# Elliptic delsarte surfaces

Heijne, Bas Leonard

# Chapter 2

# Shioda's Algorithm

In this chapter we will give a description of the methods described in Shioda's article to compute the rank of Delsarte surfaces. The method used was first described in a slightly different form in [17]. In this text we will not prove the algorithm. Instead we will focus on the way the algorithm can be applied to compute the rank of an elliptic Delsarte surface.

## 2.1 Computing the Lefschetz number

In this section we will state an algorithm to calculate the Lefschetz number, given by Shioda in [17]. We will first state the algorithm and then give some remarks. Note that given the Lefschetz number $\lambda$, the rank $r$ of the corresponding elliptic surface is given by $r = h^2 - \lambda - \rho_{\text{triv}}$.

- Start with an equation of a Delsarte surface

$$f = \sum_{i=0}^{3} t^{a_{i0}} x^{a_{i1}} y^{a_{i2}}. \tag{2.1}$$

- Homogenise this as a surface

$$F = \sum_{i=0}^{3} T^{a_{i0}} X^{a_{i1}} Y^{a_{i2}} Z^{a_{i3}}.$$

- Put the exponents in a matrix

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

- Construct the subgroup $L \subset (\mathbb{Q}/\mathbb{Z})^4$ generated by $(1, 0, 0, -1)A^{-1}$, $(0, 1, 0, -1)A^{-1}$ and $(0, 0, 1, -1)A^{-1}$.

- Define $\Lambda \subset L$ as follows. An element $v = (a_0, a_1, a_2, a_3) \in L$ is an element of $\Lambda$, precisely when it satisfies the following two conditions.

  - For all $i$ we have $a_i \neq 0 \bmod \mathbb{Z}$.
  - There exists an element $t \in \mathbb{Z}$, such that $\mathrm{ord}(tv) = \mathrm{ord}(v)$ and moreover $\sum_{i=0}^{3} \{ta_i\} \neq 2$. Here ord refers to the order in the additive group $(\mathbb{Q}/\mathbb{Z})^4$. The notation $\{a\}$ refers to the natural bijection between the set $\mathbb{Q}/\mathbb{Z}$ and $[0, 1)$.

- Then the Lefschetz number is given by $\lambda = \#\Lambda$.

For a proof of the correctness of this algorithm we refer to [17].

**Remark 2.1.1.** In the algorithm we assume that $A^{-1}$ exists. This imposes a restriction on the surfaces for which the algorithm works. Theorem 2.1.3 tells us that this will only happen in very specific cases.

**Remark 2.1.2.** There is a difference between the algorithm as stated here and how it was originally given by Shioda in [17].

In the original publication Shioda uses the cofactor matrix of $A$ instead of the inverse matrix of $A$. He then construct $L$ as a subset of $(\mathbb{Z}/d\mathbb{Z})^4$ instead of as a subset of $(\mathbb{Q}/\mathbb{Z})^4$.

The benefit of the way the algorithm is presented here is that it makes it easier to deal with families of elliptic surfaces.

**Theorem 2.1.3.** *Let $\pi : \mathcal{E} \to \mathbb{P}^1$ be an elliptic Delsarte surface. Assume that the surface does not split over a finite extension of $k(t)$, then* $\det(A) \neq 0$.

*Proof.* If we homogenise the equation defining the generic fibre of $\mathcal{E}$ then we get:

$$\tilde{F} = \sum_{i=0}^{3} t^{a_{i0}} X^{a_{i1}} Y^{a_{i2}} Z^{b_{i3}}.$$

Just as we did with $F$ we can put the exponents in a matrix.

$$B = \begin{pmatrix} a_{00} & a_{01} & a_{02} & b_{03} \\ a_{10} & a_{11} & a_{12} & b_{13} \\ a_{20} & a_{21} & a_{22} & b_{23} \\ a_{30} & a_{31} & a_{32} & b_{33} \end{pmatrix}.$$

Note that $A$ and $B$ are related in the following manner. The first three columns of $A$ and $B$ are the same. The last column of $B$ is the sum of the first and last columns of $A$ minus a constant times the vector $(1, 1, 1, 1)^T$.

