Asymptotical Information Bound of Consecutive Qubit Binary Testing

Anastasiia Varava and Grygoriy Zholtkevych

V.N. Karazin Kharkiv National University
School of Mathematics and Mechanics, 4, Svobody Sqr., 61022, Kharkiv, Ukraine
{nastia.varava,g.zholtkevych}@gmail.com

Abstract. The problem of estimating quantity of information, which can be obtained in the process of binary consecutive measuring a qubit state, is considered in the paper. The studied quantity is expressed as Shannon mutual information between the initial qubit state and the outcomes of a consecutive measurement. It is demonstrated that the maximum of information is reached by projective measurements. The maximum quantity of accessible information is calculated. It is proved that in the case of arbitrary binary test the maximum is reached asymptotically for consecutive measurements.

Keywords: Quantum information theory, quantum communication channels, accessible classical information, Shannon mutual information, pure qubit state, consecutive qubit binary testing.

1 Introduction

The theory of quantum information is a generalization of the classical information theory to the quantum world. Quantum information theory aimes to investigate what happens if information is stored in a state of a quantum system. By state of a physical system one means the mathematical description that provides a complete information on the system.

Talking about information from the point of view of quantum mechanics, we take into account some specific consequences of fundamental quantum postulates. The most important of them are the following: firstly, information, that is held in a state of a quantum system, cannot be read without changing the initial state. This property makes it largely inaccessible. Secondly, an arbitrary quantum state can not be cloned because of the no-cloning theorem. In other words, one can not create a perfect copy of the quantum system without already knowing its state in advance. And finally, quantum system can embody more information than classical, because a qubit can be in a superposition of basis state at the same time.

Industrial applications of quantum communication channels require developing sound methods for constructing them. It is well known that Shannon information theory is a mathematical background for such methods and the notion of Shannon mutual information [1,10] is a basic instrument for the classical theory

V. Ermolayev et al. (Eds.): ICTERI 2013, CCIS 412, pp. 93–111, 2013.

of communication. Thus, studying informational quantities for quantum communication channels is a very important problem for building quantum information theory.

One of the well-known problems in this context is the problem of obtaining information on a quantum state. Suppose that one experementalist prepares an individual particle in a particular physical state and then sends it to another experementalist, who is not aware of the preparation procedure, but wishes to determine the state of the particle. By making observations on the received particle, the second experementalist can obtain information about the physical state by observing how it interacts with other wellcharacterized systems, such as a measuring instrument. The amount of this information depends strongly on whether the particle is macroscopic or microscopic. In the macroscopic, classical case, one can observe the particle without disturbing it, and determine its state. In quantum mechanics, on the contrary, it is impossible to learn the quantum state of any individual physical system, because each observation will disturb its state. The amount of the achievable information on the quantum system will never be sufficient to determine the given state accurately. This is, in particular, the basis of quantum key distribution for cryptography. However, effective techniques of obtaining information on the quantum state are quite important for different applications. Such techniques can be used for characterizing optical signals, as well as in quantum computing and quantum information theory to estimate the actual states of the qubits.

Thus, the amount of accessible information on the quantum system is an important information-theoretic quantity. To study the possibility of obtaining information it is convenient to express it as Shannon mutual information between the qubit state and the outcomes of a measurement.

One of the first investigated problems with respect to the discussed quantity is the so-called problem of distinguishing quantum states. It consists of the following: suppose that quantum system is prepared in a state described by one of the density operators ρ_i $(i = 1,\ ...,\ n)$ with probability p_i. The goal is to determine which state is given using a single measurement of the considered quantum system. Thus, the task is to find measurements providing the maximum of Shannon mutual information. This problem was investigated by Holevo [5], Davies [3] and many others. Particularly, Holevo proved in [5] that obtainable information I is less or equal than the so-called Holevo bound

$$I \leq S\left(\sum_i p_i \rho_i\right) - \sum_i p_i S(\rho_i)\ ,$$

where $S(\rho) = \mathrm{Tr}(\rho \log \rho)$ is the von Neumann entropy. It follows that the amount of information obtainable by a single measurement never exceeds $\log(\dim \mathcal{H})$, where $\mathcal{H}$ is a state space of a quantum system. This result is fundamental for the above mentioned problem. The work on this question was then continued by many reserchers. In particular, in [2] its extension to sequential measurements based on the properties of quantum conditional and mutual entropies was presented.

A more general question, the problem of estimating the amount of accessible information about quantum states, was also studied by several researchers. In particular, in [11] the brief review of obtained results is given. In the chapter we continue this investigation by considering a particular case. Imagine that we do not have any preliminary information on the possible states of a quantum system. In this case all possible pure states are equiprobable, so, we can not work with a finite set of initial states. Assume also that we have in our disposal a single measuring instrument. How much classical information can we now obtain?

In the paper we consider the simplest case of this problem. Suppose we have an arbitrary pure qubit state and an instrument doing binary test of it. Assume that all possible initial states are equiprobable. Our aim is to obtain classical information on the qubit state using only the given measuring instrument. Certainly, we want to get as much classical information as possible. So, this time we investigate the amount of information accessible in this case.

It is well known that in the case of performing a single measurement the maximum of classical information is obtainable by a projective measurement. We present a simple proof of this fact. In addition, we calculate the maximum value of information and then we show that in the case of arbitrary measuring instrument this value can be attained asymptotically using consecutive testing.

This paper is organized as follows: in Section 2 the problem is set formally and the formula for Shannon mutual information of two random variables is obtained. The first one describes the density of the parameter of the initial state, and the second one corresponds to the measurement result. In Section 3 a special kind of measuring instrument which performs a projective measurement is considered. It is demonstrated that in this case we obtain the maximum of accessible information. Further, in Section 4, it is proved that in general case consecutive measurements provide to attain this value asymptotically.

2 Qubits and Their Binary Testing

In quantum computing, a qubit is the quantum analogue of the classical bit. Like a bit, a qubit has two basis states: $|0\rangle$ and $|1\rangle$. The difference is that a qubit can be in a superposition of the basis states at the same time. This means that a pure qubit state can be represented as a linear combination of $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\ ,$$

where a and b are probability amplitudes and can in general both be complex numbers such that $|a|^2 + |b|^2 = 1$.

