An Algorithm for computing Weierstrass Points

F. Hess

Computer Science Department,
Woodland Road, University of Bristol, BS8 1UB, UK

Abstract. We develop algorithms for computing differentiations and Weierstrass points of algebraic curves in any characteristic. As an application we explain how this can be used to compute special models of curves together with a map to $\mathbb{P}^1$ of low degree.

1 Introduction

A Weierstrass point on a non-singular irreducible algebraic curve is a point P for which there exist functions on the curve with unusual pole orders at P and no poles everywhere else. The finite set of Weierstrass points forms an important invariant of a curve which is of particular use for the study of automorphisms. Using Weierstrass points it can for example be shown that the automorphism group of a curve is finite.

The theory of Weierstrass points over the base field $\mathbb{C}$ dates back to the 19th century. The generalization of the theory to base fields of any characteristic was carried out around 1935 in a series of works [4–6, 13, 14, 18], most notably by F. K. Schmidt. Over finite fields as base fields a variation of the theory yields a proof of the Riemann hypothesis for curves and several improvements on it [17].

In this paper we will focus on algorithmic aspects of the theory in arbitrary characteristic. Using the framework in [7] we describe algorithms for the computation of differentiations (alias higher derivatives) and Weierstrass places, speaking in terms of the function field of a given curve. As an application of these algorithms we devise an algorithm for computing special models of curves together with a map to $\mathbb{P}^1$ of low degree. In practice, using simplified instead of unwieldy models speeds up computations considerably. One among many examples for this is the integration of elliptic and hyperelliptic functions, see the discussion in [8]. The algorithms of this work have been implemented in Kash [11] and Magma [1, 2].

We also give a brief exposition of the main statements of the theory of Weierstrass points in arbitrary characteristic as in [6, 13–15, 17]. For the convenience of the reader we do provide proofs since the prior expositions are different or somewhat unaccessible.

2 Preliminaries

For the purpose of the paper we will focus on the function fields of curves rather than the curves themselves. By F/k we denote throughout an algebraic function

field of transcendence degree one over the exact constant field k. We refer to [16] for the theory of algebraic function fields. We assume further that F/k has a separating element and is conservative, i.e. its genus g is invariant under constant field extensions. There are further restrictions on k for the algorithms in [7] to work, but k perfect is a sufficient condition. By [7] we further assume that we have algorithms to compute in F/k as a field and $k(x)$-vector space for x a separating element, that we can compute with places, divisors and Riemann-Roch spaces $\mathcal{L}(D) = \{a \in F^\times \mid (a) + D \geq 0\} \cup \{0\}$ for divisors D. In addition we will need to compute with differentials in F/k. Implementations of such algorithms are available in Kash [11] and Magma [1, 2].

The algebraic closure of k is denoted by $\bar{k}$ and the conorm map from F/k to a constant field extension Fk_1/k_1 by $\mathrm{con}_{Fk_1/F}$. Also, $i(D)$ is the index of speciality of the divisor D.

3 Weierstrass Places

In this section we state the main definitions and theorems about Weierstrass places. More generally we will consider D-Weierstrass places for D a divisor, which occurred first in [12].

Definition 1 *Let D be a divisor and P a place of degree one of F/k. The number $\mu \in \mathbb{Z}^{\geq 1}$ is called D-gap number of P if $\mathcal{L}(D + (\mu - 1)P) = \mathcal{L}(D + \mu P)$ and it is called D-pole number of P if equality does not hold.*

In other words, an integer μ is a D-pole number of P precisely if there is an element $a \in F$ such that $v_{P'}(a) + v_{P'}(D) \geq 0$ for all places $P' \neq P$ and $v_P(a) + v_P(D) + \mu = 0$. Typically one thinks of $D = 0$ in which case D-gap and D-pole numbers are simply called gap and pole numbers respectively.

We remark that if μ is not a D-gap number then $\dim(D + (\mu - 1)P) = \dim(D + \mu P) - 1$ since $\deg(P) = 1$. Also, linearly equivalent divisors have the same gap numbers for every P.

Theorem 2 *All but finitely many places of degree one from constant field extensions Fk_1/k_1 have the same $\mathrm{con}_{Fk_1/F}(D)$-gap numbers.*

Proof. Follows from Corollary 19 and the remark after Algorithm 30.

Definition 3 *The D-gap numbers of F/k are defined to be the numbers common to almost all places in Theorem 2. A place of degree one of F/k is called D-Weierstrass place if its D-gap numbers are different from the D-gap numbers of F/k.*

One of the main tasks of this paper is to explain how to compute D-gap numbers and D-Weierstrass places of F/k.

Proposition 4 *Every D-gap number μ of P satisfies $1 \leq \mu \leq 2g - 1 - \deg(D)$. There are $i(D)$ many D-gap numbers of P.*

Proof. Follows from Proposition 12 and Proposition 13.

The usual Weierstrass places and gap numbers of F/k are the D-Weierstrass places and D-gap numbers for $D = 0$ the zero divisor. The numbers in $\mathbb{Z}^{\geq 1}$ which are not gap numbers at a place P are called pole numbers of P. They occur as pole orders of elements of F/k at P and form an additive semigroup, the so called Weierstrass semigroup at P.

Theorem 5 *There exists at least one Weierstrass place of $F\bar{k}/\bar{k}$ for $g \geq 2$. For $g \in \{0,1\}$ there are no Weierstrass places.*

Proof. Follows from Corollary 20 (the ramification divisor of F/k is zero if and only if $g \in \{0,1\}$).

4 Differentiations

Classically Weierstrass places are related with differential calculus and higher derivatives by the Wronskian determinant, to be explained in the next section. In positive characteristic p every j-th derivative $d^j a/dx^j$ for $a, x \in F$ and x separating vanishes identically for $j \geq p$, making them useless for forming the Wronskian determinant. Thus j-th derivatives have to be defined differently in positive characteristic, leading to differentiations. The rest of the section is however valid in any characteristic.

