Quantum Lower and Upper Bounds for 2D-Grid and Dyck Language

Andris Ambainis, Kaspars Balodis, Jānis Iraids
Center for Quantum Computer Science, Faculty of Computing, University of Latvia

Kamil Khadiev
Kazan Federal University, Kazan, Russia

Vladislavs Kļevickis, Krišjānis Prūsis
Center for Quantum Computer Science, Faculty of Computing, University of Latvia

Yixin Shen
Université de Paris, IRIF, CNRS, F-75013 Paris, France

Juris Smotrovs, Jevgēnijs Vihrovs
Center for Quantum Computer Science, Faculty of Computing, University of Latvia

Abstract

We study the quantum query complexity of two problems.

First, we consider the problem of determining if a sequence of parentheses is a properly balanced one (*a Dyck word*), with a depth of at most k. We call this the $\textsc{Dyck}_{k,n}$ problem. We prove a lower bound of $\Omega(c^k\sqrt{n})$, showing that the complexity of this problem increases exponentially in k. Here n is the length of the word. When k is a constant, this is interesting as a representative example of star-free languages for which a surprising $\tilde{O}(\sqrt{n})$ query quantum algorithm was recently constructed by Aaronson et al. [1]. Their proof does not give rise to a general algorithm. When k is not a constant, $\textsc{Dyck}_{k,n}$ is not context-free. We give an algorithm with $O\big(\sqrt{n}(\log n)^{0.5k}\big)$ quantum queries for $\textsc{Dyck}_{k,n}$ for all k. This is better than the trival upper bound n for $k = o\big(\frac{\log(n)}{\log\log n}\big)$.

Second, we consider connectivity problems on grid graphs in 2 dimensions, if some of the edges of the grid may be missing. By embedding the "balanced parentheses" problem into the grid, we show a lower bound of $\Omega(n^{1.5-\epsilon})$ for the directed 2D grid and $\Omega(n^{2-\epsilon})$ for the undirected 2D grid. The directed problem is interesting as a black-box model for a class of classical dynamic programming strategies including the one that is usually used for the well-known edit distance problem. We also show a generalization of this result to more than 2 dimensions.

2012 ACM Subject Classification Theory of computation → Quantum query complexity

Keywords and phrases Quantum query complexity, Quantum algorithms, Dyck language, Grid path

Funding Supported by QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union's Horizon 2020 Programme (QuantAlgo project) and ERDF project 1.1.1.5/18/A/020 "Quantum algorithms: from complexity theory to experiment".

1 Introduction

We study the quantum query complexity of two problems:

Quantum complexity of regular languages. Consider the problem of recognizing whether an n-bit string belongs to a given regular language. This models a variety of computational tasks that can be described by regular languages. In the quantum case, the most commonly used model for studying the complexity of various problems is the query model. For this setting, Aaronson, Grier and Schaeffer [1] recently showed that any regular language L has one of three possible quantum query complexities on inputs of length n: $\Theta(1)$ if the language can be decided by looking at $O(1)$ first or last symbols of the word; $\tilde{\Theta}(\sqrt{n})$ if the best way to decide L is Grover's search (for example, for the language consisting of all

words containing at least one letter a); $\Theta(n)$ for languages in which we can embed counting modulo some number p which has quantum query complexity $\Theta(n)$.

As shown in [1], a language being of complexity $\tilde{O}(\sqrt{n})$ (which includes the first two cases above) is equivalent to it being star-free. Star-free languages are defined as the languages which have regular expressions not containing the Kleene star (if it is allowed to use the complement operation). Star-free languages are one of the most commonly studied subclasses of regular languages and there are many equivalent characterizations of them. One of the star-free languages mentioned in [1] is the Dyck language (with one type of parenthesis) with a constant bounded height. The Dyck language is the set of balanced strings of parentheses (and). If at no point the number of opening parentheses exceeds the number of closing parentheses by more than k, we denote the problem of determining if an input of length n belongs to this language by $\textsc{Dyck}_{k,n}$. The language is a fundamental example of a context-free language that is not regular. When more types of parenthesis are allowed, the famous Chomsky–Schützenberger representation theorem shows that any context-free language is the homomorphic image of the intersection of a Dyck language and a regular language.

Our results. We show that an exponential dependence of the complexity on k is unavoidable. Namely, for the balanced parentheses language, we have

- there exists $c > 1$ such that, for all $k \leq \log n$, the quantum query complexity is $\Omega(c^k\sqrt{n})$;
- If $k = c \log n$ for an appropriate constant c, the quantum query complexity is $\Omega(n^{1-\epsilon})$.

Thus, the exponential dependence on k is unavoidable and distinguishing sequences of balanced parentheses of length n and depth $\log n$ is almost as hard as distinguishing sequences of length n and arbitrary depth.

Similar lower bounds have recently been independently proven by Buhrman et al. [7].

Additionally, we give an explicit algorithm (see Theorem 3) for the decision problem $\textsc{Dyck}_{k,n}$ with $O\big(\sqrt{n}(\log n)^{0.5k}\big)$ quantum queries. The algorithm also works when k is not a constant and is better than the trivial upper bound of n when $k = o\Big(\frac{\log(n)}{\log\log n}\Big)$.

Finding paths on a grid. The second problem that we consider is graph connectivity on subgraphs of the 2D grid. Consider a 2D grid with vertices (i, j), $i \in \{0, 1, \ldots, n\}, j \in \{0, 1, \ldots, k\}$ and edges from (i, j) to $(i + 1, j)$ and $(i, j + 1)$. The grid can be either directed (with edges in the directions of increasing coordinates) or undirected. We are given an unknown subgraph G of the 2D grid and we can perform queries to variables x_u (where u is an edge of the grid) defined by $x_u = 1$ if u belongs to G and 0 otherwise. The task is to determine whether G contains a path from $(0, 0)$ to (n, k).

Our interest in this problem is driven by the edit distance problem. In the edit distance problem, we are given two strings x and y and have to determine the smallest number of operations (replacing one symbol by another, removing a symbol or inserting a new symbol) with which one can transform x to y. If $|x| \leq n, |y| \leq k$, the edit distance is solvable in time $O(nk)$ by dynamic programming [16]. If $n = k$ then, under the strong exponential time hypothesis (SETH), there is no classical algorithm computing edit distance in time $O(n^{2-\epsilon})$ for $\epsilon > 0$ [4] and the dynamic programming algorithm is essentially optimal.

However, SETH does not apply to quantum algorithms. Namely, SETH asserts that there is no algorithm for general instances of SAT that is substantially better than naive search. Quantumly, a simple use of Grover's search gives a quadratic advantage over naive search. This leads to the question: can this quadratic advantage be extended to edit distance (and other problems that have lower bounds based on SETH)?

Since edit distance is quite important in classical algorithms, the question about its quantum complexity has attracted a substantial interest from various researchers. Boroujeni et al. [6] invented a better-than-classical quantum algorithm for approximating the edit

distance which was later superseded by a better classical algorithm of [8]. However, there has been no quantum algorithms computing the edit distance exactly (which is the most important case).

The main idea of the classical algorithm for edit distance is as follows:

- We construct a weighted version of the directed 2D grid (with edge weights 0 and 1) that encodes the edit distance problem for strings x and y, with the edit distance being equal to the length of the shortest directed path from $(0,0)$ to (n,k).
- We solve the shortest path problem on this graph and obtain the edit distance.

As a first step, we can study the question of whether the shortest path is of length 0 or more than 0. Then, we can view edges of length 0 as present and edges of length 1 as absent. The question "Is there a path of length of 0?" then becomes "Is there a path from $(0,0)$ to (n,k) in which all edges are present?". A lower bound for this problem would imply a similar lower bound for the shortest path problem and a quantum algorithm for it may contain ideas that would be useful for a shortest path quantum algorithm.

Our results. We use our lower bound on the balanced parentheses language to show an $\Omega(n^{1.5-\epsilon})$ lower bound for the connectivity problem on the directed 2D grid. This shows a limit on quantum algorithms for finding edit distance through the reduction to shortest paths. More generally, for an $n \times k$ grid ($n > k$), our proof gives a lower bound of $\Omega((\sqrt{n}k)^{1-\epsilon})$.

The trivial upper bound is $O(nk)$ queries, since there are $O(nk)$ variables. There is no nontrivial quantum algorithm, except for the case when k is very small. Then, the connectivity problem can be solved with $O(\sqrt{n}\log^k n)$ quantum queries [11] [1] but this bound becomes trivial already for $k = \Omega(\frac{\log n}{\log\log n})$.

For the undirected 2D grid, we show a lower bound of $\Omega((nk)^{1-\epsilon})$, whenever $k \geq \log n$. Thus, the naive algorithm is almost optimal in this case. We also extend both of these results to higher dimensions, obtaining a lower bound of $\Omega((n_1 n_2 \dots n_d)^{1-\epsilon})$ for an undirected $n_1 \times n_2 \times \ldots \times n_d$ grid in d dimensions and a lower bound of $\Omega(n^{(d+1)/2-\epsilon})$ for a directed $n \times n \times \ldots \times n$ grid in d dimensions.

In a recent work, an $\Omega(n^{1.5})$ lower bound for edit distance was shown by Buhrman et al. [7], assuming a quantum version of the Strong Exponential Time hypothesis (QSETH). As part of this result they give an $\Omega(n^{1.5})$ query lower bound for a different path problem on a 2D grid. Then QSETH is invoked to prove that no quantum algorithm can be faster than the best algorithm for this shortest path problem. Neither of the two results follow directly one from another, as different shortest path problems are used.

2 Definitions

For a word $x \in \Sigma^*$ and a symbol $a \in \Sigma$, let $|x|_a$ be the number of occurrences of a in x.

For two (possibly partial) Boolean functions $g : G \to \{0,1\}$, where $G \subseteq \{0,1\}^n$, and $h : H \to \{0,1\}$, where $H \subseteq \{0,1\}^m$, we define the composed function $g \circ h : D \to \{0,1\}$, with $D \subseteq \{0,1\}^{nm}$, as $(g \circ h)(x) = g\big(h(x_1,\dots,x_m),\dots,h(x_{(n-1)m+1},\dots,x_{nm})\big)$. Given a Boolean function f and a nonnegative integer d, we define f^d recursively as f iterated d times: $f^d = f \circ f^{d-1}$ with $f^1 = f$.

Quantum query model. We use the standard form of the quantum query model. Let $f : D \to \{0,1\}, D \subseteq \{0,1\}^n$ be an n variable function we wish to compute on an input $x \in D$. We have an oracle access to the input x — it is realized by a specific unitary transformation

[1] Aaronson et al. [1] also give a bound of $O(\sqrt{n}\log^{m-1} n)$ but in this case m is the rank of the syntactic monoid which can be exponentially larger than k.

usually defined as $|i\rangle|z\rangle|w\rangle \to |i\rangle|z + x_i \pmod 2\rangle|w\rangle$ where the $|i\rangle$ register indicates the index of the variable we are querying, $|z\rangle$ is the output register, and $|w\rangle$ is some auxiliary work-space. An algorithm in the query model consists of alternating applications of arbitrary unitaries independent of the input and the query unitary, and a measurement in the end. The smallest number of queries for an algorithm that outputs $f(x)$ with probability $\geq \frac{2}{3}$ on all x is called the quantum query complexity of the function f and is denoted by $Q(f)$.

