WILD QUOTIENT SINGULARITIES OF SURFACES

DINO LORENZINI

ABSTRACT. Let $(B, \mathcal{M}_B)$ be a noetherian regular local ring of dimension 2 with residue field $B/\mathcal{M}_B$ of characteristic $p > 0$. Assume that B is endowed with an action of a finite cyclic group H whose order is divisible by p. Associated with a resolution of singularities of Spec B^H is a resolution graph G and an intersection matrix N.

We prove in this article three structural properties of wild quotient singularities, which suggest that in general, one should expect when $H = \mathbb{Z}/p\mathbb{Z}$ that the graph G is a tree, that the Smith group $\mathbb{Z}^n/\mathrm{Im}(N)$ is killed by p, and that the fundamental cycle Z has self-intersection $|Z^2| \leq p$. We undertake a combinatorial study of intersection matrices N with a view towards the explicit determination of the invariants $\mathbb{Z}^n/\mathrm{Im}(N)$ and Z. We also exhibit explicitly the resolution graphs of an infinite set of wild $\mathbb{Z}/2\mathbb{Z}$-singularities, using some results on elliptic curves with potentially good ordinary reduction which could be of independent interest.

KEYWORDS Cyclic quotient singularity, wild, intersection matrix, resolution graph, fundamental cycle.

MSC: 14B05, 14G20 (14E15, 14H20, 13H15, 14J17)

1. Introduction

Let B denote a regular local ring of dimension 2 with maximal ideal $\mathcal{M}_B$. Let H be a finite cyclic group acting on B, and let $\mathcal{Z} := \mathrm{Spec}(B^H)$. Assume that the action of H on $\mathrm{Spec}(B)$ is free off the closed point, and that $\mathcal{M}_B^H$ is the only singular point of $\mathcal{Z}$. When the order of H is not divisible by the residue characteristic p of $B/\mathcal{M}_B$, $\mathcal{M}_B^H$ is called a *tame* cyclic quotient singularity. Otherwise, $\mathcal{M}_B^H$ is a *wild* cyclic quotient singularity.

Let $f : \mathcal{X} \to \mathcal{Z}$ be a resolution of the singularity, minimal with the property that the irreducible components of $f^{-1}(\mathcal{M}_B^H)$ are smooth with normal crossings. Such a resolution exists when B^H is excellent ([1], [4], [15], [19]). Attached to this resolution are two natural objects that we now describe, the *intersection matrix* N, and the *resolution graph* G. The exceptional divisor $f^{-1}(\mathcal{M}_B^H)$ consists in n irreducible components C_i, $i = 1, \ldots, n$. Denote by $N := ((C_i \cdot C_j)_{\mathcal{X}})$ the associated symmetric matrix. The matrix N is negative definite and, in particular, $\det(N) \neq 0$. Let G denote the graph whose vertices are the n irreducible components of $f^{-1}(\mathcal{M}_B^H)$, and where two vertices C and D are linked by $(C \cdot D)_{\mathcal{X}}$ edges. For future reference, recall that the *degree* of a vertex C in a graph G is the number of edges connected to C, and a vertex of degree at least 3 on a graph is called a *node*.

Much is known about tame cyclic quotient singularities. Most importantly, their resolution graphs, called Hirzebruch-Jung strings, are the simplest possible graphs: trees without nodes. Moreover, for a given H, the set of such strings is finite and explicitly describable[1]. The key property of tame cyclic actions that allows for a description of their

Date: December 3, 2012.

D.L. was supported by NSF Grant 0902161.

[1] These facts are well-known for surfaces over $\mathbb{C}$ (see, e.g., [6], III.5, or [18], p. 207). For the general case, see [13], and also [35], 6.4 and 6.8, and [11], section 2.

resolution graphs is that such actions can be given in simple normal forms, producing explicit equations for the ring $\widehat{B}^H$. In contrast, wild cyclic actions are much more difficult to classify. Even in the simplest case of $\mathbb{Z}/p\mathbb{Z}$ acting on $k[[x, y]]$, explicit equations for $k[[x, y]]^H$ have only been obtained in a few cases, such as in equicharacteristic 2 in [2], and in some cases where $p = 3$ in [30], 5.15.

Our goal in this article is to provide information on the graphs which can arise as the resolution graph of a wild cyclic quotient singularity. To illustrate the difficulty in completely classifying such graphs for a given p, we will show when $p = 2$ that the set of non-singular matrices arising (up to permutation) as intersection matrices of the resolution of $\mathbb{Z}/2\mathbb{Z}$-quotient singularities is infinite (4.1; see also [2], p. 64, in the equicharacteristic case).

We discuss in section 2 three general structural properties of wild cyclic quotient singularities. Rather than completely stating below all the hypotheses of the three theorems, let us say that in rather general situations, we can show that a wild cyclic quotient singularity satisfies the following:

- the irreducible components of the resolution of a $\mathbb{Z}/p\mathbb{Z}$-quotient singularity are rational, and *the graph of the resolution is a tree* (Theorem 2.8).
- *The multiplicity of the local ring B^H is at most $|H|$* (Theorem 2.3). This latter result imposes additional restrictions on the possible resolution graphs since the fundamental cycle Z of a singularity depends only on the intersection matrix, and its self-intersection $|Z^2|$ is bounded by the multiplicity of B^H ([36], 2.7).
- *The order $|H|$ kills the finite Smith group $\Phi_N := \mathbb{Z}^n/N(\mathbb{Z}^n)$* (Theorem 2.6). In particular, $|\det(N)|$ is a power of p when $H = \mathbb{Z}/p\mathbb{Z}$.

In section 3, we undertake a completely combinatorial study of intersection matrices N, with a view towards an explicit determination of the invariants occurring in our theorems on quotient singularities, namely the Smith group Φ_N and the fundamental cycle Z. We obtain in particular a general explicit formula for the order of Φ_N when the graph $G(N)$ is a tree (3.14).

It is clear that one of the main question in the classification of wild $\mathbb{Z}/p\mathbb{Z}$-quotient singularities is the determination of the types of intersection matrices which can occur in the resolution of the singularity. We do not know if such intersection matrices always satisfy further combinatorial restrictions in addition to the three addressed in this paper: the associated graph $G(N)$ is a tree, the Smith group Φ_N is killed by p, and the fundamental cycle Z has $|Z^2| \leq p$.

We end section 3 with a detailed study, for each prime p, of a family of star-shaped intersection matrices N satisfying the above combinatorial restrictions (3.17). We show in section 4 that some of these matrices do appear as intersection matrices associated with $\mathbb{Z}/2\mathbb{Z}$-quotient singularities (4.1). This result uses some facts about elliptic curves with potentially good ordinary reduction which could be of independent interest. Further work on these matrices in the context of model of curves can be found in [26].

I thank Michel Raynaud for his generous contributions to this article. Several of the arguments in section 2 are due to him. I also thank Qing Liu and Werner Lüktebohmert for helpful discussions, and the referee for a careful reading of the article.

2. General properties of quotient singularities

We prove in this section several general properties of quotient singularities of surfaces and of their associated intersection matrices. Let B be a normal noetherian local domain endowed with an action of a finite group H. Let $A := B^H$. Let $\widehat{B}$ denote the completion of the local ring B with respect to its maximal ideal $\mathcal{M}_B$. Similarly, let $\widehat{A}$ denote the completion of A with respect to its maximal ideal $\mathcal{M}_A$. The action of H on B extends to an action on $\widehat{B}$, and the ring $(\widehat{B})^H$ is a normal complete domain. Consider the canonical injection $\widehat{A} \longrightarrow (\widehat{B})^H$.

Lemma 2.1. *Let B be a normal noetherian local domain endowed with an action of a finite group H. If $x \in (\widehat{B})^H$, then $\mathrm{Im}(\widehat{A})$ contains $|H|x$ and $x^{|H|}$. In particular, $(\widehat{B})^H$ is integral over $\mathrm{Im}(\widehat{A})$.*

If $|H|$ is coprime to $\mathrm{char}(A/\mathcal{M}_A)$, then the map $\widehat{A} \to (\widehat{B})^H$ is an isomorphism. If $\mathrm{char}(B) = 0$, then $\widehat{A}$ and $(\widehat{B})^H$ have same fields of fractions and, if in addition $\widehat{A}$ is normal, then the map $\widehat{A} \to (\widehat{B})^H$ is an isomorphism.

Proof. Let $x = \{b_n\}$ be an element of the projective limit $\widehat{B} := \varprojlim B/\mathcal{M}_B^n$ fixed by H. Since H is finite, $|H|x = \{\sum_{\sigma\in H} \sigma(b_n)\}$ and $x^{|H|} = \{\prod_{\sigma\in H} \sigma(b_n)\}$ belong to the projective limit $\widehat{A}$. Thus x is a root of the monic polynomial $X^{|H|} - x^{|H|}$ with coefficients in $\widehat{A}$. When $|H| \in \widehat{A}$ is invertible in $\widehat{A}$, $|H|x \in \widehat{A}$ implies $x \in \widehat{A}$, so $\widehat{A} = \widehat{B}^H$.

Assume that $|H| \neq 0$ in $\widehat{A}$. Let $y = \{c_n\} \in \widehat{B}^H$. Then $x/y = |H|x/|H|y$, and $\widehat{A}$ and $(\widehat{B})^H$ have same fields of fractions. If $\widehat{A}$ is integrally closed, then the map $\widehat{A} \to (\widehat{B})^H$ is an isomorphism because $(\widehat{B})^H$ is integral over $\mathrm{Im}(\widehat{A})$, with same field of fractions as $\widehat{A}$. □

The map $\widehat{A} \longrightarrow (\widehat{B})^H$ is clearly not surjective if $\widehat{A}$ is not normal, and the completion of a normal noetherian local domain A need not be normal in general, unless, for instance, A is excellent ([28] (33.I)). In this section, we consider the following two types of rings. Let $(B, \mathcal{M}_B)$ be a regular noetherian local domain of dimension 2, endowed with an action of a finite group H. We will say that B is if type I or type II when it satisfies the following additional conditions:

Type I: Assume that B contains a complete regular noetherian local domain R of dimension 1, such that for all $\sigma \in H$, $\sigma(R) \subseteq R$. Assume in addition that there exist an R-algebra of finite type B_0 endowed with an action of H, and a prime ideal $\mathfrak{P}$ of B_0 with $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in H$, such that the local ring B with its action of H is isomorphic to the localization of B_0 at $\mathfrak{P}$. Assume also that there exists $x \in B$ such that $\mathcal{M}_B = (\mathcal{M}_R, x)$ and such that the natural R-map $R[X]_{(\mathcal{M}_R,X)} \longrightarrow B$, sending X to x, extends to an R-isomorphism $R[[X]] \to \widehat{B}$.

