Combinatorial NLTS From the Overlap Gap Property

Eric R. Anschuetz[1], David Gamarnik[2], and Bobak Kiani[3]

[1]MIT Center for Theoretical Physics, Cambridge, MA 02139, USA
[2]Sloan School of Management, MIT, Cambridge, MA 02139, USA
[3]Department of Electrical Engineering and Computer Science, MIT, Cambridge, MA 02139, USA

arXiv:2304.00643v4 [quant-ph] 11 Nov 2024

In an important recent development, Anshu, Breuckmann, and Nirkhe [ABN23] resolved positively the so-called No Low-Energy Trivial State (NLTS) conjecture by Freedman and Hastings [FH14]. The conjecture postulated the existence of linear-size local Hamiltonians on n qubit systems for which no near-ground state can be prepared by a shallow (sublogarithmic depth) circuit. The construction in [ABN23] is based on recently developed good quantum codes. Earlier results in this direction included the constructions of the so-called Combinatorial NLTS—a weaker version of NLTS—where a state is defined to have low energy if it violates at most a vanishing fraction of the Hamiltonian terms [EH17],[AB22]. These constructions were also based on codes.

In this paper we provide a "non-code" construction of a class of Hamiltonians satisfying the Combinatorial NLTS. The construction is inspired by one in [AB22], but our proof uses the complex solution space geometry of random K-SAT instead of properties of codes. Specifically, it is known that above a certain clause-to-variables density the set of satisfying assignments of random K-SAT exhibits the overlap gap property, which implies that it can be partitioned into exponentially many clusters each constituting at most an exponentially small fraction of the total set of satisfying solutions [ACORT11]. We establish a certain robust version of this clustering property for the space of near-satisfying assignments and show that for our constructed Hamiltonians every combinatorial near-ground state induces a near-uniform distribution supported by this set. Standard arguments then are used to show that such distributions cannot be prepared by quantum circuits with depth $o(\log n)$.

Unfortunately, our Hamiltonian is only local on average due to fluctuations in the numbers of clauses in which variables are involved. On the positive side, since the clustering property is exhibited by many random structures—including proper coloring, maximum cut, and the hardcore model—we anticipate that our approach is extendable to these models as well, including certain classical models of bounded degree. We sketch such an extension here for the p-spin Ising model on a sparse random regular graph as a non-code example where exactly local Combinatorial NLTS may be achieved.

1 Introduction

A remarkable feature exhibited by some quantum systems, and not found in classical models, is the potential complexity of the state representation. Any classical state on an n-bit system is just an n-bit string and thus requires at most n bits to be represented. Quantum systems on n qubits, on the other hand, are described in general by 2^n associated complex-valued amplitudes and thus in principle lead to a representation complexity which is exponential in n. This should not necessarily be the case, however, for "physical" quantum states such as those arising as ground states of succinctly described Hamiltonians. The so-called No Low-Energy Trivial States conjecture by Freedman and Hastings [FH14] posits exactly this question: does there exist a simple-to-describe Hamiltonian for which any associated near-ground state is too complex to describe? As a proxy for descriptional simplicity they propose to focus on Hamiltonians which are sums of linearly many local Hamiltonians. Specifically, these are Hamiltonians H acting on n qubits, which can be written as $H = \sum_i H_i$, where the number of terms H_i is linear in n, each H_i has bounded by $O(1)$ operator norm, and is local, in the sense that each H_i acts on

Eric R. Anschuetz: eans@caltech.edu
David Gamarnik: gamarnik@mit.edu
Bobak Kiani: bkiani@g.harvard.edu

$O(1)$-many qubits. As a proxy for the complexity measure of state representation, we say that a state ρ is complex if it cannot be prepared by a sublogarithmic-in-n depth quantum circuit. Namely, ρ is complex if there does not exist a logarithmic-depth circuit such that the unitary U associated with this circuit satisfies $\rho = U|0\rangle\langle 0|U^\dagger$. The NLTS conjecture then posits the existence of linear-size local Hamiltonians H such that every state ρ which is a near-ground state of H (that is, a near minimizer of $\min \mathrm{Tr}(H\rho)$) is complex in the sense above.

The existence of such Hamiltonians is a necessary consequence of the validity of the quantum PCP conjecture: if a near-ground state were of low complexity, a classical representation of it could be obtained in polynomial time classically. This would then imply that the complexity class QMA satisfies QMA = NP, which is widely believed not to be the case. Thus, if the quantum PCP conjecture is valid, NLTS must hold. Validating the NLTS conjecture was then proposed as a reasonable step towards the ultimate goal of proving the quantum PCP theorem [AAV13].

A series of results [EH17, Eld21, BKKT20, AN22] gave strong evidence in favor of the conjecture, with the strongest evidence (before its eventual resolution) given by Anshu and Breuckmann [AB22]. There, the validity of the so-called *combinatorial* version of NLTS—the subject of this paper—was established. Given a linear-size local Hamiltonian $H = \sum_i H_i$ and given $\epsilon > 0$, a state ρ is an ϵ-near ground state of H in the combinatorial sense if it is a ground state for at least a $(1-\epsilon)$ fraction of Hamiltonian terms H_i. Namely, using constraint satisfaction terminology, ρ has to satisfy all but an ϵ-fraction of constraints H_i. Validity of the NLTS conjecture trivially implies its combinatorial version but not vice-versa.

A complete positive resolution of the original NLTS conjecture was finally obtained in a remarkable paper by Anshu, Breuckmann, and Nirkhe [ABN23]. Their construction as well as all of the previous constructions (to the best of our knowledge) are based on codes. Specifically, classical or quantum codes are used to design the Hamiltonians H_i. Near-code words are then shown to exhibit sufficiently strong entanglement which obstructs their low complexity representation. The construction in [ABN23] leverages a recently constructed quantum Tanner code [LZ22] to construct a Hamiltonian which exhibits the following clustering property: near-ground states induce a probability measure on a basis which is supported on a disjoint union of exponentially many clusters separated by a linear distance. Most of the time this was shown directly for the computational basis, as in [AB22] and [EH17]. On the other hand, the construction in [ABN23] is shown to exhibit this clustering in the computational and/or Hadamard bases.

Remarkably, such a clustering property is ubiquitous in a completely different research direction devoted to studying random constraint satisfaction problems and closely related models known as diluted spin glasses. Examples of the former include random instances of the K-SAT problem [ACORT11], the problem of finding a proper coloring of a graph [ACO08],[MMZ05], the largest independent set problem [COE11], and the maximum cut problem on sparse random hypergraphs [CGPR19]. An example of the latter includes an Ising or Edwards–Anderson model supported on a sparse random graph [FL03]. Many of these models are known to exhibit an *overlap gap property* (OGP), which roughly speaking states that any two (classical) near-ground states are either close or far from each other in Hamming distance. The overlap gap property was then used to prove the clustering property: the set of near ground states is supported on a disjoint union of exponentially many clusters each consisting of at most an exponentially small fraction of the total set of states. Starting from [GS17] this property was then widely used to establish various algorithmic complexity lower bounds, in particular ruling out various classical algorithms for finding near-ground states. The links between the overlap gap property and algorithmic complexity are surveyed in [Gam21] and [GMZ22]. The abundance of clustering properties exhibited in these models raises the natural question of whether it is possible to use these models for constructing NLTS. Our paper provides a positive answer to this question for the case of Combinatorial NLTS. Specifically, we use the appropriately extended clustering property of the random K-SAT model toward this goal. Naturally, the diagonal Hamiltonians arising directly from the K-SAT model cannot be used for NLTS directly since low-energy states of such Hamiltonains trivially include those with small description complexity. Instead, we resort to a method similar to one used in [AB22]. Specifically, using random instances of the K-SAT model we construct a quantum Hamiltonian such that each combinatorial near-ground state of it induces a probability measure on the computational basis which is a near-uniform distribution on the space of near-satisfying assignments of the K-SAT formula. This is obtained by projecting a tensor product of cat-like states onto the set of nearly satisfying assignments of the formula. We then use a standard argument to show that such measures cannot be prepared by shallow quantum circuits. Toward this goal we utilize a certain appropriate mixture of computational and Hadamard bases on the one hand, and prove a certain "robust" version of the overlap gap and clustering property on the other hand. These constitute the main technical contributions of our paper.

Unfortunately, the Hamiltonians we construct are local only on average, in the sense that typical Hamiltonian terms act on at most $O(1)$ many qubits, while some may act on as many as $O(\log n)$ qubits. This a direct implication of the fact that while the average degree of a sparse random graph has constant degree, the largest degree grows like $O(\log n)$ w.h.p. We conjecture, however, that a similar version of the OGP also holds for certain classical models of bounded degree, with a similar quantum extension to Combinatorial NLTS as we exhibit here. This appears to require substantially more involved technical work which we do not pursue, though we give an outline of a proof in Section 5.

On a positive note, our work shows that code structures such as those that underlie all of the prior NLTS constructions are not essential for the goal of building NLTS Hamiltonians, and in fact quantum Hamiltonians exhibiting Combinatorial NLTS can be constructed from classical random Hamiltonians supported by random graphs and hypergraphs. Indeed we conjecture that constructions of Combinatorial NLTS similar to ours can be obtained from other models exhibiting the overlap gap property, including the largest independent set problem as in [GS17] and the maximum cut problem as in [CGPR19]. We further conjecture that the class of Hamiltonians we construct based on random K-SAT instances is in fact NLTS (and not just Combinatorial NLTS), but we are not able to prove this. Finally, the potential ramification of our result for validating the quantum PCP conjecture is another interesting question for further research.

The remainder of the paper is structured as follows. Random K-SAT instances and the statement of the Combinatorial NLTS are introduced in the next section. Our main result is stated in the next section as well. In Section 3 we define the overlap gap property and the implied clustering properties. In the same section we state and prove a robust version of the overlap gap and clustering property which applies to "nearly" satisfying assignments of "nearly complete" subsets of Boolean variables. This is an extension of an older result by Achlioptas, Coja-Oghlan and Ricci-Tersenghi [ACORT11] which regards assignments with no clause violations. There both the overlap gap and the clustering properties are established for $K \geq 8$. The robustness required for our purposes forces us to resort instead to large K and the details of the bounds are somewhat delicate. We complete the proof of our main result in Section 4. Finally, we end in Section 5 with a sketch of an extension of our results to models with bounded degree.

