Fibrations of $K3$-surfaces and Belyi-maps

F.Beukers and H.Montanus

December 19, 2006

1 Introduction

In a paper by Miranda and Persson [MP89], the authors study semi-stable elliptic fibrations over $\mathbb{P}^1$ of K3-surfaces with 6 singular fibres. In their paper the authors give a list of possible fiber types for such fibrations. It turns out that there are 112 cases. The corresponding J-invariant is a so-called Belyi-function. More particularly, J is a rational function of degree 24, it ramifies of order 3 in every point above 0, it ramifies of order 2 in every point above 1, and the only other ramification occurs above infinity. To every such map we can associate a so-called 'dessin d'enfant' (a name coined by Grothendieck) which in its turn uniquely determines the Belyi map. If $f : C \to \mathbb{P}^1$ is a Belyi map, the dessin is the inverse image under f of the real segment [0,1].
Several papers, e.g. [Ir03],[Schu04], [TY04], have been devoted to the calculation of some of the rational J-invariants for the Miranda-Persson list. It turns out that explicit calculations quickly become too cumbersome (even for a computer) if one is not careful enough. The goal of this paper is to compute all J-invariants corresponding to the Miranda-Persson list. We use a trick which enables us to reduce the calculation to the solution of a set of three polynomial equations in three unknowns (see Section 7 for details). The results can be found on the website

`http://www.math.uu.nl/people/beukers/mirandapersson/Dessins.html`

On that website, an entry like 14-3-2-2-2-1 means that one finds there all dessins of J-functions with ramification orders 14,3,2,2,2,1 above infinity. Alternatively one can say that the special elliptic fibers are of type I_n with $n = 14, 3, 2, 2, 2, 1$. If to a partition there corresponds only one picture, this means that J is a rational function with coefficients in $\mathbb{Q}$. If there are several pictures, the corresponding fields of definition are indicated. On this website one also finds the explicit J-invariants.
Besides giving the computation of explicit formulas for the Miranda-Persson list this paper also contains a brief introduction to Belyi maps and dessins d'enfant.

2 Dessins d'enfant

Let X be a smooth algebraic curve and $\phi : X \to \mathbb{P}^1$ a non-constant rational function, which can be considered as a morphism of curves. A point $P \in X$ is called a *point of ramification* if $d\phi(P) = 0$. The image under ϕ of the ramification points is called the *branched set*. Let S be a finite subset of $\mathbb{P}^1$. We say that ϕ is *unramified outside* S if the branched set is contained in S. We have the following theorem.

Theorem 2.1 (Weil) *Let X be a smooth algebraic curve defined over $\mathbb{C}$ and $\phi : X \to \mathbb{P}^1$ a non-constant rational map. Suppose the ramification set of ϕ is contained in $\mathbb{P}^1(\overline{\mathbb{Q}})$. Then both X and ϕ can be defined over $\overline{\mathbb{Q}}$.*

The following remarkable theorem is crucial to the story of dessins d'enfant.

Theorem 2.2 (Belyi) *Let X be an algebraic curve defined over $\overline{\mathbb{Q}}$. Then there exists a non-constant rational map $\phi : X \to \mathbb{P}^1$ which is unramified outside $\{0, 1, \infty\}$.*

See [Be79] for a proof. Together with the previous theorem, this theorem characterises algebraic curves defined over $\overline{\mathbb{Q}}$ as algebraic curves that allow a rational map to $\mathbb{P}^1$ unramified outside $\{0, 1, \infty\}$. In other words, we have a geometric characterisation for curves defined over $\overline{\mathbb{Q}}$.
A pair (X, ϕ), where X is a smooth algebraic curve and $\phi : X \to \mathbb{P}^1$ a non-constant morphsim unramified outside $\{0, 1, \infty\}$, is called a *Belyi pair*. Two Belyi pairs (X, ϕ) and (X', ϕ') are considered equivalent if there is an isomorphism $\sigma : X \to X'$ such that $\phi' = \phi \circ \sigma$. From now on, when we speak of Belyi pairs, we mean their equivalence class.
The other surprise, due to an observation of Grothendieck, is that the geometrical criterion can be turned into a purely combinatorial description. To this end we shall use connected, bi-colored, oriented graphs.

1. A graph is called *connected* if every vertex is connected to any other vertex via a sequence of edges.

2. A graph is called *bi-colored* if every vertex is given one of two colors (say black and white) such that vertices of equal color are not connected by an edge.

3. A graph is called *oriented* if at every vertex there is a given cyclic ordering of the edges ending in the vertex.

A graph satisfying all three of properties above is called a *dessin d'enfant* or, shorter, *dessin*. Two dessins are considered equivalent if there exists a graph isomorphism between them preserving the bi-coloring and the ordering. From now on, when we speak of a dessin, we mean its equivalence class.
Before explaining the connection between Belyi pairs and dessins, we introduce two other categories of interest. An ordered triple of permutations $\sigma_0, \sigma_1, \sigma_\infty \in$

S_n, the group of permutations on $\{1, 2, \ldots, n\}$, is called a *permutation pair* if $\sigma_0\sigma_1\sigma_\infty = \mathrm{Id}$ and the group generated by σ_0, σ_1 acts transitively on $\{1, 2, \ldots, n\}$. Two permutation triples σ_i $(i = 0, 1, \infty)$ and σ'_i $(i = 0, 1, \infty)$ are considered equivalent if there exists $\tau \in S_n$ such that $\sigma'_i = \tau\sigma_i\tau^{-1}$ for $i = 0, 1, \infty$. From now on, we speak of a permutation pair, we mean its equivalence class.
Finally we consider finite extensions of $\overline{\mathbb{Q}}(z)$ unramified outside $0, 1, \infty$. Two such extensions K, K' are considered equivalent if there exists a field isomorphism $\psi : K \to K'$ fixing the subfield $\overline{\mathbb{Q}}(z)$. Again, we consider equivalence classes of such extensions.
Above we have defined four categories,

I) Belyi pairs (X, ϕ).

