

УДК 511.528

О ДВОИЧНЫХ РЕШЕНИЯХ СИСТЕМ УРАВНЕНИЙ¹

А. В. Селиверстов

*Институт проблем передачи информации им. А. А. Харкевича Российской академии наук,
г. Москва, Россия*

Решение называется двоичным, если каждая переменная равна нулю или единице. Известно, что трудно найти двоичное решение системы алгебраических уравнений, коэффициенты которых являются целыми числами с малыми абсолютными значениями. Целью работы является обоснование эффективного вероятностного сведения системы к одному новому уравнению в случае, когда существует небольшая разница между числом двоичных решений первого уравнения и числом двоичных решений всей системы. Более того, если первое уравнение линейное, то существует алгоритм псевдополиномиального времени для проверки правильности такого сведения к новому уравнению в общем случае.

Ключевые слова: алгебраическое уравнение, вероятностный алгоритм, вычислительная сложность.

DOI 10.17223/20710410/45/3

ON BINARY SOLUTIONS TO SYSTEMS OF EQUATIONS

A. V. Seliverstov

*Institute for Information Transmission Problems of the Russian Academy of Sciences
(Kharkevich Institute), Moscow, Russia*

E-mail: slvstv@iitp.ru

A solution is called binary if each variable is equal to either zero or one. It is well known that it is hard to find a binary solution to the system of algebraic equations in which the coefficients are integers with small absolute values. The aim of the paper is to propose an effective probabilistic reduction of the system to a new equation when there is a small difference between the number of binary solutions to the first equation and the number of binary solutions to the entire system. The proposed method is based on replacing the given system of equations with a linear combination of these equations. Coefficients are random integers that are independently and uniformly distributed over the segment from zero to some upper bound. The bound depends on the number of redundant binary solutions to the first equation that do not serve as solutions to the entire system. The proof uses the Schwartz — Zippel lemma. Moreover, if the first equation is linear, then there exists a pseudo-polynomial time algorithm to check the correctness of the reduction to the new equation in the general case.

Keywords: algebraic equation, probabilistic algorithm, computational complexity.

¹Работа поддержана грантом РФФИ № 18-29-13037.

Введение

Рассмотрим поиск двоичных решений системы алгебраических уравнений с целыми коэффициентами. Иначе такие решения называют булевыми. Рассмотрим сведение исходной системы уравнений к системе с меньшим числом уравнений так, чтобы максимальная степень уравнений не возрастала, а коэффициенты новых уравнений были целыми числами, абсолютные величины которых не слишком велики по сравнению с коэффициентами в исходных уравнениях.

Ограничение на степень уравнения существенно, поскольку любая система из m уравнений вида $\ell_k(\mathbf{x}) = 0$ эквивалентна над полем вещественных чисел одному уравнению $\ell_1^2(\mathbf{x}) + \dots + \ell_m^2(\mathbf{x}) = 0$. Здесь через $\mathbf{x}$ обозначен список переменных $x_1, \dots, x_n$. Ограничение на абсолютную величину коэффициентов тоже существенно, поскольку при достаточно быстро возрастающей последовательности чисел γ_k эта система имеет те же двоичные решения, что и одно уравнение $\gamma_1 \ell_1(\mathbf{x}) + \dots + \gamma_m \ell_m(\mathbf{x}) = 0$. Сведение системы линейных уравнений к одному линейному уравнению, имеющему те же двоичные решения, рассмотрено в работе [1].

Для одного линейного уравнения некоторое двоичное решение можно вычислить за псевдополиномиальное время методом динамического программирования, рассмотренным в нескольких работах Р. Э. Беллмана и (независимо) Дж. Б. Данцига в 1956–1957 гг. История развития этого метода до 1986 г. описана в [2]. Позже В. В. Смолев заметил, что если модули коэффициентов при линейных членах уравнения целые и отличаются друг от друга не более чем на небольшую величину, то время работы алгоритма существенно зависит от максимума этой величины, а не от максимума модулей коэффициентов. Более того, за псевдополиномиальное время можно найти число всех его двоичных решений [3]. Недавно опубликовано много работ, в которых улучшаются оценки памяти и времени, необходимых для решения этих задач [4–8]. Известна связь вычислительной сложности поиска двоичного решения линейного уравнения со сложностью некоторых задач, разрешимых за полиномиальное время [9].

