58th Annual IEEE Symposium on Foundations of Computer Science

# On preparing ground states of gapped Hamiltonians: An efficient Quantum Lovász Local Lemma

András Gilyén*
*Algorithms and Complexity group*
*CWI, QuSoft*
*Amsterdam, Netherlands*
gilyen@cwi.nl

Or Sattath†
*The Hebrew University,*
*Jerusalem, Israel and*
*Massachusetts Institute of Technology,*
*Cambridge, Massachusetts*
sattath@cs.huji.ac.il

***Abstract*—A frustration-free local Hamiltonian has the property that its ground state minimises the energy of all local terms simultaneously. In general, even deciding whether a Hamiltonian is frustration-free is a hard task, as it is closely related to the $\mathsf{QMA}_1$-complete quantum satisfiability problem (QSAT) – the quantum analogue of SAT, which is the archetypal NP-complete problem in classical computer science. This connection shows that the frustration-free property is not only relevant to physics but also to computer science.**

**The Quantum Lovász Local Lemma (QLLL) provides a sufficient condition for frustration-freeness. Is there an efficient way to prepare a frustration-free state under the conditions of the QLLL? Previous results showed that the answer is positive if all local terms commute. These works were based on Moser's "compression argument" which was the original analysis technique of the celebrated resampling algorithm. We generalise and simplify the "compression argument", so that it provides a simplified version of the previous quantum results, and improves on some classical results as well.**

**More importantly, we improve on the previous constructive results by designing an algorithm that works efficiently for non-commuting terms as well, assuming that the system is "uniformly" gapped, by which we mean that the system *and all its subsystems* have an inverse polynomial energy gap. Similarly to the previous results, our algorithm has the charming feature that it uses only local measurement operations corresponding to the local Hamiltonian terms.**

## I. Introduction

*Frustration-free Hamiltonians and quantum satisfiability:* Most physical systems and models are described by a local Hamiltonian $H = \sum_i H_i$ where each $k$-local term $H_i$ acts non-trivially only on at most $k$ of its subsystems. Such a Hamiltonian is called *frustration-free* if its ground state is also the ground state of each of the local terms $H_i$. Frustration-free Hamiltonians appear in various areas, for example: quantum error correcting codes [1], parent Hamiltonians for PEPS (a 2-D generalisation of matrix-product-states) [2], and various models in many-body quantum physics.

An equivalent way to ask whether a Hamiltonian $H$ is frustration-free is whether $H' = \sum_i \Pi_i$ is frustration-free, where $\Pi_i$ is the projector on the excited states of $H_i$. The quantum satisfiability problem[1] (QSAT) is to determine whether $H'$ in the above form is frustration-free. QSAT is $\mathsf{QMA}_1$-complete [3], and therefore intractable in general even for quantum computers (unless $\mathsf{BQP} = \mathsf{QMA}_1$). In this work we tackle the search problem – finding a state of a frustration-free Hamiltonian – which is, in general, even a harder task than the deciding frustration freeness.[2]

*The Classical and Quantum Lovász Local Lemma:* We would like to understand the QSAT problem, so it is natural to first look at the classical SAT and the techniques that were useful in studying it. A "local" version of SAT is called $k$-SAT. It asks whether a Boolean formula of the following form can be satisfied: $\bigwedge_{i\in[m]} c_i$, where each $c_i$ is a *clause* containing the or ($\bigvee$) of exactly $k$ distinct Boolean variables or their negation.

A natural question is, when can we be sure that a satisfying assignment exists? Since each $k$-SAT constraint excludes a $p = 2^{-k}$ fraction of assignments, $pm < 1$ is a sufficient condition (by the union bound). If we have the additional information that none of the constraints share variables, then it is clearly satisfiable. What can we say in the intermediate regime, where each constraint shares variables with at most $d$ constraints (including itself)? The (symmetric) Lovász Local Lemma [5], [6], [7], [8], applied to this setting, implies that the (symmetric) Lovász condition

$$pde \leq 1 \tag{1}$$

is a sufficient condition for satisfiability.[3] Shearer generalised the Lovász Local Lemma and showed the weakest possible sufficient condition in this framework [9].

How hard is it to find such a satisfying assignment? A series of works [10], [11], [12], [13] have culminated in an efficient constructive algorithm.

*Supported by ERC Consolidator Grant 615307-QPROGRESS.
†Supported by ERC Grant 030-8301.

[1]For technical reasons that would not be relevant for this work, there is a promise that if $H'$ is not frustration-free, the minimal energy of $H'$ is at least inverse-polynomial in the number of qubits.

[2]SAT (as well as any other NP-Complete problem) has a search-to-decision reduction [4]. No such reduction is known for QSAT.

[3]The constant $e$ in Eq. (1) is $2.71\ldots$, the base of the natural logarithm.

0272-5428/17 $31.00 © 2017 IEEE
DOI 10.1109/FOCS.2017.47

It is natural to ask the analogous questions in the quantum setting, where the Boolean variables are replaced by qubits and the clauses by rank-1 $k$-local projectors. The resemblance between a $k$-SAT clause and a rank-1 projector is the following: a $k$-SAT clause excludes one out of the $2^k$ possible configurations of the relevant variables, while a rank-1 $k$-local projector excludes one dimension out of the $2^k$ relevant dimensions. So given a set of $k$-local rank-1 projectors acting on $n$ qubits[4], under what conditions can we guarantee that the system is frustration-free? A "dimension-counting" argument can be used to show that the Lovász condition ($pde \leq 1$) [15] is indeed sufficient, as is Shearer's condition [16].

Is there an algorithm which efficiently prepares a ground state under these conditions? In the past, such constructions have been achieved only for commuting Hamiltonians, i.e. $[\Pi_i, \Pi_j] = 0$ for all $i, j$. Commuting Hamiltonians are somewhat "half-way" between classical and quantum. For example, the commuting 2-local Hamiltonian problem is in (the purely classical class) NP for qudits of all dimensions [17], whereas 2-local QSAT is $\mathsf{QMA}_1$-complete if the dimension of the qudits is large enough [18]. Yet commuting Hamiltonians, such as the toric code, can have the striking quantum property of topological order [19]. In this work we extend the previous results to non-commuting projectors, thereby entering the fully quantum regime.

*Moser-Tardos type resampling algorithm:* Following the seminal work of Moser and Tardos [12], a variety of algorithms and analysis techniques were introduced for proving efficient versions of the Lovász Local Lemma based on their resampling algorithm. The resampling algorithm starts with a random state, and repeatedly checks the constraints that we want to satisfy. If a constraint $c$ is violated, then it performs a "resampling", which is some random "local" change to the current state only affecting $c$ and a few other constraints, hopefully fixing $c$. Once all constraints are fixed, the algorithm returns a satisfying state. The main challenge is the analysis of the algorithm: proving a bound on the expected number of resamplings needed. In Algorithm 1 we present a meta-algorithm sketching this procedure, which captures the basic structure of most related algorithms.

The algorithm can be interpreted both as a classical and quantum algorithm. For example, in the case of SAT, the initial state is $n$ uniformly random Boolean variables, and a constraint is simply a clause, which is simple to check by looking at the corresponding Boolean variables. In the quantum setting of QSAT, the initial state is similarly $n$ uniformly randomly initialised 0/1 qubits (which is the maximally mixed state). A constraint $c$ corresponds to an orthogonal projector $\Pi_c$. We say that $|\psi\rangle$ *satisfies* the constraint $c$ if the quantum state is in the kernel of $\Pi_c$, and that $c$ is *unsatisfied* if $|\psi\rangle$ is not in the kernel. Finally we say that $|\psi\rangle$ *violates* $c$ if it is in the image of $\Pi_c$.

[4]The uniform $k$-locality and rank-1 constraints are only for convenience, for a general treatment see the full version [14].

**Algorithm 1** Moser-Tardos resampling meta-algorithm

1: **input** set of constraints $C$
2: initialise system to a uniformly random starting state
3: $F \leftarrow \varnothing$ ($F$ will stand for the set of *fixed* clauses)
4: **while** $F \neq C$ **do**
5: **pick** $c \in C \setminus F$ and **check** if constraint $c$ is satisfied
6: **if** "Satisfied"
7: **update** $F \leftarrow F \cup \{c\}$
8: **else if** "Violated"
9: **resample** $c$ (and thereby hopefully fix it)
10: **update** $F \leftarrow F \setminus \Gamma^+(c)$ ($\star$ $\Gamma^+(c)$ denotes the constraints possibly affected by resampling $c$ $\star$)
11: **end while**

In Algorithm 1, **pick** and **check** in line 5 and **resample** in line 9 need to be specified in order to get a well-defined algorithm. In this paper, all the results apply for any deterministic strategy for executing **pick**, see Def. 2. In order to get improved bounds, up to the optimal Shearer bound [9], we need to be more careful regarding **pick**, for more details see the full version [14]. In this article we mostly work in the so-called variable framework [11], [12], [13], which is sufficient for the SAT and QSAT applications. In this setting each constraint depends on some (qu)bits of the system. (For simplicity we will only consider systems of $n$ qubits, but all the results generalise trivially to qudits.) In this binary variable framework we simply define **resample** as reinitialising the specific constraint's (qu)bits to uniformly random true-false (0-1) values. We define $\Gamma^+(c)$ as the set of constraints $c'$ such that $c$ and $c'$ both act non-trivially on some shared (qu)bit, and $d = \max_{c \in C} |\Gamma^+(c)|$. In general one could also work with other models, as described in [20].

The **check**ing step in line 5 should be performed using some measurement operator, corresponding to $\Pi_c$. The algorithm implicitly assumes, that all the constraints in $F$ are fixed (satisfied). This loop invariant is easy to maintain in the classical and commuting quantum case by implementing **check** using the two-outcome measurement $\{\Pi_c, \mathrm{Id} - \Pi_c\}$. But, in the non-commuting setting, using this two-outcome measurement can break the loop invariant: suppose that all the constraints in $F$ are fixed, and then another constraint $\Pi_c$ is checked (i.e., measured) and is found to be satisfied. A constraint which was fixed before, and shares a qubit with $\Pi_c$, may become unsatisfied because of the collapse caused by the measurement. Because of this caveat the analysis of the previous quantum algorithms [21], [22] worked only in the commuting case. Next, we explain how to maintain this loop invariant also in the non-commuting case.

