The Explicit-Formulas Database

D. J. Bernstein
University of Illinois at Chicago

Tanja Lange
Technische Universiteit Eindhoven

hyperelliptic.org/EFD
How to perform computations on large-char elliptic curves? Which coordinates to use?

This Friday: “Edwards!”

Many previous suggestions:
Jacobian coordinates;
projective coordinates;
Hessian curves;
Jacobi quartics;
Jacobi intersections;
“2” Doche/Icart/Kohel curves;
“3” Doche/Icart/Kohel curves.

hyperelliptic.org/EFD
We’ve collected everybody’s explicit formulas
(chains of +, −, ×)
for common operations
in each coordinate system.

Common operations:
doubling; tripling; addition;
readdition; mixed addition;
Weierstrass equivalence.

Plans: more operations;
char 2; curves of genus 2;
curves of genus 3.

hyperelliptic.org/EFD
We’ve converted the formulas to a standardized format.

We’ve verified them with Magma. Currently 123 Magma scripts: e.g., one script proves Weierstrass equivalence for Billet-Joye formulas for Jacobi-quartic doubling. (Or could check random inputs.)

Found errors in literature: one wrong doubling formula, one wrong equivalence.

hyperelliptic.org/EFD
We’ve added faster formulas. Example of a speedup (21 occurrences so far!):
replace a field multiplication with a squaring and a few adds.
(oldest publication I know: 2001 Bernstein for Jacobian doubling and addition)

Please let us know if you find more speedups!
e.g. 2007 Hisil/Carter/Dawson found $7M + 1S$ Hessian doubling, sent us an EFD update.

hyperelliptic.org/EFD