В общем случае задача распознавания существования некоторого двоичного решения у системы линейных уравнений с коэффициентами из множества $\{-1, 0, 1\}$ является NP-полной [2]. Поэтому сведение такой системы уравнений к одному линейному уравнению с малыми коэффициентами возможно лишь при выполнении некоторых дополнительных условий.

Сейчас большое внимание уделяется разработке *генерических* алгоритмов полиномиального времени [10, 11]. Их можно рассматривать как частный случай эвристических алгоритмов, когда в типичном случае результатом работы алгоритма служит правильный ответ, но на малой доле входов, стремящейся к нулю при увеличении длины входа, алгоритм может отказаться от вычислений; при этом выдаётся сообщение об отказе. Аналогично определяются недетерминированные генерические алгоритмы. При этом некоторые алгоритмически трудные задачи остаются трудными и для генерических алгоритмов [12, 13].

Одно из возможных приложений рассматриваемых алгоритмов, стимулировавшее развитие новых методов поиска двоичных решений систем уравнений, — это решение биоинформатической задачи сравнения так называемых хромосомных структур с паралогами (то есть такими генами, которые трудно различить выравниванием последовательностей) и поиска оптимального соответствия между ними [14]. К поиску двоичных решений системы уравнений легко сводится также поиск решений диофантовых уравнений в произвольной ограниченной области. В этом случае целые числа из некоторого отрезка представимы последовательностью нулей и единиц [2].

1. Результаты

Теорема 1. Даны система, состоящая из $m \geq 2$ алгебраических уравнений $\ell_k(\mathbf{x}) = 0$, и целое число r из отрезка от единицы до $m-1$. Пусть подсистема, состоящая из первых r уравнений $\ell_1(\mathbf{x}) = 0, \dots, \ell_r(\mathbf{x}) = 0$, имеет не более μ избыточных двоичных решений, которые не служат решениями всей системы. Существуют такие целые числа $\gamma_{r+1}, \dots, \gamma_m$ из отрезка от нуля до μ , что каждое двоичное решение новой системы алгебраических уравнений $\ell_1(\mathbf{x}) = 0, \dots, \ell_r(\mathbf{x}) = 0$ и $\gamma_{r+1}\ell_{r+1}(\mathbf{x}) + \dots + \gamma_m\ell_m(\mathbf{x}) = 0$ служит решением исходной системы. Более того, для любого $\varepsilon > 0$ если случайные целые числа $\gamma_{r+1}, \dots, \gamma_m$ независимы и равномерно распределены на отрезке от нуля до $\lceil \mu/\varepsilon \rceil$, то указанное свойство выполнено с вероятностью большей разности $1 - \varepsilon$.

Доказательство. Обозначим через $\mathcal{M}$ множество тех двоичных решений рассматриваемой подсистемы, которые не являются решениями всей системы уравнений:

$$\mathcal{M} = \{\mathbf{x} \in \{0, 1\}^n : \ell_1(\mathbf{x}) = 0 \wedge \dots \wedge \ell_r(\mathbf{x}) = 0 \wedge \exists k \leq m (\ell_k(\mathbf{x}) \neq 0)\}.$$

Мощность $|\mathcal{M}|$ не превышает числа μ . Определим многочлен

$$f(y_{r+1}, \dots, y_m) = \prod_{\mathbf{x} \in \mathcal{M}} \left(\sum_{k=r+1}^m \ell_k(\mathbf{x}) y_k \right).$$

Если множество $\mathcal{M}$ пустое, то полагаем $f = 1$. В этом случае числа $\gamma_{r+1}, \dots, \gamma_m$ могут быть любыми, например равными нулю: $\gamma_{r+1} = \dots = \gamma_m = 0$.

