

**ICM-9312-59** Parallel Multivariate  $p$ -adic Lifting on Shared-Memory Multiprocessors, Paul S. Wang.

ABSTRACT Continuing research at Kent addresses the parallelization of multivariate  $p$ -adic lifting, a procedure important in modern gcd and factorization algorithms. The variable-by-variable EEZ Lifting algorithm with a recursive correction coefficient procedure is parallelized. Key parallel steps include: computing the residue, extracting coefficients of terms, building correction coefficients, and updating factors. Implementation is on a 26-processor Sequent Balance with a ported SACLIB package. Timing results are included.