Quantum Information and Computation, Vol. 5, No. 3 (2005) 187–215

COMMUTATIVE VERSION OF THE LOCAL HAMILTONIAN PROBLEM AND COMMON EIGENSPACE PROBLEM

SERGEY BRAVYI[a]
Institute for Quantum Information, California Institute of Technology
Pasadena, CA 91125, USA

MIKHAIL VYALYI[b]
Independent University of Moscow
Bol'shoi Vlas'evskii per. 11, Moscow 119002, Russia

Received May 4, 2004
Revised April 10, 2005

We study the complexity of a problem "Common Eigenspace" — verifying consistency of eigenvalue equations for composite quantum systems. The input of the problem is a family of pairwise commuting Hermitian operators $H_1, \ldots, H_r$ on a Hilbert space $(\mathsf{C}^d)^{\otimes n}$ and a string of real numbers $\lambda = (\lambda_1, \ldots, \lambda_r)$. The problem is to determine whether the common eigenspace specified by equalities $H_a|\psi\rangle = \lambda_a|\psi\rangle$, $a = 1, \ldots, r$ has a positive dimension. We consider two cases: (i) all operators H_a are k-local; (ii) all operators H_a are factorized. It can be easily shown that both problems belong to the class QMA — quantum analogue of NP, and that some NP-complete problems can be reduced to either (i) or (ii). A non-trivial question is whether the problems (i) or (ii) belong to NP? We show that the answer is positive for some special values of k and d. Also we prove that the problem (ii) can be reduced to its special case, such that all operators H_a are factorized projectors and all $\lambda_a = 0$.

Keywords: quantum complexity, quantum codes, multipartite entanglement

Communicated by: R Jozsa & J Watrous

1 Formulation of the problem

Quantum complexity were studied intensely during the last decade. Many quantum complexity classes were invented (to find any of them see a comprehensive list [1]). Many interesting results are known for these classes. Nevertheless, the exact relationship between quantum and classical complexity classes remain open for almost all of them. In this paper we will focus on the classical complexity class NP and its quantum analogue QMA which was defined in [2], [3].

Let us recall the definitions of these classes. A Boolean function $F\colon \mathsf{B}^* \to \mathsf{B}$ is in NP iff there is a function $R\colon \mathsf{B}^* \times \mathsf{B}^* \to \mathsf{B}$ computable in polynomial time on a classical computer and a polynomial p such that

$$\begin{array}{lll} F(x) = 1 & \Rightarrow & R(x,y) = 1 \text{ for some } y \in \mathsf{B}^*,\ |y| < p(|x|). \\ F(x) = 0 & \Rightarrow & R(x,y) = 0 \text{ for any } y \in \mathsf{B}^*,\ |y| < p(|x|). \end{array}$$

[a]e-mail: serg@cs.caltech.edu
[b]e-mail: vyalyi@mccme.ru

(Here and below $\mathsf{B} = \{0,1\}$ and B^* is the set of finite binary strings. A length of string $x \in \mathsf{B}^*$ is denoted by $|x|$.) It will be convenient to introduce two players: Arthur and Merlin. Arthur wants to compute $F(x)$, but he is not powerful enough to do that without assistance of Merlin. Merlin sends him the string y as a 'proof' that $F(x) = 1$. The properties of $R(x,y)$ guarantee that Merlin can convince Arthur that $F(x) = 1$ iff $F(x) = 1$.

The class QMA is defined analogously, but Arthur is able to process quantum information. For our purposes it suffices to mention three distinctions between QMA and NP. Firstly, there is a quantum communication channel between Arthur and Merlin. Thus Merlin's message may be a quantum superposition of many strings y. Secondly, Arthur has a quantum computer which he uses to verify the proof (i.e. the function $R(x,y)$ is computed by a quantum circuit, rather than a classical one). Thirdly, the verification may fail with a non-zero probability. However, the gap between Arthur's acceptance probabilities corresponding to $F(x) = 1$ and $F(x) = 0$ must be sufficiently large (bounded by a polynomial in $1/|x|$).

By definition, NP $\subseteq$ MA $\subseteq$ QMA, where MA is the class of Merlin-Arthur games — probabilistic analogue of the class NP. It is not known whether these inclusions are strict. A good candidate for separating QMA and MA is the group non-membership problem (GNM). Watrous [4] showed that GNM in the oracle model has succint quantum proofs. He also constructed an oracle B such that $\mathrm{GNM}(B) \notin \mathrm{MA}^B$. So, in a relativized world the inclusion $\mathrm{MA}^B \subset \mathrm{QMA}^B$ is strict.

Similarly to the class NP, the class QMA has complete problems. The first QMA-complete problem was found by Kitaev [2]. It is the k-local Hamiltonian problem with $k \geq 5$. Later Kempe and Regev [5] proved that the 3-local Hamiltonian problem is also QMA-complete. Then Kempe, Kitaev, and Regev [6] combined this result with a perturbative analysis to show that the 2-local Hamiltonian is QMA-complete. Recently, Janzing, Wocjan and Beth have found another example of QMA-complete problem, see [7]. It is a non-identity check for an unitary operator given by a quantum circuit.

Recall, that the input of the 2-local Hamiltonian problem is $x = (H, \varepsilon_l, \varepsilon_u)$, where H is a Hermitian operator (a Hamiltonian) acting on a Hilbert space $(\mathsf{C}^d)^{\otimes n}$ and $\varepsilon_l < \varepsilon_u$ are real numbers, such that $\varepsilon_u - \varepsilon_l \geq 1/\operatorname{poly}(n)$. The operator H has a form

$$H = \sum_{1 \leq a < b \leq n} H_{ab}, \tag{1}$$

where H_{ab} is a Hamiltonian acting on the particles a and b only. The function $F(x)$ to be computed[c] is defined as

$$\begin{array}{lcl} F(x) = 1 & \Leftrightarrow & H \text{ has an eigenvalue not exceeding } \varepsilon_l, \\ F(x) = 0 & \Leftrightarrow & \text{all eigenvalues of } H \text{ are greater than } \varepsilon_u. \end{array} \tag{2}$$

Merlin convinces Arthur that $F(x) = 1$ by sending him the ground state $|\Psi_0\rangle$ of the Hamiltonian H. For any Merlin's message $|\Psi\rangle$ Arthur can efficiently evaluate an expectation value $\langle\Psi|H|\Psi\rangle$, see [2], that allows him to verify Merlin's proof.

For some special classes of Hamiltonians the ground state may admit a good *classical* description (a good description must have a polynomial length and must allow classical polynomial verification algorithm for Arthur). A trivial case is a Hamiltonian H such that all

[c]Some binary encoding must be used for an input of all problems. Accordingly, all functions to be computed are Boolean functions (may be partially defined).

interactions H_{ab} are diagonal in the standard product basis of $(\mathsf{C}^d)^{\otimes n}$. Then the ground state is a basis vector. It can be described by $n \log(d)$ classical bits. The corresponding 2-local Hamiltonian problem thus belongs to NP. As an example, consider a graph $G = (V, E)$ with qubits living at vertices and an 'antifferomagnetic' Hamiltonian $H = +\sum_{(u,v)\in E} \sigma_u^z \sigma_v^z$, where σ_u^z is the Pauli operator acting on the qubit u. As was shown in [8], it yields NP-complete problem.

A less restricted case of the 2-local Hamiltonian problem is obtained by putting pairwise commutativity constraint on the individual interactions:

$$H_{ab}H_{cd} = H_{cd}H_{ab} \quad \text{for all pairs} \quad (a,b) \quad \text{and} \quad (c,d). \tag{3}$$

In this case all interactions are still diagonalized over the same basis. In particular, the ground state $|\Psi_0\rangle$ of H satisfies eigenvalue equations

$$H_{ab}|\Psi_0\rangle = \lambda_{ab}|\Psi_0\rangle \quad \text{for all} \quad 1 \le a < b \le n,$$

while the lowest eigenvalue of H is

$$E_0 = \sum_{1\le a<b\le n} \lambda_{ab}.$$

(If some pair of particles a, b do not interact with each other, i.e., $H_{a,b} = 0$, one can take $\lambda_{ab} = 0$.) However, a priori, there is no good classical description for the state $|\Psi_0\rangle$. Note that a mere list of the eigenvalues $\{\lambda_{ab}\}$ is not a good classical description, unless Arthur has an efficient algorithm to verify their consistency (there might be some configurations of the eigenvalues that do not correspond to any quantum state). So the complexity of the problem may be higher than NP.

As a simple example consider Hamiltonians associated with the one-dimensional cluster states, see [9]. The cluster state $|C_n\rangle$ is an entangled state of a linear chain of n qubits. It is specified by eigenvalue equations

$$S_a|C_n\rangle = |C_n\rangle, \quad S_a = (\sigma^z \otimes \sigma^x \otimes \sigma^z)[a-1, a, a+1], \tag{4}$$

where a runs from 1 to n and the square brackets indicates the qubits acted on by an operator (we use the periodic boundary conditions $\sigma^\alpha[0] \equiv \sigma^\alpha[n]$ and $\sigma^\alpha[n+1] \equiv \sigma^\alpha[1]$). All operators S_a pairwise commute. Define a Hamiltonian H as

$$H = -\sum_{a=1}^{n} S_a.$$

This Hamiltonian is 2-local with respect to a coarse-grained partition, such that the qubits $1, 2$ comprise the first 4-dimensional particle, the qubits $3, 4$ — the second, and so on (the partition is defined only for even n). Its unique ground state is the cluster state $|C_n\rangle$. This example demonstrates that the commutativity constraint (3) does not prevent the ground state of H from being highly entangled.

We shall prove that the ground state of any 2-local Hamiltonian (1) satisfying the commutativity constraint (3) always admits a good classical description,[d] so the corresponding 2-local

[d]The lowest eigenvalue of H may be degenerate. In this case one can choose a ground state with a good classical description.

Hamiltonian problem belongs to NP (is NP-complete for $d \geq 3$). It should be contrasted with the general 2-local Hamiltonian problem, which is QMA-complete.

We consider here this problem and some other problems involving sets of pairwise commuting Hermitian operators acting on a product space

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n. \tag{5}$$

The factors $\mathcal{H}_j$ will be referred to as 'particles'. The maximal local dimension

$$d = \max_{j=1,\ldots,n} \dim \mathcal{H}_j$$

will be regarded as a constant. Let us introduce two classes of operators. An operator $H \in \mathbf{L}(\mathcal{H})$ is called *factorized* if it can be expressed as $H = h_1 \otimes h_2 \otimes \cdots \otimes h_n$ for some $h_j \in \mathbf{L}(\mathcal{H}_j)$. For any group of particles $S \subseteq \{1,\ldots,n\}$ and for any operator $h \in \mathbf{L}(\bigotimes_{j\in S} \mathcal{H}_j)$ there exists a naturally defined operator $h[S] \in \mathbf{L}(\mathcal{H})$. It is equal to a tensor product of h with identity operators for all $j \notin S$. An operator $H \in \mathbf{L}(\mathcal{H})$ is called *strictly k-local* if it can be expressed as $H = h[S]$ for some $S \subseteq \{1,\ldots,n\}$, $|S| \leq k$, and $h \in \mathbf{L}(\bigotimes_{j\in S} \mathcal{H}_j)$. Note that if d and k are regarded as constants, both factorized and k-local operators admit a concise classical description (its length grows at most linearly with n).

Consider now a family of Hermitian operators $H_1, \ldots, H_r \in \mathbf{L}(\mathcal{H})$ such that

$$H_a H_b = H_b H_a \quad \text{for all} \quad 1 \leq a, b \leq r, \tag{6}$$

and a set of real numbers $\lambda_1, \ldots, \lambda_r$. We shall use a notation $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ for all these data as it will be a typical input of our problems. The operators H_a will be referred to as *check operators.* Define a *common eigenspace* (CES) corresponding to x as

$$\mathcal{L}_x = \{|\psi\rangle \in \mathcal{H} \,:\, H_a|\psi\rangle = \lambda_a|\psi\rangle \quad \text{for all} \quad a = 1, \ldots, r\} \tag{7}$$

If there are no vectors $|\psi\rangle \in \mathcal{H}$ satisfying all the eigenvalue equations, the common eigenspace is empty, $\mathcal{L}_x = 0$.

Problem 1 (THE k-LOCAL CES) The input is $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$, where all check operators H_a are k-local. Determine whether the common eigenspace $\mathcal{L}_x$ has a positive dimension.

Problem 2 (THE FACTORIZED CES) The input is $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$, where all check operators H_a are factorized. Determine whether the common eigenspace $\mathcal{L}_x$ has a positive dimension.

To analyze the complexity of these problems, the input x must be represented by a binary string using a suitable encoding. Assuming that an eigenvalue and a matrix element of a linear operator can be represented by a constant number of bits (see a remark at the end of this section), the length of the input is $|x| = O(d^{2k}r)$ for the k-local CES and $|x| = O(d^2nr)$ for the factorized CES. As was mentioned above, d and k are regarded as constants, so the length of the input is bounded by a polynomial, $|x| = \text{poly}\,(n+r)$. Note also that the consistency of the input, i.e., the commutativity constraint (6), can be verified by an algrorithm running in a time poly $(n+r)$ [e] If x is regarded as a binary string, both problems require computation

[e] In that respect the CES problems are different from the 2-local Hamiltonian problem. For the latter problem the consistency of the input (i.e., that the lowest eigenvalue of H does not belong to the interval $(\varepsilon_l, \varepsilon_u])$ is *promised.* This indicates that the CES problems are unlikely to be QMA-complete.

of a Boolean function

$$\begin{aligned} F(x) = 1 \quad &\Leftrightarrow \quad \mathcal{L}_x \neq 0, \\ F(x) = 0 \quad &\Leftrightarrow \quad \mathcal{L}_x = 0. \end{aligned} \tag{8}$$

Remarks: The input of the CES problems consists of operators and their eigenvalues. Operators acting on a space of fixed dimension will be represented by their matrix elements in some fixed basis. Note that the CES problems are formulated in terms of exact equalities. So, we need an appropriate 'exact' representation of (complex) numbers. A good choice is algebraic numbers of bounded degree of the extension over rationals. These numbers are represented by arrays of rationals and we have a trivial algorithm to check an exact equality for them.

