5-2020

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

Oscar Galindo

Olga Kosheleva

Vladik Kreinovich

Comments:
Technical Report: UTEP-CS-20-44

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
500 W. University
El Paso, TX 79968, USA
ogalindomo@miners.utep.edu, olgak@utep.edu, vladik@utep.edu

Abstract

In complex time-consuming computations, we rarely have uninterrupted access to a high performance computer: usually, in the process of computation, some interruptions happen, so we need to store intermediate results until computations resume. To decrease the probability of a mistake, it is often necessary to run several identical computations in parallel, in which case several identical intermediate results need to be stored. In particular, for quantum computing, we need to store several independent identical copies of the corresponding qubits – quantum versions of bits. Storing qubit states is not easy, but it is possible to compress the corresponding multi-qubit states: for example, it is possible to store the resulting 3-qubit state by using only two qubits. In principle, there are many different ways to store the state of 3 independent identical qubits by using two qubits. In this paper, we show that the current algorithm for such storage is uniquely determined by the natural symmetry requirements.

1 Formulation of the Problem

Quantum computing is inevitable. While modern computers are several orders of magnitude faster than in the past, for many practical problems, they are still too slow. For example, by using modern high performance computers, in principle, we can compute where a tornado will turn in the next 15 minutes, but even on the fastest computers, these computations will take several hours, long after the tornado has actually moved – and thus, too late to provide a warning.

One of the main reasons why it is difficult to drastically speed up modern computers is the fact that, 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 – the fastest possible process – to pass from one side of the laptop to another. During this time, even the cheapest 4 GHz central processing unit will already perform four different 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 physical phenomena which are specific for the microworld, i.e., phenomena of quantum physics; see, e.g., [4, 11]. From this viewpoint, quantum computing – i.e., computing by using units that obey laws of quantum physics – is inevitable.

Quantum computing is desirable. At first, quantum effects were viewed by computer engineers as a nuisance: indeed, we want the computer to produce the same desired result every time we ask for the same computation, while 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 in such a way that we can actually compute several things with guarantee and even faster than by using traditional non-quantum algorithms; see, e.g., [8]. The most widely known quantum algorithm of this type are Shor's algorithm that enables us to factor large integers in polynomial time – and thus, in principle, decode all the messages sent by using the commonly used RSA encryption (since 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 well known quantum algorithm is Grover's algorithm for searching for an element in an un-sorted array of n elements: while non-quantum algorithm requires at least n steps (otherwise, it may miss the desired element), Grover's algorithm can find it much faster, in time $\sqrt{n}$.

It is important to mention that most quantum algorithms – including Shor's and Grover's – remain somewhat probabilistic, in the sense that while they produce the correct result with probability close to 1, there is a certain probability of a wrong result. To decrease this probability of the error, a natural idea is to repeat computations several times – either sequentially or, if we want to retain the same computation time, by running 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.

Need to store intermediate computation results. As we have mentioned earlier, the main motivation for using quantum computing is to solve complex time-consuming problems whose computation requires a lot of time. It is very rare that for such problem, we have a dedicated computer that only solves this problem. Often, when such a time-consuming problem is being solved on a high performance computer, another higher-priority task appears, so the previous computation has to be interrupted, the intermediate computation results have to be temporarily stored – so that the computations can resume when the interrupting task is done.

Thus, for whatever algorithm we use, we need to take this need into account and instruct the computer how to store intermediate results. In particular, this is needed for quantum algorithms.

As we have mentioned in the previous subsection, 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.

What exactly do we store. The state of the usual (non-quantum) computer can be described as a sequence of bits, i.e., simple elements 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, i.e., the state of the type $a_0|0\rangle + a_1|1\rangle$, where 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 and get 0 or 1. If we apply the same measurement process to the superposition, we get 0 with probability $|a_0|^2$ and 1 with probability $|a_1|^2$. 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* $\otimes$. Crudely speaking, it means the amplitude of each state of the 2-particle system is equal to the product of the corresponding amplitudes – just like the probability of having two outcomes in two independent events is equal to the product of the corresponding probabilities. In particular, if we have two identical particles in the state $a_0|0\rangle + a_1|1\rangle$, then the state of the corresponding 2-particle system has the form

$$a_0^2|00\rangle + a_0 \cdot a_1|01\rangle + a_1 \cdot a_0|10\rangle + a_1^2|11\rangle,$$

i.e., the state

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

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:

$$a_0^2|00\rangle + \sqrt{2} \cdot a_0 \cdot a_1 \cdot \left(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle\right) + a_1^2|11\rangle.$$