Type II: Let k be a field. Suppose that B contains k, and that for all $\sigma \in H$ and all $c \in k$, $\sigma(c) = c$. Assume that there exist a k-algebra of finite type B_0 endowed with an action of H, and a prime ideal $\mathfrak{P}$ of B_0 with $\sigma(\mathfrak{P}) = \mathfrak{P}$ for all $\sigma \in H$, such that the local ring B with its action of H is isomorphic to the localization of B_0 at $\mathfrak{P}$. Assume also that there exist elements $u, v \in \mathcal{M}_B$ with $\mathcal{M}_B = (u, v)$ and such that the natural k-homomorphism $k[U, V]_{(U,V)} \to B$, sending U to u and V to v, induces an isomorphism $k[[U, V]] \to \widehat{B}$.

Lemma 2.2. *Let B be a regular noetherian local domain of type I or II. Then the ring $A := B^H$ is excellent and, hence, $\widehat{A}$ is normal and excellent too.*

Proof. Indeed, in case I, the domain R^H is a complete domain. Since the field of fractions of R is a finite extension of the field of fractions of R^H, and since R is integral over R^H, we find, using [29], 32.1, page 112, that R is a finitely generated R^H-module. Then a theorem of Eakin ([28], page 263) shows that R being noetherian implies that R^H is also noetherian. It follows that the ring R^H is excellent ([28], (34.B)). Since the domain B_0 is a finitely generated R^H-algebra, the domain B_0^H is also a finitely generated R^H-algebra ([8], Theorem 2 in V.1.9, page 323). Hence, B_0^H is excellent since R^H is ([28] (34.A)). Then B^H is also excellent since it is isomorphic to $(B_0^H)_{\mathfrak{P}\cap B_0^H}$ ([8], Prop. 23 in V.1.9). For B in case II, it is clear that B_0^H is a finitely generated k-algebra and, again, B^H is excellent. □

Let us recall now the notion of *multiplicity of a local ring* ([5], 11.4). Let A be a noetherian local ring of dimension d, with maximal ideal $\mathcal{M}_A$. Denote by length$(A/\mathcal{M}_A^n)$ the length of the A-module $A/\mathcal{M}_A^n$. Then there exists a polynomial $g_A(x) \in \mathbb{Q}[x]$, called the Hilbert-Samuel polynomial of $\mathcal{M}_A$, such that for all sufficiently large n,

$$g_A(n) = \text{length}(A/\mathcal{M}_A^n).$$

The polynomial $g_A(x)$ has degree d and, writing $g_A(x) = a_d x^d + \cdots + a_0$, the *multiplicity* mult(A) of A is defined to be $d! a_d \in \mathbb{N}$.

Theorem 2.3. *Let H be a finite cyclic group acting on a regular noetherian local domain B of dimension 2 of type I or II. In case of type II, assume that k contains the $|H|$-roots of unity. Let $A := B^H$. Then mult$(A) \leq |H|$.*

Proof. Since mult$(A) =$ mult$(\widehat{A})$, it suffices to bound mult$(\widehat{A})$. Consider first the case where B is of type I, with $\mathcal{M}_B = (\mathcal{M}_R, x)$. Consider the element $t := \prod_{\sigma \in H} \sigma(x)$. Clearly, $t \in A$. Write $\sigma(x) = c_0 + c_1 x + \cdots \in \widehat{B}$, with $c_i \in R$. Since σ preserves the maximal ideal of B, we find that $c_0 \in \mathcal{M}_R$. A straightforward calculation using the fact that σ is an automorphism shows that $c_1 \notin \mathcal{M}_R$. Thus, the power series t has reduced order $|H|$ (that is, modulo $\mathcal{M}_R$, t is exactly divisible by $x^{|H|}$). It follows from [8], VII.3, no 8, corollary of proposition 5, that the morphism $R[[T]] \to R[[x]]$, sending T to t, is injective, and $R[[x]]$ is a free $R[[T]]$-module with basis $1, x, \ldots, x^{|H|-1}$.

Consider now the inclusions

$$R^H[[t]] \subseteq R[[t]] \subseteq \widehat{B} = R[[x]].$$

It is clear that $R[[t]]$ is free of rank dividing $|H|$ over $R^H[[t]]$. It follows that $\widehat{B}$ is free of rank dividing $|H|^2$ over $R^H[[t]]$. Consider now the inclusions

$$R^H[[t]] \subseteq (\widehat{B})^H \subseteq \widehat{B}.$$

Since $R^H[[t]]$ is regular and $(\widehat{B})^H$ is normal of dimension 2 (and, hence, has depth 2), $(\widehat{B})^H$ must be a free $R^H[[t]]$-module ([28], 18.H). Its rank is the degree of the associated extension of fields of fractions, which divides $|H|$, since the degree of the field of fractions of $\widehat{B}$ over the field of fractions of $(\widehat{B})^H$ is exactly $|H|$.

Since $(\widehat{B})^H$ is a free $R^H[[t]]$-module of rank at most $|H|$, we obtain from the surjection $(\widehat{B})^H/(\mathcal{M}_{R^H[[t]]}(\widehat{B}^H))^n \to (\widehat{B})^H/(\mathcal{M}_{(\widehat{B})^H})^n$ that for all sufficiently large n,

$$g_{(\widehat{B})^H}(n) \leq |H| \cdot g_{R^H[[t]]}(n).$$

Dividing both sides by n^2 and taking the limit as $n \to \infty$, it follows immediately from the definition of multiplicity that

$$\text{mult}((\widehat{B})^H) \leq |H| \cdot \text{mult}(R^H[[t]]) = |H|.$$

Since $R^H[[t]] \subseteq \widehat{A} \subseteq (\widehat{B})^H$ and $\widehat{A}$ is also normal (2.2), the same argument shows that mult$(\widehat{A}) \leq |H|$.

Assume now that B is of type II, and let $p := \mathrm{char}(k) \geq 0$. Consider the induced action of H on the k-vector space $\mathcal{M}_B/\mathcal{M}_B^2$. After making a linear change of variables if necessary, we may assume that the action of a generator of the cyclic group H on the classes of u and v is in Jordan canonical form

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix} \text{ or } \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}.$$

The eigenvalues α and β are $|H|$-th roots of unity, and the case of a single Jordan block can only occur when $p > 0$, and which case p divides $|H|$.

Let $x := \prod_{\sigma \in H} \sigma(u)$, and $y := \prod_{\sigma \in H} \sigma(v)$. An easy computation shows that modulo the ideal $(u,v)^{|H|+1}$, $x \equiv u^{|H|}$, and $y \equiv v^{|H|}$ if the action is diagonalizable. When the action consists of a single Jordan block, we find that

$$\begin{aligned} y &\equiv v(u+\alpha v)(2\alpha u + \alpha^2 v)\ldots((|H|-1)\alpha^{|H|-2}u + \alpha^{|H|-1}v) \\ &\equiv \alpha^{\frac{(|H|-1)|H|}{2}}((\alpha v)^p - \alpha v u^{p-1})^{|H|/p}. \end{aligned}$$

One verifies that x and y form a system of parameters of $k[[u,v]]$. Hence, the map $k[[X,Y]] \to k[[u,v]]$, which sends X to x and Y to y, is injective with image $k[[x,y]]$, and $k[[u,v]]$ is a finitely generated module over $k[[x,y]]$ ([37], Corollary 2 on page 293, Remark on page 293, and Corollary 2 on page 300). One verifies then that $k[[u,v]]$ is a free $k[[x,y]]$-module of rank $|H|^2$, with basis $\{u^i v^j, 0 \leq i,j \leq |H|-1\}$. It follows as in the case of Type I that $\widehat{A}$ and $(\widehat{B})^H$ are free of rank dividing $|H|$ over $k[[x,y]]$, and that both $\mathrm{mult}(\widehat{A})$ and $\mathrm{mult}((\widehat{B})^H)$ are bounded by $|H|$. □

Remark 2.4 We review the definition of the fundamental cycle Z associated with an intersection matrix N in 3.4. Let us note here that the above theorem imposes a non-trivial condition on the fundamental cycle of the resolution of a quotient singularity, since it is known that its self-intersection $|Z^2|$ is bounded by the multiplicity of B^H ([36], 2.7).

2.5 Let A be a normal local ring of dimension 2 with maximal ideal $\mathcal{M}_A$. Let $Z := \mathrm{Spec}(A)$, and $U := Z \setminus \{\mathcal{M}_A\}$. Assume that a desingularization $f : X \to Z$ exists. This is the case for instance if A is noetherian and excellent (see, e.g., [4], 1.1). In particular, X is regular, f is proper, and the restriction of f to $X \setminus f^{-1}(\mathcal{M}_A) \to U$ is an isomorphism.

Denote by $E_1, \ldots, E_n$ the irreducible components of $f^{-1}(\mathcal{M}_A)$. Let $(C,D)_X$ denote the intersection number of two divisors C and D on the regular scheme X. The intersection matrix associated with the exceptional divisor $f^{-1}(\mathcal{M}_A)$ is the matrix $N := ((E_i, E_j)_X)_{1 \leq i,j \leq n}$. The Smith group Φ_N of the matrix N is defined to be the quotient $\mathbb{Z}^n/\mathrm{Im}(N)$ (3.2). Our next theorem describes some properties of the group Φ_N in several important instances.

We review first some facts proved, for instance, in section 14 of [17]. Let $\mathbf{E}$ denote the free $\mathbb{Z}$-module with basis the irreducible components $E_1, \ldots, E_n$ of $f^{-1}(\mathcal{M}_A)$. By construction, the restricted morphism $f : X \setminus f^{-1}(\mathcal{M}_A) \to U$ is an isomorphism. Using its inverse followed by the open immersion $X \setminus f^{-1}(\mathcal{M}_A) \to X$, we obtain a morphism $U \to X$, and an associated 'restriction' map

$$\rho : \mathrm{Pic}(X) \longrightarrow \mathrm{Pic}(U).$$

The group homomorphism ρ is surjective, with kernel $\mathbf{E}$. Define

$$\theta : \mathrm{Pic}(X) \longrightarrow \mathbf{E}^* := \mathrm{Hom}(\mathbf{E}, \mathbb{Z})$$

by the rule $\theta(\Delta)(E_i) := (\Delta, E_i)_X$, where for any divisor class Δ represented by a divisor D, we set $(\Delta, E_i)_X := (D, E_i)_X$. Let $\mathrm{Pic}^0(X) := \mathrm{Ker}(\theta)$. Then we have the following exact sequence ([17], 14.2):

$$(2.5.1)\qquad 0 \longrightarrow \rho(\mathrm{Pic}^0(X)) \longrightarrow \mathrm{Pic}\,(U) \longrightarrow \Phi_N \longrightarrow \mathrm{Coker}\,(\theta) \longrightarrow 0.$$

The group $\mathrm{Coker}\,(\theta)$ is trivial when A is Henselian ([17], 14.3 and 14.4). The group $\mathrm{Pic}\,(U)$ is isomorphic to the divisor class group $\mathrm{Cl}(A)$.

Consider now a local domain B endowed with an action of a finite group H, such that $B^H = A$. There are natural group homomorphisms $\mathrm{Cl}(A) \to \mathrm{Cl}(B)$ and $\mathrm{Cl}(B) \to \mathrm{Cl}(A)$ (the norm homomorphism), whose composition is the multiplication by $|H|$ on $\mathrm{Cl}(A)$ ([8], 535-536). When B is a unique factorization domain, such as when B is regular, then $\mathrm{Cl}(B) = (0)$, and it follows that $|H|$ kills $\mathrm{Cl}(A)$ (which is isomorphic to $\mathrm{Pic}\,(U)$).

