The Generic-Case Complexity of Finding a Binary Solution to a System of Linear Equations*

Alexandr V. Seliverstov
Institute for Information Transmission Problems
of the Russian Academy of Sciences (Kharkevich Institute)

June 25, 2025

*AMS: 90C09

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

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

Is there an $\{0,1\}$-solution to the system?

The problem is NP-complete not only over the ring of integers, but also over the field of residues modulo any odd prime.

Over the ring of integers, under a constraint on the size of the coefficients, a heuristic polynomial-time algorithm is known (Pan, Zhang, 2016). It is based on finding the shortest nonzero vector in an integer lattice.

Over an arbitrary field K of characteristic $\mathrm{char}(K) \neq 2$, for almost all systems having $n - \sqrt{2n - o(n)}$ linear equations in n variables, a heuristic polynomial-time algorithm had been proposed several years ago (Zverkov, Seliverstov, 2023).

In this work, the restriction on the number of equations is relaxed, although the generic-case complexity increases up to $O(n^6)$.

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* or *errorless heuristics*.

To estimate the number of inputs of a given size on which the algorithm quickly makes the correct decision, we use the Schwartz–Zippel lemma.

Lemma 1. (Schwartz, 1980) *Given a non-constant polynomial* $f(x_1, \ldots, x_n)$ *of degree* d *over a field* K. *If random variables* $\xi_1, \ldots, \xi_n$ *are independent and uniformly distributed on a finite set* $S \subseteq K$ *of cardinality* $|S|$, *then the inequality*

$$\mathrm{Prob}\left[f(\xi_1, \ldots, \xi_n) = 0\right] \leq \frac{d}{|S|}$$

holds, where Prob[·] *denotes the probability of the condition indicated in square brackets.*

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

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

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.

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_jx_k for $j < k$.

For $n = 3$ and $m = 1$,

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

Example. 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 SymPy.)

Lemma 2. *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*

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

Let the number of equations m be such that $mn \geq \mathrm{rank}(W) + n - m$.

The inequality holds for $n \geq m \geq n/2$. But a smaller number m is sufficient because the rank of W is small.

In the general case, n linearly independent linear equations can be derived from resulting quadratic equations as well as the initial linear equations.

Next, using these n linearly independent linear equations, one can find a solution and check whether it consists of zeros and ones.

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 generic-case complexity equals $O(n^6)$.

The probability of success is equal to the probability that the determinant of an $n \times n$ matrix does not vanish. Let K denote a field.

Theorem 1. *For our method, there is an univariate polynomial $f(n)$ so that if n is even, $n \geq m \geq n/2$, and the coefficients α_{ij} are uniformly and independently distributed on the set $S \subset K$ of cardinality $\lceil f(n)/\varepsilon \rceil$, then the upper bound on the probability of the uncertain answer equals ε.*

Example. Let us consider a linear equation

$$\alpha x_1 + \beta x_2 + 1 = 0,$$

where both α and β are nonzero.

Multiplying this 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 a system of two equations:

$$\begin{cases} \beta x_1 x_2 + (1+\alpha) x_1 = 0 \\ \alpha x_1 x_2 + (1+\beta) x_2 = 0 \end{cases}.$$

So, $W = \binom{\beta}{\alpha}$ has only one column with two entries.

Using elimination of $x_1 x_2$, we get the linear equation

$$\alpha(1+\alpha) x_1 = \beta(1+\beta) x_2.$$

For $\alpha = \beta = -1$, this equation turns into the identity. But in the general case, it is a new linear equation, which is linearly independent of original one.

If $\alpha = \beta = -1$, then there are two $\{0,1\}$-solutions to the equation $x_1 + x_2 = 1$.

Of course, the more $\{0,1\}$-solutions exist, the more difficult the task becomes.

Remark. In accordance with Lemma 2, in the general case, such bounds based on the Schwartz–Zippel lemma cannot be significantly improved without increasing runtime. However, such an improvement is possible for sparse systems of equations with a fixed arrangement of nonzero coefficients.

Unfortunately, Lemma 2 is only a rough estimate of the typical rank. Thus, in Theorem 1, the polynomial $f(n)$ is unknown.

Remark. The algorithm can be useful over a finite field too, although the Schwartz–Zippel lemma requires sufficiently many elements depending on the number of variables. Of course, if K is infinite, then a sufficiently large set $S \subset K$ exists for all n and $\varepsilon > 0$.

However, over any finite field, there is a high probability that at least one new independent linear equation can be added to the initial linear system. So, one can either take next iteration or reduce the complexity of the exhaustive search.

The second method:

if there is at least one new independent linear equation,
then extend the linear system and
run the search of new linear equations **again**;
else run an exhaustive search of $\{0,1\}$-solutions to the system.

Remark. 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.

But the probability of success at the first step is large over any field K.

In particular, one can work over a finite field too.

Theorem 2. *If $n \geq m \geq n/2$ 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.*
The generic-case complexity is equal to the complexity of finding the rank of W as well as a maximal nondegenerate submatrix.

Remark. If the number of variables is sufficiently large, then the worst-case computational complexity remains high. Nevertheless, in accordance with our result, the Merkle–Hellman cryptosystem based on the subset sum problem can be broken in almost all cases by means of a broadcast attack against it, refer to (Pan, Zhang, 2016).

Other problems can also be reduced to the problem under consideration.

Remark. Our algorithm can also be considered as method to compute the Gröbner basis of some zero-dimensional ideal in the ring of multivariate polynomials. It is essential that the ideal is zero-dimensional because it contains polynomials $x_k^2 - x_k$.

Further generalizations to other zero-dimensional ideals are also possible, but the computational complexity will be higher.

In this way, systems of non-linear algebraic equations can also be considered, refer to (Smith-Tone, Tone, 2025).

References

[1] *Pan Y., Zhang F.* Solving low-density multiple subset sum problems with SVP oracle. *Journal of Systems Science and Complexity.* 2016. Vol. 29, pp. 228–242.

[2] *Schwartz J.* Fast probabilistic algorithms for verification of polynomial identities. *J. ACM.* 1980. Vol. 27, no. 4, pp. 701–717.

[3] *Smith-Tone D., Tone C.* A correct justfication for the CHMT algorithm for solving underdetermined multivariate systems. *Finite Fields and Their Applications.* 2025. Vol. 103, no. 102547, pp. 1–18.

[4] *Zverkov O.A., Seliverstov A.V.* Effective lower bounds on the matrix rank and their applications. *Programming and Computer Software.* 2023. Vol. 49, no. 5, pp. 441–447.

Thank you