Electronic Colloquium on Computational Complexity, Report No. 336 (2026)

Asymptotic advantage of quantum one-way and SMP communication for total functions

Dmytro Gavinsky*†
Institute of Mathematics of the Czech Academy of Sciences, Žitná 25, Praha 1, Czechia
IonQ Quantum, Inc., 4505 Campus Drive, College Park, MD 20740, USA

Abstract

We exhibit a total Boolean function on n input bits whose bounded-error quantum simultaneous-message (and hence one-way) communication complexity is in $O\left(\sqrt{n}\right)$, whereas its randomised one-way (and hence simultaneous-message) communication complexity is in $\Omega(n)$. The same function admits a classical simultaneous-message protocol of cost $O\left(\sqrt{n}\right)$ when the players share $O\left(\sqrt{n}\right)$ EPR pairs.

1 The problem

All input algebra is over $\mathbb{F}_2$. Alice receives $M \in \mathbb{F}_2^{d\times d}$, Bob receives $u, z \in \mathbb{F}_2^d$ and we define

$$A_M \stackrel{\text{def}}{=} M + M^{\mathsf{T}}, \quad f_M(x) \stackrel{\text{def}}{=} x^{\mathsf{T}} M x,$$
$$F_d(M; u, z) \stackrel{\text{def}}{=} \mathbf{1}\left[A_M u = z \text{ and } f_M(u) = 0\right].$$

The encoded input length is $n \stackrel{\text{def}}{=} d^2 + 2d$. Note that the matrix A_M is alternating ($u^{\mathsf{T}} A_M u \equiv 0$).

In a one-way protocol, Alice sends one message to Bob, who outputs the answer. In a simultaneous-message (SMP) protocol, Alice and Bob each send one message to a referee, who outputs the answer. Write $R^{\rightarrow}, Q^{\rightarrow}$ for the classical and quantum one-way complexities, and $R^{\parallel}, Q^{\parallel}$ for their SMP counterparts. By default, the models have no prior entanglement; the superscript $^{\mathsf{ent}}$ allows an arbitrary prior entangled state between Alice and Bob and $^{\mathsf{ent}(e)}$ restricts that state to at most e qubits per party (note that shared entanglement does not, in general, turn $R^{\parallel}$ into $Q^{\parallel}$). All models allow public randomness. Local computation and classical encoders and decoders are unrestricted. All protocols must have error probability at most $1/3$ on any input – unless the target distribution is specified. The cost of a protocol is the maximum total transmitted number of (qu)bits.

Trivially, for any function f and integer $k \geq 0$,

$$R^{\rightarrow}(f) \leq R^{\parallel}(f), \quad Q^{\rightarrow}(f) \leq Q^{\parallel}(f),$$
$$Q^{\rightarrow}(f) \leq R^{\rightarrow}(f), \quad Q^{\parallel}(f) \leq R^{\parallel}(f),$$
$$Q^{\rightarrow}(f) \leq k + R^{\parallel,\mathsf{ent}(k)}(f).$$

We establish the following.

Theorem 1.1.

$$Q^{\parallel}(F_d),\ Q^{\rightarrow}(F_d) \ \in\ \Theta(d) = \Theta\left(\sqrt{n}\right),$$
$$R^{\rightarrow}(F_d),\ R^{\parallel}(F_d) \ \in\ \Theta\left(d^2\right) = \Theta(n),$$
$$R^{\parallel,\mathsf{ent}(2d)}(F_d) \ \in\ O(d), \quad R^{\parallel,\mathsf{ent}}(F_d) \ \in\ \Omega(d).$$

*In 2022 the author changed his first name, as explained on his Internet page.

†This work was developed in collaboration with ANNA – Anonymous Neural-Network Assistant – whom the author sincerely thanks.

ISSN 1433-8092

2 The quantum complexity

2.1 The one-way protocol

For $a \in \mathbb{F}_2^d$, define

$$\psi_M(a) \stackrel{\text{def}}{=} 2^{-d/2} \sum_{x \in \mathbb{F}_2^d} (-1)^{f_M(x)+a\cdot x}|x\rangle.$$

