The Garden-Hose Model

Harry Buhrman
CWI, University of Amsterdam
h.buhrman@cwi.nl

Serge Fehr
Centrum Wiskunde & Informatica (CWI) Amsterdam
s.fehr@cwi.nl

Christian Schaffner
University of Amsterdam, CWI
c.schaffner@uva.nl

Florian Speelman
CWI, University of Amsterdam
f.speelman@cwi.nl

ABSTRACT

We define a new model of communication complexity, called the *garden-hose model*. Informally, the garden-hose complexity of a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is given by the minimal number of water pipes that need to be shared between two parties, Alice and Bob, in order for them to compute the function f as follows: Alice connects her ends of the pipes in a way that is determined solely by her input $x \in \{0,1\}^n$ and, similarly, Bob connects his ends of the pipes in a way that is determined solely by his input $y \in \{0,1\}^n$. Alice turns on the water tap that she also connected to one of the pipes. Then, the water comes out on Alice's or Bob's side depending on the function value $f(x,y)$.

We prove almost-linear lower bounds on the garden-hose complexity for concrete functions like inner product, majority, and equality, and we show the existence of functions with exponential garden-hose complexity. Furthermore, we show a connection to classical complexity theory by proving that all functions computable in log-space have polynomial garden-hose complexity.

We consider a *randomized* variant of the garden-hose complexity, where Alice and Bob hold pre-shared randomness, and a *quantum* variant, where Alice and Bob hold pre-shared quantum entanglement, and we show that the randomized garden-hose complexity is within a polynomial factor of the deterministic garden-hose complexity. Examples of (partial) functions are given where the quantum garden-hose complexity is logarithmic in n while the classical garden-hose complexity can be lower bounded by n^c for constant $c > 0$.

Finally, we show an interesting connection between the garden-hose model and the (in)security of a certain class of *quantum position-verification* schemes.

Categories and Subject Descriptors

E.4 [**Coding and Information Theory**]: Formal models of communication

ITCS'13, January 9–12, 2013, Berkeley, California, USA.

Keywords

communication complexity; garden-hose model; position-based quantum cryptography

1. INTRODUCTION

The garden-hose model.

On a beautiful sunny day, Alice and Bob relax in their neighboring gardens. It happens that their two gardens share s water pipes, labeled by the numbers $1, 2, \ldots, s$. Each of these water pipes has one loose end in Alice's and the other loose end in Bob's garden. For the fun of it, Alice and Bob play the following game. Alice uses pieces of hose to locally connect some of the pipe ends that are in her garden with each other. For example, she might connect pipe 2 with pipe 5, pipe 4 with pipe 9, *etc.* Similarly, Bob locally connects some of the pipe ends that are in his garden; for instance pipe 1 with pipe 4, *etc.* We note that no T-pieces (nor more complicated constructions), which connect two or more pipes to one (or vice versa) are allowed. Finally, Alice connects a water tap to one of her ends of the pipes, e.g., to pipe 3 and she turns on the tap. Alice and Bob observe which of the two gardens gets sprinkled. It is easy to see that since Alice and Bob only use simple one-to-one connections, there is no "deadlock" possible and the water will indeed eventually come out on one of the two sides. Which side it is obviously depends on the respective local connections.

Now, say that Alice connects her ends of the pipes (and the tap) not in a *fixed* way, but her choice of connections depends on a private bit string $x \in \{0,1\}^n$; for different strings x and x', she may connect her ends of the pipes differently. Similarly, Bob's choice which pipes to connect depends on a private bit string $y \in \{0,1\}^n$. These strategies then specify a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ as follows: $f(x,y)$ is defined to be 0 if, using the connections determined by x and y respectively, the water ends up on Alice's side, and $f(x,y)$ is 1 if the water ends up on Bob's side.

Switching the point of view, we can now take an *arbitrary* Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ and ask: How can f be computed in the garden-hose model? How do Alice and Bob have to choose their local connections, and how many water pipes are necessary for computing f in the garden-hose model? We stress that Alice's choice for which pipes to connect may only depend on x but not on y, and vice versa; this is what makes the above questions non-trivial.

In this paper, we introduce and put forward the notion of *garden-hose complexity*. For a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, the garden-hose complexity $GH(f)$ of f is defined to be the minimal number s of water pipes needed to compute f in the garden-hose model. It is not too hard to see that $GH(f)$ is well defined (and finite) for any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$.

This new complexity notion opens up a large spectrum of natural problems and questions. What is the (asymptotic or exact) garden-hose complexity of natural functions, like equality, inner product *etc.*? How hard is it to compute the garden-hose complexity in general? How is the garden-hose complexity related to other complexity measures? What is the impact of randomness, or entanglement? Some of these questions we answer in this work; others remain open.

Lower and upper bounds.

We show a near-linear $\Omega(n/\log(n))$ lower bound on the garden-hose complexity $GH(f)$ for a natural class of functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. This class of functions includes the mod-2 inner-product function, the equality function, and the majority function. For the former two, this bound is rather tight, in that for these two functions we also show a linear upper bound. For the majority function, the best upper bound we know is quadratic. Recently, Margalit and Matsliah improved our upper bound for the equality function with the help of the IBM SAT-Solver [23] to approximately $1.448n$, and the question of how many water pipes are necessary to compute the equality function in the garden-hose model featured as April 2012's "Ponder This" puzzle on the IBM website[1]. The *exact* garden-hose complexity of the equality function is still unknown, though; let alone of other functions.

By using a counting argument, we show the existence of functions with *exponential* garden-hose complexity, but so far, no such function is known explicitly.

Connections to other complexity notions.

We show that every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ that is *log-space computable* has polynomial garden-hose complexity. And, vice versa, we show that every function with polynomial garden-hose complexity is, up to local pre-processing, log-space computable. As a consequence, we obtain that the set of functions with polynomial garden-hose complexity is exactly given by the functions that can be computed by arbitrary local pre-processing followed by a log-space computation.

We also point out a connection to communication complexity by observing that, for any function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, the *one-way communication complexity* of f is a lower bound on $GH(f)\log(GH(f))$.

Randomized and quantum garden-hose complexity.

We consider the following natural variants of the garden-hose model. In the *randomized* garden-hose model, Alice and Bob additionally share a uniformly random string r, and the water is allowed to come out on the wrong side with small probability ε. Similarly, in the *quantum* garden-hose model, Alice and Bob additionally hold an arbitrary entangled quantum state and their wiring strategies can depend on the outcomes of measuring this state before playing the garden-hose game. Again, the water is allowed to come out on the wrong side with small probability ε. Based on the observed connections of the garden-hose complexity to log-space computation and to one-way communication complexity, we can show that the resulting notion of *randomized* garden-hose complexity $GH_\varepsilon(f)$ is polynomially related to $GH(f)$. For the resulting notion of *quantum* garden-hose complexity $GH_\varepsilon^Q(f)$, we can show a separation (for a partial function) from $GH_\varepsilon(f)$.

Application to quantum position-verification.

Finally, we show an interesting connection between the garden-hose model and the (in)security of a certain class of *quantum position-verification* schemes. The goal of position-verification is to verify the geographical position *pos* of a prover P by means of sending messages to P and measuring the time it takes P to reply. Position-verification with security against collusion attacks, where different attacking parties collaborate in order to try to fool the verifiers, was shown to be impossible in the classical setting by [11], and in the quantum setting by [5], if there is no restriction put upon the attackers. In the quantum setting, this raises the question whether there exist schemes that are secure in case the attackers' quantum capabilities are limited.

We consider a simple and natural class of quantum position-verification schemes; each scheme $\mathsf{PV}^f_{\text{qubit}}$ in the class is specified by a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. These schemes may have the desirable property that the more classical resources the honest users use to faithfully execute the scheme, the more quantum resources the adversary needs in order to break it. It turns out that there is a one-to-one correspondence between the garden-hose game and a certain class of attacks on these schemes, where the attackers teleport a qubit back and forth using a supply of EPR pairs. As an immediate consequence, the (quantum) garden-hose complexity of f gives an upper bound on the number of EPR pairs the attackers need in order to break the scheme $\mathsf{PV}^f_{\text{qubit}}$. As a corollary, we obtain the following interesting connection between proving the security of quantum protocols and classical complexity theory: If there is an f in P such that there is no way of attacking scheme $\mathsf{PV}^f_{\text{qubit}}$ using a polynomial number of EPR pairs, then P $\neq$ L. Vice versa, our approach may lead to practical secure quantum position-verification schemes whose security is based on classical complexity-theoretical assumptions such as P is different from L. However, so far it is still unclear whether the garden-hose complexity by any means gives a *lower bound* on the number of EPR pairs needed; this remains to be further investigated.

2. THE GARDEN-HOSE MODEL

2.1 Definition

Alice and Bob get n-bit input strings x and y, respectively. Their goal is to "compute" an agreed-upon Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ on these inputs, in the following way. Alice and Bob have s water pipes between them, and, depending on their respective classical inputs x and y, they connect (some of) their ends of the pipes with pieces of hose. Additionally, Alice connects a water tap to one of the pipes. They succeed in computing f in the garden-hose model, if the water comes out on Alice's side whenever $f(x,y) = 0$, and the water comes out on Bob's side whenever $f(x,y) = 1$.

[1] `http://ibm.co/I7yvMz`

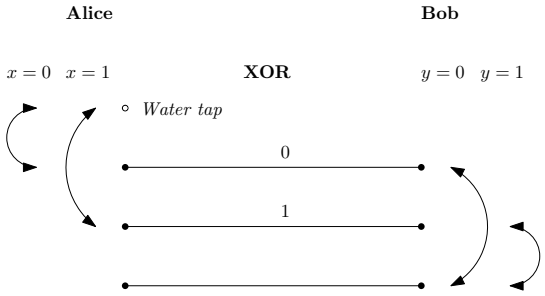

Figure 1: Computing the XOR function in the garden-hose model using three water pipes. If Alice's input bit x is 0, she connects the water tap to the first water pipe labeled "0". In case $x=1$, she connects the tap to the second pipe labeled "1".

