's – the cardinality of preimages $\#f^{-1\circ}(c)$ is the same. It is called the *degree* of f

$$\#\{c \in \mathbf{P}_1(\Bbbk) \mid \#f^{-1\circ}(c) \neq \deg f\} < \infty.$$

Since $\mathbf{P}_1(\Bbbk)$ is infinite, the degree $\deg f$ is well-defined by this statement.

An equivalent definition is

$$\deg f := [\Bbbk(\mathbf{X}) : \Bbbk(f)].$$

The sufficient condition for f to be separable is that either $\mathrm{char}(\Bbbk) = 0$ or $\mathrm{char}(\Bbbk) \nmid \deg f$.

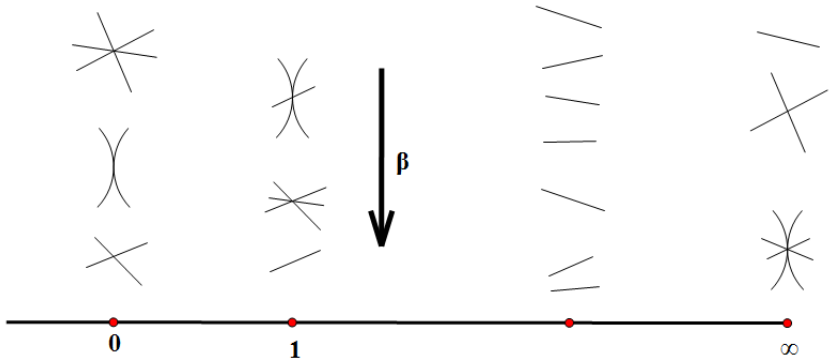
The points $c \in \mathbf{P}_1(\Bbbk)$ for which the number of c-preimages is non-standard, are called the *critical values* of f; the set of such points is denoted by

$$\mathrm{CritVal}(f) := \{c \in \mathbf{P}_1(\Bbbk) \mid \#f^{-1\circ}(c) \neq \deg f\}.$$

An alternative way of expressing the inclusion $c \in \mathrm{CritVal}(f)$ is saying that f *branches* over c.

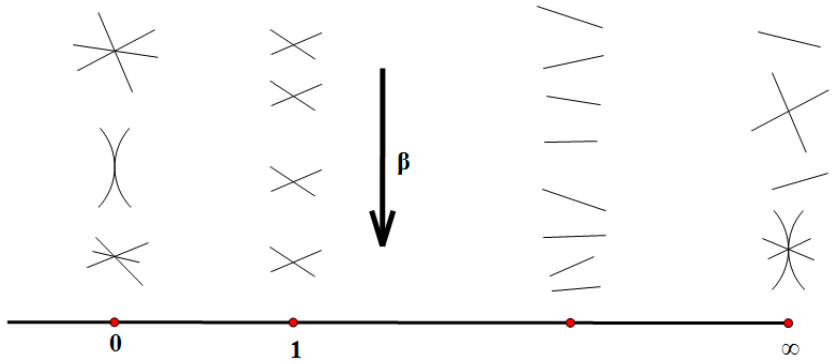
1.0. Definition. A *Belyi pair* is a pair $(\mathbf{X}, \beta)$, where $\mathbf{X}$ is a smooth irreducible curve over $\Bbbk$ and $\beta \in \Bbbk(\mathbf{X}) \setminus \Bbbk$ with $\mathrm{CritVal}(\beta) \subseteq \{\infty, 0, 1\}$. If $(\mathbf{X}, \beta)$ is a Belyi pair, then β is a *Belyi function* on $\mathbf{X}$.

In the picture below we are just trying to fix the *set-theoretical* behavior of a Belyi function – in particular, stressing the lack of ramification over a *generic* point in $\mathbf{P}_1(\Bbbk) \setminus \{0, 1, \infty\} \subseteq \mathbf{P}_1(\Bbbk) \setminus \mathrm{CritVal}(\beta)$.



According to the Belyi theorem ([1], [2]), over $\Bbbk = \mathbb{C}$ a curve $\mathbf{X}$ admits a Belyi function if and only if $\mathbf{X}$ is a *complexification*, i.e. obtained via a base change, of a curve $\mathbf{X_0}$, defined over $\overline{\mathbb{Q}}$. However, finding a Belyi function on an arbitrary curve over $\overline{\mathbb{Q}}$ is a very difficult task, and the minimal possible degree of such a function can be tremendous, see [14]. The only thing we can estimate, as it will be reminded in the next section, is the *total number of Belyi pairs of bounded degree*.

1.1. Cleanness. A Belyi pair $(\mathbf{X}, \beta)$ is called *clean*, if all the branchings over $1 \in \mathbf{P_1}(\Bbbk)$ are twofold:



The formal definition uses the standard concepts: for a point $P \in \mathbf{X}$ denote its *local ring* $\mathcal{O}_P := \{f \in \Bbbk(\mathbf{X}) \mid \mathbf{f(P)} \neq \infty\}$ with the maximal ideal $\mathfrak{m}_P := \{f \in \Bbbk(\mathbf{X}) \mid \mathbf{f(P)} = \mathbf{0}\}$. The cleanness of β means

$$\beta - 1 \in \mathfrak{m}_P^2 \setminus \mathfrak{m}_P^3$$

at all points P with $\beta(P) = 1$. Imposing the cleanness condition is not a severe one – see below.