More precisely, a pure state of a qubit is a unit vector $|\psi\rangle$ in 2-dimensional Hilbert space $\mathcal{H}_2$ over the field of complex number. As usual, a density matrix equalled the ortho-projector on the subspace $\mathbb{C} \cdot |\psi\rangle$ of $\mathcal{H}_2$ is used to represent the pure state described by the vector $|\psi\rangle$. This ortho-projector is denoted by $|\psi\rangle\langle\psi|$. Hence, one can get

$$|\psi\rangle\langle\psi| = (a\,|0\rangle + b\,|1\rangle)(\overline{a}\,\langle 0| + \overline{b}\,\langle 1|) = |a|^2\,|0\rangle\langle 0| + a\overline{b}\,|0\rangle\langle 1| + \overline{a}b\,|1\rangle\langle 0| + |b|^2\,|1\rangle\langle 1|\,.$$

If we denote $|a|^2$ and $|b|^2$ by p and q respectively then we can rewrite the previous formula in the following form

$$|\psi\rangle\langle\psi| = p\,|0\rangle\langle 0| + e^{i\alpha}\sqrt{pq}\,|0\rangle\langle 1| + e^{-i\alpha}\sqrt{pq}\,|1\rangle\langle 0| + q\,|1\rangle\langle 1|\,,$$

where $p + q = 1$, $0 \le \alpha < 2\pi$.
Now using the representation $p = \frac{1}{2} - \theta$, $q = \frac{1}{2} + \theta$ where $-\frac{1}{2} \le \theta \le \frac{1}{2}$ one can identify $|\psi\rangle\langle\psi|$ with the matrix

$$\rho(\theta,\alpha) = \begin{pmatrix} \dfrac{1}{2} - \theta & e^{i\alpha}\sqrt{\dfrac{1}{4} - \theta^2} \\ e^{-i\alpha}\sqrt{\dfrac{1}{4} - \theta^2} & \dfrac{1}{2} + \theta \end{pmatrix}. \qquad (1)$$

This matrix is called a density operator of the pure state.

In the general case a density operator for a qubit is a nonnegative definite operator on the space $\mathcal{H}_2$ such that its trace equals unity.

A binary test of a qubit is determined by a pair of operators $\{K(0), K(1)\}$ such that the equality $K(0)^\dagger K(0) + K(1)^\dagger K(1) = \mathbf{1}$ in the following meaning:

$$\begin{aligned} \Pr(0\,|\,\psi) &= \langle\psi|K(0)^\dagger K(0)|\psi\rangle \quad \text{and} \quad \Pr(1\,|\,\psi) = \langle\psi|K(1)^\dagger K(1)|\psi\rangle\,; \\ |\mathrm{Eff}(\psi\,|\,0)\rangle &= \frac{K(0)|\psi\rangle}{\sqrt{\langle\psi|K(0)^\dagger K(0)|\psi\rangle}} \quad \text{and} \quad |\mathrm{Eff}(\psi\,|\,1)\rangle = \frac{K(1)|\psi\rangle}{\sqrt{\langle\psi|K(1)^\dagger K(1)|\psi\rangle}}\,, \end{aligned}$$

where $|\psi\rangle$ describes the qubit state immediately before testing, $\Pr(s\,|\,\psi)$ is equal to obtain the outcome s as testing result, $|\mathrm{Eff}(\psi\,|\,s)\rangle$ describes the qubit state immediately after testing if the testing outcome equals s .

As known from theorem about polar decomposition [9, p. 28, Theorem 2.3] operators $K(0)$ and $K(1)$ can be represented as

$$K(0) = U(0)M(0)^{1/2} \text{ and } K(1) = U(1)M(1)^{1/2}\,, \qquad (2)$$

where $M(0) = K(0)^\dagger K(0)$ and $M(1) = K(1)^\dagger K(1)$, $U(0)$ and $U(1)$ are unitary operators.

In this chapter we consider a binary tests subclass only. Its members are characterised by the condition $U(0) = U(1) = \mathbf{1}$. Such a qubit binary test has studied in [6].

Thus, let us introduce the following definition.

Definition 1. *A pair of nonnegative definite operators* $\mathbf{T} = \{M_0, M_1\}$ *on* $\mathcal{H}_2$ *such that* $M_0 + M_1 = \mathbf{1}$ *is called a qubit binary test.*
Probabilities of test outcomes are given by the next formulae

$$\Pr(s\,|\,\psi) = \langle\psi|M(s)|\psi\rangle\,, \text{ where } s = 0,1 \text{ and } |\psi\rangle \text{ describes the state of a qubit immediately before testing.} \qquad (3)$$

The vector described the qubit state immediately after testing are given by the next formulae

$$|\mathrm{Eff}(\psi \mid s)\rangle = \frac{M(s)^{1/2}|\psi\rangle}{\sqrt{\Pr(s \mid \psi)}}\,, \quad \textit{where } s = 0, 1 \textit{ and } |\psi\rangle \textit{ describes the state of a qubit immediately before testing.} \tag{4}$$

The mathematical model of a qubit binary test is described and studied in [12].

3 Shannon Mutual Information between the Qubit State and the Outcomes of a Consecutive Measurement

To set the problem formally we firstly need some basic definitions. We use a density operator as a mathematical model of a qubit state and describe the considering pure state of a qubit by the corresponding density operator $\rho(\theta,\alpha)$ represented by the matrix $\rho(\theta,\alpha)$ (see formula (1)).

Let Θ be the equiprobability distribution on the segment $\left[-\frac{1}{2},\frac{1}{2}\right]$. It is used to model uncertainty of our knowledge about parameter θ for an initial state of the qubit.