Definition 6 *Let S/R be an unitary extension of entire rings. A differentiation of R is a homomorphism $D : R \to S[[t]]$, $a \mapsto \sum_{i=0}^{\infty} D^{(i)}(a)t^i$ such that $D^{(0)}(a) = a$ for all $a \in R$. The differentiation D is called iterative if its image is contained in $R[[t]]$ and $D^{(i)} \circ D^{(j)} = \binom{i+j}{i} \cdot D^{(i+j)}$.*

We remark that $D^{(i)}$ will take over the role of an i-th derivative. Let $D : R \to R[[t]]$ be a differentiation. Upon identifying R with $D(R)$ we obtain a differentiation $D' : D(R) \to D(R)[[t']]$, $b \mapsto \sum_{j=0}^{\infty} D(D^{(j)}(D^{-1}(b)))t'^j$. On the other hand we get a differentiation $D_t : D(R) \to R[[t]][[t']]$ defined by $t \mapsto t + t'$. We have that D is iterative if and only if $D' = D_t$. Indeed, let $a \in R$ and $b = D(a) = \sum_{i=0}^{\infty} D^{(i)}(a)t^i$. Clearly $D'(b) = \sum_{j=0}^{\infty} t'^j \sum_{i=0}^{\infty} D^{(i)}(D^{(j)}(a))t^i$. On the other hand a straightforward calculation shows $D_t(b) = \sum_{j=0}^{\infty} t'^j \sum_{i=j}^{\infty} \binom{i}{j} D^{(i)}(a)t^{i-j}$. Substituting i by $i + j$ yields the equivalence. A trivial example of an iterative differentiation is $D(a) = a$, where every element in R can be regarded as an absolute differentiation constant.

Let S be a field. A differentiation of $D : R \to S[[t]]$ can be extended in precisely one way to the field of fractions $Q(R)$ of R because of $D^{(0)}(a) = a$. Let R be a field and $\alpha \in S$. Assume α is a root of the monic and separable polynomial $f \in R[x]$. Denote by $D(f) \in D(R)[x]$ the polynomial obtained from f by applying D coefficientwise. By Hensel's lemma, $D(f)$ has a unique root $\alpha' \in S[[t]]$ such that $\alpha' = \alpha \bmod t$. Hence there is precisely one extension of D to $R[\alpha]$, given by $\alpha \mapsto \alpha'$. In both cases, if D is iterative then its extension is also iterative.

To see this assume that $D : R \to R[[t]]$ is iterative and let $\hat{D}$ be the extension of D. The image of $\hat{D}$ is contained in $Q(R)[[t]]$ and $R[\alpha][[t]]$ respectively. Since D is iterative we have $D' = D_t$. But $\hat{D}'$ and $\hat{D}_t$ are extensions of D' and D_t respectively. Hence $\hat{D}' = \hat{D}_t$ because of the proven uniqueness properties, and $\hat{D}$ is iterative. If α is transcendental over R we can extend D in more than one way. The main example is to extend by $\alpha \mapsto \alpha + t$. Then $D^{(0)}(\alpha) = \alpha$, $D^{(1)}(\alpha) = 1$ and $D^{(j)}(\alpha) = 0$ for $j > 1$. Hence $D'(\alpha + t) = (\alpha + t) + t'$. But $D_t(\alpha + t) = \alpha + (t + t')$ so this extension is iterative if D on R is.

Definition 7 *A differentiation of a function field F/k is a differentiation of F such that $D(a) = a$ for all $a \in k$. The differentiation is called with respect to x and written D_x if $x \in F$ is a separating element and $D(x) = x + t$.*

Lemma 8 *For every separating element $x \in F$ there is exactly one differentiation D_x with respect to x. Furthermore, D_x is iterative and $D_x^{(1)} = d/dx$.*

Proof. The first statements follow from the above discussion, extending the trivial differentiation $D(a) = a$ from k to F via $x \mapsto x + t$. For the last we have $D_x^{(1)} = d/dx$ on $k[x]$ because of $x \mapsto x + t$. This is then also true on the separable extension $F/k(x)$ by the uniqueness of extending the derivation d/dx, since $D_x^{(1)}$ is also a derivation on F.

Lemma 9 *Let P be a place of degree one of F/k and $\pi \in F$ a local uniformizer at P. Let $\phi : F \longrightarrow k((\pi))$ be the homomorphism which maps elements of F to their P-adic expansions. Then $\phi(D_\pi^{(j)}(a)) = \sum_{i=i_0}^{\infty} \binom{i}{j} a_i \pi^{i-j}$ for $\phi(a) = \sum_{i=i_0}^{\infty} a_i \pi^i$ and $a \in F$.*

Proof. We obtain a differentiation on $k((\pi))$ by $\pi \mapsto \pi + t$ which restricts to a differentiation of F via the embedding ϕ and which extends the differentiation D_π on $k[\pi]$. Since π is separating, both differentiations must coincide. The result now follows from the binomial series of $(\pi + t)^j$.

By Lemma 8 and the iterativity property we have $D_x^{(j)} = j!^{-1} d^j/dx^j$ in characteristic zero. Lemma 9 also shows $D_\pi : \mathfrak{o}_P \to \mathfrak{o}_P[[t]]$ and that $\phi : \mathfrak{o}_P \to k[[\pi]]$ is obtained from following D_π by the coefficientwise reduction mod P and substituting π for t.

Consider the field of fractions $\widetilde{F}$ of the Dedekind domain $F \otimes_k F$. F has two embeddings $1 \otimes_k F$ and $F \otimes_k 1$ into $\widetilde{F}$. We write $F_* = 1 \otimes_k F$ and identify $F = F \otimes_k 1$. For $a = a' \otimes_k 1$ in F we denote the corresponding element $1 \otimes_k a'$ in F_* by a_*. Now $\widetilde{F}$ is a function field over the exact constant field F_* and the generic place P_F of F is the place of degree one of $\widetilde{F}/F_*$ whose residue class map restricted to F is given by $a \mapsto a_*$. The function field $\widetilde{F}/F_*$ is the constant field extension of F by F_* and P_F is equivalent to the generic point on a curve having F/k as a function field. Since P_F is of degree one we have an embedding $\widetilde{F} \longrightarrow F_*((t))$ where $t \in \widetilde{F}$ is a local uniformizer of P_F. We have that $x \in F$ is separating precisely if $x - x_*$ is a local uniformizer for P_F. The restriction of this embedding to F yields an embedding $\phi_t : F \longrightarrow F_*[[t]]$.

Theorem 10 *Upon identifying F and F_* we have $D_x = \phi_{x-x_*}$ for any separating element $x \in F$.*

Proof. Identifying F and F_* the map ϕ_{x-x_*} clearly defines a differentiation of F. Restricted to $k[x]$ it is given by $x \mapsto x_* + t$ since this expresses a polynomial in the local uniformizer $t = x - x_*$. On $k[x]$ it is hence equal to D_x. Since x is separating the equality of D_x and ϕ_{x-x_*} on F follows from the uniqueness of extensions of differentiations.

