

**QUANTUM SOFTWARE ENGINEERING. PT. I: QUANTUM CIRCUIT (GATE) MODEL BASED COMPUTING – EDUCATION LECTURES AND PEDAGOGICAL WORKSHOP<sup>1</sup>****Ulyanov Sergey<sup>1</sup>, Reshetnikov Andrey<sup>2</sup>, Tyatyushkina Olga<sup>3</sup>, Korenkov Vladimir<sup>4</sup>**

<sup>1</sup>*Doctor of Science in Physics and Mathematics, professor;  
Dubna State University,  
Institute of the system analysis and management;  
Leader Researcher of LIT JINR  
141980, Dubna, Moscow reg., Universitetskaya str., 19;  
e-mail: ulyanovsv@mail.ru.*

<sup>2</sup>*PhD, associate professor;  
Dubna State University,  
Institute of the system analysis and management;  
141980, Dubna, Moscow reg., Universitetskaya str., 19;  
e-mail: agrehetnikov@gmail.com.*

<sup>3</sup>*Ph D, associate professor;  
Dubna State University,  
Institute of the system analysis and management;  
141980, Dubna, Moscow reg., Universitetskaya str., 19;  
e-mail: tyatyushkina@mail.ru.*

<sup>4</sup>*Doctor of Science in Physics and Mathematics, professor;  
Dubna State University,  
Institute of the system analysis and management;  
Leader Researcher of LIT JINR  
141980, Dubna, Moscow reg., Universitetskaya str., 19;  
e-mail: korenkov@jinr.ru.*

*All the quantum algorithms are based on a certain quantum computing model, varying from the quantum circuit, one-way quantum computation, adiabatic quantum computation and topological quantum computation. These four models are equivalent in computational power; among them, the quantum circuit model is most frequently used. In the circuit model, it has been proved that arbitrary single-qubit rotations plus two-qubit controlled-NOT gates are universal, i.e. they can provide a set of gates to implement any quantum algorithm. This article discusses the goal for this research: it is to given a lightning-fast (as-barebones-as-possible) definition of the quantum circuit model computing and leisurely development of quantum computation before actually getting around to sophisticated algorithms. In this article the main ideas of quantum software engineering is described.*

**Keywords:** quantum computing, quantum gate design, quantum algorithm, universal quantum circuit.

**For citation:**

Quantum software engineering. Pt. I: Quantum Circuit (Gate) Model based Computing – education Lectures and pedagogical workshop / S. Ulyanov, A. Reshetnikov, O. Tyatyushkina, V. Korenkov // System Analysis in Science and Education. – 2020. – № 3. – Pp. 129–201. – URL: <http://sanse.ru/download/408>.

---

<sup>1</sup> The text course of lectures “Quantum Software Engineering” in “International School of Big Data and Data Science”, JINR (Scientific Supervisor: V.V. Korenkov)

## КВАНТОВАЯ ПРОГРАММНАЯ ИНЖЕНЕРИЯ. Ч. 1: КВАНТОВЫЕ ВЫЧИСЛЕНИЯ НА ОСНОВЕ КВАНТОВЫХ АЛГОРИТМИЧЕСКИХ ЯЧЕЕК – ОБРАЗОВАТЕЛЬНЫЙ И ПЕДАГОГИЧЕСКИЙ ПРАКТИКУМ

Ульянов Сергей Викторович<sup>1</sup>, Решетников Андрей Геннадьевич<sup>2</sup>,  
Тятюшкина Ольга Юрьевна<sup>3</sup>, Кореньков Владимир Васильевич<sup>4</sup>

<sup>1</sup>Доктор физико-математических наук, профессор;  
ГБОУ ВО МО «Университет «Дубна»,  
Институт системного анализа и управления;  
141980, Московская обл., г. Дубна, ул. Университетская, 19;  
e-mail: ulyanovsv@mail.ru.

<sup>2</sup>Кандидат технических наук, доцент;  
ГБОУ ВО МО «Университет «Дубна»,  
Институт системного анализа и управления;  
141980, Московская обл., г. Дубна, ул. Университетская, 19;  
e-mail: agreshetnikov@gmail.com.

<sup>3</sup>Кандидат технических наук, доцент;  
ГБОУ ВО МО «Университет «Дубна»,  
Институт системного анализа и управления;  
141980, Московская обл., г. Дубна, ул. Университетская, 19;  
e-mail: tyatyushkina@mail.ru.

<sup>4</sup>Доктор физико-математических наук, профессор;  
ГБОУ ВО МО «Университет «Дубна»,  
Институт системного анализа и управления;  
141980, Московская обл., г. Дубна, ул. Университетская, 19;  
e-mail: korenkov@jinr.ru.

В данной статье рассматриваются вопросы проектирования квантовых алгоритмических ячеек для эффективного моделирования квантовых алгоритмов на классических компьютерах. Проведен анализ и выбор структуры универсальных квантовых схем для реализации логических операций. Квантовая программная инженерия рассматривается как составная часть сквозных квантовых ИТ и квантовой релятивистской информатики, особенности которых рассматриваются в данной статье.

**Ключевые слова:** квантовые вычисления, квантовый алгоритм, проектирование квантовых алгоритмических ячеек, универсальные квантовые схемы.

### Для цитирования:

Quantum software engineering. Pt. I: Quantum Circuit (Gate) Model based Computing – education Lectures and pedagogical workshop = Квантовая программная инженерия. Ч. 1: Квантовые вычисления на основе квантовых алгоритмических ячеек – образовательный и педагогический практикум / S. Ulyanov, A. Reshetnikov, O. Tyatyushkina, V. Korenkov // Системный анализ в науке и образовании: сетевое научное издание. – 2020. – № 3. – С. 129–201. – На англ. языке. – URL: <http://sanse.ru/download/408>.

### Introduction

In the 1980s by Feynman and Manin was pioneered the idea of quantum computation mainly, with Albert independently introducing quantum automata and with Benioff analyzing the link between quantum mechanics and reversible classical computation. The initial idea of Feynman was the following: Although it is perfectly possible to use a (normal) computer to simulate the behavior of  $n$ -particle systems evolving according to the laws of quantum, it seems be extremely inefficient. In particular, it seems to take an amount of time/space that is exponential in  $n$ . This is peculiar because the actual particles can be viewed as simulating themselves efficiently. So, why not call the particles themselves a "computer"? After all, although we have sophisticated theoretical models of (normal) computation, in the end computers are ultimately physical objects operating

according to the laws of physics. If we simply regard the particles following their natural quantum-mechanical behavior as a computer, then this “quantum computer” appears to be performing a certain computation (namely, simulating a quantum system) exponentially more efficiently than we know how to perform it with a normal, “classical” computer. Perhaps we can carefully engineer multi-particle systems in such a way that their natural quantum behavior will do other interesting computations exponentially more efficiently than classical computers can.

This is the basic idea behind quantum computers. As it turns out, you can get (seemingly) exponential speedups for a (seemingly) small number of natural computational problems by carefully designing a multi-particle quantum system and letting it evolve according to the (100-year old, extremely well-confirmed) laws of quantum mechanics. By far the most spectacular example is Shor's factoring algorithm, an algorithm implementable on a quantum computer that can factor any  $n$ -digit integer (with high probability) in roughly  $n^2$  time. This is contrast to the fact that the fastest known “classical” algorithm for factoring  $n$ -digit integers seems to require roughly  $2^{n^{1/3}}$  time, and in fact the presumed computational difficulty of factoring is relied upon in an enormous number of real-world cryptographic applications.

The goal for this research is to give a lightning-fast (as-barebones-as-possible) definition of the quantum circuit model computing and leisurely development of quantum computation before actually getting around to sophisticated algorithms [1].

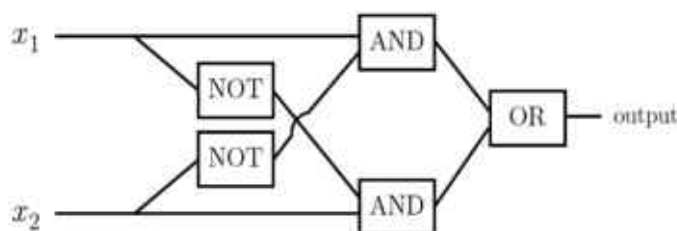
It is well known that 90% of the understanding of the quantum circuit model is achieved by reviewing three purely “classical” topics: classical Boolean circuits; reversible classical circuits; and randomized computation. The first and third of these topics should be very familiar to anyone who has studied the basics of theoretical computer science. And the second topic is very cute and elementary. Once we have these three concepts in hand, quantum circuits become practically just a tiny “twist” on randomized computation - what you might get if you tried to invent a model of randomized computation in which “probabilities” can be negative.

**Classical Boolean circuits.** Several models of computation/algorithms are studied in the classical theory of computation: Turing Machines, high-level programming languages, and Boolean circuits. It turns out that for the study of quantum computation, the Boolean circuit model is by far the easiest model to generalize (being as it the closest model of the physical reality of computers).

We begin with the following well known fact, stating that any computational task (modeled by a Boolean function) we might want to do is doable with an AND/OR/NOT Boolean circuit.

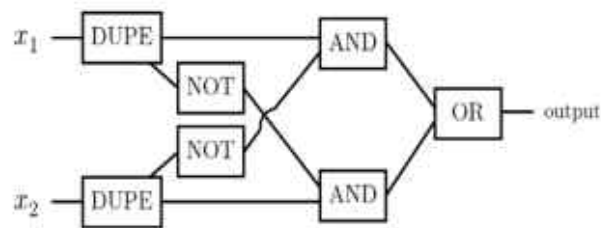
*Proposition 1.* Any Boolean function  $f : \{0,1\}^n \rightarrow \{0,1\}^m$  is computable by a Boolean circuit  $C$  using just AND, OR, and NOT gates. I.e., AND, OR, and NOT gates are *universal*.

The AND and OR gates mentioned in this proposition take 2 input bits and produce 1 output bit. The NOT gate takes 1 input bit and produces 1 output bit. Every Boolean function is computable by some circuit, we usually become interested in computing it efficiently; i.e., with a circuit  $C$  of small size. The size of the circuit,  $\text{size}(C)$ , is defined to be the number of gates it uses. Circuit size fairly closely corresponds to running time in the Turing Machine (sequential algorithm) model. For example, it is known that a circuit of size  $s$  can be evaluated in time  $O(s \log s)$  by a Turing Machine, and conversely, a Turing Machine operating in time  $t$  on length- $n$  inputs can be converted to an  $n$ -input circuit of size  $O(t \log t)$ . Here is a simple example of a circuit computing the XOR function,  $f(x_1, x_2) = x_1 \oplus x_2$ .



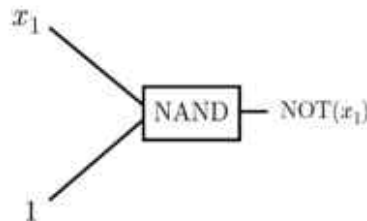
The lines in this diagram are called “wires”, and the things inside the rectangles are called “gates”. In the diagram we have followed a traditional circuit-theory convention by allowing wires to “branch”; i.e., split into two copies. In reality, some physical mechanism must exist at these branches, and in the future, it will be

convenient to make this explicit. So, we will introduce a new kind of gate called a DUPE (duplicate) gate which takes 1 input bit and outputs 2 duplicate copies of that bit. We will then redraw the above diagram as follows:



With this convention, it would be more accurate to say that AND, OR, NOT, and DUPE gates are universal for Boolean circuit computation.

It is also a well-known fact that one can get smaller universal gate sets; in fact, one can replace AND/OR/NOT gates with just NAND gates. (Recall that  $\text{NAND}(x_1, x_2) = \text{NOT}(\text{AND}(x_1, x_2))$ .) To see this, first note that we can eliminate OR gates using De Morgan's rule:  $\text{OR}(x_1, x_2) = \text{NOT}(\text{AND}(\text{NOT}(x_1), \text{NOT}(x_2)))$ . Then we can eliminate AND gates in favor of NAND gates via  $\text{AND}(x_1, x_2) = \text{NOT}(\text{NAND}(x_1, x_2))$ . Finally, we need to show that NOT gates can be eliminated using NAND gates. One way to implement  $\text{NOT}(x_1)$  with a NAND gate is as follows:



On the lower left in this diagram, we have what is called an ancilla bit: an input that is “hardwired” to the constant bit 1, for the purposes of assisting the computation. It's actually possible to implement  $\text{NOT}(x_1)$  using NAND and DUPE without the use of ancillas (specifically, via  $\text{NAND}(\text{DUPE}(x_1))$ ). However, the above method gives us a good opportunity to introduce the notion of ancillas.

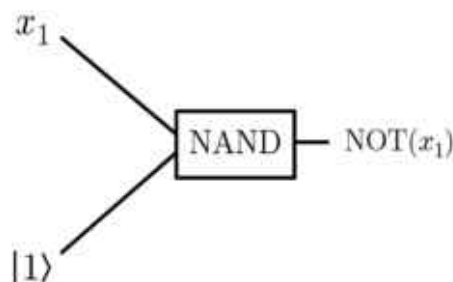
What we have just shown is the following:

*Proposition 2.* Boolean NAND and DUPE gates (along with the use of ancillas) are *universal* for computation.

In fact, we have shown something stronger: Not only can every AND/OR/NOT/DUPE circuit  $C$  be converted to an equivalent AND/OR/NOT circuit  $C'$ , this conversion can be done very efficiently; there is an efficient algorithm carrying out the conversion, and  $\text{size}(C') = O(\text{size}(C))$ .

We take this opportunity to introduce a bit of unusual notation that will play an essential role in the remainder of the course. This is the “bra - ket” notation invented by Paul Dirac.

Actually, we will postpone the mathematical definitions to the next chapters; for now, we will just introduce it as pure symbolism. We will henceforth enclose bits and bit-strings in asymmetrical brackets called kets, writing  $|0\rangle$  and  $|1\rangle$  instead of 0 and 1. We will also usually eliminate internal brackets when writing strings; e.g., writing  $|011\rangle$  instead of  $|0\rangle|1\rangle|1\rangle$ . As a small example of this notation, we will redraw the previous diagram as follows:



**Reversible computation.** In actual physical reality, a theoretical bit ( $|0\rangle$  or  $|1\rangle$ ) is implemented by a particle or bunch of particles (e.g., high or low voltage on a physical wire). Similarly, a gate is implemented by a physical object (a “switch” or some other gadget) that manipulates the bit-representations.

We then would ideally like to think of the circuit as a “closed physical system”. Unfortunately, for a typical AND/OR/NOT/DUPE circuit, this is not possible. The reason is that the laws of physics governing microscopic systems (both classical and quantum) are *reversible* with respect to time, but this is not true of most gates we would like to physically implement.

Take for example an AND gate. Suppose its output is  $|0\rangle$ . Can we infer what its inputs were? The answer is “no” - they could have been  $|00\rangle$ ,  $|01\rangle$ , or  $|10\rangle$ . The AND process is not reversible: information sometimes needs to be deleted; “entropy” is lost. According to the 2<sup>nd</sup> Law of Thermodynamics, a physical system consisting of a single AND gate cannot be “closed”; its operation must dissipate some energy - typically as escaping heat. On the other hand, a NOT gate is theoretically “reversible”: its output can be determined from its input; no information is created or destroyed in switching  $|0\rangle$  to a  $|1\rangle$  or vice versa. Thus, in principle, it is possible to construct a completely closed physical system implementing a NOT gate, without the need for energy dissipation.

*Remark.* These issues were studied in the 1960s and 1970s by Landauer and Bennett, among others. They raised the question of whether there are Boolean gates that are both reversible and universal. If so, then by using them it would be possible - at least according to the theoretical laws of physics - to have circuits doing general computation without dissipating any energy. On one hand, as we will see shortly, it is possible to find universal reversible gates. On the other hand, it turned out that from a practical point of view, the energy dissipation of standard electronic circuits did not prove to be a major problem (although laptops sometimes do get rather hot in your lap). On the other hand, it turns out to be important for the quantum circuit model that universal reversible computation is possible. So, we will now explain how to do it.

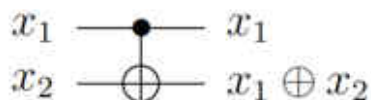
We begin with a *definition*: A Boolean gate  $G$  is said to be reversible if it has the same number of inputs as outputs, and its mapping from input strings to output strings is a bijection.

Thus, a NOT gate is reversible, whereas most other “standard” gates (e.g., AND, OR, NAND, and DUPE) cannot be reversible since they do not have an equal number of inputs and outputs.

Let's introduce a new, simple, reversible gate, the CNOT (controlled-NOT) gate. It has 2 input bits and 2 output bits, and is drawn like this:



Its behavior is as follows:



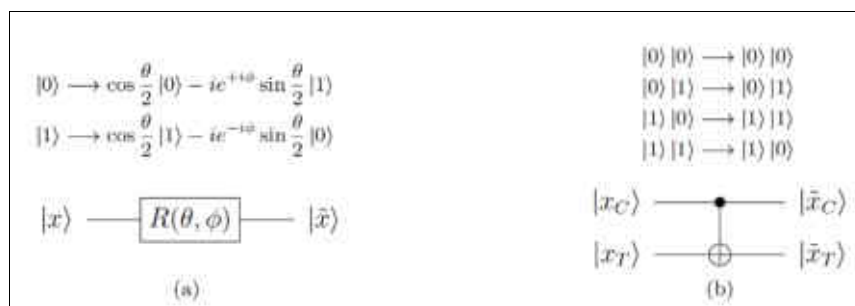
That is, the first input bit  $x_1$  is always passed through directly; the second bit gets NOT applied to it if and only if the “control” bit  $x_1$  is  $|1\rangle$ . To be even more explicit, CNOT has the following truth table:

CNOT:

input	output
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

*Remark.* There are several known quantum algorithms that offer various advantages or speedups over classical computing approaches, some even reducing the complexity class of the problem. These algorithms generally proceed by controlling the quantum interference between the components of the underlying entangled superpositions in such a way that only one or relatively few quantum states have a significant amplitude in the end. A subsequent measurement can therefore provide global information on a massive superposition state with significant probability. The coherent manipulation of quantum states that defines a quantum algorithm can be expressed through different quantum computational modes with varying degrees of tunability and control. The most powerful quantum computing mode presently known is the universal gate model, similar to universal gate models of classical computation. Here, a quantum algorithm is broken down to a sequence of modular quantum operations or gates between individual qubits.

There are many universal quantum gate families operating on single and pairwise qubits, akin to the NAND gate family in classical computing. One popular universal quantum gate family is the grouping of two-qubit CNOT gates on every pair of qubits along with rotation gates on every single qubit, as displayed below.



The rotation and controlled-NOT (CNOT) gates are an example of a universal quantum gate family when available on all qubits, with explicit evolution (above) and quantum circuit block schematics (below). (a) The single-qubit rotation gate  $R(\theta, \phi)$ , with two continuous parameters  $\theta$  and  $\phi$ , evolves input qubit state  $|x\rangle$  to output state  $|\hat{x}\rangle$ . (b) The CNOT (or reversible XOR) gate on two qubits evolves two (control and target) input qubit states  $|x_C\rangle$  and  $|x_T\rangle$  to output states  $|\hat{x}_C = x_C\rangle$  and  $|\hat{x}_T = x_C \oplus x_T\rangle$ , where  $\oplus$  is addition modulo 2, or equivalently the XOR operation.

With universal gates, an arbitrary entangled state and thus any quantum algorithm can be expressed. Alternative modes such as measurement-based or cluster-state quantum computing can be shown to be formally equivalent to the universal gate model. Like the NAND gate in classical CMOS technology, the particular choice of universal gate set or even mode of quantum computing is best determined by the quantum hardware itself and its native interactions and available controls.

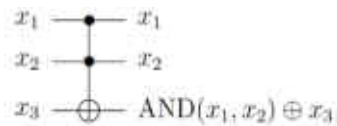
The structure of the algorithm itself may also impact the optimal choice of gate set or quantum computing mode. There are other modes of quantum computation that are not universal, involving subsets of universal gate operations, or certain global gate operations with less control over the entire space of quantum states. These can be useful for specific routines or quantum simulations that may not demand full universality.

Although global adiabatic Hamiltonian quantum computing can be made universal in certain cases, it is often better implemented as non-universal subroutines for specific state preparation.

Quantum annealing models do not appear to be universal, and there is current debate over the advantage such models can have over classical computation. Gates that explicitly include error, or decoherence processes, used to model quantum computer systems interacting with an environment via quantum simulation, we consider outside the scope of this discussion.

This mapping is indeed a bijection, confirming that CNOT is a reversible gate.

We now describe a small but important generalization, called the CCNOT (controlled-controlled-NOT) or Toffoli gate. The below diagram indicates how this 3-input, 3-output gate is drawn, as well as its behavior:



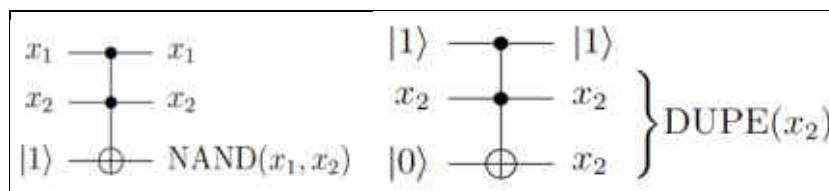
In other words, the first two inputs to a CCNOT gate are passed through directly, and the third input is negated if and only if the first two “control” input bits are both  $|1\rangle$ . Explicitly, we have the following truth table, showing that CCNOT is reversible:

CCNOT:	input	output
	$ 000\rangle$	$ 000\rangle$
	$ 001\rangle$	$ 001\rangle$
	$ 010\rangle$	$ 010\rangle$
	$ 011\rangle$	$ 011\rangle$
	$ 100\rangle$	$ 100\rangle$
	$ 101\rangle$	$ 101\rangle$
	$ 110\rangle$	$ 111\rangle$
	$ 111\rangle$	$ 110\rangle$

In general, we use the convention that attaching a dot to a  $k$ -input/ $k$ -output gate  $G$  with a vertical line means creating a “controlled- $G$ ” gate. This is the  $(k + 1)$ -input/ $(k + 1)$ -output gate that passes through its first, “control”, bit, and which either applies  $G$  or doesn't depending on whether the control bit is  $|1\rangle$  or  $|0\rangle$ . Assuming that a NOT gate is drawn as  $\oplus$ , this explains the picture used for CNOT and CCNOT gates.

The three examples of reversible gates we have seen so far - NOT, CNOT, CCNOT - also have the extra property that they are their own inverse; i.e., applying them twice in succession restores the original bits. This is a bit of a coincidence, insofar as it is not a property we insist on for reversible gates. We merely insist that reversible gates have some inverse gate; the inverse doesn't have to be the gate itself.

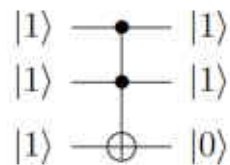
The CCNOT gate is extremely handy: as the following two pictures show, we can use it to simulate both NAND gates and DUPE gates (assuming, as always, that ancillas are allowed):



Note that, in addition to producing the desired NAND and DUPE outputs, these conversions also produce extra, unneeded bits (namely,  $x_1$  and  $x_2$  in the NAND case, and the top  $|1\rangle$  in the DUPE case). This is somewhat inevitable, given that reversible gates are required to have equally many input and output bits.

We call such unwanted outputs *garbage*.

As one more very minor note, the above conversions use both  $|0\rangle$  ancillas and  $|1\rangle$  ancillas. We can also use CCNOT gates to generate  $|0\rangle$ 's from  $|1\rangle$  ancillas as follows:



We have therefore established the following key theorem, which shows that we can do universal computation reversibly. The CCNOT gate is universal, assuming ancilla inputs (all set to  $|1\rangle$ ) and garbage outputs are allowed; any standard AND/OR/NOT circuit for a function  $f: \{0,1\}^n \rightarrow \{0,1\}^m$  may be efficiently transformed into a reversible one that looks like Fig. 1.

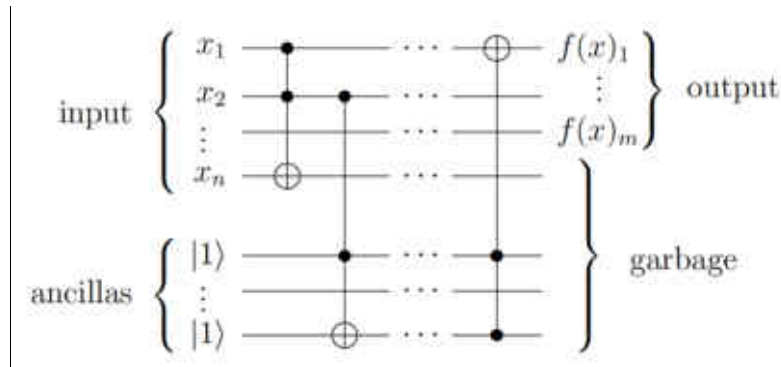
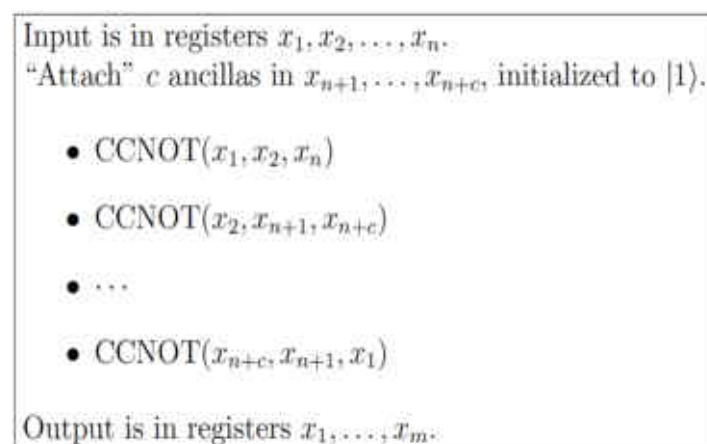


Fig. 1. A typical reversible circuit using CCNOT gates

We remark that the output bits need not be the “topmost”  $m$  bits on the right; we could designate any of the  $m$  bits on the right as the outputs. In reversible circuits we will always have  $n + \# \text{ ancillas} = m + \# \text{ garbage}$ . “In practice”, when doing reversible computing we usually also allow ourselves NOT and CNOT gates. (Given NOT gates, we may assume that all ancillas are fixed to  $|0\rangle$  rather than  $|1\rangle$ , and this is actually a more traditional assumption.)

With “standard” circuits [1,2], the number of wires carrying a bit at any one “time” (vertical slice) may vary. However, with reversible circuits, this will always equal the number of inputs + ancillas, as you can see above. Indeed, one sort of stops thinking about wires and instead thinks of each input/ancilla bit being carried in its own register, which maintains its “identity” throughout the computation. It’s very helpful to think of circuits not just as diagrams but also as “lists of instructions performed on registers”, as in the following description,



which is completely equivalent to the diagram in Fig. 1.

**Randomized computation.** Although we are well used to it now, randomized computation is a bit like the “quantum computation of the ‘60s and ‘70s” - a creative new twist on classical computation, seemingly realizable in practice and potentially allowing for big speedups over deterministic computation, but one



requiring its investigators to make a big investment in a new area of math (i.e., probability). Indeed, there are some computational tasks which we know how to provably solve efficiently using randomized computation, but which we don't know how to provably solve efficiently using only deterministic computation. (An example: on input “ $n$ ”, generate an  $n$ -digit prime number.) Unlike with quantum computation, however, we believe this is mainly due to our lack of skill in proving things, rather than an inherent major advantage of randomized computation. (E.g., we know a deterministic algorithm that we believe efficiently generates  $n$ -digit prime numbers; we just can't prove its efficiency.)

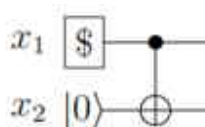
*Remark.* Similarly, random local circuits are currently intensely studied for their  $k$ -design properties, potential to demonstrate quantum supremacy, and understanding operator spread and entanglement growth. Recently, motivated by the demonstration of quantum supremacy, random circuits have become central candidates to show hardness in near-term quantum computing. For example, Google recently demonstrated a 53-qubit experimental demonstration of the hardness of sampling from the output of random circuits. In nature, whenever one studies a quantum system, leakage of information to the environment is at play. A key challenge is to address the effects of decoherence in natural settings or account for it the lab especially now that quantum error correction schemes have not been realized. To model decoherence on the output of a quantum circuit, scenarios have been considered in which after every gate a measurement is performed with some probability. Treating this probability as the order parameter, it is then seen that there is a critical probability below which the entanglement entropy is extensive and above which the state obeys an area law [1].

It is very easy to upgrade the circuit model of computation to a randomized model: we just introduce a single new gate called the COIN gate, drawn like this:

$$\boxed{\text{COIN}} \rightarrow \text{or } \boxed{\$} \rightarrow$$

It has 0 inputs and 1 output; the output is a “fair coin flip”, viz.,  $|0\rangle$  with probability  $1/2$  and  $|1\rangle$  with probability  $1/2$ . You might also imagine allowing other kinds of randomized gates; for example, a  $\text{COIN}_{\frac{1}{3}}$  gate that outputs  $|1\rangle$  with probability  $1/3$  and  $|0\rangle$  with probability  $2/3$ . It turns out that allowing such gates does not fundamentally change the model of randomized computing; although a fair COIN gate cannot simulate a  $\text{COIN}_{\frac{1}{3}}$  gate exactly, it can simulate it close-to-exactly enough that it doesn't really matter. For this reason, we say that the plain COIN gate is (effectively) universal for randomized computation.

We will now describe how to “analyze” randomized circuits. Although our style of analysis will be very simple and pedantic, it will be great practice for analyzing the closely related quantum circuits. Here is an example randomized circuit:



Alternatively, we could think of this circuit as the following “program”:

1.  $x_1$  initialized to  $\boxed{\$}$
2.  $x_2$  initialized to  $|0\rangle$
3.  $\text{CNOT}(x_1, x_2)$

The output of this circuit is  $|00\rangle$  with probability  $\frac{1}{2}$  (if the coin flip is  $|0\rangle$ ) and is  $|11\rangle$  with probability  $\frac{1}{2}$  (if the coin flip is  $|1\rangle$ ). Nevertheless, let's patiently "analyze" it.

The state of  $x_1$  after the coin flip - equivalently, after Line 1 of the program - is

$\frac{1}{2}$  probability of  $|0\rangle$ ,  $\frac{1}{2}$  probability of  $|1\rangle$  or  $\frac{1}{2} \cdot |0\rangle + \frac{1}{2} \cdot |1\rangle$ . The state of  $x_2$  after Line 2 of the program is 1 probability of  $|0\rangle$ , 0 probability of  $|1\rangle$  which we will write in our new notation as  $1 \cdot |0\rangle + 0 \cdot |1\rangle = |0\rangle$ . Here we have used the "usual" laws and notation of arithmetic in the equality. (Again, continue to think of this as shorthand notation.)

Finally, what happens at the end of the circuit, after Line 3?

One could say that we have:

$$\text{State of } x_1 : \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle, \text{ State of } x_2 : \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle.$$

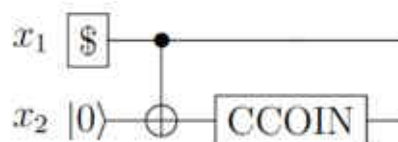
While in some sense this is true (each "register" is equally likely to be  $|0\rangle$  or  $|1\rangle$ ), it's grossly misleading. It makes it look as if the two bits are independent, when in fact they are *correlated*.

So, the above analysis is true but incomplete; to truly capture the correlations in the system we should say: *Joint state* of  $x_1, x_2$  :  $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$ . In presented analyses of randomized circuits, we will keep track of the joint state of all registers all along. For example, in the circuit we have been analyzing the joint state just *prior* to Line 3 would be:  $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$ .

Let's practice some more analysis of "*r*-bit circuits" (where "*r*" standards for "randomized"). For the purposes of practice, we'll invent a new randomized gate,  $\rightarrow \boxed{\text{CCOIN}} \rightarrow$  (CCOIN - "controlled-coin"), which has 1 input and 1 output. Its behavior is the following:

input	output
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$\begin{cases}  0\rangle & \text{with prob. } \frac{1}{2} \\  1\rangle & \text{with prob. } \frac{1}{2} \end{cases}$

Now let's extend the 2 r-bit circuit we had previously been analyzing, as follows:



Equivalently, we are adding the instruction "4. CCOIN( $x_1, x_2$ )" to the program. Now prior to the CCOIN gate, the joint state of the system is :  $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$ .

What is the state after the new CCOIN gate? Here is how you would say it in words: Prior to the CCOIN gate, the state:  $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$  tells us that there is a 1/2 probability that  $x_1$  is  $|0\rangle$  and  $x_2$  is  $|0\rangle$ . In this case, the CCOIN does not touch  $x_1$ , so it stays  $|0\rangle$ , and the CCOIN gate leaves  $x_2$  as  $|0\rangle$  as per its definition.

Thus, the *final state* in this case is still  $|00\rangle$ .

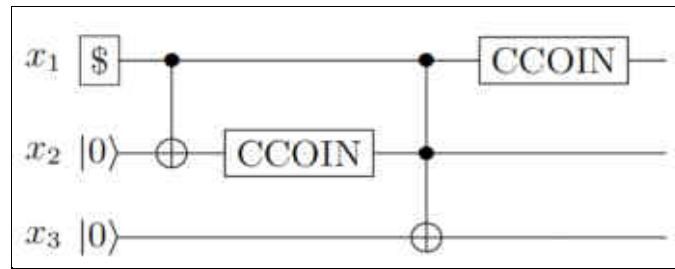
On the other hand, the quantum state:  $\frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle$  tells us that there is a 1/2 probability that  $x_1$  is  $|1\rangle$  and  $x_2$  is  $|1\rangle$ . In this case, the CCOIN does not touch  $x_1$ , so it stays  $|1\rangle$ , and the CCOIN gate changes  $x_2$  to  $|0\rangle$  with probability 1/2 and to  $|1\rangle$  with probability as per its definition. Thus overall the final state is  $|00\rangle$  with probability 1/2, is  $|10\rangle$  with probability  $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$  and is  $|11\rangle$  with probability  $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ .

Here is the math symbolism you would write to exactly model those words:

$$\text{The final state is } \frac{1}{2}|00\rangle + \frac{1}{2}\left(\frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{4}|10\rangle + \frac{1}{4}|11\rangle.$$

So, the natural “arithmetic” you would write with this formalism matches up with the actual probabilistic calculations.

Let’s add a few more twists. Suppose that  $x_3$  is a new register that was in the system all along (we forgot to tell you about it), initialized to  $|0\rangle$  and never touched. Then we would say that the final state of the system is  $\frac{1}{2}|000\rangle + \frac{1}{4}|100\rangle + \frac{1}{4}|110\rangle$ . Finally, suppose we now added a CCOIN( $x_1$ ) instruction, so that the final circuit looked like this:



Now we can calculate the final state as follows.

We start with state  $\frac{1}{2}|000\rangle + \frac{1}{4}|100\rangle + \frac{1}{4}|110\rangle$  and proceed through the “terms” (probabilistic cases) in it. For each one, the last two  $r$ -bits in the string will be unchanged, since the final CCOIN gate only operates on  $x_1$ . If the first  $r$ -bit is  $|0\rangle$  then it will stay  $|0\rangle$ , as per CCOIN’s definition. On the other hand, if the first  $r$ -bit is  $|1\rangle$  then it will become  $|0\rangle$  with probability 1/2 and become  $|1\rangle$  with probability 1/2 (generating two “terms”). Then we simplify. The calculation is:

$$\frac{1}{2}|000\rangle + \frac{1}{4}\left(\frac{1}{2}|000\rangle + \frac{1}{2}|100\rangle\right) + \frac{1}{4}\left(\frac{1}{2}|011\rangle + \frac{1}{2}|111\rangle\right) = \frac{5}{8}|000\rangle + \frac{1}{8}|100\rangle + \frac{1}{8}|011\rangle + \frac{1}{8}|111\rangle.$$

And indeed, had you been asked to compute the final joint state of the 3  $r$ -bits in the above circuit, however be analyzed it would ultimately be pretty close to the pedantic style, and it would have indeed computed that there’s a 5/8 chance of ending with  $|000\rangle$ , a 0 chance of ending with  $|001\rangle$ , a 1/8 chance of ending with  $|100\rangle$ , etc.

*Remark.* An obvious yet important takeaway from this kind of analysis is the following: Suppose we have a circuit with  $n$   $r$ -bit registers. At any time, the state of the circuit can be written as  $\sum_{x \in \{0,1\}^n} p_x |x\rangle$ , where the “coefficient” probabilities  $p_x$  are nonnegative and summing to 1.

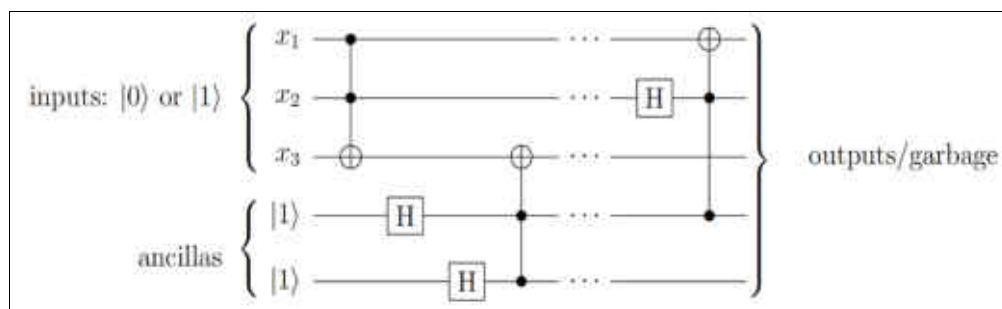
**On measurement.** As a small note, we typically imagine that we provide the inputs to a randomized circuit, and then we observe (or measure) the outputs. The probabilistic “state” of the registers at some intermediate time in the circuit’s execution reflects only the uncertainty that the observers have about the registers’ values. Of course, in reality the registers always have some definite value; it’s merely that these variables are “hidden” to us. Analytically, once we observe one or more of the  $r$ -bits, the probabilistic state “collapses” to reflect the information we learned.

For example, in the randomized circuit we analyzed in the previous section, the final state is  $\frac{5}{8}|000\rangle + \frac{1}{8}|100\rangle + \frac{1}{8}|011\rangle + \frac{1}{8}|111\rangle$ . Suppose for example we measure just the first register,  $x_1$ . The probability amplitude we observe a  $|0\rangle$  is  $\frac{5}{8} + \frac{1}{8} = \frac{6}{8} = \frac{3}{4}$ . Supposing we do observe a  $|0\rangle$ , if we wanted to continue the analysis, we would use the law of conditional probability to deduce that the state of the system “collapses” to

$$\frac{5/8}{3/4}|000\rangle + \frac{1/8}{3/4}|011\rangle = \frac{5}{6}|000\rangle + \frac{1}{6}|011\rangle$$

Here, since we observed that the first bit was  $|0\rangle$ , only the strings consistent with that outcome survive, and the remaining probabilities are renormalized.

**Quantum computing.** Finally, we can introduce the (barest essentials) of the quantum circuit model of computation. As mentioned, it is kind of like what you would get if you took randomized computation but found a way to allow the “probabilities” to be negative. It can also arguably be described as classical reversible computation augmented with the Hadamard gate  $\rightarrow \boxed{H} \rightarrow$ . In other words, a typical quantum circuit with 5 qubit (quantum bit) registers might look like this:



As usual, it is sufficient to just use CCNOT gates in addition to Hadamard gates, but for convenience we also allow NOT and CNOT gates too.