Let a symmetric matrix Γ be called an adversary matrix for f if the rows and columns of Γ are indexed by inputs $x \in D$ and $\Gamma_{xy} = 0$ if $f(x) = f(y)$. Let $\Gamma^{(i)}$ be a similarly sized matrix such that $\Gamma^{(i)}_{xy} = \begin{cases} \Gamma_{xy} & \text{if } x_i \neq y_i \\ 0 & \text{otherwise} \end{cases}$. Then let $Adv^{\pm}(f) = \max_{\Gamma \text{ - an adversary matrix for } f} \frac{\|\Gamma\|}{\max_i \|\Gamma^{(i)}\|}$ be called the adversary bound and let $Adv(f) = \max_{\substack{\Gamma \text{ - an adversary matrix for } f \\ \Gamma \text{ - nonnegative}}} \frac{\|\Gamma\|}{\max_i \|\Gamma^{(i)}\|}$ be called the positive adversary bound. The following facts will be relevant for us: $Adv(f) \leq Adv^{\pm}(f)$; $Q(f) = \Theta(Adv^{\pm}(f))$ [14]; $Adv^{\pm}$ composes exactly even for partial Boolean functions f and g, meaning, $Adv^{\pm}(f \circ g) = Adv^{\pm}(f) \cdot Adv^{\pm}(g)$ [10, Lemma 6]

Reductions. We will say that a Boolean function f is reducible to g and denote it by $f \leqslant g$ if there exists an algorithm that given an oracle O_x for an input of f transforms it into an oracle O_y for g using at most $O(1)$ calls of oracle O_x such that $f(x)$ can be computed from $g(y)$. Therefore, from $f \leqslant g$ we conclude that $Q(f) \leq Q(g)$ because one can compute $f(x)$ using the algorithm for $g(y)$ and the reduction algorithm that maps x to y.

Dyck languages of bounded depth. Let Σ be an alphabet consisting of two symbols: (and). The Dyck language L consists of all $x \in \Sigma^*$ that represent a correct sequence of opening and closing parentheses. We consider languages L_k consisting of all words $x \in L$ where the number of opening parentheses that are not closed yet never exceeds k. The language L_k corresponds to a query problem $\textsc{Dyck}_{k,n}(x_1, ..., x_n)$ where $x_1, \ldots, x_n \in \{0, 1\}$ describe a word of length n in the natural way: the i^{th} symbol of x is (if $x_i = 0$ and) if $x_i = 1$. $\textsc{Dyck}_{k,n}(x) = 1$ iff the word x belongs to L_k. For all $x \in \{0, 1\}^n$, we define $f(x) = |x|_0 - |x|_1$, where $|x|_a$ is a number of a symbols in x. We call f the **balance**. For all $0 \leq i \leq j \leq n-1$, we define $x[i, j] = x_i, x_{i+1} \cdots x_j$. Finally, we define $h(x) = \max_{0 \leq i \leq n-1} f(x[0, i])$ and $h^-(x) = \min_{0 \leq i \leq n-1} f(x[0, i])$. A substring $x[i, j]$ is called a t-substring if $f(x[i, j]) = t$ for some integer t. A substring $x[i, j]$ is *minimal* if it does not contain a substring $x[i', j']$ such that $(i, j) \neq (i', j')$, $f(x[i', j']) = f(x[i, j])$ and $i \geq i' \geq j' \geq j$.

Connectivity on a directed 2D grid. Let $G_{n,k}$ be a directed version of an $n \times k$ grid in two dimensions, with vertices $(i, j), i \in [n], j \in [k]$ and directed edges from (i, j) to $(i+1, j)$ (if $i < n$) and from (i, j) to $(i, j+1)$ (if $j < k$). If G is a subgraph of $G_{n,k}$, we can describe it by variables x_e corresponding to edges e of $G_{n,k}$: $x_e = 1$ if the edge e belongs to G and $x_e = 0$ otherwise. We consider a problem Directed-2D-Connectivity in which one has to determine if G contains a path from $(0, 0)$ to (n, k): $\textsc{Directed-2D-Connectivity}_{n,k}(x_1, \ldots, x_m) = 1$ (where m is the number of edges in $G_{n,k}$) iff such a path exists.

Connectivity on an undirected 2D grid. Let $G_{n,k}$ be an undirected $n \times k$ grid and let G be a subgraph of $G_{n,k}$. We describe G by variables x_e in a similar way and define $\textsc{Undirected-2D-Connectivity}_{n,k}(x_1, \ldots, x_m) = 1$ iff G contains a path from $(0, 0)$ to (n, k). We also consider d dimensional versions of these two problems, on $n \times n \times \ldots n$ grids (with the grid being of the same length in all the dimensions). In the directed version (Directed-dD-Connectivity), we have a subgraph G of a directed grid (with edges directed in the directions from $(0, \ldots, 0)$ to $(n, \ldots, n)$) and $\textsc{Directed-dD-Connectivity}(x_1, \ldots, x_m) = 1$ iff G contains a directed path from $(0, \ldots, 0)$ to $(n, \ldots, n)$. The undirected version is defined similarly, with an undirected grid instead of a directed one.

3 A quantum algorithm for membership testing of Dyck$_{k,n}$

In this section, we give a quantum algorithm for $\textsc{Dyck}_{k,n}(x)$, where k can be a function of n. The general idea is that $\textsc{Dyck}_{k,n}(x) = 0$ if and only if one of the following conditions holds: (i) x contains a $+(k+1)$-substring; (ii) x contains a substring $x[0,i]$ such that the balance $f(x[0,i]) = -1$; (iii) the balance of the entire word $f(x) \neq 0$.

3.1 $\pm k$-Substring Search algorithm

The goal of this section is to describe a quantum algorithm which searches for a substring $x[i,j]$ that has a balance $f(x[i,j]) \in \{+k,-k\}$ for some integer k. Throughout this section, we find and consider only minimal substrings. For any two [minimal] $\pm k$-substrings $x[i,j]$ and $x[k,l]$: $i < k \implies j < l$. This induces a natural linear order among all $\pm k$-substrings according to their starting (or, equivalently, ending) positions. Furthermore, substrings of opposite signs do not intersect at all. This algorithm is the basis of our algorithms for $\textsc{Dyck}_{k,n}$. The algorithm works in a recursive way. It searches for two $\pm(k-1)$-substrings $x[l_1,r_1]$ and $x[l_2,r_2]$ such that there are no $\pm(k-1)$-substrings between them. If both substrings $x[l_1,r_1]$ and $x[l_2,r_2]$ are $+(k-1)$-substrings, then we get a $+k$-substring in total. If both substrings are $-(k-1)$-substrings, then we get a $-k$-substring in total.

We first discuss three building blocks for our algorithm. The first one is $\textsc{FindFrom}_k(l,r,t,d,s)$ and accepts as inputs: the borders l and r, where l and r are integers such that $0 \leq l \leq r \leq n-1$; a position $t \in \{l,\ldots,r\}$; a maximal length d for the substring, where d is an integer such that $0 < d \leq r-l+1$; the sign of the balance $s \subseteq \{+1,-1\}$. $+1$ is used for searching for a $+k$-substring, -1 is used for searching for a $-k$-substring, $\{+1,-1\}$ is used for searching for both. It outputs a triple (i,j,σ) such that $t \in [i,j]$, $j-i+1 \leq d$, $f(x[i,j]) \in \{+k,-k\}$ and $\sigma = \text{sign}(f(x[i,j])) \in s$. The substring should be the leftmost one that contains t, i.e. there is no other minimal $x[i',j']$ such that $i' < i$, $t \in [i',j']$, $f(x[i',j']) = f(x[i,j])$. If no such substrings have been found, the algorithm returns NULL.

The second one is $\textsc{FindFromRight}_k$. It is similar to the $\textsc{FindFrom}_k$, but finds the rightmost $\pm k$-substring, i.e. there is no other minimal $x[i',j']$ such that $j' > j$, $t \in [i',j']$, $f(x[i',j']) = f(x[i,j])$

The third one is $\textsc{FindFirst}_k(l,r,s,direction)$ and accepts as inputs: the borders l and r, where l and r are integers such that $0 \leq l \leq r \leq n-1$; the sign of the balance $s \subseteq \{+1,-1\}$. $+1$ is used for searching for a $+k$-substring, -1 is used for searching for a $-k$-substring, $\{+1,-1\}$ is used for both; a $direction \in \{left, right\}$. It outputs a triple (i,j,σ) such that $l \leq i \leq j \leq r$, $f(x[i,j]) \in \{+k,-k\}$ and $\sigma = \text{sign}(f(x[i,j])) \in s$. Furtherfore, if the direction is "right", then $x[i,j]$ is the first substring starting from the index l to the right that satisfies all previous conditions. If the direction is "left", then $x[i,j]$ is the first substring starting from the index r to the left that satisfies all previous conditions. The algorithm returns NULL, if it cannot find such a substring.

These three building blocks are interdependent since $\textsc{FindFrom}_k$ uses $\textsc{FindFirst}_{k-1}$ and $\textsc{FindFromRight}_{k-1}$ as subroutines, $\textsc{FindFirst}_k$ uses $\textsc{FindFrom}_k$ and $\textsc{FindFromRight}_k$ as subroutines. A description of $\textsc{FindFrom}_k(l,r,t,d,s)$ follows. The algorithm is presented in Appendix A. The description of $\textsc{FindFromRight}_k(l,r,t,d,s)$ is similar and presented in Appendix B.

When $k=2$, the procedure $\textsc{FindFrom}_2(l,r,t,d,s)$ checks that $x_t = x_{t-1}$ and $\text{sign}(f(x[t-1,t])) \in s$. If yes, it has found the substring. Otherwise, it checks if $x_t = x_{t+1}$ and $\text{sign}(f(x[t,t+1])) \in s$. If both checks fail, the procedure returns NULL. For $k > 2$ the procedure is the following.

Step 1. Check whether t is inside a $\pm(k-1)$-substring of length at most $d-1$, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFrom}_{k-1}(l, r, t, d-1, \{+1, -1\})$. If $v \neq$ NULL, then $(i_1, j_1, \sigma_1) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 2. Otherwise, the algorithm goes to Step 6.

