Библиографический список

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / пер. с англ. В. Б. Афанасьева. – М.: Техносфера, 2006. – 320 с.

УДК 004(063)

Машины Тьюринга, сложность и случайность

А.Н. Гамова, А.С. Платонов
СГУ, г. Саратов

Машины Тьюринга бывают детерминированными и недетерминированными. Собственно вычисления происходят на детерминированных машинах Тьюринга, недетерминированные машины чаще используются для подтверждения разрешимости проблемы (распознавания языка). Модель вычислений на недетерминированной машине Тьюринга восходит к идеям Х. Эверетта о многозначности мира. Для недетерминированной машины Тьюринга это означает существование нескольких команд с одинаково левой частью и разными правыми частями. На каждой развилке дерева вычислений недетерминированной машины Тьюринга мир разбивается на несколько новых миров, в каждом из которых это событие заканчивается по-своему. Если произошло допускание на одной из веток дерева вычислений, работа недетерминированной машины заканчивается. Для того, чтобы машина не допустила входную строку, необходимо, чтобы это случилось на каждой ветке. Рассмотрим феномен проявления недетерминированности на примере задачи о рюкзаке.

Постановка задачи: В комнате находится N предметов разной массы и стоимости. Требуется заполнить ими рюкзак, максимизируя их суммарную стоимость, при условии, что общая масса предметов не больше заданного целого числа K.

Алгоритм:
итоговая стоимость = сумме стоимостей всех предметов в комнате;
ЦИКЛ
недетерминированный блок
масса ← 0, стоимость ←0;
ЦИКЛ выйти_или_не_выйти из цикла;
взять предмет из комнаты и поместить его в рюкзак;
масса ← масса + масса предмета;
стоимость ← стоимость + стоимость предмета;

если комната пуста, выйти из цикла;
конец цикла;

если стоимость = итоговой стоимости и масса <= *K*,

напечатать ответ: множество предметов рюкзака;

завершить работу программы;

конец блока

пока итоговая стоимость >= 0;

сообщить, что решение не существует.

Недетерминированность проявляется в строке «выйти_или_не_выйти из цикла». Здесь в одном мире происходит выход из цикла, в другом – выполнение тела цикла продолжается. «Взять предмет из комнаты» означает получить столько миров, сколько осталось предметов в комнате. В каждом из миров осуществляется свой собственный перебор. Если решение существует, оно будет найдено в одном из миров (на одной из веток вычисления недетерминированной машины).

Если оценивать время работы недетерминированного алгоритма, решающего задачу о рюкзаке, то внешний цикл программы выполнится не более $C*N$ раз, где C – верхняя граница стоимости каждого предмета, внутренний – не более N раз. Итоговая сложность недетерминированного алгоритма $O(C*N^2)$ или $O(N^2)$, т.е. полиномиальная.

Внутри класса разрешимых проблем существует своя собственная классификация сложности, называемая теорией сложности. Здесь детерминированные и недетерминированные машины Тьюринга, решающие проблему за полиномиальное время, попадают в разные классы. Класс проблем, решаемых детерминированной машиной Тьюринга за полиномиальное время, называется классом с полиномиальной сложностью P, соответственно, решаемых недетерминированной машиной Тьюринга за полиномиальное время, – классом NP, экспоненциальных проблем. Очевидно, что разрешимые проблемы, решаемые недетерминированными машинами Тьюринга за полиномиальное время, можно промоделировать с помощью детерминированных машин за счет увеличения сложности.

Возвращаясь к задаче о рюкзаке, решим ее в реальном времени, т.е. с помощью детерминированной машиной Тьюринга. Придется сделать $O(2^N)$ операций. Такие проблемы образуют класс NP, экспоненциальных задач. Для выявления других экспоненциальных проблем применяется метод полиномиального сведения. Суть метода в том, что с помощью некоторого алгоритма из класса P входные параметры задачи A преобразуются во входные данные задачи B, а затем результат, полу-

ченный при решении задачи B, снова полиномиально сводится к выходу задачи A. Проблема B не проще проблемы A.

Метод сводимости, применяемый в математической логике для доказательства неразрешимости проблем, существенно отличается от метода сводимости в теории сложности вычислений. Доказательство неразрешимости проблем основано на общих математических принципах: понятии алгоритма и формальной системы. Утверждение о труднорешаемости проблемы опирается на недоказанный принцип, что $P \neq NP$ и тот факт, что для всех труднорешаемых проблем не известно ни одной детерминированной машины Тьюринга, решающей эту проблему за полиномиальное время. В противном случае, используя полиномиальную сводимость проблем из класса NP, можно было бы доказать равенство классов P и NP. Сама же сводящая функция не просто алгоритмически вычислима, но должна иметь полиномиальный алгоритм, чтобы не переносить свою сложность на проблему, к которой с ее помощью сводится известная труднорешаемая проблема. Подкласс класса NP, образованный проблемами, к которым полиномиально сводится любая проблема из класса NP, составляют архи-сложные проблемы, называемые NP-полными.

Интересна сама природа сложности. Даже основанный на простых принципах механизм может вести себя очень сложно. Возьмем в качестве примера одномерный клеточный автомат, представленный бесконечной в обе стороны лентой, с черными или белыми клетками. Изменение цвета клетки на очередном шаге определяется цветом ее соседей на предыдущем шаге и задается, и полностью описывается, восемью правилами. Правила, по которым происходит изменение окраски ленты, на первый взгляд просты и мало отличаются друг от друга. Однако один набор правил порождает последовательность с выраженными закономерностями (рис. 1–2), другой – архи-сложную последовательность (рис. 3). Распознать близость последовательности к архи-сложным (случайным) можно только через присущие им закономерности.