Note that it does not matter out of which pipe the water flows, only on which side it flows. What makes the game non-trivial is that Alice and Bob must do their "plumbing" based on their local input only, and they are not allowed to communicate. We refer to Figure 1 for an illustration of computing the XOR function in the garden-hose model.

We formalize the above description of the garden-hose game, given in terms of pipes and hoses *etc.*, by means of rigorous graph-theoretic terminology. However, we feel that the above terminology captures the notion of a garden-hose game very well, and thus we sometimes use the above "watery" terminology. We start with a balanced bi-partite graph $(A \cup B, E)$ which is 1-regular and where the cardinality of A and B is $|A| = |B| = s$, for an arbitrary large $s \in \mathbb{N}$. We slightly abuse notation and denote both the vertices in A and in B by the integers $1, \ldots, s$. If we need to distinguish $i \in A$ from $i \in B$, we use the notation i^A and i^B. We may assume that E consists of the edges that connect $i \in A$ with $i \in B$ for every $i \in \{1, \ldots, s\}$, i.e., $E = \left\{\left\{i^A, i^B\right\} : 1 \leq i \leq s\right\}$. These edges in E are the *pipes* in the above terminology. We now extend the graph to $(A_\circ \cup B, E)$ by adding a vertex 0 to A, resulting in $A_\circ = A \cup \{0\}$. This vertex corresponds to the *water tap*, which Alice can connect to one of the pipes. Given a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, consider two functions $E_{A_\circ}$ and E_B; both take as input a string in $\{0,1\}^n$ and output a set of edges (without self loops). For any $x, y \in \{0,1\}^n$, $E_{A_\circ}(x)$ is a set of edges on the vertices $A_\circ$ and $E_B(x)$ is a set of edges on the vertices B, so that the resulting graphs $(A_\circ, E_{A_\circ}(x))$ and $(B, E_B(y))$ have maximum degree at most 1. $E_{A_\circ}(x)$ consists of the *connections* among the pipes (and the tap) on Alice's side (on input x), and correspondingly for $E_B(y)$. For any $x, y \in \{0,1\}^n$, we define the graph $G(x,y) = (A_\circ \cup B, E \cup E_{A_\circ}(x) \cup E_B(y))$ by adding the edges $E_{A_\circ}(x)$ and $E_B(y)$ to E. $G(x,y)$ consists of the pipes with the connections added by Alice and Bob. Note that the vertex $0 \in A_\circ$ has degree at most 1, and the graph $G(x,y)$ has maximum degree at most two 2; it follows that the maximal path $\pi(x,y)$ that starts at the vertex $0 \in A_\circ$ is uniquely determined. $\pi(x,y)$ represents the flow of the water, and the endpoint of $\pi(x,y)$ determines whether the water comes out on Alice or on Bob's side (depending on whether the final vertex is in $A_\circ$ or in B).

DEFINITION 2.1. *A* garden-hose game *is given by a graph function $G : (x,y) \mapsto G(x,y)$ as described above. The number of pipes s is called the* size *of G, and is denoted as $s(G)$. A garden-hose game G is said to* compute *a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ if the endpoint of the maximal path $\pi(x,y)$ starting at 0 is in $A_\circ$ whenever $f(x,y) = 0$ and in B whenever $f(x,y) = 1$.*

DEFINITION 2.2. *The deterministic* garden-hose complexity *of a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is the size $s(G)$ of the smallest garden-hose game G that computes f. We denote it by $GH(f)$.*

2.2 Upper and Lower Bounds

In this section, we present upper and lower bounds on the number of pipes required to compute some particular (classes of) functions in the garden-hose model. We first give a simple upper bound on $GH(f)$ which is implicitly proven in the attack on Scheme II in [18].

PROPOSITION 2.3. *For every Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, the garden-hose complexity $GH(f)$ is at most $2^n + 1$.*

PROOF. We identify $\{0,1\}^n$ with $\{1, \ldots, 2^n\}$ in the natural way. For $s = 2^n + 1$ and the resulting bipartite graph $(A_\circ \cup B, E)$, we can define $E_{A_\circ}$ and E_B as follows. $E_{A_\circ}(x)$ is set to $\{(0,x)\}$, meaning that Alice connects the tap with the pipe labeled by her input x. To define E_B, group the set $Z(y) = \{a \in \{0,1\}^n : f(a,y) = 0\}$ arbitrarily into disjoint pairs $\{a_1, a_2\} \cup \{a_3, a_4\} \cup \ldots \cup \{a_{\ell-1}, a_\ell\}$ and set $E_B(y) = \{\{a_1, a_2\}, \{a_3, a_4\}, \ldots, \{a_{\ell-1}, a_\ell\}\}$. If $\ell = |Z(y)|$ is odd so that the decomposition into pairs results in a left-over $\{a_\ell\}$, then a_ℓ is connected with the "reserve" pipe labeled by 2^n+1.

By construction, if $x \in Z(y)$ then $x = a_i$ for some i, and thus pipe $x = a_i$ is connected on Bob's side with pipe a_{i-1} or a_{i+1}, depending on the parity of i, or with the "reserve" pipe, and thus $\pi(x,y)$ is of the form $\pi(x,y) = (0, x^A, x^B, v^B, v^A)$, ending in $A_\circ$. On the other hand, if $x \notin Z(y)$, then pipe x is not connected on Bob's side, and thus $\pi(x,y) = (0, x^A, x^B)$, ending in B. This proves the claim. □

We notice that we can extend this proof to show that the garden-hose complexity $GH(f)$ is at most $2^{D(f)+1} - 1$, where $D(f)$ is the deterministic communication complexity of f. See Appendix A for a sketch of the method.

DEFINITION 2.4. *We call a function f* injective for Alice, *if for every two different inputs x and x' there exists y such that $f(x,y) \neq f(x',y)$. We define* injective for Bob *in an analogous way: for every $y \neq y'$, there exists x such that $f(x,y) \neq f(x,y')$ holds.*

PROPOSITION 2.5. *If f is injective for Bob or f is injective for Alice, then*[2]

$$GH(f) \log(GH(f)) \geq n\,.$$

PROOF. We give the proof when f is injective for Bob. The proof for the case where f is injective for Alice is the same. Consider a garden-hose game G that computes f. Let s be its size $s(G)$. Since, on Bob's side, every pipe is connected to at most one other pipe, there are at most $s^s = 2^{s \log(s)}$ possible choices for $E_B(y)$, i.e., the set of connections on Bob's side. Thus, if $2^{s \log(s)} < 2^n$, it follows from the pigeonhole principle that there must exist y and y' in $\{0,1\}^n$ for which $E_B(y) = E_B(y')$, and thus for which $G(x,y) =$

[2]All logarithms in this paper are with respect to base 2.

$G(x, y')$ for all $x \in \{0,1\}^n$. But this cannot be since G computes f and $f(x, y) \neq f(x, y')$ for some x due to the injectivity for Bob. Thus, $2^{s \log(s)} \geq 2^n$ which implies the claim. □

We can use this result to obtain an almost linear lower bound for several functions that are often studied in communication complexity settings such as:

- Bitwise inner product: $\mathrm{IP}(x, y) = \sum_i x_i y_i \pmod 2$
- Equality: $\mathrm{EQ}(x, y) = 1$ if and only if $x = y$
- Majority: $\mathrm{MAJ}(x, y) = 1$ if and only if $\sum_i x_i y_i \geq \lceil \frac{n}{2} \rceil$

The first two of these functions are injective for both Alice and Bob, while majority is injective for inputs of Hamming weight at least $n/2$, giving us the following corollary.

COROLLARY 2.6. *The functions bitwise inner product, equality and majority have garden-hose complexity in* $\Omega(\frac{n}{\log(n)})$.

By considering the water pipes that actually get wet, one can show a lower bound of n pipes for equality [25]. On the other hand, we can show upper bounds that are linear for the bitwise inner product and equality, and quadratic in case of majority. We refer to [29] for the proof of the following proposition.

PROPOSITION 2.7. *In the garden-hose model, the equality function can be computed with* $3n+1$ *pipes, the bitwise inner product with* $4n+1$ *pipes and majority with* $(n+2)^2$ *pipes.*

In general, garden-hose protocols can be transformed into (one-way) communication protocols by Alice sending her connections $E_{A_\circ}(x)$ to receiver Bob, which will require at most $GH(f)\log(GH(f))$ bits of communication. Bob can then locally compute the function by combining Alice's message with $E_B(y)$ and checking where the water exits.[3] We summarize this observation in the following proposition.

PROPOSITION 2.8. *Let* $D^1(f)$ *denote the deterministic one-way communication complexity of* f. *Then,*

$$D^1(f) \leq GH(f)\log(GH(f))\,.$$

As a consequence, lower bounds on the communication complexity carry over to the garden-hose complexity (up to logarithmic factors). Notice that this technique will never give lower bounds that are better than linear, as problem in communication complexity can always be solved by sending the entire input to the other party. It is an interesting open problem to show super-linear lower bounds in the garden-hose model, e.g. for the majority function.

PROPOSITION 2.9.
There exist functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *for which* $GH(f)$ *is exponential.*

PROOF. The existence of functions with an exponential garden-hose complexity can be shown by a simple counting argument. There are $2^{2^{2n}}$ different functions $f(x, y)$. For a given size $s = s(G)$ of G, for every $x \in \{0,1\}^n$, there are at most $(s+1)^{s+1}$ ways to choose the connections $E_{A_\circ}(x)$ on Alice's side, and thus there are at most $((s+1)^{s+1})^{2^n} = 2^{2^n(s+1)\log(s+1)}$ ways to choose the function $E_{A_\circ}$. Similarly for E_B, there are at most $2^{2^n s \log(s)}$ ways to choose E_B. Thus, there are at most $2^{2\cdot 2^n(s+1)\log(s+1)}$ ways to choose G of size s. Clearly, in order for every function f to have a G of size s that computes it, we need that $2\cdot 2^n(s+1)\log(s+1) \geq 2^{2n}$, and thus that $(s+1)\log(s+1) \geq 2^{n-1}$, which means that s must be exponential. □

2.3 Polynomial Garden-Hose Complexity and Log-Space Computations

A family of Boolean functions $\{f_n\}_{n\in\mathbb{N}}$ is *log-space computable* if there exists a deterministic Turing machine M and a constant c, such that for any n-bit input x, M outputs the correct output bit $f_n(x)$, and at most $c \cdot \log n$ locations of M's work tapes are ever visited by M's head during computation.