II) Dessins (d'enfant).

III) Permutation triples.

IV) Finite extensions of $\overline{\mathbb{Q}}(z)$.

We like to make these classes more refined by introducing the order n.

I(n) Belyi pairs (X, ϕ) where $\deg(\phi) = n$.

II(n) Dessins (d'enfant) with n edges.

III(n) Permutation triples in S_n.

IV(n) Finite extensions of $\overline{\mathbb{Q}}(z)$ of degree n, unramified outside $0, 1, \infty$.

We now give an explicit set of natural bijections $I(n) \to IV(n) \to III(n) \to II(n) \to I(n)$ whose composition is the identity map $I(n) \to I(n)$. The reader should verify that in each case the mapping is actually well defined on equivalence classes.

$I(n) \to IV(n)$. To a Belyi pair (X, ϕ) we associate the function field $\overline{\mathbb{Q}}(X)$ as an extension of $\overline{\mathbb{Q}}(\phi)$.

$IV(n) \to III(n)$. Let K be the degree n extension of $\overline{\mathbb{Q}}(z)$. Choose $y \in K$ such that $K = \overline{\mathbb{Q}}(z, y)$. Let $P(z, y)$ be the minial polynomial of y over $\overline{\mathbb{Q}}(z)$. For the following consideration we need to consider an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and then work over $\mathbb{C}$ with a monodromy argument.
Choose a point $z_0 \neq 0, 1, \infty$ and such that $P(z_0, y)$ is well defined and has n distinct zeros. Consider the n Taylor series solutions $y_1, y_2, \ldots, y_n$ of $P(z, y) = 0$ around z_0. Choose a closed path $\gamma_0 \in \pi_1(\mathbb{C} \setminus \{0, 1\}, z_0)$, which loops around 0 exactly once in the positive direction, and zero times around 1. Analytic continuation of the functions $y_1, \ldots, y_n$ permutes these functions. Denote this permutation by σ_0. Similarly we choose a loop γ_1 going around 1 exactly once in the positive direction. Analytic continuation along γ_1 generates a permutation σ_1. Together, the permutations $\sigma_0, \sigma_1, \sigma_\infty = (\sigma_0\sigma_1)^{-1}$ form a permutation triple. Transitivity of the group generated by σ_0, σ_1 follows from the irreducibility of $P(y)$.

$III(n) \to II(n)$. Let $\sigma_i \in S_n$ $(i = 0, 1, \infty)$ be a permutation triple. Take n line segments each with a black and a white endpoint. We now identify the black points and the white points in the following manner to obtain a dessin. We number the segments $1, 2, \ldots, n$. For each cycle in the cycle decomposition of σ_0 we identify the black points corresponding to the numbers in that cycle and choose the ordering of the cycle as ordering on the edges ending in the newly formed black vertex. We proceed in the same way with the white vertices using the cycle decomposition of σ_1. Because the group generated by σ_0, σ_1 actes transitively on $1, 2, \ldots, n$, the resulting graph is connected.

$II(n) \to I(n)$. Let D be a dessin. The argument used here is a topological one. Choose a closed compact oriented surface which allows an embedding $D \to S$ such that

1. The vertex orientation of D coincides with the positive orientation on S
2. $S \setminus D$ is a finite union of simply connected open sets $U_1, U_2, \ldots, U_r$ with piecewise smooth boundaries.

These properties determine the genus g of S uniquely. We now complete the embedded dessin into a triangulation of S. Choose in every open set U_i a gray point and connect it by edges to all vertices on D which are on the boundary of U_i. This gives a triangulation of S. There are two kinds of triangles. Positive ones, in which the ordering of the vertices is black-white-gray, and negative ones, in which the ordering of the vertices is black-gray-white. Both types occur equally often. Now construct a continous map $\phi : S \to \mathbb{P}^1$ such that

1. the positive triangles are mapped homeomorphically onto the northern hemisphere ($\mathrm{Im}(z) \geq 0$) with the black, white and grey vertices mapping to $0, 1, \infty$.
2. the negative triangles are mapped homeomorphically onto the southern hemisphere ($\mathrm{Im}(z) \leq 0$) with the black, white and grey vertices mapping to $0, 1, \infty$.

Now pull-back the complex structure of $\mathbb{P}^1$ to a complex structure on S via ϕ. In this way S becomes a compact Riemann surface, hence an algebraic curve.

Of course, any other mapping between these sets is a composition of one or more of the above ones. There are a few useful shortcuts though.

$I(n) \to II(n)$. Given a Belyi pair X, ϕ the corresponding dessin is simply $\phi^{-1}([0, 1])$ where the two sets of vertices are $\phi^{-1}(0)$ and $\phi^{-1}(1)$. The orientation around the vertices is induced by the positive orientation on X.

$II(n) \to III(n)$. Let n be the number of edges of the dessin. We number these edges $1, 2, \ldots, n$. For σ_0 we take the permutation induced by the cyclic ordering around the black vertices, for σ_1 we take the permutation induced by the ordering around the white vertices. Because the dessin is connected, the subgroup of S_n generated by σ_0, σ_1 acts transitively on $1, 2, \ldots, n$.

In each of the sets I, II, III, IV there are natural subsets which are also in 1-1 correspondence. They are

I' Connected graphs with n edges and a cyclic order at each vertex. These graphs arise if we take a dessin in which every white vertex has multiplicity 2 (i.e. there are two edges emanating from it) and where the white vertices are subsequently erased.

II' Belyi pairs (X, ϕ) with $\deg(\phi) = 2n$, such that every point in $\phi^{-1}(1)$ is ramified of order two.