2 Model, construction, and the main result

2.1 Random K-SAT formulas

We begin by describing a random instance of the Boolean constraint satisfaction problem, specifically the K-SAT problem. A Hamiltonian is constructed from this classical constraint satisfaction problem which is different but nonetheless related to instances of problems studied in so-called quantum SAT [Bra11]. An integer K is fixed. A collection of Boolean variables $x_1, \ldots, x_n$ is fixed, each taking values in $\{0,1\}$. A K-clause C over these variables is a disjunction of the form $y_1 \vee y_2 \vee \cdots \vee y_K$, consisting of exactly K elements where each $y_j, j \in [k]$ is either one of $x_1, \ldots, x_n$ or one of the negations $\neg x_1, \ldots, \neg x_n$. For example, a $K = 4$-clause with $y_1 = x_3, y_2 = \neg x_{17}, y_3 = \neg x_6, y_4 = \neg x_2$, gives rise to the clause $(x_3 \vee \neg x_{17} \vee \neg x_6 \vee \neg x_2)$.

A formula Φ is a conjunction $\Phi \triangleq C_1 \wedge \cdots \wedge C_m$ of any collection of K-clauses $C_1, \ldots, C_m$. A solution is any assignment $x = (x_1, \ldots, x_n) \in \{0,1\}^n$. A solution x is said to satisfy a clause C if the Boolean evaluation of this clause is 1, namely, if at least one of the variables x_i appearing in this clause satisfies it. For the example 4-clause above, any solution with $x_3 = 1$ satisfies this clause, and so does any solution with $x_{17} = 0, x_6 = 0, x_2 = 0$. Notice that for each clause C there exists a unique assignment of the K variables in this clause which does not satisfy it which we denote by $v(C) \in \{0,1\}^K$. A solution x satisfies the formula Φ if it satisfies every clause in the formula.

For every clause C_j we denote by $(j,1), \ldots, (j,K)$ the indices of variables appearing in C_j for convenience. For example, if, say, $C_5 = (\neg x_4 \vee \neg x_1 \vee \neg x_9 \vee x_{12})$ and $C_8 = (x_{32} \vee x_{17} \vee \neg x_{16} \vee \neg x_{12})$, then $(5,1) = 4, (5,2) = 1, (5,3) = 9, (5,4) = 12$ and $(8,1) = 32, (8,2) = 17, (8,3) = 16, (8,4) = 12$.

We now turn to the description of a (uniform) random instance of a K-SAT problem. For a fixed K, n, m we consider the space of all $(2n)^K$ clauses (with repetition of variables within a clause allowed and the literals within a clause ordered). The random formula is generated by selecting $C_1, \ldots, C_m$ independently and uniformly at random from this space of all clauses. An instance of a random formula is denoted by $\mathbf{\Phi}(n,m)$, where the dependence on K is kept implicit. We consider a proportional setting where a ratio m/n is fixed to be a constant as n increases. A relevant regime for us will be when m/n is of the form $\alpha 2^K \log 2$ for some $\alpha \in (1/2, 1)$. In this case the set of satisfying assignments exhibits a clustering property crucial for our construction. The derivation

Symbol	Description
x_i	Boolean variable
n	Number of SAT variables
m	Number of clauses
$\Phi(n,m)$	Random SAT formula with n variables and m clauses
C_i	Clause i in random formula $\Phi(n,m)$
$C(x_i)$	Set of clauses containing variable x_i
K	Locality of clauses
N	Number of qubits ($N = Km$)
$v(C_j)$	Unique non-satisfying solution of clause C_j
$D(i)$	Subset of qubits corresponding to the variable x_i

Table 1: Description of notation used in construction of the quantum Hamiltonian (Equation (1)).

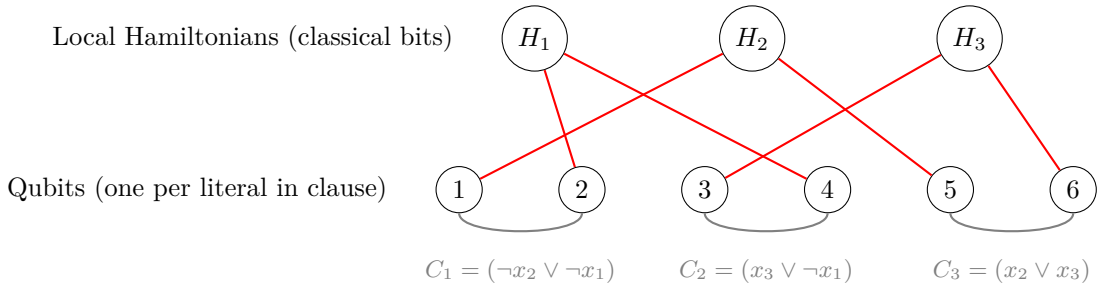

Figure 1: A visualization of an example Hamiltonian $H = H_1 + H_2 + H_3$ from (1) constructed from a classical 2-SAT formula of 3 clauses where $C_1 = (\neg x_2 \vee \neg x_1)$, $C_2 = (x_3 \vee \neg x_1)$, and $C_3 = (x_2 \vee x_3)$. Here, each term of the Hamiltonian H_i as described in (1) is 4-local as the $|\mathrm{CAT}(i)\rangle$ states are each supported on two qubits on disjoint clauses which correspond to the matrices $Q^{-1}_{C_j,\gamma}$ that are 2-local.

of this clustering property is the subject of Section 3.

Next we turn to a construction of a sparse Hamiltonian based on an instance of a K-SAT model.

2.2 Construction of a quantum Hamiltonian and the main result

We now turn to the description of a quantum Hamiltonian which will give a rise to a combinatorial NLTS construction. This construction is inspired by the one in [AB22]. We fix a realization of a random formula $\mathbf{\Phi}(n,m)$ on variables $x_1,\ldots,x_n$ and clauses $C_1,\ldots,C_m$ which we also denote by $\mathbf{\Phi}(n,m)$ for convenience. For each $j = 1,\ldots,m$ the associated variables are denoted by $x_{j,k}, k \in [K]$. That is, each $x_{j,k}$ is one of $x_1,\ldots,x_n$. We consider a quantum system on mK qubits. These qubits are denoted by $(1,1),\ldots,(1,K),(2,1),\ldots,(2,K),\ldots,(m,1),\ldots,(m,K)$, where we recall that (j,k) denotes the index of the k-th variable appearing in clause C_j. For each $i \in [n]$ we denote by $D(i)$ the subset of qubits corresponding to the variable x_i. Namely, it is the set of all qubits with indices (j,k) such that $(j,k) = i$. As an example, if the variable x_3 appears in the clause C_4 in position 2, C_7 in position 5, and C_{12} in position 1—and does not appear in any other clause—then $D(x_3) = \{(4,2),(7,5),(12,1)\}$. Note that the sets $D(i)$ are disjoint and that their union is the set of all qubits $\{(j,k), j \in [m], k \in [K]\}$. For each $i \in [n]$, we also denote the set of clauses containing variable x_i by $C(x_i) = \{C_j : i \in \{(j,1),\ldots,(j,K)\}\}$. For example, if there are three clauses: $C_1 = (\neg x_4 \vee \neg x_1 \vee \neg x_9 \vee x_7)$, $C_2 = (\neg x_5 \vee x_2 \vee \neg x_1 \vee x_3)$, and $C_3 = (\neg x_3 \vee \neg x_8 \vee x_4 \vee x_6)$, then $C(x_1) = \{C_1, C_2\}$.

For each $i \in [n]$ we denote by $|\mathrm{CAT}(i)\rangle$ the CAT state associated with qubits in $D(i)$. That is, $|\mathrm{CAT}(i)\rangle = \frac{1}{\sqrt{2}}|00\ldots0\rangle + \frac{1}{\sqrt{2}}|11\ldots1\rangle$ with qubits supported on $D(i)$. We denote by $|\mathrm{CAT}\rangle$ the tensor product of these states:

$|\mathrm{CAT}\rangle \triangleq \bigotimes_{i\in[n]} |\mathrm{CAT}(i)\rangle$.

Next, for each $j \in [m]$ we consider the projection onto the space spanned by vectors orthogonal to $|v(C_j)\rangle$, where, as we recall, $v(C_j)$ is the unique non-satisfying solution of the clause C_j. That is, we consider the operator:

$$Q_{C_j} \triangleq \sum_{v\in\{0,1\}^K, v\neq v(C_j)} |v\rangle\langle v|$$

applied to the subset $\{(j,1),\ldots,(j,K)\}$ of $N = Km$ qubits corresponding to the clause C_j, tensored with the identity operator on the remaining qubits. For any element $|z\rangle$ of the computational basis we have that $Q_{C_j}|z\rangle = |z\rangle$ if $z \in \{0,1\}^N$ encodes a satisfying solution of C_j and $Q_{C_j}|z\rangle = 0$ otherwise. Thus, indices of $|z\rangle$ can be interpreted as assigning values to the classical variables $x_1,\ldots,x_n$. Note that most $|z\rangle$ will not correspond to a globally valid assignment to $x_1,\ldots,x_n$, as any valid assignment must be consistent with the projectors onto the CAT states; states corresponding to such invalid assignments will have eigenvalue 0 due to these projectors.

The operator Q_{C_j} is not invertible due to the existence of non-satisfying solutions z. As in [AB22] we consider an approximating but invertible operator by fixing a constant $\gamma > 0$ and defining:

$$Q_{C_j,\gamma} \triangleq (1-\gamma)Q_{C_j} + \gamma I,$$

acting on the same set of K qubits again tensored with the identity operator on the remaining qubits. We also define an invertible operator

$$Q(\gamma) \triangleq \prod_{1\le j\le m} Q_{C_j,\gamma}.$$

Next, for each variable $x_i, i \in [n]$ we consider the tensor product:

$$Q_{x_i,\gamma} \triangleq \prod_{j:C_j\in C(x_i)} Q_{C_j,\gamma},$$

again tensored with the identity on the remaining qubits. Namely, we take a tensor product of operators $Q_{C_j,\gamma}$ associated with clauses C_j containing variable x_i. This is an invertible operator on the set of all N qubits; $Q^{-1}_{x_i,\gamma}$ denotes its inverse.

Finally, we consider the Hamiltonian:

$$\begin{aligned} H_i &= Q^{-1}_{x_i,\gamma}\left(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|\right)Q^{-1}_{x_i,\gamma}, \qquad i\in[n] \\ H &= \sum_{i\in[n]} H_i. \end{aligned} \tag{1}$$

Intuitively, each H_i penalizes the energy of a state $|\phi\rangle$ if it violates clauses in $C(x_i)$ for the i-th variable or has support over computational bases $|z\rangle$ which are not consistent with the CAT projectors. We note that $|\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|$ is the projection operator onto the state $|\mathrm{CAT}(i)\rangle$. The operator H is "local on average" when $m = O(n)$ as each summand H_i acts on approximately K^2m/n qubits in expectation. Furthermore, the largest locality—namely, the largest number of qubits per H_i—is at most $O(\log n)$ in this case, as it corresponds to a maximum of $O(n)$ binomial random variables with $O(n)$ trials and success probabilities $O(n^{-1})$.

