How to Efficiently Store Intermediate Results in Quantum Computing: Theoretical Explanation of the Current Algorithm

Oscar Galindo, Olga Kosheleva, and Vladik Kreinovich
University of Texas at El Paso
El Paso, Texas 79968, USA
ogalindomo@utep.edu, olgak@utep.edu, vladik@utep.edu
1. **Quantum Computing (QC) Is Inevitable**

- Modern computers are several orders of magnitude faster than in the past.
- However, for many practical problems, they are still too slow.
- For example, we can compute where a tornado will turn in the next 15 minutes.
- However, these computations will take several hours – too late for a warning.
- Why is it difficult to drastically speed up modern computers?
- According to relativity theory, all speeds are limited by the speed of light.
- For a usual laptop whose size is about 30 cm, it takes 1 nanosecond for light to pass through.
2. QC Is Inevitable (cont-d)

- During this time, even the cheapest 4 GHz central processing unit will already perform 4 operations.

- To make computations much faster, we thus need to make all the elements of the computer much smaller.

- These elements are already comparable to the size of molecules.

- The only way to make them even smaller is to have elements the size of a few molecules.

- At such sizes, we need to take into account quantum phenomena which are specific for the microworld.

- So, quantum computing – computing by using units that obey quantum laws – is inevitable.
3. Quantum Computing Is Desirable

- At first, quantum effects were viewed by computer engineers as a nuisance.
- We want the computer to produce the same desired result every time we ask for the same computation.
- However, in quantum physics, most outcomes are probabilistic – their outcome changes with repetition.
- Good news is that computer scientists came up with a way to utilize quantum effects so that:
  - we can actually compute several things with guarantee and
  - we can compute even faster than by using traditional non-quantum algorithms.
- The most widely known quantum algorithm of this type is Shor’s algorithm.
4. QC Is Desirable (cont-d)

- It enables us to factor large integers in polynomial time.
- Thus, in principle, we can decode all the messages sent by using the commonly used RSA encryption.
- The security of this encryption scheme is based on the fact that:
  - the only known non-quantum algorithms for factoring integers
  - would require astronomically large time to factor currently used 200-digit integers.
- Another is Grover’s algorithm for searching for an element in an un-sorted array of \( n \) elements.
- Non-quantum algorithm requires at least \( n \) steps – otherwise, it may miss the desired element).
5. QC Is Desirable (cont-d)

• Grover’s algorithm can find it much faster, in time $\sqrt{n}$.

• Most quantum algorithms – including Shor’s and Grover’s – remain probabilistic.

• They produce the correct result with probability close to 1.

• However, is a certain probability of a wrong result.

• To decrease this probability of the error, a natural idea is to repeat computations several times.

• If we want to retain the same computation time, we need to run several quantum processors in parallel:
  – if the probability that one processor errs is $p_0$,
  – then the probability that all $k$ parallel quantum processors err is $p_0^k$, i.e., much smaller.
6. Need to Store Intermediate Results

- The main motivation for using quantum computing is to solve complex problems.
- Their computation requires a lot of time.
- Often, when a problem is being solved, another higher-priority task appears; so:
  - the previous computation has to be interrupted,
  - the intermediate computation results have to be temporarily stored.
- In particular, this is needed for quantum algorithms.
- To decrease the probability of an error, we need to repeat computations in parallel.
- Thus, when an interrupt occurs, we need to store several copies of the same intermediate result.
7. What Exactly Do We Store

- The state of the usual (non-quantum) computer can be described as a sequence of bits.
- A bit is a simple element that can be only in two different states: 0 and 1.
- In quantum physics, for every two classical states, we can also have a superposition of these states:
  \[ a_0|0\rangle + a_1|1\rangle. \]
- Here \( a_0 \) and \( a_1 \) are complex numbers known as amplitudes for which \( |a_0|^2 + |a_1|^2 = 1 \).
- For the classical bit, we can measure its state: 0 or 1.
- If we measure the superposition:
  - we get 0 with probability \( |a_0|^2 \) and
  - we get 1 with probability \( |a_1|^2 \).
8. What Exactly Do We Store (cont-d)

- The probabilities of two possible outcomes should add up to 1.
- This explains the above constraint on the possible pairs \((a_0, a_1)\) of complex values.
- The state of several independent particles can be described by using a so-called tensor product \(\otimes\).
- The amplitude of each state of the 2-particle system is equal to the product of the corresponding amplitudes.
- This is just like the probability of having two outcomes in two independent events is equal to the product.
- Suppose that we have two identical particles in the state \(a_0|0\rangle + a_1|1\rangle\).
9. What Exactly Do We Store (cont-d)