III' Permutation triples in S_{2n} such that σ_1 is a product of n disjoint cycle pairs.

IV' Finite extensions of $\overline{\mathbb{Q}}(z)$ of degree $2n$, unramified outside $0, 1, \infty$ and ramification order 2 in every place above 1.

Following Schnepps [Schn94, p50] we call I' the set of *clean dessins*. We can always recover the original dessin from the clean one by putting a white vertex in the middle of each edge. Although it seems like a restriction, any dessin can be mapped to a clean dessin as follows. Let $\phi : X \to \mathbb{P}^1$ be the Belyi map corresponding to the general dessin. Then the map $X \to \mathbb{P}^1$ given by $P \mapsto 4\phi(P)(1 - \phi(P))$ is again a Belyi map which now corresponds to a clean dessin. This is based on the idea that $x \mapsto 4x(1 - x)$ maps ∞ to ∞, the points $0, 1$ to 0 and it ramifies of order 2 above 1. The clean dessin is simply obtained from the original dessin by changing the color of the white points to black.

Theorem 2.3 *Let $\phi : X \to \mathbb{P}^1$ be a Belyi map of degree N. Let n_0, n_1, n_∞ be the number of distinct points in $\phi^{-1}(0), \phi^{-1}(1), \phi^{-1}(\infty)$ respectively. Then*

$$2g(X) - 2 = N - n_0 - n_1 - n_\infty.$$

Proof This is an application of the Riemann-Hurwitz theorem. Consider the differential form

$$d\left(\frac{1}{\phi(x) + 1}\right) = -\frac{d\phi}{(\phi(x) + 1)^2}.$$

If e_a is the ramification order at a point $a \in X$ such that $\phi(a) \neq -1$, then this form has a zero of order $e_a - 1$ in a. Since ϕ is unramified above -1, the form has N poles of order two. So, by Riemann-Hurwitz, $2g - 2 = \sum_a (e_a - 1) - 2N$, where the sum is taken over all a with $\phi(a) \neq -1$. The sum of all ramification indices above a given point is of course N. Moreover, $e_a > 1 \Rightarrow a \in \phi^{-1}(0, 1, \infty)$. Hence $\sum_a (e_a - 1) = 3N - n_0 - n_1 - n_\infty$ and our Theorem follows.

qed

3 Counting dessins

We adress the following question. Given the ramification indices above $0, 1, \infty$ how many corresponding dessins are there?

Before we answer the question we need a slight extension of the concept of permutation triples and dessins. By a *generalised permutation triple* we mean any three $g_0, g_1, g_\infty \in S_n$ such that $g_0 g_1 g_\infty = \mathrm{Id}$. So we dropped the transitivity condition. In the same way as before we shall consider equivalence classes of permutation triples. A *generalised dessin* is simply a bicolored oriented graph, without the condition of connectivity. Again we consider only equivalence classes of generalised dessins.
Furthermore, we call $g \in S_n$ an automorphism of the triple g_i $(i = 0, 1, \infty)$ if $g g_i g^{-1} = g_i$ for $i = 0, 1, \infty$. We denote the automorphsim group by $\mathrm{Aut}(g_0, g_1, g_\infty)$. An automorphsim of a generalised dessin is of course an automorphism as bicolored oriented graph. We oberve the following.

Remark 3.1 *The natural bijection between II(n) and III(n) extends to a natural bijection between generalised dessins and generalised permutation triples. Moreover, the automorphism group of a generalised dessin and the automorphism group of the corresponding generalised permutation triple are isomorphic.*

One can also extend the classes I(n) and IV(n) and their correspondence with generalised dessins. The class I(n) must be extended to sets of Belyi-pairs where the sum of the degrees of the maps is n. The class IV(n) would have to be extended to commutative $\overline{\mathbb{Q}}(z)$-algebras of dimension n. But we shall not pursue this here.
The answer to our question is based on the following theorem (see also [Ser92]).

Theorem 3.2 *Let $n \in \mathbb{N}$. Let C_0, C_1, C_∞ be three conjugacy classes in S_n. The number of triples $g_0 \in C_0, g_1 \in C_1, g_\infty \in C_\infty$ such that $g_0 g_1 g_\infty = \mathrm{Id}$ is given by*

$$N_{C_0,C_1,C_\infty} = \frac{|C_0||C_1||C_\infty|}{n!} \sum_{\chi} \frac{\chi(C_0)\chi(C_1)\chi(C_\infty)}{\dim(\chi)}$$

where the sum is over all irreducible characters of S_n and $\dim(\chi)$ denotes the dimension of the representation corresponding to χ.

Notice that for any solution g_0, g_1, g_∞ of the problem the conjugates $g g_i g^{-1}$, $(i = 0, 1, \infty)$ are also solutions. So we arrive at the observation that $N(C_0, C_1, C_\infty))/n!$ counts the number of equivalence classes of $g_i \in C_i$ $(i = 0, 1, \infty)$ with $g_0 g_1 g_\infty = \mathrm{Id}$ with a weight equal to $1/|\mathrm{Aut}(g_0, g_1, g_\infty)|$.
Notice that conjugacy classes of S_n are in 1-1 correspondence with partitions of n, hence with sets of ramification indices that add up to n. So suppose we have given n, three partitions p_0, p_1, p_∞ of n corresponding to ramification indices above $0, 1, \infty$, and C_0, C_1, C_∞ their corresponding conjugacy classes. Then $N(C_0, C_1, C_\infty)/n!$ counts the number of generalised dessins with the given ramification data, where each dessin D is counted with weight $1/|\mathrm{Aut}(D)|$.

