Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

Using quantum communications for maritime signal flags

To cite this article: M. C. Plesa and M. I. Plesa, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 151-157.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-020

Using quantum communications for maritime signal flags

Plesa Maria-Carmen and Plesa Mihail-Iulian

Technical College "Costin D. Nenițescu" Pitesti
University of Bucharest

E-Mail: carmenplesa64@gmail.com

Abstract. Quantum communications are becoming very quickly a reality. There are huge advancement made in the field of quantum internet. Recently, IBM has announced the first commercial quantum computer with 20 qubits. Given all the advancements in the field, in this paper we investigate how quantum technologies can be applied in maritime communications. In this paper we address the problem of international maritime flag signals. More exactly, we proposed some quantum communication schemes for international maritime signal flags. We are also study the efficiency and security boost that quantum communications give in this type of maritime communication.

1. Introduction

Quantum computers are no longer an experiment. Recently, IBM has announced the first commercial quantum computer, IBM Q System One [1]. Most papers in the area of quantum computing popularize the fact that our cryptographic primitives are in danger [2]. This is true, one important algorithm is the quantum algorithm for factorization. This algorithm can solve the problem of factorizing two integers in polynomial time, making all our current practical cryptography useless. Although quantum computers are a threat from the perspective of cryptography, there are also many advantages. One of these advantages is quantum communication. These type of communication are much faster than the classical counterparts. The major purpose of this paper is to offer an introduction to quantum communication. We will see how these type of communication are analogous with maritime flag communications. We will also offer an implementation of a quantum communication scheme using IBM Q composer.

1.1. Maritime flags

International maritime signal flags refer at a set of rules by which one or more flags are used to communicate messages between ships. Every day we listen to music from our radios in the car, traveling from home to work. We receive messages from our beloved ones on WhatsApp. We post our messages to our friends and to the world using Facebook or Twister. Taking all this into account, we may ask what is the purpose of communicating a message using signal flags? An old proverb says that “a picture worth a thousand words”. Communications by signal flags are used mostly in two cases: when there is a danger (e.g. men overboard) or when the radio cannot be useful (e.g. when the radio system is down or there is a necessity for maintaining radio silence). At sea, not all colors are easily

recognized but only a few of them. These are red, blue, yellow, black and white. The most used combinations of these colors are: red and white, yellow and blue, blue and white. There are 26 flags for each letter from the English alphabet. These are depicted in Figure 1.

Figure 1: Flags for letters

There are also 10 flags for each digit plus 3 flags symbolizing “first”, “second” and “third”. Those are depicted in Figure 2.

There is a major difference between flags signal communication and radio communication. The communication by flags can be “intercepted” only by those who see the flags. To see the flags, one ship must be in proximity of the ship which raised the flags. That means the ship which wants to communicate will always know who receive the message. On the other hand, in radio communications, multiple parties can intercept one communication without the transmitter knowing it. More technically we can say that flag communications cannot be intercepted without leaving any proof of that interception. We will see how can we achieve the same goal and more using quantum communications.