We can extend D_x to $\widetilde{F}$ by setting $D_x(a) = a$ for $a \in F_*$, or by F_*-linearity in other words. This equals the differentiation D_x obtained by x viewed as separating element of $\widetilde{F}$ and we also have $D_x = \phi_{x-x_*}$ on $\widetilde{F}$.

By Theorem 10 the change of separating element for a differentation has the effect of changing the local uniformizer. More precisely, let $x, y \in F$ be separating. Then $\phi_{y-y_*}(x - x_*) = D_y(x - x_*) = D_y(x) = dx/dy \cdot t + O(t^2)$ and this series has to be substituted for t in $D_x(a)$ in order to obtain $D_y(a)$ for $a \in F$. This discussion yields the usual chain rule for (higher) derivatives. The other familiar rules follow from the properties of a differentiation as in Definition 6 and 7.

5 Orders and Ramification Divisors of Linear Systems

Let L be a linear system of F/k. Recall that L is a set of effective divisors $\{ (a) + E \mid a \in V \backslash \{0\} \}$ for a divisor E and some k-linear subspace V of $\mathcal{L}(E)$. We say that L is defined by E and V. The complete linear system L defined by E is the linear system defined by E and $\mathcal{L}(E)$. If L is defined by E and V then it is clearly also defined by $E - (a)$ and aV for any $a \in F^\times$. Furthermore, for any $E \in L$ we have that L is defined by E and the k-linear space V generated by $\{ a \in F^\times \mid (a) = D - E \text{ for } D \in L \}$. So alternatively one can think of L as an equivalence class of tuples (E, V), where $(E, V) \sim (E - (a), aV)$.

In the following we write $\deg(L) := \deg(E)$ and $\dim(L) := \dim(V)$. Also, let $L(\mu P) := \{ D \in L \mid v_P(D) \geq \mu \}$ for $\mu \in \mathbb{Z}^{\geq 0}$.

Definition 11 *Let L be a linear system and P a place of degree one. The integer $\mu \in \mathbb{Z}^{\geq 0}$ is called (Wronskian) order of L at P if $L(\mu P) \neq L((\mu + 1)P)$.*

Any P for which 0 is not an order of L is called a base point of L. Let L be a linear system defined by E and V. We write $V(\mu P) := \{ a \in V \mid v_P(a) \geq \mu \}$. Then $V(\mu P) \neq V((\mu + 1)P)$ if and only if μ is an order of L.

Proposition 12 *Let L be the complete linear system defined by $W - D$. Then μ is a D-gap number of P if and only if $\mu - 1$ is an order of L at P.*

Proof. Abbreviate $V = \mathcal{L}(W - D)$. From the theorem of Riemann-Roch we obtain

$$\dim(D + (\mu - 1)P) - \dim(D + \mu P) = i(D + (\mu - 1)P) - i(D + \mu P) - 1,$$

so μ is a D-gap number if and only if $i(D+(\mu-1)P) > i(D+\mu P)$. We have $\dim V(\mu P) = i(D+\mu P)$, so this is equivalent to $V((\mu-1)P) \neq V(\mu P)$ and $\mu-1$ being an order of V at P.

According to Proposition 12, in order to compute gap numbers and Weierstrass places it suffices to investigate the orders of L at various places.

Proposition 13 *Every order μ of L at P satisfies $0 \leq \mu \leq \deg(L)$. There are $\dim(L)$ orders of L at P.*

Proof. Let L be defined by E and V such that $v_P(E) = 0$. Then $V(\mu P) \subseteq \mathcal{L}(E-\mu P)$. By definition, $\mu \geq 0$. Furthermore, for $\mu > \deg(L) = \deg(E)$ we have $\dim V(\mu P) \leq \dim(E-\mu P) = 0$ and hence $V(\mu P) = V((\mu+1)P) = 0$, so this μ is not an order. Thus $0 \leq \mu \leq \deg(L)$ for orders. In order to prove that there are $\dim(L) = \dim(V)$ orders we take $\phi : F \longrightarrow k((\pi))$ to be a P-adic expansion map. We have that k-linearly independent elements are mapped to k-linearly independent series. Using a Gaussian elimination process we see that there is a unique basis w_i of V such that $\phi(w_i) = \pi^{\mu_i} + O(\pi^{\mu_i+1})$ and $0 \leq \mu_1 < \cdots < \mu_{\dim(L)}$. Thus the μ_i are all $\dim(L)$ orders of L.

We now want to investigate the orders of L defined by E and V for almost all places simultaneously. For this we consider the linear system L as a linear system of $\tilde{F}$ via the conorm map and investigate it at the generic place P_F.

Definition 14 *The orders of L are defined to be the orders of L at P_F.*

Proposition 15 *Let L be defined by E and V and let $v_1, \ldots, v_n$ be a k-basis of V. Let x be a separating element of F/k. The orders of L are the lexicographically smallest integers $0 = \varepsilon_1 < \cdots < \varepsilon_n$ such that $\det(D_x^{(\varepsilon_i)}(v_j))_{i,j} \neq 0$. The following transformation properties hold: If $w_i = \sum_j \lambda_{i,j} v_j$ and $(\lambda_{i,j})_{i,j} \in k^{n\times n}$ then $\det(D_x^{(\varepsilon_i)}(w_j))_{i,j} = \det(\lambda_{i,j})_{i,j} \det(D_x^{(\varepsilon_i)}(v_j))_{i,j}$. Moreover $\det(D_x^{(\varepsilon_i)}(av_j))_{i,j} = a^n \det(D_x^{(\varepsilon_i)}(v_j))_{i,j}$ for $a \in F$. If y is separating variable then $\det(D_y^{(\varepsilon_i)}(v_j))_{i,j} = (dx/dy)^{\sum_i \varepsilon_i} \det(D_x^{(\varepsilon_i)}(v_j))_{i,j}$. We have $\varepsilon_i \leq \mu_i$ if $0 \leq \mu_1 < \cdots < \mu_n$ are integers such that $\det(D_x^{(\mu_i)}(v_j))_{i,j} \neq 0$, or if the μ_i are the orders of L at a place P.*

