

Upper bounds on the accuracy of an assisted classical channel

Brett Hemenway,^{1,*} Carl A. Miller,^{2,†} Yaoyun Shi,^{2,‡} and Mary Wootters^{1,§}

¹*Mathematics Department, University of Michigan, Ann Arbor, MI 48109, USA*

²*Dept. of Electrical Engineering and Computer Science,
University of Michigan, Ann Arbor, MI 48109, USA*

(Dated: January 10, 2012)

If Alice attempts to communicate a single bit to Bob over a noisy classical channel, the *one-shot success probability* is the probability that Bob correctly receives this bit. It has recently been shown that the one-shot success probability can be increased if Alice and Bob share non-signaling correlations or entanglement. We investigate the limitations of this assistance. We provide tight upper bounds on the amount that a non-signaling correlation can increase the one-shot success probability. In the case of binary correlations, we extend these to tight upper bounds on the entanglement-assisted one-shot success probability.

If two parties, Alice and Bob, communicate over a classical channel \mathcal{N} , neither shared entanglement [1] nor the assistance of non-signaling correlations [2] can increase the classical capacity of the channel. However, recent work has shown that other notions of capacity can be increased [2–4]. Previous work on entanglement or non-signaling enhanced communication over classical channels has focused on the (one-shot) zero error capacity, which measures the number of different messages Alice can send to Bob perfectly. The non-signaling enhanced zero error capacity can be written as the solution to linear programs [2, 5]. In the quantum setting, upper bounds are known for the entanglement assisted zero error capacity [6]; these bounds are often the best bounds available in the unassisted case, suggesting that there are strong limitations to the amount of assistance that entanglement can provide.

A dual notion to that of one-shot zero error capacity is one-shot success probability, which measures the probability of success when Alice tries to send a message to Bob with a single use of the channel. The one-shot success probability has been considered before. In [5], a formula is derived for the best non-signaling assisted one-shot success probability for a fixed channel. In [4], Prevedel et al give an example of a channel where the unassisted, entanglement-assisted, and non-signaling assisted one-shot success probabilities are all different. In light of these results, it is natural to ask how large the gaps between these different success probabilities can be—that is, how much can entanglement or non-signaling correlations aid Alice and Bob? It is known that entanglement cannot be completely helpful: if the unassisted success probability is less than one, then so is the entanglement assisted success probability [2]. How much shared entanglement can improve the success probability has remained open, and while the optimal non-signaling-assisted success rate can be written as the solution to a linear program, this gap has not been explicitly bounded.

In this work, we prove a bound on the amount of assistance that non-signaling correlations can provide. We

prove that the ratio

$$\frac{\text{Succ}_{NS}(\mathcal{N}) - \frac{1}{2}}{\text{Succ}(\mathcal{N}) - \frac{1}{2}} \quad (1)$$

is always less than or equal to 2 (where $\text{Succ}(\mathcal{N})$ and $\text{Succ}_{NS}(\mathcal{N})$ denote the unassisted and non-signalling assisted one-shot success probabilities, respectively). We also demonstrate a family of examples which show that this ratio can be made arbitrarily close to 2, thus showing that our bound is optimal. Then we prove a similar tight bound on the amount of assistance that can be provided by binary quantum correlations (Theorem 3).

Terminology and Notation. Alice’s goal is to send a bit a to Bob over the classical channel \mathcal{N} with input alphabet \mathcal{X} and output alphabet \mathcal{Y} . Alice and Bob are assisted by the bipartite correlation \mathcal{D} . The component D_1 of \mathcal{D} accepts bits as input and returns elements of \mathcal{X} as output. The component D_2 accepts elements of \mathcal{Y} as inputs and returns bits as outputs. Bob will choose a bit, b , which represents his guess at Alice’s message a . The protocol succeeds if $a = b$.

We will denote random variables by capital letters. The letters X , Y , A , and B will denote random variables whose ranges are, respectively, \mathcal{X} , \mathcal{Y} , $\{0,1\}$, and $\{0,1\}$.

The simplest way for Alice and Bob to use \mathcal{D} to assist with communication over \mathcal{N} is the following protocol (shown in Figure 1). Let A denote Alice’s message.

