Preface

Tal Mor · Alain Tapp

Published online: 30 November 2012
© Springer Science+Business Media Dordrecht 2012

This special issue of “Natural Computing (NACO)” together with its companion issue of Theoretical Computer Science, Section C (TCS-C), is dedicated to the closely related topics of quantum communication complexity and non-locality, honoring the first paper defining *quantum communication complexity*, by Andrew Yao, published in 1993.

Communication complexity is a field in Computer Science in which one is interested in the efficiency of communication, when trying to accomplish a task that depends on *distributed data* (Yao 1979); this is done while ignoring the computing resources used by the protocol. Consider two distant parties, Alice (A) and Bob (B), each having an n -bit string, X_A in Alice’s hands and X_B in Bob’s hands. Consider three simple examples: Task 1—Alice needs to calculate whether her string equals Bob’s string. Task 2—Alice needs to calculate whether the total number of ones in the two strings (together) is even or odd. Task 3—Alice needs to calculate whether the total number of ones in the two strings is larger than n . For a single bit ($n = 1$) the first two tasks are identical, and the third task means calculating an AND-gate, $X_A \cdot X_B$. Clearly, for $n = 1$ each task requires a communication of a single bit.¹ For a larger n , one can trivially ask Bob to send all his n bits to Alice, but often one might be able to do better. Task 1 requires the transmission of all n bits from Bob to Alice, Task 2 requires the sending of just a single bit, the parity of Bob’s string, and Task 3 can be accomplished with a logarithmic

amount of communication, since Bob only needs to communicate the number of ones in his string. For many problems in communication complexity, no one knows (yet) what the optimal protocol and the minimal communication are. Instead, researchers try to find the best protocol they can, or alternatively, to derive lower bounds on the communication required by any protocol.

Resources in communication complexity can go beyond just communicating bits. In task 1, for example, having a preparation step done prior to receiving the strings (and therefore independently of the input strings), may help in reducing the communication, if the correct answer can be given with high probability rather than with certainty: Shared random strings $(S_1, S_2, \dots, S_k)$ of the same length n help in guessing if $X_A = X_B$. This is done (for each $t \in \{1, \dots, k\}$), by comparing the parities of $S_t \cdot X_A$ and $S_t \cdot X_B$ (the parities of subsets of the strings), where the subset t is chosen by the ones in the string S_t . If Alice’s and Bob’s strings (X_A and X_B) are identical then, for each subset, Alice and Bob will calculate the same parity. But if their strings are not identical, then each such parity bit has a one-in-two probability of being different. Hence in this case, a constant number (k) of such tests will almost surely reveal that Alice’s and Bob’s strings are not identical, and will only fail with a very small probability, exponentially small in k . In this protocol, if one test (or more, of course) fails, then Alice concludes with certainty that the strings are different; if all tests pass, Alice concludes that the strings are identical, yet in this case, she has a small probability to be wrong.

Even without pre-sharing any data, the possibility of tolerating some error already allows solving this problem

T. Mor (✉)
Computer Science Department, Technion, 32000 Haifa, Israel
e-mail: talmo@cs.technion.ac.il

A. Tapp
DIRO, Université de Montréal, Montréal, QC, Canada

¹ Note that for task 3, the need for one bit is true only when Alice’s bit equals 1; if her bit equals 0 then no communication is required.

with less than n bits. For an excellent review of communication complexity presenting this problem and many other problems, see (Kushilevitz and Nisan 1997).

Non-locality implies that a task cannot be done, even using an infinite amount of pre-shared knowledge. Consider (again) the simple problem in which Alice and Bob each have one bit and where Alice needs to calculate $X_A \cdot X_B$, but this time, without letting Alice and Bob communicate at all. If we assume that all inputs are equiprobable, then Alice can simply guess that the outcome is 0, and with probability $3/4$ she will be right. If she first looks at her input, she can tell the output is certainly 0 in half the cases, and she can guess the output in the other half, but her overall probability of obtaining the correct answer is still $3/4$. Pre-sharing a random bit, or even an infinite number of pre-shared bits will make no difference here. Is there a way for Alice to improve her probability of guessing $X_A \cdot X_B$ beyond $3/4$? If there were, some non-local action would have taken place. However, that task is indeed impossible, and even quantum physics does not enable miracles here.

On the other hand, a similar task *is* possible in the quantum domain and is at the heart and core of quantum non-locality: Instead of asking if Alice can guess $X_A \cdot X_B$, we want Alice and Bob to provide outputs Y_A and Y_B (respectively) that are equal if and only if $X_A \cdot X_B = 0$. In other words, Alice's and Bob's goal² is to output Y_A and Y_B satisfying $Y_A \oplus Y_B = X_A \cdot X_B$.

In a non-quantum world, that task can (still), similarly to the other problem just mentioned, be accomplished with, at most, a probability $3/4$ of success. This is done quite easily—both Alice and Bob will always output zeroes; with probability of $3/4$, $X_A \cdot X_B = 0$, and their protocol succeeds. However, they cannot do better than this, and again, pre-sharing of one or many bits will not help them.