Let $\mathcal{M}$ be a set of all possible qubit binary tests. Consider $\mathbf{T} \in \mathcal{M}$, $\mathbf{T} = \{M_0, M_1\}$. Let $\{|0\rangle, |1\rangle\}$ be the ortho-normal basis in $\mathcal{H}_2$ such that $|0\rangle$, $|1\rangle$ are eigenvectors of the operator M_0 corresponding to eigenvalues $0 \le m_1 \le m_2 \le 1$ respectively. In this case the operators M_0 and M_1 are represented in a such way:

$$M_0 = \begin{pmatrix} m_1 & 0 \\ 0 & m_2 \end{pmatrix}\,, \quad M_1 = \begin{pmatrix} 1-m_1 & 0 \\ 0 & 1-m_2 \end{pmatrix}\,.$$

Denote by $\Sigma = \{0,1\}$ the set of outcomes for the given qubit binary test. The probability distribution on this set is defined by the following formulae:

$$\Pr(0 \mid \rho) = \mathrm{Tr}(\rho \cdot M_0), \quad \Pr(1 \mid \rho) = \mathrm{Tr}(\rho \cdot M_1).$$

As we already mentioned, our aim is to obtain classical information value of the initial state as much as possible, using only the given instrument to measure. For this purpose we perform consecutive qubit binary testing. In other words, we repeat our measurement n times to observe the result of each iteration. After n iterations we obtain a sequence $\mathbf{x^{(n)}} = (x_1, \ldots, x_n)$, where $x_i \in \Sigma (i = 1,\ ...,\ n)$. As it is shown in [12],

$$\Pr(\mathbf{x^{(n)}} \mid \rho(\theta,\alpha)) = m_1^k(1-m_1)^{n-k}\left(\frac{1}{2}-\theta\right) + m_2^k(1-m_2)^{n-k}\left(\frac{1}{2}+\theta\right),$$

where k is a number of '1' in the outcomes sequence $\mathbf{x^{(n)}}$.

In further computations it is suitable to use some properties of Bernstein basis polynomials of degree n [8]:

$$B_{n,k}(z) = \binom{n}{k} z^k (1-z)^{n-k},$$

so, we rewrite the last equation as follows:

$$\Pr(\mathbf{x^{(n)}} \mid \rho(\theta,\alpha)) = \binom{n}{k}^{-1} \left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right).$$

Let $\mathbf{X^{(n)}} \in \{0,1\}^n$ be a random variable describing an outcomes sequence. The density of $\mathbf{X^{(n)}}$ with respect to Θ is defined by the following formula

$$p(\mathbf{x^{(n)}}|\theta) = \Pr(\mathbf{x^{(n)}} \mid \rho(\theta,\alpha)).$$

The main objective of this section is to compute Shannon mutual information [1,10] of random variables $\mathbf{X^{(n)}}$ and Θ. It is equal to

$$I(\mathbf{X^{(n)}};\Theta) = H(\mathbf{X^{(n)}}) - H(\mathbf{X^{(n)}}|\Theta), \tag{5}$$

where $H(\mathbf{X^{(n)}})$ is Shannon entropy of $\mathbf{X^{(n)}}$, and $H(\mathbf{X^{(n)}}|\Theta)$ is conditional entropy [1,10]:

$$H(\mathbf{X^{(n)}}|\Theta) = \int_{-\frac{1}{2}}^{\frac{1}{2}} H(\mathbf{X^{(n)}}|\Theta=\theta)d\theta .$$

Let us compute the marginal distribution of the random variable $\mathbf{X^{(n)}}$, which corresponds to the joint density function $p(\mathbf{x^{(n)}},\theta)$. The latter is described in a such way:

$$p(\mathbf{x^{(n)}},\theta) = \binom{n}{k}^{-1} \left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right) .$$

The marginal distribution $p(\mathbf{x^{(n)}})$ is defined as follows:

$$p(\mathbf{x^{(n)}}) = \int_{-\frac{1}{2}}^{\frac{1}{2}} p(\mathbf{x^{(n)}},\theta)d\theta = \binom{n}{k}^{-1} \left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\int_{-\frac{1}{2}}^{\frac{1}{2}} d\theta - \right.$$
$$\left.(B_{n,k}(m_1)-B_{n,k}(m_2))\int_{-\frac{1}{2}}^{\frac{1}{2}} \theta d\theta\right) = \binom{n}{k}^{-1} \frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2} .$$

Firstly, let us compute entropy of $\mathbf{X^{(n)}}$:

$$H(\mathbf{X^{(n)}}) = -\sum_{\mathbf{x^{(n)}}\in\{0,1\}^n} p(\mathbf{x^{(n)}})\log p(\mathbf{x^{(n)}}) = -\sum_{k=0}^{n}\binom{n}{k} p(\mathbf{x^{(n)}})\log p(\mathbf{x^{(n)}}) .$$

Substituting the expression of marginal distribution, we obtain

$$H(\mathbf{X^{(n)}}) = \sum_{k=0}^{n}\left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\right)\log\left(\binom{n}{k}\right) -$$
$$\sum_{k=0}^{n}\left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\right)\cdot\log\left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\right) . \tag{6}$$

Secondly, we can compute $H(\mathbf{X^{(n)}}|\Theta)$:

$$H(\mathbf{X^{(n)}}|\Theta) = -\int_{-\frac{1}{2}}^{\frac{1}{2}} H(\mathbf{X^{(n)}}|\Theta=\theta)d\theta = -\int_{-\frac{1}{2}}^{\frac{1}{2}} \sum_{k=0}^{n} \binom{n}{k} p(\mathbf{x^{(n)}}|\theta) \log p(\mathbf{x^{(n)}}|\theta) d\theta \ .$$

By direct calculations it is easy to check that

$$\begin{aligned} H(\mathbf{X^{(n)}}|\Theta) = &\sum_{k=0}^{n} \left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\right) \log\left(\binom{n}{k}\right) - \\ &\sum_{k=0}^{n} \int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right) \cdot \\ &\log\left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right) d\theta \ . \end{aligned} \tag{7}$$

Now, using (5), (6) and (7), one can obtain the expression for Shannon mutual information

$$\begin{aligned} I(\mathbf{X^{(n)}};\Theta) = &\sum_{k=0}^{n} \Bigg(\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right) \cdot \\ &\log\left(\left(\frac{1}{2}-\theta\right) B_{n,k}(m_1) + \left(\frac{1}{2}+\theta\right) B_{n,k}(m_2)\right) d\theta - \\ &\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2} \cdot \log\left(\frac{B_{n,k}(m_1)+B_{n,k}(m_2)}{2}\right)\Bigg) \ . \end{aligned}$$

It is easy to see that if k is such that $B_{n,k}(m_1) = B_{n,k}(m_2)$, then the corresponding summand is equal to zero:

$$\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(B_{n,k}(m_1) \cdot \log B_{n,k}(m_1)\right) d\theta - B_{n,k}(m_1) \cdot \log B_{n,k}(m_1) = 0 \ .$$

Note that in the case of equality $m_1 = m_2$ the polynomials $B_{n,k}(m_1)$ and $B_{n,k}(m_2)$ are equal for each k, so, we can not obtain any information about the initial state. Thus we futher consider the case $m_1 < m_2$.