This completes the construction of our local (on average) Hamiltonian H. We claim that a suitable choice of α, K, and γ verifies the requirements of the combinatorial NLTS. Specifically, we fix ϵ and define a combinatorial notion of a state being near the ground state.

Definition 2.1. *A pure state $|\psi\rangle$ on $N = Km$ qubits is an ϵ-near ground state (in the combinatorial sense) if there exists any subset $S \subset [n]$—termed an* associated subset*—such that $|S| \ge (1-\epsilon)n$ and such that $|\psi\rangle$ is a ground state for all H_i with $i \in S$. Namely, $H_i|\psi\rangle = 0$ for all $i \in S$.*

We note that a near ground state $|\psi\rangle$ can have multiple associated subsets $S \subset [n]$ that meet the criteria in the above definition.

Next, we fix a positive integer T and consider depth-T circuits. Such circuits are defined inductively as follows. A depth-1 circuit is a unitary U_1 obtained as a tensor product of unitary operators each acting on a disjoint union of 2-qubit subsets. For any $t \le T-1$, suppose U_t is any depth-$(t-1)$ circuit. Then, a depth-t circuit is defined as any circuit of the form VU_{t-1}, where U_{t-1} is any depth-$(t-1)$ circuit and V is any depth-1 circuit.

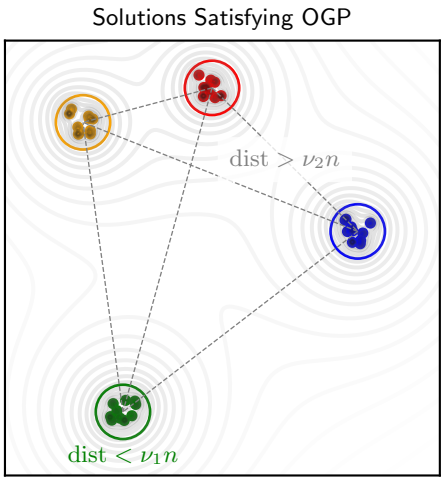

Figure 2: An illustrative visualization of the (ν_1, ν_2)-OGP shown here as a contour plot for an idealized optimization landscape. Solutions are clustered in balls of radius at most $\nu_1 n$ and each pair of disjoint clusters is at least distance $\nu_2 n$ apart.

Definition 2.2. *Given $T > 0$, a state $|\psi\rangle$ is T-trivial if there exists a depth-T circuit U_T such that $|\psi\rangle = U_T|0\rangle^{\otimes N}$.*

We are now ready to state our main result.

Theorem 2.3. *There exist $\alpha, K, \gamma, \epsilon, \tau > 0$ such that the following holds w.h.p. as $n \to \infty$: the Hamiltonian H is frustration free (i.e., it has ground state energy $\lambda_{\min}(H) = 0$), and for every sufficiently large n, if $|\psi\rangle$ is an ϵ-near ground state with respect to the Hamiltonian (1), then for $T \leq \tau \log n$ it holds that $|\psi\rangle$ is not T-trivial.*

3 Robust overlap gap property and clustering in random K-SAT instances

In this section we derive certain structural properties of the solution space geometry of near-satisfying solutions of the random K-SAT problem. In particular, we will show that it exhibits the so-called overlap gap property (OGP); namely, the clustering of near-satisfying assignments when the parameters α and K are set appropriately. This clustering property will be pivotal in the proof of our main result, Theorem 2.3.

Definition 3.1. *Given $0 < \nu_1 < \nu_2 < 1/2$ and a subset $A \subset \{0,1\}^n$ we say that A exhibits an (ν_1, ν_2)-overlap-gap-property—abbreviated as a (ν_1, ν_2)-OGP—if for every $x^1, x^2 \in A$ either $n^{-1}d(x^1, x^2) \leq \nu_1$ or $n^{-1}d(x^1, x^2) \geq \nu_2$, where $d(\cdot, \cdot)$ denotes the Hamming distance in $\{0,1\}^n$.*

When a set A exhibits an (ν_1, ν_2)-OGP and additionally $\nu_1 < (1/2)\nu_2$, there exists a unique partitioning of A into a disjoint union of L clusters $A = \bigcup_{1 \leq \ell \leq L} CL_\ell$, $CL_{\ell_1} \cap CL_{\ell_2} = \emptyset, \ell_1 \neq \ell_2$ such that for every ℓ and every $x^1, x^2 \in CL_\ell$, it holds that $n^{-1}d(x^1, x^2) \leq \nu_1$ and for every $\ell_1 \neq \ell_2$ and every $x^j \in CL_{\ell_j}, j = 1, 2$, $n^{-1}d(x^1, x^2) \geq \nu_2$. According to this definition the possibility of a unique cluster—that is, $L = 1$—is allowed. This clustering property is obtained simply as follows. Define equivalency classes by saying $x \sim y$ iff $n^{-1}d(x, y) \leq \nu_1$. The reflexivity and symmetry are immediate. The transitivity is obtained as well: if $n^{-1}d(x, y), n^{-1}d(y, z) \leq \nu_1$ then $n^{-1}d(x, z) \leq 2\nu_1 < \nu_2$ and thus, by (ν_1, ν_2)-OGP, $n^{-1}d(x, z) \leq \nu_1$. We call this the (ν_1, ν_2)-clustering of A.

Given a K-SAT formula Φ on variables with indices $[n]$ and clauses $C_1, \ldots, C_m$, we denote by $\mathrm{SAT}(\Phi) \subset \{0,1\}^n$ the (possibly empty) set of satisfying solutions of Φ. Furthermore, for every $r \geq 0$ let $\mathrm{SAT}(\Phi, r)$ denote the set of solutions in $\{0,1\}^n$ which violate at most r clauses so that $\mathrm{SAT}(\Phi, 0) = \mathrm{SAT}(\Phi)$. Given a formula Φ and a subset $S \subset [n]$, let $C(S)$ be the set of clauses in Φ such that each clause in $C(S)$ consists entirely of variables x_i with $i \in S$. This should not be confused with $C(x_i)$, which denotes the set of clauses containing the variable x_i. Similarly, for every $r \geq 0$ let $\mathrm{SAT}(\Phi(C(S), r)) \subset \{0,1\}^n$ denote the set of solutions in $\{0,1\}^n$ which violate at most r clauses among those in $C(S)$. Given $\epsilon > 0$ we denote by $\mathrm{SAT}(\Phi, \epsilon, r)$ the set $\bigcup_{S:|S| \geq (1-\epsilon)n} \mathrm{SAT}(\Phi(C(S), r))$ and let $Z(\Phi, \epsilon, r) = |\mathrm{SAT}(\Phi, \epsilon, r)|$.

Our main technical result is as follows.

Theorem 3.2. *Let $\alpha \in (1/2+1/5,1)$. For large enough n, there exist $0<\nu_1<(1/2)\nu_2<\nu_2<1/2$ and $c_2>c_1>0$ such that the following holds. There exist large enough K and small enough $\bar{\epsilon},\bar{\lambda}$ such that for every $0<\epsilon\le\bar{\epsilon}, 0\le\lambda\le\bar{\lambda}$ the set $\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n),\epsilon,\lambda n)$ satisfies (ν_1,ν_2)-OGP w.h.p. as $n\to\infty$. Furthermore, also w.h.p. as $n\to\infty$,*

$$|\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n))| = |\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n),0,0)| \ge \exp(c_2 n)$$

and the associated unique (ν_1,ν_2)-clustering CL_ℓ of $\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)$ satisfies

$$|CL_\ell| \le \exp(c_1 n),$$

for all ℓ.

The theorem roughly speaking says that the set of all nearly optimal assignments of every nearly complete subset of variables (with respect to the induced set of clauses) exhibits an OGP. Furthermore, the implied clustering of this set has the property that each cluster constitutes at most an exponentially small fraction (at most roughly $2^{-(c_2-c_1)n}$)) of the total set of these assignments. The remainder of the section is devoted to the proof of this theorem.

3.1 Lower bound on the number of satisfying assignments

In this Section we quote relevant results from prior literature which give lower bounds on the cardinality of the satisfying set $\mathrm{SAT}(\mathbf{\Phi}(n,m))$; that is, the number of satisfying assignments of our random formula $\mathbf{\Phi}(n,m)$.

Theorem 3.3. *Suppose $\beta < 2^K(\log 2) - \frac{(K+1)(\log 2)+3}{2}$ and $K\ge 3$. Then w.h.p. as $n\to\infty$ $\mathbf{\Phi}(n,\beta n)$ is satisfiable. Furthermore, w.h.p. as $n\to\infty$*

$$n^{-1}\log|\mathrm{SAT}(\mathbf{\Phi}(n,\beta n))| \ge \log 2 + (1/2)\beta\log\left(1-2^{1-K}+2^{-2K}-K2^{-K}\left(1-2^{-K}\right)\left(2^{1-K}+3K2^{-2K}\right)\right) - o(1).$$

This theorem can be found in [ACORT11] as Theorem 6 complemented with a lower bound (26).

Considering now the regime of interest to us, namely $\beta=\alpha 2^K\log 2, \alpha<1$, and using the Taylor expansion $\log(1+x)=x+O(x^2)$, we can simplify the lower bound as $\log 2-(\log 2)\alpha - O(1/2^K)$. We obtain the following corollary.

Corollary 3.4. *For every $\alpha\in(0,1)$ and $\delta>0$, the following holds for all large enough K: w.h.p. as $n\to\infty$,*

$$n^{-1}\log|\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n))| \ge (\log 2)(1-\alpha)-\delta. \tag{2}$$

3.2 Bounds on controlled first and second moments

We fix $1/2>\epsilon>0$ and $\lambda>0$ (which are arbitrary for now), and $\alpha\in(0,1)$. Let $m=\alpha 2^K(\log 2)n$. We write $\mathbf{\Phi}(n,m)$ as $\mathbf{\Phi}(n)$ for short. Recall that $Z(\mathbf{\Phi}(n),\epsilon,\lambda n)=|\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)|$. We now compute bounds on a "controlled" (appropriately defined) second moment of $Z(\mathbf{\Phi}(n),\epsilon,\lambda n)$.

Fix $t\in\{0,1,\dots,n\}$ and let $\mathrm{SAT}_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)$ denote the set of ordered pairs $x^1,x^2\in\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)$ such that $d(x^1,x^2)=n-t$. We let $Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)=|\mathrm{SAT}_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)|$. Note that $Z^2(\mathbf{\Phi}(n),\epsilon,\lambda n)=\sum_t Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)$.

