## CoCoALib - Slug #1165

# MinPoly over QQ: verification may be very slow

12 Mar 2018 08:05 - Anna Maria Bigatti

Status: Closed Start date: 12 Mar 2018

Priority: Normal Due date:

Assignee: Anna Maria Bigatti % Done: 100%

Category:ImprovingEstimated time:7.70 hoursTarget version:CoCoALib-0.99600Spent time:7.00 hours

### Description

The verification step after the modular algorithm may be very slow.

On the other side it is easy to construct examples on which MinPolyHeuristic fails (despite very unlikely in general). Investigate on how to make a faster verification.

#### Related issues:

Related to CoCoALib - Feature #1167: New class VerificationLevel

Related to CoCoALib - Bug #1101: Bug in MinPolyModular (insufficient rational...

Closed 13 Mar 2018

11 Sep 2017

#### History

#### #1 - 12 Mar 2018 08:24 - Anna Maria Bigatti

- % Done changed from 0 to 10

An impressive example is given by 87 points in QQ<sup>3</sup>. MinPoly takes ~4s and the verification take 44s on my Mac.

Improvement in doing NF at every Horner step instead of every second step. (used to be ~80s)

#### #2 - 12 Mar 2018 08:57 - Anna Maria Bigatti

Tried with TwinFloat: good for the 87 points (10 times faster) bad for example QQ-rand (10 times slower)

### #3 - 16 Mar 2018 08:57 - Anna Maria Bigatti

- Assignee set to Anna Maria Bigatti
- % Done changed from 10 to 70

After many many experiments, code is settled as this:

- MinPolyQuot(f, I, x) makes the complete verification (over QQ)
- MinPolyQuot(f, I, x, N) makes N verifications mod N random primes ~2\*10^9

(N in CoCoA-5 is an integer, and in CoCoALib is a VerificationLevel)

With 3 primes takes < 1s in all examples from "UsingMinPoly"

### #4 - 16 Mar 2018 08:58 - Anna Maria Bigatti

- Related to Feature #1167: New class VerificationLevel added

### #5 - 16 Mar 2018 08:58 - Anna Maria Bigatti

- Related to Bug #1101: Bug in MinPolyModular (insufficient rational reconstruction) added

20 Apr 2024 1/2

## #6 - 17 Mar 2018 09:16 - Anna Maria Bigatti

Working well, but now this should also be accessible by IsRadical, IsMaximal,... Think well before doing this!!

## #7 - 31 Jul 2018 14:21 - Anna Maria Bigatti

- Status changed from New to Feedback
- % Done changed from 70 to 90

## #8 - 03 Aug 2018 17:37 - John Abbott

- Status changed from Feedback to Closed
- % Done changed from 90 to 100
- Estimated time changed from 10.00 h to 7.70 h

20 Apr 2024 2/2