4 An example: planar dessins

As first examples we consider Belyi pairs $(\mathbb{P}^1, \phi)$, so we take $X = \mathbb{P}^1$. A Belyi map $\mathbb{P}^1 \to \mathbb{P}^1$ is called a *rational Belyi map.* The automorphism group of $\mathbb{P}^1$ is given by the fractional linear transforms $z \to \frac{az+b}{cz+d}$ where $ad - bc \neq 0$. So it is clear that if $\phi(z)$ is a rational Belyi map, then any equivalent one is given by $\phi\left(\frac{az+b}{cz+d}\right)$ with $ad - bc \neq 0$.

Consider a dessin in $\mathbb{P}^1$ corresponding to a rational Belyi map and suppose it does not contain ∞. After stereographic projection this dessin becomes a dessin in the complex plane, i.e. a two-colored planar graph. The cyclic order of the edges around every vertex is induced by the positive orientation in the plane.

Now let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a Belyi map, which we write as $\phi(x) = \frac{A(x)}{B(x)}$ where $A(x), B(x)$ are polynomials with gcd equal to 1. Define $C(x) = A(x) - B(x)$. Then $\phi^{-1}(0), \phi^{-1}(\infty), \phi^{-1}(1)$ are the zeros of $A(x), B(x), C(x)$ respectively. Here ∞ is counted as zero of $A(x)$ if $\deg(A) < \deg(B), \deg(C)$, and similarly for B, C. Let S be the set of distinct zeros of ABC (possibly including ∞) and let N be the degree of ϕ. Then our genus formula implies that

$$-2 = N - |S| \Rightarrow |S| = N + 2.$$

In fact, for any triple of polynomials $A(x), B(x), C(x)$ with $A(x) + B(x) + C(x) = 0$ and $\gcd(A, B, C) = 1$ we know that $|S| \geq N + 2$, where $N = \max(\deg(A), \deg(B), \deg(C))$. This inequality is known as Mason-Stothers inequality or the ABC-theorem. So we see that Belyi maps provide us with optimal cases of Mason's inequality.

5 J-maps

In this paper we shall be interested in special Belyi-maps which we call J-maps. above 0 and unique ramification order 2 above 1. Because of this the degree of a J-map is always a multiple of 6, say $6m$. The corresponding dessin d'enfant now has vertices of multiplicity two in the points $\phi^{-1}(1)$. We might as well suppress these points and we are left with a graph with $3m$ edges and preciesly $2m$ vertices, each with multiplicity 3. In the group theoretic description the element σ_0 now has cycle type $33\cdots 3$ ($2m$ threes) and σ_1 has cycle type $22\cdots 2$ ($3m$ twos).

Proposition 5.1 *Equivalence classes of J-maps are in 1-1-correspondence with torsion-free finite index subgroups Γ of $PSL(2,\mathbb{Z})$. The index $[PSL(2,\mathbb{Z}) : \Gamma]$ equals the degree of the J-map.*

The proof of this Proposition is fairly straightforward and can be found as a small part in [St81].

We remark that the subgroups in the above Proposition are in general not congruence subgroups. In fact the majority is not. However the congruence subgroups are of course of special interest. In recent work by Sebbar and McKay [Seb01],[McSe01] a complete classification is given of all torsion-free subgroups Γ that are congruence subgroups and such that $\mathcal{H}/\Gamma$ is a rational curve.

Proposition 5.2 *Let $J : X \to \mathbb{P}^1$ be a J-map. Let $n_J = \#J^{-1}(\infty)$, g the genus of X and $6m = \text{degree}(J)$. Then $2g - 2 = m - n_J$.*

Proof Riemann-Hurwitz implies that

$$\begin{aligned} 2g-2 &= -12m + 3m \cdot 1 + 2m \cdot 2 + \sum_{P \in J^{-1}(\infty)} (e_P - 1) \\ &= -12m + 3m + 4m + 6m - n_J \\ &= m - n_J \end{aligned}$$

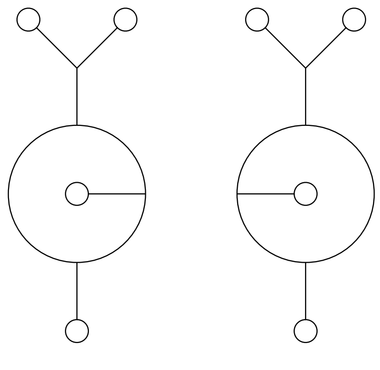
qed

6 Counting rational J-maps

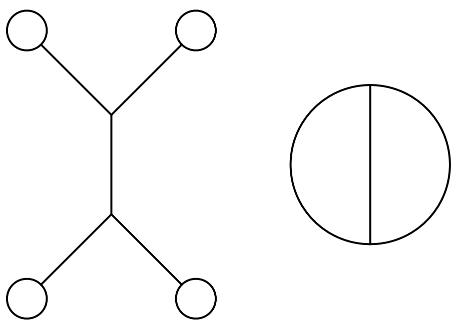
A J-map is called *rational* if $X = \mathbb{P}^1$. In this section we count the number of equivalence classes of rational J-maps of degree 24. One way to do this would be to draw all possible dessins d'enfant. However, this is a bit risky since it is easy to overlook possible graphs. That is why we shall do the drawing in conjunction with the group theoretic count using Theorem 3.2.

For a J-map of degree $6m$ the cycle types are $33\cdots3$ above 0 ($2m$ threes, this is C_0), $22\cdots2$ above 1 ($3m$ twos, this is C_1) and a partition of $6m$ above ∞ into $m+2$ parts (this is C_∞). In the Appendix we have given the table of values for $N_{C_0C_1C_\infty}/(6m)!$ for these cycle types in the cases $m = 4$. We do not include the details of this computation in this paper, since the calculation of the character table of S_{24} has been rather cumbersome. Suffice it to say that we used the software package **Lie** with some special tweaks to find the table.