Step 2. Check whether $i_1 - 1$ is inside a $\pm(k-1)$-substring of length at most $d-1$ and choose the rightmost one: $v = (i, j, \sigma) \leftarrow \textsc{FindFromRight}_{k-1}(l, r, i_1 - 1, d-1, \{+1, -1\})$. If $v =$ NULL, then the algorithm goes to Step 3. If $v \neq$ NULL and $\sigma = \sigma_1$, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and go to Step 8. Otherwise, go to Step 4.

Step 3. Search for the first $\pm(k-1)$-substring on the left from $i_1 - 1$ at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(\min(l, j_1 - d + 1), i_1 - 1), \{+1, -1\}, left)$. If $v \neq$ NULL and $\sigma_1 = \sigma$, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and go to Step 8. Otherwise, go to Step 4.

Step 4. Check whether $j_1 + 1$ is inside a $\pm(k-1)$-substring of length at most $d-1$, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFrom}_{k-1}(l, r, j_1 + 1, d-1, \{+1, -1\})$. If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and go to Step 8. Otherwise, go to Step 5.

Step 5. Search for the first $\pm(k-1)$-substring on the right from $j_1 + 1$ at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(j_1 + 1, \min(i_1 + d - 1, r), \{+1, -1\}, right)$. If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$, then go to Step 8. Otherwise, return NULL.

Step 6. Search for the first $\pm(k-1)$-substring on the right at distance at most d from t, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(t, \min(t + d - 1, r), \{+1, -1\}, right)$ If $v \neq$ NULL, then $(i_1, j_1, \sigma_1) \leftarrow (i, j, \sigma)$ and go to Step 7. Otherwise, returns NULL.

Step 7. Search for the first $\pm(k-1)$-substring on the left from t at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(\max(l, t - d + 1), t), \{+1, -1\}, left)$ If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and go to Step 8. Otherwise, returns NULL.

Step 8. If $\sigma_1 = \sigma_2$, $\sigma_1 \in s$ and $\max(j_1, j_2) - \min(i_1, i_2) + 1 \leq d$, output $(\min(i_1, i_2), \max(j_1, j_2), \sigma_1)$, otherwise return NULL.

Using this basic procedure, we then search for a $\pm k-$substring by searching for a t and d such that $\textsc{FindFrom}_k(l, r, t, d, s)$ returns a non-NULL value. Unfortunately, our algorithms have two-sided bounded error: they can, with small probability, return NULL even if a substring exists or return a wrong substring instead of NULL. In this setting, Grover's search algorithm is not directly applicable and we need to use a more sophisticated search [9]. Furthermore, simply applying the search algorithm naively does not give the right complexity. Indeed, if we search for a substring of length roughly d (say between d and $2d$), we can find one with expected running time $O(\sqrt{(r-l)/d})$ because at least d values of t will work. On the other hand, if there are no such substrings, the expected running time will be $O(\sqrt{r-l})$. Intuitively, we can do better because if there is a substring of length at least d then there are at least d values of t that work. Hence, we only need to distinguish between no solutions, or at least d. This allows to stop the Grover iteration early and make $O(\sqrt{(r-l)/d})$ queries in all cases.

▶ **Lemma 1** (Modified from [9], Appendix E). *Given n algorithms, quantum or classical, each computing some bit-value with bounded error probability, and some $T \geqslant 1$, there is a quantum algorithm that uses $O(\sqrt{n/T})$ queries and with constant probability: returns the index of a "1", if there are at least T "1s" among the n values; returns* NULL *if there are no "1"; returns anything otherwise.*

The algorithm that uses above ideas is presented in Algorithm 1.

We can then write an algorithm $\textsc{FindAny}_k(l, r, s)$ that searches for any $\pm k$-substring. We consider a randomized algorithm that uniformly chooses a of power 2 from $[2^{\lceil \log_2 k \rceil}, (r-l)]$, i.e. $d \in \{2^{\lceil \log_2 k \rceil}, 2^{\lceil \log_2 k \rceil + 1}, \ldots, 2^{\lceil \log_2 (r-l) \rceil}\}$. For the chosen d, we run Algorithm 1. So, the algorithm will succeed with probability at least $O(1/\log(r-l))$. We can apply Amplitude

Algorithm 1 FindFixedLen$_k(l, r, d, s)$. Search for any $\pm k$-substring of length $\in [d/2, d]$

Find t such that $v_t \leftarrow$ FindFrom$_k(l, r, t, d, s) \neq$ NULL using Lemma 1 with $T = d/2$.
return v_t or NULL if none.

amplification and ideas from Lemma 1 to this and get an algorithm that uses $O(\sqrt{\log(r-l)})$ iterations.

Algorithm 2 FindAny$_k(l, r, s)$. Search for any $\pm k$-substring.

Find $d \in \{2^{\lceil \log_2 k \rceil}, 2^{\lceil \log_2 k \rceil + 1}, \ldots, 2^{\lceil \log_2 (r-l) \rceil}\}$ such that:
$v_d \leftarrow$ FindFixedLen$_k(l, r, d, s) \neq$ NULL using amplitude amplification.
return v_d or NULL if none.

Finally, we present the algorithm that finds the first $\pm k$-substring – FindFirst$_k$. Let us consider the case $direction = right$. We first find the smallest segment from the left such that its length w is a power of 2 and it contains a $\pm k$-substring. We do so by doubling the length of the segment until we find a $\pm k$-substring. We now have a segment that contains a $\pm k$-substring and we want to find the leftmost one. We do so by the following variant of binary search. At each step let $mid = \lfloor (lBorder + rBorder)/2 \rfloor$ be the middle of the search segment $[lBorder, rBorder]$. There are three cases:

- There is a k-substring in $[lBorder, mid]$, then the leftmost k-substring is in this segment.
- There are no k-substrings in $[lBorder, mid]$, but mid is inside a k-substring. Then the leftmost k-substring that contains mid is the required substring.
- There are no k-substrings in $[lBorder, mid]$ and mid is not inside a k-substring. Then the required substring is in $[mid + 1, rBorder]$.

Each iteration of the loop the algorithm halves the search space or finds the first k-substring itself if it contains mid. If $direction = left$, we replace FindFrom$_k$ by FindFromRight$_k$ that finds the rightmost $\pm k$-substring that containts t. A detailed description of this algorithm is presented in Appendix C.

▶ **Proposition 2.** *For any $\varepsilon > 0$ and k, algorithms* FindFrom$_k$, FindFixedLen$_k$, FindAny$_k$ *and* FindFirst$_k$ *have two-sided error probability $\varepsilon < 0.5$ and return, when correct:*

- *If t is inside a $\pm k-$substring of sign s of length at most d in $x[l, r]$, then* FindFrom$_k$ *will return such a substring, otherwise it returns* NULL. *The expected running time is $O(\sqrt{d}(\log(r-l))^{0.5(k-2)})$.*
- FindFixedLen$_k$ *either returns a $\pm k-$substring of sign s and length at most d in $x[l, r]$, or* NULL. *It is only guaranteed to return a substring if there exists $\pm k-$substring of length at least $d/2$, otherwise it can return* NULL. *The expected running time is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-2)})$.*
- FindAny$_k$ *returns any $\pm k-$substring of sign s in $x[l, r]$, otherwise it returns* NULL. *The expected running time $O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$.*
- FindFirst$_k$ *returns the first $\pm k-$substring of sign s in $x[l, r]$ in the specified direction, otherwise it returns* NULL. *The expected running time is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$.*

Proof. We prove the result by induction on k. The base case of $k = 2$ is obvious because of simplicity of FindFrom$_2$ and FindFromRight$_2$ procedures. We first prove the correctness of all the algorithms, assuming there are no errors. At the end we explain how to deal with the errors.

We start with FindFrom$_k$: there are different cases to be considered when searching for a $+k$-substring $x[i, j]$ of length $\leq d$.

1. Assume that there are j_1 and i_2 such that $i < j_1 < i_2 < j$, $|f(x[i, j_1])| = |f(x[i_2, j])| = k-1$ and $\text{sign}(f(x[i, j_1])) = \text{sign}(f(x[i_2, j])) \in s$. If $t \in \{i_2, \ldots, j\}$, then the algorithm finds $x[i_2, j]$ in Step 1 and the first invocation of $\textsc{FindFirst}_{k-1}$ in Step 3 finds $x[i, j_1]$. If $t \in \{i, \ldots, j_1\}$, then the algorithm finds $x[i, j_1]$ in Step 1 and the second invocation of $\textsc{FindFirst}_{k-1}$ in Step 5 finds $x[i_2, j]$. If $j_1 < t < i_2$, then the third invocation of $\textsc{FindFirst}_{k-1}$ in Step 6 finds $x[i_2, j]$ and the forth invocation of $\textsc{FindFirst}_{k-1}$ in Step 7 finds $x[i, j_1]$.
2. Assume that there are j_1 and i_2 such that $i < i_2 < j_1 < j$, $|f(x[i, j_1])| = |f(x[i_2, j])| = k-1$ and $\text{sign}(f(x[i, j_1])) = \text{sign}(f(x[i_2, j])) \in s$. If $t \in \{i, \ldots, j_1\}$, then the algorithm finds $x[i, j_1]$ in Step 1. After that, it finds $x[i_2, j]$ in Step 4. If $t \in \{j_1 + 1, \ldots, j\}$, then the algorithm finds $x[i_2, j]$ in Step 1. After that, it finds $x[i, j_1]$ in Step 2.

By induction, the running time of each $\textsc{FindFrom}_{k-1}$ invocation is $O(\sqrt{d}(\log(r-l))^{0.5(k-3)})$, and the running time of each $\textsc{FindFirst}_{k-1}$ invocation is $O(\sqrt{d}(\log(r-l))^{0.5(k-2)})$.

We now look at FindFixedLen$_k$: by construction and definition of $\textsc{FindFrom}_k$, if the algorithm returns a value, it is a valid substring (with high probability). If there exists a substring of length at least $d/2$, then any query to $\textsc{FindFrom}_k$ with a value of t in this interval will succeed, hence there are at least $d/2$ solutions. Therefore, by Lemma 1, the algorithm will find one with high probability and make $O\left(\sqrt{\frac{r-l}{d/2}}\right)$ queries. Each query has complexity $O(\sqrt{d}(\log(r-l))^{0.5(k-2)})$ by the previous paragraph, hence the running time is bounded by $O(\sqrt{r-l}(\log(r-l)^{0.5(k-2)})$.

We can now analyze FindAny$_k$: Assume that the shortest $\pm k$-substring $x[i, j]$ is of length $g = j - i + 1$. Therefore, there is a d such that $d \le g \le 2d$ and the $\textsc{FindFixedLen}_k$ procedure returns a substring for this d with constant success probability. So, the success probability of the randomized algorithm is at least $O(1/\log(l-r))$. Therefore, the amplitude amplification does $O(\sqrt{\log(r-l)})$ iterations. The running time of $\textsc{FindFixedLen}_k$ is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-2)})$ by induction, hence the total running time is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-2)}\sqrt{\log(l-r)}) = O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$.

