

Множество $S \subset \mathbb{N}_0 := \{0, 1, 2, 3, \dots\}$ называется 2-автоматным если существует конечный автомат, распознающий язык двоичных записей чисел из S . Например, 2-автоматны множества всех степеней двоек, всех чётных чисел и всех чисел, в двоичной записи которых нечётное число единиц, но не 2-автоматны множества всех степеней троек, всех точных квадратов и всех простых чисел.

Пусть \mathbb{F}_2 — поле из двух элементов, а $\mathbb{F}_2[t]$ и $\mathbb{F}_2[[t]]$ — кольца многочленов и формальных степенных рядов над \mathbb{F}_2 соответственно. Формальный степенной ряд $\sum_{n=0}^{+\infty} f_n t^n = f \in \mathbb{F}_2[[t]]$ называется алгебраическим, если он является корнем какого-нибудь ненулевого многочлена с коэффициентами из $\mathbb{F}_2[t]$. Например, алгебраичны решения уравнений $f^2 + f + t = 0$, $(1+t)f + t^4 = 0$, $(t^2 + t + 1)f^3 + (t^4 + t)f + t^8 = 0$ из кольца $\mathbb{F}_2[[t]]$ формальных степенных рядов над полем \mathbb{F}_2 .

Theorem 0.1 (Теорема Кристеля). *Формальный степенной ряд $\sum_{n=0}^{+\infty} f_n t^n$ алгебраичен тогда и только тогда, когда множество $\{n \mid f_n = 1\} \subset \mathbb{N} \cup \{0\}$ 2-автоматно.*

План доказательства 2-автоматности каждого алгебраического степенного ряда.

- 1) В определении 2-автоматности, можно считать, что распознаются развёрнутые двоичные записи чисел из S . (то есть читаем от младших разрядов к старшим).
- 2) $(f + g)^2 = f^2 + g^2$ в $\mathbb{F}_2, \mathbb{F}_2[t]$ и $\mathbb{F}_2[[t]]$ — будем этим нагло пользоваться.
- 3) Введём операцию Λ_r для $r = 0, 1$ на подмножествах \mathbb{N}_0 и на элементах $\mathbb{F}_2[[t]]$: $\Lambda_r(S) := \{n \mid n \in \mathbb{N}_0, 2n + r \in S\}$ (эта операция соответствует “прочитыванию” цифры r в терминах правых контекстов. Аналогично для любого $f \in \mathbb{F}_2[[t]]$ существуют и единственны такие $f_0, f_1 \in \mathbb{F}_2[[t]]$, что $f = f_0^2 + t f_1^2$. Определим $\Lambda_r(f) := f_r$. Это как раз соответствует прочитыванию цифры r в терминах 2-автоматных множеств.
- 4) Теперь, чтобы доказать 2-автоматность алгебраического ряда $f \in \mathbb{F}_2[[t]]$, достаточно предъявить конечное множество Q степенных рядов, замкнутое относительно операций Λ_0 и Λ_1 и содержащее f .
- 5) Любой алгебраический степенной ряд — корень уравнения вида $p_0 f^{2^0} + p_1 f^{2^1} + \dots + p_n f^{2^n} = 0$, где $n \in \mathbb{N}$, а $p_i \in \mathbb{F}_2[t]$ и не все равны 0 (какая-то алгебра).
- 6) Не сильно умаляя общности, можно считать, что $p_0 = 1$ (какая-то алгебра). Тогда утверждается, что для достаточно большого d (d зависит от степеней p_i) подойдёт множество всех формальных степенных рядов вида $q_0 f^{2^0} + q_1 f^{2^1} + \dots + q_n f^{2^n}$, где каждое q_i независимо пробегает множество всех многочленов над \mathbb{F}_2 степени не больше d (их всего 2^{d+1} штук — конечное число).
- 7) GGWP. В другую сторону я не успел толком рассказать на паре.

□