To enumerate all rational J-maps with $m = 4$ we consider each case in Table 1 from the Appendix in the following way. Suppose for example that C_∞ is given by the partition 14-6-1-1-1-1 of 24. In Table 1 we find the counting number 25/12. Let us draw all dessins corresponding to these data, where we do not draw the vertices above 1 and the vertices above 0 are recognizable by the three-fold branchings in the picture.



These are two mirror images (the orientations are induced by the orientation in the plane) and each has trivial automorphism group. So they contribute 2 to our character formula. The remaining 1/12 are accounted for by the following generalised dessin



The smaller dessin has opposite orientations at the vertices, so it is not a planar dessin. It has an automorphism group of order 6. The larger dessin is planar and has an automorphism group of order 2. So the total automorphism group has order 12, which explains the missing 1/12 in our character formula. Moreover, we are now certain that we have listed all possible dessins corresponding to the partition 14-6-1-1-1-1. On the website we have only pictured the connected dessins.

7 Computation of rational J-maps

Proposition 7.1 *Let ϕ be a rational J-map of degree $6m$ such that $\phi(\infty)=\infty$. Then there exist polynomials $c_4, c_6 \in \mathbb{C}[t]$ of degrees $2m, 3m$ respectively and a polynomial Δ of degree $< 6m$ such that*

1. $\gcd(c_4, c_6) = 1$

2. $c_4^3 - c_6^2 = \Delta$

3. *Δ has $m+1$ distinct zeros.*

Proof. Since ϕ is a rational function which ramifies of order 2 in every point above 1 and order 3 in every point above 0, there exist polynomials c_4, c_6, Δ such that $\phi(t) = c_4^3/\Delta = 1 + c_6^2/\Delta$. Hence $c_4^3 - c_6^2 = \Delta$. Since ϕ has degree $6m$, the degrees of c_4, c_6, Δ follow. From Proposition 5.2 it follows that Δ has precisely $n_J - 1$ distinct zeros (∞ is left out) which equals $(m+2-2g)-1 = m+1$.
qed

Proposition 7.2 *Let notations and assumptions be as in the previous Proposition. Let $\delta = \gcd(\Delta, \Delta')$ and $\Delta = p\delta, \Delta' = q\delta$. The leading coefficient of δ is* *chosen the same as that of Δ, i.e. p is monic. Then c_4, c_6, Δ can be normalised in such a way that*

$$\begin{aligned} c_6 &= c_4 q - 3c_4' p \\ c_4^2 &= c_6 q - 2c_6' p \\ \delta &= 3c_4' c_6 - 2c_6' c_4 \end{aligned}$$

Moreover, there exists a polynomial l of degree $\le m-1$ such that $c_4 = q^2 + lp$.

Proof The identity $c_4^3 - c_6^2 = p\delta$ and its derivative $3c_4^2 c_4' - 2c_6 c_6' = q\delta$ can be rewritten in the following vector notation,

$$c_4^2 \begin{pmatrix} c_4 \\ 3c_4' \end{pmatrix} + c_6 \begin{pmatrix} -c_6 \\ -2c_6' \end{pmatrix} + \delta \begin{pmatrix} -p \\ -q \end{pmatrix} = 0.$$

We consider this as a system of linear equations in the unknowns c_4^2, c_6. The coefficient determinant is $2c_4 c_6' - 3c_6 c_4'$. Suppose it vanishes identically. This implies $(c_6^2/c_4^3)' = 0$, hence c_6^2/c_4^3 is in $\mathbb{C}$, which cannot happen. We conclude that $2c_4 c_6' - 3c_6 c_4' \neq 0$ and solving the equation gives us the existence of $\lambda \in \mathbb{C}(z)^*$ such that

$$\lambda \begin{pmatrix} c_6 \\ c_4^2 \\ \delta \end{pmatrix} = \begin{pmatrix} c_4 q - 3c_4' p \\ c_6 q - 2c_6' p \\ 3c_4' c_6 - 2c_4 c_6' \end{pmatrix}.$$

Since $\gcd(c_4, c_6) = 1$ we can infer that $\lambda \in \mathbb{C}[z]$. We note that the degrees of p, q are $m+1$ and m respectively. So from the first equation it follows that

$$\deg(\lambda) + 3m \le \deg(c_4) + \deg(q) = 2m + m = 3m.$$

Hence $\deg(\lambda) \le 0$ and so $\lambda \in \mathbb{C}^*$. By the substitution $c_4 \to \lambda^{-2} c_4, c_6 \to \lambda^{-3} c_6, \delta \to \lambda^{-6}\delta$ we can see to it that the new λ equals 1.
Finally notice that p and c_4 are relatively prime. Consider the first two equations modulo p. We obtain $c_6 \equiv c_4 q (\bmod\ p)$ and $c_4^2 \equiv c_6 q (\bmod\ p)$. Elimination of c_6 yields $c_4^2 \equiv c_4 q^2 (\bmod\ p)$. Since c_4 and p are relatively prime this implies $c_4 \equiv q^2 (\bmod\ p)$ from which our last assertion follows.

qed

Suppose we wish to compute the rational J-maps with cycle type $n_1, n_2, \ldots, n_{m+1}, n_{m+2}$ above ∞. In particular $n_i > 0$ for all i and $\sum_i n_i = 6m$. We assume that $J(\infty) = \infty$ and that ∞ has ramification order n_{m+2}. The polynomial Δ in Proposition 7.2 has the form

$$\Delta = \Delta_0 \prod_{i=1}^{m+1} (z - a_i)^{n_i}, \Delta_0 \in \overline{\mathbb{Q}}^*.$$

The polynomials p, q in Proposition then have the form

$$p = \prod_{i=1}^{m+1} (z - a_i), \qquad q = p \sum_{i=1}^{m+1} \frac{n_i}{z - a_i}. \tag{1}$$

Proposition 7.3 *Suppose we have polynomials p, q given as in (1). Suppose there exist polynomials c_4, c_6 of degrees $2m, 3m$ in z such that*

$$c_6 = c_4 q - 3c_4' p \qquad c_4^2 = c_6 q - 2c_6' p.$$

Then $c_4^3 - c_6^2$ is proportional to $\prod_{i=1}^{m+1}(z-a_i)^{n_i}$. Moreover, if there exists a polynomial l of degree $\le m-1$ such that $c_4 = q^2 + lp$, then c_4, c_6 are relatively prime.