Finally, we analyze FindFirst$_k$: See Appendix C.

We now turn to error analysis. The case of $\textsc{FindFrom}_k$ is easy: the algorithm makes at most 5 recursive calls, each having a success probability of $1-\varepsilon$. Hence it will succeed with probability $(1-\varepsilon)^5$. We can boost this probability to $1-\varepsilon$ by repeating this algorithm a constant number of times. Note that this constant depends on ε.

The analysis of $\textsc{FindFixedLen}_k$ follows directly from [9] and Lemma 1: since $\textsc{FindFrom}_k$ has two-sided error ε, there exists a search algorithm with two-sided error ε. ◀

3.2 The Algorithm for Dyck$_{k,n}$

To solve $\textsc{Dyck}_{k,n}$, we modify the input x. As the new input we use $x' = 1^k x 0^k$. $\textsc{Dyck}_{k,n}(x) = 1$ iff there are no $\pm(k+1)$-substrings in x'. This idea is presented in Algorithm 3.

Algorithm 3 $\textsc{Dyck}_{k,n}()$. The Quantum Algorithm for $\textsc{Dyck}_{k,n}$.

$x \leftarrow 1^k x 0^k$
$v = \textsc{FindAny}_{(k+1)}(0, n+2k-1, \{+1, -1\})$
return $v == \text{NULL}$

▶ **Theorem 3** (Appendix D). *Algorithm 3 solves* $\textsc{Dyck}_{k,n}$ *and the expected running time of Algorithm 3 is* $O(\sqrt{n}(\log n)^{0.5k})$. *The algorithm has two-side error probability* $\varepsilon < 0.5$.

4 Lower bounds for Dyck languages

▶ **Theorem 4.** *There exist constants $c_1, c_2 > 0$ such that $Q\Big(\textsc{Dyck}_{c_1\ell m, c_2(2m)^\ell}\Big) = \Omega\big(m^\ell\big)$.*

Proof. We will use the partial Boolean function $\textsc{Ex}_m^{a|b} = \begin{cases} 1, & \text{if } |x|_0 = a \\ 0, & \text{if } |x|_0 = b. \end{cases}$

We prove the theorem by a reduction $\Big(\textsc{Ex}_{2m}^{m|m+1}\Big)^\ell \leqslant \textsc{Dyck}_{c_1\ell m, c_2(2m)^\ell}$, with the reduction described in appendix F. It is known that $Adv^{\pm}\Big(\textsc{Ex}_{2m}^{m|m+1}\Big) \geq Adv\Big(\textsc{Ex}_{2m}^{m|m+1}\Big) > m$ [2, Theorem 5.4]. The Adversary bound composes even for partial Boolean functions [10, Lemma 1], therefore $Q\bigg(\Big(\textsc{Ex}_{2m}^{m|m+1}\Big)^\ell\bigg) = \Omega\big(m^\ell\big)$. Via the reduction the same bound applies to $\textsc{Dyck}_{c_1\ell m, c_2(2m)^\ell}$. ◀

▶ **Theorem 5.** *For any $\epsilon > 0$, there exists $c > 0$ such that $Q(\textsc{Dyck}_{c\log n, n}) = \Omega\big(n^{1-\epsilon}\big)$.*

Proof. For any $\epsilon > 0$, there exists an m such that $Adv^{\pm}\Big(\textsc{Ex}_{2m}^{m|m+1}\Big) \geq (2m)^{1-\epsilon}$. Without loss of generality we may assume that $(2m)^\ell = n$. From Theorem 4 with $\ell = \log_{2m} n$ we obtain $c_2(2m)^\ell = c_2 n$ and height $c_1 m\ell = \Theta(\log n)$. The query complexity is at least $\Big((2m)^{1-\epsilon}\Big)^\ell = \Big((2m)^\ell\Big)^{1-\epsilon} = n^{1-\epsilon}$. Therefore $Q(\textsc{Dyck}_{c\log n, n}) = \Omega\big(n^{1-\epsilon}\big)$. ◀

For constant depths the following bound can be derived:

▶ **Theorem 6.** *There exists a constant $c_1 > 0$ such that $Q(\textsc{Dyck}_{c_1\ell, n}) = \Omega(2^{\frac{\ell}{2}}\sqrt{n})$.*

Proof. Let $m = 4$ in the Theorem 4. Then, $Q\Big(\textsc{Dyck}_{c_1\ell, c_2 8^\ell}\Big) = \Omega\big(4^\ell\big)$ for some constants $c_1, c_2 > 0$. Consider the function $\textsc{And}_{\frac{n}{c_2 8^\ell}} \circ \textsc{Dyck}_{c_1\ell, c_2 8^\ell}$ with a promise that $\textsc{And}_k$ has as an input either k or $k-1$ ones. The query complexity of this function is $\Omega\bigg(\sqrt{\frac{n}{c_2 8^\ell}}\, 4^\ell\bigg) = \Omega(2^{\frac{\ell}{2}}\sqrt{n})$. The computation of the composition $\textsc{And}_{\frac{n}{c_2 8^\ell}} \circ \textsc{Dyck}_{c_1\ell, c_2 8^\ell}$ can be straightforwardly reduced to $\textsc{Dyck}_{c_1\ell, n}$ by a simple concatenation of $\textsc{Dyck}_{c_1\ell, c_2 8^\ell}$ instances. ◀

5 Quantum complexity of st-Connectivity in grids

5.1 Quantum complexity of Directed-2D-Connectivity$_{n,k}$

▶ **Theorem 7.** *For any $n \geq k$ and $\epsilon > 0$, $Q(\textsc{Directed-2D-Connectivity}_{n,k}) = \Omega\big((\sqrt{n}k)^{1-\epsilon}\big)$.*

In particular, if we have a square grid then

▶ **Corollary 1.** *For any $\epsilon > 0$, $Q(\textsc{Directed-2D-Connectivity}_{n,n}) = \Omega\big(n^{1.5-\epsilon}\big)$.*

Proof of Theorem 7. For any sequence w of m opening and closing parentheses it is possible to plot the changes of depth, i.e., the number of opening parentheses minus the number of closing parentheses, for all prefixes of the sequence, see Figure 1. We can connect neighboring points by vectors $(1,1)$ and $(1,-1)$ corresponding to opening and closing parentheses respectively. Clearly $w \in L_d$ if and only if the path starting at the origin $(0,0)$ ends at $(m,0)$ and never crosses $y = 0$ and $y = d$. Consequently a path corresponding to $w \in L_d$ always remains within the trapezoid bounded by $y = 0$, $y = d$, $y = x$, $y = -x + m$. This suggests a way of mapping $\textsc{Dyck}_{d,m}$ to the $\textsc{Directed-2D-Connectivity}_{n,k}$ problem:

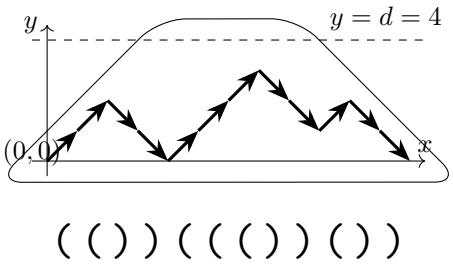

Figure 1 Representation of the Dyck word "(())((()))()"

1. An opening parenthesis in position i corresponds to a "column" of upwards sloping available edges $(i-1,l) \to (i,l+1)$ for all $l \in \{0,1,\ldots,d-1\}$ such that $i-1+l$ is even. A closing parenthesis in position i corresponds to downwards sloping available edges $(i-1,l) \to (i,l-1)$ for all $l \in \{1,\ldots,d\}$ such that $i-1+l$ is even. See Figure 2.
2. The edges outside the trapezoid adjacent to the trapezoid are forbidden (see Figure 3), i.e., it is sufficient to "insulate" the trapezoid by a single layer of forbidden edges. The only exception are the edges adjacent to the $(0,0)$ and $(m,0)$ vertex as those will be used in the construction (step 4).

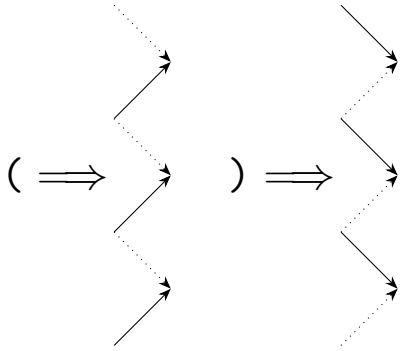

Figure 2 $\textsc{Dyck}_{d,m}$ to Directed-2D-Connectivity variable mapping

3. Rotate the trapezoid by 45 degrees counterclockwise. This isolated trapezoid can be embedded in a directed grid and its starting and ending vertices are connected by a path if and only if the corresponding input word is valid.
4. Finally we can lay multiple independent trapezoids side by side and connect them in parallel forming an $\textsc{Or}_t$ of $\textsc{Dyck}_{d,m}$ instances; see Figure 4.

This concludes the reduction $\textsc{Or}_t \circ \textsc{Dyck}_{d,m} \leqslant \textsc{Directed-2D-Connectivity}_{n,k}$, where $n = (d+1)t + \frac{m}{2} - d - 1$ and $k = \frac{m}{2} + 1$. By the well known composition result of Reichardt [14] we know that $Q(\textsc{Or}_t \circ \textsc{Dyck}_{d,m}) = \Theta(Q(\textsc{Or}_t) \cdot Q(\textsc{Dyck}_{d,m}))$. All that remains is to

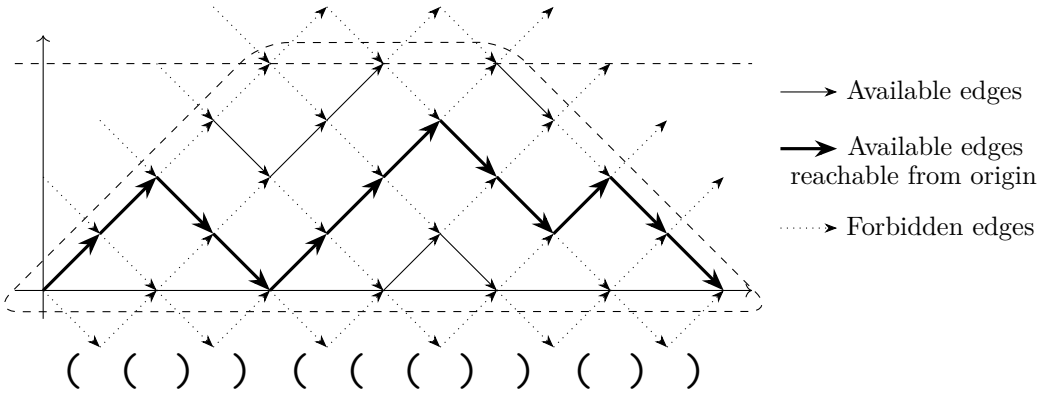

Figure 3 Mapping of a complete input corresponding to Dyck word "(())((()))()" to Directed-2D-Connectivity

pick suitable t, d and m for the proof to be complete. Let k be the vertical dimension of the grid and $k \leq n$. Then we take $m = \Theta(k)$, $d = \log m$ and $t = \frac{n}{d}$. ◀

Constructing a non-trivial quantum algorithm appears to be difficult and we conjecture that the actual complexity may be $\Omega(nk)$, except for the case when k is small, compared to n. For very small k (up to $k = \Theta(\frac{\log n}{\log\log n})$), a better quantum algorithm is possible.