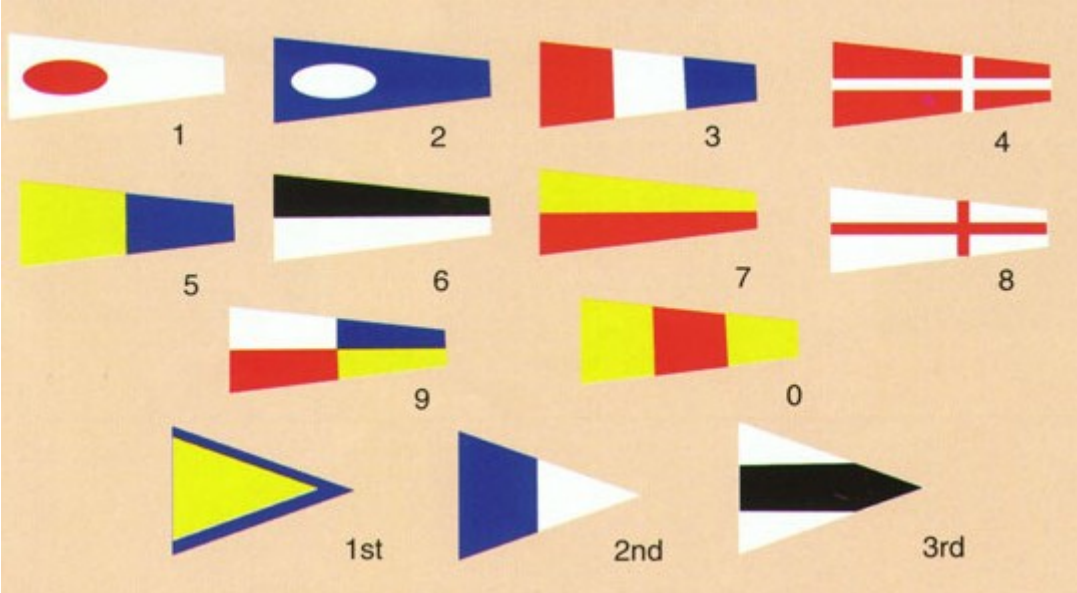

Figure 2: Flags for numbers

1.2. A short introduction into quantum computing

The playground of quantum computations is a Hilbert vector space [3]. That is vector space in which one can define the norm of a vector. The quantum analog of a classical bit is now a vector in a Hilbert space. This vector is called a qubit. Like all vector spaces, we must have a base. The most used basis in quantum computations is the $|0\rangle$ $|1\rangle$ basis. An arbitrary vector can be described in this basis as in equation (1).

$$|\psi\rangle = p_1|0\rangle + p_2|1\rangle \tag{1}$$

where $p_1$and $p_2$are complex numbers [4]. The vector $|\psi\rangle$ is not an arbitrary vector from a vector space. It describes a quantum state. For that reason, in order to model quantum effects, a restriction must be put on the numbers $p_1$and p_2. The restriction is the following:

$$p_1^2 + p_2^2 = 1 \tag{2}$$

This restriction comes naturally from the mathematical modeling of quantum superposition. To understand more intuitively what a quantum superposition is, let's consider the following example. Suppose we have an electron orbiting around the nucleus of an atom. Suppose that there are two possible states for that electron: the lower orbit and the upper orbit. We know from quantum physics that the electron can make a "step" from a lower orbit to the upper one or vice-versa. We also know that the electron will never make "half" of the step. When we measure the electron, we will find it into lower orbit or upper orbit but never in between. But what happens when we don't measure the electron. Is it in the state of lower orbit or in the state of upper orbit? The truth is that we don't know until we measure it. Before the measurement happens, we say the electron is in its lower orbit with the probability $p_1^2$and in its upper orbit with a probability of p_2^2. We can say from one point of view that the electron is in the same time in lower and upper orbit. This is the quantum superposition. We call the lower and upper orbit states, basis states. Linking this physical example with the mathematical modeling we obtain exactly what is described in the equations (1) and (2). A qubit is a quantum superposition. The basis states are often two vectors that we denote by $|0\rangle$and $|1\rangle$. When we measure a

qubit, we can obtain one of the two possible basis states. Basically, when measuring a qubit, one obtains a classical bit. The advantage of the qubit over its classical counterpart is the following: while a classical bit of information can take just two values (0 and 1), a qubit can take in theory an infinity of values (every combination of complex numbers $p_1$and $p_2$determines a qubit). We will see that in fact, we don't use an infinite number of combinations, but only a few of them. The state $\langle\psi|$can be described by the vector $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$when considering mathematical modeling.

Making a classical computation resumes at transforming one set of bits into another set of bits. By analogy, making a quantum computation resumes at transforming a qubit into another qubit. Mathematically, quantum computations can be described using unitary transformations from within a vector space. A unitary transformation can be described by a matrix for which the inverse is its transpose conjugate, that is:

$$UU^* = U^*U = I \tag{3}$$

where $U$is the matrix that describes the unitary transformation.

Looking at a unitary transformation we can say how the qubit is changing after the computation. For example, suppose we have a qubit in the basis state (the basis states are also known as ground states) $\langle 0|$. Let's consider the Hadamard transformation given by (4).