Fix $x^1,x^2\in\{0,1\}^n$, where x^j has variable assignments $x^j_i, i\in[n]$ and $d(x^1,x^2)=n-t$. Fix $S_1,S_2\subset[n]$ with $|S_1|,|S_2|\ge(1-\epsilon)n$. Let $S=S_1\cap S_2$. Denote by $S(x^1,x^2)\subset S$ the set of coordinates in S where x^1 and x^2 agree:

$$S(x^1,x^2)=\{i\in S: x^1_i=x^2_i\}.$$

Consider a clause C in $\mathbf{\Phi}$ conditioned on the event $C\in C(S_1)\cap C(S_2)=C(S)$. In particular, C consists entirely of variables in S. Let us compute the probability that C is satisfied by both x^1 and x^2 when conditioned on this event. We denote by $x\in\mathrm{SAT}(C)$ the event that string x satisfies C. Let E_C be the event that C has distinct variables. Then (for sufficiently large n)

$$\begin{aligned}
\mathbb{P}(x^1,x^2\in\mathrm{SAT}(C)) &\le 1-\mathbb{P}(E_C)\left(\mathbb{P}(x^1\notin\mathrm{SAT}(C)\mid E_C)+\mathbb{P}(x^2\notin\mathrm{SAT}(C)\mid E_C)-\mathbb{P}(x^1,x^2\notin\mathrm{SAT}(C)\mid E_C)\right)\\
&= 1-\left(2/2^K-\mathbb{P}(x^1,x^2\notin\mathrm{SAT}(C))\right)\prod_{i=1}^{K-1}\left(1-\frac{i}{n}\right)\\
&\le 1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K-\mathbb{P}(x^1,x^2\notin\mathrm{SAT}(C)\mid E_C)\right).
\end{aligned}$$

We claim that

$$\mathbb{P}(x^1, x^2 \notin \mathrm{SAT}(C) \mid E_C) \leq 2^{-K} \left(|S(x^1, x^2)|/|S|\right)^K. \tag{3}$$

Indeed, in order for C to be violated by both x^1 and x^2 it has to be the case that C consists entirely of variables in $S(x^1, x^2)$, since otherwise it contains a variable x_i where $x_i^1 \neq x_i^2$ and at least one of x^1, x^2 satisfies C. Conditioned on the event that C consists entirely of variables in $S(x^1, x^2)$ the likelihood that it is violated (by both x^1, x^2) is 2^{-K}. Similarly, the likelihood that C consists entirely of variables in $S(x^1, x^2)$ is upper-bounded $\left(|S(x^1, x^2)|/|S|\right)^K$. The claim follows.

We now obtain a bound on the likelihood that x^1 and x^2 belong to the set $\mathrm{SAT}_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)$ simultaneously.

Lemma 3.5. *There exist functions $g, h : \mathbb{R}_+ \to \mathbb{R}_+$ which depend on α, K satisfying $\lim_{z\to 0} g(z) = \lim_{z\to 0} h(z) = 0$ such that for any x^1, x^2 with $d(x_1, x_2) = n - t$, for all large enough n it holds that:*

$$\mathbb{P}\left(x^1, x^2 \in \mathrm{SAT}_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)\right) \leq n^2 \exp\left(g(\epsilon)n + h(\lambda)n\right) \left(1 - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{n}\right)^K\right)\right)^m.$$

Proof. Fix x^1, x^2 and $S_j, |S_j| \geq (1-\epsilon)n, j = 1, 2$. As before let $S = S_1 \cap S_2$. Then $|S| \geq (1-2\epsilon)n$ and $C(S) \subset C(S_j), j = 1, 2$. We assume that x^j satisfies all but λn clauses in $C(S_j)$. Then x^1 and x^2 satisfy at least $|C(S)| - 2\lambda n$ clauses in the set of clauses $C(S)$. We trivially have that $|S(x^1, x^2)| \leq t$. Fix $m_0 \leq m$ and fix any subset $\mathcal{C} \subset [m]$ with cardinality m_0. Conditioned on the event $C(S) = \{C_j, j \in \mathcal{C}\}$, by our earlier claim and the union bound, the event $x^1, x^2 \in \mathrm{SAT}(\mathbf{\Phi}(n), C(S), \lambda n)$ occurs with probability at most

$$\sum_{r \leq \lambda n} \binom{m_0}{r} \left(1 - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K + 2^{-K}\left(|S(x^1, x^2)|/|S|\right)^K\right)\right)^{m_0 - r}$$
$$\leq n\binom{m}{\lambda n}\left(1 - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^{m_0 - 2\lambda n}.$$

The likelihood of $|C(S)| = m_0$ is

$$\binom{m}{m_0}\left(\frac{|S|}{n}\right)^{Km_0}\left(1 - \left(\frac{|S|}{n}\right)^K\right)^{(m-m_0)} \leq \binom{m}{m_0}\left(\frac{|S|}{n}\right)^{Km_0}\left(1 - (1-2\epsilon)^K\right)^{(m-m_0)}$$
$$\leq \binom{m}{m_0}\left(1 - (1-2\epsilon)^K\right)^{m-m_0}.$$

We obtain

$$\begin{aligned}
&\mathbb{P}\left(x^1, x^2 \in \mathrm{SAT}(\mathbf{\Phi}(n), C(S), \lambda n)\right) \\
&\leq \sum_{m_0 \leq m} \binom{m}{m_0}\left(1 - (1-2\epsilon)^K\right)^{m-m_0} n\binom{m}{\lambda n}\left(1 + \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^{m_0 - 2\lambda n} \\
&= n\binom{m}{\lambda n}\left(1 + (1 - (1-2\epsilon)^K) - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^m \\
&\times \left(1 - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^{-2\lambda n} \\
&\leq n\binom{m}{\lambda n}\left(1 + (1 - (1-2\epsilon)^K) - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^m \left(1 - 2^{-K+1}\right)^{-2\lambda n}. \qquad (4)
\end{aligned}$$

Taking now a union bound over the choices of S we obtain an upper bound on $\mathbb{P}\left(x^1, x^2 \in \mathrm{SAT}_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)\right)$ which is (4) multiplied by $\sum_{(1-2\epsilon)n \leq i \leq n}\binom{n}{i} \leq (2\epsilon n)\binom{n}{2\epsilon n}$. Thus:

$$\begin{aligned}
&\mathbb{P}\left(x^1, x^2 \in \mathrm{SAT}_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)\right) \\
&\leq (2\epsilon n)\binom{n}{2\epsilon n} n\binom{m}{\lambda n}\left(1 + (1 - (1-2\epsilon)^K) - \left(1 - O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{(1-2\epsilon)n}\right)^K\right)\right)^m \left(1 - 2^{-K+1}\right)^{-2\lambda n}.
\end{aligned}$$

We recall that $m \le 2^K(\log 2)n = \Theta(n)$. We also have that:

$$\binom{n}{2\epsilon n} \le \left(\frac{ne}{2\epsilon n}\right)^{2\epsilon n} = \exp(2\epsilon \log(e/(2\epsilon))n).$$

We have that $g_0(\epsilon) \triangleq 2\epsilon\log(e/(2\epsilon)) \to 0$ as $\epsilon \to 0$. We treat similarly the other terms dependent on ϵ and λ. In particular, we use that $1-(1-2\epsilon)^K \to 0$ as $\epsilon \to 0$. Finally, we use that $(2\epsilon n)n \le n^2$, and complete the proof. $\square$

The cardinality of the set of pairs x^1, x^2 with $d(x^1,x^2) = n-t$ is $2^n\binom{n}{t}$. Applying Lemma 3.5 we obtain:

$$\mathbb{E}[Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)] \le 2^n\binom{n}{t}n^2\exp\left(g(\epsilon)n + h(\lambda)n\right)\left(1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{n}\right)^K\right)\right)^m$$

for all sufficiently large n. By allowing t to be in a range of values of the form $a_1 n \le t \le a_2 n$ we also obtain:

$$\begin{aligned}\mathbb{E}\left[\sum_{a_1 n \le t \le a_2 n} Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)\right] \le & n^3\exp\left(g(\epsilon)n + h(\lambda)n\right) \\ & \times \max_{a_1 n\le t\le a_2 n} 2^n\binom{n}{t}\left(1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(\frac{t}{n}\right)^K\right)\right)^m. \quad (5)\end{aligned}$$

Here, the extra factor n is associated with summing over $a_1 n \le t \le a_2 n$ which is at most $(a_2-a_1)n \le n$.

We extract from the right-hand side the expression under the max which dominates the entire expression in exponential in n terms. In particular, let

$$z_2(n,t,K,\alpha) \triangleq 2^n\binom{n}{t}\left(1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}(t/n)^K\right)\right)^m,$$

so that the expression under the max is $\max_{a_1 n\le t\le a_2 n} z_2(n,t,K,\alpha)$. Using $\binom{n}{t} = \exp(nH(t/n)+o(n))$ where $H(x) = -x\log x - (1-x)\log(1-x)$ is the binary entropy function, we obtain:

$$n^{-1}\log z_2(n,t,K,\alpha) = \log(2) + H(t/n) + (m/n)\log\left(1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}\left(t/n\right)^K\right)\right) + o(1).$$

Recall that $m = \alpha 2^K(\log 2)n, \alpha < 1$. We also write $t = sn$. We obtain after Taylor expanding the log function that

$$\begin{aligned} n^{-1}\log z_2(n,t,K,\alpha) &= \log(2) + H(s) + \alpha(\log 2)2^K\log\left(1-\left(1-O\left(\frac{K}{n}\right)\right)\left(2/2^K - 2^{-K}s^K\right)\right) + o(1) \\ &= \log(2) + H(s) - 2(\log 2)\alpha + (\log 2)\alpha s^K + O_K\left(2^{-K}\right) + o(1) \\ &\triangleq C(\alpha,s,K) + o(1). \end{aligned}$$

Lemma 3.6. *There exist $0 < \nu_1 < 2\nu_1 < \nu_2 < 1/2$ such that for every $\alpha \in (1/2+1/10, 1)$ the following holds.*

$$\lim_{K\to\infty}\sup_{s\in[1-\nu_1,1]} C(\alpha,s,K) = \lim_{K\to\infty} C(\alpha,1,K) = (\log 2)(1-\alpha) > 0, \quad (6)$$

$$\lim_{K\to\infty}\sup_{s\in[1-\nu_2,1-\nu_1]} C(\alpha,s,K) \le (\log 2)(1/2-\alpha) \le -(\log 2)/10 < 0. \quad (7)$$

We note that the first identity regards only ν_1. The choice of $\alpha > 1/2+1/10$ is somewhat arbitrary and can be replaced by any constant $1 > c > 1/2$ which does not depend on K.

Proof. Consider the part of $C(\alpha,s,K)$ which depends on s, namely, $H(s) + (\log 2)\alpha s^K$. We consider separately the cases $s \le 1 - \log K/K$ and $s > 1 - \log K/K$. In the first case we note that $s^K = O(1/K) \to 0$ as $K \to \infty$.