*The progressive measurement channel:* We first need one more notation. We denote by $\Pi^F$ the projection onto

$\ker(\sum_{c\in F}\Pi_c)$. Note that for $c$ the image of $\Pi_c$ is violated, whereas for $F$ the image of $\Pi^F$ is satisfied for any $c' \in F$, e.g., $\Pi^{\{c\}} = I - \Pi_c$. We changed from sub- to superscript to help avoiding confusion caused by this difference.

Suppose that $|\psi\rangle$ satisfies all the constraints in $F$, i.e., $|\psi\rangle = \Pi^F|\psi\rangle$, and $\{\Pi^{F\cup\{c\}}, \mathrm{Id} - \Pi^{F\cup\{c\}}\}$ is measured. The unnormalised post-measurement state associated with outcome $\Pi^{F\cup\{c\}}$ is $\Pi^{F\cup\{c\}}|\psi\rangle$, which we obtain with probability $\langle\psi|\Pi^{F\cup\{c\}}|\psi\rangle$.[5] If instead $\{\Pi_c, \mathrm{Id}-\Pi_c\}$ is measured, the post-measurement state $|\varphi\rangle$ associated with outcome $\Pi_c$ has the property that $|\varphi\rangle = \Pi_c|\varphi\rangle$, and due to locality also $|\varphi\rangle = \Pi^{F\setminus\Gamma^+(c)}|\varphi\rangle$. One of our key observations is, that the outcomes $\Pi^{F\cup\{c\}}$ and $\Pi_c$ are in some sense complementary to each other.

We call a quantum channel a *progressive* measurement channel, if it combines these two properties[6]: for an input state $|\psi\rangle \in \mathrm{im}(\Pi^F)$, it has two classically labelled outputs (corresponding to measurement labels): the "Satisfied" output is $\Pi^{F\cup\{c\}}|\psi\rangle$, and the "Violated" output is $\rho$ such that $\rho = \Pi_c\rho = \Pi^{F\setminus\Gamma^+(c)}\rho$ and $\mathrm{Tr}[\rho] = 1 - \left\|\Pi^{F\cup\{c\}}|\psi\rangle\right\|^2$. Here, the name *progressive* is used to emphasize that for a state which satisfies $F$, the channel either adds $c$ to the set of fixed constraints, or provides a state in which $c$ is violated (but the state $\rho$ keeps at least $F \setminus \Gamma^+(c)$ satisfied).

We show two different but closely related constructions, which satisfy the requirements of a progressive measurement channel. In Section II-C we show an explicit (but inefficient) procedure and prove that it is a progressive measurement channel. The construction itself and its analysis is fairly simple. In Section III we show how to efficiently construct an approximate progressive measurement channel. The proof that this efficient construction satisfies the requirements needed for a progressive measurement channel is more complicated, and some of the details are deferred to the full version.

The main idea of the efficient variant is to use weak measurements coupled with a quantum Zeno effect[7]. This variant uses only $\Pi_c$ and $\Pi^F$ measurements, and the number of measurements it performs depends on the spectral gap of $\sum_{c'\in F\cup\{c\}}\Pi_{c'}$. It repeats the following $T$ times: (strongly) measure $\Pi^F$, followed by a weak measurement of $\Pi_c$. If $\Pi_c$ is found to be violated, we immediately return with the classical "Violated" label. If we ever get measurement outcome $I - \Pi^F$, we immediately abort, otherwise we return "Satisfied". We show that by choosing the weak measurement parameter to be weak enough, the probability of abort becomes proportionally small. Also if we choose $T$ to be large enough, then the procedure closely approximates a progressive measurement channel. Finally we show how to appropriately approximate a $\Pi^F$ measurement by repeated $\Pi_{c'}$ measurements for $c' \in F$.

We think that the definition and efficient construction of a progressive measurement channel could be of independent interest, and might find applications in other quantum algorithms.

*New existential proof:* Our work does not require any of the previous existential proofs, and therefore provides an alternative proof for the main results in [15] and [16].

*Our contributions:* We present three main results in this paper.

Our first contribution is the adaptation of the "forward-looking" analysis technique of [20] to the quantum setting, which enables the generalization for the non-commuting case, and makes it possible to extend the previous commuting results up to Sherarer's bound (see the full version [14]). This is done via our Key Lemma 8, which borrows ideas from [20], [25]. It is proved using semi-definite inequalities which introduce quantum analogues of uniform probability bounds.

Our second contribution is the generalisation and simplification of Moser's "entropy compression argument" [11] that was originally used for proving efficiency of the resampling algorithm. This generalisation simplifies the proof of the previous commuting quantum results from [21], [22]. On top of the quantum implications, it also improves the runtime analysis of some classical algorithms, see the discussion in Section II-A. Last, but not least, it gives valuable insight through the "Log compression" Lemma 3 showing that the core of the "entropy compression argument" can be distilled to a straightforward counting argument.

Our third and most important contribution is that we prove a constructive Quantum Lovász Local Lemma for *non-commuting* projectors. We construct the appropriate progressive measurement channel which can handle the non-commuting case in a way suggested by our Key Lemma 8.

The algorithm's running time is polynomial in the number of the constraints and qubits, but also depends inverse-polynomially on the uniform gap, see Eq. (14) and the discussion there. The main open question left is whether this dependency on the uniform gap is necessary. Specifically, given a Hamiltonian $H$ which satisfies the Lovász condition, and an energy bound $\epsilon$, is there a quantum algorithm which can output a state with energy at most $\epsilon$ in time $poly(n, |C|, 1/\epsilon)$? (The running time should neither depend on the uniform gap, nor on the gap of the Hamiltonian.)

[5]This measurement could be approximated by measuring the energy of the Hamiltonian $H' = \sum_{c'\in F\cup\{c\}}\Pi_{c'}$ (by applying phase estimation to the unitary $e^{iH'}$, see, e.g. [23]), and checking whether the energy is 0. However, we will use a different approach for such measurements.

[6]The formal definition is slightly different, and is adapted for our needs, see Def. 7. The progressive measurement channels that we discuss in Sections II-C and III satisfy these two properties.

[7]The quantum Zeno effect is a quantum technique which uses frequently repeated measurements to prevent unwanted changes in the quantum state of some quantum system [24].

## II. The ideal algorithm

### A. Generalised compression argument.

Our generalisation starts form key insights of both classical [20], [25] and quantum [21], [22] literature. The generalised approach we present makes the proof significantly simpler than in the original work of Moser [11], probably providing the simplest known proof of any Moser-Tardos type algorithm. It works for any deterministic constraint-selection rule, and can be applied beyond the variable framework [20].

*Definition 1 (Logs):* The log of the first $T$ steps of Algorithm 1 is a string $L \in \{S,V\}^T$ containing the first $T$ outcomes of **check** where $S$ stands for "Satisfied", and $V$ for "Violated").

Let $\mathcal{L}^{(r)}$ denote the the set of all valid logs which contain exactly $r$ $V$'s, and ends with a $V$.

*Definition 2:* (Constraint-selection Strategy) A deterministic constraint-selection strategy is a function $s$, which given the current log $L$, determines which next constraint to **pick** at line 5 of Algorithm 1.

*Lemma 3:* (Log compression) Suppose we run Algorithm 1 using a deterministic constraint-selection strategy. Then the log uniquely encodes the sequence of resamples that happened during the algorithm. Moreover, if $\Gamma^+(c) \leq d$ for all $c \in C$, then for all $r \in \mathbb{N}$ we have $|\mathcal{L}^{(r)}| \leq \binom{|C|+rd}{r}$.

*Proof:* Since the constraint-selection strategy is deterministic and initially $F = \emptyset$, we can recover the content of the set $F$ after each execution of the main loop at line 4 by only looking at the binary log telling us whether a resampling happened or not. Therefore the log compresses the whole resample history into a binary string.

Now observe, that any log $L \in \mathcal{L}^{(r)}$ contains at most $|C| + rd$ entries: Suppose the algorithm performed $k-1$ steps before the $r$-th resampling. At this step $0 < |C \setminus F|$ since a resampling is performed at the $k$-th step. On the other hand $F$ starts with 0 elements, and gains one element with the $k-r$ successful checks, and looses at most $d-1$ elements after each resampling. Therefore $|C \setminus F| \leq |C| - (k-r) + (r-1)(d-1) \leq |C| + rd - k$ and so $k < |C| + rd$.

Finally we map each $L \in \mathcal{L}^{(r)}$ to a binary string of length $|C| + rd$ by extending it with "$S$"s. Note that this mapping is injective, and observe that the number of length $|C| + dr$ binary sequences containing $r$ "$V$"s is $\binom{|C|+dr}{r}$, which by injectivity proves the desired upper bound on $|\mathcal{L}^{(r)}|$. ∎

*Theorem 4:* Let $d = \max_{c \in C} |\Gamma^+(c)|$. Suppose we run Algorithm 1 using a deterministic constraint-selection strategy, and in each step we log the constraint that we checked and whether it was satisfied or not. Let $L_k = \ell_1, \ell_2, \ldots, \ell_k$ denote the log obtained during the first $k$ steps. Let $r = 4|C|$, if

(i) $pde \leq 1$, and
(ii) $\Pr(\text{seeing a specific log } L_k \in \mathcal{L}^{(r)} \text{ during a run}) \leq p^r$

then Algorithm 1 terminates with constant probability making less than $4|C|$ resamplings. If also
(iii) during the algorithm the constraints in $F$ remain fixed[8],

then upon termination Algorithm 1 provides a satisfying state.