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4}$$

We can observe that the state $\langle 0|$ can be written as $\langle 0| = 1\langle 0| + 0\langle 1|$ and the state $\langle 1|$ can be written as $\langle 1| = 0\langle 0| + 1\langle 1|$, thus we can write the state $\langle 0|$ as the vector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and the state $\langle 1|$ as the vector $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

We can now see what is the effect of a Hadamard gate on a qubit originally in state $\langle 0|$.

$$\langle\psi| = H\langle 0| = \frac{1}{\sqrt{(2)}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{(2)}} \\ \frac{1}{\sqrt{(2)}} \end{pmatrix} \tag{6}$$

Applying a Hadamard gate to a qubit initially in the state $\langle 0|$ we obtain a qubit in the state $\langle\psi|$ as described in (6). Taking into consideration (1), when we measure this qubit we will obtain 0 with a probability of $\frac{1}{2}$ and 1 with the same probability. In practice, we can determine these probabilities by repeating the experiment a number of times after that we can calculate the frequencies of the results. On IBM Q Composer the corresponding circuit to equation (6) is depicted in Figure 3 [5].

Figure 3: The IBM Q Composer Circuit for a Hadamard gate

We have run the circuit from Figure 3 1000 time and we have the following frequencies described in Figure 4.

Figure 4: The distribution of results obtained by running the circuit from Figure 3

We can see that the above experiment is consistent with the theoretical result from (6).
Other quantum gates and their effects are depicted in Figure 5.

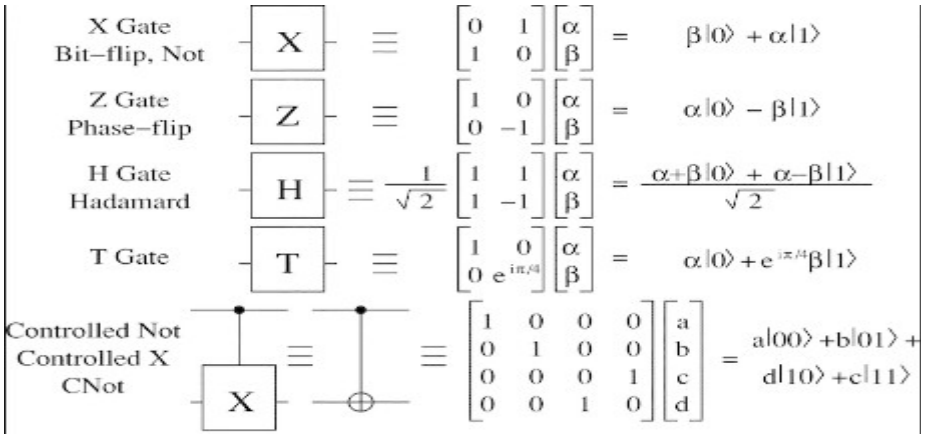

Figure 5: Quantum gates

One important quantum gate that acts on a system of two qubits is the C-NOT gate. This gate flips the second qubit when the first one is 1 and leave the system as it is whenever the first qubit is 0.

2. Superdense coding

Superdense coding represents a quantum communication method more efficient than classical communications. With this method, one party can send to another party two classical bits of information using just one qubit. It is necessary first to talk about a special quantum state, the Bell state [6].

2.1. Bell state

The Bell state or the entangled state is a special state of a quantum system consisting of two qubits. There are four Bell states described in equations (7)-(10) [7].

$$\langle \phi^1| = \frac{1}{\sqrt{(2)}}(\langle 00| + \langle 11|) \tag{7}$$

$$\langle \phi^2| = \frac{1}{\sqrt{(2)}}(\langle 00| - \langle 11|) \tag{8}$$

$$\langle \phi^3| = \frac{1}{\sqrt{(2)}}(\langle 01| + \langle 10|) \tag{9}$$

$$\langle \phi^4| = \frac{1}{\sqrt{(2)}}(\langle 01| - \langle 10|) \tag{10}$$

What is special at a Bell state is that when we measure one of the qubits we can say for sure what will be the value of the other qubit after measurement. For example, consider the state $\langle \phi^1|$. There is a probability of $\frac{1}{2}$ that the system is in the state $\langle 00|$ and a $\frac{1}{2}$ probability that the system is in the state $\langle 11|$.