## Basic concepts in quantum gate-based computing

The fact that electronic computers can implement universal computation does not imply that they can always do this efficiently. The word efficiently in this context refers specifically to how fast computational resources (memory and depth [the depth of a Boolean circuit is the maximum number of gates on any path from the input to the output] required by the sequence of operations composing the computation) grows as the size of the problem increases. It is asserted as a premise in computer science that efficient algorithms employ resources that grow polynomially with the size of the problem, meaning proportionally to a (rather low) power of the problem size. In contrast, exponential scaling is considered inefficient. For some computational problems, the most efficient algorithms known scale exponentially with system size. One example of such problems is factoring, for which the most efficient known algorithm scales proportionally to  $\exp(cn^{1/3})$ , with  $n$  being the number of digits (in binary) of the number we want to factor.

**Remark.** A completely automatic synthesis framework for oracle functions is a central part in many quantum algorithms. The proposed framework for resource-constrained oracle synthesis (ROS) is a LUT-based hierarchical method in which every step is specifically tailored to address hardware resource constraints. ROS embeds a LUT mapper designed to simplify the successive synthesis steps, costing each LUT according to the

resources used by its corresponding quantum circuit. In addition, the framework exploits a SAT-based quantum garbage management technique. Those two characteristics give ROS the ability to beat the state-of-the-art hierarchical method both in number of qubits and in number of operations. The efficiency of the framework is demonstrated by synthesizing quantum oracles for Grover's algorithm.

**Preliminaries** Example (q-bits). The states of a spin-1/2 particle (system  $\Sigma(1)$ ) can be thought as points lying on the sphere  $S^2$  of radius 1 (in suitable units). The complex space associated to this system is  $\mathbb{C}^2$  (spinor space). This fact can be argued as follows [3]. Identify  $\xi = x + iy \in \mathbb{C}$  with the point  $(x, y, 0) \in \mathbb{R}^3$  and consider the point  $P = P(\xi)$  of  $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$  obtained by stereographic projection from  $N =$

$$(0, 0, 1): P = \left( \frac{2x}{x^2 + y^2 + 1}, \frac{2y}{x^2 + y^2 + 1}, \frac{x^2 + y^2 - 1}{x^2 + y^2 + 1} \right) \quad (\text{see, Fig. 2})$$

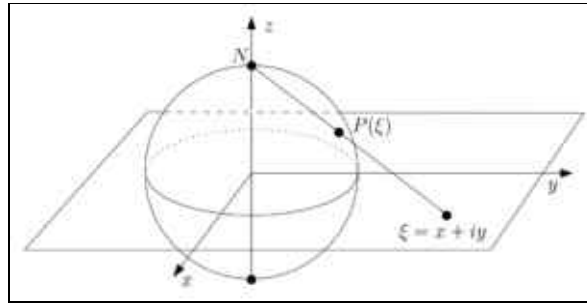


Fig. 2. Stereographic projection

Setting  $P(\infty) = N$ , we get a bijection between  $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$  and  $S^2$ . The inverse map is given by  $(x, y, z) \mapsto \frac{x}{1-z} + i \frac{y}{1-z}$ , for  $z < 1$ , and  $N = [0, 0, 1] \mapsto \infty$ , for  $z = 1$ .

On the other hand, we also have  $\hat{\mathbb{C}} \simeq P\mathbb{C}^2 = P_{\mathbb{C}}^1$ , for any element  $[\xi_0, \xi_1] \in \mathbb{C}^2$  is proportional to a unique vector of the form  $[1, \xi]$  when  $\xi_0 \neq 0$ , and to  $[0, 1]$  if  $\xi_0 = 0$ . Thus, we have a bijective map  $\hat{\mathbb{C}} \mapsto P_{\mathbb{C}}^1$ ,  $\xi \mapsto [1, \xi]$ ,  $\infty \mapsto [0, 1]$ . The inverse map is given by  $[\xi_0, \xi_1] \mapsto \begin{cases} \xi = \xi_1 / \xi_0 & \text{if } \xi_0 \neq 0 \\ \infty & \text{if } \xi_0 = 0 \end{cases}$ . These

considerations indicate that we may take  $\mathbb{C}^2$  as the space associated to  $\Sigma^{(1)}$ . The sphere  $S^2$ , with the structure of  $P_{\mathbb{C}}^1$ , is called the Riemann sphere. It is the simplest compact Riemann surface. In quantum computation references, it is often called the Bloch sphere or even the Poincare–Bloch sphere.

*Remark.* Let  $P = (x, y, z)$  be a point of  $S^2$  and define  $\varphi$  as the argument of  $x + iy$  and  $\theta$  as the angle between  $OP$  and  $ON$ , where  $O$  is the center of the sphere. The relation between the spherical coordinates  $(\varphi, \theta)$  and the cartesian coordinates  $(x, y, z)$  is given by the formulas  $x = \sin \theta \cos \varphi$ ,  $y = \sin \theta \sin \varphi$ ,  $z = \cos \theta$ . The point in  $\hat{\mathbb{C}}$  corresponding to  $P(x, y, z)$  is

$$\xi = \frac{x}{1-z} + i \frac{y}{1-z} = \frac{\sin \theta \cos \varphi}{1 - \cos \theta} + i \frac{\sin \theta \sin \varphi}{1 - \cos \theta} = \frac{\sin \theta}{1 - \cos \theta} e^{i\varphi} = e^{i\varphi} \cot \frac{\theta}{2}.$$

Since this corresponds to the point  $\left[1, e^{i\varphi} \cot \frac{\theta}{2}\right] \sim \left[e^{-i\varphi/2} \sin \frac{\theta}{2}, e^{i\varphi/2} \cos \frac{\theta}{2}\right] \in P_{\mathbb{C}}^1$ , we conclude that

$p = e^{-i\varphi/2} \sin \frac{\theta}{2} |0\rangle + e^{i\varphi/2} \cos \frac{\theta}{2} |1\rangle \in P_{\mathbb{C}}^1$  is the point corresponding to  $P$  under the identification  $S^2 \simeq P_{\mathbb{C}}^1$ . The picture below in Fig. 3 illustrates this relation and also shows some special cases (up to a normalization factor).

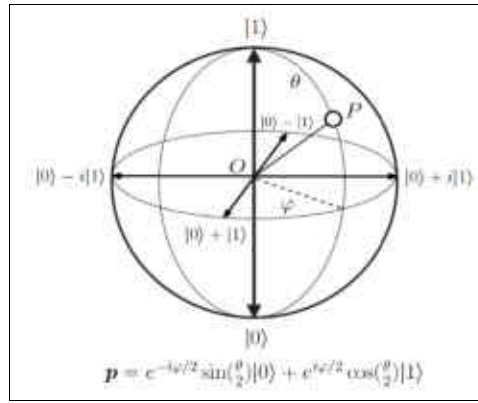


Fig. 3. Bloch sphere of q-bit

Thus  $R_z(\alpha)(p)$  corresponds to  $\rho_z(\alpha)(P)$ , where  $\rho_z(\alpha)$  denotes the rotation about the axis  $O_z$  of amplitude  $\alpha$ . This is a special case of a well-known relation between matrices  $U \in SU(1)$  and rotations of  $S^2$ . This relation can be explained as follows. We can view a matrix  $U = \begin{pmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{pmatrix} \in SU(1)$  as a linear map  $\mathbb{C}^2 \rightarrow \mathbb{C}^2$ :

$\begin{pmatrix} \xi_0 \\ \xi_1 \end{pmatrix} \mapsto U \begin{pmatrix} \xi_0 \\ \xi_1 \end{pmatrix}$ . This map induces a projective map of  $P_c^1$ ,  $[\xi_0, \xi_1] \mapsto [u_0\xi_0 + u_1\xi_1, -\bar{u}_1\xi_0 + \bar{u}_0\xi_1]$  and hence

a map  $\hat{U} : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ ,  $\xi \mapsto \frac{\bar{u}_0\xi - \bar{u}_1}{u_1\xi + u_0}$ ,  $\infty \mapsto \frac{\bar{u}_0}{u_1}$ . This map induces, in turn, the map  $\vec{U} : S^2 \rightarrow S^2$  such that

$\hat{U}(P(\xi)) = P(\hat{U}\xi)$ . If we take  $U$  to be one of the matrices

$$R_z(\varphi) = \begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix}, R_y(\theta) = \begin{pmatrix} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} \\ -\sin \frac{\theta}{2} & \cos \frac{\theta}{2} \end{pmatrix}, R_x(\psi) = \begin{pmatrix} \cos \frac{\psi}{2} & -i \sin \frac{\psi}{2} \\ -i \sin \frac{\psi}{2} & \cos \frac{\psi}{2} \end{pmatrix}.$$

This, together with the relations  $p = e^{-\varphi/2} \sin \frac{\theta}{2} |0\rangle + e^{\varphi/2} \cos \frac{\theta}{2} |1\rangle = R_z(\varphi) R_y(\theta) |1\rangle$ , show that, in terms of  $S^2$ ,  $P = \rho_z(\varphi) \rho_y(\theta) N$ , whose geometric content is clear by the definitions of  $\varphi$  and  $\theta$ . Conversely, this relation, together with the interpretation of  $R_z$  and  $R_y$ , provides a proof of the formula for  $p$ .

The state of a qubit can be modified by applying quantum operations. All possible operations are reversible and can be represented by unitary matrices. Both single-qubit operations and 2-qubit operations are available, the latter changing the state of a qubit according to the state of a second one.

There are different universal sets of quantum operations, targeting different technologies. In this section, we refer to the set that consists of the following operations: Controlled-NOT (CNOT), Hadamard ( $H$ ) and rotations of an arbitrary angle  $\theta$  over the  $Z$ -axis of the Bloch sphere ( $R_z(\theta)$ ). All quantum operations can be represented by unitary matrices of dimension  $2^n \times 2^n$ , where  $n$  is the number of qubits affected by the operations.

For the selected universal set, the representative matrices are:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, R_z(\theta) = \begin{pmatrix} e^{\frac{i\theta}{2}} & 1 \\ 1 & e^{\frac{i\theta}{2}} \end{pmatrix}.$$

A quantum oracle is defined as a “black box” operation performing a multi-output Boolean function  $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ . The effect of an oracle  $O$  performing the operation  $f$  over two registers, one of  $n$  qubits to store

the inputs,  $|x\rangle$ , and one of  $m$  qubits to store the outputs,  $|y\rangle$ , can be described as follows:  $O(|x\rangle \otimes |y\rangle) \mapsto |x\rangle \otimes |y \oplus f(x)\rangle$ . The cost of a quantum circuit depends on the number of qubits required for the computation, and the number of operations that are performed. Automatic tools can be used to take into account technology constraints by synthesizing low cost quantum circuits.

**Rademacher-Walsh spectrum.** We call a function  $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ , where  $\mathbb{F}_2 = \{0, 1\}$ , a Boolean function over  $n$  variables. A Boolean function can be represented by its truth table in the  $\{1, -1\}$  encoding, which is a bitstring  $b_{2^n-1} b_{2^n-2} \dots b_0$  of size  $2^n$  where  $b_x = (-1)^{f(x_1 \dots x_n)}$ , where  $x = (x_1 x_2 \dots x_n)_2$ . The Hadamard transform matrix over  $n$  variables is defined as:  $H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$ ,  $H_0 = 1$ . Each row of the Hadamard transform matrix is equal to the truth table of the parity function between a subset of the  $n$  variables. For example, the last row of an  $n$ -variable Hadamard matrix will be the truth table of the parity function  $p = x_1 \oplus x_2 \oplus \dots \oplus x_n$ .

The Rademacher-Walsh spectrum  $S$  of the function  $f$  expressed as a truth table in the  $\{1, -1\}$  encoding  $F$  is defined as:  $S = H_n F$ . Each coefficient of the spectrum represents the correlation with a parity function of a subset of the inputs.

*Example.* Given the 3-input majority Boolean function  $f(x_1, x_2, x_3) = \langle x_1 x_2 x_3 \rangle$ , its truth table is:  $F = (1 \ 1 \ 1 \ -1 \ 1 \ -1 \ -1 \ -1)$ . The Rademacher-Walsh spectrum of  $f$  is:

$$S = H_3 F = (0 \ 4 \ 4 \ 0 \ 4 \ 0 \ 0 \ -4)$$

*Example: Geometrical Representation of Two-Qubit States and Their Entanglement.* The set of two-qubit pure states with real amplitudes and their geometrical representation onto a real projective space discussed. In this representation, the maximally entangled states –those locally equivalent to the Bell States –form two disjoint circles perpendicular to each other. Taking the natural Riemannian metric on this space, the set of states connected by local gates are equidistant to this pair of circles. Moreover, the unentangled, or so-called product states, are  $\pi/4$  units away to the maximally entangled states. This is, the unentangled states are the farthest away to the maximally entangled states. In this way, if we define two states to be equivalent if they are connected by local gates, we have that there are as many equivalent classes as points in the interval  $[0, \pi/4]$  with the point 0 corresponding to the maximally entangled states. The point  $\pi/4$  corresponds to the unentangled states which geometrically are described by a Klein bottle. Finally, for every  $0 < d < \pi/4$  the point  $d$  corresponds to a disjoint pair of Klein bottles. We also show that if a state is  $d$  units away from the maximally entangled

states, then its entanglement entropy is  $S(d) = 1 - \log_2 \sqrt{\frac{(1 + \sin 2d)^{1 + \sin 2d}}{(1 - \sin 2d)^{-1 + \sin 2d}}}$ . Finally, this geometrical inter-

pretation allows to clearly see the known result that any pair of two-qubit states with real amplitudes can be connected with a circuit that only has single-qubit gates and one controlled-Z gate [4].

*Remark.* To describe the geometry of the real two qubit states we will start by describing a similar situation one dimension lower. Let us assume that the Earth is a perfect sphere with radius 1. In this case the equatorial line would be a perfect circle of radius 1. The name equatorial line turns out to be appropriate due to the fact that circles of radius 1 on the sphere are geodesics. If we take two points on the Equator, the shortest path connecting these two points must be part of the equatorial line. Let us think of the points on Earth that are exactly at a distance  $d$  from the equatorial line and let us denote this set as  $\Sigma_d$ . The distance is being considered from the point of view of the geometry of the sphere. In the case when  $d = 0.785398\dots = \pi/4$ , the set  $\Sigma_d$  consists of all those points on the Earth that are on a latitude 45 degrees north and 45 degrees south. It is not difficult to see that, in general, for positive values of  $d < \pi/2$ ,  $\Sigma_d$  is the union of two disjoint circles of Euclidean radius  $\cos(d)$ . When  $d = \pi/2$ ,  $\Sigma_d$  reduces to only two points, the south and north pole.

Let us move from the two-dimensional sphere  $\mathbb{S}^2 = \{(x_1, x_2, x_3) : x_1^2 + x_2^2 + x_3^2 = 1\}$  to the three-dimensional sphere  $\mathbb{S}^3 = \{(x_1, x_2, x_3, x_4) : x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1\}$ . If  $(x_1, x_2, x_3, x_4)$  are the coordinates of any



vector in  $\mathbb{R}^4$  with respect to the orthonormal basis  $u_1, u_2, u_3, u_4$ , and we consider the circle,  $E = \{\cos(\theta)u_3 + \sin(\theta)u_4, \theta \in \mathbb{R}\}$ , then this circle is a geodesic in  $\mathbb{S}^3$ . Recall that circles of radius one are the geodesics of Euclidean spheres of any dimension. For any positive  $d < \pi/2$ , let us consider the set  $\Sigma_d$  of points in  $\mathbb{S}^3$  that are exactly at a distance  $d$  from the circle  $E$ . This time the set  $\Sigma_d$  is not the disjoint union of two circles but just one torus.

More precisely,  $\Sigma_d = \{x \in \mathbb{S}^3 : x_1^2 + x_2^2 = \sin^2(d), x_1^2 + x_2^2 = \cos^2(d)\}$ . A direct computation shows that, viewing  $\Sigma_d$  as a surface of  $\mathbb{S}^3$ , its Gauss curvature is zero and the principal curvatures are  $\tan(d)$  and  $-\cot(d)$ . The surface  $\Sigma_{\pi/4}$  played an important role in the study of minimal surface on  $\mathbb{S}^3$  since it was conjectured by Lawson in 1970 that this surface was the only embedded minimal torus on the sphere. The conjecture was finally solved by Brendle in 2013. When  $d = \pi/2$  the set  $\Sigma_d$  reduces to a circle of radius 1. More precisely,  $\Sigma_{\pi/2} = \{\cos(\theta)u_1 + \sin(\theta)u_2, \theta \in \mathbb{R}\}$ . A remarkably simple geometrical representation emerges when it performs the analysis above in the appropriate basis: Bell basis. The collection of all two-qubit states with real entries is represented by the three-dimensional sphere  $\mathbb{S}^3$  where the antipodal points have been identified, as a consequence of  $|\psi\rangle$  and  $-|\psi\rangle$  being two indistinguishable states.

This space is called the real projective space and it is denoted by  $\mathbb{P}^3$  (see Fig. 4).

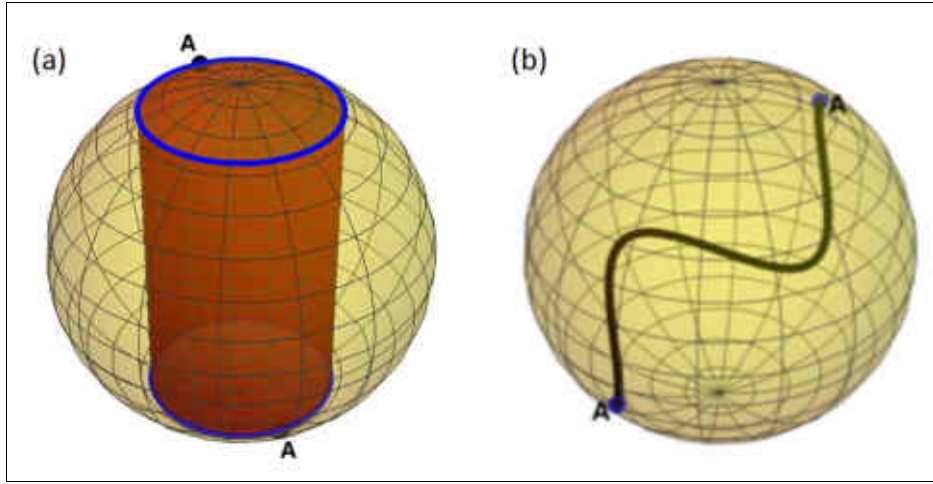


Fig. 4. Visualizing  $\mathbb{P}^3$  as a pac-man universe. (a) The blue circles represent the same circle, where, for example the two antipodal points denoted as  $A$  are identified as one. [Note that the brown surface plus the two blue circles with the aforementioned boundary condition represent a Klein bottle.] (b) In this pac-man model of  $\mathbb{P}^3$ , the curve shown is a closed curve [4]

We notice that the points in the north hemisphere  $NH = \{(x_1, x_2, x_3, x_4) \in \mathbb{S}^3 : x_4 \geq 0\}$  contains a representative for every point in  $\mathbb{P}^3$ . This representative is unique except for those point in the equator  $x_4 = 0$ . We have that each pair of antipodal point in the equator represents the same point in  $\mathbb{P}^3$ . Using the following identification from the ball  $B = \{(u_1, u_2, u_3) : u_1^2 + u_2^2 + u_3^2 \leq 1\}$  to  $NH$  given by  $\xi(u) = (u_1, u_2, u_3, \sqrt{1 - (u_1^2 + u_2^2 + u_3^2)})$  as shown in Fig. 4 we can visualize the projective space as the 3D "pacman" universe build with the ball  $B$  with the property that anytime we reach the boundary of the ball, then we show up at the antipodal point. In this representation, the maximally entangled states, those equivalent to the state  $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$  up to local unitary transformations, contain all Bell states and are represented by a pair of circles (see Fig. 5(c)). Recall that by definition, a two-qubit state is absolutely maximally entangled (AME), if the trace with respect to either one of the two qubits is  $1/2 I_2$  with  $I_2$  the 2 by 2 identity matrix.



Continuing with the visualization of the states, the unentangled states are represented by a Klein bottle (see Fig. 5(a)), and for any other state, their equivalent states are represented by a pair of disjoint Klein bottles (see Fig. 5(b)).

Finally, we show that when we apply the gate controlled-Z (CZ) to a particular equivalent class, we get a set containing points from all the equivalent classes. As a consequence, this provides a geometrical proof that every pair of real two-qubit states can be connected by circuit that contains local gates and only one CZ gate. That only one entangling gate is necessary for arbitrary two qubit states is a known result and it fits within the general theory and research devoted to efficiently prepare  $n$ -qubit states, and for a subroutine in Rigetti's Quil platform.

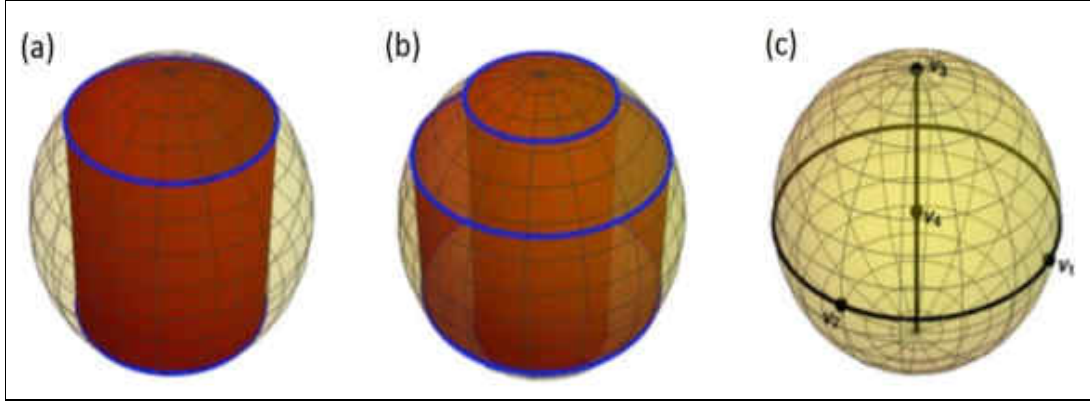


Fig. 5. (a) Image of  $\Omega_g$  with  $\Omega_g = \pi / 4$ , representing the unentangled or product states by the single Klein bottle depicted here. (b) Image of the set  $\Omega_g = \mathbf{S}_d \cup \mathbf{S}_{\pi/2-d}$  with  $d = \pi / 6$ . All the states in this pair of Klein bottles are equivalent under local gates. For any state with  $d$  between 0 (maximal entanglement) and  $\pi / 4$  (product states), its entanglement  $S(d) = 1 - \log_2 \sqrt{\frac{(1 + \sin 2d)^{1+\sin 2d}}{(1 - \sin 2d)^{-1+\sin 2d}}}$  (c) The two curves are indeed two circles representing the maximally entangled states, which include the points  $v_1$  through  $v_4$  representing the four states from the Bell basis (see convention used for the basis states)

For completeness sake, let us define some gates that we will be using. The local gates  $R_y(\theta)$  and  $X$  act on one qubit state and are given by the matrices

$$R_y(\theta) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \text{ and } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

The CZ gate, acts on a pair of qubits, its matrix is given by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Let us consider the following subset of two qubits

$$RQ_2 = \{ |w\rangle = w_1 |00\rangle + w_2 |01\rangle + w_3 |10\rangle + w_4 |11\rangle : w_i \in \mathbb{R} \}$$

and let us define the Bell basis as

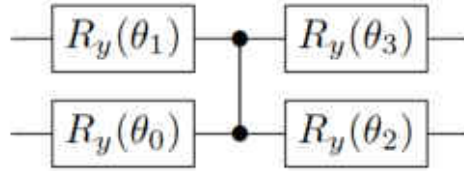
$$|v_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |v_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |v_3\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |v_4\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

and let us call  $(x_1, x_2, x_3, x_4)$  the coordinates of  $RQ_2$  with respect to the basis  $|v_1\rangle, \dots, |v_4\rangle$ . Notice that for the state  $|w\rangle = w_1 |00\rangle + w_2 |01\rangle + w_3 |10\rangle + w_4 |11\rangle$  the following relation holds,

$$x_1 = \frac{w_1 - w_4}{\sqrt{2}}, \quad x_2 = \frac{w_2 + w_3}{\sqrt{2}}, \quad x_3 = \frac{w_1 + w_4}{\sqrt{2}}, \quad x_4 = \frac{w_2 - w_3}{\sqrt{2}}.$$

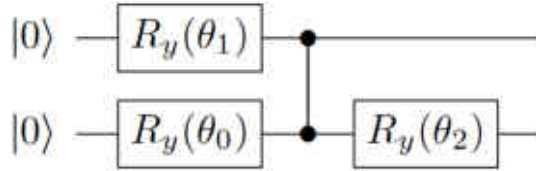
Using the notation  $E = \{ \cos(\theta)v_3 + \sin(\theta)v_4, \theta \in \mathbb{R} \}$  and  $\Sigma_d$  introduced earlier we have,

1. The set  $RAM E_2$  of maximally entangled states in  $RQ_2$  is the union of the two circles  $E$  and  $E^\perp = \{\cos(\theta)v_1 + \sin(\theta)v_2, \theta \in \mathbb{R}\}$ . Moreover, every pair of states in  $RAM E_2$  are connected by local gates with real entries.
2. The set  $\Sigma_{\pi/4}$  is the set of nonentangled states in  $RQ_2$ . This set is also characterized as the set of point that are farthest away from the set  $RAM E_2$ . They all are  $\pi/4$  away from the set  $RAM E_2$ .
3. For any  $d$  between 0 and  $\pi/4$ , the set  $\Omega_d = S_d \cup S_{\pi/2-d}$  has the property that any pair of states in  $\Omega_d$  are connected by local gates. Moreover, if  $0 \leq d_1 < d_2 \leq \pi/4$  and  $|\phi_1\rangle \in \Omega_{d_1}$  and  $|\phi_2\rangle \in \Omega_{d_2}$  then,  $|\phi_1\rangle$  and  $|\phi_2\rangle$  are not connected by local gates.
4. The entanglement entropy of any state in  $\Omega_d$  is  $1 - \log_2 \sqrt{\frac{(1 + \sin 2d)^{1+\sin 2d}}{(1 - \sin 2d)^{-1+\sin 2d}}}$ .
5. For any pair of states  $|\phi_1\rangle$  and  $|\phi_2\rangle$  in  $RQ_2$  there exists angles  $\theta_0, \theta_1, \theta_2$  and  $\theta_3$  such that the circuit



sends  $|\phi_1\rangle$  to  $|\phi_2\rangle$ .

6. If  $|w\rangle = w_1|00\rangle + w_2|01\rangle + w_3|10\rangle + w_4|11\rangle$  then the circuit



with

$$\theta_0 = \text{Arg}(w_1 + iw_2) - \text{Arg}(w_3 + iw_4), \theta_1 = 2 \arccos(\sqrt{w_1^2 + w_2^2})$$

$$\theta_2 = \text{Arg}(w_1 + iw_2) + \text{Arg}(w_3 + iw_4)$$

prepares  $|w\rangle$ .

If we identify  $|w\rangle$  with  $-|w\rangle$ , remember that there is not physical way to tell them apart, then the tori in this theorem become Klein bottles.

Geometrical proof that one CZ and local gates are enough to connect any two-qubit states with real amplitudes in Fig. 6 demonstrated.

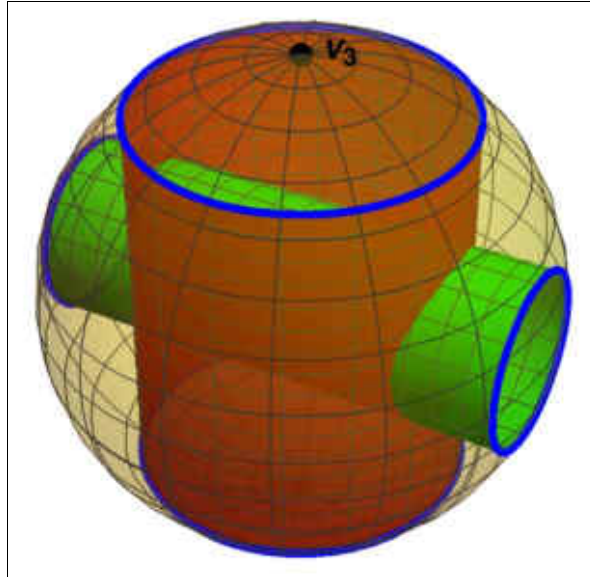


Fig. 6. Geometrical proof that one CZ and local gates are enough to connect any two-qubit states with real amplitudes

Consider two states:  $|\psi_0\rangle$  in  $S_d$  and  $|\psi_1\rangle$  in  $S_{d_1}$ . Since the surface  $S_{d_1}$  (brown) satisfy the equation  $x_1^2 + x_2^2 = \sin^2(d_1)$ , and the surface  $CZS_d$  (green) satisfy the equation  $x_2^2 + x_3^2 = \sin^2(d)$  then these two surfaces intercept. This interception represents a geometrical proof that one CZ and local gates are enough to connect two states, since there is a state  $|\psi_3\rangle$  in  $S_d$  which maps to a state  $|\psi_2\rangle$  in  $\Lambda = S_{d_1} \cap CZS_d$ , i.e.,  $|\psi_2\rangle = CZ|\psi_3\rangle$ . Since  $|\psi_3\rangle$  lives in  $S_d$  it can be obtained from  $|\psi_0\rangle$  by local gates. Likewise, the target state  $|\psi_1\rangle$  can be obtained from  $|\psi_2\rangle$  with only local gates since they both now live in  $S_{d_1}$ . The proof is given in [4]

**Quantum circuits.** *Quantum computing processes qubits.* A qubit can be in one of the “classical” logic states, 0 and 1, or in any superposition of these states. The state of a qubit  $q$  can be defined by the linear combination of the classical states using two complex coefficients,  $q = a_0|0\rangle + a_1|1\rangle$ , with  $a_0, a_1 \in \mathbb{C}$  and  $|a_0|^2 + |a_1|^2 = 1$ . The Bloch sphere is a powerful representation of a qubit state. The two poles of the sphere represent the two classical states, while all the points of the sphere represent superposed states. On the equator of the Bloch sphere there are all superposed states with  $|a_0|^2 = |a_1|^2 = 1/2$  characterized by different angles with respect to the Z-axis.

A 2-qubit system can be defined as:  $q = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ , with  $a_{00}, a_{01}, a_{10}, a_{11} \in \mathbb{C}$  and  $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$ . As a consequence, 4 complex coefficients are needed to represent a two-qubit state, while 8 complex coefficients are necessary to describe a 3-qubit system. In general, to represent the state of  $n$  qubits and to simulate the quantum system behavior on a classical computer,  $2^n$  complex coefficients are required. While modeling a combinational functionality for the use in a quantum computation, it is possible to consider all the inputs as Boolean values—even when embedded as part of a quantum algorithm where entangled states in superposition are being applied.

The most widely used and the basis for writing quantum programs nowadays is the *quantum circuit* model. Quantum circuits comprise a set of qubits (two-level quantum systems, with basis  $|0\rangle$  and  $|1\rangle$ , just like spins) and quantum unitary operations, known as quantum gates. A quantum circuit is a series of quantum gates acting on a set (or register) of qubits, where each operation acts on a subset of the qubits. Provided the correct set of quantum gates, a quantum circuit can implement universal computation, meaning it can implement any possible Boolean function. The basis of the procedure goes as follows. Suppose we wish to implement a

function:  $F: \mathbb{X}^n \rightarrow \mathbb{Y}^m$ , where  $n \leq m$ , without loss of generality. For that purpose, we implement a quantum computation using a quantum circuit  $U$ , such that:  $U|x_1, \dots, x_m, 0, \dots, 0\rangle = \sum_{y_1, \dots, y_m} c_{y_1, \dots, y_m} |y_1, \dots, y_m\rangle$

Where we have assumed that we can initialize the qubits in a known initial state, for example, a computational state  $|x_1, \dots, x_n\rangle$ . This initial state encodes the information regarding the input for the function, and correspondingly, the states  $|y_1, \dots, y_m\rangle$  encode potential outputs. However, unlike classical computers, the output of the quantum computer is a quantum state with an exponential number of amplitudes. To read the answers from the quantum register, we need to perform measurements on the output quantum state. A particular binary string,  $y_1, \dots, y_m$  is measured with probability  $|c_{y_1, \dots, y_m}|^2$ , as pointed out earlier.

Therefore, to implement  $F$  we need to design a sequence of quantum gates (a quantum algorithm) such that the resulting circuit,  $U$ , prepares an output state that produces  $F(x_1, \dots, x_n)$  with probability close to 1 when measured. Described this way, we see that a quantum model of computation is possible. However, does it offer any advantage compared to classical computing?

Information in quantum computers is encoded in quantum states. Instead of composing with the direct product, as with classical states, quantum states are composed using the tensor product rule. For example, in the quantum circuit model, general states are expressed as tensor products of two-level quantum systems or qubits. The state of a single qubit can be conveniently represented using a Bloch sphere (see Fig. 7(a)).

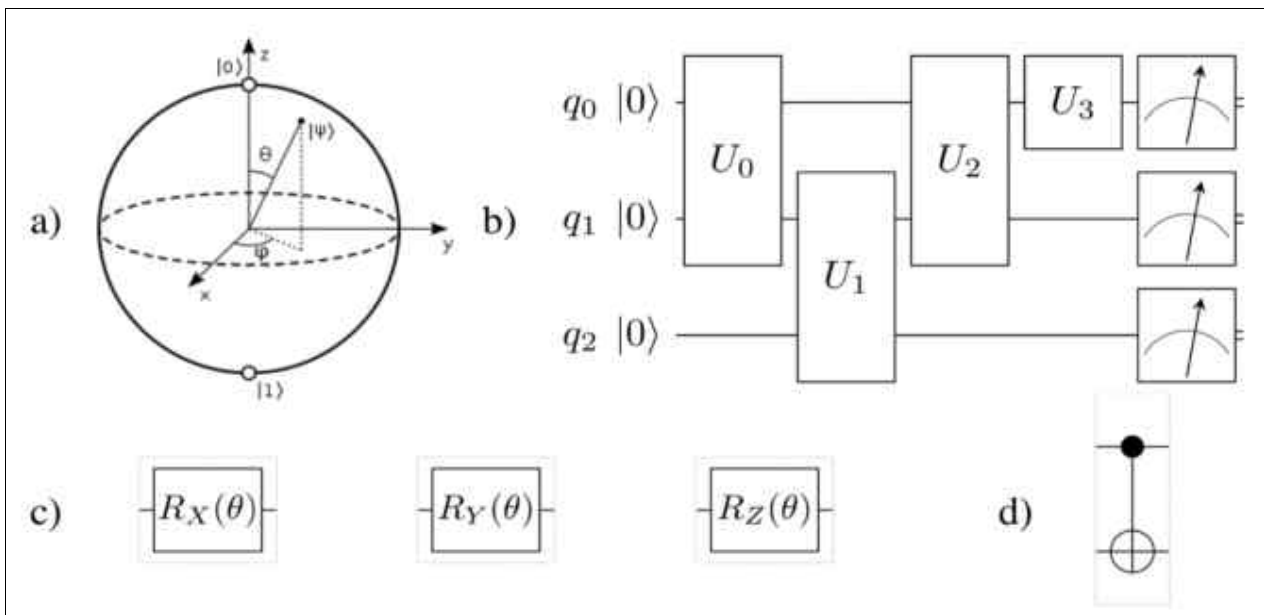


Fig. 7. Some basic elements of quantum computing: a) Bloch sphere representation of a qubit: the state of a qubit can be described as  $|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\phi} \sin(\theta/2)|1\rangle$ . X, Y and Z rotations can be pictured as rotations in the corresponding axes. b) Example of a quantum circuit: the circuit acts on three qubits, represented by the wires labeled as  $q_i$ , and comprises 3 two-qubits gates and 1 single-qubit gate, represented by the rectangles. The 'meter' symbol represents a measurement in the Z basis. c) Graphical representation of single qubit rotations. d) Graphical representation of a CNOT gate

*Example.* Correspondingly, an arbitrary state of a qubit can be expressed as a superposition of two orthogonal basis states. Another aspect of the quantum representation of information is measurement. Extracting information from a quantum state requires measurement, whose outcome statistics are governed by Born's rule. To measure a quantum state, we project it to a specific basis. One example is measurement in the computational basis comprised of all the possible tensor products of states  $|0\rangle$  and  $|1\rangle$  in  $n$  qubits. The conventional one-qubit basis in quantum computing is given by the eigenstates of Pauli matrices:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

where the eigenstates of the  $Z$  matrix correspond to the computational basis. An  $n$  qubit state in a one-qubit basis can be written  $|\psi\rangle = \sum_{x_1, \dots, x_m} c_{x_1, \dots, x_m} |x_1, \dots, x_m\rangle$  such that the state  $|x_1, \dots, x_m\rangle$  is observed with probability  $|c_{x_1, \dots, x_m}|^2$  when  $|\psi\rangle$  is measured in this basis. Correspondingly, quantum states can be interpreted as probability vectors with an  $\ell^2$ -norm normalization condition, compared to the  $\ell^1$ -norm normalization condition of the corresponding discrete probability vector.

In quantum information theory, it is sometimes convenient to represent quantum states as density operators. For a pure state, its density matrix is defined as  $\rho = |\psi\rangle\langle\psi|$ . The density matrix formalism enables the description of quantum ensembles, which correspond to classical probability distributions over a set of quantum states,  $\rho = \sum_k |\psi_k\rangle\langle\psi_k|$ . Table 1 contrasts some of the basic elements and properties of classical and quantum information in the density matrix formalism.

Table 1. Comparison of properties of quantum and classical information

Property	Classical	Quantum
Combining systems	$S_1 \times S_2$	$ S_1\rangle \otimes  S_2\rangle$
Normalization	$\sum_k p_k = 1$	$\text{Tr}[\rho] = 1$
Positivity	$p_k \in \mathbb{R}^+$	$\langle k \rho k\rangle \geq 0$
Expectation values	$\sum_k p_k f(k)$	$\text{Tr}[\rho F]$ where $F = F^\dagger$
Marginals	$\sum_k p_{km} = p_m$	$\text{Tr}_B[\rho^{AB}]$
Entropy	$\sum_k p_k \log p_k$	$\text{Tr}[\rho \log \rho]$

The normalization and positivity properties are associated to a probabilistic interpretation of quantum states. We also compare the formulas for expectation values, marginals, and entropy of classical probability distribution and quantum states. For a diagonal density matrix, the classical and quantum formulas for entropy become equivalent.

Another important aspect of quantum information is the property of entanglement. An entangled quantum state of a joint system is a state that cannot be factored as a tensor product of states of the individual components, independently of the basis used to represent the total system. An example of an entangled state in two qubits is  $(|00\rangle + |11\rangle)/\sqrt{2}$ . One way to quantify entanglement is through the Schmidt rank, which can be calculated using Singular Value Decomposition given a specific partitioning of the system. Perturbative approaches or techniques based on matrix product states can better approximate quantum states with relatively low entanglement but struggle with highly entangled (strongly correlated) states. This difficulty motivates the idea that quantum computers can offer an advantage simulating strongly correlated systems, such as those arising naturally in many problems of condensed matter physics and quantum chemistry. Entanglement is one of the ingredients necessary for quantum computation to provide a computational advantage.

**Physical models of qubits and transformation on Bloch sphere.** A spin-qubit transformation protocol is proposed for an electron in a mesoscopic quantum ring with tunable Rashba interaction controlled by the external electric field. The dynamics of an electron driven around the ring by a series of Landau-Zener-like transitions between a finite number of local voltage gates is determined analytically. General single-qubit transformations are demonstrated to be feasible in a dynamical basis of localized pseudo-spin states. It is also demonstrated that by the use of suitable protocols based on changes of the Rashba interaction full Bloch sphere can be covered. The challenges of a possible realization of the proposed system in semiconductor heterostructures are discussed. The spintronics, a promising new branch of electronics based on electron's spin as the information carrier instead of its charge, has emerged in the last few decades. The use of spin promises several important advantages in information processing, most notably longer coherence times and lower power consumption compared to classical electronic devices. To avoid the use of the magnetic field for spin

manipulation, the spin-orbit interaction (SOI) might be used to control electron's spin. Rashba type SOI, emerging as a consequence of structural inversion asymmetry of the effective potential in the semiconductor heterostructure, seems especially promising for this task since its magnitude can be artificially controlled by applying the external electric field perpendicular to the plane of the heterostructure. Potential use of this phenomenon was first demonstrated by SOI field effect transistor, proposed by Datta in 1990, followed by several other proposals for two-dimensional spintronic devices.