Theorem 2.6. *Let A be a normal local ring of dimension 2 such that $Z := \mathrm{Spec}\, A$ admits a desingularization $f : X \to Z$. Keep the notation introduced in 2.5.*

(a) *Assume that there exists a complete regular local ring B endowed with an action of a finite group H and such that $B^H = A$. Then $|H|$ kills Φ_N.*
(b) *Assume that there exists a regular local ring B of type I or II endowed with an action of a finite group H such that $B^H = A$. Assume also that either $|H|$ is coprime to $\mathrm{char}\,(A/\mathcal{M}_A)$, or that $\mathrm{char}\,(A) = 0$. Then $|H|$ kills Φ_N.*
(c) *Let $\mathcal{O}_K$ be a Henselian discrete valuation ring, with algebraically closed residue field k and field of fractions K. Let V/K be a smooth proper geometrically connected curve. Let L/K denote the Galois extension minimal with the property that V_L/L has semi-stable reduction. Let $\mathcal{Y}/\mathcal{O}_L$ denote the minimal regular semi-stable model of V_L/L. Let $H := \mathrm{Gal}(L/K)$ and let $\mathcal{Z} := \mathcal{Y}/H$. Assume that H is generated by an element σ, and call σ_k the morphism induced by σ on $\mathcal{Y}_k$. Let P be a ramification point of the map $\mathcal{Y}_k \to \mathcal{Y}_k/\langle\sigma_k\rangle$ and assume that $\sigma(\mathcal{O}_{\mathcal{Y},P}) \subseteq \mathcal{O}_{\mathcal{Y},P}$. Let Q be the image of P in $\mathcal{Z}$. Let $A := \mathcal{O}_{\mathcal{Z},Q}$. Then $|H|$ kills the group Φ_N associated with a resolution of* $\mathrm{Spec}\, A$.

Proof. (a) It suffices to note that $A = B^H$ is also complete, and, hence, Henselian, so that $\mathrm{Coker}\,(\theta)$ is trivial. Since $|H|$ kills $\mathrm{Pic}\,(U)$, it also kills Φ_N in this case.

(b) Let $\widehat{B}$ denote the completion of the local ring B with respect to its maximal ideal $\mathcal{M}_B$. Consider the canonical injection $\widehat{A} \to (\widehat{B})^H$. Under our hypotheses, it follows from 2.1 and 2.2 that A is excellent, and that this map is an isomorphism. Since a resolution of $\mathrm{Spec}\,(A)$ gives by base change a resolution of $\mathrm{Spec}\,(\widehat{A})$ ([4], 1.7), we may apply part (a) to $\mathrm{Spec}\,((\widehat{B})^H)$ to conclude that $|H|$ kills Φ_N.

(c) Let $\mathcal{X} \to \mathcal{Z}$ denote a desingularization of $\mathcal{Z} := \mathcal{Y}/H$. Let $Z := \mathrm{Spec}(A)$, and let $X := \mathcal{X} \times_{\mathcal{Z}} Z \to Z$ be a desingularization of Z. Let N be the intersection matrix associated with X. By hypothesis, the regular domain $\mathcal{O}_{\mathcal{Y},P}$ is endowed with an action of H, and its ring of invariants $\mathcal{O}_{\mathcal{Y},P}^H$ is nothing but $\mathcal{O}_{\mathcal{Z},Q} = A$. Thus, the discussion in 2.5 can be applied to A, and we find using the sequence (2.5.1) that Φ_N is killed by $|H|$ if $\mathrm{Coker}\,(\theta) = (0)$. Let us now show that $\mathrm{Coker}\,(\theta) = (0)$. By hypothesis, $\mathcal{O}_K$ is Henselian. Given any irreducible component C of multiplicity r in the special fiber $\mathcal{X}_k$, there exists a field M/K of degree r and a M-rational point P on V/K whose closure $\overline{\{P\}}$ in $\mathcal{X}$ intersects $\mathcal{X}_k$ exactly in one smooth point of C, with $(\overline{\{P\}}, C)_{\mathcal{X}} = 1 = (\overline{\{P\}}, \mathcal{X}^{red})_{\mathcal{X}}$ (use for instance [12], 8.4). For each irreducible component E_i in the desingularization of Q in X, we can restrict to X the corresponding divisor $\overline{\{P_i\}}$ on $\mathcal{X}$. This shows that the map $\theta : \mathrm{Pic}\,(X) \to \mathbf{E}^*$ is surjective, since $\mathbf{E}^*$ is generated by the images of the classes $\overline{\{P_1\}}, \dots, \overline{\{P_n\}}$. $\square$

Example 2.7 Theorem 2.6, when applicable, shows in particular that the absolute value $|\det(N)|$ of the determinant of the intersection matrix N of a resolution of a $\mathbb{Z}/p\mathbb{Z}$-quotient singularity is a power of p.

In [31], Example 10, a $(\mathbb{Z}/2\mathbb{Z})$-quotient singularity has resolution graph E_8, thus producing an example with $\det(N) = 1$. It would be interesting to determine whether an intersection matrix N with $\det(N) = 1$ can possibly appear as the intersection matrix of a $\mathbb{Z}/p\mathbb{Z}$-quotient singularity for infinitely many p.

In [31], Example 7, a $(\mathbb{Z}/3\mathbb{Z})$-quotient singularity B^H has resolution graph E_6, which has determinant $p = 3$. This singularity is rational, with fundamental cycle Z having $Z^2 = -2$. Since the singularity is rational, it follows that the multiplicity of B^H is equal to $|Z^2|$ ([3], Corollary 6), and we note that in this example, $|Z^2| < p$.

In both examples from [31] quoted above, the ring of invariant B^H is explicitly described, but the details of the resolutions of the singularities are omitted. This author has not independently verified the omitted computations.

Theorem 2.8. *Let B be a complete regular noetherian local ring of dimension 2, endowed with an action of a finite group H. Assume that the residue field k of B is algebraically closed of characteristic $p > 0$. Let $A := B^H$. Assume that there exists a desingularization $f : X \to \operatorname{Spec}(A)$. Assume also that the components of $f^{-1}(\mathcal{M}_A)$ are smooth and that the divisor $f^{-1}(\mathcal{M}_A)$ has normal crossings. Then the graph associated with $f^{-1}(\mathcal{M}_A)$ is a tree, and each irreducible component of $f^{-1}(\mathcal{M}_A)$ is a rational curve.*

Proof. As we explained just before 2.6, our hypotheses imply that the group $\operatorname{Pic}(U) = \operatorname{Cl}(A)$ is killed by $|H|$. Therefore, since the kernel $\mathbf{E}$ of the natural map $\operatorname{Pic}(X) \to \operatorname{Pic}(U)$ is free, we find that the torsion subgroup of $\operatorname{Pic}(X)$ is killed by $|H|$.

The ring A is normal and excellent, so that a desingularization $f : X \to \operatorname{Spec}(A)$ exists, and any such proper birational morphism f can be obtained as the blow-up of an ideal I of A whose radical is $\mathcal{M}_A$ ([19], C. on page 155). As in section IV.6 of [10], we let n_0 denote an integer such that $H^q(X, I^n\mathcal{O}_X) = 0$ for all $n > n_0$ and $q > 0$. Let X_n denote the base change of $X \to \operatorname{Spec}(A)$ with $\operatorname{Spec}(A/I^{n+1}) \to \operatorname{Spec}(A)$. Then [10], IV.6.1, shows that the canonical homomorphism $\operatorname{Pic}(X_{n+1}) \to \operatorname{Pic}(X_n)$ is bijective for all $n > n_0$. As in the proof of [10], IV.6.2, Grothendieck's Existence Theorem shows that $\operatorname{Pic}(X) = \varprojlim \operatorname{Pic}(X_n)$, so that $\operatorname{Pic}(X) = \operatorname{Pic}(X_n)$ if $n > n_0$.

Let X_k denote the fiber of f above the closed point of $\operatorname{Spec}(A)$. The natural composition $X_k^{red} \to X_k \to X_n$ is then defined by a nilpotent ideal J. We claim that the natural map $\operatorname{Pic}(X_n) \to \operatorname{Pic}(X_k^{red})$ is surjective with kernel a torsion group killed by a power of p. Indeed, let N denote the nilradical of the structure sheaf of X_n. Then there exists a filtration of the form $(0) = N^sJ \subset N^{s-1}J \subset \cdots \subset NJ \subset J$. Each of these ideals defines a closed subscheme of X_n, with natural morphisms

$$X_k^{red} = X^{(0)} \longrightarrow X^{(1)} \longrightarrow \ldots \longrightarrow X^{(s-1)} \longrightarrow X^{(s)} = X_n.$$

Recall now Proposition 4.1 in [8]: Let R be a local noetherian ring, and let $Y \to \operatorname{Spec}(R)$ be a proper morphism. Let $\mathcal{N}$ be the nilradical of $\mathcal{O}_Y$, and let $\mathcal{J}$ be an ideal of $\mathcal{O}_Y$ such that $\mathcal{N}\mathcal{J} = (0)$. Let Y' denote the closed subscheme of Y defined by $\mathcal{J}$. Then the sequence of canonical homomorphisms

$$H^1(Y, \mathcal{J}) \longrightarrow \operatorname{Pic}(Y) \longrightarrow \operatorname{Pic}(Y') \longrightarrow H^2(Y, \mathcal{J})$$

is exact. We can use this proposition for each morphism $X^{(i-1)} \to X^{(i)}$. Since the schemes $X^{(i)}$ have dimension 1, the sheaf cohomology groups H^2 must all vanish. Since $p \in \mathcal{M}_A$, we find that the group H^1 occurring in each exact sequence is killed by a power of p, and the claim follows.

Let C_i, $i = 1, \dots, n$, denote the irreducible components of X_k. The smooth commutative group scheme $\mathrm{Pic}^0_{X_k^{red}/k}$ is an extension of the abelian variety $\prod_{i=1}^n \mathrm{Pic}^0_{C_i/k}$ by a torus of dimension equal to the first Betti number of the graph associated with X_k ([9], 9.2/8). To prove our theorem, it suffices to show that $\mathrm{Pic}^0_{X_k^{red}/k}$ is trivial. Suppose that it is not trivial. Then there exists a nontrivial torsion point L in $\mathrm{Pic}^0_{X_k^{red}/k}(k)$ of order ℓ coprime to $p|H|$. Since $\mathrm{Pic}(X_n) \to \mathrm{Pic}(X_k^{red})$ is surjective and its kernel is a torsion group, L lifts to a torsion point of order divisible by ℓ in $\mathrm{Pic}(X_n) = \mathrm{Pic}(X)$, contradicting the fact that $|H|$ kills the torsion subgroup of $\mathrm{Pic}(X)$. □

Remark 2.9 It is asserted in the Math Review of [2] (MR0374136) that the exceptional configuration of the resolution of a certain $\mathbb{Z}/2\mathbb{Z}$-singularity forms a cycle of rational curves. Theorem 2.8 contradicts this assertion.

