COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 70 2022

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

Representations of Divisors on Hyperelliptic Curves and Plane Curves with Quasi-toric Relations

by

Ai TAKAHASHI and Hiro-o TOKUNAGA[1]

(Received June 26, 2021)
(Revised October 16, 2021)

Abstract. In the study of hyperelliptic curve cryptography, presentations of semi-reduced divisors on a hyperelliptic curve play important roles. In this note, we give an interpretation for such presentations from viewpoints of Gröbner bases. We then apply it to construct plane curves with infinitely many quasi-toric relations of type $(2, n, 2)$.

Introduction

Let $\mathcal{C}$ be a hyperelliptic curve of genus g defined over a field K, $\mathrm{char}(K) \neq 2$ given by an affine equation

$$\mathcal{C} : y^2 = f(x), \quad f(x) = x^{2g+1} + c_1 x^{2g} + \ldots + c_{2g}, \quad c_i \in K \ (1 \leq i \leq 2g)$$

where $f(x) = 0$ has no multiple roots in $\overline{K}$, an algebraic closure of K. We denote the point at infinity by O. In the study of hyperelliptic curve cryptography ([2, 4, 7, 12]), a pair of two polynomials (u, v) $(u, v \in \overline{K}[x])$ is used in order to describe semi-reduced divisors on $\mathcal{C}$ (See Section 1 for semi-reduced divisors) and to consider the addition in the Jacobian of $\mathcal{C}$. Such a pair was first considered in [15] and is called the Mumford representation of a semi-reduced divisor. For a semi-reduced divisor $\mathfrak{d}$, $\mathfrak{d}$ is given by zeros of the ideal $\langle u, y - v, y^2 - f \rangle$ generated by $u, y - v, y^2 - f$ in $\overline{K}[x, y]$ with multiplicities. In [13], another description for semi-reduced divisors was given. We call it the Leitenberger representation.

In this article, we give interpretations concerning these two representations from viewpoints of Gröbner bases (Propositions 2.8 and 2.13). Namely we consider reduced Gröbner bases of $\langle u, y - v, y^2 - f \rangle$ with respect to two monomial orders given in Section 2.3.1. We then give a description for the addition law on $\mathrm{Pic}^0(\mathcal{C})$ along this line in Section 2.3.4. We hope that our approach by using Gröbner bases may make the addition procedure simple at least from conceptual viewpoint.

As a geometric application of our observation on the two representations of semi-reduced divisors, we study plane curves with quasi-toric relations and give a method for explicit construction of such curves in Proposition 3.1. Here, following [3, Definition 2.13],

[1]Partially supported by JSPS KAKENHI Grant Number JP20K03561

Key words and phrases. hyperelliptic curve, Gröbner bases, presentations of semi-reduced divisors, quasi-toric relations.

MSC2020 14Q05, 14H40, 14H50.

we say that a plane curve $\mathcal{B}$ in $\mathbb{P}^2$ satisfies a quasi-toric relation of type (p, q, r) if there exist a sextuple $(F_1, F_2, F_3, h_1, h_2, h_3)$ of non-zero homogeneous polynomials such that

- it satisfies the following relation
$$h_1^p F_1 + h_2^q F_2 + h_3^r F_3 = 0\,,$$
and
- the curve $\mathcal{B}$ is given by $F_1 F_2 F_3 = 0$.

Plane curves that satisfy quasi-toric relations of certain types have been studied in [3, 9, 10] in terms of the embedded topology of plane curves. We apply Proposition 3.1 to the case of $g = 1$ and construct new explicit examples of curves satisfying infinitely many quasi-toric relations of type $(2, n, 2)$ $n = 3, 5, 7$ in Section 4.

REMARK 1. (i) Note that the cases of $(2, 5, 2)$ and $(2, 7, 2)$ were not considered since such cases are not of *elliptic type* in the terminology of [3], i.e., of types $(2, 3, 6)$, $(3, 3, 3)$, $(2, 4, 4)$.

(ii) If a plane curve satisfies a quasi-toric relation of type $(2, 3, 6)$, it satisfies infinitely many countable such relations by [3, Theorem 4.7]. On the other hand, our examples in this article contain a continuous parameter, which makes a difference.

(iii) After the previous version of this article was uploaded in arXiv, Kloosterman extended our result ([11]). Yet, as he comments in the Introduction in [11], we hope that our examples are still worthwhile to be published.

In Section 4, we also apply our method to construct weak n-contact curves to a smooth cubic. For a smooth cubic E, a plane curve D is said to be a weak n-contact curve to E if the divisor $D|_E$ on E defined by D is of the form $D|_E = n\left(\sum_{i=1}^{d} P_i\right) + s\,O$ for some non-negative integer s. As we have seen in [16], a weak n-contact curve to a cubic satisfying $D|_E = nP + sO$, i.e., D meets at a torsion point of order n and meets at O plays a key role to construct examples of certain Zariski tuples. In Examples 4.4 and 4.5, we construct 5- (resp. 7-) contact curves to E which intersect at a torsion point of order 5 (resp. 7) on E and meets at O. Note that these examples are new as we only treat the cases of $n = 3, 4, 6, 8$ in [16],.

This article consists of 4 sections. In Section 1, we introduce semi-reduced divisors on a hyperelliptic curve and explain their presentations. In Section 2, we give our interpretation for two different representations of semi-reduced divisors from a viewpoint of Gröbner bases. In Section 3 and 4, we apply our observation in Section 2 to study plane curves with quasi-toric relations and weak n-contact curves.

1. Semi-reduced divisors on hyperellitpic curves

Let $\mathcal{C}$ be a hyperelliptic curve defined over K given by the affine equation in the Introduction. We give a summary for semi-reduced divisors considered in hyperelliptic cryptography [4, 7, 12, 14] and our previous article [16]. Our notation here are those in [16].

Let $\mathfrak{d}$ be a divisor on $\mathcal{C}$ and $\mathrm{Supp}(\mathfrak{d})$ denotes its supporting set. Let $\iota : (x, y) \mapsto (x, -y)$ be the hyperelliptic involution on $\mathcal{C}$. For any divisor $\mathfrak{d}$ on $\mathcal{C}$ with $\mathfrak{d} = \sum_{P \in \mathcal{C}} m_P P$, by considering points of the form $P + \iota(P)$ contained in $\mathfrak{d}$, we have a decomposition $\mathfrak{d} = \mathfrak{d}_{\mathrm{sr}} + \mathfrak{d}_o$ such that

(i) the divisor $\mathfrak{d}_o$ is of the form $\bar{\mathfrak{d}} + \iota(\bar{\mathfrak{d}})$ for some divisor $\bar{\mathfrak{d}}$, and
(ii) if we write $\mathfrak{d}_{\mathrm{sr}} = \sum_{P \in \mathcal{C}} m'_P P$, then m'_P satisfies the following conditions:
  (a) $m'_P = 1$ if $m'_P > 0$ and $P = \iota(P)$, and
  (b) $m'_{\iota(P)} = 0$ if $m'_P > 0$ and $P \neq \iota(P)$.

We here define a semi-reduced divisor on $\mathcal{C}$ following to [7].

DEFINITION 1.1. Let $\mathfrak{d}$ be a divisor on a hyperelliptic curve $\mathcal{C}$.

(i) The divisor $\mathfrak{d}$ is said to be affine divisor if $\mathrm{Supp}(\mathfrak{d}) \subset \mathcal{C}_{\mathrm{aff}} := \mathcal{C} \setminus \{O\}$.
(ii) An effective affine divisor $\mathfrak{d}$ is said to be *semi-reduced* if $\mathfrak{d}_o$ is empty.
(iii) A semi-reduced divisor $\sum_i m_i P_i$ is said to be h-reduced if $\sum_i m_i \leq g$.

REMARK 1.2. In [7, 14], a h-reduced divisor is simply called a reduced divisor. Here, in order to avoid confusion for the terminology *reduced divisor* used in standard textbooks in algebraic geometry e.g., [8], we use the terminology '*h-reduced*.'

Here are some properties for semi-reduced divisors:

LEMMA 1.3. (a) *For any divisor* $\mathfrak{d} = \sum_P m_P P$ *with* $\mathrm{Supp}(\mathfrak{d}) \neq \emptyset$, *there exists a semi-reduced divisor* $\mathrm{sr}(\mathfrak{d})$ *such that* (i) $\mathfrak{d} - (\deg \mathfrak{d})O \sim \mathrm{sr}(\mathfrak{d}) - (\deg \mathrm{sr}(\mathfrak{d}))O$ *and* (ii) $|\mathfrak{d}| \geq |\mathrm{sr}(\mathfrak{d})| (= \deg \mathrm{sr}(\mathfrak{d}))$. *Here we put* $\deg \mathfrak{d} := \sum_P m_P$ *and* $|\mathfrak{d}| := \sum_P |m_P|$.

(b) *Let* $\mathfrak{d}$ *be any semi-reduced divisor on* $\mathcal{C}$ *with* $\deg \mathfrak{d} > g$. *Then there exists a unique h-reduced divisor* $\mathrm{r}(\mathfrak{d})$ *such that* $\mathfrak{d} - (\deg \mathfrak{d})O \sim \mathrm{r}(\mathfrak{d}) - (\deg \mathrm{r}(\mathfrak{d}))O$.

(c) *With two statements as above, we see that for any element* $\mathfrak{d} \in \mathrm{Div}^0(\mathcal{C})$, *there exists a unique h-reduced divisor* $\mathrm{r}(\mathfrak{d})$ *such that* $\mathfrak{d} \sim \mathrm{r}(\mathfrak{d}) - (\deg \mathrm{r}(\mathfrak{d}))O$.

As for proofs, see [7, 14].