There are a few things we can say about the matrices $A$ and $B$. Either both matrices $A$ and $B$ are singular or both are non-singular. Since $F$ is homogeneous we find that $\sum_{i=0}^{3} a_{ij} = \deg(F)$, and hence does not depend on $j$. Likewise since $\tilde{F}$ is homogeneous we find $a_{1j} + a_{2j} + b_{3j}$ is a constant not depending on $j$. Since $F$ and $\tilde{F}$ are irreducible we find that each column of $A$ and $B$ contains a zero.

We will first proof that if there is a relation between the last three column of $B$ then is the genus of the generic fibre of $\mathcal{E}$ zero, and hence not an elliptic curve. After this we will proof that if the first column of $B$ depends on the last three columns then $\mathcal{E}$ splits over a finite extension of the base field. The combination of these result will proof the theorem.

We will begin with the possibility that the last three columns are linearly dependent. Let $B_1$, $B_2$ and $B_3$ be the last three columns of $B$. By assumption there exist $\lambda_i$'s, not all zero, such that

$$\lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3 = 0.$$

We claim that there is a row with precisely two zeroes in the columns $B_1$, $B_2$ and $B_3$. This can be seen by the following argument.

As we know, each of the $B_i$'s contains at least one entry which is zero. If every zero is in a different row then the $\lambda_i$'s would all have different sign. This is of course impossible. Not all the zeroes are in the same row since

$$B_1 + B_2 + B_3 = \deg(\tilde{F}) \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

The two columns with the zeroes on the same row are linearly dependent. The corresponding affine equation for our curve is of the form

$$c_0 + c_1 \xi^{\alpha} \eta^{\lambda\alpha} + c_2 \xi^{\beta} \eta^{\lambda\beta} + c_3 \xi^{\gamma} \eta^{\lambda\gamma} = 0.$$

Let $m$ be a zero of the polynomial

$$c_0 + c_1 m^{\alpha} + c_2 m^{\beta} + c_3 m^{\gamma} = 0,$$

then $\eta = mt^{\lambda}$, $\eta = 1/t$ is a parametrisation of the curve. So the genus of the curve is zero.

Now assume the first column is dependent on the last three columns. This means that there exist $\lambda_i \in \mathbb{Q}$ such that $B_0 = \lambda_1 B_1 + \lambda_2 B_2 + \lambda_3 B_3$. Then over some finite extension of $k(t)$ we can map the curve $E$ to a curve that is defined over $k$. This map is given by $(X : Y : Z) \to (t^{\lambda_1} X : t^{\lambda_2} Y : t^{\lambda_3} Z)$. □

**Remark 2.1.4.** The implication of this theorem goes only one way. It is possible that $\det(A) \neq 0$, and that $\mathcal{E}$ splits over an extension of $k(t)$. Such an extension can, however, not be of the form $k(s) \supset k(t)$ with $s^n = t$.

An example of this can be given by the surface defined by:

$$Y^2 + X^3 + t + 1.$$

This surface does not split over $k(t)$. It does however split over $k(s)$, where $s$ is defined by $s^6 = t + 1$.

**Corollary 2.1.5.** *If* $\det(A) = 0$*, then either the elliptic surface splits and the rank is infinity or the elliptic surface splits over a finite extension and the rank is zero.*

*Proof.* If the elliptic surface splits, then it is of the form $\mathcal{E} \cong E \otimes \mathbb{P}^1$. This means that any point on $E$ corresponds to a section. The rank of $E$ is already infinite.

If the elliptic surface splits over a finite extension we can see that the corresponding Mordell-Weil rank is zero. This means that the discriminant of the elliptic surface is of the form $\Delta = ct^r$. Here $c$ is a constant in $k$ an $r$ is an integer between 2 and 8. The $j$-invariant as such an elliptic surface is constant. From this we see that there are precisely two singular fibres, one over 0 an one over infinity. There are three possibilities: both fibres are of type $I_0^*$, one is of type IV and the other of type IV$^*$ or one is of type II and the other of type II$^*$. In any of these cases we find $\rho_{\text{triv}} = 10$. By the Shioda-Tate formula we now find that $r = 0$. □

**Remark 2.1.6.** From here on we will assume that all elliptic surfaces do not split.

## 2.2 An example

In this section we will compute the maximal rank of a certain family of elliptic surfaces. In the following chapter we will encounter this family in a natural way. For now we just consider this as an example.

