

On Systems of Three Linear Equations Modulo Three

Alexandr Seliverstov

Abstract. For a system of three linear equations in at least eight variables modulo three, either there is a binary solution to the system, or one can eliminate two variables so that the new system has a binary solution if and only if the initial system has a binary solution. In this way, one can improve the previously published algorithm, which had been implemented in Python by Oleg Zverkov, for finding some binary solution to a system of linear equations modulo three.

Introduction

Let us denote by $GF(3)$ the field of residues modulo three. Elements of the field $GF(3)$ are numbers $\{0, 1, 2\}$. Let us write $-1 = 2$ instead of $-1 \equiv 2 \pmod{3}$.

A solution to a system of equations in which the value of each variable belongs to the set $\{0, 1\}$ is called a $(0, 1)$ -solution.

The recognition problem of deciding whether there is a $(0, 1)$ -solution to a system of linear equations over the field $GF(3)$ is NP-complete. However, for a single equation, this problem can be easily solved: only a linear equation of the type $x_k = 2$ does not have a $(0, 1)$ -solution because each linear equation that depends non-trivially on at least two variables has a $(0, 1)$ -solution.

Definition. Let a system of linear equations in variables x_1, \dots, x_n contain more than one equation and some equation non-trivially depends on x_k . A new system of linear equations is obtained from the original system by eliminating the variable x_k when two conditions hold:

1. The new system does not depend on the variable x_k ;
2. The original system is equivalent to the union of the new system and exactly one equation (depending on x_k) equal to a linear combination of the equations of the original system.

For a system $A\mathbf{x} = \mathbf{b}$, if two columns in the matrix A are proportional to each other, then corresponding variables can be eliminated so that the new system has a $(0, 1)$ -solution if and only if the initial system has a $(0, 1)$ -solution, refer to [1].

Example. Let us consider the system of two linear equations in four variables:

$$\begin{cases} x_1 + x_2 & = 1 \\ x_1 - x_2 + x_3 + x_4 & = 0 \end{cases} .$$

Eliminating the variable x_3 yields one equation $x_1 + x_2 = 1$ so that each of its $(0, 1)$ -solutions can be extended to a $(0, 1)$ -solution to the system of two equations. In fact, two variables are simultaneously eliminated.

In the same way, one can simplify any system of a few equations in sufficiently many variables, refer to [1].

Theorem 1. *There is a polynomial-time algorithm that takes as input a system of m linear equations in n variables over the field $GF(3)$ and, subject to the condition*

$$m \leq \log_3 \log_3(2n - 1),$$

accepts the input if and only if the system has a $(0, 1)$ -solution.

Results

Next, let us consider systems of three equations over $GF(3)$. How to decide whether it has a $(0, 1)$ -solution? It is easy.

Theorem 2. *For all $n \geq 8$, if an $3 \times n$ matrix A over $GF(3)$ has no pair of columns that are proportional to each other, then for all 3-dimensional columns \mathbf{b} , there is a $(0, 1)$ -solution to the system $A\mathbf{x} = \mathbf{b}$.*

Proof. The proof of Theorem 2 is based on the classification of matrices up to column permutations and elementary row operations. For each class, checking whether there is a $(0, 1)$ -solution to the system $A\mathbf{x} = \mathbf{b}$ regardless of the choice of column \mathbf{b} can be reduced to calculating the Gröbner basis for some polynomial ideal. The calculations have been performed with the Maple computer algebra system. \square

Remark. If the matrix A has two columns proportional to each other, then one can eliminate two variables. For $n \geq 14$, each $3 \times n$ matrix over $GF(3)$ has columns proportional to each other. So, one can improve the former algorithm in the segment $8 \leq n \leq 13$. For $n = 7$, there is a counter-example.