Пусть множество $\mathcal{M}$ непустое. Если некоторая последовательность целых чисел $\gamma_{r+1}, \dots, \gamma_m$ достаточно быстро возрастает, то значение $f(\gamma_{r+1}, \dots, \gamma_m)$ отлично от нуля. Следовательно, многочлен f не равен нулю тождественно. С другой стороны, выполнено неравенство $\deg f \leq \mu$. По лемме Шварца — Зиппеля [15] существуют искомые целые числа $\gamma_{r+1}, \dots, \gamma_m$ из отрезка от нуля до μ , для которых $f(\gamma_{r+1}, \dots, \gamma_m) \neq 0$, и доля таких наборов чисел не меньше разности $1 - \varepsilon$ при $\varepsilon > 0$. ■

Замечание 1. Теорема 1 остаётся справедливой, если рассматривать не $(0, 1)$ -решения, а (α, β) -решения для произвольных чисел $\alpha \neq \beta$.

Далее ограничимся случаем, когда $r = 1$. В этом случае теорема 1 позволяет свести систему уравнений к системе двух уравнений. Переход от двух уравнений к одному, равному их линейной комбинации и имеющему те же двоичные решения, приводит к относительно небольшому увеличению коэффициентов (хотя в общем случае трудно свести систему из многих уравнений к одному при таком ограничении). Далее рассмотрено сведение системы уравнений к одному, имеющему те же двоичные решения, которое для краткости называется *новым уравнением*.

Теорема 2. Даны система из $m \geq 2$ алгебраических уравнений $\ell_k(\mathbf{x}) = 0$ и вещественное число $\varepsilon > 0$. Пусть первое уравнение $\ell_1(\mathbf{x}) = 0$ имеет не более μ избыточных двоичных решений, которые не служат решениями всей системы. Если случайные целые числа $\gamma_2, \dots, \gamma_m$ независимы и равномерно распределены на отрезке от нуля до $\lceil \mu/\varepsilon \rceil$, то с вероятностью большей разности $1 - \varepsilon$ каждое двоичное решение нового уравнения $\ell_1(\mathbf{x}) + \lambda(\gamma_2\ell_2(\mathbf{x}) + \dots + \gamma_m\ell_m(\mathbf{x})) = 0$ служит решением исходной системы. Здесь коэффициент λ равен произвольному целому числу, превосходящему сумму модулей всех коэффициентов многочлена ℓ_1 .

Доказательство. Применяя теорему 1 для случая $r = 1$, сведём исходную систему уравнений к системе двух уравнений вида

$$\begin{cases} \ell_1(\mathbf{x}) = 0, \\ \gamma_2\ell_2(\mathbf{x}) + \dots + \gamma_m\ell_m(\mathbf{x}) = 0 \end{cases}$$

с тем же набором двоичных решений. В каждой точке с координатами из множества $\{0, 1\}$ модуль значения функции ℓ_1 меньше числа λ . По модулю λ новое уравнение эквивалентно первому уравнению. Поэтому каждое двоичное решение нового уравнения служит решением первого уравнения $\ell_1 = 0$. Следовательно, оно служит решением и для второго уравнения, равного линейной комбинации (с рациональными коэффициентами) первого и нового уравнений. ■

Замечание 2. Требование, чтобы число μ было маленьким, существенно для практического применения рассмотренной сводимости, поскольку при больших значениях μ коэффициенты γ_k тоже могут быть большими. С другой стороны, число μ является лишь верхней границей; не требуется знание точного значения разности чисел двоичных решений у первого уравнения и у всей системы уравнений. Кроме того, небольшое увеличение значения μ может быть удобно для вычислений. Если $\lceil \mu/\varepsilon \rceil = 2^\nu - 1$ для целого ν , то равномерно распределённая случайная величина γ_k легко получается конкатенацией независимых симметричных бернуллиевских случайных величин, равных цифрам двоичной записи. Создание равномерного распределения на перестановках (то есть на множестве из $\nu!$ элементов) на основе бернуллиевских случайных величин обсуждается в [16].

Теорема 3. Дан многочлен $f(x_1, \dots, x_n)$ степени d , имеющий m мономов. Обозначим через $\ell(y_1, \dots, y_m)$ линейную форму, коэффициенты которой равны коэффициентам многочлена f , расставленным в любом порядке. Для любого числа α число двоичных решений уравнения $f(\mathbf{x}) = \alpha$ не более чем в $(2^d - 1)^m$ раз превосходит число двоичных решений линейного уравнения $\ell(\mathbf{y}) = \alpha$.