To prove (6), by taking ν_1 sufficiently close to 0, we obtain that $\max_{1-\nu_1 \le s \le 1} H(s)$ is sufficiently close to 0 and in particular is at most $(1/2)\log 2 < (\log 2)\alpha$. As a result, in this case:

$$\begin{aligned}\lim_{K\to\infty} \sup_{s\in[1-\nu_1, 1-\log K/K]} C(\alpha, s, K) &\le \log(2) + (1/2)\log 2 - 2(\log 2)\alpha \\ &< (\log 2)(1-\alpha).\end{aligned}$$

When $s > 1 - \log K/K$ we have that $(\log 2)\alpha s^K \le (\log 2)\alpha$ and $H(s) \to 0$ as $K \to \infty$, and thus (6) is obtained by taking $s = 1$.

For (7) we note that for any fixed $0 < \nu_1 < 2\nu_1 < \nu_2 < 1/2$ we have that $\lim_K \sup_{1-\nu_2 \le s \le 1-\nu_1} s^K = 0$ and thus

$$\begin{aligned}\lim_{K\to\infty} \sup_{s\in[1-\nu_2, 1-\nu_1]} C(\alpha, s, K) &\le \log(2) + H(1-\nu_2) - 2(\log 2)\alpha \\ &= 2(\log 2)(1/2 - \alpha) + H(1-\nu_2) \\ &\le -2(\log 2)/10 + H(1-\nu_2).\end{aligned}$$

Taking ν_2 sufficiently close to 0 so that $H(1-\nu_2) < (\log 2)/10$ we obtain (7). □

We now use these bounds for (5) to arrive at the following corollary:

Corollary 3.7. *There exist $0 < \nu_1 < 2\nu_1 < \nu_2 < 1/2$ such that for every $\alpha \in (1/2 + 1/10, 1)$ and $\delta > 0$ the following holds. For every sufficiently large K there exist $\bar\epsilon, \bar\lambda > 0$ such that for all $\epsilon \le \bar\epsilon, \lambda \le \bar\lambda$, for all sufficiently large n,*

$$\limsup_{n\to\infty} n^{-1} \log \mathbb{E}\left[\sum_{t\in[(1-\nu_1)n, n]} Z_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)\right] \le (\log 2)(1-\alpha) + \delta,$$

$$\limsup_{n\to\infty} n^{-1} \log \mathbb{E}\left[\sum_{t\in[(1-\nu_2)n, (1-\nu_1)n]} Z_2(\mathbf{\Phi}(n), \epsilon, \lambda n, t)\right] \le -(\log 2)/(40).$$

We note that δ appears only in the first identity. The reasons for allowing δ to be arbitrarily small is to allow the bound to hold for any choice of α in the stated range. This will be necessary for the proof of Theorem 3.2 below.

Proof. We fix ν_1, ν_2 as in Lemma 3.6. Let $\alpha \in (1/2 + 1/10, 1)$ and let $\delta > 0$ be arbitrary. We find K_0 sufficiently large so that for all $K \ge K_0$,

$$\begin{aligned}\sup_{s\in[1-\nu_1, 1]} C(\alpha, s, K) = C(\alpha, 1, K) &\le (\log 2)(1-\alpha) + \delta/2, \\ \sup_{s\in[1-\nu_2, 1-\nu_1]} C(\alpha, s, K) &\le -(\log 2)/20 < 0.\end{aligned}$$

For every $K \ge K_0$ we find $\bar\epsilon, \bar\lambda$ sufficiently small so that $g(\epsilon) + h(\lambda) < \min(\delta/2, \log(2)/40)$ for all $\epsilon \le \bar\epsilon, \lambda \le \bar\lambda$. The required bounds are obtained from (5) and using the fact that $-(\log 2)/20 + 2(\log 2)/40 = -(\log 2)/40$. □

3.3 Proof of Theorem 3.2

We are now ready to prove Theorem 3.2.

Proof of Theorem 3.2. We fix ν_1, ν_2 as in the setting of Corollary 3.7. Similarly, we fix any $\alpha \in (1/2 + 1/5, 1)$ and any sufficiently small $\delta > 0$ such that

$$\delta \le \frac{1}{7}(\log 2)(1-\alpha). \tag{8}$$

We find large enough K and small enough $\bar\epsilon, \bar\lambda$ so that Corollary 3.7 applies. Furthermore, we assume that K is large enough so that the bound in Corollary 3.4 applies as well. We let $\epsilon < \bar\epsilon$ and $\lambda < \bar\lambda$ be arbitrary. By Markov's

inequality applied to the second bound in Corollary 3.7 and by lowering the constant to $-(\log 2)/50$ we obtain that for all large enough n:

$$\mathbb{P}\left(\sum_{t\in[(1-\nu_2)n,(1-\nu_1)n]} Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)\geq 1\right)\leq \exp\left(-n(\log 2)/50\right),$$

and thus $Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)=0$ for all $t\in[(1-\nu_2)n,(1-\nu_1)n]$ w.h.p. as $n\to\infty$. This means that w.h.p. as $n\to\infty$ for every two subsets $S_j, j=1,2$ such that $|S_j|\geq(1-\epsilon)n$ and every two solutions $x_j, j=1,2$ such that x_j violates at most λn clauses out of the clauses $C(S_j)$—that is, clauses consisting entirely of variables in S_j—it is the case that either $n^{-1}d(x_1,x_2)\leq\nu_1$ or $n^{-1}d(x_1,x_2)\geq\nu_2$. In particular, the set $\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)$ exhibits the (ν_1,ν_2)-OGP.

Consider the implied unique (ν_1,ν_2)-clustering $CL_\ell, \ell\geq 1$ of this set. Note that we trivially have that

$$\bigcup_\ell CL_\ell=\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)\supset\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n)).$$

By Corollary 3.4 w.h.p. as $n\to\infty$:

$$|\mathrm{SAT}(\mathbf{\Phi}(n),\epsilon,\lambda n)|\geq|\mathrm{SAT}(\mathbf{\Phi}(n,\alpha 2^K(\log 2)n))|\geq\exp\left(n(\log 2)(1-\alpha)-n\delta\right). \tag{9}$$

Note that

$$\frac{1}{4}\left(\max_\ell|CL_\ell|\right)^2\leq\sum_\ell\binom{|CL_\ell|}{2}=\sum_{t\in[(1-\nu_1)n,n]}Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t).$$

By the first part of Corollary 3.7, applying Markov's inequality we have that w.h.p. as $n\to\infty$:

$$\sum_{t\in[(1-\nu_1)n,n]}Z_2(\mathbf{\Phi}(n),\epsilon,\lambda n,t)\leq\exp\left((\log 2)(1-\alpha)n+2\delta n\right).$$

Then we obtain that w.h.p. as $n\to\infty$

$$\max_\ell|CL_\ell|\leq 2\exp\left(\frac{1}{2}(\log 2)(1-\alpha)n+\delta n\right)\leq\exp\left(\frac{1}{2}(\log 2)(1-\alpha)n+2\delta n\right).$$

We set $c_1=\frac{1}{2}(\log 2)(1-\alpha)+2\delta$, $c_2=(\log 2)(1-\alpha)-\delta$ and the proof is complete by our choice of δ in (8) leading to $0<c_1<c_2$. □

4 Proof of Combinatorial NLTS

In this section we give the proof of Theorem 2.3.

We first establish a simple upper tail bound on $m-|C(S)|$ when $S\subset[n]$ satisfies $|S|\geq(1-\epsilon)n$. Recall that $C(S)$ is the set of clauses in an instance Φ such that each clause in $C(S)$ consists entirely of variables x_i with $i\in S$.

Proposition 4.1. *For every $\alpha\leq 1$, $K\geq 1$, $\eta>0$ and $m=\alpha 2^K(\log 2)n$, there exists small enough $\epsilon>0$ so that w.h.p. as $n\to\infty$ the formula $\mathbf{\Phi}(n,m)$ satisfies $m-|C(S)|\leq\eta n$ for all $S\subset[n],|S|=(1-\epsilon)n$.*

Proof. Fix $S\subset[n]$. The probability that a random clause belongs to $C(S)$ (namely, consists entirely of variables $x_i, i\in S$) is $(|S|/n)^K$. Then

$$\mathbb{E}[m-|C(S)|]=m\left(1-(|S|/n)^K\right).$$

Note that $|C(S)|$ satisfies the bounded difference property that changing the clause choice from C_j to a different clause C_j' changes $|C(S)|$ by at most 1. Thus, applying McDiarmid's inequality to bound the probability that $m-|C(S)|$ exceeds its expectation by t, we obtain that for every $t\geq 0$

$$\mathbb{P}\left(m-|C(S)|\geq\mathbb{E}[m-|C(S)|]+t\right)\leq\exp\left(-\frac{2t^2}{m}\right).$$

In particular,

$$\mathbb{P}\left(m - |C(S)| \geq n\eta\right) \leq \exp\left(-2\frac{\left(n\eta - m\left(1 - (|S|/n)^K\right)\right)^2}{m}\right).$$

Assume that $\epsilon > 0$ is small enough so that $\eta - 2^K(1-(1-\epsilon)^K) > 0$. Assuming S satisfies $|S| = (1-\epsilon)n$ for this choice of ϵ and using $m \leq 2^K n$ we obtain:

$$\begin{aligned}
\mathbb{P}\left(m - |C(S)| \geq \eta\right) &\leq \exp\left(-2\frac{\left(n\eta - m\left(1 - (1-\epsilon)^K\right)\right)^2}{m}\right) \\
&\leq \exp\left(-\frac{\left(n\eta - 2^K n\left(1 - (1-\epsilon)^K\right)\right)^2}{2^{K-1}n}\right) \\
&= \exp\left(-n\frac{\left(\eta - 2^K\left(1 - (1-\epsilon)^K\right)\right)^2}{2^{K-1}}\right).
\end{aligned}$$

By the union bound,

$$\mathbb{P}\left(\exists S \subset [n] : |S| = (1-\epsilon)n, m - |C(S)| \geq \eta\right) \leq \binom{n}{\epsilon n}\exp\left(-n\frac{\left(\eta - 2^K\left(1 - (1-\epsilon)^K\right)\right)^2}{2^{K-1}}\right).$$

We have that

$$\binom{n}{\epsilon n} \leq (ne/(\epsilon n))^{\epsilon n} = \exp(n\epsilon\log(e/\epsilon)).$$

As $\epsilon \to 0$ we have that $\epsilon\log(e/\epsilon) \to 0$. Similarly, $1-(1-\epsilon)^K \to 0$ as $\epsilon \to 0$. The upper bound is then $\exp(-\Theta(n))$, and the proof is complete. □

We fix for now an arbitrary instance of the formula $\Phi(n,m)$. We only assume that it is satisfiable: $\mathrm{SAT}(\Phi(n,m)) \neq \emptyset$. Fix $\epsilon > 0$ and let $\eta = \eta(\Phi, S)$ be defined by:

$$\eta \triangleq \frac{1}{n}\max_{S\subseteq[n]:|S|=(1-\epsilon)n}(m - |C(S)|). \tag{10}$$

Namely, $n\eta$ is the largest number of clauses across all choices of $S, |S| = (1-\epsilon)n$ containing at least one variable in S^c.

