THE SEARCH FOR A QUANTUM COMPUTER THROUGH BRAIDING QUANTUM GATES

REBECCA S. CHEN

1. Personal Section

It is difficult to say when my passion for mathematics was first kindled. I have liked doing number problems and logic puzzles for as long as I can recall: one of my earliest memories is of using toothpicks to guide a brave mouse across shark-infested waters to steal the king's cheese (a challenge found in *The Puzzle Book*, which I owned when I was younger). My interest was further strengthened by participation in math competitions and a math club organized by Professor Ron Ji at IUPUI. However, soon after entering high school, I began to feel that I would like to go beyond solving contest problems and engage in the creative process of mathematical discovery. A family friend, Professor Eric Rowell, is always enthusiastic about his research area–braid groups and their representations–so in the spring of 2010, I asked him for a possible project. Prof. Rowell suggested studying the generalized Yang-Baxter equation proposed by him and his collaborators in quantum information theory. This project idea intrigued me partly because of the potential applications in quantum computation, a field that my growing interest in computer science made me eager to learn more about.

Although the project itself–a combination of algebraic computation and computer numerical checking to classify new solutions to the generalized Yang-Baxter equation–was long and often frustrating, one of the most challenging aspects was the large body of knowledge I had to assimilate before I could even begin. I spent a summer mastering the basics of linear algebra and braid groups by reading books and doing exercises. Afterwards, my work on the project was accomplished largely at home, with communication with Prof. Rowell done through email. He suggested reference materials in addition to supplying critique, encouragement, and the occasional invaluable insight.

Overall, my project deepened and broadened my understanding of not only the research process but also the interplay between seemingly disparate fields. The generalized Yang-Baxter equation lies at the interface of mathematics, physics, and quantum information theory. Drawing on concepts from all three of these areas allowed me to start to grasp their commonalities and differences, as well as the necessity of reaching across boundaries between disciplines to tackle the ever more complex and fascinating problems that await us in the future.

To other high school students who are looking to do research that synthesizes science and mathematics, I hesitate to give advice, in the conventional sense of the word, since no two individuals are driven by the same motivations or circumstances. But from my own experience, I can offer the following observation. My work is not a stand-alone project, nor would I have succeeded to the extent that I did, had I attempted it as one. Instead, it is more like a rung of a ladder, supported by rungs that others built, and serving as support for future rungs.

2. Research Section

Solutions to the Yang-Baxter equation–an important equation in mathematics and physics–lead to matrix representations of a collection of all braids known as the braid group. Such representations have applications in fields such as knot theory, statistical mechanics, and, most recently, quantum information science. In particular, representations with a special property called unitarity are desired because they generate braiding quantum gates. These quantum analogs of classical gates are actively studied in the ongoing quest to build a topological quantum computer that could be exponentially more powerful than our computers today.

A generalized form of the Yang-Baxter equation was proposed a few years ago by Eric Rowell et al. By solving the generalized Yang-Baxter equation, we found new unitary braid group representations. Our representations give rise to braiding quantum gates and thus have the potential to aid in the construction of useful quantum computers.

2.1. **Background Information: The Yang-Baxter Equation.** The Yang-Baxter equation (YBE) in dimension d is a matrix equation whose solution is a $d \times d$ matrix R with complex number entries. The equation can be written as follows, where I_V may be thought of as the $d \times d$ identity matrix, and $\otimes$ is the tensor product, a matrix operator somewhat akin to multiplication:

$$\text{(YBE)}\ \ (R \otimes I_V)(I_V \otimes R)(R \otimes I_V) = (I_V \otimes R)(R \otimes I_V)(I_V \otimes R).$$

Figure 1 is a pictorial representation of the equation. Two crossed strands are the solution matrix R and a straight strand is the identity matrix. Multiplication goes from bottom to top. The reason this representation is useful will be seen in the background information on the braid group.

2.2. **Background Information: The Braid Group.** As mentioned previously, the braid group is a collection of all braids. To gain a basic understanding of the mathematical braid, we think of a braid in a girl's hair: it is created through a series of steps, in each of which we take two of the braid's three strands and cross either the left strand over the right or the right over the left, in alternating fashion.