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:

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

$$\sqrt{3} \cdot a_0 \cdot a_1^2 \left(\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle \right) + a_1^3|111\rangle. \quad (1)$$

Good news: we can store this 3-qubit state in 2 bits. The expression (1) is 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 $|\hat{1}\hat{1}\rangle$, where $\hat{0}$ and $\hat{1}$ denote 0 and 1 states of each qubit of the 2-qubit system. Thus, if we, e.g., perform a transformation T_0 that maps:

- the state $|000\rangle$ into
$$T_0(|000\rangle) = |\hat{0}\hat{0}\rangle, \quad (2)$$
- the state $\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle$ into
$$T_0\left(\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle \right) = |\hat{0}\hat{1}\rangle, \quad (3)$$
- the state $\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle$ into
$$T_0\left(\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle \right) = |\hat{1}\hat{0}\rangle, \quad (4)$$
  and
- the state $|111\rangle$ into
$$T_0(|111\rangle) = |\hat{1}\hat{1}\rangle, \quad (5)$$

then the original 3-qubit state (1) gets transformed – without losing any information – into the following 2-qubit state:

$$a_0^3|\hat{0}\hat{0}\rangle + \sqrt{3} \cdot a_0^2 \cdot a_1|\hat{0}\hat{1}\rangle + \sqrt{3} \cdot a_0 \cdot a_1^2|\hat{1}\hat{0}\rangle + a_1^3|\hat{1}\hat{1}\rangle. \quad (6)$$

The more qubits we need to store, the more difficult is it, 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; see, e.g., [1, 2, 3, 5, 6, 7, 9, 10].

Natural question. In the original transformation T_0, we used the basic states $|\hat{0}\hat{0}\rangle$, $|\hat{0}\hat{1}\rangle$ $|\hat{1}\hat{0}\rangle$, and $|\hat{1}\hat{1}\rangle$. In principle, instead of these basic states, we can use any four states

$$a_{i,00}|\hat{0}\hat{0}\rangle + a_{i,01}|\hat{0}\hat{1}\rangle + a_{i,10}|\hat{1}\hat{0}\rangle + a_{i,11}|\hat{1}\hat{1}\rangle, \quad i = 1, \ldots, 4,$$

as long as each of them is a valid state – in the sense that

$$|a_{i,00}|^2 + |a_{i,01}|^2 + |a_{i,10}|^2 + |a_{i,11}|^2 = 1$$

for all i, and that every two different states $i \neq j$ are *orthogonal* in the sense that

$$\sum_{a,b} a_{i,ab} \cdot a^*_{j,ab} = 0,$$

where a^* means a complex conjugate, i.e., $(x + y\mathrm{i})^* \stackrel{\text{def}}{=} x - y\mathrm{i}$, where $\mathrm{i} \stackrel{\text{def}}{=} \sqrt{-1}$.

So why is the proposed scheme for 3-to-2-qubit compression based on the standard basis and not on any alternative?

What we do in this paper. In this paper, we show that the use of the standard basic can be uniquely determined by natural symmetry requirements.

2 What Are Natural Symmetries?

General (non-quantum) natural symmetries. Let us first consider natural symmetries which are motivated by the problem itself and have nothing to do with quantum physics.

Swapping the objects. 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. In terms of the corresponding states, this means that:

- we keep the states $|\hat{0}\hat{0}\rangle$ and $|\hat{1}\hat{1}\rangle$ and
- we swap the states $|\hat{0}\hat{1}\rangle$ and $|\hat{1}\hat{0}\rangle$.