We start with some preliminary derivations. We introduce a (somewhat noncanonical) basis of $\mathbb{C}^{2^N}$. For any $r > 0$ and any $\sigma \in \{0,1\}^r$, denote by $\bar{\sigma} \in \{0,1\}^r$ a bit string obtained by flipping elements of σ to the opposite element (e.g., for $\sigma = (0,0,1,0)$, we have that $\bar{\sigma} = (1,1,0,1)$). The set of elements of our basis are defined by:

$$\left\{\bigotimes_{i\in[n]}\left(\frac{1}{\sqrt{2}}|\sigma_i\rangle \pm \frac{1}{\sqrt{2}}|\bar{\sigma}_i\rangle\right) : \sigma_i \in \{0,1\}^{|D(i)|}, i \in [n]\right\}, \tag{11}$$

where again $D(i)$ is the subset of qubits corresponding to the variable x_i. Here, to avoid ambiguity due to $\bar{\bar{\sigma}} = \sigma$, we assume that σ is smaller than $\bar{\sigma}$ in lexicographic order. Note that the cat state $|\mathrm{CAT}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ is an element of the basis (11). For each i the operator $(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|)$ is diagonal in this basis, and for each element $|w\rangle$ of this basis we have that

$$(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|)|w\rangle = 0 \tag{12}$$

if the i-th element of the representation of w in (11) is exactly $|\mathrm{CAT}(i)\rangle$ and

$$(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|)|w\rangle = |w\rangle \tag{13}$$

otherwise.

Let $\{|z\rangle\}, z \in \{0,1\}^N$ denote the computational basis. Each element of the basis (11) expands in the computational basis in a straightforward way as follows. For each element of the basis

$$|w\rangle = \bigotimes_{i\in[n]} \left(\frac{1}{\sqrt{2}}|\sigma_i\rangle \pm \frac{1}{\sqrt{2}}|\bar{\sigma}_i\rangle \right)$$

let $B(w)$ be the set of bit strings $z \in \{0,1\}^N$ such that for each subset $D(i), i \in [n]$ it holds that $z_{D(i)} = \sigma_i$ or $= \bar{\sigma}_i$. Then

$$|w\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{z\in B(w)} (-1)^{R(w,z)}|z\rangle, \tag{14}$$

where $R(w,z)$ is the number of -1-s appearing in the projection of $|w\rangle$ onto $|z\rangle$.

We now characterize the ϵ-near ground states in terms of the elements of this basis.

Lemma 4.2. *Suppose $|\psi\rangle$ is an ϵ-near ground state for H and $S \subset [n]$ is (any) associated subset. Define the (unnormalized) state $|\phi\rangle \triangleq Q^{-1}(\gamma)|\psi\rangle$. Suppose $|w\rangle$ is an element of the basis such that for some $i \in S$, the i-th element of $|w\rangle$ in the representation (11) is distinct from $|\mathrm{CAT}(i)\rangle$. Then $\langle\phi|w\rangle = 0$.*

Namely, the expansion of $|\phi\rangle$ in this basis consists only of elements $|w\rangle$ of the form $\bigotimes_{i\in[n]} \left(\frac{1}{\sqrt{2}}|\sigma_i\rangle \pm \frac{1}{\sqrt{2}}|\bar{\sigma}_i\rangle \right)$ where $\frac{1}{\sqrt{2}}|\sigma_i\rangle \pm \frac{1}{\sqrt{2}}|\bar{\sigma}_i\rangle = |\mathrm{CAT}(i)\rangle$ for each $i \in S$.

Proof. For every $i \in S$ we have that

$$\begin{aligned}
0 &= \langle\psi|H_i|\psi\rangle \\
&= \langle\phi|Q(\gamma)H_iQ(\gamma)|\phi\rangle \\
&= \langle\phi|Q(\gamma)Q^{-1}_{x_i,\gamma}\left(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|\right)Q^{-1}_{x_i,\gamma}Q(\gamma)|\phi\rangle \\
&= \langle\phi|\left(\bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}\right)\left(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|\right)\left(\bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}\right)|\phi\rangle,
\end{aligned}$$

where $\bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}$ is assumed to act as identity operator on qubits associated with clauses in $C(x_i)$, namely qubits in the set $\{(j,k), j \in C(x_i), k \in [K]\}$. Let $|\tilde{\psi}_i\rangle \triangleq \bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}|\phi\rangle$. Then:

$$0 = \langle\tilde{\psi}_i|\left(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|\right)|\tilde{\psi}_i\rangle.$$

We expand $|\tilde{\psi}_i\rangle$ in the basis $|\tilde{\psi}_i\rangle = \sum_w \langle w|\tilde{\psi}_i\rangle|w\rangle$ previously introduced to obtain:

$$0 = \sum_{w_1,w_2} \langle\tilde{\psi}_i|w_1\rangle\langle w_2|\tilde{\psi}_i\rangle\langle w_1|\left(I - |\mathrm{CAT}(i)\rangle\langle\mathrm{CAT}(i)|\right)|w_2\rangle.$$

Applying (12) and (13) we obtain:

$$0 = \sum_{w\in Y_i} |\langle|\tilde{\psi}_i|w\rangle|^2,$$

where the sum is over the subset Y_i of elements $|w\rangle$ of the basis such that its i-th element in the representation (11) is distinct from $|\mathrm{CAT}(i)\rangle$. We thus obtain that $\langle\tilde{\psi}_i|w\rangle = 0$ for all $|w\rangle \in Y_i$ and thus the expansion of $\tilde{\psi}_i$ in this basis contains only elements $|w\rangle$ with the i-the element equal to $|\mathrm{CAT}(i)\rangle$.

Recall that $|\tilde{\psi}_i\rangle = \left(\bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}\right)|\phi\rangle$. The operator $\bigotimes_{j\notin C(x_i)} Q_{C_j,\gamma}$ acts as the identity operator on qubits in $D(i)$. Then $\langle\phi|w\rangle = 0$ if the i-th element of $|w\rangle$ is distinct from $|\mathrm{CAT}(i)\rangle$. Since this applies to all $i \in S$ the proof is complete. □

Fix an ϵ-near ground state $|\psi\rangle = Q(\gamma)|\phi\rangle$ and any associated subset $S \subset [n]$. Let $W(S)$ be the subset of the basis consisting of $|w\rangle$ such that for each $i \in S$, the i-th element of $|w\rangle$ is $|\mathrm{CAT}(i)\rangle$ in our representation (11). From (10) we have that:

$$|W(S)| \leq 2^{nK\eta} \tag{15}$$

since $|S| \geq (1-\epsilon)n$ and each element of $D(i), i \notin S$ appears in at least one clause outside of $C(S)$. The implication of Lemma 4.2 and (14) taken together is that $|\phi\rangle$ as in Lemma 4.2 can be written as:

$$\begin{aligned} |\phi\rangle &= \sum_{|w\rangle \in W(S)} \langle w|\phi\rangle \, |w\rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)^n \sum_{|w\rangle \in W(S)} \langle w|\phi\rangle \sum_{z \in B(w)} (-1)^{R(w,z)} |z\rangle. \end{aligned}$$

This implies that for every element of the computational basis $|z\rangle$ we have that:

$$\langle \phi|z\rangle = \left(\frac{1}{\sqrt{2}}\right)^n \sum_{w : z \in B(w), |w\rangle \in W(S)} \langle w|\phi\rangle \, (-1)^{R(w,z)}, \tag{16}$$

with the understanding that the value is zero if the sum is empty. From this, using (15), and the Cauchy–Schwartz inequality $|\langle \phi|w\rangle| \leq \|\phi\|_2$, we obtain an upper bound for every z:

$$|\langle \phi|z\rangle| \leq \left(\frac{1}{\sqrt{2}}\right)^n \|\phi\|_2 |W(S)| \leq \left(\frac{1}{\sqrt{2}}\right)^n \|\phi\|_2 2^{K\eta n}. \tag{17}$$

Let $\bar{S} \subset \{0,1\}^N$ consist of bit strings $z \in \{0,1\}^N$ which are consistent on S, namely such that for each $i \in S$ the values of z on $D(i)$ are all identically 0 or identically 1. We have that:

$$|\bar{S}| = 2^{(1-\epsilon)n} |W(S)| \leq 2^{n + K\eta n}. \tag{18}$$

Any $z \in \bar{S}$ can be projected to a partial assignment of variables $x_i, i \in S$ in a natural way. We denote by $x_S(z) \in \{0,1\}^S$ this projection. Since every clause C in $C(S)$ consists entirely of variables in $x_i, i \in S$, for every such clause C and for every $z \in \bar{S}$, this clause is either satisfied or violated by the projection $x_S(z)$, regardless of the values of the value of the variables $x_i, i \notin S$. Denote by $\ell(z) \geq 0$ the number of clauses in $C(S)$ violated by the projection $x_S(z)$. Note that even though $z \in \{0,1\}^N$ might not represent a consistent assignment of all variables x_i, for each clause C_j it is still well defined whether C_j is satisfied by z or not. We decompose $\bar{S}$ as $\bigcup_{r \geq 0} \bar{S}(r)$, where $\bar{S}(r)$ is the set of strings $z \in \bar{S}$ with $\ell(z) = r$.

Lemma 4.3. *The following bounds hold for every $r \geq 0$ and $z \in \bar{S}(r)$:*

$$\gamma^{r+\eta n} |\langle \phi|z\rangle| \leq |\langle \psi|z\rangle| \leq \gamma^r |\langle \phi|z\rangle|. \tag{19}$$

Proof. $Q(\gamma)$ is diagonal in the computational basis. For every $z \in \bar{S}$ we have that $Q(\gamma)|z\rangle = \gamma^v |z\rangle$, where v is the total number of clauses in $\{C_j, j \in [m]\}$ violated by z, including here clauses that contain classical variables x_i for which z is inconsistent. Thus:

$$|\langle \psi|z\rangle| = |\langle \phi|Q(\gamma)|z\rangle| = \gamma^v |\langle \phi|z\rangle|.$$

Note that when $z \in \bar{S}(r)$ we have by (10) that $r \leq v \leq r + \eta n$. Then (19) follows. □

For every $r \geq 0$ and every $z \in \bar{S}(r)$, by applying Lemma 4.3 to (17) we obtain:

$$|\langle \psi|z\rangle| \leq \gamma^r \left(\frac{1}{\sqrt{2}}\right)^n \|\phi\|_2 2^{K\eta n}. \tag{20}$$

We now obtain a complementary lower bound. Fix any two bit strings $z_1, z_2 \in \bar{S}$ which agree on the set of qubits $\bigcup_{i\notin S} D(i)$. Note then that for every $|w\rangle \in W(S)$, $z_1 \in B(w)$ iff $z_2 \in B(w)$. Furthermore, we claim that for every $|w\rangle \in W(S)$

$$R(w, z_1) = R(w, z_2).$$

Indeed, all minuses contributing to $R(w, z)$ arise from minuses in $w = \bigotimes_{i\in[n]} \left(\frac{1}{\sqrt{2}}|\sigma_i\rangle \pm \frac{1}{\sqrt{2}}|\bar{\sigma}_i\rangle\right)$ associated with $i \notin S$ by the definition of $W(S)$, and those are identical for z_1 and z_2 since they are identical outside of $\bigcup_{i\in S} D(i)$. We then obtain from (16) that $\langle\phi|z_1\rangle = \langle\phi|z_2\rangle$.