We will consider the elliptic curves over $k(t)$ that are defined by a polynomial of the form

$$f = t^a + (t^b + t^c)X^3 + t^dY^2 = 0,$$

where $a, b, c, d$ are non-negative integers with $c > b$. We want to find the maximal rank that occurs in this family.

Let $E$ be the curve defined by $f$ and $E'$ the curve defined by

$$t^{6a} + (t^{6b} + t^{6c})X^3 + t^{6d}Y^2 = 0.$$

Then we have a natural monomorphism $\phi : E(k(t)) \longrightarrow E'(k(t))$, defined by $\phi(x(t), y(t)) = (x(t^6), y(t^6))$. In particular we find the rank of $E(k(t))$ is at most the rank of $E'(k(t))$. So we will restrict ourselves to computing the rank of $E'$.

The map given by $\xi = t^{2(b-a)}X$, $\eta = t^{3(d-a)}Y$ defines an isomorphism from $E'$ to the curve $E''$ given by

$$\tilde{f} = 1 + (1 + t^n)\xi^3 + \eta^2 = 0.$$

Here $n = 6(c - b)$.

Take $m > 0$ a positive integer. Let $E'''$ be the curve given by

$$1 + (1 + t^{nm})\xi^3 + \eta^2 = 0.$$

There is an injective morphism from $E''$ to $E'''$ given by

$$(\xi(t), \eta(t)) \longrightarrow (\xi(t^m), \eta(t^m)).$$

From this we see that $\text{rank}(E''') \geq \text{rank}(E')$. We conclude that to find the maximal rank in our family of elliptic surfaces 2.2 we can assume $m|n$, for any convenient $m$.

We will compute the Lefschetz number using the technique described in 2.1. To do this we first homogenise $\tilde{f}$. This gives

$$\tilde{F} = Z^{n+3} + T^nX^3 + X^3Z^n + Y^2Z^{n+1}.$$

We compute the matrices $A$ and $A^{-1}$.

$$A = \begin{pmatrix} 0 & 0 & n+3 & 0 \\ 3 & 0 & 0 & n \\ 3 & 0 & n & 0 \\ 0 & 2 & n+1 & 0 \end{pmatrix} \quad \text{and} \quad A^{-1} = \begin{pmatrix} -\frac{n}{3(n+3)} & 0 & \frac{1}{3} & 0 \\ -\frac{n+1}{2(n+3)} & 0 & 0 & \frac{1}{2} \\ \frac{1}{n+3} & 0 & 0 & 0 \\ \frac{1}{n+3} & \frac{1}{n} & -\frac{1}{n} & 0 \end{pmatrix}.$$

By definition $L$ is the subgroup of $(\mathbb{Q}/\mathbb{Z})^*$ generated by

$$w_1 = (1,0,0,-1)\,A^{-1} = \left(-\frac{1}{3}, -\frac{1}{n}, \frac{n+3}{3n}, 0\right),$$

$$w_2 = (0,1,0,-1)\,A^{-1} = \left(-\frac{1}{2}, -\frac{1}{n}, \frac{1}{n}, \frac{1}{2}\right),$$

$$w_3 = (0,0,1,-1)\,A^{-1} = \left(0, -\frac{1}{n}, \frac{1}{n}, 0\right).$$

By inspecting these generators we see that $L$ is also generated by

$$v_1 = w_1 - w_3 = \left(-\frac{1}{3}, 0, \frac{1}{3}, 0\right),$$

$$v_2 = w_2 - w_3 = \left(-\frac{1}{2}, 0, 0, \frac{1}{2}\right),$$

$$v_3 = w_3 = \left(0, -\frac{1}{n}, \frac{1}{n}, 0\right).$$

We see that $L$ consists of elements of the form $iv_3$, $v_1+iv_3$, $2v_1+iv_3$, $v_2+iv_3$, $v_1+v_2+iv_3$ and $2v_1+v_2+iv_3$. For each form there are exactly $n$ elements. To compute $\lambda$ we have to find out which of these elements lie in $\Lambda$.