Доказательство. Каждое двоичное решение уравнения $f(\mathbf{x}) = \alpha$ соответствует двоичному решению уравнения $\ell(\mathbf{y}) = \alpha$, где значение переменной y_k равно значению соответствующего монома. При этом равенство $y_k = 0$ соответствует равенству нулю хотя бы одной из переменных, входящих в k -й моном. Каждый моном зависит самое большее от d переменных и обнуляется на самое большее $2^d - 1$ наборах двоичных значений этих переменных. Поэтому каждое решение уравнения $\ell(\mathbf{y}) = \alpha$ соответствует не более чем $(2^d - 1)^m$ двоичным решениям уравнения $f(\mathbf{x}) = \alpha$. ■

Пример 1. Рассмотрим многочлен $f = x_1x_2 + x_3x_4 + \dots + x_{2m-1}x_{2m}$. Линейное уравнение $y_1 + \dots + y_m = 0$ имеет только нулевое двоичное решение. По теореме 3 число двоичных решений уравнения $f(\mathbf{x}) = 0$ не превосходит числа 3^m , тогда как число всех наборов двоичных значений переменных $\mathbf{x}$ равно 4^m . Рассуждая, как при доказательстве теоремы 3, легко видеть, что эта оценка числа двоичных решений точная.

2. Обсуждение

Рассмотрим случай, когда первое уравнение системы линейное, а число его двоичных решений известно (оно может быть вычислено за псевдополиномиальное время [3]). Даже в этом случае трудно вычислить оптимальное значение μ в теореме 2. Однако если угадано некоторое значение μ и для этого значения случайно выбраны целые коэффициенты γ_k из отрезка от нуля до $\lceil \mu/\varepsilon \rceil$, то *a posteriori* можно проверить правильность выбора μ и коэффициентов γ_k , следовательно, проверить корректность вычисления. Для этого надо оценить сверху число решений полученного нового уравнения. Очевидно, любое решение системы служит решением этого уравнения. Поэтому при любом выборе коэффициентов γ_k число двоичных решений нового уравнения не меньше, чем число двоичных решений исходной системы. Если разность числа двоичных решений первого и нового уравнений превосходит число μ или отрицательна,

то сведение системы к новому уравнению должно быть признано некорректным. Причиной неудачи может быть как неправильно угаданное значение μ , так и неудачная реализация случайных коэффициентов γ_k . Если же эта разность положительна и не превосходит числа μ , то с вероятностью не меньше разности $1 - \varepsilon$ значение μ корректно, следовательно, новое уравнение тоже корректное.

Если все уравнения системы линейные, то новое уравнение тоже линейное и число его двоичных решений можно вычислить за псевдополиномиальное время. Так, по аналогии с генерическими алгоритмами, можно получить вероятностный алгоритм псевдополиномиального времени, который для систем линейных уравнений на большой доле входов с большой вероятностью выдаёт корректное новое уравнение, а на оставшейся доле входов, а также с малой вероятностью на любом входе выдаёт сообщение об отказе от вычисления. Такой алгоритм может сделать ошибку, не выдавая никакого предупреждения, но вероятность такой ошибки можно ограничить сверху сколь угодно малым положительным числом.

Если (алгебраическое) уравнение нелинейное, но имеет мало мономов, то число его двоичных решений можно оценить сверху посредством теоремы 3, рассматривая мономы как независимые переменные. При этом число решений линейного уравнения снова оценивается псевдополиномиальным алгоритмом. Такая оценка будет точнее для уравнений с меньшим числом мономов. Поскольку рассматриваются только двоичные решения, такое уравнение можно считать мультилинейным. В случае, когда система имеет двоичные решения, линейность первого уравнения существенна для вычисления верхней оценки оптимального значения μ в теореме 2 за псевдополиномиальное время. С другой стороны, несмотря на грубость оценки числа двоичных решений, когда таковые существуют, теорема 3 часто позволяет точно подтвердить отсутствие двоичных решений у нового уравнения и, следовательно, их отсутствие у исходной системы нелинейных уравнений.

Приведём пример, когда система уравнений имеет столько же двоичных решений, что и первое уравнение.