▶ **Theorem 8** (Appendix G). $Q(\text{Directed-2D-Connectivity}_{n,k}) = O\left(\sqrt{ne^k\left(1+\frac{\log_2 n}{k}\right)^k}\right)$.

5.2 Lower bounds for Undirected-2D-Connectivity$_{n,k}$

Even though it is possible to use the construction from Section 5.1 to give a lower bound of $\Omega\big((\sqrt{n}k)^{1-\epsilon}\big)$ for the undirected case because the paths for each instance of Dyck never bifurcate or merge, this lower bound can be further improved to a nearly tight estimate.

▶ **Theorem 9.** *For any $n \geq k$, $k = \Omega(\log n)$, $\epsilon > 0$, $Q(\text{Undirected-2D-Connectivity}_{n,k}) = \Omega\big((nk)^{1-\epsilon}\big)$.*

Proof. We start off by representing an input as a path in a trapezoid, see Figure 3. But now instead of connecting multiple instances of Dyck in parallel we will embed one long instance by folding it when it hits the boundary of the graph. To implement a fold we will use simple gadgets depicted in Figure 5.

This way a Dyck instance of length m and depth $\log m$ can be embedded in an $n \times k$ grid such that $\frac{nk}{\log m} = \Theta(m)$. Using Theorem 5 we conclude that solving Undirected-2D-Connectivity$_{n,k}$ requires at least $\Omega\big((nk)^{1-\epsilon}\big)$ quantum queries. ◀

5.3 Lower bounds for d-dimensional grids

For undirected d-dimensional grids we give a tight bound on the number of queries required to solve connectivity.

▶ **Theorem 10.** *For any $\epsilon > 0$, for undirected d-dimensional grids of size $n_1 \times n_2 \times \ldots \times n_d$ that are not "almost-one-dimensional", i.e., there exists $i \in [d]$ such that $\frac{\prod_{j=1}^{d} n_j}{n_i} = \Omega(\log n_i)$:*

$$Q(\text{Undirected-dD-Connectivity}_{n_1,n_2,\ldots,n_d}) = \Omega((n_1 \cdot n_2 \cdot \ldots \cdot n_d)^{1-\epsilon}).$$

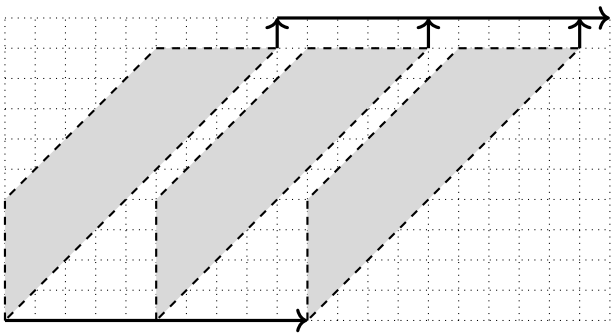

Figure 4 Reduction $\text{Or}_t \circ \text{Dyck} \leqslant$ Directed-2D-Connectivity

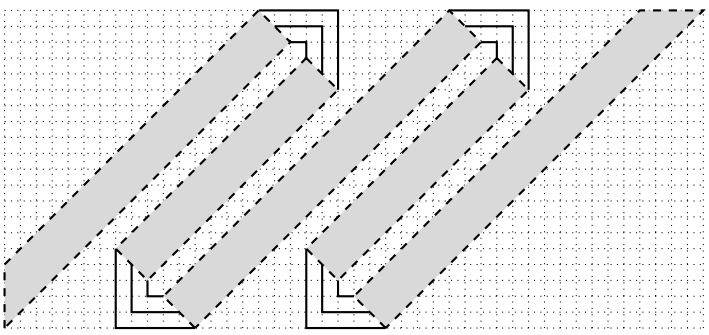

Figure 5 Folding of a long Dyck instance in an undirected grid

Proof. This follows from the 2D case by using the fact that a d-dimensional grid of size $n_1 \times n_2 \times \ldots \times n_{d-1} \times n_d$ contains as a subgraph a $(d-1)$-dimensional grid of size $n_1 \times n_2 \times \ldots \times n_{d-2} \times n_{d-1}n_d$. One way to see this is to consider a bijective mapping of the vertices $(x_1, \ldots, x_{d-1}, x_d)$ to $(x_1, \ldots, x_{d-2}, x_d n_{d-1} + x_{d-1})$ if x_d is even and to $(x_1, \ldots, x_{d-2}, x_d n_{d-1} + n_{d-1} - 1 - x_{d-1})$ if x_d is odd. It is a bijection because x_d and x_{d-1} can be recovered from $x_d n_{d-1} + n_{d-1} - 1 - x_{d-1}$ by computing the quotient and remainder on division by n_{d-1}. One can view this procedure as "folding" where we take layers (vertices corresponding to some $x_d = l$) and fold them into the $(d-1)$-st dimension alternating the direction of the layers depending on the parity of the layer l. ◀

For directed d-dimensional grids we can only slightly improve over the $n^{\frac{d}{2}}$ trivial lower bound.

▶ **Theorem 11.** *For directed d-dimensional grids of size $n_1 \times n_2 \times \ldots \times n_d$ such that $n_1 \leq n_2 \leq \ldots \leq n_d$ and $\epsilon > 0$, $Q(\text{Directed-dD-Connectivity}_{n_1,n_2,\ldots,n_d}) = \Omega((n_{d-1} \prod_{i=1}^{d} n_i)^{\frac{1}{2}-\epsilon})$.*

▶ **Corollary 2.** *For directed d-dimensional grids of size $n \times n \times \ldots \times n$ and $\epsilon > 0$, $Q(\text{Directed-dD-Connectivity}_{n,n,\ldots,n}) = \Omega(n^{\frac{d+1}{2}-\epsilon})$.*

Proof of Theorem 11. For each $I \in [n_1] \times [n_2] \times \ldots \times [n_{d-2}]$ we take take a 2-dimensional hard instance G_I of $\text{Directed-2D-Connectivity}_{n_{d-1},n_d}$ having query complexity $\Omega(n_{d-1}^{1-\epsilon} n_d^{\frac{1}{2}-\epsilon})$. We then connect them in parallel like so:

- Make available the entire $(d-2)$-dimensional subgrid from $(1, 1, \ldots, 1, 1, 1)$ to $(n_1, n_2, \ldots, n_{d-2}, 1, 1)$ and similarly the subgrid from $(1, 1, \ldots, 1, n_{d-1}, n_d)$ to $(n_1, n_2, \ldots, n_{d-2}, n_{d-1}, n_d)$;
- For each $I \in [n_1] \times [n_2] \times \ldots \times [n_{d-2}]$ embed the instance G_I in the subgrid $(I, 1, 1)$ to (I, n_{d-1}, n_d);
- Forbid all other edges.

This construction computes $\text{Or}_{\prod_{i=1}^{d-2} n_i} \circ \text{Directed-2D-Connectivity}_{n_{d-1},n_d}$ whose complexity is at least $\Omega(\sqrt{\prod_{i=1}^{d-2} n_i} n_{d-1}^{1-\epsilon} n_d^{\frac{1}{2}-\epsilon}) = \Omega((n_{d-1} \prod_{i=1}^{d} n_i)^{\frac{1}{2}-\epsilon})$. ◀

6 Conclusion

We have shown quantum lower bounds on two problems in the query model:

- recognizing Dyck languages of bounded depth (i.e. determining whether a sequence of parentheses is a balanced sequence of depth at most k);
- determining connectivity on grids of dimension 2 and more where some edges may be missing (and we have query access to the information whether edges are present).

The first bound shows that the complexity increases exponentially in k, as $\Omega(\sqrt{n}c^k)$. This provides a lower bound counterpart to the recent result of Aaronson et al. [1] who constructed an $\tilde{O}(\sqrt{n})$ quantum algorithm for all star-free languages (which includes the Dyck languages of bounded depth) where $\tilde{O}$ term has exponential dependence on the complexity of the language (measured by the rank of its syntactic monoid).

The lower bound for the directed 2D grid is important as it implies an $\Omega(n^{1.5-\epsilon})$ lower bound on the most natural approach towards a quantum algorithm for edit distance (by reducing it to connectivity on 2D grid). More generally, we think that the connectivity problems introduced in this paper are a natural new class of problems that is worth studying in the quantum algorithms context.

Some directions for future work are:

1. **Better algorithm/lower bound for the directed 2D grid?** Can we find an $o(n^2)$ query quantum algorithm or improve our lower bound? A nontrivial quantum algorithm would be particularly interesting, as it may imply a quantum algorithm for edit distance.

2. **Quantum algorithms for directed connectivity?** More generally, can we come up with better quantum algorithms for directed connectivity? The span program method used by Belovs and Reichardt [5] for the undirected connectivity does not work in the directed case. As a result, the quantum algorithms for directed connectivity are typically based on Grover's search in various forms, from simply speeding up depth-first/breadth-first search to more sophisticated approaches [3]. Developing other methods for directed connectivity would be very interesting.
3. **Quantum speedups for dynamic programming.** Dynamic programming is a widely used algorithmic method for classical algorithms and it would be very interesting to speed it up quantumly. This has been the motivating question for both the connectivity problem on the directed 2D grid studied in this paper and a similar problem for the Boolean hypercube in [3] motivated by algoritms for Travelling Salesman Problem. There are many more dynamic programming algorithms and exploring quantum speedups of them would be quite interesting.

References

1 Scott Aaronson, Daniel Grier, and Luke Schaeffer. A quantum query complexity trichotomy for regular languages. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:61, 2018.

2 Andris Ambainis. Quantum lower bounds by quantum arguments. *Journal of Computer and System Sciences*, 64(4):750–767, 2002.

3 Andris Ambainis, Kaspars Balodis, Janis Iraids, Martins Kokainis, Krisjanis Prusis, and Jevgenijs Vihrovs. Quantum speedups for exponential-time dynamic programming algorithms. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019*, pages 1783–1793, 2019. URL: `https://doi.org/10.1137/1.9781611975482.107`, `doi:10.1137/1.9781611975482.107`.

4 Arturs Backurs and Piotr Indyk. Edit distance cannot be computed in strongly subquadratic time (unless seth is false). In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 51–58. ACM, 2015.