2. Representations for semi-reduced divisors

We keep our notation and terminologies as in Section 1. Let $\langle y^2 - f \rangle \subset \overline{K}[x, y]$ be the ideal generated by $y^2 - f$, where f is the polynomial in the Introduction. The quotient ring $\overline{K}[x, y]/\langle y^2 - f \rangle$ is said to be the coordinate ring of $\mathcal{C}$ and we denote it by $\overline{K}[\mathcal{C}]$. The quotient field of $\overline{K}[\mathcal{C}]$ is the rational function field $\overline{K}(\mathcal{C})$ of $\mathcal{C}$. An element of $\overline{K}[\mathcal{C}]$ is called a polynomial function, i.e., a rational function with poles only at O. For $g \in \overline{K}[x, y]$, its class in $\overline{K}[\mathcal{C}]$ gives a polynomial function on $\mathcal{C}$, which we denote by $[g]$.

For our later use, we define a $\overline{K}[x]$-submodule $\mathrm{Rem}(y^2)$ of $\overline{K}[x, y]$ as follows:

$$\mathrm{Rem}(y^2) = \{b_0(x) + b_1(x)y \mid b_0(x), b_1(x) \in \overline{K}[x]\}$$

Since any element in $\overline{K}[\mathcal{C}]$ can be represented by the class of an element in $\mathrm{Rem}(y^2)$ uniquely ([14, §2]), we use elements in $\mathrm{Rem}(y^2)$ as normal forms of polynomial functions in $\overline{K}[\mathcal{C}]$. Also we denote the local ring at P by $\mathcal{O}_P(\mathcal{C})$ and its valuation by ord_P.

2.1. The Mumford representation

In [15], Mumford gave a description of $\mathrm{Pic}^0(\mathcal{C})$ by two polynomials of one variable, from which we have a semi-reduced divisor. In the study of hyperelliptic cryptography it is called the Mumford representation. We explain it briefly.

Let $\mathfrak{d} = \sum_{i=1}^{r} e_i P_i (e_i > 0)$ be a semi-reduced divisor on $\mathcal{C}$ and put $P_i = (x_i, y_i)$ $(i = 1, \ldots, r)$.

LEMMA 2.1. *There exist unique polynomials $u(x), v(x) \in \overline{K}[x]$ such that*

(i) $u(x) := \prod_{i=1}^{r} (x - x_i)^{e_i}$,
(ii) $\deg v(x) < \deg u(x)$, $\mathrm{ord}_{P_i}([y - v(x)]) \geq e_i$, *and*
(iii) $v(x)^2 - f$ *is divisible by* u.

In particular, $\deg u = \deg \mathfrak{d}$.

For a proof, see [7, Lemma 10.3.5].

DEFINITION 2.2. Let $\mathfrak{d}$ be a non-zero semi-reduced divisor on a hyperelliptic curve $\mathcal{C}$. The pair of polynomials (u, v) is said to be the Mumford representation of $\mathfrak{d}$. By $\mathfrak{d}(u, v)$, we mean a non-zero semi-reduced divisor with the Mumford representation (u, v). For $\mathfrak{d} = 0$, we take $u(x) = 1$ and $v(x) = 0$ as its Mumford representation.

Note that if u and v as above exist, we recover $\mathfrak{d}$:

$$\mathfrak{d} = (\gcd(\mathrm{div}([u]), \mathrm{div}([y - v])))_{\mathrm{aff}} ,$$

where, for $g_i \in \overline{K}[x, y]$ $(i = 1, 2)$ and divisors, $\mathrm{div}([g_i])$, of functions $[g_i] (i = 1, 2)$, we define

$$\begin{aligned} &\gcd(\mathrm{div}([g_1]), \mathrm{div}([g_2])) \\ &:= \sum_{P \in \mathcal{C}_{\mathrm{aff}}} \min(\mathrm{ord}_P([g_1]), \mathrm{ord}_P([g_2]))P - \left(\sum_P \min\left(\mathrm{ord}_P([g_1]), \mathrm{ord}_P([g_2])\right) \right) O , \end{aligned}$$

and $(\gcd(\mathrm{div}([g_1]), \mathrm{div}([g_2])))_{\mathrm{aff}} := \sum_{P \in \mathcal{C}_{\mathrm{aff}}} \min(\mathrm{ord}_P([g_1]), \mathrm{ord}_P([g_2]))P$.

As it is shown in [2, 7, 14], one can compute the addition law on $\mathrm{Pic}^0(\mathcal{C})$ in terms of Mumford representations of two semi-reduced divisors. Also if we are given a semi-reduced divisor $\mathfrak{d}(u, v)$, we have an algorithm to compute the h-reduced divisor $\mathrm{r}(\mathfrak{d}(u, v))$ as in Lemma 1.3 in terms of u, v.

2.2. The Leitenberger representation

In this subsection, we recall another representation of a non-zero semi-reduced divisor $\mathfrak{d}$ considered in [13], which is based on Jacobi's interpolation functions. Let $\mathfrak{d} = \sum_{i=1}^{r} P_i$ be a non-zero semi-reduced divisor on $\mathcal{C}$. By Lemma 1.3, there exists a unique h-reduced divisor, $\mathrm{r}(\mathfrak{d})$, such that

$$\mathfrak{d} - (\deg \mathfrak{d}) O \sim \mathrm{r}(\mathfrak{d}) - (\deg \mathrm{r}(\mathfrak{d})) O .$$

Hence we have

$$\mathfrak{d} + \iota^* \mathrm{r}(\mathfrak{d}) - (\deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d})) O \sim \mathrm{r}(\mathfrak{d}) + \iota^* \mathrm{r}(\mathfrak{d}) - 2(\deg \mathrm{r}(\mathfrak{d})) \sim 0 ,$$

and there exists $\psi \in \overline{K}[\mathcal{C}]$, unique up to constants, such that

$$\mathrm{div}(\psi) = \mathfrak{d} + \iota^* \mathrm{r}(\mathfrak{d}) - (\deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d}))O\,.$$

Thus we have

LEMMA 2.3. $\deg \mathrm{r}(\mathfrak{d}) = \min\{r \mid \mathbb{L}(-\mathfrak{d}+(\deg \mathfrak{d}+r)O) \neq \{0\}\}$. *Here for a divisor* $\mathfrak{d}$, $\mathbb{L}(\mathfrak{d})$ *denotes vector space consisting of rational functions* ξ *such that* $\mathrm{div}(\xi)+\mathfrak{d}$ *is effecitve and* 0.

By choosing $b = b_0 + b_1 y \in \mathrm{Rem}(y^2)$ such that $\psi = [b]$, we have

LEMMA 2.4. *The effective divisor* $\mathfrak{d}+\iota^*\mathrm{r}(\mathfrak{d})$ *is semi-reduced if and only if* $\gcd(b_0, b_1) = 1$.

Proof. Suppose that $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ is not semi-reduced. We then infer that $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ is of the form $\mathfrak{d}_1 + P + \iota^* P$ for some effective divisor $\mathfrak{d}_1$ and $P = (x_P, y_P)$. As $P + \iota^* P - 2O \sim 0$, $\mathfrak{d}_1 - (\deg(\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})) - 2)O \sim 0$. This implies that there exists $\tilde{b} \in \mathrm{Rem}(y^2)$ such that $\mathrm{div}([\tilde{b}]) = \mathfrak{d}_1 - (\deg(\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})) - 2)O$, and we have $\mathrm{div}((x - x_P)\tilde{b}) = \mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d}) - (\deg(\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d}))O$. As $(x - x_P)\tilde{b} \in \mathrm{Rem}(y^2)$, $b = c(x - x_P)\tilde{b}$ for some $c \in \overline{K}\backslash\{0\}$. This means $x - x_P | \gcd(b_0, b_1)$. Conversely, if $\gcd(b_0, b_1)$ is not constant, the divisor $(\gcd(\mathrm{div}([b_0]), \mathrm{div}([b_1])))_{\mathrm{aff}}$ is contained in $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$. Therefore $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ is not semi-reduced. □

LEMMA 2.5. *Let* $\mathfrak{d} = \sum_{i=1}^r e_i P_i$ *be a semi-reduced divisor such that* $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ *is semi-reduced. Let* u *be as in Lemma 2.1 and let* $b \in \mathrm{Rem}(y^2)$ *as above. Then* $\mathfrak{d} := (\gcd(\mathrm{div}([u]), \mathrm{div}([b])))_{\mathrm{aff}}$.

Proof. Since $\mathrm{div}([u]) = \sum_{i=1}^r e_i(P_i + \iota^* P_i) - (2 \deg \mathfrak{d})O$, $\mathrm{div}([b]) = \mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d}) - (\deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d}))O$ and $\mathrm{Supp}(\mathfrak{d}) \cap \mathrm{Supp}(\mathrm{r}(\mathfrak{d})) = \emptyset$, our statement follows.

□

DEFINITION 2.6. Let $\mathfrak{d}$ be a semi-reduced divisor on $\mathcal{C}$ and let $\mathrm{r}(\mathfrak{d})$ be the corresponding reduced divisor. Assume that

(♣) $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ is semi-reduced.

The pair of polynomials (u, b), $u \in \overline{K}[x]$, $b \in \mathrm{Rem}(y^2)$ (up to $\overline{K}\backslash\{0\}$) in Lemma 2.5 is called the Leitenberger representation of $\mathfrak{d}$.

REMARK 2.7. (i) If $\mathrm{r}(\mathfrak{d}) = O$, the condition ♣ is satisfied as $\mathfrak{d}$ is an affine divisor. In particular we have $\mathrm{div}([b]) = \mathfrak{d} - (\deg \mathfrak{d})O$.