Proof. Using Theorem 10 and its notation we have $D_x = \phi_{x-x_*}$, so Proposition 15 is nothing else but a proposition about P_F-adic expansions. The first transformation property is clear by the F_*-linearity of ϕ_{x-x_*}. Analogous to the proof of Proposition 13 we can consider a basis w_i of $\sum_i F_* v_i$ of the form $\phi_{x-x_*}(w_i) = b_i t^{\varepsilon_i} + O(t^{\varepsilon_i+1})$ with some $b_i \in F_*^\times$, obtained by a transformation of determinant one. Clearly $\det(D_x^{(\varepsilon_i)}(v_j))_{i,j} = \det(D_x^{(\varepsilon_i)}(w_j))_{i,j} = \prod_i b_i$ and the lexicographical minimality of the ε_i and $\varepsilon_1 = 0$ follow immediately. Furthermore, multiplication by a and changing the local uniformizer are F_*-linear operations, so any two bases with equal determinant are mapped to bases with equal determinant by these operations. Because of $\phi(aw_i) = a_* b_i t^{\varepsilon_i} + O(t^{\varepsilon_i+1})$ for $a_* \in F_*$ and $\phi_{y-y_*}(w_i) = b_i (dx_*/dy_*)^{\varepsilon_i} t^{\varepsilon_i} + O(t^{\varepsilon_i+1})$ the two transformation statements

follow immediately. Finally, because of the construction, ε_r is the smallest index such that the span of the $(D_x^{(m)}(v_j))_j$ for $0 \leq m < \varepsilon_r$ has dimension $r-1$. This implies the first statement about the μ_i. For the second we may assume that $v_P(E) = 0$. But then $\det(D_x^{(\mu_i)}(v_j))_{i,j} \neq 0$ from the proof of Proposition 13.

Definition 16 *Let L be a linear system defined by E and V. Let $v_1, \ldots, v_n$ be a basis of V, x a separating element of F/k and $\varepsilon_1, \ldots, \varepsilon_n$ be the orders of L. The divisor $R(L) := (\det(D_x^{(\varepsilon_i)}(v_j))_{i,j}) + (\sum_i \varepsilon_i)(dx) + nE$ is called ramification divisor of L.*

By Proposition 15 the ramification divisor depends indeed only on L. The determinants in Proposition 15 are called Wronskian determinants.

Theorem 17 *Let L be a linear system, ε_i the orders of L and μ_i the orders of L at P. Then for the valuation $v_P(R(L)) \geq \sum_{i=1}^{\dim(L)} (\mu_i - \varepsilon_i)$ and equality holds if and only if $\det(\binom{\mu_i}{\varepsilon_j})_{i,j} \neq 0$ in k.*

Proof. [17] Let L be defined by E and V such that $v_P(E) = 0$. We take $\phi : F \longrightarrow k((\pi))$ to be a P-adic expansion map. Let w_i be a basis of V with $\phi(w_i) = \pi^{\mu_i} + O(\pi^{\mu_i+1})$. Using Lemma 9 we obtain

$$\begin{aligned}
\det\big(\phi(D_x^{(\varepsilon_i)}(w_j))\big)_{i,j} &= \det\Big(\binom{\mu_j}{\varepsilon_i}\pi^{\mu_j-\varepsilon_i} + O(\pi^{\mu_j-\varepsilon_i+1})\Big)_{i,j} \\
&= \det\Big(\binom{\mu_j}{\varepsilon_i}\pi^{\mu_j} + O(\pi^{\mu_j+1})\Big)_{i,j} \cdot \pi^{-\sum_i \varepsilon_i} \\
&= \det\Big(\binom{\mu_j}{\varepsilon_i}\Big)_{i,j} \cdot \pi^{\sum_i(\mu_i-\varepsilon_i)} + O(\pi^{1+\sum_i(\mu_i-\varepsilon_i)}).
\end{aligned}$$

Lemma 18 *If ε is an order of L and $\mu \in \mathbb{Z}^{\geq 0}$ such that $\binom{\varepsilon}{\mu} \neq 0$ in k then μ is also an order of L. In particular, if $p = 0$ or $p > \deg(L)$ then $0, \ldots, \dim(L)-1$ are the orders of L.*

Proof. [17] Let $\mu_1, \ldots, \mu_n$ be the orders of L at P and $\varepsilon_1, \ldots, \varepsilon_n$ the orders of L. If $0 \leq \nu_1 < \cdots < \nu_n$ are integers such that $\det(\binom{\mu_i}{\nu_j})_{i,j} \neq 0$ in k then $\varepsilon_i \leq \nu_i$ for $1 \leq i \leq n$. Indeed, as in the proof of Theorem 17, $\det(D_x^{(\nu_i)}(w_j))_{i,j} = \det(\binom{\mu_i}{\nu_j})_{i,j}\pi^{\sum_i(\mu_i-\nu_i)} + \cdots \neq 0$. The assertion now follows from Proposition 15.

Since $\binom{\varepsilon}{\mu} \neq 0$ we have $0 \leq \mu \leq \varepsilon$. Since $\mu = 0$ is an order we may assume $\mu > 0$. Let r be the largest integer such that $\varepsilon_r < \mu$. The matrix consisting of the rows $(\binom{\varepsilon_1}{\varepsilon_i}, \ldots, \binom{\varepsilon_r}{\varepsilon_i}, \binom{\varepsilon}{\varepsilon_i})$ for $1 \leq i \leq r$ and $(\binom{\varepsilon_1}{\mu}, \ldots, \binom{\varepsilon_r}{\mu}, \binom{\varepsilon}{\mu})$ is upper triangular and has determinant $\binom{\varepsilon}{\mu} \neq 0$ in k. By the first paragraph of the proof applied to a suitable linear subsystem of L we have $\varepsilon_{r+1} \leq \mu$ and hence $\mu = \varepsilon_{r+1}$ by the definition of r. The second statement follows from the first and Proposition 13.

We remark that $\binom{\varepsilon}{\mu} \neq 0 \bmod p$ if and only if $\mu \geq 0$ and the p-adic expansion of μ is coefficientwise less than or equal to the p-adic expansion of ε.

Corollary 19 *Let ε_i be the orders of L and μ_i the orders of L at P. The ramification divisor $R(L)$ is effective and of degree* $\deg(R(L)) = (2g-2)(\sum_{i=1}^{\dim(L)} \varepsilon_i) + \dim(L)\deg(L)$. *We have $\varepsilon_i \leq \mu_i$ and equality holds for all $1 \leq i \leq \dim(L)$ if and only if P is not in the support of $R(L)$.*

Corollary 20 *The D-Weierstrass places are precisely the places of degree one in the support of $R(L)$ where L is the complete linear system defined by $W - D$. The D-gap numbers of F/k are $\varepsilon_1 + 1, \ldots, \varepsilon_{\dim(L)} + 1$ for ε_i the orders of L.*

Proof. For Corollary 19 combine Theorem 17 and Proposition 15. For Corollary 20 combine Corollary 19 and Proposition 12.

