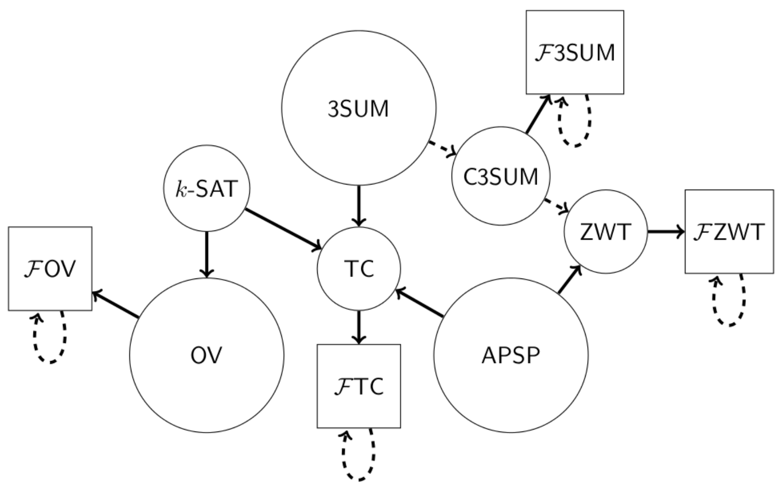
Average-Case Fine-Grained Hardness

Marshall Ball, Alon Rosen, Manuel Sabin, Prashant Nalini Vasudevan

Randomized Algorithms

1. *Worst case* – outputs a correct answer for every input with a probability at least 2/3.
2. *Average case* – outputs a correct answer with a probability 2/3 over an uniform distribution of inputs.

Problems



SETH For every $\varepsilon > 0$ there is k such that there is no algorithm for k-SAT running in time $2^{(1-\varepsilon)n}$.

OV Given two sets U, V of n vectors from $0, 1^d$, decide whether there exist $u \in U$ and $v \in V$ such that $\langle u, v \rangle = 0$ (over $\mathbb{Z}$), $d \in O(\log n)$.

3SUM Given a set $S \subset \{-n^3, \ldots, n^3\}$ of size n, decide if there exist distinct $a, b, c \in S$ such that $a + b = c$.

C3SUM Given three n-element arrays, A, B, and C, with entries in $\{-n^3, \ldots, n^3\}$, decide whether exist $i, j \in [n]$ such that $A[i] + B[j] = C[i + j]$.

APSP Find distance between every pair of vertices in a weighted graph $G = (V, E), w : E \to [n^c]$ for some sufficiently large c.

ZWT Given a weighted graph $G = (V, E), w : E \to [n]$, decide whether there exists a triangle with edge weights w_1, w_2, w_3 such that $w_1 + w_2 + w_3 = 0$.

TC Given a vertex-colored graph $G = (V, E), C : V \to [k]$, decide whether for each triple of three colors $a, b, c \in [k]$ there exists vertices $x, y, z \in V$ that form a triangle and $C(x) = a, C(y) = b$, and $C(z) = c$.

$\mathcal{F}$P Polynomial representation of a problem P.

Problems	No Algo in Time
SAT	$2^{(1-\varepsilon)n}$
OV, 3SUM, C3SUM	$n^{2-\varepsilon}$
APSP, ZWT, TC	$n^{3-\varepsilon}$

Main Tool

Strategy: Represent problems as polynomials and use the following lemma for reduction from the average case to the worst case.

Definition 1. A family of functions $\mathcal{F} = \{f_n\}$ is computable in time t on average if there is an algorithm that runs in $t(n)$ time on the domain of f_n and, for all large enough n, computes f_n correctly with probability at least 2/3 over the uniform distribution of inputs in its domain.

Lemma 2. *Consider positive integers n, d, and p, and an $\varepsilon \in (0, 1/3)$ such that $d > 9, p$ is prime and $p > 12d$. Suppose that for some polynomial $f : \mathbb{Z}_p^n \to \mathbb{Z}_p$ of degree d, there is an algorithm A running in time t such that:*

$$\Pr_{x \in \mathbb{Z}_p^n}[A(x) = f(x)] \geq 1 - \varepsilon$$

Then there is a randomized algorithm B that runs in time $O(nd^2 \log^2 p + d^3 + tD)$ such that for any $x \in \mathbb{Z}_p^n$:

$$\Pr[B(x) = f(x)] \geq \frac{2}{3}$$