Protocol 1:

1. Alice gives the bit A as input to D_1 .
2. Alice sends the output X from D_1 across \mathcal{N} .
3. Bob gives the element Y he receives from \mathcal{N} as input to D_2 .
4. Bob treats the output bit B from D_2 as his received message.

We will denote by D_{ay}^{xb} the conditional probability that Alice receives x and Bob receives b given their respective inputs a and y .

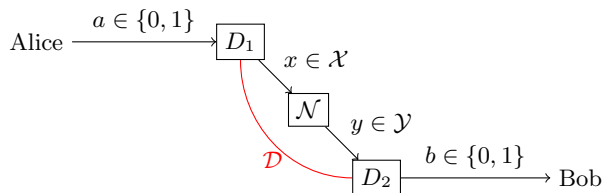


FIG. 1. Alice and Bob communicate over \mathcal{N} , with assistance from the correlation \mathcal{D} .

A correlation is *non-signaling* if Alice's output is independent of Bob's input and vice-versa:

$$D_{ay}^{x*} = D_{a*}^{x*} \text{ and } D_{ay}^{*b} = D_{*y}^{*b}.$$

A correlation is *local-deterministic* if it can be specified simply by a pair of functions $f: \{0,1\} \rightarrow \mathcal{X}$, $g: \mathcal{Y} \rightarrow \{0,1\}$. A correlation is *local* if it is a convex combination of local-deterministic distributions.

For any non-signaling correlation \mathcal{H} , let $\text{Succ}_{\mathcal{H}}(\mathcal{N})$ denote the probability of a successful bit transmission when \mathcal{H} is used to assist \mathcal{N} via Protocol 1. Let $\text{Succ}(\mathcal{N})$ denote the optimal unassisted success probability for a bit-transmission across \mathcal{N} . (The latter quantity is equal to the maximum of $\text{Succ}_{\mathcal{L}}(\mathcal{N})$ over all local-deterministic distributions \mathcal{L} .)

Non-Signaling Correlations. Here, we will prove a bound on the quantity $\text{Succ}_{\mathcal{D}}(\mathcal{N})$ in terms of $\text{Succ}(\mathcal{N})$. Our proof is based on relating protocols that require non-signaling assistance to protocols that do not. Let us consider the following protocol.

Protocol 2:

1. Alice chooses an element $t \in \mathcal{X}$.
2. Alice flips a coin to obtain an additional bit, C . She uses this bit as input to D_1 .
3. Alice compares C and A . If these two bits agree, then Alice uses the output X from D_1 as input to channel \mathcal{N} . Otherwise, Alice gives the letter t as input to \mathcal{N} .
4. Bob uses the output of \mathcal{N} as input to D_2 , and treats the output of D_2 as his received message.

We can directly calculate the success probability of this protocol. In the event that $C = A$, the probability of a successful transmission is equal to $\text{Succ}_{\mathcal{D}}(\mathcal{N})$. On the other hand, in the event that $C \neq A$, the received bit B is entirely independent of A , and therefore the probability of a successful transmission is $1/2$. Therefore, the success probability for Protocol 2 is

$$\frac{1}{4} + \frac{1}{2} \cdot \text{Succ}_{\mathcal{D}}(\mathcal{N}). \quad (2)$$

Now, observe that Protocol 2 can be simulated using shared randomness. (Alice and Bob can communicate beforehand and establish shared random variables (C', X')

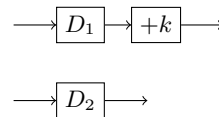


FIG. 2. The correlation $\mathcal{D}[k]$.

whose joint distribution is identical to the joint distribution (C, X) that Alice would obtain if she were to use the device D_1 . Alice and Bob can then use C' and X' to simulate the protocol.) Therefore the success probability (2) cannot exceed the unassisted success probability $\text{Succ}(\mathcal{N})$. This implies

$$\left[\text{Succ}_{\mathcal{D}}(\mathcal{N}) - \frac{1}{2} \right] \leq 2 \cdot \left[\text{Succ}(\mathcal{N}) - \frac{1}{2} \right]. \quad (3)$$

The following result, which is a strengthening of (3), is based on a more complex version of the reasoning above.