Let $\mathbf{A_n}$ be a set of non-negative integers defined as follows:

$$\mathbf{A_n} = \{k \in \{0,\ ...,\ n\} | B_{n,k}(m_1) \neq B_{n,k}(m_2)\} \ .$$

Denote by $\overline{\mathbf{A_n}}$ the complement of the set $\mathbf{A_n}$, i.e. $\overline{\mathbf{A_n}} = \{0,\ ...,\ n\} \backslash \mathbf{A_n}$. Now we can consider only values of k from this set, but we keep on working with all summands. We demonstrate further that it is more suitable. Instead of omitting zero summands, let us present them in the following way:

$$0 = \left(B_{n,k}(m_1) - \frac{B_{n,k}(m_1)}{2\ln(2)} \right) - \frac{2\ln 2 - 1}{2\ln 2} \cdot B_{n,k}(m_1) \ .$$

Thus, we have

$$\begin{aligned} I(\mathbf{X^{(n)}};\Theta) = \sum_{k\in\mathbf{A_n}} \Bigg(\int_{-\frac{1}{2}}^{\frac{1}{2}} \left(\left(\frac{1}{2} - \theta\right) B_{n,k}(m_1) + \left(\frac{1}{2} + \theta\right) B_{n,k}(m_2) \right) \cdot \\ \log\left(\left(\frac{1}{2} - \theta\right) B_{n,k}(m_1) + \left(\frac{1}{2} + \theta\right) B_{n,k}(m_2) \right) d\theta - \\ \frac{B_{n,k}(m_1) + B_{n,k}(m_2)}{2} \cdot \log\left(\frac{B_{n,k}(m_1) + B_{n,k}(m_2)}{2} \right) \Bigg) + \\ \sum_{k\in\overline{\mathbf{A_n}}} \left(\left(B_{n,k}(m_1) - \frac{B_{n,k}(m_1)}{2\ln(2)} \right) - \frac{2\ln 2 - 1}{2\ln 2} \cdot B_{n,k}(m_1) \right) \ . \end{aligned}$$

After integration we obtain

$$\begin{aligned} I(\mathbf{X^{(n)}};\Theta) = \sum_{k\in\mathbf{A_n}} \Bigg(-\frac{B_{n,k}(m_1) + B_{n,k}(m_2)}{4\ln 2} + \\ \frac{B_{n,k}(m_2)^2 \log B_{n,k}(m_2) - B_{n,k}(m_1)^2 \log B_{n,k}(m_1)}{2(B_{n,k}(m_2) - B_{n,k}(m_1))} - \\ \frac{B_{n,k}(m_1) + B_{n,k}(m_2)}{2} \cdot \log\left(\frac{B_{n,k}(m_1) + B_{n,k}(m_2)}{2} \right) \Bigg) + \\ \sum_{k\in\overline{\mathbf{A_n}}} \left(\left(B_{n,k}(m_1) - \frac{B_{n,k}(m_1)}{2\ln(2)} \right) - \frac{2\ln 2 - 1}{2\ln 2} \cdot B_{n,k}(m_1) \right) \ . \end{aligned}$$

Taking into account that for k from the set $\overline{\mathbf{A_n}}$ the equality $B_{n,k}(m_1) = B_{n,k}(m_2)$ is held, we can rewrite this formula as follows:

$$\begin{aligned} I(\mathbf{X^{(n)}};\Theta) = \sum_{k=0}^{n} \frac{2\ln 2 - 1}{4\ln 2} (B_{n,k}(m_1) + B_{n,k}(m_2)) - \sum_{k\in\overline{\mathbf{A_n}}} \frac{2\ln 2 - 1}{2\ln 2} B_{n,k}(m_1) + \\ \sum_{k\in\mathbf{A_n}} \Bigg(\frac{B_{n,k}(m_2)^2 \log B_{n,k}(m_2) - B_{n,k}(m_1)^2 \log B_{n,k}(m_1)}{2(B_{n,k}(m_2) - B_{n,k}(m_1))} - \\ \frac{(B_{n,k}(m_1) + B_{n,k}(m_2)) \cdot \log\left(B_{n,k}(m_1) + B_{n,k}(m_2)\right)}{2} \Bigg) \ . \end{aligned}$$

Simplifying this expression and using the evident equality, $\sum_{k=0}^{n} B_{n,k}(z) = 1$, we get the following expression for mutual information:

$$I(\mathbf{X^{(n)}};\Theta) = \frac{2\ln 2 - 1}{2\ln 2} - \sum_{k \in \overline{\mathbf{A_n}}} \frac{2\ln 2 - 1}{2\ln 2} B_{n,k}(m_1) + \frac{1}{2} \cdot \sum_{k \in \mathbf{A_n}} \left(\frac{B_{n,k}(m_2)^2 \log B_{n,k}(m_2) - B_{n,k}(m_1)^2 \log B_{n,k}(m_1)}{(B_{n,k}(m_2) - B_{n,k}(m_1))} - \frac{(B_{n,k}(m_2)^2 - B_{n,k}(m_1)^2) \cdot \log(B_{n,k}(m_1) + B_{n,k}(m_2))}{(B_{n,k}(m_2) - B_{n,k}(m_1))} \right) . \quad (8)$$

4 Extremal Property of Projective Measurements

In this section we consider a special kind of measurement. Let $m_1 = 0$ and $m_2 = 1$. In this case the qubit binary test $\mathbf{T} = \{M_0, M_1\}$ looks as follows:

$$M_0 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} , \quad M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} .$$

The first interesting property of this measurement is its repeatability. Actually, note that $M_i \cdot M_j = \delta_{i,j} \cdot M_i$. So, M_0 and M_1 are orthoprojectors, and $\mathbf{T}$ is a projective measurement. Thus, in this case the repeated measurements give the same result. We demonstrate further that due to this property consecutive testing do not provide any extra information. The second and the most remarkable property is that we can obtain the maximum of the accessible information if and only if we use a projective measurement.

First of all let us compute the amount of information obtainable by the considering measurement. In the considered case we have only two values of k such that the corresponding polymomials $B_{n,k}(m_1)$ and $B_{n,k}(m_2)$ are not equal. So, $\mathbf{A_n} = \{0, n\}$, and

$$\forall k \in \overline{\mathbf{A_n}} : B_{n,k}(m_1) = B_{n,k}(m_2) = 0 .$$

Now using (8) it is easy to see that considering $m_1 = 0$ and $m_2 = 1$ we obtain

$$I(\mathbf{X^{(n)}};\Theta) = \frac{2\ln 2 - 1}{2\ln 2} .$$

Our next goal is to show that the obtained amount of information can not be reached using any other qubit binary test. For this purpose we investigate the function describing the accessible information (8).