Let z^* be any maximizer $z^* = \arg\max_{z\in\{0,1\}^N} |\langle\phi|z\rangle|$. The maximization can be restricted to $z \in \bar{S}$ since by (16) it has to be the case that $z \in B(w)$ for some $w \in W(S)$. We thus trivially have from (18) that:

$$|\langle\phi|z^*\rangle|^2 \geq 2^{-(1+K\eta)n}\|\phi\|_2^2.$$

Recall that $\bar{S}(0) \subset \bar{S}$ consists of bit strings z such that their projection $x_S(z)$ satisfies all clauses $C_j \in C(S)$. Namely, it is the set of bit strings in $\bar{S}$ such that $\ell(z) = 0$. For every $z \in \bar{S}(0)$, let z^{z^*} be obtained from z by changing coordinates of z in $\bigcup_{i\notin S} D(i)$ to the one of z^* and leaving them intact otherwise. By the above, $\langle\phi|z^{z^*}\rangle = \langle\phi|z^*\rangle$. Note that for any two strings $z_1, z_2 \in \bar{S}(0)$ which differ on $\bigcup_{i\in S} D(i)$ we have that $z_1^{z^*} \neq z_2^{z^*}$. We therefore obtain:

$$\sum_{z\in\bar{S}(0)} |\langle\phi|z^{z^*}\rangle|^2 \geq |\bar{S}(0)|2^{-(1+K\eta)n}\|\phi\|_2^2.$$

Applying the lower bound part of Lemma 4.3 we obtain the lower bound:

$$\sum_{z\in\bar{S}(0)} |\langle\psi|z^{z^*}\rangle|^2 \geq |\bar{S}(0)|\gamma^{2\eta n}2^{-(1+K\eta)n}\|\phi\|_2^2.$$

Combining this as an upper bound on $\|\phi\|_2^2$ with (20) we obtain the following estimate on measurement probabilities $|\langle\psi|z\rangle|^2$ for $z \in \bar{S}(r)$:

$$\begin{aligned}
|\langle\psi|z\rangle|^2 &\leq \frac{\gamma^{2r}\left(\frac{1}{2}\right)^n 2^{2K\eta n}}{|\bar{S}(0)|\gamma^{2\eta n}2^{-(1+K\eta)n}} \sum_{z\in\bar{S}(0)} |\langle\psi|z^{z^*}\rangle|^2 \\
&= \frac{\gamma^{2r-2\eta n}2^{3K\eta n}}{|\bar{S}(0)|} \sum_{z\in\bar{S}(0)} |\langle\psi|z^{z^*}\rangle|^2 \\
&\leq \frac{\gamma^{2r-2\eta n}2^{3K\eta n}}{|\bar{S}(0)|} \\
&\leq \frac{\gamma^{2r}\left(\frac{2}{\gamma}\right)^{3K\eta n}}{|\bar{S}(0)|},
\end{aligned}$$

where the third bound uses $\|\psi\|_2 = 1$. This an important finding which we summarize as follows.

Theorem 4.4. *For every $r \geq 0$ and $z \in \bar{S}(r)$*

$$|\langle\psi|z\rangle|^2 \leq \frac{\gamma^{2r}\left(\frac{2}{\gamma}\right)^{3K\eta n}}{|\bar{S}(0)|}.$$

Loosely speaking, the bound in the theorem states that the probability weight associated with strings z violating r clauses is at most roughly $\gamma^{2r}/|\bar{S}(0)|$. We will argue that the cardinality of $\bar{S}(0)$ is exponentially large with a controlled exponent. By making r linear in n, then, the contribution of these r-violating bit strings will be negligible, and thus most of the probability mass of $|\langle z|\psi\rangle|^2$ is spread over the nearly satisfying solutions. Furthermore, the probability weight associated with each individual string in $\bar{S}(0)$ is also roughly at most $1/|\bar{S}(0)|$. Namely, $|\langle z|\psi\rangle|^2$ is roughly uniform over nearly satisfying solutions.

From our robust OGP, the distribution of $|\psi\rangle$ over nearly satisfying solution is thus well-spread in the sense that it has large mass over clusters that are far apart. To translate this into a lower bound on circuit depth we will use the Lemma below, variants of which can be found throughout the literature [EH17, MKB22, ABN23].

Lemma 4.5 (Fact 4 of [ABN23]). *Let p be a distribution on n bits generated by measuring the output of a quantum circuit acting on the initial state $|0\rangle^{\otimes n}$. If there exist sets $S_1, S_2 \subseteq \{0,1\}^n$ where the Hamming distance between elements of S_1 and S_2 is at least $d(S_1, S_2)$ and $p(S_1) \geq \mu$ and $p(S_2) \geq \mu$, then the depth T of the circuit must be at least*

$$T \geq \frac{1}{3} \log \left(\frac{d(S_1, S_2)^2}{400n \log(1/\mu)} \right). \tag{21}$$

4.1 Proof of Theorem 2.3

Proof of Theorem 2.3. We assume the setting of Theorem 3.2. Our formula Φ is $\mathbf{\Phi}(n, m)$. The parameters α, K, etc. are as in the theorem.

We select $\epsilon \leq \bar{\epsilon}, \lambda \leq \bar{\lambda}$ and γ as follows. We fix any $0 < \lambda \leq \bar{\lambda}$. We select γ small enough so that so that $\gamma^{2\lambda} < 1/8$. We select $\eta > 0$ small enough so that

$$\left(\frac{2}{\gamma}\right)^{4K\eta} \leq 2^{\frac{c_2 - c_1}{2}} \tag{22}$$

$$\gamma^{2\lambda - 3K\eta} < 1/8. \tag{23}$$

$$4K\eta < 1. \tag{24}$$

We finally select $\epsilon < \bar{\epsilon}$ also small enough with respect to K and η such that Proposition 4.1 applies.

Assume that the high probability event underlying Theorem 3.2 and Proposition 4.1 takes place for this choice of parameters. Denote by CL_ℓ the associated (ν_1, ν_2)-clustering of the set $\mathrm{SAT}(\mathbf{\Phi}(n, \epsilon, \lambda n))$. In particular, $|CL_\ell| \leq 2^{c_1 n}$ for all ℓ. Fix an ϵ-near ground state $|\psi\rangle$ and any associated subset $S \subset [n], |S| \geq (1-\epsilon)n$. In particular, $\bar{S}(0) \neq \emptyset$, and furthermore by the conclusion of Theorem 3.2:

$$|\bar{S}(0)| \geq 2^{c_2 n}. \tag{25}$$

We claim the following relations:

$$\begin{aligned}
\sum_{r > \lambda n} \sum_{z \in \bar{S}(r)} |\langle \psi | z \rangle|^2 &\leq O(n) \frac{\gamma^{2\lambda n} \left(\frac{2}{\gamma}\right)^{3K\eta n}}{|\bar{S}(0)|} |\bar{S}| \\
&\leq O(n) \gamma^{2\lambda n} \left(\frac{2}{\gamma}\right)^{3K\eta n} 2^{n + K\eta n} \\
&\leq \gamma^{2\lambda n - 3K\eta n} 4^n \\
&\leq (1/2)^n.
\end{aligned}$$

The first inequality follows from Theorem 4.4 and the fact that the total number of clauses and thus terms in the sum $r \geq \lambda n$ is $O(n)$. The second inequality follows from (18) and $|\bar{S}(0)| \geq 1$. The third inequality follows from (24) ,and the last inequality follows from (23). Thus, the overall probability measure associated with strings $z \in \bar{S}(r), r > \lambda n$ is exponentially small (at most $(1/2)^n$).

Consider now strings $z \in \bigcup_{r \leq \lambda n} \bar{S}(r)$. The projection $x_S(z)$ to the assignment of variables in S corresponds to the partial assignment $x : S \to \{0,1\}$ with the property that it violates at most λn clauses out of $|C(S)|$ clauses consisting of variables in S. Thus there exists an extension $\tilde{x}$ of x onto an assignment of variables in $[n] \setminus S$ such that the extension $\tilde{x}$ belongs to one of the clusters CL_ℓ. For any such cluster CL_ℓ, let BCL_ℓ be the set of strings $z \in \bigcup_{r \leq \lambda n} \bar{S}(r)$ with this property. Namely, for every $z \in BCL_\ell$, there is an extension $\tilde{x}$ of $x_S(z)$ such that $\tilde{x} \in CL_\ell$. We now obtain an upper bound on the cardinality of BCL_ℓ. For any fixed assignment $x : S \to \{0,1\}$, there exists at most $2^{K\eta n}$ strings z such that $x_S(z)$ coincided with this assignment. These strings correspond to the at most $K\eta n$ qubits in $\bigcup_{i \notin S} D(i)$. Thus:

$$|BCL_\ell| \leq 2^{K\eta n} |CL_\ell| \leq 2^{K\eta n} 2^{c_1 n}.$$

Applying Theorem 4.4 we obtain:

$$\begin{aligned}\sum_{z\in BCL_\ell}|\langle\psi|z\rangle|^2 &\le 2^{K\eta n}|CL_\ell|\frac{\left(\frac{2}{\gamma}\right)^{3K\eta n}}{|\bar{S}(0)|}\\ &\le \left(\frac{2}{\gamma}\right)^{4K\eta n}\frac{|CL_\ell|}{|\bar{S}(0)|}\\ &\le \left(\frac{2}{\gamma}\right)^{4K\eta n}2^{-(c_2-c_1)n}\\ &\le 2^{-\frac{c_2-c_1}{2}n},\end{aligned}$$

where the second-to-last inequality uses (25) and the last inequality uses (22).