*Proof:* Suppose we set a bound $r = 4|C|$ on the number of resamplings, such that we terminate with "timeout" upon the $r$-th resampling. The "Log compression" Lemma 3 shows that the number of logs that we might obtain at "timeout" is at most $\binom{|C|+rd}{r}$. Using the bound

$$\binom{n}{k} \leq \left(\frac{en}{k} - \frac{e}{2}\right)^k \tag{2}$$

from the Appendix, we upper bound $\binom{|C|+rd}{r}$ by $(d - 1/4)^r e^r$. Combining this with (ii) using the union bound, we can see that the probability of termination with "timeout" is at most

$$p^r \left(d - \frac{1}{4}\right)^r e^r \overset{(i)}{\leq} \left(\frac{p(d-1/4)e}{pde}\right)^r = \left(1 - \frac{1}{4d}\right)^r \leq e^{-\frac{r}{4d}} \leq \frac{1}{e}.$$

Finally, note that if Algorithm 1 terminates normally (without "timeout") then $F = C$, and by (iii) it means that the final state is a satisfying state. ∎

*Remark 5:* Since every randomised strategy is a convex combination of deterministic strategies, the above theorem implies that for any randomised constraint-selection strategy the probability of performing at least $4|C|$ resamplings is also at most $1/e$.

Theorem 4 gives a fast algorithm whenever the conditions (i)-(iii) are met. It is easy to show that properties (ii)-(iii) hold for the classical variable setting for $p$ which is the maximal probability of encountering a constraint in the uniformly random distribution (so, for example, in a $k$-SAT formula, $p = 2^{-k}$), and even for more general settings if an appropriate resampling procedure is used, e.g., as in [20]. This improvement partially answers an open question posed in [20], by providing an improved upper bound on the number of resamplings for the case of the symmetric Lovász condition.

In the quantum case, we can choose $p$ to be the maximal probability of measuring any particular constraint in a maximally mixed state (so, for example, in a $k$-QSAT formula, $p = 2^{-k}$). In the commuting case, if **check** is performed using standard projective measurements of the constraint projectors, then (ii) and (iii) hold (see Proposition 13), and therefore Theorem 4 implies the results of [21], [22]. Our proof is not only simpler, but due to the use of our optimised bound (2), our result do not require a slack in the condition $pde \leq 1$. (As shown above, we require slack in the condition

[8]This requirement is mostly trivial in the classical case, since constraints can only appear after resamplings, which is handled by Algorithm 1. But in the non-commutative quantum case it becomes problematic, as was discussed in the introduction.

$p(d-1/4)e \leq 1$, which can actually be pushed to be a slack in $p(d-1/2)e \leq 1$.) Since property (ii) holds even in the non-commuting case, the algorithm is guaranteed to terminate under the Lovász condition (i.e., when property (i) is satisfied), but the problem is that the output may not be satisfying for all constraints.

### B. The progressive measurement channel and the key lemma

To adapt the algorithm to the quantum setting we introduce a quantum channel $\mathcal{M}_c^F$, which performs some quantum operation on the $n$-qubit quantum register determined by the classical input $(F, c)$, where $F$ is the set of already "fixed" constraints, and $c$ is the next constraint to address. In the case of commuting projectors $\mathcal{M}_c^F$ will be simply the application of a projective measurement $(\Pi_c, \mathrm{Id} - \Pi_c)$ where the classical measurement outcomes are labelled with $(V, S)$ standing for ("Violated","Satisfied") respectively.

*Definition 6:* (Quantum-classical states) For the description of quantum-classical states consisting of an $N$ dimensional quantum system and a $k$ dimensional classical system we are going to use elements of $\mathbb{C}^{N\times N} \otimes \mathbb{R}^k$. We can interpret these as quantum states of restricted form via defining an embedding of $\mathbb{R}^k$ to $\mathbb{C}^{k\times k}$ using diagonal matrices.

For $c \in C$ let $b(c) \subseteq [n]$ be the set of qubits on which $\Pi_c$ acts non-trivially. Let $\Pi_c^{loc}$ denote $\Pi_c$ restricted to $b(c)$, so that we can write $\Pi_c = \Pi_c^{loc} \otimes \mathrm{Id}_{[n]\setminus b(c)}$.

*Definition 7:* We say that $\mathcal{M}$ is a **progressive measurement channel** if the following holds: Conditional on receiving classical information $F \subseteq C$ and $c \in C$, the quantum channel $\mathcal{M}_c^F$ performs the quantum operation $\mathcal{M}_c^F : \mathbb{C}^{N\times N} \to \mathbb{C}^{N\times N} \otimes \mathbb{R}^2$, satisfying the following properties:

- **(i)** The quantum channel labels its output with the classical labels $(S, V)$ corresponding to ("Satisfied","Violated") outcomes, so that for input $\rho$ the output state is written as:
  $\mathcal{M}_c^F(\rho) = \mathcal{M}_{c,S}^F(\rho) \otimes S + \mathcal{M}_{c,V}^F(\rho) \otimes V$.
- **(ii)** For the (unnormalised) input state $\Pi^F$, the output state labelled as "Satisfied" is upper bounded by $\Pi^{F\cup\{c\}}$:
  $\mathcal{M}_{c,S}^F(\Pi^F) \preceq \Pi^{F\cup\{c\}}$.
- **(iii)** For the input state $\Pi^F$, the output state labelled as "Violated" is upper bounded by a state of tensor product form:
  $\mathcal{M}_{c,V}^F(\Pi^F) \preceq \Pi_c^{loc} \otimes \tilde{\Pi}^{F\setminus\Gamma^+(c)}$, where $\Pi^{F\setminus\Gamma^+(c)} = \mathrm{Id}_{b(c)} \otimes \tilde{\Pi}^{F\setminus\Gamma^+(c)}$.

One might be puzzled why is it important to transform states to the "Violated" image of $\Pi_c$. (The weaker alternative to property (**iii**) would be $\mathcal{M}_{c,V}^F(\Pi^F) \preceq \Pi^{F\setminus\Gamma^+(c)}$. Since the qubits in $c$ are resampled after $c$ is found to be unsatisfied, it might not be immediately clear why we set any conditions on these qubits.) The reason is that it ensures that the resampling operation uniformly mixes quantum states, for more details see the proof of Lemma 8. The **resampling operation** on $\rho$ in line 9 can be formally described as

$$R_c(\rho) = \mathrm{Tr}_{b(c)}[\rho] \otimes \frac{\mathrm{Id}_{b(c)}}{2^k}. \tag{3}$$

In order to state and prove the Key Lemma, we need to define several concepts. For a log $L$, let $\rho_L$ denote the unnormalised quantum state after having seen and processed all measurement results in $L$, i.e., including the resampling step in line 9 if the last result was "$V$". Let $F_L$ denote the inner variables $F$ of Algorithm 1 after it has seen and processed all the measurement results described by $L$. Moreover, for $X \in \{S, V\}$ let $(L, X) \in \{S, V\}^{T+1}$ be the log obtained by appending $X$ to the end of log $L$. If the algorithm did not terminate after $L$, then let $c_L$ denote the next constraint Algorithm 1 will address.

*Lemma 8:* (Key lemma) If we run Algorithm 1 using a progressive measurement channel $\mathcal{M}$, then for every log $L$ which contains $r$ occurrences of $V$,

$$\rho_L \preceq p^r \cdot \frac{\Pi^{F_L}}{N}, \tag{4}$$

where $N = 2^n$.

*Proof:* We prove (4) for a log $L \in \{S, V\}^T$ by induction on $T$. For $T = 0$ we have $\rho_L = \rho_0 = \mathrm{Id}/N$, $\Pi^{F_L} = \mathrm{Id}$ and $p^r = p^0 = 1$ so the relation holds with equality. Now suppose that (4) holds for all logs $L \in \{S, V\}^T$. For the induction step it is enough to show that (4) also holds for $(L, S)$ and $(L, V)$, whenever $(L, S)$ and $(L, V)$ are valid logs. Let us denote by $r$ the number of "V"s in $L$, $F = F_L$, $F_S = F_L \cup \{c_L\}$, $F_V = F_L \setminus \Gamma^+(c_L)$ and $c = c_L$. Observe $F_{(L,S)} = F_S$ and $F_{(L,V)} = F_V$. First we show the inductive step for $(L, S)$:

$$\begin{aligned}
\rho_{(L,S)} =& \mathcal{M}_{c,S}^F(\rho_L) && \text{(by definition)}\\
\preceq& \mathcal{M}_{c,S}^F\left(p^r \cdot \frac{\Pi^F}{N}\right) && \text{(by the inductive hypothesis)}\\
\preceq& p^r \cdot \frac{\Pi^{F_S}}{N} && \text{(by property (**ii**))}\\
=& p^r \cdot \frac{\Pi^{F_{(L,S)}}}{N} && (F_{(L,S)} = F_L)
\end{aligned}$$

Indeed, the number of violations in $(L, S)$ remains $r$. Now

we show the inductive step for $(L, V)$:

$$\begin{aligned}
\rho_{(L,V)} =& R_c\big(\mathcal{M}^F_{c,V}(\rho_L)\big) && \text{(by definition)}\\
\preceq& R_c\left(\mathcal{M}^F_{c,V}\left(p^r\cdot\frac{\Pi^F}{N}\right)\right) && \text{(induction hypothesis)}\\
\preceq& \frac{p^r}{N}\cdot R_c\Big(\Pi^{loc}_c\otimes\tilde{\Pi}^{F_V}\Big) && \text{(by property (\textbf{iii}))}\\
=& \frac{p^r}{N}\mathrm{Tr}[\Pi^{loc}_c]\cdot\frac{\mathrm{Id}_{b(c)}}{2^k}\otimes\tilde{\Pi}^{F_V} && \text{(Eq. (3) )}\\
=& \frac{p^{r+1}}{N}\cdot\mathrm{Id}_{b(c)}\otimes\tilde{\Pi}^{F_V} && (\mathrm{Tr}(\Pi^{loc}_c)=1,\ p=\frac{1}{2^k})\\
=& \frac{p^{r+1}}{N}\cdot\Pi^{F_V} && \text{(by property (\textbf{iii}))}\\
=& \frac{p^{r+1}}{N}\cdot\Pi^{F_{(L,V)}} && (F_{L,V}=F_V)
\end{aligned}$$

Note that the number of violations in $(L, V)$ is $r + 1$, as required. ∎

Taking the trace of Eq. (9) shows property (ii) in Theorem 4 for a progressive measurement channel, and property (iii) in Theorem 4 follows from Def. 7-(**iii**). Therefore, the only missing ingredient for an efficient algorithm is to efficiently implement a progressive measurement channel. This is done in two steps: we next show an exact (but inefficient) progressive measurement channel (Def. 9), and later, in Section III show a closely related efficient variant of it.