These vectors form an orthonormal basis. Alice sends $\psi_M(0)$ to Bob, using d qubits. Bob rejects if $u \cdot z = 1$ (as A_M is alternating). Otherwise he measures using the projectors $(I \pm P_{u,z})/2$, where

$$P_{u,z}|x\rangle \stackrel{\text{def}}{=} (-1)^{z\cdot x}|x+u\rangle,$$

and accepts iff the outcome is $+1$. For $u \cdot z = 0$, the operator $P_{u,z}$ is Hermitian, satisfies $P_{u,z}^2 = I$ and maps each $\psi_M(a)$ to a basis vector or its negative:

$$f_M(x+u) + f_M(x) = f_M(u) + (A_M u)\cdot x,$$
$$P_{u,z}\psi_M(a) = (-1)^{f_M(u)+a\cdot u}\psi_M(a + A_M u + z).$$

The accepting component is the midpoint of $\psi_M(0)$ and $P_{u,z}\psi_M(0)$, as shown in Figure 1. Its squared norm is the acceptance probability:

$$\begin{aligned} \Pr[\text{accept}] &= \frac{1 + \langle \psi_M(0)|P_{u,z}|\psi_M(0)\rangle}{2} \\ &= \frac{1 + (-1)^{f_M(u)}\mathbf{1}[z = A_M u]}{2}. \end{aligned} \tag{1}$$

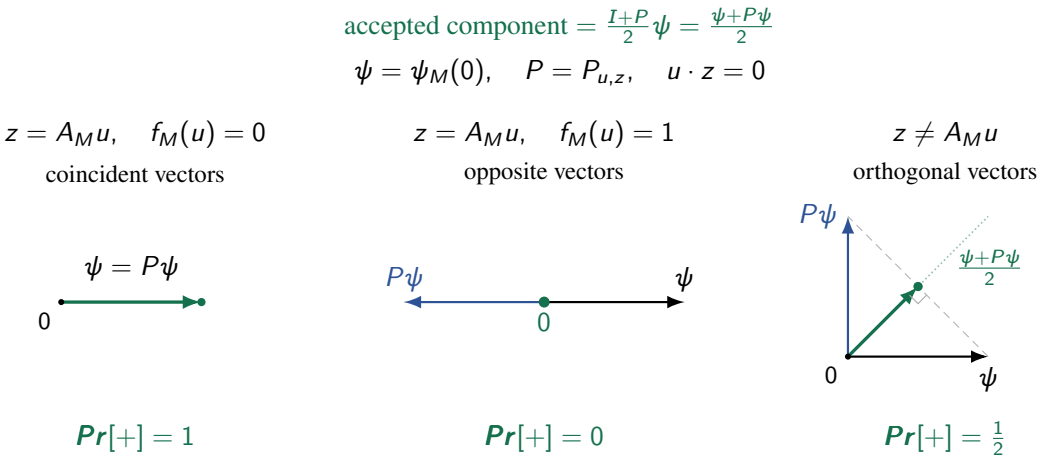


Figure 1: The accepting component is shown in green.

Repeating the test independently twice and accepting iff both tests pass gives one-sided error at most $1/4$, using $2d$ qubits.

2.2 SMP versions

Alice and Bob share d EPR pairs. Alice applies the phase $|x\rangle \mapsto (-1)^{f_M(x)}|x\rangle$ to her share and measures in the Hadamard basis. She sends her d-bit outcome a to the referee, leaving Bob with $\psi_M(a)$. If $u \cdot z = 1$, Bob chooses $s \in \{-1, 1\}$ uniformly at random; otherwise he measures using $(I \pm P_{u,z})/2$ and

records the outcome s. He sends (u, s) to the referee. The referee accepts iff $s = (-1)^{a \cdot u}$. For $u \cdot z = 0$,

$$\begin{aligned} \Pr\left[\text{accept}\middle|a\right] &= \frac{1 + (-1)^{a \cdot u} \left\langle \psi_M(a) \middle| P_{u,z} \middle| \psi_M(a) \right\rangle}{2} \\ &= \frac{1 + (-1)^{f_M(u)} \mathbf{1}[z = A_M u]}{2}, \end{aligned}$$

which is the same probability as in (1). For $u \cdot z = 1$, the acceptance probability is $1/2$. Repeating twice independently, sending u only once and accepting iff both runs accept gives one-sided error at most $1/4$, using $2d$ EPR pairs and $3d + 2$ classical bits.

For quantum SMP, Bob sends his $2d$-bit classical input (u, z) to the referee, who runs the one-way protocol on Alice's quantum message.

2.3 Other bounds

On $M = \mathrm{diag}(b)$, $z = 0$, the function is the complement of inner product. Cleve, van Dam, Nielsen and Tapp [1] give an $\Omega(d)$ lower bound even for two-way quantum communication with arbitrary prior entanglement, matching the $O(d)$ protocols above. Classical two-way communication has cost in $\Theta(d)$: Bob sends (u, z) and Alice returns the answer. The classical one-way and SMP upper bounds follow by transmitting the inputs.