(ii) If ♣ is not satisfied, i.e., $\mathfrak{d} + \iota^*\mathrm{r}(\mathfrak{d})$ is not semi-reduced, Jacobi's interpolation rational function considered in [13] does not seem to give the desired polynomial function b as $\gcd(b_0, b_1)$ in Lemma 2.4 is not 1. Here is such an example. Let $\mathcal{C}$ be a hyperelliptic curve over $\mathbb{C}$ given by

$$\mathcal{C} : y^2 = x^5 - x^3 + 2x^2 + 2$$

Let $\mathfrak{d}_0 = \mathfrak{d}(u_0, v_0)$ be a semi-reduced divisor of degree 4 given by

$$u_0 = x^4 - x^3 - (t^2 - 2)x - t^2 - 3t - 2$$
$$v_0 = t(x + 1) + 2\,,$$

$t \in \mathbb{C}$. By the reduction algorithm for semi-reduced divisors we have $\mathrm{r}(\mathfrak{d}_0) = (-1, -2)$. Put $\mathfrak{d} = (1, 2) + \mathfrak{d}_0$. Then we have $\mathrm{r}(\mathfrak{d}) = (1, 2) + (-1, -2)$. Hence $\mathfrak{d} + \iota^* \mathrm{r}(\mathfrak{d})$ is not semi-reduced as $\mathfrak{d} + \iota^* \mathrm{r}(\mathfrak{d})$ contains $(1, 2) + (1, -2)$. In this case, we have $u = (x - 1)u_0$ and

$$b = (x - 1)(tx + t + 2 - y)\,.$$

In particular, $\mathfrak{d} \neq (\gcd(\mathrm{div}([u]), \mathrm{div}([b])))_{\mathrm{aff}}$.

2.3. Ideals arising from the two representations of semi-reduced divisors and their bases

Let $\mathfrak{d} = \sum_P e_P P$ be a semi-reduced divisor on $\mathcal{C}$. We define ideals $I(\mathfrak{d}) \subset \overline{K}[\mathcal{C}]$ and $\widetilde{I(\mathfrak{d})} \subset \overline{K}[x, y]$.

$$I(\mathfrak{d}) := \{[g] \in \overline{K}[\mathcal{C}] \mid \mathrm{ord}_P([g]) \geq e_P, \text{ for } \forall P \in \mathrm{Supp}(\mathfrak{d})\}\,,$$
$$\widetilde{I(\mathfrak{d})} := \{g \in \overline{K}[x, y] \mid [g] \in I(\mathfrak{d})\}$$

Let (u, v) and (u, b) be its Mumford and Leitenberger representation, respectively. By their definition, we infer that $u, y - v, b \in \widetilde{I(\mathfrak{d})}$. In this section, we give characterization of these polynomials in terms of Gröbner bases of $\widetilde{I(\mathfrak{d})}$ with respect to certain monomials orders. Let us introduce two monomial orders which we use for our purpose.

2.3.1. Two monomial orders on $K[x, y]$ and $\overline{K}[x, y]$

As for general facts on monomial orders and Gröbner bases, we refer to [5]. In this note, we consider two monomial orders $>_1$ and $>_2$ as follows:

- $>_1$ is the pure lexicographic order with $y > x$.
- $>_2$ is a weighted lexicographic order as follows: For a monomial $y^m x^n$, we put $\mathrm{wdeg}(y^m x^n) = (2g + 1)m + 2n$. We say $y^{m_1} x^{n_1} >_2 y^{m_2} x^{n_2}$ if and only if
  (i) $\mathrm{wdeg}(y^{m_1} x^{n_1}) > \mathrm{wdeg}(y^{m_2} x^{n_2})$ or
  (ii) $(2g + 1)m_1 + 2n_1 = (2g + 1)m_2 + 2n_2$ and $n_1 < n_2$

The monomial order $>_2$ is nothing but a weighted reverse lexicographic order for y, x with weight $(2g + 1, 2)$. It coincides with the C_{ab}-order considered in [1] for $(a, b) = (2g + 1, 2)$.

By $\mathrm{LM}_i(g)$, $\mathrm{LC}_i(g)$ and $\mathrm{LT}_i(g)$, we denote the leading monomial, coefficient and term of g with respect to $>_i$, respectively. Also we denote the multidegree with respect to $>_i$ by $\mathrm{multideg}_i$. Note that if $g \in \overline{K}[x]$ (resp. $K[x]$), $\mathrm{LM}_i(g)$, $\mathrm{LC}_i(g)$ and $\mathrm{LT}_i(g)$ $(i = 1, 2)$ are the leading monomial, coefficient and term of g, respectively in $\overline{K}[x]$ (resp. $K[x]$).

In [1], a description on the ideal class group for C_{ab} curves was given via Gröbner bases. This article can be considered as a hyperelliptic curve version of [1]. In the following two subsections, we will give descriptions for the divisor class group via Gröbner bases of $\widetilde{I(\mathfrak{d})}$.

2.3.2. The Mumford representation and the reduced Gröbner basis of $\widetilde{I(\mathfrak{d})}$ with respect to $>_1$

Let us start the following proposition:

PROPOSITION 2.8. *Let (u, v) be the Mumford representation of $\mathfrak{d}$. Then $\widetilde{I(\mathfrak{d})} = \langle u, y - v\rangle$ and $v^2 - f \in \langle u\rangle$ in $\overline{K}[x]$. In particular, $\{u, y - v\}$ is the reduced Gröbner basis of $\widetilde{I(\mathfrak{d})}$ with respect to $>_1$.*

Proof. Since (u, v) is the Mumford representation of $\mathfrak{d}$, by definition, we have $u, y - v \in \widetilde{I(\mathfrak{d})}$ and $u|(v^2 - f)$. In particular, $\langle u, y - v\rangle \subseteq \widetilde{I(\mathfrak{d})}$ and $\{y - v, u\}$ is the reduced Gröbner basis of $\langle u, y - v\rangle$ by computing the S-polynomial of u and $y - v$ with respect to $>_1$. We now show that $\widetilde{I(\mathfrak{d})} \subseteq \langle u, y - v\rangle$. Choose any $g \in \widetilde{I(\mathfrak{d})}$, we apply [5, Chapter 2, Theorem 3 (Division Algorithm)] to our case: g and $F = (y - v, u)$ with respect to $>_1$. Then we have

$$g = q_1(y - v) + q_2 u + r, \quad r \in \overline{K}[x], \deg r < \deg u \text{ if } r \neq 0, q_1, q_2 \in \overline{K}[x, y]\,.$$

As $r \in \widetilde{I(\mathfrak{d})}$,

$$\operatorname{ord}_{P_i}([r]) \geq e_{P_i} \quad (\forall P_i = (x_{P_i}, y_{P_i}) \in \operatorname{Supp}(\mathfrak{d}))\,,$$

and $r(x_{P_i}) = 0$ for $P_i = (x_{P_i}, 0) \in \operatorname{Supp}(\mathfrak{d})$. Since $\overline{K}[x]$ can be regarded as a subset of $\overline{K}[\mathcal{C}]$, we infer that $u|r$, i.e., $r = 0$. Hence $\widetilde{I(\mathfrak{d})} = \langle u, y - v\rangle$.

□

REMARK 2.9. Our proof of Proposition 2.8 implies that any element $g \in \overline{K}[x] \cap \widetilde{I(\mathfrak{d})}$ is divisible by u, i.e., $\overline{K}[x] \cap \widetilde{I(\mathfrak{d})} = \langle u\rangle$. For $v_1 \in \overline{K}[x]$ such that $y - v_1 \in \widetilde{I(\mathfrak{d})}$, $(y - v) - (y - v_1) = v - v_1 \in \langle u\rangle$. Hence if $\deg v_1 < \deg u$, $v_1 = v$.

REMARK 2.10. If $\mathfrak{d}$ is a semi-reducd divisor defined over K, the two polynomials of its Mumford representation can be chosen from $K[x]$ by [7, Lemma 10.3.10].

2.3.3. The Leitenberger representation and the reduced Gröbner basis of $\widetilde{I(\mathfrak{d})}$ with respect to $>_2$

We next consider an interpretation for the Leitenberger representation. To this purpose, we use the monomial order $>_2$. We first remark that for $b = b_0 + b_1 y \in \operatorname{Rem}(y^2)$ we have $\operatorname{wdeg}(\operatorname{LT}_2(b)) = -\operatorname{ord}_O([b])$. In fact, as $\operatorname{multideg}_2(b) = \max\{(0, \deg b_0), (1, \deg b_1)\}$, we have $\operatorname{wdeg}(\operatorname{LT}_2(b)) = \max\{2\deg b_0, 2g + 1 + \deg b_1\}$. On the other hand, $\operatorname{ord}_O([b]) = -\max\{2\deg b_0, 2g + 1 + \deg b_1\}$ (see [14, Definition 3.3], for example).

LEMMA 2.11. *Let $\mathfrak{d}$ be a semi-reduced divisor and $\mathrm{r}(\mathfrak{d})$ denotes the unique reduced divisor as in Section 1. Put $w_o = \min\{\operatorname{wdeg}(\operatorname{LM}_2(g)) \mid g \in \widetilde{I(\mathfrak{d})}, [g] \neq 0\}$. Then*

$$\deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d}) = w_o$$

holds.

Proof. Our proof consists of 2 steps.

Step 1. We show that $w_{\deg} := \min\{\operatorname{multideg}_2(g) \mid g \in \widetilde{I(\mathfrak{d})}, [g] \neq 0\}$ is attained by some elements in $\widetilde{I(\mathfrak{d})} \cap \operatorname{Rem}(y^2)$. In particular,

$$w_o = \min\{\operatorname{wdeg}(\operatorname{LM}_2(b)) \mid b \in \widetilde{I(\mathfrak{d})} \cap \operatorname{Rem}(y^2), [b] \neq 0\}\,.$$

Choose $g \in \widetilde{I(\mathfrak{d})}$ arbitrary. Note that g can be expressed uniquely as follows:

$$g = q_g(y^2 - f) + b_g,\ q_g \in \overline{K}[x, y],\ b_g = b_{0,g} + b_{1,g} y \in \operatorname{Rem}(y^2) \cap \widetilde{I(\mathfrak{d})}\,.$$

As $\mathrm{multideg}_2(q_g(y^2-f)) = \mathrm{multideg}_2(q_g)+(2,0)$ and $\mathrm{multideg}_2(b_g) = \max\{(0, \deg b_{0,g}), (1, \deg b_{1,g})\}$, by [5, Lemma 8, Ch.2, §2],

$$\begin{aligned}\mathrm{multideg}_2(g) &= \max\{\mathrm{multideg}_2(q_g(y^2-f)), \mathrm{multideg}_2(b_g)\}\\ &\geq \mathrm{multideg}_2(b_g)\,.\end{aligned}$$

Hence $w_{\deg}$ is attained by some element b in $\widetilde{I(\mathfrak{d})} \cap \mathrm{Rem}(y^2)$ with $[b] \neq 0$.