At first let us rewrite this function in a more suitable way. Consider the general case, in which $0 < m_1 < m_2 < 1$. We will demonstrate futher that the exceptional cases, when $0 = m_1 < m_2 < 1$ or $0 < m_1 < m_2 = 1$, are similar to the latter.

Taking into account that in the general case $\forall k \in \{0, \ ..., \ n\}$ $B_{n,k}(m_1) > 0$, let us denote the ratio between $B_{n,k}(m_2)$ and $B_{n,k}(m_1)$ by a new function:

$$t_{n,k}(m_1, m_2) = \frac{B_{n,k}(m_2)}{B_{n,k}(m_1)} \ .$$

Thus, by direct calculations we obtain the following formula for mutual information:

$$I(\mathbf{X}^{(\mathbf{n})}; \Theta) = \frac{2\ln 2 - 1}{2\ln 2} - \frac{2\ln 2 - 1}{2\ln 2} \sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) - \frac{1}{2} \sum_{k \in \mathbf{A_n}} B_{n,k}(m_1) \cdot \left(\frac{t_{n,k}(m_1, m_2)^2 \cdot \log\left(\frac{t_{n,k}(m_1, m_2)}{t_{n,k}(m_1, m_2) + 1}\right) + \log\left(t_{n,k}(m_1, m_2) + 1\right)}{1 - t_{n,k}(m_1, m_2)} \right) . \quad (9)$$

Let $f(t)$ be a function defined as follows:

$$f(t) = \frac{t^2 \cdot \log\left(\frac{t}{t+1}\right) + \log(t+1)}{1 - t} \ .$$

Now it is easy to see that the formula (9) can be written as

$$I(\mathbf{X}^{(\mathbf{n})}; \Theta) = \frac{2\ln 2 - 1}{2\ln 2} - \left(\frac{2\ln 2 - 1}{2\ln 2} \sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) + \frac{1}{2} \sum_{k \in \mathbf{A_n}} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) \right) . \quad (10)$$

We claim that in the considered case ($0 < m_1 < m_2 < 1$) mutual information is less than

$$\frac{2\ln 2 - 1}{2\ln 2} \ .$$

To prove this fact it is enough to notice that the variable part of expression (10) is always negative. Actually, we know that $B_{n,k}(m_1) > 0$ and $t_{n,k}(m_1, m_2)$ is a ratio of two positive values, so, it is also positive. In addition, it is easy to show in the classical way that for all $t \in (0, 1) \cup (1, \infty)$ function $f(t)$ is greater than zero.

Now we need to consider the special case, in which $0 < m_1 < 1$, $m_2 = 1$. It is evident that the case when $m_1 = 0$, $0 < m_2 < 1$ is similar to the latter.

Suppose that $0 < m_1 < 1, m_2 = 1$. Thus, on the one hand, for all k we have $B_{n,k}(m_1) > 0$. On the other hand, for all $k < n$ $B_{n,k}(m_2) = 0$, and only for $k = n$ $B_{n,k}(m_2) = 1$. It is easy to see that in this case we obtain

$$I(\mathbf{X^{(n)}};\Theta) = \frac{2\ln 2 - 1}{2\ln 2} + \frac{1}{2}\cdot\left(\frac{B_{n,n}(m_2)^2 \log B_{n,n}(m_2) - (B_{n,n}(m_2)^2 - 1)\cdot\log\left(1 + B_{n,n}(m_2)\right)}{B_{n,n}(m_2) - 1}\right) = \frac{2\ln 2 - 1}{2\ln 2} - \frac{1}{2}\cdot f(B_{n,n}(m_2)) < \frac{2\ln 2 - 1}{2\ln 2} .$$

Thus, now we know that

$$I(\mathbf{X^{(n)}};\Theta) \le \frac{2\ln 2 - 1}{2\ln 2} ,$$

and, in particular, the equality is held if and only if the considered binary test is projective.

5 Asymptotic Properties of Consecutive Measurements

In the previous section we have considered the case when the given qubit binary test is a projective measurement. We have proved that only this type of measurement allows to achieve the maximum of information about the initial state. As far as the measurement is projective, repeating of the measuring procedure does not provide any extra information. In addition, we have found the maximum value of the accessible information:

$$\max_{\mathbf{T}\in\mathcal{M},\ n\in\mathbb{N}}\{I(\mathbf{X^{(n)}};\Theta)\} = \frac{2\ln 2 - 1}{2\ln 2} .$$

In this section we return to considering of the general view of a qubit test, and we work with consecutive qubit testing. So, this time we investigate the dependence of the amount of information on n – the number of iterations. The objective of this section is to prove that the maximum of accessible information can be reached asymptotically by performing consecutive measurements using an arbitrary qubit binary test.

More strictly, our aim is to prove the next theorem:

Theorem 1. *Suppose we have a pure qubit state and we perform consecutive qubit binary testing using the given test* $\mathbf{T} = \{M_1, M_2\}$*. Then for arbitrary* $\varepsilon > 0$ *there exists a corresponding number of iterations* $n(\varepsilon)$ *such that for all subsequent iterations* ($n > n(\varepsilon)$) *the following inequality is held:*

$$\max_{\mathbf{T}\in\mathcal{M},\ m\in\mathbb{N}}\{I(\mathbf{X^{(m)}};\Theta)\} - I(\mathbf{X^{(n)}};\Theta) < \varepsilon .$$

In other words, as far as the mutual information can be written as

$$I(\mathbf{X^{(n)}};\Theta) = \frac{2\ln 2 - 1}{2\ln 2} - \left(\frac{2\ln 2 - 1}{2\ln 2}\sum_{k\in\overline{\mathbf{A_n}}} B_{n,k}(m_1) + \frac{1}{2}\sum_{k\in\mathbf{A_n}} B_{n,k}(m_1)\cdot f(t_{n,k}(m_1,m_2))\right) ,$$

we need to find $n_1(\varepsilon)$ such that for all $n > n_1(\varepsilon)$

$$\sum_{k \in \mathbf{A_n}} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{2} , \tag{11}$$

and $n_2(\varepsilon)$ such that for all $n > n_2(\varepsilon)$

$$\sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) < \frac{\varepsilon}{2} . \tag{12}$$

Therefore, for $n > n(\varepsilon) = \max\{n_1(\varepsilon), n_2(\varepsilon)\}$ both of these inequalities are held.