5 Aleksandrs Belovs and Ben W. Reichardt. Span programs and quantum algorithms for st-connectivity and claw detection. In *Algorithms - ESA 2012 - 20th Annual European Symposium, Ljubljana, Slovenia, September 10-12, 2012. Proceedings*, pages 193–204, 2012. URL: `https://doi.org/10.1007/978-3-642-33090-2_18`, `doi:10.1007/978-3-642-33090-2\_18`.

6 Mahdi Boroujeni, Soheil Ehsani, Mohammad Ghodsi, MohammadTaghi HajiAghayi, and Saeed Seddighin. Approximating edit distance in truly subquadratic time: Quantum and mapreduce. In *Proceedings of the Twenty-Ninth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1170–1189. SIAM, 2018.

7 Harry Buhrman, Subhasree Patro, and Florian Speelman. The quantum strong exponential-time hypothesis, 2019. `arXiv:1911.05686`.

8 Diptarka Chakraborty, Debarati Das, Elazar Goldenberg, Michal Koucký, and Michael E. Saks. Approximating edit distance within constant factor in truly sub-quadratic time. In *59th Annual IEEE Symposium on Foundations of Computer Science (FOCS), Paris, France, Oct 7-9, 2018*, pages 979–990, 2018. `arXiv:1810.03664`.

9 Peter Høyer, Michele Mosca, and Ronald de Wolf. Quantum search on bounded-error inputs. In Jos C. M. Baeten, Jan Karel Lenstra, Joachim Parrow, and Gerhard J. Woeginger, editors, *Automata, Languages and Programming*, pages 291–299, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

10 Shelby Kimmel. Quantum adversary (upper) bound. In *International Colloquium on Automata, Languages, and Programming*, pages 557–568. Springer, 2012.

509 **11** Vladislavs Kļevickis. Čaulu programmas ceļa atrašanai grafā (span programs for finding a
510 path in a graph). Undergraduate 3rd year project, University of Latvia, 2017.
511 **12** Robin Kothari. An optimal quantum algorithm for the oracle identification problem. In *31st*
512 *International Symposium on Theoretical Aspects of Computer Science*, page 482, 2014.
513 **13** C. Y.-Y. Lin and H.-H. Lin. Upper bounds on quantum query complexity inspired by the
514 elitzur–vaidman bomb tester. *Theory of Computing*, 12(18):1–35, 2016.
515 **14** Ben W. Reichardt. Reflections for quantum query algorithms. In *Proceedings of the Twenty-*
516 *second Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '11, pages 560–569,
517 Philadelphia, PA, USA, 2011. Society for Industrial and Applied Mathematics. URL: `http:`
518 `//dl.acm.org/citation.cfm?id=2133036.2133080`.
519 **15** Ben W. Reichardt. Span programs are equivalent to quantum query algorithms. *SIAM*
520 *J. Computing*, 43(3):1206–1219, 2014. URL: `https://doi.org/10.1137/100792640`, `doi:`
521 `10.1137/100792640`.
522 **16** Robert A Wagner and Michael J Fischer. The string-to-string correction problem. *Journal of*
523 *the ACM (JACM)*, 21(1):168–173, 1974.

A An Algorithm for the FindFrom$_k$ Subroutine

Algorithm 4 FindFrom$_k(l, r, t, d, s)$. Search any $\pm k$-substring.

$v = (i_1, j_1, \sigma_1) \leftarrow$ FindFrom$_{k-1}(l, r, t, d-1, \{+1, -1\})$
if $v \neq$ NULL **then** ▷ if t is inside a $\pm(k-1)$-substring
  $v' = (i_2, j_2, \sigma_2) \leftarrow$ FindFromRight$_{k-1}(l, r, i_1 - 1, d-1, \{+1, -1\})$
  if $v' =$ NULL **then**
    $v' = (i_2, j_2, \sigma_2) \leftarrow$ FindFirst$_{k-1}(\min(l, j_1 - d + 1), i_1 - 1), \{+1, -1\}, left)$
  if $v' \neq$ NULL and $\sigma_2 \neq \sigma_1$ **then**
    $v' \leftarrow$ NULL
  if $v' =$ NULL **then**
    $v' = (i_2, j_2, \sigma_2) \leftarrow$ FindFrom$_{k-1}(l, r, j_1 + 1, d-1, \{+1, -1\})$
    if $v' =$ NULL **then**
      $v' = (i_2, j_2, \sigma_2) \leftarrow$ FindFirst$_{k-1}(j_1 + 1, \min(i_1 + d - 1, r), \{+1, -1\}, right)$
  if $v' =$ NULL **then**
    return NULL
else
  $v = (i_1, j_1, \sigma_1) \leftarrow$ FindFirst$_{k-1}(t, \min(t + d - 1, r), \{+1, -1\}, right)$
  if $v =$ NULL **then**
    return NULL
  $v' = (i_2, j_2, \sigma_2) \leftarrow$ FindFirst$_{k-1}(\max(l, t - d + 1), t), \{+1, -1\}, left)$
  if $v' =$ NULL **then**
    return NULL
if $\sigma_1 = \sigma_2$ and $\sigma \in s$ and $\max(j_1, j_2) - \min(i_1, i_2) + 1 \leq d$ **then**
  return $(\min(i_1, i_2), \max(j_1, j_2), \sigma_1)$
else
  return NULL

B The Description of the FindFromRight$_k$ Algorithm

Let us present the algorithm for FindFromRight$_k$. When $k = 2$, the procedure first checks whether $x_t = x_{t+1}$ and $\text{sign}(f(x[t, t+1])) \in s$. Otherwise, it checks if $x_t = x_{t-1}$ and $\text{sign}(f(x[t-1, t])) \in s$. If neither pair of conditions is satisfied, the procedure returns NULL. For $k > 2$ the procedure is the following.

Step 1. Check whether t is inside a $\pm(k-1)$-substring of length at most $d-1$, i.e. $v = (i, j, \sigma) \leftarrow$ FindFromRight$_{k-1}(l, r, t, d-1, \{+1, -1\})$.
If $v \neq$ NULL, then $(i_1, j_1, \sigma_1) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 2. Otherwise, the algorithm goes to Step 6.

Step 2. Check whether $j_1 + 1$ is inside a $\pm(k-1)$-substring of length at most $d-1$, i.e. $v = (i, j, \sigma) \leftarrow$ FindFrom$_{k-1}(l, r, j_1 + 1, d-1, \{+1, -1\})$.
If $v =$ NULL, then the algorithm goes to Step 3. If $v \neq$ NULL and $\sigma = \sigma_1$, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 8. Otherwise, the algorithm goes to Step 4.

Step 3. Search for the first $\pm(k-1)$-substring on the right from $j_1 + 1$ at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow$ FindFirst$_{k-1}(j_1 + 1, \min(i_1 + d - 1, r), \{+1, -1\}, right)$.

If $v \neq$ NULL and $\sigma_1 = \sigma$, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 8. Otherwise, the algorithm goes to Step 4.

Step 4. Check whether $i_1 - 1$ is inside a $\pm(k-1)$-substring of length at most $d-1$, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFromRight}_{k-1}(l, r, i_1 - 1, d-1, \{+1, -1\})$.
If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 8. Otherwise, the algorithm goes to Step 5.

Step 5. Search for the first $\pm(k-1)$-substring on the left from $i_1 - 1$ at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(\min(l, j_1 - d + 1), i_1 - 1), \{+1, -1\}, left)$.
If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$. The algorithm goes to Step 8. Otherwise, the algorithm fails and returns NULL.

Step 6. Search for the first $\pm(k-1)$-substring on the right at distance at most d from t, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(t, \min(t + d - 1, r), \{+1, -1\}, right)$
If $v \neq$ NULL, then $(i_1, j_1, \sigma_1) \leftarrow (i, j, \sigma)$ and the algorithm goes to Step 7. Otherwise, the algorithm fails and returns NULL.

Step 7. Search for the first $\pm(k-1)$-substring on the left from t at distance at most d, i.e. $v = (i, j, \sigma) \leftarrow \textsc{FindFirst}_{k-1}(\max(l, t - d + 1), t), \{+1, -1\}, left)$
If $v \neq$ NULL, then $(i_2, j_2, \sigma_2) \leftarrow (i, j, \sigma)$ and go to Step 8. Otherwise, the algorithm fails and returns NULL.

Step 8. If $\sigma_1 = \sigma_2$, $\sigma_1 \in s$ and $\max(j_1, j_2) - \min(i_1, i_2) + 1 \leq d$, then output $[\min(i_1, i_2), \max(j_1, j_2)]$, otherwise the algorithm fails and returns NULL.

Algorithm 5 $\textsc{FindFromRight}_k(l, r, t, d, s)$. Search any $\pm k$-substring.

```
v = (i_1, j_1, σ_1) ← FindFromRight_{k-1}(l, r, t, d − 1, {+1, −1})
if v ≠ NULL then                                   ▷ if t is inside a ±(k − 1)-substring
    v' = (i_2, j_2, σ_2) ← FindFrom_{k-1}(l, r, j_1 + 1, d − 1, {+1, −1})
    if v' = NULL then
        v' = (i_2, j_2, σ_2) ← FindFirst_{k-1}(j_1 + 1, min(i_1 + d − 1, r), {+1, −1}, right)
    if v' ≠ NULL and σ_2 ≠ σ_1 then
        v' ← NULL
    if v' = NULL then
        v' = (i_2, j_2, σ_2) ← FindFromRight_{k-1}(l, r, i_1 − 1, d − 1, {+1, −1})
        if v' = NULL then
            v' = (i_2, j_2, σ_2) ← FindFirst_{k-1}(min(l, j_1 − d + 1), i_1 − 1), {+1, −1}, left)
    if v' = NULL then
        return NULL
else
    v = (i_1, j_1, σ_1) ← FindFirst_{k-1}(t, min(t + d − 1, r), {+1, −1}, right)
    if v = NULL then
        return NULL
    v' = (i_2, j_2, σ_2) ← FindFirst_{k-1}(max(l, t − d + 1), t), {+1, −1}, left)
    if v' = NULL then
        return NULL
if σ_1 = σ_2 and σ ∈ s and max(j_1, j_2) − min(i_1, i_2) + 1 ≤ d then
    return (min(i_1, i_2), max(j_1, j_2), σ_1)
else
    return NULL
```

C FindFirst$_k$ Algorithm's Description, Complexity and Proof of Correctness

C.1 FindFixedPos$_k$

Let us first describe a subroutine used by FindFirst$_k$.

FindFixedPos$_k(l, r, t, s, left)$ searches for the leftmost substring $x[i, j]$ such that $\text{sign}(f(x[i, j])) \in s$ and $|f(x[i, j])| = k$, i.e. $i \le t \le j$ and there is no $x[i', j']$ such that $i' \le t \le j'$, $i' < i$ and $f(x[i', j']) = f(x[i, j])$.

