smalljac in sage

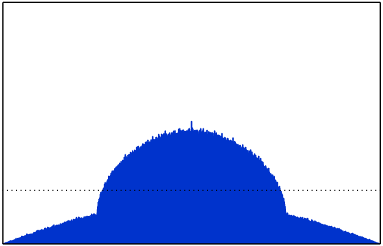
Pavel Panchekha and Andrew V. Sutherland

Massachusetts Institute of Technology

ANTS X Rump Session

Back to Banff (ANTS VIII)

Computing L-series of hyperelliptic curves, Kedlaya-S



smalljac version 4.0

Fast computation of L-polynomials (or Frobenius charpolys) and Jacobian group structures for genus $g \leq 2$ curves.

- Many performance enhancements.
- Prime bounds extended (2^{40} in genus 1, 2^{30} in genus 2).
- Now handles all genus 2 curves.
- Quadratic number fields.
- Sato-Tate group identification (heuristic).

smalljac in sage

Fully integrated into (64-bit) sage.

Improves performance of existing sage functionality:

- `E.aplist(B)` typically 5x to 10x faster than using Pari (or Magma's `TraceOfFrobenius`), handles B up to 2^{40}.
- `E.abelian_group()` 5x to 20x faster.
- `C.frobenius_polynomial()` 10x to 20x faster for genus 2 curves (and *much* faster than Magma's `LPolynomial`).

smalljac in sage

Adds new functionality to sage:

- `aplists` for curves over quadratic fields (e.g., $\mathbb{Q}(\sqrt{5})$)
- `grouplists` computes Jacobian group structures
- moments of L-poly coefficients
- histogram generation
- Sato-Tate group identification (as in FKRS 2012)

Demo

click here