DEFINITION 2.10. *We define* $\mathrm{L}_{(2)}$, *called* logarithmic space with local pre-processing, *to be the class of Boolean functions* $f(x, y)$ *for which there exists a Turing machine* M *and two* arbitrary *functions* $\alpha(x), \beta(y)$, *such that*[4] $M(\alpha(x), \beta(y)) = f(x, y)$ *and* $M(\alpha(x), \beta(y))$ *runs in space logarithmic in the size of the original inputs* $|x| + |y|$.

This definition can be extended in a natural way by considering Turing machines and circuits corresponding to various complexity classes, and by varying the number of players. For example, a construction as in Proposition 2.3 and a similar reasoning as in Proposition 2.14 below can be used to show that every Boolean function is contained in $\mathrm{PSPACE}_{(2)}$. As main result of this section, we show that our newly defined class $\mathrm{L}_{(2)}$ is equivalent to functions with polynomial garden-hose complexity. We leave it for future research to study intermediate classes such as $\mathrm{AC}^0_{(2)}$ which are related to the polynomial hierarchy of communication complexity [1].

THEOREM 2.11. *The set of functions* f *with polynomial garden-hose complexity* $GH(f)$ *is equal to* $\mathrm{L}_{(2)}$.

The two directions of the theorem follow from Theorem 2.12 and Proposition 2.14.

THEOREM 2.12. *If* $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ *is log-space computable, then* $GH(f)$ *is polynomial in* n.

PROOF SKETCH, FULL PROOF IN APPENDIX B.1.
Let M be the deterministic log-space Turing machine deciding $f(x, y) = 0$. Using techniques from [19], M can be made *reversible* incurring only a constant loss in space. As M is a log-space machine, it has at most polynomially many configurations. The idea for the garden-hose strategy is to label the pipes with those configurations of the machine M where the input head of M "switches sides" from the x-part of the

[3] In fact, garden-hose protocols can even be transformed into communication protocols in the more restrictive *simultaneous-message-passage* model, where Alice and Bob send simultaneous messages consisting of their connections $E_{A_\circ}(x)$ and $E_B(y)$ to the referee who then computes the function. The according statements of Propositions 2.8, 2.19 and 2.20 can be derived analogously.

[4] For simplicity of notation, we give two arguments to the Turing machine whose concatenation is interpreted as the input.

input to the y-part or vice versa. Thanks to the reversibility of M, the players can then use one-to-one connections to wire up (depending on their individual inputs) the open ends of the pipes on their side, so that eventually the water flow corresponds to M's computation of $f(x,y)$. □

In the garden-hose model, we allow Alice and Bob to locally pre-process their inputs before computing their wiring. Therefore, it immediately follows from Theorem 2.12 that any function f in $\mathrm{L}_{(2)}$ has polynomial garden-hose complexity, proving one direction of Theorem 2.11.

We saw in Proposition 2.9 that there exist functions with large garden-hose complexity. However, a negative implication of Theorem 2.12 is that proving the existence of a *polynomial-time computable* function f with exponential garden-hose complexity is at least as hard as separating L from P, a long-standing open problem in complexity theory.

COROLLARY 2.13. *If there exists a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ in P that has super-polynomial garden-hose complexity, then $P \neq L$.*

It remains to prove the other inclusion of Theorem 2.11.

PROPOSITION 2.14. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a Boolean function. If $GH(f)$ is polynomial (in n), then f is in $\mathrm{L}_{(2)}$.*

PROOF. Let G be the garden-hose game that achieves $s(G) = GH(f)$. We write s for $s(G)$, the number of pipes, and we let $E_{A_\circ}$ and E_B be the underlying edge-picking functions, which on input x and y, respectively, output the connections that Alice and Bob apply to the pipes. Note that by assumption, s is polynomial. Furthermore, by the restrictions on $E_{A_\circ}$ and E_B, on any input, they consist of at most $(s+1)/2$ connections.

We need to show that f is of the form $f(x,y) = g(\alpha(x), \beta(y))$, where α and β are arbitrary functions $\{0,1\}^n \to \{0,1\}^m$, $g : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ is log-space computable, and m is polynomial in n. We define α and β as follows. For any $x, y \in \{0,1\}^n$, $\alpha(x)$ is simply a natural encoding of $E_{A_\circ}(x)$ into $\{0,1\}^m$, and $\beta(y)$ is a natural encoding of $E_B(y)$ into $\{0,1\}^m$. In the hose-terminology we say that $\alpha(x)$ is a binary encoding of the connections of Alice, and $\beta(y)$ is a binary encoding of the connections of Bob. Obviously, these encodings can be done with m of polynomial size. Given these encodings, finding the endpoint of the maximum path $\pi(x,y)$ starting in 0 can be done with logarithmic space: at any point during the computation, the Turing machine only needs to maintain a pointer to the position of the water and a binary flag to remember on which side of the input tape the head is. Thus, the function g that computes $g(\alpha(x), \beta(y)) = f(x,y)$ is log-space computable in m and thus also in n. □

2.4 Randomized Garden-Hose Complexity

It is natural to study the setting where Alice and Bob share a common random string and are allowed to err with some probability ε. More formally, we let the players' local strategies $E_{A_\circ}(x,r)$ and $E_B(y,r)$ depend on the shared randomness r and write $G_r(x,y) = f(x,y)$ if the resulting garden-hose game $G_r(x,y)$ computes $f(x,y)$.

DEFINITION 2.15. *Let r be the shared random string. The* randomized garden-hose complexity *of a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is the size $s(G_r)$ of the smallest garden-hose game G_r such that $\forall x,y : \Pr_r[G_r(x,y) = f(x,y)] \geq 1-\varepsilon$. We denote this minimal size by $GH_\varepsilon(f)$.*

In Appendix B.2, we show that the error probability can be made exponentially small by repeating the protocol a polynomial number of times.

PROPOSITION 2.16. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function such that $GH_\varepsilon(f)$ is polynomial in n, with error $\varepsilon \leq \frac{1}{2} - n^{-c}$ for a constant $c > 0$. For every constant $d > 0$ there exists a polynomial $q(\cdot)$ such that $GH_{2^{-n^d}}(f) \leq q\big(GH_\varepsilon(f)\big)$.*

Using this result, any randomized strategy can be turned into a deterministic strategy with only a polynomial overhead in the number of pipes.

PROPOSITION 2.17. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function such that $GH_\varepsilon(f)$ is polynomial in n and $\varepsilon \leq \frac{1}{2} - n^c$ for a constant $c > 0$. Then there exists a polynomial $q(\cdot)$ such that $GH(f) \leq q\big(GH_\varepsilon(f)\big)$.*

PROOF SKETCH. By Proposition 2.16 there exists a randomized garden-hose protocol $G_r(x,y)$ of size $q(GH_\varepsilon(f))$ with error probability at most 2^{-2n-1}. The probability for a random string r to be wrong for all inputs is at most $2^{2n} \cdot 2^{-2n-1} < 1$. In particular, there exists a string $\hat{r}$ which works for every input (x,y). □

Using this Proposition 2.17, we conclude that the lower bound from Proposition 2.9 carries over to the randomized setting.

COROLLARY 2.18.
There exist functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ for which $GH_\varepsilon(f)$ is exponential.

With the same reasoning as in Proposition 2.8, we get that lower bounds on the randomized one-way communication complexity with public shared randomness carry over to the randomized garden-hose complexity (up to a logarithmic factor).

PROPOSITION 2.19. *Let $R^{1,\mathrm{pub}}_\varepsilon(f)$ denote the minimum communication cost of a one-way-communication protocol which computes f with an error ε using public shared randomness. Then, $R^{1,\mathrm{pub}}_\varepsilon(f) \leq GH_\varepsilon(f)\log(GH_\varepsilon(f))$.*

For instance, the linear lower bound $R^{pub}_\varepsilon(IP) \in \Omega(n)$ from [12] for the inner-product function yields $GH_\varepsilon(IP) \in \Omega(\frac{n}{\log n})$.

2.5 Quantum Garden-Hose Complexity

Let us consider the setting where Alice and Bob share an arbitrary entangled quantum state besides their water pipes. Depending on their respective inputs x and y, they can perform local quantum measurements on their parts of the entangled state and wire up the pipes depending on the outcomes of these measurements. We denote the resulting *quantum garden-hose complexity* with $GH^Q(f)$ in the deterministic case and with $GH^Q_\varepsilon(f)$ if errors are allowed.

With the same reasoning as in Proposition 2.8, we get that lower bounds on the entanglement-assisted one-way communication complexity carry over to the quantum garden-hose complexity (up to a logarithmic factor).

PROPOSITION 2.20. *For $\varepsilon \geq 0$, let $Q^1_\varepsilon(f)$ denote the minimum cost of an entanglement-assisted one-way communication protocol which computes f with an error ε. Then, $Q^1_\varepsilon(f) \leq GH^Q_\varepsilon(f)\log(GH^Q_\varepsilon(f))$.*

For instance, the lower bound $Q^1_\varepsilon(IP) \in \Omega(n)$ which follows from results in [13] gives $GH^Q_\varepsilon(IP) \in \Omega(n/\log n)$. For the disjointness function, $Q^1_\varepsilon(DISJ) \in \Omega(\sqrt{n})$ from [26] implies $GH^Q_\varepsilon(DISJ) \in \Omega(\sqrt{n}/\log n)$.

In Appendix D, we present partial functions which give a separation between the quantum and classical garden-hose complexity in the deterministic and in the randomized setting.