Theorem 3. *Over $GF(3)$, for all $m \geq 1$, there is a system of m linear equations in $n = 3m - 2$ variables that has no $(0, 1)$ -solution and for which the matrix A of coefficients at the linear terms has no pair of columns that are proportional to each other.*

Proof. Let A consist of the $m \times m$ identity submatrix and other $m \times (2m - 2)$ submatrix be so that in the first row, all entries except two are zero, and the last two entries are 1. The following rows, except for the last one, are obtained from the previous row by a cyclic permutation with a shift by two positions. In the last row of the submatrix the entries 1 and 2 alternate. For example:

$$1 \times 1 : \quad A = (1),$$

On systems of three linear equations modulo three

$$2 \times 4: \quad A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix},$$

$$3 \times 7: \quad A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 & 2 \end{pmatrix},$$

$$4 \times 10: \quad A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 1 & 2 & 1 & 2 \end{pmatrix}.$$

Let all entries in column \mathbf{b} be equal to zero except for the last one, and let the last entry be equal to 2. Then the system of equations $A\mathbf{x} = \mathbf{b}$ has no $(0, 1)$ -solution. The subsystem of equations, except for the last one, has two $(0, 1)$ -solutions: either all variables vanish, or all variables are equal to 1. But none of these solutions extends to a $(0, 1)$ -solution of the entire system. \square

Discussion

In accordance with Theorem 2, for $m \geq 3$ and $n \geq 8$, if the $m \times n$ matrix A contains an $m \times 8$ submatrix of rank three, where is no pair of columns that are proportional to each other, then one can simultaneously eliminate corresponding eight variables so that the new system has a $(0, 1)$ -solution if and only if the initial system has a $(0, 1)$ -solution. Unfortunately, looking for such a submatrix is hard because the run time of exhaustive search is bounded as $O(n^8)$. However, using the branch-and-bound method, one can significantly reduce the time of such a submatrix search. In the general case, almost all $m \times 4$ submatrices have rank four. So, the expected time seems to be $O(n^4)$. The author hopes that even such weak results may be interesting because it is better to get closer to the truth than to ignore it.

Method

Let us fix an $m \times n$ matrix A over $GF(3)$. To verify the existence of a $(0, 1)$ -solution to the system $A\mathbf{x} = \mathbf{b}$ for all \mathbf{b} , it is convenient to calculate the reduced Gröbner basis for an ideal I generated by the forms in all variables x_k and b_j as well as by all polynomials $x_k^2 - x_k$. Eliminating the variables x_k , we obtain an ideal in the variables b_j . If the elimination ideal is generated by the polynomials $b_j^3 - b_j$, then the corresponding zero-dimensional variety contains all $GF(3)$ -points, refer to [2].

For example, calculations with Maple use commands like

with(Groebner) : Basis(I, plex(x₁, ..., x_n, b₁, b₂, b₃), characteristic = 3);

after which the polynomials depending only on b_1 , b_2 , and b_3 are selected.

Remark. Using Gröbner bases, it is possible to perform the check faster than using the exhaustive search. So, Theorem 2 is a truly computer assisted result that could hardly be proved without computer algebra systems.

Conclusion

Our results allow us to improve the previously published algorithm (refer to [1]) for finding some $(0, 1)$ -solution to a system of linear equations modulo three. Instead of eliminating two variables, sometimes eight variables can simultaneously be eliminated. It requires that the rank of an eight-column submatrix equals three, but there is no pair of columns that are proportional to each other. Unfortunately, the computational complexity of looking for a set of variables to eliminate increases dramatically, but it is bounded by a polynomial in the number of variables. On the other hand, we illustrate the role of computer algebra systems for solving combinatorial problems as well as for creating new algorithms.

Funding. 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] O.A. Zverkov, A.V. Seliverstov. *On binary solutions to a system of linear equations modulo three*. Programming and Computer Software, 2025, vol. 51, no. 2, pp. 109–116. <https://doi.org/10.1134/S0361768824700919>
- [2] D.A. Cox, J.B. Little, D.B. O Shea. *Using algebraic geometry*. Springer, 1998.

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