### C. The exact measurement channel – ideal non-commuting generalisation

We are now ready to provide the first explicit construction of a progressive measurement channel, which we call the exact measurement channel. We argue that this is probably the most faithful generalisation of the commuting algorithm for the non-commuting case. The proposed quantum operation applies a measurement conditionally followed by a unitary operation. The combined procedure respects the loop-invariant, and handles new constraints in a way which seems essential for the resampling algorithm.

*Definition 9:* We define the **exact measurement channel**, denoted here by $\mathcal{M}$, in the following way: conditional on receiving classical information $F \subseteq C$ and $c \in C$, the quantum channel $\mathcal{M}^F_c : \mathbb{C}^{N\times N} \to \mathbb{C}^{N\times N}\otimes\mathbb{R}^2$ performs the projective measurement $\big(\Pi^{F\cup\{c\}}, \mathrm{Id} - \Pi^{F\cup\{c\}}\big)$. If the outcome is $\Pi^{F\cup\{c\}}$ it labels its output with $S$ standing for "Satisfied". If the outcome is $\mathrm{Id} - \Pi^{F\cup\{c\}}$ it labels its output with $V$ standing for "Violated", and applies the unitary operation $\mathrm{Rot} = WU^\dagger$, where $W\Sigma U^\dagger$ is a singular value decomposition of $\Pi_c\Pi^F$.[9] For the output state corresponding to pure input state $|\psi\rangle$ we use notation $\mathcal{M}^F_c(|\psi\rangle) = |\psi_S\rangle\otimes S + |\psi_V\rangle\otimes V$, where $|\psi_S\rangle = \Pi^{F\cup\{c\}}|\psi\rangle$ and $|\psi_V\rangle = WU^\dagger\big(\mathrm{Id} - \Pi^{F\cup\{c\}}\big)|\psi\rangle$.

In the above definition we have some ambiguity about the map $WU^\dagger$, since the singular value decomposition is not unique; this is not an issue as shown in the full version.

We want to emphasize that the progressive measurement channel is meaningful on its own, and might find applications outside the QLLL framework. For this reason, and to keep the things conceptually simple, in the following we present an example where we calculate some of the important maps explicitly, although it diverges from some of the conditions and assumptions we had before, namely the Lovász condition does not hold, one of the projectors is not rank-1, and it uses a qudit (not a qubit).

*Example 10:* Consider a qudit of of dimension 4, and the following 2 projectors: $\Pi_1 = |0\rangle\langle 0|$, $\Pi_2 = \frac{1}{2}(|0\rangle+|1\rangle)(\langle 0|+\langle 1|) + |2\rangle\langle 2|$. Let $F = \{1\}$, $c = 2$. In this case, $\Pi_c\Pi^F = \Pi_2\Pi^{\{1\}} = \frac{1}{2}(|0\rangle + |1\rangle)\langle 1| + |2\rangle\langle 2|$. A possible choice for $W$ and $U^\dagger$ yields $WU^\dagger = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 1| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 0| + |2\rangle\langle 2| + |3\rangle\langle 3|$. $\Pi^{F\cup\{c\}} = \Pi^{\{1,2\}} = |3\rangle\langle 3|$. The state $|\psi\rangle = \frac{1}{\sqrt{3}}(|1\rangle + |2\rangle + |3\rangle)$ satisfies $F$: $\Pi^F|\psi\rangle = |\psi\rangle$. The "Satisfied" post-measurement state is $|\psi_S\rangle = \frac{1}{\sqrt{3}}|3\rangle$, which occurs with probability $\frac{1}{3}$. The "Violated" post-measurement state is

$$\begin{aligned}
|\psi_V\rangle &= WU^\dagger(\mathrm{Id} - \Pi^{F\cup\{c\}}|\psi\rangle) = WU^\dagger\frac{1}{\sqrt{3}}(|1\rangle + |2\rangle)\\
&= \frac{1}{\sqrt{3}}\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + |2\rangle\right) \qquad (5)
\end{aligned}$$

which occurs with probability $\frac{2}{3}$.

In the rest of this subsection, we show in Lemma 12 that the exact measurement channel is a progressive measurement channel (and therefore respects the loop invariant), and in Proposition 13 that in the commuting case, the exact measurement channel can be implemented by simply measuring $\{\mathrm{Id} - \Pi_c, \Pi_c\}$. This shows that the exact measurement channel is a generalization of the simple projective measurement that is performed in the classical and commuting algorithms [12], [21], [22]. Before we prove these results, we need some identities of the relevant subspaces.

*Proposition 11:* Suppose $W\Sigma U^\dagger$ is a singular value decomposition of $\Pi_c\Pi^F$ (i.e., $\Pi_c\Pi^F = W\Sigma U^\dagger$ with $W^\dagger = W^{-1}$, $U^\dagger = U^{-1}$ and $\Sigma$ non-negative real and diagonal), then the following identities hold:

$$\Pi_{\mathrm{im}(\Pi_c\Pi^F)} = W\mathrm{sgn}(\Sigma)W^\dagger \qquad (6)$$

$$\Pi^F - \Pi^{F\cup\{c\}} = U\mathrm{sgn}(\Sigma)U^\dagger \qquad (7)$$

$$\Pi_{\mathrm{im}(\Pi_c\Pi^F)} \preceq \Pi_c\Pi^{F\setminus\Gamma^+(c)} \qquad (8)$$

In the above, $\mathrm{sgn}(\Sigma)$ uses the natural extension of the sign function to diagonal (and in this case, non-negative) matrices, moreover for a subspace $S$ we denote by $\Pi_S$ the orthogonal projector to $S$.

[9] There is a choice of $W$ and $U^\dagger$ in the SVD decomposition, for which $\Pi^{F\cup\{c\}} = Rot\Pi^{F\cup\{c\}}Rot^\dagger$. In this case, the unitary $Rot$ can be applied in both cases – when the outcome is "Satisfied" or "Violated". We apply it only in the "Violated" outcome purely for the convenience in the analysis.

*Proof:*

(6): $\big(W\mathrm{sgn}(\Sigma)W^\dagger\big)\Pi_c\Pi^F = \big(W\mathrm{sgn}(\Sigma)W^\dagger\big)W\Sigma U^\dagger = W\Sigma U^\dagger = \Pi_c\Pi^F$, since $W\mathrm{sgn}(\Sigma)W^\dagger$ is an orthogonal projector it implies that $\Pi_{\mathrm{im}(\Pi_c\Pi^F)} \preceq W\mathrm{sgn}(\Sigma)W^\dagger$. But also $\mathrm{rank}\big(\Pi_{\mathrm{im}(\Pi_c\Pi^F)}\big) = \mathrm{rank}\big(\Pi_c\Pi^F\big) = \mathrm{rank}\big(W\mathrm{sgn}(\Sigma)W^\dagger\big)$, thus $\Pi_{\mathrm{im}(\Pi_c\Pi^F)} = W\mathrm{sgn}(\Sigma)W^\dagger$.

(7): Similarly to (6) $\Pi_{\mathrm{im}(\Pi^F\Pi_c)} = U\mathrm{sgn}(\Sigma)U^\dagger$, so it is enough to show that $\Pi^F - \Pi^{F\cup\{c\}} = \Pi_{\mathrm{im}(\Pi^F\Pi_c)}$. Again $\Pi_{\mathrm{im}(\Pi^F\Pi_c)} \preceq \Pi^F - \Pi^{F\cup\{c\}}$, since $\big(\Pi^F - \Pi^{F\cup\{c\}}\big)\Pi^F\Pi_c = \Pi^F\Pi_c - \Pi^{F\cup\{c\}}\Pi_c = \Pi^F\Pi_c$.

But

$$\begin{aligned}\mathrm{rank}\big(\Pi_{\mathrm{im}(\Pi^F\Pi_c)}\big) &= \mathrm{rank}\big(\Pi^F\Pi_c\big)\\ &= \mathrm{rank}\big(\Pi_c\Pi^F\big)\\ &= \mathrm{rank}\big(\Pi^F\big) - \dim(\ker(\Pi_c)\cap\mathrm{im}(\Pi^F)\\ &= \mathrm{rank}\big(\Pi^F\big) - \mathrm{rank}\Big(\Pi^{F\cup\{c\}}\Big)\\ &= \mathrm{rank}\Big(\Pi^F - \Pi^{F\cup\{c\}}\Big).\end{aligned}$$

Here, the second equality is justified by $\mathrm{rank}(A) = \mathrm{rank}\big(A^\dagger\big)$, and the third equality by $\mathrm{rank}(AB) = \mathrm{rank}(B) - \dim(\ker(A)\cap\mathrm{im}(B))$ (see, e.g. [26, p. 210]).

So $\Pi^F - \Pi^{F\cup\{c\}} = \Pi_{\mathrm{im}(\Pi^F\Pi_c)}$ and thus $\Pi^F - \Pi^{F\cup\{c\}} = U\mathrm{sgn}(\Sigma)U^\dagger$.