3 The classical complexity

We use the following estimate, proved in Section 4.

Proposition 3.1 (*Uniform moments*). *For any function $g : \mathbb{F}_2^d \times \mathbb{F}_2^d \to \{-1, 1\}$, define*

$$R_g(M) \stackrel{def}{=} \mathop{\mathbf{E}}_{u \in \mathbb{F}_2^d} \left[g\Big(u, (M + M^{\mathsf{T}})u\Big) (-1)^{u^{\mathsf{T}} M u} \right].$$

Then, for every even $p \geq 2$,

$$\mathop{\mathbf{E}}_{M \in \mathbb{F}_2^{d \times d}} \left[\left| R_g(M) \right|^p \right] \leq 2^{2p^2 - \frac{1}{10} pd}.$$

Choose $M \in \mathbb{F}_2^{d \times d}$, $u \in \mathbb{F}_2^d$ and $z = A_M u$. Assume a fixed c-bit message, at a cost of at most one extra bit, and fix the randomness while retaining average success at least $2/3$. After message $j \in [2^c]$, write Bob's answer on (u, z) as $h_j(u, z) \in \{-1, 1\}$, with $+1$ denoting acceptance. The correct answer on this distribution is $(-1)^{f_M(u)} = (-1)^{u^{\mathsf{T}} M u}$, so

$$\begin{aligned} \frac{1}{3} &\leq \mathop{\mathbf{E}}_{M} \left[\max_{j \in [2^c]} \left\{ \left| \mathop{\mathbf{E}}_{u} \left[h_j(u, A_M u) \cdot (-1)^{u^{\mathsf{T}} M u} \right] \right| \right\} \right] = \mathop{\mathbf{E}}_{M} \left[\max_{j \in [2^c]} \left\{ \left| R_{h_j}(M) \right| \right\} \right] \\ &\leq \left(2^c \cdot \mathop{\mathbf{E}}_{j \in [2^c], M} \left[\left| R_{h_j}(M) \right|^p \right] \right)^{1/p} \\ &\leq \left(2^c \cdot 2^{-\frac{1}{10} pd + O(p^2)} \right)^{1/p}. \end{aligned}$$

Taking logarithms gives $c \geq \frac{1}{10} pd - O(p^2)$; choosing an even $p \in \Theta(d)$ with a sufficiently small proportionality constant yields $c \in \Omega(d^2)$. Together with $R^{\rightarrow} \leq R^{\|}$ and the bounds of Section 2, this proves Theorem 1.1.

4 The moment estimate

Proof of Proposition 3.1. All averaged vector variables below are independent and uniform on $\mathbb{F}_2^d$. For vector spaces, $\leq$ denotes subspace inclusion. The Fourier transform of g in its second argument is

$$\hat{g}(u;s) \stackrel{\text{def}}{=} \mathop{\boldsymbol{E}}_{z}\big[g(u,z)(-1)^{z\cdot s}\big].$$

Parseval gives

$$\sum_{s}\big|\hat{g}(u;s)\big|^2 = 1. \tag{2}$$

In particular, $max_{u,s}\Big\{\big|\hat{g}(u;s)\big|\Big\} \leq 1$ and $\sum_{u,s}\big|\hat{g}(u;s)\big| \leq 2^{3d/2}$ by Cauchy–Schwarz. Fourier inversion gives:

$$\begin{aligned} R_g(M) &= \mathop{\boldsymbol{E}}_{u}\Big[g(u,A_Mu)(-1)^{f_M(u)}\Big] \\ &= 2^d\cdot\mathop{\boldsymbol{E}}_{u,z}\Big[g(u,z)(-1)^{f_M(u)}\mathop{\boldsymbol{E}}_{s}\Big[(-1)^{(A_Mu+z)\cdot s}\Big]\Big] \\ &= 2^d\cdot\mathop{\boldsymbol{E}}_{r,s}\Big[\hat{g}(r+s;s)(-1)^{f_M(r)+f_M(s)}\Big]. \end{aligned}$$

