ПРОГРАММИРОВАНИЕ, 2026, № 2, с. 3–12

КОМПЬЮТЕРНАЯ АЛГЕБРА

УДК 004.421.6 + 512.624.3

ГЕНЕРИЧЕСКАЯ СЛОЖНОСТЬ ПОИСКА ДВОИЧНОГО РЕШЕНИЯ СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ

© 2026 г. А. В. Селиверстов*

**Институт проблем передачи информации им. А.А. Харкевича Российской академии наук*
127051 Москва, Большой Каретный переулок, д. 19 с. 1
E-mail: slvstv@iitp.ru

Поступила в редакцию 23.08.2025

Мы рассматриваем задачу поиска двоичного решения для системы линейных уравнений над полем с характеристикой, отличной от двух. Для большой доли систем, у которых число уравнений больше половины или равно половине числа переменных, проверка существования решения из нулей и единиц выполняется за полиномиальное время. Но известны бесконечные серии таких систем уравнений, для которых этот метод не позволяет получить ответ. В частности, для любого соотношения числа уравнений и числа переменных, трудным остался случай, когда система имеет больше одного двоичного решения. Наш метод также эффективен над конечным полем нечётной характеристики, поскольку во многих случаях позволяет сводить исходную задачу к аналогичной задаче меньшей сложности. Обсуждается связь с распознаванием максимального идеала в кольце многочленов от нескольких переменных. Вычислен ранг вспомогательной матрицы для некоторых случаев.

Ключевые слова: конечное поле, система линейных уравнений, ранг, идеал, полиномиальное время, система компьютерной алгебры

1. ВВЕДЕНИЕ

Рассмотрим систему из m линейных уравнений от n неизвестных над полиномиально вычислимым полем, характеристика которого не равна двум. Задача о существовании $\{0,1\}$-решения, где каждая переменная принимает значения из множества $\{0,1\}$, NP-полная. Частные случаи, когда рассматриваются уравнения с целыми коэффициентами, известны как задача о разбиении множества и задача о рюкзаке [1, 2]. Эта задача над конечным полем простой характеристики p сводится к аналогичной задаче над полем из p элементов. В частности, случай поля характеристики два сводится к обычной задаче линейной алгебры над полем из двух элементов. Но уже над полем характеристики три эта задача NP-полная, поскольку к ней легко сводится задача о выполнимости 3-КНФ с дополнительным условием, что в каждой элементарной дизъюнкции точно один литерал истинный.

Над кольцом целых чисел для задачи распознавания существования $\{0,1\}$-решения у системы линейных уравнений известен эвристический алгоритм полиномиального времени, применимый при дополнительных ограничениях на размер коэффициентов [3]. Этот подход основан на поиске кратчайшего ненулевого вектора в целочисленной решётке. Но в худшем случае задача вычислительно трудная.

Над произвольным полиномиально вычислимым полем для почти всех систем линейных уравнений, содержащих $n - \sqrt{2n - o(n)}$ линейных уравнений от n переменных, ранее был предложен эвристический алгоритм полиномиального времени [4, 5]. В этой работе ограничение на число уравнений ослаблено, но в типичном случае вычислительная сложность ограничена сверху функцией $O(n^6)$. Недетерминированное снижение вычислительной сложности задачи при близких ограничениях на число уравнений обсуждается в работе [6].

Мы оцениваем алгебраическую сложность. На практике требуется вычислимость операций над

основным полем за полиномиальное время [7, 8]. Над конечным полем битовая сложность близка к алгебраической. Напротив, над полем рациональных чисел битовая сложность часто оказывается высокой из-за роста длины записи числовых коэффициентов [9].

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Рассматривая задачу распознавания, мы предполагаем *три* возможных ответа. Вход может быть не только принят или отвергнут, но возможно явное уведомление об отказе от конкретного ответа. В любом случае ответ должен быть дан за конечное время без ошибки, а доля входов, на которых возникает отказ, мала среди всех входов того же размера. Такие алгоритмы называются генерическими (*generic*) или безошибочными эвристиками (*errorless heuristics*) [10, 11, 12].

Для оценки числа входов фиксированного размера, на которых происходит отказ, удобно использовать лемму Шварца–Зиппеля [13]. Над конечным полем этот результат Ойстин Оре (Øystein Ore) опубликовал в 1922 году [14].