A variation on Theorem 2.8 is as follows.

Lemma 2.10. *Let $\mathcal{O}_K$ be a complete discrete valuation domain with algebraically closed residue field k and field of fractions K. Let X_K/K be a smooth proper geometrically connected curve. Let L/K denote the Galois extension minimal with the property that X_L/L has semi-stable reduction. Let $H := \mathrm{Gal}(L/K)$. Let $\mathcal{Y}/\mathcal{O}_L$ denote the minimal regular semi-stable model of X_L/L. Let $\mathcal{Z} := \mathcal{Y}/H$.*

(1) *Let Norm$(\mathcal{Z})/\mathcal{O}_L$ denote the normalization of $\mathcal{Z} \times_{\mathcal{O}_K} \mathcal{O}_L$ in the function field $L(X_L)$. Then the natural morphism $\varphi : \mathcal{Y} \to \mathrm{Norm}(\mathcal{Z})/\mathcal{O}_L$ is an isomorphism.*
(2) *Let $f : \mathcal{X} \to \mathcal{Z}$ denote a desingularization of $\mathcal{Z}$. Then any exceptional curve of f is rational.*
(3) *Assume that $\mathrm{Jac}(X_L)$ has good reduction over $\mathcal{O}_L$. Assume also that f is minimal with the property that every irreducible component of $\mathcal{X}_k$ is smooth and $\mathcal{X}_k$ is a divisor with normal crossings. Then the graph associated with the preimage in $\mathcal{X}$ of a singular point of $\mathcal{Z}$ is a tree.*

Proof. (1) The natural morphism $\varphi : \mathcal{Y} \to \mathrm{Norm}(\mathcal{Z})/\mathcal{O}_L$ is clearly an isomorphism on the generic fibers. The normalization map $\mathrm{Norm}(\mathcal{Z}) \to \mathcal{Z} \times_{\mathcal{O}_K} \mathcal{O}_L$ is finite. This follows from the fact that since $\mathcal{O}_K$ is a complete discrete valuation domain, then $\mathcal{Z}$ is an excellent scheme. It also follows from the fact that L/K is separable. We thus conclude that the model $\mathrm{Norm}(\mathcal{Z})/\mathcal{O}_L$ is proper. The morphism φ is quasi-finite, since the quotient map $\mathcal{Y} \to \mathcal{Z}$ is finite. We may therefore apply Zariski's Main Theorem to obtain that φ is an open immersion. Since the special fiber of the target of φ is connected and the special fiber of the source is proper, we find that φ is in fact an isomorphism.

(2) Consider the natural $\mathcal{O}_L$-morphism $\mathrm{Norm}(\mathcal{X}) \to \mathrm{Norm}(\mathcal{Z})$ induced by the $\mathcal{O}_K$-morphism $f : \mathcal{X} \to \mathcal{Z}$. Since the morphism $\mathrm{Norm}(\mathcal{Z}) \to \mathcal{Z} \times_{\mathcal{O}_K} \mathcal{O}_L \to \mathcal{Z}$ is finite, any component of $\mathrm{Norm}(\mathcal{X})$ above an exceptional component of f in $\mathcal{X}$ is contracted under $\mathrm{Norm}(\mathcal{X}) \to \mathrm{Norm}(\mathcal{Z})$. Since $\mathrm{Norm}(\mathcal{Z})$ is regular and minimal by (1), any component contracted by $\mathrm{Norm}(\mathcal{X}) \to \mathrm{Norm}(\mathcal{Z})$ is rational. Thus, all exceptional components of f are also rational.

(3) The fact that $\mathrm{Jac}(X_L)$ has good reduction over $\mathcal{O}_L$ implies that the toric rank of $\mathrm{Jac}(X_K)$ over $\mathcal{O}_K$ is zero. Under our hypotheses on $\mathcal{X}$, the toric rank of $\mathrm{Jac}(X_K)$ can be computed as the first Betti number of the graph associated with $\mathcal{X}_k$ (see, e.g., [21], 1.4). Thus, this graph is a tree. Since any subgraph of a tree is a tree, (3) follows. □

3. Intersection matrices

We develop in this section a completely combinatorial study of intersection matrices N, with a view towards an explicit determination of the invariants occurring in our theorems on quotient singularities. At the end of this section, starting in 3.17, we explicitly describe, for each prime p, a family of star-shaped intersection matrices N satisfying the combinatorial restrictions suggested by our theorems in the previous section. Many of these matrices do indeed arise as intersection matrices associated with cyclic quotient singularities (see 4.1, and [26], [27]).

Definition 3.1 An $n \times n$ *intersection matrix* $N = (c_{ij})$ is a symmetric negative definite integer matrix with negative coefficients on the diagonal, and non-negative coefficients off the diagonal. We associate a graph $G = G(N)$ to N as follows. Pick n vertices $v_1, \dots, v_n$, and for $i \neq j$ link v_i to v_j in G by exactly c_{ij} edges. We will always assume, unless stated otherwise, that G is connected. When this is the case, N is called *irreducible.*

Definition 3.2 Let N be an intersection matrix. Recall that there exist matrices $P, Q \in \mathrm{GL}_n(\mathbb{Z})$ such that $PNQ = \mathrm{diag}(d_1, \dots, d_n)$ with $d_1 \mid d_2 \mid \dots \mid d_n$. The diagonal matrix PNQ is called the Smith Normal form of N. We define the *Smith group* Φ_N of N to be the group $\Phi_N := \mathbb{Z}^n/N(\mathbb{Z}^n)$. Then $\mathbb{Z}^n/N(\mathbb{Z}^n)$ is isomorphic to $\prod_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$. Clearly, $|\Phi_N| = \det(N)$. We present in 3.14 a general formula for the size of Φ_N when $G(N)$ is a tree.

Recall that if $X, Y \in \mathbb{Z}^n$, we write $X > 0$ (resp., $X \geq 0$) if all coefficients of X are positive (resp., if all coefficients are non-negative). We write $X > Y$ if $X - Y > 0$, and we write $X \geq Y$ if $X - Y \geq 0$.

3.3 Let N be any symmetric integer matrix with negative integers on the diagonal, and non-negative integers off the diagonal, and assume that its associated graph is connected. In general, such a matrix need not be negative semi-definite. However, we claim that *if there exists a integer vector $R > 0$ such that $NR \leq 0$, then either $NR = 0$ and N is negative semi-definite, or $NR \neq 0$ and N is non-singular and negative definite.*

Indeed, exercise 4.14 in [7], chapter 6, page 155, shows that $-N$ is an M-matrix, and exercise 4.15 implies that $-N$ is positive semi-definite. Suppose now that $NR \neq 0$. Then N is non-singular because otherwise $-N$ does not satisfy condition (5) of Theorem 4.16 in chapter 6 of [7] (alternatively, use Theorem 2.7 (ii) of *loc. cit.*). Then Theorem 2.3 in [7], page 134, implies that all principal minors of $-N$ are positive. Alternatively, use exercise 2.6 on page 141.

When exhibiting below a symmetric integer matrix N with negative integers on the diagonal, and non-negative integers off the diagonal, we will always find it helpful to also exhibit an integer vector $R > 0$ with $NR \leq 0$ and $NR \neq 0$, providing in this way a proof that N is negative definite.

Definition 3.4 Attached to an intersection matrix N is a unique vector $Z > 0$ with positive integer coefficients, and such that the coefficients of NZ are negative or zero, and Z is minimal for this property. This vector is called the *fundamental cycle of* N ([3], p. 132).

The vector Z is in general quite a difficult invariant to understand. Therefore, for each $i = 1, \dots, n$, we define below a vector R_i associated to N which is an upper bound for the fundamental cycle Z of N (i.e., $Z \leq R_i$), and is quite easy to compute in terms of N. We found such substitutes for Z quite useful, since for instance, as we shall see in 3.14, given N and one such vector R_i, the order of Φ_N can be given explicitly. In addition, such vectors R_i naturally arise when considering the resolution of singularities of a normal model of a curve.

Let N^* denote the adjoint of N. By definition, N^* is the matrix whose (i,j)-term is the (i,j)-cofactor of the transpose of N, so that $NN^* = \det(N)\mathrm{Id}_n = N^*N$. (When $N=(a)$, we set $N^*=(1)$.) Let $e_1,\ldots,e_n$ denote the standard basis of $\mathbb{Z}^n$. A symmetric irreducible non-singular positive definite matrix with non-positive off-diagonal coefficients has an adjoint with only positive coefficients ([7], Chapter 6, 2.5-2.7). As the intersection matrix N is non-singular, $-N$ has the above properties, and we find that $(-1)^{n+1}N^*$ has only non-negative coefficients. It follows that if we let $(-1)^{n+1}R_i$ denote the i-th column vector of N^* divided by the greatest common divisor of its coefficients, then R_i has positive coefficients, and $NR_i = -p_ie_i$ for some positive integer p_i. Note that the matrix N can be completely recovered from the graph $G(N)$ and the equality $NR_i = -p_ie_i$. Let us also note the following easy fact.

Lemma 3.5. *Let τ_i denote the class of the vector e_i in the quotient group $\Phi_N := \mathbb{Z}^n/N(\mathbb{Z}^n)$. Then the order of τ_i is p_i.*

Proof. Suppose that the order of τ_i is a. By construction, $NR_i = -p_ie_i$. Thus $a \mid p_i$. By hypothesis, there exists a vector $S \in \mathbb{Z}^n$ such that $NS = ae_i$. Write $ab = p_i$, and consider the equation $N(bS+R_i)=0$. Since N is invertible, $bS = -R_i$. Since the greatest common denominators of the coefficients of R_i is 1, we find that $b=1$. □

3.6 By minimality of the fundamental cycle Z, the vector $S := \inf_i(R_i)$ is also an upper bound for Z. However, even though the vector S is canonically associated with N, it is not in general the fundamental cycle of N.

The knowledge of a vector R_i provides a bound on the self-intersection $|Z^2|$. Indeed, since $Z \le R_i$, write $R_i = Z + X$ with $X \ge 0$. Then $R_i^2 = Z^2 + 2Z\cdot X + X^2$. Since N is negative definite, $X^2 \le 0$, and since Z is the fundamental cycle, $Z \cdot X \le 0$. Hence,

$$|Z^2| \le |R_i^2|, \text{ for all } i = 1,\ldots,n.$$

We also note here a bound for $|Z^2|$ of a different type. Let $1 \le z_{min}$ denote the smallest coefficient of the vector Z. Let e denote the exponent of the group Φ_N. Then

$$|Z^2| \le e z_{min}. \tag{3.6.1}$$

Indeed, write ${}^tZ = (z_1,\ldots,z_n)$, and assume that $z_{min} = z_i$. Then $|Z^2| \le |Z\cdot R_i| = p_iz_i \le ez_{min}$ (3.5). Our next lemma is immediate from this inequality. We also note that $|Z^2| \le p_iz_i$ implies that if $|\Phi_N| = 1$, then $Z = R_j$ for some j, and $|Z^2| = z_{min}$.