If matrix elements are algebraic numbers and a size of the matrix is fixed then eigenvalues of the matrix are also algebraic numbers (roots of a characteristic polynomial) of a bounded degree of the extension over rationals.

To keep the bounded degree condition we put some additional restrictions to an input of factorized CES. Namely, we require that eigenvalues of all factors must belong to the *same* extension of bounded degree over rational numbers. So the eigenvalues which appear in the input belong to the same field.

It is important that such data can be efficiently manipulated. In other words there are algorithms running in polynomial time which solve all common linear algebra tasks in a space of bounded dimension (solving systems of linear equations, finding eigenvalues and eigenvectors of an operator and so on), see books [13, 14] for the subject.

2 Summary of main results

Our first theorem states the upper bound on the complexity of the CES problems.

Theorem 1 *The k-local and the factorized* CES *problems belong to* QMA.

Intuitively, it follows from the fact that any state $|\psi\rangle \in \mathcal{L}_x$ is a sound proof that $\mathcal{L}_x$ is not empty. Merlin's proving strategy in both problems is to send Arthur an arbitrary state $|\psi\rangle \in \mathcal{L}_x$. The key part of Arthur's verification algorithm is to measure eigenvalues of the check operators, see Section 3 for details.

The next theorem establishes the lower bound on the complexity of the CES problems.

Theorem 2 *The k-local* CES *is* NP*-hard for $k = 2$, $d \geq 3$ or $k \geq 3$, $d \geq 2$. The factorized* CES *is* NP*-hard for $d \geq 2$.*

We construct NP-hard instances without resorting to quantum mechanics at all — the corresponding check operators are classical, that is diagonal in the standard product basis. Namely, we will show that NP-complete problems 3-coloring and 3-CNF can be reduced to 'classical' CES problems, see Section 3 for details.

Our main result is that the CES problems belong to NP for special values of k and d.

Theorem 3 *The 2-local* CES *belongs to* NP*.*

We prove this theorem using the concept of interaction algebra introduced by Knill, Laflamme, and Viola in [16] and the elementary representation theory for finite-dimensional C^*-algebras. Roughly speaking, we find a fine-grained partition of each particle into smaller subsystems which we call subparticles. These subparticles are naturally grouped into interacting pairs, such that there is no interaction between different pairs. To verify that the common eigenspace is non zero, it suffuces to do this for each pair of subparticles independently. It can be done efficiently. The fine-grained partition reveals itself only on certain subspace of $\mathcal{H}$. It can be specified locally and Merlin's proof is just a description of this subspace. Amazingly, the structure of the common eigenspace resembles very much the structure of states with "quantum Markov chain" property, see [10].

It follows from Theorems 2,3 that the 2-local CES is NP-complete problem for $d \geq 3$. Besides, Theorem 3 has the following corollary:

Corollary 1 *The problem* 2*-local Hamiltonian with the pairwise commutativity constraint (3) belongs to* NP*.*

As far as the factorized CES is concerned, we present the following results.

Theorem 4 *The factorized* CES *with* $d = 2$ *belongs to* NP*.*

The proof of this theorem relies on the explicit formula for the dimension of the common eigenspace. Although Arthur can not use this formula to compute the dimension efficiently, sometimes it allows him to verify that two different instances of the problem yield the common eigenspace of the same dimension. It happens if the two instances satisfy simple consistency relations. We show that for any instance x of the factorized CES there exist another instance y consistent with x, such that all check operators of y are diagonal in the standard product basis. Merlin's proof that $\mathcal{L}_x \neq 0$ is just a description of the instance y and a basis vector belonging to $\mathcal{L}_y$.

To state the next theorem let us define *the factorized projectors* CES. It is the factorized CES problem whose input satisfies additional constraints.

Problem 3 (THE FACTORIZED PROJECTORS CES**)** The same as the factorized CES, but all check operators H_a are tensor products of orthogonal projectors and all $\lambda_a = 0$.

We shall prove that any factorized CES problem can be divided into two independent subproblems. The first subproblem is the factorized CES with all check operators being tensor products of the Pauli operators σ^x, σ^y, and σ^z. It can be solved efficiently using the stabilizer formalism, see [17]. The second subproblem is the factorized projectors CES. Both subproblems are defined on a subspace $\mathcal{H}' \subseteq \mathcal{H}$. This subspace is defined locally and admits a good classical description. Arthur can efficiently identify the two subproblems provided that Merlin sends him a description of $\mathcal{H}'$. In other words, we prove that Problem 2 can be non-deterministically reduced to Problem 3.

Theorem 5 *If the factorized projectors* CES *with a given* $d \geq 2$ *belongs to* NP *then the factorized* CES *with the same* d *also belongs to* NP*.*

We shall derive two interesting corollaries of Theorem 5.

Corollary 2 *The factorized* CES *with a constraint* ($\lambda_a \neq 0$ *for* $1 \leq a \leq r$) *belongs to* NP*.*

Corollary 3 *The factorized* CES *with a constraint* ($H_a H_b \neq 0$ *for* $1 \leq a, b \leq r$) *belongs to* NP*.*

The rest of the paper is organized as follows. Section 3 contains the proof of Theorems 1,2. Section 4 elucidates the connection between the k-local CES and the k-local Hamiltonian problems. Theorem 3 is proved in Section 5. Section 6 is devoted to a proof of Theorem 5 and its corollaries. In Section 7 we prove that the factorized projectors CES for qubits ($d = 2$) belongs to NP. Being combined with Theorem 5, this result immediately implies that the factorized CES for qubits belongs to NP, i.e., Theorem 4. Unfortunately we do not know how to generalize the algorithm described in Section 7 to the case $d \geq 3$. The reason this algorithm fails for $d \geq 3$ is rather non-trivial and can be understood with the help of Kochen-Specker theorem [19]. We briefly discuss a connection with Kochen-Specker theorem in the concluding part of Section 7.

3 Inclusion in QMA and NP-hardness

The proof of Theorem 1 is contained in the following two lemmas.

Lemma 1 *The k-local* CES *belongs to* QMA.

Proof: Let $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ be an instance of the k-local CES, $\mathcal{L}_x$ be the common eigenspace, and $F(x)$ be the Boolean function (8) to be computed. Merlin's proof that $F(x) = 1$ will be a quantum state $|\eta\rangle \in \mathcal{H}$, see (5). We shall construct a polynomial (in $|x|$) size quantum circuit that tells Arthur whether to accept or reject the proof (i.e. decide that $F(x) = 1$ or $F(x) = 0$).

The Hilbert space $\mathcal{H}$ can be encoded using $n \log_2 d$ qubits. Under this encoding any check operator H_a acts non-trivially on at most $k \log_2 d$ qubits (this number does not depend on the complexity parameters n, r and must be regarded as a constant).

One can assume without loss of generality, that all operators H_a are orthogonal projectors and all $\lambda_a = 1$ (otherwise, consider the spectral decomposition of H_a and substitute H_a by the projector corresponding to the eigenvalue λ_a). Define a POVM measurement M_a corresponding to the decomposition $I = H_a + (I - H_a)$. Since the operator H_a acts only on a constant number of qubits, Arthur can implement the measurement M_a by a quantum circuit of a constant size.[f] Suppose Arthur implements the measurements $M_1, \ldots, M_r$ and gets outcomes $\lambda'_1, \ldots, \lambda'_r \in \{0, 1\}$ (the order is not essential, since the measurements commute). The post-measurement state $|\eta'\rangle$ satisfies eigenvalue equations

$$H_a|\eta'\rangle = \lambda'_a|\eta'\rangle, \quad a = 1, \ldots, r.$$

Arthur accepts the proof $|\eta\rangle$ iff all $\lambda'_a = 1$ (in which case $|\eta'\rangle \in \mathcal{L}_x$ and thus $\mathcal{L}_x \neq 0$).

If $F(x) = 1$, Merlin can send Arthur a state $|\eta\rangle \in \mathcal{L}_x$. Then Arthur accepts the proof with a probability 1. If $F(x) = 0$, Arthur rejects all proofs $|\eta\rangle$ with a probability 1. The size of the quantum circuit used in the protocol is bounded by poly (r). This is enough to place the problem to QMA.

□

Lemma 2 *The factorized* CES *belongs to* QMA.

Proof: Let $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ be an instance of the factorized CES, $\mathcal{L}_x$ be the common eigenspace, $F(x)$ be the Boolean function (8) to be computed, and $|\eta\rangle \in \mathcal{H}$ be the Merlin's proof that $F(x) = 1$.

Arthur may pick up $a = 1, \ldots, r$ in random and check the equality $H_a|\eta\rangle = \lambda_a|\eta\rangle$ for the chosen value of a only. To do that Arthur performs a destructive measurement of the eigenvalue of H_a on the state $|\eta\rangle$. If the measured eigenvalue equals λ_a, he accepts the proof, otherwise rejects it. Denote p_0 and p_1 probabilities for Arthur to accept the proof provided that $F(x) = 0$ and $F(x) = 1$ respectively. Let $H_a = \bigotimes_{j=1}^n H_{a,j}$. Without loss of generality we can assume that all factors $H_{a,j}$ are Hermitian operators. Arthur must perform n separate projective eigenvalue measurements for all factors $H_{a,j}$. Because each factor $H_{a,j}$

[f] We shall skip the details concerning the approximation precision. In all cases considered in this paper the approximation precision can be easily made arbitrarily small with only poly-logarithmic overhead.

acts on $\log_2 d$ qubits, the whole measurement can be realized by a quantum circuit of a size $O(n)$ (recall that d is regarded as a constant). After that Arthur computes the product of n measured eigenvalues to evaluate λ_a.

If $|\eta\rangle \in \mathcal{L}_x$, Arthur always accepts the proof and thus $p_1 = 1$. Suppose $\mathcal{L}_x = 0$. We shall prove that $p_0 \le 1 - 1/r$. Let $|\eta_0\rangle \in \mathcal{H}$ be the state which maximizes the acceptance probability p_0. For any real vector $\chi = (\chi_1, \ldots, \chi_r)$ denote $P(\chi) \in \mathbf{L}(\mathcal{H})$ the projector on the subspace specified by equalities $H_a|\psi\rangle = \chi_a|\psi\rangle$, $a = 1, \ldots, r$ (a vector χ is analogous to an error syndrome in quantum codes theory). Since the projectors $P(\chi)$ pairwise commute, they make up a unity decomposition, i.e. $\sum_\chi P(\chi) = I$. Denote also

$$f(\chi) = \langle \eta_0 | P(\chi) | \eta_0 \rangle.$$

For the chosen Arthur's verification algorithm we have

$$p_0 = \frac{1}{r} \sum_{a=1}^{r} \sum_{\chi \,:\, \chi_a = \lambda_a} |f(\chi)|^2.$$

Changing the order of the summations we come to

$$p_0 = \frac{1}{r} \sum_{\chi} |f(\chi)|^2 \left(\sum_{a \,:\, \chi_a = \lambda_a} 1 \right).$$

But since $\mathcal{L}_x = 0$ we have $\chi_a \neq \lambda_a$ for at least one $a = 1, \ldots, r$ whenever $P(\chi) \neq 0$. Thus

$$p_0 \le \frac{1}{r} \sum_{\chi} |f(\chi)|^2 (r-1) = 1 - \frac{1}{r}.$$

So we have a gap $p_1 - p_0 = 1/r = \Omega(1/|x|)$ between acceptance probabilities of positive and negative instances. As was said in the beginning of Section 2, this is enough to place the problem in QMA.

□

The following two lemmas constitute the proof of Theorem 2.

Lemma 3 *The* 2*-local* CES *is* NP*-hard for* $d \ge 3$.

Proof: We will show that the NP-complete 3-coloring problem can be reduced to 2-local CES with $d = 3$. (An idea used in this reduction was suggested by Beth and Wocjan in [8]). Let $G = (V, E)$ be an arbitrary graph. The 3-coloring problem is to determine whether the graph G admits a coloring of the vertices with 3 colors such that each edge has endpoints of different colors. Let $n = |V|$ and $r = 3|E|$. Choose a Hilbert space $\mathcal{H} = (\mathbb{C}^3)^{\otimes n}$ such that each vertex of the graph carries a space $\mathbb{C}^3$. The operators H_a will be assigned to the edges with three operators assigned to each edge. These operators are responsible for three forbidden coloring of the edge. It is convenient to introduce a composite index $a = (uv, c)$, where $(uv) \in E$ is an edge and $c \in \{1, 2, 3\}$ is a color. Then the 2-local CES $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ is defined as

$$H_{uv,c} = (|c,c\rangle\langle c,c|)[u,v], \quad \lambda_{uv,c} = 0, \quad (uv) \in E, \quad c = 1,2,3. \tag{9}$$

Obviously, existence of non-trivial common eigenspace $\mathcal{L}_x$ is equivalent to existence of 3-coloring for the graph G. (Note that the projectors (9) also provide an instance of the factorized projectors CES.) We have shown that 2-local CES with $d \ge 3$ is NP-hard.

□

Lemma 4 *The k-local* CES *is* NP*-hard for $d = 2$, $k \geq 3$.*

Proof: We will prove that NP-complete 3-CNF problem can be reduced to 3-local CES with $d = 2$. Recall that 3-CNF (conjunctive normal form) is a Boolean function of the form $L(x) = C_1(x) \wedge C_2(x) \wedge \cdots \wedge C_r(x)$, $x = (x_1, \ldots, x_n) \in \mathsf{B}^n$, where each *clause* $C_a(x)$ is a disjunction of three literals (a literal is a variable or negation of a variable). An example of three-literal clause is $x_1 \vee x_3 \vee (\neg x_5)$. The 3-CNF problem is to determine whether an equation $L(x) = 1$ admits at least one solution. Choose a Hilbert space $\mathcal{H} = (\mathsf{C}^2)^{\otimes n}$. The operators H_a and the eigenvalues λ_a must be assigned to the clauses $C_a(x)$ according to the following table:

$C_a(x)$	H_a	λ_a
$x_i \vee x_j \vee x_k$	$(\|0,0,0\rangle\langle 0,0,0\|)[i,j,k]$	0
$x_i \vee x_j \vee (\neg x_k)$	$(\|0,0,1\rangle\langle 0,0,1\|)[i,j,k]$	0
...	...	...
$(\neg x_i) \vee (\neg x_j) \vee (\neg x_k)$	$(\|1,1,1\rangle\langle 1,1,1\|)[i,j,k]$	0

It is easy to check that the common eigensubspace for the 3-local CES introduced above is non-trivial iff the equation $L(x) = 1$ has at least one solution. Thus we have reduced 3-CNF problem to the 3-local CES.