1.2. Examples. We give a couple of series of the simplest ones.

Generalized Fermat curves are defined by the affine equation

$$x^m + y^n = 1.$$

Under some restrictions on the char($\Bbbk$)

$$\beta := x^m = 1 - y^n$$

is a Belyi function on a generalized Fermat curve, usually not a clean one.

The concept of a curve *with many automorphisms* has two versions: in the zero and the positive characteristic of the ground field – in the latter case the cardinality of the automorphism group is *quartic* in genus (unlike the former case where the Hurwitz bound $\#\mathrm{Aut}\mathbf{X} \leq 84(g_{\mathbf{X}} - 1)$ holds). In many cases the factorization map

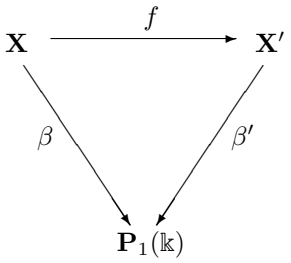
$$\beta : \mathbf{X} \longrightarrow \frac{\mathbf{X}}{\mathrm{Aut}\mathbf{X}}$$

is a Belyi function. One should be careful in the case of positive characteristic, since the factorization map is often non-separable.

A detailed treatment of the *Klein quartic* can be found in [13], and that of the Bring curve – in [28].

1.3. Two categories of Belyi pairs. The objects of the category $\mathcal{BELP}(\Bbbk)$ are *Belyi pairs* $(\mathbf{X}, \beta)$ over $\Bbbk$ as defined above. A morphism in

$\mathcal{BELP}(\Bbbk)$ from $(\mathbf{X}, \beta)$ to $(\mathbf{X}', \beta')$ is defined as such a morphism $f : \mathbf{X} \to \mathbf{X}'$ of curves that the diagram



commutes.

The category $\mathcal{BELP}_2(\Bbbk)$ is a full subcategory of $\mathcal{BELP}(\Bbbk)$ consisting of the *clean* Belyi pairs.

1.4. Cleaning functor. Suppose that $\mathrm{char}(\Bbbk) \neq 2$. Then the introduced categories are close enough: it is easy to check that the functor

$$\mathcal{BP}(\Bbbk) \to \mathcal{BP}_2(\Bbbk) : (\mathbf{X}, \beta) \mapsto (\mathbf{X}, \mathbf{4}\beta(\mathbf{1} - \beta))$$

is well-defined. Thus the problems of counting the objects of bounded complexity in both categories are basically equivalent.

1.5. Fields of definition and Galois orbits. In the above-mentioned case $\Bbbk = \overline{\Bbbk_0}$ denote

$$\Gamma := \mathrm{Gal}(\Bbbk/\Bbbk_0)$$

the corresponding Galois group. Then the action

$$\Gamma : \mathcal{BP}(\Bbbk)$$

is defined: take any standard model of $\Bbbk(\mathbf{X})$ – planar with the simplest singularities, or tri-canonical, or whatsoever, – and apply the elements of Γ coefficientwise to the equations of the curve and to the Belyi function on it. Since a Belyi pair is defined by the finite set of elements, algebraic over $\Bbbk_0$, all the Γ-orbits thus defined are finite. Therefore for each $(\mathbf{X}, \beta) \in \mathcal{BP}(\Bbbk)$ we have a stationary subgroup of Γ of finite index

$$(\mathbf{X}, \beta) \leftrightarrow \Gamma_{(\mathbf{X},\beta)}$$

and by Galois theory

$$(\mathbf{X}, \beta) \leftrightarrow \Gamma_{(\mathbf{X},\beta)} \leftrightarrow \mathbb{F}_{(\mathbf{X},\beta)},$$

where the last field satisfies $\Bbbk_0 \subseteq \mathbb{F}_{(\mathbf{X},\beta)} \subset \Bbbk$. We call this field the *field of definition*[1] of a Belyi pair $(\mathbf{X}, \beta)$. Tautologically

$$\#(\Gamma \cdot (\mathbf{X}, \beta)) = (\Gamma : \Gamma_{(\mathbf{X},\beta)}) = (\mathbb{F}_{(\mathbf{X},\beta)} : \Bbbk_0).$$

If a Belyi pair $(\mathbf{X}, \beta)$ can be defined over some finite extension $\mathbb{K} \supseteq \Bbbk_0$ (i.e., there exists a model of $\mathbf{X}$ over $\mathbb{K}$ with the coefficients of β belonging to $\mathbb{K}$), then it is obviously true that $\mathbb{F}_{(\mathbf{X},\beta)} \subseteq \mathbb{K}$. However, it can happen that a Belyi pair $(\mathbf{X}, \beta)$ can <u>not</u> be defined over its field of definition; the obstruction lies in some non-commutative Galois cohomology set, see [4] or [7] for the case $\Bbbk_0 = \mathbb{Q}$. The author is unaware of similar examples over $\Bbbk_0 = \mathbb{F}_p$.