For the use in quantum computation, the spin transformation would ideally be applied to a single-electron qubit, trapped in a quantum dot, with its position determined by an external electric potential. Spin transformation for an arbitrary motion of an electron in one-dimension system can be expressed analytically which also allows for exact analysis of errors in qubit transformations due to the noise in driving fields and the effects of finite temperature. Note, however, that since the Rashba spin rotation axis in this system is perpendicular to the direction of electrons' motion, one-dimensional motion provides only a limited range of possible spin transformations.

The system of electron on a quantum ring with the Rashba coupling is particularly convenient in this regard since it allows for the study of spin transformations in a two-dimensional system using effectively one-dimensional Hamiltonian. The motion of the electron around the ring with the Rashba coupling, tuned using external gate voltage, can be used to realize an arbitrary single-qubit transformation in the qubit basis of Kramers states [5].

However, the position of external potential can be shifted for an arbitrary azimuthal angle, which is usually not the case in realistic spintronic devices, where the potential is typically defined using fixed external voltage gates, applied to the surface of the semiconductor, as shown in Fig. 8.

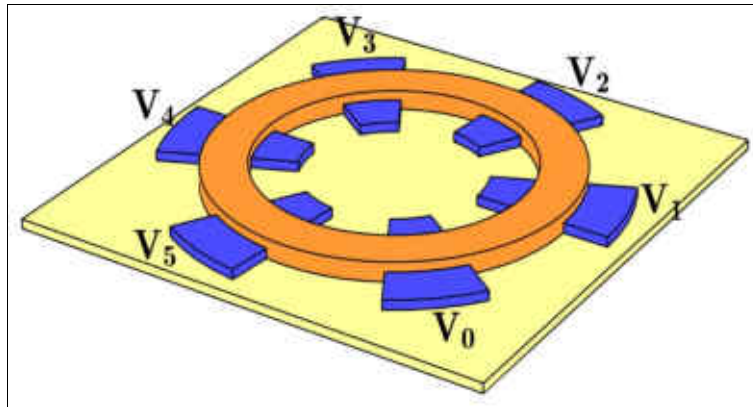


Fig. 8. Schematic representation of a quantum ring device with six voltage gates used to control the electron position

The minima of the potential can, therefore, occur only at specific positions. To describe more realistic devices, this limiting factor should be taken into account.

The spin transformations, accompanying the electron's transition between sites on a ring, will be expressed in terms of nearest-neighbor hopping terms. These are obtained by the Fourier transformation of Bloch states into the basis of localized Wannier functions

$$\phi_{ns}(\varphi) = \frac{1}{\sqrt{N}} \sum_{j=\frac{1}{2}}^{N-\frac{1}{2}} e^{-in(j-\frac{1}{2})\varphi} \psi_{js}(\varphi) = e^{i\frac{\varphi}{2}} w_{ns}(\varphi) U_z^\dagger(\varphi) U_y^\dagger(\vartheta_\alpha) \chi_s.$$

*Remark.* The electronic ground state of a periodic system is usually described in terms of extended Bloch orbitals, but an alternative representation in terms of localized “Wannier functions” was introduced by Gregory Wannier in 1937. The connection between the Bloch and Wannier representations is realized by families of transformations in a continuous space of unitary matrices, carrying a large degree of arbitrariness. Since 1997, methods have been developed that allow one to iteratively transform the extended Bloch orbitals of a first-principles calculation into a unique set of *maximally localized* Wannier functions (MLWF), accomplishing the solid-state equivalent of constructing localized molecular orbitals, or “Boys orbitals” as previously known from the chemistry literature [6].



This leads to very intuitive interpretation of the Wannier states and their spin properties. The electron in the Wannier state  $|\phi_{ns}\rangle$  is localized around the position  $n\varphi_\alpha$  with spin tilted from  $z$  direction towards the centre of the ring for  $s = 1/2$  and from  $z$  direction away from the centre for  $s = -1/2$ , as shown in Fig. 9.

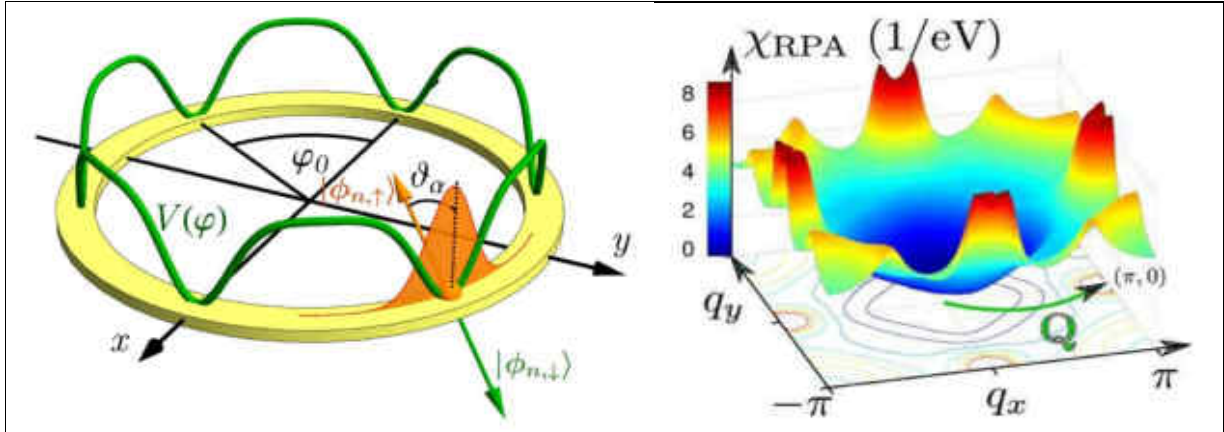


Fig. 9. Schematic representation of the Wannier state  $|\phi_{ns}\rangle$  as an electron, localized at a minimum of periodic potential, with tilted spin

Since the spin properties of Wannier functions depend on the strength of the Rashba coupling  $|\phi_{ns}\rangle$ , these states are not the best choice for the analysis of spin transformations of the electron. It is more convenient to construct a new basis states as a local superposition of Wannier states at the same site  $n$ , so-called spin Wannier basis, with spin properties independent of spin-orbit coupling, resembling pure spin states. To emphasize that this basis resembles pure spin states, we sometimes use arrows  $\uparrow$  and  $\downarrow$  as the pseudo-spin index  $s$  instead of  $\pm \frac{1}{2}$ , respectively. The coefficients of linear superposition of such states

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\tilde{\phi}_{n\uparrow}\rangle + e^{i\chi}\sin\left(\frac{\theta}{2}\right)|\tilde{\phi}_{n\downarrow}\rangle$$

can then be directly related to the direction the vector of spin expectation values on the Bloch sphere,  $\theta$  and  $\chi$  as  $\langle\psi|s|\psi\rangle \approx \frac{\hbar}{2}(\sin\theta\cos\chi, \sin\theta\sin\chi, \cos\theta)$ , which significantly simplifies the analysis of spin transformations and makes the states  $|\tilde{\phi}_{ns}\rangle$  a suitable qubit basis. We define qubit basis as Wannier pseudo-spin pair on the site  $n = 0$ ,  $|0\rangle = |\tilde{\phi}_{0\uparrow}\rangle$ ,  $|1\rangle = |\tilde{\phi}_{0\downarrow}\rangle$ . We also define the Bloch sphere, corresponding to this basis, defined by polar and azimuthal angles  $\Theta$  and  $\Phi$ , which correspond to the qubit state  $|\psi_Q\rangle = \cos\left(\frac{\Theta}{2}\right)|0\rangle + e^{i\Phi}\sin\left(\frac{\Theta}{2}\right)|1\rangle$ .

Single qubit transformation is achieved by transferring the electron around the ring by controlled changes of gate potentials at different sites. To transfer the electron from one site to its neighboring site, we slowly decrease the depth of potential well on the first site and increase the depth of the potential on the site onto which we want to transfer the electron. Such charge transfer has already been demonstrated experimentally for  $N = 4$  sites. From mathematical perspective, this results in a Landau-Zenner-like transition of the electron from the superposition of spin Wannier states  $|\tilde{\phi}_{ns}\rangle$  on the initial site to the superposition of spin Wannier states  $|\tilde{\phi}_{n+1,s}\rangle$  on the final site. The total qubit transformation with angles on the Bloch sphere  $\Theta$  and  $\Phi$ , corresponding to the final qubit state, obtained from initial state  $|0\rangle$  by applying corresponding transformation.



As an example of spin rotation, we performed the Z-gate qubit transformation, corresponding to  $\Theta = \pi$  and arbitrary  $\Phi$ . This transformation can be realized on a ring with  $N = 6$  sites with  $m = 1$  revolution of the electron around the ring and Rashba amplification factor  $K_\alpha = 5$ . The transformation is schematically presented in Fig. 10.

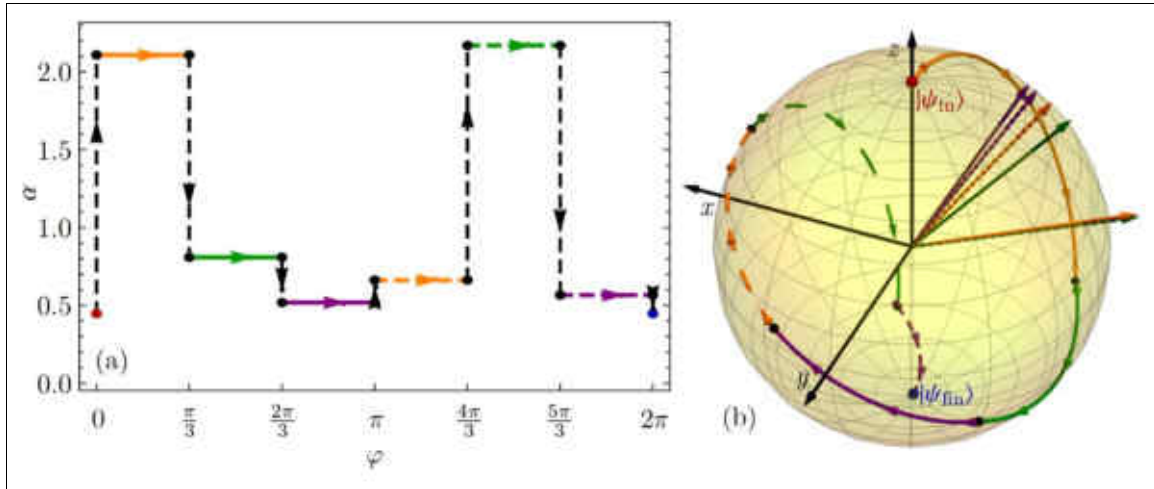


Fig. 10. An example of qubit Z-gate transformation. (a) Movement of the system in parametric space with coordinates being electron's position  $\varphi$  and Rashba coupling  $\alpha$ , transforming the initial state  $|\psi_{in}\rangle = |0\rangle$  (red dot) to the final state  $|\psi_{fin}\rangle = |1\rangle$  (blue dot). Before each shift of electron using Landau-Zenner transition, the value of Rashba coupling is adjusted to the appropriate value, calculated using Monte-Carlo simulation. (b) Resulting spin transformations are represented as a rotations around axes, determined by the Rashba coupling. Orange, green and purple solid and dashed lines on (a) correspond to the rotational axes and spin rotation paths on (b) [5]

Figure 10(a) shows how values of the Rashba coupling need to be changed between the shifts of electron position. On Fig. 10(b) the rotations of electron spin is schematically presented on the Bloch sphere with arrows representing the rotation axis of each spin rotation, with colors and dashing corresponding to the ones in Fig. 10(a). Although this representation is very instructive, note that only the initial (red dot) and final (blue dot) state on the Bloch sphere correspond to qubit states, defined as being located at site  $n = 0$ . The intermediate points on Bloch sphere are defined in a space, corresponding to the rotation  $U_{full}$  and can be related to actual physical states only if the full rotation is decomposed back into single-transition rotations and the intermediate results are expressed in spin Wannier basis  $|\tilde{\phi}_{ns}\rangle$ .

## Model dynamics for quantum computing

A model master equation suitable for quantum computing dynamics can be applied for the description of an ideal quantum computer (QC), as a system of qubits evolves in time unitarily and, by virtue of their entanglement, interfere quantum mechanically to solve otherwise intractable problems. In the real situation, a QC is subject to decoherence and attenuation effects due to interaction with an environment and with possible short-term random disturbances and gate deficiencies. The stability of a QC under such attacks is a key issue for the development of realistic devices. The influence of the environment can be incorporated by a master equation that includes unitary evolution with quantum gates, supplemented by a Lindblad term. Lindblad operators of various types are explored; namely, steady, pulsed, gate friction, and measurement operators.

In the master equation, the Lindblad term describe short time intrusions by random Lindblad pulses. The phenomenological master equation is then extended to include a nonlinear Beretta term that describes the evolution of a closed system with increasing entropy. An external Bath environment is stipulated by a fixed temperature in two different ways. Here explored the case of a simple one-qubit system in preparation for generalization to multi-qubit, qutrit and hybrid qubit–qutrit systems. This model master equation can be used to test the stability of memory and the efficiency of quantum gates. The properties of such hybrid master equations

are explored, with emphasis on the role of thermal equilibrium and entropy constraints. Several significant properties of time-dependent qubit evolution are revealed by this simple study.

A quantum computer (QC) is a physical device that uses quantum interference to enhance the probability of getting an answer to another wise intractable problem. A quantum system's ability to interfere depends on its entanglement and on maintenance of its coherent phase relations. In a real system, there are always environmental effects and also random disturbances that can cause the quantum system to lose its ability to display quantum interference. That process is called decoherence, as is discussed in an extensive literature on how a quantum system becomes classical, often rapidly, due to its interaction with an external environment. That process might also be viewed as a measuring device. A major concern in the development of a realistic quantum computer is to understand, control, and/or correct for detrimental environmental effects.

A general theory of how such "open systems" evolve in time is provided by the operator sum representation (OSR), which replaces the unitary evolution of a closed system by a more general form that accounts for the fact that the system under study (the quantum computer) is affected by an environment. That general form involves Kraus operators and is often described as a mapping. An oft-used approximation is that in the system–environment interaction the environment restores itself rapidly to its initial condition, and therefore only the present situation of the environment is relevant. That is, one invokes a Markov approximation, which has the environment affecting the system, but the system's effect on the environment vanishes rapidly. It is assumed that the system and environment are initially uncorrelated and are described as a product state.

The Markov approximation is not always applicable; that depends on the dynamics of the environment and its interaction with the system. It is physically possible that the system affects an environment that is able to partially preserve that influence and feed part of it back to the system. Indeed, there are important papers that indicate that the Markov approximation is in doubt. Nevertheless, our initial approach is to adopt the Markov approximation, with plans to test its applicability.

Beretta provide a general master equation based on novel concepts of non-equilibrium statistical mechanics as applied to quantum systems. The Beretta master equation for describing an open system has not been used much for QC perhaps because it is nonlinear and it alters entropy addition rules. The Beretta description includes definitions of entropy, work, and heat for non-equilibrium systems. The resultant master equation has many important features, as illustrated below. Indeed, it incorporate the Beretta master equation for QC and extend it using a phenomenological viewpoint. The above assumptions provide a practical dynamic framework for examining not only the influence of an environment on the efficacy of a QC, but also the loss of reliability in the action of gates or the general loss of coherence. The master equation incorporates the main features of a density matrix; namely, Hermiticity, unit trace and positive definite character, while also including the evolution of a closed system and the effects of gates, noise and of an external bath.

## *A master equation model: unitary evolution, gates and pulses*

The master equation for the time evolution of the system's density matrix is presented in developing a simple model that incorporates the main features of the qubit dynamics for a quantum computer. These main features include seeing how the dynamics evolve under the action of gates and the role of both closed system dynamics and of open system decoherence, dissipation and the system's approach to equilibrium. From the density matrix can determine a variety of observables, such as the polarization vector, the power and heat rates, the purity, fidelity, and entropy all as a function of time [7].

**A. Unitary evolution.** The density matrix for a closed system is driven by a Hamiltonian  $H(t)$ ; that can be explicitly time dependent, as  $\rho(t) = U(t)\rho(0)U^\dagger(t)$  where the unitary operator is  $U(t) = e^{-\frac{i}{\hbar}H(t)t}$ . For infinitesimal time increments this yields the unitary evolution or commutator term:  $\frac{d\rho(t)}{dt} = -\frac{i}{\hbar}[H(t), \rho(t)]$ . This term species the reversible motion of a closed system. To include dissipation, an additional operator  $\mathcal{L}$  will be added  $\dot{\rho} = -\frac{i}{\hbar}[H(t), \rho(t)] + \mathcal{L}$  which describes an irreversible open system.

**B. Hamiltonian.** The Hamiltonian  $H(t) = H_0 + V(t)$  is a Hermitian operator in spin space; for one qubit it is a  $2 \times 2$  matrix. It consists of a time independent  $H_0$ ; plus a time dependent part  $V(t)$ : For  $n_q = 1$ , a typical Hamiltonian is (the level splitting)

$$H_0 \equiv -\frac{1}{2} \hbar \omega_L \hat{\sigma} \cdot \hat{z} = -\frac{1}{2} \hbar \omega_L \sigma_z,$$

which describes a 2 level system with eigenvalues  $-\frac{1}{2} \hbar \omega_L$  for state  $|0\rangle$  and  $+\frac{1}{2} \hbar \omega_L$  for state  $|1\rangle$  (see Fig. 11).

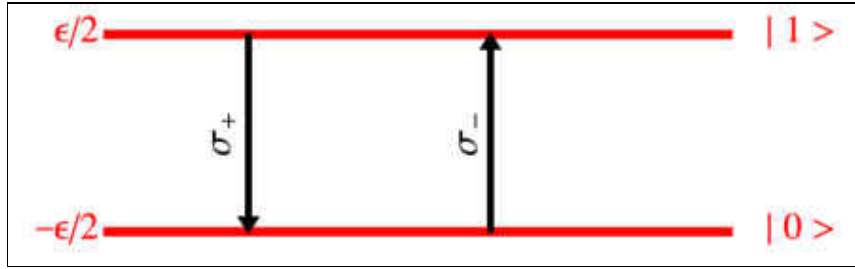


Fig. 11. The qubit levels with splitting  $\epsilon = \hbar \omega_L$ . With conventions the operator  $\sigma_- \equiv \frac{\sigma_x - i\sigma_y}{\sqrt{2}}$  raises the qubit to the polarization-down state  $|1\rangle$ , while  $\sigma_+ \equiv \frac{\sigma_x + i\sigma_y}{\sqrt{2}}$  lowers the qubit to the polarization-up ground state  $|0\rangle$

The polarization vector for this case precesses about the  $\hat{z}$  direction with the Larmor angular frequency  $\omega_L$ . This follows from the unitary evolution term

$$\frac{d\vec{P}(t)}{dt} = \text{Tr}\left(\vec{\sigma} \frac{d\rho(t)}{dt}\right) = -i \frac{\omega_L}{2} \text{Tr}(\vec{\sigma} \cdot [\vec{\sigma} \cdot \hat{z}, \rho(t)]) = -\vec{\omega}_L \times \vec{P}(t),$$

where  $\vec{\omega}_L = \omega_L \hat{z}$ , which is a Larmor precession of the polarization vector about the direction  $\hat{z}$ . The polarization vector then has a fixed value of  $P_z$  and the  $x$  and  $y$  components vary as

$$P_x(t) = P_x(0) \cos(\omega_L t) + P_y(0) \sin(\omega_L t), \quad P_y(t) = P_y(0) \cos(\omega_L t) - P_x(0) \sin(\omega_L t).$$

The above is equivalent to  $\dot{\vec{P}} = \sum_{j=1,3} M_{i,j} P_j$  with  $M = \begin{pmatrix} 0 & \omega_L & 0 \\ -\omega_L & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ . This form will be extended to

dissipative cases later. Thus, the level splitting  $\hbar \omega_L$  produces a precessing polarization with a fixed  $z$ -axis value and circular motion in the  $x$ - $y$  plane (see Fig. 12).

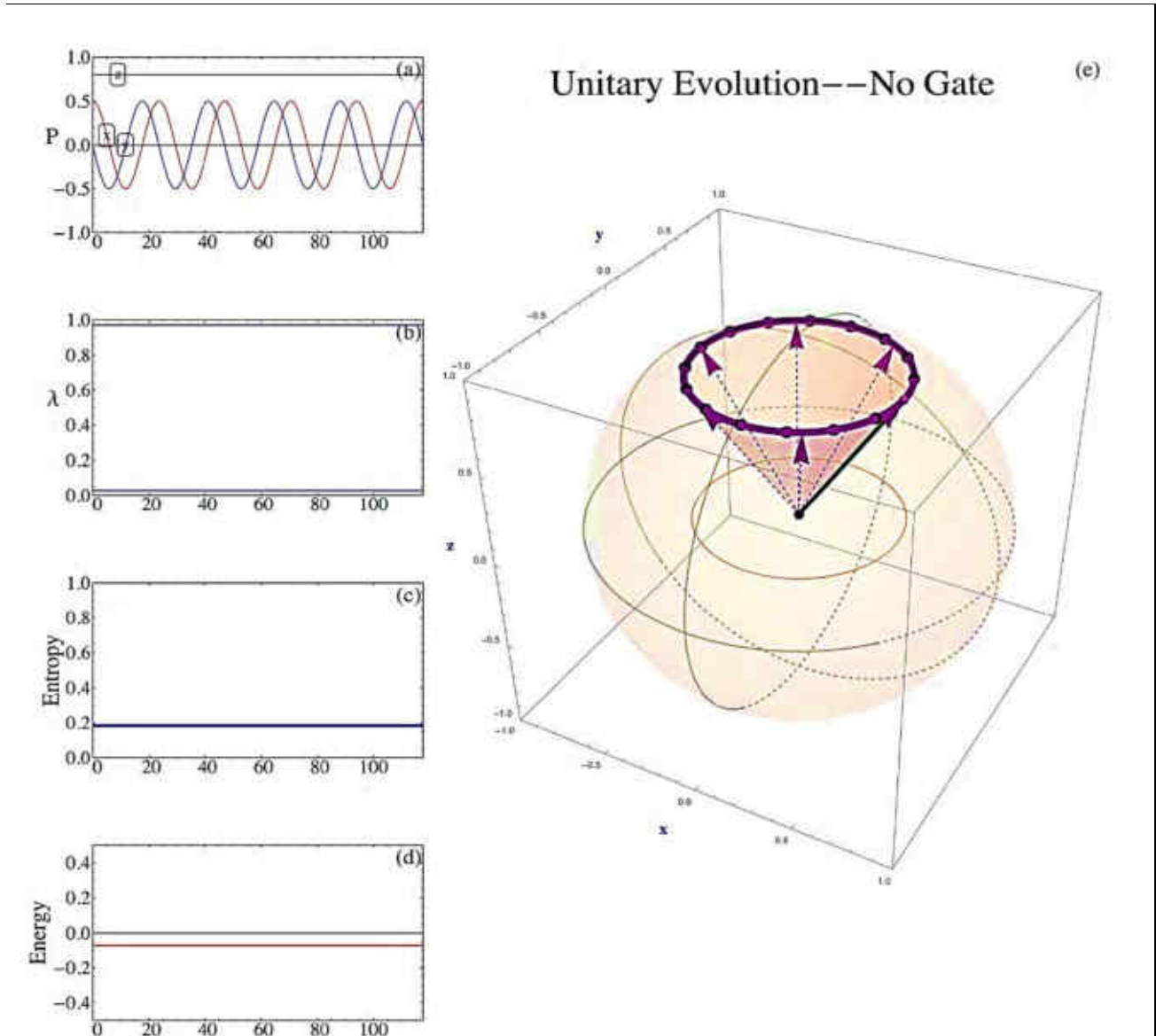


Fig. 12. Polarization vector precession (no gates and no dissipation): (a) fixed  $P_z$  and oscillating  $P_x$ ,  $P_y$  components versus time, (b) the two (fixed) eigenvalues  $\lambda$  of  $\rho(t)$ ; (c) the fixed entropy, and (d) the fixed energy (power and heat rate are zero). The Bloch sphere (e) with solid vector indicating the initial location of the polarization (which originates from the center of the Bloch sphere) while the subsequent motion follows the thick path as also shown by the dashed polarization vectors at subsequent times. [The dots indicate equal time interval locations of the polarization vector. The precession is also projected to the x-y plane]

The basic Hamiltonian  $H_0$  is selected to be time independent. The initial density matrix and level splitting parameters used in our examples 4 are listed in Table 2. Energy is in  $\mu$  eV, frequency in GHz and time is in nanoseconds (nsec). The initial density matrix and level parameters are in Table 2.

Table 2. Initial Density Matrix &amp; Level Parameters

Name	Value
$P_1$	0.5
$P_2$	0.0
$P_3$	0.8
$\mathbf{P}$	0.943
Initial Purity	0.945
Initial Entropy	0.186
Initial Temperature	0.93 mK
Larmor frequency $\omega_L$	0.2675 GHz
Larmor Period $T_L$	23.5 nsec
Level split $\hbar\omega_L$	0.1761 $\mu\text{eV}$

**One-qubit ideal gates.** For QC application, the Hamiltonian  $H(t) = H_0 + V(t)$  is used to incorporate two effects. The first is the level splitting. Here  $\omega_L$  denotes the Larmor angular frequency associated with the level splitting  $\hbar\omega_L$ , which sets the Larmor time scale  $T_L = 2\pi / \omega_L$  for the system. The  $V(t)$  term is used to include quantum gates  $\Omega$ , which are  $2 \times 2$  Hermitian matrices. For example, a single qubit NOT gate is  $\Omega = \sigma_1$ . The NOT acts as:  $\sigma_x|0\rangle = |1\rangle$ ,  $\sigma_x|1\rangle = |0\rangle$ . This basic gate is simply a spinor rotation about the  $\hat{x}$  axis by  $\pi$  radians. Clearly, two NOTs return to the original state.  $\text{NOT} \cdot \text{NOT} = \sigma_1^2 = I_2$ .

A gate operator  $\Omega$  is introduced as a Hamiltonian generator  $V_G(t)$ :  $V_G(t) \equiv \hbar\theta_G(t)\Omega$ , where  $\theta_G(t)$  is a gate pulse that is centered at time  $t_0$  with a width  $\tau$ . The pulse  $\theta_G(t)$  has inverse time units. Thus the pulse essentially starts at  $t_1 = t_0 - \tau/2$  and ends at  $t_2 = t_0 + \tau/2$ ; we typically take this pulse to be of Gaussian form,  $\theta_G(t) \rightarrow \theta_g(t)$

$$\theta_g(t) = \frac{\sqrt{\pi}}{2\tau} e^{-\left(\frac{t-t_0}{\tau}\right)^2}$$

The unitary operator associated with this gate generator is:  $U_G(t, t_1) = e^{-\frac{i}{\hbar} \int_{t_1}^t V_G(t') dt'}$ .

We call  $V_G(t)$  the gate generator since it generates the effect of a specific gate. The pulse function  $\theta_G(t)$  is designed to generate a suitable rotation over an interval  $t_1$  to  $t_2$ . Since we want to have a smooth pulse, we take these pulses to be of either Gaussian  $\theta_g(t)$  or soft square  $\theta_s(t)$  shape. The soft square shape is defined by

$$\theta_s(t) = N_f \frac{1}{2} \left[ \text{Erf}\left(\frac{t-t_1}{\tau}\right) - \text{Erf}\left(\frac{t-t_2}{\tau}\right) \right],$$

where  $N_f$  is fixed by the  $\int_{-\infty}^{\infty} \theta_G(t) dt = \frac{\pi}{2}$  condition.

The NOT gate pulse represents a series of infinitesimal rotations about the  $x$ -axis and in order to give the correct NOT gate effect, we need to normalize the pulse by  $\int_{-\infty}^{\infty} \theta_G(t) dt = \frac{\pi}{2}$ . The same form can be applied to a one qubit Hadamard

$$\Omega = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{\sigma_1 + \sigma_3}{\sqrt{2}},$$

which is a spinor rotation about the  $(\hat{x} + \hat{z})/\sqrt{2}$  axis by  $\pi$  radians.

**Bias gates.** Application of such a gate pulse does not carry out the objective of achieving a NOT gate, unless we do something to remove the level splitting at least during the action of the pulse. This corresponds to a temporary stoppage of precession. We therefore, introduce a bias pulse which is designed to make the levels degenerate during the gate pulse. The strength of the bias is adjusted by some type of non-intrusive monitoring, or by fore-knowledge of the fixed level splitting, to temporarily establish level degeneracy. During the action of the gate, the levels have to be completely degenerate, otherwise disruptive phases accumulate. Therefore, we use a soft square bias pulse that straddles the time interval of the gate pulse. The soft square bias pulse shape is defined by:  $\theta_B(t) \equiv \theta_s(t)/\theta_s(t_0)$ , which is preferred over a square pulse since it has finite derivatives and thus yields smooth variations of power as shown later. The width of the above bias pulse is  $\tilde{t}_2 - \tilde{t}_1$  and  $\tau$  is the thickness of the edges. To be sure that no precession occurs during a gate the time values used in the bias pulse  $\tilde{t}_2$  and  $\tilde{t}_1$  are taken to be slightly larger and slightly smaller than the gate pulse values  $t_2$  and  $t_1$ .

The bias pulse  $\theta_B(t)$  is added to the Hamiltonian to create a temporary degeneracy as  $V_B(t) = \frac{\hbar\omega_L}{2} \theta_B(t) \sigma_3$ , where the bias normalization is  $\int_{-\infty}^{\infty} \theta_B(t) dt = 1$ . Note  $\theta_B(t)$  is unitless, whereas  $\theta_G(t)$  has 1/time units.

Combining these terms, we have for a single pulse, with gate and bias

$$H_1(t) = -\frac{\hbar\omega_L}{2} (1 - \theta_B(t)) \sigma_3 + \hbar\theta_G(t) \Omega.$$

Here we see that the bias turns off precession and the gate term generates the action of a gate  $\Omega$ . Without a bias pulse to produce level degeneracy, awkward phases accumulate that are detrimental to clean-acting gates. Aside from intervals when the gate and the bias pulse act, the polarization vector precesses at the Larmor frequency, which is zero for degenerate levels. The bias pulse is simply an action to stop the precession, then the gate pulse rotates the qubit, and subsequently precession is restored once the bias is removed. That process is equivalent to stopping a spinning top, rotate it, and then get it spinning again, which requires some work. As discussed later the power supplied to the system during a gate pulse is determined by

$$\frac{d}{dt} W(t) = \text{Tr}(\rho(t) \dot{H}(t)) = \frac{\hbar\omega_L}{2} \dot{\theta}_B(t) P_z(t) + \hbar \dot{\theta}_G(t) \langle \Omega \rangle.$$

The derivative of the Hamiltonian divides into a gate plus a bias term.

**Gate and Bias Cases.** In Figs 13 and 14, the one-qubit polarization vector motion for a NOT and a Hadamard gate are shown with no dissipation ( $\mathcal{L} \rightarrow 0$ ) and with a bias pulse acting during the gate pulse. The detailed case shows that during the NOT pulse one gets the expected change of  $P_x \rightarrow P_x$ ;  $P_y \rightarrow -P_y$ ;  $P_z \rightarrow -P_z$ . The power supplied to the system during the NOT gate is also displayed separately for the gate power and the bias power. These are explained by the bias power =  $(\hbar\omega_L/2) \dot{\theta}_B(t) P_z(t)$  and the gate power =  $\hbar \dot{\theta}_G(t) P_x(t)$ , where the x-polarization is fixed during the NOT gate, but the z-polarization flips.

The values of the polarization from the time  $t_1$  when the gate pulse starts to its end at  $t_2$  explain the shapes seen in Fig. 13.

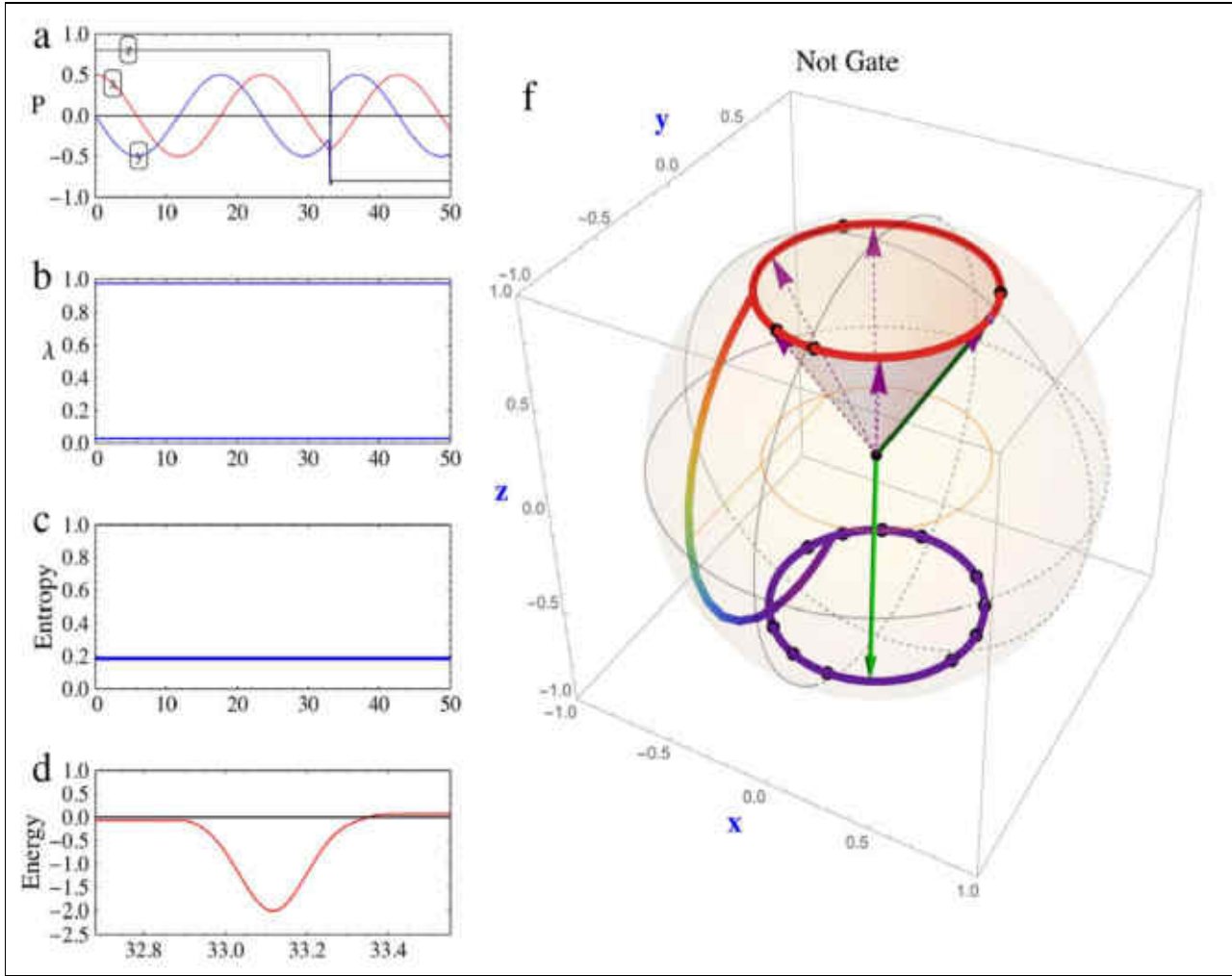


Fig. 13. Polarization vector trajectory for unitary Not Gate with level splitting and bias. Dissipation is off  $\mathcal{L} \rightarrow 0$ . (a) changes in polarization with time,  $P_x \rightarrow P_x$ ;  $P_y \rightarrow -P_y$ ;  $P_z \rightarrow -P_z$  during Not Gate pulse ; (b) the two (fixed) eigenvalues  $\lambda$  of  $\rho(t)$ ; (c) the fixed entropy ; (d) the energy versus time ; (e) Power by gate (G) and bias (B) (heat rate is zero). here  $P_y$  is negative during the gate; and (f) precession about positive  $\hat{z}$  is moved to  $-\hat{z}$  axis by NOT gate. The dots indicate equal time interval locations of the polarization vector

During the Hadamard pulse one gets the expected change of  $P_x \rightarrow P_z$ ;  $P_y \rightarrow -P_y$ ;  $P_z \rightarrow P_x$ . The power supplied to the system during the Hadamard gate is also displayed separately for the gate power and the bias power. These are explained by the bias power =  $P_z(t)(\hbar\omega_L/2)\dot{\theta}_B(t)$  and the gate power =  $\hbar(P_x(t) + P_z(t))\dot{\theta}_G(t)/\sqrt{2}$  where the y-polarization flips during the Hadamard gate, and the z and x polarization interchange. The values of the polarization during the pulse explain the shapes seen in Fig. 14.



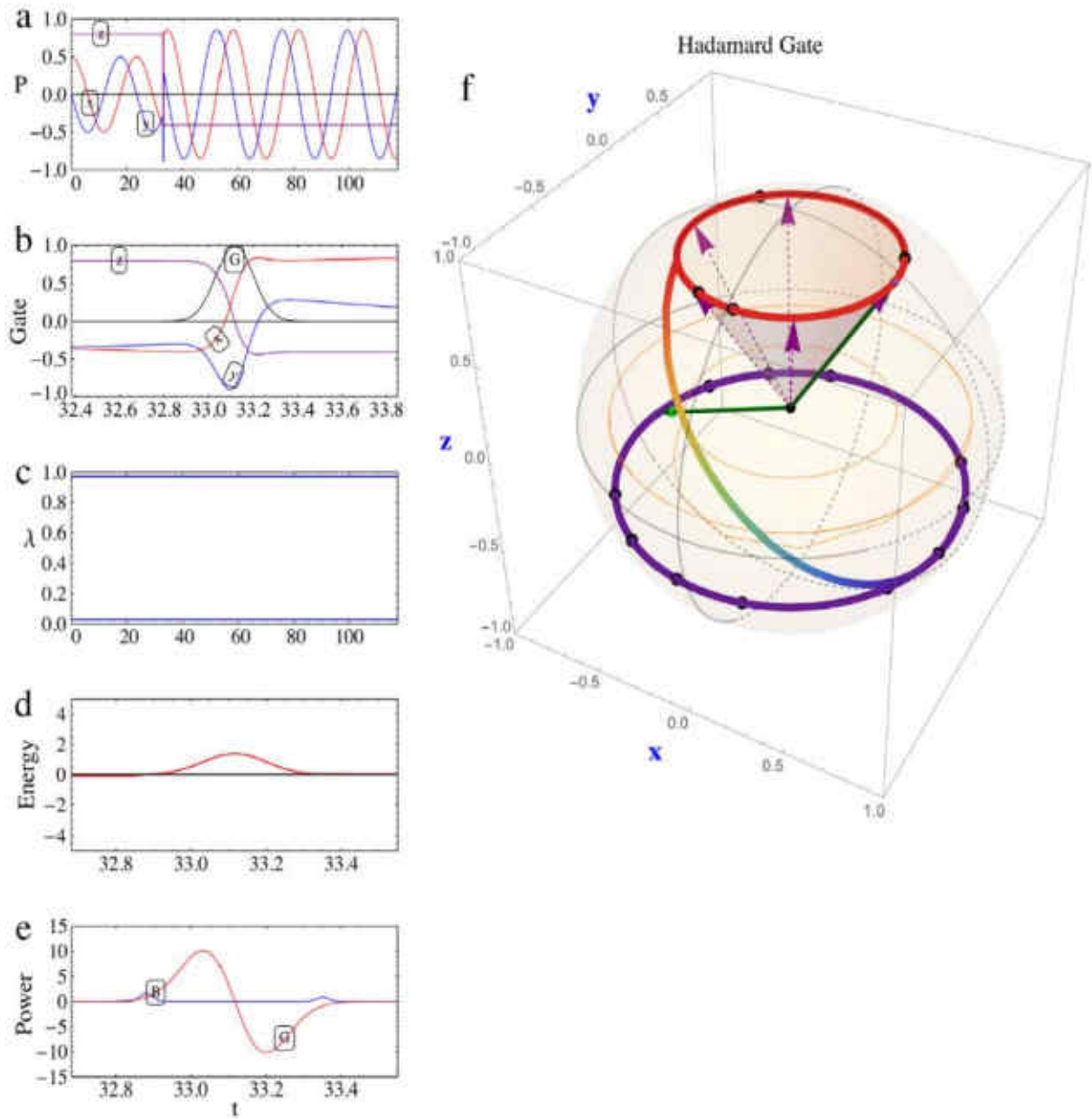


Fig. 14. Polarization vector trajectory for a unitary Hadamard gate with level splitting and bias. Dissipation is off  $\mathcal{L} \rightarrow 0$ . (a) Polarization versus time; (b) Polarization evolution  $P_x \rightarrow P_z$ ;  $P_y \rightarrow -P_y$ ;  $P_z \rightarrow P_x$  during Hadamard gate pulse (G) when gate starts  $t_1 = 32.9$  nsec,  $(P_x, P_y, P_z) = (-0.402, -0.301, 0.798)$ ; (c) the two (fixed) eigenvalues  $\lambda_1, \lambda_2$  of  $\rho(t)$ ; (d) the energy versus time; (e) Power by gate (G) and bias (B) (heat rate is zero); and (f) Polarization vector trajectory, precession about positive  $\hat{z}$  continues after polarization is moved as shown by Hadamard gate

The gate pulses can produce net work done on the system. No heat transfer occurs by way of the gate or bias, that exchange arises later from dissipation. After the gate pulses are complete, the precession continues about the  $\hat{z}$  axis.

