ЛЕКЦИЯ 14

#Р-ПОЛНЫЕ ЗАДАЧИ

1. Проблема сводимости

Полная задача в некотором классе — это задача, которая сама лежит в этом классе, причем к ней сводится любая другая задача. Но не совсем понятно, что значит сводимость в терминах класса #P. Этот класс отличается от остальных тем, что это класс не задач распознавания, а поиска (ответом будет число), поэтому в этом случае будет трудно корректно определить сводимость по Карпу. Вместо этого будем использовать сводимость по Куку (то есть использование оракула).

Определение 50: *Задача подсчета f является #**P-полной**, если верны следующие свойства:*

1. *f есть количество всех подходящих сертификатов для верификатора.*

   Верификатор получает два аргумента: тот же, что и у f, и сертификаты.

2. *С использованием f в качестве оракула можно решить любую задачу из #P за полиномиальное время.* ♣

Данное определение выражает сводимость по Куку (то есть возможность использовать задачу в качестве оракула).

Теорема 26 Пусть f — #P-полная, $f \in \mathrm{FP}$ (f вычисляется за полиномиальное время). Тогда $\mathrm{FP} = \#\mathrm{P}$. $*$

Док-во: Каждый вызов f в качестве оракула можно заменить вычислением ответа. Вызов полиномиальной процедуры полиномиальное число раз даст полиномиальное время работы.

Теорема 27 Задача из #SAT является #P-полной. $*$

Док-во: Конструкция доказательства этой теоремы аналогична конструкции доказательства теоремы Кука–Левина за исключением того, что количество подходящих сертификатов будет переводиться в количество выполняющих наборов.

2. Задача вычисления перманента

Для любой матрицы A определено понятие **детерминанта**:

$$\det A = \sum_{\sigma} (-1)^{\sigma} \prod_{i=1}^{n} A_{i,\sigma(i)}.$$

Для нахождения детерминанта можно воспользоваться приведением матрицы к ступенчатому виду. Соответствующий алгоритм будет полиномиальным ($\sim n^3$).

***Определение 51: Перманент** матрицы A:*

$$\mathrm{perm}(A) = \sum_{\sigma} \prod_{i=1}^{n} A_{i,\sigma(i)}.$$

Физический смысл детерминанта — ориентированный объём многомерного параллелепипеда, натянутого на соответствующие вектора. Перманент имеет комбинаторный смысл: пусть A — матрица, состоящая из 0 и 1. Тогда $\mathrm{perm}(A)$ — количество совершенных паросочетаний в двудольном графе, заданным этой матрицей (**совершенное паросочетание** — это паросочетание из n ребер; все вершины в этом случае разбиты на пары, соединенные ребрами).

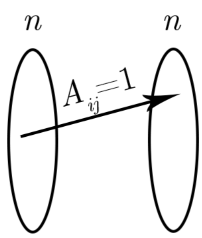

Рис. 14.1

Если значение перманента отлично от нуля, то существует такое σ, что все вершины i соединены с σ ребром, которое образует паросочетания. И наоборот: каждое совершенное паросочетание соответствует некоторому единичному слагаемому в сумме в формуле для перманента.

По набору паросочетаний можно проверить, лежит ли $\mathrm{perm}(A)$ в #P или нет. Существует алгоритм, который позволяет выявить наличие паросочетаний. По **теореме Холла о паросочетаниях** (паросочетания существуют тогда и только тогда, когда из любого подмножества левой доли множество его соседей больше, чем само множество) нельзя непосредственно построить этот алгоритм.

Проверка наличия паросочетаний есть полиномиальная задача, а подсчет их количества — #P-полная задача.

3. Целочисленная интерпретация перманента

Можно рассматривать любые целочисленные значения в матрице A, а не только 0 или 1.

Определение 52: *Пусть задан полный ориентированный граф на n вершинах с целочисленными весами ребер. Тогда* **перманент** *есть суммарный вес циклических покрытий. Каждой перестановке σ соответствует разбиение вершин на циклы, и этому весу будет соответствовать произведение всех весов на всех ребрах* ($\mathrm{perm}(A)$ *— сумма весов всех циклических разбиений).* ♣

Теорема 28 Задача нахождения $\mathrm{perm}(A)$ является #P-полной. ∗

Док-во: Сведём #SAT к перманенту на целых числах, а затем перманент на целых числах — к перманенту на 0 и 1.

1 часть.

По формуле ϕ построим граф $\phi \to G$ — взвешенный полный ориентированный граф, такой что

$$\mathrm{perm}(G) = 4^{3m} \# \phi,$$

где $\#\phi$ — количество выполняющих наборов, m — число скобок.

Если ребро не рисуется в следующих схемах для гаджетов, то его вес равен нулю. Если рисуется, но не подписывается, то его вес равен единице.