In other words, the transformation takes the form

$$N_0(|\hat{0}\hat{0}\rangle) = |\hat{0}\hat{0}\rangle, \quad N_0(|\hat{0}\hat{1}\rangle) = |\hat{1}\hat{0}\rangle, \quad N_0(|\hat{1}\hat{0}\rangle) = |\hat{0}\hat{1}\rangle, \quad N_0(|\hat{1}\hat{1}\rangle) = |\hat{1}\hat{1}\rangle.$$

Swapping the states. 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 simply swap these two states, i.e., 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: $|0\rangle \leftrightarrow |1\rangle$, i.e., we have the transformation n_1 for which:

$$n_1(|0\rangle) = |1\rangle, \quad n_1(|1\rangle) = |0\rangle.$$

In the resulting 2-qubit state, the two qubits are, in general, in two different states. Thus, for the 2-qubit states, we have three options:

- we can swap the states $\hat{0}_1$ and $\hat{1}_1$ of the first qubit:

  $$N_1(|\hat{0}_1\rangle) = |\hat{1}_1\rangle, \quad N_1(|\hat{1}_1\rangle) = |\hat{0}_1\rangle, \quad N_1(|\hat{0}_2\rangle) = |\hat{0}_2\rangle, \quad N_1(|\hat{1}_2\rangle) = |\hat{1}_2\rangle;$$

  so

  $$N_1(|\hat{0}\hat{0}\rangle) = |\hat{1}\hat{0}\rangle, \quad N_1(|\hat{0}\hat{1}\rangle) = |\hat{1}\hat{1}\rangle, \quad N_1(|\hat{1}\hat{0}\rangle) = |\hat{0}\hat{0}\rangle, \quad N_1(|\hat{1}\hat{1}\rangle) = |\hat{0}\hat{1}\rangle;$$

- we can also swap the states $\hat{0}_2$ and $\hat{1}_2$ of the second qubit:

  $$N_2(|\hat{0}_1\rangle) = |\hat{0}_1\rangle, \quad N_2(|\hat{1}_1\rangle) = |\hat{1}_1\rangle, \quad N_2(|\hat{0}_2\rangle) = |\hat{1}_2\rangle, \quad N_2(|\hat{1}_2\rangle) = |\hat{0}_2\rangle;$$

  so

  $$N_2(|\hat{0}\hat{0}\rangle) = |\hat{0}\hat{1}\rangle, \quad N_2(|\hat{0}\hat{1}\rangle) = |\hat{0}\hat{0}\rangle, \quad N_2(|\hat{1}\hat{0}\rangle) = |\hat{1}\hat{1}\rangle, \quad N_2(|\hat{1}\hat{1}\rangle) = |\hat{1}\hat{0}\rangle.$$

We can also have a composition $N = N_1(N_2) = N_2(N_1)$ of these two symmetries, when we swap the states of both qubits:

$$N(|\hat{0}_1\rangle) = |\hat{1}_1\rangle, \quad N(|\hat{1}_1\rangle) = |\hat{0}_1\rangle, \quad N(|\hat{0}_2\rangle) = |\hat{1}_2\rangle, \quad N(|\hat{1}_2\rangle) = |\hat{0}_2\rangle,$$

so

$$N(|\hat{0}\hat{0}\rangle) = |\hat{1}\hat{1}\rangle, \quad N(|\hat{0}\hat{1}\rangle) = |\hat{1}\hat{0}\rangle, \quad N(|\hat{1}\hat{0}\rangle) = |\hat{0}\hat{1}\rangle, \quad N(|\hat{1}\hat{1}\rangle) = |\hat{0}\hat{0}\rangle.$$

Specific quantum symmetries. As we have mentioned, in the quantum case, all we observe are probabilities of different measurement results, and 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 α for which $|\alpha| = 1$. However, all known quantum computing algorithms only use real-valued amplitudes. Because of this, in this paper, we will also restrict ourselves to real-valued amplitudes – and thus, to real-valued factors α. 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.