Another case of a Hadamard gate is shown in Fig. 15.

In this case, the Hamiltonian is smoothly rotated from  $\hat{z}$  to  $\hat{x}$  during the Hadamard gate pulse. This Hamiltonian rotation, which is equivalent to rotating a level splitting magnetic field from the  $z$  to  $x$  direction, is accomplished by setting:



$$H_1(t) \rightarrow -\frac{\hbar\omega_L}{2}(1-\theta_B(t))(\eta(t_0-t)\sigma_3 + \eta(t_0-t)\sigma_1) + \hbar\theta_G(t)\mathcal{H},$$

$$\eta(t) \equiv \frac{1 + \text{Erf}(t/a)}{2}$$

Here  $\eta$  is a smooth step function of width  $a$ . As a result, the precession which started around the  $\hat{z}$  continues about the  $\hat{x}$  axis after the Hadamard gate pulse as shown in Fig. 15.

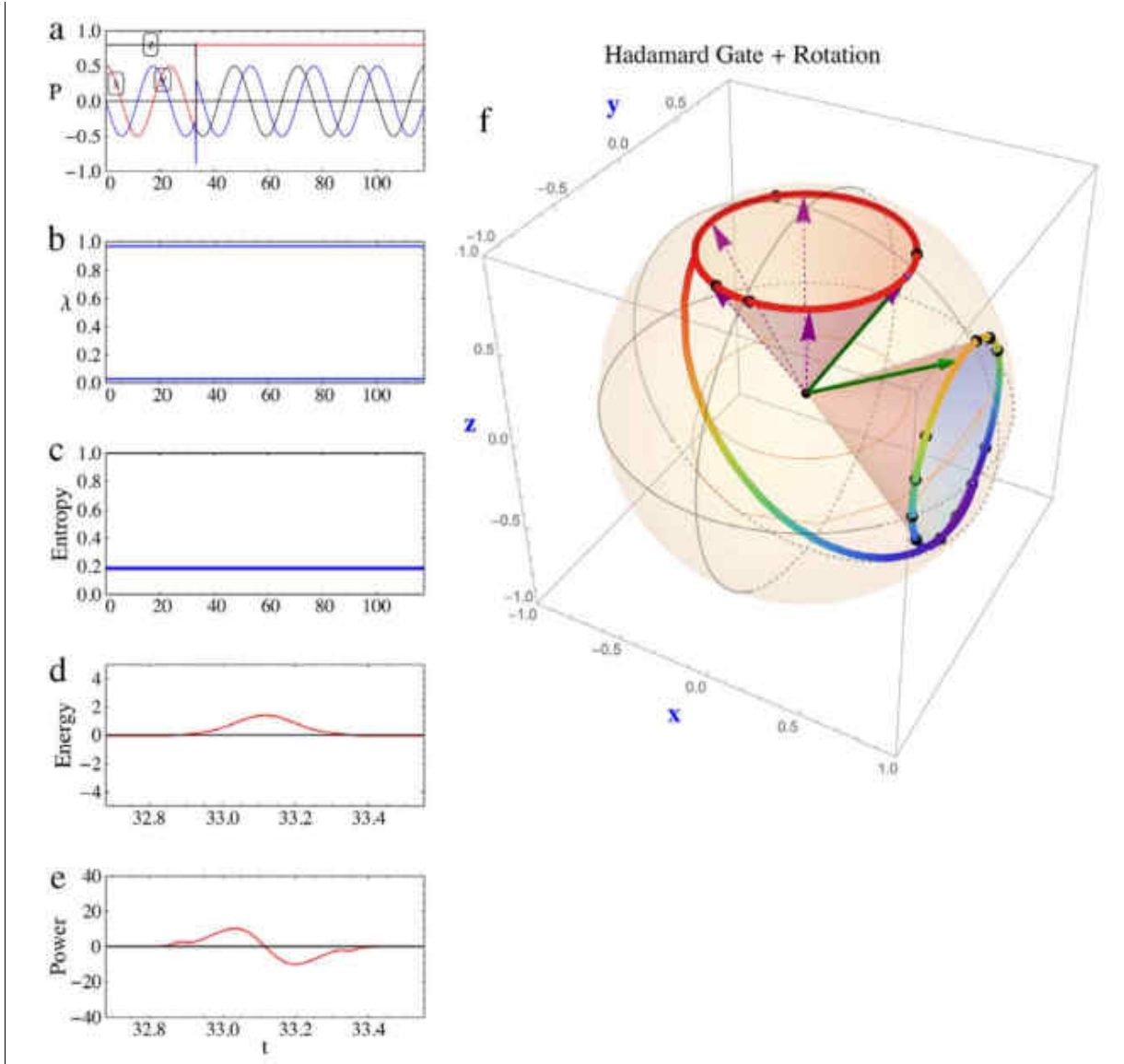


Fig. 15. Polarization vector trajectory for unitary Hadamard Gate plus bias and with  $\mathcal{L}$ . The precession axis is changed from the  $\hat{z}$  to the  $\hat{x}$  axis during the gate pulse. (a) changes in polarization  $P_x \rightarrow P_x$ ;  $P_y \rightarrow -P_y$ ;  $P_z \rightarrow -P_z$  during Hadamard gate pulse; (b) the two (fixed) eigenvalues  $\lambda_1, \lambda_2$  of  $\rho(t)$ ; (c) the fixed entropy; (d) the energy versus time changes due to gate, bias and Hamiltonian axis rotation; (e) Power by gate, bias and Hamiltonian rotation (heat rate is zero); (f) precession starts about  $\hat{z}$  axis and continues about  $\hat{x}$  axis after polarization is moved by Hadamard gate. The dots indicate equal time interval locations of the polarization vector

**Gate pulses and instantaneous gates.** To fully replicate the results obtained when a set of instantaneous gates act, as in a QC algorithm, it is necessary to invoke additional steps. One possible step is to apply a bias pulse over the full set of gate pulses, thereby making the qubits degenerate during a QC action, including final measurements. Another way, which we prefer, is to let the precession continue between gate pulses,

which means that each gate acts with an associated bias pulse, as illustrated earlier. Then one needs to design the gate pulses and associated measurements to act at appropriate times to replicate the standard description of instantaneous gates. For example, we define a delay time  $T_D$  as an integer  $n_D$  multiple of the Larmor period  $T_L$ . The first gate starts at a time  $t_1^{(1)} \equiv T_D = n_D T_L$ . The first pulse ends at a time  $t_2^{(1)} \equiv t_1^{(1)} + \tau$ . The next gate starts at a time  $t_1^{(2)} \equiv t_1^{(1)} + T_D$  and ends at a time  $t_2^{(2)} \equiv t_1^{(2)} + \tau$ . This setup repeats for  $N_G$  gates and yields the final time that we use to define the completion of the QC process as  $T_f \equiv N_G T_D + \tau = N_G T_D + t_2 - t_1$ . At the time  $T_f$  the action of the gates is complete and the corresponding density matrix  $\rho(T_f)$  is the same as the instantaneous, static gate result  $U_G \rho(0) U_G^\dagger$ ; where  $U_G$  is a product of the  $N_G$  gate operators. The general result for the final time is  $T_f = N_G T_D + \tau + n_T T_L$ .

For example, consider a three-gate case for one qubit  $U_G \equiv \mathcal{H} \cdot \sigma_x \cdot \mathcal{H} \equiv \sigma_z$  which is a three gate  $N_G = 3$  Hadamard-Not-Hadamard sequence.

This case is illustrated in Fig. 16.

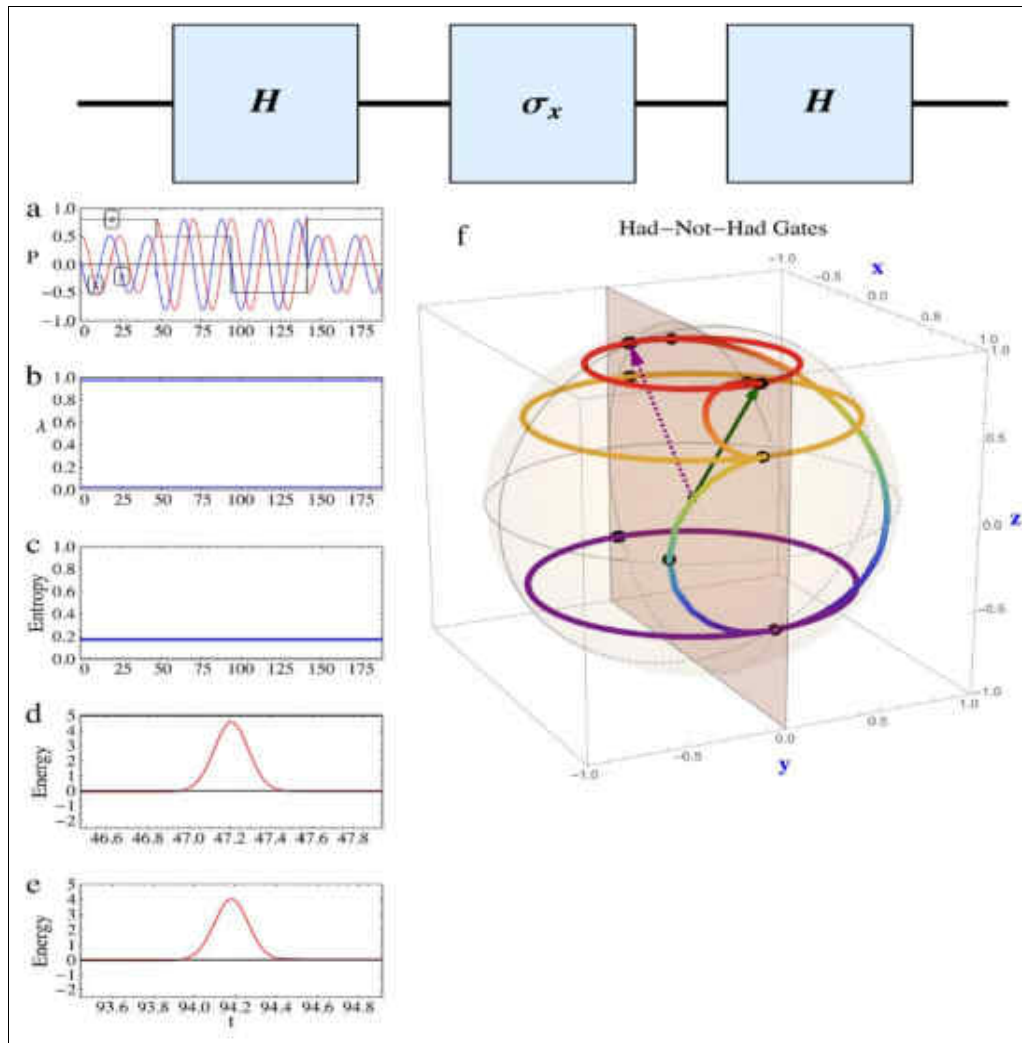


Fig. 16. Polarization for Hadamard-Not-Hadamard pulse gates. (a) Polarization vectors, (b) Eigenvalues, (c) Entropy, (d) Energy of first pulse, (e) Energy of second pulse, all versus time. Then in (f) Trajectories and initial and final polarization vectors, along with the three rapid gate pulses. The initial polarization vector (solid green arrow)  $(P_x, P_y, P_z) = (0.5, 0.1, 0.8)$  and final polarization vector (dashed purple arrow)  $(-0.5, -0.1, 0.8)$  are seen to give the expected  $\sigma_z$  gate result

For a sequence of  $N_G$  gates  $H(t) = \sum_{i=1}^{N_G} H_1(t - t_i^0) = \sum_{i=1}^{N_G} -\frac{\hbar \omega_L}{2} (1 - \theta_B(t - t_i^0)) \sigma_3 + \theta(t - t_i^0) \Omega_i$ , where

$\Omega_i$  is the  $i^{\text{th}}$  gate acting at the time centered at  $t_0 + t_i^0$ . This can generate a chain of gates.

We conclude that one can replicate the action of instantaneous static gates, which is central to the usual description of QC algorithms, by including a bias pulse during the gate action, and by applying the gates on the Larmor period time-grid.

**Schrodinger, Heisenberg, Dirac (Interaction) and Rotating Frame Pictures.** The Schrodinger picture for the density matrix is used, so that all aspects of the dynamics are described by the density matrix through its polarization and spin correlation observables. Other choices are to either use the Heisenberg picture, where the time development is incorporated into the Hermitian operators, or use the Dirac or Interaction picture, wherein the operators evolve in time with the “free” Hamiltonian  $H_0(t)$ . Then the Dirac picture density

matrix  $\tilde{\rho}(t) = e^{+iH_0(t)t/\hbar} \rho(t) e^{-iH_0(t)t/\hbar}$  evolves as:  $\frac{d\tilde{\rho}(t)}{dt} = -\frac{i}{\hbar} [\tilde{V}(t), \tilde{\rho}(t)] + \tilde{\mathcal{L}}$ , where the tilde denotes

interaction picture operators. For the choice of  $H_0(t) = -\frac{\hbar \omega_L}{2} \sigma_3$  going to the Dirac picture is simply going to a frame rotating about the z-axis in which frame the Larmor precession vanishes. That is called the *rotating frame*. Since we include gates into  $V(t)$  and hence  $\tilde{V}(t)$ , the gate bias pulse that we introduce in the Schrodinger picture, corresponds to a rotating frame that stops rotating during the action of a gate.

There are advantages offered by each of these choices. We stick with the Schrodinger description because it most clearly reveals the full dynamics by viewing the time evolution of the spin observables.

## The master equation model

The master equation for the time evolution of the system's density matrix is now presented. We seek a simple model that incorporates the main features of qubit dynamics for a quantum computer. These main features include seeing how the dynamics evolve under the action of gates and the role of both closed system dynamics and of open system decoherence, dissipation and the system's approach to equilibrium. From the density matrix we can determine a variety of observables, such as the polarization vector, the power and heat rates, the purity, fidelity, and entropy all as a function of time.

**Definition of the Model Master Equation.** To the unitary evolution, we now we add a term  $\mathcal{L}(t)$  which is required to be Hermitian and traceless so that the density matrix  $\rho(t)$  maintains its hermiticity and trace one properties. In addition,  $\mathcal{L}(t)$  has to keep  $\rho(t)$  positive definite. To identify explicit physical effects, we separate  $\mathcal{L}(t)$  into three terms:

$$\begin{aligned} \frac{d\rho}{dt} &= -\frac{i}{\hbar} [H(t), \rho(t)] + \mathcal{L}, \quad \mathcal{L} = \mathcal{L}_1 + \mathcal{L}_2 + \mathcal{L}_3, \\ \mathcal{L}_1 &= \Gamma \left\{ L(t) \rho(t) L^\dagger(t) - \frac{L^\dagger(t) L(t) \rho(t) + \rho(t) L^\dagger(t) L(t)}{2} \right\}, \quad \text{Lindblad} \\ \mathcal{L}_2 &= \gamma_2 \rho(t) (\tilde{S} - \langle \tilde{S} \rangle) - \gamma_2 \beta_2(t) \left\{ \frac{\rho(t) H(t) + H(t) \rho(t)}{2} - \rho(t) \langle H(t) \rangle \right\}, \quad \text{Beretta} \\ \mathcal{L}_3 &= \gamma_3 \rho(t) (\tilde{S} - \langle \tilde{S} \rangle) - \gamma_3 \beta_3(t) \left\{ \frac{\rho(t) H(t) + H(t) \rho(t)}{2} - \rho(t) \langle H(t) \rangle \right\}, \quad \text{Bath} \end{aligned}$$

the operator  $\tilde{S} \equiv -\log_e \rho(t)$  involves a base  $e$  logarithm to assure that a Gibbs density matrix is obtained in equilibrium (see later). The QC entropy is defined with a base 2 operator  $\tilde{S} \equiv -\log_2 \rho(t)$  with entropy equal to  $\langle S \rangle = \langle \tilde{S} \rangle = -\text{Tr}(\rho(t) \log_2 \rho(t))$ . The conversion factor is  $\tilde{S} \equiv -\log_e(2) \hat{S}$  and

$\langle \tilde{S} \rangle \equiv \log_e(2) \langle \tilde{S} \rangle$  with  $\log_e(2) = 0.693147$ . The level splitting, gates and bias pulses are included in  $H(t)$ . The state dependent, and hence time dependent, functions  $\beta_2(t), \beta_3(t)$  will be defined later.

When we discuss equilibrium, a form that combines the Beretta and Bath terms is used:

$$\mathcal{L}_{23}(t) = \gamma_{23} \rho(t) (\tilde{S} - \langle \tilde{S} \rangle) - \gamma_{23} \beta_{23}(t) \left\{ \frac{\rho(t) H(t) + H(t) \rho(t)}{2} - \rho(t) \langle H(t) \rangle \right\}$$

with  $\gamma_{23} = \gamma_2 + \gamma_3$  and  $\beta_{23}(t) = \frac{\gamma_2 \beta_2(t) + \gamma_3 \beta_3(t)}{\gamma_{23}}$ .

The  $\mathcal{L}_1$  is of Lindblad form, where the  $L(t)$  are time-dependent Lindblad spin-space operators, which we will represent later as pulses. The most important properties of the  $\mathcal{L}_1, \dots, \mathcal{L}_3$  operators are that they are Hermitian and traceless, which means that as the density matrix evolves in time, it remains Hermitian and of unit trace. They also have the property of maintaining the positive definite property of the density matrix. Note  $\Gamma$  sets the rate of the Lindblad contribution  $\mathcal{L}_1$ , in inverse time units. In the heuristic master equation, we use the Lindblad form to describe the impact of external noise on the system, where we represent the noise as random pulses. In addition, we also the Lindblad form used to describe dissipative/friction effects on the quantum gates, by having the Lindblad pulses coincide with the action time of the gate pulses. We also show later that a strong Lindblad pulse can represent a quantum measurement.

The  $\mathcal{L}_2$  term is the Beretta contribution, which describes a closed system. The closed system involves no heat transfer, with motion along a path of increasing entropy, as occurs for example with a non-ideal gas in an insulated container. This is accomplished by a state dependent  $\beta_2(t)$  that is presented later. Note  $\gamma_2$ , sets the strength of the Beretta contribution  $\mathcal{L}_2$ , in inverse time units as a fraction of the Larmor angular frequency.

In Table 3, typical values used in test cases are shown; these parameters are selected to focus on the role of each term. Realistic values can be invoked for various experimental conditions.

Table 3. Test Master Equation Parameters

Name	Value	Units
$\omega_L$	0.2675	GHz
$\Gamma$	0.00213	GHz
$\gamma_2$	0.0426	GHz
$\gamma_3$	0.0852	GHz
$\beta_3$	0.000425	1/ $\mu$ eV

*Remark.* In one simple version of the Bath contribution  $\mathcal{L}_3$ , the Bath temperature  $T$  in Kelvin stipulates a fixed value of  $\beta_3(t) \rightarrow \beta_3 \equiv 1/(k_B T)$ , where  $k_B$  is the Boltzmann constant (86.17  $\mu$  eV /Kelvin). A more general  $\mathcal{L}_3$  Bath contribution, based on a general theory of thermodynamics, defines a state dependent  $\beta_3(t)$  by using a fixed temperature  $T_Q$  to specify a fixed  $\dot{Q}(t)/\dot{S}(t)$  ratio (see later). Note  $\gamma_3$  sets the strength of the Bath contribution  $\mathcal{L}_3$ , in inverse time units as a fraction of the Larmor angular frequency.

Some general properties of the master equation and quantum entropy in Appendix are considered.

## One qubit system and the full model master equation

The full model master equation includes unitary evolution with gate pulses, the Lindblad  $\mathcal{L}_1$  with noise pulses, the Beretta  $\mathcal{L}_2$  to describe a closed system, and a bath  $\mathcal{L}_3$  term to include contact with a bath of fixed temperature. This provides a flexible model that can be used to gain insight into QC dynamics and gauge the requisite condition for a successful QC process. A simple example given here, with additional cases and tools to be posted.

**Full master equation Not gate.** In Fig. 17, a full model master equation case is displayed with a single Not gate.

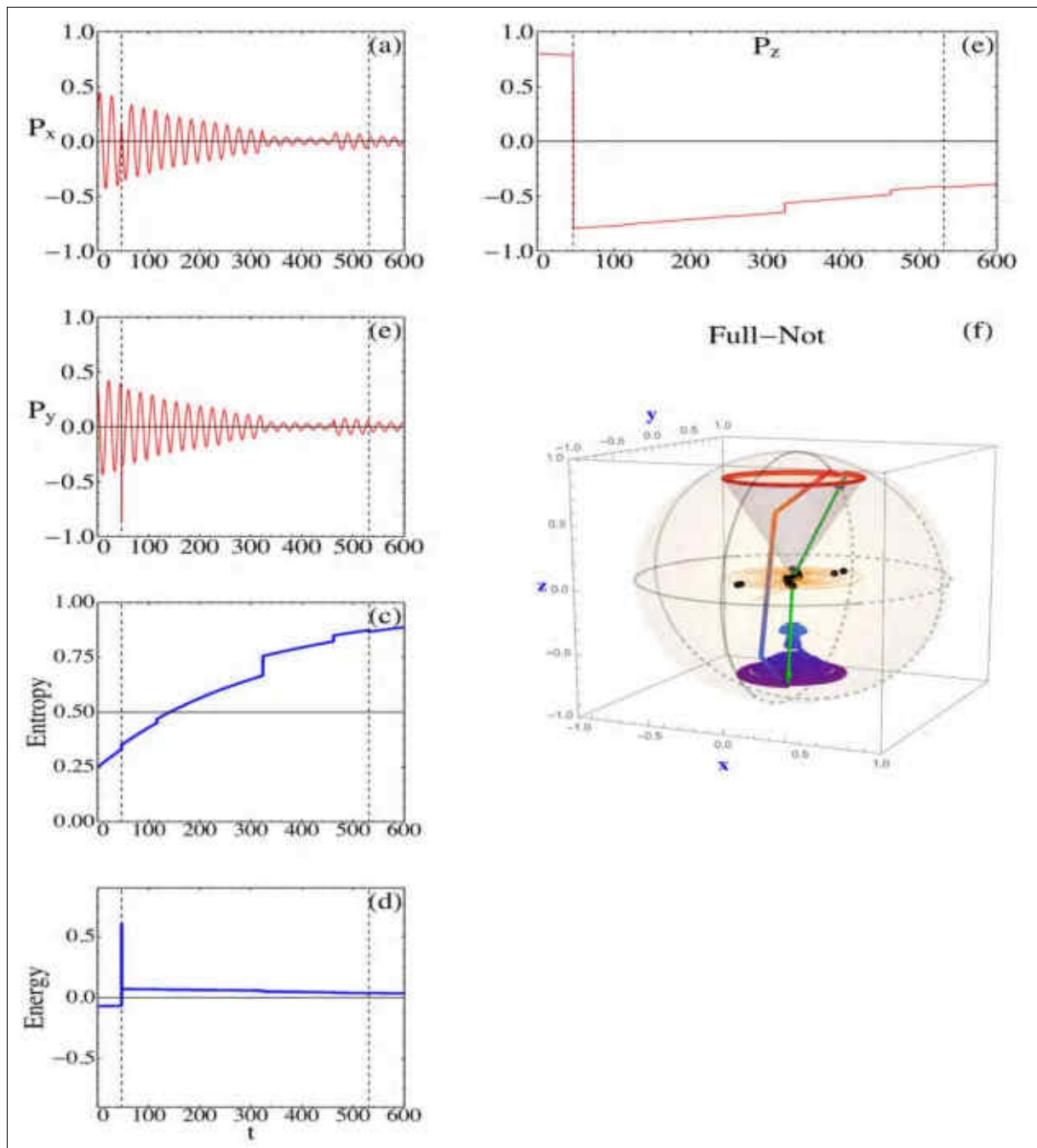


Fig. 17. A Full master equation case with a Not gate, Lindblad noise and Beretta and Bath terms

The initial polarization  $\vec{P} = \{0.2, 0.4, 0.8\}$  precesses about the z-axis with a Larmor angular frequency of  $\omega_L = 0.2675$  GHz: Eight random equispaced Lindblad pulses act during the  $t = 46.9$  to 531 nsec interlude;

the overall Lindblad strength is set as  $\Gamma = 0.4\omega_L$ . At 46.9 nsec a Not gate acts. The Beretta (closed system) strength is set as  $\gamma_2 = 0.01\omega_L$ . The bath term strength  $\gamma_3 = 0.005\omega_L$  and the bath temperature is 27:3 Kelvin: The evolution of the polarization shows a  $P_z$  gate flip followed by attenuation and noise alterations, as expected. The Lindblad noise shows up as jagged entropy evolution, where the random nature of the Lindblad pulses allows for entropy decreases as well as increases. The energy plot shows the Not and bias pulse work and the energy flip to increased energy occupation.

In Fig. 18, the fidelity, entropy and purity evolutions are presented with values on the Larmor grid (integer multiples of TL) indicated by red dots (fidelity), blue diamonds (entropy) and orange squares (1-purity).

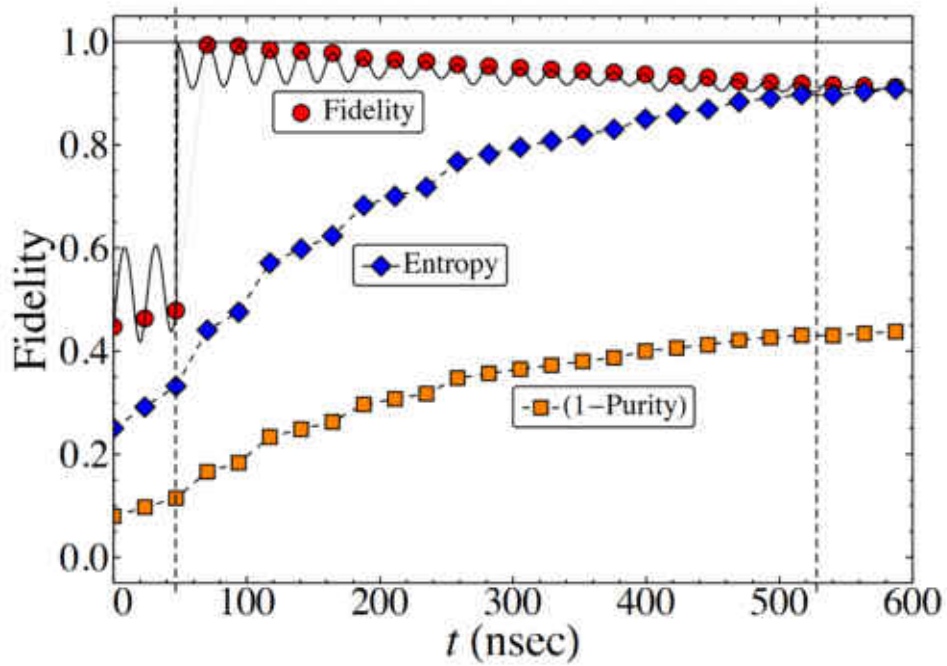


Fig. 18. Fidelity with a NOT gate, noise and Beretta and Bath terms.

[Between the vertical dashed lines eight Lindblad noise pulses occur. Fidelity, entropy and purity are shown on the Larmor period grid. The full master equation density matrix is compared to the expected  $\rho_e = \sigma_1 \cdot \rho(0) \cdot \sigma_1$  by examining the Fidelity( $\rho(t), \rho_e$ ). The fidelity jumps to one after the gate, then drifts down due to noise, Beretta and Bath terms]

There is a clear reduction in fidelity due to noise and gradual fall off from the Beretta and bath effects. Both entropy and purity reveal the affect of Lindblad noise.

In Fig. 19, the case of two sequential Not gates shown.



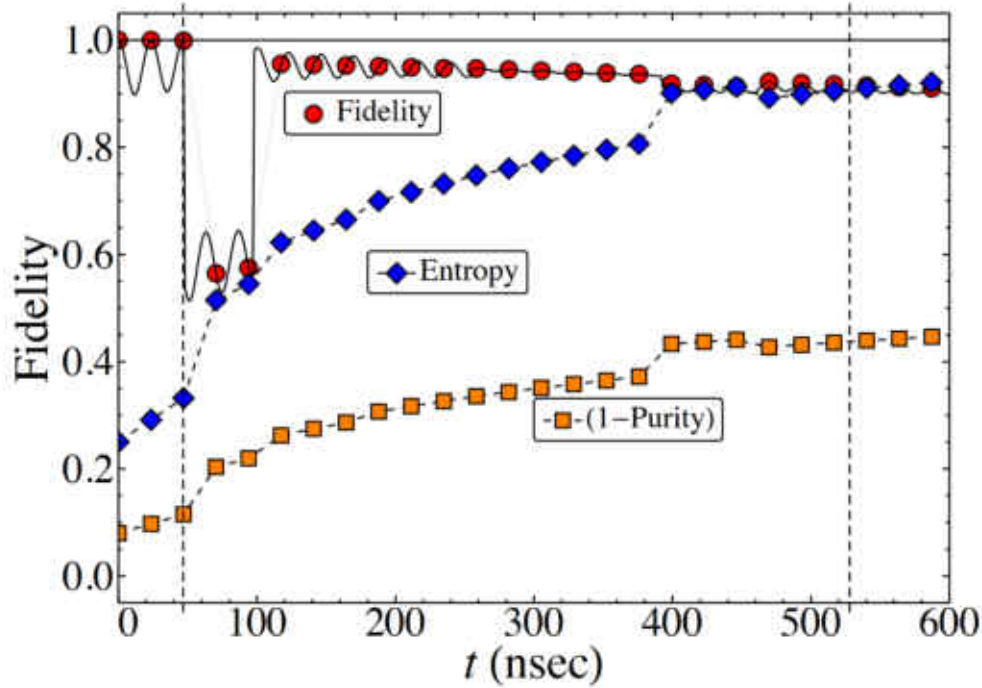


Fig. 19. Fidelity for two sequential not gates, Beretta and bath terms as in Fig. 18.  
[Noise occurs between the vertical dashed lines, but differs from prior plot. After the second not gate, the fidelity does not equal 1, due to the noise, Beretta and bath effects]

Studies of other gate sequences and alternate noise scenarios reveal similar properties. Cases of no gates, but noise, Beretta and bath terms can be used to identify quantum memory losses.

The main result from this study is the design of a dynamical density matrix model that incorporates the essential features of a quantum computer. Although much of the input is well-known, it is shown here how to implement unitary gate pulses, plus an associated bias pulse, to replicate the usual quantum gates. The bias pulse is introduced to obviate the accumulation of detrimental phase accumulations due to qubit non-degeneracy. To replicate the QC static gate network for a sequence of gates, it is shown that the various gates also need to be applied on the Larmor time grid. The model also includes dissipative, decoherence and thermodynamic effects. The Lindblad addition to unitary dynamics has the essential feature of maintaining the unit trace, Hermiticity and positive definite nature of the evolving density matrix. A general Lindblad form, after examining various static Lindblad operators, is used to incorporate random noise and gate friction effects; these are input as non-static pulses. In addition, strong rapid Lindblad operators are implemented as measurements, and the associated restriction to be valid measurements examined. Although many other effects can also be cast into Lindblad form, it is much simpler to design separate forms for closed systems and for system-Bath interactions. The closed system form is one developed by Beretta based on a general study of non-equilibrium thermodynamics. Two types of system-Bath interactions are examined, one that has been studied before, and another one also originated by Beretta that is illustrated herein to have physical advantages. Another result of this study is provided by several examples of how to apply the full model including random noise, gate friction, closed system entropy increase, and system-Bath interactions to a set of unitary gates. Fidelity is used to gauge the stability of such a QC setup.

This illustrates how the model can be used as a tool to examine and design valid experiments to achieve stable quantum computation.

## Semiconductor quantum computation

A qubit is a two-level system that exhibits quantum properties: superposition and entanglement. Superposition refers to the ability that a qubit has to not only reside in the state  $|0\rangle$  or  $|1\rangle$  like a classical bit, but also in the state

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle.$$

Here  $\theta$  and  $\phi$  are real numbers that define a point on a unit 3D sphere. Thus, an arbitrary qubit state can be described as a point on the surface of a sphere, as depicted in Fig. 20a, which is termed a Bloch sphere. The basis states  $|0\rangle$  and  $|1\rangle$  are the north and south poles of the sphere, respectively, while the two super-position states  $1/\sqrt{2}(|0\rangle + |1\rangle)$  and  $1/\sqrt{2}(|0\rangle - |1\rangle)$  are on the equator.

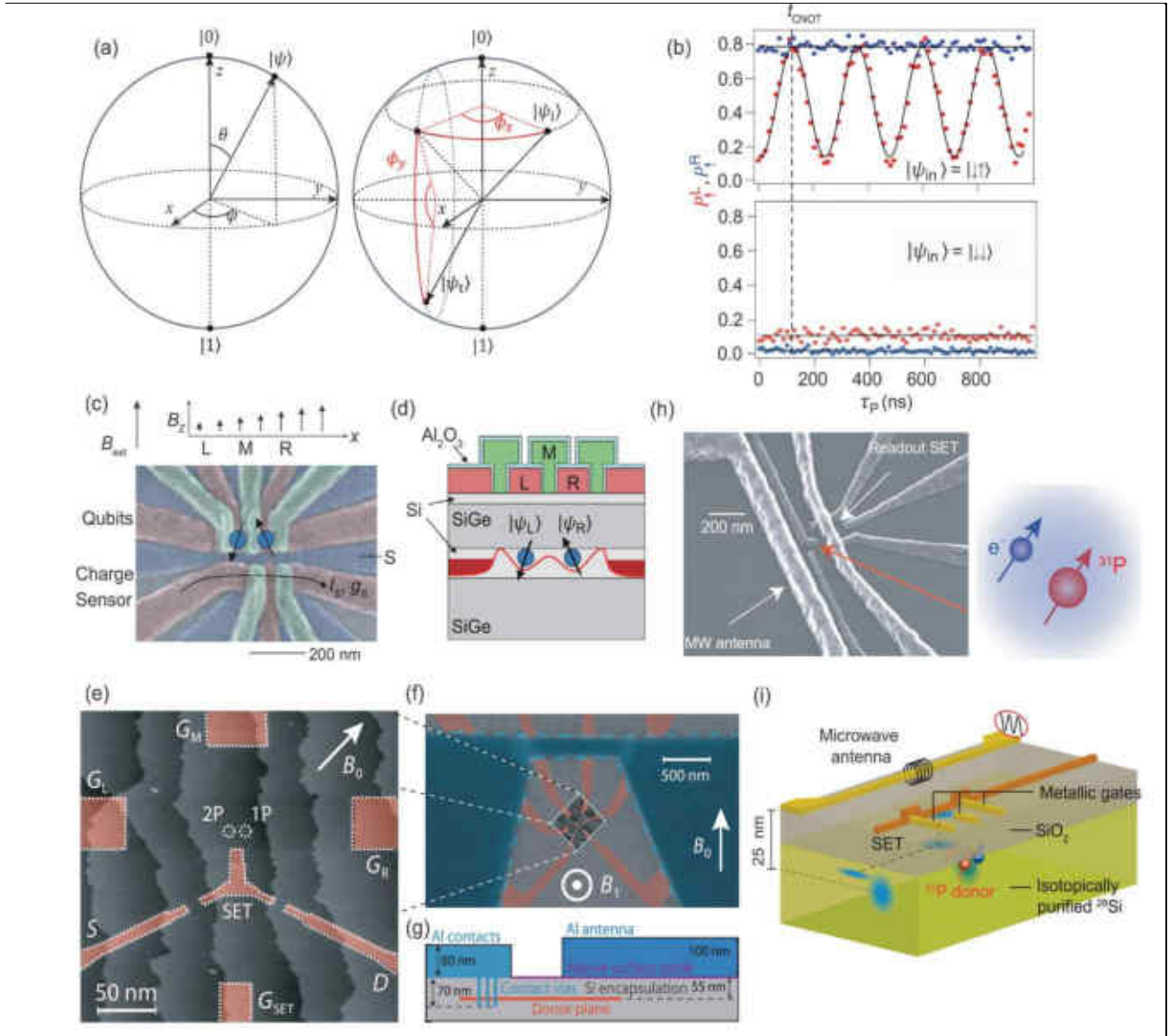


Fig. 20. Single- and two-qubit gate control and devices for semiconductor qubits. (a) Bloch-sphere representation of a qubit. A superposition state  $|\psi\rangle$  can be represented by a point on the sphere (left). An arbitrary rotation from the initial state  $|\psi_i\rangle$  to the target state  $|\psi_t\rangle$  can be decomposed by successive rotations about the  $z$  and  $y$  axes for  $\phi_z$  and  $\phi_y$ , respectively (right). (b) The spin-up probability of the spin-up state for the right qubit  $P_\uparrow^R$  (blue) and the left qubit  $P_\uparrow^L$  (red) as a function of interaction time  $\tau_p$  for input states  $|\uparrow\uparrow\rangle$  and  $|\downarrow\downarrow\rangle$ . The vertical dashed line at  $\tau_p = 130$  ns corresponds to a CNOT gate. (Adapted from [8].) (c) and (d) are a false-color SEM image and a schematic cross-section of a Si/SiGe DQD, respectively. The DQD with two electrons confined in the potential created by gates L, M and R is used to form two spin-1/2 qubits and a SET under the DQD is used to work as a charge sensor. A slanting Zeeman field was created by a micro-magnet (not shown) for qubit control. (Adapted from [9].) (e), (f) and (g) are images and schematics for the device fabricated by STM hydrogen lithography. (Adapted from [8].) (e) Large-scale STM image of the



device; red areas are P-doped to form a SET, source and drain leads, and electrostatic gates. A donor molecule (2P) and single donor (1P) are shown by two circles. (f) False-color composite SEM and STM image showing the buried donor structures (red) and the aluminum antenna (blue). (g) Vertical cross-section of the donor device, showing the thicknesses (not to scale) and relative positions of the silicon, phosphorus, oxide and aluminum layers. (h) and (i) are a SEM image and schematic oblique view of a device fabricated by ion implantation, highlighting the position of the P donor, the MW antenna and the readout SET. (Adapted from [8] and [9])

All the quantum algorithms are based on a certain quantum computing model, varying from the quantum circuit, one-way quantum computation, adiabatic quantum computation and topological quantum computation. These four models are equivalent in computational power; among them, the quantum circuit model is most frequently used. In the circuit model, it has been proved that arbitrary single-qubit rotations plus two-qubit controlled-NOT gates are universal, i.e. they can provide a set of gates to implement any quantum algorithm.