Лемма 1 (Шварц–Зиппель)**.** *Дан отличный от константы многочлен $f(x_1, \ldots, x_n)$ степени d над полем K. Если случайные переменные $\xi_1, \ldots, \xi_n$ независимо и равномерно распределены на конечном множестве $S \subseteq K$ мощности $|S|$, то выполнено неравенство*

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

Здесь через Prob[·] *обозначена вероятность выполнения условия в квадратных скобках.*

Поиск $\{0,1\}$-решений системы линейных уравнений сводится к вычислению базиса Грёбнера нульмерного идеала, порождаемого набором из m линейных функций и многочленов вида $x_k^2 - x_k$ для всех индексов. Всего $m+n$ порождающих многочленов. Сложность вычисления базиса Грёбнера существенно зависит от максимальной степени многочленов, используемых на промежуточных шагах. Наш метод основан на верхней оценке этой степени.

Методы вычисления базисов Грёбнера совершенствуются, отметим программу GInv 2.0 [15] и оптимизацию алгоритма F_4, предложенную Стёпкиным [16]. Другой алгоритм XL предложен в 2000 году [17, 18]. В худшем случае базис Грёбнера может иметь большой размер. Согласно [19, 20], существует такая константа $c > 0$, что для любого n число элементов любого базиса Грёбнера для некоторого идеала, порождённого $O(n)$ многочленами от n переменных степени не выше n, не меньше числа $2^{2^{cn}}$. С другой стороны, над любым полем алгебраическая сложность вычисления редуцированного базиса Грёбнера нульмерного идеала, порождённого многочленами от n переменных степени не выше d, ограничена сверху многочленом от d^n. Эта верхняя оценка улучшена в работе [21], но часто сложность намного меньше, чем в худшем случае, что и обусловило широкое применение этих методов, в частности, для решения систем уравнений. Низкая вычислительная сложность поиска некоторого решения системы алгебраических уравнений в типичном случае обоснована при достаточно малом числе уравнений [22], но сложность низкая и при меньших ограничениях. Более того, над конечным полем поиск решений любой системы уравнений сводится к работе с нульмерным идеалом [23, 24].

3. РЕЗУЛЬТАТЫ

Рассмотрим систему из m линейных уравнений от n переменных:

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

Независимо умножая каждое уравнение на каждую из переменных и принимая во внимание равенства $x_k^2 = x_k$, которые выполнены для каждого $\{0,1\}$-решения, получим mn новых уравнений второй степени.

Игнорируя в этих уравнениях линейные члены, получим набор из mn билинейных форм, коэффициенты которых составляют матрицу W. Строки этой матрицы соответствуют билинейным формам, а столбцы соответствуют мономам вида x_jx_k для индексов $j < k$. Всего mn строк и $n(n-1)/2$ столбцов. Матрица W будет подматрицей в матрице Маколея (Macaulay matrix) [18], но в W меньше столбцов. Матрица W квадратная при $n = 2m + 1$.

Например, для $m = 1$ и $n = 3$ получится 3×3 матрица

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

Её определитель равен $\det(W) = -2\alpha_{11}\alpha_{12}\alpha_{13}$. Поэтому матрица всегда вырождена над полем характеристики два, но над другим полем она вырождена только при обращении в нуль любого из коэффициентов α_{11}, α_{12} или α_{13}.

Лемма 2. *Пусть матрица W вычислена для системы из m линейных уравнений от n переменных над чисто трансцендентным расширением поля K, а все коэффициенты α_{ij} алгебраически независимые друг от друга над K. Ранг этой матрицы удовлетворяет неравенству*

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

Доказательство. Пусть матрица W состоит из m подматриц по n строк в каждой, k-я подматрица соответствует k-му уравнению, а строка с номером $kn + j$ соответствует умножению k-го уравнения на x_j. Рассмотрим в матрице W квадратную подматрицу U, полученную удалением из W первой строки, двух строк с номерами $n+1$ и $n + 2$, трёх строк с номерами $2n + 1$, $2n + 2$ и $2n + 3$ и т. д., а также удалением последних столбцов, чтобы осталась квадратная матрица. Порядок матрицы U равен

$$\sum_{i=1}^{m}(n - i) = mn - \frac{m(m+1)}{2}.$$

На главной диагонали матрицы U расположены ненулевые элементы, произведение которых равно слагаемому в разложении определителя $\det(U)$. Это слагаемое равно $\alpha_{11}^{n-1}\alpha_{22}^{n-2}\cdots\alpha_{mm}^{n-m}$. В силу алгебраической независимости чисел α_{ij}, это слагаемое не сокращается. Следовательно, $\det(U) \neq 0$. Ранг матрицы W не ниже ранга матрицы U. □