THEOREM 2.21. *There exist partial Boolean functions f and g such that*

1. $GH^Q(f) \in O(\log n)$ *and* $GH(f) \in \Omega(\frac{n}{\log n})$,
2. $GH^Q_\varepsilon(g) \in O(\log n)$ *and* $GH_\varepsilon(g) \in \Omega(\frac{\sqrt{n}}{\log n})$.

3. APPLICATION TO POSITION-BASED QUANTUM CRYPTOGRAPHY

The goal of *position-based cryptography* is to use the geographical position of a party as its only "credential". For example, one would like to send a message to a party at a geographical position *pos* with the guarantee that the party can decrypt the message only if he or she is physically present at *pos*. The general concept of position-based cryptography was introduced by Chandran, Goyal, Moriarty and Ostrovsky [11].

A central task in position-based cryptography is the problem of *position-verification*. We have a *prover* P at position *pos*, wishing to convince a set of *verifiers* $V_0, \ldots, V_k$ (at different points in geographical space) that P is indeed at that position *pos*. The prover can run an interactive protocol with the verifiers in order to convince them. The main technique for such a protocol is known as distance bounding [3]. In this technique, a verifier sends a random nonce to P and measures the time taken for P to reply back with this value. Assuming that the speed of communication is bounded by the speed of light, this technique gives an upper bound on the distance of P from the verifier.

The problem of secure position-verification has been studied before in the field of wireless security, and there have been several proposals for this task ([3, 27, 30, 7] [9, 28, 31, 8]). However, [11] shows that there exists no protocol for secure position-verification that offers security in the presence of *multiple colluding* adversaries. In other words, the set of verifiers cannot distinguish between the case when they are interacting with an honest prover at *pos* and the case when they are interacting with multiple colluding dishonest provers, none of which is at position *pos*.

The impossibility result of [11] relies heavily on the fact that an adversary can locally store all information he receives *and* at the same time share this information with other colluding adversaries, located elsewhere. Due to the quantum no-cloning theorem, such a strategy will not work in the quantum setting, which opens the door to secure protocols that use quantum information. The quantum model was first studied by Kent et al. under the name of "quantum tagging" [17, 18]. Several schemes were developed [18, 21, 10, 22, 20] and proven later to be insecure. Finally in [5] it was shown that in general no unconditionally secure quantum position-verification scheme is possible. Any scheme can be broken using a double exponential amount of EPR pairs in the size of the messages of the protocol. Later, Beigi and König improved in [2] the double exponential dependence to single exponential making use of port-based teleportation [15, 16].

Due to the exponential overhead in EPR pairs, the general no-go theorem does not rule out the existence of quantum schemes that are secure for all practical purposes. Such schemes should have the property that the protocol, when followed honestly, is feasible, but cheating the protocol requires unrealistic amounts of resources, for example EPR pairs or time.

3.1 A Single-Qubit Scheme

Our original motivation for the garden-hose model was to study a particular quantum protocol for secure position verification, described in Figure 2. The protocol is of the generic form described in Section 3.2 of [5]. In Step 0, the verifiers prepare challenges for the prover. In Step 1, they send the challenges, timed in such a way that they all arrive at the same time at the prover. In Step 2, the prover computes his answers and sends them back to the verifiers. Finally, in Step 3, the verifiers verify the timing and correctness of the answer.

As in [5], we consider here for simplicity the case where all players live in one dimension, the basic ideas generalize to higher dimensions. In one dimension, we can focus on the case of two verifiers V_0, V_1 and an honest prover P in between them.

We minimize the amount of quantum communication in that only one verifier, say V_0, sends a qubit to the prover, whereas both verifiers send classical n-bit strings $x, y \in \{0,1\}^n$ that arrive at the same time at the prover. We fix a publicly known Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ whose output $f(x,y)$ decides whether the prover has to return the qubit (unchanged) to verifier V_0 (in case $f(x,y) = 0$) or to verifier V_1 (if $f(x,y) = 1$).

0. V_0 randomly chooses two n-bit strings $x, y \in \{0,1\}^n$ and privately sends y to V_1. V_0 prepares an EPR pair $(|0\rangle_V|0\rangle_P + |1\rangle_V|1\rangle_P)/\sqrt{2}$. If $f(x,y) = 0$, V_0 keeps the qubit in register V. Otherwise, V_0 sends the qubit in register V privately to V_1.
1. V_0 sends the qubit in register P to the prover P together with the classical n-bit string x. V_1 sends y so that it arrives at the same time as the information from V_0 at P.
2. P evaluates $f(x,y) \in \{0,1\}$ and routes the qubit to $V_{f(x,y)}$.
3. V_0 and V_1 accept if the qubit arrives in time at the correct verifier and the Bell measurement of the received qubit together with the qubit in V yields the correct outcome.

Figure 2: Position-verification scheme $\mathsf{PV}^f_{\mathbf{qubit}}$ using one qubit and classical n-bit strings.

The motivation for considering this protocol is the following: As the protocol uses only one qubit which needs to be correctly routed, the honest prover's quantum actions are trivial to perform. His main task is evaluating a classical Boolean function f on classical inputs x and y whose bit size n can be easily scaled up. On the other hand, our results suggest that the adversary's job of successfully attacking the protocol becomes harder and harder for larger input strings x, y.

3.2 Connection to the Garden-Hose Model

In order to analyze the security of the protocol $\mathsf{PV}^f_{\text{qubit}}$, we define the following communication game in which Alice and Bob play the roles of the adversarial attackers of $\mathsf{PV}^f_{\text{qubit}}$. Alice starts with an unknown qubit $|\phi\rangle$ and a classical n-bit string x while Bob holds the n-bit string y. They also share some quantum state $|\eta\rangle_{AB}$ and both players know the Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. The players are allowed one round of simultaneous classical communication combined with arbitrary local quantum operations. When $f(x,y) = 0$, Alice should be in possession of the qubit $|\phi\rangle$ at the end of the protocol and on $f(x,y) = 1$, Bob should hold it.

As a simple example consider the case where $f(x,y) = x \oplus y$, the XOR function, with 1-bit inputs x and y. Alice and Bob then have the following way of performing this task perfectly by using a pre-shared quantum state consisting of three EPR pairs (three ebits). Label the first two EPR pairs 0 and 1. Alice teleports[5] $|\phi\rangle$ to Bob using the pair labeled with her input x. This yields measurement result $i \in \{0,1,2,3\}$, while Bob teleports his half of the EPR pair labeled y to Alice using his half of the third EPR pair while obtaining measurement outcome $j \in \{0,1,2,3\}$. In the round of simultaneous communication, both players send the classical measurement results and their inputs x or y to the other player. If $x \oplus y = 1$, i.e. x and y are different bits, Bob can apply the Pauli operator σ_i to his half of the EPR pair labeled $x = y \oplus 1$, correctly recovering $|\phi\rangle$. Similarly, if $x \oplus y = 0$, it is easy to check that Alice can recover the qubit by applying $\sigma_i\sigma_j$ to her half of the third EPR pair.

If Alice and Bob are *constrained* to the types of actions in the example above, i.e., if they are restricted to teleporting the quantum state back and forth depending on their classical inputs, there is a one-to-one correspondence between attacking the position-verification scheme $\mathsf{PV}^f_{\text{qubit}}$ and computing the function f in the garden-hose model. The quantum strategy for attacking $\mathsf{PV}^f_{\text{qubit}}$ in the example above exactly corresponds to the strategy depicted in Figure 1 for computing the XOR-function in the garden-hose model.

More generally, we can translate any strategy of Alice and Bob in the garden-hose model to a perfect quantum attack of $\mathsf{PV}^f_{\text{qubit}}$ by using one EPR pair per pipe and performing Bell measurements where the players connect the pipes.

Our hope is that also the converse is true: if many pipes are required to compute f (say we need super-polynomially many), then the number of EPR pairs needed for Alice and Bob to successfully break $\mathsf{PV}^f_{\text{qubit}}$ with probability close to 1 by means of an *arbitrary* attack (not restricted to Bell measurements on EPR pairs) should also be super-polynomial.

The examples of (partial) functions from Theorem 2.21 show that the classical garden-hose complexity $GH(f)$ does not capture the amount of EPR pairs required to attack $\mathsf{PV}^f_{\text{qubit}}$. It is conceivable that one can show that arbitrary attacks can be cast in the quantum garden-hose model and hence, the quantum garden-hose complexity $GH^Q_\varepsilon(f)$ (or a variant of it[6]) correctly captures the amount of EPR pairs required to attack $\mathsf{PV}^f_{\text{qubit}}$. We leave this question as an interesting problem for future research.

[5]See Appendix C.1 for a brief introduction to quantum teleportation.

[6]In addition to the number of pipes, one might have to account for the size of the entangled state as well.

We stress that for this application, any polynomial lower bound on the number of required EPR pairs is already interesting.

3.3 Lower Bounds on Quantum Resources to Perfectly Attack $\mathsf{PV}^f_{\text{qubit}}$

In Appendix E, we show that for a function that is injective for Alice or injective for Bob (according to Definition 2.4), the dimension of the quantum state the adversaries need to handle (including possible quantum communication between them) in order to attack protocol $\mathsf{PV}^f_{\text{qubit}}$ perfectly has to be of order at least linear in the classical input size n. In other words, they require at least a logarithmic number of qubits in order to successfully attack $\mathsf{PV}^f_{\text{qubit}}$.

THEOREM 3.1. *Let f be injective for Bob. Assume that Alice and Bob perform a perfect attack on protocol PV^f_{qubit}. Then, the dimension d of the overall state (including the quantum communication) is in $\Omega(n)$.*

In the last subsection, we show that there exist functions for which perfect attacks on $\mathsf{PV}^f_{\text{qubit}}$ requires the adversaries to handle a polynomial amount of qubits.