□

Obviously, the 3-local CES assigned to 3-CNF problem in the previous lemma is a special case of the factorized projectors CES (and thus a special case of the factorized CES). So we have proved all statements of Theorem 2.

4 The k-local commuting Hamiltonian

We shall now discuss the k-local Hamiltonian problem. Recall that the problem is to evaluate the Boolean function (2) with the Hamiltonian

$$H = \sum_{a=1}^{r} H_a, \quad H_a \text{ is strictly } k\text{-local for all } a. \tag{10}$$

If, additionally, all terms in H pairwise commute,

$$H_a H_b = H_b H_a \quad \text{for all} \quad a, b,$$

we shall call the problem "k-local commuting Hamiltonian". The goal of this section is to reduce the k-local commuting Hamiltonian to the k'-local CES. In the first Lemma a non-determistic reduction with $k' = k$ is put forward. It also shows that Corollary 1 indeed follows from Theorem 3. The second Lemma [18] establishes a deterministic reduction with $k' = k + 1$.

Lemma 5 *If the k-local* CES *belongs to* NP *then the k-local commuting Hamiltonian also belongs to* NP*.*

Proof: Obviously, we can choose a complete set of eigenvectors of H which are eigenvectors of all operators H_a also. To prove that H indeed has an eigenvalue not exceeding ε_l Merlin can send Arthur a set of eigenvalues $(\lambda_1, \ldots, \lambda_r)$ such that

(i) $\sum_{a=1}^{r} \lambda_a \le \varepsilon_l$,
(ii) $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ is a positive instance of k-local CES (i.e. $\mathcal{L}_x \neq 0$).
Although Arthur can not verify (ii) by himself, according to assumption of the lemma this verification belongs to NP. So Arthur can ask Merlin to include a proof of (ii) in his message. It follows that k-local commuting Hamiltonian problem belongs to NP.

□

Lemma 6 *The problem k-local commuting Hamiltonian can be polynomially reduced to the* $(k+1)$*-local* CES.

Proof: Let $x = (H, \varepsilon_l, \varepsilon_u)$ be an instance of the k-local commuting Hamiltonian. Here the Hamiltonian H has the form (10). Taking the spectral decomposition of each operator H_a we can rewrite the Hamiltonian as follows:

$$H = \sum_{a=1}^{R} \varepsilon_a \Pi_a, \quad \Pi_a \Pi_b = \Pi_b \Pi_a \quad \text{for all} \quad a, b,$$

where all Π_a are orthogonal projectors. Note that the number of terms R is at most $R = rd^k$, that is only linear in the length of the input $|x|$ (recall that d and k are regarded as constants). For any binary string $y = (y_1, \ldots, y_R)$ define the corresponding energy

$$E(y) = \sum_{a=1}^{R} \varepsilon_a y_a,$$

and the eigenspace

$$\mathcal{L}_y = \{|\psi\rangle \in \mathcal{H} \, : \, \Pi_a |\psi\rangle = y_a |\psi\rangle \quad \text{for all} \quad a = 1, \ldots, R\}.$$

Then x is a positive instance of the problem iff there exist a binary string y such that $E(y) \le \varepsilon_l$ and $\mathcal{L}_y \neq 0$. Let us define a Boolean function

$$\begin{array}{lcl} f(y) = 1 & \Leftrightarrow & E(y) \le \varepsilon, \\ f(y) = 0 & \Leftrightarrow & E(y) > \varepsilon, \end{array} \tag{11}$$

where $\varepsilon = (\varepsilon_l + \varepsilon_u)/2$. Obviously, $f(y)$ can be computed by an algorithm running in a polynomial time, or equivalently, there exists a polynomial classical circuit that computes $f(y)$. Accordingly, $f(y)$ can be written as a 3-CNF formula that uses $poly(R)$ ancillary bits, see [2], Theorem 3.5. More strictly, it means that there exists a 3-CNF formula $g(y, z)$ that takes as arguments two binary strings $y \in \mathsf{B}^R$, $z \in \mathsf{B}^Q$, $Q = poly(R)$, and such that

$$f(y) = 1 \quad \text{iff} \quad g(y, z) = 1 \quad \text{for some} \quad z \in \mathsf{B}^Q.$$

By combining the two strings y and z into a single string $\tilde{y} \in B^{R+Q}$, we can write

$$g(\tilde{y}) = C_1(\tilde{y}) \wedge C_2(\tilde{y}) \wedge \cdots \wedge C_M(\tilde{y}), \quad M = \text{poly}\,(R). \tag{12}$$

Here each clause C_j involves at most three bits $\tilde{y}_a$. Summarizing, x is a positive instance iff there exists a string $\tilde{y} = (y, z) \in \mathsf{B}^{R+Q}$ such that $g(\tilde{y}) = 1$ and $\mathcal{L}_y \neq 0$.

We are now ready to present an instance of the $(k+1)$-local CES associated with x. The CES problem is defined on the space

$$\mathcal{H}' = \mathcal{H} \otimes (\mathsf{C}^2)^{\otimes R} \otimes (\mathsf{C}^2)^{\otimes Q}.$$

The second register of R qubits will 'keep' the binary string y. The third register is auxiliary. Denote $|0_a\rangle\langle 0_a|$ and $|1_a\rangle\langle 1_a|$ the projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ applied to the a-th qubit of the second register. The CES problem has two families of check operators. The first one is

$$H'_a = \Pi_a \otimes |1_a\rangle\langle 1_a| \otimes I + (I - \Pi_a) \otimes |0_a\rangle\langle 0_a| \otimes I, \quad a = 1, \ldots R.$$

Roughly speaking, H'_a ties a value of y_a to an eigenvalue of the projector Π_a. Note that the operators H'_a are strictly $(k+1)$-local. The check operators of the second family act only on the second and the third registers. They are associated with the clauses C_j in (12). Let us introduce an operator $\hat{C}_j$ acting on $R+Q$ qubits such that its action on the basis vectors $|\tilde{y}\rangle \in (\mathsf{C}^2)^{\otimes(R+Q)}$ is

$$\hat{C}_j|\tilde{y}\rangle = C_j(\tilde{y})|\tilde{y}\rangle.$$

The corresonding check operator acting on $\mathcal{H}'$ is $I \otimes \hat{C}_j$. It is strictly 3-local, which is also $(k+1)$-local for $k \ge 2$ (for $k=1$ the statement of the lemma is trivial). Consider a common eigenspace

$$\mathcal{M} = \{|\psi\rangle \in \mathcal{H}' \, : \, H'_a|\psi\rangle = |\psi\rangle, \quad I \otimes \hat{C}_j|\psi\rangle = |\psi\rangle \quad \text{for all} \quad a = 1, \ldots, R; \; j = 1, \ldots, M\}.$$

It follows from the definitions that $\mathcal{M} \ne 0$ iff there exist a product state $|\psi\rangle \otimes |y\rangle \otimes |z\rangle \in \mathcal{H}'$ such that $|\psi\rangle \in \mathcal{L}_y$ and $f(y) = 1$. It means that x is a positive instance of the k-local commuting Hamiltonian problem.

□

5 The 2-local common eigenspace problem

Let us start from revisiting the example of cluster states, see Section 1. Recall that the chain of n qubits is partitioned into two-qubit particles as shown on Fig. 1. There are n check operators $S_1, \ldots, S_n$, see (4). The common eigenspace $\mathcal{L}$ is defined by equations $S_a|\psi\rangle = |\psi\rangle$, where a runs from 1 to n. In this example $\mathcal{L}$ is one-dimensional with the basis vector $|C_n\rangle$. Although $|C_n\rangle$ is a highly entangled state, its entanglement has very simple structure with respect to the coarse-grained partition. Indeed, denote the qubits comprising the j-th particle as $j.l$ and $j.r$, see Fig. 1. A pair of qubits $j.r$ and $(j+1).l$ will be referred to as a bond. Let V_j be the controlled-σ^z operator applied to the qubits $j.l$ and $j.r$, and $V = V_1 \otimes \cdots \otimes V_n$. It is an easy exercise to verify that the state $V|C_n\rangle$ is a tensor product over the bonds:

$$V|C_n\rangle = |\phi[1.r, 2.l]\rangle \otimes |\phi[2.r, 3.l]\rangle \otimes \cdots \otimes |\phi[n.l, 1, r]\rangle, \tag{13}$$

where the square brackets indicate owners of a state and $|\phi\rangle \sim |0,0\rangle + |0,1\rangle + |1,0\rangle - |1,1\rangle$ is specified by eigenvalue equations $(\sigma^x \otimes \sigma^z)|\phi\rangle = (\sigma^z \otimes \sigma^x)|\phi\rangle = |\phi\rangle$. In other words, $|C_n\rangle$ can be prepared from a collection of bipartite pure states distributed between the particles by local unitary operators. This fact is not just a coincidence. We will show later that for any instance of the 2-local CES the common eigenspace is either empty or contains a state which can be created from a collection of bipartite pure states by applying local isometries (local unitary embeddings into a larger Hilbert space).

We continue by making a simplification that allow one to reduce the number of check operators. Let $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ be an instance of the 2-local CES and $\mathcal{L}_x$ be the common eigenspace. For each pair of particles (j,k) consider a subset $S_{jk} \subseteq \{1,2,\ldots,r\}$ such that $a \in S_{jk}$ iff H_a acts trivially on all particles $l \notin \{j,k\}$. Define an eigenspace

$$\mathcal{L}_{jk} = \{|\psi\rangle \in \mathcal{H} \,:\, H_a|\psi\rangle = \lambda_a|\psi\rangle \quad \text{for all} \quad a \in S_{jk}\}.$$

Denote $\Pi_{jk} \in \mathcal{L}(\mathcal{H})$ the orthogonal projector onto $\mathcal{L}_{jk}$ (we shall use a convention $\Pi_{jk} = \Pi_{kj}$). Clearly, $\{\Pi_{jk}\}$ is a family of pairwise commuting 2-local operators and the common eigenspace $\mathcal{L}_x$ is specified by equations

$$\mathcal{L}_x = \{|\psi\rangle \in \mathcal{H} \,:\, \Pi_{jk}|\psi\rangle = |\psi\rangle \quad \text{for all} \quad 1 \le j < k \le n\}. \tag{14}$$

Summarizing, it suffices to prove Theorem 3 only for the following version of the 2-local CES.

Input: A family of 2-local pairwise commuting projectors $x = \{\Pi_{jk}\}$, $1 \le j < k \le n$.
Problem: Determine whether the common eigenspace (14) has a positive dimension.

Our first goal is to introduce a notion of *irreducible* instance and prove Theorem 3 for irreducible instances only. Define an algebra

$$\mathcal{N}_j = \{O \in \mathbf{L}(\mathcal{H}_j) \,:\, O[j]\,\Pi_{jk} = \Pi_{jk}\,O[j] \quad \text{for all} \quad k \ne j\}. \tag{15}$$

It includes all operators acting on the particle j and commuting with any check operator.

Definition 1 *An instance x of the 2-local* CES *is irreducible iff the algebras $\mathcal{N}_j$ are trivial, i.e., $\mathcal{N}_j = \mathsf{C} \cdot I$ for all $j = 1, \ldots, n$.*

For example, the 2-local CES corresponding to the cluster state is irreducible. Indeed, an operator $O \in \mathcal{N}_j$ acting on the qubits $j.r$ and $j.l$ (see Figure 1) must commute with the Pauli operators $\sigma^x \otimes \sigma^z$, $\sigma^z \otimes \sigma^x$, $I \otimes \sigma^z$, $\sigma^z \otimes I$, which is possible only if $O \sim I$. On the other hand, the 2-local CES corresponding to a commuting Hamiltonian $H = \sum_{(j,k)} t_{jk}\,\sigma^z_j \sigma^z_k$ (see Section 4) is reducible, since $\mathcal{N}_j$ includes σ^z_j. Arthur can check whether an instance is irreducible using an efficient algorithm, since the constraints (15) are given by linear equations on a space of bounded dimension. We shall now prove that any irreducible instance of the 2-local CES is positive ($\mathcal{L}_x \ne 0$), unless one of the projectors is the zero one. The proof is based on the following lemma.

Lemma 7 *Let $x = \{\Pi_{jk}\}$ be an irreducible instance of the 2-local* CES. *There exist*

- *Hilbert spaces $\mathcal{H}_{j.k}$, $1 \le j,k \le n$, such that $\mathcal{H}_{j.j} = \mathsf{C}$,*

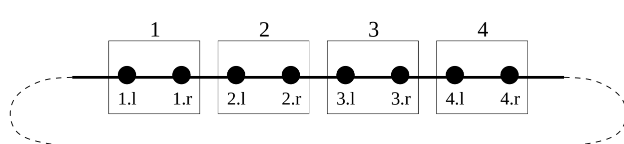

Fig. 1. A chain of 8 qubits is partitioned into $n = 4$ particles with local dimensions $d = 4$.

- *A tensor product structure* $\mathcal{H}_j = \bigotimes_{k=1}^n \mathcal{H}_{j.k}$,

such that the projector Π_{jk} *acts non-trivially only on the two factors* $\mathcal{H}_{j.k} \otimes \mathcal{H}_{k.j}$ *in the decomposition* $\mathcal{H} = \bigotimes_{l,m=1}^n \mathcal{H}_{l.m}$.