1.6. Passports and their realizations. The main invariant of a Belyi pair is the set of multiplicities:

$$\operatorname{div}(\beta) = a_1 A_1 + \cdots + a_\alpha A_\alpha - c_1 C_1 - \cdots - c_N C_N,$$

$$\operatorname{div}(\beta - 1) = b_1 B_1 + \cdots + b_n B_n - c_1 C_1 - \cdots - c_N C_N.$$

We collect them in a table called the *passport* of a Belyi pair:

$$\operatorname{pass}(\mathbf{X}, \beta) := \begin{pmatrix} a_1 & b_1 & c_1 \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ a_\alpha & b_n & c_N \end{pmatrix}$$

Lemma 1. *For any passport of a Belyi pair* $(\mathbf{X}, \beta)$

$$a_1 + ... + a_\alpha = b_1 + ... + b_n = c_1 + ... + c_N =: d. \tag{1a}$$

The genus g *of* $\mathbf{X}$ *can be defined by the equality*

$$\alpha + n + N =: d + 2 - 2g. \tag{1b}$$

Proof. For (1a) we define $d := \deg \beta$ and use the well-known property of the degree of a branched covering. To establish (1b) note that, according to the definition of Belyi function

$$\operatorname{div}(\mathrm{d}\beta) = \sum_{i=1}^{\alpha} (a_i - 1) A_i + \sum_{j=1}^{n} (b_j - 1) B_j - \sum_{k=1}^{N} (c_k + 1) C_k$$

for some points $A_1, \ldots, C_N \in \mathbf{X}$, and use $\deg(\mathrm{d}\beta) = 2g - 2$. □

Denote the *set of realizations of a passport* Π*, satisfying the above conditions* (1a) *and* (1b),

---

[1] it is often called the *field of moduli*, but we are going to use the word *moduli* in its traditional algebro-geometrical sense.

$$\mathcal{R}_{\mathit{\Pi}}(\Bbbk) := \frac{\{(\mathbf{X},\beta) \in \mathcal{BP}(\Bbbk) \mid \mathrm{pass}(\mathbf{X},\beta) = \mathit{\Pi}\}}{\text{isomorphism}}.$$

This definition makes sense since the categories $\mathcal{BP}(\Bbbk)$ are equivalent to the small ones.

Theorem 1. *For any algebraically closed field $\Bbbk$ and any passport $\mathit{\Pi}$, satisfying the above conditions* (1a) *and* (1b)*, the set $\mathcal{R}_{\mathit{\Pi}}(\Bbbk)$ is finite.*

Idea of the proof The set $\mathcal{R}_{\mathit{\Pi}}(\Bbbk)$ is in a natural bijective correspondence with the corresponding 0-dimensional subscheme of the moduli space $\mathcal{M}_g(\Bbbk)$, where g is defined by (1b). The detailed proof will appear elsewhere. □

So the basic counting question is to study the cardinalities of these sets:

$$\boxed{\#\mathcal{R}_{\mathit{\Pi}}(\Bbbk) = ???}$$

We don't have a complete answer even in the case $\Bbbk = \mathbb{C}$; however, see the discussion below.

As the following simple example shows, this cardinality can depend on the field:

$$\mathcal{R}_{(333)}(\overline{\mathbb{Q}}) = (y^2 = 1 - x^3, \beta = \frac{y+1}{2}),$$

while

$$\mathcal{R}_{(333)}(\overline{\mathbb{F}_3}) = \varnothing.$$

Finally, the general behavior of $\#\mathcal{R}_{\mathit{\Pi}}(\Bbbk)$'s can be studied in the Galois-theoretic terms.

Lemma 2. *For any Belyi pair $(\mathbf{X},\beta)$*

$$\mathit{\Gamma} \cdot (\mathbf{X},\beta) \subseteq \mathcal{R}_{pass(\mathbf{X},\beta)}$$

Proof. Indeed, the entries of the passports are Galois-invariant since they consist of the multiplicities of c-points of Belyi functions for the Galois-invariant points of $\mathbf{P_1}(\Bbbk)$. □

This obvious fact should be taken into account together with the following

Observation. *"Generically" $\mathit{\Gamma} \cdot (\mathbf{X},\beta) = \mathcal{R}_{\mathrm{pass}(\mathbf{X},\beta)}$*

Of course, this equality holds only in the absence of more subtle Galois-invariants – non-trivial automorphisms and others.

2 Dessins

This section is devoted to the objects whose relation with the objects studied in the previous one are far from obvious. This relation has been basically

discovered by Alexander Grothendieck, see [12], and many papers and several books s were devoted to it. The books [17] and [10] are addressed to the beginners; however, we are going to use the different basic concepts, and the reason for it will be explained soon.

2.0. The category of Grothendieck dessins. The objects of the category $\mathcal{DESS}$ are *dessins d'enfant* in the sense of [12], i.e. such triples of topological spaces

$$\mathrm{X}_0 \subset \mathrm{X}_1 \subset \mathrm{X}_2,$$

that X_0 is a non-empty finite set, whose elements are called *vertices*, X_2 is a compact connected orient*ed* surface and X_1 is an *embedded graph*, which means that the complement $\mathrm{X}_1 \setminus \mathrm{X}_0$ is homeomorphic to a disjoint union of real intervals, called *edges*. We demand as well that the complement $\mathrm{X}_2 \setminus \mathrm{X}_1$ is homeomorphic to a disjoint union of open discs, called *faces*. The difference between dessins and *two-dimensional cell complexes* lies in the concepts of *morphisms*.