THEOREM 3.2. *For any starting state $|\psi\rangle$ of dimension d, there exists a Boolean function f on inputs $x, y \in \{0,1\}^n$ such that any perfect attack on PV^f_{qubit} requires d to be exponential in n.*

These results can be seen as first steps towards establishing the desired relation between classical difficulty of honest actions and quantum difficulty of the actions of dishonest players. We leave as future work the generalization of these lower bounds to the more realistic case of imperfect attacks and also to more relevant quantities like some entanglement measure between the players (instead of the dimension of their shared state).

4. CONCLUSION AND OPEN QUESTIONS

The garden-hose model is a new model of communication complexity. We connected functions with polynomial garden-hose complexity to a newly defined class of log-space computations with local pre-processing. Alternatively, the class $\mathrm{L}_{(2)}$ can also be viewed as the set of functions which can be decided in the simultaneous-message-passing (SMP) model where the referee is restricted to log-space computations. Many open questions remain. Can we find better upper and lower bounds for the garden-hose complexity of the studied functions? The constructions given in [29] still leave a polynomial gap between lower and upper bounds for many functions. It would also be interesting to find an explicit function for which the garden-hose complexity is provably super-linear or even exponential, the counting argument in Proposition 2.9 only shows the existence of such functions. It is possible to extend the basic garden-hose model in various ways and consider settings with more than two players, non-Boolean functions or multiple water sources. Furthermore, it is interesting to relate our findings to very recent results about space-bounded communication complexity [4].

Garden-hose complexity is a tool for the analysis of a specific scheme for position-based quantum cryptography. This scheme requires the honest prover to work with only a single qubit, while the dishonest provers potentially have to manipulate a large quantum state, making it an appealing

scheme to further examine. The garden-hose model captures the power of attacks that only use teleportation, giving upper bounds for the general scheme, and lower bounds when restricted to these attacks.

An interesting additional restriction on the garden-hose model would involve limiting the computational power of Alice and Bob. For example to polynomial time, or to the output of quantum circuits of polynomial size. Bounding not only the amount of entanglement, but also the amount of computation with a realistic limit might yield stronger security guarantees for the cryptographic schemes.

5. ACKNOWLEDGMENTS

HB is supported by an NWO Vici grant and the EU project QCS. FS is supported by the NWO DIAMANT project. CS is supported by an NWO Veni grant. We thank Louis Salvail for useful discussions about the protocol $\mathsf{PV}^{f}_{\text{qubit}}$.

6. REFERENCES

[1] L. Babai, P. Frankl, and J. Simon. Complexity classes in communication complexity theory. In *Foundations of Computer Science, 1986., 27th Annual Symposium on*, pages 337–347, 1986.

[2] S. Beigi and R. König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT'93*, pages 344–359. Springer, 1994.

[4] J. Brody, S. Chen, P. A. Papakonstantinou, H. Song, and X. Sun. Space-bounded communication complexity. to appear at ITCS 2013, 2012.

[5] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: Impossibility and constructions. In P. Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 429–446. Springer Berlin / Heidelberg, 2011.

[6] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. classical communication and computation. In *Proceedings of the thirtieth annual ACM symposium on Theory of computing*, STOC '98, pages 63–68, New York, NY, USA, 1998. ACM.

[7] L. Bussard. *Trust Establishment Protocols for Communicating Devices*. PhD thesis, Eurecom-ENST, 2004.

[8] S. Capkun, M. Cagalj, and M. Srivastava. Secure localization with hidden and mobile base stations. In *IEEE INFOCOM*, 2006.

[9] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM*, pages 1917–1928, 2005.

[10] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky. Position-based quantum cryptography. arXiv:1005.1750v2, May 2010.

[11] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *CRYPTO 2009*, pages 391–407. Springer, 2009.

[12] B. Chor and O. Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM J. Comput.*, 17(2):230–261, Apr. 1988.

[13] R. Cleve, W. v. Dam, M. Nielsen, and A. Tapp. Quantum entanglement and the communication complexity of the inner product function. In *Selected papers from the First NASA International Conference on Quantum Computing and Quantum Communications*, QCQC '98, pages 61–74. Springer-Verlag, 1998.

[14] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, STOC '07, pages 516–525, New York, NY, USA, 2007. ACM.

[15] S. Ishizaka and T. Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101(24):240501, Dec 2008.

[16] S. Ishizaka and T. Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A*, 79(4):042306, Apr 2009.

[17] A. Kent, W. Munro, T. Spiller, and R. Beausoleil. Tagging systems, 2006. US patent nr 2006/0022832.

[18] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011.

[19] K.-J. Lange, P. McKenzie, and A. Tapp. Reversible space equals deterministic space. In *Proceedings of Computational Complexity. Twelfth Annual IEEE Conference*, pages 45–50. IEEE Comput. Soc, Apr. 1997.

[20] H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83(1):012322, Jan 2011.

[21] R. A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81(4):042319, Apr 2010.

[22] R. A. Malaney. Quantum location verification in noisy channels. In *GLOBECOM'10*, pages 1–6, 2010. arXiv:1004.4689v1.

[23] O. Margalit and A. Matsliah. Mage - the CDCL SAT solver developed and used by IBM for formal verification `http://ibm.co/P7qNpC`. personal communication, 2012.

[24] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.

[25] K. Pietrzak. personal communication, 2011.

[26] A. A. Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya Mathematics*, 67(1):145–159, 2003.

[27] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *WiSe'03*, pages 1–10, 2003.

[28] D. Singelee and B. Preneel. Location verification using secure distance bounding protocols. In *IEEE MASS'10*, 2005.

[29] F. Speelman. Position-based quantum cryptography and the garden-hose game. Master's thesis, University of Amsterdam, 2011. arxiv:1210.4353.

[30] A. Vora and M. Nesterenko. Secure location verification using radio broadcast. In *OPODIS'04*, pages 369–383, 2004.

[31] Y. Zhang, W. Liu, Y. Fang, and D. Wu. Secure localization and authentication in ultra-wideband sensor networks. *IEEE Journal on Selected Areas in Communications*, 24:829–835, 2006.

APPENDIX

A. UPPER BOUND BY COMMUNICATION COMPLEXITY

We show that the garden-hose complexity $GH(f)$ of any function f is at most $2^{D(f)+1}-1$, where $D(f)$ is the deterministic communication complexity of f.

Consider a protocol where Alice and Bob alternate in sending one bit. The pipes between Alice and Bob are labeled with all possible non-empty strings of length up to $D(f)$, with one extra reserve pipe.

Let $A_v(x)$ be the bit Alice sends after seeing transcript $v \in \{0,1\}^*$ given input x and let $B_v(x)$ be the bit Bob sends after a transcript v on input y. (Since Alice and Bob alternate, Alice sends a bit on even length transcripts, while Bob sends when the transcript has odd length.) Alice connects the tap to 0 or 1 depending on the first sent bit. Then, Alice makes connections

$$\{\{v, vA_v(x)\} | v \in \{0,1\}^* \text{ with } |v| \text{ even and } 1 \leq |v| \leq D(f)\}.$$

Here $vA_v(x)$ is the concatenation of v and $A_v(x)$. Bob's connections are given by the set

$$\{\{v, vB_v(x)\} | v \in \{0,1\}^* \text{ with } |v| \text{ odd and } 1 \leq |v| \leq D(f)\}.$$

Now, for all transcripts of length $D(f)$, Alice knows the function outcome. (Assume $D(f)$ is even for simplicity.) For those $2^{D(f)}$ pipes she can route the water to the correct side by connecting similar outcomes, as in the proof of Proposition 2.3, using one extra reserve pipe. This brings the total used pipes to $1+\sum_{i=1}^{D(f)} 2^i = 2^{D(f)+1}-1$. The correctness can be verified by comparing the path of the water to the communication protocol: the label of the pipe the water is in, when following it through the pipes for r "steps", is exactly the same as the transcript of the communication protocol when executing it for r rounds.

B. PROOFS

B.1 Proof of Theorem 2.12

THEOREM 2.12 *If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is log-space computable, then $GH(f)$ is polynomial in n.*

PROOF. Let M be a deterministic Turing machine deciding $f(x,y) = 0$. We assume that M's read-only input tape is of length $2n$ and contains x on positions 1 to n and y on positions $n+1$ to $2n$. By assumption M uses logarithmic space on its work tapes.

In this proof, a *configuration* of M is the location of its tape heads, the state of the Turing machine and the content of its work tapes, excluding the content of the read-only input tape. This is a slightly different definition than usual, where the content of the input tape is also part of a configuration. When using the normal definition (which includes the content of all tapes), we will use the term *total configuration*. Any configuration of M can be described using a logarithmic number of bits, because M uses logarithmic space.

A Turing machine is called *deterministic*, if every total configuration has a unique next one. A Turing machine is called *reversible* if in addition to being deterministic, every total configuration also has a unique predecessor. An $S(n)$ space-bounded deterministic Turing machine can be simulated by a reversible Turing machine in space $O(S(n))$ [19]. This means that without loss of generality, we can assume M to be a reversible Turing machine, which is crucial for our construction. Let M also be *oblivious*[7] in the tape head movement on the input tape. This can be done with only a small increase in space by adding a counter.

Alice's and Bob's perfect strategies in the garden-hose game are as follows. They list all configurations where the head of the input tape is on position n coming from position $n+1$. Let us call the set of these configurations C_A. Let C_B be the analogous set of configurations where the input tape head is on position $n+1$ after having been on position n the previous step. Because M is oblivious on its input tape, these sets depend only on the function f, but not on the input pair (x,y). The number of elements of C_A and C_B is at most polynomial, being exponential in the description length of the configurations. Now, for every element in C_A and C_B, the players label a pipe with this configuration. Also label $|C_A|$ pipes ACCEPT and $|C_B|$ of them REJECT. These steps determine the number of pipes needed, Alice and Bob can do this labeling beforehand.