• Then the state of the corresponding 2-particle system has the form

\[ a_0^2 |00\rangle + a_0 \cdot a_1 |01\rangle + a_1 \cdot a_0 |10\rangle + a_1^2 |11\rangle. \]

• This state is equal to

\[ a_0^2 |00\rangle + a_0 \cdot a_1 \cdot (|01\rangle + |10\rangle) + a_1^2 |11\rangle. \]

• Here, the sum \(|01\rangle + |10\rangle\) is not a state, since the sum of the squares of the coefficients is equal to 2.

• We can make it a state if we divide this sum by \(\sqrt{2}\).

• In terms of this state, we get the following expression:

\[ a_0^2 |00\rangle + \sqrt{2} \cdot a_0 \cdot a_1 \cdot \left( \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle \right) + a_1^2 |11\rangle. \]
10. What Exactly Do We Store (cont-d)

- If we have three identical particles, then we similarly get the state

\[ a_0^3|000\rangle + a_0^2 \cdot a_1(|001\rangle + |010\rangle + |100\rangle) + \\
\]

\[ a_0 \cdot a_1^2(|011\rangle + |101\rangle + |110\rangle) + a_1^3|111\rangle. \]

- To make each of the two sums a state, we can divide it by \( \sqrt{3} \).

- Thus, we get the following expression:

\[ a_0^3|000\rangle + \sqrt{3} \cdot a_0^2 \cdot a_1 \left( \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle \right) + \\
\]

\[ \sqrt{3} \cdot a_0 \cdot a_1^2 \left( \frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle \right) + a_1^3|111\rangle. \]
11. We Can Store This 3-Qubit State in 2 Bits

- We have a linear combination of four different states.
- But every 2-qubit state is also a linear combination of four states, namely $|\hat{0}\hat{0}\rangle$, $|\hat{0}\hat{1}\rangle$, $|\hat{1}\hat{0}\rangle$, and $|\hat{1}\hat{1}\rangle$.
- Thus, we can perform a transformation $T_0$ that maps:
  - the state $|000\rangle$ into $T_0(|000\rangle) = |\hat{0}\hat{0}\rangle$,
  - the state $\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle$ into
    $$T_0\left(\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle\right) = |\hat{0}\hat{1}\rangle,$$
  - the state $\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle$ into
    $$T_0\left(\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle\right) = |\hat{1}\hat{0}\rangle,$$
  - the state $|111\rangle$ into $T_0(|111\rangle) = |\hat{1}\hat{1}\rangle$, 

Proof
12. Storing 3-Qubit State in 2 Bits (cont-d)

- The original 3-qubit state gets transformed – without losing information – into the following 2-qubit state:

\[ a_0^3|00\rangle + \sqrt{3} \cdot a_0^2 \cdot a_1|01\rangle + \sqrt{3} \cdot a_0 \cdot a_1^2|10\rangle + a_1^3|11\rangle. \]

- The more qubits we store, the more difficult it is.
- So, from the practical viewpoint, this decrease in number of qubits is a great advantage.
- A similar decrease in the number of qubits is possible for any number \( k \) of identical qubits.
13. Natural Question

- In the original transformation $T_0$, we used the basic states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

- In principle, instead of these basic states, we can use any four states

$$a_{i,00}|00\rangle + a_{i,01}|01\rangle + a_{i,10}|10\rangle + a_{i,11}|11\rangle, \quad i = 1, \ldots, 4.$$

- The only conditions are:
  
  - that each of them is a valid state – in the sense that
    $$|a_{i,00}|^2 + |a_{i,01}|^2 + |a_{i,10}|^2 + |a_{i,11}|^2 = 1,$$  
  and

  - that every two different states $i \neq j$ are orthogonal in the sense that
    $$\sum_{a,b} a_{i,ab} \cdot a_{j,ab}^* = 0.$$

- Here $a^*$ means a complex conjugate, i.e., $(x + yi)^* \overset{\text{def}}{=} x - yi$, where $i \overset{\text{def}}{=} \sqrt{-1}$. 
14. Natural Question (cont-d)

- So why is the proposed scheme for 3-to-2-qubit compression based on the standard basis?
- Why not use any alternative basis?
- We will show that the standard basis is uniquely determined by natural symmetry requirements.
15. General (Non-Quantum) Natural Symmetries