As Fig. 20a shows, for a certain initial state  $|\psi_i\rangle$  on the Bloch sphere, an arbitrary target state  $|\psi_f\rangle$  can be achieved just by successive rotations about the  $z$  and  $y$  axes for  $\phi_z$  and  $\phi_y$ , respectively. In fact, as long as one can control rotations around two different axes of the Bloch sphere, arbitrary single-qubit rotations can be performed; this is also known as universal single-qubit control. On the other hand, a two-qubit controlled-NOT (CNOT) gate implies that one qubit state can be controlled by another.

It acts on two qubits and a  $\pi$  rotation around the  $x$  axis is performed on the target qubit only when the control qubit state is  $|1\rangle$ . This intriguing phenomenon is shown in Fig. 19b, an experimental result from Zajac *et al.*, in which the ground state  $|0\rangle$  ( $|1\rangle$ ) is denoted by spin-down  $|\downarrow\rangle$  (spin-up  $|\uparrow\rangle$ ).

In this figure, as manifested by the spin-up probabilities, the left qubit (red) shows rotations around the  $x$  axis as a function of interaction time when the right qubit (blue) is initialized in  $|1\rangle$ , whereas it keeps its initial state all the time when the right qubit is initialized oppositely. The vertical dashed line at which the two left qubit states are exactly opposite corresponds to a CNOT gate. Therefore, the core issue of building a quantum computer is to prepare a qubit with high-fidelity single- and two-qubit gates. The control fidelity depends on two factors: the coherence time and the manipulation time. Coherence time, also called dephasing time, is usually termed  $T_2$  and indicates how long a qubit can keep its quantum properties, while manipulation time, characterized by a rotation angle of  $\pi$  ( $T_\pi$ ) or  $2\pi$  ( $T_{2\pi}$ ), refers to the time required for a single manipulation.

A typical device of gate-defined lateral quantum dots is shown in Fig. 20c and d; the electrodes on the surface of the Si/SiGe heterostructure can form quantum potentials in the Si well to trap electrons, and the electron spins can be manipulated as qubits when an external magnetic field is applied. The upper half of Fig. 1c is a double quantum dot (DQD) to form two spin-1/2 qubits and the lower half is a single quantum dot (SQD) acting as a charge sensor to measure the charge states of the DQD, which is also called a single electron transistor (SET).

In fact, quantum dots can be formed in various systems, including GaAs/AlGaAs heterostructures, silicon metal-oxide-semiconductor (MOS) and silicon-on-insulator (SOI), nanowires, nanotubes, graphene, van der Waals heterostructures, and self-assembled crystals.

It is worth mentioning that quantum dots based on Si/SiO<sub>2</sub> and SOI technology are both CMOS compatible and we denote the former as silicon MOS and the latter as SOI for clarity. On the heels of the proposal for quantum-dot-based electron spins, Bruce Kane showed that the nuclear spin of a single <sup>31</sup>P donor in silicon can also be controlled as a qubit. There are two approaches to fabricate the device: scanning tunneling microscopy (STM) hydrogen lithography and ion implantation. For the former approach, the STM tip enables atomic-scale precision of placing P atoms in silicon. Figure 1e is an STM image of a device fabricated using this approach, showing a single donor (1P) and a donor molecule (2P) in the center for spin manipulation and beneath them is a SET for charge sensing. The blue area in Fig. 20f is an aluminum antenna generating an oscillating magnetic field over the device, and Fig. 20g is the vertical cross-section showing the relative position of the antenna and the silicon device.

For the latter approach, P ions are implanted into a very small region of the silicon using mask resists. Figure 1g and h show a scanning electron microscopy (SEM) image and the schematic of a device fabricated by ion implantation. In Fig. 20g, a P donor was implanted in the area denoted by the red arrow, and the spins

of both the electron bound to the donor and the donor nucleus can be used as qubits. Also, the SET and the AI antenna are used for readout and manipulation. In 2003, Hayashi and co-workers also investigated the coherent manipulation of electronic states of a DQD in the GaAs/AlGaAs heterostructure and showed the opportunity to implement a charge qubit in a semiconductor DQD. These proposals together resulted in a subsequent firestorm of experimental activities.

So far, single- and two-qubit gate control has been achieved with fidelity above 99.9% and 98% respectively, approaching the surface code threshold for fault-tolerant computing.

Also, thanks to the advanced semiconductor technology, several proposals taking advantage of today's semiconductor processing tools to scale up to 2D grids have been put forward. Therefore, it is believed that there is a huge opportunity to real-ize a scalable fault-tolerant semiconductor quantum computer in the future.

Both the spin and charge degrees of the electrons and donor nucleus can be employed as qubits. For the spin degree, spin-1/2 qubits, singlet–triplet qubits and exchange-only qubits have been proposed and realized in experiments successively. To take advantage of both spin and charge degrees, the hybrid qubit has also been presented as a competitive candidate.

Once an electron or nucleus is put into a magnetic field  $B_0$ , the energy levels of spin-up and spin-down are no longer degenerate and split by the so-called Zeeman energy. This is a two-level system that can be used as a qubit and we call it a spin-1/2 qubit to distinguish it from other types of spin qubits. To manipulate this type of qubit, microwave (MW) bursts via an antenna were used to generate an oscillating magnetic field, as illustrated in Fig. 20f and h. This approach is called electron spin resonance (ESR) for controlling electron spins or nuclear magnetic resonance (NMR) for controlling nuclear spins.

**Single-qubit gate in semiconductor.** Once an electron or nucleus is put into a magnetic field  $B_0$ , the energy levels of spin-up and spin-down are no longer degenerate and split by the so-called Zeeman energy. This is a two-level system that can be used as a qubit and we call it a spin-1/2 qubit to distinguish it from other types of spin qubits. To manipulate this type of qubit, microwave (MW) bursts via an antenna were used to generate an oscillating magnetic field, as illustrated in Fig. 20f and 1h. This approach is called electron spin resonance (ESR) for controlling electron spins or nuclear magnetic resonance (NMR) for controlling nuclear spins.

The qubit to rotate around the  $x$  axis. In particular, the nutation between  $|0\rangle$  and  $|1\rangle$  is usually called *Rabi oscillation*. When the MW is halted for a time, or the relative phase of successive MW bursts is varied, the qubit will acquire a rotation angle around the  $z$  axis. Universal single spin control can thus be achieved using this approach. Alternatively, another approach to manipulate the spin-1/2 qubit is electric-dipole spin resonance (EDSR). In this approach, a magnetic field gradient is applied with the help of spin–orbital coupling (SOC) of the semiconductor or an integrated micromagnet, and the electron in this environment can feel an effective oscillating magnetic field if it is driven by an oscillating electric field. Therefore, MW bursts can be applied directly on a single electrode and  $B_1$  is proportional to its voltage amplitude.

One example using this approach is shown in Fig. 20c; there is a magnetic field gradient in the device generated by an integrated micro-magnet (not shown), and the MW bursts are applied on gate  $S$  for qubit control.

Readout of the spin-1/2 qubits relies on a spin–charge conversion as spin-selective tunneling or spin blockade, and after the con-version the charge signal is detected by a nearby charge sensor.

The procedure for spin-selective tunneling is illustrated in Fig. 21a and b, when a spin-1/2 qubit is under MW control, the energy levels of both spin states are under the Fermi level of the drain, and, after control, the energy levels in the quantum dot are tuned so that the energy level of spin-up is higher than the Fermi level of the drain and spin-down is lower. In this energy-level alignment, only the electron with spin-up can tunnel out of the quantum dot and thus the spin state can be distinguished by observing the electron tunneling signal. This approach was first demonstrated by Elzerman *et al.* in 2004 and they achieved single-shot readout of a single electron spin for the first time.

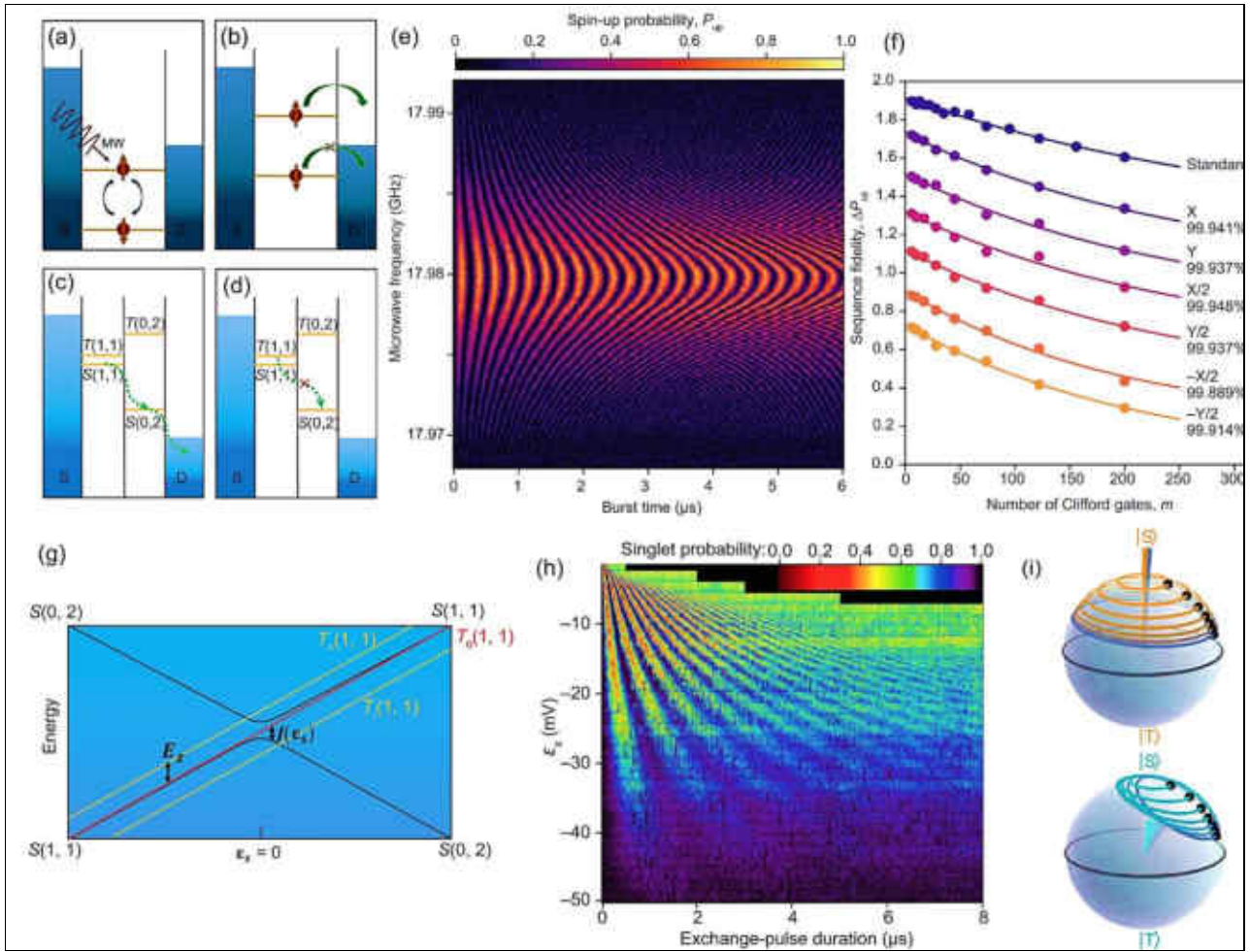


Fig. 21. Spin-1/2 qubit and singlet-triplet qubit. (a) and (b) are diagrams showing the process of control and readout based on spin-selective tunneling. (a) At the stage for qubit control, both energy levels of spin-up and spin-down are under the Fermi level of drain. (b) At the stage for readout, the energy levels in the dot are tuned so that the Fermi level of drain is between the energy levels of spin-down and spin-up. (c) and (d) are diagrams showing the phenomenon of spin blockade:  $S(1, 1)$  can move to  $S(0, 2)$  while  $T(1, 1)$  cannot. (e) The probability of spin-up  $P_{up}$  as a function of MW burst time and frequency detuning. (Adapted from [8,9].) (f) Sequence fidelities for standard (topmost) and interleaved randomized benchmarking (annotated in the figure along with extracted fidelities). Traces are offset by an increment of 0.2 for clarity. Visibilities are within  $0.72 \pm 0.012$ . (Adapted from [7,8].) (g) Energy-level spectrum of two spin states in a DQD as a function of detuning  $\epsilon_s$ . A magnetic field splits the triplet states by the Zeeman energy  $E_z$  and the exchange interaction splits  $S$  and  $T_0$  by  $J(\epsilon_s)$ . (h) Singlet probability as a function of exchange-pulse duration and detuning  $\epsilon_s$ . (Adapted from [8].) (i) Bloch-sphere representations of state evolution in the case  $J(\epsilon_s) > \Delta E_z$  (top) and  $J(\epsilon_s) < \Delta E_z$  (bottom). (Adapted from [8])

An adaptation of Elzerman's method is used the tunneling rate difference instead of the energy difference of two energy levels to differentiate spin states. As for the spin blockade, it utilizes another spin as an ancilla qubit to read the spin state in the singlet-triplet basis. There are four basis states for two spins in a magnetic field and they can be sorted into a singlet and three triplets:

$$S = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle), \quad T_0 = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle), \quad T_+ = |\uparrow\uparrow\rangle, \quad T_- = |\downarrow\downarrow\rangle$$

Here,  $S$  and  $T_0$  are separated by the exchange interaction strength  $J$ , and the three triplets are split by the Zeeman energy  $E_z$ . We denote the singlet with each electron occupying one quantum dot as  $S(1, 1)$  and the one with two electrons both occupying the right dot as  $S(0, 2)$ . This type of notation also applies to the triplets. If we suppose that both spins are initialized in  $|\downarrow\downarrow\rangle$ , the MW bursts on the left spin will lead the two spin states

to oscillate between  $|\downarrow\downarrow\rangle$  and  $|\uparrow\downarrow\rangle$ . In experiments,  $|\downarrow\downarrow\rangle$  is usually mapped to  $T(1, 1)$  and  $|\uparrow\downarrow\rangle$  is mapped to  $S(1, 1)$ .

As illustrated in Fig. 21c and d, only the  $S(1, 1)$  state can transit to  $S(0, 2)$  and other states are prohibited because of spin blockade. Thus, a nearby charge sensor that can differentiate charge states  $(1, 1)$  and  $(0, 2)$  is able to read out the spin state. For simplicity, in the figure we use  $T(1, 1)$  for those triplets.

Other approaches include manipulating spins of holes that are bound to acceptors in silicon or that are trapped in quantum dots fabricated from the p-GaAs/AlGaAs heterostructure, the silicon MOS, Ge/GeSi heterostructures and core-shell nanowires.

Another type of spin qubit is encoded by two eigen-states of two spins. Usually, the encoded states are  $S$  and  $T_0$ , and we thus call it singlet-triplet qubit. The effective control Hamiltonian can be written as follows:

$$H_{ST} = J(\varepsilon_s) \sigma_z / 2 + \Delta E_z \sigma_x / 2$$

Here,  $J(\varepsilon_s)$  is the energy of exchange splitting of  $S$  and  $T_0$ , where the detuning  $\varepsilon_s$  denotes the electrochemical potential difference of different charge occupation states, and  $\Delta E_z$  is the Zeeman energy difference of two spins, which may be caused by different  $g$ -factors, i.e.  $\Delta E_z = \Delta g \mu_B B_z$ , or magnetic field gradients, i.e.

$$\Delta E_z = g \mu_B \Delta B_z$$

As shown in Fig. 20g, when the detuning point is set negative and far away from zero,  $J(\varepsilon_s)$  will be vanishing and thus the qubit will rotate around the  $x$  axis; in contrast, when the detuning point is tuned in the positive direction until  $J(\varepsilon_s) \gg \Delta E_z$ , the qubit will rotate around the  $z$  axis. In this control procedure, only the parameter  $\varepsilon_s$  is used and thus the need for ESR or EDSR is removed compared to spin-1/2 qubits. After manipulation, the qubit can be measured directly using spin blockade. The singlet-triplet qubit was first demonstrated experimentally in GaAs quantum dots with  $T_2^* \sim 10$  ns and a rotation period  $T_{2\pi} \sim 720$  ps around the  $z$  axis by Petta *et al.* in 2005.

The  $S$ - $T_0$  oscillations in the experiment can be observed in Fig. 21h.

Figure 21i shows the Bloch sphere representations of state evolution in the case

$$J(\varepsilon_s) > \Delta E_z, \text{ and } J(\varepsilon_s) < \Delta E_z.$$

However, the spin blockade can be lifted easily due to the small splitting of the two low-lying valley states in the Si/SiGe heterostructure, which puts a great hurdle in front of the reproducibility of singlet-triplet qubits in this material.

Apart from these, singlet-triplet qubits can also be encoded by  $S$  and  $T_+$ , or implemented in other systems, such as donors in silicon and hybrid donor-dot architecture. It is noteworthy that for donors in silicon, the transitions between  $(1, 1)$  and  $(0, 2)$  are harder to distinguish for the special charge sensor arrangement and thus the energy-selective readout or tunnel-rate-selective readout like spin-1/2 qubits are preferred. These two readout methods for singlet-triplet qubits have been investigated by Broome *et al.* and Dehollain *et al.*, respectively. For the hybrid donor-dot singlet-triplet qubits, the readout relies on the afore-mentioned latching-enhanced spin blockade.

**Exchange-only qubit.** Though singlet-triplet qubits can be driven all electrically, they still need a Zeeman energy difference to achieve universal single-qubit control. How about implementing a qubit solely by exchange interaction? This idea leads to the exchange-only qubit. As illustrated in Fig. 22a, this type of qubit is composed of three electrons in a triple quantum dot (TQD).

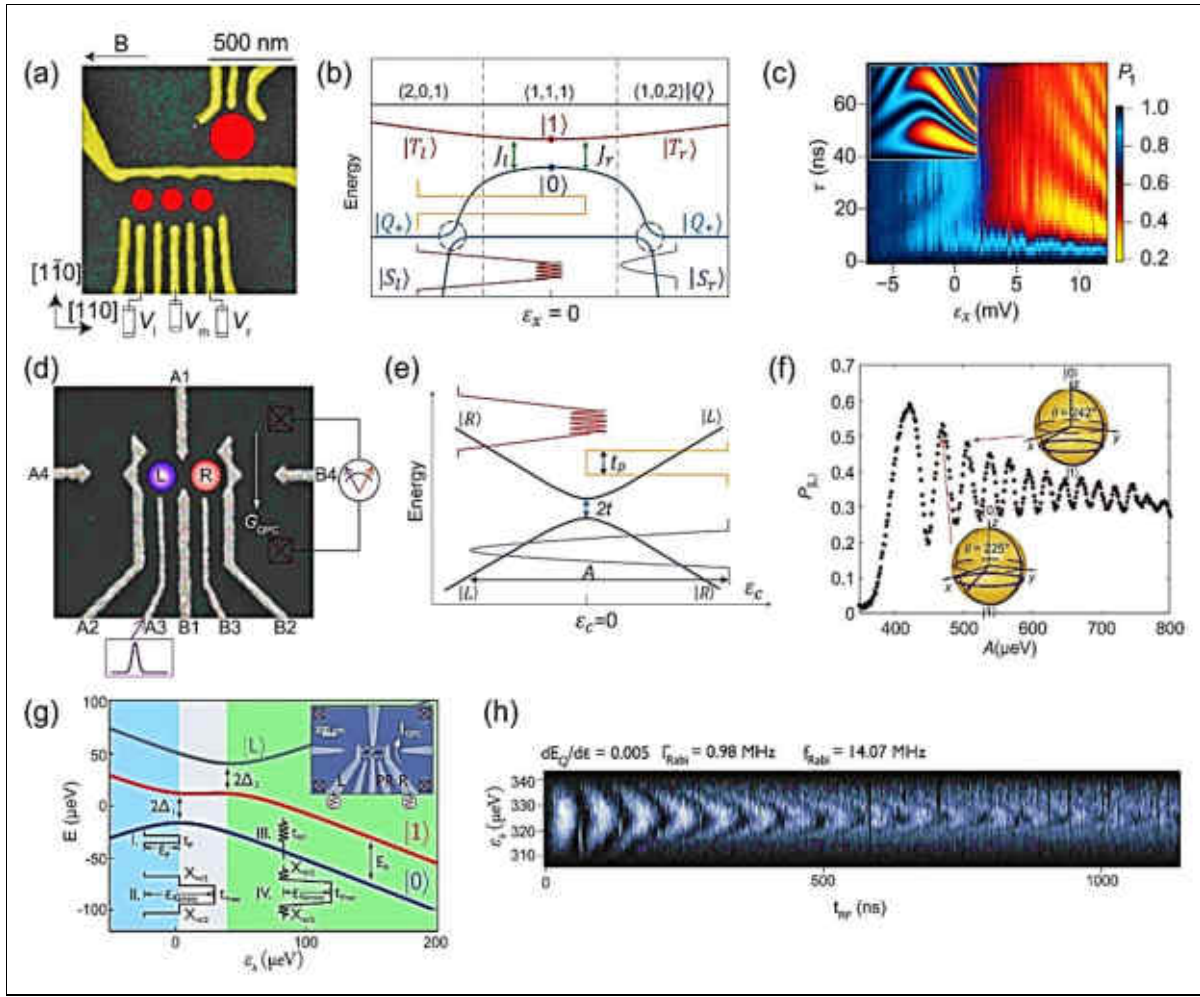


Fig. 22. Implementations of the exchange-only qubit, the charge qubit and the hybrid qubit. (a) False-color SEM image of a TQD device for an exchange-only qubit, with a SET on the top for charge sensing. (Adapted from [8].) (b) Energy levels as a function of detuning  $\epsilon_x$  for the exchange-only qubit. Two anti-crossings are shown by two dotted circles. Yellow, red and gray pulse shapes are shown to denote the relative positions of detuning for Larmor oscillation, Rabi oscillation and LZS interferences. (c) The probability  $P_1$  of detecting the state  $|S_L\rangle$  as a function of pulse position  $\epsilon_x$  and wait time  $\tau$ . Inset is a simulation result of qubit evolution as a function of exchange without noise. (Adapted from [8].) (d) A SEM image of a DQD device for a charge qubit with two QPCs for readout.  $|L\rangle$  and  $|R\rangle$  are denoted by two circles in the DQD. (Adapted from [9].) (e) Energy levels of a charge qubit as a function of detuning  $\epsilon_c$ . Red, yellow and gray pulse shapes are shown to denote the relative positions of detuning for Rabi oscillation, Larmor oscillations and LZS interferences. (f) Charge-state probability  $P_{|L\rangle}$  as a function of LZS pulse amplitude  $A$ . The Bloch-sphere representations for two interference nodes are also labeled. (Adapted from [9].) (g) Energy spectrum as a function of  $\epsilon_h$  and pulse sequences for the hybrid qubit. Inset is a SEM image of a DQD device with a QPC for readout. (Adapted from [9].) (h) Rabi oscillations demonstrating a decay time longer than  $1 \mu s$ . (Adapted from [9])

There are eight basis states for three spins, and among them are singlet-like state and triplet like states, respectively, which can be inferred from the state of the left (right) two spins. The two exchange-splitting energies  $J_l(\epsilon_x)$  and  $J_r(\epsilon_x)$  are associated with the left pair and the right pair of quantum dots, respectively, and the detuning  $\epsilon_x$  denotes the relative electrochemical potential of the charge configurations (2, 0, 1), (1, 1, 1) and (1, 0, 2). As depicted in Fig. 3a, the ground state  $|0\rangle = 1/\sqrt{6}(|\uparrow\uparrow\downarrow\rangle + |\downarrow\uparrow\uparrow\rangle - 2|\uparrow\downarrow\uparrow\rangle)$  and the excited state  $|1\rangle = 1/\sqrt{2}(|\uparrow\uparrow\downarrow\rangle - |\downarrow\uparrow\uparrow\rangle)$  are encoded in the center of the (1, 1, 1) charge configuration with  $J_l(\epsilon_x) = J_r(\epsilon_x)$ . Also, there are two extra states  $|Q\rangle = 1/\sqrt{3}(|\uparrow\uparrow\downarrow\rangle + |\uparrow\downarrow\uparrow\rangle - 2|\downarrow\uparrow\uparrow\rangle)$  and  $|Q_+\rangle = |\uparrow\uparrow\uparrow\rangle$  in the



energy-level spectrum that may offer leakage channels when the qubit is under control. The control Hamiltonian can be described as:

$$H_{EX} = -J_l(\varepsilon_x)\sigma_l/2 - J_r(\varepsilon_x)\sigma_r/2 \text{ in which } \sigma_l = (\sigma_z - \sqrt{3}\sigma_x)/2, \quad \sigma_r = (\sigma_z + \sqrt{3}\sigma_x)/2.$$

In the Bloch sphere, the axes  $\sigma_l$  and  $\sigma_r$  are  $120^\circ$  apart and thus universal single-qubit control can be achieved by directly tuning  $J_l(\varepsilon_x)$  and  $J_r(\varepsilon_x)$  via detuning pulses. This method is called Larmor precession and, as an example, a control pulse sequence (yellow) is drawn in Fig. 21b, indicating a detuning pulse from  $|S_l\rangle$  to (1, 1, 1). After manipulation, the qubit state can be measured via spin blockade with  $|0\rangle$  mapped to  $|S_l\rangle(|S_r\rangle)$  and  $|1\rangle$  mapped to  $|T_l\rangle(|T_r\rangle)$ . In 2010, Laird *et al.* first demonstrated an exchange-only qubit in a GaAs TQD with this approach, and then, in 2013, Medford *et al.* measured an inhomogeneous dephasing time  $T_2^* \sim 25$  ns and a rotation time  $T_{2\pi}$  as short as  $\sim 21$  ps. The coherent oscillations in their experiment are shown in Fig. 21c. Another approach to control exchange-only qubits is to use Rabi oscillations. As the red pulse sequence in Fig. 21b shows, qubit manipulation can be implemented directly by applying MW bursts at zero detuning with a frequency in resonance with the energy gap between  $|0\rangle$  and  $|1\rangle$ .

The qubit controlled in this way is also called a resonant exchange qubit. In 2013, Medford *et al.* demonstrated a resonant exchange qubit and reported an intrinsic dephasing time  $T_2 \sim 19$   $\mu$ s and a rotation time  $T_{2\pi} \sim 10$  ns. To make further improvements, other investigations also include reducing magnetic noise by performing experiments in silicon quantum dots and suppressing charge noise by using MW bursts in a highly symmetric regime. Moreover, the spin states of a TQD can also be controlled through Landau–Zener–Stuckelberg (LZS) interferences. This was demonstrated by Gaudreau *et al.* in 2011 and they encoded a qubit using the state  $|0\rangle$  and  $|Q_+\rangle$ . The hyperfine interaction that couples these two states results in two anti-crossings in the energy-level spectrum, which are denoted by dotted circles in Fig. 22b. An adiabatic pulse passing through one of the anti-crossings with an appropriate rise time can create a super-position state of  $|0\rangle$  and  $|Q_+\rangle$  due to a Landau–Zener transition, and after a time the pulse goes across the anti-crossing again and back to its original position, resulting in LZS interferences. After that, a measurement in the basis of qubit eigenstates will show corresponding coherent oscillations. From the fit to the LZS model with their experimental results, they extracted a dephasing time  $T_2^*$  around 8–15 ns.

Besides the spin degree, quantum control of the charge states of an electron is also of interest. For a charge qubit, the ground state  $|0\rangle$  and the excited state  $|1\rangle$  can be defined by the excess electron occupation of a DQD, and as illustrated in Fig. 22d, they are usually denoted by  $|R\rangle$  and  $|L\rangle$ , respectively.

Readout of the qubit states can be implemented directly by a proximate charge sensor, a SET or a quantum point contact (QPC), or just the transport current from source to drain, so that it removes the need of any conversion like spin qubits. In Fig. 22d, the current through QPC is shown by the white arrow. The energy levels are depicted in Fig. 22e. The adiabatic short pulse that they used to drive the qubit is shown in Fig. 3e; as described in the previous subsection, the LZS interference is finished after the pulse goes across the anti-crossing and back to its original position. The measured interferences as a function of pulse amplitude  $A$  are depicted in Fig. 22f, and, as shown by the Bloch spheres labeled at two interference nodes, the qubit is rotated around the  $z$  axis by  $2\pi$  between every two successive interference fringes while the rotation angle of the  $x$  axis,  $\theta$ , increases monotonically with pulse amplitude. Therefore, the qubit can be rotated around both the  $x$  and  $z$  axes within a single pulse and these rotations can be controlled arbitrarily by adjusting the pulse amplitude. Moreover, the charge qubit can also be controlled by applying resonant MW bursts at  $\varepsilon_c = 0$  to induce Rabi oscillations and the two-axis control using MW bursts is just like that of spin-1/2 qubits and resonant exchange qubits.

**Hybrid qubit.** Inspired by the fact that the coherence times of spin qubits are usually very long and the manipulation times of charge qubits are very short, one may question whether we can create a new type of qubit combining the advantages of both. An attempt originating from this idea is the hybrid qubit. This type of qubit is encoded by two eigenstates of three electron spins in a DQD and was first demonstrated in a Si/SiGe heterostructure.

Figure 22g shows its energy levels as well as the device set-up. The two lowest energy levels for qubit control are  $|0\rangle = |\downarrow\rangle_L |S\rangle_R$ ,  $|1\rangle = 1/\sqrt{3} |\downarrow\rangle_L |T_0\rangle_R - 2/\sqrt{3} |\uparrow\rangle_L |T_-\rangle_R$ . The subscript  $L$  ( $R$ ) denotes the spin state in the left (right) quantum dot, and the higher state  $|L\rangle$  in Fig. 22g is a primary leakage channel.

On the basis of these three states, the Hamiltonian can be written as

$$H_\varepsilon = \begin{pmatrix} -\varepsilon_h/2 & t_1 & t_2 \\ t_1 & -\varepsilon_h/2 & 0 \\ t_2 & 0 & -\varepsilon_h/2 + E_R \end{pmatrix}.$$

Here,  $t_1$  and  $t_2$  are the tunnel couplings between  $|0\rangle$  and  $|1\rangle$ ,  $|1\rangle$  and  $|L\rangle$ , respectively, and  $\varepsilon_h$  is the detuning between charge states (2, 1) and (1, 2), while  $E_R$  is the energy separation between the two lowest valley-orbit states in the right dot. The energy-level spectrum can be divided into three regions: charge-like region (blue), hybrid region (gray) and spin-like region (green). In the spin-like region,  $E_R$  is just the splitting energy of  $|0\rangle$  and  $|1\rangle$ . The charge-like region can be used for readout using spin blockade with  $|S\rangle_R$  mapped to  $|0\rangle$  and  $|T_0\rangle_R$  as well as  $|T_-\rangle_R$  mapped to  $|1\rangle$ . In the readout regime, spin blockade will permit the transition between (1, 2) and (2, 1) for  $|S\rangle_R$  and prohibit it for  $|T_0\rangle_R$  and  $|T_-\rangle_R$ . Therefore,  $|0\rangle$  and  $|1\rangle$  can be distinguished from the charge occupation after the conversion. For qubit control, as shown by the pulses labeled (I)–(IV) in Fig. 22g, it can be performed either in the hybrid region by Larmor precession or in the spin-like region by Rabi oscillation. In the Larmor precession regime, a control pulse stops at  $\varepsilon_h = 0$  and  $\varepsilon_h > 0$  will rotate the qubit about the  $x$  and  $z$  axes, respectively. To make further progress, the detuning point for control should be more positive into the spin-like region with longer coherent times and thus Rabi oscillation is preferable. The approach for Rabi oscillations is to set the qubit in the spin-like region and apply MW bursts to rotate it around the  $x$  axis and vary the relative phase of successive MW bursts to rotate it around the  $z$  axis. An example of the Rabi oscillations is shown in Fig. 22h. The increased number of electrons allows the mixture of charge and spin degrees to be tuned freely such that the energy levels can be encoded like in a Si/SiGe DQD. Later, it was extended the hybrid qubit into a TQD. With an extra quantum dot for energy-level tuning, they realized a tunable operation frequency from 2 to 15 GHz, allowing a large range for frequency multiplexing. In fact, the valley splitting in Si/SiGe quantum dots is not so controllable and varies from sample to sample. These new types of hybrid qubits are free of valley states and thus are more reproducible and scalable.

## Two-qubit gate in semiconductor

In contrast to single-qubit gates, which all require two-axis control, the two-qubit gate can be realized in many different ways. In fact, the CNOT gate is not the only two-qubit gate for universal quantum computing. Others include the square root of the SWAP gate ( $\sqrt{\text{SWAP}}$ ) and the controlled phase gate (CZ). The SWAP gate swaps the two-qubit state and the  $\sqrt{\text{SWAP}}$  gate performs half the way of such SWAP. The CZ gate acts on two qubits in such a way that a  $\pi$  rotation around the  $z$  axis is performed on the target qubit only when the control qubit state is  $|1\rangle$ . In the semiconductor quantum devices, these different two-qubit gates can also be divided into three different categories considering the source of interaction: exchange interaction, Coulomb interaction and circuit quantum electrodynamics (cQED). In the following subsections, we will introduce the realization of two-qubit gates using different types of interactions and discuss the progress.

**Exchange interaction.** Exchange interaction is a quantum mechanical effect for identical particles. In this context, it refers to the interaction between two spins. Two-qubit gates using exchange interaction have been proposed for spin-1/2 qubits, singlet–triplet qubits, exchange-only qubits and hybrid qubits. Among these, the exchange interaction between spin-1/2 qubits have been investigated most thoroughly in experiments and thus we mainly discuss it in the following. The interaction strength  $J$  and Zeeman energy difference  $\Delta E_z$  are two competing factors in controlling two interacting spins, and their relative magnitude determines the energy levels of the system.



Figure 23a depicts the energy-level spectrum in four different cases: (I) When both  $\Delta E_z$  and  $J$  equal zero, the qubit eigenstates are directly product states and all single spin-flip transitions are energetically degenerate. (II) If only  $\Delta E_z$  is non-zero, two spins can be addressed at different transition frequencies and single spin qubit control can be achieved. (III) If  $\Delta E_z$  and  $J$  are non-zero and  $J$  is much bigger than  $\Delta E_z$ , the two-qubit eigenstates are no longer effectively product states but singlet and triplets. This is just like the case of singlet–triplet qubits, and a  $\sqrt{\text{SWAP}}$  gate can be implemented with a  $\pi/2$  rotation around the  $z$  axis. (IV) If  $\Delta E_z$  and  $J(\varepsilon_s)$  are non-zero and  $J$  is much smaller than  $\Delta E_z$ , the qubit eigenstates can still be viewed as product states with small corrections due to spin–charge hybridization.

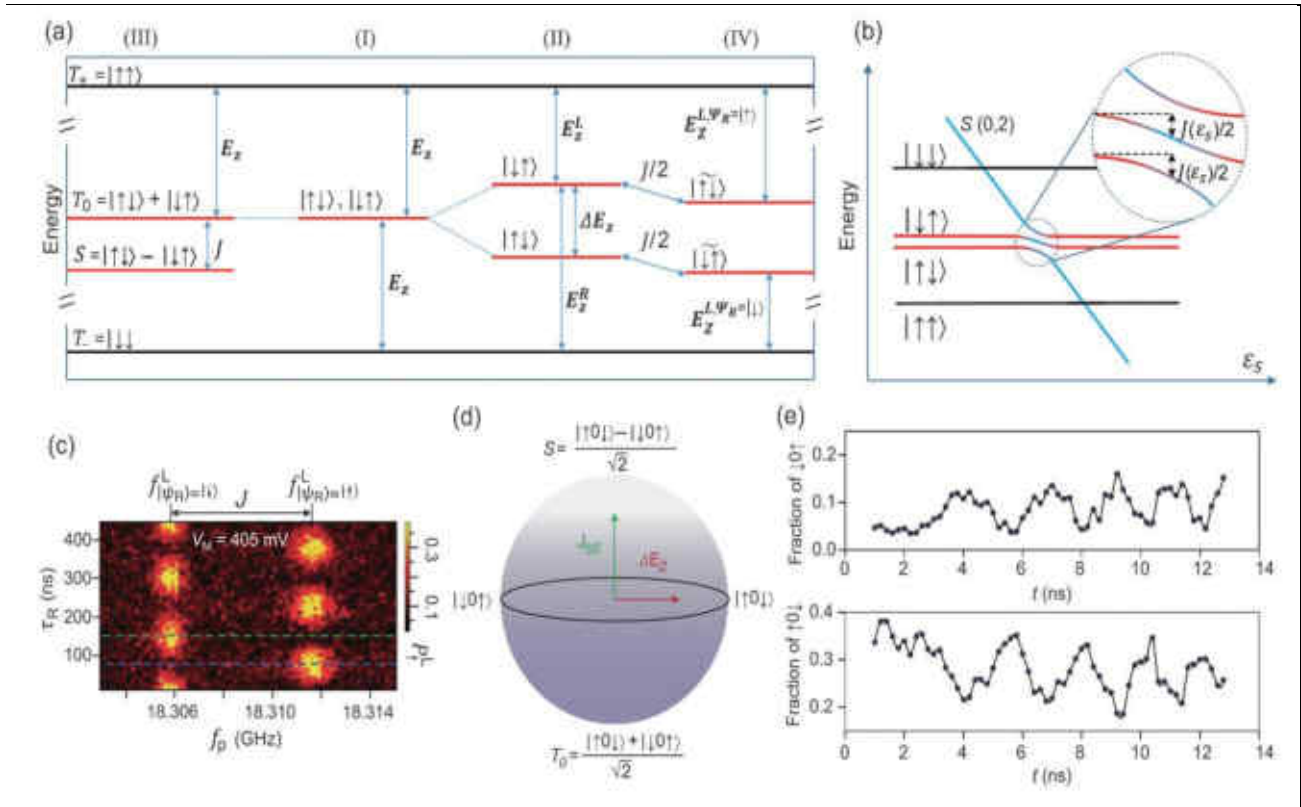


Fig. 23. Two-qubit gates based on exchange interaction. (a) Eigenenergies of two spins in a DQD in the presence of a magnetic field gradient  $\Delta E_z$  and relevant transitions between them for four distinct realistic parameter regimes: (I) both  $\Delta E_z$  and  $J$  equal zero; (II) only  $\Delta E_z$  is non-zero; (III) both  $\Delta E_z$  and  $J$  are non-zero and  $J$  is much bigger than  $\Delta E_z$ ; and (IV) both  $\Delta E_z$  and  $J$  are non-zero and  $J$  is much smaller than  $\Delta E_z$ . (b) Energy levels of two spin states as a function of detuning  $\varepsilon_s$  in condition (IV). The energy shift  $J(\varepsilon_s)/2$  of the antiparallel-spin states is denoted in the enlarged dotted circle. (c) The probability of spin-up states for the left qubit  $P_{\uparrow}^L$  as a function of the MW burst time  $\tau_R$  and MW frequency  $f_p$ . The MW bursts are applied on the right qubit. Two resonance frequencies of the left qubit are split by  $J$ . (Adapted from [7].) (d) Bloch-sphere representation of the singlet–triplet subspace in the superexchange regime with control axes  $J_{SE}$  and  $\Delta E_z$ . (Adapted from [7].) (e) Observation of superexchange-driven spin oscillations.