For every configuration in C_A, with corresponding pipe p, Alice runs the Turing machine starting from that configuration until it either accepts, rejects, or until the input tape head reaches position $n+1$. If the Turing machine accepts, Alice connects p to the first free pipe labeled ACCEPT. On a reject, she leaves p unconnected. If the tape head of the input tape reaches position $n+1$, she connects p to the pipe from C_B corresponding to the configuration of the Turing machine when that happens. By her knowledge of x, Alice knows the content of the input tape on positions 1 to n, but not the other half. Alice also runs M from the starting configuration, connecting the water tap to a target pipe with a configuration from C_B depending on the reached configuration.

Bob connects the pipes labeled by C_B in an analogous way: He runs the Turing machine starting with the configuration with which the pipe is labeled until it halts or the position of the input tape head reaches n. On accepting, the pipe is left unconnected and if the Turing machine rejects, the pipe is connected to one of the pipes labeled REJECT. Otherwise, the pipe is connected to the one labeled with the

[7] A Turing machine is called *oblivious*, if the movement in time of the heads only depend on the length of the input, known in advance to be $2n$, but not on the input itself. For our construction we only require the input tape head to have this property.

configuration in C_A, the configuration the Turing machine is in when the head on the input tape reached position n.

In the garden-hose game, only one-to-one connections of pipes are allowed. Therefore, to check that the described strategy is a valid one, the simulations of two different configurations from C_A should never reach the same configuration in C_B. This is guaranteed by the reversibility of M as follows. Consider Alice simulating M starting from different configurations $c \in C_A$ and $c' \in C_A$. We have to check that their simulation can not end at the same $d \in C_B$, because Alice can not connect both pipes labeled c and c' to the same d. Because M is reversible, we can in principle also simulate M backwards in time starting from a certain configuration. In particular, Alice can simulate M backwards starting with configuration d, until the input tape head position reaches $n+1$. The configuration of M at that time can not simultaneously be c and c', so there will never be two different pipes trying to connect to the pipe labeled d.

It remains to show that, after the players link up their pipes as described, the water comes out on Alice's side if M rejects on input (x, y), and that otherwise the water exits at Bob's. We can verify the correctness of the described strategy by comparing the flow of the water directly to the execution of M. Every pipe the water flows through corresponds to a configuration of M when it runs starting from the initial state. So the side on which the water finally exits also corresponds to whether M accepts or rejects. □

B.2 Proof of Proposition 2.16

PROPOSITION 2.16 *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a function such that $GH_\varepsilon(f)$ is polynomial in n, with error $\varepsilon \leq \frac{1}{2} - n^{-c}$ for a constant $c > 0$. For every constant $d > 0$ there exists a polynomial $q(\cdot)$ such that $GH_{2^{-n^d}}(f) \leq q\big(GH_\varepsilon(f)\big)$.*

PROOF. The new protocol $G'_r(x, y)$ takes the majority of $k = 8n^{2c+d}$ outcomes of $G_{r_i}(x, y)$ where $r_1, \ldots, r_k$ are k independent and uniform samples of the random string. We have to establish (i) that taking the majority of k instances of the original protocol indeed gives the correct outcome with probability at least $1 - 2^{-n^d}$ and (ii) that $G'_r(x, y)$ requires only polynomial pipes.

(i) Let X_i be the random variable that equals 1 when $G_{r_i}(x, y) = f(x, y)$ and 0 otherwise. Note that the X_i are independent and identically distributed random variables with expectation $E[X_i] \geq 1 - \varepsilon =: p$. Whenever $\sum_{i=1}^k X_i \geq \frac{k}{2}$ the protocol gives the correct outcome. Use the Chernoff bound to get

$$\Pr\left[\sum_{i=1}^{k} X_i < (1-\zeta)pk\right] \leq e^{-\frac{\zeta^2}{2}pk}$$

for any small ζ. Picking $\zeta = n^{-c}$, so that $(1-\zeta)pk$ is still greater than $\frac{k}{2}$, and filling in k, we can upper bound the probability of failure by

$$e^{-\frac{8n^{2c+d}}{2n^{2c}}p} \leq 2^{-n^d}$$

(ii) In Theorem 2.12 we show that any log-space computable function can be simulated by a polynomial-sized garden-hose strategy. Thus, if checking the majority of k garden-hose strategies can be done in logarithmic space (after local pre-computations by Alice and Bob), then $G'_r(x, y)$ can be computed using a polynomial number of pipes.

Let $A_i = E_{A_\circ}(x, r_i)$ be the local wiring of Alice for strategy G on input x with randomness r_i, and let $B_i = E_B(y, r_i)$. Alice locally generates $(A_1, \ldots, A_k)$ and Bob locally generates $(B_1, \ldots, B_k)$. In the proof of Proposition 2.14 it was shown that simulating the outcome of a single garden-hose strategy (A_i, B_i) can be done in logarithmic space. Here we follow the same construction, but instead of getting the outcome of a single strategy we simulate all k strategies. This can still be done in logarithmic space, since we can re-use the memory needed to simulate each of the k strategies. To find the majority, we need to add a counter to keep track of the simulation outcomes, using only an extra $\log k$ bits of space. □

C. QUANTUM PRELIMINARIES

For Appendices D and E, we assume that the reader is familiar with basic concepts of quantum information theory. We refer to [24] for an introduction and merely fix some notation here.

C.1 Quantum Teleportation

An important example of a 2-qubit state is the *EPR pair*, which is given by $|\Phi\rangle_{AB} = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2} \in \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$ and has the following properties: if qubit A is measured in the computational basis, then a uniformly random bit $x \in \{0,1\}$ is observed and qubit B collapses to $|x\rangle$. Similarly, if qubit A is measured in the Hadamard basis, then a uniformly random bit $x \in \{0,1\}$ is observed and qubit B collapses to $H|x\rangle$.

The goal of quantum teleportation is to transfer a quantum state from one location to another by only communicating classical information. Teleportation requires preshared entanglement among the two locations. To teleport a qubit Q in an arbitrary unknown state $|\psi\rangle_Q$ from Alice to Bob, Alice performs a Bell-measurement on Q and her half of an EPR pair, yielding a classical measurement outcome $k \in \{0,1,2,3\}$. Instantaneously, the other half of the corresponding EPR pair, which is held by Bob, turns into the state $\sigma_k|\psi\rangle$, where $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ denote the four Pauli-corrections $\{\mathbb{I}, X, Z, XZ\}$, respectively. The classical information k is then communicated to Bob who can recover the state $|\psi\rangle$ by performing σ_k on his EPR half.

D. SEPARATIONS BETWEEN QUANTUM AND CLASSICAL GARDEN-HOSE COMPLEXITY

D.1 Deterministic Setting

Using techniques from [6], we show a separation between the garden-hose model and the quantum garden-hose model in the deterministic setting for the function EQ', defined as:

$$EQ'(x,y) = \begin{cases} 1 & \text{if } \Delta(x,y) = 0\,, \\ 0 & \text{if } \Delta(x,y) = n/2\,, \end{cases}$$

where $\Delta(x, y)$ denotes the Hamming distance between two n-bit strings x and y. We show that the zero-error quantum garden-hose complexity of EQ' is logarithmic in the input length.

THEOREM D.1. $GH^Q(EQ') \in O(\log n)$.

PROOF. Alice and Bob start with the fully entangled quantum state of $\log n$ qubits, i.e. with $\frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle|i\rangle$. Counting

indices of the input bits from 0 to $n-1$, Alice gives a phase of -1 to state $|i\rangle$ whenever $x_i = 0$ and Bob does the same thing with his half when the bit $y_i = 0$, yielding the state

$$\frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} (-1)^{x_i+y_i} |i\rangle|i\rangle \,.$$

After both Alice and Bob perform a Hadamard transformation on their qubits, we obtain

$$\frac{1}{n\sqrt{n}} \sum_i \sum_{a,b} (-1)^{x_i+y_i} (-1)^{a\cdot i} (-1)^{b\cdot i} |a\rangle|b\rangle \,.$$

So the probability $p_{a,b}$ of obtaining outcome a, b when measuring in the computational basis is

$$p_{a,b} = \frac{1}{n^3} \left| \sum_i (-1)^{x_i+y_i+(a+b)\cdot i} \right|^2$$

If $x = y$, then $p_{a,b} = 0$ wherever $a \neq b$. If $\Delta(x, y) = n/2$, then $p_{a,b} = 0$ wherever $a = b$. It follows that $EQ'(x, y) = EQ(a, b)$ — determining the equality of the n-bit strings x and y is equivalent to computing the equality of the $\log(n)$-bit strings a and b. The garden-hose protocol for equality needs a number of pipes that is linear in the input size. After the quantum steps above, Alice and Bob can use $O(\log n)$ water pipes to compute $EQ(a, b)$. □

We can also show that the deterministic classical garden-hose complexity has an almost-linear lower bound.

THEOREM D.2. $GH(EQ') \in \Omega(\frac{n}{\log n})$

PROOF. Theorem 1.7 of [6] shows that the zero-error classical communication complexity of EQ' is lower bounded by $\Omega(n)$. The statement then follows from Proposition 2.8. □

D.2 Randomized Setting

The Noisy Perfect Matching problem (NPM) is a variant of the Boolean Hidden Matching introduced in [14] where they prove an exponential gap between the classical one-way communication complexity and the quantum one-way communication complexity of NPM. We adapt the given quantum one-way protocol to our setting, showing that the quantum garden-hose complexity is only logarithmic. This gives a separation between the classical and quantum garden-hose complexity of a partial function in the randomized setting.

The NPM problem is described as follows:[8]

Alice's input: $x \in \{0, 1\}^{2n}$.

Bob's input: a perfect matching M on $\{1, \ldots, 2n\}$ and a string $w \in \{0, 1\}^n$. The matching M consists of n edges, $e_1 = (i_1, j_1), \ldots, e_n = (i_n, j_n)$.

Promise: $\exists b \in \{0, 1\}$ such that $\Delta(M \cdot x \oplus b^n, w) \leq n/3$, where $\Delta(\cdot, \cdot)$ is the Hamming distance and the k-th bit of the n-bit string $M \cdot x$ equals $x_{i_k} \oplus x_{j_k}$.

Function value: b.