In order to give a short definition of morphisms in $\mathcal{DESS}$, we add $\mathrm{X}_{-1} = \varnothing$ to each triple as above and call a continuous mapping of surfaces *admissible*, if it respects the orientation, is *open*[2] and respects the differences, i.e. such a mapping of triples $f : (\mathrm{X}_2, \mathrm{X}_1, \mathrm{X}_0) \to (\mathrm{Y}_2, \mathrm{Y}_1, \mathrm{Y}_0)$ should satisfy

$$f(\mathrm{X}_i \setminus \mathrm{X}_j) \subseteq \mathrm{Y}_i \setminus \mathrm{Y}_j$$

for $-1 \leq j < i \leq 3$. The two admissible mappings are called *admissibly equivalent*, if they are homotopic in the class of admissible mappings, and the morphisms in $\mathcal{DESS}$ are defined as classes of admissible equivalence of admissible mappings.

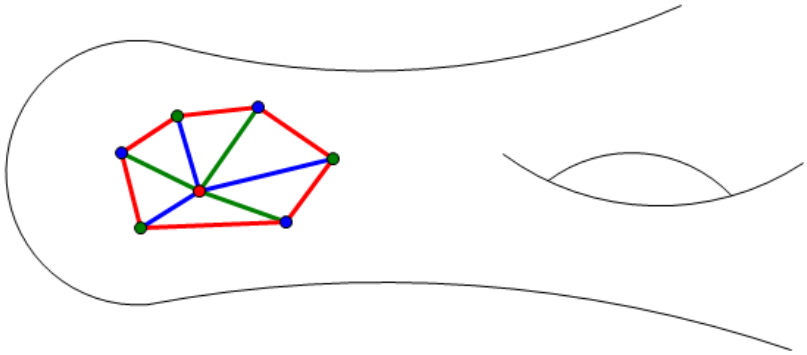
2.1 The category of colored triangulations. The objects of the category $\mathcal{DESS}_3$ are the *tricolored* dessins, i.e. the dessins $\mathrm{X}_0 \subset \mathrm{X}_1 \subset \mathrm{X}_2$ endowed with a *coloring mapping*

$$\mathrm{col}_3 : X_1 \longrightarrow \{blue, green, red\},$$

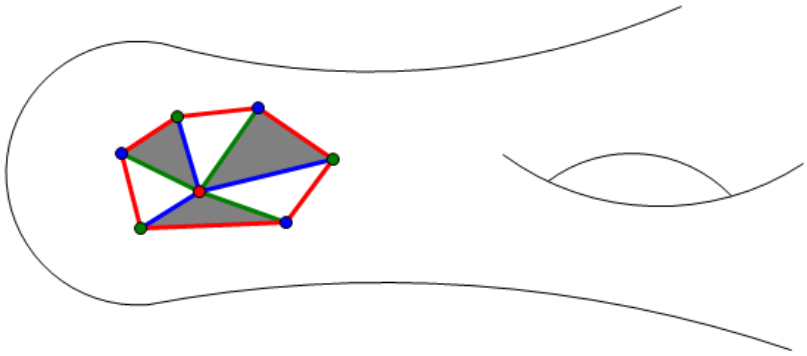
constant on the edges. It is demanded that

(0) any vertex is incident to edges of only <u>two</u> colors;
(1) any edge has <u>two</u> vertices in its closure;
(2) any face has <u>three</u> edges in its closure, colored pairwise differently.

[2] according to the somewhat forgotten theory, developed by S. Stoilow, any open mapping of Riemann surfaces is locally topologically conjugated to a holomorphic one, see [26].



Taking into account the assumption **(0)**, we color every vertex by the (only remaining) color, that is different from the colors of incident edges. Due to the assumption **(2)** the connected components of $X_2 \setminus X_1$ will be called (topological) *triangles*. It can be deduced from the *orientability* of X_2 that these triangles can also be colored, now in *black* and *white*, in such a way that the *neighboring* triangles – i.e., having a common edge – will be colored differently.



So the coloring mapping col_3 can be extended to

$$\mathrm{col}_5 : X_2 \longrightarrow \{black, blue, green, red, white\},$$

with exactly two choices of black/white coloring, corresponding to the orientations of X_2. We agree that the positive-counter-clockwise orientation of the white triangles corresponds to the *blue-green-red-blue* cyclic order of the colors of edges in its closure; this choice will be motivated below.

The objects of $\mathcal{DESS}_3$ will be called *colored triangulations*; we note, however, that there is precisely one object of this category, that is not a triangulation of a surface in the usual sense; this object is formed by a pair of black and white triangles with colored edges after identifying edges with the same color.

The morphisms in $\mathcal{DESS}_3$ are defined in the same way as in $\mathcal{DESS}$ with the additional assumption of *color-respecting*[3].

