Quantum Algorithms for Variants of Subset-Sum via Dynamic Programming

```
Team: hackHack
```

Link to the original paper

Jonathan Allcock, Yassine Hamoudi, Antoine Joux, Felix Klingelhöfer, Miklos Santha

Introduction

The **SUBSET-SUM** is the problem of deciding whether a given multiset of n integers has a subset whose elements sum to a target integer m.

Input : A Multiset $\{a_1, a_2, a_3 \dots a_n\}$ and a target value t.

Output : A Subset $S \subseteq [n]$ such that $\sum_{i \in S} a_i = m$

There are multiple variants to the SUBSET-SUM problem. We are primarily interested in the following

MODULAR SUBSET-SUM

Given a multiset $\{a_1, a_2, a_3 \dots a_n\}$ of positive integers, a target integer m and a modulus q, our task is to find a subset $S \subseteq [n]$ such that $\sum_{i \in S} a_i = m \bmod q$

Input : A Multiset $\{a_1, a_2 \dots a_n\}$ and a target value t and modulus q

Output : A Subset $S \subseteq [n]$ such that $\sum_{i \in S} a_i = m \bmod q$

SHIFTED-SUMS

Input : A Multiset $\{a_1, a_2 \dots a_n\}$ and a shift s

Output : $S_1 \neq S_2 \subseteq [n]$ such that $\sum_{i \in S_1} a_i + s = \sum_{i \in S_2} a_i$

EQUAL-SUMS

Similar to the SHIFTED-SUMS problem, with the assumption that $s = 0$, meaning that we are required to find two subsets, which sum up to the same value

PIGEONHOLE EQUAL-SUMS

Similar to the EQUAL-SUMS problem, with the assumption that $\sum_{i=1}^{n} a_i < 2^n - 1$. This restriction allows us to have atleast one guaranteed solution, by application of the pigeonhole principle.

Classical and Quantum Running Times for the variants

Problem	*Classical*	*Quantum*
SUBSET-SUMS	$2^{n/2}$	$2^{n/3}$
SHIFTED-SUMS	$2^{0.773n}$	$2^{0.504n}$
PIGEONHOLE-EQUAL-SUMS	$2^{n/2}$	$2^{2n/5}$

Goals

Our goal will be to implement the algorithms mentioned in the paper. These will involve the following prior techniques:

- Quantum search found as theorem 3 in
  M. Boyer, G. Brassard, P. Høyer, and A. Tapp. "Tight Bounds on Quantum Searching" (1998)
- Variable-time amplitude amplification found as theorem 2 in
  A. Ambainis. "Variable Time Amplitude Amplification and Quantum Algorithms for Linear Algeb
  in addition to novel ones such as the quantum pair finding algorithm (stated as Theorem 2.8 in the current work) and the usage of quantum representation technique for the previously listed problems.
  The paper proposes dynamic programming in order to implement low-cost oracle queries which we also aim to implement efficiently.

Overall, we hope to get a better understanding of the current work and state-of-the-art quantum algorithms designed to solve inherently hard and interesting problems. By providing a solid implementation of the current work, we hope to make positive progress in the field.