(Adapted from [7])

In this regime, each qubit transition frequency is no longer independent of the state of the other and thus permits CZ or CNOT operations.

For the  $\sqrt{\text{SWAP}}$  gate, it was first demonstrated by Petta *et al.* using GaAs quantum dots in 2005, reporting an operation on input state  $|\uparrow\downarrow\rangle$  or  $|\downarrow\uparrow\rangle$  with a time of 180 ps. However, limited by the measurement method, they could not perform the  $\sqrt{\text{SWAP}}$  gate for other input states like  $|\uparrow\uparrow\rangle$  or  $|\downarrow\downarrow\rangle$ . In 2011, Nowack *et al.* first demonstrated independent single-shot readout of two electron spins using energy-selective readout, and upon this result they measured the full truth table for a SWAP gate with four different input states. In the same year, Brunner *et al.* combined the SWAP<sup>*n*</sup> gate (*n* means multiples of the operation time of a SWAP gate) with single-qubit rotations and demonstrated two-qubit entanglement. For the CZ gate in semiconductor the energy levels as functions of detuning  $\varepsilon_s$  are shown in Fig. 23b; a vanishing detuning lowers the antiparallel-spin states with  $J(\varepsilon_s)/2$  and thus allows a phase shift of  $J(\varepsilon_s)t_{\text{wait}}/2$  when applying a detuning pulse for a fixed time  $t_{\text{wait}}$ , resulting in a unitary transformation in the basis of  $|\uparrow\uparrow\rangle, |\uparrow\downarrow\rangle, |\downarrow\uparrow\rangle$  and  $|\downarrow\downarrow\rangle$ :

$$U_{\text{c phase}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & e^{if(\varepsilon_i)t_{\text{wait}}/2} & 0 & 0 \\ 0 & 0 & e^{if(\varepsilon_i)t_{\text{wait}}/2} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

when  $t_{\text{wait}}$  equals  $\pi/J(\varepsilon_s)$ , this gate control corresponds to a CZ gate only with additional single-qubit *z* rotations.

In 2018, Watson *et al.* used dynamical decoupling pulses to improve the performance of CZ gates and performed the Deutsch–Josza algorithm and the Grover search algorithm with a natural Si/SiGe DQD, suggesting the first implementation of a programmable two-qubit quantum processor. The Bell-state tomography, which is a characterization of the two-qubit gate performance, indicated prepared state fidelities of 85–89%. Considering the state preparation and measurement (SPAM) errors brought about by the Bell-state tomography, they then used character randomized benchmarking to study the CZ gate control fidelity and obtained a value of ~91%.

For the CNOT gate, it can be realized by directly driving the qubits via MW bursts for a time when *J* is non-zero. As Fig. 22a suggests, MW bursts with a frequency resonant with the transition of  $|\uparrow\downarrow\rangle$  to  $|\uparrow\uparrow\rangle$  and off-resonant with other transitions can cause the left qubit to rotate only when the right qubit state is  $|\uparrow\rangle$ . As a result, the rotation of the left qubit is controlled by the right qubit state, and it corresponds to a CNOT gate when the controlled rotation angle equals  $\pi$ , as illustrated in Fig. 22b. Actually, the CNOT gate here has to be calibrated to eliminate the conditional phase caused by exchange interaction, and usually we call it a conditional rotation (CROT) gate. The device is shown in Fig. 22c, and they used the middle gate M to directly control the inter-dot tunneling and thereby the exchange interaction. When the interaction is turned on, the resonance frequency of the left qubit is dependent on the right qubit state. As illustrated in Fig. 22c, the response of the left qubit to MW bursts oscillates between two frequencies as the right qubit is under Rabi oscillation, and the two state-dependent resonance frequencies are separated by *J*. On top of that, the CROT gate can also be implemented with a constant *J*. With this new approach, in 2018, Huang *et al.* set up a new record with fidelity up to 98% via two-qubit randomized benchmarking based on a purified silicon MOS DQD.

**Coulomb interaction.** A typical device and a schematic of the charge configurations of *S* and *T*<sub>0</sub> are shown in Fig. 24a and b, respectively.

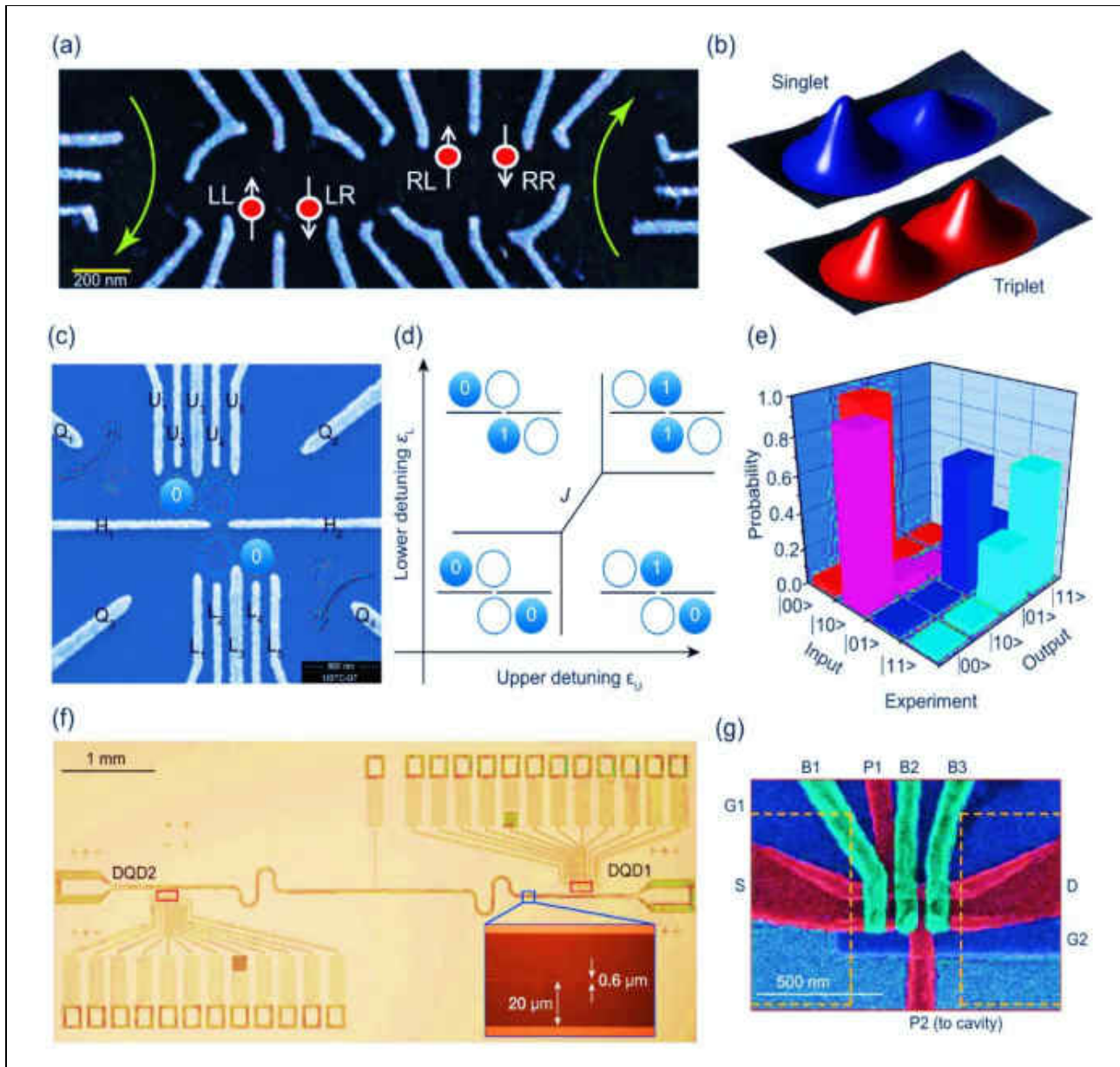


Fig. 24. Two-qubit gates based on Coulomb interaction and circuit quantum electrodynamics (cQED) with a DQD. (a) SEM image of a device for entangling two singlet–triplet qubits. The approximate locations of the electrons in the two qubits are denoted by red circles with arrows. The current paths for the SETs are denoted by green arrows. (Adapted from [8].) (b) Schematic of the charge configuration for singlet (blue) and triplet (red). (Adapted from [8].) (c) SEM image of a device for coupling two charge qubits. The solid blue circles denote the charge configuration for the corresponding state and two current paths for QPCs are denoted by blue arrows. (Adapted from [9].) (d) Diagram showing Coulomb-interaction-induced  $J$  as a function of detuning for the upper DQD  $\epsilon_U$  and lower DQD  $\epsilon_L$ . (Adapted from [120].) (e) Probabilities for the output states of a CROT operation acquired experimentally by preparing qubits in different input states  $|00\rangle, |01\rangle, |10\rangle$  and  $|11\rangle$ . (Adapted from [9].) (f) Optical image of the superconducting resonator coupling two DQDs. The inset shows an optical image of the center pin and vacuum gap. (Adapted from [9].) (g) False-color SEM image of a DQD with gate P2 coupled to the resonator. The micro-magnets for spin–photon coupling are indicated by orange dashed lines. (Adapted from [9])

Coulomb interaction is the electrostatic coupling between two or more electrons. The two-qubit gate based on Coulomb interaction has been pro-posed for singlet–triplet qubits, exchange-only qubits, hybrid qubits and charge qubits. So far, both experiments on singlet– triplet qubits and charge qubits have been demonstrated. For singlet–triplet qubits, the two-qubit gate was first experimentally investigated by Weperen *et al.* in 2011 using two electrostatically coupled DQDs. They found that the precession frequency of the singlet–triplet qubit

can be controlled by the charge arrangement of an electrostatically coupled DQD. Then, in 2012, Shulman *et al.* utilized the different charge occupations of  $S$  and  $T_0$  to control the precession frequency of another qubit. The level structure of the interacting two-qubit system was probed and correlated oscillations were observed. In 2015, on the basis of these results, Li *et al.* demonstrated a CROT gate of two strongly coupled charge qubits typical device is depicted in Fig. 24c, showing two electrostatically coupled GaAs DQDs. Charge qubits are formed in each DQD and can be controlled independently by detuning. Figure 24d shows the inter-action between two charge qubits when controlling the detuning. The zero-detuning point for the upper qubit, i.e. the anti-crossing point for the qubit to change from  $|0\rangle$  to  $|1\rangle$ , will shift to a higher point by an amount  $J_{12}$  when the lower qubit state is changed from  $|0\rangle$  to  $|1\rangle$ . Here we denote the lower point as  $\mathcal{E}_U^{\Psi_L=|0\rangle}$  and the higher point  $\mathcal{E}_U^{\Psi_L=|1\rangle}$ . A CNOT gate can thus be applied by pulsing the upper qubit to  $\mathcal{E}_U^{\Psi_L=|0\rangle}$  so that the upper qubit will be rotated only if the lower qubit state is  $|0\rangle$ . In this way, they measured the truth table (see Fig. 5e) of a CROT gate and extracted a control fidelity of  $\sim 68\%$ .

To take a step further, in 2018, Li *et al.* demonstrated three-qubit controlled rotations using three coupled GaAs DQDs, which is a first attempt to go beyond the two-qubit limit in semiconductor devices and suggests that semiconductor qubits are amenable to large-scale manufacture.

**Readout of qubits.** The readout method of most types of semiconductor qubits depends on a proximate charge sensor. Once the charge state of the quantum dot or a donor changes, the resistance of the charge sensor will change accordingly. There-fore, the readout speed and fidelity are directly related to the bandwidth and signal-to-noise-ratio (SNR) of the charge sensor. To include both the bandwidth and SNR, in the following we use the charge sensitivity to characterize the performance of a readout method: Charge sensitivity =  $1 / ((\text{SNR}) \cdot \sqrt{\text{Bandwidth}}) (e / \sqrt{\text{Hz}})$ . A typical state-of-the-art charge sensor with a transconductance amplifier at room temperature (RT) can achieve a charge sensitivity down to  $820 \mu e / \sqrt{\text{Hz}}$  for a 30 kHz bandwidth. To improve its performance, several approaches have been investigated.

The first approach is to couple an impedance-matching radio frequency (rf) resonant circuit to the integrated charge sensor, usually a SET or a QPC, to form an rf-SET or an rf-QPC. Its operating principle is to detect the modulation of the reflected or transmitted rf signal by resistance change of the charge sensor. The impedance-matching network lowers the high resistance of the charge sensor, usually  $> 50 \text{ k}\Omega$ , towards the characteristic impedance of a transmission line  $\sim 50 \text{ k}\Omega$ .

Thus, the RC time constant of the circuit is reduced and thereby the working bandwidth is improved. The first demonstration of using an rf-SET to detect charge states in semiconductor was in 2003, when Lu *et al.* fabricated an aluminum rf-SET to detect real-time electron tunneling in a GaAs quantum dot. In 2007, Reilly *et al.* and Cassidy *et al.* reported the characterization of rf-QPCs fabricated using the GaAs/AlGaAs hetero-structure. Both the rf-SET and the rf-QPC can offer a charge sensitivity lower than  $200 \mu e / \sqrt{\text{Hz}}$  with a bandwidth over 1 MHz. For the applications in qubit readout, in 2009, Barthel *et al.* used an rf-QPC to detect a singlet-triplet qubit and reported a single-shot measurement with fidelity over 90% for a bandwidth  $\sim 143 \text{ kHz}$ . The rf-QPC that they used is depicted in Fig. 24a, with an ohmic contact (box) coupled to an impedance-matching network formed by an inductor and a parasitic capacitance of the bond pads and wires. In 2010, by using a GaAs quantum-dot-based rf-SET, they even improved the measurement bandwidth to 10 MHz for the read-out of a singlet-triplet qubit. Beyond that, this technique also applies to other types of qubits such as charge qubits, spin-1/2 qubits and exchange-only qubits.

The second approach is to use cryo-amplifiers. For conventional measurement methods, the readout bandwidth is also limited by the transconductance amplifier at room temperature (RT). When the readout bandwidth is increased, the RT amplifier gain will decrease and so does the SNR. In fact, the SNR can still be increased if the amplification is introduced at a lower temperature before the dominant noise comes in. Inspired by this idea, several attempts have been made to fabricate a suitable cryo-amplifier located much closer to the device, including employing a high-electron-mobility transistor (HEMT) and a SiGe heterojunction bipolar transistor (HBT). In 2016, Tracy *et al.* demonstrated the single-shot readout of a P-donor-electron spin-1/2 qubit with 96% visibility of Rabi oscillations by using a cryogenic two-stage HEMT circuit adjacent to the qubit device, as shown in Fig. 25b.



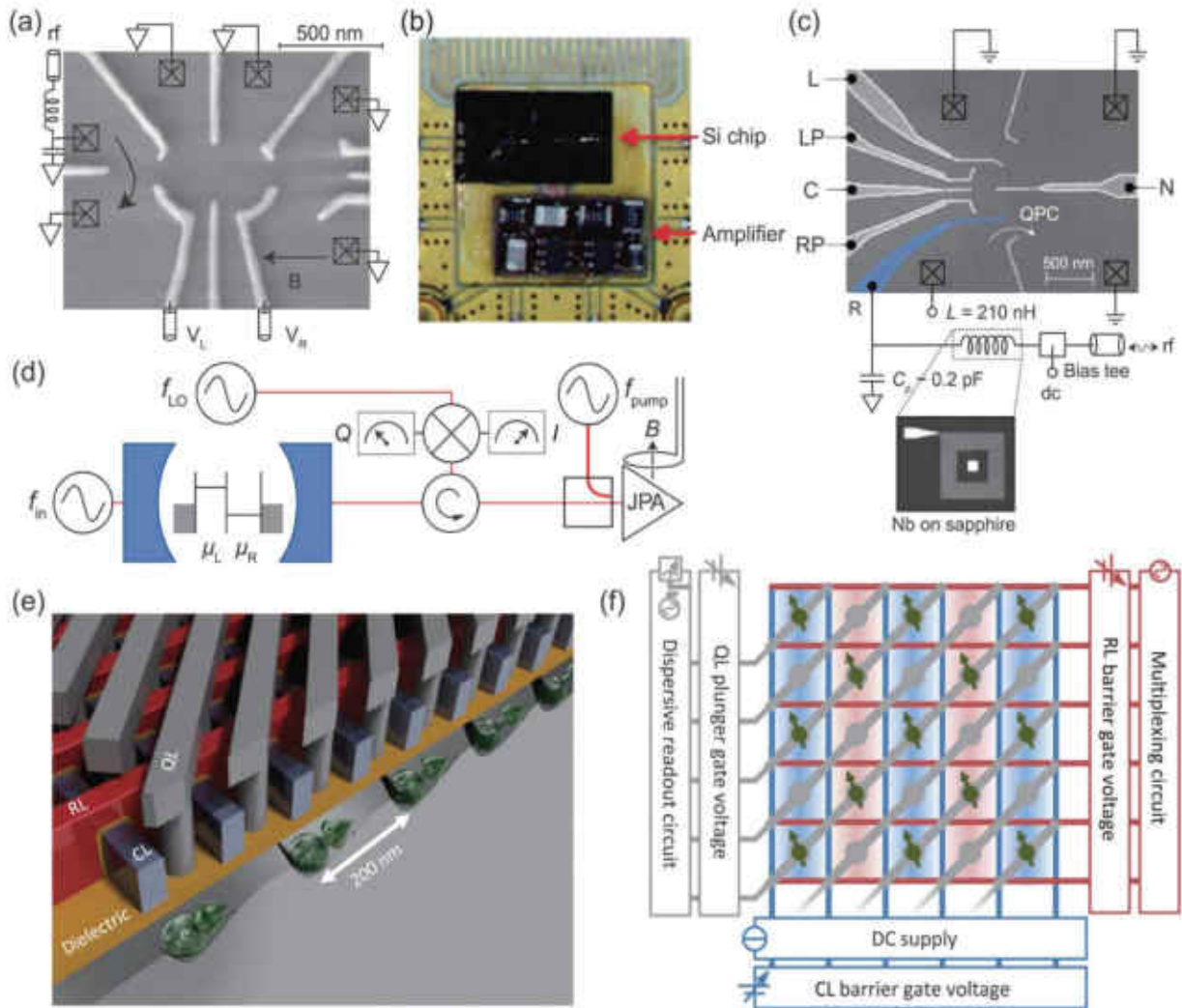


Fig. 25. Approaches to improve readout quality and a crossbar network for large-scale integration. (a) SEM image of a device using an rf-QPC, indicating ohmic contacts (boxes), fast gate lines, impedance-matching circuit, grounded contacts, and the external magnetic field direction. (Adapted from [8].) (b) Picture of a silicon device with an adjacent cryogenic amplifier circuit mounted on printed circuit board. (Adapted from [8].) (c) False-color SEM image of a device using an rf gate sensor. One electrode (blue) is coupled directly via a bond wire to an off-chip Nb/Al<sub>2</sub>O<sub>3</sub> superconducting lumped-element resonator. (Adapted from [9].) (d) Diagram of the device using a distributed superconducting resonator with the input field  $f_{in}$ . The output field is sent to a JPA through a circulator and then demodulated into the  $I$  and  $Q$  quadratures with a local oscillator tone  $f_{LO}$ . A directional coupler is used to couple the pump field at frequency  $f_{pump}$  (Adapted from [8].) (e) and (f) are a 3D model and schematic representation of the crossbar network for a 2D quantum-dot array. CLs (blue), RLs (red), and QLs (gray) connect the qubit grid to outside electronics for control and readout [9]

For a bandwidth of 100 kHz, they achieved an SNR of 9 and a charge sensitivity of  $300 \mu e/\sqrt{\text{Hz}}$ , nearly twice as good as the values of the state-of-the-art charge sensor with an RT amplifier.

Unlike the approaches mentioned above, the third approach gets rid of a charge sensor by coupling the surface electrode of a DQD directly to a resonator. For experiments, in 2010, Petersson *et al.* first demonstrated a lumped-element resonator circuit coupled to the reservoir of a DQD in GaAs and used it to probe charge and spin states. Then, in 2013, Colless *et al.* coupled the lumped-element resonator to a gate electrode of a DQD and named it an  $r_f$  gate sensor. An  $r_f$  gate sensor is shown in Fig. 25c, with a lumped-element resonator constituted by an inductor  $L \sim 210 \text{ nH}$  and a parasitic capacitance  $C_p \sim 0.2 \text{ pF}$ . In 2015, Gonzalez-Zalba *et al.* demonstrated a record sensitivity of  $37 \mu e/\sqrt{\text{Hz}}$  for a bandwidth  $\sim 1 \text{ kHz}$  with a gate sensor for silicon SOI

quantum dots. This value was further improved to  $1.3\mu\text{e}/\sqrt{\text{Hz}}$  in 2018 for a band-width of  $\sim 10$  Hz. Single-shot readout of singlet–triplet qubits using rf-gate sensors was realized by Pakkiam *et al.*, Urdampilleta *et al.* and West *et al.* in 2018 with donors in silicon, a silicon MOS DQD and a silicon SOI DQD, respectively. Among them, the best reported readout fidelity is 99.7% for a 1 kHz bandwidth. In 2015, Stehlik *et al.* added a Josephson para-metric amplifier (JPA) at the output of the resonator to amplify the signal, as shown in Fig. 24d, resulting in a charge sensitivity of  $80\mu\text{e}/\sqrt{\text{Hz}}$  for a bandwidth of 2.6 MHz. Later, Mi *et al.* replaced the JPA for a traveling-wave parametric amplifier (TWPA) and demonstrated strong coupling of the DQD to a resonator. With the help of a slanting magnetic field generated by a micro-magnet, in 2018, they further demonstrated strong spin–photon coupling and performed dispersive readout of a spin-1/2 qubit. For charge qubits, in 2017, Scarlino *et al.* demonstrated dispersive readout of a charge qubit and measured an intrinsic dephasing time  $T_2$  up to  $(43.1\pm 4.3)$  ns. Furthermore, coupling to resonators not only requires no charge sensor, but also allows frequency multiplexing. Since 2014, the proposals of multiplexing readout of spin and charge qubits have been demonstrated for larger-scale applications.

**Scalable design.** Now that high-fidelity control and readout of single-and two-qubit gates in semiconductor have been demonstrated, the next challenge lies in how to scale them to tens and hundreds of qubits. The corresponding constraints and problems have been investigated thoroughly since 2015, including the geometry and operation time constraints, engineering configuration for the quantum–classical interface, and even the quantifying of system extensibility. In the light of these discussions, several proposals for scaling up have been proposed, varying from the crossbar network for spin-1/2 qubits in silicon MOS quantum dots, the 2D lattice of donor qubits in silicon, to hybrid architecture like donor–dot structure and flip-flop qubit structure.

In these proposals, the key issue is the wiring strategy of readout lines and control lines for single-and two-qubit gates as well as the balance between feasibility and high-quality performance. Here, we take the crossbar network of silicon spin-1/2 qubits as an example to illustrate these considerations. In Li *et al.*'s work, as Fig. 25e and f shows, three successive layers that play the roles of column barrier lines (CL), row barrier lines (RL), and diagonal plunger lines (PL) form a 2D array. Successively tuning CLs, RLs and PLs, electrons can be loaded from reservoirs at the array boundary into the qubit array for single-electron occupation. Moreover, the CLs also carry direct currents to generate a magnetic field gradient  $\Delta E_z$  for adjacent columns, while the QLs are connected to a dispersive readout circuit to play the role of gate sensors. To perform single-qubit rotations, global superconducting strip lines above the chip are used to provide in-plane oscillating magnetic fields. A  $\sqrt{\text{SWAP}}$  gate can be performed by two spins in the adjacent rows of the same column without  $\Delta E_z$ , while the spin–charge conversion relies on the two spins in the adjacent columns of the same row with  $\Delta E_z$ , which can constitute a spin-blockade regime with QLs to probe the tunneling event. Qubits can be moved freely along the rows and columns of the grid to perform a two-qubit gate or readout with the help of spin shuttling. Also, the spin shuttling can be used to add a controllable phase for a single qubit, thus a rotation around the  $z$  axis is achieved without extra control. However, obviously, the local control of one location may cause unwanted side effects in another location owing to the shared control property of these lines. Another previous design that connects every quantum dot in the grid directly via floating gates and vertical transistors can alleviate this problem. However, as a trade-off, the mediating floating gates and vertical transistors require more extensive manufacturing developments.

More than that, there is still a gap between the proposed architectures and the reproducible quantum dots in current experiments. For example, the proposed dot tuning and charge sensing in a 2D grid have not been demonstrated simultaneously in experiments. For future advances, more experiments are needed to fill the gap. **Example: CMOS Position-Based Charge Qubits.** The key building block of the semiconductor charge qubit can be realized in CMOS fully depleted silicon-on-insulator (FDSOI) technology and is shown in Figs. 26(a) and 26(b).

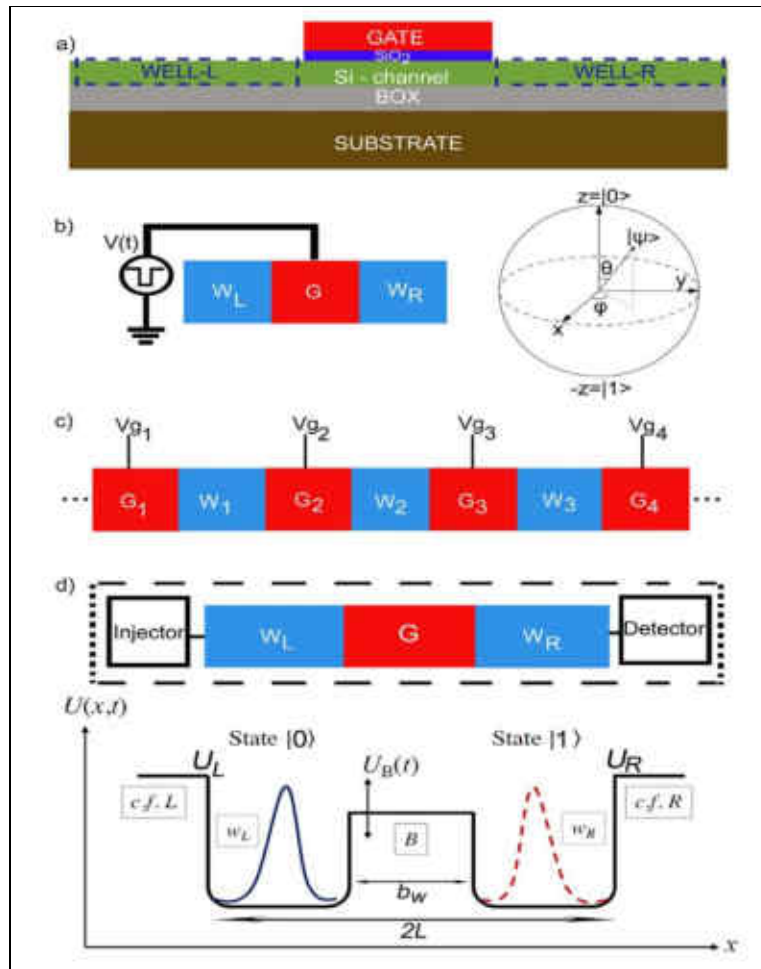


Fig. 26. (a) A representative example of a CMOS transistor-like silicon-on-insulator device that serves as a coupled quantum dot system. (b) Charge qubit formed by two coupled quantum dots (QD). (c) QDs in series forming a quantum register. (d) Block diagram of the system showing an injector and a detector. The injection of an electron is performed through an injector on the left quantum dot of the register whilst the readout is carried out on the right quantum dot by using a single-electron detector. The double-QD (DQD) system forms a charge qubit. [The potential function  $U(x, t)$  appearing in the Hamiltonian of the system is controlled by the voltages applied at the terminals of the structure, with the barrier  $U_B(t)$  varying in time in the most general case. When in a coherent state, an electron injected into such a system can tunnel quantum mechanically through the barrier between the two quantum dots. The electron exists in a superposition of left and right quantum dot states described by its wavefunction. Measurement of the electron position causes wavefunction collapse (it is a destructive/projective measurement); the electron is found to be in either the left or right quantum dot with probabilities related to the wavefunction density (repeated independent measurements yield the left and right position probabilities)]

It resembles a transistor and comprises two depleted silicon dots separated by a silicon channel, which acts as a tunneling barrier whose potential energy is controlled electrostatically by the gate. Each dot acts as a single quantum dot (QD). When the barrier separating the QDs is very high, quantum mechanical tunneling is exponentially suppressed and the QDs are effectively decoupled. A single electron injected into the system is then trapped in either left or right dot and the quantum state has a very long lifetime. By lowering the barrier, a single electron can tunnel between the left and right dots in the double QD (DQD) device. The potential barrier  $U_B(t)$  between the two dots, controlled by the voltage applied at the gate of the device, can vary with time in the most general case, and hence allows control over the electronic tunneling in the DQD (see Fig. 26(d)). To complete the structure, one adds an injector (a device which is able to inject a single electron into one quantum dot) and a detector (a device which is able to detect an electron at the same or the other quantum dot). This geometry allows one to define a charge qubit. It is assumed that the state of the qubit, as a closed system, can be expressed as a superposition of eigenstates. When coupled to other similar QDs in a chain, as shown in Fig. 26(c), the dynamics of an injected electron can be manipulated on a larger scale. Such an array of QDs is similar to a charge-coupled device (CCD) and allows formation of a quantum register.



Since the QDs are physical quantum dots with spatial extent along the lateral  $x$ -axis as shown in Fig. 26(d), the states  $|0\rangle$  and  $|1\rangle$  are associated with time-independent wavefunctions  $|\phi_L(x)\rangle$  and  $|\phi_R(x)\rangle$ , defined such that  $|\phi_L(x)\rangle$  maximizes the electronic occupancy of the left quantum dot and  $|\phi_R(x)\rangle$  maximizes the electronic occupancy of the right quantum dot. To faithfully model the physical DQD device, the quantum dots do not have infinite potential walls. Although the probability of locating the electron in either quantum dot is relatively high, there is a finite probability that the electron can exist in classically forbidden regions, such as in the barrier region between the quantum dots, or outside of the device entirely, leading to a loss of quantum information from the system. This motivates us to construct the basis  $|\phi\rangle$  that minimizes any such non-ideality. A measure of the non-ideality (or residual error factor) is then  $\varepsilon = 1 - p_{w_L} - p_{w_R}$  and the probability of locating an electron in quantum dot  $\varsigma = L$  or  $R$  as  $p_{w_L}$  and  $p_{w_R}$ .

The localized-state basis of Wannier functions is defined such as to maximize the probability to locate an electron in the relevant quantum dot. For a DQD qubit comprising two quantum dots, one can straightforwardly determine the maximally localized basis functions, as shown in Fig. 27.

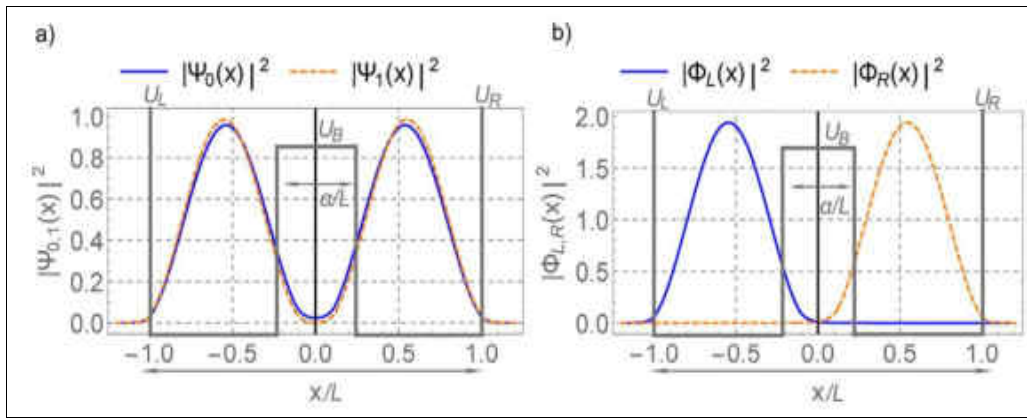


Fig. 27. Representation of qubit states in the proposed DQD device. (a) Probability density of and electron in eigenstates of the DQD device. (b) Corresponding maximally localized functions

Figure 26(a) shows the probability density for an electron in eigenstate  $|\psi_0\rangle$  or  $|\psi_1\rangle$  as a function of position along the  $x$ -axis, highlighting how the eigenbasis is typically delocalized over the entire device. By contrast, Fig. 27(b) shows the probability density for an electron in the maximally localized (Wannier) basis  $|\phi_L(x)\rangle$  or  $|\phi_R(x)\rangle$ , demonstrating suitability as a charge qubit basis. Note however that even in the maximally localized basis, there is appreciable tunneling amplitude inside the classically forbidden barrier region. The full control of the Bloch sphere requires one to be able to change both angles,  $\theta$  and  $\varphi$ . However, it is easy to see that an equilibrium system in the eigenfunction representation is characterised by a fixed angle  $\theta$  with the angle  $\varphi$  precessing at the frequency of occupancy oscillations.

The eigenfunction representation of the two-quantum dot system is shown in Fig. 28 (see the left column) where we show the effect of the potential function variation on the angle  $\theta$ .

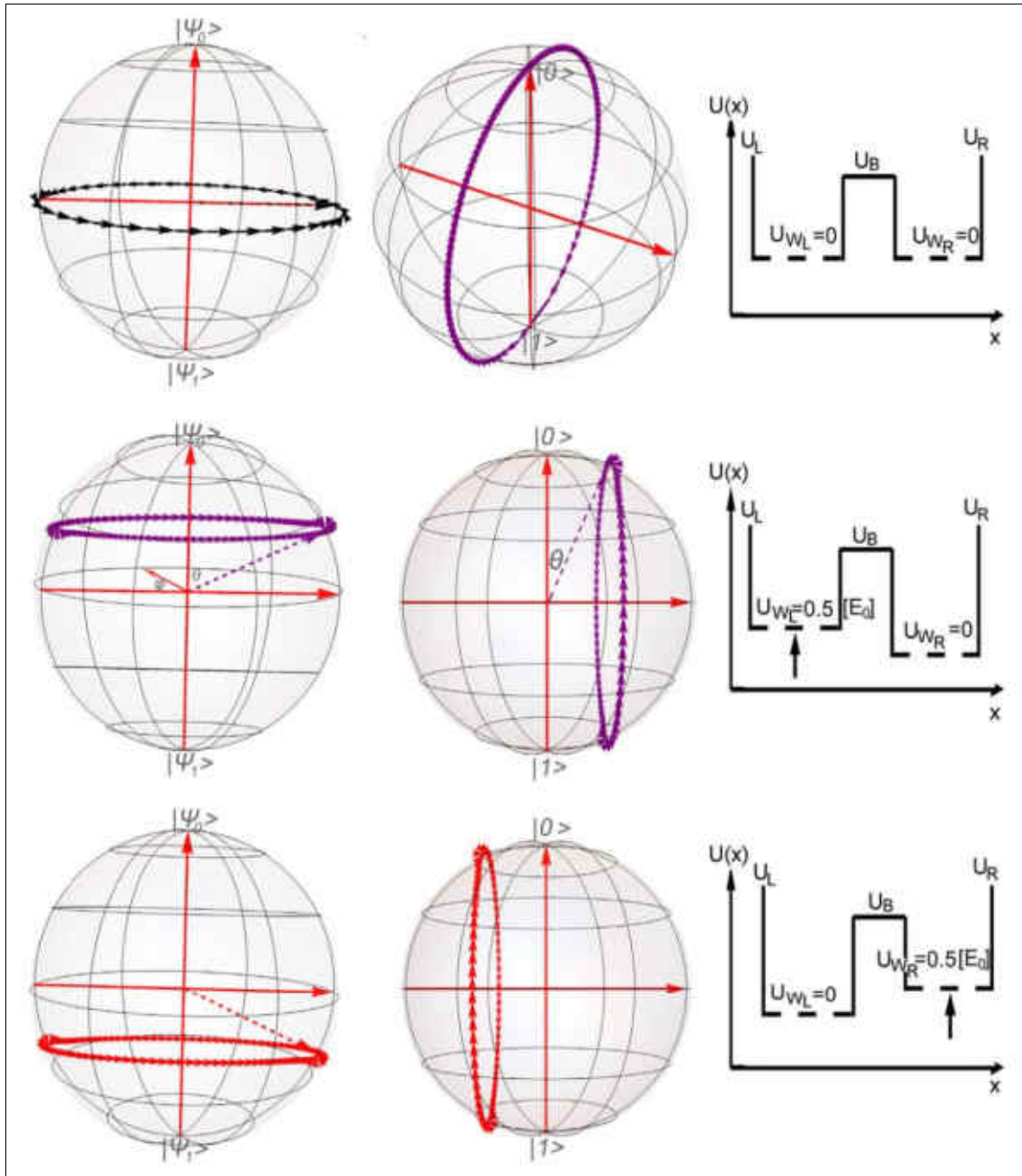


Fig. 28. Rotation of the angle  $\{|\psi_0\rangle, |\psi_1\rangle\}$  both in the eigenfunction basis and position basis  $\{|0\rangle, |1\rangle\}$

The state vector describing such a system precession with the frequency  $\delta\omega$  along the paths shown in those figures is defined by the height of the barriers separating the quantum dots.

In Fig. 29(a), the Von Neumann entanglement entropy  $S_N(t)$  is plotted between two single-electron registers interacting electrostatically via the Coulomb interaction. Each line consists of two DQs which correspond to two qubits, denoted as qubit #1 and qubit #2. Interestingly, it is visible that an almost maximally entangled state can be achieved in this case ( $\sim 2\ln 2$ ) for the selected parameters. In principle, the maximum entanglement is harder to achieve as the spatial degrees of freedom for each particle increases. Finally, the maximum entanglement entropy  $S_N$  as a function of the tunneling probability  $t_h$ , for a given time period  $t_{\max} = 10[\text{ns}]$ , is plotted in Fig. 29(b).