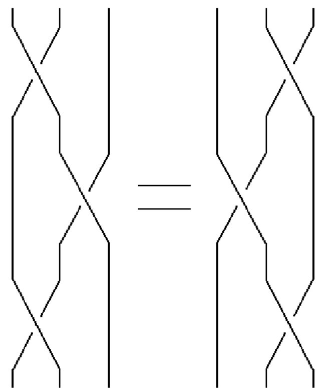

Figure 1. The Yang-Baxter equation

If we are instead free to choose at every step which crossing to do, we can generate any three-strand braid.

More generally, any braid on n strands can be generated using the elements $\sigma_1, \sigma_2, ..., \sigma_{n-1}$ (see Figure 2). For example, the famous 4-braid (Figure 3) of C. F. Gauss, the first mathematician to seriously consider braids as a mathematical concept, is $\sigma_3\sigma_2^{-1}\sigma_2^{-1}\sigma_1\sigma_3$, where the product $\alpha\beta$ of two braids α and β is the "stacking" of β on α.

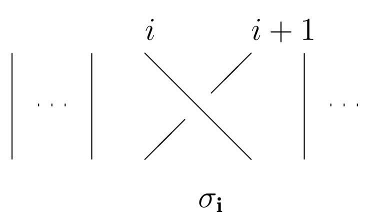

Figure 2. Braid group generator

The braid group has two defining relations:

(1) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $1 \leq i \leq n-2$, and

(2) $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geq 2$.

Figure 3. Gauss' 4-braid

The first is commonly called the braid relation and the second far commutativity (Figure 4).

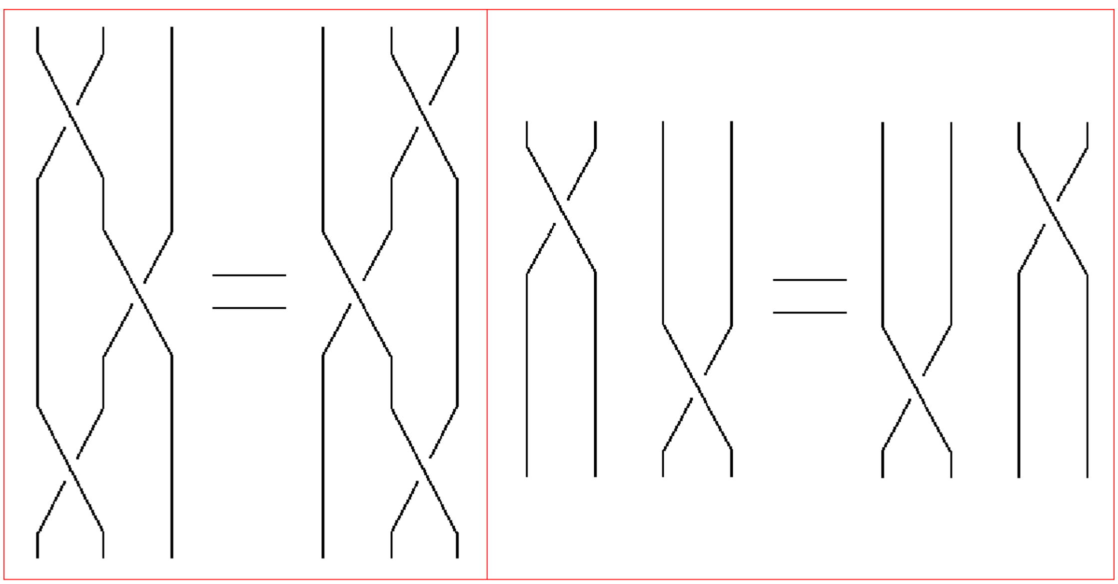

Figure 4. The braid relation (left) and far commutativity (right)

A matrix representation of the braid group is created by assigning a matrix to every braid so that both relations are satisfied. It is easy to see that the braid relation looks exactly like our picture of the YBE. In fact, the assignment that we used for that picture leads to a representation of the braid group that also satisfies far commutativity and thus is a valid representation. For example, the 4-braid in

Figure 3 is represented by the matrix

$$(I_V \otimes I_V \otimes R)(I_V \otimes R^{-1} \otimes I_V)(I_V \otimes R^{-1} \otimes I_V)(R \otimes I_V \otimes I_V)(I_V \otimes I_V \otimes R).$$

2.3. **Background Information: Topological Quantum Computation.** Given two anyons in a plane, we can switch their positions by either a clockwise swap or a counterclockwise swap. When we map their trajectories in space-time (i.e., their world lines) during the swaps, we get a braid group generator and its inverse! Furthermore, all possible braidings of any number of anyons can be generated by switching adjacent anyons in this fashion.