A more subtle case is the case in which Alice's and Bob's method of providing their outcomes must work not only on average, but also for the worst case. The method mentioned above, in which both output a “0”, will not work now, because in the worst case the inputs are both “1”, and Alice and Bob will fail in their task. In this worst-case scenario, however, if Alice and Bob use a probabilistic strategy and also use pre-shared bits, they can still recover the success probability of $3/4$ as in the average case scenario. Of course, again, they cannot do any better than that.

Quantum resources for communication include transmitting quantum bits (qubits) instead of just classical bits (with or without pre-shared randomness), and using pre-shared “quantum entanglement”.

It was noted by Bell (1964), almost 50 years ago, that by using pre-shared quantum entanglement (and no communication whatsoever) a different task which is classically impossible, becomes possible using a quantum setup. A few years later (Clauser et al. 1969), following Bell's idea, the problem presented here, of obtaining outputs such that $Y_A \oplus Y_B = X_A \cdot X_B$, was solved with a probability of success higher than $3/4$ using pre-shared quantum entanglement and no communication whatsoever. To accomplish that, Alice and Bob choose the bases of their measurements (each of them applies a measurement on one member of the entangled pair) depending on the inputs, and the resulting probability of success is $\cos^2(\pi/8) = (2 + \sqrt{2})/4 \approx 85\%$.

It is also interesting to note that this is the highest probability of success allowed by any quantum protocol. In principle, a different type of Physics could allow pre-sharing of other things instead (or in addition to) common classical data and an entangled quantum state. A different type of Physics could allow pre-sharing a non-quantum non-local box (Popescu and Rohrlich 1994), called the Popescu-Rohrlich box, that yields 100 % success in this task, while still being “non-signaling”, namely, while still being consistent with relativity theory and not allowing communicating information faster than light (i.e., not violating Einstein's causality). This type of non-quantum non-locality (which is not expected to exist in the physical world) is often called *superstrong non-locality*, or *stronger-than-quantum non-locality*.

For basic notions such as “quantum bits”, measurements of quantum bits, and “quantum entanglement”, see for instance (Rieffel and Polak 2000). It is probably fair to say that quantum non-locality was initiated by Bell (1964). The classical bound of $3/4$ is obtained, in a slightly different terminology, in (Clauser et al. 1969) and is known as the Bell-CHSH inequality. For a description of the Bell-CHSH inequality, via the terminology used here, including the classical bound of $3/4$, and the quantum result of about 85 %, see the paper by van Dam, “Implausible consequences of superstrong nonlocality”, originally from 2005, published in this special issue.

Quantum non-locality is related to communication complexity, as can be seen from the example above, in which there is no communication at all (while the task of bypassing the probability of $3/4$ requires communication when using classical resources only). Interesting cases of quantum non-locality, that are not considered as “communication complexity” (as the notion of complexity is irrelevant there), are cases in which pre-shared entanglement is used to provide a communication advantage *per se*.

Bennett and Wiesner (1992) showed that by using pre-shared entanglement combined with sending a *single* qubit, Alice can communicate to Bob two classical bits. This type of quantum non-locality is now called *superdense coding*.

² In recent years, such a task is called a “non-local game”, and winning the game then means performing better than classically possible.

Quantum non-locality also applies in cases where the task itself has no classical analog, and cannot be performed with just classical communication, pre-shared randomness, and *local* quantum operations. The best example is quantum teleportation of a qubit, using pre-shared entanglement and two classical bits. It is important to mention that “quantum nonlocality without entanglement” was also found (Bennett et al. 1999). It is also important to note that some notions such as teleportation do have classical processes that resemble them (Mor 2006).

Quantum communication complexity officially began in 1993 when Andrew Yao defined this term and gave it as the title of Section 5 of his paper “Quantum circuit complexity” (Yao 1993). He proposed the idea that one might be able to prove a lower bound on a specific quantum *circuit* complexity problem, using a lower bound on a quantum *communication* complexity problem. Interestingly, the communication complexity problem he handled was Task 3 mentioned above. Yao discussed the model that allows communication of qubits and no pre-shared entanglement. Later, Cleve and Buhrman (1997) discussed a different model in which the parties use pre-shared entanglement, yet communicate only classical bits. Most research work done since then, first by van Dam, Grover, Høyer, Kremer, Nielsen, Tapp and Wigderson, and later by other researchers as well, used one of these two models. Rarely, protocols in quantum communication complexity combine both pre-shared entanglement and qubits communication.

For the two companion issues we invited three leading researchers in the field of quantum communication complexity and quantum non-locality, Gilles Brassard, Richard Cleve, and Lev Vaidman, to present the papers of their choice. We also invited Wim van Dam to present his interesting paper “Implausible consequences of superstrong nonlocality”. Seven other submitted papers were carefully chosen and are presented here as well. Our choice of which papers will go to each of the two journals was mainly based on how well they fit in the theoretical computer science journal, versus the journal with a broader scope, NACO.