Let us fix a certain positive value of ε. At first we consider the left side of inequality (11). Let us divide the set $\mathbf{A_n}$ into two non-intersecting subsets:

$$\mathbf{\Gamma_n}(m_1) = \{k \in \mathbf{A_n}\} : \left|\frac{k}{n} - m_1\right| < \tilde{\delta}(m_1, m_2) ,$$

$$\mathbf{\Delta_n}(m_1) = \{k \in \mathbf{A_n}\} : \left|\frac{k}{n} - m_1\right| \geq \tilde{\delta}(m_1, m_2) ,$$

where $\tilde{\delta}(m_1, m_2)$ is a certain positive function.

It was demonstrated in [8], that for $0 < m_1 < 1$ and $\delta > 0$:

$$\sum_{k \in \mathbf{\Delta_n}(m_1)} B_{n,k}(m_1) \leq \frac{1}{4n\delta^2} . \tag{13}$$

On the one hand, it is easy to see that $f(t)$ is a bounded function. Suppose that for all $t \in (0, 1) \cup (1, \infty)$ $f(t) < C$, where C is a certain positive constant. Thus we have

$$\sum_{k \in \mathbf{\Delta_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) \leq \frac{C}{4n\tilde{\delta}^2(m_1, m_2)} .$$

So, we can choose a value $n_{1,1}(\varepsilon)$ such that for all $n > n_{1,1}(\varepsilon)$

$$\sum_{k \in \mathbf{\Delta_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{4} .$$

On the other hand, we can see that when k is close to $n \cdot m_1$, the value of $t_{n,k}(m_1, m_2)$ goes to zero as n goes to infinity. As far as $\lim_{t \to 0} f(t) = 0$, there exists a value $n_{1,2}(\varepsilon)$ such that for all $n > n_{1,2}(\varepsilon)$

$$\sum_{k \in \mathbf{\Gamma_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{4} .$$

Now let $n_1(\varepsilon)$ be a maximum of values $n_{1,1}(\varepsilon)$ and $n_{1,2}(\varepsilon)$. Thus, for all $n > n_1(\varepsilon)$ inequality (11) is held.

Finally, let us consider inequality (12). Note that in the case of inequality $m_1 < m_2$ the set $\overline{\mathbf{A_n}}$ contains at most one element. Actually, by construction

$k \in \overline{\mathbf{A_n}}$ if and only if $B_{n,k}(m_1) = B_{n,k}(m_2)$. Solving this equation for the variable k, we have

$$k_0 = n \cdot \frac{\ln\left(\dfrac{1-m_1}{1-m_2}\right)}{\ln\left(\dfrac{(1-m_1)\cdot m_2}{(1-m_2)\cdot m_1}\right)}$$

If n, m_1 and m_2 are such that k_0 is an integer then $\overline{\mathbf{A_n}} = \{k_0\}$. If not, the set $\overline{\mathbf{A_n}}$ is empty. It is easy to show that $\lim\limits_{n\to\infty} B_{n,k}(m_1) = 0$, so, we can easily find $n_2(\varepsilon)$ such that for all $n > n_2(\varepsilon)$ inequality (12) is held.

Now let us build a rigorous proof of the considering statement using this heuristic consideration. To do it, we firstly need several trivial propositions.

Proposition 1. *The following statements are correct:*

1. *for all* $x \in (0,1)$ *the inequality*

$$x > \ln(x+1)$$

is true;

2. *for all* $x > 0$ *the inequality*

$$\ln\left(\frac{x}{x+1}\right) < -\frac{1}{x+1}$$

is true too.

Proof. Consider the first statement. One can directly obtain it using the Tailor series expansion of $\ln(x+1)$:

$$\ln(x+1) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n = x + \sum_{n=1}^{\infty} x^{2n}\left(\frac{x}{2n+1} - \frac{1}{2n}\right) <$$

$$x + \sum_{n=1}^{\infty} x^{2n}\left(\frac{1}{2n+1} - \frac{1}{2n}\right) < x$$

Now let us prove the second statement. By using Euler's transform on Tailor series expansion shown above, we have

$$\ln\frac{\tilde{x}}{\tilde{x}-1} = \sum_{n=1}^{\infty} \frac{1}{n\tilde{x}^n} > \frac{1}{\tilde{x}}$$

for every $|\tilde{x}| > 1$.

Let $\tilde{x} = x + 1$, then $|\tilde{x}| > 1$ and

$$\ln\frac{x+1}{x} > \frac{1}{x+1},$$

so,

$$\ln\frac{x}{x+1} < -\frac{1}{x+1}.$$

□

Proposition 2. *Let $x, y \in (0,1)$ and $x \neq y$ then the following inequality is held:*

$$\left(\frac{x}{y}\right)^y \left(\frac{1-x}{1-y}\right)^{(1-y)} < 1 \;.$$

Proof. Let $g(x) = x^c \cdot (1-x)^{(1-c)}$ be a function of $x \in (0,1)$, where $c \in (0,1)$ is a certain constant. It is easy to prove in a standart way that

$$\max_{x \in (0,1)} g(x) = g(c)$$

Let $c = y$. Then for $x \neq y$:

$$x^y \cdot (1-x)^{(1-y)} < y^y \cdot (1-y)^{(1-y)},$$

so,

$$\left(\frac{x}{y}\right)^y \left(\frac{1-x}{1-y}\right)^{(1-y)} < 1.$$

□

Now we can prove the above formulated theorem.