The weight of a D-Weierstrass place P is defined to be $v_P(R(L))$. Also, $R(L)$ is called D-ramification divisor and, for $D = 0$, ramification divisor of F/k.

From the preceding discussion it is clear that the D-Weierstrass places are the places of degree one of F/k where the specialization of the generic place is not stable. The use of differentials is just the use of generic P_F-adic expansions.

6 Algorithms for Differentiations and Weierstrass Places

6.1 Differentiations

In characteristic zero we have $D_x^{(j)}(a) = j!^{-1} d^j a/dx^j$ for all $j \in \mathbb{Z}^{\geq 0}$. The computation of $D_x^{(j)}(a)$ can therefore be reduced to iteratively compute the derivation d/dx, which is easily achieved. In characteristic $p > 0$ however $D_x^{(j)}(a)$ cannot be computed in this way. Theorem 10 suggests that $D_x^{(j)}(a)$ be computed as the j-th coefficient of the P_F-adic expansion of a with respect to the local uniformizer $x - x_*$. For this there are well known techniques like Hensel or Newton lifting available. As it turns out we can do computations even more effectively, which will be described now.

Theorem 21 *Assume $p > 0$. Let $l, r, s \in \mathbb{Z}^{\geq 0}$ with $l \geq 1$, $s < p^l$ and let $a \in F$. There are unique $\lambda_i \in F$ such that $a = \sum_{i=0}^{p^l-1} \lambda_i^{p^l} x^i$ and for these we have*

$$D_x^{(rp^l+s)}(a) = \sum_{i=0}^{p^l-1} \binom{i}{s} D_x^{(r)}(\lambda_i)^{p^l} x^{i-s}. \tag{22}$$

Proof. The λ_i are obtained by representing a in the basis $1, x, \ldots, x^{p^l-1}$ of the F^{p^l}-vector space F. Next we note that $\binom{rp^l+s}{rp^l} = 1 \bmod p$. Indeed, if $s > 0$ then $\binom{rp^l+s-1}{rp^l-1} = 0 \bmod p$ since $rp^l + s$ is not divisible by p^l. Using the additivity of binomial coefficients we obtain $\binom{rp^l+s}{rp^l} = \binom{rp^l+s-1}{rp^l} \bmod p$. Hence we may assume $s = 0$. But then $\binom{rp^l}{rp^l} = 1$ and in conclusion $\binom{rp^l+s}{rp^l} = 1 \bmod p$, as claimed. Using the iterativity property we obtain

$$D_x^{(rp^l+s)} = D_x^{(rp^l)} \circ D_x^{(s)}. \tag{23}$$

From Definition 7 we have $D_x(x^j) = D_x(x)^j = (x+t)^j = \sum_{i=0}^{j} \binom{j}{i} x^{j-i} t^i$. This means $D_x^{(i)}(x^j) = \binom{j}{i} x^{j-i}$. Now let $b, c \in F$ be arbitrary. Again from the definition we see that $D_x(b^{p^l}) = D_x(b)^{p^l}$. Reading off coefficients yields $D_x^{(i)}(b^{p^l}) = 0$ for $i \neq 0 \bmod p^l$. Using $D_x(b^{p^l} c) = D_x(b^{p^l}) D_x(c)$ and $s < p^l$ we thus obtain $D_x^{(s)}(b^{p^l} c) = b^{p^l} D_x^{(s)}(c)$, and combining these observations gives

$$D_x^{(s)}(a) = \sum_{i=0}^{p^l-1} \binom{i}{s} \lambda_i^{p^l} x^{i-s}. \tag{24}$$

For $0 \leq j < p^l$ we have $D_x^{(rp^l)}(x^j) = 0$ and $D_x^{(rp^l)}(b^{p^l}) = D_x^{(r)}(b)^{p^l}$. Similarly as above this yields $D_x^{(rp^l)}(b^{p^l} x^j) = D_x^{(r)}(b)^{p^l} x^j$ and applying $D_x^{(rp^l)}$ to both sides of equation (24) proves equation (22).

In order to compute differentiations using Theorem 21 we need to find p-th power representations $a = \sum_i \lambda_i^p x^i$. One way of achieving this is to realize F as an inseparable extension of F^p of degree p. The following algorithm however gives an easy to implement alternative.

Algorithm 25 *(Power representation)*

Input: *A function field F/k with separating element x and $a \in F$.*
Output: *Elements $\lambda_i \in F$ such that $a = \sum_{i=0}^{p-1} \lambda_i^p x^i$*

1. *Set $a_0 := a$ and $a_j := j^{-1} da_{j-1}/dx$ for $1 \leq j < p$.*
2. *Set $b_{p-1} := a_{p-1}$. For $j = p-2, \ldots, 0$ set $b_j := a_j - \sum_{i=j+1}^{p-1} \binom{i}{j} b_i x^{i-j}$.*
3. *Return $\lambda_i := b_i^{1/p}$ for $0 \leq i < p$.*

Proof. We have $a_j = D_x^{(j)}(a)$ for $0 \leq j < p$ and $D_x^{(j)}(a) = \sum_{i=j}^{p-1} \binom{i}{j} \lambda_i^p x^{i-j}$. This shows that the algorithm indeed computes the λ_i.

Algorithm 26 *(Differentiations I)*

Input: *A function field F/k with separating element x, an integer $j \geq 0$ and an element $a \in F$.*
Output: *The differentiation $D_x^{(j)}(a)$.*

1. *If $j = 0$ then return a.*
2. *Write $j = rp + s$ with $r, s \in \mathbb{Z}^{\geq 0}$ and $s < p$.*
3. *Compute $e := D_x^{(s)}(a) = (s!)^{-1} d^s a/dx^s$.*
4. *If $r = 0$ then return e.*
5. *Write $e = \sum_{i=0}^{p-1} \lambda_i^p x^i$ using algorithm 25.*
6. *Compute $\mu_i := D_x^{(r)}(\lambda_i)$ using Algorithm 26 recursively.*
7. *Return $\sum_{i=0}^{p-1} \mu_i^p x^i$.*

Proof. The correctness of the algorithm follows from Theorem 21, equation (24).

We could use equation (22) directly in Algorithm 26. However, it is more effective to apply step 3 first since in the p-th power representation computation afterwards more of the λ_i will be zero.