Пусть числа уравнений m и переменных n удовлетворяют неравенству

$$mn \geqslant \operatorname{rank}(W) + n - m.$$

Это неравенство выполнено при $n \geqslant m \geqslant n/2$, но оно выполнено и для меньшего числа уравнений, когда ранг матрицы W маленький. С другой стороны, типичное значение ранга не слишком мало по лемме 2. В общем случае любое $\{0, 1\}$-решение удовлетворяет новой системе из n линейно независимых уравнений, из которых не меньше половины уже были в исходной системе, а остальные получены из квадратных уравнений исключением квадратичных членов. Далее, используя эти n линейно независимых уравнений, легко найти единственное решение и проверить, состоит ли оно из нулей и единиц. Мы будем называть этот метод *первым алгоритмом*.

Легко привести пример, когда этот метод нельзя применить. Если исходная система имела больше одного $\{0, 1\}$-решения, то новая система тоже будет иметь более одного решения над основным полем K. И если характеристика поля K не равна двум, то среди этих решений будут решения, которые отличаются от $\{0, 1\}$-решения. С геометрической точки зрения, каждая прямая, проходящая через две $\{0, 1\}$-точки, проходит и через третью точку с другими координатами. Итак, мы рассматриваем лишь генерический алгоритм, который даст неопределённый ответ в случае, когда не удалось найти достаточно большого числа линейно независимых уравнений. Генерическая сложность ограничена сверху функцией $O(n^6)$. Для успеха достаточно невырожденности некоторой $n \times n$ матрицы, составленной из линейных коэффициентов новой системы линейных уравнений. Вероятность успеха можно оценить, используя лемму Шварца–Зиппеля. Но сначала рассмотрим пример одного уравнения от двух переменных.

Пример. Рассмотрим линейное уравнение

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

где оба коэффициента α и β ненулевые. Умножая это уравнение на каждую из переменных и принимая во внимание равенства $x_1^2 = x_1$ и $x_2^2 = x_2$, получим систему из двух уравнений, которой удовлетворяет каждое из $\{0, 1\}$-решений:

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

Матрица W содержит один столбец и две строки: $W = \binom{\beta}{\alpha}$. Элиминируя моном x_1x_2, мы получим

линейное уравнение

$$\alpha(1+\alpha)x_1 - \beta(1+\beta)x_2 = 0.$$

В случае $\alpha = \beta = -1$, это уравнение становится тождеством. При этом существуют два $\{0,1\}$-решения уравнения $x_1 + x_2 = 1$. Алгоритм даст неопределённый ответ. В случае $\alpha+\beta = -2$ новое уравнение линейно зависит от исходного. Алгоритм тоже даст неопределённый ответ. Но когда $\alpha + \beta \neq -2$, получено новое уравнение, линейно независимое от исходного, а система двух уравнений не имеет $\{0,1\}$-решения, алгоритм сообщит об этом.

Теорема 1. *Существует такая функция $f(n)$, что для любого рационального $\varepsilon > 0$ и для любого чётного n при условии $2m \geqslant n$, если коэффициенты α_{ij} независимо и равномерно распределены на множестве $S \subseteq K$ мощности $\lceil f(n)/\varepsilon \rceil$, то верхняя граница вероятности неопределённого ответа первого алгоритма равна ε.*

Доказательство. Без ограничения общности, можно считать, что $n = 2m$. Сначала рассмотрим систему из m линейных уравнений специального вида, в которой k-е уравнение зависит от двух переменных x_{2k-1} и x_{2k}:

$$\begin{cases} \beta_1 x_1 + \beta_2 x_2 + 1 = 0 \\ \cdots \\ \beta_{2k-1} x_{2k-1} + \beta_{2k} x_{2k} + 1 = 0 \\ \cdots \\ \beta_{n-1} x_{n-1} + \beta_n x_n + 1 = 0 \end{cases}.$$

Повторяя рассуждения из примера, получим новые линейные уравнения

$$\begin{cases} \beta_1(1+\beta_1)x_1 - \beta_2(1+\beta_2)x_2 = 0 \\ \cdots \\ \beta_{2k-1}(1+\beta_{2k-1})x_{2k-1} - \beta_{2k}(1+\beta_{2k})x_{2k} = 0 \\ \cdots \\ \beta_{n-1}(1+\beta_{n-1})x_{n-1} - \beta_n(1+\beta_n)x_n = 0 \end{cases}.$$

Вместе эти уравнения составляют систему из n линейных уравнений от n переменных. Обозначим через M матрицу размера $n \times n$, составленную из коэффициентов при линейных членах. Определитель матрицы M равен многочлену от коэффициентов $\beta_1, \ldots, \beta_n$ исходной системы:

$$\det(M) = \pm \prod_{k=1}^{n/2} \beta_{2k-1}\beta_{2k}(2 + \beta_{2k-1} + \beta_{2k}),$$

где знак зависит от порядка уравнений. Если все коэффициенты β_k ненулевые и выполнены неравенства $\beta_{2k-1} + \beta_{2k} \neq -2$, то матрица M невырожденная.