Proof (of Theorem 1). As we already know, the mutual information can be presented as

$$I(\mathbf{X}^{(\mathbf{n})}; \Theta) = \frac{2\ln 2 - 1}{2\ln 2} - \left(\frac{2\ln 2 - 1}{2\ln 2} \sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) + \right.$$
$$\left. \frac{1}{2} \sum_{k \in \mathbf{A_n}} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) \right) \;.$$

We also know that

$$\max_{\mathbf{T} \in \mathcal{M},\; n \in \mathbb{N}} \{ I(\mathbf{X}^{(\mathbf{n})}; \Theta) \} = \frac{2\ln 2 - 1}{2\ln 2} \;.$$

To prove the theorem it is enough to show that there exists $n(\varepsilon)$ such that for all $n > n(\varepsilon)$

$$\sum_{k \in \mathbf{A_n}} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) + \sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) < \varepsilon \;.$$

Consider an arbitrary $\varepsilon > 0$. Let us divide the set $\mathbf{A_n}$ into subsets $\mathbf{\Gamma_n}(m_1)$ and $\mathbf{\Delta_n}(m_1)$ in the following way:

$$\mathbf{\Gamma_n}(m_1) = \{k \in \mathbf{A_n}\} : \left| \frac{k}{n} - m_1 \right| < \tilde{\delta}(m_1, m_2) \;,$$

$$\mathbf{\Delta_n}(m_1) = \{k \in \mathbf{A_n}\} : \left| \frac{k}{n} - m_1 \right| \geq \tilde{\delta}(m_1, m_2) \;,$$

where $\tilde{\delta}(m_1, m_2)$ is a certain positive function of m_1 and m_2 defined further. Our aim is to prove that there exists such $n(\varepsilon)$ that for all $n > n(\varepsilon)$:

$$\sum_{k \in \mathbf{\Delta_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{4}\ , \tag{14}$$

$$\sum_{k \in \mathbf{\Gamma_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{4}\ , \tag{15}$$

$$\sum_{k \in \overline{\mathbf{A_n}}} B_{n,k}(m_1) < \frac{\varepsilon}{2}\ . \tag{16}$$

Firstly, let us consider inequality (14). We had already mentioned that for all $t \in (0, 1) \cup (1, \infty)$ $f(t) \geq 0$, and it is easy to see that for considered values of t $f(t) < 2$. So, using the above mentioned property of Bernstein basis polynomials (13), we have:

$$\sum_{k \in \mathbf{\Delta_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) \leq \frac{1}{2n\tilde{\delta}^2(m_1, m_2)}\ .$$

Let $n_{1,1}(\varepsilon)$ be sufficiently great. Then for all $n > n_{1,1}(\varepsilon)$ the considering inequality (14) is held.

Secondly, let us consider inequality (15). On the one hand, it is not hard to find such $\delta(\varepsilon)$ that

$$\forall t \in (0, \delta(\varepsilon)):\ \ f(t) = \frac{t^2 \cdot \log\left(\dfrac{t}{t+1}\right) + \log(t+1)}{1-t} < \frac{\varepsilon}{4}\ .$$

On the other hand, for sufficiently great values of n for all $k \in \mathbf{\Gamma_n}(m_1)$ we have $t_{n,k}(m_1, m_2) < \delta(\varepsilon)$. It follows that for great values of n we obtain

$$\sum_{k \in \mathbf{\Gamma_n}(m_1)} B_{n,k}(m_1) \cdot f(t_{n,k}(m_1, m_2)) < \frac{\varepsilon}{4} \cdot \sum_{k=0}^{n} B_{n,k}(m_1) = \frac{\varepsilon}{4}\ .$$

Let $\delta(\varepsilon) = \min\left(\frac{\sqrt{1+(\varepsilon/2\cdot\ln(2))^2}-1}{\varepsilon/2\cdot\ln(2)}; \frac{1}{2}\right)$. Then for $t \in (0,\ \delta(\varepsilon))$ we have

$$t < \frac{\varepsilon \cdot \ln(2)}{4}(1 - t^2).$$

As far as $0 < t \leq \frac{1}{2} < 1$, we obtain

$$\frac{t - \frac{t^2}{t+1}}{(1-t)\cdot\ln(2)} = \frac{t}{(1-t^2)\cdot\ln(2)} < \frac{\varepsilon}{4}\ .$$

If we combine this with Proposition 1, then for all $t \in (0, \delta(\varepsilon))$ we have

$$f(t) = \frac{t^2 \cdot \ln\left(\frac{t}{t+1}\right) + \ln(t+1)}{(1-t) \cdot \ln(2)} < \frac{t + t^2 \cdot \left(-\frac{1}{t+1}\right)}{(1-t) \cdot \ln(2)} = \frac{t - \frac{t^2}{t+1}}{(1-t) \cdot \ln(2)} < \frac{\varepsilon}{4} \, .$$

Now we need to find such $n_{1,2}(\varepsilon)$ that for all $k \in \mathbf{\Gamma_n}(m_1) : t_{n,k}(m_1, m_2) < \delta(\varepsilon)$. By definition,

$$t_{n,k}(m_1, m_2) = \left(\frac{m_2}{m_1}\right)^k \cdot \left(\frac{1-m_2}{1-m_1}\right)^{n-k} \, .$$

As far as $\frac{m_2}{m_1} > 1$, $t_{n,k}(m_1, m_2)$ strictly increases with respect to k. So, if $\left|\frac{k}{n} - m_1\right| < \tilde{\delta}(m_1, m_2)$ then

$$t_{n,k}(m_1, m_2) < \left(\left(\frac{m_2}{m_1}\right)^{m_1 + \tilde{\delta}(m_1,m_2)} \cdot \left(\frac{1-m_2}{1-m_1}\right)^{1-m_1-\tilde{\delta}(m_1,m_2)}\right)^n \, .$$

Consider the right side of this inequality. Note that

$$\left(\frac{m_2}{m_1}\right)^{m_1 + \tilde{\delta}(m_1,m_2)} \cdot \left(\frac{1-m_2}{1-m_1}\right)^{1-m_1-\tilde{\delta}(m_1,m_2)}$$

srtictly increases with respect to $\tilde{\delta}(m_1, m_2)$. It is equal to 1 when $\tilde{\delta}(m_1, m_2) = \tilde{\delta}^*(m_1, m_2)$, where

$$\tilde{\delta}^*(m_1, m_2) = \left(\frac{\ln\left(\frac{1-m_2}{1-m_1}\right)}{\ln\left(\frac{(1-m_2) \cdot m_1}{(1-m_1) \cdot m_2}\right)} - m_1\right) \, .$$

According to Proposition 2,

$$\left(\frac{m_2}{m_1}\right)^{m_1} \cdot \left(\frac{1-m_2}{1-m_1}\right)^{1-m_1} < 1 \, ,$$

we see that for $\tilde{\delta}(m_1, m_2) \in (0, \tilde{\delta}^*(m_1, m_2))$ we have

$$\left(\frac{m_2}{m_1}\right)^{m_1 + \tilde{\delta}(m_1,m_2)} \cdot \left(\frac{1-m_2}{1-m_1}\right)^{1-m_1-\tilde{\delta}(m_1,m_2)} < 1 \, .$$

Let

$$\tilde{\delta}(m_1, m_2) = \frac{\tilde{\delta}^*(m_1, m_2)}{2}.$$

Now it is easy to put $n_{1,2}(\varepsilon)$ such that for all $n > n_{1,2}(\varepsilon)$ inequality (15) is held.