Algorithm 26 can be improved in two ways. Firstly, suppose we want to compute the first n differentiations of an element. Applying Algorithm 26 for these values takes $O(n^2)$ derivation computations d/dx altogether. We can however obtain an iterative version using only $O(n\lceil\log_p(n)\rceil)$ derivation computations d/dx as follows. Let $a = \sum_{i=0}^{p-1} \lambda_i^p x^i$ and assume that we have computed $D_x^{(rp+s)}(a)$. If $s < p-1$ we compute $D_x^{(rp+s+1)}(a) = (s+1)^{-1} d(D_x^{(rp+s)}(a))/dx$. If $s = p-1$ we compute $D_x^{(rp+s+1)}(a) = D_x^{((r+1)p)}(a) = \sum_{i=0}^{p-1} D_x^{(r+1)}(\lambda_i)^p x^i$ applying this strategy recursively to the values $D_x^{(r)}(\lambda_i)$ (which have to be stored). In the following let N denote a function on the symbols a, s, b, L which is thought of as a set of symbol-value pairs. The subscript i on a tuple denotes the i-th entry.

Algorithm 27 *(Recursion)*

Input: *The function N.*
Output: *The changed function N.*

1. *If $N(s) < p-1$ then compute $N(s) := N(s)+1$, $N(b) := N(s)^{-1} dN(b)/dx$ and return N. Terminate.*
2. *If $N(L)$ is undefined then compute $N(a) = \sum_{i=0}^{p-1} \lambda_i^p x^i$ using Algorithm 25 and define $N(L) := (\,\{\,(a,\lambda_i),(s,0),(b,\lambda_i)\,\} \mid 0 \le i \le p-1\,)$.*
3. *Set $N(s) := 0$ and compute $N(L) := (\,Recursion(N(L)_i) \mid 0 \le i \le p-1\,)$, $N(b) := \sum_{i=0}^{p-1} (N(L)_i(b))^p x^i$.*
4. *Return N.*

Algorithm 28 *(Differentiations II)*

Input: *The function field F/k with separating element x and an $a \in F$.*
Output: *The differentiations $D_x^{(0)}(a), D_x^{(1)}(a), \ldots$.*

1. *Set $N := \{\,(a,a),(s,0),(b,a)\,\}$.*
2. *Repeat returning $N(b)$ and redefining $N := Recursion(N)$.*

Proof. The validity of the algorithm follows from the above considerations. For the running time statement we observe that computing $D_x^{(j_0)}(a), \ldots, D_x^{(j_0+p^j)}(a)$ for $j_0 + p^j < p^{j+1}$ takes $\le (j+1)p^j$ derivation computations. This is clearly true for $j = 0$. Computing p times p^j successive differentiations costs $\le p(j+1)p^j + pp^j = (j+2)p^{j+1}$ derivation computations so the assertion follows by induction.

We remark that the number of elements to be stored in Algorithm 26 and 28 is $O(n)$ as opposed to $O(1)$ in characteristic zero.

For the second improvement we observe that the differentiations have (depending on the representation of F/k) certain denominators which can be estimated. Dealing with numerators and denominators separately can save expensive element inversions and gcd computations. To be more explicit, let $F = k(x,y)$ with $f(x,y) = 0$ and $f \in k[x,z]$ irreducible, monic and separable in the second variable z. We denote the derivative of f with respect to y by $f'(x,y)$.

Proposition 29 *We have* $b^{j+1} f'(x,y)^{2j-1} D_x^{(j)}(a/b) \in k[x,y]$ *for* $a, b \in k[x,y]$ *with* $b \neq 0$ *and* $j \geq 1$.

Proof. The $D_x^{(j)}(a)$ are the coefficients of the P_F-adic expansion of $a \in \widetilde{F}$ with respect to the prime element $x - x_*$. The proof follows by investigating the denominators which arise in an univariate Newton lifting. We leave the details to the reader.

If F/k is represented as the field of fractions of the coordinate ring of a non-plane affine curve, multivariate Newton lifting has to be used instead so that $f'(x,y)$ is replaced by the Jacobian determinant in an appropriate manner.

6.2 Weierstrass Places

The algorithm for computing Weierstrass places is now fairly straightforward by the previous discussion.

Algorithm 30 *(Weierstrass places)*

Input: *A function field F/k with separating element x and a divisor D.*
Output: *The D-gap numbers and D-Weierstrass places.*

1. *Compute the canonical divisor $W := (dx)$.*
2. *If $\dim(W - D) = 0$ then the ramification divisor of the complete linear system defined by $W - D$ is zero and there are no D-gap numbers and D-Weierstrass places. Terminate.*
3. *Compute a basis $v_1, \ldots, v_n$ of $\mathcal{L}(W - D)$.*
4. *Set $\varepsilon_1 := 0$, $M := (v_1, \ldots, v_n)$, $i := 1$, $\varepsilon := 0$ and $G := \{\}$.*
5. *Let $i := i + 1$. If $i > n$ then go to step 8.*
6. *Let $\varepsilon := \varepsilon + 1$. If $\binom{\varepsilon}{g} \neq 0$ in k for some $g \in G$ then $G := G \cup \{\varepsilon\}$ and repeat step 6.*
7. *Let $M' \in F^{i \times n}$ be the matrix obtained by appending $(D_x^{(\varepsilon)}(v_1), \ldots, D_x^{(\varepsilon)}(v_n))$ to M. If $\operatorname{rank} M' > \operatorname{rank} M$ then $M := M'$, $\varepsilon_i := \varepsilon$ and go to step 5. Otherwise let $G := G \cup \{\varepsilon\}$ and go to step 6.*
8. *Compute the ramification divisor $R := (\det(M)) + (\sum_{i=1}^{n} \varepsilon)(dx) + n(W - D)$ of the complete linear system defined by $W - D$.*
9. *Return $\varepsilon_1 + 1, \ldots, \varepsilon_n + 1$ and the degree one places in the support of R.*

Proof. The algorithm is correct by Corollary 20, Lemma 18 and Proposition 4.

The most expensive part of Algorithm 30 is the computation of the orders and the Wronskian determinant. The differentiations are best computed using Algorithm 28. In order to check that the rank has increased it is convenient to work with an echelonized version of M instead, in order to save subsequent echelonization work. Additionally, the denominators of the differentiations as in Proposition 29 can be treated separately in the linear algebra.