The procedure is similar to FindAny$_k$. First, we consider a randomized algorithm that uniformly chooses d as a power of 2 that is at most $r - l$. For this d, it runs FindFrom$_k(l, r, t, d, s)$ algorithm and searches for a non-NULL result. The probability of getting a correct result is at least $O(1/\log(r-l))$. Then, we apply the Amplitude amplification method and the idea from Lemma 1 that requires $O(\sqrt{\log(r-l)})$ iterations. Similarly, we find the maximal d that finds a substring. This algorithm also performs $O(\sqrt{\log(r-l)})$ iterations due to [13, 12]. The total complexity of the algorithm is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$ due to the complexity of FindFrom$_k$.

▶ **Lemma 12.** FindFixedPos$_k(l, r, t, s, left)$ *returns the leftmost minimal substring* $x[i, j]$ *such that* $sign(f(x[i, j])) \in s$ *or NULL if there is no such substring. The expected running time is* $O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$.

Proof. Let us show by induction that FindFrom$_k(l, r, t, d, s)$ returns the leftmost substring $x[i, j]$ such that $\text{sign}(f(x[i, j])) \in s$. If $k = 2$, we check whether $x_t = x_{t-1}$ before $x_t = x_{t+1}$.

Assume that there is another minimal substring $x[i', j']$ such that $i' \le t \le j'$, $f(x[i, j]) = f(x[i', j'])$ and $i' < i$.

1. Assume that there are j_1 and i_2 such that $i < j_1 < i_2 < j$, $|f(x[i, j_1])| = |f(x[i_2, j])| = k-1$ and $\text{sign}(f(x[i, j_1])) = \text{sign}(f(x[i_2, j])) \in s$.
   By induction one of the invocations of FindFrom$_{k-1}$ or FindFirst$_{k-1}$ finds $x[i_2, j]$ and it the leftmost. Therefore, $j' = j$. If $i' < i$, then $x[i', j']$ is not minimal or $|f(x[i', j'])| > |f(x[i, j])|$, a contradiction.
2. Assume that there are j_1 and i_2 such that $i < i_2 < j_1 < j$, $|f(x[i, j_1])| = |f(x[i_2, j])| = k-1$ and $\text{sign}(f(x[i, j_1])) = \text{sign}(f(x[i_2, j])) \in s$. By induction $x[i_2, j]$ is the leftmost $\pm(k-1)$-substring. Therefore, $j' = j$. If $i' < i$, then $x[i', j']$ is not minimal or $|f(x[i', j'])| > |f(x[i, j])|$, a contradiction.

If $d > r - l$ the algorithm finds $x[i, j]$. If $d < r - l$, the algorithm could find the wrong substring (not the leftmost one containing t). So, we should to find the maximal d such that FindFrom$_k$ finds a substring. In that case, when we amplify the randomized version of the algorithm, we get the required one.

Searching by Grover's search for the maximal d requires the same $O(\sqrt{r-l})$ expected number of iterations due to [13, 12]. The total complexity of the algorithm is $O(\sqrt{r-l}(\log(r-l))^{0.5(k-1)})$ due to the complexity of the FindFrom$_k$ procedure. ◀

FindFixedPos$_k(l, r, t, s, right)$ searches for the rightmost substring $x[i, j]$ such that $\text{sign}(f(x[i, j])) \in s$ and $|f(x[i, j])| = k$, i.e. $i \le t \le j$ and there is no $x[i', j']$ such that $i' \le t \le j'$, $j < j'$ and $f(x[i', j']) = f(x[i, j])$.

The algorithm is similar to FindFixedPos$_k(l, r, t, s, left)$, but uses FindFromRight$_k$.

C.2 FindFirst$_k$ Algorithm's Description

The FindFirst$_k$ procedure calls FindLeftFirst$_k$ or FindRightFirst$_k$ depending on the direction. Since both version are essentially symmetric, we only present the search from the left below (i.e. when the direction is right). For reasons that become clear in the proof, we need to boost the success probability of some calls. We do so by repeating them several times and taking the majority: by this we mean that we take the most common answer, and return an error in case of a tie.

Algorithm 6 FindRightFirst$_k(l, r, s)$. The algorithm for searching for the first $\pm k$-substring.

$lBorder \leftarrow l, rBorder \leftarrow r$
$d \leftarrow 1$ ▷ depth of the search
while $lBorder + 1 < rBorder$ **do**
  $mid \leftarrow \lfloor (lBorder + rBorder)/2 \rfloor$
  $v_l \leftarrow$ FindAny$_k(lBorder, mid, s)$ ▷ repeat $2d$ times and take the majority
  if $v_l \neq$ NULL **then**
    $rBorder \leftarrow mid$
  if $v_l =$ NULL **then**
    $v_{mid} \leftarrow$ FindFixedPos$_k(lBorder, rBorder, mid, s, left)$ ▷ majority of $2d$ runs
    if $v_{mid} \neq$ NULL **then**
      $v \leftarrow v_{mid}$
      Stop the loop.
    if $v_{mid} =$ NULL **then**
      $lBorder \leftarrow mid + 1$
  $d \leftarrow d + 1$
return v

C.3 Proof of Claim on FindFirst$_k$ Procedure from Proposition 2

Let us prove the correctness of the algorithm for $direction = right$ and $s = \{+1\}$. The proof for other parameters is similar.

First, we show the correctness of the algorithm assuming there are no errors. The algorithm is essentially a binary search. At each step we find the middle of the search segment $[lBorder, rBorder]$ that is $mid = \lfloor (lBorder + rBorder)/2 \rfloor$. There are three options.

- There is a k-substring in $[lBorder, mid]$, then the leftmost k-substring is in this segment.
- There are no k-substrings in $[lBorder, mid]$, but mid is inside a k-substring. If we find the leftmost substring containing min, it is the required substring.
- There are no k-substrings in $[lBorder, mid]$ and mid is not inside a k-substring. Then the required substring is in $[mid + 1, rBorder]$.

In each iteration of the loop the algorithm finds a smaller segment containing the leftmost k-substring or finds it if it contains mid. We find the k-substring in the iteration that corresponds to the $[lBorder, rBorder]$ segment such that $(rBorder - lBorder)/2 \leq j - i$ or earlier.

Second, we compute complexity of the algorithm (taking into account the repetitions and majority votes). The u-th iteration of the loop considers a segment $[lBorder, rBorder]$. The length of this segment is at most $w \cdot 2^{-(u-1)}$ where $w = r - l$. The complexity of FindAny$_k(lBorder, mid, s)$ is at most $O\left(\sqrt{w \cdot 2^{-(u-1)-1}}\left(\log\left(w \cdot 2^{-(u-1)-1}\right)\right)^{0.5(k-1)}\right) =$

$O\left(\sqrt{w \cdot 2^{-(u-1)-1}}(\log{(r-l)})^{0.5(k-1)}\right)$. Also, FINDFIXEDPOS$_k(lBorder, rBorder, mid, s, left)$ has complexity $O\left(\sqrt{w \cdot 2^{-(u-1)}}\left(\log{(w \cdot 2^{-(u-1)})}\right)^{0.5(k-1)}\right) = O\left(\sqrt{w \cdot 2^{-(u-1)}}(\log{(r-l)})^{0.5(k-1)}\right)$. So the total complexity of the u-th iteration is $O\left(u\sqrt{w \cdot 2^{-(u-1)}}(\log{(r-l)})^{0.5(k-1)}\right)$, since at the u-th iteration, we repeat each call $2u$ times to take a majority. The number of iterations is at most $\log_2 w$. Let us compute the total complexity of the binary search part:

$$
\begin{aligned}
O\left(\sum_{u=1}^{\log_2 w} 2u\sqrt{w \cdot 2^{-(u-1)}}(\log{(r-l)})^{0.5(k-1)}\right) &= O\left(\sqrt{w}(\log{(r-l)})^{0.5(k-1)} \sum_{u=1}^{\log_2 w} u(\sqrt{2})^{-(u-1)}\right) \\
&= O\left(\sqrt{w}(\log{(r-l)})^{0.5(k-1)} \sum_{u=0}^{\infty}(u+1)(\sqrt{2})^{-u}\right) \\
&= O\left(\sqrt{w}(\log{(r-l)})^{0.5(k-1)} \frac{\sqrt{2}^2}{(\sqrt{2}-1)^2}\right) \\
&= O\left(\sqrt{w}(\log{(r-l)})^{0.5(k-1)}\right).
\end{aligned}
$$

Finally, we need to analyze the success probability of the algorithm: at the u^{th} iteration, the algorithm will run each test $2u$ times and each test has a constant probability of failure ε. Hence for the algorithm to fail (that is make a decision that will not lead to the first $\pm k$-substring) at iteration u, at least half of the $2u$ runs must fail: this happens with probability at most

$$\binom{2u}{u}\varepsilon^u \leqslant \left(\frac{2ue}{u}\right)^u \varepsilon^u \leqslant (2e\varepsilon)^u.$$

Hence the probability that the algorithm fails is bounded by

$$\sum_{u=1}^{\log_2 w}(2e\varepsilon)^u \leqslant \sum_{u=1}^{\infty}(2e\varepsilon)^u \leqslant \frac{2e\varepsilon}{1-2e\varepsilon}.$$

By taking ε small enough (say $2e\varepsilon < \frac{1}{3}$), which is always possible by repeating the calls a constant number of times to boost the probability, we can ensure that the algorithm a probability of failure less than $1/2$.

D Proof of Theorem 3

Proof. Let us show that if x' contains $\pm(k+1)$-substring then one of three conditions of DYCK$_{k,n}$ problem is broken.

Assume that x' contains $(k+1)$ substring $x'[i,j]$. If $j \geq k+n$, then $f(x[i-k, n-1]) > 0$, because $f(x'[n,j]) = j-n+1 \leq k < k+1$. Therefore, prefix $x[0, i-k]$ is such that $f(x[0, i-k-1]) < 0$ or $f(x[0, n-1]) > 0$ because $f(x[0, n-1]) = f(x[0, i-k]) + f(x[i-k-1, n-1])$. So, in that case we break one of conditions of DYCK$_{k,n}$ problem.

If $j < k+n$ then $x[i-k, j-k]$ is $(k+1)$ substring of x.

Assume that x' contains $-(k+1)$ substring $x'[i,j]$. If $i < k$, then $f(x[0, j-k]) < 0$, because $f(x'[i, k-1]) = -(k-i) \geq -k > -(k+1)$ and $f(x[0, j-k]) = f(x'[k,j]) = f(x[i,j]) - f(x[i, k-1])$. So, in that case the second condition of DYCK$_{k,n}$ problem is broken.

The complexity of Algorithm 3 is the same as the complexity of FINDANY$_{k+1}$ for x' that is $O(\sqrt{n+2k}(\log(n+2k))^{0.5k})$ due to Proposition 2.