(8): The proof follows form the following line of (in)equalities which are justified below:

$$\begin{aligned}\Pi_{\mathrm{im}(\Pi_c\Pi^F)} &= \Pi_c\Pi_{\mathrm{im}(\Pi_c\Pi^F)}\Pi_c\\ &\preceq \Pi_c\Pi^{F\setminus\Gamma^+(c)}\Pi_c\\ &= \Pi_c^2\Pi^{F\setminus\Gamma^+(c)}\\ &= \Pi_c\Pi^{F\setminus\Gamma^+(c)}.\end{aligned}$$

First observe that $\Pi_c\big(\Pi_c\Pi^F\big) = \Pi_c\Pi^F$ so $\Pi_c\Pi_{\mathrm{im}(\Pi_c\Pi^F)} = \Pi_{\mathrm{im}(\Pi_c\Pi^F)}$, implying the first equality. The penultimate equality is due to $\Pi_c\Pi^{F\setminus\Gamma^+(c)} = \Pi^{F\setminus\Gamma^+(c)}\Pi_c$, which follows from the fact that these operators act on disjoint qubits. Finally note that $\Pi^{F\setminus\Gamma^+(c)}\Pi^F = \Pi^F$. Therefore, $\Pi^{F\setminus\Gamma^+(c)}\big(\Pi_c\Pi^F\big) = \Pi_c\Pi^{F\setminus\Gamma^+(c)}\Pi^F = \Pi_c\Pi^F$ so $\Pi_{\mathrm{im}(\Pi_c\Pi^F)} \preceq \Pi^{F\setminus\Gamma^+(c)}$, which justifies the inequality. ∎

Using the above proposition we can easily show in the following lemma that the exact measurement channel is indeed progressive (see Def. 7).

*Lemma 12:* Suppose $|\psi\rangle = \Pi^F|\psi\rangle$. If we apply the exact measurement channel $\mathcal{M}_c^F$ on $|\psi\rangle$, then

- **(i)** $|\psi_S\rangle = \Pi^{F\cup\{c\}}|\psi\rangle$, and the outcome "S" happens with probability $\mathrm{Tr}(\Pi^{F\cup\{c\}}|\psi\rangle\langle\psi|)$.
- **(ii)** $|\psi_V\rangle = \Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}|\psi_V\rangle$ (where $\Pi^{F\setminus\Gamma^+(c)} = \mathrm{Id}_{b(c)}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}$).
- **(iii)** $\mathcal{M}_{c,V}^F(\Pi^F) \preceq \Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}$.

*Proof:* Property (**i**) is trivial by Definition 9.

By Definition 9 $|\psi_V\rangle = WU^\dagger\big(\mathrm{Id} - \Pi^{F\cup\{c\}}\big)|\psi\rangle$. Note that by $|\psi\rangle = \Pi^F|\psi\rangle$ we have

$$\Big(\mathrm{Id} - \Pi^{F\cup\{c\}}\Big)|\psi\rangle = \Big(\Pi^F - \Pi^{F\cup\{c\}}\Big)|\psi\rangle. \qquad (9)$$

Using (7) we can see $WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big) = WU^\dagger U\mathrm{sgn}(\Sigma)U^\dagger = W\mathrm{sgn}(\Sigma)U^\dagger$. Considering $(\mathrm{sgn}(\Sigma))^2 = \mathrm{sgn}(\Sigma)$ and $U^\dagger U = \mathrm{Id}$ we get $W\mathrm{sgn}(\Sigma)U^\dagger = W\mathrm{sgn}(\Sigma)W^\dagger WU^\dagger U\mathrm{sgn}(\Sigma)U^\dagger$ and by (6)-(7) we get $W\mathrm{sgn}(\Sigma)W^\dagger WU^\dagger U\mathrm{sgn}(\Sigma)U^\dagger = \Pi_{\mathrm{im}(\Pi_c\Pi^F)}WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big)$. Therefore, we proved $WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big) = \Pi_{\mathrm{im}(\Pi_c\Pi^F)}WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big)$. By (8) we have $\Pi_{\mathrm{im}(\Pi_c\Pi^F)} \preceq \Pi_c\Pi^{F\setminus\Gamma^+(c)} = \Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}$ which implies that $WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big) = \Big(\Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}\Big)WU^\dagger\big(\Pi^F - \Pi^{F\cup\{c\}}\big)$ proving $|\psi_V\rangle = \Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}|\psi_V\rangle$ via (9).

For the proof of property (**iii**) note that $\mathcal{M}_{c,V}^F(I) \preceq I$, which implies that $\mathcal{M}_{c,V}^F(\Pi^F) \preceq \mathcal{M}_{c,V}^F(I) \preceq I$. This together with property (**ii**) implies that $\mathcal{M}_{c,V}^F(\Pi^F) \preceq \Pi_c^{loc}\otimes\tilde{\Pi}^{F\setminus\Gamma^+(c)}$. ∎

For completeness we show that Definition 9 is indeed a generalisation of the commuting case.

*Proposition 13:* Suppose that all local projectors commute, and that the input state $|\psi\rangle$ is such that $|\psi\rangle = \Pi^F|\psi\rangle$, then the output of the exact quantum channel $\mathcal{M}_c^F$ coincides with the output of the projective measurement $(\mathrm{Id}-\Pi_c, \Pi_c)$, i.e., $|\psi_S\rangle = (\mathrm{Id} - \Pi_c)|\psi\rangle$ and $|\psi_V\rangle = \Pi_c|\psi\rangle$.

*Proof:* Since all local projectors commute we have $\Pi^F = \prod_{c'\in F}(\mathrm{Id} - \Pi_{c'})$. By Definition 9 $|\psi_S\rangle = \Pi^{F\cup\{c\}}|\psi\rangle$ and due to commutation we have $\Pi^{F\cup\{c\}} = (\mathrm{Id} - \Pi_c)\Pi^F$, so $|\psi_S\rangle = (\mathrm{Id} - \Pi_c)\Pi^F|\psi\rangle = (\mathrm{Id} - \Pi_c)|\psi\rangle$.

By Definition 9 $|\psi_V\rangle = WU^\dagger\big(\mathrm{Id} - \Pi^{F\cup\{c\}}\big)|\psi\rangle$, furthermore similarly to the proof of Lemma 12 $\big(\mathrm{Id} - \Pi^{F\cup\{c\}}\big)|\psi\rangle = \big(\mathrm{Id} - \Pi^{F\cup\{c\}}\big)\Pi^F|\psi\rangle = \big(\Pi^F - \Pi^{F\cup\{c\}}\big)|\psi\rangle$ by our assumption on $|\psi\rangle$. Using (7) we get that $|\psi_V\rangle = WU^\dagger U\mathrm{sgn}(\Sigma)U^\dagger|\psi\rangle = W\mathrm{sgn}(\Sigma)U^\dagger|\psi\rangle$. By commutation we have that $\Pi_c\Pi^F = \Pi^F\Pi_c$ is an orthogonal projector and thus $\Sigma = \mathrm{sgn}(\Sigma)$. Therefore, $W\mathrm{sgn}(\Sigma)U^\dagger = W\Sigma U^\dagger = \Pi_c\Pi^F$ and thus $|\psi_V\rangle = \Pi_c\Pi^F|\psi\rangle = \Pi_c|\psi\rangle$. ∎

If we could implement the exact measurement channel, then as Lemma 12 and Lemma 8 together with Theorem 4 show we would get an efficient algorithm for preparing frustration-free states.

Unfortunately we do not know how to implement the exact measurement channel efficiently for non-commuting projectors. However, in Section III we show how to efficiently implement a closely related quantum channel. Combined with our generalised compression argument of Theorem 4 this finally yields an efficient algorithm for uniformly gapped Hamiltonians under the Lovász condition (1). Our approximate channel has the drawback that even if the input is a pure

quantum sate its outputs can in general only be described by a probabilistic mixture of pure states.

## III. Efficient implementation

In this subsection we describe and analyse on a high level how the efficient algorithm works. The analysis will be hand-wavy, but the approximations that we use can be made precise, providing a fully rigorous proof. A detailed analysis can be found in the full version [14].

### A. Weak measurements.

We next show an efficient construction for a progressive mesaurement channel, which is closely related to the exact measurement channel introduced before. It uses *weak measurements* combined with a quantum Zeno-like effect. This approach is somewhat similar to the ideas described in [27].

Instead of directly measuring $\Pi_c$, we repeat the following many times: we perform a weak measurement (as explained below) on $\Pi_c$. If the weak measurement finds that $c$ is violated, we just apply the usual resampling step. If the outcome is that $c$ is satisfied, we (strongly) measure all constraints in $F$ simultaneously. If they are not simultaneously satisfied, we abort, and repeat otherwise. When the loop ends, we measure whether all constraints in $F \cup \{c\}$ are simultaneously satisfied, and abort if not. The fully rigorous analysis which carefully bounds all the abort errors is deferred to the full version.

**Algorithm 2** An Approximate Progressive Measurement Channel

1: **input** $\rho, F, c$ such that $\rho = \Pi^F \rho \Pi^F$
2: **repeat** $T$ times **do**
3: measure $\Pi_c$ weakly
4: **if** violated **then**
5: **return** $\rho'$, "Violated" with $c$
6: **end if**
7: measure $\Pi^F$ **if** violated **then terminate with** "ABORT: MEASURE WEAKER"
8: **end repeat**
9: measure $\Pi^{F\cup\{c\}}$ **if** violated **then terminate with** "ABORT: USE LARGER T"
10: **return** $\rho'$, "Satisfied" for $F \cup \{c\}$

For now we assume, that we can measure the projector $\Pi^F$ $\left(\text{or } \Pi^{F\cup\{c\}}\right)$, which is an orthogonal projector to the subspace where all the constraint in $F$ (or $F \cup \{c\}$) are satisfied, see Algorithm 2. Later we will implement an approximation to this measurement operator.