- A natural symmetry in a system consisting of several similar objects is the possibility to swap these objects.
- In the original 3-qubit system, all three qubits are in the same state.
- So swapping these qubits does not change anything.
- On the other hand, in the resulting 2-qubit state, the two qubits are, in general, in different states.
- Thus, it makes sense to *swap* these qubits:
  - we keep the states $|\hat{0}\hat{0}\rangle$ and $|\hat{1}\hat{1}\rangle$:
    \[
    N_0(|\hat{0}\hat{0}\rangle) = |\hat{0}\hat{0}\rangle, \quad N_0(|\hat{1}\hat{1}\rangle) = |\hat{1}\hat{1}\rangle; \quad \text{and}
    \]
  - we swap the states $|\hat{0}\hat{1}\rangle$ and $|\hat{1}\hat{0}\rangle$:
    \[
    N_0(|\hat{0}\hat{1}\rangle) = |\hat{1}\hat{0}\rangle, \quad N_0(|\hat{1}\hat{0}\rangle) = |\hat{0}\hat{1}\rangle.
    \]
16. Non-Quantum Natural Symmetries (cont-d)

- Another natural idea is to swap (rename) the states of each object.

- In our case, we deal with binary states, i.e., physical systems that can be in two possible states.

- Which of these two states we identify with 0 and which with 1 is arbitrary.

- From this viewpoint, not much should change if we swap these two states: rename 0 as 1 and 1 as 0.

- In the original 3-qubit system, all three qubits are in the same state.

- So if we change one, we have to change all the others: 
  \[ |0\rangle \leftrightarrow |1\rangle. \]

- So, we have \( n_1(|0\rangle) = |1\rangle \) and \( n_1(|1\rangle) = |0\rangle. \)
17. Non-Quantum Natural Symmetries (cont-d)

- In the resulting 2-qubit state, the two qubits are, in general, in two different states.

- We can swap the states \( \hat{0}_1 \) and \( \hat{1}_1 \) of the first qubit:
  \[
  N_1(|\hat{0}_1\rangle) = |\hat{1}_1\rangle, \quad N_1(|\hat{1}_1\rangle) = |\hat{0}_1\rangle.
  \]

- We can swap the states \( \hat{0}_2 \) and \( \hat{1}_2 \) of the second qubit:
  \[
  N_2(|\hat{0}_2\rangle) = |\hat{1}_2\rangle, \quad N_2(|\hat{1}_2\rangle) = |\hat{0}_2\rangle.
  \]

- We can also have a composition \( N = N_1(N_2) = N_2(N_1) \) of these two symmetries.
18. Specific Quantum Symmetries

• In the quantum case, all we observe are probabilities of different measurement results.

• These probabilities are determined only by the absolute values of the amplitudes; thus:
  – if we multiply each state by a complex number whose absolute value is 1,
  – we will not notice any difference.

• In principle, there exist many complex numbers $\alpha$ for which $|\alpha| = 1$.

• However, all known quantum computing algorithms only use real-valued amplitudes.

• Because of this, we will also restrict ourselves to real-valued amplitudes – and thus, to real-valued $\alpha$. 

19. Quantum Symmetries (cont-d)

- For each numbers, the only two numbers with absolute value 1 are numbers 1 and -1.
- Multiplying by 1 does not change anything.
- So the only non-trivial transformations that we should consider are multiplications by -1.
- For the 3-qubit states, we have two options:
  - we can replace the original 0-state $|0\rangle$ with $-|0\rangle$ and keep the state $|1\rangle$ unchanged:
    $$n_2(|0\rangle) = -|0\rangle, \quad n_2(|1\rangle) = |1\rangle;$$
  - we can also replace the original 1-state $|1\rangle$ with $-|1\rangle$ and keep the state $|0\rangle$ unchanged:
    $$n_3(|0\rangle) = |0\rangle, \quad n_3(|1\rangle) = -|1\rangle.$$
- In addition to the transformations $n_1, n_2,$ and $n_3$, we can also have compositions of these transformations.
20. Quantum Symmetries (cont-d)

- For the first qubit of the resulting 2-qubit state, we have two choices:
  - we can replace $|\hat{0}_1\rangle$ with $-|\hat{0}_1\rangle$; we denote it $N_2$;
  - or we can replace $|\hat{1}_1\rangle$ with $-|\hat{1}_1\rangle$; we denote it $N_4$.

