On Some Submatrix of the Macaulay Matrix

Alexandr Seliverstov

Abstract. We consider the generic-case complexity of the Gröbner basis of a zero-dimensional ideal in the ring of multivariate polynomials over a field. The ideal is generated by some linear functions as well as all univariate polynomials $x_k^2 - x_k$. The generic rank of an auxiliary matrix is also estimated.

Introduction

We assume three possible answers: the input may not only be accepted or rejected, but also an explicit notification of uncertainty of the choice is possible. In any case, the answer must be obtained in a finite time and without errors, and if an easily verifiable condition is met, then the notification of uncertainty can be issued only for a small fraction of inputs among all inputs of a given size. Such algorithms are called *generic* [1] or *errorless heuristics*.

Our algorithm can be considered as method to compute the Gröbner basis of a zero-dimensional ideal in the ring of multivariate polynomials over a field K. The ideal is generated by all univariate polynomials $x_k^2 - x_k$ and some linear functions.

On the Macaulay matrix definition as well as the Gröbner basis computation refer to [2, 3, 4, 5, 6]. In fact, we consider a submatrix of the Macaulay matrix.

Results

Let us consider a system of m linear equations in n variables:

$$\begin{cases} \alpha_{11}x_1 + \dots + \alpha_{1n}x_n + \alpha_{10} = 0 \\ \cdots \\ \alpha_{m1}x_1 + \dots + \alpha_{mn}x_n + \alpha_{m0} = 0 \end{cases}.$$

Multiplying each linear equation by each of the variables and taking into account the equalities $x_k^2 = x_k$, which are satisfied with $\{0, 1\}$-solutions, we obtain mn new equations of the second degree. In the general case, a new linearly independent linear equation can be derived from resulting quadratic equations.

Discarding the terms depending only on one variable, we obtain a set of mn bilinear forms, the coefficients of which form a matrix denoted by W. The rows correspond to the bilinear forms, and the columns correspond to monomials of the form $x_j x_k$ for $j < k$.

For $n = 3$ and $m = 1$, the 3×3 matrix

$$W = \begin{pmatrix} \alpha_{12} & \alpha_{13} & 0 \\ \alpha_{11} & 0 & \alpha_{13} \\ 0 & \alpha_{11} & \alpha_{12} \end{pmatrix}$$

is degenerate over a field of characteristic $\mathrm{char}(K) = 2$ because

$$\det(W) = -2\alpha_{11}\alpha_{12}\alpha_{13}.$$

Next, for $n = 5$ and $m = 2$, the 10×10 matrix W is degenerate over any field because $\mathrm{rank}(W) \leq 9$.

For $n = 7$ and $m = 3$, the 21×21 matrix W is also degenerate over any field because $\mathrm{rank}(W) \leq 18$. (The rank is computed with Maple.)

Theorem 1. *Let the matrix W be computed for m linear equations in n variables over a purely transcendental extension of the field K, where all coefficients α_{ij} are algebraically independent of each other. The rank of the matrix satisfies the inequality*

$$\mathrm{rank}(W) \geq mn - \frac{m(m+1)}{2}.$$

Hypothesis 1. *If the matrix W be computed for two linear equations in $n \geq 2$ variables, then the rank of the matrix satisfies the inequality* $\mathrm{rank}(W) \leq 2n - 1$.

For $2 \leq n \leq 9$, the hypothesis has been confirmed using Maple.

Theorem 2. *Let us assume Hypothesis 1 holds. If the matrix W be computed for m linear equations in $n \geq 2$ variables, then the rank of the matrix satisfies the inequality* $\mathrm{rank}(W) \leq mn - m + 1$.

Hypothesis 2. *If the matrix W be computed for m linear equations in n variables and the inequality $n \geq 2m + 1$ holds, then the rank of the matrix satisfies the inequality*

$$\mathrm{rank}(W) \leq mn - \frac{m(m-1)}{2}.$$

Theorem 3. *If $mn > \mathrm{rank}(W)$ and the free terms α_{i0} are uniformly and independently distributed on the set $S \subset K$ of cardinality $\lceil 1/\varepsilon \rceil$, then there is no new linear equation with the probability not exceeding ε. Otherwise, the new linear equation can be found using $O(n^6)$ algebraic operations over the field K.*

Conclusion

So, for almost all systems of linear equations, if the number of equations is sufficiently large, then one can easily either find a $\{0,1\}$-solution, or prove that there is no such solution. The method is not applicable when the system has many $\{0,1\}$-solutions. Thus, we have a polynomial upper bound on the generic-case complexity, but not in the worst case.

The author is thankful to Alexander N. Rybalov (Omsk Branch of Sobolev Institute of Mathematics).

The research was carried out within the state assignment of Ministry of Science and Higher Education of the Russian Federation for IITP RAS.

References

[1] A.N. Rybalov, On the generic complexity of solving equations over natural numbers with addition, *Prikladnaya Diskretnaya Matematika*, 2024, no. 64, pp. 72–78 (in Russian). https://doi.org/10.17223/20710410/64/6

[2] N. Courtois, A. Klimov, J. Patarin, and A. Shamir, Efficient algorithms for solving overdefined systems of multivariate polynomial equations, In: Preneel, B. (eds) Advances in Cryptology – EUROCRYPT 2000. EUROCRYPT 2000. Lecture Notes in Computer Science, vol. 1807. Springer, Berlin, Heidelberg, 2000. https://doi.org/10.1007/3-540-45539-6

[3] Yu.A. Blinkov, S.I. Salpagarov, A.A. Mamonov, and I.A. Akopian, Development of a system for evaluating the performance of computer algebra algorithms in finding Gröbner bases, *Computer Tools in Education*, 2024, no. 2, pp. 39–47. https://doi.org/10.32603/2071-2340-2024-2-39-47

[4] R. La Scala, F. Pintore, S.K. Tiwari, and A. Visconti, A multistep strategy for polynomial system solving over finite fields and a new algebraic attack on the stream cipher Trivium, *Finite Fields and Their Applications*, 2024, vol. 98, no. 102452, pp. 1–33. https://doi.org/10.1016/j.ffa.2024.102452

[5] S.M. Styopkin, The new is the well-forgotten old — F4 algorithm optimization, *Computational Mathematics and Mathematical Physics*, 2025, vol. 65, no. 3, pp. 582–590. https://doi.org/10.1134/S0965542524702154

[6] Shuhei Nakamura, Solving systems of polynomial equations via Macaulay matrices, *Cryptology ePrint Archive*, 2025, no. 793. https://eprint.iacr.org/2025/793

Alexandr Seliverstov
Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)
Moscow, Russia
e-mail: slvstv@iitp.ru