Step 2. Choose $b_{\min} := b_{0,\min} + b_{1,\min} y$ such that $w_{\deg} = \mathrm{multideg}_2 b_{\min}$. As $b_{\min} \in \widetilde{I(\mathfrak{d})}$,

$$\mathrm{div}([b_{\min}]) = \mathfrak{d} + \mathfrak{d}' - (\deg \mathfrak{d} + \deg \mathfrak{d}')O$$

for some effective divisor $\mathfrak{d}'$ and $w_o = (\deg \mathfrak{d} + \deg \mathfrak{d}')$. Choose $\tilde{b} \in \mathrm{Rem}(y^2)$ such that

$$\mathrm{div}([b_{\min}]) = \mathfrak{d} + \iota^* \mathrm{r}(\mathfrak{d}) - (\deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d}))O\,.$$

By Lemmas 2.3, $w_o = \deg \mathfrak{d} + \deg \mathrm{r}(\mathfrak{d})$ and we have $[\tilde{b}] = [cb_{\min}]$ for some $c \in K^\times$ by the uniqueness of such rational functions up to constant. Hence our statement follows. □

Choose $b_{\mathfrak{d}} = b_0 + b_1 y \in \mathrm{Rem}(y^2) \cap \widetilde{I(\mathfrak{d})}$ as in Lemma 2.11 with $\mathrm{LC}_2(b_{\mathfrak{d}}) = 1$. Note that $b_{\mathfrak{d}}$ is unique and $\mathrm{ord}_O([b_{\mathfrak{d}}]) = -w_o$. Let $\mathcal{G}_2$ be the reduced Gröbner basis of $\widetilde{I(\mathfrak{d})}$ with respect to $>_2$. By our proof of Lemma 2.11, we infer that $g_o \in \mathrm{Rem}(y^2)$ for any $g_o \in \mathcal{G}_2$ with $[g_o] \neq 0$.

LEMMA 2.12. *The polynomial $b_{\mathfrak{d}}$ is a member of $\mathcal{G}_2$ such that* $\mathrm{multideg}_2$ *is minimum in the set* $\{g \in \mathcal{G}_2 \mid [g] \neq 0\}$.

Proof. Choose $g_o \in \mathcal{G}_2$ so that $\mathrm{multideg}_2$ is minimum in $\{g \in \mathcal{G}_2 \mid [g] \neq 0\}$. By our choice of $b_{\mathfrak{d}}$, $\mathrm{multideg}_2(b_{\mathfrak{d}}) \leq \mathrm{multideg}_2(g_o)$. On the other hand, $\mathrm{LT}_2(b_{\mathfrak{d}})$ is divisible by $\mathrm{LT}_2(g)$ for some $g \in \mathcal{G}_2$ with $[g] \neq 0$ as $b_{\mathfrak{d}} \in \mathrm{Rem}(y^2) \cap \widetilde{I(\mathfrak{d})}$. Hence $\mathrm{multideg}_2(b_{\mathfrak{d}}) \geq \mathrm{multideg}_2(g_o)$ and this implies $\mathrm{multideg}_2(b_{\mathfrak{d}}) = \mathrm{multideg}_2(g_o)$. Since $b_{\mathfrak{d}}, g_o \in \mathrm{Rem}(y^2)$ and both leading coefficients of $b_{\mathfrak{d}}$ and g_o is 1, if $b_{\mathfrak{d}} \neq g_o$, then we have $b_{\mathfrak{d}} - g_o \in \widetilde{I(\mathfrak{d})}$, $[b_{\mathfrak{d}} - g_o] \neq 0$ and $\mathrm{multideg}_2(b_{\mathfrak{d}} - g_o) < \mathrm{multideg}(b_{\mathfrak{d}})$. This contradicts to our choice of $b_{\mathfrak{d}}$. Hence $b_{\mathfrak{d}} = g_o \in \mathcal{G}_2$. □

Let $\mathfrak{d}$ be a semi-reduced divisor satisfying ♣. Let (u, v) be the Mumford representation of $\mathfrak{d}$ and let $b_{\mathfrak{d}}$ be as above. Then $(u, b_{\mathfrak{d}})$ is the Leitenberger representation of $\mathfrak{d}$ and we have the following proposition:

PROPOSITION 2.13. *The ideal $\widetilde{I(\mathfrak{d})}$ coincides with $\langle u, b_{\mathfrak{d}}, y^2 - f\rangle$. In particular, $I(\mathfrak{d}) = \langle [u], [b_{\mathfrak{d}}]\rangle$*

Proof. Put $b_{\mathfrak{d}} = b_0 + b_1 y$. As $\mathfrak{d}$ satisfies ♣, $\gcd(b_0, b_1) = 1$. If $\gcd(u, b_1) \neq 1$, there exists $P = (x_P, y_P) \in \mathcal{C}$ such that $u(x_P) = 0$ and $b_1(x_P) = 0$. As $b_{\mathfrak{d}} \in \widetilde{I(\mathfrak{d})}$, we infer that $b_{\mathfrak{d}}(x_P, y_P) = 0$ or $b_{\mathfrak{d}}(x_P, -y_P) = 0$, i.e., $b_0(x_P) = 0$ also holds. This contradicts to $\gcd(b_0, b_1) = 1$. Hence $\gcd(u, b_1) = 1$. By choosing $h_1, h_2 \in \overline{K}[x]$ such that $h_1 u + h_2 b_1 = 1$, we have

$$h_1 u y + h_2 b_{\mathfrak{d}} = y + h_2 b_0\,.$$

Take v_1 so that $-v_1 \equiv h_2 b_0 \pmod{u}$. As $y - v$, $y - v_1 \in \widetilde{I(\mathfrak{d})}$, we infer that $v_1 - v \in \widetilde{I(\mathfrak{d})} \cap \overline{K}[x]$. By Remark 2.9, $v_1 - v$ is divisible by u, which implies $v = v_1$. Hence $\langle u, y - v\rangle \subseteq \langle u, b_{\mathfrak{d}}, y^2 - f\rangle$ and our statement follows from Proposition 2.8. □

REMARK 2.14. If the semi-reduced divisore $\mathfrak{d}$ as above is defined over K, u, $y - v \in K[x, y]$ by Remark 2.10. Hence we infer that $b_{\mathfrak{d}} \in K[x, y]$ since computation to obtain $\mathcal{G}_2$ can be done in $K[x, y]$.

2.3.4. Remark on the addition on $\mathrm{Pic}^0(\mathcal{C})$

Let us recall that that both of the Mumford and Leitenberger representations have been used in order to compute the *'addition'* on $\mathrm{Pic}^0(\mathcal{C})$, explicitly, in [7, 12, 13, 14]. In this subsection we give a remark about the addition from our viewpoint.

Suppose that two h-reduced divisors $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are given. The addition on $\mathrm{Pic}^0(\mathcal{C})$ consists of two steps:

- Step 1. To find a semi-reduced divisor $\mathfrak{d}_3$ such that $\mathfrak{d}_1 + \mathfrak{d}_2 - \deg(\mathfrak{d}_1 + \mathfrak{d}_2)O \sim \mathfrak{d}_3 - \deg(\mathfrak{d}_3)O$.
- Step 2. To find $\mathrm{r}(\mathfrak{d}_3)$.

We first consider the Step 1. Assume that $\mathfrak{d}_1 + \mathfrak{d}_2$ can be rewritten of the form $\mathfrak{d}_o + \bar{\mathfrak{d}} + \iota^*\bar{\mathfrak{d}}$, where $\mathfrak{d}_o$ is a non-zero semi-reduced divisor and $\bar{\mathfrak{d}}$ is an effective divisor. Then we can take $\mathfrak{d}_o$ as $\mathfrak{d}_3$. Let (u_3, v_3) be the Mumford representation of $\mathfrak{d}_3$. Write $\bar{\mathfrak{d}} = \sum_j e_j P_j$, $P_j = (x_{P_j}, y_{P_j})$ and put $u_o = \prod_j (x - x_{P_j})^{e_j}$. Then we see that $\mathrm{div}([u_o]) = \bar{\mathfrak{d}} + \iota^*\bar{\mathfrak{d}} - 2(\deg \bar{\mathfrak{d}})O$ holds. Under these notation, we have

PROPOSITION 2.15. *Assume that* $\mathfrak{d}_3 \neq 0$. *Both* $u_o u_3$ *and* $u_o(y - v_3)$ *are contained in the reduced Gröbner basis of* $I(\widetilde{\mathfrak{d}_1 + \mathfrak{d}_2})$ *with respect to* $>_1$.

