On systems of three linear equations modulo three

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

Computer Assisted Mathematics 2025
July 15–17, 2025

Let us denote by $GF(3)$ the field of residues modulo three.
Elements of the field $GF(3)$ are numbers $\{0, 1, 2\}$.
For example, 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 two or more variables has a $(0, 1)$-solution.

x	y	$x + y$	$x + 2y$
0	0	0	0
0	1	1	2
1	0	1	1
1	1	2	0

Let a system of linear equations in variables $x_1, \ldots, x_n$ contain more than one equation and some equation non-trivially depends on x_k.

Definition. A new system of linear equations is obtained from the original system by eliminating the variable x_k if two conditions hold:
(1) the new system does not depend on the variable x_k and
(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.

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

Eliminating the variable x_3 yields one equation:

$$x_1 + x_2 = 1$$

and each of its $(0, 1)$-solutions can be extended to a $(0, 1)$-solution to the system of two equations.
Eliminating a variable can result in a system having a larger number of $(0, 1)$-solutions than the original system had.

Proposition. *Given an $m \times n$ matrix A over the field $GF(3)$.*
If $m \leq \log_3(2n-1)$, then there are two linearly dependent columns.
These columns can be found in polynomial time.

For example,
any 3×14 matrix over $GF(3)$ has linearly dependent columns.

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.

In the same way, one can simplify any system of a few equations in sufficiently many variables.

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.

Remark. For $m = 3$, the algorithm from Theorem 1 is applicable for

$$n \geq 3,812,798,742,494$$

Refer to

O.A. Zverkov, A.V. Seliverstov.
On binary solutions to a system of linear equations modulo three.
Programming and Computer Software, 2025, 51:2, 109–116.

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.

Remark. If the matrix A has two columns proportional to each other, then one can eliminate two variables.

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:

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

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

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

$$\begin{cases} x_1 & & & & & +x_6 & +x_7 & = & 0 \\ & x_2 & & +x_4 & +x_5 & & & = & 0 \\ & & x_3 & +x_4 & -x_5 & +x_6 & -x_7 & = & 2 \end{cases}.$$

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.

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.

For example, calculations with Maple use commands like

$$with(Groebner) : Basis(I, plex(x_1, \ldots, x_n, b_1, b_2, b_3), characteristic = 3);$$

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 (Zverkov & S. 2025) 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.

Thank you!