Let $F' = Fk_1$ be the constant field extension of F by k_1 and $\operatorname{con}_{F'/F}$ the conorm map from F to F'. Since D_x is extended by k_1-linearity to F' we have

$R(\mathrm{con}_{F'/F}(L)) = \mathrm{con}_{F'/F}(R(L))$. We can thus compute $\mathrm{con}_{F'/F}(D)$-Weierstrass places over the larger constant field k_1 without really having to work in k_1. If for example k_1 is the algebraic closure of k then any place P in the support of $R(L)$, L the complete linear system defined by $W - D$, gives rise to $\deg(P)$ many Galois conjugate D-Weierstrass places defined over the splitting field of the residue class field of P. This results in a very effective way of computing Weierstrass places and their fields of definition without extending the constant field.

Finally we remark that Algorithm 30 can clearly also be used to compute ramification divisors and orders of arbitrary linear systems.

7 Special Models of Algebraic Curves

As an application we describe in this section how the preceding sections may be used to compute a special model of the curve such that projection onto one of the variables gives a map to $\mathbb{P}^1$ of low degree. Equivalently, given a function field with some generators, try to find other generators such that one of them generates a rational subfield of small index, and return the equations they satisfy.

More specifically, assume P is a place of degree one of the function field F/k. For the first pole number r of P we have in general $r \leq g+1$. However, if P is a Weierstrass place we may hope that r is considerably smaller than $g+1$. For a hyperelliptic function field we would for example have $r = 2$ while in general we cannot expect to be better than roughly $r = g/2$. Now, if we are given $x \in F$ such that its pole divisor satisfies $(x)_\infty = rP$ we know $[F : k(x)] = r$ and thus have a rational subfield of small index. The strategy is to use such places in the following algorithm. Note that in order to obtain a Weierstrass place of degree one it might be necessary to work with a constant field extension.

Algorithm 31 *(Special model)*

Input: *A function field F/k with separating element a_1 and generators a_i such that $F = k(a_1)[a_2, \ldots, a_n]$. A place P of degree one.*

Output: *Return a separating element b_1 and generators $b_2, \ldots, b_r$ such that $F = k(b_1)[b_2, \ldots, b_r]$, together with a non-singular affine model given by the algebraic relations between the b_i. The b_i are expressed in the a_i. The number r is the first pole number of P.*

1. *Compute the first pole number r of P together with an element $b_1 \in F$ such that $(b_1)_\infty = rP$.*
2. *Let $i := 1$ and $d_1 := 0$.*
3. *If $i = r$ goto step 5. Otherwise let $i := i + 1$.*
4. *Compute the smallest pole number d_i of P such that $d_i \neq d_j \bmod r$ for $1 \leq j < i$. Compute an element $b_i \in F$ such that $(b_i)_\infty = d_i P$. Goto step 3.*
5. *Using linear algebra over k compute $\lambda_{i,j,\nu} \in k[b_1]$ with $\deg(\lambda_{i,j,\nu}) \leq (d_i + d_j - d_\nu)/r$ such that $\lambda_{i,j,1} + \sum_{\nu=2}^{r} \lambda_{i,j,\nu} b_\nu = b_i b_j$ for $2 \leq i, j \leq r$.*
6. *Return the b_i and the equations computed in the previous step.*

Proof. See also [7, Section 7]. Considering the degree function $\deg = -v_P$ and using a Gröbner reduction (or saturation) argument one can easily see that the b_i exist and that $1, b_2, \ldots, b_r$ forms a $k[b_1]$-basis of the integral closure $\mathrm{Cl}(k[b_1], F)$. Thus $b_i b_j$ can be expressed as a $k[b_1]$-linear combination of the basis, and these equations give a full description of $\mathrm{Cl}(k[b_1], F)$. The degree bound for the $\lambda_{i,j,\nu}$ follows because there is no degree cancellation possible since $d_i \neq d_j \bmod r$.

If we additionally apply the inversion algorithm given below we may skip step 5 and obtain the model from the inversion algorithm.

Remark 32 *Homogenizing this affine model yields a non-singular weighted projective model if b_1 and the homogenizing variable are counted with weight 1 and b_i with weight $\lceil d_i/r \rceil$ for $2 \leq i \leq r$. Also, one can show $\lceil d_i/r \rceil \leq \lceil (2g-1)/r \rceil + 1$ which gives the bound $2\lceil (2g-1)/r \rceil + 2$ for the degrees of the models. We further note that r and the d_i are not in general a minimal set of generators of the Weierstrass semigroup at P. Accordingly, there can be relations of the form $b_j = \prod_{i=1}^{j-1} b_i^{m_i}$ with $m_i \in \mathbb{Z}^{\geq 0}$ leading to the elimination of variables from the model. Further improvements in this direction are possible.*

For $g = 0$ one could ask whether the function field F/k is rational. There are no Weierstrass places available but the canonical class contains a divisor W of degree -2. Then $\dim(-W) = 3$ and $D := (a) - W$ for non constant $a \in \mathcal{L}(-W) \backslash k$ is an effective divisor of degree 2. There is hence a place P of degree one or two in D which we can compute. After a possible quadratic constant field extension by the residue class field of P we can assume $\deg(P) = 1$. Then for $x \in \mathcal{L}(P) \backslash k$ we have $F = k(x)$. If we want to avoid a constant field extension when $\deg(P) = 2$ we can compute a conic as the algebraic relation between the two non constant elements in $\mathcal{L}(P)$. On the conic we could then try to find a rational point [3]. For a further discussion see [9].

For $g = 1$ one could ask whether the function field F/k is elliptic. Again, there are no Weierstrass places available but if we are given a place of degree one, Algorithm 31 can be applied to obtain a Weierstrass model (the trace term should additionally be eliminated in characteristic $\neq 2$). For a further discussion see [8].

For $g \geq 2$ one could ask whether the function field F/k is hyperelliptic. In this case there exist Weierstrass places which can be used as input for Algorithm 31 to obtain a hyperelliptic model, after a possible constant field extension. However, there is a generally better method available which is able to work with any place of degree one, see [10].