We can assume $n \geq 2k$ (otherwise, we can update $k \leftarrow n/2$). Hence,

$$O(\sqrt{n+2k}(\log(n+2k))^{0.5k}) = O(\sqrt{2n}(\log(2n))^{0.5k}) = O(\sqrt{n}(2\log n)^{0.5k}) = O(\sqrt{n}(\log n)^{0.5k})$$

The error probability is the same as the complexity of $\textsc{FindAny}_{k+1}$. ◀

E Proof of Lemma 1

The main loop of the algorithm of [9] is the following, assuming the algorithms have error at most 1/9:

- for $m = 0$ to $\lceil \log_9 n \rceil$-1 do:
  1. run A_m 1000 times,
  2. verify the 1000 measurements, each by $O(\log n)$ runs of the corresponding algorithm,
  3. if a solution has been found, then output a solution and stop
- Output 'no solutions'

The key of the analysis is that if the (unknown) number t of solutions lies in the interval $[n/9^{m+1}, n/9^m]$, then A_m succeeds with constant probability. In all cases, if there are no solutions, A_m will never succeeds with high probability (ie the algorithm only applies good solutions).

In our case, we allow the algorithm to return anything (including NULL) if $t < T$. This means that we only care about the values of m such that $n/9^m \geqslant T$, that is $m \leqslant \log_9 \frac{n}{T}$. Hence, we simply run the algorithm with this new upper bound for d and it will satisfy our requirements with constant probability. The complexity is

$$\sum_{m=0}^{\lfloor log_9 \frac{n}{T} \rfloor} 1000 \cdot O(3^m) + 1000 \cdot O(\log n) = O(3^{\log_9 \frac{n}{T}}) = O(\sqrt{n/T}).$$

F Reduction for the proof of Theorem 4

Before we describe the reduction in detail, we sketch the main idea. Let $\text{imbal}(x) = |x|_0 - |x|_1$. Note that

$$\text{Ex}_{2m}^{m|m+1}(x) = 0 \iff \text{imbal}(x) = 2$$

$$\text{Ex}_{2m}^{m|m+1}(x) = 1 \iff \text{imbal}(x) = 0$$

whereas

$$\textsc{Dyck}_{k,n}(x) = 1 \iff \begin{array}{r} \max\limits_{p\ -\ \text{prefix of } x} \text{imbal}(p) \leq k \wedge \\ \min\limits_{p\ -\ \text{prefix of } x} \text{imbal}(p) \geq 0 \wedge \\ \text{imbal}(x) = 0. \end{array}$$

If we could make sure that the minimum and maximum constraints are satisfied, $\textsc{Dyck}_{k,n}$ could be used to compute $\text{Ex}_{2m}^{m|m+1}$. To ensure the minimum constraint, we map each 0 to 00 and 1 to 01. However, this increases $\text{imbal}(x)$ by $2m$ which can be fixed by appending 1^{2m} at the end. Importantly, the resulting sequence x' has $\text{imbal}(x') = \text{imbal}(x)$. The first constraint (maximum over prefixes) can be fulfilled by having a sufficiently large k; $k = 2m + 3$ would suffice here. The same idea can be applied iteratively to $\text{Ex}_{2m}^{m|m+1}$ where

the inputs, which could now be the results of functions $\left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell-1} = x_i$, have been recursively mapped to sequences x_i' with $\mathrm{imbal}(x_i') = \begin{cases} 2 \text{ if } x_i = 0 \\ 0 \text{ if } x_i = 1 \end{cases}$.

The reduction formally is as follows.

We call a string $B \in \{0,1\}^w$ of even length a (w,h)-sized block with width w and height h iff for any prefix x of B: $0 \leq \mathrm{imbal}(x) \leq h$ and either $\mathrm{imbal}(B) = 0$ or $\mathrm{imbal}(B) = 2$.

We establish a correspondence between inputs to $\left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell}$ that satisfy the promise and (w,h)-sized blocks B for appropriately chosen w, h, so that $\left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell} = 1$ iff $\mathrm{imbal}(B) = 0$.

For $l = 0$ (the input bits), we have 0 corresponding to a $(2,2)$-sized block of 00 and 1 to a $(2,2)$-sized block of 01.

For $l > 0$, let us have input bits $x = (x_1, x_2, \ldots, x_{2m})$ of $\mathrm{Ex}_{2m}^{m|m+1}$ satisfying the input promise. Assume that the bits (that could be equal to values of $\left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell-1}$) correspond to (w,h)-sized blocks $B_1, B_2, \ldots, B_{2m}$. Define the sequence $B' = B_1 B_2 \ldots B_{2m} 1^{2m}$. Then it is easy to verify the following claims:

1) B' is a $(2m(w+1), 2(m+1)+h)$-sized block;

2) The output bit of $\mathrm{Ex}_{2m}^{m|m+1}(x)$ *corresponds* to B' because

$$\mathrm{imbal}(B') = \sum_{i=1}^{2m} \mathrm{imbal}(B_i) + \mathrm{imbal}(1^{2m}) = \begin{cases} 2 \text{ if } \mathrm{Ex}_{2m}^{m|m+1}(x) = 0 \\ 0 \text{ if } \mathrm{Ex}_{2m}^{m|m+1}(x) = 1 \end{cases}.$$

For $l = 0$, the inputs correspond to $(2,2)$-sized blocks. Each level adds $2(m+1)$ to the height of the blocks reaching $2 + 2\ell(m+1) = O(m\ell)$. The width of blocks reaches $O((2m)^\ell)$.

Since for all (w,h)-sized blocks B: $\textsc{Dyck}_{h,w}(B) = 1 \iff \mathrm{imbal}(B) = 0$ one can solve the $\left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell}$ problem by running $\textsc{Dyck}_{h,w}$ on the *corresponding* block.

See Figure 6.

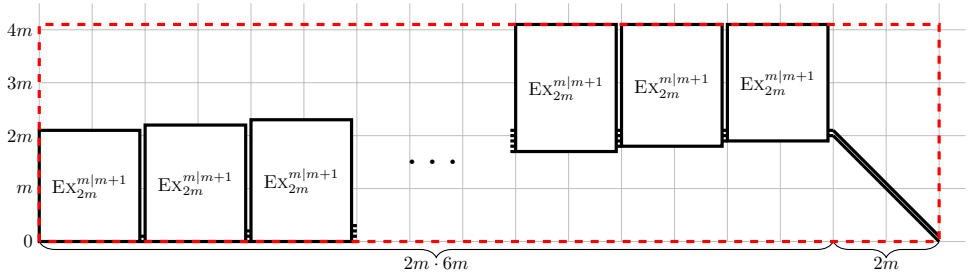

Figure 6 The reduction $\mathrm{Ex}_{2m}^{m|m+1} \circ \mathrm{Ex}_{2m}^{m|m+1} \leqslant \textsc{Dyck}_{4m+6,12m^2+2m}$. The line of the graph follows the input word along the x-axis and shows the number of yet-unclosed parenthesis along the y-axis (i.e., a zoomed-out version of Figure 1). The input word $B_1 B_2 \ldots B_{2m} 1^{2m}$ corresponds to the outer function $\mathrm{Ex}_{2m}^{m|m+1}$ with B_j being a block corresponding to the output of an inner $\mathrm{Ex}_{2m}^{m|m+1}$. The ticks at the starts and ends of blocks depict that if the line enters the block at height i, it exits at height i or $i+2$. In the block the line never goes below 0 or above $h+i$. The red dashed part then forms a new block B'. By replacing the blocks B_j with blocks B' we can further iterate $\mathrm{Ex}_{2m}^{m|m+1}$ to get the reduction $\mathrm{Ex}_{2m}^{m|m+1} \circ \left(\mathrm{Ex}_{2m}^{m|m+1}\right)^{\ell-1} \leqslant \textsc{Dyck}_{O(\ell m), O\left((2m)^\ell\right)}$.

G A quantum algorithm for Directed-2D-Connectivity$_{n,k}$

In this section, we prove Theorem 8 by constructing a quantum algorithm for Directed-2D-Connectivity$_{n,k}$. The main idea is to construct an AND-OR formula for Directed-2D-Connectivity$_{n,k}$ and to use the quantum algorithm for AND-OR formulae by Reichardt [15] which evaluates an AND-OR formula of size L with $O(\sqrt{L})$ queries.

We first deal with the case when $n = 2^m$ for some non-negative integer m. The idea for the construction of the AND-OR formula is to split the grid in two: any path from $(0,0)$ to (n,k) must pass through a vertex $(n/2, r)$ for some $r:\ 0 \le r \le k$. For the paths to and from $(n/2, r)$ we can apply this reasoning recursively. Let us denote by $F_{\mu,\kappa,i,j}$ our formula for the path from vertex (i,j) to $(i+2^\mu, j+\kappa)$, and by $L_{\mu,\kappa}$ its size (the number of variable instances it has; it does not depend on i, j). Thus we have the recurrent formulae

$$F_{\mu,\kappa,i,j} = \bigvee_{r=0}^{\kappa} \left(F_{\mu-1,r,i,j} \wedge F_{\mu-1,\kappa-r,i+2^{\mu-1},j+r}\right),$$

$$L_{\mu,\kappa} = \sum_{r=0}^{\kappa} (L_{\mu-1,r} + L_{\mu-1,\kappa-r}) = 2\sum_{r=0}^{\kappa} L_{\mu-1,r}.$$

For the base case $F_{0,\kappa,i,j}$ (i. e. for a $1 \times \kappa$ grid) we simply use an OR of all the paths (represented as an AND of all its edges). There are $\kappa+1$ paths, each of length $\kappa+1$, thus $L_{0,\kappa} = (\kappa+1)^2$.

It follows by induction on μ that $L_{\mu,\kappa} < 2^{\mu+1} \cdot \binom{\kappa+\mu+2}{\kappa}$. For the induction basis we have $L_{0,\kappa} < (\kappa+1)(\kappa+2) = 2\binom{\kappa+2}{\kappa}$, and for the induction step:

$$L_{\mu,\kappa} = 2\sum_{r=0}^{\kappa} L_{\mu-1,r} < 2^{\mu+1} \sum_{r=0}^{\kappa} \binom{r+\mu+1}{r} = 2^{\mu+1}\binom{\kappa+\mu+2}{\kappa}.$$

Using a well-known upper bound for binomial coefficients we obtain: $L_{m,k} < 2^{m+1}(e\cdot(k+m+2)/k)^k = O\Big(n(e(1+\frac{\log_2 n}{k}))^k\Big)$. There exists a quantum algorithm with $O(\sqrt{L})$ queries for a formula of size L [15], thus we obtain the complexity mentioned in the theorem statement.

For an arbitrary n we can find the smallest m for which $n \le 2^m$ and use the formula for the $2^m \times k$ grid obtained by adding ancillary edges from the vertex (n,k) to $(2^m, k)$ (using the edge variables of the added part of the grid as constants). Since the value of n thus increases no more than two times, the complexity estimation increases by at most a constant multiplier.