By tuning the weak measurement parameter and the number of repetitions, we can control and reduce the probability of aborting in this procedure. Therefore, the two probable outcomes are that we either end up with adding $c$ to $F$, the set of fixed constraints, or we find the state violating $c$ and therefore resample $c$.

One may wonder: if the probability of abort is kept small, are these strong measurements of $\Pi^F$ really necessary? Yes – similarly to the "hot pot never boils" phenomenon, and the quantum Zeno effect, even though the outcome of the measurement is known with very high probability in advance, the measurement changes the overall state dramatically when applied frequently.

Now we explain what we mean by a weak measurement, and how it can be combined with the quantum Zeno effect. Consider the two-outcome measurement $\{\Pi_c, \mathrm{Id} - \Pi_c\}$. We can implement a weak measurement on $|\psi\rangle$ with intensity parameter $\theta$ using an ancilla qubit and a $\Pi_c$-controlled rotation $U_c^\theta$ defined via

$$R^\theta := \begin{pmatrix} \sqrt{1-\theta} & -\sqrt{\theta} \\ \sqrt{\theta} & \sqrt{1-\theta} \end{pmatrix}, U_c^\theta := \Pi_c \otimes R^\theta + (\mathrm{Id} - \Pi_c) \otimes \mathrm{Id}. \tag{10}$$

We apply the unitary $U_c^\theta$ on $|\psi\rangle \otimes |0\rangle$ and do a projective measurement on the ancilla qubit. Let us denote by $|\psi_1\rangle = \sqrt{\theta}\Pi_c|\psi\rangle$ the (unnormalised) state corresponding to measurement outcome 1. So $|\psi_1\rangle \propto \Pi_c|\psi\rangle$ just as we expect from a projective (strong) measurement. Similarly, let

$$|\psi_0\rangle := (\mathrm{Id} - \Pi_c)|\psi\rangle + \sqrt{1-\theta}\Pi_c|\psi\rangle \approx |\psi\rangle - (\theta/2)\Pi_c|\psi\rangle \tag{11}$$

denote the (unnormalised) state corresponding to outcome 0.

Suppose $|\psi\rangle$ satisfies $F$, i.e., $|\psi\rangle = \Pi^F|\psi\rangle$ for the orthogonal projector $\Pi^F$ which projects to the subspace where all the constraints in $F$ are satisfied. The probability of measuring 0 on the ancilla qubit and finding the state outside the support of $\Pi^F$ has probability $\left\|\left(\mathrm{Id} - \Pi^F\right)|\psi_0\rangle\right\|^2 \approx \left\|\left(\mathrm{Id} - \Pi^F\right)(|\psi\rangle - (\theta/2)\Pi_c|\psi\rangle)\right\|^2 = \left\|\left(\mathrm{Id} - \Pi^F\right)(\theta/2)\Pi_c|\psi\rangle\right\|^2 \leq \theta^2\|\Pi_c|\psi\rangle\|^2$. The main message is the following: the probability of measuring a violation of $\Pi^F$ is a $\theta$ factor less, than the probability of finding a violation to the constraint $\Pi_c$. Whenever we find $c$ violated we exit the loop, therefore the expected number of times we find a violation of $c$ is at most 1, throughout the whole procedure. Since in every step the probability of finding a violation of $\Pi^F$ is a $\theta$ factor smaller, the aggregate probability of violating $\Pi^F$ is bounded by $\theta$. Analogously to the quantum Zeno effect, by setting $\theta$ small enough we can go below any desired error probability. This argument lies at the heart of the proof.

In some sense our error bound is even stronger than in the usual quantum Zeno effect: the probability of moving out of the support of $\Pi^F$ is proportional to $\|\Pi_c|\psi\rangle\|^2$, so the smaller the overlap with $\Pi_c$ gets, the smaller the error probability becomes. This is the reason why in the full version [14] we can show that the overall probability of abort at line 7 is bounded by $\theta$ independently of $T$ - the number of repetitions.

### B. Correctness and complexity of Algorithm 2

Now we describe a hand-wavy argument showing that for small enough $\theta$ and large enough $T$ our Algorithm 2 closely approximates a progressive measurement channel, and argue how big we should choose the parameter $T$ in order to achieve low probability of aborting on line 9. (The arguments are made precise in the full version [14].)

Let $W\Sigma U^\dagger$ be a singular value decomposition of $\Pi_c\Pi^F$. Let $\sigma_i := \Sigma_{ii}$, and let $u_i := U_{.i}$ be the $i$-th column of $U$, similarly let $w_i := W_{.i}$ be the $i$-th column of $W$. For simplicity assume, that we apply the procedure to a pure initial state $|\psi^0\rangle$, and let $|\psi^t\rangle$ denote the unnormalised state after $t$ weak and strong measurements, corresponding to the case when no positive $\Pi_c$ nor negative $\Pi^F$ measurement outcomes were observed. Let

$$|\psi^t\rangle := \sum_j a_j^t |u_j\rangle,$$

where $a_j^t$ is the amplitude of $|u_j\rangle$ in $|\psi^t\rangle$. Using Eq. (11), $|\psi^{t+1}\rangle \approx \Pi^F|\psi^t\rangle - (\theta/2)\Pi^F\Pi_c|\psi^t\rangle$. Assuming that $\Pi^F|\psi^0\rangle = |\psi^0\rangle$, we get that $\Pi^F|\psi^t\rangle = |\psi^t\rangle$ for all $t \geq 0$, and so

$$\sum_j a_j^{t+1}|u_j\rangle = |\psi^{t+1}\rangle \approx \Pi^F|\psi^t\rangle - \theta/2\Pi^F\Pi_c|\psi^t\rangle$$
$$= |\psi^t\rangle - \frac{\theta}{2}\Pi^F\Pi_c\Pi^F|\psi^t\rangle,$$

which is further equal to

$$= \left(I - \frac{\theta}{2}\Pi^F\Pi_c\Pi^F\right)|\psi^t\rangle = \left(I - \frac{\theta}{2}U\Sigma^2U^\dagger\right)|\psi^t\rangle$$
$$= \sum_j \left(1 - \frac{\theta}{2}\sigma_j^2\right)a_j^t|u_j\rangle.$$

For small $\theta$ we can move to a continuous-time approximation, and use the differential equation $\dot{a}_j \approx -\frac{\theta}{2}\sigma_j^2 a_j$, which yields the solution

$$a_j^t \approx e^{-\frac{\theta}{2}\sigma_j^2 t}a_j^0. \tag{12}$$

Observe that $a_j^t$ remains constant whenever $\sigma_j = 0$; similarly it is easy to see that if $|\psi^0\rangle \in \mathrm{im}\big(\Pi^{F\cup\{c\}}\big)$, then $|\psi^T\rangle = |\psi^0\rangle$. Thus the quantum states that are supported on the image of $\Pi^{F\cup\{c\}}$ remain undisturbed during Algorithm 2.

We want to ensure that the probability of finding the quantum state $|\psi^T\rangle$ in the kernel of $\Pi^{F\cup\{c\}}$ is low, in order to keep the probability of aborting at line 9 small. That is we want $\big\|(I - \Pi^{F\cup\{c\}})|\psi^T\rangle\big\|^2$ to becomes small. Now observe that

$$(I - \Pi^{F\cup\{c\}})|\psi^T\rangle = (I - \Pi^{F\cup\{c\}})\Pi^F|\psi^T\rangle$$
$$= (\Pi^F - \Pi^{F\cup\{c\}})|\psi^T\rangle \overset{(7)}{=} U\mathrm{sgn}(\Sigma)U^\dagger|\psi^T\rangle,$$

and therefore it is enough to ensure that $a_j^t$ gets close to 0 for all $j$ such that $\sigma_j > 0$. Let $\sigma_{\min}$ denote the minimal non-zero $\sigma_j$ value. By choosing $T \approx \log(1/\theta)/(\theta\sigma_{\min}^2)$ we can show that the probability of abort is less than $\approx \theta$. As we show in the full version, $\sigma_{\min}^2$ can be lower bounded by $\lambda_{\min}^{\neq 0}\big(\Pi_c + \sum_{c'\in F}\Pi_{c'}\big)$, the smallest non-zero eigenvalue of $\Pi_c + \sum_{c'\in F}\Pi_{c'}$, therefore we will choose $T = \Omega(1/(\theta\lambda_{\min}^{\neq 0}\big(\Pi_c + \sum_{c'\in F}\Pi_{c'}\big)))$. Thus with this choice of $T$ Algorithm 2 satisfies property (**ii**) with $\sim\theta$ slack.

Let $\rho^{V,t}$ denote the unnormalised density operator corresponding to a "Violated" outcome obtained via the weak $\Pi_c$ measurement in the $t$-th iteration. Note that after observing such an outcome Algorithm 2 terminates. Then

$$\rho^{V,t+1} = \sqrt{\theta}\Pi_c|\psi^t\rangle\langle\psi^t|\Pi_c\sqrt{\theta} = \theta\Pi_c\Pi^F|\psi^t\rangle\langle\psi^t|\Pi^F\Pi_c$$
$$= \theta W\Sigma U^\dagger|\psi^t\rangle\langle\psi^t|U\Sigma W^\dagger,$$

and so

$$\rho_{ij}^{V,t+1} := \langle w_i|\rho^{V,t+1}|w_j\rangle = \theta\big(\sigma_i a_i^t\big)\cdot\big(\sigma_j a_j^t\big)^*$$
$$\approx \theta\sigma_i\sigma_j e^{-\frac{\theta}{2}(\sigma_i^2+\sigma_j^2)t}a_i^0\cdot\big(a_j^0\big)^*.$$

We can approximate the aggregate "Violated" outcomes as

$$\rho_{ij}^{V,\mathrm{out}} := \sum_{t=1}^{\infty}\rho_{ij}^t$$
$$\approx \int_0^\infty \theta\sigma_i\sigma_j e^{-\frac{\theta}{2}(\sigma_i^2+\sigma_j^2)t}a_i^0\cdot\big(a_j^0\big)^*\,dt = \frac{2\sigma_i\sigma_j}{\sigma_i^2+\sigma_j^2}\rho_{ij}^{\mathrm{in}},$$

where we defined $\rho_{ij}^{\mathrm{in}} = \langle u_i|\rho^{\mathrm{in}}|u_j\rangle$ with $\rho^{\mathrm{in}} = |\psi^0\rangle\langle\psi^0|$. The change of basis $u_i \to w_j$ in $\rho^{\mathrm{in}} \to \rho^{\mathrm{out}}$ corresponds to the unitary map $WU^\dagger$, which we described in the exact quantum channel. Note that due to linearity this also describes the behaviour of Algorithm 2 for any, potentially mixed input state, in the infinitesimal limit. Thus it is easy to see that in this limit Algorithm 2 satisfies property (**iii**). More careful analysis shows that property (**iii**) actually holds for any choice of $\theta$ and $T$. But we need to choose small enough $\theta$ and large enough $T$ values in order to keep the probability of abort small. For more details see the full version [14].