- For the second qubit of the resulting 2-qubit state, we also have two choices:
  - we can replace $|\hat{0}_2\rangle$ with $-|\hat{0}_2\rangle$; we denote it $N_5$;
  - we can replace $|\hat{1}_2\rangle$ with $-|\hat{1}_2\rangle$; we denote it $N_6$.

- We can also combine the transformations $N_0 - N_6$. 
21. Natural Symmetries: Summarizing

- Based on the above analysis, there are three natural transformation $n_i$ of the original qubits:
  - $n_1(|0\rangle) = |1\rangle$ and $n_1(|1\rangle) = |0\rangle$;
  - $n_2(|0\rangle) = -|0\rangle$ and $n_2(|1\rangle) = |1\rangle$;
  - $n_3(|0\rangle) = |0\rangle$ and $n_3(|1\rangle) = -|1\rangle$;

- We can also have their compositions.

- For the resulting 2-qubit state, we have transformations $N_0$ through $N_6$ and their compositions.
22. General Idea of Invariance And How It Can Be Applied Here

• What does it mean that a dependency is invariant?

• Let’s consider the relation $A = s^2$ between the length $s$ of the square’s side and its area $A$.

• This relation is invariant with respect to changing the measuring unit for length.

• This is equivalent to replacing $s$ with $\lambda \cdot s$, e.g., $2 \text{ m} = 100 \cdot 2 = 200 \text{ cm}$.

• In precise terms, it means that:
  – for each such transformation of length,
  – we can find a similar transformation of areas for which the above formula remains true.

• In this case, this transformation is $A \rightarrow \lambda^2 \cdot A$.

• This notion of invariance is ubiquitous in physics.
23. General Idea of Invariance (cont-d)

• Similarly, in our case, invariance would mean that:
  – for each of the following four natural transformation $n_i$ of the original qubits,
  – there exists a natural transformation $N$ of the resulting 2-qubit state such that $N(T_0(n_i)) = T_0$. 
24. **What Natural Symmetry of the 2-Qubit State Corresponds To Swaps**

- If we swap \( (n_1) \) the original qubits, and then apply \( T_0 \), we get:

\[
T_0(n_1(|000\rangle)) = T_0(|111\rangle) = |\hat{1}\hat{1}\rangle;
\]

\[
T_0 \left( n_1 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) =
\]

\[
T_0 \left( \frac{1}{\sqrt{3}} \cdot (|110\rangle + |101\rangle + |011\rangle) \right) = |\hat{1}\hat{0}\rangle;
\]

\[
T_0 \left( n_1 \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) \right) =
\]

\[
T_0 \left( \frac{1}{\sqrt{3}} \cdot (|100\rangle + |010\rangle + |001\rangle) \right) = |\hat{0}\hat{1}\rangle;
\]

\[
T_0(n_1(|111\rangle)) = T_0(|000\rangle) = |\hat{0}\hat{0}\rangle.
\]

- To get back \( T_0 \), it is sufficient to swap 0 and 1 states of both qubits: \( N_1(N_2(T_0(n_1))) = T_0 \).
25. Changing the Sign $n_2$ of the Original $0$ State

- If we first apply $n_2$ and then $T_0$, we get:
  \[ T_0(n_2(|000\rangle)) = T_0(-|000\rangle) = -|\hat{0}\hat{0}\rangle; \]
  \[ T_0 \left( n_2 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) = \]
  \[ T_0 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) = |\hat{0}\hat{1}\rangle; \]
  \[ T_0 \left( n_2 \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) \right) = \]
  \[ T_0 \left( -\frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) = -|\hat{1}\hat{0}\rangle; \]
  \[ T_0(n_2(|111\rangle)) = T_0(|111\rangle) = |\hat{1}\hat{1}\rangle. \]

- To get back $T_0$, it is sufficient to replace $|\hat{0}\hat{2}\rangle$ with $-|\hat{0}\hat{2}\rangle$ (transformation $N_5$).
26. Changing the Sign $n_3$ of the Original 1 State

- If we apply $n_3$ and then $T_0$, we get:
  \[ T_0(n_3(|000\rangle)) = T_0(|000\rangle) = |00\rangle; \]
  \[ T_0 \left( n_3 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) = \]
  \[ T_0 \left( -\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) = -|01\rangle; \]
  \[ T_0 \left( n_3 \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) \right) = \]
  \[ T_0 \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) = |10\rangle; \]
  \[ T_0(n_3(|111\rangle)) = T_0(-|111\rangle) = -|11\rangle. \]