Lemma 3.7. *Assume that Φ_N is killed by an integer e, and that the fundamental cycle Z of N has a coefficient equal to 1. Then $|Z^2| \le e$.*

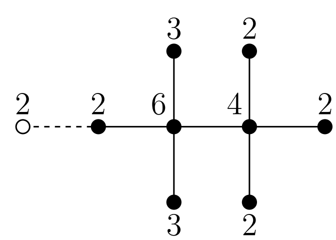
Remark 3.8 An intersection matrix N of type E_8 has trivial Smith group Φ_N and a fundamental cycle Z with $|Z^2| = z_{min} = 2$. Such an intersection matrix is shown in [31], Example 10, to occur as the intersection matrix associated with a $\mathbb{Z}/2\mathbb{Z}$-quotient singularity.

Remark 3.9 Let $\mathcal{X} \to \mathcal{Z}$ be a resolution of a singularity. Let $\mathcal{X}' \to \mathcal{X}$ be a proper birational morphism of regular schemes. Then the fundamental cycle Z' associated with the exceptional divisor of $\mathcal{X}' \to \mathcal{Z}$, and its intersection matrix N', can be easily expressed in terms of the fundamental cycle Z associated with the exceptional divisor of $\mathcal{X} \to \mathcal{Z}$ and its intersection matrix N (see, e.g., [36], 2.9). It is easy to check that $Z^2 = (Z')^2$, that z_{min} is also the minimum of the coefficients of Z', and that the groups Φ_N and $\Phi_{N'}$ are isomorphic.

Example 3.10 Our next example shows that the bound in (3.6.1) is sharp when $e > 1$, and that the hypothesis in 3.7 that the fundamental cycle Z of N has a coefficient equal to 1 cannot be removed. We give below a matrix N with its fundamental cycle Z, and an explicit computation of NZ. In our example, $e = 2$, and Φ_N is of order 16 (use 3.14). One checks by a direct computation that Φ_N is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$, that $z_{min} = 2$, and $|Z^2| = ez_{min} = 4$. It turns out that $Z = R_1$ in our example.

$$\begin{pmatrix} -4 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -2 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} 2 \\ 6 \\ 3 \\ 3 \\ 4 \\ 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} -2 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Notation 3.11 Let N be an intersection matrix. We found it useful to represent the data (N, R_i) using the graph $G(N)$ as follows. The graph $G(N)$ has vertices represented by bullets $\bullet$. A positive number next to a vertex represent the coefficient of this vertex in R_i, and a negative number next to a vertex is the self-intersection of the vertex in N. We represent the relation $NR_i = -p_i e_i$ by attaching a 'virtual' vertex to C_i, represented by an open circle, and we adorn this virtual vertex by p_i. In many situations, it is possible to think of this virtual vertex as the vertex of a larger graph to which $G(N)$ is attached. Note that $G(N)$, R_i, and NR_i, suffice to recover N. With this notation, the matrix $(N, R_1 = Z)$ in above example is represented as follows:



3.12 For later use in describing intersection matrices, we record here the following standard construction. Given an ordered pair of positive integers r and s with $\gcd(r, s) = 1$, we construct an associated intersection matrix $N = N(r, s)$ with vector $R_1 = R_1(r, s)$ and $NR_1 = -re_1$.

Suppose first that $r > s$. We can then find integers $b_1, \dots, b_m > 1$ and $s_1 = s > s_2 > \dots > s_m = 1$ such that $r = b_1 s - s_2$, $s_1 = b_2 s_2 - s_3$, and so on, until we get $s_{m-1} = b_m s_m$. These equations are best written in matrix form:

$$\begin{pmatrix} -b_1 & 1 & \dots & 0 \\ 1 & -b_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & \dots & 1 & -b_m \end{pmatrix} \begin{pmatrix} s_1 \\ \vdots \\ \vdots \\ s_m \end{pmatrix} = \begin{pmatrix} -r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We let N denote the above square matrix, and let R_1 be the first column matrix above. It is well-known that $\det(N) = \pm r$ (see, e.g, [24], 2.6).

The fundamental cycle Z of N is simply $Z = (1, \dots, 1)$. It is thus easy to find many examples of such matrices N with (up to sign) prime determinant, say p, and $|Z^2| \le p$.

When $r < s$, we first write $r = s - (s - r)$, and then proceed as above with the ordered pair s and $s - r$. We get

$$\begin{pmatrix} -1 & 1 & \dots & 0 \\ 1 & -c_1 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & \dots & 1 & -c_{m'} \end{pmatrix} \begin{pmatrix} s \\ s-r \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} -r \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We let again N denote the above square matrix, and R_1 the first column matrix. We leave it to the reader to check that $\det(N) = \pm r$ (use [24], 2.6).

For completeness, we note the following lemma.

Lemma 3.13. *Let N be an intersection matrix whose associated graph $G(N)$ does not have a node. Then Φ_N is cyclic of order $|\det(N)|$.*

Proof. By hypothesis, the graph $G(N)$ is a chain of, say, m vertices. Then there exists a permutation matrix T such that $T^{-1}NT$ is equal to a matrix of the form introduced in 3.12. Looking at the lower-left corner, we find an $(m-1) \times (m-1)$-minor having determinant 1. Thus, the Smith normal form of N must be $\mathrm{diag}(1, \dots, 1, \det(N))$. Hence, Φ_N is cyclic. □

Let N be an intersection matrix such that $G(N)$ is a tree. When the additional data of one of the vectors R_i defined in 3.4 is given, we show below how to compute the order of Φ_N. The group structure of Φ_N, on the other hand, is much more difficult to predict.

Given a graph G and a vertex v_i, let $d_{v_i}(G)$, or simply $d_i(G)$, denote the *degree* of v_i in G, that is, the number of edges of G attached to v_i. We call a vertex v_i with $d_i(G) = 1$ a *terminal* vertex. Note that a tree with at least two vertices always has a terminal vertex and, thus, in the explicit formula for $|\det(N)|$ given below, the right hand side is a priori only a rational number.

Theorem 3.14. *Let N be an $n \times n$-intersection matrix whose graph $G = G(N)$ is a connected tree with vertices $C_1, \dots, C_n$. Assume given a vector R_i defined in 3.4 with $NR_i = -p_i e_i$. Write ${}^tR_i := (r_1, \dots, r_n)$. Then*

$$|\det(N)| = p_i r_i \prod_{j=1}^{n} r_j^{d_j(G(N))-2},$$

and $p_i \gcd(p_i, r_i)$ divides $|\det(N)|$.

Proof. To prove the theorem, we first construct a larger integer matrix $M = (M_{ij})$ which contains the matrix N as a *principal* minor (i.e., the elements on the diagonal of N are also on the diagonal of M when N is viewed as a minor of M). The most favorable case is when $p_1 \mid r_1$.

When $p_1 \mid r_1$, let M be the symmetric $(n+1) \times (n+1)$-matrix, with N in its lower right corner, and with the coefficients of the first row of M being 0, except for $M_{11} := -r_i/p_i$ and $M_{1,i+1} := 1$. It follows that if we set ${}^tR := (p_i, {}^tR_i)$, then $MR = 0$. The pair $(-M, R)$ defines an arithmetical graph in the sense of [20], p. 481. The graph $G(M)$ associated with M has vertices $D_1, \dots, D_{n+1}$, with D_k linked to D_ℓ by $M_{k\ell}$ edges if $k \neq \ell$. It turns out that the graph $G(M)$ contains the graph $G(N)$, with vertices $C_1 = D_2, \dots, C_n = D_{n+1}$, and to obtain $G(M)$ from $G(N)$, one additional vertex, D_1, is attached by exactly one edge to C_i. In particular, $G(M)$ is a tree. Let Φ_M denote the torsion subgroup of $\mathbb{Z}^{n+1}/\mathrm{Im}(M)$. If M^{11} denote the minor of M obtain by removing the first row and first column from M, then $|\det(M^{11})| = |\Phi_M| p_i^2$ ([20], 1.3). Since $G(M)$ is a tree, the order of Φ_M is given explicitly by a formula involving the coefficients of R and the degrees of the vertices in $G(M)$ ([20], 2.5). Using this formula and the fact that $M^{11} = N$, we find that

$$|\det(N)| = \left(p_i^{-1} \prod_{j=1}^{n} r_j^{d_{C_j}(G(M))-2}\right) \cdot p_i^2.$$

Since $d_{C_j}(G(M)) = d_{C_j}(G(N))$ for $j \neq 0$ and $j \neq i$, and since $d_{C_i}(G(M)) - d_{C_i}(G(N)) = 1$, the theorem follows when $p_1 \mid r_1$.

The case where $p_i \nmid r_i$ requires a slightly more complicated construction. In order to be able to later refer to it when needed, we number it.

3.15 Using the data (N, R_i), we describe below how to embed the graph $G(N)$ into the graph of an arithmetical graph $(G(M), M, R)$, generalizing what we did above when $p_i \mid r_i$.

We proceed as follows when $p_i \nmid r_i$. We attach to $G(N)$ at C_i a chain of vertices $D_1, \dots, D_m$ to obtain the graph $G(M)$: D_1 is linked with one edge to both C_i and D_2, D_2 is linked by one edge to both D_1 and D_3, and so on. The terminal vertex on the chain is D_m. The matrix M restricted to the vertices of $G(N)$ is the matrix N. The matrix M restricted to the chain $D_1, \dots, D_m$ is up to permutation the matrix $N(r, s)$ constructed as in 3.12 with the ordered pair $r := r_i/\gcd(r_i, p_i)$ and $s := p_i/\gcd(r_i, p_i)$. (This latter requirement specifies the integer m and all the elements on the diagonal of M which corresponds to the vertices $D_1, \dots, D_m$.)

We define the vector R as follows: R is equal to R_i when restricted to $G(N)$, and when restricted to the chain $D_1, \dots, D_m$, it is equal to $\gcd(r_i, p_i)$ times the associated vector $R_1(r, s)$ constructed as in 3.12. One checks that by construction, $MR = 0$. The matrix M, with $MR = 0$ and its associated graph $G(M)$, defines an arithmetical tree. The minor of M corresponding to the chain $D_1, \dots, D_m$ has determinant $\pm r_i/\gcd(p_i, r_i)$.

We can now complete the proof of Theorem 3.14 when $p_i \nmid r_i$. Complete the tree $G(N)$ into an arithmetical tree $(G(M), M, R)$ as above. Consider the principal minor M_{D_1} of M, obtained from M by removing the row and the column corresponding to the vertex D_1 (whose coefficient in R is p_i). If $p_i \nmid r_i$, the matrix M_{D_1} consists of two blocks, and the determinant of both blocks can be computed explicitly to give

$$|\det(M_{D_1})| = |\det(N)| \cdot p_i/\gcd(p_i, r_i).$$

We now compute $\det(M_{D_1})$ in a different way using the fact that $G(M)$ is an arithmetical tree, to obtain $|\det(M_{D_1})| = |\Phi_M| p_i^2$, with an explicit formula for $|\Phi_M|$ given by

$$|\Phi_M| = \gcd(r_i, p_i)^{-1} \prod_{j=1}^{n} r_j^{d_{C_j}(G(M))-2}$$

([20], 1.3 and 2.5). Since now $|\det(N)| = |\Phi_M| p_i \gcd(p_i, r_i)$, Theorem 3.14 follows. □

Example 3.16 An A_n-singularity is resolved by a chain of n (-2)-curves. Call N_n its matrix (which up to permutation is of the form given in 3.20). Lemma 3.13 shows that the Smith group of N_n is cyclic. Its order is $n+1$, and can be determined using Theorem 3.14 with the relation $(n, n-1, \dots, 2, 1)N_n = (-(n+1), 0, \dots, 0)$.