Theorem 1. *The quantity $\text{Succ}_{\mathcal{D}}(\mathcal{N})$ satisfies*

$$\left[\text{Succ}_{\mathcal{D}}(\mathcal{N}) - \frac{1}{2} \right] \leq 2 \left(1 - \frac{1}{|\mathcal{X}|} \right) \left[\text{Succ}(\mathcal{N}) - \frac{1}{2} \right].$$

Proof. We may assume, without loss of generality, that the set \mathcal{X} is equal to $\mathbb{Z}/r\mathbb{Z}$ for some $r \geq 1$. Let us define a series of correlations $\mathcal{D}[0], \mathcal{D}[1], \dots, \mathcal{D}[r-1]$ by

$$(D[k])_{ay}^{xb} = D_{ay}^{(x-k)b}. \quad (4)$$

(See Figure 2.)

Let $\mathcal{D}' = (\mathcal{D}[0] + \mathcal{D}[1] + \dots + \mathcal{D}[r-1]) / r$. Consider the quantity $\text{Succ}_{\mathcal{D}'}(\mathcal{N})$. When Protocol 1 is applied with \mathcal{D}' , the input X to channel \mathcal{N} is completely independent of Alice's message. As a consequence, $\text{Succ}_{\mathcal{D}'}(\mathcal{N}) = \frac{1}{2}$. By linearity,

$$\frac{\sum_{k \in \mathcal{X}} \text{Succ}_{\mathcal{D}[k]}(\mathcal{N})}{r} = \frac{1}{2}. \quad (5)$$

Consider the quantity $\min_{k \in \mathcal{X}} \text{Succ}_{\mathcal{D}[k]}(\mathcal{N})$. As a consequence of (5), we have

$$\min_{k \in \mathcal{X}} \text{Succ}_{\mathcal{D}[k]}(\mathcal{N}) - \frac{1}{2} \leq \frac{-1}{r-1} \left[\text{Succ}_{\mathcal{D}}(\mathcal{N}) - \frac{1}{2} \right]. \quad (6)$$

Consider the following protocol.

Protocol 3:

1. Alice chooses an element $s \in \mathcal{X}$ which is such that the quantity $\text{Succ}_{\mathcal{D}[s]}(\mathcal{N})$ is minimized.
2. Alice flips a coin to obtain a new bit, C . She uses this bit as input to D_1 , and obtains output X .
3. Alice compares C and A . If these two bits agree, then Alice uses X as the input to channel \mathcal{N} . Otherwise, Alice uses $(X + s)$ as the input to \mathcal{N} .
4. Bob uses the output of \mathcal{N} as input to D_2 , and treats the output of D_2 as his received message.

In the event that $A = C$, the probability of success of this protocol is $\text{Succ}_{\mathcal{D}}(\mathcal{N})$. In the event that $A \neq C$, the probability of success is $1 - \text{Succ}_{\mathcal{D}[s]}(\mathcal{N})$. Thus, the success probability of Protocol 3 is

$$\frac{1}{2} \cdot \text{Succ}_{\mathcal{D}}(\mathcal{N}) + \frac{1}{2} \cdot [1 - \text{Succ}_{\mathcal{D}[s]}(\mathcal{N})]. \quad (7)$$

Applying (6), we find that

$$\begin{aligned} & \frac{1}{2} \cdot \text{Succ}_{\mathcal{D}}(\mathcal{N}) + \frac{1}{2} \cdot [1 - \text{Succ}_{\mathcal{D}[s]}(\mathcal{N})] \\ & \geq \frac{1}{2} + \left[\frac{1}{2} + \frac{1}{2(r-1)} \right] \cdot \left(\text{Succ}_{\mathcal{D}}(\mathcal{N}) - \frac{1}{2} \right). \end{aligned} \quad (8)$$

Additionally, Protocol 3 (like Protocol 2) can be simulated using only shared randomness. Therefore the success probability of Protocol 3 cannot be any larger than $\text{Succ}_{\mathcal{D}}(\mathcal{N})$. From (8), we must have

$$\frac{1}{2} + \left[\frac{1}{2} + \frac{1}{2(r-1)} \right] \cdot \left(\text{Succ}_{\mathcal{D}}(\mathcal{N}) - \frac{1}{2} \right) \leq \text{Succ}(\mathcal{N}).$$

The desired result follows by an algebraic manipulation. \square

Optimality. We will now discuss an example in which equality occurs in Theorem 1. This example is inspired by [4].