- To get back $T_0$, it is sufficient to replace $|\hat{1}_2\rangle$ with $-|\hat{1}_2\rangle$ (transformation $N_6$).
27. Main Result: \( T_0 \) Is the Only Invariant Transformation

- Our result is that \( T_0 \) is the only real-valued transformation \( T \) that is similarly invariant, i.e., for which
  \[
  N_1(N_2(T(n_1))) = T, \quad N_5(T(n_2)) = T, \quad \text{and} \quad N_6(T(n_3)) = T.
  \]

- To be more precise, \( T_0 \) is unique:
  - modulo rotations of the state of the first qubit of the 2-qubit output and
  - modulo changing signs of some of the resulting four states.
28. Proof

- Let us consider a general real-valued transformation:

\[ T(|000\rangle) = a_{1,00}|\hat{0}\hat{0}\rangle + a_{1,01}|\hat{0}\hat{1}\rangle + a_{1,10}|\hat{1}\hat{0}\rangle + a_{1,11}|\hat{1}\hat{1}\rangle; \]

\[ T \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) = \]

\[ a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle; \]

\[ T_0 \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) = \]

\[ a_{3,00}|\hat{0}\hat{0}\rangle + a_{3,01}|\hat{0}\hat{1}\rangle + a_{3,10}|\hat{1}\hat{0}\rangle + a_{3,11}|\hat{1}\hat{1}\rangle; \]

\[ T(|111\rangle) = a_{4,00}|\hat{0}\hat{0}\rangle + a_{4,01}|\hat{0}\hat{1}\rangle + a_{4,10}|\hat{1}\hat{0}\rangle + a_{4,11}|\hat{1}\hat{1}\rangle. \]
29. Proof (cont-d)

- The condition that $N_5(T(n_2)) = T$ implies, in particular, that

$$N_5 \left( T \left( n_2 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) \right) = T \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right).$$

- The left-hand side of this equality is equal to

$$N_5 \left( T \left( n_2 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) \right) = N_5 \left( T \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) = N_5(a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle) = -a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle - a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle.$$
30. Proof (cont-d)

- Thus, the desired equality has the form
  \[-a_{2,00}\hat{0}\hat{0} + a_{2,01}\hat{0}\hat{1} - a_{2,10}\hat{1}\hat{0} + a_{2,11}\hat{1}\hat{1} =\]
  \[a_{2,00}\hat{0}\hat{0} + a_{2,01}\hat{0}\hat{1} + a_{2,10}\hat{1}\hat{0} + a_{2,11}\hat{1}\hat{1}.\]

- Therefore, $a_{2,00} = a_{2,10} = 0$, and the above expression has a simplified form:
  \[T\left(\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle)\right) =\]
  \[a_{2,01}\hat{0}\hat{1} + a_{2,11}\hat{1}\hat{1}.\]

- The right-hand side is a state, so we must have
  \[a_{2,01}^2 + a_{2,11}^2 = 1.\]

- Thus there exists an angle $\alpha$ for which $a_{2,01} = \cos(\alpha)$ and $a_{2,11} = \sin(\alpha)$. 
31. Proof (cont-d)

• In terms of this angle, we have

\[
T \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) = \cos(\alpha)|\hat{0}\rangle + \sin(\alpha)|\hat{1}\rangle = (\cos(\alpha)|\hat{0}\rangle + \sin(\alpha)|\hat{1}\rangle) \otimes |1\rangle.
\]

• Similarly, the condition that \(N_6(T(n_3)) = T\) implies, in particular, that

\[
N_6 \left( T \left( n_3 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) \right) = T \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right).
\]
32. Proof (cont-d)

- The left-hand side of this equality is equal to
  \[
  N_6 \left( T \left( n_3 \left( \frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) \right) = \\
  N_6 \left( T \left( -\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle) \right) \right) = \\
  N_6(-\cos(\alpha)|\hat{0}\hat{1}\rangle - \sin(\alpha)|\hat{1}\hat{1}\rangle) = \\
  \cos(\alpha)|\hat{0}\hat{0}\rangle + \sin(\alpha)|\hat{1}\hat{1}\rangle.
  \]

- Thus, this equality is always satisfied.