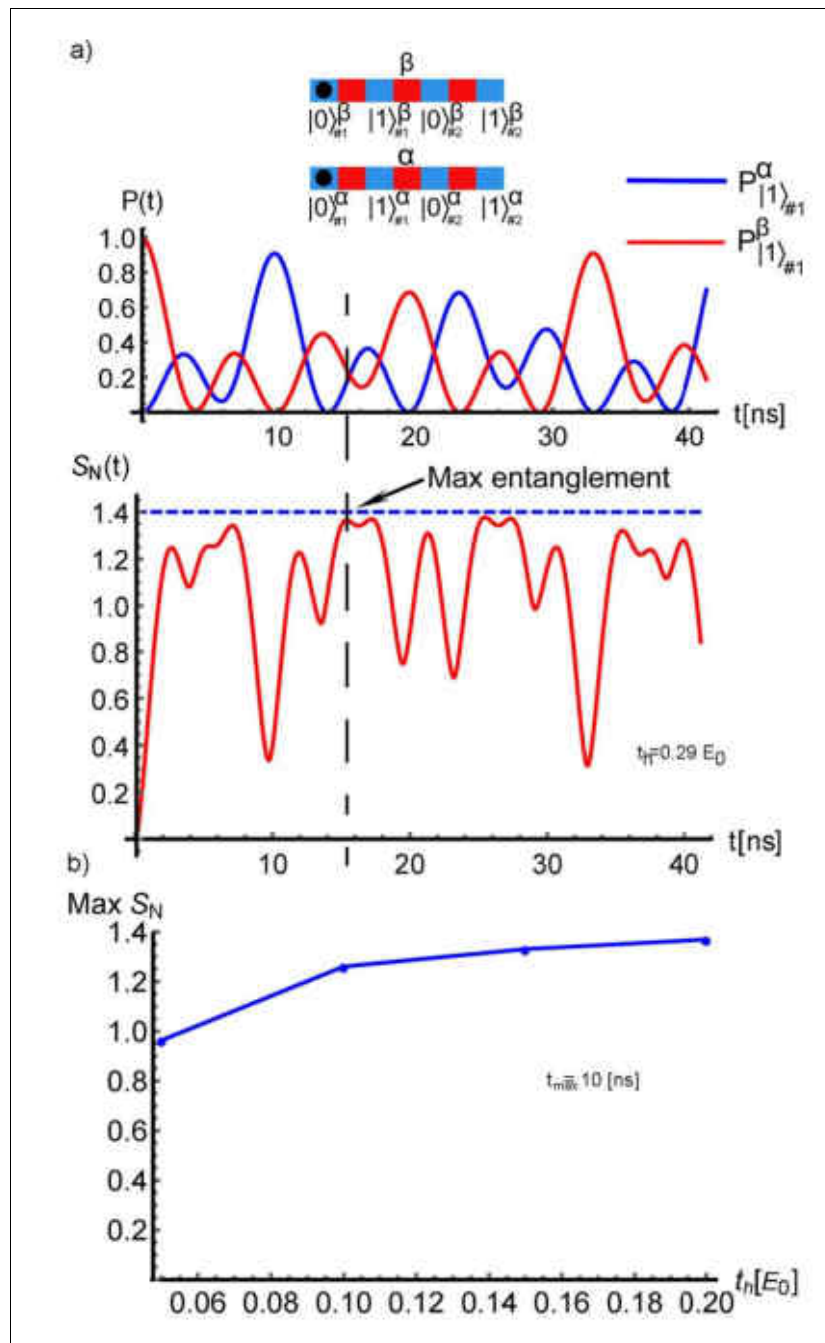


Fig. 29. (a) Von Neumann entanglement entropy  $S_N(t)$  between two single-electron registers interacting electrostatically via Coulomb interaction. Each line consists of two DQDs which corresponds to two qubits, denoted as qubit#1 and qubit#2; (b) Maximum entanglement  $S_N(t)$  as a function of the tunneling probability  $t_h$  in a given time duration,  $t_{max} = 10$  ns

As the tunneling probability  $t_h$  increases, the system can become maximally entangled.

This provides a formal definition, robustness analysis and discussion on the control of a charge qubit intended for semiconductor implementation in scalable CMOS quantum computers. The construction of the charge qubit requires maximally localized functions, and such functions for double quantum dot structures with dimensions corresponding to a 22-nm FDSOI CMOS technology. Then an individual qubit can be manipulated in terms of the two angles of the Bloch sphere.

**Silicon quantum circuits: CMOS-based cryogenic control.** A practical quantum computer comprises two main building blocks – a quantum processor with millions of qubits and classical instrumentation to generate control signals (input) and to process readout signals (output) [1]. A standard setup for semiconducting or superconducting qubits has the qubits operating in a dilution refrigerator at  $\sim 20$  mK, while bulky microwave

vector sources and arbitrary waveform generators are placed at room temperature and connected to the qubits via long cables and attenuators (Fig. 30a, left).

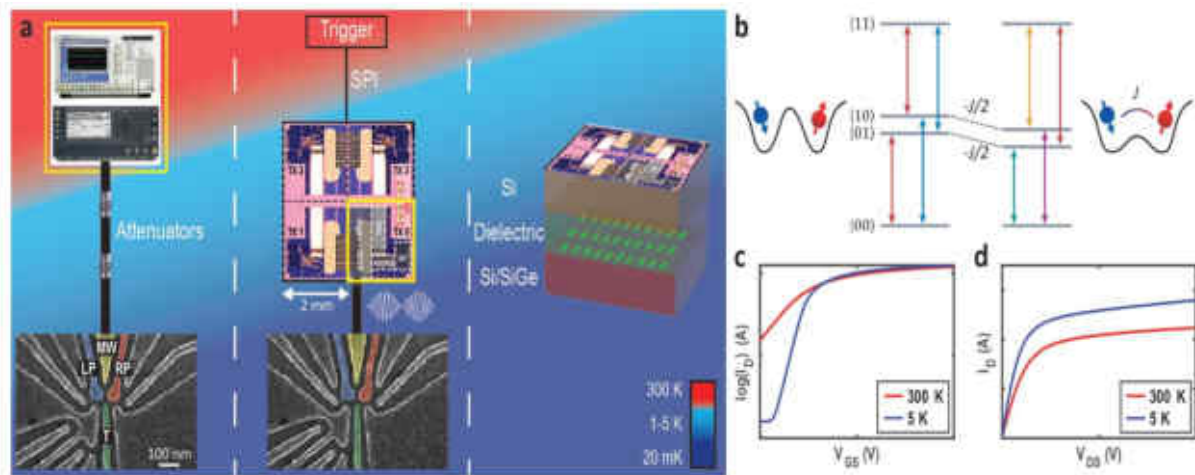


Fig. 30. The cryogenic quantum control system. *a*. Three stages of development of the control system towards full integration. *b*. Energy level diagram without (left) and with (right) exchange coupling ( $J$ ). The resonance frequency of each qubit depends on the other qubit only when the coupling is on (low tunnel barrier between the dots). *c*, *d*. FinFET NMOS device characteristics at room temperature versus 5 K: drain current ( $I_D$ ) versus gate-source voltage ( $V_{GS}$ ) at drain-source voltage  $V_{DS} = 1$  V (*c*) and  $I_D$  versus  $V_{DS}$  at  $V_{GS} = 0.4$  V (*d*). [From left to right: room temperature instruments connected to qubits via coax lines and attenuators; cryo-controller placed at 1-5 K directly connected to the qubits and triggered from room temperature using a serial peripheral interface (SPI); a future perspective of fully integrated control electronics and qubits on the same package/die. Two single electron spins used as qubits are located underneath gates LP (blue) and RP (red), as shown in the SEM image. Multiplexed microwave signals are sent to gate MW (yellow) to control both qubits. Gate T (green) is used to tune the coupling between the qubits]

This approach has recently enabled an experimental demonstration of the advantage of quantum computing over classical computing in a random circuit sampling experiment, that utilizes a superconducting quantum processor consisting of 53 qubits. This system requires more than 200 coaxial control lines from room temperature to the quantum chip operated below 20 mK. This brute-force approach to reach higher qubit numbers will soon hit its limits. A promising path forward is to bring the control electronics close to the quantum chip, at cryogenic temperatures. Here the challenge is that the power dissipation of the control electronics easily surpasses the typical cooling power of  $10 \mu\text{W}$  available at 20 mK. Silicon spin qubits are well-positioned for co-integration with dissipative classical electronics, since they can be operated above 1 K, where the cooling power is orders of magnitude higher (Fig. 30a, right). Therefore, an important next step is to design and implement a quantum control chip operating at 1-3 K, and to test its overall performance in driving real qubits. In order to benchmark the limits of the controller, it is advantageous to keep the qubits at  $\sim 20$  mK, where the qubits are most coherent and the demands on the controller are highest (Fig. 29a, middle). A cryogenic quantum controller for practical quantum information processing must meet multiple criteria: a form factor compatible with integration in a cryogenic refrigerator; frequency multiplexing to facilitate scalability; low power consumption within the limit of refrigerator cooling power; sufficiently high output power to enable fast operations compared to the qubit coherence times; high signal-to-noise ratio (SNR) and spurious-free-dynamic-range (SFDR) for high-fidelity control; the ability to generate complex pulse shapes and perform a universal set of quantum operations; an integrated instruction set memory for the efficient execution of complex algorithms. All these requirements can be met by commercial CMOS circuits designed to operate at a few K.

It utilized a quantum control chip operating at 3 K (cryo-controller, named Horse Ridge) and fabricated in Intel 22 nm-FinFET low-power CMOS technology to coherently control two electron spin qubits in a silicon double quantum dot cooled to  $\sim 20$  mK. Extensive electrical characterization and benchmarking using the quantum processor show that the cryo-controller meets all the above criteria.

Figure 31 shows the system-level architecture of the cryo-controller, which consists of a digital signal generation unit with an analog/RF front-end.



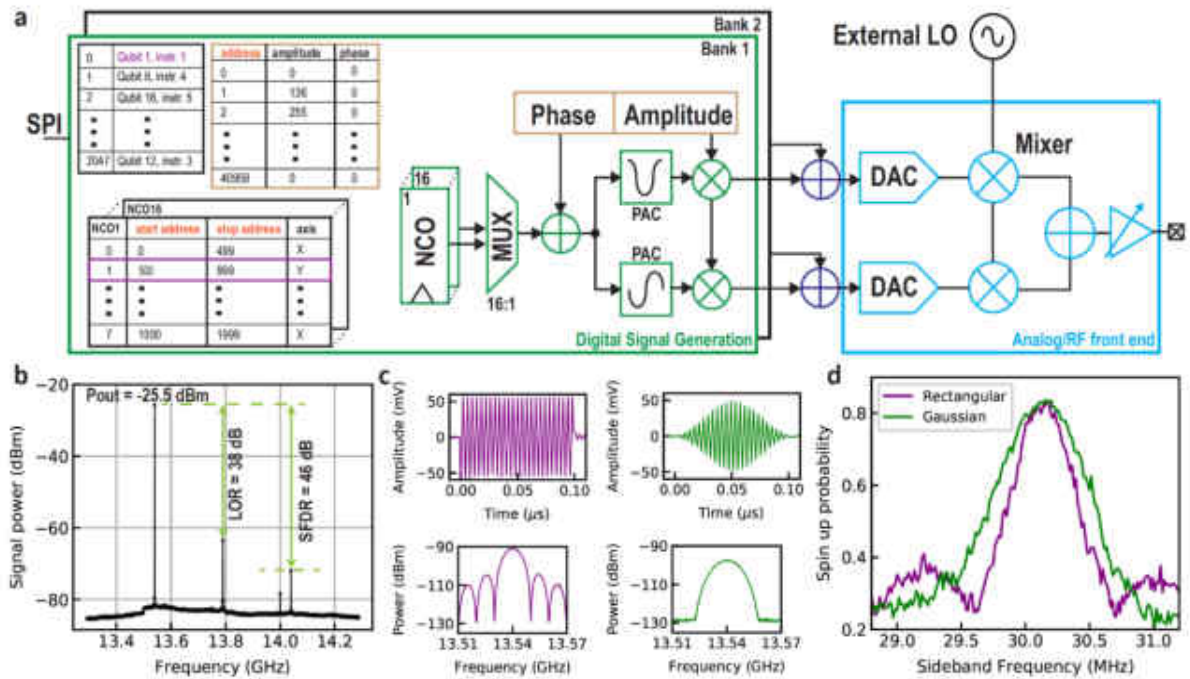


Fig. 31. The Horse Ridge cryogenic controller characterized at 3 K. *a.* System-level representation showing the digital signal generation and analog/RF front end of the cryo-controller, programmable via the SPI. *b.* Continuous-wave output spectrum from the cryo-controller at 13.54 GHz showing the main output tone, SFDR and LO rejection ratio (LOR). *c.* Rectangular (purple) and Gaussian (green) shaped bursts before up-conversion and the corresponding spectra after up-conversion. *d.* Qubit response for different burst envelopes, obtained when sweeping the NCO frequency around the qubit resonance across a span of ~3 MHz with a resolution of 15 kHz

At the core of the digital signal generation, a numerically controlled oscillator (NCO) outputs a sequence of bit strings every clock period. This bit string encodes a phase that is intended to track the reference phase of one particular qubit. The output of 16 NCOs is multiplexed and fed to a phase-to-amplitude converter (PAC) to generate a sinusoidal (in-phase) and cosinusoidal (quadrature-phase) signal. The NCO phases are constructed via a phase accumulator, which increments the phase in steps determined by a digital frequency tuning word (FTW). The 22-bit FTWs in combination with the 1 GHz clock frequency of the phase accumulator gives a frequency resolution of ~ 238 Hz.

**Test the functionality of the cryo-controller for controlling uncoupled qubits.** The LO frequency is set to 13:54 GHz.  $Q_1$  is then offset from the LO by 24 MHz and  $Q_2$  by - 90 MHz. The qubit resonances are found by sweeping one single-sideband tone generated by one NCO (Fig. 32a), using the 22-bit FTW.

Then one NCO used from each bank to generate two tones on resonance with the two qubits and drive simultaneous Rabi oscillations on both qubits (Fig. 32b). Here a 5 μs rectangular envelope is uploaded to the envelope memory, and saved as an instruction. The duration of the microwave burst is swept by updating the start or stop address of this instruction. The AIIXY and QST results indicate that the single-qubit gate set is well calibrated, offering a good starting point for bench-marking the gate fidelity. The cryo-controller allows for much more complex sequences, containing up to 2048 instructions for each of the four transmitters. Each instruction defines a microwave burst at one of 32 independent frequencies with an amplitude and phase profile that can be arbitrarily shaped. The cryo-controller can be conveniently embedded in existing micro-architectures and programmed via standard QASM variants. This quantum-classical architecture can thus be directly applied to multi-qubit algorithms and noisy intermediate-scale quantum devices [14].

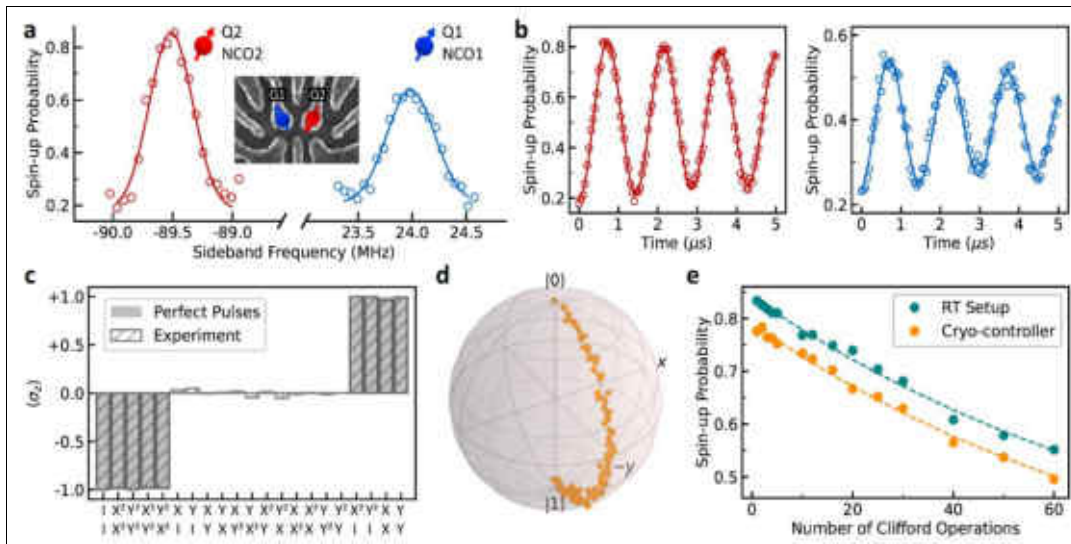


Fig. 32. Frequency-multiplexed qubit control and fidelity benchmarks with the cryo-controller *a*. Spectra showing the qubit resonances. Inset: SEM image indicating the qubits' positions. *b*. Frequency-multiplexed control producing simultaneous Rabi oscillations of  $Q_2$  (left) and  $Q_1$  (right). The decay arises mainly from the residual coupling between the two qubits. *c*.  $\langle \sigma_z \rangle$  of  $Q_2$  measured after an AllXY sequence. The output power is calibrated to achieve a  $\sim 1$  MHz Rabi frequency (the same applies to the QST and RB experiments). The visibility is normalized by removing the readout error. *d*. Trajectory of the state of  $Q_2$  under an  $X^2$  gate reconstructed by QST. Orange data points indicate the qubit state after incrementing microwave burst times. *e*. Randomized benchmarking of  $Q_2$  performed by the cryo-controller and the room temperature setup

Randomized compiling for scalable quantum computing on a noisy superconducting quantum processor. The successful implementation of algorithms on quantum processors relies on the accurate control of quantum bits (qubits) to perform logic gate operations. In this era of noisy intermediate-scale quantum (NISQ) computing, systematic miscalibrations, drift, and crosstalk in the control of qubits can lead to a coherent form of error which has no classical analog. Coherent errors severely limit the performance of quantum algorithms in an unpredictable manner, and mitigating their impact is necessary for realizing reliable quantum computations. Moreover, the average error rates measured by randomized benchmarking and related protocols are not sensitive to the full impact of coherent errors, and therefore do not reliably predict the global performance of quantum algorithms,<sup>6</sup> leaving us unprepared to validate the accuracy of future large-scale quantum computations. Randomized compiling is a protocol designed to overcome these performance limitations by converting coherent errors into stochastic noise, dramatically reducing unpredictable errors in quantum algorithms and enabling accurate predictions of algorithmic performance from error rates measured via cycle benchmarking. In the NISQ era, different error types limit the accuracy of quantum algorithms. Interactions between qubits and the surrounding environment lead to decoherence. In contrast, systematic imperfections in qubit control and crosstalk on multi-qubit processors result in coherent errors. Randomized compiling (RC) is a scalable protocol for reducing coherent error rates in situ without requiring a priori knowledge of the specific error model, while also closing the gap between NISQ algorithm performance and predictions from randomized benchmarks. It demonstrated the experimental implementation of RC in the context of the universal circuits required for NISQ applications and achieving quantum advantage<sup>1</sup> on a superconducting quantum processor (see Fig. 33a).

RC effectively reduces and stabilizes the otherwise unpredictable impact of actual performance-limiting coherent errors in both random circuits of variable depth and the quantum Fourier transform (QFT) algorithm. RC tailors' coherent errors into stochastic noise by combining the results of many logically-equivalent circuits. By inserting and compiling random single-qubit (virtual) twirling gates into a circuit in a way that preserves the overall unitary operation, RC creates a family of "randomized" circuits that are logically equivalent to the original "bare" circuit, without increasing circuit depth. Any bare circuit composed of  $K$  cycles of interleaved single-qubit "easy" gates and two-qubit "hard" gates can be randomized using the following method, shown in Fig. 1b. Coherent errors can be very detrimental on multi-qubit processors due to the complex nature of crosstalk, and will become a serious impediment to progress as the size of quantum processors continues to grow. While their average error rate can be measured using unitary RB, this does not capture the full impact these errors have on idle qubits, such as those not explicitly involved in an entangling gate. Instead rely on



cycle benchmarking, a scalable protocol that isolates errors affecting all qubits during any parallel gate cycle. Furthermore, the effective noise of any cycle under CB is equal to the tailored noise under RC, enabling accurate predictions of algorithmic performance under RC via CB process infidelities.

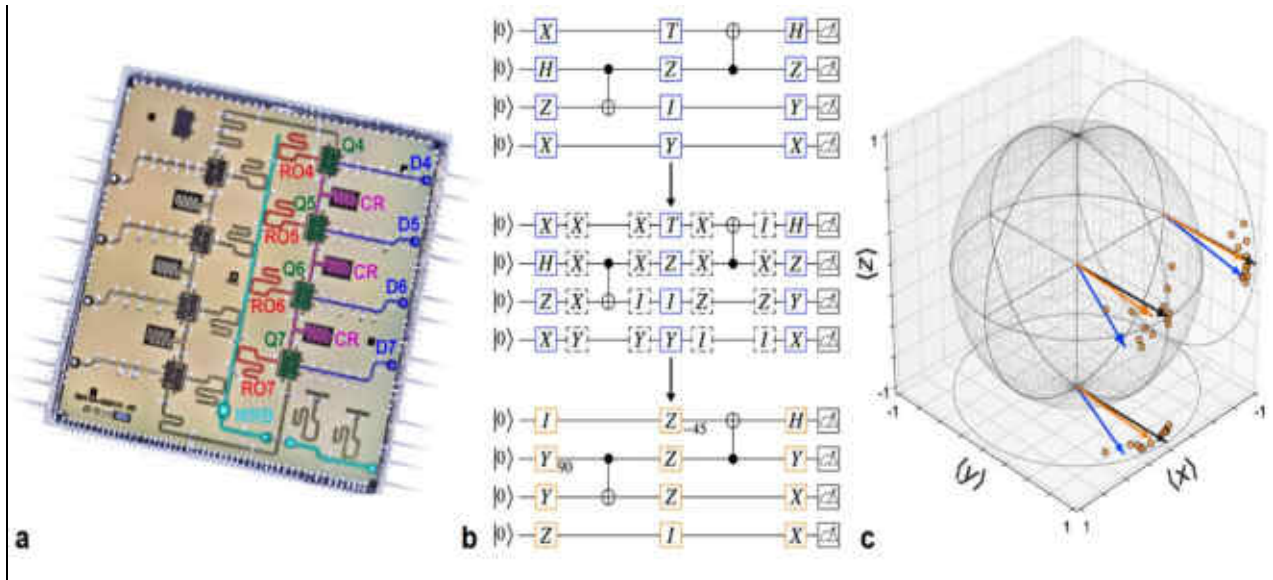


Fig. 33. Experimental realization of noise tailoring via randomized compiling on a superconducting quantum processor. *a*, False-colored micrograph of the eight-qubit superconducting quantum processor. *b*, Randomization of a quantum circuit. The circuit, split into  $K$  cycles of easy/hard gates (top), is converted into a logically-equivalent circuit by inserting random single-qubit twirling gates in each easy cycle, inverting them in the following cycle (middle), and then compiling the twirling gates into a new easy gate cycle (bottom). *c*, Experimental single-qubit state-tomography results demonstrating noise tailoring: the combined result (orange vector) of 12 randomizations (orange points) is more co-aligned with the ideal final state (black vector) than the final state of the bare circuit (blue vector), but has a lower purity due to the tailored noise, which causes decoherence

Figure 34a outlines the process by which CB can be used to re-construct single- and two-body gate errors that occur during any hard gate cycle involving a single CNOT gate and identity gates on the spectator qubits.

Using this method, the major sources of errors was identified in the system and compensate the most harmful effects with targeted decoupling pulses or virtual phase gates. The results plotted in Fig. 33b show that the residual error syndromes are broadly distributed, collectively contributing to the process infidelity of each cycle and making further targeted error mitigation less fruitful.

**Quantum Fourier Transform.** RC can be applied to any algorithm, including those at the heart of many quantum applications, like the quantum Fourier transform. Much like the classical discrete Fourier transform, the QFT maps singular inputs (i.e.,  $|0000\rangle$ ) into uniform distributions, and maps superposition states (i.e.,  $|++++\rangle$ ) into singular distributions. To measure the performance of RC for different resultant probability distributions, we applied the QFT to various single-qubit product states involving permutations of  $|0\rangle, |1\rangle$ , as well as random input states  $SU(2)_{\text{rand}}^{\otimes 4} |0000\rangle$ ; see Fig. 35a for several example of the measured distributions.

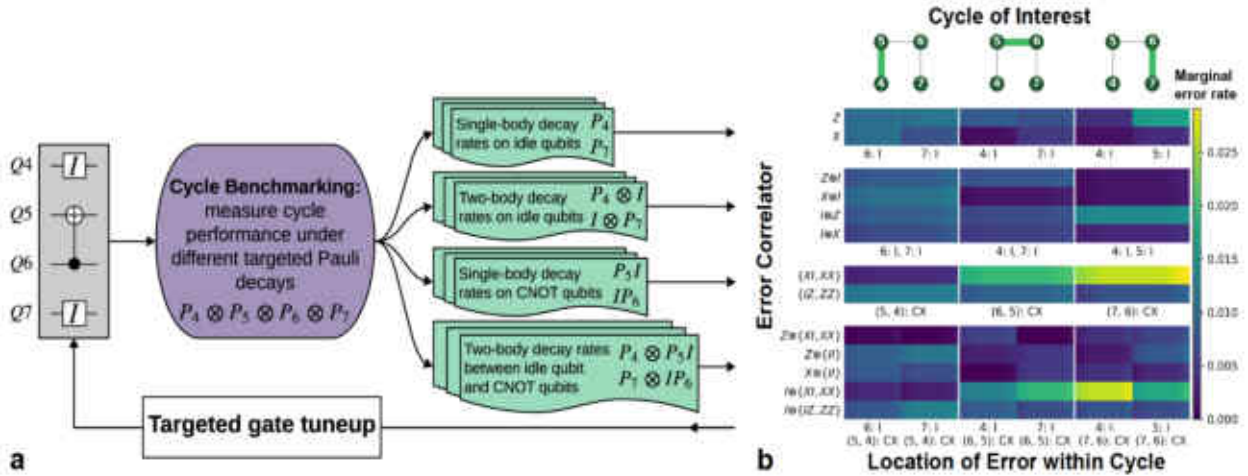


Fig. 34. Cycle error reconstruction of the tailored noise under cycle benchmarking. *a*, Schematic of the process by which single- and two-body gate error rates can be reconstructed using targeted CB measurements of any parallel gate cycle (e.g., CNOT between  $Q_5$  and  $Q_6$ ). These decay rates provide detailed information about the marginal probability of errors occurring during the cycle, as shown in *b*. *b*, Cycle error reconstruction results of four-qubit cycles containing a single CNOT gate and identity gates on the spectator qubits. [The y-axis (x-axis) labels the type of error (where the error occurs), and the color (gradient) indicates the marginal error rate from all Pauli contributions (95% confidence interval)]

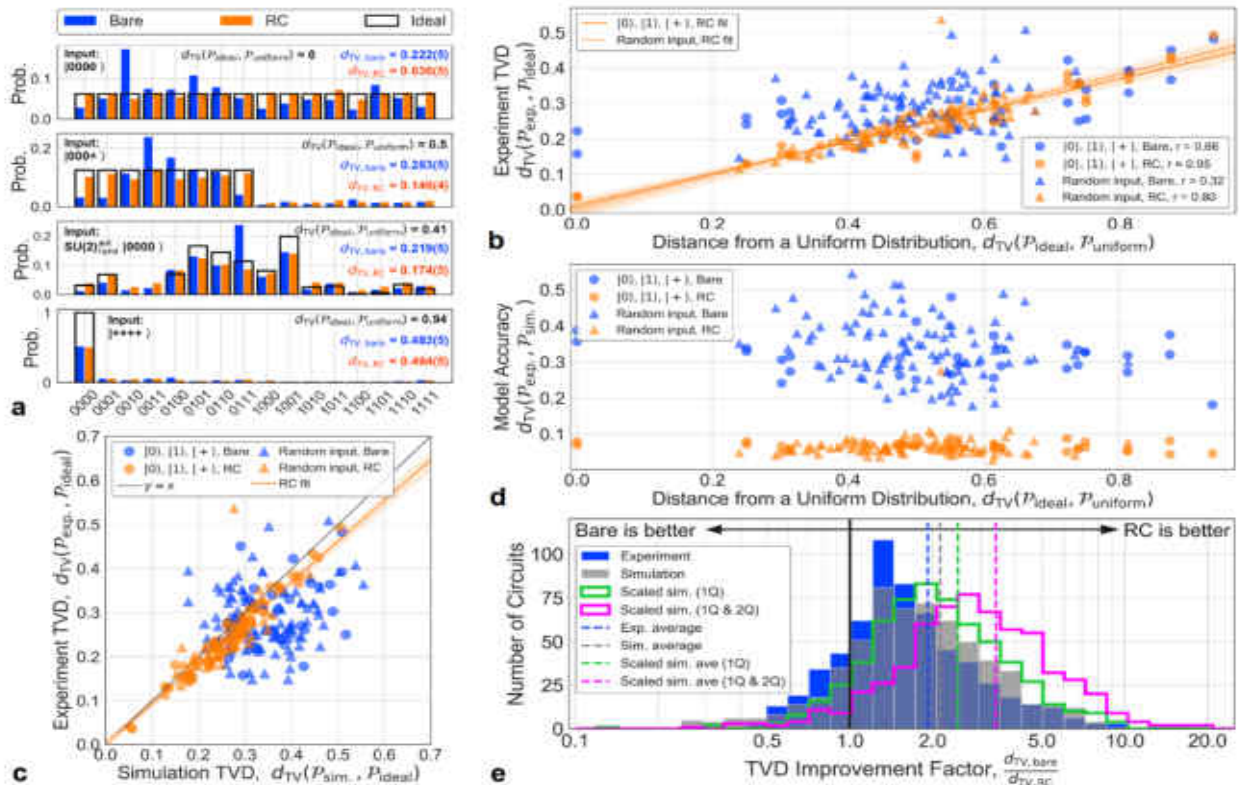


Fig. 35. Improving the quantum Fourier transform with randomized compiling. *a*, Measured probability distributions for the QFT applied to  $|0000\rangle$ ,  $|000+\rangle$ ,  $|++++\rangle$ , and a random input state  $SU(2)_{\text{rand}} |0000\rangle$ . *b*, Bare and RC TVDs for all four-qubit QFT results, as a function of distribution uniformity of the ideal results. RC provides more improvement as the resultant distribution spans more basis states. *c*, Experimental vs. simulated TVDs from a theoretical model of our system based on single-body errors from Fig. 34b. *d*, Accuracy of our model compared to experimental results. *e*, Summary of the improvement under RC for all two-, three-, and four-qubit random input QFT results, showing good agreement between experiment (blue) and theory (grey)

Each bare QFT circuit was measured 10,000 times.  $N = 50$  randomizations were generated for each bare circuit, and each randomization was measured 200 times. All “random” input states were generated by applying random  $SU(2)$  unitaries to each qubit independently before applying the QFT algorithm. 100 random inputs were generated for the data presented in Fig. 35b.

Simulations in which single-qubit (green) and two-qubit (pink) error rates have been scaled down by a factor of 10 suggest that RC performance increases as error rates decrease.

Figures 35 a,b show that RC is most (least) effective at mitigating coherent errors when the algorithm generates a uniform (singular) distribution across all measurement basis states. This is due to the basis-dependence of the TVD: if the target state is an eigenstate of the measurement basis, the raw probabilities will not be sensitive to off-diagonal terms in the error process resulting from coherent errors, so RC provides no overall benefit. Therefore, distribution uniformity is a good proxy for the susceptibility of the target state to coherent errors with respect to the measurement basis, and is thus correlated with improvement under RC. While the model cannot accurately predict the individual results of non-randomized circuits, it does predict the general distribution of improvement under RC (simulated (gray) results in Fig. 35e), including the approximate fraction of cases.

RC provides a strategy for mitigating complex and intractable crosstalk dynamics, extending the computational reach of noisy quantum processors. Additionally, novel error reconstruction methods using CB are well-suited to characterize the new and emergent forms of crosstalk errors seen on multi-qubit processors, and offer a method for accurately predicting error rates under RC. This improved predictability is essential for scalable quantum computing, and is necessary for comparing experimental error rates to fault tolerant thresholds. Furthermore, these methods and results have broad relevance across all experimental and theoretical efforts exploring quantum computing applications, from fundamental physics, to quantum chemistry and biologically-motivated problems. To this end, RC is not just a stopgap measure in the NISQ era, but will continue to be a powerful technique beyond NISQ [15].

**Quantum Optics Hardware: Quantum Computer-Aided design.** Photonic systems are highly flexible and controllable for small to medium-sized quantum systems, and offer resilience against decoherence. Those properties make them a first choice in many proof-of-concepts in quantum information science. Examples range from observations of fundamental quantum properties, such as indefinite causal orders or early demonstrations of Wigner's friend paradox, high-dimensional quantum communication systems such as quantum key distribution, entanglement swapping or quantum teleportation and experimental quantum machine learning and new propositions for quantum technologies. The parameters of a quantum system grow exponentially with the number of involved quantum particles. Hence, the associated memory requirement goes well beyond the limit of best classic computers for quantum systems composed of a few dozen particles leading to huge challenges in their numerical simulation. This implied that verification, let alone, design of new quantum devices and experiments, is fundamentally limited to small system size. It is not clear how the full potential of large quantum systems can be exploited. Universal quantum computer have unique advantages too, two of them are particularly relevant here: First, the initial state preparation can be deterministic in contrast to widely used probabilistic photon state sources. Second, the access to universal gates allows more efficient measurement protocols. Photonic states can be transformed by optical elements which can be represented by digital quantum gates.

Figure 36 shows the gate-based representation of important optical elements for high-dimensional quantum optics.

The parametrized setup which can generate a post-selected heralded 332-state is shown in Fig. 37 where the state is created in the photonic paths b; c; d and a measurement of the photon in path a is used for heralding.

While the preparation of the state is non-trivial with a quantum optical setup, it can be directly prepared on a digital computer as shown in Fig. 36. Another advantage of the simulation on a digital quantum computer is the direct generation of initial states (here high dimensional bell states) which, on real photonic devices, have to be created in a probabilistic way (like spontaneous parametric down-conversion – SPDC). In other words, on the digital quantum computer simulated only the runs of the experiment with successful initialization. For this example, it is possible to approximate each internal degree of freedom by a single qubit and use an efficient encoding  $E$  for the implementation of the single-photon projector leading to an overall circuit size of 15 qubits [16].

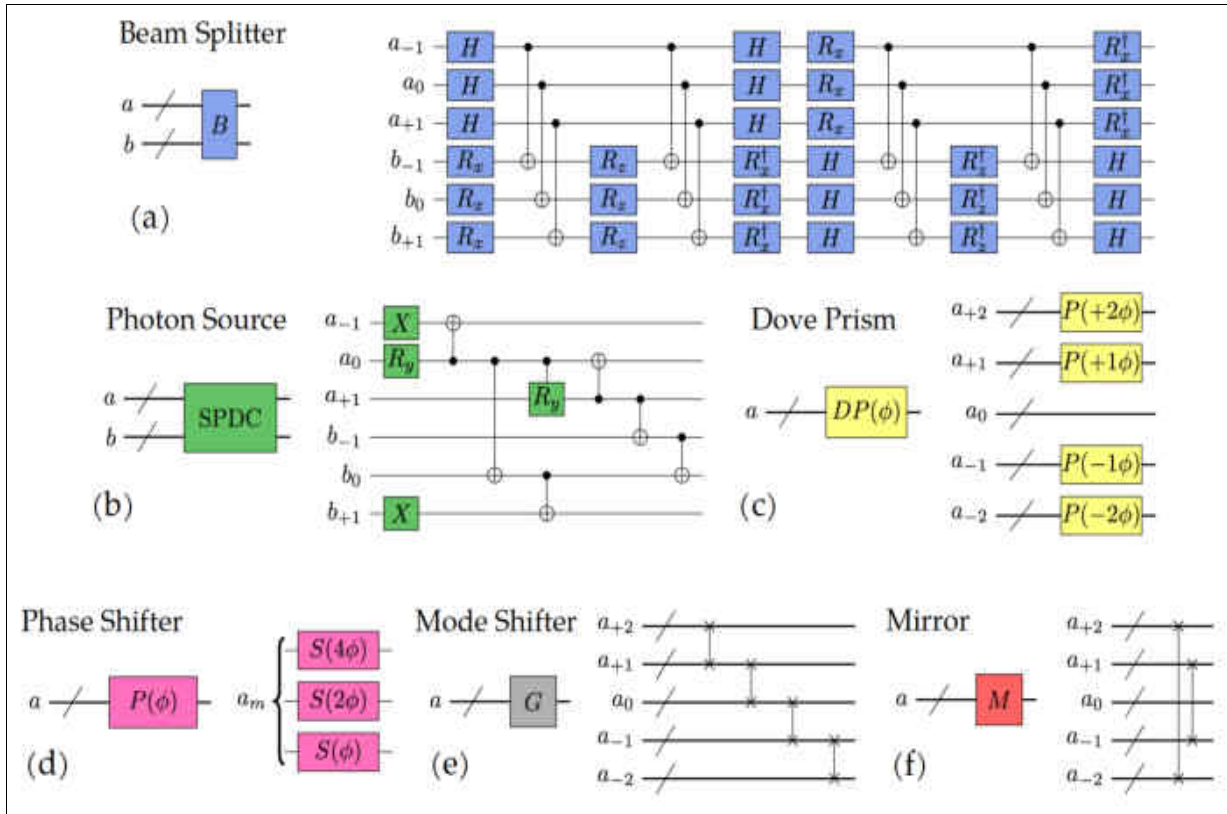


Fig. 36. Quantum circuits for multi-photonic high-dimensional quantum optics. Optical paths are denoted by  $a$ ;  $b$ ;  $c$  while internal mode numbers are denoted by subscripts. (a) Example of a beam splitter as used in Fig. 36 where each internal mode is represented by one qubit. The general multi-photon beam is constructed with a Trotter expansion and is too large to show here. (b) Direct emulation of a high-dimensional entangled photon state created by spontaneous parametric down conversion in a nonlinear crystal. (c) Mode dependent phase shifter (Dove prism) implemented as multiple phase shifters acting on the corresponding modes. (d) Mode independent phase shifter where the photonic occupation number is encoded in binary into 3 qubits (up to 7 photons per mode). (e) Cyclic approximation to a mode shifter (hologram) implemented by photonic swap gates (each swap acts on all the qubits which represent the mode). (f) Mirror implemented by photonic swap gates. [Here the orbital angular momentum of photons as a high dimensional degree of freedom used. In general, this approach can be applied to any discrete high dimensional quantum numbers. Each internal mode is represented by several qubits representing the photon occupation number]

As such, it anticipated the application of quantum designed quantum hardware to quantum computing hardware, quantum sensors, quantum memories, or quantum communication networks.

**Example: Application of Grover's quantum search algorithm to High-Energy Physics Data at the Large Hadron Collider.** A novel method of applying a scientific quantum algorithm, Grover's algorithm, to search for rare events in proton-proton collisions at 13 TeV collision energy using CERN's Large Hadron Collider was demonstrated in [17]. The search is of an unsorted database from the ATLAS detector in the form of ATLAS Open Data. As indicated by the Higgs boson decay channel  $H \rightarrow ZZ^* \rightarrow 4l$ , the detection of four leptons in one event may be used to reconstruct the Higgs boson and, more importantly, evince Higgs boson decay to some new phenomena, such as  $H \rightarrow ZZ_d \rightarrow 4l$ . In searching the dataset for collisions resulting in the detection of four leptons, the study demonstrates the effectiveness and potential of applying quantum computing to high-energy particle physics. A classical simulation of Grover's algorithm, and multiple quantum computers, each with several qubits, it is demonstrated that this application makes the proper selection in the unsorted dataset. The implementation of the method on several classical simulators and on several of IBM's quantum computers using the IBM Qiskit Open Source Software exhibits the promising prospects of quantum computing in high-energy physics.