This little calculation also explains, that for infinitesimally small $\theta$ the procedure is always successful, and projects out the complete overlap with $\Pi_c$ if repeated indefinitely. Also it is converging exponentially to its infinite version with respect to $T$ - the number of iterations. The limiting quantum channel is just the exact measurement channel with an additional decoherence channel applied on the "Violated" branch, therefore it is actually a progressive measurement channel. The additional decoherence channel decreases the coherence terms between subspaces of different singular values by a multiplicative factor of $\frac{2\sigma_i\sigma_j}{\sigma_i^2+\sigma_j^2}$. Thus, the strength of the decoherence depends on the (multiplicative) difference between the singular values, and does not happen at all if the singular values equal. Note that this phenomenon is only present for non-commuting projectors, since in the commuting case $\sigma_i \in \{0, 1\}$.

Applying this formula to Example 10, the output associated with the "Violated" outcome becomes the (impure) mixed state:

$$\rho_V = \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{2}{9} \approx 0.22 & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{2}{9} & 0 \\ \frac{2}{9} & \frac{2}{9} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

This should be compared to the exact measurement channel, where the output is the following pure state (see Eq. (5)):

$$\rho_V = \begin{pmatrix} \frac{1}{6} & \frac{1}{6} & \frac{1}{3\sqrt{2}} \approx 0.24 & 0 \\ \frac{1}{6} & \frac{1}{6} & \frac{1}{3\sqrt{2}} & 0 \\ \frac{1}{3\sqrt{2}} & \frac{1}{3\sqrt{2}} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

We want to stress that in the infinitesimal limit the approximate progressive measurement channel converges to a progressive measurement channel (and in particular, the probability of aborting vanishes), but it does not converge to the exact measurement channel. Indeed our definition of a progressive measurement channel leaves quite some room for different instantiations.

Since in general the projector $\Pi^F$ can be hard to handle, we need to establish an efficient way to perform the $\Pi^F$ measurement. Fortunately we only use this measurement when we are almost certain about its outcome. This makes it possible to approximate this complex measurement operator by repeatedly measuring $\Pi_{c'}$ for uniformly randomly chosen $c' \in F$ – see Algorithm 3. As we show in the full version, roughly[10] $\widetilde{\mathcal{O}}\Big(|F| \Big/ \lambda_{\min}^{\neq 0}\big(\sum_{c' \in F} \Pi_{c'}\big)\Big)$ repetitions achieve a good approximation. (We can proceed similarly for the projector $\Pi^{F \cup \{c\}}$.) Using this trick the complexity of implementing Algorithm 2 with $\theta$-approximation error is

$$\widetilde{\mathcal{O}}\left(\frac{|F|}{\theta} \Bigg/ \lambda_{\min}^{\neq 0}\left(\Pi_c + \sum_{c' \in F} \Pi_{c'}\right) \lambda_{\min}^{\neq 0}\left(\sum_{c' \in F} \Pi_{c'}\right)\right). \tag{13}$$

**Algorithm 3** $\tilde{\Pi}^{F,\tau}$ - an approximate projection on $\Pi^F$

1: **input** quantum state $\rho$
2: **repeat** $\tau$ times **do**
3: choose $c \in F$ uniformly at random
4: **measure** $\Pi_c$
5: **if** result "$c$ is violated" **then**
6: **return** "VIOLATED"
7: **end repeat**
8: **return** "APPROXIMATELY SATISFIED"

*The gap constraint:* The gap of a Hamiltonian – the energy difference between its (distinct) two[11] lowest energy levels – denoted $\Delta(H)$, plays an important role both in physics and computer science, particularly in Hamiltonian complexity theory, see for example [28], [29], [30], [31]. Suppose $H = \sum_{c \in} \Pi_c$, then we define the uniform gap of $H$ as

$$\gamma(H) := \min_{S \subseteq C} \Delta\left(\sum_{c \in S} \Pi_c\right). \tag{14}$$

We use our algorithm under conditions which guarantee that the minimal eigenvalue of $H$ is 0, therefore $\lambda_{\min}^{\neq 0}\big(\sum_{c' \in S} \Pi_{c'}\big) = \Delta\big(\sum_{c' \in S} \Pi_{c'}\big)$ for all $S \subseteq C$. Thus we can upper bound the runtime expression of (13) by

$$\widetilde{\mathcal{O}}\big(|C|/(\theta\gamma^2(H))\big), \tag{15}$$

giving inverse quadratic dependence on the uniform gap. This notion of uniform gap plays an important role in another recent state preparation algorithm [32], since it seems a natural requirement for algorithms that gradually build up a quantum state.

### C. The final algorithm.

To obtain a working quantum algorithm we just need to run Algorithm 1 performing the **check**ing step using the approximate Progressive Measurement Channel of Algorithm 2. We need to set the weakness parameter small enough, so that no abort error should happen throughout the whole algorithm. It turns out, that if we set the weak measurement parameter $\theta = \mathcal{O}(1/|C|)$, then with high probability we avoid any abort branch in Algorithm 2, since the expected number of resamplings is $\mathcal{O}(|C|)$, for more details see the full version [14]. Note that this way, the only quantum operations that our algorithm uses are (weak and strong) measurements of the projectors $\Pi_c : c \in C$, and of course resampling of qubits.

As Theorem 4 shows under the Lovász condition ($pde \leq 1$), the expected number of resamplings is $\mathcal{O}(|C|)$, and therefore as the proof of Lemma 3 shows the expected number of **check** operations performed by Algorithm 1 is $\mathcal{O}(|C|d)$. Thus we use the progressive measurement channel at most $\mathcal{O}(|C|d)$ times in expectation, with weakness parameter $\theta = \mathcal{O}(|C|)$. Using the expression in Eq. (15) and some standard boosting techniques we get a final algorithm that in the non-commuting case performs a total number of

$$\tilde{\mathcal{O}}\left(\frac{|C|^3 \cdot d}{\gamma^2} \cdot \log^2\left(\frac{1}{\delta}\right)\right),$$

(weak and strong) $\Pi_c : c \in C$ measurements[12], where $\gamma$ is the uniform gap, and $\delta$ is an upper bound on the trace distance of the output state from a density operator which is supported on the ground space.

In the full version of this paper [14] we also analyse our algorithm's runtime under Shearer's condition. The

[10] By $\tilde{\mathcal{O}}(t)$ we mean $\mathcal{O}(t \cdot \mathrm{polylog}(t))$.

[11] In case there is a single energy level, we define the gap to be $\infty$.

[12] The log factors are actually at most quadratic.

exact formula for the runtime bound we prove is more complicated, but it is easy to compare to classical results. Let $R_c$ be the upper bound of [13] on the expected number of resamplings of the classical Moser-Tardos algorithm. The number of (weak and strong) measurements performed by our quantum algorithm is

$$\tilde{\mathcal{O}}\left(\frac{R_c^2|C|^2n^2}{\gamma^2}\log^2\left(\frac{1}{\delta}\right)\right),$$

where $n$ is the number of qubits and the other parameters are as before.

## ACKNOWLEDGEMENTS

A.G. thanks Ronald de Wolf for support and many valuable discussions, Mário Szegedy for recommending relevant literature on the classical constructive LLL, Martin Schwarz and Niel de Beaudrap for discussions. O.S. thanks Dorit Aharonov for her valuable comments.

## REFERENCES

[1] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, vol. 54, no. 3, pp. 1862–1868, 1996. [Online]. Available: https://doi.org/10.1103/PhysRevA.54.1862

[2] D. Pérez-García, F. Verstraete, M. M. Wolf, and J. I. Cirac, "PEPS as unique ground states of local Hamiltonians," *Quantum Information & Computation*, vol. 8, no. 6, pp. 650–663, 2008. [Online]. Available: http://www.rintonpress.com/xxqic8/qic-8-67/0650-0663.pdf

[3] S. Bravyi, "Efficient algorithm for a quantum analogue of 2-SAT," in *Contemporary Mathematics*, K. Mahdavi, D. Koslover, and L. L. Brown, Eds. American Mathematical Society, 2011, vol. 536. [Online]. Available: http://www.ams.org/books/conm/536/10552/conm536-10552.pdf

[4] M. Bellare and S. Goldwasser, "The complexity of decision versus search," *SIAM J. Comput.*, vol. 23, no. 1, pp. 97–119, 1994. [Online]. Available: https://doi.org/10.1137/S0097539792228289

[5] P. Erdős and L. Lovász, "Problems and results on 3-chromatic hypergraphs and some related questions," in *Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II*. North-Holland, Amsterdam, 1975, pp. 609–627. Colloq. Math. Soc. János Bolyai, Vol. 10. [Online]. Available: http://www.renyi.hu/~p_erdos/1975-34.pdf

[6] N. Alon and J. Spencer, *The Probabilistic Method*. John Wiley, 1992. [Online]. Available: http://www.wiley.com/WileyCDA/WileyTitle/productCd-1119061954.html