Интуитивно ясно, что «архи-сложные последовательности» ведут себя как случайные, а случайность есть отсутствие закономерностей. «Не случайными» считаются последовательности, в которых много закономерностей. Под закономерностью понимается любое проверяемое свойство последовательности, присущее лишь узкому классу последовательностей. Более точное определение закономерности – степень организованности, которую более естественно характеризовать сложностью алгоритма, позволяющего восстанавливать последова-

тельно удлиняющиеся начальные отрезки бесконечной последовательности. П. Мартин-Лефом предложена теория проверки последовательности «на случайность» через выполнимость законов теории вероятности (тесты на случайность). Если какой-то тест не пройден, эта закономерность присуща данной последовательности, так что она не случайная.

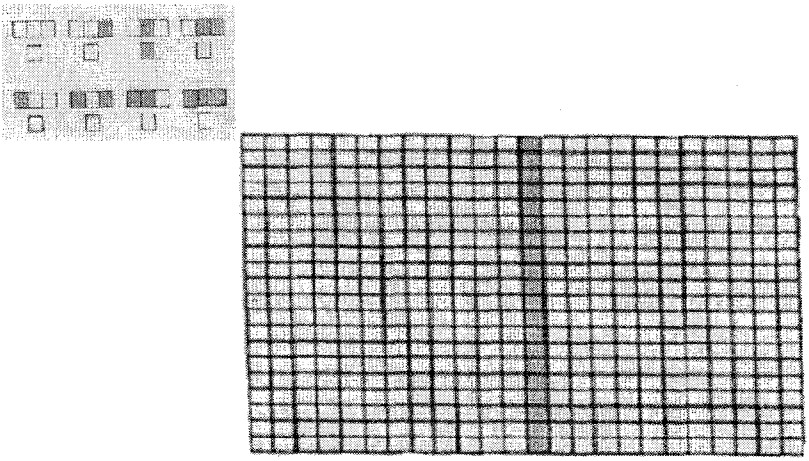

Рис. 1

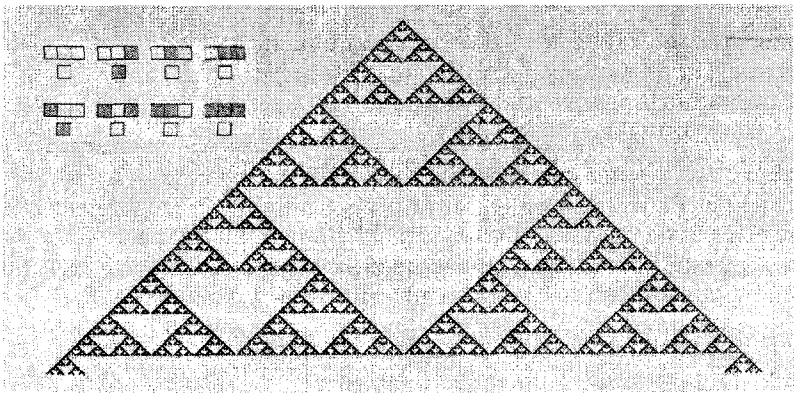

Рис. 2

Если по полученным на рисунках последовательностям попробовать подобрать порождающие их правила перехода, то это вряд ли удастся для последней последовательности, разве только путем полного перебора возможных правил. Последнее указывает на принадлежность обратной функции к классу *NP*. Произвольная сложная проблема из класса *NP* не обязана быть труднорешаемой, т.е. *NP*-полной. Аналогично, только последовательность, выдержавшая все тесты, является случайной.

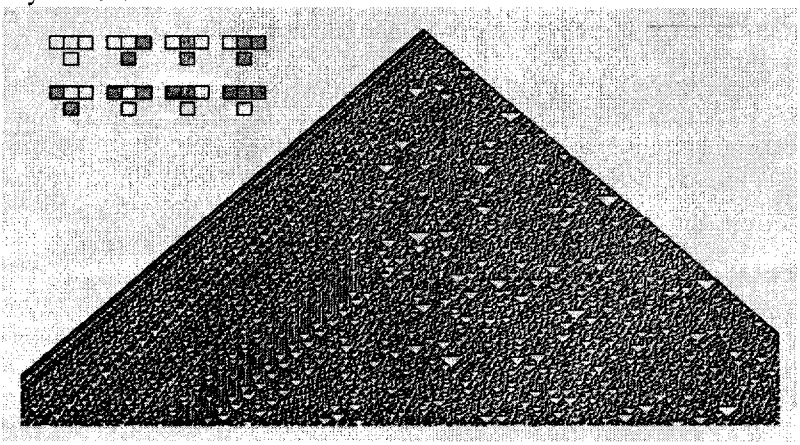

Рис. 3

Применительно к криптографии последовательность на рисунке 3 дает пример односторонней функции.

Библиографический список

1. Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений / пер. с англ. – 2-е изд. – М.-СПб.-Киев: Изд. дом «Вильямс», 2002.– 528 с.

2. Martin-Lof P. The definition of random sequences // Information and Control, 9 (1966), 602-619.