The lemma says that there exists a fine-grained partition of the system, such that the particle j is decomposed into several subparticles $\{j.k\}$. The interaction between the particles j and k affects only the subparticles $j.k$ and $k.j$, that is $\Pi_{jk} = h_{jk}[j.k, k.j]$ for some projector $h_{jk} \in \mathbf{L}(\mathcal{H}_{j.k} \otimes \mathcal{H}_{k.j})$. Accordingly, the common eigenspace $\mathcal{L}_x$ has a tensor product structure:

$$\mathcal{L}_x = \bigotimes_{j<k} \mathcal{M}_{jk}, \tag{16}$$

where $\mathcal{M}_{jk} \subseteq \mathcal{H}_{j.k} \otimes \mathcal{H}_{k.j}$ is specified by an equation $h_{jk}|\psi\rangle = |\psi\rangle$. It follows that $\mathcal{L}_x \neq 0$ iff all the projectors Π_{jk} are non-zero (indeed, $\mathcal{M}_{jk} \neq 0$ iff $h_{jk} \neq 0$ iff $\Pi_{jk} \neq 0$). So the lemma has the following amazing corollary.

Corollary 4 *An irreducible instance of the* 2*-local* CES *is positive unless* $\Pi_{jk} = 0$ *for some pair of particles* (j,k).

Now we move on to the proof of Lemma 7. The main mathematical tool is the representation theory for finite-dimensional C^*-algebras. In the subsequent discussion the term C^*-algebra refers to any algebra of operators on a finite-dimensional Hilbert space which is †-closed and contains the identity. The center a C^*-algebra $\mathcal{A}$ is defined as

$$Z(\mathcal{A}) = \{X \in \mathcal{A} \,:\, XY = YX \quad \text{for all} \quad Y \in \mathcal{A}\}.$$

An algebra has a trivial center iff $Z(\mathcal{A}) = \mathsf{C} \cdot I$. We shall use the following fact (for the proof see the book [15], or Theorem 5 in [16]):

Fact 1: *Let* $\mathcal{H}$ *be a Hilbert space and* $\mathcal{A} \subseteq \mathbf{L}(\mathcal{H})$ *be a* C^**-algebra with a trivial center. There exists a tensor product structure* $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ *such that* $\mathcal{A}$ *is the subalgebra of all operators acting on the factor* $\mathcal{H}_1$ *i.e.,*

$$\mathcal{A} = \mathbf{L}(\mathcal{H}_1) \otimes I.$$

Proof of Lemma 7: Consider any pair of particles (j,k) and let $\Pi_{jk} = h[j,k]$ for some $h \in \mathbf{L}(\mathcal{H}_j \otimes \mathcal{H}_k)$. Our goal is to construct two C^*-algebras $\mathcal{A}_{j.k} \subseteq \mathbf{L}(\mathcal{H}_j)$ and $\mathcal{A}_{k.j} \subseteq \mathbf{L}(\mathcal{H}_k)$ such that $h \in \mathcal{A}_{j.k} \otimes \mathcal{A}_{k.j}$. The main element of the construction was proposed by Knill, Laflamme, and Viola [16], who studied †-closed algebras generated by an interaction between a system and an environment. Consider a decomposition

$$h = \sum_\alpha A_\alpha \otimes B_\alpha, \tag{17}$$

where each of the families of operators $\{A_\alpha \in \mathbf{L}(\mathcal{H}_j)\}$ and $\{B_\alpha \in \mathbf{L}(\mathcal{H}_k)\}$ is a linearly independent one. Denote $\mathcal{M}_{j.k}$ and $\mathcal{M}_{k.j}$ the linear spaces spanned by $\{A_\alpha\}$ and $\{B_\alpha\}$ respectively (if $h = 0$, put $\mathcal{M}_{j.k} = \mathcal{M}_{k.j} = 0$). One can easily verify that $\mathcal{M}_{j.k}$ and $\mathcal{M}_{k.j}$ do not depend upon the choice of the decomposition (17). An identity

$$h^\dagger = h = \sum_\alpha A_\alpha^\dagger \otimes B_\alpha^\dagger,$$

tells us that $\mathcal{M}_{j.k}$ and $\mathcal{M}_{k.j}$ are closed under Hermitian conjugation. Define $\mathcal{A}_{j.k} \subseteq \mathbf{L}(\mathcal{H}_j)$ and $\mathcal{A}_{k.j} \subseteq \mathbf{L}(\mathcal{H}_k)$ as the minimal C^*-algebras such that $\mathcal{M}_{j.k} \subseteq \mathcal{A}_{j.k}$ and $\mathcal{M}_{k.j} \subseteq \mathcal{A}_{k.j}$. Equivalently, $\mathcal{A}_{j.k}$ is generated by the family $\{A_\alpha\} \cup I$ and $\mathcal{A}_{k.j}$ is generated by $\{B_\alpha\} \cup I$. (The fact that h is a projector is irrelevant for this construction.)

Consider any triple of particles j, k, l and the C^*-algebras $\mathcal{A}_{j.k}, \mathcal{A}_{j.l} \subseteq \mathbf{L}(\mathcal{H}_j)$. The first claim is that these algebras commute i.e.,

$$XY = YX \quad \text{for all} \quad X \in \mathcal{A}_{j.k} \quad \text{and} \quad Y \in \mathcal{A}_{j.l}. \tag{18}$$

Indeed, the projectors Π_{jk} and Π_{jl} can be represented as

$$\Pi_{jk} = H[j,k,l], \quad \Pi_{jl} = G[j,k,l],$$

where the operators $H, G \in \mathbf{L}(\mathcal{H}_j \otimes \mathcal{H}_k \otimes \mathcal{H}_l)$ admit decompositions

$$H = \sum_\alpha A_\alpha \otimes B_\alpha \otimes I, \quad G = \sum_\beta C_\beta \otimes I \otimes D_\beta.$$

Here each of the families $\{A_\alpha\}$, $\{B_\alpha\}$, $\{C_\beta\}$, and $\{D_\beta\}$ is a linearly independent one. The commutativity constraint $\Pi_{jk}\Pi_{jl} = \Pi_{jl}\Pi_{jk}$ yields

$$\sum_{\alpha,\beta} (A_\alpha C_\beta - C_\beta A_\alpha) \otimes B_\alpha \otimes D_\beta = 0.$$

All terms in the sum are linearly independent due to the second and the third factors. Thus the equality is possible only if $A_\alpha C_\beta = C_\beta A_\alpha$ for all α and β. Since the algebras $\mathcal{A}_{j.k}$ and $\mathcal{A}_{j.l}$ are generated by $\{A_\alpha\}$ and $\{C_\beta\}$ respectively, we conclude that they commute.

Consider any pair of particles $j \neq k$ and prove that the center $Z(\mathcal{A}_{j.k})$ is trivial. Indeed, it follows from (18) that any central element $Z \in Z(\mathcal{A}_{j.k})$ commutes with all elements of the algebras $\mathcal{A}_{j.l}$ (including $l = k$). Since $\Pi_{jl} = h[j,l]$ for some $h \in \mathcal{A}_{j.l} \otimes \mathcal{A}_{l.j}$, we conclude that the operator $Z[j] \in \mathbf{L}(\mathcal{H})$ commutes with all the projectors Π_{jl} (including Π_{jk}). Since we consider an irreducible instance of CES, this is possible only if $Z = \lambda \cdot I$ for some complex number λ. Thus $Z(\mathcal{A}_{j.k}) = \mathsf{C} \cdot I$.

Let us show how $\mathcal{H}_j$ acquires the tensor product structure for some particular j. Choose any $k \neq j$ and make use of Fact 1 with $\mathcal{H} \equiv \mathcal{H}_j$ and $\mathcal{A} \equiv \mathcal{A}_{j.k} \subseteq \mathbf{L}(\mathcal{H}_j)$. It follows that $\mathcal{H}_j$ admits a decomposition

$$\mathcal{H}_j = \mathcal{H}_{j.k} \otimes \mathcal{H}'_j, \tag{19}$$

such that the algebra $\mathcal{A}_{j.k}$ is the algebra of all operators acting on the factor $\mathcal{H}_{j.k}$ i.e.,

$$\mathcal{A}_{j.k} = \mathbf{L}(\mathcal{H}_{j.k}) \otimes I. \tag{20}$$

Consider now a third particle $l \notin \{j,k\}$. Let us examine the commutativity relation between the algebras $\mathcal{A}_{j.k}$ and $\mathcal{A}_{j.l}$. It is consistent with the decompositions (19,20) iff $\mathcal{A}_{j.l}$ acts trivially on the factor $\mathcal{H}_{j.k}$. In other words, any element $X \in \mathcal{A}_{j.l}$ has a form $X = I \otimes X'$ for some $X' \in \mathbf{L}(\mathcal{H}'_j)$. We can now make use of Fact 1 with $\mathcal{H} \equiv \mathcal{H}'_j$ and $\mathcal{A} \equiv \mathcal{A}_{j.l}$ to get a finer decomposition

$$\mathcal{H}_j = \mathcal{H}_{j.k} \otimes \mathcal{H}_{j.l} \otimes \mathcal{H}''_j,$$

such that

$$\mathcal{A}_{j.k} = \mathbf{L}(\mathcal{H}_{j.k}) \otimes I \otimes I \quad \text{and} \quad \mathcal{A}_{j.l} = I \otimes \mathbf{L}(\mathcal{H}_{j.l}) \otimes I.$$

Repeating these arguments we arrive to a decomposition $\mathcal{H}_j = (\bigotimes_{k\ne j} \mathcal{H}_{j.k}) \otimes \mathcal{H}_{j.j}$, such that the algebra $\mathcal{A}_{j.k}$ coincides with the algebra of all linear operators on the factor $\mathcal{H}_{j.k}$. As for the last factor $\mathcal{H}_{j.j}$, it is acted on by neither of the algebras. This factor however can not appear for an irreducible problem. Indeed, any operator $X \in \mathbf{L}(\mathcal{H}_j)$ acting only on $\mathcal{H}_{j.j}$ would commute with all the algebras $\mathcal{A}_{j.k}$. Accordingly, an operator $X[j]$ would commute with all the projectors Π_{jk}. This is possible only if $X = \lambda \cdot I$. Thus the algebra $\mathbf{L}(\mathcal{H}_{j.j})$ is just the algebra of complex numbers. It follows that $\mathcal{H}_{j.j} = \mathsf{C}$. Summarizing, we get

$$\mathcal{H}_j = \bigotimes_{k=1}^{n} \mathcal{H}_{j.k}, \quad \mathcal{H}_{j.j} = \mathsf{C}, \quad \mathcal{A}_{j.k} = I \otimes \cdots \otimes I \otimes \mathbf{L}(\mathcal{H}_{j.k}) \otimes I \otimes \cdots \otimes I.$$

It follows from the definitions above that Π_{jk} acts non-trivially only on the factor $\mathcal{H}_{j.k}$ in $\mathcal{H}_j$ and only on the factor $\mathcal{H}_{k.j}$ in $\mathcal{H}_k$. The lemma is proved.

□

The next step is to generalize Lemma 7 to reducible instances. We first outline the generalization and then put it formally. For each particle j a local 'classical variable' α_j will be defined. Each value of α_j specifies a subspace $\mathcal{H}_j^{\alpha_j} \subseteq \mathcal{H}_j$, such that a decomposition $\mathcal{H}_j = \bigoplus_{\alpha_j} \mathcal{H}_j^{\alpha_j}$ is a direct sum. This decomposition is preserved by all check operators. If one fixes the classical variables $\alpha_1, \ldots, \alpha_n$ for each particle, one gets some subspace $\mathcal{H}^{(\alpha_1 \cdots \alpha_n)} \subseteq \mathcal{H}$. The restriction of the problem on this subspace is almost irreducible (in the sense specified below), so Lemma 7 can be applied. In other words, for fixed values of the classical variables the fine-grained partition into subparticles emerges. The subparticles are naturally grouped into pairs, such that there are no any interactions between different pairs. Arthur can solve the restricted problem efficiently. Accordingly, the role of Merlin is just to send Arthur the values of the classical variables $\alpha_1, \ldots, \alpha_n$ for which the intersection $\mathcal{L}_x \bigcap \mathcal{H}^{(\alpha_1 \cdots \alpha_n)}$ is not empty.

Lemma 8 *Let $x = \{\Pi_{jk}\}$ be an instance of the 2-local* CES*. There exist*

- *Direct sum decompositions $\mathcal{H}_j = \bigoplus_{\alpha_j} \mathcal{H}_j^{(\alpha_j)}$,*
- *Hilbert spaces $\mathcal{H}_{j.k}^{(\alpha_j)}$, $1 \le j, k \le n$,*
- *A tensor product structure $\mathcal{H}_j^{(\alpha_j)} = \bigotimes_{k=1}^n \mathcal{H}_{j.k}^{(\alpha_j)}$,*

such that the projector Π_{jk} can be represented as

$$\Pi_{jk} = \bigoplus_{\alpha_j} \bigoplus_{\alpha_k} \Pi_{jk}^{(\alpha_j \alpha_k)}, \quad \Pi_{jk}^{(\alpha_j \alpha_k)} \in \mathbf{L}(\mathcal{H}_j^{(\alpha_j)} \otimes \mathcal{H}_k^{(\alpha_k)}),$$

where $\Pi_{jk}^{(\alpha_j \alpha_k)}$ acts non-trivially only on the two factors $\mathcal{H}_{j.k}^{(\alpha_j)} \otimes \mathcal{H}_{k.j}^{(\alpha_k)}$ in the tensor product decomposition of $\mathcal{H}_j^{(\alpha_j)} \otimes \mathcal{H}_k^{(\alpha_k)}$.

Remarks: (1) As in Lemma 7, the notation $j.k$ refers to subparticles of the particle j. (2) It should be noted that the spaces $\mathcal{H}_{j.j}^{(\alpha_j)}$ are acted on by neither of the check operators. That is why they do not appear in Lemma 7. However, if the problem is reducible, and there exist an operator $h[j]$ commuting with all check operators, it acts *only* on the spaces $\mathcal{H}_{j.j}^{(\alpha_j)}$. (4) Any of the Hilbert spaces listed in Lemma 8 may be one-dimensional.