Informally, the question asked is whether the parity on the edges of M, where the vertices are entries of x, is close to the parities specified by w, or not.

[8]For this example, we deviate from the earlier convention of giving two n-bit strings as input to the players.

THEOREM D.3. $GH^Q(\text{NPM}) \in O(\log n)$.

PROOF. Alice and Bob use $\log(2n)$ EPR pairs as quantum state $|\psi\rangle = \frac{1}{\sqrt{2n}} \sum_{i=0}^{2n-1} |i\rangle|i\rangle$. Alice inserts her input bits $x = x_0 \ldots x_{2n-1}$ as phases of the shared superposition, yielding the shared state

$$\frac{1}{\sqrt{2n}} \sum_{i=0}^{2n-1} (-1)^{x_i} |i\rangle_A |i\rangle_B \,.$$

Bob performs the following measurement: he uses projectors $P_k = |i_k\rangle\langle i_k|_B + |j_k\rangle\langle j_k|_B$ corresponding to the n edges. As they form a perfect matching, we have $\sum_{k=1}^n P_k = I$ and $P_k P_{k'} = \delta_{kk'} P_k$, so $\{P_k\}_k$ is a valid orthogonal measurement. Let us denote Bob's measurement outcome by ℓ. Setting $i := i_\ell$ and $j := j_\ell$, the post-measurement state is

$$(-1)^{x_i} |i\rangle_A |i\rangle_B + (-1)^{x_j} |j\rangle_A |j\rangle_B \,.$$

Alice then performs a Hadamard transform $H^{\otimes 2n} \otimes I$ on her part of the state, resulting in

$$\sum_{a=0}^{2n-1} |a\rangle_A \left[(-1)^{x_i+a\cdot i} |i\rangle_B + (-1)^{x_j+a\cdot j} |j\rangle_B \right] .$$

Alice measures her register in the computational basis and obtains outcome a. Bob performs a Hadamard gate on basis states $|i\rangle_B$ and $|j\rangle_B$, that is, $H_{i,j} = \frac{1}{2}(|i\rangle\langle i|_B + |i\rangle\langle i|_B + |j\rangle\langle j|_B - |j\rangle\langle j|_B)$, resulting in the state

$$|a\rangle_A \left(\frac{1}{2} \left[(-1)^{x_i+a\cdot i} + (-1)^{x_j+a\cdot j} \right] |i\rangle_B + \frac{1}{2} \left[(-1)^{x_i+a\cdot i} - (-1)^{x_j+a\cdot j} \right] |j\rangle_B \right) .$$

and measures in the computational basis. He gets outcome i if and only if $x_i \oplus a \cdot i = x_j \oplus a \cdot j$ which is equivalent to $x_i \oplus x_j = a \cdot (i \oplus j)$. In case $x_i \oplus x_j \neq a \cdot (i \oplus j)$, Bob gets outcome j.

In the garden-hose game played after the measurements, Alice and Bob perform the garden-hose protocol for the inner-product function described in [29] with a and $i \oplus j$ as their respective inputs. The protocol can be easily adapted so that at the end of it, the water will be in one particular pipe (known to Bob) on Bob's side if $a \cdot (i \oplus j) = 0$, let us call this pipe 0-pipe. The water will be in another "1-pipe" (known to Bob) if $a \cdot (i \oplus j) = 1$. Furthermore, Bob knows from his second measurement outcome if they are computing $x_i \oplus x_j$ or $x_i \oplus x_j \oplus 1$. In the first case, Bob looks at the ℓ-th bit of w and leaves the 0-pipe open if $w_\ell = 1$ and routes the 1-pipe to Alice, and if $w_\ell = 0$ he keeps the 1-pipe open and sends back the 0-pipe. This strategy computes the function value $w_\ell \oplus x_i \oplus x_j$, with ℓ uniformly random in $\{1, \ldots, n\}$. The promise guarantees that it gives the correct value b with probability at least $\frac{2}{3}$. The second case (when Bob knows that $a \cdot (i \oplus j) \neq x_i \oplus x_j$) is handled by the "inverse" strategy. □

THEOREM D.4. $GH_\varepsilon(\text{NPM}) \in \Omega(\frac{\sqrt{n}}{\log n})$.

PROOF. Combining the lower bound on the classical one-way communication complexity from [14] of $\Omega(\sqrt{n})$ with Proposition 2.19 gives the statement. □

E. LOWER BOUNDS ON QUANTUM RESOURCES FOR A PERFECT ATTACK

We show that for a function that is injective for Alice or injective for Bob (according to Definition 2.4), the dimension of the state the adversaries need to handle (including possible quantum communication between them) in order to attack protocol $\mathsf{PV}^f_{\text{qubit}}$ perfectly has to be of order at least linear in the classical input size n. We start by showing two lemmas. The actual bound is shown in Section E.3.

In the last subsection, we show that there exist functions for which perfect attacks on $\mathsf{PV}^f_{\text{qubit}}$ requires the adversaries to handle a polynomial amount of qubits.

E.1 Localized Qubits

Assume we have two bipartite states $|\psi^0\rangle$ and $|\psi^1\rangle$ with the property that $|\psi^0\rangle$ allows Alice to locally extract a qubit and $|\psi^1\rangle$ allows Bob to locally extract the same qubit. Intuitively, these two states have to be different.

More formally, we assume that both states consist of five registers $R, A, \tilde{A}, B, \tilde{B}$ where registers R, A, B are one-qubit registers and $\tilde{A}$ and $\tilde{B}$ are arbitrary. We assume that there exist local unitary transformations $U_{A\tilde{A}}$ acting on registers $A\tilde{A}$ and $V_{B\tilde{B}}$ acting on $B\tilde{B}$ such that[9]

$$U_{A\tilde{A}}|\psi^0\rangle_{RA\tilde{A}B\tilde{B}} = |\beta\rangle_{RA} \otimes |P\rangle_{\tilde{A}B\tilde{B}} \tag{1}$$

$$V_{B\tilde{B}}|\psi^1\rangle_{RA\tilde{A}B\tilde{B}} = |\beta\rangle_{RB} \otimes |Q\rangle_{A\tilde{A}\tilde{B}}\,, \tag{2}$$

where $|\beta\rangle_{RA} := (|00\rangle_{RA} + |11\rangle)_{RA})/\sqrt{2}$ denotes an EPR pair on registers RA and $|P\rangle_{\tilde{A}B\tilde{B}}$ and $|Q\rangle_{A\tilde{A}\tilde{B}}$ are arbitrary pure states.

LEMMA E.1. *Let $|\psi^0\rangle, |\psi^1\rangle$ be states that fulfill (1) and (2). Then,*

$$\big|\,\langle\psi^0|\psi^1\rangle\,\big| \leq 1/2\,.$$

PROOF. Multiplying both sides of (1) with $U^\dagger_{A\tilde{A}}$ and multiplying (2) with $V^\dagger_{B\tilde{B}}$, we can write

$$\begin{aligned}\big|\,\langle\psi^0|\psi^1\rangle\,\big| &= \big|\,\langle\beta|_{RA}\langle P|_{\tilde{A}B\tilde{B}}\, U_{A\tilde{A}}\, V^\dagger_{B\tilde{B}}\, |\beta\rangle_{RB}|Q\rangle_{A\tilde{A}\tilde{B}}\,\big| \\ &= \big|\,\langle\beta|_{RA}\langle P'|_{\tilde{A}B\tilde{B}}|\beta\rangle_{RB}|Q'\rangle_{A\tilde{A}\tilde{B}}\,\big| \\ &= \big|\,\langle P'|_{\tilde{A}B\tilde{B}}\langle\beta|_{RA}|\beta\rangle_{RB}|Q'\rangle_{A\tilde{A}\tilde{B}}\,\big|\,,\end{aligned}$$

where we used that $U_{A\tilde{A}}$ and $V_{B\tilde{B}}$ commute and defined $|P'\rangle_{\tilde{A}B\tilde{B}} := V_{B\tilde{B}}|P\rangle_{\tilde{A}B\tilde{B}}$ and $|Q'\rangle_{A\tilde{A}\tilde{B}} := U_{A\tilde{A}}|Q\rangle_{A\tilde{A}\tilde{B}}$. The last equality is just rearranging terms that act on different registers.

Note that writing out the partial inner product between $|\beta\rangle_{RA}$ and $|\beta\rangle_{RB}$ gives

$$\langle\beta|_{RA}|\beta\rangle_{RB} = \frac{1}{2}\big(\langle 0|_A|0\rangle_B + \langle 1|_A|1\rangle_B\big)\,,$$

where the operator in the parenthesis "transfers" a qubit from register A to register B. Hence,

$$\begin{aligned}\big|\,\langle\psi^0|\psi^1\rangle\,\big| &= \big|\,\langle P'|_{\tilde{A}B\tilde{B}}\frac{1}{2}\big(\langle 0|_A|0\rangle_B + \langle 1|_A|1\rangle_B\big)|Q'\rangle_{A\tilde{A}\tilde{B}}\,\big| \\ &= \frac{1}{2}\cdot\big|\,\langle P'|_{\tilde{A}B\tilde{B}}|Q'\rangle_{B\tilde{A}\tilde{B}}\,\big| \\ &\leq \frac{1}{2}\,,\end{aligned}$$

where the last step follows from the fact that the inner product between any two unit vectors on the same registers can be at most 1. □

E.2 Squeezing Many Vectors in a Small Space

For the sake of completeness, we reproduce here an argument similar to [24, Section 4.5.4] about covering the state space of dimension d with patches of radius ε.