Далее рассмотрим систему уравнений общего вида. В частности, как в лемме 2, можно рассмотреть систему, в которой коэффициенты алгебраически независимы друг от друга. В полученной новой системе можно элиминировать квадратичные мономы, используя лишь операции сложения и умножения. Элиминация всех квадратичных мономов возможна, поскольку ранг матрицы W не превышает числа mn. В итоге получится система новых уравнений, коэффициенты которых выражаются многочленами от коэффициентов исходных уравнений. Определитель матрицы M, составленной из коэффициентов линейных членов, будет многочленом от коэффициентов. Обозначим через $f(n)$ степень этого многочлена в худшем случае.

Вообще говоря, матрица M зависит от порядка элиминации мономов. Более того, при фиксированном порядке для некоторых наборов коэффициентов вместо элиминации переменной будет возникать нулевая строка в матрице M. Но рассмотренный пример показывает, что для каждого $n = 2m$ существует такой порядок, при котором многочлен $\det(M)$ не равен нулю тождественно.

Согласно лемме Шварца–Зиппеля, если коэффициенты исходных уравнений независимо и равномерно распределены на множестве $S \subseteq K$ мощности $\lceil f(n)/\varepsilon \rceil$, то вероятность вырождения матрицы M не превышает ε. Невырожденности матрицы M достаточно для успешного завершения работы алгоритма, хотя успех возможен и в случае вырожденной M. □

Сделаем несколько замечаний. Согласно лемме 2, не используя дополнительных ограничений, границу применимости первого алгоритма, основанную на лемме Шварца–Зиппеля, трудно заметно улучшить без значительного увеличения времени работы алгоритма в типичном случае. Но это не исключает возможности улучшения для разреженных систем. С другой стороны, вид функции $f(n)$ в теореме 1 зависит от оценки ранга матрицы W. Но лемма 2 служит лишь грубой оценкой максимального ранга. Кроме того,

чем меньше ранг матрицы W, тем меньше нужно уравнений в исходной системе при фиксированном числе переменных.

Этот же метод применим и над конечным полем, хотя лемма Шварца–Зиппеля не позволяет оценить вероятность успеха. Если поле K бесконечное, то всегда существует достаточно большое конечное множество $S \subset K$. Над конечным полем теорема 1 бесполезная, поскольку функция $f(n)$ возрастает с ростом n. Однако над любым полем можно рассматривать задачу поиска хотя бы одного линейно независимого линейного уравнения, которому должны удовлетворять все $\{0,1\}$-решения исходной системы уравнений. Очевидную модификацию алгоритма обозначим как *второй алгоритм*. Повторное применение второго алгоритма позволяет, вообще говоря, сводить исходную задачу к аналогичной задаче с меньшей разностью $n-m$. Однако этот процесс редукции может прерваться до получения окончательного ответа, поскольку каждый раз применяется генерический алгоритм. Ниже мы оценим вероятность успеха одного шага, т. е. добавления хотя бы одного нового линейного уравнения, линейно независимого от исходных.

С другой стороны, даже небольшое снижение разности $n-m$ приводит к снижению вычислительной сложности, поскольку новая задача может быть решена полным перебором $\{0,1\}$-оценок для $(n-m)$ переменных или же сведена методом ветвей и границ к нескольким аналогичным задачам от малого числа переменных в каждой.

Мы рассматриваем произвольно фиксированные коэффициенты линейных членов.

Теорема 2. *Пусть $\varepsilon > 0$, $m < n$ и коэффициенты $\alpha_{11}, \ldots, \alpha_{mn}$ линейных членов системы из m линейно независимых линейных уравнений от n уравнений удовлетворяют условию $mn > \operatorname{rank}(W)$. Если свободные члены α_{i0} линейных уравнений независимо и равномерно распределены на множестве $S \subseteq K$ мощности $\lceil 1/\varepsilon \rceil$, то второй алгоритм не добавляет ни одного линейно независимого линейного уравнения с вероятностью не выше числа ε.*