Let us introduce a string variable $\alpha = (\alpha_1, \ldots, \alpha_n)$ and a subspace

$$\mathcal{H}^{(\alpha)} = \mathcal{H}_1^{(\alpha_1)} \otimes \cdots \otimes \mathcal{H}_n^{(\alpha_n)},$$

such that $\mathcal{H} = \bigoplus_\alpha \mathcal{H}^{(\alpha)}$. A straightforward corollary of the lemma is that the common eigenspace can be represented as a direct sum:

$$\mathcal{L}_x = \bigoplus_\alpha \mathcal{M}^{(\alpha)}, \quad \mathcal{M}^{(\alpha)} = \mathcal{L}_x \bigcap \mathcal{H}^{(\alpha)} \tag{21}$$

where each subspace $\mathcal{M}^{(\alpha)}$ has a tensor product structure:

$$\mathcal{M}^{(\alpha)} = \left(\bigotimes_{j=1}^n \mathcal{H}_{j.j}^{(\alpha_j)} \right) \otimes \left(\bigotimes_{j<k} \mathcal{M}_{jk}^{(\alpha_j \alpha_k)} \right), \quad \mathcal{M}_{jk}^{(\alpha_j \alpha_k)} \subseteq \mathcal{H}_{j.k}^{(\alpha_j)} \otimes \mathcal{H}_{k.j}^{(\alpha_k)}. \tag{22}$$

(Some of the subspaces $\mathcal{M}_{jk}^{(\alpha_j \alpha_k)}$ may be zero though.) Indeed, the lemma says that

$$\Pi_{jk}^{(\alpha_j \alpha_k)} = h_{jk}^{(\alpha_j \alpha_k)}[j.k, k.j], \quad \text{for some} \quad h_{jk}^{(\alpha_j \alpha_k)} \in \mathbf{L}\left(\mathcal{H}_{j.k}^{(\alpha_j)} \otimes \mathcal{H}_{k.j}^{(\alpha_k)} \right).$$

Thus the eigenvalue equations $\Pi_{jk}|\psi\rangle = |\psi\rangle$ specifying $\mathcal{L}_x$ lead to (21,22) with

$$\mathcal{M}_{jk}^{(\alpha_j \alpha_k)} = \left\{ |\phi\rangle \in \mathcal{H}_{j.k}^{(\alpha_j)} \otimes \mathcal{H}_{k.j}^{(\alpha_k)} \, : \, h_{jk}^{(\alpha_j \alpha_k)} |\phi\rangle = |\phi\rangle \right\}. \tag{23}$$

Theorem 3 is a simple corollary of Lemma 8. Indeed, Merlin's proof that $\mathcal{L}_x \neq 0$ may be a description of the subspaces $\mathcal{H}_j^{(\alpha_j)} \subseteq \mathcal{H}_j$, $j = 1, \ldots, n$, such that $\mathcal{L}_x \bigcap \mathcal{H}^{(\alpha)} \neq 0$. Arthur uses Merlin's message to find the restricted projectors $\Pi_{jk}^{(\alpha_j \alpha_k)}$. It follows from (21,22,23) that $\mathcal{L}_x \neq 0$ iff $\Pi_{jk}^{(\alpha_j \alpha_k)} \neq 0$ for all j and k. Arthur can verify it efficiently.

As an alternative way to prove Theorem 3, let us show that the common eigenspace $\mathcal{L}_x$ always contains a state with a good classical description. Indeed, choose some value of α for which $\mathcal{L}_x \bigcap \mathcal{H}^{(\alpha)} \neq \emptyset$. Denote $V_j : \mathcal{H}_j^{(\alpha_j)} \to \mathcal{H}_j$ an isometry corresponding to the embedding $\mathcal{H}_j^{(\alpha_j)} \subseteq \mathcal{H}_j$. Choose arbitrary states $|\phi_{jk}\rangle \in \mathcal{M}_{jk}^{(\alpha_j \alpha_k)}$ and $|\phi_j\rangle \in \mathcal{H}_{j.j}^{(\alpha_j)}$. Denote

$$|\phi\rangle = \bigotimes_{j=1}^n |\phi_j\rangle \otimes \left(\bigotimes_{k<l} |\phi_{kl}\rangle \right) \in \mathcal{H}^{(\alpha)}.$$

This state is just a collection of bipartite pure states and local unentangled states. As such it has a concise classical description. The state $|\phi'\rangle = (V_1 \otimes \cdots \otimes V_n)|\phi\rangle$ belongs to $\mathcal{L}_x$ and also has a concise classical description. Indeed, an eigenvalue equation $\Pi_{jk}|\phi'\rangle = |\phi'\rangle$ follows from identities

$$\Pi_{jk} V = V \Pi_{jk}^{(\alpha_j \alpha_k)}, \quad \Pi_{jk}^{(\alpha_j \alpha_k)} |\phi\rangle = |\phi\rangle,$$

where we denoted $V = V_1 \otimes \cdots \otimes V_n$. To prove that $\mathcal{L}_x \neq 0$ Merlin can send Arthur a description of the spaces $\mathcal{H}_{j.k}^{(\alpha_j)}$, the states $|\phi_j\rangle$, $|\phi_{jk}\rangle$, and the isometries V_j.

In the rest of this section we prove Lemma 8. It requires a generalization of Fact 1 to C^*-algebras with a non-trivial center (the statement given below coincides with Theorem 5 in [16]).

Fact 2: *Let $\mathcal{H}$ be a Hilbert space and $\mathcal{A} \subseteq \mathbf{L}(\mathcal{H})$ be a C^*-algebra. There exist a direct sum decomposition $\mathcal{H} = \bigoplus_\alpha \mathcal{H}^{(\alpha)}$ and a tensor product structure $\mathcal{H}^{(\alpha)} = \mathcal{H}_1^{(\alpha)} \otimes \mathcal{H}_2^{(\alpha)}$ such that*

$$\mathcal{A} = \bigoplus_\alpha \mathbf{L}(\mathcal{H}_1^{(\alpha)}) \otimes I.$$

The center $Z(\mathcal{A})$ is generated by orthogonal projectors on the subspaces $\mathcal{H}^{(\alpha)}$.

Proof of Lemma 8: For each $j \neq k$ define a C^*-algebra $\mathcal{A}_{j.k} \subseteq \mathbf{L}(\mathcal{H}_j)$ in the same way as in the proof of Lemma 7. A key role is played by a C^*-algebra $\mathcal{A}_{j.j} \equiv \mathcal{N}_j \subseteq \mathbf{L}(\mathcal{H}_j)$, see (15). These algebras obey certain commutativity relations. Namely, for any $k \neq l$ one has

$$XY = YX \quad \text{for all} \quad X \in \mathcal{A}_{j.k} \quad \text{and} \quad Y \in \mathcal{A}_{j.l}. \tag{24}$$

These relations follow from (18) for $j \notin \{k, l\}$ and from the definition of $\mathcal{A}_{j.j}$ for $j \in \{k, l\}$. Thus any element of the center $Z(\mathcal{A}_{j.k})$ commutes with all algebras under consideration. As such, it must be an element of $\mathcal{A}_{j.j}$, that is $Z(\mathcal{A}_{j.k}) \subseteq \mathcal{A}_{j.j}$. But the algebras $\mathcal{A}_{j.k}$ and $\mathcal{A}_{j.j}$ pairwise commute, so one has

$$Z(\mathcal{A}_{j.k}) \subseteq Z(\mathcal{A}_{j.j}) \quad \text{for all} \quad k. \tag{25}$$

Let us apply Fact 2 with $\mathcal{A} \equiv \mathcal{A}_{j.j}$ and $\mathcal{H} \equiv \mathcal{H}_j$. One gets a direct sum decomposition

$$\mathcal{H}_j = \bigoplus_{\alpha_j} \mathcal{H}_j^{(\alpha_j)}, \quad \mathcal{H}_j^{(\alpha_j)} = \mathcal{H}_{j.j}^{(\alpha_j)} \otimes \mathcal{K}_j^{(\alpha_j)}, \tag{26}$$

such that

$$\mathcal{A}_{j.j} = \bigoplus_{\alpha_j} \mathbf{L}(\mathcal{H}_{j.j}^{(\alpha_j)}) \otimes I \equiv \bigoplus_{\alpha_j} \mathcal{A}_{j.j}^{(\alpha_j)}. \tag{27}$$

Consider any pair of particles (j, k) and any operator $h \in \mathcal{A}_{j.k}$. It follows from (24) that h commutes with any element of $\mathcal{A}_{j.j}$. In particular, it commutes with any element of its center, $Z(\mathcal{A}_{j.j})$. Since an orthogonal projector onto $\mathcal{H}_j^{(\alpha_j)}$ is an element of $Z(\mathcal{A}_{j.j})$ (see Fact 2), we conclude that h preserves the subspaces $\mathcal{H}_j^{(\alpha_j)}$. Thus the algebra $\mathcal{A}_{j.k}$ has the same direct sum structure:

$$\mathcal{A}_{j.k} = \bigoplus_{\alpha_j} \mathcal{A}_{j.k}^{(\alpha_j)}, \quad \mathcal{A}_{j.k}^{(\alpha_j)} \subseteq \mathbf{L}(\mathcal{H}_j^{(\alpha_j)}).$$

It follows from (25) that each subalgebra $\mathcal{A}_{j.k}^{(\alpha_j)}$ has a trivial center. Moreover, the commutativity relation (24) implies that $\mathcal{A}_{j.k}^{(\alpha_j)}$ acts only on the factor $\mathcal{K}_j^{(\alpha_j)}$ in the decomposition (26).

Let us fix any $\alpha = (\alpha_1, \ldots, \alpha_n)$ and consider the subspace $\mathcal{H}^{(\alpha)} = \bigotimes_{j=1}^n \mathcal{H}_j^{(\alpha_j)} \subseteq \mathcal{H}$. Since a check operator Π_{jk} is an element of the tensor product $\mathcal{A}_{j.k} \otimes \mathcal{A}_{k.j}$ (see the proof of Lemma 7), the decomposition $\mathcal{H} = \bigoplus_\alpha \mathcal{H}^{(\alpha)}$ is preserved by all check operators. Therefore one can define restricted check operators

$$\Pi_{jk}^{(\alpha)} = \Pi_{jk}|_{\mathcal{H}^{(\alpha)}} \in \mathbf{L}(\mathcal{H}^{(\alpha)}). \tag{28}$$

From (26) one gets

$$\mathcal{H}^{(\alpha)} = \left(\bigotimes_{j=1}^{n} \mathcal{H}_{j.j}^{(\alpha_j)} \right) \otimes \mathcal{K}^{(\alpha)}, \quad \mathcal{K}^{(\alpha)} \equiv \bigotimes_{j=1}^{n} \mathcal{K}_j^{(\alpha_j)}. \tag{29}$$

It follows that the restricted check operators (28) act only on the factor $\mathcal{K}^{(\alpha)}$.

Consider an instance y of the 2-local CES with the Hilbert space $\mathcal{K}^{(\alpha)}$ and the check operators (28). This instance is irreducible. Indeed, suppose an operator $Z \in \mathbf{L}(\mathcal{K}_j^{(\alpha_j)})$ belongs to the set $\mathcal{N}_j$ (see Definition 1) corresponding to the instance y. Denote $Z' = I \otimes Z \in \mathbf{L}(\mathcal{H}^{(\alpha)})$, where I acts on all factors except for $\mathcal{K}_j^{(\alpha_j)}$ in the decomposition (29). By definition, $Z' \in \mathcal{A}_{j.j}^{(\alpha_j)}$, see (27). But we know that the algebra $\mathcal{A}_{j.j}^{(\alpha)}$ acts only on the factor $\mathcal{H}_{j.j}^{(\alpha_j)}$ in the decomposition (29). Thus Z is proportional to the identity, that is y is irreducible. By applying Lemma 7 to y we get the desired tensor product decomposition of $\mathcal{H}_j^{(\alpha_j)}$ and $\Pi_{jk}^{(\alpha)}$ (it suffices to delete all the superscripts).

□

It should be mentioned that for k-local CES problem with $k \geq 3$ the check operators do not necesseraly commute with each *locally*, as it is the case for the 2-local CES, see (18). Thus the techniques presented above can not be directly applied to $k > 2$.

6 The factorized common eigenspace problem

In this section we prove Theorem 5. First of all we shall answer a simple question: under what circumstances do factorized Hermitian operators commute with each other?

Lemma 9 *Let $H_1, H_2 \in \mathbf{L}(\mathcal{H})$ be tensor products of Hermitian operators:*

$$H_a = \bigotimes_{j=1}^{n} H_{a,j}, \quad H_{a,j}^{\dagger} = H_{a,j}, \quad a = 1, 2, \quad j = 1, \ldots, n.$$

Then the commutator $[H_1, H_2] = 0$ iff one of the following conditions hold

1. *$H_{1,j} H_{2,j} = \pm H_{2,j} H_{1,j}$ for each j in the range $1, \ldots, n$. The number of anticommuting factors is even.*
2. *$H_{1,j} H_{2,j} = 0$ for some $j \in [1, n]$. Equivalently, $H_1 H_2 = 0$.*

Proof: Obviously, either of conditions stated in the lemma is sufficient. Suppose that $[H_1, H_2] = 0$ and prove that at least one of the conditions is true. We have

$$\bigotimes_{j=1}^{n} H_{1,j} H_{2,j} = \bigotimes_{j=1}^{n} H_{2,j} H_{1,j}. \tag{30}$$

If both sides of this equality equal zero then $H_{1,j} H_{2,j} = 0$ for at least one $j \in [1, n]$. Suppose that both sides are non-zero operators, i.e. $H_{1,j} H_{2,j} \neq 0$ for all j. Then by definition of a tensor product, there exists a set of complex numbers $r_1, \ldots, r_n$ such that

$$H_{1,j} H_{2,j} = r_j H_{2,j} H_{1,j}, \quad j = 1, \ldots, n \quad \text{and} \quad \prod_{j=1}^{n} r_j = 1. \tag{31}$$

This equality says that the operator $H_{2,j}$ maps any eigenvector of $H_{1,j}$ to an eigenvector of $H_{1,j}$. Under this map an eigenvalue of $H_{1,j}$ is multiplied by r_j. It means that r_j must be a real number. Taking Hermitian conjugation of (31) we get an equality $H_{2,j}H_{1,j} = r_j H_{1,j} H_{2,j}$. Combining it with (31) yields $r_j^2 = 1$, i.e. $r_j = \pm 1$, which completes the proof.