Each "swap" is done by application of a braiding quantum gate. In fact, a computation is performed by repeatedly applying such gates (Figure 5). Thus, braiding quantum gates can be directly generated by matrix representations of the braid group, with one additional constraint: the representation must be unitary. A unitary matrix M is one such that $M^\dagger M = I$, where $M^\dagger$ is the conjugate transpose of M–the matrix obtained by flipping M along its diagonal and taking the complex conjugate of each entry.

2.4. **Problem Overview: The (d, m, l)-generalized Yang-Baxter Equation.** Unitary solutions to the YBE lead to unitary braid group representations, which generate braiding quantum gates. This project looks at what unitary solutions exist to the generalized Yang-Baxter equation (gYBE) and whether such solutions lead to braid group representations. Whereas the regular YBE is indexed by a single natural number, its dimension d, the gYBE has three parameters d, m, and l, and its solution, which we call a (d, m, l)-R-matrix is a complex matrix of size $d^m \times d^m$:

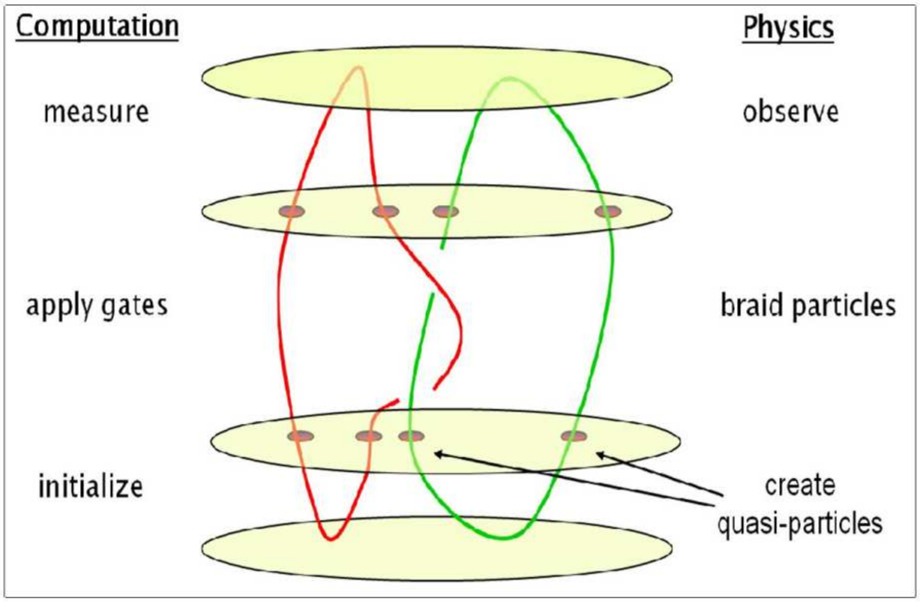

FIGURE 5. Topological quantum computation

$$\text{(gYBE)}\quad (R\otimes I_V^{\otimes l})(I_V^{\otimes l}\otimes R)(R\otimes I_V^{\otimes l}) = (I_V^{\otimes l}\otimes R)(R\otimes I_V^{\otimes l})(I_V^{\otimes l}\otimes R).$$

We focus on the $(2,3,1)$-gYBE, whose solution is of size 8×8:

$$R_1R_2R_1 = R_2R_1R_2,$$

where $R_1 = R\otimes I_2$ and $R_2 = I_2\otimes R$.

The $(2,3,1)$-gYBE can also be given a pictorial representation (Figure 6). An x-shaped crossing is the action of the $(2,3,1)$-R-matrix, and there are three strands leading to and from each crossing because $m=3$.