Доказательство. Новое линейное уравнение, которое ищет второй алгоритм, однородное, а коэффициенты при линейных членах равны линейным комбинациям свободных членов α_{i0} исходных линейных уравнений. Напротив, линейные члены исходных уравнений не зависят от α_{i0}. Линейная независимость нового уравнения от исходных m уравнений выражается отличием от нуля определителя некоторой квадратной подматрицы максимального порядка в матрице размера $(m+1) \times n$. Поскольку $m < n$, порядок этой подматрицы равен сумме $1+m$. Эта подматрица содержит элементы из строки, соответствующей новому уравнению. Расположение этой подматрицы зависит лишь от заранее фиксированных значений линейных членов исходных уравнений. Поскольку в этой подматрице только одна строка зависит от α_{i0}, её определитель равен мультилинейной функции от α_{i0}. Согласно лемме Шварца–Зиппеля, если подматрица выбрана правильно, то вероятность обращения определителя в нуль не превосходит числа ε. □

Следствие 1. *Пусть $\varepsilon > 0$, $n = 2m$ и произвольно фиксированы коэффициенты $\alpha_{11}, \ldots, \alpha_{mn}$ линейных членов системы из m линейно независимых линейных уравнений от n уравнений. Если свободные члены α_{i0} линейных уравнений независимо и равномерно распределены на множестве $S \subseteq K$ мощности $\lceil 1/\varepsilon \rceil$, то второй алгоритм не добавляет ни одного линейно независимого линейного уравнения с вероятностью не выше числа ε.*

Доказательство. Поскольку при $n = 2m$ выполнены неравенства

$$mn > \frac{n(n-1)}{2} \geqslant \operatorname{rank}(W),$$

результат следует из теоремы 2. □

4. ЭМПИРИЧЕСКАЯ ОЦЕНКА

Были рассмотрены матрицы W для систем линейных уравнений над чисто трансцендентным расширением поля рациональных чисел. Коэффициенты уравнений алгебраически независимые. Вычисление ранга выполнено, используя пакет LinearAlgebra системы компьютерной алгебры Maple. При нечётных $3 \leqslant n \leqslant 9$ для одного уравнения ранг матрицы W равен n, для системы из двух уравнений ранг матрицы W равен

$2n-1$. Для системы из трёх уравнений от семи переменных ранг матрицы W равен 18. В этих случаях ранг матрицы W равен выражению

$$mn - \frac{m(m-1)}{2}.$$

Это подтверждает, что граница в лемме 2 ниже максимального ранга матрицы W. Можно надеяться, что при $n = 2m+1$, когда матрица W квадратная, эмпирическая оценка равна точной верхней границе ранга матрицы W над полем характеристики нуль.

Гипотеза 1. *Если* $n \geqslant 2m+1$, *то*

$$\operatorname{rank}(W) \leqslant mn - \frac{m(m-1)}{2}.$$

Также гипотеза проверена для некоторых целочисленных матриц W. При $m = 3$ и $n = 9$ максимальный по выборке ранг был равен 24. При $m = 4$ и $n = 9$ максимальный по выборке ранг был равен 30.

Если гипотеза верна, то в следствии 1 условие $n = 2m$ можно ослабить, рассматривая системы с меньшим числом уравнений от того же числа переменных.

5. ОБСУЖДЕНИЕ

Генерическая сложность первого и второго алгоритмов зависит от сложности вычисления ранга матрицы. Известно, что сложность вычисления ранга близка к сложности матричного умножения [25, 26]. Кроме того, ранг матрицы быстро вычислим на многопроцессорной машине [27].

Вычислительная сложность в худшем случае экспоненциально быстро возрастает с ростом числа переменных. Однако первый алгоритм позволяет с большой вероятностью взломать криптосистему Меркля–Хеллмана с открытым ключом, основанную на задаче о разбиении множества, используя широковещательную атаку (broadcast attack). Метод сведения этой задачи к поиску $\{0,1\}$-решения системы линейных уравнений совпадает с описанием из работы [3].

Первый алгоритм можно рассматривать как способ вычисления базиса Грёбнера некоторого нульмерного идеала в кольце многочленов от нескольких переменных. Важно, что идеал нульмерный, поскольку он содержит многочлены вида $x_k^2 - x_k$. Более того, требование единственности $\{0,1\}$-решения означает, что идеал максимальный. Иными словами, происходит отделение друг от друга множеств несобственных и максимальных идеалов специального вида.

Дальнейшее обобщение на другие нульмерные идеалы тоже возможно. Однако вычислительная сложность будет выше, поскольку придётся рассматривать многочлены большей степени. В этом случае вместо матрицы W нужно рассматривать матрицу коэффициентов при мономах больших степеней, а размер этой матрицы больше размера матрицы W.