Finally, let us find such $n_2(\varepsilon)$ that for $n > n_2(\varepsilon)$ condition (16) is satisfied. We have already seen that $|\overline{\mathbf{A_n}}| \leq 1$, and the equality is held when

$$k_0 = n \cdot \frac{\ln\left(\dfrac{1-m_1}{1-m_2}\right)}{\ln\left(\dfrac{(1-m_1)\cdot m_2}{(1-m_2)\cdot m_1}\right)}$$

is an integer. Let us denote the right side as $n \cdot c(m_1, m_2)$ and write k_0 as $k_0 = n \cdot c(m_1, m_2)$.

Referring to the standard way of proving the Stirling's formula, we can write the following inequality:

$$\sqrt{2\pi n} \cdot \left(\frac{n}{e}\right)^n \leq n! \leq e \cdot \sqrt{n} \cdot \left(\frac{n}{e}\right)^n .$$

It follows that

$$\binom{n}{k} \leq \frac{e}{2\pi}\sqrt{\frac{n}{k(n-k)}} \cdot \left(\frac{n}{k}\right)^k \cdot \left(\frac{n}{n-k}\right)^{n-k} .$$

So, it is now easy to see that

$$B_{n,k}(m_1) \leq \frac{e}{2\pi}\sqrt{\frac{n}{k(n-k)}} \cdot \left(\frac{n \cdot m_1}{k}\right)^k \cdot \left(\frac{n\cdot(1-m_1)}{n-k}\right)^{n-k} .$$

Substituting $k_0 = n \cdot c(m_1, m_2)$ for k in the last inequality, we get

$$B_{n,k_0}(m_1) \leq \frac{e}{2\pi}\sqrt{\frac{1}{n \cdot c(m_1,m_2)(1-c(m_1,m_2))}} \cdot \left(\left(\frac{m_1}{c(m_1,m_2)}\right)^{c(m_1,m_2)} \cdot \left(\frac{1-m_1}{1-c(m_1,m_2)}\right)^{1-c(m_1,m_2)}\right)^n . \tag{17}$$

It follows from Proposition 2 that

$$\left(\frac{m_1}{c(m_1,m_2)}\right)^{c(m_1,m_2)} \cdot \left(\frac{1-m_1}{1-c(m_1,m_2)}\right)^{1-c(m_1,m_2)} < 1 .$$

Now using (17) it is not hard to put $n_2(\varepsilon)$ such great that for $n > n_2(\varepsilon)$ inequality (16) is held.

Finally, let $n(\varepsilon) = \max\{n_{1,1}(\varepsilon), n_{1,2}(\varepsilon), n_2(\varepsilon)\}$. Now for all $n > n(\varepsilon)$

$$\max_{\mathbf{T}\in\mathcal{M},\ m\in\mathbb{N}}\{I(\mathbf{X^{(m)}};\Theta)\} - I(\mathbf{X^{(n)}};\Theta) < \varepsilon .$$

The theorem is proved. □

6 Conclusions

In the paper the problem of obtaining classical information about the pure qubit state using a single qubit binary test has been considered. It has been demonstrated that the maximum of information is reached if and only if the using measurement is projective. The maximum value of information has been calculated:

$$\max_{\mathbf{T}\in\mathcal{M},\, n\in\mathbb{N}} \left\{ I(\mathbf{X}^{(\mathbf{n})};\Theta) \right\} = \frac{2\ln 2 - 1}{2\ln 2}\,.$$

It follows, in particular, that to distinguish two arbitrary pure qubit states using a single binary test it is necessary to have at least four pairs of qubits prepared in the considered states.

It has been shown that the maximum of reachable information can be attained asymptotically using an arbitrary consecutive qubit binary test. Thus, if we have a certain measuring instrument performing a qubit binary test, we can obtain an amount of information arbitrary close to the maximum.

As known [4,7], Yu. Manin and R. Feynman proposed to use quantum systems to simulate others quantum systems. The results obtained in the paper show that this idea should be refined: one should take into account all dependences between an input data, a behaviour of a simulating system, and a structure of an output data.

Our further research will deal with generalizing results of the paper for the case of an n-level quantum system and a measurement with m outcomes.

References

1. Cover, T.M., Thomas, J.A.: Elements of Information Theory. John Wiley & Sons, Inc. (1991)
2. Cerf, N.J., Adami, C.: Accessible information in quantum measurement Caltech. Kellogg Lab & Santa Barbara. KITP & UC, Santa Barbara (1996)
3. Davies, E.B.: Information and Quantum Measurement. IEEE Trans. Inf. Theory IT-24, 596–599 (1978)
4. Feynman, R.P.: Simulating Physics with Computer. Int. J. Theor. Phys. 21, 467–488 (1982)
5. Holevo, A.S.: Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. Problemy Peredachi Informatsii 9(3), 3–11 (1973) (in Russian)
6. Holevo, A.S.: Statistical Structure of Quantum Theory. Springer, Berlin (2001)
7. Manin, Y.I.: Mathematics as metaphor: selected essays of Yuri I. Manin. AMS (2007)
8. Natanson, I.P.: Constructive function theory, vol. 1. Ungar, New York (1964)
9. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information, 10th Anniversary edn. Cambridge University Press, Cambridge (2010)
10. Shannon, C.E., Weaver, W.: The Mathematical Theory of Communication. University of Illinois Press, Urbana (1949)

11. Suzuki, J., Assad, S.M., Englert, B.-G.: Mathematics of Quantum Computation and Quantum Technology. In: Chen, G., Lomonaco, S.J., Kauffman, L. (eds.) Accessible information about quantum states: An open optimization problem. ch. 11. Chapman & Hall/CRC, Boca Raton (2007)
12. Thawi, M., Zholtkevych, G.M.: About One Model of Consecutive Qubit Binary Testing. Bull. Khark. Nat. Univ. 890(13), 71–81 (2010)