Proof. From the two equations for c_4, c_6 it easily follows that

$$c_4^2(c_4 q - 3c_4' p) = c_6(c_6 q - 2c_6' p).$$

Hence

$$(c_4^3 - c_6^2)q = (c_4^3 - c_6^2)' p$$

and thus

$$\frac{(c_4^3 - c_6^2)'}{(c_4^3 - c_6^2)} = \frac{q}{p} = \sum_{i=1}^{m+1} \frac{n_i}{z - a_i}.$$

In other words, $c_4^3 - c_6^2$ is a constant times $\prod_i (z-a_i)^{n_i}$.
Suppose $c_4 = q^2 + lp$. Since p, q have no common zeros, the same holds for c_4 and p. Suppose c_4, c_6 have a common zero ρ. Then, from the first equation it follows that $\mathrm{ord}_\rho(c_6) = \mathrm{ord}_\rho(c_4) - 1$. From the second it follows that $2\mathrm{ord}_\rho(c_4) = \mathrm{ord}_\rho(c_6) - 1$. This gives a contradiction. Hence c_4 and c_6 are relatively prime.
qed

Given $p(z), q(z)$ as above, we solve the system of equations

$$\begin{aligned} c_6 &= c_4 q - 3c_4' p \\ c_4^2 &= c_6 q - 2c_6' p \\ c_4 &= q^2 + lp \end{aligned}$$

in polynomials c_4, c_6, l of degrees $2m, 3m, m-1$. We can eliminate c_4, c_6 from these equations to obtain the following single equation for $l(z)$:

$$\begin{aligned} 0 \;=\;& p(pl^2 + q^2 l + 5p'ql - 6(p')^2 l + 2pq'l - 6pp''l \\ &+5pql' - 18pp'l' + 12q^2 q' - 6p^2 l'' - 12p'qq' - 12p(q')^2 - 12pqq'') \end{aligned}$$

Note that we can divide by p on both sides. Denote by Q the polynomial on the right between parentheses. In principle Q has degree $3m-1$. We now write $l = \sum_{i=0}^{m-1} l_i z^i$ and determine the coefficients l_i recursively for $i = m-1, m-2, \ldots$ by setting the coefficient of $z^{3m-1}, z^{3m-2}, \ldots$ in Q equal to zero.
Let us first compute the leading coefficient of Q. The leading coefficient of p equals 1, the leading coefficient of q equals $N := \sum_{i=1}^{m+1} n_i$. Then it is straightforward to compute the leading coefficient of Q. It reads

$$(l_{m-1} + N^2)(l_{m-1} + 12mN - 36m^2).$$

Since $l_{m-1} + N^2$ is also the leading coefficient of c_4, which we assumed to be non-zero, we conclude that

$$l_{m-1} = 36m^2 - 12mN.$$

Fix $k < m-1$. The coefficient l_k occurs in the expansion of Q as polynomial in z. However, closer examination reveals that l_k does not occur in the coefficients of z^r in Q when $r > 2m+k$. When $r = 2m+k$ the coefficient l_k occurs linearly with coefficient

$$(N - 5m - k - 1)(N - 12m + 6k + 6),$$

where we have used our evaluation of l_{m-1}. Setting the coefficient of z^{2m+k} in Q equal to zero allows us to compute l_k in terms of l_i with $i > k$ and the a_i, n_i. In particular we see by induction that l_k is polynomial in the a_i. Notice that the calculation of l_k is only possible if $(N - 5m - k - 1)(N - 12m + 6k + 6)$ is non-zero. The procedure will work whenever $N \leq 5m$. Add n_{m+2} on both sides and use $N + n_{m+2} = 6m$ to find that the latter condition is equivalent to $n_{m+2} \geq m$. In our computations this condition could always be fullfilled. It may give some problems when $m > 4$.

Setting the coefficient of z^{2m+k} in Q equal to zero allows us to compute l_k in terms of l_i with $i > k$ and the a_i, n_i. In particular we see by induction that l_k is polynomial in the a_i.

Once we have have expressed the coefficients l_k in terms of the zeros a_i, we can substitute this in the equation $Q = 0$. By construction the coeffients of z^j will be zero for $j = 2m, 2m+1, \ldots, 3m-1$. The requirement that the coefficients of z^j for $j = 0, 1, \ldots, 2m-1$ should be zero provides us with a set of polynomial equations for the unknown points $a_1, a_2, \ldots, a_{m+1}$.

8 A sample computation

As an illustration of the algorithm from the previous section we compute the J-map corresponding to the case $m = 4$ and the partition 19-1-1-1-1-1 above ∞.

We assume $n_6 = 19$ and take Δ is proportional to $z^5 + az^4 + bz^3 + cz^2 + dz + e$. We do this rather than taking Δ proportional to $\prod_{i=1}^{5}(z - a_i)$. In the latter case the numbers a_i may turn out to be algebraic, which may cmplicate our calculations. Furthermore, by shifting z over a constant we can see to it that $a = 0$. So Δ is taken proportional to $z^5 + bz^3 + cz^2 + dz + e$.