Write $Y \stackrel{\text{def}}{=} (r_1,\ldots,r_p,s_1,\ldots,s_p)\in\mathbb{F}_2^{d\times 2p}$. In the expansion of $R_g(M)^p$, averaging over M retains exactly the terms with $YY^{\mathsf{T}} = \sum_i r_i r_i^{\mathsf{T}} + \sum_i s_i s_i^{\mathsf{T}} = 0$:

$$\begin{aligned} \mathop{\boldsymbol{E}}_{M}\Big[\big|R_g(M)\big|^p\Big] &= 2^{-pd}\cdot\sum_{YY^{\mathsf{T}}=0}\prod_i\hat{g}(r_i+s_i;s_i) \\ &\leq 2^{-pd}\cdot\sum_{L\leq\mathbb{F}_2^{2p}:\,L\subseteq L^\perp} Z_L, \\ Z_L &\stackrel{\text{def}}{=} \sum_{Y:\,\mathrm{rows}(Y)\subseteq L}\prod_i\big|\hat{g}(r_i+s_i;s_i)\big|. \end{aligned} \tag{3}$$

Taking absolute values and summing over all self-orthogonal subspaces gives the inequality, since $YY^{\mathsf{T}} = 0$ makes the rowspace of Y self-orthogonal.

Fix one such L, choose a generator matrix $G = (R\ S)$ whose rows form a basis of L and put $k \stackrel{\text{def}}{=} \dim(L) \leq p$ and $m \stackrel{\text{def}}{=} \mathrm{rank}(R+S)$. Greedily choose a maximal family of column pairs (R_i,S_i) such that all selected columns are linearly independent and let q be the number of selected pairs. List the selected pairs first in each block and perform row operations; these preserve Z_L and m. Every matrix Y with rows in L then has the unique form

$$Y = \underbrace{(X_1\ X_2\ X_3)}_{X\in\mathbb{F}_2^{d\times k}}\underbrace{\left(\begin{array}{cc|cc} I_q & * & 0 & * \\ 0 & * & I_q & * \\ \hline 0 & R' & 0 & S' \end{array}\right)}_{G=(R\ S)} = \big(X_1\quad *\,|\,X_2\quad *\big).$$

Here X_1, X_2 have q columns each and X_3 has $k-2q$; the starred blocks are determined by G and X. We first note that

$$2m \leq p + 3q. \tag{4}$$

Indeed, deleting the selected columns from the bottom $k-2q$ rows leaves a self-orthogonal matrix $(R'\ S')$. By maximality, each pair (R'_i,S'_i) is dependent, so

$$(R'+S')(R'+S')^{\mathsf{T}} = R'R'^{\mathsf{T}} + S'S'^{\mathsf{T}} = 0.$$

Hence

$$m \leq 2q + \mathrm{rank}\big(R'+S'\big) \leq 2q + \frac{p-q}{2}.$$

There are two bounds for Z_L. First, fixing X_1, X_2 leaves $2^{d(k-2q)}$ choices of X_3. Discarding the other factors using $|\hat{g}| \leq 1$ gives

$$Z_L \leq 2^{d(k-2q)} \cdot \left(\sum_{u,s} \left|\hat{g}(u;s)\right| \right)^q \leq 2^{d(k-q/2)}.$$

Second, there are 2^{dk} coefficient matrices X and 2^{dm} possible difference arrays $v \stackrel{\text{def}}{=} (r_i + s_i)_i = X(R+S)$. Cauchy–Schwarz and (2) give

$$\begin{aligned} Z_L^2 &\leq 2^{dk} \cdot \sum_{Y\,:\,\mathrm{rows}(Y) \subseteq L} \prod_i \left|\hat{g}(r_i + s_i; s_i)\right|^2 \\ &\leq 2^{dk} \cdot \sum_v \prod_i \left(\sum_{s_i} \left|\hat{g}(v_i; s_i)\right|^2 \right) = 2^{d(k+m)}. \end{aligned}$$

Cubing the first bound and multiplying by the second, using (4) and $k \leq p$, gives

$$\begin{aligned} Z_L^5 &\leq 2^{d(4k+m-\frac{3}{2}q)} \leq 2^{\frac{9}{2}pd}, \\ Z_L &\leq 2^{\frac{9}{10}pd}. \end{aligned}$$

Every self-orthogonal L has dimension at most p and is the rowspace of some binary $p \times 2p$ matrix. There are 2^{2p^2} such matrices; hence (3) gives

$$\mathop{\boldsymbol{E}}_M \left[\left| R_g(M) \right|^p \right] \leq 2^{2p^2 - \frac{1}{10}pd},$$

as required. ■*Proposition 3.1*

References

[1] Richard Cleve, Wim van Dam, Michael Nielsen and Alain Tapp. Quantum entanglement and the communication complexity of the inner product function. *Theoretical Computer Science*, 486:11–19, 2013.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il