6. БЛАГОДАРНОСТИ

Автор благодарит Ксаверия Малышева и Антона Мамонова за обсуждение, Александра Рыбалова за обнаружение ошибки в черновом варианте, а также организаторов конференции Computer Algebra, прошедшей в Москве 23–25 июня 2025 года, где была апробация некоторых результатов этой работы.

7. ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа выполнена в рамках государственного задания ИППИ РАН, утвержденного Минобрнауки России.

СПИСОК ЛИТЕРАТУРЫ

1. *Cacchiani V., Iori M., Locatelli A., Martello S.* Knapsack problems — An overview of recent advances. Part II: Multiple, multidimensional, and quadratic knapsack problems // Comput. and Operat. Res. 2022. Vol. 143. No. 105693. P. 1–14. DOI: 10.1016/j.cor.2021.105693

2. *Alonistiotis G., Antonopoulos A., Melissinos N., Pagourtzis A., Petsalakis S., Vasilakis M.* Approximating subset sum ratio via partition computations // Acta Informatica. 2024. Vol. 61. P. 101–113. DOI: 10.1007/s00236-023-00451-7

3. *Pan Y., Zhang F.* Solving low-density multiple subset sum problems with SVP oracle // Journal of Systems Science and Complexity. 2016. Vol. 29. P. 228–242. DOI: 10.1007/s11424-015-3324-9

4. *Селиверстов А.В.* Двоичные решения для больших систем линейных уравнений // Прикладная дискретная математика. 2021. № 52. С. 5–15. DOI: 10.17223/20710410/52/1

5. *Селиверстов А.В.* Обобщение задачи о сумме подмножеств и кубические формы // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 1. С. 51–60. DOI: 10.31857/S0044466923010118

6. *Бойков А.А., Селиверстов А.В.* О кубе и проекциях подпространства // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2023. Т. 33. № 3. С. 402–415. DOI: 10.35634/vm230302

7. *Алаев П.Е.* Конечно порожденные структуры, вычислимые за полиномиальное время // Сибирский математический журнал. 2022. Т. 63. № 5. С. 953–974.

8. *Алаев П.Е.* Сложность операции обращения в группах // Алгебра и логика. 2023. Т. 62. № 2. С. 155–178.

9. *Байрамов Р.Э., Блинков Ю.А., Левичев И.В., Малых М.Д., Мележик В.С.* Аналитическое исследование кубатурных формул на сфере в системах компьютерной алгебры // Журнал вычислительной математики и математической физики. 2023. Т. 63. № 1. С. 93–101. DOI:10.31857/S0044466923010052

10. *Rybalov A.N.* Generic polynomial algorithms for the knapsack problem in some matrix semigroups // Siberian Electronic Mathematical Reports. 2023. Vol. 20. No. 1. P. 100–109. (In Russian) DOI: 10.33048/semi.2023.20.009

11. *Рыбалов А.Н.* О генерической сложности решения уравнений над натуральными числами со сложением // Прикладная дискретная математика. 2024. № 64. С. 72–78. DOI: 10.17223/20710410/64/6

12. *Лопатин А.А., Рыбалов А.Н.* О генерической сложности решения уравнений над бициклическим моноидом // Прикладная дискретная математика. 2025. № 67. С. 110–117. DOI: 10.17223/20710410/67/6

13. *Schwartz J.* Fast probabilistic algorithms for verification of polynomial identities. Journal of the ACM. 1980. Vol. 27. No. 4. P. 701–717. DOI: 10.1145/322217.322225

14. *Atserias A., Tzameret I.* Feasibly constructive proof of Schwartz–Zippel lemma and the complexity of finding hitting sets // Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC'25), June 23–27, 2025, Prague, Czechia. ACM, New York, NY, USA, 2025. 12 p. DOI: 10.1145/3717823.3718276

15. *Блинков Ю.А., Салпагаров С.И., Мамонов А.А., Акопян И.А.* Разработка системы для оценки производительности алгоритмов компьютерной алгебры при нахождении базисов Грёбнера // Компьютерные инструменты в образовании. 2024. № 2. С. 39–47. DOI: 10.32603/2071-2340-2024-2-39-47

16. *Стёпкин С.М.* Новое – это хорошо забытое старое. Оптимизация алгоритма F4 // Ж. вычисл. матем. и матем. физ. 2025. Т. 65. № 3. С. 338–346.