For the first qubit of the resulting 2-qubit state, we have two choices:

- we can replace $|\hat{0}_1\rangle$ with $-|\hat{0}_1\rangle$:

$$N_3(|\hat{0}\hat{0}\rangle) = -|\hat{0}\hat{0}\rangle,\quad N_3(|\hat{0}\hat{1}\rangle) = -|\hat{0}\hat{1}\rangle,\quad N_3(|\hat{1}\hat{0}\rangle) = |\hat{1}\hat{0}\rangle,\quad N_3(|\hat{1}\hat{1}\rangle) = |\hat{1}\hat{1}\rangle;$$

- or we can replace $|\hat{1}_1\rangle$ with $-|\hat{1}_1\rangle$:

$$N_4(|\hat{0}\hat{0}\rangle) = |\hat{0}\hat{0}\rangle,\quad N_4(|\hat{0}\hat{1}\rangle) = |\hat{0}\hat{1}\rangle,\quad N_4(|\hat{1}\hat{0}\rangle) = -|\hat{1}\hat{0}\rangle,\quad N_4(|\hat{1}\hat{1}\rangle) = -|\hat{1}\hat{1}\rangle;$$

For the second qubit of the resulting 2-qubit state, we also have two choices:

- we can replace $|\hat{0}_2\rangle$ with $-|\hat{0}_2\rangle$:

$$N_5(|\hat{0}\hat{0}\rangle) = -|\hat{0}\hat{0}\rangle,\quad N_5(|\hat{0}\hat{1}\rangle) = |\hat{0}\hat{1}\rangle,\quad N_5(|\hat{1}\hat{0}\rangle) = -|\hat{1}\hat{0}\rangle,\quad N_5(|\hat{1}\hat{1}\rangle) = |\hat{1}\hat{1}\rangle;$$

- or we can replace $|\hat{1}_2\rangle$ with $-|\hat{1}_2\rangle$:

$$N_6(|\hat{0}\hat{0}\rangle) = |\hat{0}\hat{0}\rangle,\quad N_6(|\hat{0}\hat{1}\rangle) = -|\hat{0}\hat{1}\rangle,\quad N_6(|\hat{1}\hat{0}\rangle) = |\hat{1}\hat{0}\rangle,\quad N_6(|\hat{1}\hat{1}\rangle) = -|\hat{1}\hat{1}\rangle.$$

We can also combine the transformations $N_0 - N_6$.

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 $n_3(|1\rangle) = -|1\rangle$;

and their compositions. For the resulting 2-qubit state, we have transformations N_0 through N_6 and their compositions

3 Symmetries that Keep the Original Transformation Invariant

Original transformation: reminder. The original transformation T_0 is described by the formulas (2)-(5).

General idea of invariance and how it can be applied here. What does it mean that some dependencies are invariant? For example, the relation $A = s^2$ between the length s of the square's side and its area A is invariant with respect to changing the measuring unit for length (which is equivalent to replacing s with $\lambda \cdot s$, e.g., 2 m = $100 \cdot 2 = 200$ 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 $A \to \lambda^2 \cdot A$. This notion of invariance is ubiquitous in physics; see, e.g., [4, 11].

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 after applying both transformations, we get exactly the same formulas (2)-(5) for the transformation T_0: $N(T_0(n_i)) = T_0$.

What natural symmetry of the 2-qubit state corresponds to swaps. If we first apply the swap n_1 to the original qubits, and then apply the transformation T_0, then we get the following transformation $T_0(n_1)$:

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

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

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

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

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

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

One can easily see that to get back the original transformation T_0, it is sufficient to swap 0 and 1 states of both qubits, i.e., consider the transformation $N = N_1(N_2)$ for which

$$N(|00\rangle) = |11\rangle, \quad N(|01\rangle) = |10\rangle, \quad N(|10\rangle) = |01\rangle, \quad N(|11\rangle) = |00\rangle;$$

then, indeed,

$$N_1(N_2(T_0(n_1))) = T_0. \tag{7}$$

What natural symmetry of the 2-qubit space corresponds to changing the sign of the original 0 state. If we first apply the transformation n_2 and then T_0, we will get the following transformation $T_0(n_2)$:

$$T_0(n_2(|000\rangle)) = T_0(-|000\rangle) = -|\hat{0}\hat{0}\rangle;$$

$$T_0\left(n_2\left(\frac{1}{\sqrt{3}}\cdot(|001\rangle + |010\rangle + |100\rangle)\right)\right) =$$