The theory is fundamentally symmetric with respect to the three colors involved; this is the reason why the traditional approach, developed in [17] and [10], where two of them are distinguished, does not satisfy us completely.

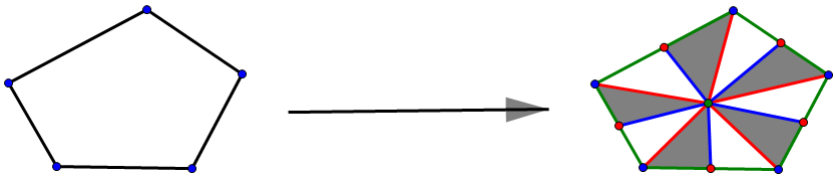
2.2. Relations between two types of dessins. There is an obvious color-forgetting functor

$$\mathcal{DESS}_3 \longrightarrow \mathcal{DESS}.$$

In the other direction there is a non-trivial one

$$\mathcal{DESS} \hookrightarrow \mathcal{DESS}_3,$$

which we introduce by the picture:



2.3. Counting dessins. For several decades the powerful "physical" methods are used in the study of the quantities of dessins of bounded complexity; the corresponding key words are *matrix integrals* and *map enumeration*. The progress is still impressive. E.g., recently the generating function for the weighted[4] quantities of dessins with the prescribed set of degrees of 2-valencies has been (in a certain sense) written down – see [16].

However, the quantities of dessins with prescribed sets of both 0- and 2-valencies are still out of reach. As it will follow from the results of the next section, this problem is equivalent to counting Belyi pairs over $\mathbb{C}$ with a prescribed passport.

3 Correspondence between Belyi pairs and dessins

In this section we work over $\Bbbk = \mathbb{C}$.

3.0. The functor "draw". We define the functor

$$\mathbf{draw} : \mathcal{BELP}_2(\mathbb{C}) \longrightarrow \mathcal{DESS}.$$

---

[3] The "same" category was considered in [15] under the name *oriented hypermaps*; our vertexes of three colors were called *hypervertices, hyperedges* and *hyperfaces*.

[4] a dessin D is counted with the weight $\frac{1}{\#\mathrm{Aut}\, D}$

To a clean Belyi pair $(\mathbf{X}, \beta) \in \mathcal{BELP}_2(\mathbb{C})$ a dessin d'enfant with

$$X_2 := \mathbf{top}(\mathbf{X})$$

is assigned; here **top** means the forgetful functor that assigns to a complex algebraic curve (= Riemann surface) the underlying topological oriented surface.

Next define

$$X_1 := \beta^{-1\circ}([0,1]) \text{ and } X_0 := \beta^{-1\circ}(\{0\}).$$

The branching condition imposed on β over 1 implies that while $P \in X_2$ moves along some edge (a connected component of $X_1 \setminus X_0$) from one vertex (an element of X_0) to another, the point $\beta(P)$ moves from 0 to 1 and back, the edge being *folded* in the point of $\beta^{-1\circ}(1)$; a local coordinate z centered at this point can be chosen so that $\beta = 1 + z^2$ in its domain.

A morphism of Belyi pairs obviously defines the corresponding morphism of dessins.

Theorem 2. *The functor* **draw** *defines the equivalence of the categories* $\mathcal{BELP}_2(\mathbb{C})$ *and* $\mathcal{DESS}$.

A detailed proof can be found in [22].

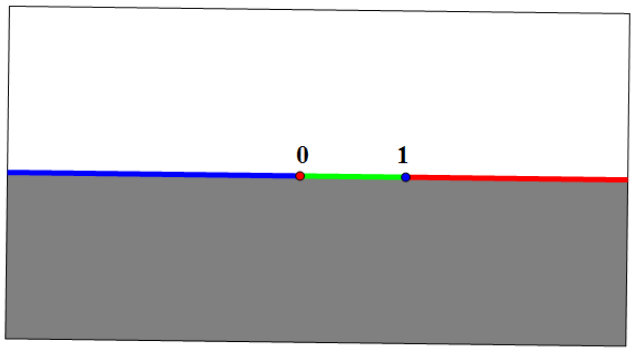
3.1. The functor "paint". In order to define the functor

$$\mathbf{paint} : \mathcal{BELP}(\mathbb{C}) \longrightarrow \mathcal{DESS}_3;$$

we introduce the *Belyi sphere* $\mathbf{P}_1(\mathbb{C})^{\mathsf{Bel}}$ which is the *colored Riemann sphere* $\mathbf{P}_1(\mathbb{C})$. Decomposing $\mathbf{P}_1(\mathbb{C}) = \mathbb{C} \coprod \{\infty\}$, we define this coloring as

$$\mathrm{col}_5^{\mathsf{Bel}} : \mathbf{P}_1(\mathbb{C}) \longrightarrow \{black, blue, green, red, white\} :$$

$$z \mapsto \begin{cases} black \text{ if } z \in \mathbb{C} \setminus \mathbb{R} \text{ and } \Im z < 0, \\ white \text{ if } z \in \mathbb{C} \setminus \mathbb{R} \text{ and } \Im z > 0, \\ blue \text{ if } z \in \mathbb{R}_{<0} \text{ or } z = 1, \\ green \text{ if } z \in (0,1) \text{ or } z = \infty, \\ red \text{ if } z \in \mathbb{R}_{>1} \text{ or } z = 0. \end{cases}$$



The choice of the colors is motivated as follows. The *black* and *white* for the lower and the upper parts is quite traditional (hell and heaven...), while the real line is colored in such a way that *blue* (symbolizing *cold*) corresponds to negative numbers, while *red* (symbolizing *hot*) corresponds to positive ones. The *green* is just in between and is assigned no meaningful association. The vertices of the colored topological "triangle" $\mathbf{P}_1(\mathbb{R})$ have the same color as the opposite side.