[7] J. Kratochvíl, P. Savický, and Z. Tuza, "One more occurrence of variables makes satisfiability jump from trivial to np-complete," *SIAM J. Comput.*, vol. 22, no. 1, pp. 203–210, 1993. [Online]. Available: https://doi.org/10.1137/0222015

[8] M. Szegedy, "The Lovász local lemma - A survey," in *Computer Science - Theory and Applications - 8th International Computer Science Symposium in Russia, CSR 2013, Ekaterinburg, Russia, June 25-29, 2013. Proceedings*, 2013, pp. 1–11. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-38536-0_1

[9] J. B. Shearer, "On a problem of Spencer," *Combinatorica*, vol. 5, no. 3, pp. 241–245, 1985. [Online]. Available: https://doi.org/10.1007/BF02579368

[10] J. Beck, "An algorithmic approach to the Lovász local lemma. I," *Random Structures & Algorithms*, vol. 2, no. 4, pp. 343–366, 1991. [Online]. Available: http://dx.doi.org/10.1002/rsa.3240020402

[11] R. A. Moser, "A constructive proof of the Lovász local lemma," in *STOC*, 2009, pp. 343–350. [Online]. Available: http://doi.acm.org/10.1145/1536414.1536462

[12] R. A. Moser and G. Tardos, "A constructive proof of the general Lovász local lemma," *J. ACM*, vol. 57, no. 2, p. 11, 2010. [Online]. Available: http://doi.acm.org/10.1145/1667053.1667060

[13] K. B. R. Kolipaka and M. Szegedy, "Moser and Tardos meet Lovász," in *STOC*, 2011, pp. 235–244. [Online]. Available: http://doi.acm.org/10.1145/1993636.1993669

[14] A. Gilyén and O. Sattath, "On preparing ground states of gapped hamiltonians: An efficient quantum Lovász local lemma [full version]," 2016. [Online]. Available: http://arxiv.org/abs/1611.08571

[15] A. Ambainis, J. Kempe, and O. Sattath, "A quantum Lovász local lemma," *J. ACM*, vol. 59, no. 5, p. 24, 2012. [Online]. Available: http://doi.acm.org/10.1145/2371656.2371659

[16] O. Sattath, S. C. Morampudi, C. R. Laumann, and R. Moessner, "When a local Hamiltonian must be frustration-free," *PNAS*, vol. 113, no. 23, pp. 6433–6437, 2016. [Online]. Available: https://doi.org/10.1073/pnas.1519833113

[17] S. Bravyi and M. Vyalyi, "Commutative version of the local Hamiltonian problem and common eigenspace problem," *Quantum Information & Computation*, vol. 5, no. 3, pp. 187–215, 2005. [Online]. Available: http://www.rintonpress.com/xqic5/qic-5-3/187-215.pdf

[18] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe, "The power of quantum systems on a line," *Communications in Mathematical Physics*, vol. 287, no. 1, pp. 41–65, 2009. [Online]. Available: https://doi.org/10.1007/s00220-008-0710-3

[19] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," *Annals of Physics*, vol. 303, no. 1, pp. 2–30, 2003. [Online]. Available: https://doi.org/10.1016/S0003-4916(02)00018-0

[20] N. Harvey and J. Vondrák, "An algorithmic proof of the Lovász local lemma via resampling oracles," in *FOCS*, 2015. [Online]. Available: http://theory.stanford.edu/~jvondrak/data/LLL-resampling.pdf

[21] M. Schwarz, T. S. Cubitt, and F. Verstraete, "Quantum information-theoretic proof of the commutative quantum Lovász local lemma," 2013. [Online]. Available: https://arxiv.org/abs/1311.6474

[22] O. Sattath and I. Arad, "A constructive quantum Lovász local lemma for commuting projectors," *Quantum Information & Computation*, vol. 15, no. 12, pp. 987–996, 2015. [Online]. Available: http://www.rintonpress.com/xxqic15/qic-15-1112/0987-0996.pdf

[23] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, *Classical and quantum computation*, ser. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2002, vol. 47, translated from the 1999 Russian original by Lester J. Senechal. [Online]. Available: http://dx.doi.org/10.1090/gsm/047

[24] B. Misra and E. C. G. Sudarshan, "The zeno's paradox in quantum theory," *Journal of Mathematical Physics*, vol. 18, no. 4, pp. 756–763, 1977. [Online]. Available: http://dx.doi.org/10.1063/1.523304

[25] V. Kolmogorov, "Commutativity in the algorithmic Lovász local lemma," in *FOCS*, 2016, pp. 780–787. [Online]. Available: https://doi.org/10.1109/FOCS.2016.88

[26] C. Meyer, *Matrix analysis and applied linear algebra*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2000. [Online]. Available: http://dx.doi.org/10.1137/1.9780898719512

[27] D. K. Burgarth, P. Facchi, V. Giovannetti, H. Nakazato, S. Pascazio, and K. Yuasa, "Exponential rise of dynamical complexity in quantum computing through projections," *Nature Communications*, vol. 5, p. 5173, 2014. [Online]. Available: https://doi.org/10.1038/ncomms6173

[28] M. B. Hastings, "An area law for one-dimensional quantum systems," *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2007, no. 08, p. P08024, 2007. [Online]. Available: http://stacks.iop.org/1742-5468/2007/i=08/a=P08024

[29] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Quantum computation by adiabatic evolution," 2000. [Online]. Available: https://arxiv.org/abs/quant-ph/0001106

[30] D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, "Adiabatic quantum computation is equivalent to standard quantum computation," *SIAM Review*, vol. 50, no. 4, pp. 755–787, 2008. [Online]. Available: https://doi.org/10.1137/080734479

[31] T. S. Cubitt, D. Perez-Garcia, and M. M. Wolf, "Undecidability of the spectral gap," *Nature*, no. 7581, pp. 207–211. [Online]. Available: https://doi.org/10.1038/nature16059

[32] Y. Ge, A. Molnár, and J. I. Cirac, "Rapid adiabatic preparation of injective projected entangled pair states and Gibbs states," *Phys. Rev. Lett.*, vol. 116, no. 8, p. 080503, 2016. [Online]. Available: https://doi.org/10.1103/PhysRevLett.116.080503

[33] S. Jukna, *Extremal Combinatorics - With Applications in Computer Science (2nd ed.)*, ser. Texts in Theoretical Computer Science. Springer, 2011.

## APPENDIX

*Lemma 14:* If $0 < k < n$ are positive integers, then

$$\binom{n}{k} < \left(\frac{en}{k} - \frac{e}{2}\right)^k \left( < \left(\frac{en}{k}\right)^k \right) \tag{16}$$

*Proof:* We use the following upper bound [33, Cor. 22.9] on binomial coefficients

$$\begin{aligned} \forall\, 0 < k < n:\ \binom{n}{k} &\le 2^{n\cdot H(k/n)} \\ &= 2^{n\left(-\frac{k}{n}\log_2\left(\frac{k}{n}\right) - \frac{n-k}{n}\log_2\left(\frac{n-k}{n}\right)\right)} \\ &= e^{\left(k\ln\left(\frac{n}{k}\right) + (n-k)\ln\left(\frac{n}{n-k}\right)\right)}. \end{aligned}$$

(In the statement above, $H(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ denotes the binary entropy.) We use this inequality to prove (16). It remains is to show, that

$$\begin{aligned} e^{\left(k\ln\left(\frac{n}{k}\right) + (n-k)\ln\left(\frac{n}{n-k}\right)\right)} &< \left(\frac{en}{k} - \frac{e}{2}\right)^k \\ &\Updownarrow \\ \ln\left(\frac{n}{k}\right) + \left(\frac{n}{k} - 1\right)\ln\left(\frac{n}{n-k}\right) &< 1 + \ln\left(\frac{n}{k} - \frac{1}{2}\right) \\ &\Updownarrow \\ 0 < 1 + \ln\left(1 - \frac{1}{2}\frac{k}{n}\right) + \left(\frac{n}{k} - 1\right)\ln\left(1 - \frac{k}{n}\right). \end{aligned} \tag{17}$$

For $x = k/n$ let $f(x) := 1 + \ln(1-x/2) + (1/x - 1)\ln(1-x)$ denote the right hand side of (17). In order to prove that $f(x) > 0$ for all $x \in (0,1)$, we first observe that

$$\lim_{x\to 0} f(x) = 1 + \lim_{x\to 0} \frac{\ln(1-x)}{x} = 0.$$

Finally we prove $f(x) > 0$ by showing that $f'(x) > 0$ for all $x \in (0,1)$:

$$\begin{aligned} f'(x) &= -\frac{1}{2-x} - \frac{1}{x^2}\ln\left(\frac{1}{1-x}\right) - (1/x - 1)\frac{1}{1-x} \\ &= -\frac{1}{2-x} + \frac{1}{x^2}\ln\left(\frac{1}{1-x}\right) + \frac{1}{x} \\ &= \frac{1}{x} - \frac{1}{2-x} + \frac{1}{x^2}\ln\left(\frac{1+x/(2-x)}{1-x/(2-x)}\right) \\ &\overset{(18)}{>} \frac{1}{x} - \frac{1}{2-x} + \frac{1}{x^2}\frac{2x}{2-x} = 0. \end{aligned}$$

The last inequality can be deduced using the Taylor series $\forall y \in (-1,1)\ \ln(1+y) = \sum_{\ell=1}^{\infty} \frac{(-y)^\ell}{-\ell}$:

$$\begin{aligned} \forall z \in (0,1):\ \ln\left(\frac{1+z}{1-z}\right) &= \ln(1+z) - \ln(1-z) \\ &= 2z\sum_{k=0}^{\infty}\frac{z^{2k}}{2k+1} > 2z. \end{aligned} \tag{18}$$

■

Note, that by using one more term in (18) one can strengthen (16) to $\binom{n}{k} < \left(\frac{en}{k} - \frac{e}{2} - \frac{ek}{42n}\right)^k$.