Proof. If $\bar{\mathfrak{d}} = 0$, we can take 1 as u_o. Hence our statement follows from Proposition 2.8. Now we assume $\bar{\mathfrak{d}} \neq 0$. Put $I_3 = I(\widetilde{\mathfrak{d}_1 + \mathfrak{d}_2})$. Since $\overline{K}[\mathcal{C}]$ is a Dedekind domain, we have $I(\bar{\mathfrak{d}} + \iota^*\bar{\mathfrak{d}}) = \langle [u_o] \rangle$ and

$$I(\mathfrak{d}_1 + \mathfrak{d}_2) = I(\mathfrak{d}_3) I(\mathfrak{d}_o + \iota^*\mathfrak{d}_o) = \langle [u_o][u_3], [u_o][y - v_3] \rangle .$$

Hence $I_3 = \langle u_o u_3, u_o(y - v_3), y^2 - f \rangle$. Since $\mathfrak{d}_3, \bar{\mathfrak{d}} \neq 0$, for any element g in I_3, $\mathrm{div}([g])_{\mathrm{aff}} - \bar{\mathfrak{d}} - \iota^*\bar{\mathfrak{d}}$ is effective, where $\mathrm{div}([\bullet])_{\mathrm{aff}} := \sum_{P \in \mathcal{C}_{\mathrm{aff}}} \mathrm{ord}_P([\bullet])P$ for $\bullet \in \overline{K}[\mathcal{C}]$. Therefore no polynomial of the form $y - b, b \in \overline{K}[x]$, is contained in I_3. As $y^2 - f \in I_3$, by [5, Chapter 5, §3], the reduced Gröbner basis $\mathcal{G}(I_3)$ of I_3 is of the form $\{g_1, g_2, g_3\}$ such that $\mathrm{LT}_1(g_1) = x^{n_1}, \mathrm{LT}_1(g_2) = x^{n_2} y, \mathrm{LT}_1(g_3) = y^2$. We first show that $g_1 = u_o u_3$, i.e., $I_3 \cap \overline{K}[x] = \langle u_o u_3 \rangle$. As $g_1 \in I_3$ and $\mathrm{div}([g_1])_{\mathrm{aff}} - \mathrm{div}([u_o][u_3])_{\mathrm{aff}}$ is effective, $g_1 = u_o u_3 g_1' + h(y^2 - f)$ for some $g_1' \in \mathrm{Rem}(y^2), h \in \overline{K}[x, y]$. Since $g_1 \in \overline{K}[x]$, we infer that $g_1' \in \overline{K}[x]$ and $h = 0$. On the other hand, as $u_o u_3 \in I_3 \cap \overline{K}[x]$, x^{n_1} divides $\mathrm{LT}_1(u_o u_3)$. Hence we have $\mathrm{LT}_1(g_1) = \mathrm{LT}_1(u_o u_3)$ and $g_1 = u_o u_3$. We next consider g_2. As $g_2 \in I_3$, $g_2 - u_o g_2' \in \langle y^2 - f \rangle$ for some $g_2' \in \mathrm{Rem}(y^2) \setminus \overline{K}[x]$. This means that y^2 divides $\mathrm{LT}_1(g_2 - u_o g_2')$. As $g_2 \in \mathrm{Rem}(y^2)$, we infer that $g_2 = u_o g_2'$. This implies $\mathrm{LT}_1(u_o(y - v_3)) = x^{\deg u_o} y$ divides $\mathrm{LT}_1(g_2) = x^{n_2} y$. On the other hand, since $u_o(y - v_3) \in I_3$, $x^{n_2} y$ divides $\mathrm{LT}_1(u_o(y - v_3))$. This implies that $\mathrm{LT}_1(u_o(y - v_3)) = \mathrm{LT}_1(g_2)$ and we have $u_o(y - v_3) - g_2 \in I_3 \cap \overline{K}[x]$. Hence we have $u_o(y - v_3) = g_2 + r g_1$ for some $r \in \overline{K}[x]$. As $g_1, g_2 \in \mathcal{G}(I_3)$ and $\deg v_3 < \deg u_3$, we infer that $\deg r g_1 < \deg g_1$ if $r \neq 0$. Thus we have $r = 0$ and $g_2 = u_o(y - v_3)$. □

By our proof of Proposition 2.15, we have the following corollary.

COROLLARY 2.16. *If we let* $\widetilde{f \equiv f_o \mod u_o u_3}$, *then* $\{u_o u_3, u_o(y - v_3), y^2 - f_o\}$ *is the reduced Gröbner basis of* $\widetilde{I(\mathfrak{d}_1 + \mathfrak{d}_2)}$ *with respect to* $>_1$.

Now the Step 1 can be summarized in the following way:

By Proposition 2.15, if $\mathfrak{d}_1$ and $\mathfrak{d}_2$ are given by the Mumford representations (u_1, v_1) and (u_2, v_2), respectively, the Mumford representation of $\mathfrak{d}_3$ can be obtained in the following way:

(i) Compute the reduced Gröbner basis $\mathcal{G}$ of $\langle u_1 u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2), y^2 - f\rangle$ with respect to $>_1$.

(ii) If $\mathcal{G}$ consists of two elements, it means $\mathfrak{d}_3 = 0$ or $\mathcal{G} = \{u_3, y - v_3\}$ where the pair $\{u_3, v_3\}$ is the Mumford representation of $\mathfrak{d}_3$.

(iii) If $\mathcal{G}$ consists of three elements, we put $\mathcal{G} = \{g_1, g_2, g_3\}$ such that $g_1 \in \overline{K}[x]$, g_2 is of the form $b_0(x) + b_1(x)y \in \mathrm{Rem}(y^2)$ and $g_3 = y^2 + \ldots$. By Proposition 2.15, the Mumford representation of $\mathfrak{d}_3$ is $(g_1/b_1, -b_0/b_1)$.

As for the Step 2, it can be summarized as follows:

PROPOSITION 2.17. *Suppose that* $\mathfrak{d}_3$ *satisfies* ♣ *and let* $(u, b_{\mathfrak{d}_3})$ *be its Leitenberger representation as in Proposition 2.13. The Leitenberger representation of* $\mathrm{r}(\mathfrak{d}_3)$ *is given by* $(u_1, b_{\mathfrak{d}_3})$ *where* $u_1 \in \overline{K}[x]$ *is a monic polynomial obtained as follows:* $u_1 := u'/\mathrm{LC}_2(u')$, *where* $b_{\mathfrak{d}_3} = b_0 + b_1 y$ *and* $u' := (b_0^2 - b_1^2 f)/u$.

Proof. By the definition of the Leitenberger representation, our statement is straightforward. □

REMARK 2.18. One of the remaining questions may be how our approach is efficient from computational point of view. It may be interesting, but we do not go on this direction further as our main interest in this article is to study curves with quasi-toric relations.

3. Plane curves with quasi-toric relations of type $(2, n, 2)$

Let us start with explaining how we apply our previous consideration to obtain curves with quasi-toric relation of type $(2, n, 2)$. Let $\mathcal{C}$ be a hyperelliptic curve of genus g defined over K as in the Introduction. Let $\mathfrak{d}_o$ be a non-zero semi-reduced divisor defined over K such that (i) $k(\mathfrak{d}_o - (\deg \mathfrak{d}_o)O) \not\sim 0$, $1 \le k < n$ and (ii) $n(\mathfrak{d}_o - (\deg \mathfrak{d}_o)O) \sim 0$, i.e., $\mathfrak{d}_o - (\deg \mathfrak{d}_o)O$ gives rise to a torsion element of order n in $\mathrm{Pic}^0(\mathcal{C})$. Assume that $\mathfrak{d}_o$ is given by a Mumford representation (u_o, v_o). Then we have $I(\mathfrak{d}_o) = \langle [u_o], [y - v_o]\rangle$ and $\widetilde{I(n\mathfrak{d}_o)} = \widetilde{I(\mathfrak{d}_o)^n} = \langle u_o^n, u_o^{n-1}(y - v_o), \ldots, (y - v_o)^n, y^2 - f\rangle$. We compute the reduced Gröbner basis $\mathcal{G}_2$ of $\widetilde{I(n\mathfrak{d}_o)}$ with respect to $>_2$. Let g_n be an element of $\mathcal{G}_2 \setminus \{y^2 - f\}$ with minimum multidegree. By Remark 2.7, our proof of Lemma 2.12 and Remark 2.14, $g_n \in \mathrm{Rem}(y^2) \cap K[x, y]$ and $\mathrm{div}([g_n]) = n(\mathfrak{d}_o - (\deg \mathfrak{d}_o)O)$. Hence we can choose g_n as $b_{n\mathfrak{d}_o}$. Now put $b_{n\mathfrak{d}_o} = b_0 + b_1 y$. We have $[b_{n\mathfrak{d}_o} \iota^* b_{n\mathfrak{d}_o}] = [b_0^2 - b_1^2 y^2] = [b_0^2 - b_1^2 f] = [r(u_o)^n]$, $r \in \overline{K}\setminus\{0\}$ as $\mathrm{div}([b_{n\mathfrak{d}_o} \iota^* b_{n\mathfrak{d}_o}]) = n\mathfrak{d}_o + n\iota^*\mathfrak{d}_o - 2n(\deg \mathfrak{d}_o)O = \mathrm{div}([(u_o)^n])$. In particular, as $\mathfrak{d}_o$ is defined over K, we have $b_{n\mathfrak{d}_o} \in K[x, y]$. Hence $b_0^2 - b_1^2 f, u_o \in K[x]$ and

$$(*) \quad b_0^2 - b_1^2 f = r(u_o)^n, \ r \in \overline{K}\setminus\{0\}$$

holds in $K[x]$.

Now assume that $K = \mathbb{C}(t)$ and $a, b, c \in \mathbb{C}[t]$. In this case, $f(x) \in \mathbb{C}[t, x]$ and we have a plane curve $\mathcal{B}_o$ in $\mathbb{P}^2$ given by the affine equation $f(x) = 0$. Then we have the following:

PROPOSITION 3.1. *Under the above setting, put $\mathcal{B} = \mathcal{B}_o + L_\infty$, where L_∞ denotes the line at infinity. If $r \in \mathbb{C}\backslash\{0\}$ and $u_{n\mathfrak{d}_o}, b_{n\mathfrak{d}_o}$ are also in $\mathbb{C}[t, x]$, then either $\mathcal{B}_o$ or $\mathcal{B}$ satisfies a quasi-toric relation of type* $(2, n, 2)$.

Proof. By homogenizing $(*)$, our statement is straightforward. □

Based on this approach, we construct examples of plane curves satisfying quasi-toric relations of type $(2, n, 2)$ with continuous parameter in Section 4.

