[redacted] [redacted] Final paper.

[redacted]

10-15 pages, expository papers (no original research required!)

Deadline: December 13 at noon

If you [redacted] send a draft by December 6, I'll look over it and give comments! [redacted]

Some ideas:

- Discuss fast mult./division/gcd/... over $\mathbb{Z}$ instead of $K[x]$.

- Faster pol/integer mult. algorithms than Schönhage-Strassen
  cf. introduction of Clausen-van Loeven for a survey of previous results

- Faster [redacted] alg. for computing Frobenius normal form, characteristic pol., ...

- Black box linear algebra
  Instead of being given the n^2 coeff. of an $n \times n$-matrix M, what if we have an oracle that tells us [redacted] the vector Mv for any $v \in K^n$ we provide in time $T(n)$.
  How quickly can we compute $\det(M)$, $\chi_M(x)$, MN,...?
  Berlekamp-Massey alg., Wiedemann's algorithm, Freivald's alg

- ~~Factoring~~ root counting / root finding / factoring
  - polynomials over $\mathbb{R}, \mathbb{C}$

    Sturm's theorem, Newton's method, ...

- Real algebraic geometry

  cf. Basu-Pollack-Roy: Algorithms in Real Algebraic Geometry

  e.g. cylindrical decomposition