Inversion

Algorithm 31 represents the b_i in the generators a_i of the function field. It is desirable to also have expressions for the generators a_i in terms of the b_i. We consider the following general problem: Let $k(a_1)[a_2, \ldots, a_n]$ and $k(b_1)[b_2, \ldots, b_m]$ be two representations of the same function field F/k with a_1 and b_1 separating. Assume $k(a_1)[a_2, \ldots, a_n] = k(a_1)[x_2, \ldots, x_n]/I$ for some prime ideal I of dimension

zero and $b_i = f_i(a_2, \ldots, a_n)$ with $f_i \in k(a_1)[x_2, \ldots, x_n]$. The problem is to compute J with $k(b_1)[b_2, \ldots, b_m] = k(b_1)[y_2, \ldots, y_m]/J$, and $g_j \in k(b_1)[y_2, \ldots, y_m]$ such that $a_j = g_j(b_2, \ldots, b_m)$. In other words, the problem is to compute the algebraic relations between the other generators and invert the isomorphism given by the expression of the b_i in the a_j. To achieve this let T_a be the ideal of $k(a_1)[x_2, \ldots, x_n, y_1, \ldots, y_m]$ generated by I and $y_i - f_i(x_2, \ldots, x_n)$ for $1 \leq i \leq m$. We have that T_a is a prime ideal because of the linearity of the added expressions and since I is prime. Furthermore, a Gröbner basis of T_a consists of a Gröbner basis of I together with the elements $y_i - f_i(x_2, \ldots, x_n)$ for $1 \leq i \leq m$. The elimination ideal $T_a \cap k(a_1)[y_1]$ is then also prime and contains a monic irreducible generator m_a. Clearly m_a is the minimal polynomial of b_1 over $k(a_1)$. By substituting b_1 for y_1 in T_a we obtain a prime ideal T'_a such that $k(a_1)[b_1][x_2, \ldots, x_n, y_2, \ldots, y_m]/T'_a \cong F$. From m_a we obtain the minimal polynomial m_b of a_1 over $k(b_1)$ and $k(a_1)[b_1] \cong k(b_1)[a_1]$. According to this isomorphism we can rewrite T'_a into T'_b such that $k(b_1)[a_1][x_2, \ldots, x_n, y_2, \ldots, y_m]/T'_b \cong F$. Reversing the above construction symmetrically we first obtain T_b by substituting x_1 for a_1 and then $J = k(b_1)[y_2, \ldots, y_m] \cap T_b$. Furthermore, finding the normal forms of the variables x_i for $1 \leq i \leq n$ mod T'_b with respect to the lexicographical term order gives the g_i. The above intersections and the last reduction step can be carried out by Gröbner basis computations.

8 Examples

8.1 Weierstrass Places

We consider the function field F/k defined by $y^7 + y = x^4$ over $\mathbb{F}_{49}$. Its genus is 9 and it has 176 places of degree one, the maximal number possible for this finite field and genus. Using the algorithms in section 6 we compute the following data. The gap numbers of F/k are $1, 2, 3, 4, 5, 8, 9, 10, 15$. All 176 places of degree one are Weierstrass places. There are 8 Weierstrass places of weight 9 with gap numbers $1, 2, 3, 5, 6, 9, 10, 13, 17$ and 168 Weierstrass places of weight 5 with gap numbers $1, 2, 3, 4, 5, 9, 10, 11, 17$. The ramification divisor has degree 912. The whole computation takes about 30s on a 600MHz computer, using Magma [1, 2].

8.2 Special Models

We consider the function field F/k defined by $y^{10} + 4y^7 + xy^6 + (4x^5 + x^2)y^5 + 3x^5y^2 + 2x^6y + 4x^{10} + x^7 = 0$ over $\mathbb{F}_5$. Its genus is 6 and the ramification divisor contains four places of degree 1 and weights $1, 10, 11, 13$, two places of degree 2 and weights $1, 13$, one place of degree 3 and weight 1, and 14 places of degree 6 and weights $1, \ldots, 1, 11$. In Algorithm 31 we take the Weierstrass place of degree 1 and weight 10 which has 3 as its first pole number. We obtain the affine model with Gröbner basis $x^7 - yz + 1, y^2 - z$, hence the plane model $y^3 = x^7 + 1$. We further obtain $b_1 = a_1/(2a_1 + a_2)$ and $b_2 = 2a_1 + a_2$, and for the inverse representation $a_1 = b_1/(b_1^7 + 1)b_2^4$ and $a_2 = (3b_1 + 1)/(b_1^7 + 1)b_2^4$. The internal integral basis computation takes about $2.6s$. The ramification divisor is then

computed and factorized in about 10s. The rest of the computation takes a further 3s, again on a 600MHz computer using Magma [1, 2].

9 Acknowledgements

I would like to thank H. Stichtenoth for suggesting that the computation of Weierstrass places be an interesting problem. I also thank M. van Hoeij for valuable comments on how to compute hyperelliptic models of curves. This work was supported by NaFöG and EPSRC grants and a stay with the Magma group.

References

1. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comp.*, 24, 3/4:235–265, 1997.
2. Comp. algebra group. Magma. `http://www.maths.usyd.edu.au:8000/u/magma/`, 2001.
3. J. E. Cremona and D. Rusin. Efficient solution of rational conics. Preprint available under `http://www.maths.nott.ac.uk/personal/jec/conics.ps.gz`, 2002.
4. H. Hasse. Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenem Konstantenkörper. *J. Reine angew. Math.*, 172:55–64, 1934.
5. H. Hasse. Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik. *J. Reine angew. Math.*, 175:50–54, 1936.
6. H. Hasse and F. K. Schmidt. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. *J. Reine angew. Math.*, 177:215–237, 1937.
7. F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comp.*, 33(4):425–445, 2002.
8. M. van Hoeij. An algorithm for computing the Weierstrass normal form. In A. H. M. Levelt, editor, *Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC '95*, pages 90–95, Montreal, Canada, 1995. ACM Press, New York.
9. M. van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comp.*, 23, 2-3:209–227, 1997.
10. M. van Hoeij. An algorithm for computing the Weierstrass normal form of hyperelliptic curves. Preprint available under `http://arXiv.org/`, 2002.
11. Kant group. Kash. `http://www.math.tu-berlin.de/~kant`, 2001.
12. H. Matzat. *Ein Vortrag über Weierstraß Punkte.* Universität Karlsruhe, 1975.
13. F. K. Schmidt. Die Wronskische Determinante in beliebigen differenzierbaren Funktionenkörpern. *Math. Z.*, 45:62–74, 1939.
14. F. K. Schmidt. Zur arithmetischen Theorie der algebraischen Funktionen. II: Allgemeine Theorie der Weierstraßpunkte. *Math. Z.*, 45:75–96, 1939.
15. H. Stichtenoth. *Algebraische Funktionenkörper einer Variablen.* Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, 1978.
16. H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin-Heidelberg-New York, 1993.
17. K.-O. Stöhr and J. F. Voloch. Weierstrass points and curves over finite fields. *Proc. London Math. Soc. (3)*, 52(1):1–19, 1986.
18. O. Teichmüller. Differentialrechnung bei Charakteristik p. *J. Reine angew. Math.*, 175:89–99, 1936.