4. Examples for the case of $g = 1$

In this section, we consider the case of $g = 1$ and apply our results on Leitenberger representations in Section 2 to study explicit construction of plane curves. In this case, $\mathcal{C}$ is an elliptic curve and we denote it by

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c, \quad a,\ b,\ c \in K \quad O = [0, 1, 0]\,.$$

Let $T = (x_T, y_T)$ be a torsion point of order n and assume that $T \in E(K)$. By the definition of the addition law on E, $\mathrm{r}(nT) = O$. Let $l_{[-1]T}$ be a line given by $y = r(x - x_T) - y_T$, $r \in K\backslash\{0\}$. Put $l_{[-1]T} \cap E = \{[-1]T, P_1, P_2\}$ and $\mathfrak{d}_T := P_1 + P_2$. Then $\mathfrak{d}_T$ is a semi-reduced divisor defined over K of degree 2 whose Mumford representation is given by

$$u_{\mathfrak{d}_T} = \frac{f(x) - \{r(x - x_T) - y_T\}^2}{x - x_T}, \quad v_{\mathfrak{d}_T} = r(x - x_T) - y_T\,.$$

As $n(\mathfrak{d}_T - 2O) \sim n(T - O) \sim 0, \mathrm{r}(n\mathfrak{d}_T) = 0$. Hence ♣ is satisfied for $n\mathfrak{d}_T$ by Remark 2.7. Now we apply our consideration in Section 3 to some explicit cases.

REMARK 4.1. (i) In the case of $K = \mathbb{C}$, by applying our argument in Section 3 to nT, we see that the curve given by $b_{nT} = 0$ is an n-contact curve to E.

(ii) By [6, Theorem 5.1], our method by using the cases of genus 1 works for $n \leq 12 (\neq 11)$. In particular, if n is odd prime, $n = 3, 5, 7$ are all possible cases.

REMARK 4.2. In the examples below, $K = \mathbb{C}(t)$ and we consider families of semi-reduced divisors $\mathfrak{d}(r)$ given by the Mumford representations $(u(r), v(r))$, where $u(r), v(r) \in K[r, x]$ and the value of r is chosen from $\mathbb{C}$ so that $\mathfrak{d}(r)$ is a semi-reduced divisors on E. Let

$$I(r) := \langle u(r)^n, u(r)^{n-1}(y - v(r)), \ldots (y - v(r))^n, y^2 - f(x)\rangle \subset K(r)[x, y]\,.$$

We first compute the reduced Gröbner basis, $\mathcal{G}_2(r)$ of $I(r)$ with respect to $>_2$. Choose $g(r) \in \mathcal{G}_2(r)$. As $g(r) \in I(r)$, $g(r)$ has an expression

$$(*) \qquad g(r) = h_0(r)u(r)^n + h_1(r)u(r)^{n-1}(y - v(r)) + \ldots + h_n(r)(y - v(r))^n + h_{n+1}(r)(y^2 - f(x))\,,$$

where $h_i(r) \in K(r)[x, y]$. Assume that $(*)$ can be well-defined for a fixed value $r_o \in \mathbb{C}$. Then, as $I(r_o) = I(\widetilde{n\mathfrak{d}(r_o)})$, $g(r_o) \in I(\widetilde{n\mathfrak{d}(r_o)})$. If $[g(r_o)] \neq 0$ and $\mathrm{wdeg}(\mathrm{LM}_2(g(r_o))$ is the minimum value w_o, then we see $g(r_o) = g_{n\mathfrak{d}(r_o)} \in \mathcal{G}_2(I(\widetilde{n\mathfrak{d}(r_o)}))$ by Lemmas 2.11 and 2.12, where $\mathcal{G}_2(I(\widetilde{n\mathfrak{d}(r_o)}))$ is the reduced Gröbner basis of $I(\widetilde{n\mathfrak{d}(r_o)})$ with respect to $>_2$. In particular, if $\mathfrak{d}(r_o) - (\deg \mathfrak{d}(r_o))O$ is a torsion of order n, then $\mathrm{r}(n\mathfrak{d}(r_o)) = 0$ and $w_o = n \deg \mathfrak{d}(r_o)$. Hence if $\mathrm{wdeg}(\mathrm{LM}_2(g(r_o))) = n \deg \mathfrak{d}(r_o)$, $g(r_o) = g_{n\mathfrak{d}(r_o)}$. The above observation does not necessarily mean that $\mathcal{G}_2(r)$ is a comprehensive Gröbner basis as we only check one element of $\mathcal{G}_2(r)$ and need to choose r so that $(*)$ is defined (see [17] for comprehensive Gröbner bases). As for more general treatment for $\mathcal{G}_2(\mathfrak{d}(r_o))$, we refer to [5, Section 3, Exercise 7, Ch. 6]. Note that by Remark 2.9, for an element of the form $y - v$, a similar argument holds between the reduced Gröbner basis, $\mathcal{G}_1(r)$, with respect to $>_1$ and that of $I(\widetilde{n\mathfrak{d}(r_o)})$ with respect to $>_1$, $\mathcal{G}_1(I(\widetilde{n\mathfrak{d}(r_o)}))$.

4.1. Explicit examples

We consider examples for $n = 3, 5, 7$. Our computation and argument are based on Remark 4.2. We use Maple for our computation.

EXAMPLE 4.3. Let E_3 be an elliptic curve defined over $\mathbb{C}(t)$ given by $y^2 = f_3$, $f_3(x) = x^3 + (x + t)^2$. $T := (0, t)$ is a point on E_3 of order 3. Note that the tangent line at T is a weak 3-contact curve to E.

Plane curves with quasi-toric relation of type $(2, 3, 2)$. Let $l_{[-1]T}$ be a line through $[-1]T$. We may assume that $l_{[-1]T}$ is given by $y = rx - t$ $(r \in \mathbb{C}\backslash\{0\})$. Put $l_{[-1]T} \cap E_3 = \{[-1]T, P_1, P_2\}$ and $\mathfrak{d}_T := P_1 + P_2$, $P_i = (x_i, y_i)$. The Mumford representation of $\mathfrak{d}_T$ is $(u_{\mathfrak{d}_T}, v_{\mathfrak{d}_T})$, where

$$u_{\mathfrak{d}_T} = x^2 + (1 - r^2)x + 2t(1 + r), \quad v_{\mathfrak{d}_T} = rx - t\,.$$

Now we apply our argument in Section 3 to $\widetilde{I(3\mathfrak{d})}$. Then we have $b_{3\mathfrak{d}_T} = b_0 + b_1 y$ where

$$\begin{aligned} b_0 &= x^3 + (2 + 3r + 3r^2)x^2 + (1 + 3r + 3r^2 + r^3 + t - 3tr)x \\ &\quad + t + 3rt + 3r^2t + r^3t + 2t^2\,, \\ b_1 &= x(-1 - 3r) - 1 - 3r - 3r^2 - r^3 + 2t\,, \end{aligned}$$

and

$$b_0^2 - b_1^2(x^3 + (x + t)^2) = (x^2 + (1 - r^2)x + 2(1 - r)t)^3\,.$$

By Proposition 3.1, we make use of the above equality to find curves satisfying infinitely many quasi-toric relations of type $(2, 3, 2)$ with a continuous parameter r. By homogenizing both hand side $[T, X, Z]$, $t = T/Z$, $x = X/Z$, we have

$$\begin{aligned} &(Z^3 b_0(T/Z, X/Z))^2 + (Z(b_1(T/Z, X/Z))^2(Z(X^3 + (X + T)^2 Z)) \\ &= (X^2 + (1 - r^2)XZ + 2(1 - r)TZ)^3\,. \end{aligned}$$

Since we can choose r from a suitable Zariski open set of $\mathbb{C}$, $\mathcal{B}$ given by $Z(X^3 + (X + T)^2 Z) = 0$ satisfies infinitely many quasi-toric relations of type $(2, 3, 2)$ such that $F_1 =$

$1, F_2 = -1, F_3 = Z(X^3+(X+T)^2Z), h_1 = Z^3 b_0(T/Z, X/Z), h_2 = X^2+(1-r^2)XZ+2(1-r)TZ$, and $h_3 = Z(b_1(T/Z, X/Z)$.

EXAMPLE 4.4. Let E_5 be the elliptic curve over $\mathbb{C}(t)$ given by

$$E_5 : y^2 = f_5(t,x) = x^3 + \frac{1}{4}(t^2+4t-4)x^2 + \frac{1}{2}t(t-1)x + \frac{1}{4}(t-1)^2 .$$

Put $T := \left[0, \dfrac{t-1}{2}\right]$. T is a point on E_5 of order 5.

Weak 5-contact curves. Since $\widetilde{I(5T)} = \langle x^5, x^4(y-\frac{t-1}{2}), x^3(y-\frac{t-1}{2})^2, x^2(y-\frac{t-1}{2})^3, x(y-\frac{t-1}{2})^4, (y-\frac{t-1}{2})^5, y^2-f_5\rangle$, we have the reduced Gröbner basis $\mathcal{G}_2(\widetilde{I(5T)})$ of $\widetilde{I(5T)}$ with respect to $>_2$ and b_{5T} is as follows:

$$\mathcal{G}_2(\widetilde{I(5T)}) = \{g_1, g_2, g_3\} ,$$

where

$$\begin{aligned} 2g_1 &= (-t-2)x^2 + 2xy + (-2t+1)x + 2y + 1 - t , \\ g_2 &= y^2 - f_5 , \\ 2g_3 &= 2x^4 - 2x^3 + tx + 2x^2 + t - 2y - 1 . \end{aligned}$$

Since $\mathrm{multideg}_2(g_1) = (1,1), \mathrm{wdeg}(\mathrm{LM}_2(g_1)) = 5$ and $\mathrm{multideg}_2(g_3) = (4,0)$, $\mathrm{wdeg}(\mathrm{LM}_2(g_3)) = 8$, we have $b_{5T} = g_1$. Hence $b_{5T} := b_0 + b_1 y, b_0 := (-t-2)x^2 + (-2t+1)x + 1 - t, b_1 := 2x+2$ and we have

$$b_0^2 - b_1^2 f_5 = -4x^5 .$$

For a general $t \in \mathbb{C}$, the curve D_{5T} given by $b_{5T} = 0$ is a weak 5-contact curve to E_5 such that $D_{5T}|_{E_5} = 5T + O$.