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

$$T_0\left(n_2\left(\frac{1}{\sqrt{3}}\cdot(|011\rangle+|101\rangle+|110\rangle)\right)\right)=$$

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

$$T_0(n_2(|111\rangle))=T_0(|111\rangle)=|\hat{1}\hat{1}\rangle.$$

One can see that to get back the original transformation T_0, it is sufficient to replace $|\hat{0}_2\rangle$ with $-|\hat{0}_2\rangle$, i.e., to apply the transformation N_5:

$$N_5(T_0(n_2))=T_0. \tag{8}$$

What natural symmetry of the 2-qubit space corresponds to changing the sign of the original 1 state. If we first apply the transformation n_3 and then T_0, we will get the following transformation $T_0(n_3)$:

$$T_0(n_3(|000\rangle))=T_0(|000\rangle)=|\hat{0}\hat{0}\rangle;$$

$$T_0\left(n_3\left(\frac{1}{\sqrt{3}}\cdot(|001\rangle+|010\rangle+|100\rangle)\right)\right)=$$

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

$$T_0\left(n_3\left(\frac{1}{\sqrt{3}}\cdot(|011\rangle+|101\rangle+|110\rangle)\right)\right)=$$

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

$$T_0(n_3(|111\rangle))=T_0(-|111\rangle=-|\hat{1}\hat{1}\rangle.$$

One can see that to get back the original transformation T_0, it is sufficient to replace $|\hat{1}_2\rangle$ with $-|\hat{1}_2\rangle$, i.e., to apply the transformation N_6:

$$N_6(T_0(n_3))=T_0. \tag{9}$$

4 Main Result: T_0 Is the Only Invariant Transformation

Formulation of our main result. We claim – and we will prove it – that the only real-valued transformation T that is similarly invariant, i.e., for which

$$N_1(N_2(T(n_1)))=T,\quad N_5(T(n_2))=T,\ \text{and}\ N_6(T(n_3))=T, \tag{10}$$

is, in effect, the transformation T_0 – 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.

Proof. Let is consider a general real-valued transformation:

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

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

$$a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle; \tag{12}$$

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

$$a_{3,00}|\hat{0}\hat{0}\rangle + a_{3,01}|\hat{0}\hat{1}\rangle + a_{3,10}|\hat{1}\hat{0}\rangle + a_{3,11}|\hat{1}\hat{1}\rangle; \tag{13}$$

$$T(|111\rangle) = a_{4,00}|\hat{0}\hat{0}\rangle + a_{4,01}|\hat{0}\hat{1}\rangle + a_{4,10}|\hat{1}\hat{0}\rangle + a_{4,11}|\hat{1}\hat{1}\rangle. \tag{14}$$

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

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

$$T\left(\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle)\right). \tag{15}$$

The left-hand side of this equality is equal to

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

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

$$N_5(a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle) =$$

$$-a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle - a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle.$$

Thus, due to (12), the equality (15) has the form

$$-a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle - a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle =$$

$$a_{2,00}|\hat{0}\hat{0}\rangle + a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,10}|\hat{1}\hat{0}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle.$$

Therefore, $a_{2,00} = a_{2,10} = 0$, and the expression (12) has a simplified form:

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

$$a_{2,01}|\hat{0}\hat{1}\rangle + a_{2,11}|\hat{1}\hat{1}\rangle.$$

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 α for which $a_{2,01} = \cos(\alpha)$ and $a_{2,11} = \sin(\alpha)$. In terms of this angle, we have

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

$$(\cos(\alpha)|\hat{0}\rangle + \sin(\alpha)|\hat{1}\rangle) \otimes |1\rangle. \tag{16}$$

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

$$N_6\left(T\left(n_3\left(\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle)\right)\right)\right) =$$

$$T\left(\frac{1}{\sqrt{3}} \cdot (|001\rangle + |010\rangle + |100\rangle)\right). \tag{17}$$

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, due to (16), the equality (17) is always satisfied.