Furthermore, the colors of the pieces of the real line occur in the *alphabetical* order. The motivation of the choice of "colored" orientation can be given now: the traditional counter-clockwise detour around the white triangle correspond to moving along the real line form $-\infty$ to ∞.

Now we can finalize the definition of the functor **paint**: for a Belyi pair $(\mathbf{X}, \beta)$ the surface $X_2 := \mathbf{top}(\mathbf{X})$ is colored by $\mathrm{col}_5 := \beta^* \mathrm{col}_5^{\mathsf{Bel}}$, i.e. the points of the surface are colored according to the colors of their images under the Belyi mapping: for any $P \in X_2$

$$\mathrm{col}_5(P) := \mathrm{col}_5^{\mathsf{Bel}}(\beta(P)).$$

Obviously, the set X_1 turns out to be the closure of the union of the green edges and X_0 the set of isolated red points.

Theorem 3. *The functor* **paint** *defines the equivalence of the categories* $\mathcal{BELP}(\mathbb{C})$ *and* $\mathcal{DESS}_3$.

A detailed proof can be found in [22].

3.2. Implications of Belyi theorem. According to the above-quoted theorem, the category inclusion

$$\mathcal{BP}_2(\overline{\mathbb{Q}}) \overset{\sim}{\hookrightarrow} \mathcal{BP}_2(\mathbb{C})$$

is *a* category equivalence. We emphasize that it is not canonical: introduce the *absolute Galois group*

$$\mathbb{\Gamma} := \mathrm{Aut}(\overline{\mathbb{Q}})$$

and note that the inclusion $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ is defined only up to the $\mathbb{\Gamma}$-action.

According to the previously formulated results, we have the $\mathbb{\Gamma}$-set of category equivalences

$$\boxed{\mathcal{BP}_2(\overline{\mathbb{Q}}) \overset{\simeq}{\longleftrightarrow} \mathcal{DESS}}$$

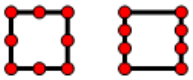
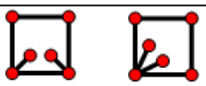
and, as we have just seen, it has some invariant meaning only being considered together with the enigmatic action of $\mathbb{\Gamma}$ on $\mathcal{DESS}$.

So the true arithmetic meaning can be given not to individual dessins, but only to their $\mathbb{\Gamma}$-orbits.

4 Belyi pairs over finite fields

The theory is in its infancy. However, it is inevitable, and we start this last section with the demonstration of the occurrence of Belyi pairs over $\mathbb{F}_p$'s in the course of the constructive realization of the equivalence $\mathcal{BP}_2(\overline{\mathbb{Q}}) \overset{\simeq}{\longleftrightarrow} \mathcal{DESS}$.

4.0. Example. The Belyi pairs, corresponding to the clean unicellular 4-edged toric dessins, were calculated in [23]. In the course of calculations it was impossible to ignore the flows of powers of small primes in the denominators. It turned out that in all the cases these primes have the invariant meaning: they are the *bad primes* of the corresponding elliptic curves, see [25]. The results are summarized in the following table.

Dessins	Bad primes
	2,3
	2
	2,3
	3,7
	2,5,7
	3
	2,3,7

Here all the toric dessins are drawn either in the square or in the hexagon; it is meant that the opposite sides are identified. They are grouped in the raws according to the sets of valencies; these raws constitute the Galois orbits, except the two cases (in the second and the penultimate raws) where the Galois orbits are split due to the obvious symmetries.

In most cases the bad primes have an obvious combinatorial meaning; they divide one of the valencies. However, the occurrence of 7 can not be explained this way. Instead we see the *sum of valencies* phenomenon: the badness of 7 is explained by $7 = 2 + 5$ and $7 = 3 + 4$. The similar phenomenon in the case of plane trees was explained by the author's students [27] and [20].

4.1. Good and bad primes. This subsection is written in a somewhat informal style, since some details of the corresponding concepts have not yet been written up (however, see [11]).

If for a Belyi pair $(\mathbf{X}, \beta)$ over $\overline{\mathbb{Q}}$ both the equations of $\mathbf{X}$ and the coefficients of β can be chosen in a finite extension $\mathbb{K} \supseteq \mathbb{Q}$, such a field $\mathbb{K}$ is called a *field of realization* of $(\mathbf{X}, \beta)$. Let $\mathcal{O}$ be the *ring of integers* of $\mathbb{K}$; it is clear that $(\mathbf{X}, \beta)$ then can be *realized* over $\mathcal{O}$ (nobody claims any kind of *uniqueness* of such a realization).