2.5. **Approach:**(2×2)**-diagonally unitary.** Prior to this project, only one essentially new solution to the $(2,3,1)$-gYBE was known:

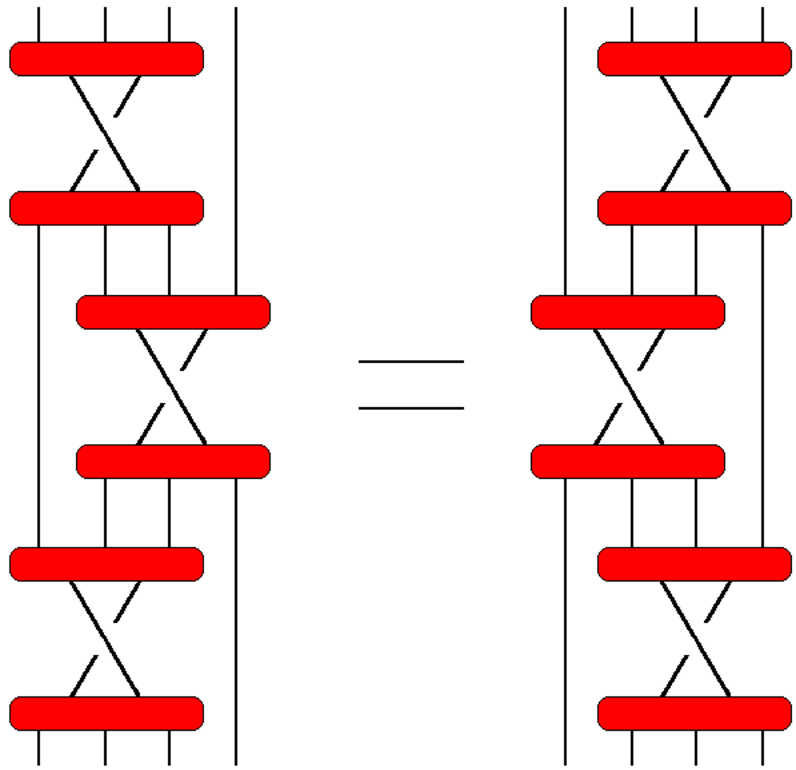

Figure 6. The $(2,3,1)$-generalized Yang-Baxter equation

Let $\zeta = e^{2\pi i/8}$. Then this solution, which we call the Rowell solution, is

$$R_\zeta = \frac{1}{\sqrt{2}}\begin{pmatrix} \zeta^{-1} & 0 & -\zeta^{-1} & 0 \\ 0 & \zeta & 0 & \zeta \\ \zeta & 0 & \zeta & 0 \\ 0 & -\zeta^{-1} & 0 & \zeta^{-1} \end{pmatrix} \oplus \frac{1}{\sqrt{2}}\begin{pmatrix} \zeta & 0 & \zeta & 0 \\ 0 & \zeta^{-1} & 0 & -\zeta^{-1} \\ -\zeta^{-1} & 0 & \zeta^{-1} & 0 \\ 0 & \zeta & 0 & \zeta \end{pmatrix}.$$

The $\oplus$ operator is the direct sum, which takes its two inputs and puts them along the diagonal of the output matrix, setting all other entries to 0.

The Rowell solution has the property that not only is the solution itself unitary but every 2×2 block whose entries do not consist of all zeroes is also unitary.

Also, each of these unitary 2×2 blocks is diagonal–that is, all entries not along the diagonal are zeroes. We searched for solutions to the $(2,3,1)$-gYBE of the same form as the Rowell solution: $R = X \oplus Y$, where X and Y are such that their 2×2 blocks are all diagonal and unitary. When a 4×4 matrix has this property, we dubbed it (2×2)-diagonally unitary.

2.6. **Theorem: Three Families of New Solutions.** We classified three families of new solutions to the $(2,3,1)$-gYBE. Our main result is as follows:

Theorem 2.1. *If an 8×8 unitary matrix solution R to the $(2,3,1)$-gYBE is of the form $R = X \oplus Y$, where the 4×4 matrix X is (2×2)-diagonally unitary, then*

(1) *R is equivalent to an $R(\theta)$ in one of the following three families for some $0 \leq \theta \leq \pi$:*

(a)

$$R(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & i & 0 & e^{i\theta} \\ -i & 0 & i & 0 \\ 0 & -ie^{-i\theta} & 0 & 1 \end{pmatrix} \oplus \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 & e^{i\theta} & 0 \\ 0 & 1 & 0 & -e^{2i\theta} \\ -ie^{-i\theta} & 0 & 1 & 0 \\ 0 & ie^{-2i\theta} & 0 & i \end{pmatrix},$$

(b)

$$R(\theta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & i & 0 & e^{i\theta} \\ -1 & 0 & 1 & 0 \\ 0 & e^{-i\theta} & 0 & i \end{pmatrix} \oplus \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 & e^{i\theta} & 0 \\ 0 & 1 & 0 & -e^{2i\theta} \\ e^{-i\theta} & 0 & i & 0 \\ 0 & e^{-2i\theta} & 0 & 1 \end{pmatrix},$$