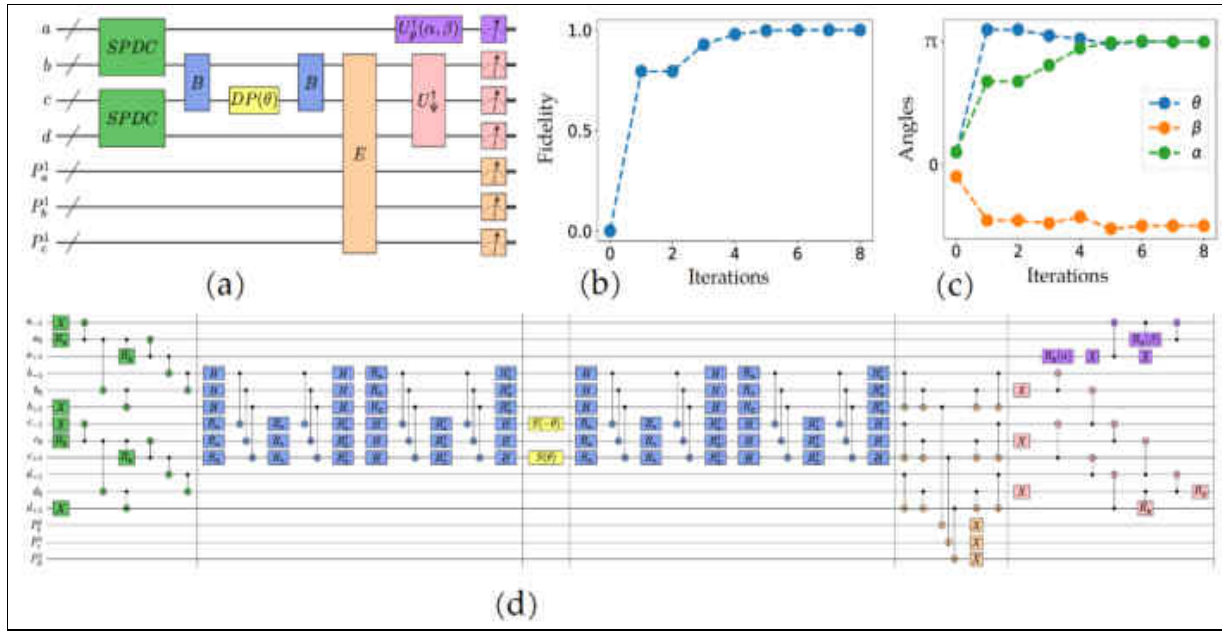


Fig. 37. Optimization of an asymmetric high-dimensional entangled state (a) Abstract representation of the optimization setup. Optical elements are shown in green, blue and yellow and are described in Fig. 36.  $U_p^\dagger(\alpha, \beta)$  transforms a parametrized photonic qutrit to zero which acts as a trigger for the three-photon state in paths b, c, d, E emulates the post-selection by transferring information about the photon number in paths b, c, d to auxiliary qubits  $P_b^1, P_c^1, P_d^1$ . Similar as the trigger in a  $U_\psi^\dagger$  transforms the target state into zero which is then measured. The probability of measuring zero directly corresponds to the fidelity of the setup with the target state. The setup is parametrized with three angles (one for the Dove prism and two for the trigger). (b-c) Optimization of the setup with the 'BFGS' optimizer. (d) Explicit circuit for the setup in (a)

Prior to the current study, the fundamentally distinct form of quantum computing had yet to be applied in the search of particle physics databases in this way. With high-energy particle physics being a data-intensive science, a large amount of data is collected at the Large Hadron Collider (LHC) at CERN and in the mega science project NICA at JINR (Dubna), where particles are accelerated and collided at high energies. Detectors such as that of the ATLAS (A Toroidal Lhc ApparatuS) collaboration collect data on the resulting shower of particles. With collisions run at higher energies, and as more and more particle decay channels are discovered, the ability to make novel scientific conclusions with this data requires increasingly improved methods of data sorting, pattern recognition, and data analysis. The current study demonstrates the development and application of a quantum search algorithm to complete tasks and answer essential questions in particle physics—specifically, to search for signals of the Higgs boson decay products in events detected at CERN's LHC, permitting "reconstruction" of the Higgs boson [17].

*Remark.* The eagerly anticipated LHC upgrade will enable the acceleration of particles to unprecedented energies and proton-proton ( $pp$ ) collision frequencies. The latest ATLAS Open Data release contains databases of  $pp$  collision events at a highest-ever 13 TeV collision energy. Large databases, containing vast amounts of event data recorded by the ATLAS detector, must be filtered, sorted, and searched. In current study [17], was developed the approach to the enormity of these databases in a novel manner—by implementing a quantum search. The augmented computational power of quantum computing as compared to its classical counterpart, which stems from quantum superposition, expedites the search; while classical bits have two possible states, 0 and 1, quantum bits, or qubits, may exist in the measurable  $|0\rangle$  and  $|1\rangle$  states as well as in a quantum superposition of  $|0\rangle$  and  $|1\rangle$ . Grover's algorithm selects a target quantum state and increases the probability that the system is measured in that state. An application of QSA to the search of an HEP database was developed and run on a variety of quantum computers and simulations. The ATLAS Open Data containing events from 13 TeV  $pp$  collision energy was searched. The database contains data on lepton transverse momenta as detected by the ATLAS collaboration's detector. It searched the database for collisions' products, or events, in which four leptons were detected at the appropriate energy and mass window, evincing the presence of the Higgs boson in the post-collision particle showers, as indicated by the Higgs boson's  $4l$  decay channel.

Figure 38 demonstrates how the Grover iteration alters measurement probability.

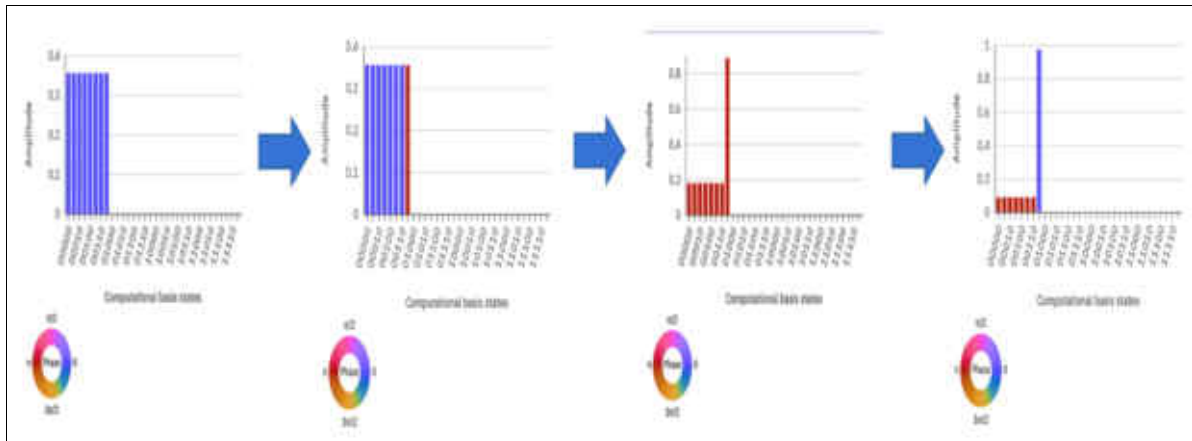


Fig. 38. The effect of Grover's algorithm on the the amplitude of each qubit state.

[The amplitudes of all 8 possible states of the three-qubit quantum chip are shown at various stages of the algorithm. The system is placed in an equal superposition (far left), with each state's amplitude being  $\frac{1}{2\sqrt{2}}$ . Progressing to the right, the phase transformation and amplitude amplification of the target state are shown. The process is repeated in a second iteration, resulting in a greater target state amplitude (far right)]

The three-qubit quantum chip is placed in an equal superposition, with each state's amplitude being  $1 / 2\sqrt{2}$ . The target amplitude is multiplied by  $-1$  (a phase shift of  $\pi$ ) before the algorithm performs amplitude amplification on the target state. After the second iteration of quantum algorithm, the target state amplitude, and thus the state's probability of measurement, is closer to 1. Quantum algorithm was run on simulated qubits in the *R* programming language and in IBM's Qiskit using Python. The algorithm was then run on the hardware of real IBM quantum computers, producing slightly less distinct peaks in target state measurement probability - the product of quantum decoherence. Quantum algorithm was successfully used to search the ATLAS database for events with four leptons. When run on the simulator, the correct state was selected with 100% probability, and the code yielded the event(s) with four leptons. However, when run on IBM quantum hardware, quantum decoherence reduced the peak in target state probability. It was examined ways in which the decoherence was mitigated.

The probability distribution of each quantum state's measurement following steps and iterations of Grover's algorithm reflects the manipulation of amplitude to yield a peak in probability of target state measurement. A three-qubit quantum chip placed in an equal superposition demonstrates a  $1/8$  probability of each possible state being measured. After one iteration of GA, there is a probability of 0.78 that the chip is measured in the target state (Fig. 39).

Following two iterations of Grover's algorithm on three qubits, the target state is selected with a probability of 0.94 on the QC simulator. The results shown in Fig. 39, a corroborated models for the optimization of quantum algorithm iterations, which indicate that the ideal number of iterations on  $n$  qubits is  $\frac{\pi}{4} \sqrt{2^n}$  assum-

ing no hardware error. When three iterations of GA were run on a three-qubit system, the correct state was selected with a probability of 0.33. Figure 39, a shows the results of Grover's algorithm with a varying number of iterations on three qubits. The optimization of target state measurement probability is a key element of conducting quantum searches with Grover's algorithm; this factor was considered along with quantum decoherence when applying the quantum search to ATLAS data. Grover's algorithm was executed on increasing numbers of qubits on real IBM quantum computers, which demonstrated a similar peak distinction once measured. The probability distributions of runs on QCs were compared to those of simulated runs. As seen in Fig. 39, b, the peak in probability is slightly less distinct after runs on real QCs due to quantum decoherence.

Grover's algorithm was run on a varying number of qubits. The algorithm continued to yield a distinct peak in target probability after one iteration, as seen in Fig. 40.



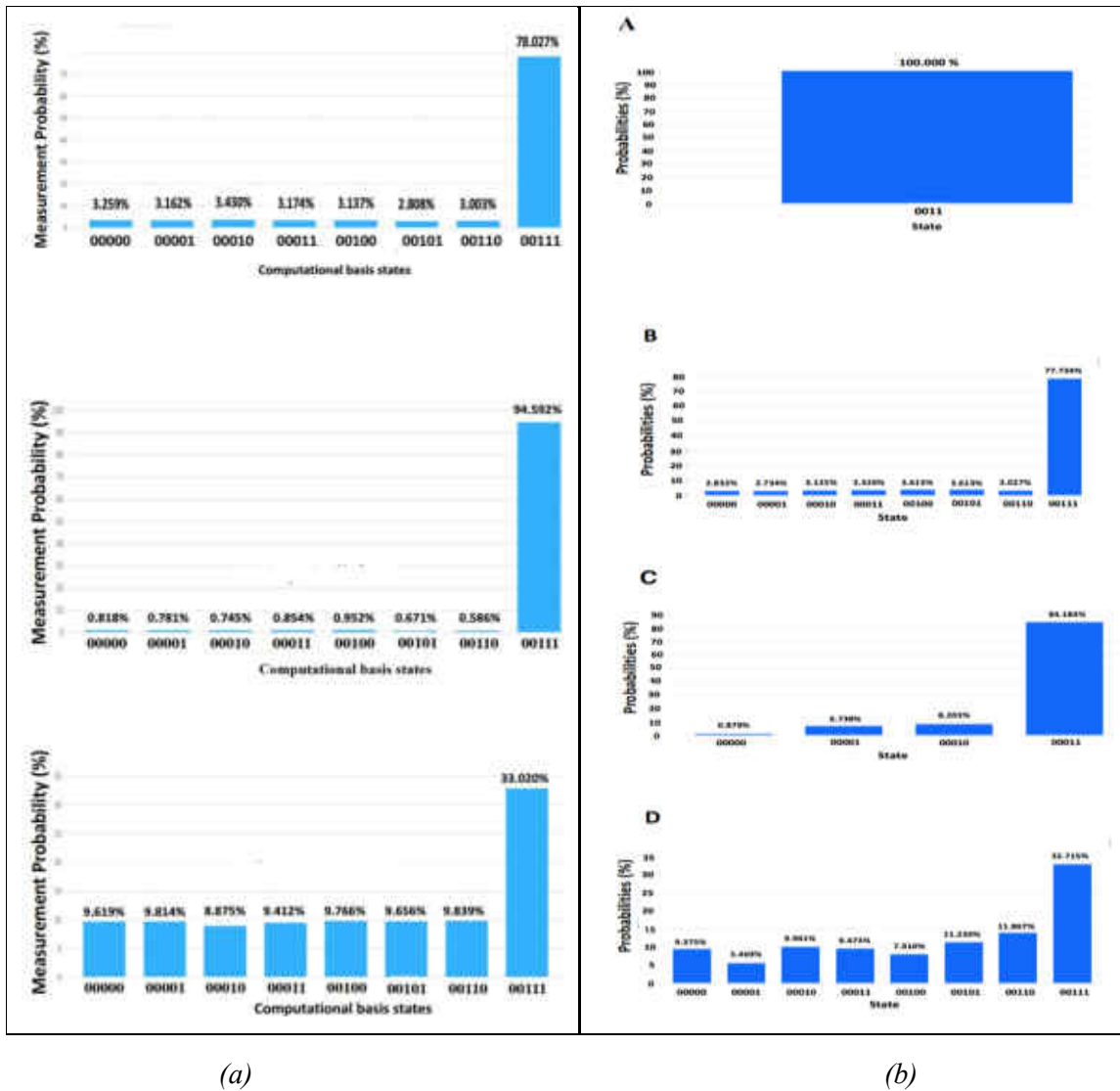


Fig. 39. Probability of target state measurement with multiple iterations.

a) Optimized probability of target state measurement occurs after  $\frac{\pi}{4}\sqrt{2^n}$  iterations, rounded to the nearest

integer. For a three-qubit quantum system the optimal number of iterations is  $\frac{\pi}{4}\sqrt{2^3} \approx 2.2 \approx 2 \approx 2$ ; b)

Grover's algorithm applied to two-and three-qubit systems in Qiskit. The probability of each two-qubit (A, C) and three-qubit (B, D) state is presented upon measurement after one iteration of GA on the Qiskit simulator (A, B) and on real IBM QCs (C, D)

Physics model of search motivation. The Higgs boson that was discovered at the LHC, if it is the standard model (SM) boson, will couple to SM particles in a manner that is unlike any other lepton, quark, or gauge boson; its coupling strength is related to the particle's mass. If the nature of its coupling depends on the mass of the state it couples to, it may provide a new means to search for phenomena that are beyond the SM of particle physics. The Higgs boson could provide a portal to a so-called Dark Sector of new particles and interactions, coupling to them in a unique way that cannot be probed with other SM probes. Completely new physical states may therefore be accessible experimentally, via coupling to the Higgs boson, in a way that did not exist previously. Theoretical studies, supported by astrophysical and cosmological experimental data, indicate that these Dark Sector particles can lead to very rare events in LHC collisions. An LHC Dark Sector search consists of detecting a resonance that decays to leptons. Leptons are a class of structureless particles with spin-1/2 that do not exhibit strong interactions. Leptons can be electrons ( $e$ ), muons ( $\mu$ ), tau particles ( $\tau$ ), or neutrinos ( $\nu_e, \nu_\mu, \nu_\tau$ ). In the study described here, was choose to search for a resonance that decays to electron-positron or positive muon and negative muon pairs.

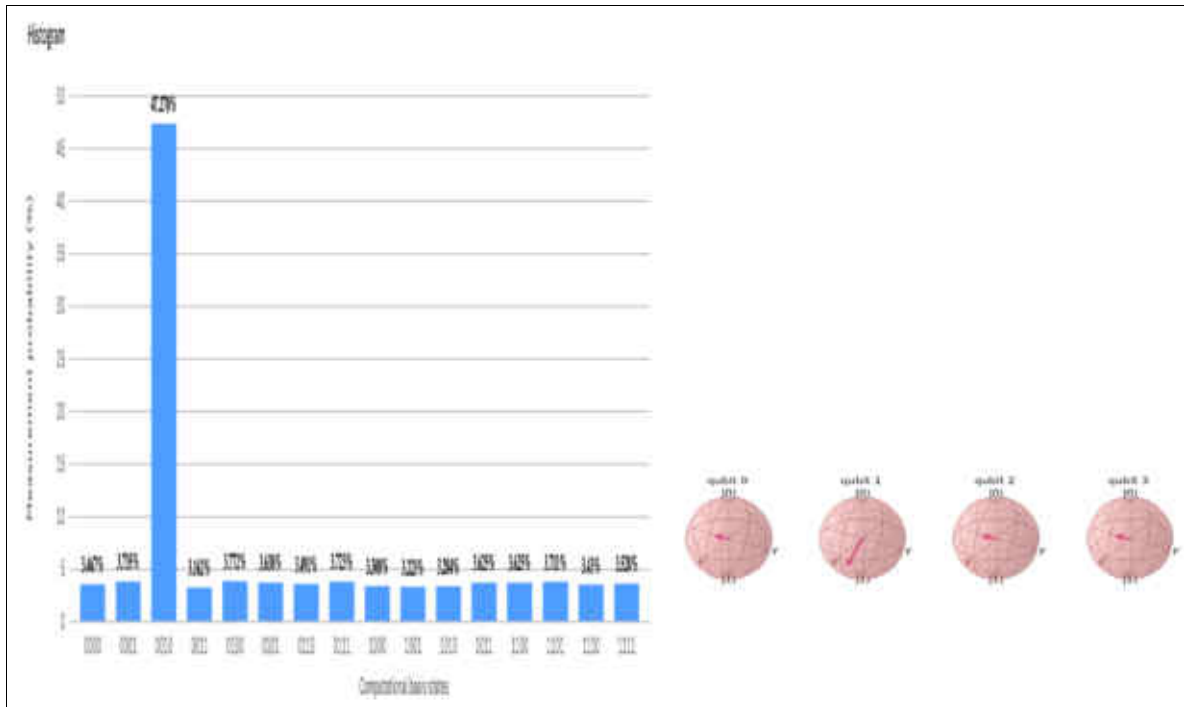


Fig. 40. Four-qubit quantum search and qubit representation.

[The algorithm yielded a distinct peak in probability of target state measurement (left) when run on four qubits. The final multi-qubit state that is conducive for a successful search is shown in Bloch sphere representations of each qubit (right)]

This resonance that signals a new particle would be seen above a broad spectrum of background SM events. Electron and positron candidates consist of clusters of energy deposited in the electromagnetic calorimeter associated with their tracks inside the detectors. The clusters matched to tracks are required to satisfy a set of identification criteria that require the longitudinal and transverse shower profiles to be consistent with those expected for electromagnetic showers. These are registered as hits, which are then translated in software to electron and positron energies, momenta, charges, and position at any given time. Positive and negative muon candidates are formed by matching reconstructed detector tracks in one ATLAS spectrometer subsystem with either complete or partial tracks reconstructed in a separate ATLAS subsystem. If a complete track is present, the two independent momentum measurements are combined. The particles are identified as muons if their calorimetric energy deposits are consistent with a minimum ionising particle. The detector data has already been formatted to run using classical algorithms on a classical computer. This format had to be changed to suit the quantum algorithm that is being used for the results shown here. It is understood that for future analyses that will employ quantum search algorithms such as the one described here; it will be much more efficient to store that data in a quantum format initially. This formatting should be the next step taken after collecting the tracking hits, energy deposits, shower profiles, etc, as described above.

The collected information, as described before, is converted into database entries that are appropriate for the designed method of Dark Sector searches using exotic decays of the Higgs boson, and which are in a format that can be understood and handled by the quantum search algorithm. In this study, Grover's quantum search algorithm was used, and the database searched contained the transverse momenta of detected leptons. Data pertaining to the exotic decays of the Higgs boson used in Dark sector searches was sought. The Higgs boson may decay into a  $ZZ^*$  ( $Z^0$  boson and an off-shell  $Z^0$  boson) pair, which in turn decay into four leptons. This decay channel is commonly represented as  $H \rightarrow ZZ^* \rightarrow 4l$ . In rare cases, the decay channel  $H \rightarrow ZZ_d \rightarrow 4l$ , where the  $Z_d$  refers to a Dark Sector vector boson that is beyond the standard model of particle physics, can occur. Once produced, the Higgs boson decays quickly, leaving the four leptons at the end of the decay channel to be detected by the ATLAS detector. A search was designed on a database of detected leptons; the search was for collisions, or events, in which four leptons were detected. The data presented in this existing work was taken from the LHC's recent run at a record-high proton-proton collision energy of 13 TeV, where the chances of Higgs boson production are higher.

Figure 41 shows the matrices with which the QC simulator in *R* simulates a quantum computer.

	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	0.3535534	0.3535534	0.3535534	0.3535534	0.3535534	0.3535534	0.3535534	0.3535534
[2]	0.3535534	-0.3535534	0.3535534	-0.3535534	0.3535534	-0.3535534	0.3535534	-0.3535534
[3]	0.3535534	0.3535534	-0.3535534	-0.3535534	0.3535534	0.3535534	-0.3535534	-0.3535534
[4]	0.3535534	-0.3535534	-0.3535534	0.3535534	0.3535534	-0.3535534	-0.3535534	0.3535534
[5]	0.3535534	0.3535534	0.3535534	0.3535534	-0.3535534	-0.3535534	-0.3535534	-0.3535534
[6]	0.3535534	-0.3535534	0.3535534	-0.3535534	-0.3535534	0.3535534	-0.3535534	0.3535534
[7]	0.3535534	0.3535534	-0.3535534	-0.3535534	-0.3535534	-0.3535534	0.3535534	0.3535534
[8]	0.3535534	-0.3535534	-0.3535534	0.3535534	-0.3535534	0.3535534	0.3535534	-0.3535534

Fig. 41. QC simulation matrix.

[A matrix of qubit wave-function amplitudes in the *R* Programming QC Simulator]

In place of physical changes of qubit amplitudes, the simulator runs mathematical transformations. Registration with IBM granted access to real quantum computers in addition to QC simulators through Qiskit. From then on, a classical computer was employed to create and modify code in Python. The simulation backend `ibmq_qasm_simulator` was used for testing numerous times before algorithms were run on real devices. After running Grover's algorithm in different ways on both real and simulated quantum hardware as to develop the best method for application to real encoded data, the search of LHC data was developed. The database contained the transverse momenta (the component of momentum that is perpendicular to the beam line of collided particles) of detected leptons. Leptons were recorded with their event number. To distinguish between leptons in the same event, "in-instance" values were assigned. Any first lepton detected in its event had an instance = 0; the second detected lepton in its event, an in-instance = 1; for the third, instance = 2, and for the fourth, instance = 3.

Figure 42 is a sample from the database and displays the arrangement of the data.

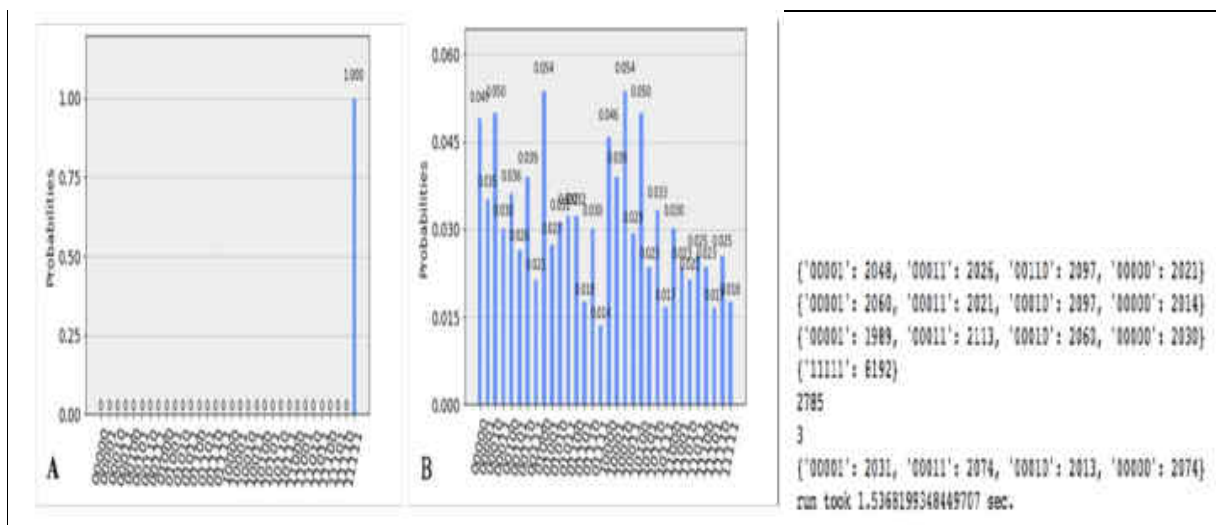
Thus, the presence of a lepton instance value of three in the database indicated that four leptons were detected following one collision.

To apply the quantum search algorithm to the ATLAS data, the data was encoded into the quantum circuit. Classical data, in groups of four entries, was placed into the quantum states of a five-qubit quantum system as follows. As each lepton received an "instance" value for the event in which it was detected by ATLAS, the marked state corresponded to instance = 3. The search was run on the five-qubit quantum system, with `q[0]` and `q[1]` defining the index of the lepton in its group of four leptons searched by GA, and with `q[2]` and `q[3]` keying in the value of the lepton "instance" with respect to event, as in the database. Qubit `q[4]` served as an ancillary qubit. A classical computer was used to compose code to run on IBM devices. An interactive simulator called Quirk was employed for developmental purposes. Quirk allows developers to drag quantum gates onto a circuit and demonstrates the direct effect on the amplitude, probability, and representation of each state at the end of the circuit. Quirk provides real-time simulated results as the circuit changes, rather than requiring users to run the circuit and a final measurement step in order to obtain the results of the simulation. The code was run on each group of data entries thousands of times to yield accurate probability distributions for the final state of the quantum system. All iterations on the data subsets not containing the marked lepton state yielded a quantum system in equal superposition and thus an equal probability of measurement in each state. Those iterations on groups of four data entries containing an index value of 3 were hypothesized to leave the quantum system with a higher probability - mathematically, 100% - of measuring the marked state with index = 3. In order to solely yield the data entry (row) number in the database and the transverse momentum of exclusively leptons with index = 3, the code yielded these values for those states with a probability of being measured  $\geq (.80)$ . The algorithm was first run and tested on IBM's `ibmq_qasm_simulator` backend before it was run on several IBM quantum computers [17].

* 2533 *	0 * 72516.546 *
* 2534 *	0 * 246668.31 *
* 2535 *	0 * 165265.67 *
* 2536 *	0 * 108012.57 *
* 2537 *	0 * 155143.73 *
* 2538 *	0 * 34341.609 *
* 2539 *	0 * 164251.06 *
* 2539 *	1 * 111820.89 *
* 2539 *	2 * 106602.97 *
* 2539 *	3 * 17182.996 *
* 2540 *	0 * 118106.53 *
* 2541 *	0 * 33087.984 *
* 2542 *	0 * 33969.863 *

Fig. 42. A sample from the Open Data keyed into the circuit

**Grover's Algorithm Application to LHC Data: First Encoding.** The classical simulator backend `ibmq_qasm_simulator` yielded the target state with a probability of 1.0 (100%), as seen in Fig. 43,a and Fig. 43,b.



(a)

(b)

Fig. 43. a) Histogram of probabilities by quantum state with the ATLAS data encoded. (Left): The group of four data entries included the target lepton index = 3. The algorithm was run on Qiskit's `ibmq_qasm_simulator` backend, a classical simulation. B (Right): This group of four data entries contained the target lepton index = 3. The effects of decoherence can be seen. The algorithm was run on the quantum device `ibmq_16_melbourne`. b) Final state measurement counts for five groups of four data entries, each searched by quantum algorithm. [The fourth group contains the target lepton index = 3, and its corresponding state was measured all 8192 times on the simulator back-end.]

The search run on the real 15-qubit quantum computer `ibmq_16_melbourne` demonstrated a limited peak amplification, the consequence of quantum decoherence (Fig. 43,a). The code that was written generates distinct quantum circuits depending upon the values in the database. One quantum circuit, a map of all the quantum gates implemented in one run of Grover's algorithm on the ATLAS data, is shown in Fig. 44.

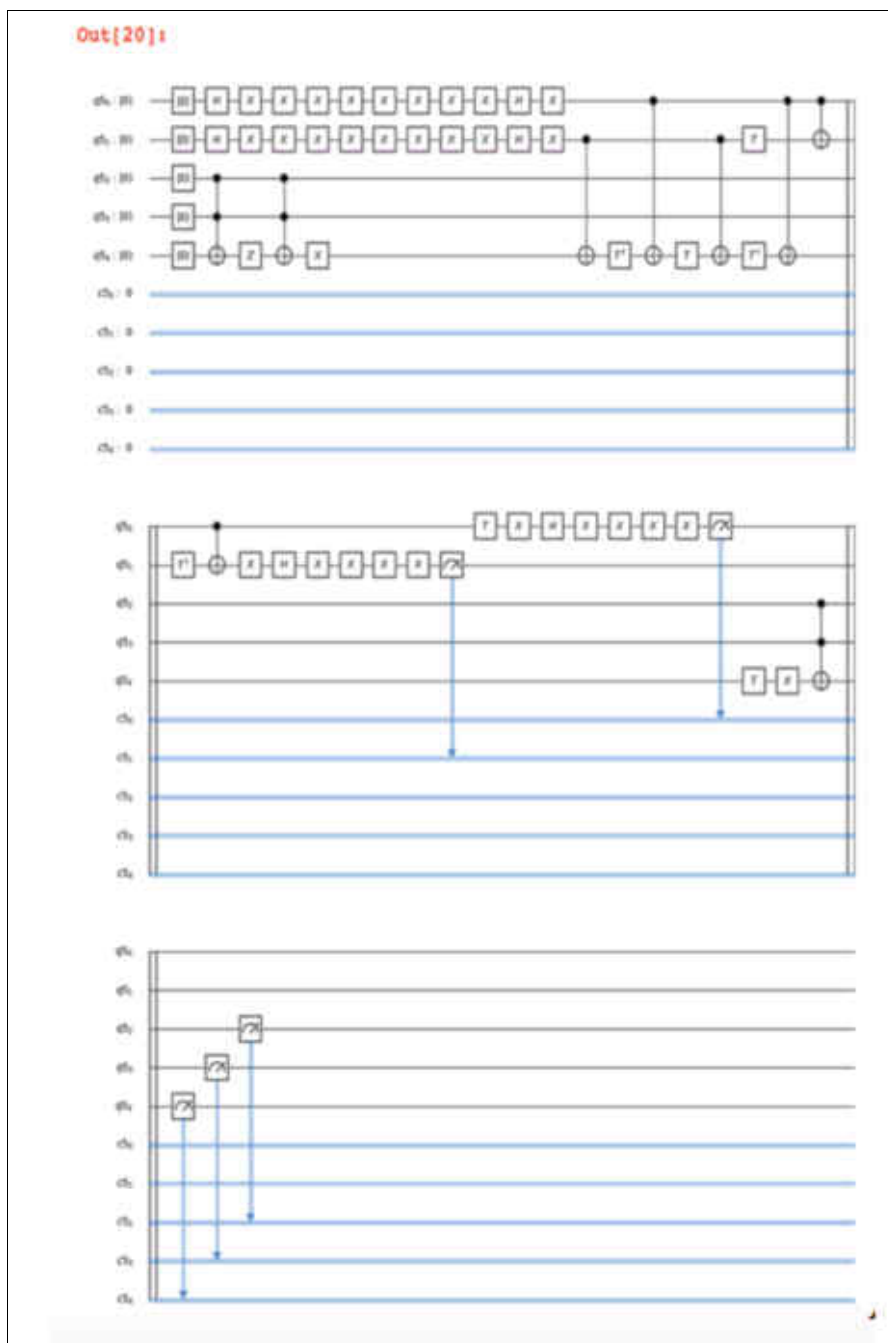


Fig. 44. Quantum circuit.  
[A quantum circuit generated in the selection process]

**Grover's Algorithm Application to LHC Data: Second Procedure.** The second method of encoding classical data to be searched requires fewer quantum gates and saw successful results on both the simulator and real quantum computers. After decreasing the number of quantum gates and running the code on several devices with the lowest error rates, we concluded that with the current level of QC engineering, decoherence to the degree of limiting meaningful results occurred with the amount of quantum gates our primary method of encoding the data requires. A different method of encoding data into the quantum computer was developed for the purpose of obtaining successful results with the latest existing quantum computers rather than anticipating advancements in their engineering. It was sought a method successful beyond theoretical quantum information. The casting of unsorted data - in groups of 8 - into the quantum computer began by defining qubits  $q[0]$  and  $q[1]$  as the value register. These two qubits encode the instance values of the database, which, as previously, are in the discrete set  $\{0, 3\}$ , as did  $q[2]$  and  $q[3]$  in the primary encoding method already described. In this second method,  $q[2]$ ,  $q[3]$ , and  $q[4]$  served to facilitate a binary encoding of index values contained in the discrete set  $\{0, 7\}$ . The procedure is described in [17]. The search using the second encoding method was run on QCs and QC simulators, all obtaining results that reflect success. As with the first encoding method, the



simulator selected the correct state with a probability of 1.0, or 100%. On the quantum computer `ibmq_vigo`, the five-qubit system was measured in the correct state 87.012% of the time, as seen in Fig. 45.

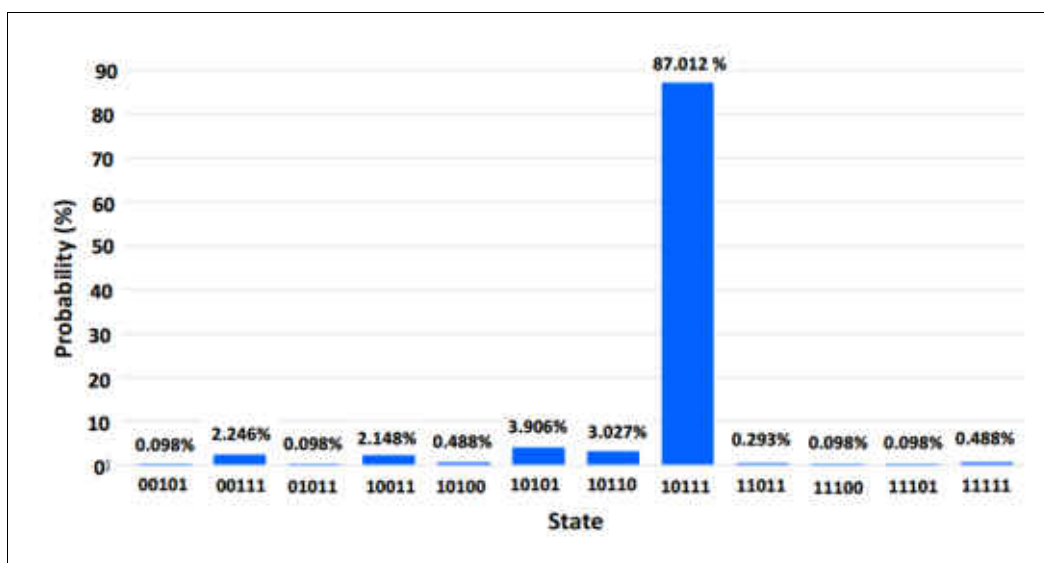


Fig. 45. Histogram of final state probabilities after 8,192 runs on the quantum computer `ibmq_vigo`. [The correct state was selected with a probability of 87.012 %, or 7,128 of 8,192 runs. The 20 of 32 states not shown in the histogram were states in which the system was not measured on any run]

With limited quantum decoherence owing to the modified, more efficient encoding method, the runs of the real quantum computer were successful. The application of a quantum search to data from *pp* collisions at 13 TeV collision energy is novel, and the 100% correct selection rate on the simulator demonstrates that, mathematically, the maneuvers on qubit amplitudes successfully yielded the correct result upon measurement. Yet at first, when the primary encoding method was run on the 15-qubit back-end `ibmq_16_melbourne`, where the quantum speed-up is reaped, the peak amplification was reduced as compared to the simulator devices. In a simulated environment, without quantum decoherence, quantum search algorithm successfully and effectively searched ATLAS Open Data for events with four leptons - with 100% accuracy; selected the target state with high probability when run on a real QC, demonstrating the viability of this extremely advantageous search method. The presented results are promising in databases directly for-matted to be searched by quantum computers; with LHC databases constructed in this way, quantum computers will expedite the data sorting, search, and analysis processes. The 100% success rate of Grover's algorithm in the simulated environment in searching the ATLAS Open Data for four leptons in the same event substantiates the theoretical viability of quantum algorithm. The algorithm's success on quantum computing simulators extends to the runs on real quantum computers, where the benefits of quantum computing to efficacy lie. The findings indicate that the use of quantum computing in particle physics would contribute to the acceleration of scientific discovery by, as shown via both the simulation as well as quantum computers, improving data selection at the LHC. There was mild discrepancy between the results on the quantum computers and those on the simulators - a product of quantum decoherence. With a strategically planned encoding process and with the reduction of quantum gates in our code, decoherence was mitigated. The result is a valuable set of results that offer promise to both quantum computing and particle physics.

## Conclusions

Quantum methods still face many challenges, not the least of which being the high error rates and low qubit counts of existing hardware. Ultimately, the success of quantum computational IT will depend on the ability to construct larger and better controlled quantum computers. The question of how large and how well controlled these machines must be will be determined by the quality of the procedures that we have developed to carry out the calculations of interest. It is therefore crucial that we continue to develop and optimize new algorithms, mappings, error correction codes and procedures, basis sets, and error mitigation techniques. Now highlight potential research directions to aid in this goal [1, 2, 8–17].



## References

1. Loceff, M. A Course in Quantum Computing for the Community College. – Foothill College. – 2015. – Vol. 1.
2. Entwicklungsstand Quantencomputer / F. K. Wilhelm [et al.]. – Federal Office for Information Security. – 2017.
3. Rue, J., Xambo, S. Mathematical essential of quantum computing. – ICMAT Severo Ochoa Project SEV-2011-0087 (Spain). – 2020.
4. Upgrading the Bloch sphere: Projective space foliated by Klein bottles as a geometrical representation of two-qubit states and their entanglement / O. Perdomo [et al.] // arXiv:1903.01940v1 [quant-ph]. – 5 Mar 2019.
5. Kregar, A., Ramšak, A. Qubit transformations on Rashba ring with periodic potential // New J. Phys. – 2020. – Vol. 22. – No 8. – Pp. 083048.
6. Marzari N, et al. Maximally localized Wannier functions: Theory and applications // arXiv:1112.5411v2 [cond-mat.mtrl-sci]. – 12 May 2012.
7. Tabakin, P. Model Dynamics for Quantum Computing // arXiv:1611.00664v2 [quant-ph]. Annals of Physics. – 2017. – Vol. 383. – Pp 33–78.
8. Superconducting quantum computing: A Review / H-L. Huang [et al.] // arXiv:2006.10433v1 [quant-ph]. – 18 Jun 2020.
9. Willsch, D. Supercomputer simulations of transmon quantum computers // arXiv:2008.13490v1 [quant-ph] 31 Aug 2020.
10. CMOS Position-Based Charge Qubits: Theoretical Analysis of Control and Entanglement / E. Blokhina [et al.] // IEEE Access. – 2020. – Vol. 8. – Pp. 4182–4197.
11. Quantum computational chemistry / S. McArdle [et al.] // Review of modern physics. – 2020. – Vol. 92. – No 1.
12. Ivancova, O. V., Korenkov, V. V., Ulyanov, S.V. Quantum software engineering Textbook 2: Quantum supremacy modelling. Part I: Design IT and information analysis of quantum algorithms. – M. : Kurs. – 2020.
13. Ivancova, O.V., Korenkov, V.V., Ulyanov, S.V. Quantum software engineering Textbook 2: Quantum supremacy modelling. Part II: Quantum search algorithms simulator – computational intelligence toolkit. – M. : Kurs. – 2020.
14. CMOS-based cryogenic control of silicon quantum circuits / X. Xue [et al.] // arXiv:2009.14185v1 [quant-ph]. – 29 Sep 2020.
15. Randomized compiling for scalable quantum computing on a noisy superconducting quantum processor / A. Hashim [et al.] // arXiv:2010.00215v1 [quant-ph]. – 1 Oct 2020.
16. Quantum Computer-Aided design of Quantum Optics Hardware / J. S. Kottmann [et al.] // arXiv:2006.03075v1 [quant-ph]. – 4 Jun 2020.
17. Armenakas, A. E., Baker, O. K. Application of a Quantum Search Algorithm to High-Energy Physics Data at the Large Hadron Collider // arXiv:2010.00649v1 [quant-ph]. – 1 Oct 2020.