Будем использовать следующую конструкцию **гаджета для переменной**:

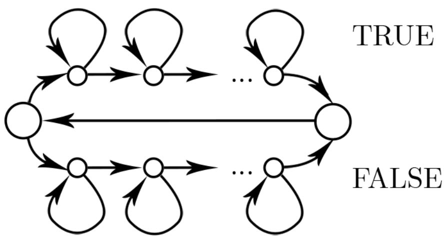

Рис. 14.2

Крайние точки в этом гаджете больше нигде не фигурируют.

Если представить этот гаджет изолированным от любых других, то в таком случае будут существовать всего два способа покрыть его циклами. Они будут соответствовать значениям 1 и 0 (TRUE и FALSE).

Для **гаджета для скобки** будем использовать следующую конструкцию:

Считаем, что все формулы лежат в 3-КНФ, т. е. все скобки содержат по три литерала.

Если в разбиении на циклы есть все три ребра, то вес центра равен нулю (потому что из вершины в этом случае нельзя никуда попасть). Для любых остальных случаев есть только одно разбиение этого графа.

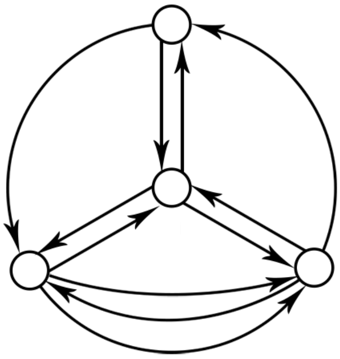

Рис. 14.3

Теперь рассмотрим **XOR-гаджет**. Нужно изменить ребра $u \to u'$ и $v \to v'$, чтобы из этих ребер в любом циклическом покрытии с неизменным весом обязательно было ровно одно.

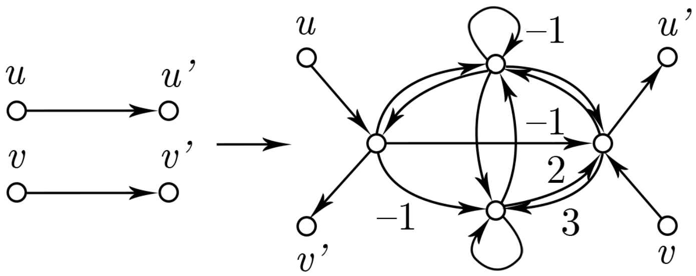

Рис. 14.4

Из конструкции этого графа следует, что при подключении к другим гаджетам он будет давать четырехкратное увеличение веса.

XOR-гаджет подключается к петлям гаджета для переменной и к внешним ребрам гаджета для скобки (при этом кратность гаджета для скобки исчезает).

Рассмотрим конструкцию для скобки $(x \wedge \overline{y} \wedge z)$.

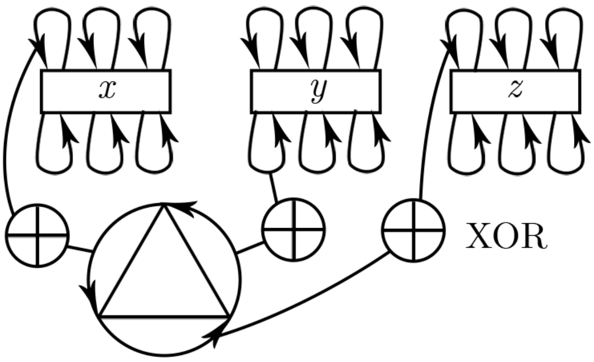

Рис. 14.5

Если набор не выполняющий, то вес будет равен нулю. Если выполняющий, то каждый XOR будет давать умножение на 4 (внутри гаджетов для переменной и скобок вес равен единице). Всего XOR'ов $3m$. Таким образом, суммарный вклад будет равен 4^{3m}.

2 часть.

Теперь переведем целочисленные значения в {0,1}. Если необходимо представить степени числа 2, то можно воспользоваться схемами, представленными ниже.

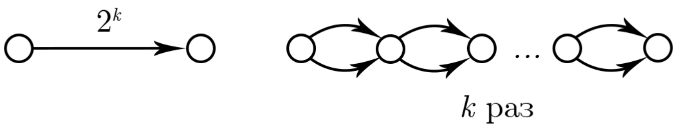

Рис. 14.6

Для избавления от кратных вершин можно воспользоваться конструкцией из ромбов.

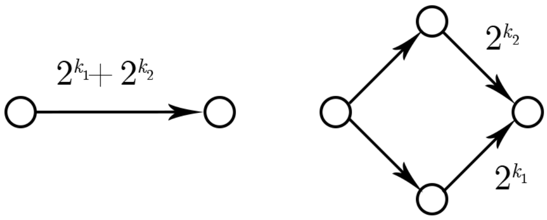

Рис. 14.7

Значение перманента лежит в интервале $[-n!\,, n!\,]$. Посчитаем остаток по модулю числа $m \gg 2n!$. Тогда все веса тоже можно считать по этому модулю:

$$-1 \to m - 1,$$

а с $m - 1$ провести такую же процедуру. В результате получится, что все веса лежат в {0,1}.