Plane curves with quasi-toric relations of type $(2,5,2)$. We choose any semi-reduced divisor $\mathfrak{d}_T$ of degree 2 such that $v_{\mathfrak{d}_T}$ in the Mumford representation $(u_{\mathfrak{d}_T}, v_{\mathfrak{d}_T})$ is of the form $r(x-x_T) - y_T$, $r \in \mathbb{C}\backslash\{0\}$. We infer that $u_{\mathfrak{d}_T}$ and $v_{\mathfrak{d}_T}$ satisfy

$$v_{\mathfrak{d}_T}^2 - f = -(x-x_T)u_{\mathfrak{d}_T} ,$$

$$u_{\mathfrak{d}_T} = x^2 - (r^2 - \frac{1}{4}t^2 - t + 1)x + rt - r + \frac{t^2}{2} - \frac{t}{2}, \quad v_{\mathfrak{d}_T} = rx - \frac{1}{2}(t-1) .$$

Now we apply our argument to $\widetilde{I(5\mathfrak{d}_T)}$. $\mathcal{G}_2(\widetilde{I(5\mathfrak{d}_T)})$ contains a polynomial $g = x^5 +$ lower terms and $[g] \neq 0$. As $\deg 5\mathfrak{d}_T = 10$, we choose g as $b_{5\mathfrak{d}_T}$ and put $64 b_{5\mathfrak{d}_T} = b_0 + b_1 y$ where

$$\begin{aligned} b_0 = {} & 32 - 128t + 32r^5 t + 80r^4 t^2 + 80r^3 t^3 + 40r^2 t^4 + 10rt^5 - 80r^4 t - 80r^3 t^2 \\ & - 40r^2 t^3 - 10rt^4 - 128t^3 + 32t^4 - 32r^5 - t^5 + 64x^5 + t^6 \\ & + (640r^2 + 160rt + 48t^2 + 320r + 192t - 128)x^4 \\ & + (320r^4 + 320r^3 t + 320r^2 t^2 + 80rt^3 + 12t^4 + 640r^3 + 1280r^2 t + 480rt^2 + 96t^3 \\ & - 640r^2 + 160t^2 - 160r - 368t + 160)x^3 + (32r^5 t + 80r^4 t^2 + 80r^3 t^3 + 40r^2 t^4 \end{aligned}$$

$$
\begin{aligned}
&+ 10rt^5 + t^6 + 64r^5 + 320r^4t + 480r^3t^2 + 320r^2t^3 + 100rt^4 + 12t^5 + 320r^3t \\
&+ 800r^2t^2 + 240rt^3 + 56t^4 - 320r^3 - 1120r^2t - 400rt^2 + 8t^3 + 320r^2 + 320rt \\
&- 208t^2 - 160r + 208t - 64)x^2 + (64r^5t + 160r^4t^2 + 160r^3t^3 + 80r^2t^4 + 20rt^5 \\
&+ 2t^6 - 32r^5 + 80r^4t + 240r^3t^2 + 200r^2t^3 + 70rt^4 + 9t^5 - 160r^4 - 320r^3t \\
&- 240r^2t^2 - 240rt^3 + 6t^4 + 480rt^2 - 16t^3 - 480rt - 48t^2 + 160r + 80t - 32)x \\
&+ 192t^2\,,
\end{aligned}
$$

$$
\begin{aligned}
b_1 = {} & (-320r - 32t - 64)x^3 + (-640r^3 - 320r^2t - 160rt^2 - 16t^3 - 640r^2 - 640rt \\
&- 96t^2 + 320r + 32t)x^2 + (-64r^5 - 160r^4t - 160r^3t^2 - 80r^2t^3 - 20rt^4 - 2t^5 \\
&- 320r^4 - 640r^3t - 480r^2t^2 - 160rt^3 - 20t^4 - 320rt^2 - 32t^3 + 640rt + 128t^2 \\
&- 320r - 160t + 64)x - 64r^5 - 160r^4t - 160r^3t^2 - 80r^2t^3 - 20rt^4 - 2t^5 + 64t^3 \\
&- 192t^2 + 192t - 64\,,
\end{aligned}
$$

and

$$b_0^2 - b_1^2 f_5 = -4(4u_{\mathfrak{d}_T})^5\,.$$

By homogenizing both hand side $[T, X, Z]$, $t = T/Z$, $x = X/Z$, we have

$$
\begin{aligned}
&(Z^8 b_0(T/Z, X/Z))^2 + (Z^6 b_1(T/Z, X/Z))^2 (Z^4 f_5(T/Z, X/Z)) \\
&= 4Z(-4XZ^2r^2 + 4TZ^2r - 4Z^3r + T^2X \\
&\quad + 2T^2Z + 4TXZ - 2TZ^2 + 4X^2Z - 4XZ^2)^5\,.
\end{aligned}
$$

Since we can choose r from a suitable Zariski open set of $\mathbb{C}$, $\mathcal{B}$ given by $-4Z^5(f_5(T/Z, X/Z)) = 0$ satsifies infinitely many quasi-toric relations of type (2, 5, 2) such that

$$
\begin{aligned}
&h_1 = Z^8 b_0(T/Z, X/Z)\,,\\
&h_2 = -4XZ^2r^2 + 4TZ^2r - 4Z^3r + T^2X + 2T^2Z + 4TXZ - 2TZ^2 + 4X^2Z - 4XZ^2\,,\\
&h_3 = Z^6 b_1(T/Z, X/Z)\,,\\
&F_1 = 1, \quad F_2 = -4Z, \quad F_3 = Z^4 f_5(T/Z, X/Z)\,.
\end{aligned}
$$

EXAMPLE 4.5. Let E_7 be the elliptic curve over $\mathbb{C}(t)$ given by

$$E_7 : y^2 = f_7(t, x) = x^3 + \frac{1}{4}(t^4 - 6t^3 + 3t^2 + 2t + 1)x^2 + \frac{1}{2}(t^5 - 2t^4 + t^2)x + \frac{1}{4}(t^6 - 2t^5 + t^4)\,.$$

Put $T := \left[0, \dfrac{t^3 - t^2}{2}\right]$. T is a point on E_5 of order 7.

Weak 7-contact curves. Since $\widetilde{I(7T)} = \langle x^7, x^6(y - \frac{t^3-t^2}{2}), x^5(y - \frac{t^3-t^2}{2})^2, x^4(y - \frac{t^3-t^2}{2})^3, x^3(y - \frac{t^3-t^2}{2})^4, x^2(y - \frac{t^3-t^2}{2})^5, x(y - \frac{t^3-t^2}{2})^6, (y - \frac{t^3-t^2}{2})^7, y^2 - f_7\rangle$, have the reduced Gröbner basis $\mathcal{G}_2(\widetilde{I(7T)})$ of $\widetilde{I(7T)}$ with respect to $>_2$ and b_{7T} is as follows:

$$\mathcal{G}_2(\widetilde{I(7T)}) = \{g_1, g_2, g_3\}\,,$$

where

$$\begin{aligned}
g_1 &= y^2 - f_7\,,\\
2g_2 &= (-t^2+3t+3)x^3 + 2x^2y + (-3t^3+4t^2+3t+1)x^2 + (4t+2)yx\\
&\quad + (-3t^4+2t^3+2t^2)x + 2yt^2 - t^5 + t^4\,,\\
2g_3 &= 2x^5 + (-4t-2)x^4 + (6t^2+8t+2)x^3 + (-t^5-3t^4+8t^3+12t^2+6t+1)x^2\\
&\quad + (2t^3+12t^2+10t+2)yx + (-2t^6-7t^5+4t^4+8t^3+2t^2)x\\
&\quad + (2t^4+6t^3+2t^2)y - t^7 - 2t^6 + 2t^5 + t^4\,.
\end{aligned}$$

Since $\mathrm{multideg}_2(g_2) = (2,1)$, $\mathrm{wdeg}(\mathrm{LM}_2(g_2)) = 7$ and $\mathrm{multideg}_2(g_3) = (5,0)$, $\mathrm{wdeg}(\mathrm{LM}_2(g_3)) = 10$, we have $b_{7T} = g_2$. Hence $b_{7T} := b_0 + b_1 y$, $b_0 := (-t^2+3t+3)x^3 + (-3t^3+4t^2+3t+1)x^2 + (-3t^4+2t^3+2t^2)x - t^5 + t^4$, $b_1 := 2x^2 + (4t+2)x + 2t^2$ and we have

$$b_0^2 - b_1^2 f_7 = -4x^7\,.$$

For a general $t \in \mathbb{C}$, the curve D_{7T} given by $b_{7T} = 0$ is a weak 7-contact curve to E_7 such that $D_{7T}|_{E_7} = 7T + 2O$.

