CORR 99-23

Sharp upper bounds for arithmetics in hyperelliptic function fields

Andreas Stein

Abstract In this paper, we analyze and compare optimized arithmetics in hyperelliptic function fields. We present upper bounds on the number of operations in various situations. In most cases, these upper bounds can be derived without any heuristic assumption. The upper bounds are sharp and closely match our experimental results. They also coincide with the average case bounds in most of the cases. Since any hyperelliptic function field can be represented as a real quadratic function field, the real quadratic case is the more general case. We show that the group operation in imaginary quadratic function fields and the corresponding infrastructure operation in real quadratic function fields basically have the identical complexity. The additional operations caused by the distance function in the real case are negligible. The main advantage of the real case is the existence of an additional operation, namely the baby step operation. This operation is by a factor of approximately $4g$ faster than the infrastructure operation, where g denotes the genus of the hyperelliptic curve. Therefore, most of the algorithms in imaginary quadratic function fields can be sped up by performing arithmetic in a birationally equivalent real quadratic function field.