Пример 2. Рассмотрим систему двух уравнений

$$\begin{cases} x_1 + \dots + x_n = 1, \\ \sum_{j < k} x_j x_k = 0. \end{cases}$$

Двоичные решения первого уравнения имеют вид $(0, \dots, 0, 1, 0, \dots, 0)$, где ровно одна переменная равна единице, а прочие равны нулю. Каждое из них служит решением второго уравнения.

Пример 3. Рассмотрим систему двух уравнений

$$\begin{cases} x_1 + \dots + x_n = 2, \\ x_1 x_2 + x_2 x_3 + \dots + x_{n-1} x_n = 0. \end{cases}$$

Двоичные решения первого уравнения таковы, что ровно две переменные равны единице. Число таких решений равно $n(n-1)/2$. Двоичное решение первого уравнения служит решением второго уравнения при условии, что равные единице переменные не оказались соседними. Поэтому число избыточных двоичных решений первого уравнения равно $n-1$.

ЛИТЕРАТУРА

1. *Seliverstov A. V.* Binary solutions to some systems of linear equations // OPTA 2018. Communications in Computer and Information Science. V.871. Cham: Springer, 2018. P.183–192. https://doi.org/10.1007/978-3-319-93800-4_15
2. *Схрейвер А.* Теория линейного и целочисленного программирования. Т. 2. М.: Мир, 1991. 344 с.
3. *Смолев В. В.* Об одном подходе к решению булевого линейного уравнения с целыми положительными коэффициентами // Дискретная математика. 1993. Т. 5. № 3. С. 81–89.
4. *Gál A., Jang J.-T., Limaye N., et al.* Space-efficient approximations for Subset Sum // ACM Trans. Computation Theory. 2016. V. 8. No. 4. Article 16. <https://doi.org/10.1145/2894843>
5. *Bringmann K.* A near-linear pseudopolynomial time algorithm for subset sum // SODA'17 Proc. Twenty-Eighth Ann. ACM-SIAM Symp. on Discrete Algorithms. Philadelphia: SIAM, 2017. P. 1073–1084.
6. *Koiliaris K. and Xu C.* A faster pseudopolynomial time algorithm for subset sum // SODA'17 Proc. Twenty-Eighth Ann. ACM-SIAM Symp. on Discrete Algorithms. Philadelphia: SIAM, 2017. P. 1062–1072.
7. *Bateni M. H., Hajiaghayi M. T., Seddighin S., and Stein C.* Fast algorithms for knapsack via convolution and prediction // Proc. 50th Ann. ACM SIGACT Symp. on the Theory of Computing (STOC'18). N.Y.: ACM, 2018. P. 1269–1282. <https://doi.org/10.1145/3188745.3188876>
8. *Curtis V. V. and Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem // Europ. J. Operat. Res. 2019. V. 275. P. 460–466. <https://doi.org/10.1016/j.ejor.2018.11.055>
9. *Cygan M., Mucha M., Węgrzycki K., and Włodarczyk M.* On problems equivalent to $(\min, +)$ -convolution // ACM Trans. Algorithms. 2019. V. 15. No. 1. Article 14. <https://doi.org/10.1145/3293465>
10. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694. [https://doi.org/10.1016/S0021-8693\(03\)00167-4](https://doi.org/10.1016/S0021-8693(03)00167-4)
11. *Рыбалов А. Н.* О генерической сложности проблемы разрешимости систем диофантовых уравнений в форме Сколема // Прикладная дискретная математика. 2017. № 37. С. 100–106.
12. *Рыбалов А. Н.* О генерической NP-полноте проблемы выполнимости булевых формул // Прикладная дискретная математика. 2017. № 36. С. 106–112.
13. *Рыбалов А. Н.* Релятивизованные генерические классы P и NP // Прикладная дискретная математика. 2018. № 40. С. 100–104.
14. *Lyubetsky V. A., Gershgorin R. A., and Gorbunov K. Yu.* Chromosome structures: reduction of certain problems with unequal gene content and gene paralogs to integer linear programming // BMC Bioinformatics. 2017. V. 18. No. 40. <https://doi.org/10.1186/s12859-017-1944-x>
15. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27. No. 4. P. 701–717. <https://doi.org/10.1145/322217.322225>
16. *Bacher A., Bodini O., Hwang H.-K., and Tsai T.-H.* Generating random permutations by coin-tossing: classical algorithms, new analysis, and modern implementation // ACM Trans. Algorithms. 2017. V. 13. No. 2. Article 24. <https://doi.org/10.1145/3009909>