Plane curves with quasi-toric relations of type $(2,7,2)$. We first choose any semi-reduced divisor $\mathfrak{d}_T$ of degree 2 such that $v_{\mathfrak{d}_T}$ in the Mumford representation $(u_{\mathfrak{d}_T}, v_{\mathfrak{d}_T})$ is of the form $r(x - x_T) - y_T$, $r \in \mathbb{C}\backslash\{0\}$. We infer that $u_{\mathfrak{d}_T}$ and $v_{\mathfrak{d}_T}$ satisfy

$$\begin{aligned}
f - v_{\mathfrak{d}_T}^2 &= (x - x_T)u_{\mathfrak{d}_T}\,,\\
u_{\mathfrak{d}_T} &= x^2 - (r^2 - \frac{1}{4}t^4 + \frac{3}{2}t^3 - \frac{3}{4}t^2 - \frac{1}{2}t - \frac{1}{4})x + rt^3 - rt^2 + \frac{t^5}{2} - t^4 + \frac{t^2}{2},\\
v_{\mathfrak{d}_T} &= rx - \frac{1}{2}t^3 + \frac{1}{2}t^2\,.
\end{aligned}$$

Now we apply our argument to $\widetilde{I(7\mathfrak{d})}$. $\mathcal{G}_2(\widetilde{I(7\mathfrak{d}_T)})$ contains a polynomial $g = x^7 +$ lower terms and $[g] \neq 0$. As $\deg 7\mathfrak{d}_T = 14$, we choose g as $b_{7\mathfrak{d}_T}$ and put $256 b_{7\mathfrak{d}_T} = b_0 + b_1 y$. Then we have

$$b_0^2 - b_1^2 f_7 = -4(-4u_{\mathfrak{d}_T})^7\,.$$

We here omit explicit forms of b_0 and b_1 as they are too long. By homogenizing both hand side $[T, X, Z]$, $t = T/Z$, $x = X/Z$, we have

$$\begin{aligned}
&(Z^{19}b_0(T/Z, X/Z))^2 + (Z^{16}b_1(T/Z, X/Z))^2(Z^6 f_7(T/Z, X/Z))\\
&= 4Z^3(-4XZ^4r^2 + 4T^3Z^2r - 4T^2Z^3r + 2T^5 + T^4X - 4T^4Z - 6T^3XZ + 3T^2XZ^2\\
&+2T^2Z^3 + 2TXZ^3 + 4X^2Z^3 + XZ^4)^7\,.
\end{aligned}$$

Since we can choose r from a suitable Zariski open set of $\mathbb{C}$, $\mathcal{B}$ given by $-4Z^9 f_7(T/Z, X/Z) = 0$ satisfies infinitely many quasi-toric relations of type $(2,7,2)$ such that

$$\begin{aligned}
h_1 &= Z^{19}b_0(T/Z, X/Z)\,,\\
h_2 &= -4XZ^4r^2 + 4T^3Z^2r - 4T^2Z^3r + 2T^5 + T^4X - 4T^4Z - 6T^3XZ + 3T^2XZ^2\\
&\quad +2T^2Z^3 + 2TXZ^3 + 4X^2Z^3 + XZ^4\,,
\end{aligned}$$

$$h_3 = Z^{16} b_1(T/Z, X/Z)\,,$$
$$F_1 = 1, \quad F_2 = -4Z^3, \quad F_3 = Z^6 f_7(T/Z, X/Z)\,.$$

5. An explicit example for the case of $g = 2$

In this section, we will give an example of a plane curve satisfying infinitely many quasi-toric relations of type $(2, 3, 2)$ based on a hyperelliptic curve of genus 2 over $\mathbb{C}(t)$. Again our computation are argument based on Remark 4.2. Let us consider the hyperelliptic curve $\mathcal{C}$ of genus 2 given by $\mathcal{C} : y^2 = f(t, x)$, where

$$\begin{aligned} f(t,x) &= -(x^2 - x - t^2)^3 + (x^3 - t^3 - 1)^2 \\ &= 3x^5 + 3(t^2-1)x^4 - (2t^3 + 6t^2 + 1)x^3 + 3(-t^4 + t^2)x^2 + 3t^4 x + 2t^6 + 2t^3 + 1\,. \end{aligned}$$

In order to make the equation simple, we set the coefficient of x^5 in $f(t, x)$ is 3 and it produced no effect on our result for the existence of quasi-toric relations. Consider the h-reduced divisor $\mathfrak{d}_o$ given by

$$u_o = x^2 - x - t^2, \quad v_o = (x^3 - t^3 - 1)(\mathrm{mod} u_o) = (1 + t)x - t^3 + t^2 - 1\,.$$

By our our definition of $\mathcal{C}$, $\mathfrak{d}_o - 2O$ gives rise to a torsion of order 3 in $\mathrm{Pic}^0(\mathcal{C})$. In fact, by our argument as before, we see that $I(3\mathfrak{d}_o) = \langle [y - (x^3 - t^3 - 1)] \rangle$, i.e., $3(\mathfrak{d}_o - 2O) = \mathrm{div}([y - (x^3 - t^2 - 1)])$. Now for $r \in \mathbb{C}$, put

$$\begin{aligned} v_1 &:= r(x^2 - x - t^2) - v_o\,, \\ u_1 &:= \frac{1}{3}\frac{f - v_o^2}{u_o} \\ &= x^3 + \frac{3t^2 - r^2}{3}x^2 + \frac{(-2t^3 + 2rt^2 + r^2 + 2r - 1)}{3}x \\ &\quad -\frac{t^4}{3} - \frac{2}{3}(r+1)t^3 + \frac{1}{3}(r^2 + 2r + 1)t^2 - \frac{2}{3}r - \frac{2}{3}\,. \end{aligned}$$

Let $\mathfrak{d}_1$ be the divisor given by the Mumford representation (u_1, v_1). By Remark 2.7, the divisor $3\mathfrak{d}_1$ satisfies ♣ for general r as $\mathrm{r}(3\mathfrak{d}_1) = 0$. Now we apply our argument to $\widetilde{I(3\mathfrak{d}_1)}$. We see that a polynomial such that $g = (x^2 + \text{lower terms})y + \text{lower terms}$ and $[g] \neq 0$ is contained in $\mathcal{G}_2(\widetilde{I(3\mathfrak{d}_1)})$. As $\deg 3\mathfrak{d}_1 = 9$, we can choose g as $b_{3\mathfrak{d}_1}$. Then we have $3b_{3\mathfrak{d}_1} = b_0 + b_1 y$ where

$$\begin{aligned} b_0 &= (-9r - 9)x^4 + (-9t^2 r - r^3 - 9t^2 - 9r^2 - 9r)x^3 \\ &\quad + (6t^3 r - 6t^2 r^2 + 3t^3 + 9t^2 + 3r^2 + 12r + 6)x^2 \\ &\quad + (-3t^5 + 6t^4 r + 3t^3 r^2 + 9t^4 + 3t^3 r + 6t^2 r^2 + 12t^2 r + 3t^2 + 3r^2 + 3r)x \\ &\quad + 3t^6 - 3t^5 r + 3t^4 r^2 + t^3 r^3 - 3t^5 + 6t^4 r + 3t^3 r^2 \\ &\quad + 3t^4 + 3t^3 r + 5t^3 - 3t^2 r + r^3 - 3t^2 + 3r^2 + 3r + 3\,, \\ b_1 &= 3x^2 + (3t^2 + 3r^2 + 9r + 6)x + (-2t^3 + 3t^2 r + r^3 + 3t^2 + 3r^2 + 3r - 1)\,. \end{aligned}$$

and $b_0^2 - b_1^2 f = -(3u_1)^3$. Put $h_1 = Z^6 b_0(T/Z, X/Z)$, $h_2 = Z^4 u_1(T/Z, X/Z)$, $h_3 = Z^3 b_1(T/Z, X/Z)$, $F_1 = 1$, $F_2 = 1$ and $F_3 = Z^6 f(T/Z, X/Z)$. Then the curve $\mathcal{B}_o$ given

by $F_2 = 0$ satisfies infinitely many quasi-toric relations as we can choose r from a suitable Zariski open set of $\mathbb{C}$.

References

[1] S. Arita: *An addition algorithm in Jacobian of C_{ab} curves*, Discrete Appl. Math. **130** (2003), 13–31

[2] D.G. Cantor: *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **48** (1987), 95–101.

[3] J.-I. Cogolludo-Agustín and A. Libgober: *Mordell-Weil groups of elliptic threefolds and the Alexander module of plane curves*, J. Reine Angew. Math., **697**(2014), 15–55.

[4] C. Costello and K. Lauter: *Group law computations on Jacobians of hyperelliptic curves* Selected areas in cryptography, Lecture Notes in Comput. Sci., **7118** (2012), 92–17 .

[5] D. Cox, J. Little and D. O'Shea: Ideals, Varieties and Algorithms 4th Edition, Undergraduate Text in Math., Springer-Verlag (2015) .

[6] D. Cox and W. Parry: *Torsion in elliptic curves over $k(t)$*, Compositio Math. **41** (1980), 337–354.

[7] S. Galbraith: Mathematics of Public Key Cryptography, Cambridge Univ. Press. 2012. webpage: https://www.math.auckland.ac.nz/ sgal018/crypto-book/crypto-book.html

[8] S. Iitaka: Algebraic Geometry, Graduate Texts in Math. **76**, Springer-Verlag 1982.

[9] R. Kloosterman: *Mordell-Weil lattices and toric decompositions of plane curves*, Math. Ann. 367 (2017), 755–783.

[10] R. Kloosterman: *Determining all (2,3)-torus structures of a symmetric plane curve*, Ark. Mat. 56 (2018), 341–349.

[11] R. Kloosterman: *Curves with rational families of quasi-toric relations*, arXiv:2104.14219.

[12] K. Lauter: *The equivalence of the geometric and algebraic group laws for Jacobians of genus 2 curves*, Topics in algebraic and noncommutative geometry, Contemp. Math., 324, Amer. Math. Soc. (2003), 165–171.

[13] F. Leitenberger: *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46** (2005), 125–130.

[14] A. J. Menezes, Y.-H. Wu and R.J. Zuccherato: *An elementary introduciton to hyperelliptic curves*, in "N. Koblitz: Algebraic Aspects of Cryptography," Springer-Verlag, Berlin, (1998), 157–178.

[15] D. Mumford: Tata lectures on theta. II. Jacobian theta functions and differential equations. With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura. Progress in Mathematics, **43**. Birkäuser Boston, Inc., Boston, MA, 1984.

[16] A. Takahashi and H. Tokunaga: *An explicit construction for n-contact curves to a smooth cubic via divisions and Zariski tuples*, to appear in Hokkaido Math. J., arXiv:2008.13467.

[17] V. Weispfenning: *Comprehensive Gröbner bases*, Journal of Symbolic Computation, **14** (1992), 1–29.

Ai TAKAHASHI
Department of Mathematics and Information Sciences,
Tokyo Metropolitan University, 1–1 Minami-Ohsawa,
Hachiohji 192–0397 JAPAN
Hiro-o TOKUNAGA
Department of Mathematical Sciences,
Graduate School of Science,
Tokyo Metropolitan University, 1–1 Minami-Ohsawa,
Hachiohji 192–0397 JAPAN
e-mail: tokunaga@tmu.ac.jp