

The Problems

SUBSET-SUM

Input: Multiset $\{a_1, \dots, a_n\}$ and target m

Output: $S \subseteq \{1, \dots, n\}$ such that $\sum_{i \in S} a_i = m$

SHIFTED-SUMS

Input: Multiset $\{a_1, \dots, a_n\}$ and shift s

Output: $S_1 \neq S_2 \subseteq \{1, \dots, n\}$ s.t. $\sum_{i \in S_1} a_i + s = \sum_{i \in S_2} a_i$

Special cases of **SHIFTED-SUMS**:

EQUAL-SUMS

Input: Set $\{a_1, \dots, a_n\}$

Output: $S_1 \neq S_2 \subseteq \{1, \dots, n\}$ s.t. $\sum_{i \in S_1} a_i = \sum_{i \in S_2} a_i$

PIGEONHOLE EQUAL-SUMS

Input: Set $\{a_1, \dots, a_n\}$ s.t. $\sum_{i=1}^n a_i < 2^n - 1$

Output: $S_1 \neq S_2 \subseteq \{1, \dots, n\}$ s.t. $\sum_{i \in S_1} a_i = \sum_{i \in S_2} a_i$

Known Results

Classical results:

- **SUBSET-SUM** $\in \tilde{O}(2^{n/2})$ [HS'74] Meet in the Middle
- **SUBSET-SUM** $\in \tilde{O}(n + m)$ [Bri'17]
- **SETH** $\Rightarrow \forall \epsilon > 0, \exists \delta > 0, \text{SUBSET-SUM} \notin O(m^{1-\epsilon} 2^{n\delta})$ [ABHS'19]
- **EQUAL-SUMS** $\in \tilde{O}(3^{n/2}) \leq O(2^{0.793n})$ [Woe'08] MiM
- **EQUAL-SUMS** $\in O(2^{0.773n})$ [MNPW'19]

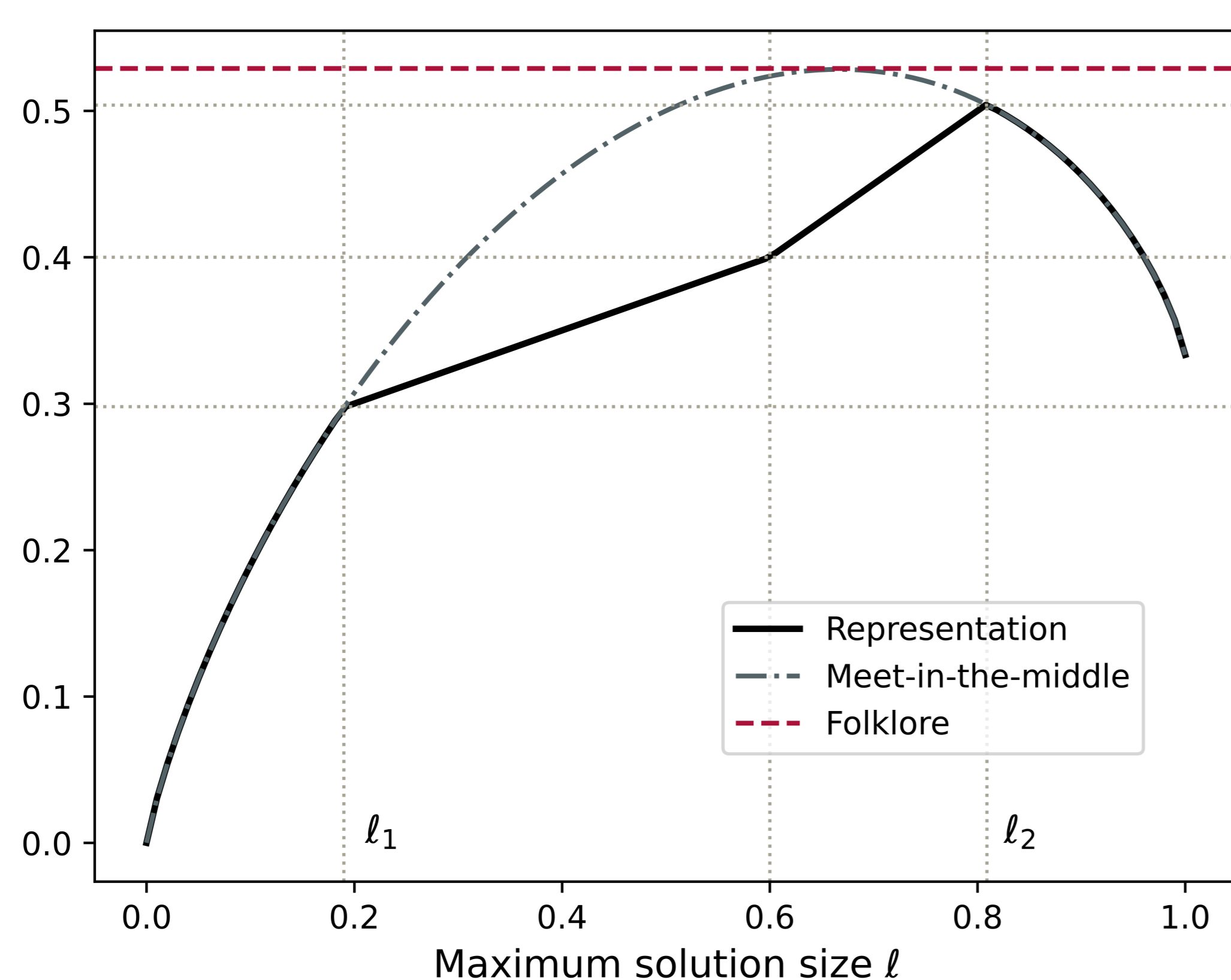
Quantum results:

- **SUBSET-SUM** $\in \tilde{O}(2^{n/3})$ [BJLM'13] MiM
- **EQUAL-SUMS** $\in \tilde{O}(3^{n/3}) \leq O(2^{0.529n})$ MiM

Our Results

	Classical	Quantum
SUBSET-SUM (not MiM)	$\tilde{O}(2^{n/2})$	$\tilde{O}(2^{n/3})$
SHIFTED-SUMS	$O(2^{0.773n})$	$O(2^{0.504n})$
PIGEONHOLE EQUAL-SUMS	$\tilde{O}(2^{n/2})$	$\tilde{O}(2^{2n/5})$

Quantum Shifted-Sums complexity



Dynamic Programming Datastructure

$$T_{p,k} = \left\{ S \subseteq \{1, \dots, n\} : \sum_{i \in S} a_i \equiv k \pmod{p} \right\}$$

1 - Compute the size $|T_{p,k}|$ by dynamic programming:

Let $t_p[i, j] = |\{S \subseteq \{1, \dots, i\} : \sum_{i \in S} a_i \equiv j \pmod{p}\}|$.

The table $t_p[i, j]$ can be constructed in time $O(np)$:

$$t_p[i, j] = t_p[i-1, j] + t_p[i-1, (j - a_i) \bmod p].$$

2 - Given random access to the table t_p , we construct an **oracle** that gives access to the elements of $T_{p,k}$ in time $O(n)$ (for a certain total order $<$ over $T_{p,k}$).

Main Ideas for Quantum SHIFTED-SUMS

Maximum solution size, $\ell \in (0, 1)$:

$$\ell n = \max \{ |S_1| + |S_2| : S_1, S_2 \text{ disjoint solutions} \}$$

Suppose that ℓ is known. Then:

- If $\ell < 0.190$ or $\ell > 0.809$, use **quantum MiM**.
- If $0.190 \leq \ell \leq 0.809$, use **representation technique**.

Example when $\ell = 3/5$:

- 1 - Choose a **random prime** $p \in \{2^{2n/5}, \dots, 2^{2n/5+1}\}$.
- 2 - Choose a **random index** $k \in [0, p-1]$.
- 3 - Search for a solution in $T_{p,k}$ using the **dynamic programming oracle** and Ambainis' **Collision Finding**.

→ Expected bin size $|T_{p,k}| \approx 2^{3n/5}$,

- Sufficiently **large** to contain a solution.
- Sufficiently **small** to keep the cost of search low: $\tilde{O}(2^{2n/5})$.

Additional ideas when $\ell < 3/5$:

- Choose $p \in \{2^{(1+\ell)n/4}, \dots, 2^{(1+\ell)n/4+1}\}$.
- **Multiple solutions** in a random $T_{p,k}$.
- New **faster** Collision Finding for multiple collisions.

Additional ideas when $\ell > 3/5$:

- Choose $p \in \{2^{2n/5}, \dots, 2^{2n/5+1}\}$.
- Solution in a random $T_{p,k}$ with **exp. small probability**.
- Use **Variable-Time Amplitude Amplification** to boost the success probability of sampling a good $T_{p,k}$.