To translate the above into a circuit lower bound we apply Lemma 4.5. Let $p(z)=|\langle\psi|z\rangle|^2$ be the distribution of bit strings resulting from measuring $|\psi\rangle$ in the computational basis. From the above, we have that the probability of measuring a bit string violating at most λn clauses is at least

$$p\left(\bigcup_{r\le\lambda n}\bar{S}(r)\right)\ge 1-(1/2)^n, \tag{26}$$

which is greater than 0.95 for large enough n. Each of the bit strings in $\bigcup_{r\le\lambda n}\bar{S}(r)$ is an element of a cluster BCL_ℓ. Furthermore, we have that $p(BCL_\ell)\le 2^{-\frac{c_2-c_1}{2}n}$. Therefore, for large enough n, we partition the union of all clusters $\cup_\ell BCL_\ell$ into disjoint sets S_1 and S_2 such that each has size $p(S_1),p(S_2)\ge 0.45=\mu$. From the (ν_1,ν_2)-OGP, elements of S_1 and S_2 must be at least distance $d(S_1,S_2)\ge\nu_2 n$ apart as S_1 and S_2 contain disjoint clusters. Applying Lemma 4.5 we finally have that:

$$T\ge\frac{1}{3}\log\left(\frac{\nu_2^2 n}{400\log(1/0.45)}\right)=\Omega(\log(n)). \tag{27}$$

□

5 Local Hamiltonians with bounded degree

One arguable limitation of our result is that in our model the degree (number of local Hamiltonians per qubit) remains bounded only on average, while at maximum can be as large as the largest degree in our random K-SAT model ($O(\log n/\log\log n)$). We now show that this is fixable by switching to a different model; namely, the p-spin Ising model on a sparse random regular graph. We will not go into full proof of the result and just lay out key ideas for brevity.

We first describe the model on a general p-uniform hypergraph. First recall that a p-uniform hypergraph on the set of nodes $[n]$ is a collection $e_1,\dots,e_m$ of cardinality p subsets of $[n]$ called hyperedges. The case where $p=2$ corresponds to an undirected graph in the usual sense. Suppose real values J_e—which we call couplings—are associated with all hyperedges $e_1,\dots,e_m$. We consider a (classical) Hamiltonian H which associates an energy $H(\sigma)=\sum_e J_e\prod_{1\le i\le p}\sigma(e(i))$ with each spin assignment $\sigma:[n]\to\{\pm1\}$. Here, $e(i)\in[n]$ denotes the i-node in hyperedge e (the ordering is irrelevant since a product is taken).

We now consider this model on a graph $\mathbb{G}_{n,d,p}$ which is a d-regular p-uniform hypergraph generated uniformly at random from all such graphs. We call a hypergraph d-regular if every node is included in precisely d hyperedges; note that the identity $nd=mp$ should hold. The existence of such graphs is a classical result [JŁR00]. We also assume that the couplings J_e are generated i.i.d. uniformly from $\{\pm1\}$ (namely, they are Rademacher distributed), independently from everything else. We now lay out some facts about this model and either provide references for them or lay out road maps for proving them using methods which are now fairly standard.

(a) The ground state energy $\min_\sigma H(\sigma)$ satisfies $\min_\sigma H(\sigma)=-\eta_{\text{Parisi}}\sqrt{d}(1+o_d(1))n$ w.h.p. as $n\to\infty$. Here, $o_d(1)$ hides a factor converging to zero as d increases. This fact was proven in [DMS17] for $p=2$ both for random regular graphs (discussed above) and also Erdös-Rényi graphs with average degree d. The case of

general p was proven in [CGPR19] for Erdös-Rényi hypergraphs, and is anticipated to hold for regular graphs as well using the same ideas, though this is not documented in the literature. The interpolation is done from the mean field model, namely, the model where all $\binom{n}{p}$ couplings are present (a complete hypergraph), also with Rademacher-distributed couplings. This interpolation was proven recently also for quantum spin glass models and variants such as the so-called SYK model [AGK24]. The validity of this interpolation can be proven using the Lindeberg's method [Sen18] which also implies the universality property: the Rademacher distribution can be replaced with any zero mean, variance 1 sufficiently well-behaved distribution.

(b) The mean field models exhibit the overlap gap property when p is even and satisfies $p \geq 4$. This was proven in [CGPR19], and a simpler proof is found in [GJK23] for the case of large (even or odd) p. Furthermore, the overlap gap property "survives" the interpolation process, and, as a result, holds in Erdös-Rényi and random regular hypergraphs as well for d sufficiently large when $p \geq 4$ is even. For the Erdös-Rényi case this was proven in [CGPR19] and is expected to be true for random regular hypergraphs as well using the same technique, though is not documented in the literature.

Combining these facts we obtain a model—the p-spin Ising model on random regular hypergraphs—which exhibits an overlap gap property. Next, we can construct a quantum Hamiltonian (with zero ground state energy up to a shift by the identity) from this classical Hamiltonian using the same method as for the random K-SAT Hamiltonian. Since d does not depend on the number of spins n, our new quantum Hamiltonian is not only p-local, but also has bounded (by dp) degree as per our construction. This procedure thus produces a local bounded degree quantum Hamiltonian which exhibits a combinatorial NLTS property.

Acknowledgements

The authors thank Aram Harrow and Brice Huang for valuable discussions. E.R.A. acknowledges funding by STAQ under award NSF Phy-1818914. D.G. acknowledges funding from NSF Grant DMS-2015517.

References

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum PCP conjecture. *SIGACT News*, 44(2):47–79, June 2013. doi:10.1145/2491533.2491549.

[AB22] Anurag Anshu and Nikolas P. Breuckmann. A construction of combinatorial NLTS. *Journal of Mathematical Physics*, 63(12):122201, December 2022. doi:10.1063/5.0113731.

[ABN23] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. NLTS Hamiltonians from good quantum codes. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, pages 1090–1096, New York, NY, USA, 2023. Association for Computing Machinery. doi:10.1145/3564246.3585114.

[ACO08] Dimitris Achlioptas and Amin Coja-Oghlan. Algorithmic barriers from phase transitions. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 793–802, 2008. doi:10.1109/FOCS.2008.11.

[ACORT11] Dimitris Achlioptas, Amin Coja-Oghlan, and Federico Ricci-Tersenghi. On the solution-space geometry of random constraint satisfaction problems. *Random Structures & Algorithms*, 38(3):251–268, 2011. doi:10.1002/rsa.20323.

[AGK24] Eric R. Anschuetz, David Gamarnik, and Bobak T. Kiani. Bounds on the ground state energy of quantum p-spin Hamiltonians, 2024. arXiv:2404.07231, doi:10.48550/arXiv.2404.07231.

[AN22] Anurag Anshu and Chinmay Nirkhe. Circuit lower bounds for low-energy states of quantum code Hamiltonians. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 6:1–6:22, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.6.

[BKKT20] Sergey Bravyi, Alexander Kliesch, Robert Koenig, and Eugene Tang. Obstacles to variational quantum optimization from symmetry protection. *Physical Review Letters*, 125:260505, December 2020. doi:10.1103/PhysRevLett.125.260505.

[Bra11] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. In Kazem Mahdavi, Deborah Koslover, and Leonard L. Brown, III, editors, *Cross Disciplinary Advances in Quantum Computing*, volume 536 of *Contemporary Mathematics*, pages 33–48. American Mathematical Society, Providence, RI, USA, 2011. doi:10.1090/conm/536/10552.

[CGPR19] Wei-Kuo Chen, David Gamarnik, Dmitry Panchenko, and Mustazee Rahman. Suboptimality of local algorithms for a class of max-cut problems. *The Annals of Probability*, 47(3):1587–1618, 2019. doi:10.1214/18-AOP1291.

[COE11] Amin Coja-Oghlan and Charilaos Efthymiou. *On independent sets in random graphs*, pages 136–144. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2011. doi:10.1137/1.9781611973082.12.

[DMS17] Amir Dembo, Andrea Montanari, and Subhabrata Sen. Extremal cuts of sparse random graphs. *The Annals of Probability*, 45(2):1190–1217, 2017. doi:10.1214/15-AOP1084.

[EH17] Lior Eldar and Aram W. Harrow. Local Hamiltonians whose ground states are hard to approximate. In *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 427–438, Los Alamitos, CA, USA, October 2017. IEEE Computer Society. doi:10.1109/FOCS.2017.46.

[Eld21] Lior Eldar. Robust quantum entanglement at (nearly) room temperature. In James R. Lee, editor, *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 49:1–49:20, Dagstuhl, Germany, 2021. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2021.49.

[FH14] Michael H. Freedman and Matthew B. Hastings. Quantum systems on non-k-hyperfinite complexes: a generalization of classical statistical mechanics on expander graphs. *Quantum Information & Computation*, 14(1–2):144–180, January 2014. doi:10.26421/qic14.1-2-9.

[FL03] Silvio Franz and Michele Leone. Replica bounds for optimization problems and diluted spin systems. *Journal of Statistical Physics*, 111(3):535–564, May 2003. doi:10.1023/A:1022885828956.

[Gam21] David Gamarnik. The overlap gap property: A topological barrier to optimizing over random structures. *Proceedings of the National Academy of Sciences*, 118(41):e2108492118, 2021. doi:10.1073/pnas.2108492118.

[GJK23] David Gamarnik, Aukosh Jagannath, and Eren C. Kızıldağ. Shattering in the Ising pure p-spin model, 2023. arXiv:2307.07461, doi:10.48550/arXiv.2307.07461.

[GMZ22] David Gamarnik, Cristopher Moore, and Lenka Zdeborová. Disordered systems insights on computational hardness. *Journal of Statistical Mechanics: Theory and Experiment*, 2022(11):114015, November 2022. doi:10.1088/1742-5468/ac9cc8.

[GS17] David Gamarnik and Madhu Sudan. Limits of local algorithms over sparse random graphs. *The Annals of Probability*, 45(4):2353–2376, 2017. doi:10.1214/16-AOP1114.

[JLR00] Svante Janson, Tomasz Łuczak, and Andrzej Rucinski. *Random Regular Graphs*, chapter 9, pages 233–270. John Wiley & Sons, Ltd, 2000. doi:https://doi.org/10.1002/9781118032718.ch9.

[LZ22] Anthony Leverrier and Gilles Zemor. Quantum Tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883, Los Alamitos, CA, USA, November 2022. IEEE Computer Society. doi:10.1109/FOCS54457.2022.00117.

[MKB22] Ali Hamed Moosavian, Seyed Sajad Kahani, and Salman Beigi. Limits of short-time evolution of local Hamiltonians. *Quantum*, 6:744, June 2022. doi:10.22331/q-2022-06-27-744.

[MMZ05] M. Mézard, T. Mora, and R. Zecchina. Clustering of solutions in the random satisfiability problem. *Physical Review Letters*, 94:197205, May 2005. doi:10.1103/PhysRevLett.94.197205.

[Sen18] Subhabrata Sen. Optimization on sparse random hypergraphs and spin glasses. *Random Structures & Algorithms*, 53(3):504–536, 2018. doi:10.1002/rsa.20774.