We also have $(1, \dots, 1)N_n = (-1, 0, \dots, 0, -1)$, so that $Z = (1, \dots, 1)$ and $|Z^2| = 2$. When $n+1 = p$ is prime, it would be of interest to determine whether the matrix N_n can arise as the intersection matrix of a $\mathbb{Z}/p\mathbb{Z}$-quotient singularity. This question has recently been addressed in [14].

Example 3.17 Recall that a tree with exactly one node is called *star-shaped*. For each prime p, and for any integer $a \geq 2$, we exhibit below a class of intersection matrices N whose associated graph $G(N)$ is a star-shaped tree with exactly one node C, and $a+1$ terminal chains attached to it. A criterion for the Smith group Φ_N to be killed by p is given in 3.21, and a criterion for $|Z^2| \leq p$ is found in 3.22. The simplest matrices in the family are represented in 3.18.

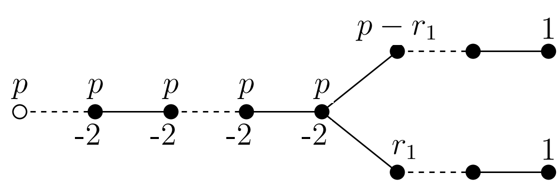
Fix $\alpha \geq 0$. Fix $a \geq 2$, and consider positive integers $r_1, \dots, r_a < p$, such that p divides $r_1 + \cdots + r_a$. The square matrix N (of some size n) that we are going to construct will have a graph G, and an associated vector R with $NR = -pe$ for some vector e belonging to the standard basis of $\mathbb{Z}^n$.

Let $D_1, \dots, D_a$, and C_1, denote the vertices of G connected to C. We set the coefficient of R corresponding to C to be p, the coefficient corresponding to D_i to be r_i, and the coefficient of C_1 to be p. The self-intersection of C is $(C \cdot C) := -(r_1 + \cdots + r_a + p)/p$.

The matrix N 'restricted' to the chain started by D_i is taken to be the matrix constructed in 3.12 using the ordered pair p and r_i. The vector R 'restricted' to the chain started by D_i is taken to be the corresponding vector described in 3.12. In particular, the coefficient of R corresponding to the terminal vertex of the chain is 1. The terminal chain started by C_1 consists of $\alpha - 1$ vertices, all of self-intersection -2. The vector R restricted to this terminal chain has all its coefficients equal to p.

It is easy to check that the vector NR has all its coefficients equal to 0, except for the coefficient corresponding to the last vertex on the chain started by C_1, where the coefficient of NR is $-p$.

Example 3.18 Let us denote by $N(p, \alpha, r_1)$ the simplest intersection matrix in the class of matrices introduced in 3.17: we take $a = 2$, and $r_2 := p - r_1$, so that the self-intersection of the node C is -2. We represent this intersection matrix and its associated vector R as follows, using the conventions introduced in 3.11:



The integer α is the number of vertices in the graph which have self-intersection -2 and multiplicity p. When $p = 2$, then r_1 must be 1, and the intersection matrix $N(2, \alpha, 1)$ corresponds to the Dynkin diagram D_m with $m = \alpha + 2$ being the number of vertices of the graph.

3.19 Consider the data (N, R) described in 3.17. Then we can use Theorem 3.14 to find that $|\Phi_N| = p^a$.

3.20 Let us explicitly note here that the matrix N restricted to the chain started by C_1 is the square matrix below, with the following relation:

$$\begin{pmatrix} -2 & 1 & 0 & & 0 \\ 1 & -2 & \ddots & \ddots & \\ 0 & \ddots & \ddots & 1 & 0 \\ & \ddots & 1 & -2 & 1 \\ 0 & & 0 & 1 & -2 \end{pmatrix} \begin{pmatrix} \alpha - 1 \\ \alpha - 2 \\ \vdots \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -\alpha \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}.$$

Lemma 3.21. *Let N denote the intersection matrix introduced in* 3.17*. Then Φ_N is killed by p if and only if p divides α.*

Proof. We proceed to perform a row and column reduction of the matrix N. Each chain can be dealt with separately, using the row and column operations in 2.5 of [24]. We leave it to the reader to check that the matrix N is row and column equivalent to a matrix consisting of two blocks, the Identity matrix of the appropriate size, and the matrix

$$A := \begin{pmatrix} (C\cdot C) & r_1 & \dots & r_a & \alpha-1 \\ 1 & -p & 0 & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \vdots \\ 1 & \vdots & \ddots & -p & 0 \\ 1 & 0 & \dots & 0 & -\alpha \end{pmatrix}.$$

Using its last line, the matrix A can be further reduced to the matrix

$$A' := \begin{pmatrix} 0 & r_1 & \dots & r_a & x \\ 0 & -p & 0 & \dots & \alpha \\ \vdots & 0 & \ddots & 0 & \vdots \\ 0 & \vdots & & -p & \alpha \\ 1 & 0 & \dots & 0 & 0 \end{pmatrix}$$

(where x is a entry that we need not make explicit). Let A'' denote the top right principal minor of A', of size $(a+1 \times a+1)$. Since $p^a = |\Phi_N|$, the group Φ_N is killed by p if and only if p divides the greatest common divisor of the determinants of the (2×2)-minors of A''. Clearly, if p kills Φ_N, then p divides the determinant

$$\begin{vmatrix} r_1 & x \\ 0 & \alpha \end{vmatrix}$$

and, hence, $p \mid \alpha$ since $p > r_1$. Suppose now that $p \mid \alpha$. Then, after having reduced A'' modulo p, it is easy to show that p divides the determinant of any (2×2)-minor of A''. $\square$

Lemma 3.22. *Assume that $\alpha \geq p$. Then the fundamental cycle Z of the intersection matrix N introduced in* 3.17 *is such that $|Z^2| \leq p$.*

Proof. Consider the vector $R > 0$ with $NR \leq 0$ associated with N in 3.17. Then $R \geq Z$, and $|R^2| \geq |Z^2|$ (3.6), but this inequality is not strong enough to prove our lemma in general since $|R^2| = p^2$. However, since R has a coefficient equal to 1 and $R \geq Z$, we find that $z_{min} = 1$, so that when Φ_N is killed by p, the lemma follows from 3.7.

When $\alpha \geq p$, let us modify the vector R as follows. Denote by $E_1, E_2, \dots, E_{\alpha-1}$ the consecutive vertices on the chain of $G(N)$ started by C_1, so that E_1 is the terminal vertex. In particular, $E_{\alpha-1} = C_1$, and for convenience, we will let $E_\alpha := C$, where C is the node of $G(N)$. Define $S \in \mathbb{Z}^n_{>0}$ to be a vector equal to R when restricted to the graph of $G(N)$ minus $E_1, \dots, E_{p-1}$, and set the coefficient of S corresponding to E_i to be i. Then $S > 0$, and it is easy to check that $NS = -e$, where e is the standard basis vector corresponding to the vertex E_p. Since the coefficient of S corresponding to E_p is equal to p, we find that $|S^2| = p$, so that $|Z^2| \leq p$, as desired. $\square$

For future reference, we record here:

Corollary 3.23. *Let $N = N(p, \alpha, r_1)$ be the intersection matrix introduced in* 3.18*, with fundamental cycle Z. When p divides α, then $\Phi_N \simeq (\mathbb{Z}/p\mathbb{Z})^2$ and $|Z^2| \leq p$.*

Proof. Follows from 3.19, 3.21, and 3.22. □

Intersection matrices of type $N(2, 2\beta, 1)$ are shown in 4.1 to arise as intersection matrices of wild $\mathbb{Z}/2\mathbb{Z}$-quotient singularities. A larger subclass of the matrices introduced in 3.17 will be shown to arise as intersection matrices of $\mathbb{Z}/p\mathbb{Z}$-quotient singularities for all odd primes p in [26] and [27]. These matrices also arise in Theorem 2.2 of [25].

4. Examples with $p = 2$

It is known that a tame $\mathbb{Z}/2\mathbb{Z}$-quotient singularity has a resolution with an irreducible exceptional divisor. In contrast, as the following theorem shows, there is no bound on the number of irreducible components in the exceptional divisor of the minimal resolutions of wild $\mathbb{Z}/2\mathbb{Z}$-quotient singularities.

Theorem 4.1. *Let $\beta \geq 1$ be any integer. Then there exist an excellent regular local ring B of mixed characteristic $(0, 2)$, and when β is odd, an excellent regular local ring B' of equicharacteristic 2, both endowed with an action of $\mathbb{Z}/2\mathbb{Z}$, such that the resolution of the associated wild quotient singularities on $\operatorname{Spec} B^H$ and $\operatorname{Spec}(B')^H$ have intersection matrices equal up to permutation to the matrix $N(2, 2\beta, 1)$ described in* 3.18.

This theorem will follow from results on the reduction of certain elliptic curves which may be of independent interest. The proof of Theorem 4.1 is postponed to 4.8.

Recall that an elliptic curve C/k over an algebraically closed field of characteristic $p > 0$ is called *ordinary* if $C(k)$ has exactly p points of order dividing p. Otherwise, it is called *supersingular* and $C(k)$ does not have any point of order exactly p. When $p = 2$, only one isomorphism class of elliptic curves is supersingular, the class with j-invariant $j = 0$.

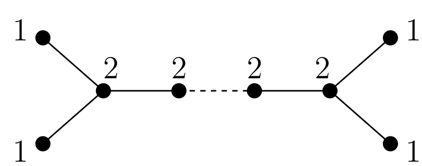
Let $\mathcal{O}_K$ be a Henselian discrete valuation domain, with field of fractions K, uniformizer π_K, and algebraically closed residue field k. We let $p := \operatorname{char}(k)$. Let E/K be an elliptic curve having potentially good reduction. By definition, E/K is such that there exists a finite Galois extension L/K such that E_L/L has a smooth model $\mathcal{Y}/\mathcal{O}_L$. The generic fiber of $\mathcal{Y}$ is isomorphic to the curve E_L/L. We denote by $\mathcal{Y}_k$ the special fiber, which by assumption is an elliptic curve. When $\mathcal{Y}_k$ is an ordinary elliptic curve, we say that E/K has *potentially good ordinary reduction*.

