Errata

After now a year has passed since I submitted my Habilitation thesis "On arithmetic and the discrete logarithm problem in class groups of curves", I realized some mistakes and inaccuracies. Two of the mistakes are quite important, and in fact a particular statement in the work is incorrect. The other mistakes and inaccuracies are relatively minor. I now first discuss the two important mistakes.

1. Lemma 2.109 and more generally the first item of Remark 2.106 are incorrect. It is not true that reductions along a divisor of degree 1 are always unique. Here is a counterexample:

   Let $\mathcal{C}/k$ be a hyperelliptic curve with a k-rational point P which is not a Weierstraß point. Let $\tilde{D} := P + \iota(P)$ and let $D_0 := 2\,\iota(P) - P$, where ι is the hyperelliptic involution. Then $\tilde{D} - D_0 = 2P - \iota(P)$, which is not linearly equivalent to a point. Thus $\tilde{D}$ is reduced along D_0, but $|\tilde{D}|$ has dimension 1.

   The statements hold however if the divisor D_0 is effective. In particular, reductions along a k-rational point are always unique.

   I remark that the incorrect statements mentioned here are not used in the index calculus algorithms in Chapter 3.

2. In order to prove Theorem 2, I wanted to apply Proposition 3.32 with $C := \frac{1}{2g_0}(1 - \frac{1}{g_0}) \cdot \frac{\log(\sqrt{2}-1)}{\log(\sqrt{2})}$ (see page 154). However, this number is negative as $\sqrt{2} - 1 < 1$. In fact, the Hasse-Weil bound does not give a non-trivial lower bound on $\#\,\mathrm{Cl}^0(\mathcal{C})$ for $q = 2, 3, 4$.

   However, in Lachaud, Martin-Deschamps: Nombre de points de jacobiennes sur un corps fini (Acta. Arith. **56**, 1990, pp. 329-340) the following lower bound on $\#\,\mathrm{Cl}^0(\mathcal{C})$ is proven:

   $$\#\,\mathrm{Cl}^0(\mathcal{C}) \geq \frac{(q-1)^2}{(q+1)\cdot q} \cdot \frac{1}{g+1} \cdot q^g$$

   By this bound, we have $\#\,\mathrm{Cl}^0(\mathcal{C}) \in \tilde{\mathcal{O}}(q^g)$ for all curves $\mathcal{C}/\mathbb{F}_q$. With this result, Theorem 3 immediately implies Theorem 2.

   Additionally, the result from [Heß05] cited on page viii also holds if the expected running time is expressed in terms of $\#\,\mathrm{Cl}^0(\mathcal{C})$ instead of q^g.

In addition to these mistakes, I have found some relatively minor inaccuracies which I list now in the order of occurrence.

- Page xi, line 4: Replace "[Sem98]" by "[Sem04]".
- Page 100, line 5 of the proof of Lemma 2.108: Replace "then so is every divisor" by "then so is every effective divisor".
- Page 122, Step 5 of the algorithm: Replace $[\gamma]_\ell$ by $[\underline{\gamma}]_\ell$.
- Page 131, line -11: Replace "*superpolynomial* in the cardinality of the ground field" by "*superpolynomial* in the input length".
- Page 133, Proposition 3.16: Replace the first four sentences by: "Let us fix some $g \geq 2$. Then there exists some algorithm such that the following holds: Upon input of a curve $\mathcal{C}/\mathbb{F}_q$ of genus g, elements $a, b \in \mathrm{Cl}^0(\mathcal{C})$ and a system $c_1, \ldots, c_u$ whose size is polynomially bounded in $\log(q)$, if the algorithm terminates, it outputs the discrete logarithm of b with respect to a. Moreover, if $c_1, \ldots, c_u$ is a generating system, the expected running time of the algorithm is in $\tilde{\mathcal{O}}(q^{2-2g})$."
- Page 133, Proposition 2.17 and Proposition 3.18: Insert after "a curve $\mathcal{C}/\mathbb{F}_q$": "of genus g".
- Page 137: Replace the "Procedure" by the following:

Procedure: Construction of the tree of large prime relations

Construct a labeled rooted tree T with vertex set contained in $\mathcal{L} \dot\cup \{*\}$ as follows:
Let T consist only of the root $*$, labeled with 0.
Let $N_{\max} \longleftarrow \lceil q^{1-1/g+1/g^2} \rceil$.
Let $s \longleftarrow 1$.
Repeat
    Repeat
        Choose $s_1, \ldots, s_u \in \mathbb{Z}/N\mathbb{Z}$ uniformly and independently at random.
        Compute the along P_0 reduced divisor D in free representation with $[D] - \deg(D) \cdot [P_0] = \sum_j s_j c_j$.
        If D splits as $D = \sum_j r_j F_j + Q$ with $Q \in \mathcal{L} - (\mathcal{F} \cup T)$,
            insert an edge from $*$ to Q into T, labeled with $(r_j)_j$ (in sparse representation).
        If D splits as $D = \sum_j r_j F_j + r_P P + Q$ with $P \in T_{s-1}, Q \in \mathcal{L} - (\mathcal{F} \cup T)$ and $r_P > 0$,

insert an edge from P to Q into T, labeled with $(r_j)_j$ and r_P.

In both cases label Q with s and the edge with $(r_j)_j$ (in sparse representation).

Until T contains $\min\{2^{s-1} \cdot \lceil q^{1-1/g} \rceil,\, N_{\max}\}$ edges.

If the number of edges equals $N_{\max}$, STOP.

Let $s \longleftarrow s+1$.

- Page 139, line 12: Replace "$[D - P_0]$" by "$[D - g \cdot P_0]$".
- Page 143, last paragraph: Replace "D_0" by "E" (twice) and "an divisor" by "a divisor".
- Page 146, line 12: Replace "uniformly randomly generated divisors" by "a uniformly randomly distributed divisor".
- Page 150, Step 2 in the algorithm for Lemma 3.27: Replace "For $i = 0, \ldots, \lceil \frac{n}{m} \rceil$" by "For $\ell = 0, \ldots, \lceil \frac{n}{m} \rceil$".
- Page 152, line -3: Replace "is is" by "is".
- Page 153, in the paragraph below Theorem 2. Replace "As in Proposition 2.117, the divisor classes are represented by an along D_0 reduced divisors, where the height of D_0 is polynomially bounded in d" by "As in Proposition 2.117, the divisor classes are represented by along D_0 reduced divisors, where D_0 has degree 1 and a height which is polynomially bounded in d".
- Page 156, line 20: Replace "$g^{\Omega(1)}$" by "$\frac{1}{g^{\Omega(1)}}$".
- Page 163, line -5: Replace "merely merely" by "merely".
- Page 167, Propositions 3.42 and 3.43: Perform changes analogously to the changes for Propositions 3.16 and 3.17 on page 133.
- Page 171: Perform changes in the "procedure" similarly to the changes in the "procedure" on page 137.
- Page 172: Replace lines 10-22 by the following:

  "We thus obtain: A tree of large prime relations of size $\lceil q^{1-\frac{1}{n}} \rceil$ is constructed in an expected time of $\tilde{O}(q^{2-\frac{2}{n}})$.

  Let us now assume that we are in Stage s with $s \geq 2$. We set

  $$M := \mathcal{F}^{n-2} \times (\mathcal{F} \cup T_{s-1}) \times (\mathcal{L} - T)\ .$$

  Now for q large enough (and independently of T, in particular independently of s) this set has cardinality $\geq (q^{1-\frac{1}{n}})^{n-2} \cdot 2^{s-2} \cdot q^{1-\frac{1}{n}} \cdot \frac{q}{4} =$

$2^{s-2} \cdot (q^{1-\frac{1}{n}})^{n-1} \cdot \frac{q}{4}$. For q large enough the probability that one try gives rise to a new edge is

$$\geq \frac{D}{16} \cdot 2^{s-2} \cdot q^{-(1-\frac{1}{n})} \ .$$

This implies that for q large enough (independently of s) the following holds: Given any tree T_{s-1} with $2^{s-2} \cdot \lceil q^{1-\frac{1}{n}} \rceil$ edges, the expected number of tries until a tree T with $\min\{2^{s-1} \cdot \lceil q^{1-\frac{1}{n}} \rceil, N_{\max}\}$ edges is constructed is

$$\leq \frac{32}{D} \cdot (q+1)^{2-\frac{2}{n}} \ .\text{"}$$

- Page 181, line 2 of Proposition 3.64: Replace "$n \cdot d^n$" by "$n! \cdot d^n$".
- Page 191, line 14: Replace "$\mathrm{Res}_k^K(A)$" by "$\mathrm{Res}_k^K(A')$".
- Page 193, line 19: Replace "is is" by "is".
- Page 217, line 16: Replace "in in" by "in".
- Page 228, line -1: Replace "[Gau04]" by "[Gau04b]".
- Page 229, line 4: Replace "Wie" by "Wir".

Leipzig, May 7 2009
Claus Diem