Elements of the form $iv_3, v_1+iv_3$ and $2v_1+iv_3$ do not lie in $\Lambda$, since they all have zero as their last coordinate.

An element of the form $v_2+iv_3$ does not lie in $\Lambda$. If $i=0$ this follows from the fact that the second and third coordinate are zero. If $i \neq 0$ then this follows from the fact that we can compute for all $t$ with $(t,2n)=1$:

$$\left\{\frac{ti}{n}\right\} + \left\{-\frac{ti}{n}\right\} + \left\{\frac{t}{2}\right\} + \left\{-\frac{t}{2}\right\} = 2.$$

We will now determine when $v_1+v_2+iv_3 \in \Lambda$. Take $j,m \in \mathbb{Z}_{\geq 0}$ such that $j/m = i/n$ and $(j,m)=1$. Write $v_1+v_2+iv_3 = (\frac{1}{6}, -\frac{j}{m}, \frac{1}{3}+\frac{j}{m}, \frac{1}{2})$. The conditions $\left\{\frac{t}{6}\right\} \neq 0$, $\left\{-\frac{jt}{m}\right\} \neq 0$, $\left\{\frac{t}{3}+\frac{jt}{m}\right\} \neq 0$ and $\left\{\frac{t}{2}\right\} \neq 0$ are satisfied precisely when $j \neq 0$ and $\frac{j}{m} \neq \frac{2}{3}$.

In all other cases we have $v_1+v_2+iv_3 \in \Lambda$ if and only if there exists a $t$ such that $(t,6m)=1$ and

$$\left\{\frac{t}{6}\right\} + \left\{-\frac{jt}{m}\right\} + \left\{\frac{t}{3}+\frac{jt}{m}\right\} + \left\{\frac{t}{2}\right\} \neq 2.$$

It is easy to compute, if $j \neq 0$ and $\frac{j}{m} \neq \frac{2}{3}$ then

$$\left\{\frac{t}{6}\right\} + \left\{-\frac{jt}{m}\right\} + \left\{\frac{t}{3} + \frac{jt}{m}\right\} + \left\{\frac{t}{2}\right\} = \begin{cases} 1 & \text{if } t \equiv 1 \mod 6 \text{ and } \left\{\frac{tj}{m}\right\} > \frac{2}{3}, \\ 2 & \text{if } t \equiv 1 \mod 6 \text{ and } \left\{\frac{tj}{m}\right\} < \frac{2}{3}, \\ 3 & \text{if } t \equiv 5 \mod 6 \text{ and } \left\{\frac{tj}{m}\right\} < \frac{1}{3}, \\ 2 & \text{if } t \equiv 5 \mod 6 \text{ and } \left\{\frac{tj}{m}\right\} > \frac{1}{3}. \end{cases}$$

By considering a pair $\pm t$, this means that $v_1 + v_2 + iv_3 \in \Lambda$ if and only if $\left\{\frac{tj}{m}\right\} < \frac{1}{3}$ for some $t \equiv 5 \mod 6$, with $(t, 6m) = 1$. We now distinguish between the various possibilities:

- The case $m \leq 3$ is easy and leads to $(v_1 + v_2 + iv_3) \notin \Lambda$. This happens precisely when $i \in \{0, n/2, n/3, 2n/3\}$.
- Assume $m > 3$ and $3 \not| \; m$ or $j \equiv 2 \mod 3$. Then $t \in \mathbb{Z}$ exists with $t \equiv 5 \mod 6$ and $t \equiv j^{-1} \mod m$. For this $t$ we find $\left\{\frac{tj}{m}\right\} < \frac{1}{3}$, hence $(v_1 + v_2 + iv_3) \in \Lambda$.
- In the case that $m > 3$, $3|m$, $j \equiv 1 \mod 3$, assume moreover that there exists a $c \equiv 2 \mod 3$, with $(c, m) = 1$ and $\left\{\frac{c}{m}\right\} < \frac{1}{3}$. We can find $t \equiv 5 \mod 6$ such that $t \equiv cj^{-1} \mod m$. For that $t$ we have $\left\{\frac{tj}{m}\right\} < \frac{1}{3}$. This means $(v_1 + v_2 + iv_3) \in \Lambda$. This happens for all $m > 3$ except when $m \in \{6, 12, 30\}$, as is shown in lemma 2.2.1 below.
- The final case is $m > 3$, $3|m$, $j \equiv 1 \mod 3$ and there exists no $c \equiv 2 \mod 3$, with $(c, m) = 1$ and $\left\{\frac{c}{m}\right\} < \frac{1}{3}$. Assume that $v_1 + v_2 + iv_3 \in \Lambda$. Then $t \equiv 5 \mod 6$ exists, coprime to $6m$ such that $\left\{\frac{tj}{m}\right\} < \frac{1}{3}$. Hence $c = jt$ satisfies $c \equiv 2 \mod 3$, $gcd(c, m) = 1$ and $\left\{\frac{c}{m}\right\} < \frac{1}{3}$, contrary to our assumption.