We find easily that $p = z^5 + bz^3 + cz^2 + dz + e$ and $q = 5z^4 + 3b * z^2 + 2c * z + d$. We now use Proposition 7.2 to get $c_4 = q^2 + (l_3z^3 + l_2z^2 + l_1z + l_0)p$ where $l_3 = -576$. Substitute this in $c_6 = c_4q - 3c_4'p$ and substitute that in $(c_4^2 - c_6q)/p + 2c_6' = 0$. We get the equation

$$450l_2z^{10} + (l_2^2 + 527l_1 - 64872b)z^9 + \cdots = 0$$

Setting the coefficient of z^{10} equal to zero gives us $l_2 = 0$. We are left with the equation

$$(527l_1 - 64872b)z^9 + (592l_0 - 43392c)z^8 + \cdots = 0$$

Setting the coefficient of z^9 equal to zero gives us $l_1 = 64872b/527$. Notice also that setting the coefficient of z^8 equal to zero gives us $l_0 = 43392c/592$. We are left with an equation of the form

$$Q_7 z^7 + Q_6 z^6 + \cdots + Q_0 = 0$$

where

$$\begin{aligned}
Q_7 &= -25920d + 6486480b^2/961 \\
Q_6 &= 12096e - 13384224bc/1147 \\
Q_5 &= 855360bd/31 + 6486480c^2/1369 \\
&\quad +6486480b^3/961 \\
\vdots &\quad \vdots
\end{aligned}$$

Setting Q_5, Q_6, Q_7 equal to zero gives us a set of polynomal equations in b, c, d, e whose solution reads

$$b = 62t^2, \quad c = 148t^3, \quad d = 1001t^4, \quad e = 8852t^5$$

where t can be chosen arbitrarily. Surprisingly enough, all coefficients Q_i $(i = 0, \ldots, 7)$ vanish for this choice of b, c, d, e. Hence we have found a solution which, choosing $t = 1$, reads

$$\begin{aligned}
c_4 &= 19^2(z^8 + 84z^6 + 176z^5 + 2366z^4 + 13536z^3 \\
&\quad +26884z^2 + 218864z + 268777) \\
c_6 &= 19^3(z^{12} + 126z^{10} + 264z^9 + 6195z^8 + 31392z^7 \\
&\quad +163956z^6 + 1260528z^5 + 3531639z^4 \\
&\quad +19770400z^3 + 62912622z^2 + 94024776z + 291742453) \\
\Delta &= c_4^3 - c_6^2 \\
&= -2^{38}3^3 19^6(z^5 + 62z^3 + 148z^2 + 1001z + 8852)
\end{aligned}$$

Always, when the computation is done, one can reduce the complexity of the coefficients to a large extent by performing a variable substitution. In our example we substitute z by $4z - 1$ and obtain a new relation

$$c_4^3 - c_6^2 = -16(4z^5 - 5z^4 + 18z^3 - 3z^2 + 14z + 31)$$

where

$$\begin{aligned}
c_4 &= 4(z^8 - 2z^7 + 7z^6 - 6z^5 + 11z^4 + 4z^3 + 12z + 1) \\
c_6 &= 4(2z^{12} - 6z^{11} + 24z^{10} - 38z^9 + 78z^8 \\
&\quad -48z^7 + 60z^6 + 72z^5 - 30z^4 + 120z^3 + 27z^2 + 9z + 29)
\end{aligned}$$

9 Appendix

In this section we list the values of $N(C_\infty) := N_{C_0C_1C_\infty}/24!$ for S_{24} where C_0 has cycle type consisting of 8 three's, C_1 has cycle type consisting of 12 two's and where C_∞ consists of exactly six cycles. We list only those cases for which $N(C_\infty) \neq 0$.

Table 1: Counting dessins in the case $m = 4$

Partition						$N(C_\infty)$		Partition						$N(C_\infty)$
19	1	1	1	1	1	1		18	2	1	1	1	1	5/2
17	3	1	1	1	1	1		17	2	2	1	1	1	2
16	4	1	1	1	1	11/4		16	3	2	1	1	1	3
16	2	2	2	1	1	4/3		15	5	1	1	1	1	2
15	4	2	1	1	1	9/2		15	3	3	1	1	1	1
15	3	2	2	1	1	3		15	2	2	2	2	1	5/6
14	6	1	1	1	1	25/12		14	5	2	1	1	1	4
14	4	3	1	1	1	5/2		14	4	2	2	1	1	5/2
14	3	3	2	1	1	2		14	3	2	2	2	1	3/2
14	2	2	2	2	2	1/6		13	7	1	1	1	1	1
13	6	2	1	1	1	13/6		13	5	3	1	1	1	1
13	5	2	2	1	1	2		13	4	4	1	1	1	1
13	4	3	2	1	1	2		13	4	2	2	2	1	1/3
13	3	3	2	2	1	1		13	3	2	2	2	2	1/3
12	7	2	1	1	1	2		12	6	3	1	1	1	19/18
12	6	2	2	1	1	19/12		12	5	4	1	1	1	1
12	5	3	2	1	1	4		12	5	2	2	2	1	4/3
12	4	4	2	1	1	7/4		12	4	3	3	1	1	11/6
12	4	3	2	2	1	3		12	4	2	2	2	2	1/4
12	3	3	3	2	1	1		12	3	3	2	2	2	11/18
11	9	1	1	1	1	4/3		11	8	2	1	1	1	7/2
11	7	3	1	1	1	3		11	7	2	2	1	1	2
11	6	4	1	1	1	37/12		11	6	3	2	1	1	25/6
11	6	2	2	2	1	13/36		11	5	5	1	1	1	3/2
11	5	4	2	1	1	7/2		11	5	3	3	1	1	2
11	5	3	2	2	1	1		11	5	2	2	2	2	1/6
11	4	4	3	1	1	3/2		11	4	4	2	2	1	1/4
11	4	3	3	2	1	1		11	4	3	2	2	2	1/6
11	3	3	3	3	1	1/12		10	10	1	1	1	1	5/4
10	9	2	1	1	1	13/6		10	8	3	1	1	1	1
10	8	2	2	1	1	1/4		10	7	4	1	1	1	5/2
10	7	3	2	1	1	2		10	7	2	2	2	1	3/2
10	6	5	1	1	1	25/6		10	6	4	2	1	1	71/24
10	6	3	3	1	1	1/12		10	6	3	2	2	1	5/3
10	6	2	2	2	2	19/72		10	5	5	2	1	1	5/4