REFERENCES

1. *Seliverstov A. V.* Binary solutions to some systems of linear equations. OPTA 2018. Communications in Computer and Information Science, vol.871, Cham, Springer, 2018, pp.183–192. https://doi.org/10.1007/978-3-319-93800-4_15
2. *Schrijver A.* Theory of Linear and Integer Programming. N.Y., John Wiley and Sons, 1986.
3. *Smolev V. V.* On an approach to the solution of a Boolean linear equation with positive integer coefficients. Discrete Mathematics and Applications, 1993, vol. 3, no. 5, pp. 523–530. <https://doi.org/10.1515/dma.1993.3.5.523>
4. *Gál A., Jang J.-T., Limaye N., et al.* Space-efficient approximations for subset sum. ACM Trans. Computation Theory, 2016, vol. 8, no.4, article 16. <https://doi.org/10.1145/2894843>
5. *Bringmann K.* A near-linear pseudopolynomial time algorithm for subset sum. SODA'17 Proc. Twenty-Eighth Ann. ACM-SIAM Symp. on Discrete Algorithms, SIAM, Philadelphia, 2017, pp. 1073–1084.
6. *Koiliaris K. and Xu C.* A faster pseudopolynomial time algorithm for subset sum. SODA'17 Proc. Twenty-Eighth Ann. ACM-SIAM Symp. on Discrete Algorithms, SIAM, Philadelphia, 2017, pp. 1062–1072.
7. *Bateni M. H., Hajiaghayi M. T., Seddighin S., and Stein C.* Fast algorithms for knapsack via convolution and prediction. Proc. 50th Ann. ACM SIGACT Symp. on the Theory of Computing (STOC'18), N.Y., ACM, 2018, pp.1269–1282. <https://doi.org/10.1145/3188745.3188876>
8. *Curtis V. V., and Sanches C. A. A.* An improved balanced algorithm for the subset-sum problem. Europ. J. Operat. Res., 2019, vol. 275, pp. 460–466. <https://doi.org/10.1016/j.ejor.2018.11.055>
9. *Cygan M., Mucha M., Węgrzycki K., and Włodarczyk M.* On problems equivalent to $(\min, +)$ -convolution. ACM Trans. on Algorithms, 2019, vol. 15, no. 1, article 14. <https://doi.org/10.1145/3293465>
10. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks. J. Algebra, 2003, vol. 264, no. 2, pp. 665–694. [https://doi.org/10.1016/S0021-8693\(03\)00167-4](https://doi.org/10.1016/S0021-8693(03)00167-4)
11. *Rybalov A. N.* O genericheskoy slozhnosti problemy razreshimosti sistem diofantovykh uravneniy v forme Skolema [On generic complexity of decidability problem for Diophantine systems in the Skolem's form]. Prikladnaya Diskretnaya Matematika, 2017, no. 37, pp. 100–106. (in Russian)
12. *Rybalov A. N.* O genericheskoy NP-polnote problemy vpolnimosti bulevykh formul [On generic NP-completeness of the Boolean satisfiability problem]. Prikladnaya Diskretnaya Matematika, 2017, no. 36, pp. 106–112. (in Russian)
13. *Rybalov A. N.* Relyativizovannye genericheckie klassy P i NP [Relativized generic classes P and NP]. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 100–104. (in Russian)
14. *Lyubetsky V. A., Gershgorin R. A., and Gorbunov K. Yu.* Chromosome structures: reduction of certain problems with unequal gene content and gene paralogs to integer linear programming. BMC Bioinformatics, 2017, vol. 18, no. 40. <https://doi.org/10.1186/s12859-017-1944-x>
15. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities. J. ACM, 1980, vol. 27, no. 4, pp. 701–717. <https://doi.org/10.1145/322217.322225>
16. *Bacher A., Bodini O., Hwang H.-K., and Tsai T.-H.* Generating random permutations by coin-tossing: classical algorithms, new analysis, and modern implementation. ACM Trans. Algorithms, 2017, vol. 13, no. 2, article 24. <https://doi.org/10.1145/3009909>