Assume L/K Galois, and let $H := \operatorname{Gal}(L/K)$. Attached to the extension L/K is a sequence of (not necessarily distinct) subgroups of H, the *higher ramification groups* $H = H_0 \rhd H_1 \rhd \dots$. The valuation of the different of the extension $\mathcal{O}_L/\mathcal{O}_K$ is expressed using Hilbert's formula: $\sum_{i=0}^{\infty}(|H_i| - 1)$ (see, e.g., [32], IV.2, Proposition 4). For convenience, we define $s_{L/K}$ by the formula

$$s_{L/K} + 1 = \sum_{i=0}^{\infty}(|H_i| - 1).$$

Then $s_{L/K} > 0$ if and only if L/K is wild.

Recall that the special fibers of minimal regular models of elliptic curves are labeled with a Kodaira symbol. The symbol I_n^* refers to a special fiber consisting in a configuration of $n+5$ rational curves, 4 of them of multiplicity 1, and $n+1$ of multiplicity 2, with dual graph given by



Theorem 4.2. *Let $\mathcal{O}_K$ be a Henselian discrete valuation domain with algebraically closed residue field k of characteristic 2. Let E/K be an elliptic curve with additive reduction and potentially good ordinary reduction. Then there exists a quadratic extension L/K such that E_L/L has a smooth model $\mathcal{Y}/\mathcal{O}_L$, and E/K has reduction of type $I^*_{4s_{L/K}}$.*

Proof. We first treat the equicharacteristic case. Any ordinary elliptic curve can be given over K by an equation $y^2+xy = x^3+a_2x^2+a_6$, with $a_6 \neq 0$ (the non-trivial 2-torsion point is $(0, \sqrt{a_6})$) (see, e.g., [33], App. A, 1.1). This latter equation has $\Delta = a_6$, and $j = 1/a_6$. It follows that this curve has potentially good reduction if and only if $a_6 \notin \pi_K\mathcal{O}_K$. Since the curve with $j = 0$ is supersingular when $p = 2$, we find that the reduction is potentially good and ordinary if and only if $a_6 \in \mathcal{O}_K^*$. The reduction is good when $a_2 \in \mathcal{O}_K$ (reduce mod π_K the above equation). In general, this curve achieves good reduction over $L := K(z)$ with $z^2 + z + a_2 = 0$ (to see this, make the change of variables $y = Y + zx$). Since we assume that E/K has additive reduction, the extension L/K must be non-trivial and ramified.

Let v denote the discrete valuation of K, and v_L the valuation of L. We claim that it is possible to change coordinates such that the new coefficient a_2' has odd negative valuation. Indeed, suppose that $a_2 = u/\pi_K^{2m}$ with $v(u) = 0$. Since k is algebraically closed, it is possible to find $b \in \mathcal{O}_K$ such that $\pi_K \mid (b^2 + u)$. Then the change of variables $y = Y + \frac{b}{\pi_K^m}x$ produces the new equation

$$Y^2 + xY = x^3 + \frac{b^2 + \pi_K^m b + u}{\pi_K^{2m}}x^2 + a_6,$$

with $v(\frac{b^2+\pi_K^m b+u}{\pi_K^{2m}}) > -2m$. Since the extension L/K must be ramified, repeating this process finitely many times must lead to a new equation where the new coefficient a_2' has odd negative valuation. It is easy to check that L is the splitting field of both $z^2 + z + a_2$ and $t^2 + t + a_2'$.

Assume then that $a_2 = u\pi^{-r} \in K^*$ with negative odd valuation $-r$ and u a unit. Our elliptic curve E/K is given by the equation $y^2 + xy = x^3 + a_2x^2 + a_6$. Set s such that $r = 2s - 1$. An integral equation for E/K with $v(\Delta) = 12s$ is given by

$$y^2 + \pi^s xy = x^3 + \pi^{2s}Dx^2 + \pi^{6s}a_6.$$

It follows from Tate's Algorithm ([34], IV 9.4, p. 367) that this equation for E/K is already minimal. More precisely, our equation satisfies the conditions of Step 7 in *loc. cit.* We leave it to the reader to show that the reduction is of type I^*_{4r}. An easy computation shows that the higher ramification groups satisfy $H_0 = \cdots = H_r = \mathbb{Z}/2\mathbb{Z}$, and $H_{r+1} = \{0\}$, so that $r = s_{L/K}$, as desired. This complete the proof of the theorem in the equicharacteristic 2 case.

Assume now that K is of mixed characteristic 2. An elliptic curve has potentially good ordinary reduction if and only if its j-invariant is a unit in $\mathcal{O}_K$. Let $j_0 \in \mathcal{O}_K^*$, and let E_{j_0}/K be the elliptic curve given by the equation

$$y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}.$$

This is an elliptic curve with $j(E_{j_0}) = j_0$ and $\Delta = j_0^2/(j_0 - 1728)^3$. Since $v(j_0) = 0$, we find that this curve has good (ordinary) reduction over $\mathcal{O}_K$.

Since $j_0 \neq 0$ and $j_0 \neq 1728$ by hypothesis, an elliptic curve with j-invariant j_0 has only two automorphisms. Therefore, we find that two curves with same j-invariant j_0 are quadratic twists of each other.

Since we assume that $\mathcal{O}_K$ has algebraically closed residue field, we find that any non-trivial extension L/K is ramified. It follows that an elliptic curve E/K with j-invariant j_0 and with additive reduction and potentially good ordinary reduction is a quadratic twist of E_{j_0}/K by a ramified quadratic extension L/K. Pick $D \in \mathcal{O}_K$ such that $L := K(\sqrt{D})$ has degree 2 over K, and consider the quadratic twist E_D/K given by the equation

$$y^2 = x^3 + \frac{D}{4}x^2 - D^2Ax - D^3B, \tag{4.2.1}$$

with $A = 36/(j_0 - 1728)$ and $B = 1/(j_0 - 1728)$. Without loss of generality, we may assume that $v(D) = 0$ or 1. Consider first the case where $v(D) = 1$. The equation (4.2.1) is not integral, and an obvious change of variables transforms it in

$$y^2 = x^3 + Dx^2 - 2^4D^2Ax - 2^6D^3B.$$

We conclude from Tate's algorithm that the reduction is of type I^*_{2n} with $n = 4v(2)$. The valuation of the different of the extension L/K is computed as follows: $\sqrt{D}$ is a uniformizing parameter, and $\sigma(\sqrt{D}) - \sqrt{D} = -2\sqrt{D}$ has valuation $v_L(2) + 1$. It follows that $\sum_{i=0}^{\infty}(|H_i| - 1) = v_L(2) + 1$, so that the reduction is $I^*_{4v_L(2)}$, as desired.

When $v(D) = 0$, consider an Eisenstein equation for L/K, given by the equation $z^2 + az + b$, with $v(a) \geq 1$ and $v(b) = 1$. It follows that $a^2 - 4b = Dc^2$ for some element with $v(c) \geq 0$. More precisely, we must have $v(a) = v(c) \leq v(2)$. The valuation of the different of the extension L/K is computed as follows: a root β of $z^2 + az + b = 0$ is a uniformizing parameter, and $\sigma(\beta) - \beta = -a - 2\beta$. Thus, $v_L(\sigma(\beta) - \beta) = v_L(a)$. It follows that $\sum_{i=0}^{\infty}(|H_i| - 1) = v_L(a)$. Our goal is to show that the reduction is then $I^*_{4(v_L(a)-1)}$. Note that $\frac{D}{4} - \frac{a^2}{4c^2} = -\frac{b}{c^2}$. Make the change of variables $y = Y + \frac{a}{2c}x$ in (4.2.1) to obtain an equation of the form

$$y^2 + \frac{a}{c}xy = x^3 - \frac{b}{c^2}x^2 - D^2Ax - D^3B.$$

This equation is not integral, and an obvious change of variables transforms it into

$$y^2 + axy = x^3 - bx^2 - c^4D^2Ax - c^6D^3B.$$

We conclude from Tate's algorithm that the reduction is of type I^*_{2n} with $n = 4v(a) - 2$, as desired. □

Remark 4.3 The proof of Theorem 4.2 in the equicharacteristic case exhibits explicitly elliptic curves satisfying all the conditions in the theorem. Indeed, choose an odd integer $r > 0$. Then there exists a quadratic extension L/K such that $s_{L/K} = r$: take L to be the splitting field of $z^2 + z + \pi_K^{-r}$. There also exists an elliptic curve E/K with good ordinary reduction over L, and reduction over K of type I^*_{4r}: take E/K given by the Weierstrass equation $y^2 + xy = x^3 + \pi_K^{-r}x^2 + 1$.

Remark 4.4 The proof of Theorem 4.2 in the mixed characteristic case exhibits explicitly elliptic curves satisfying all the conditions in the theorem. Indeed, when the field K of mixed characteristic 2 is fixed, the proof shows that an elliptic curve E/K with additive reduction and potentially good ordinary reduction has reduction over K of type I^*_{4m} with $0 < m \leq 2v(2)$.

Choose an even integer $r > 0$ and a field K of mixed characteristic 2 with $v(2) = r/2$. Then there exist a quadratic extension L/K such that $s_{L/K} = r$: take L to be the splitting field of $z^2 - \pi_K$. There also exists an elliptic curve E/K with good ordinary reduction over L, and reduction over K of type I^*_{4r}: take E/K given by the Weierstrass equation (4.2.1) with $j_0 = 1$ and $D = \pi_K$.

Choose an odd integer $r > 0$ and a field K of mixed characteristic 2 with $v(2) = (r+1)/2$ (so that $2 = u\pi_K^{(r+1)/2}$). Then there exist a quadratic extension L/K such that $s_{L/K} = r$: take L to be the splitting field of $z^2 + \pi_K^{(r+1)/2} z + \pi_K$. There also exists an elliptic curve E/K with good ordinary reduction over L, and reduction over K of type I_{4r}^*: take E/K given by the Weierstrass equation (4.2.1) with $j_0 = 1$ and $D = 1 - \pi_K u^2$.

Remark 4.5 Theorem 4.2 complements Theorem 2.8 in [25], where X/K is assumed to have potentially multiplicative reduction.

Corollary 4.6. *Let $\mathcal{O}_K$ be a Henselian discrete valuation domain with algebraically closed residue field k of characteristic 2. Let E/K and E'/K be two isogenous elliptic curves with potentially good ordinary reduction. Then these curves have same reduction type. Over $\mathbb{Q}_2^{unr}$, this reduction type is either I_4^* or I_8^*.*

Proof. Since the curves are isogenous, the quadratic extension L/K such that E_L/L has good reduction also has the property that E'_L/L has good reduction. Theorem 4.2 shows that the reduction of both curves is then of type $I_{4s_{L/K}}^*$. As noted in 4.4, over the field $\mathbb{Q}_2^{unr}$ with $v(2) = 1$, the reduction is of type I_{4m}^* with $0 < m \leq 2v(2)$. □

Let $\mathcal{O}_K$ be a Henselian discrete valuation domain, with field of fractions K and algebraically closed residue field k of characteristic 2. Let E/K be an elliptic curve with additive reduction, and potentially good reduction. Assume that there exists a quadratic extension L/K such that E_L/L has a smooth model $\mathcal{Y}/\mathcal{O}_L$. Theorem 4.2 shows that such L/K always exists when the reduction is potentially good ordinary.