Let m be a positive integer. Let

$$\mathcal{Z} = \mathbb{F}_2^m, \quad (9)$$

$$\mathcal{W} = (\mathbb{F}_2^m \setminus \{0\}) \times \mathbb{F}_2. \quad (10)$$

Let \mathcal{M} be a channel defined as follows:

1. The input alphabet of \mathcal{M} is \mathcal{Z} , and the output alphabet of \mathcal{M} is \mathcal{W} .
2. For any given input $\mathbf{v} \in \mathbb{F}_2^m$, the output of \mathcal{M} is uniformly distributed over the set

$$\{(\mathbf{w}, \mathbf{w} \cdot \mathbf{v}) \mid \mathbf{w} \in \mathbb{F}_2^m \setminus \{0\}\}. \quad (11)$$

(Here, $\mathbf{w} \cdot \mathbf{v} \in \mathbb{F}_2$ denotes the inner product of \mathbf{w} and \mathbf{v} .)

Let (E_1, E_2) be a two part input-output device defined as follows. (See Figure 3.)

1. The input alphabet for E_1 is \mathbb{F}_2 , and the output alphabet for E_1 is \mathcal{Z} .
2. The input alphabet for E_2 is \mathcal{W} , and the output alphabet for E_2 is \mathbb{F}_2 .
3. If the inputs to E_1 and E_2 are $a \in \{0, 1\}$ and $(\mathbf{w}, r) \in (\mathbb{F}_2^m \setminus \{0\}) \times \mathbb{F}_2$, then the output of E_1 is uniformly distributed over all vectors $\mathbf{a} = (a_1, a_2, \dots, a_m)$ that satisfy $a_1 = a$, and the output of E_2 is $a \oplus r \oplus (\mathbf{w} \cdot \mathbf{a})$.

It can be checked that the correlation \mathcal{E} arising from (D_1, D_2) is non-signaling. Additionally, one can see (by substitution) that using \mathcal{E} to assist \mathcal{M} yields a perfect transmission of a single bit.

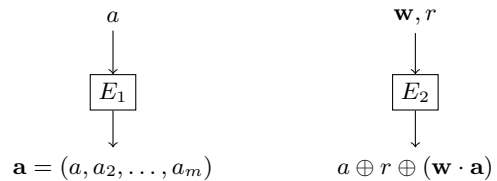


FIG. 3. The device (E_1, E_2) .

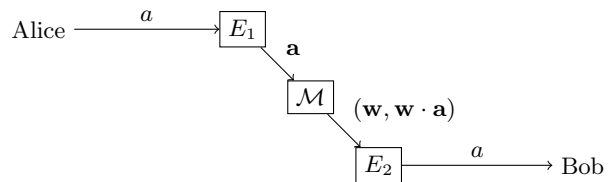


FIG. 4. A perfect communication protocol.

Now, let us calculate the quantity $\text{Succ}(\mathcal{M})$. For any two distinct vectors $\mathbf{x}_0, \mathbf{x}_1 \in \mathbb{F}_2^m$, the probability that a randomly chosen vector $\mathbf{w} \in \mathbb{F}_2^m \setminus \{0\}$ will satisfy $\mathbf{w} \cdot \mathbf{x}_0 \neq \mathbf{w} \cdot \mathbf{x}_1$ is equal to $2^{m-1}/(2^m - 1)$. This fact has the following consequence: if Alice employs the deterministic encoding strategy $[0 \mapsto \mathbf{x}_0, 1 \mapsto \mathbf{x}_1]$ to send a single bit, then the optimal probability with which Bob can decode is

$$\left[\frac{2^{m-1}}{2^m - 1} \right] (1) + \left[\frac{2^{m-1} - 1}{2^m - 1} \right] \left(\frac{1}{2} \right) \quad (12)$$

$$= \frac{2^m + 2^{m-1} - 1}{2^{m+1} - 2}. \quad (13)$$

Therefore, $\text{Succ}(\mathcal{M})$ is equal to quantity (13), while $\text{Succ}_{\mathcal{E}}(\mathcal{M})$ is equal to 1. Theorem 1 asserts the following bound on $\text{Succ}_{\mathcal{E}}(\mathcal{M})$:

$$\begin{aligned} \text{Succ}_{\mathcal{E}}(\mathcal{M}) & \leq \frac{1}{2} + 2 \left(1 - \frac{1}{|\mathcal{Z}|} \right) \left[\text{Succ}(\mathcal{M}) - \frac{1}{2} \right] \\ & = \frac{1}{2} + 2 \left(\frac{2^m - 1}{2^m} \right) \left(\frac{2^m + 2^{m-1} - 1}{2^{m+1} - 2} \right) \\ & = 1. \end{aligned}$$

Therefore, equality is achieved in Theorem 1 when $(\mathcal{N}, \mathcal{D}) = (\mathcal{M}, \mathcal{E})$.

Entanglement. We will now be concerned with *binary* non-signaling devices (i.e., devices with inputs and outputs in $\{0, 1\}$), and we assume throughout this section that $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. For any binary non-signaling correlation \mathcal{G} , let

$$f_1(\mathcal{G}) = \sum_{a,x,b,y \in \{0,1\}} (-1)^{x \oplus b \oplus (a \wedge y)} G_{ay}^{xb}. \quad (14)$$

This is the function which defines the CHSH inequality [7]. Additionally, let f_2, f_3 , and f_4 be the functions defined by the same expression with $a \wedge y$ replaced by $\neg a \wedge y$, $a \wedge \neg y$, and $\neg a \wedge \neg y$, respectively.

We note the following facts. (See [8].)

1. A non-signaling correlation \mathcal{G} is local if and only if $-2 \leq f_i(\mathcal{G}) \leq 2$ for $i = 1, 2, 3, 4$.
2. If \mathcal{G} is a quantum correlation, then for $i = 1, 2, 3, 4$,

$$-2\sqrt{2} \leq f_i(\mathcal{G}) \leq 2\sqrt{2}. \quad (15)$$

3. There are eight non-signaling correlations $\{\mathcal{P}_i^+\}_{i=1}^4$ and $\{\mathcal{P}_i^-\}_{i=1}^4$, satisfying

$$f_j(\mathcal{P}_i^\pm) = \begin{cases} \pm 4 & \text{if } j = i \\ 0 & \text{otherwise} \end{cases} \quad (16)$$

(These are the Popescu-Rohrlich (PR) boxes.)

4. Every non-signaling correlation is a convex combination of local correlations and the eight PR boxes.

Item 4 above can be made stronger. For any two distinct PR boxes \mathcal{P} and \mathcal{P}' , the correlation $(\mathcal{P} + \mathcal{P}')/2$ is local. From this, it follows that any convex combination of local boxes and PR boxes can be simplified into an expression of the form

$$\alpha\mathcal{L} + (1 - \alpha)\mathcal{Q}, \quad (17)$$

where \mathcal{L} is local, \mathcal{Q} is a PR box, and $\alpha \in [0, 1]$. Any non-signaling correlation can thus be expressed as a convex combination of a local correlation and a single PR box.

Proposition 2. *Let \mathcal{D} be a binary quantum correlation. Then, there exists a decomposition*

$$\mathcal{D} = \beta\mathcal{L}' + (1 - \beta)\mathcal{Q}, \quad (18)$$

where \mathcal{L}' is local and \mathcal{Q} is a PR box, with $\beta \geq 2 - \sqrt{2}$.

Proof. Let $\mathcal{D} = \alpha\mathcal{L} + (1 - \alpha)\mathcal{Q}$, where \mathcal{L} is local and \mathcal{Q} is a PR box. Let us assume that $\mathcal{Q} = \mathcal{P}_j^+$. The argument for the case $\mathcal{Q} = \mathcal{P}_j^-$ is similar. Let

$$\mathcal{L}_\beta = \frac{\alpha\mathcal{L} + (\beta - \alpha)\mathcal{P}_j^+}{\beta}. \quad (19)$$

for any $\beta \in [\alpha, 1]$. Then \mathcal{L}_β is local whenever $f_j(\mathcal{L}_\beta) \leq 2$. If $f_j(\mathcal{L}_1) < 2$, then $\mathcal{L}_1 (= \mathcal{D})$ is local, and the proposition follows easily. Otherwise, there is a value $\beta \in [\alpha, 1]$ such that $f_j(\mathcal{L}_\beta) = 2$. We have

$$\mathcal{D} = \beta \cdot \mathcal{L}_\beta + (1 - \beta)\mathcal{P}_j^+. \quad (20)$$

