Factoring Multilinear Boolean Polynomials

Michael Monagan
Simon Fraser University, Canada

30th Applications of Computer Algebra - ACA 2025

We present two new algorithms for factoring multilinear boolean polynomials. The first is a Monte Carlo algorithm. The second is a deterministic algorithm based on recursive GCD computations. We've implemented both algorithms in C and also Emelyanov and Ponomaryov's FDE algorithm for comparison. Our Monte Carlo algorithm is much faster than their FED algorithm and our GCD algorithm is much faster than our Monte Carlo algorithm. But we do not know the complexity of our GCD algorithm.