□

This lemma motivates the following definition.

Definition 2 Let $H_1, H_2 \in \mathbf{L}(\mathcal{H})$ be Hermitian factorized commuting operators. We say that H_1 and H_2 commute *in a singular way* iff $H_1 H_2 = 0$. Otherwise we say that H_1 and H_2 commute *in a regular way.*

Thus saying that H_1 and H_2 commute in a regular way implies that all factors of H_1 and H_2 either commutes or anticommutes.

Let $x = (H_1, \ldots, H_r; \lambda_1, \ldots, \lambda_r)$ be an instance of the factorized CES problem. By definition,

$$H_a = \bigotimes_{j=1}^{n} H_{a,j}, \quad H_{a,j}^\dagger = H_{a,j} \quad \text{for all} \quad a = 1, \ldots, r, \quad j = 1, \ldots, n. \tag{32}$$

It will be convenient to define a table $T_x = \{H_{a,j}\}$ whose entries are Hermitian operators. Let us agree that the columns of the table T_x correspond to particles (the index j), while the rows correspond to the check operators (the index a). Let us give one more definition:

Definition 3 A row a of the table T_x is called *regular* if $\lambda_a \neq 0$. If $\lambda_a = 0$ the row a is called *singular.*

Generally, some rows of T_x commute in a regular way and some rows commute in a singular way. Note that two regular rows always commute in a regular way unless $\mathcal{L}_x = 0$. Indeed, if $H_a H_b = 0$ for some regular rows a, b, then for any $|\psi\rangle \in \mathcal{L}_x$ one has $0 = H_a H_b |\psi\rangle = \lambda_a \lambda_b |\psi\rangle$. Since $\lambda_a, \lambda_b \neq 0$, this is possible only if $|\psi\rangle = 0$. It is the presence of rows which commute in a singular way which makes the problem highly non-trivial. In this case the operators $H_{a,j}$ and $H_{b,j}$ may neither commute nor anticommute and their eigenspaces may be embedded into $\mathcal{H}_j$ more or less arbitrarily. In this situation we can not expect that the common eigenspace $\mathcal{L}_x$ contains a state which has a 'good' classical description.

As before, Merlin claims that x is a positive instance ($\mathcal{L}_x \neq 0$) and Arthur must verify it. First of all we note that Arthur may perform two significant simplifications of the table T_x by himself.

Simplification 1: Note that $\operatorname{Im} H_a = \bigotimes_{j=1}^n \operatorname{Im} H_{a,j}$ for any $a \in [1, r]$ and that the subspace $\operatorname{Im} H_a$ is preserved by all other check operators. If the a-th row is a regular one then, in addition, $\mathcal{L}_x \subseteq \operatorname{Im} H_a$. Thus we can restrict the problem on the subspace $\mathcal{H}' \subseteq \mathcal{H}$ defined as

$$\mathcal{H}' = \bigcap_{a\,:\,\lambda_a \neq 0} \operatorname{Im} H_a = \bigotimes_{j=1}^{n} \mathcal{H}'_j, \quad \mathcal{H}'_j = \bigcap_{a\,:\,\lambda_a \neq 0} \operatorname{Im} H_{a,j}. \tag{33}$$

Obviously, restricted check operators $H_a|_{\mathcal{H}'}$ are factorized and pairwise commuting. Thus the modified problem is the factorized CES with a constraint that *an operator $H_{a,j}$ is non-degenerate whenever a is a regular row.* Since Arthur can easily find the subspaces $\mathcal{H}'_j$ and the restricted operators $H_a|_{\mathcal{H}'}$, we can assume that the original instance x already satisfies this constraint.

Simplification 2: For any singular row b denote $H'_{b,j} \in \mathbf{L}(\mathcal{H}_j)$ a projector on the subspace $\operatorname{Im} H_{b,j} \subseteq \mathcal{H}_j$. Denote

$$H'_b = \bigotimes_{j=1}^{n} H'_{b,j}.$$

Obviously, $\operatorname{Im} H_b = \operatorname{Im} H'_b = \bigotimes_{j=1}^n \operatorname{Im} H_{b,j}$, so that

$$\operatorname{Ker} H_b = \operatorname{Ker} H'_b. \tag{34}$$

The subspace $\operatorname{Im} H'_b$ is preserved by all check operators H_a, so that

$$[H_a, H'_b] = 0 \quad \text{for all } a = 1, \ldots, r. \tag{35}$$

Thus if we substitute each $H_{b,j}$ by $H'_{b,j}$ (i.e. substitute H_b by H'_b), the new family of operators is pairwise commuting. So it corresponds to some factorized CES problem. The equality (34) tells us that both problems have the same answer. Applying, if necessary, the substitutions $H_b \to H'_b$, we can assume that the original problem x satisfies the following constraint: *$H_{b,j}$ is a projector whenever b is a singular row.* In other words, we can assume that singular rows of the table T_x constitute a factorized projectors CES.

Lemma 10 *If a is a regular row and b is a singular row then $[H_{a,j}, H_{b,j}] = 0$ for all $j = 1, \ldots, n$.*

Proof: Since the operators $\{H_{a,j}\}_j$ are non-degenerate, we have $H_a H_b \neq 0$, i.e. a regular and a singular row can commute only in a regular way. Thus $H_{a,j}$ and $H_{b,j}$ either commute or anticommute for all j. Suppose that $H_{a,j} H_{b,j} = -H_{b,j} H_{a,j}$ for some j. Since $H_{a,j} H_{b,j} \neq 0$, the operator $H_{a,j}$ maps an eigenvector of $H_{b,j}$ to an eigenvector of $H_{b,j}$ reversing a sign of the eigenvalue. But after the simplifications $H_{b,j}$ became a projector and thus it can not anticommute with $H_{a,j}$.

□

Let us summarize the results of the two simplifications:

- $H_{a,j}$ is non-degenerate whenever a is a regular row.
- $H_{a,j}$ is a projector whenever a is a singular row.
- $[H_{a,j}, H_{b,j}] = 0$ for all j whenever a is regular and b is singular.

In the remaining part of the section we describe a non-deterministic reduction of the simplified factorized CES problem to the factorized projectors CES. The reduction is based on the following possible transformations of the table T_Λ and the vector $\{\lambda_a\}$:

(i). Suppose there exists $j \in [1, n]$ and a Hermitian operator $Z \in \mathbf{L}(\mathcal{H}_j)$ such that Z commutes with all $H_{1,j}, \ldots, H_{r,j}$. Then $Z[j]$ commutes with all $H_1, \ldots, H_r$ and thus preserves the subspace $\mathcal{L}_x$. Assuming that $\mathcal{L}_x \neq 0$, the operator Z has some eigenvalue ω such that the intersection $\mathcal{L}_x \bigcap \operatorname{Ker}(Z[j] - \omega)$ is non-zero. So a transformation

$$\mathcal{H}_j \to \mathcal{H}'_j \equiv \operatorname{Ker}(Z - \omega I) \quad \text{and} \quad H_{a,j} \to H_{a,j}|_{\mathcal{H}'_j}, \quad a = 1, \ldots, r$$

leads to an equivalent instance. To implement this transformation, Merlin should send a description of (j, Z, ω) to Arthur.

(ii). Suppose for some $j \in [1,n]$ we have $\mathcal{H}_j = \mathcal{H}'_j \otimes \mathcal{H}''_j$ and $H_{a,j} = H'_{a,j} \otimes H''_{a,j}$ for all $a = 1,\ldots,r$ (here $H'_{a,j}$ acts on the factor $\mathcal{H}'_j$ and $H''_{a,j}$ acts on the factor $\mathcal{H}''_j$). A transformation replacing the j-th column by two new columns with entries $\{H'_{a,j}\}$ and $\{H''_{a,j}\}$ leads to an equivalent problem.

(iii). Suppose in some column j all operators $H_{a,j}$ are proportional to the identity: $H_{a,j} = r_a I$ for some real numbers r_a, $a = 1,\ldots,r$. We may delete the j-th column from the table and perform a transformation $\lambda_a \to \lambda_a / r_a$, $a = 1,\ldots,r$.

(iv). For any column j we can perform a transformation

$$H_{a,j} \to U H_{a,j} U^\dagger, \quad a = 1,\ldots,r,$$

where $U \in \mathbf{L}(\mathcal{H}_j)$ is an arbitrary unitary operator.

(v). For any non-zero real number r we can replace some $H_{a,j}$ by $rH_{a,j}$ and replace λ_a by $r\lambda_a$.

(vi). Swaps of the columns and swaps of the rows.

We claim that the transformations (i) – (vi) allow to transform the simplified instance x into a *canonical* form x_c. The instance x_c consists of two independent problems. The first problem is the factorized CES with $\lambda_a = \pm 1$ and all check operators being tensor products of the Pauli operators and the identity. The second problem is the factorized projectors CES. More strictly, the table T_{x_c} for the instance x_c has the following structure:

Pauli operators	I	$\lambda_a = \pm 1$
I	factorized projectors	$\lambda_a = 0$

The table is divided into four blocks. Columns in the left half of the table represent the qubits, i.e. $\mathcal{H}_j = \mathsf{C}^2$. All operators $H_{a,j}$ sitting at the north-west block are either the Pauli operators $\sigma_x, \sigma_y, \sigma_z$, or the identity. All operators $H_{a,j}$ sitting at the south-east block are projectors. Any operator $H_{a,j}$ sitting in the blocks labeled by 'I' is the identity. The whole Hilbert space $\mathcal{H}$ factorizes: $\mathcal{H} = \mathcal{H}' \otimes \mathcal{H}''$, where the factor $\mathcal{H}' = \mathsf{C}^2 \otimes \cdots \otimes \mathsf{C}^2$ corresponds to the left half and $\mathcal{H}''$ — to the right half of the table. The common eigenspace also factorizes: $\mathcal{L}_{x_c} = \mathcal{L}' \otimes \mathcal{L}''$, where $\mathcal{L}'$ is a code subspaces of some stabilizer code (see [2, 17] for the subject), and $\mathcal{L}''$ is the factorized projectors CES. Obviously $\mathcal{L}_{x_c} \neq 0$ iff $\mathcal{L}' \neq 0$ and $\mathcal{L}'' \neq 0$. Arthur can verify that $\mathcal{L}' \neq 0$ (and even compute the dimension of $\mathcal{L}'$) using an efficient algorithm, see [2]. Thus the original instance x has been reduced to an instance of the factorized projectors CES (since Arthur must use Merlin's message each time he implement the transformation (i), this reduction is non-deterministic). Summarizing, Theorem 5 follows from the following lemma.

Lemma 11 *The transformations* (i) – (vi) *allow one to transform any instance of the factorized* CES *into the canonical form.*

Proof: Let T_x be a table representing a simplified instance of the factorized CES. The first step is to apply the transformation (i) as long as it is possible. To describe operators Z suitable for the transformation (i) it is convenient to use a language of C^*-algebras.

Definition 4 *A column algebra $\mathcal{A}_j \subseteq \mathbf{L}(\mathcal{H}_j)$ of a column j is the C^*-algebra generated by the operators $H_{a,j}$ for all regular rows a.*

Let $Z(\mathcal{A}_j) \subseteq \mathcal{A}_j$ be a center of the column algebra $\mathcal{A}_j$. By definition, any operator $Z \in Z(\mathcal{A}_j)$ commutes with all $H_{a,j}$ for regular a. On the other hand, Z commutes with all $H_{b,j}$ for singular b, see Lemma 10. Thus Arthur can use *any* operator $Z \in Z(\mathcal{A}_j)$ to implement the transformation (i). We would like to choose Z such that after the transformation (i) the column algebra of the column j would have a trivial center. Making use of Fact 2 from Section 5 one can identify a direct sum decompositions $\mathcal{H}_j = \bigoplus_\alpha \mathcal{H}_j^{(\alpha)}$ such that $\mathcal{A}_j = \bigoplus_\alpha \mathcal{A}_j^{(\alpha)}$, where the algebra $\mathcal{A}_j^{(\alpha)} \subseteq \mathbf{L}(\mathcal{H}_j^{(\alpha)})$ has a trivial center. Let $Z^{(\alpha)} \in Z(\mathcal{A}_j)$ be a projector onto the subspace $\mathcal{H}_j^{(\alpha)}$. Obviously, the common eigenspace $\mathcal{L}_x$ is preserved by all operators $Z^{(\alpha)}[j]$. Assuming that $\mathcal{L}_x \ne 0$, there must exist a vector $|\psi\rangle \in \mathcal{L}_x$ such that $Z^{(\alpha)}|\psi\rangle = |\psi\rangle$ for some α. Let us apply transformation (i) with $Z = Z^{(\alpha)}$ and $\omega = 1$ for all columns j of the table (the information about all α's is contained in Merlin's message). The column algebra of the column j for the transformed problem is obviously $\mathcal{A}_j^{(\alpha)}$. Now we can assume that all column algebras $\mathcal{A}_j$ have a trivial center.

Then according to Fact 1 from Section 5, the spaces $\mathcal{H}_j$ have a tensor product structure

$$\mathcal{H}_j = \mathcal{H}_j' \otimes \mathcal{H}_j'', \tag{36}$$

such that the column algebra $\mathcal{A}_j$ acts on the factor $\mathcal{H}_j'$ only:

$$\mathcal{A}_j = \mathbf{L}(\mathcal{H}_j') \otimes I.$$

Take some singular row b. The operator $H_{b,j}$ commutes with all elements of $\mathcal{A}_j$, see Lemma 10. It means that $H_{b,j}$ acts only on the factor $\mathcal{H}_j''$:

$$H_{b,j} = I \otimes H_{b,j}'' \quad \text{whenever } \lambda_b = 0,$$

for some operator $H_{b,j}'' \in \mathbf{L}(\mathcal{H}_j'')$. Since $H_{b,j}$ is a projector, the same does $H_{b,j}''$. Summarizing, the whole space $\mathcal{H}$ has a tensor product structure

$$\mathcal{H} = \mathcal{H}' \otimes \mathcal{H}'', \quad \mathcal{H}' = \bigotimes_{j=1}^{n} \mathcal{H}_j', \quad \mathcal{H}'' = \bigotimes_{j=1}^{n} \mathcal{H}_j'',$$

such that all regular rows act only on $\mathcal{H}'$ while all singular rows act only on $\mathcal{H}''$. Applying poly $(n+r)$ transformations (ii), (iii), and (vi) we can split the original instance x into two independent instances: x' (regular rows) and x'' (singular rows), such that $\mathcal{L}_x = \mathcal{L}_{x'} \otimes \mathcal{L}_{x''}$. It remains to prove that x' is equivalent to non-triviality check for some stabilizer quantum code.

