A Result on the Construction of Group Generators for the Class Group of Algebraic Function Fields

Hannes Grund
TU-Berlin, grund@math.tu-berlin.de
Neofonie GmbH, Hannes.Grund@neofonie.de

Introduction

We extend known constructions of generating sets for the class group of algebraic function fields - in particular, we generalize a result of D. Kohel and I. Shparlinski given for elliptic curves to the class group of function fields in general (see [SK]), which in turn improves the construction given in [HE] at least with respect to the size of the constructed set, given the size of the base field is large enough compared to some other data.
While it is known from computational group theory, that sampling a "sufficiently" large number of elements from a group yields a generating set with equally "sufficiently" high probability, one might ask for deterministic constructions producing a provable generating set for a concrete group. Similar questions where thoroughly studied in the context of finite fields, where one seeks for a generator or at least a generating set for multiplicative group of a given field.

Result

Let $F/\mathbf{F}_q$ be an algebraic function field over some finite field, of genus g_F. p its characteristic. Let the divisors of F being mapped to the zero class group $\mathcal{C}_F^0$ of F with respect to some fixed divisor, let F_d be the degree d constant field extension of F, the divisors of F_d being mapped to $\mathcal{C}_F^0$ by composing the latter mapping with the norm $N_{F_d/F}$ on divisors. Denote by $\mathbf{P_d}$ the degree one primes of F_d, define $N_d := |\mathbf{P}_d|$.
The result of [He], Theorem 34, essentially states that $\mathcal{C}_F^0$ is essentially generated by the norms of the primes in $\mathbf{P}_d$ provided d is sufficiently large - the required degree d may deduced by the estimates implied by the theorem of Hasse-Weil on certain character sums, i.e. any d fulfilling $N_d > (2g_F - 2)q^{d/2}$ forces the norms of the degree one primes of F_d to generate the class group. Since by Hasse-Weil, $\left|N_d - \left(q^d + 1\right)\right| \leq (2g_F - 2)\, q^{d/2}$, one obtains a generating set roughly of size q^d.
For what follows the basic idea is, most abstract spoken, having pinned down such a d to impose some further condition on the primes in $\mathbf{P}_d$, thus defining an possibly substantially smaller subset of these, yet generating $\mathcal{C}_F^0$, we adopt the idea found in [SK]:
For any d let $I_d \subseteq \mathbf{F}_{q^d}$ an "interval", i.e. choose an subgroup $B \subseteq \mathbf{F}_{q^d}^+$, some $\beta \in \mathbf{F}_d$ and numbers $0 \leq r \leq s < p$, define $I_d := \bigcup_{k=r\ldots s} (B + r\beta)$ - thus I_d is the union of some translations of B along a piece of line $r\beta, \ldots, s\beta$. Furthermore choose some $f \in F$, denote by S the poles of f, $N_S := |S|$, let f be such that $P \in S$ has degree one, and $v_P(f) \neq 0 \mod p$ for any $P \in S$, finally denote by S_d the degree one primes of F_d lying above those in S.
Define $D_f := (2g_F - 2 + N_S + \deg(f)_\infty)(1 + \log p)$. Now define

$$T(I_d) := \{\mathfrak{P} \in P_d \mid \mathfrak{P} \notin S_d, f(\mathfrak{P}) \in I_d\} \cup S_d \tag{1}$$

then we have the following:

Theorem 1 *For the size of $T(I_d)$ holds the following inequality*

$$\left||T(I_d)| - \left(\left(1 - \frac{|I_d|}{q^d}\right) N_S + \frac{|I_d|}{q^d} N_d\right)\right| \leq D_f q^{d/2} \tag{2}$$

and if d is such that $N_d - (2g_F - 2)q^{d/2} > 0$, then the norms of the primes in $T(I_d)$ generate the class group, permitted the following holds on the size of I_d:

$$\frac{|I_d|}{q^d} > \frac{2D_f q^{d/2}}{N_d - (2g_F - 2)\, q^{d/2}} \tag{3}$$

A few remarks: The conditions stated in theorem depend on the size of I_d only, for an interesting result one is led to keep the size of I_d small, whereby the size of $T(I_d)$ should be small. By the very definition any interval is of size Cp^l for some $C \leq p$ and l, which puts some mild restriction on the size of the interval.
Inspecting the right hand side of the second inequality in the theorem one sees that if the "gap" $N_d - (2g_F - 2)\, q^{d/2}$ is large the right hand side becomes small, permitting one to choose an small interval.
Now N_d is roughly of size q^d, hence the right hand size has order about $\approx q^{-d/2}$, finally yielding an lower bound on the size of the interval of about $\mathcal{O}\left(q^{d/2}\right)$. Suppose this bound can be attained by choosing an optimal interval size $|I_d| = Cp^l$ up to a negligible difference, then $|T(I_d)|$ is equally of size $\mathcal{O}\left(q^{d/2}\right)$, by the first stament given in the theorem, which is an improvement of about $q^{d/2}$ compared to the result of [HE]. Finally, the constants hidden in the "$\mathcal{O}$" being essentially D_f which depends on the characteristic, the genus and the poles of f. While these results hold true asymptotically, for concrete instances of curves the construction may fail to improve the result of [HE], Thereom 34, that may happen if the field size is "too small", with respect to the other data. (We give an example below)

Limitations

We give examples how the above bounds play out for concrete instances of curves:
Consider the curve $C : y^2 = x^7 - 1$ over the prime field $\mathbf{F}_{4194319}$, it has genus 3, one computes $N_1 = 4194320$, comparing with $(2g_F - 2)p^{1/2}$ shows that the that the class group is generated by the primes having degree 1. One is permitted to choose an interval I of size 400124, for the expected number of primes found in $T(I)$ the theorem predicts $200454 < |T(I)| < 599797$.
Consider the curve given by the same equation over the field $\mathbf{F}_{2053}$, the genus is 3 as well, one computes $N_1 = 2054$, the class group is already generated by the primes of degree one, but the lower bound on the size of the interval is larger than the field size.

References

[SK] D. Kohel, I. Shparlinski; On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields, Proc. Algorithmic Number Theory Symposium, Leiden, 2000, Lect. Notes in Comp. Sci., Springer-Verlag, Berlin, v.1838, 395-404.

[SGK] Igor Shparlinski, Joachim von zur Gathen, Marek Karpinski, Counting Curves and their Projections, Computational Complexity 6 (1997), 64-99

[He] F. Hess; Computing relations in divisor class groups of algebraic curves over finite fields; Submitted to J. Symbolic Comp.