- The condition \( N_1(N_2(T(n_1))) = T \) then implies that
  \[
  T \left( \frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle) \right) = \\
  (\sin(\alpha)|\hat{0}\rangle + \cos(\alpha)|\hat{1}\rangle) \otimes |1\rangle.
  \]
33. Proof (cont-d)

- For the state $|000\rangle$, the condition that $N_5(T(n_2))) = T$ implies that

$$N_5(T(n_2(|000\rangle))) = T(|000\rangle).$$

- Here, $N_5(T(n_2(|000\rangle))) = N_5(T(-|000\rangle)) = N_5(-a_{1,00} |\hat{0}\hat{0}\rangle - a_{1,01} |\hat{0}\hat{1}\rangle - a_{1,10} |\hat{1}\hat{0}\rangle - a_{1,11} |\hat{1}\hat{1}\rangle) = a_{1,00} |\hat{0}\hat{0}\rangle - a_{1,01} |\hat{0}\hat{1}\rangle + a_{1,10} |\hat{1}\hat{0}\rangle - a_{1,11} |\hat{1}\hat{1}\rangle).$

- Thus, the above equality takes the form

$$a_{1,00} |\hat{0}\hat{0}\rangle - a_{1,01} |\hat{0}\hat{1}\rangle + a_{1,10} |\hat{1}\hat{0}\rangle - a_{1,11} |\hat{1}\hat{1}\rangle = a_{1,00} |\hat{0}\hat{0}\rangle + a_{1,01} |\hat{0}\hat{1}\rangle + a_{1,10} |\hat{1}\hat{0}\rangle + a_{1,11} |\hat{1}\hat{1}\rangle.$$

- So, $a_{1,01} = a_{1,11} = 0$, and the above expression has a simplified form $T(|000\rangle) = a_{1,00} |\hat{0}\hat{0}\rangle + a_{1,10} |\hat{1}\hat{0}\rangle$. 
34. **Proof (cont-d)**

- Similarly, we can conclude that there exists an angle \( \beta \) for which \( \cos(\beta) = a_{1,00} \) and \( \sin(\beta) = a_{1,10} \), thus

\[
T(|000\rangle) = \cos(\beta)|00\rangle + \sin(\beta)|10\rangle = (\cos(\beta)|0\rangle + \sin(\beta)|1\rangle) \otimes |0\rangle.
\]

- The condition \( N_1(N_2(T(n_1))) = T \) then implies that

\[
T(|111\rangle) = (\sin(\beta)|0\rangle + \cos(\beta)|1\rangle) \otimes |1\rangle.
\]

- The fact that the states \( T(|000\rangle) \) and \( T(|111\rangle) \) must be orthogonal means that

\[
\cos(\alpha) \cdot \sin(\beta) + \sin(\alpha) \cdot \cos(\beta) = \sin(\alpha + \beta) = 0.
\]

- So the sum \( \alpha + \beta \) is either equal to 0 or to \( \pi \).
35. Proof (cont-d)

- If this sum is equal to 0, then $\beta = -\alpha$, $\sin(\beta) = -\sin(\alpha)$, $\cos(\beta) = \cos(\alpha)$, so:

$$T(|000\rangle) = (\cos(\alpha)|\hat{0}\rangle - \sin(\alpha)|\hat{1}\rangle) \otimes |\hat{0}\rangle;$$

$$T(|111\rangle) = (-\sin(\alpha)|\hat{0}\rangle + \cos(\alpha)|\hat{1}\rangle) \otimes |\hat{1}\rangle.$$  

- For the rotated states $|\hat{0}'\rangle \overset{\text{def}}{=} \cos(\alpha)|\hat{0}\rangle - \sin(\alpha)|\hat{1}\rangle$ and $|\hat{1}'\rangle \overset{\text{def}}{=} \cos(\alpha) \cdot |1\rangle + \sin(\alpha)|0\rangle$, we get exactly $T_0$:

$$T_0(|000\rangle) = |\hat{0}' \hat{0}\rangle,$$

$$T_0 \left( \frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle \right) = |\hat{0}' \hat{1}\rangle,$$

$$T_0 \left( \frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle \right) = |\hat{1}' \hat{0}\rangle,$$

$$T_0(|111\rangle) = |\hat{1}' \hat{1}\rangle.$$
36. Proof (cont-d)

- When $\alpha + \beta = -\pi$:
  - we get a similar transformation,
  - but with an additional need to change the sign of the resulting basis states.

- The result has been proven.
37. Acknowledgments

This work was supported in part by the National Science Foundation grants:

- 1623190 (A Model of Change for Preparing a New Generation for Professional Practice in Computer Science),
- HRD-1242122 (Cyber-ShARE Center of Excellence).