  In this case we find $(v_1 + v_2 + iv_3) \notin \Lambda$. By the following lemma, this final possibility for $m$ and $j$ happens only if $m \in \{6, 12, 30\}$. In other words only if $i \in \{\frac{n}{6}, \frac{n}{12}, \frac{7n}{12}, \frac{n}{30}, \frac{7n}{30}, \frac{13n}{30}, \frac{19n}{30}\}$.

**Lemma 2.2.1.** *6, 12 and 30 are the only integers $n > 3$ with the property that there does not exist a prime $p \equiv 2 \mod 3$ such that $3p < n$ and $p \not| n$.*

*Proof.* If $n$ satisfies this property then it can be written as $n = Kp_1p_2 \ldots p_t$, with the $p_i$ all primes with $p_i \equiv 2 \mod 3$ and $3p_i < n$. Order the $p_i$ such that $p_i < p_{i+1}$. We construct the number $N = 3p_1 \ldots p_{t-1} + p_t$ and see that it has a prime $p \equiv 2 \mod 3$ dividing it, with $p \neq p_i$. If $n > 51$ we find

$$p/n \leq N/n = \frac{3}{Kp_t} + \frac{1}{Kp_1 \ldots p_{t-1}} \leq \frac{3}{17} + \frac{1}{2 \cdot 5 \cdot 11} < \frac{1}{3}.$$

This means $3p < n$, but $p$ is not any of the $p_i$, a contradiction. So if $n$ satisfies the conditions of the lemma we have $n \leq 51$. Checking the lemma for $n \leq 51$ is easy. □

The cases $v_1 + v_2 + iv_3$ and $2v_1 + v_2 + iv_3$ are similar, since $-(v_1 + v_2 + iv_3) = 2v_1 + v_2 + (n - i)v_3$ and the fact that $v \in \Lambda \Leftrightarrow -v \in \Lambda$.

To ensure that all the special values $\{0, \frac{n}{2}, \frac{n}{3}, \frac{2n}{3}, \frac{n}{6}, \frac{n}{12}, \frac{7n}{12}, \frac{n}{30}, \frac{7n}{30}, \frac{13n}{30}, \frac{19n}{30}\}$ for $i$ encountered in the calculations are actually integers we assume that $60|n$. In that case we find $\lambda = 2n - 22$.

To compute the rank of the curve we bring the curve to Weierstrass form and compute the rank there. Define $\tilde{\eta} = (1+t^n)\eta$ and $\tilde{\xi} = (1+t^n)\xi$ then we get the formula

$$\tilde{\eta}^2 + \tilde{\xi}^3 + (1+t^n)^2 = 0.$$

We use theory explained in [15] to show that the second Betti number is $h^2 = 4n - 2$. We can now compute $\rho = h^2 - \lambda \leq 2n + 20$.

We also compute

$$\Delta = -432(t^n + 1)^4.$$

$$j = 0.$$

From this we see, using again that $3|n$, that the elliptic surface has $n$ singular fibres of type IV at the roots of $t^n + 1 = 0$ and no other singular fibres. So we find $\rho_{\text{triv}} = (2n + 2)$.

Combining these facts gives

$$r = \rho - \rho_{\text{triv}} \leq (2n + 20) - (2n + 2) = 18.$$

This concludes the example and we find that the rank of $E$ over $k(t)$ is $\leq 18$ and it equals 18 in the case $E''$ with $60|n$.