17. *Courtois N., Klimov A., Patarin J., Shamir A.* 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. DOI: 10.1007/3-540-45539-6

18. *Nakamura Sh.* Solving systems of polynomial equations via Macaulay matrices // Cryptology ePrint Archive. 2025. Paper 2025/793. URL: https://eprint.iacr.org/2025/793

19. *Huynh D.T.* A superexponential lower bound for Gröbner bases and Church–Rosser commutative Thue systems // Information and Control. 1986. Vol. 68. No. 1-3. P. 196–206.

20. *Mayr E.W.* Some complexity results for polynomial ideals // Journal of Complexity. 1997. Vol. 13. P. 303–325.

21. *Hashemi A., Lazard D.* Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving // International Journal of Algebra and Computation. 2011. Vol. 21. No. 5. P. 703–713. DOI: 10.1142/S0218196711006364

22. *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. P. 1–18. DOI: 10.1016/j.ffa.2024.102547

23. *Bettale L., Faugère J., Perret L.* Hybrid approach for solving multivariate systems over finite fields // Journal of Mathematical Cryptology. 2009. Vol. 3. No. 3. P. 177–197. DOI: 10.1515/JMC.2009.009

24. *La Scala R., Pintore F., Tiwari S.K., Visconti A.* 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. P. 1–33. DOI: 10.1016/j.ffa.2024.102452

25. *Cheung H.Y., Kwok T.C., Lau L.C.* Fast matrix rank algorithms and applications // Journal of the ACM. 2013. V. 60. No. 5. Article No. 31. P. 1–25. DOI: 10.1145/2528404

26. *Neiger V., Pernet C.* Deterministic computation of the characteristic polynomial in the time of matrix multiplication // Journal of Complexity. 2021. V. 67. No. 101572. P. 1–35. DOI: 10.1016/j.jco.2021.101572

27. *Chistov A.L.* Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic // In: L. Budach (eds) Fundamentals of Computation Theory. FCT 1985. Lecture Notes in Computer Science, vol. 199. Springer, Berlin, Heidelberg, 1985. P. 63–69. DOI: 10.1007/BFb0028792

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)*

Bolshoy Karetny per. 19, build. 1, Moscow 127051 Russia

We consider the problem of finding a binary solution to a system of linear equations over a field with characteristic different from two. For a large fraction of systems in which the number of equations is equal to or more than half the number of variables, the existence of a solution consisting of zeros and ones can be verified in polynomial time. But there are known infinite series of such systems of equations so that this method does not allow one to obtain an answer. In particular, if the system has more than one binary solution, then the problem of finding a binary solution remains difficult for any ratio of the number of equations to the number of variables. Our method is also effective over a finite field of odd characteristic because in many cases it allows one to reduce the original problem to a similar problem of lower complexity. The relationship with recognizing the maximal ideal in the ring of polynomials in several variables is discussed. The rank of the auxiliary matrix is calculated for some cases.

Keywords: finite field, system of linear equations, rank, ideal, polynomial time, computer algebra system

8. FUNDING

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

9. REFERENCES

1. Cacchiani, V., Iori, M., Locatelli, A., and Martello, S., Knapsack problems — An overview of recent advances. Part II: Multiple, multidimensional, and quadratic knapsack problems, *Comput. and Operat. Res.*, 2022, vol. 143, no. 105693, pp. 1–14. DOI: 10.1016/j.cor.2021.105693

2. Alonistiotis, G., Antonopoulos, A., Melissinos, N., Pagourtzis, A., Petsalakis, S., and Vasilakis, M., Approximating subset sum ratio via partition computations, *Acta Informatica*, 2024, vol. 61, pp. 101–113. DOI: 10.1007/s00236-023-00451-7

3. Pan, Y., and Zhang, F., Solving low-density multiple subset sum problems with SVP oracle, *J. Syst. Sci. Complex.*, 2016, vol. 29, pp. 228–242. DOI: 10.1007/s11424-015-3324-9

4. Seliverstov, A.V., Binary solutions to large systems of linear equations, *Prikladnaya Diskretnaya Matematika*, 2021, no. 52, pp. 5–15 (in Russian). DOI: 10.17223/20710410/52/1

5. Seliverstov, A.V., Generalization of the subset sum problem and cubic forms, *Comput. Math. Math. Phys.*, 2023, vol. 63, no. 1, pp. 48–56. DOI: 10.1134/S0965542523010116

6. Boykov, A.A., and Seliverstov, A.V., On a cube and subspace projections, *Vestnik Udmurtskogo Universiteta. Matematika. Mekhanika. Komp'yuternye Nauki*, 2023, vol. 33, no. 3, pp. 402–415 (in Russian). DOI: 10.35634/vm230302

