# A new black box GCD algorithm using sparse Hensel lifting

Garrett Paluck
Simon Fraser University, Canada

30th Applications of Computer Algebra - ACA 2025

Let $a$ and $b$ be polynomials in $\mathbb{Z}[x_1, \ldots, x_n]$ that are given by black boxes for their evaluation. We present a new GCD algorithm for recovering the monic GCD $g = \gcd(a, b)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ in the sparse representation. Our algorithm recovers $g$ one variable at a time from bivariate images obtained using bivariate Hensel lifting. We have implemented our algorithm in Maple.

Our algorithm has three practical advantages over previous black box algorithms. First, it is a modular GCD algorithm; it recovers the rational coefficients in $g$ using Chinese remaindering and rational number reconstruction. Second, it can easily omit computation of the content of $g$ in a chosen variable $x$ which means it's faster for applications which need only the primitive part of $g$ in $x$. Third, it recovers the square-free factorization of $g$ which means it's faster when the square-free factors of $g$ are all smaller than $g$.

In the talk we'll present our new GCD algorithm and benchmarks comparing it with previous work; we compare CPU time and the number of black box probes of the algorithms.