Table 1: Counting dessins in the case $m = 4$, (continued)

Partition						$N(C_\infty)$		Partition						$N(C_\infty)$
10	5	4	3	1	1	1/2		10	5	4	2	2	1	3
10	5	3	2	2	2	7/6		10	4	4	4	1	1	1/4
10	4	4	3	2	1	1		10	4	4	2	2	2	5/24
10	4	3	3	2	2	1		10	3	3	3	3	2	1/24
9	9	3	1	1	1	1/9		9	9	2	2	1	1	2
9	8	4	1	1	1	7/12		9	8	3	2	1	1	19/6
9	8	2	2	2	1	1/6		9	7	5	1	1	1	1
9	7	4	2	1	1	2		9	7	3	2	2	1	3
9	6	6	1	1	1	55/216		9	6	5	2	1	1	19/6
9	6	4	3	1	1	37/36		9	6	3	3	2	1	10/3
9	6	3	2	2	2	1/108		9	5	5	3	1	1	1/6
9	5	5	2	2	1	1		9	5	4	3	2	1	3
9	5	3	3	3	1	1		9	4	4	3	2	2	1/12
9	4	3	3	3	2	1		9	3	3	3	3	3	1/36
8	8	4	2	1	1	9/8		8	8	3	3	1	1	3/2
8	8	2	2	2	2	7/24		8	7	6	1	1	1	2
8	7	5	2	1	1	3		8	7	4	3	1	1	5/2
8	7	4	2	2	1	2		8	7	3	3	2	1	1
8	7	3	2	2	2	1/6		8	6	6	2	1	1	307/144
8	6	5	3	1	1	2		8	6	5	2	2	1	7/6
8	6	4	4	1	1	13/48		8	6	4	3	2	1	29/12
8	6	4	2	2	2	157/144		8	6	3	3	2	2	1/12
8	5	5	4	1	1	3/8		8	5	5	2	2	2	1/12
8	5	4	3	3	1	2		8	5	4	3	2	2	1
8	4	4	4	3	1	1		8	4	4	4	2	2	9/16
8	4	3	3	3	3	1/48		7	7	7	1	1	1	1/3
7	7	6	2	1	1	1/6		7	7	5	3	1	1	2
7	7	4	4	1	1	5/4		7	7	4	2	2	2	1/12
7	7	3	3	2	2	1		7	6	6	3	1	1	1/6
7	6	6	2	2	1	1		7	6	5	4	1	1	1
7	6	5	3	2	1	19/6		7	6	4	4	2	1	1
7	6	4	3	3	1	1/6		7	5	5	4	2	1	2
7	5	5	3	2	2	1		7	5	4	4	3	1	1
7	5	4	3	3	2	1		6	6	6	4	1	1	1855/2592
6	6	6	3	2	1	19/72		6	6	6	2	2	2	1855/7776
6	6	5	5	1	1	175/144		6	6	5	4	2	1	7/6
6	6	5	3	3	1	1		6	6	4	4	2	2	187/288
6	6	4	3	3	2	1/2		6	6	3	3	3	3	235/864
6	5	5	3	3	2	1/12		6	5	4	4	3	2	1
6	4	4	4	3	3	1/36		5	5	5	5	2	2	1/4
5	5	4	4	3	3	1/2		4	4	4	4	4	4	1/24

10 References

[Be79] G.Belyi, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk USSR, Ser.Mat. 43:2(1979), 269-276 (in Russian). English translation: Math USSR Izv. 14(1979), 247-256.

[Ir03] Y.Iron, An explicit presentation of a K3 surface that realizes [1,1,1,1,1,19], MSc. Thesis, Hebrew University of Jerusalem, 2003.

[McSe01] J.McKay, A.Sebbar, Arithmetic semistable elliptic surfaces, Proceedings on Moonshine and related topics (Montral, QC, 1999), 119-130, CRM Proc. Lecture Notes, 30, Amer. Math. Soc., Providence, RI, 2001

[MP89] R.Miranda-U.Persson, Configurations of I_n fibers on elliptic K3-surfaces, Math. Z. 201 (1989), 339-361.

[Schn94] L.Schneps (editor), The Grothendieck Theory of Dessins d'Enfants, LMS Lecture Notes 200, CUP 1994.

[Schu04] M.Schütt, Elliptic fbrations of some extremal semi-stable K3-surfaces, to appear in Rocky Mountain J. of Math. (arxiv: math.AG/0412049).

[SchuT06] M. Schütt, J.Top, Arithmetic of the [19,1,1,1,1,1] fibration, Comm. Math. Univ. St.Pauli 55 (2006), 9-16.

[Seb01] A.Sebbar, Classification of torsion-free genus zero congruence groups, Proc. Amer. Math. Soc. 129 (2001), 2517-2527 (electronic).

[Ser92] J.P.Serre, Topics in Galois Theory, A.K.Peters 1992.

[St81] W.W.Stothers, Polynomial identities and Hauptmoduln, Quart.J. Math. Oxford (2) 32 (1981), 349-370.

[TY04] J.Top and N.Yui, Explicit equations of some elliptic modular surfaces, to appear in Rocky Mountain J. of Math.