7. Alaev, P.E., Finitely generated structures computable in polynomial time, *Siberian Math. J.*, 2022, vol. 63, no. 5. pp. 801–818. DOI: 10.1134/S0037446622050019

8. Alaev, P.E., The complexity of inversion in groups, *Algebra and Logic*, 2023, vol. 62, no. 2, pp. 103–118. DOI: 10.1007/s10469-024-09730-9

9. Bayramov, R.E., Blinkov, Y.A., Levichev, I.V., Malykh, M.D., and Melezhik, V.S., Analytical study of cubature formulas on a sphere in computer algebra systems, *Comput. Math. Math. Phys.*, 2023, vol. 63, pp. 77–85. DOI: 10.1134/S0965542523010050

10. Rybalov, A.N., Generic polynomial algorithms for the knapsack problem in some matrix semigroups, *Siberian Electronic Mathematical Reports*, 2023, vol. 20, no. 1, pp. 100–109 (in Russian). DOI: 10.33048/semi.2023.20.009

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

12. Lopatin, A.A., and Rybalov, A.N., On generic complexity of equation solving over the bicyclic monoid, *Prikladnaya Diskretnaya Matematika*, 2025, no. 67, pp. 110–117 (in Russian). DOI: 10.17223/20710410/67/6

13. Schwartz, J., Fast probabilistic algorithms for verification of polynomial identities, *J. ACM*, 1980, vol. 27, no. 4, pp. 701–717. DOI: 10.1145/322217.322225

14. Atserias, A., and Tzameret, I., Feasibly constructive proof of Schwartz–Zippel lemma and the complexity of finding hitting sets, *Proceedings of the 57th Annual ACM Symposium on Theory of Computing* (STOC'25), June 23–27, 2025, Prague, Czechia. ACM, New York, NY, USA, 2025. DOI: 10.1145/3717823.3718276

15. Blinkov, Y.A., Salpagarov, S.I, Mamonov, A.A., and Akopian, I.A., 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. DOI: 10.32603/2071-2340-2024-2-39-47

16. Styopkin, S.M., The new is the well-forgotten old — F4 algorithm optimization, *Comput. Math. Math. Phys.*, 2025, vol. 65, no. 3, pp. 582–590. DOI: 10.1134/S0965542524702154

17. Courtois, N., Klimov, A., Patarin, J., Shamir, A., 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. DOI: 10.1007/3-540-45539-6

18. Nakamura, Sh., Solving systems of polynomial equations via Macaulay matrices, *Cryptology ePrint Archive*, 2025, paper 2025/793. URL: https://eprint.iacr.org/2025/793

19. Huynh, D.T., A superexponential lower bound for Gröbner bases and Church–Rosser commutative Thue systems, *Inform. and Control*, 1986, vol. 68, no. 1-3, pp. 196–206.

20. Mayr, E.W., Some complexity results for polynomial ideals, *J. Complexity*, 1997, vol. 13, pp. 303–325.

21. Hashemi, A., and Lazard, D., Sharper complexity bounds for zero-dimensional Gröbner bases and polynomial system solving, *Int. J. Algebra Comput.*, 2011, vol. 21, no. 5, pp. 703–713. DOI: 10.1142/S0218196711006364

22. Smith-Tone, D., and 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. DOI: 10.1016/j.ffa.2024.102547

23. Bettale, L., Faugère, J., and Perret, L., Hybrid approach for solving multivariate systems over finite fields, *Journal of Mathematical Cryptology*, 2009, vol. 3, no. 3, pp. 177–197. DOI: 10.1515/JMC.2009.009

24. La Scala, R., Pintore, F., Tiwari, S.K., and Visconti, A., 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. DOI: 10.1016/j.ffa.2024.102452

25. Cheung, H.Y., Kwok, T.C., and Lau, L.C., Fast matrix rank algorithms and applications, *J. ACM*, 2013, vol. 60, no. 5, article 31. DOI: 10.1145/2528404

26. Neiger, V., and Pernet, C., Deterministic computation of the characteristic polynomial in the time of matrix multiplication, *J. Complexity*, 2021, vol. 67, no. 101572, pp. 1–35. DOI: 10.1016/j.jco.2021.101572

27. Chistov, A.L., Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. In: L. Budach (eds) Fundamentals of Computation Theory. FCT 1985. Lecture Notes in Computer Science, vol. 199. Springer, Berlin, Heidelberg, 1985, pp. 63–69. DOI: 10.1007/BFb0028792