ACA 2021 Book of Abstracts

https://aca2021.sba-research.org/ July 23-27, 2021 (online)

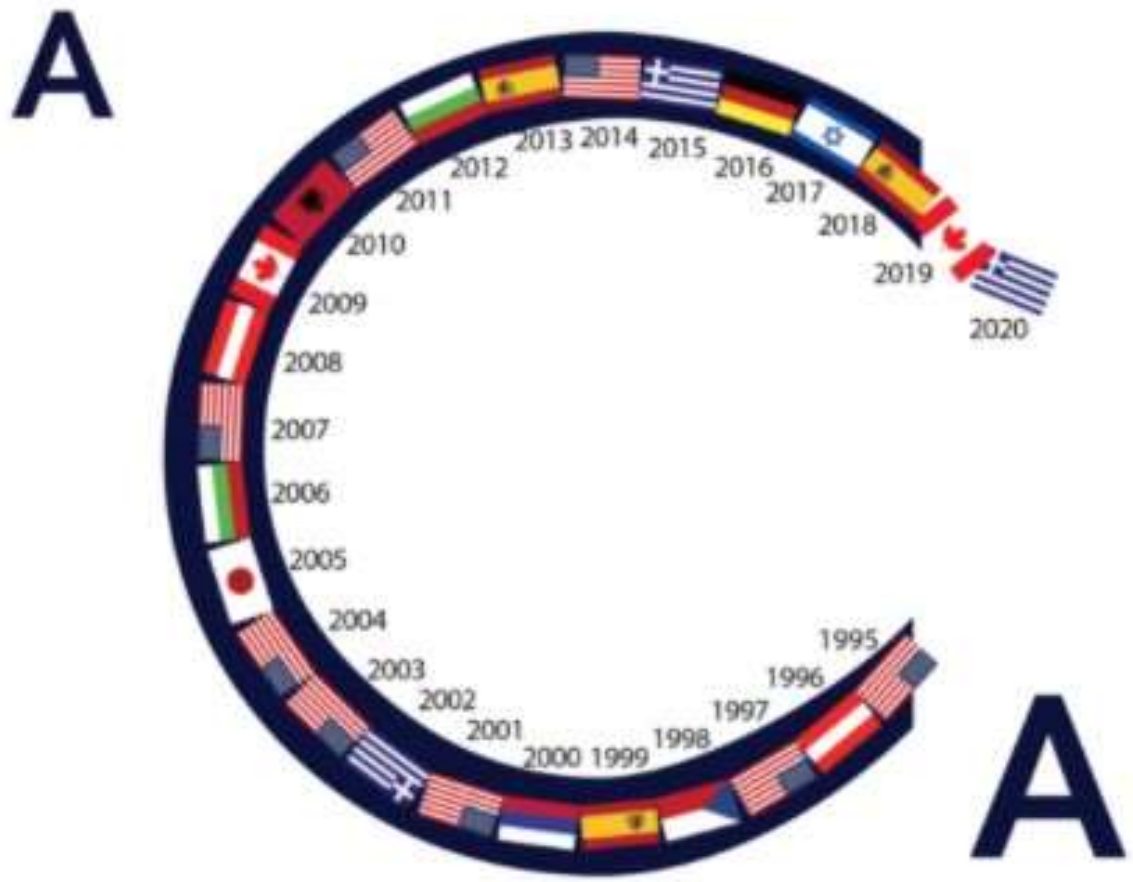
Bernhard Garn

Ludwig Kampel

Ilias Kotsireas

Dimitris Simos

Michael Wester



Applications of Computer Algebra – ACA 2021
Virtual. Online | July 23-27, 2021
Session on *Symbolic and Exact Linear Algebra over Rings and Fields*

Coppersmith's block Wiedemann method for polynomial problems

Gilles Villard [gilles.villard@ens-lyon.fr]

CNRS, ENS de Lyon, Inria, UCBL, Univ. Lyon, LIP laboratory, Lyon, France

Coppersmith has introduced a block version of Wiedemann's algorithm [1,11]. The method allows to obtain algorithms with best known complexity bounds for various matrix and polynomial problems. We can mention for example:

- Determinant of a matrix over a ring [5];
- Sparse linear systems and inversion of sparse matrices [4, 2, 8];
- Annihilating polynomials of structured matrices [6];
- Resultant of bivariate polynomials [10];
- Fast modular composition of univariate polynomials [7];
- Manipulation of zero-dimensional ideals [3].

We will review the general approach and discuss new improvement for the resultant problem, using a combination of techniques for structured matrices and high-order lifting [9].

Keywords
Coppersmith's block Wiedemann algorithm, resultant of polynomials, structured matrices

References

[1] D. COPPERSMITH, *Solving homogeneous linear equations over GF(2) via block Wiedemann algorithm*. Mathematics of Computation, 62(205), 1994.

[2] W. EBERLY, M. GIESBRECHT, P. GIORGI, A. STORJOHANN, G. VILLARD, *Faster inversion and other black box matrix computation using efficient block projections*. Proc. ISSAC, Waterloo, Canada, ACM Press, 2007.

[3] S. G. HYUN, V. NEIGER, H. RAHKOOY, É. SCHOST., *Block-Krylov techniques in the context of sparse-FGLM algorithms*. Journal of Symbolic Computation, 98, 2020.

[4] E. KALTOFEN, *Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems*. Mathematics of Computation, 64(210), 1995.

[5] E. KALTOFEN, G. VILLARD, *On the complexity of computing determinants*. Computational Complexity, 13:91-130, 2005.

[6] P. KARPMAN, C. PERNET, H. SIGNARGOUT, G. VILLARD., *Computing the characteristic polynomial of generic Toeplitz-like and Hankel-like Matrices*. Proc. ISSAC, Saint Petersburg, Russia, ACM Press, 2021.

[7] V. NEIGER, B. SALVY, É. SCHOST, G. VILLARD, *Fast modular composition*. In preparation.

[8] R. PENG, S. VEMPALA, *Solving sparse linear systems faster than matrix multiplication*. Proc. ACM-SIAM SODA, 2021.

[9] A. STORJOHANN, *High-order lifting and integrality certification*. Journal of Symbolic Computation, 36, 2003.

[10] G. VILLARD, *On computing the resultant of generic bivariate polynomials*. Proc. ISSAC, New York, USA, ACM Press, 2018.

[11] D. WIEDEMANN, *Solving sparse linear equations over finite fields*. IEEE Trans. Information Theory 32(1):54–62, 1986.