(c)

$$R(\theta) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & e^{i\theta} \\ -1 & 0 & 1 & 0 \\ 0 & -e^{-i\theta} & 0 & 1 \end{pmatrix} \oplus \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & -e^{i\theta} & 0 \\ 0 & 1 & 0 & -e^{2i\theta} \\ e^{-i\theta} & 0 & 1 & 0 \\ 0 & e^{-2i\theta} & 0 & 1 \end{pmatrix}.$$

(2) *Any two different* $(2,3,1)$-*R-matrices in the three families above are not equivalent to each other.*

(3) *For each* $(2,3,1)$-*R-matrix above,* X *is different from* Y *except when* $\theta = \pi$ *in the third family. Therefore, neither* X *nor* Y *is a solution to the YBE unless for* $\theta = \pi$ *in the third family.*

For the proof, please refer to Section 3.1 of [C].

2.7. **Applications: Braiding Quantum Gates.** Since the braid relation is again automatically satisfied, to check whether unitary solutions to the $(2,3,1)$-gYBE lead to braid group representations, it is necessary to determine whether far commutativity is satisfied (Figure 7) by the representation given by the assignment seen in the pictorial representation of the gYBE (Figure 6). We found that far commutativity is satisfied if and only if the 2×2 blocks of X and Y are all diagonal or $X = Y$. Thus, all of our solutions lead to valid unitary representations of the braid group, which have applications in quantum information theory.

2.8. **Conclusion.** The quest to build a topological quantum computer is at the cutting edge of technology, with exciting theoretical and experimental breakthroughs being made at astonishing rates. However, an obstacle to further progress is that there exists no way to reliably generate the braiding quantum gates indispensable to computation. This project makes theoretical headway in overcoming

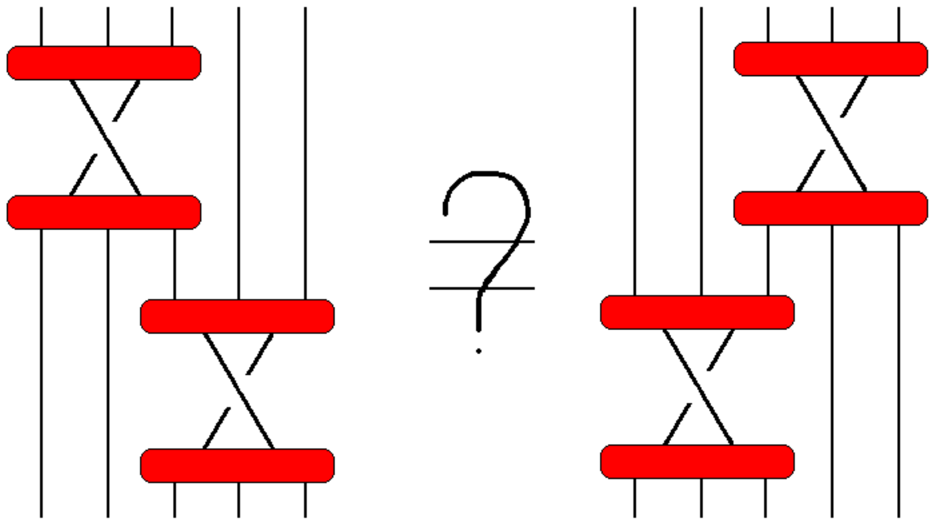

FIGURE 7. Far commutativity for the (2,3,1)-generalized Yang-Baxter equation

this problem by introducing the method of solving the generalized Yang-Baxter equation to find unitary braid group representations that directly generate braiding quantum gates. Not only does the project find three families of solutions to the $(2, 3, 1)$-generalized Yang-Baxter equation, but it also presents a systematic approach that other researchers could repeat to search for further solutions. The realization of the resulting braiding quantum gates in physical systems would lead to large-scale topological quantum computers that would be much more efficient than any known classical computer, bringing great benefits to society through revolutionary scientific advances in fields such as chemistry and material science.

REFERENCES

[C] R. S. Chen, *Generalized Yang-Baxter Equations and Braiding Quantum Gates,* Journal of Knot Theory and Its Ramifications, 21(2012), No. 9, Article No. 1250087, arXiv:1108.5215v1.