Резензия к материалам на тему "Reading MCSP throught SAT"

21 февраля 2019 г.

В качестве источника используются презентация "Reading **MCSP** throught **SAT**"(Rahul Santhanam [University of Oxford]).

1 Основная постановка задачи MCSP

Пусть дана булева функция, представленная таблицей истинности, а также параметр s, не превосходящий размра таблицы. Вопрос, на который нужен ответ: есть ли для данной функции схема, не препосходящая s.

2 Освещаемые темы

Важные вопросы, затрагиваемые статьей:

1. Сравнение задач **MCSP** и **SAT**;
2. Сложность доказательства NP-полноты **MCSP**;
3. Сложность доказательства полиномиальности **MCSP**;

3 Основные определения и результаты

Утв. Любая булева функция от n переменных имеет схему размера $O(2^n)$.
Утв. Для большинства булевых функций, сложность схемы по крайней мере $\Omega(2^n/10n)$.
Опр. Пусть есть задача L, тогда явной конструкцией будем называть задачу: найти $X_n \in L$, такой что $|X_n| = n$.
Утв. Пусть **MCSP** - NP-полная, и есть естественная сводимость **SAT** к **MCSP**, а также NP не содержится в **SUBEXP**, тогда разрешима основная проблема схемной сложности.
Опр. $(AC)^o$ - язык, распознаваемый булевой схемой глубины $O(log(n))$.
Опр. BPP - класс сложности предикатов, вычилимых за полиномиальное время с ошибкой не более 1/3.
Опр. ZPP - класс сложности предикатов, вычилимых в среднем за полиномиальное время безошибочно.
Утв. MCSP $\subseteq$ **P** $\Rightarrow$ **BPP** $\subseteq$ **ZPP**.

4 Заключение

Основной мотив изучать эти вопросы - естественность возникновения задачи **MCSP**, а также связь с криптографией, вопросами сложности. Приводятся рассуждения, иллюстрирующие трудность ответа на поставленные вопросы.