The quantity β must be at least $2 - \sqrt{2}$, since otherwise (15) would be violated. \square

We introduce a small piece of notation (to match the setup of [4]). Suppose that \mathcal{D} is a nonsignaling correlation whose first component D_1 accepts an input bit A and returns an output letter X . Let \mathcal{D}° denote the device whose first component D_1° accepts the bit A and returns the *pair* (A, X) . (Note that the output alphabet of D_1° is twice as large as that of D_1 .)

Theorem 3. *Suppose that \mathcal{D} is a binary quantum correlation. Then $\text{Succ}_{\mathcal{D}^\circ}(\mathcal{N})$ satisfies*

$$\left[\text{Succ}_{\mathcal{D}^\circ}(\mathcal{N}) - \frac{1}{2} \right] \leq \left(\frac{1}{2} + \frac{1}{\sqrt{2}} \right) \left[\text{Succ}(\mathcal{N}) - \frac{1}{2} \right].$$

Proof. This follows directly from Theorem 1 and Proposition 2 by linearity. \square

In [4], Prevedel et al present a channel \mathcal{N} and a quantum correlation \mathcal{D} such that $\text{Succ}(\mathcal{N}) = 5/6$, but $\text{Succ}_{\mathcal{D}}(\mathcal{N}) = \frac{2}{3} + \frac{1}{3\sqrt{2}}$. Plugging 5/6 into Theorem 3 yields $\text{Succ}_{\mathcal{D}}(\mathcal{N}) \leq \frac{2}{3} + \frac{1}{3\sqrt{2}}$. Thus we have shown that the protocol of [4] achieves the optimal increase in accuracy for binary quantum devices. (We note that this generalizes [9], which shows the optimality of [4] for a particular channel within a class of protocols.)

Conclusion. We have given tight bounds for the amount of assistance non-signaling correlations can provide to the one-shot success probability. If the correlations are binary, we extended these results to obtain tight bounds for the entanglement assisted success probability, showing that the results of [4] are optimal. The obvious open question is whether or not the entanglement results can be extended to apply to quantum devices of arbitrary alphabet size. Our arguments imply that a decomposition analogous to Proposition 2 for larger devices will immediately yield a more general version of Theorem 3.

The authors would like to thank Vincent Russo for his help with the preparation and editing of this paper. We also thank Aubrey da Cunha, Xiaodi Wu, and Kim Winick for many useful discussions when we were creating our results. This research was supported in part by the National Basic Research Program of China under Awards 2011CBA00300 and 2011CBA00301, and the NSF of the United States under Awards 1017335.

* bhemem@umich.edu

† carlmi@umich.edu

‡ shiyy@umich.edu

§ wootters@umich.edu

- [1] C. Bennett, P. Shor, J. Smolin, and A. Thapliyal, IEEE Transactions on Information Theory **48**, 2637 (2002).
- [2] T. Cubitt, D. Leung, W. Matthews, and A. Winter, IEEE Transactions on Information Theory **57**, 5509 (2011).
- [3] T. Cubitt, D. Leung, W. Matthews, and A. Winter, Physical Review Letters **104**, 230503 (2010).
- [4] R. Prevedel, Y. Lu, W. Matthews, R. Kaltenback, and K. J. Resch, Physical Review Letters **106**, 110505 (2011).
- [5] W. Matthews, Arxiv preprint arXiv:1109.5417 (2011).
- [6] S. Beigi, Physical Review A **82**, 010303 (2010).
- [7] J. Clauser, M. Horne, A. Shimony, and R. Holt, Physical Review Letters **23**, 880 (1969).
- [8] B. S. Tsirel'son, Hadronic Journal Supplement **8**, 329 (1993).
- [9] H. Williams and P. Bourdon, Arxiv preprint arXiv:1109.1029 (2011).