Given a nonzero prime ideal $\mathfrak{p} \lhd \mathcal{O}$, we can construct the pair $(\mathbf{X}, \beta) \mod \mathfrak{p}$ over the algebraic closure of the finite field $\frac{\mathcal{O}}{\mathfrak{p}}$. If the curve $\mathbf{X} \mod \mathfrak{p}$ is smooth (or, equivalently, has the same genus as $\mathbf{X}$) and $\deg(\beta \mod \mathfrak{p}) = \deg(\beta)$ then $\mathbb{K}$, a model and $\mathfrak{p}$ are called *good* for $(\mathbf{X}, \beta)$. A prime p is called *good* for $(\mathbf{X}, \beta)$, if such a good choice exists with $\operatorname{char}\left(\frac{\mathcal{O}}{\mathfrak{p}}\right) = p$. Otherwise p is *bad* for $(\mathbf{X}, \beta)$.

For a dessin D denote $(\mathbf{X}_D, \beta_D)$ the corresponding Belyi pair over $\overline{\mathbb{Q}}$ and introduce the *set of primes of bad reduction*

$$\operatorname{bad}_D := \{p \in \{2, 3, 5, \dots\} \mid p \text{ is bad for } (\mathbf{X_D}, \beta_\mathbf{D})\}.$$

As for many other objects of arithmetic geometry, all the sets bad_D are *finite*.

In the previous subsection the sets of bad primes were presented without any attempts of precise definitions; the reason is that in the case of genus 1 the prime is bad if and only if it divides the *discriminant* of the curve.

It is an outstanding problem

to define the sets bad_D in terms of the combinatorics of D.

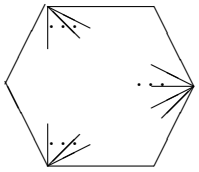
4.2. Counting. The author is currently unaware of the passports that are realizable over $\overline{\mathbb{F}_p}$ but not realizable over $\mathbb{C}$. Hence typically

$$\#\mathcal{R}_{\Pi}(\mathbb{F}_p) \leq \#\mathcal{R}_{\Pi}(\mathbb{C}),$$

and the inequality often becomes strict due to the bad reduction.

The numbers of bad reductions often behave systematically in *families* of dessins. Unfortunately, a mathematical definition of a family of dessins (similar, say, to the definition of a family of algebraic varieties) hardly exists, so we just consider an example.

The passports $\begin{pmatrix} n\ n & 3 \\ & 1 \\ & \dots \\ & 1 \end{pmatrix}$ with natural $n \geq 3$ correspond to the unicellular toric dessins



(the opposite sides identified). In terms of [5] these are the dessins whose *pruning* is a *toric hexagon*, defined by the passport (333).

Now, using the notation $\#\#\mathcal{Z} := \sum_{z\in\mathcal{Z}} \frac{1}{\#\mathrm{Aut}z}$ for the weighted sum, introduce for a field $\Bbbk$

$$\mathrm{Hex}_n(\Bbbk) := \#\#\mathcal{R}\begin{pmatrix} n\ n & 3 \\ & 1 \\ & \dots \\ & 1 \end{pmatrix}(\Bbbk),$$

and give the promised example:

$$\mathrm{Hex}_n(\mathbb{C}) - \mathrm{Hex}_n(\overline{\mathbb{F}_{\mathrm{l}}}) = \sum_{0<k<\frac{n}{p}} (n-kp).$$

The proof can be found in [21]. The summing of the arithmetic progression in the right-hand side has not been performed in order to emphasize the nature of the bad reduction which is explained in terms of geometry of the modular curves.

4.3. On the cohomology of moduli spaces. The geometry of moduli spaces $\mathcal{M}_{g,N}$ of $N-$pointed curves of genus g is related to dessins in more than one way. The famous decomposition (constructed by Mumford, Harer, Penner, Witten and others)

$$\mathcal{M}_{g,N}(\mathbb{C}) \simeq \coprod_{D\in\mathbf{DESS}_{g,N}} \mathbb{R}_{>0}^{\mathrm{E}(D)},$$

where $\mathbf{DESS}_{g,N}$ stands for the set of isomorphism classes of N-cellular dessins of genus g with all the 0-valencies ≥ 3 and $\mathrm{E}(D)$ is the set of edges of a dessin D, provides a direct way to the singular cohomology of $\mathcal{M}_{g,N}(\mathbb{C})$. In the case $(g,N)=(2,1)$ this approach (modified a bit for a level-3 smooth cover) was realized in [6].

In [18] it was shown that replacing $\mathbb{R}_{>0}$ be $\mathbb{N}$ (i.e. considering ribbon graphs with only integer edge lengths) results in replacing $\mathbb{C}$ by $\overline{\mathbb{Q}}$, so more "arithmetic" cohomology theories become available. The Witten-Kontsevich

integrals then are replaced by counting the integral points in the polytopes, the perfect techniques for which was developed in [19].

The methods of calculating cohomology of moduli spaces by *counting curves* over finite fields, i.e. determining $\#\mathcal{M}_{g,N}(\mathbb{F}_{p^r})$, are based on the (now proved) Weil conjectures. The applications of these methods can be found for example in [3].