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

$$T\left(\frac{1}{\sqrt{3}} \cdot (|011\rangle + |101\rangle + |110\rangle)\right) =$$

$$(\sin(\alpha)|\hat{0}\rangle + \cos(\alpha)|\hat{1}\rangle) \otimes |1\rangle. \tag{18}$$

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

$$N_5(T(n_2(|000\rangle))) = T(|000\rangle). \tag{19}$$

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, due to (11), the equality (19) 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 expression (11) has a simplified form

$$T(|000\rangle) = a_{1,00}|\hat{0}\hat{0}\rangle + a_{1,10}|\hat{1}\hat{0}\rangle.$$

Similar to the above, we can conclude that there exists an angle β for which $\cos(\beta) = a_{1,00}$ and $\sin(\beta) = a_{1,10}$, thus

$$T(|000\rangle) = \cos(\beta)|\hat{0}\hat{0}\rangle + \sin(\beta)|\hat{1}\hat{0}\rangle = (\cos(\beta)|\hat{0}\rangle + \sin(\beta)|\hat{1}\rangle) \otimes |\hat{0}\rangle. \tag{20}$$

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

$$T(|111\rangle) = (\sin(\beta)|\hat{0}\rangle + \cos(\beta)|\hat{1}\rangle) \otimes |\hat{1}\rangle. \tag{21}$$

The fact that the states (16) and (21) 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 π. If this sum is equal to 0, then $\beta = -\alpha$, $\sin(\beta) = -\sin(\alpha)$, $\cos(\beta) = \cos(\alpha)$, and the formulas (20) and (21) take the form

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

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

Thus, for the rotated states

$$|\hat{0}'\rangle \stackrel{\text{def}}{=} \cos(\alpha)|\hat{0}\rangle - \sin(\alpha)|\hat{1}\rangle$$

and

$$|\hat{1}'\rangle \stackrel{\text{def}}{=} \cos(\alpha) \cdot |1\rangle + \sin(\alpha)|0\rangle,$$

the formulas (16), (18), (20), and (21) take the desired form

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

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

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

$$T_0(|111\rangle) = |\hat{1}'\hat{1}\rangle.$$

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

The result has been proven.

Acknowledgments

This work was supported in part by the US National Science Foundation grants 1623190 (A Model of Change for Preparing a New Generation for Professional Practice in Computer Science) and HRD-1242122 (Cyber-ShARE Center of Excellence).

References

[1] D. Bacon, I. L. Chuang, and A. W. Harrow, "Efficient Quantum Circuits for Schur and Clebsch-Gordan Transforms", *Physical Review Letters*, 2006, Vol. 97, Paper 170502.

[2] R. Blume-Kohout, "Optimal, reliable estimation of quantum states", *New Journal of Physics*, 2010, Vol. 12, Paper 043034.

[3] J. Eisert, T. Felbinger, P. Papadopoulos, M. B. Plenio and M. Wilkens, "Classical Information and Distillable Entanglement", *Physical Review Letters*, 2000, Vol. 84, Paper 1611.

[4] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics*, Addison Wesley, Boston, Massachusetts, 2005.

[5] M. Hayashi and K. Matsumoto, "Quantum universal variable-length source coding", *Physical Review A*, 2002, Vol. 66, Paper 022311.

[6] M. Keyl and R. F. Werner, "Estimating the spectrum of a density operator", *Physical Review A*, 2001, Vol. 64, Paper 052311.

[7] I. Marvian and R. W. Spekkens, "A generalization of Schur-Weyl duality with applications in quantum estimation", *Communications in Mathematical Physics*, 2014, Vol. 331, pp. 431–475.

[8] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, U.K., 2000.

[9] M. Plesch and V. Bužek,"Efficient compression of quantum information", *Physical Review A*, 2010, Vol. 81, Paper 032317.

[10] L. A. Rozema, D. H. Mahler, A. Hayat, P. S. Turner, and A. M. Steinberg, "Quantum Data Compression of a Qubit Ensemble", *Physical Review Letters*, 2014, Vol. 113, Paper 160504.

[11] K. S. Thorne and R. D. Blandford, Modern Classical Physics: Optics, Fluids, Plasmas, Elasticity, Relativity, and Statistical Physics, Princeton University Press, Princeton, New Jersey, 2017.