This special issue consists of four papers.

The first paper “A family of nonlocal games with continuous inputs” by Aharon, Machnes, Reznik, Silman and Vaidman, chosen by Vaidman as his invited paper, considers non-local games of the Bell-CSHS type in which the input is continuous.

The second paper “Implausible consequences of superstrong nonlocality”, by van Dam was invited, as it is an important historical paper that was never published, and appeared on the arXiv in 2005. The paper demonstrates that the superstrong non-locality presented by the Popescu Rohrlich boxes has highly surprising consequences for communication complexity. The third paper “Oblivious transfer, non-local boxes, and quantum channels”, by

Gisin, Popescu, Scarani, Wolf, and Wullschlegel, presents non-cryptographic oblivious transfer and considers interesting relations between this (new) primitive and qubit transmission, that closely resemble the relations between non-local boxes and entangled pair of qubits. The last paper “Experimental multipartner quantum communication complexity employing just one qubit” by Trojek, Schmid, Bourennane, Brukner, Żukowski and Weinfurter considers two problems in communication complexity including the so called modulo-4 sum problem. The paper reviews earlier experimental implementations (by the same coauthors) and presents their analyses.

The companion issue of TCS-C consists of seven papers.

The first paper “Strict hierarchy among Bell theorems” by Brassard and Méthot, chosen by Brassard as his invited paper, classifies three levels of Bell-like non-locality (including quantum pseudo-telepathy, in which the probability of success using a quantum strategy is one).

The second paper “Quantum entanglement and the communication complexity of the inner product function” by Cleve, van Dam, Nielsen and Tapp, chosen by Cleve as his invited paper, is an historical paper in the field of quantum communication complexity, whose arXiv version first appeared in 1997 and its conference version was published in 1999. This paper considers the problem mentioned in its title when the two parties pre-share entangled qubits. It analyzes both the exact case and the case in which some error is allowed.

The third paper “Deterministic quantum non-locality and graph colorings” by Galliard, Tapp and Wolf, considers a special case of non-local games, pseudo-telepathy, and makes connections between the game strategies and graph coloring.

The fourth paper “The impossibility of non-signaling privacy amplification” by Hänggi, Renner and Wolf, considers quantum key distribution based on causality (non-signaling) by itself, instead of relying on the rules of quantum physics. As its title hints, the result is negative, showing an advantage of quantum physics over non-local boxes, in this respect.

The fifth paper “Quantum weakly nondeterministic communication complexity” by Le Gall considers quantum versus classical communication complexity in the (exact) non-deterministic setting, presenting a quadratic separation.

The sixth paper “Towards characterizing the non-locality of entangled quantum states” by Renner and Wolf, considers the special case of non-local games mentioned above, pseudo-telepathy, and presents a striking example in which the quantum advantage is impressive. The paper then characterizes several more general cases.

The last paper “Classical, quantum and nonsignalling resources in bipartite games” by Brassard, Broadbent,

Hänggi, Méthot and Wolf, considers bipartite non-local games (with various resources) using the help of graph theory. Its main results are alternate proofs that some existence questions are NP-complete.

We are most grateful to the authors of all submissions, and to the reviewers for their thorough and thoughtful reviews. We are especially grateful to Gilles Brassard who, in addition to contributing and refereeing papers and providing helpful remarks on this Preface, also acted as co-editor for two of the papers. Finally, we would very much like to thank Grzegorz Rozenberg, editor-in-chief of TCS-C and NACO, for much advice.

References

- Bell JS (1964) On the Einstein-Podolsky-Rosen paradox. *Physics* 1:195–200
- Bennett CH, DiVincenzo DP, Fuchs CA, Mor T, Rains E, Shor PW, Smolin JA, Wootters WK (1999) Quantum nonlocality without entanglement. *Phys Rev A* 59: 1070–1091
- Bennett CH, Wiesner SJ (1992) Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys Rev Lett* 69:2881–2884
- Clauser JF, Horne MA, Shimony A, Holt RA (1969) Proposed experiment to test local hidden-variable theories. *Phys Rev Lett* 23:880–884
- Cleve R, Buhrman H (1997) Substituting quantum entanglement for communication. *Phys Rev A* 56:1201–1204
- Kushilevitz E, Nisan N (1997) *Communication Complexity*. Cambridge University Press, Cambridge
- Mor T (2006) On classical teleportation and classical non-locality. *Int J Quantum Inf* 4:161–171
- Popescu S, Rohrlich D (1994) Quantum nonlocality as an axiom. *Found Phys* 24:379–385
- Rieffel E, Polak W (2000) An introduction to quantum computing for non-physicists. *ACM Comput Surv* 32:300–335
- Yao AC-C (1979) Some complexity questions related to distributive computing. In: *Proceedings of the 11th ACM STOC*, p 209–213
- Yao AC-C (1993) Quantum circuit complexity. In: *Proceedings of the 34th FOCS*, p 352–361