Since counting Belyi pairs is closely related to counting curves and counting dessins (together with the principles of bad reduction, the first steps of understanding which were mentioned above), there is a fundamental hope of blending all these approaches.

References

1. Belyi, G.V.: Galois extensions of a maximal cyclotomic fields. Mathematics of the USSR Izvestiya **14**, no.2, 247-256 (1980)
2. Belyi, G.V.: A new proof of the three-point theorem. Mathem. Sb. **193**, no.3, 21-24 (2002)
3. Bergstrom J., Tommasi O.: The rational cohomology of $\mathcal{M}_4$. Math. Ann. **338** (1), 207-239 (2007)
4. Couveignes, J.-M.: Calcul et rationalité de fonctions de Belyi en genre 0. Annales de l'institut Fourier **44**.1, 1-38 (1994)
5. Do, N., Norbury, P.: Pruned Hurwitz numbers. arXiv:1312.7516 [math.GT] (2013)
6. Dunin-Barkowski, P., Popolitov, A., Shabat, G., Sleptsov, A.: On the homology of certain smooth covers of moduli spaces of algebraic curves. Differential Geometry and its Applications **40**, 86-102 (2015)
7. Filimonenkov, V.O., Shabat, G.B.: Fields of definition of rational functions of one variable with three critical values. Fundam. Prikl. Mat. **1**:3, 781-799 (1995)
8. Frenkel, E.: Lectures on the Langlands Program and Conformal Field Theory. Les Houches (2005)
9. Gannon, T.: Moonshine beyond the Monster: The Bridge Connecting Algebra. Modular Forms and Physics, CUP (2006)
10. Girondo, E., Gonzalez-Diez, G.: Introduction to Compact Riemann Surfaces and Dessins d'Enfants. London Mathematical Society Student Texts (2012)
11. Goldring, W.: Unifying Themes Suggested by Belyi's Theorem. Number Theory, Analysis and Geometry (Serge Lang Memorial Volume), pp. 181-214. Springer-Verlag (2011)
12. Grothendieck, A.: Esquisse d'un Programme. Unpublished manuscript (1984), english translation by P. Lochak and L. Schneps in Geometric Galois actions, vol. 1, London Math. Soc. Lecture Note Ser. vol. 242, pp. 5-48. Cambridge Univ. Press, Cambridge (1997)
13. Elkies, N.D.: The Klein quartic in number theory. In "The Eightfold Way: The Beauty of Klein's Quartic Curve", pp.51-102, Cambridge Univ. Press (1999)
14. Javanpeykar, A., Bruin, P.: Polynomial bounds for Arakelov invariants of Belyi curves. Algebra and Number Theory **8** no.1, 89-140 (2014)
15. Jones, G., Singerman D.: Maps, hypermaps and triangle groups. The Grothendieck Theory of Dessins d'Enfant, London Math. Soc. Lecture Notes **200**, pp.115-146, Cambridge Univ. Press (1994)
16. Kazarian, M., Zograf, P.: Virasoro constraints and topological recursion for Grothendieck's dessin counting. Lett. Math. Phys. **105**:8, 1057-1084 (2015)

17. Lando, S., Zvonkin, A.: Graphs on Surfaces and Their Applications. Springer-Verlag (2004)
18. Mulase, M., Penkava, M.: Ribbon Graphs, Quadratic Differentials on Riemann Surfaces, and Algebraic Curves Defined over $\overline{\mathbb{Q}}$. Asian Journal of Mathematics **2** (4), 875-920 (1998)
19. Norbury, P.: Counting lattice points in the moduli space of curves. Math. Res. Lett. **17**, 467-481 (2010)
20. Oganesyan, D.: Zolotarev polynomials and reduction of Shabat polynomials into a positive characteristic. Moscow University Mathematics Bulletin **71** (6), 248-252 (2016)
21. Oganesyan, D.: Abel pairs and modular curves. Zap. Nauchn. Sem. POMI **446**, 165-181 (2016)
22. Shabat, G.: Combinatorial-topological methods in the theory of algebraic curves. Theses, Lomonosov Moscow State University (1998)
23. Shabat, G.B.: Unicellular four-edged toric dessins. Fundamentalnaya i prikladnaya matematika **18** no.6, pp.209-222 (2013)
24. Shabat, G.B., Voevodsky, V.A.: Drawing curves over number fields. P. Cartier, L. Illusie, N. Katz, G. Laumon, Y. Manin, K. Ribet (Eds.), The Grothendieck Festschrift (5th ed.) vol.3, Birkhauser, Basel, pp.199-227 (1990)
25. Silverman, J.H.: The Arithmetic of Elliptic Curves (2nd Edition). Graduate Texts in Mathematics **106**, Springer-Verlag (2009)
26. Stoilow, S.: Leçons sur les principes topologiques de la théorie des fonctions analytiques. Gauthier-Villars, Paris (1956)
27. Vashevnik, A.M.: Prime numbers of bad reduction for dessins of genus 0. J. Math. Sci. **142** 2, 1883-1894 (2007)
28. Weber, M.: Kepler's small stellated dodecahedron as a Riemann surface. Pacific J. Math. **220**, 167-182 (2005)