**Арифметические схемы**

В теории вычислительной сложности **арифметические схемы** представляют собой стандартные модели, описывающие вычисления полиномов. Они позволяют определить наиболее эффективный способ вычисления соответствующего полинома.

**Определение 1.** Арифметической схемой C над полем Fи множеством переменных X = { x1, … , xn } называется направленный ациклический граф, обладающий следующими свойствами:

* каждый узел графа с полустепенью входа 0 называется входным гейтом и помечается либо переменной xi, либо элементом поля F;
* все остальные узлы, называемые гейтами, помечаются символами операций «+» (sum gate) или «\*» (product gate).

Каждая схема обладает двумя основными метриками сложности – размером и глубиной. **Размером арифметической схемы** C называется ее общее число гейтов |C|. **Глубиной** **арифметической схемы C** называется длина максимального пути в схеме depth(C). **Глубиной гейта v** называется максимальная длина пути до v (depth(v)).

Необходимо также отметить, что арифметическая схема всегда рассматривается как способ вычисления полинома в F[X], а не функции из F|X| в F. В общем случае каждый полином определяет уникальную функцию, но функция обычно может быть выражена с помощью нескольких различных полиномов.

**Оптимизация вычисления полиномов с помощью арифметических схем**

Поиск решения данной задачи для некоторого полинома f состоит из двух этапов:

* **Ограничение сверху** – на данном этапе осуществляется поиск схемы, вычисляющей f;
* **Ограничение снизу** – вторым этапом выполняется доказательство того, что данная схема вычисления является оптимальной для выбранного полинома f, т. е. что данная схема имеет минимально возможные значения параметров размера и глубины.