Noise in quantum and classical computation & non-locality
Unger, F.P.

Citation for published version (APA):
Appendix C  
Classical entanglement-assisted communication complexity of inner product

We show here that the classical communication complexity of the inner product function under shared entanglement is

$$R^*_\epsilon(IP_n) \geq n - 2\log_2 \frac{1}{1-2\epsilon}, \quad (C.1)$$

where $\epsilon > 0$ is (a lower bound on) the desired error probability. The proof is via a reduction from the quantum communication complexity of inner product with entanglement [65]

$$Q^*_\epsilon(IP_n) \geq \frac{1}{2}n - \log_2 \frac{1}{1-2\epsilon}. \quad (C.2)$$

Here $Q^*_\epsilon(IP_n)$ is the minimum number $c$ such that there is a protocol which uses arbitrary entanglement, communicates at most $c$ qubits and for every $x, y \in \{0,1\}^n$ it correctly outputs $IP_n(x, y)$ with probability at least $1 - \epsilon$. The bound (C.1) already appears in [65], but only for the model of one-way communication. We show that this bound even holds without a restriction on the number of rounds.

The problem of proving (C.1) came up in a discussion with Ronald de Wolf who pointed out the following easy reduction to me [103].

**Proof:** Assume there is an entanglement-assisted protocol $P$ for $IP_n$ which needs at most $\bar{c}$ classical bits to compute $IP_n$ correctly with probability at least $1 - \epsilon$. We will show that $\bar{c}$ must be at least as large as the right-hand side of (C.1).

Consider the following protocol for computing $IP_{kn}$ for inputs $x, y \in \{0,1\}^{kn}$: Chop $x$ into $k$ blocks $x^i$, $1 \leq i \leq k$, of length $n$ each. Do the same for $y$. Run $P$ to compute all instances $IP_n(x^i, y^i)$ and then output $\bigoplus_{i=1}^k IP_n(x^i, y^i)$. It is straightforward to prove (by induction on $k$) that this protocol $P^{\otimes k}$ will correctly compute $IP_{kn}(x, y)$ with probability

$$\Pr[P^{\otimes k}(x, y) = IP(x, y)] \geq \frac{1}{2} + \frac{1}{2}(1 - 2\epsilon)^k. \quad (C.3)$$
Further, by assumption protocol \( P^{\otimes k} \) uses at most \( k\bar{c} \) bits of classical communication, and it is easy to design \( P^{\otimes k} \) such that it never uses more than \( \bar{c} \) rounds of communication.

If \( P^{\otimes k} \) sends \( c_i \) classical bits in the \( i \)-th round, then this can be simulated with \( \lceil c_i/2 \rceil \) many qubits using superdense coding. Simulating the whole protocol \( P^{\otimes k} \) in this way results in a protocol which never communicates more than

\[
\sum_{i=1}^{\bar{c}} \lceil c_i/2 \rceil \leq \sum_{i=1}^{\bar{c}} \frac{c_i+1}{2} \leq (k + \frac{1}{2}) \bar{c} \tag{C.4}
\]

qubits, where we used that \( P^{\otimes k} \) needs \( \sum_{i=1}^{\bar{c}} c_i \leq k\bar{c} \) classical bits. From this and equations (C.3) and (C.2) it then follows that

\[
(k + \frac{1}{2}) \bar{c} + 1 \geq \frac{1}{2} kn - \log_2 \frac{1}{1-2^{(k+n+1)/(1-2^{1-2\epsilon})}} = \frac{1}{2} kn - k \log_2 \frac{1}{1-2\epsilon}.
\]

Since this inequality has to hold for any \( k \), we can conclude that \( \bar{c} \geq n - 2 \log_2 \frac{1}{1-2\epsilon} \), which proves our claim. \( \blacksquare \)