LEMMA E.2. *Let $\mathcal{B}$ be a set of 2^n distinct unit vectors in a complex Hilbert space of dimension d, with pairwise absolute inner product at most $1/2$. Then, the dimension d has to be in $\Omega(n)$.*

PROOF. For any two vectors $|v\rangle, |w\rangle$, we can rotate the space such that $|v\rangle = |0\rangle$ and $|w\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ for two orthogonal vectors $|0\rangle$ and $|1\rangle$. The *Euclidean distance* between $|v\rangle$ and $|w\rangle$ can be expressed as

$$\begin{aligned}\big|\,|v\rangle - |w\rangle\,\big| &= |(1-\cos\theta)|0\rangle - \sin\theta|1\rangle| \\ &= \sqrt{(1-\cos\theta)^2 + \sin^2\theta} \\ &= \sqrt{1 - 2\cos\theta + \cos^2\theta + \sin^2\theta} \\ &= \sqrt{2}\sqrt{1-\cos\theta}\,.\end{aligned}$$

If $|v\rangle$ and $|w\rangle$ have absolute inner product at most $1/2$, we have that $|\cos\theta| \leq 1/2$ and hence $\big|\,|v\rangle - |w\rangle\,\big| \geq 1$. Therefore, the vectors in $\mathcal{B}$ have pairwise Euclidean distance at least 1. The set of unit vectors $|w\rangle$ with Euclidean distance at most δ from $|v\rangle$ is called *patch of radius δ around $|v\rangle$*. It follows that patches of radius $1/2$ around every vector in the set $\mathcal{B}$ do not overlap.

The space of all d-dimensional state vectors can be regarded as the real unit $(2d-1)$-sphere, because the vector has d complex amplitudes and hence $2d$ real degrees of freedom with the restriction that the sum of the squared amplitudes is equal to 1. Notice that the Euclidean distance between complex vectors $|v\rangle$, $|w\rangle$ remains unchanged if we regard these vectors as points of the real unit $(2d-1)$-sphere.

The surface area of a patch of radius $1/2$ near any vector is lower bounded by the volume of a $(2d-2)$-sphere of radius ε where ε is a constant slightly less than $1/2$.[10] We use the formula $S_k(r) = 2\pi^{(k+1)/2}r^k/\,\Gamma((k+1)/2)$ for the surface area of a k-sphere of radius r, and $V_k(r) = 2\pi^{(k+1)/2}r^{k+1}/[(k+1)\,\Gamma((k+1)/2)]$ for the volume of a k-sphere of radius r. The total surface area of all patches, which is at least $2^n \cdot V_{2d-2}(\varepsilon)$, is not more than the total surface of the whole sphere $S_{2d-1}(1)$. Inserting the formulas, we get

$$2^n \cdot 2\pi^{d-\frac{1}{2}}\,\frac{\varepsilon^{2d-1}}{(2d-1)\,\Gamma(d-\frac{1}{2})} \leq 2\pi^d\,\frac{1}{\Gamma(d)}$$

Using the fact that $\frac{\Gamma(d-\frac{1}{2})}{\Gamma(d)} \leq \frac{1}{d}$, we conclude that

$$2^n \leq \sqrt{\pi}(2-\frac{1}{d})\varepsilon^{-(2d-1)} \leq 2\sqrt{\pi}\varepsilon^{-(2d-1)}\,.$$

As $\varepsilon < 1/2$, we obtain that d has to be in $\Omega(n)$. □

E.3 The Lower Bound

We consider perfect attacks on protocol $\mathsf{PV}^f_{\text{qubit}}$ from Figure 2. We allow the players one round of simultaneous

[9] We always assume that these transformations act as the identities on the registers we do not specify explicitly.

[10] The patch is a "bent" version of this volume.

quantum communication which we model as follows. Let $|\psi\rangle_{RA\tilde{A}A_C B\tilde{B}B_C}$ be the pure state after Alice received the EPR half from the verifier. The one-qubit register R holds the verifier's half of the EPR-pair, the one-qubit register A contains Alice's other half of the EPR-pair, the register $\tilde{A}$ is Alice's part of the pre-shared entangled state and the register A_C holds the qubits that will be communicated to Bob. The registers $B\tilde{B}B_C$ belong to Bob where B holds one qubit and $\tilde{B}$ is Bob's part of the entangled state and the B_C register will be sent to Alice. We denote by q_A the total number of qubits in registers $\tilde{A}$ and A_C and by q_B the total number of qubits in $\tilde{B}$ and B_C. The overall state is thus a unit vector in a complex Hilbert space of dimension $d := 2^{2+q_A+1+q_B}$.

In the first step of their attack, Alice performs a unitary transform U^x depending on her classical input x on her registers $A\tilde{A}A_C$. Similarly, Bob performs a unitary transform V^y depending on y on registers $B\tilde{B}B_C$. After the application of these transforms, the communication registers A_C and B_C and the classical inputs x and y are exchanged. A final unitary transform (performed either by Alice or Bob) depending on both x, y "unveils" the qubit either in Alice's register A or in Bob's register B.

THEOREM E.3. *Let f be injective for Bob. Assume that Alice and Bob perform a perfect attack on protocol PV^f_{qubit}. Then, the dimension d of the overall state (including the quantum communication) is in $\Omega(n)$.*

PROOF. We assume that the player's actions are unitary transforms as described before the theorem.

We investigate the set $\mathcal{B}$ of overall states after Bob performed his operation, but *before* Alice acts on the state. These states depend on Bob's input $y \in \{0,1\}^n$,

$$\mathcal{B} := \left\{ V^y_{B\tilde{B}B_C} |\psi\rangle_{RA\tilde{A}A_C B\tilde{B}B_C} : y \in \{0,1\}^n \right\}.$$

We claim that for any two different n-bit strings $y \neq y'$, the corresponding two vectors $V^y|\psi\rangle$ and $V^{y'}|\psi\rangle$ in $\mathcal{B}$ have an absolute inner product of at most $1/2$.

Due to the injectivity of f, there exists an input x for Alice such that $f(x,y) \neq f(x,y')$. Applying Alice's unitary transform U^x to both vectors does not change their inner product, i.e.

$$|\langle\psi|(V^y)^\dagger V^{y'}|\psi\rangle| = |\langle\psi|(V^y)^\dagger (U^x)^\dagger U^x V^{y'}|\psi\rangle|.$$

As $f(x,y) \neq f(x,y')$, the qubit has to end up on different sides. Formally, there exist unitary transforms $K_{A\tilde{A}B_C}$ and $L_{B\tilde{B}A_C}$ that "unveil" the qubit in register A or B respectively. Hence, we can apply Lemma E.1 to prove the claim that the two vectors $V^y|\psi\rangle$ and $V^{y'}|\psi\rangle$ have an absolute inner product of at most $1/2$. In particular, all of the vectors in $\mathcal{B}$ are distinct. Applying Lemma E.2 yields the theorem. □

E.4 Functions For Which Perfect Attacks Need a Large Space

Using similar arguments as above, we can show the existence of functions for which perfect attacks require polynomially many qubits.

THEOREM E.4. *For any starting state $|\psi\rangle$ of dimension d, there exists a Boolean function on inputs $x, y \in \{0,1\}^n$ such that any perfect attack on PV^f_{qubit} requires d to be exponential in n.*

We believe that the statement with the reversed order of quantifiers is true as well (but our current proof does not suffice for this purpose), so that we can guarantee the existence of one particular function (independent of the starting state) for which perfect attacks require large states.

PROOF SKETCH. We consider covering the sphere with K patches of vectors whose pairwise absolute inner product is larger than $\frac{\sqrt{3}}{2}$ (which corresponds to an Euclidean distance of $\varepsilon = \sqrt{2}\sqrt{1+\sqrt{3}/2} \approx 0.52$). This partitioning also induces a partitioning on all possible unitary operations of Alice and Bob. We say that two actions A and A' are in the same patch if they take the starting state $|\psi\rangle$ to the same patch. In other words, if two actions are in the same patch then

$$\left|\langle\psi|A'^\dagger A|\psi\rangle\right| \geq \frac{\sqrt{3}}{2}.$$

Claim. Given two actions of Alice A, A' coming from the same patch i, and two actions of Bob B, B' coming from the same patch j, the inner product between $BA|\psi\rangle$ and $B'A'|\psi\rangle$ has magnitude at least $\frac{1}{2}$.

PROOF OF THE CLAIM. Since Alice and Bob act on different parts of the state, their actions commute. Write $|\psi_A\rangle := A'^\dagger A|\psi\rangle$ and $|\psi_B\rangle := B^\dagger B'|\psi\rangle$. Then the inner product can be written as

$$\langle\psi|A'^\dagger B'^\dagger BA|\psi\rangle = \langle\psi|B'^\dagger BA'^\dagger A|\psi\rangle = \langle\psi_B|\psi_A\rangle$$

Note that

$$\left|\langle\psi|\psi_A\rangle\right| = \left|\langle\psi|A'^\dagger A|\psi\rangle\right| \geq \frac{\sqrt{3}}{2},$$

so the angle θ between $|\psi_A\rangle$ and $|\psi\rangle$ is at most $\arccos\frac{\sqrt{3}}{2} = \frac{\pi}{6}$. The same holds for the angle between $|\psi_B\rangle$ and $|\psi\rangle$. We can upper bound the total angle between $|\psi_A\rangle$ and $|\psi_B\rangle$ by the sum of these angles, giving a total angle of at most $\frac{\pi}{3}$. This corresponds to a lower bound on the inner product of $\cos\frac{\pi}{3} = \frac{1}{2}$. □

So there exists no pair of combined actions AB and $A'B'$, with A and A' in patch i and B and B' in patch j, such that the qubit ends up on Alice's side for AB and on Bob's side for $A'B'$. Therefore, the combination of i and j completely determines the destination of the qubit and hence the output of the function. If K denotes the number of patches, then there are K^{2^n} possible strategies for Alice and K^{2^n} possible strategies for Bob. Hence, the number of combined strategies (possibly resulting in different functions) is at most $K^{2\cdot 2^n}$.

It is shown in [24, Section 4.5.4] that we need at least $K = \Omega(\frac{1}{\varepsilon^{d-1}})$ patches. Using the same counting argument as in Proposition 2.9, we have that

$$2^{2^{2n}} \geq \Omega\left(\frac{1}{\varepsilon^{(d-1)2\cdot 2^n}}\right),$$

from which follows that for some function, d has to be exponential in n. □