Although the probability that the first is in the state $\langle 0|$, if we find the qubit in this state after measuring, we will know for sure that that the second qubit is also in that state $\langle 0|$. More intuitively, we can see this by looking at the equation (7) and see that we only have two possible combinations in which the system can be after measurement.

2.2. The coding algorithm

To describe the protocol, we will use two parties, Alice and Bob.

Step 1. Alice and Bob create two qubits in a Bell state. On qubit belongs to Alice and one to Bob.

Step 2. If Alice wishes to transmit the number $x \in \{0,1,2,3\}$, she will apply to her qubit the gate G_x where $G_0 = I, G_1 = Z, G_2 = X, G_3 = Z * X$.

Step 3. Alice will send her qubit to Bob

Step 4. Bob will apply to the system formed by Alice's qubit and his qubit a C-NOT gate with Alice's qubit as control qubit and his qubit as target qubit. After that, he will act with a Hadamard gate on Alice's qubit and measure the system. The result will encode the number x. For example, if Alice wanted to transmit the number 3 (in binary 10), when Bob measures the system he will find Alice's qubit in state 1 and his qubit in state 0.

The core of the protocol is the entangled state. We will now describe how to implement a Bell state on IBM Q. The circuit is depicted in Figure 6.

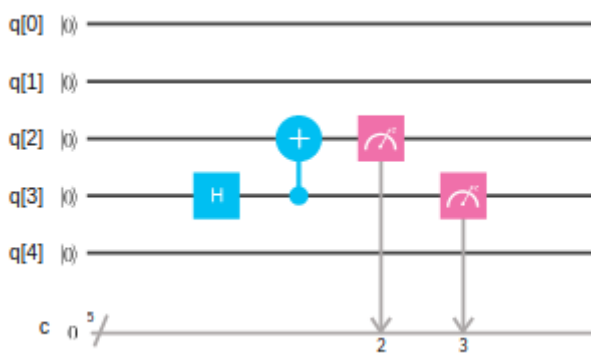

Figure 6: Bell circuit

If we run the circuit from Figure 6 1000 times, we obtain the statistics described in Figure 7.

Figure 7: The results of Bell circuit

We can see that we have obtained the state $|00\rangle$ within 50.4% cases and the state $|11\rangle$ in 49.6% cases.

This method of communication is similar to maritime flag communication. As we have stated in the previous section, in a maritime flag communication we can see who can intercept the communication. This is valid in superdense coding too. In order to decode the message, one party must have both qubits. That means, if a third entity wishes to determine what message Alice send, it will have to be in close proximity of Bob in order to manipulate his qubit. In a maritime flag communication, we do not have to encode the information using only two classical bits. As we have seen, we have a flag for each letter so we can transmit 26 symbols. In superdense coding, we are not limited at only 2 classical bits of information. Instead, we can use 4 symbols to encode our information.

3. Conclusions

In this paper, we wanted to provide a simple introduction to the quantum computing field. Although, at first sight, the maritime flag communications and superdense coding have nothing in common we have shown the opposite. Both forms of communication have in common the property that no one can intercept the communication without revealing its presence. We also wanted to show that quantum computing is no longer an experiment by providing some real circuit implementations on IBM Q Composer. The analogy between maritime flag communication and superdense coding shows how quantum information can be applied in a real-world situation. In this paper we don't claim any novelty on the scientific part, we just showed how to distance fields may be closer in unexpected ways.

References

[1] https://www.research.ibm.com/ibm-q/system-one/
[1] https://arxiv.org/abs/quant-ph/9508027
[2] http://mathworld.wolfram.com/HilbertSpace.html
[3] https://quantumexperience.ng.bluemix.net/qx/tutorial?page=002-Introduction~2F001-Introduction
[4] https://quantumexperience.ng.bluemix.net/qx/editor
[5] https://en.wikipedia.org/wiki/Superdense_coding
[6] https://quantumexperience.ng.bluemix.net/qx/tutorial?page=introduction