Since we have already known that all singular rows can be isolated, let us assume that all rows of the table T_x are regular. Thus all operators $H_{a,j}$ are non-degenerate and all column algebras $\mathcal{A}_j$ have a trivial center. Applying, if necessary, the transformation (iii) we can get rid of 'free' factors $\mathcal{H}_j''$ in (36), so we can also assume that

$$\mathcal{A}_j = \mathbf{L}(\mathcal{H}_j).$$

For any column j the operators $H_{a,j}$ either commute or anticommute with each other. It follows that the operator $H_{a,j}^2$ belongs to the center of $\mathcal{A}_j$. Thus $H_{a,j}^2 \sim I$. Applying, if necessary, the transformation (v) we can make $H_{a,j}^2 = I$ for all a and j. Note that $\lambda_a = \pm 1$ for all a after this transformation, otherwise $\mathcal{L}_x = 0$ by obvious reasons. A connection with stabilizer codes is established by the following lemma (we shall prove it later):

Lemma 12 *Let $\mathcal{S}$ be a Hilbert space, $G_1, \ldots, G_r \in \mathbf{L}(\mathcal{S})$ be Hermitian operators such that*

$$G_a^2 = I, \quad G_a G_b = \pm G_b G_a \quad \textit{for all } a, b,$$

and such that the algebra generated by $G_1, \ldots, G_r$ coincides with $\mathbf{L}(\mathcal{S})$. Then there exists an integer m, a tensor product structure $\mathcal{S} = (\mathsf{C}^2)^{\otimes m}$ and a unitary operator $U \in \mathbf{L}(\mathcal{S})$ such that $UG_aU^\dagger$ is a tensor product of the Pauli operators and the identity (up to a sign) for all a.

Take $\mathcal{S} = \mathcal{H}_j$ and $G_a = H_{a,j}$ for some column j. Let $U \in \mathbf{L}(\mathcal{H}_j)$ be a unitary operator whose existence is guaranteed by Lemma 12. Applying the transformations (iv) with the operator U followed by the transformation (ii) to the j-th column we split it into m columns. Each of new columns represents a qubit. The entries of all new columns are either the Pauli operators or the identity. Performing this transformation for all columns independently, we transform the original instance of the factorized CES to the factorized CES with all check operators being tensor products of the identity and the Pauli operators. The total number of transformations (i) – (vi) that we made is poly $(n + r)$.

□

Proof of Lemma 12: The family $G_1, \ldots, G_r$ contains at least one anticommuting pair $G_aG_b = -G_bG_a$, since otherwise the algebra generated by G_a's has a non-trivial center. Without loss of generality, $G_1G_2 = -G_2G_1$. The operator G_1 has only eigenvalues ± 1 and G_2 swaps the subspaces corresponding to the eigenvalue $+1$ and -1. Thus both subspaces have the same dimension and we can introduce a tensor product structure $\mathcal{S} = \mathsf{C}^2 \otimes \mathcal{S}'$ such that

$$UG_1U^\dagger = \sigma_z \otimes I, \quad UG_2U^\dagger = \sigma_x \otimes I,$$

for some unitary operator $U \in \mathbf{L}(\mathcal{S})$. Using the fact that all other G_a's either commute or anticommute with G_1 and G_2 one can easily show that each G_a also has a product form:

$$UG_aU^\dagger = \tilde{G}_a \otimes G'_a, \quad \tilde{G}_a \in \{I, \sigma_x, \sigma_y, \sigma_z\}, \quad G'_a \in \mathbf{L}(\mathcal{S}').$$

Obviously, the family of operators $G'_1, \ldots, G'_r$ satisfies

$$(G'_a)^\dagger = G'_a, \quad (G'_a)^2 = I, \quad G'_aG'_b = \pm G'_bG'_a. \tag{37}$$

Denote $\mathcal{A} \subseteq \mathbf{L}(\mathcal{S}')$ the C^*-algebra generated by the operators $G'_1, \ldots, G'_r$. It has a trivial center. Indeed, if $Z \in \mathcal{A}$ is a non-trivial central element then $I \otimes Z$ is a non-trivial central element of $\mathbf{L}(\mathcal{S})$, which is impossible. Applying Fact 1 from Section 5 to the pair $(\mathcal{S}', \mathcal{A})$, we conclude that there exists a tensor product structure

$$\mathcal{S}' = \mathcal{S}'' \otimes \mathcal{S}''', \quad \mathcal{A} = \mathbf{L}(\mathcal{S}'') \otimes I.$$

But the factor $\mathcal{S}'''$ is acted on by neither of G_a's and thus $\mathcal{S}''' = \mathsf{C}$. We have proved that

$$\mathcal{A} = \mathbf{L}(\mathcal{S}'). \tag{38}$$

Taking into account (37) and (38) we can apply induction with respect to $\dim \mathcal{S}$ (the base of induction corresponds to $\mathcal{S} = \mathsf{C}$).

□

We conclude this section by proving Corollaries 2 and 3. Obviously, if $\lambda_a \neq 0$ for all a then all rows of the table T_x are regular and thus the factorized CES can be non-deterministically reduced to non-triviality check for an additive quantum code. Suppose now that $H_a H_b \neq 0$ for all a and b. It means that all rows of the table (both regular and singular) commute in a regular way. Thus the factorized projectors CES which appears in our reduction has the following special property: for any column j all projectors $H_{a,j}$ pairwise commute. Therefore the space $\mathcal{H}_j$ has a basis in which all projectors $H_{a,j}$ are diagonal. So the problem becomes classical and belongs to NP by obvious reasons.

7 The factorized projectors common eigenspace problem for qubits

In this section we prove that the factorized projectors CES for qubits ($d = 2$) belongs to NP. Let us start from a general note that applies to an arbitrary d. Consider an instance $x = (H_1, \ldots, H_r) = \{H_{a,j}\}$ of the factorized projectors CES and the common eigenspace

$$\mathcal{L}_x = \{|\psi\rangle \in \mathcal{H} \, : \, H_a|\psi\rangle = 0 \quad \text{for all} \quad a = 1, \ldots, r\}.$$

If we do not care about computational complexity, the dimension of $\mathcal{L}_x$ can be calculated using the following simple formula:

$$\begin{aligned} \dim \mathcal{L}_x \quad &= \quad \mathrm{Rk}(I) - \sum_a \mathrm{Rk}(H_a) + \sum_{a<b} \mathrm{Rk}(H_a H_b) - \sum_{a<b<c} \mathrm{Rk}(H_a H_b H_c) \\ &\quad + \cdots + (-1)^r \, \mathrm{Rk}(\prod_{a=1}^{r} H_a), \end{aligned} \tag{39}$$

where $\mathrm{Rk}(A) \equiv \dim \mathrm{Im}\, A$ is a rank of the operator A. All summation here are carried out in the range $[1, r]$. Formula (39) is analogous to exclusion-inclusion formula for cardinality of a union of sets. We can apply it since all projectors H_a are diagonalizable over the same basis and each projector can be identified with the set of basis vectors which belong to $\mathrm{Im}\, H_a$.

Let $\Omega \subseteq \{1, \ldots, r\}$ be an arbitrary subset of check operators. Denote

$$r(\Omega) = \mathrm{Rk}(\prod_{a\in\Omega} H_a)\, . \tag{40}$$

Formula (39) has the following important consequence. Let $x = \{H_{a,j}\}$ and $x' = \{H'_{a,j}\}$ be two instances of the factorized projectors CES with the same n and r. If for any subset of check operators Ω the quantities $r(\Omega)$ for the instances x and x' coincide then both instances have the same answer. So we can try to simplify the original instance x by modifying the projectors $H_{a,j}$ in such a way that all quantities $r(\Omega)$ are preserved. Although this approach seems to fail in a general case (see a discussion at the end of this section), it works perfectly for qubits.

In a case of qubits we have $\mathcal{H}_j = \mathsf{C}^2$ for all j and $\mathcal{H} = (\mathsf{C}^2)^{\otimes n}$. Each operator $H_{a,j} \in \mathbf{L}(\mathsf{C}^2)$ is either the identity operator or a projector of rank one. Let us fix the number of qubits n and the number of check operators r. Recall, that the input $x = \{H_{a,j}\}$ is regarded as a table, such that the columns correspond to the qubits and the rows correspond to the check operators. We start from introducing an appropriate terminology.

Definition 5 A table $x = \{H_{a,j}\}$ is called *commutative* if $[H_a, H_b] = 0$ for all a and b.

Definition 6 A table $x' = \{H'_{a,j}\}$ is called *consistent with* a table $x = \{H_{a,j}\}$ if for any column j one has

- $\mathrm{Rk}(H_{a,j}) = \mathrm{Rk}(H'_{a,j})$ for all a.
- $H_{a,j} = H_{b,j} \;\Rightarrow\; H'_{a,j} = H'_{b,j}$.
- $H_{a,j}H_{b,j} = 0 \;\Rightarrow\; H'_{a,j}H'_{b,j} = 0$.

Two following lemmas show that we can substitute the original table x by any table x' consistent with x without changing the answer of the problem.

Lemma 13 *Let x be a commutative table. If a table x' is consistent with x then x' is also a commutative table.*

Proof: Let $x = \{H_{a,j}\}$, $x' = \{H'_{a,j}\}$, $H_a = \bigotimes_{j=1}^n H_{a,j}$, and $H'_a = \bigotimes_{j=1}^n H'_{a,j}$.

Suppose that H_a and H_b commute in a singular way i.e., $H_aH_b = 0$. It means that $H_{a,j}H_{b,j} = 0$ for some j. Since x' is consistent with x, we have $H'_{a,j}H'_{b,j} = 0$. Thus H'_a and H'_b also commute (in a singular way).

Suppose now that H_a and H_b commute in a regular way, that is $H_aH_b \neq 0$, $H_aH_b = H_bH_a$. It follows from Lemma 9 that $H_{a,j}H_{b,j} = \pm H_{b,j}H_{a,j}$ for all j. Since both $H_{a,j}$ and $H_{b,j}$ are projectors, they can not anticommute, so we conclude that $[H_{a,j}, H_{b,j}] = 0$ for all j. Besides, we know that $H_{a,j}H_{b,j} \neq 0$. It is easy to see that both conditions can be met by one-qubit projectors only if for any fixed j at least one of the following statements is true:
(i) At least one of $H_{a,j}$ and $H_{b,j}$ is the identity operator.
(ii) $H_{a,j} = H_{b,j}$.
Now we can make use of the fact that x' is consistent with x. If the statement (i) is true, one has $\mathrm{Rk}(H_{a,j}) = 2$ or (and) $\mathrm{Rk}(H_{b,j}) = 2$. It follows that $\mathrm{Rk}(H'_{a,j}) = 2$ or (and) $\mathrm{Rk}(H'_{b,j}) = 2$, that is at least one of the projectors $H'_{a,j}$ and $H'_{b,j}$ is the identity. If the statement (ii) is true, one has $H'_{a,j} = H'_{b,j}$. In both cases $H'_{a,j}H'_{b,j} \neq 0$ and $[H'_{a,j}, H'_{b,j}] = 0$. Since it holds for all j, we conclude that H'_a and H'_b commute (in a regular way).

□

Lemma 14 *Let x be a commutative table. If a table x' is consistent with x then all quantities $r(\Omega)$ for the tables x and x' coincide.*

Proof: Let $x = \{H_{a,j}\}$, $x' = \{H'_{a,j}\}$, $H_a = \bigotimes_{j=1}^n H_{a,j}$, and $H'_a = \bigotimes_{j=1}^n H'_{a,j}$. According to Lemma 13 the table x' is commutative, so for any Ω we can define a quantity

$$r'(\Omega) = \mathrm{Rk}(\prod_{a\in\Omega} H'_a)\,. \tag{41}$$

We should prove that $r(\Omega) = r'(\Omega)$ for all $\Omega \subseteq \{1, \ldots, r\}$. There are two possibilities:
(i) $r(\Omega) > 0$. It means that $H_aH_b \neq 0$ for all $a, b \in \Omega$. Thus all operators H_a, $a \in \Omega$ commute in a regular way and $[H_{a,j}, H_{b,j}] = 0$ for all $a, b \in \Omega$ and for all j. In this situation the formula (40) for $r(\Omega)$ factorizes:

$$r(\Omega) = \prod_{j=1}^n r_j(\Omega), \quad r_j(\Omega) = \mathrm{Rk}(\prod_{a\in\Omega} H_{a,j})\,. \tag{42}$$

Let us consider some particular j. The family of projectors $\{H_{a,j}\}_{a\in\Omega}$ is diagonalizable over the same basis. Denote corresponding basis vectors as $|\psi_0\rangle$ and $|\psi_1\rangle$, $\langle\psi_\alpha|\psi_\beta\rangle = \delta_{\alpha,\beta}$. Each member of the family $\{H_{a,j}\}_{a\in\Omega}$ is one of the following projectors: I, $|\psi_0\rangle\langle\psi_0|$, and $|\psi_1\rangle\langle\psi_1|$. The requirement $r_j(\Omega) > 0$ implies that the projectors $|\psi_0\rangle\langle\psi_0|$ and $|\psi_1\rangle\langle\psi_1|$ do not enter into this family simultaneously. Thus there exist integers k_1 and k_2, $k_1 + k_2 = |\Omega|$, such that the family $\{H_{a,j}\}_{a\in\Omega}$ consists of k_2 identity operators I and k_1 projectors of rank one $|\psi\rangle\langle\psi|$ (with $|\psi\rangle = |\psi_0\rangle$ or $|\psi\rangle = |\psi_1\rangle$). Now let us look at the family $\{H'_{a,j}\}_{a\in\Omega}$. Since x' is consistent with x, this family also consists of k_2 identity operators I and k_1 projectors of rank one $|\varphi\rangle\langle\varphi|$ for some $|\varphi\rangle \in \mathsf{C}^2$. Therefore $[H'_{a,j}, H'_{b,j}] = 0$ for all $a, b \in \Omega$ and

$$r'_j(\Omega) = \mathrm{Rk}(\prod_{a\in\Omega} H'_{a,j}) = r_j(\Omega).$$

Also it means that the quantity $r'(\Omega)$ factorizes, $r'(\Omega) = \prod_{j=1}^{n} r'_j(\Omega)$, and thus $r'(\Omega) = r(\Omega)$.
(ii) $r(\Omega) = 0$. It means that $\prod_{a\in\Omega} H_a = 0$. Suppose first that $H_a H_b = 0$ for some $a, b \in \Omega$. Since x' is consistent with x it implies that $H'_a H'_b = 0$ (see the first part of the proof of Lemma 13) and so that $r'(\Omega) = 0$. Now suppose that $H_a H_b \neq 0$ for all $a, b \in \Omega$. By definition, it means that all check operators H_a, $a \in \Omega$ commute in a regular way, i.e. $[H_{a,j}, H_{b,j}] = 0$ for all $a, b \in \Omega$ and for all j. In particular, the family $\{H_{a,j}\}_{a\in\Omega}$ is diagonalizable over the same basis. In this situation we can use a decomposition (42). We know that $r_j(\Omega) = 0$ for some j. But it happens iff the family $\{H_{a,j}\}_{a\in\Omega}$ contains a pair of rank one projectors corresponding to mutually orthogonal states, i.e. $H_{a,j} H_{b,j} = 0$ for some $a, b \in \Omega$. But it implies $H_a H_b = 0$ which contradicts our assumption.