The Galois group $H := \mathrm{Gal}(L/K)$ acts on $\mathcal{Y}$ and on $\mathcal{Y}_k$. Let $P \in \mathcal{Y}_k$ be a closed point of $\mathcal{Y}$ fixed by the action of H. The associated local ring $\mathcal{O}_{\mathcal{Y},P}$ is then endowed with an action of H, and it is natural to wonder whether the desingularization of $\mathrm{Spec}(\mathcal{O}_{\mathcal{Y},P})^H$ can be described explicitly. While this seems to be a difficult problem when $\mathcal{Y}_k$ is supersingular, we do so below in the case where $\mathcal{Y}_k$ is ordinary.

Corollary 4.7. *Let $\mathcal{O}_K$ be a Henselian discrete valuation domain with algebraically closed residue field k of characteristic 2. Let E/K be an elliptic curve with additive reduction, and potentially good ordinary reduction. Then the intersection matrix associated with the minimal resolution of* $\mathrm{Spec}(\mathcal{O}_{\mathcal{Y},P})^H$ *is up to permutation equal to the matrix $N(2, 2s_{L/K}, 1)$.*

Proof. Let L/K denote the quadratic extension such that E_L/L has a smooth model $\mathcal{Y}/\mathcal{O}_L$. Denote by $\mathcal{Z}/\mathcal{O}_K$ the (normal) quotient $\mathcal{Y}/H$. Let σ denote the automorphism of $\mathcal{Y}_k/k$ induced by the action of a generator of H on $\mathcal{Y}$. Under our hypothesis, σ is the standard involution of the elliptic curve $\mathcal{Y}_k$, and it has exactly two fixed points P_1 and P_2. The scheme $\mathcal{Z}$ is singular exactly at the images of these fixed points ([26], 5.2), which we denote by Q_1 and Q_2. We know that the minimal regular model of E/K is of the form $I_{4s_{L/K}}^*$. In particular, it contains four components of multiplicity 1. Consider a minimal resolution $\mathcal{X}_1 \to \mathcal{Z}$ of Q_1, and a minimal resolution $\mathcal{X}_2 \to \mathcal{X}_1$ of the preimage of Q_2 in $\mathcal{X}_1$. Let $\mathcal{X}_2 \to \mathcal{X}$ denote the contraction to the minimal regular model $\mathcal{X}$ of E/K. We claim that both resolutions $\mathcal{X}_1 \to \mathcal{Z}$ and $\mathcal{X}_2 \to \mathcal{X}_1$ have exceptional divisors which contain irreducible curves of multiplicity 1 in the special fiber $(\mathcal{X}_1)_k$ and $(\mathcal{X}_2)_k$, respectively. Indeed, if for instance $\mathcal{X}_1$ contains no curves of multiplicity 1 in $(\mathcal{X}_1)_k$, then by inspection of all possible Kodaira types, we would find that all curves in the resolution of Q_1 would get contracted under $\mathcal{X}_2 \to \mathcal{X}$. But by construction, the only curve on $(\mathcal{X}_2)_k$ which possibly can be of self-intersection -1 is the irreducible component corresponding to $\mathcal{Z}_k$. This component has multiplicity 2 ([26], 5.1). Such a curve can only be of self-intersection -1 if it intersects normally two components of multiplicity 1. This is a contradiction as we are assuming that no curves of multiplicity 1 are found in the minimal desingularization of Q_1.

Without loss of generality, we can assume that the origin of the elliptic curve E/K reduces to the point Q_1 in $\mathcal{Z}$. Our discussion above implies that there exists a component of multiplicity 1 in the resolution of Q_2, and since the field K is Henselian with algebraically closed residue field, we find that there exists $P \in E(K)$ reducing in $\mathcal{Z}_k$ to Q_2. Consider the translation τ_P by P on E/K. This translation extends to an automorphism τ of the quotient $\mathcal{Z}$. Thus, the singularities Q_1 and Q_2 are isomorphic, and since the minimal model of E/K has type $I^*_{4s_{L/K}}$, we find that each singularity is of type $N(2, 2s_{L/K}, 1)$. □

4.8 *Proof of Theorem 4.1.* Theorem 4.1 follows immediately from 4.3, 4.4, and 4.7. □

Remark 4.9 The class of intersection matrices which occur in the resolution of a wild $\mathbb{Z}/2\mathbb{Z}$-quotient singularity is far from being understood. In particular, one may wonder whether there is any restriction on the number of nodes in a minimal resolution graph $G(N)$. We conclude this section with a remark on how one could construct $\mathbb{Z}/2\mathbb{Z}$-quotient singularities such that the graph associated with a minimal desingularization of the singularity has more than one node.

Choose a discrete valuation field K and an elliptic curve E/K such that there exists a quadratic extension L/K such that E_L/L has good supersingular reduction. Assume that the reduction of E/K is of type I^*_n for some $n > 0$, so that the graph I^*_n has two nodes. Let $\mathcal{Y}/\mathcal{O}_L$ denote the smooth model of E_L/L. Since $[L : K] = 2$, $H := \mathbb{Z}/2\mathbb{Z}$ acts on $\mathcal{Y}_k$. The automorphism group of $\mathcal{Y}_k$ injects into $\mathrm{SL}_2(\mathbb{F}_3)$, and so contains a unique element of order 2, the canonical involution of $\mathcal{Y}_k/k$. Since $\mathcal{Y}_k$ is supersingular, this involution has a single fixed point, so the quotient $\mathcal{Z} := \mathcal{Y}/H$ has a single singular point. Let $\mathcal{X} \to \mathcal{Z}$ be a minimal resolution of this singularity. Let $\mathcal{X} \to \mathcal{X}_0$ denote the contraction to the minimal regular model of E/K. Since the special fiber of $\mathcal{X}_0$ has graph I^*_n with two nodes, the graph of the exceptional divisor in $\mathcal{X}$ must have at least two nodes.

Finding explicit equations for E/K with $[L : K] = 2$, potential supersingular reduction, and reduction over K of type I^*_n for some $n > 0$, is not completely obvious. One such equation is given in Example 2 of [16], p. 179, over the field $\mathbb{Q}(\sqrt{26})$.

References

[1] S. Abhyankar, *Resolution of singularities of arithmetical surfaces*, in Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), 111–152, Harper & Row, New York, 1965

[2] M. Artin, *Wildly ramified $\mathbb{Z}/2\mathbb{Z}$ actions in dimension* 2, Proc. AMS **52** (1975), 60–64.

[3] M. Artin, *On isolated rational singularities of surfaces*, Amer. J. Math. **88** (1966), 129–136.

[4] M. Artin, *Lipman's proof of resolution of singularities for surfaces*, in *Arithmetic geometry*, G. Cornell and J. Silverman, Editors, Springer-Verlag, 1986.

[5] M. Atiyah and I. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[6] W. Barth, C. Peters, and A. Van de Ven, *Compact complex surfaces*, Springer-Verlag, Berlin, 1984.

[7] A. Berman and R. Plemmons, *Nonnegative matrices in the mathematical sciences*, Academic Press, 1979.

[8] N. Bourbaki, *Commutative algebra. Chapters 1–7*, Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics, Springer-Verlag, Berlin, 1998.

[9] S. Bosch, W. Lüktebohmert, and M. Raynaud, *Néron Models*, Springer Verlag, 1990.

[10] J.-F. Boutot, *Schéma de Picard local*, Lecture Notes in Mathematics **632**, Springer, Berlin, 1978.

[11] B. Conrad, B. Edixhoven, and W. Stein, $J_1(p)$ *has connected fibers*, Doc. Math. **8** (2003), 331–408.

[12] O. Gabber, Q. Liu, and D. Lorenzini, *The index of an algebraic variety*, Invent. math. (2012) DOI 10.1007/s00222-012-0418-z

[13] L. H. Halle, *Stable reduction of curves and tame ramification*, Math. Z. **265** (2010), no. 3, 529-550.
[14] H. Ito and S. Schroeer, *Wild quotient surface singularities whose dual graphs are not star-shaped*, Preprint, September 2012.
[15] H. Hironaka, *Desingularization of excellent surfaces*, 1967 Bowdoin College lectures, appendix to V. Cossart, J. Giraud, and U. Orbanz, *Resolution of surface singularities*, Lecture Notes in Mathematics, 1101. Springer-Verlag, Berlin, 1984.
[16] M. Kida, *Potential good reduction of elliptic curves*, J. Symbolic Comput. **34** (2002), no. 3, 173–180.
[17] J. Lipman, *Rational singularities, with applications to algebraic surfaces and unique factorization*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 195–279.
[18] J. Lipman, *Introduction to resolution of singularities*, in Algebraic geometry, AMS Proc. Sympos. Pure Math. **29** (1975), 187–230.
[19] J. Lipman, *Desingularization of two-dimensional schemes*, Ann. of Math. (2) **107** (1978), no. 2, 151-207.
[20] D. Lorenzini, *Arithmetical graphs*, Math. Ann. **285** (1989), 481–501.
[21] D. Lorenzini, *Groups of components of Néron models of Jacobians*, Comp. Math. **73** (1990), 145–160.
[22] D. Lorenzini, *Jacobians with potentially good ℓ-reduction*, J. reine angew. Math. **430** (1992), 151–177.
[23] D. Lorenzini, *On the group of components of a Néron model*, J. reine angew. Math. **445** (1993), 109–160.
[24] D. Lorenzini, *Reduction of points in the group of components of the Néron model of a Jacobian*, J. reine angew. Math. **527** (2000), 117–150.
[25] D. Lorenzini, *Models of curves and wild ramification*, Pure Appl. Math. Q. (Special issue in honor of John Tate) **6** (2010) no 1, 41–82.
[26] D. Lorenzini, *Wild models of curves*, Preprint.
[27] D. Lorenzini, *Wild quotients of products of curves*, Preprint.
[28] H. Matsumura, *Commutative algebra*, Second edition, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.
[29] M. Nagata, *Local Rings*. New York-London-Sydney: Interscience Publishers, 1962.
[30] B. Peskin, *Quotient singularities and wild p-cyclic actions*, J. Algebra **81** (1983), 72–99.
[31] B. Peskin, *On rings of invariants with rational singularities*, Proc. AMS **87** (1983), 621–626.
[32] J.-P. Serre, *Local Fields*, Translated from the French by Marvin Jay Greenberg, Springer-Verlag New York, 1979.
[33] J. Silverman, *The arithmetic of elliptic curves*, Corrected reprint of the 1986 original. Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 2009.
[34] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math; **151**, Springer-Verlag, 1994.
[35] E. Viehweg, *Invarianten der degenerierten Fasern in lokalen Familien von Kurven*, J. reine angew. Math. **293/294** (1977), 284–308.
[36] P. Wagreich, *Elliptic singularities of surfaces*, Amer. J. Math. **92** (1970), 419–454.
[37] O. Zariski and P. Samuel, *Commutative algebra*, Vol. II, The University Series in Higher Mathematics, D. Van Nostrand Co., Inc., Princeton, N. J.-Toronto-London-New York, 1960.

Department of mathematics, University of Georgia, Athens, GA 30602, USA
E-mail address: lorenzin@uga.edu