□

What is the most simple form of a table x' consistent with the original table x? We will show that for any table x there exists a table $x' = \{H'_{a,j}\}$ consistent with x such that $H'_{a,j} \in \{I, |0\rangle\langle 0|, |1\rangle\langle 1|\}$ for all a and j. Here $|0\rangle, |1\rangle \in \mathsf{C}^2$ is some fixed orthonormal basis of C^2 (computational basis). This statement is true even for tables that are not commutative. Moreover, given the table x, one can find the table x' using an efficient algorithm.

All check operators H'_a for the table x' are diagonal in the computational basis of $(\mathsf{C}^2)^{\otimes n}$, therefore Merlin's proof that x' is a positive instance might be a binary string $(x_1, x_2, \ldots, x_n)$ such that $H'_a|x_1\rangle\otimes|x_2\rangle\otimes\cdots\otimes|x_n\rangle = 0$ for all a (in fact, one can regard H'_a as classical clauses of a CNF formula). Lemma 14 guarantees that x' is equivalent to x. Thus existence of a table x' with the specified properties implies that the factorized projectors CES for qubits belongs to NP.

It remains to prove the following lemma.

Lemma 15 *For any table x there exists a table $x' = \{H'_{a,j}\}$ consistent with x such that $H'_{a,j} \in \{I, |0\rangle\langle 0|, |1\rangle\langle 1|\}$ for all a and j. The table x' can be found by an algorithm running in a time $O(r^2 n)$.*

Proof: Let $x = \{H_{a,j}\}$. A transformation from x to the desired table x' is defined independently for each column, so let us focus on some particular column, say $j = 1$. At first, we define an *orthogonality graph* $G = (V, E)$. A vertex $v \in V$ is a set of rows which contain the same projector. In other words, we introduce an equivalence relation on the set of rows: $a \sim b \;\Leftrightarrow\; H_{a,1} = H_{b,1}$ and define a vertex $v \in V$ as an equivalence class of rows. Thus, by definition, each vertex $v \in V$ carries a projector $H(v) \in \mathbf{L}(\mathsf{C}^2)$. A pair of vertices

$u, v \in V$ is connected by an edge iff the projectors corresponding to u and v are orthogonal: $(u,v) \in E \Leftrightarrow H(u)H(v) = 0$.

Consider as an example the following table ($r = 100$): $H_{1,1} = I$, $H_{2,1} = H_{3,1} = 1/2(I+\sigma_z)$, $H_{4,1} = 1/2(I-\sigma_z)$, $H_{5,1} = 1/2(I+\sigma_x)$, $H_{6,1} = 1/2(I-\sigma_x)$, $H_{7,1} = \cdots = H_{100,1} = 1/2(I+\sigma_y)$. Then an orthogonality graph consists of six vertices, $V = \{1,2,3,4,5,6\}$, with $H(1) = I$, $H(2) = 1/2(I+\sigma_z)$, $H(3) = 1/2(I-\sigma_z)$, $H(4) = 1/2(I+\sigma_x)$, $H(5) = 1/2(I-\sigma_x)$, and $H(6) = 1/2(I+\sigma_y)$. The set of edges is $E = \{(2,3),(4,5)\}$.

If one represents G by its adjacency matrix, it can be found in $O(r^2)$ computational steps.

It is a special property of qubits that any orthogonality graph always splits to several disconnected edges representing pairs of orthogonal projectors and several disconnected vertices representing unpaired projectors of rank one and the identity operator.

Suppose we perform a transformation

$$H(v) \to H'(v), \quad v \in V, \tag{43}$$

for some projectors $H'(v) \in \mathbf{L}(\mathsf{C}^2)$ which satisfy

$$\mathrm{Rk}(H(v)) = \mathrm{Rk}(H'(v)) \quad \text{for all } v \in V; \quad H'(u)H'(v) = 0 \quad \text{for all } (u,v) \in E. \tag{44}$$

As each vertex of the graph represents a group of cells of the table, the transformation (43) can be also regarded as a transformation of the tables $x \to x'$. Note that the table x' is consistent with the table x, since the restrictions (44) are just rephrasing of Definition 6.

To construct the table x' with the desired properties we proceed as follows. For each disconnected edge $(u,v) \in E$ define the transformation (43) as $H'(u) = |0\rangle\langle 0|$, $H'(v) = |1\rangle\langle 1|$ (it does not matter, how exactly 0 and 1 are assigned to endpoints of the edge — one can use an arbitrary map from the Bloch sphere to $\{|0\rangle, |1\rangle\}$ such that orthogonal states are mapped to the different states). For any disconnected vertex $v \in V$, we define $H'(v) = I$ if $H(v) = I$ and $H'(v) = |0\rangle\langle 0|$ if $\mathrm{Rk}(H(v)) = 1$. Overall, this algorithm requires $O(r^2 n)$ computational steps.

□

We conclude this section by several remarks concerning the factorized projectors CES problem with $d > 2$. For simplicity, let us put an additional constraint, namely that each projector $H_{a,j}$ is either the identity operators or a projector of rank one (a projector on a pure state). Definitions 5 and 6 are still reasonable in this setting. Moreover, it is easy to check that Lemmas 13 and 14 are still valid (the proofs given above can be repeated almost literally). A natural generalization of Lemma 15 might be the following:
For any table x there exists a table $x' = \{H'_{a,j}\}$ consistent with x such that for all a and j $H'_{a,j} \in \{I, |1\rangle\langle 1|, \ldots, |d\rangle\langle d|\}$.
Here some fixed orthonormal basis $|1\rangle, \ldots, |d\rangle \in \mathsf{C}^d$ is chosen. Unfortunately, this statement is wrong even for $d = 3$. Counterexamples may be obtained by constructions used in the proof of the Kochen-Specker theorem [19]. According to this theorem there exist families of projectors $P_1, \ldots, P_r \in \mathbf{L}(\mathsf{C}^d)$ $(d \geq 3)$ which do not admit an assignment

$$P_a \to \varepsilon_a \in \{0,1\}, \quad a = 1, \ldots, r, \tag{45}$$

such that

$$\sum_{a \in \Omega} \varepsilon_a = 1 \quad \text{whenever} \quad \sum_{a \in \Omega} P_a = I. \tag{46}$$

Here $\Omega \subseteq \{1, \ldots, r\}$ may be an arbitrary subset. Peres [20] suggested an explicit construction of such family for $d = 3$ and $r = 33$. This family consists of the projectors of rank one, i.e. $P_a = |\psi_a\rangle\langle\psi_a|$, $|\psi_a\rangle \in \mathsf{C}^3$, $a = 1, \ldots, 33$.

Suppose a table $x = \{H_{a,j}\}$ consists of 33 rows and the first column accommodates the family of projectors suggested by Peres: $H_{a,1} = |\psi_a\rangle\langle\psi_a|$, $a = 1, \ldots, 33$. Let $x' = \{H'_{a,j}\}$ be a table whose existence is promised by the generalized Lemma 15. Since x' is consistent with x, one has $\mathrm{Rk}(H'_{a,1}) = \mathrm{Rk}(H_{a,1}) = 1$, so neither of the projectors $H'_{a,1}$, $a = 1, \ldots, 33$, is the identity. Then the only possibility (if the lemma is true) is that $H'_{a,1} \in \{|1\rangle\langle 1|, |2\rangle\langle 2|, |3\rangle\langle 3|\}$. A consistency property implies also that

$$\sum_{a\in\Omega} H_{a,1} = I \quad \Rightarrow \quad \sum_{a\in\Omega} H'_{a,1} = I. \tag{47}$$

Indeed, the equality on the lefthand side is possible iff $|\Omega| = 3$ and all projectors $\{H_{a,1}\}_{a\in\Omega}$ are pairwise orthogonal. Then the projectors $\{H'_{a,1}\}_{a\in\Omega}$ are also pairwise orthogonal and we get the equality on the righthand side. The family of projectors $\{H'_{a,1}\}$ obviously admits an assignment (45,46). Indeed, we can put

$$\varepsilon_a = \begin{cases} 1 & \text{if} \quad H'_{a,1} = |3\rangle\langle 3|, \\ 0 & \text{if} \quad H'_{a,1} = |1\rangle\langle 1| \text{ or } |2\rangle\langle 2|. \end{cases}$$

But the property (47) implies that the assignment $H_{a,1} \to \varepsilon_a$, $a = 1, \ldots, 33$ also satisfies the requirements (46). It is impossible. Therefore the generalization of Lemma 15 given above is wrong.

In fact, the proof of Lemma 15 needs a regular d-coloring of a graph which admits d-dimensional orthogonal representation. As we have seen, this is not always possible. It might happen however that all 'pathological' (which violate Lemma 15) *commutative* tables lead to simple instances of factorized projectors CES. Indeed, a difficult instance must contain pairs of rows commuting in a singular way and pairs commuting in a regular way. The number of pairs of each type must be sufficiently large. For example, if all rows commute in a regular way, the problem belongs to NP according to Corollary 3. If all rows commute in a singular way, we can easy compute $\dim \mathcal{L}_0$ using the exclusion-inclusion formula (39). The number of 'pathological' columns in the table also must be sufficiently large. To construct difficult instances we must meet all these requirements which seems to be hard.

Acknowledgements

We would like to thank P. Wocjan for interesting discussions which motivated this line of research. We thank A. Kitaev and J. Preskill for helpful comments and suggestions. We are grateful to the referee of the paper for numerous remarks and corrections. The main part of this work was done when M.V. was visiting Institute for Quantum Information, Caltech. The work was supported by RFBR grant 02-01-00547, and by the National Science Foundation under Grant No. EIA-0086038.

References

1. S. Aaronson, *The complexity zoo*, http://www.complexityzoo.com/

2. A. Kitaev, A. Shen, and M. Vyalyi (2002), *Classical and quantum computation*, AMS.
3. D. Aharonov and T. Naveh (2002), *Quantum NP — a survey*, quant-ph/0210077.
4. J. Watrous (2000), *Succinct quantum proofs for properties of finite groups*, Proceedings of IEEE FOCS, p. 537.
5. J. Kempe and O. Regev (2003), *3-Local Hamiltonian is QMA-complete*, Quantum Information and Computation, Vol. 3(3), p. 258-64.
6. J. Kempe, A. Kitaev, and O. Regev (2004), *The Complexity of the Local Hamiltonian Problem*, quant-ph/0406180.
7. D. Janzing, P. Wocjan, and Th. Beth (2003), *Identity check is QMA-complete*, quant-ph/0305050.
8. P. Wocjan and Th. Beth (2003), *The 2-local Hamiltonian problem encompasses NP*, International Journal of Quantum Information, Vol. 1(3), p. 349-357.
9. H. Briegel and R. Raussendorf, *Persistent entanglement in arrays of interacting particles*, quant-ph/0004051.
10. P. Hayden, R. Jozsa, D. Petz, A. Winter (2004), *Structure of states which satisfy strong subadditivity of quantum entropy with equality*, Commun. Math. Phys., 246(2), p. 359.
11. B. Terhal and D. DiVincenzo (2004), *Adaptive quantum computation, constant depth quantum circuits and Arthur-Merlin games*, Quantum Information and Computation, Vol. 4(2), p. 122-133.
12. A. Calderbank, E. Rains, P. Shor, and N. Sloane (1996), *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. 78, p. 405; quant-ph/9605005.
13. A. Aho, J. Hopcroft, and J. Ullman (1974), *The Design and Analysis of Computer Algorithms*, Addison-Wesley Reading, Massachusetts.
14. D. Bini and V.Y. Pan (1994), *Polynomial and matrix computation*, Vol. 1. Birkhäuser, Boston, Cambridge, MA.
15. M. Takesaki (1979), *Theory of operator algebras I*, Springer-Verlag, New York-Heidelberg-Berlin.
16. E. Knill, R. Laflamme, and L. Viola (2000), *Theory of Quantum Error Correction for General Noise*, Phys. Rev. Lett. 84, p. 2525.
17. M. Nielsen and I. Chuang (2000), *Quantum Computation and Quantum Information*, Cambridge University Press.
18. This Lemma and its proof were suggested by the referee of the paper.
19. S. Kochen and E. P. Specker (1967), *The problem of hidden variables in quantum mechanics*, J. Math. Mech. 17, p. 59.
20. A. Peres (1991), *Two simple proofs of the Kochen-Specker theorem*, Journal of Physics A24, p. L175.