Constructing concrete hard instances of the maximum independent set problem

Naoto Shiraishi$^1$ and Jun Takahashi$^2$

$^1$Department of Physics, Keio University, Hiyoshi 3-14-1, Kohoku-ku, Yokohama, Japan
$^2$Institute of Physics, Chinese Academy of Sciences, No.8, 3rd South Street, Zhongguancun, Beijing, People’s Republic of China
E-mail: naoto.shiraishi@gakushuin.ac.jp and jt@iphy.ac.cn

Received 23 June 2019
Accepted for publication 27 August 2019
Published 4 November 2019

Online at stacks.iop.org/JSTAT/2019/113401
https://doi.org/10.1088/1742-5468/ab409d

Abstract. We provide a deterministic construction of hard instances for the maximum independent set problem (MIS). The constructed hard instances form an infinite graph sequence with increasing size, which possesses similar characteristics to sparse random graphs and in which MIS cannot be solved efficiently. We analytically and numerically show that the linear programming relaxation with cutting planes, which is one of the standard method to solve the MIS problem, cannot upper bound the size of the maximum independent set tightly.

Keywords: typical-case computational complexity
Contents

1. Introduction 2
2. Maximum independent set problem and characterization of hardness 3
3. Linear programming relaxation with cutting planes 5
4. Construction of the graph sequence 6
5. Demonstration of hardness 7
  5.1. Lower bound on refutation obtained by linear programming relaxation with cutting planes 7
  5.2. Upper bound on independent ratio 10
6. Discussion 11
Acknowledgments 12
Appendix A. Table of presence or absence of short cycles with odd length 12
Appendix B. Hoffman’s bound for graphs with a self loop 14
References 15

1. Introduction

Hardness of optimization problems has been an important topic not only in computer science but also in physics, cryptography theory, and engineering. Traditional computational complexity theory in computer science mainly concerns the worst-case hardness, where many significant results including NP-completeness and hardness of approximation have been developed [1]. Recently, the cooperation of computer science and statistical physics has shed light on the problems of the average-case hardness, in which we consider the hardness of random instances of the problem. For the randomized version, the conventional approach with reduction has found only a few examples [2–7], and instead the statistical mechanics approach has established rich structures of computational hardness. In the statistical mechanics approach, similarities between some optimization problems and some physical models were first pointed out [8–10], and then the easy-to-hard transition threshold where random instances become typically easy/hard has been evaluated [11–16] with some mathematical supports [17–20]. In addition, similarities to the spin glass transition phenomena including replica symmetry breaking and the complex structure of the state space has also been studied intensively [21–31] including rigorous approaches [32–37].

In spite of these successes, one of the most important questions, why hard problem are hard, has not yet been fully addressed. One stumbling block to clarifying the origin of hardness is that we do not have concrete examples of hard instances. Studies on
both the worst-case hardness and average-case hardness employ existence proofs, and no instance is actually specified as a hard instance. We emphasize that even if random graphs are known to satisfy a property (in our case: being a hard instance) with high probability, the explicit construction of a graph with this property is in general a very hard task [38, 39]. Due to the lack of concrete hard instances, we can access only the ensemble-averaged properties, and fail to clarify the solution space structure of each hard instance. While there have been attempts to obtain hard instances mainly for a benchmark of some new algorithms [40–47], these constructions are still probabilistic, not deterministic, and thus the problem mentioned above still remains. In addition, the hardness of instances is usually confirmed only empirically, which restricts analytical investigation of computational hardness. A concrete hard instance which reflects properties of typical hard instances will serve as a platform for a further and fresh understanding of the origin of hardness in hard problems.

In this paper, we construct the first example of concrete hard instances of an optimization problem called the maximum independent set problem (MIS). We provide a construction of an infinite sequence of graphs with increasing size, which is deterministic, not probabilistic. An algorithm exactly solving an optimization problem carries out two tasks; searching and refuting, and we focus on the hardness of the latter refutation process. The average hardness of refutation for another optimization problem was previously conjectured [48, 49], and by fixing the employed algorithm to a specific type, e.g. Sum-of-Squares method, semidefinite-programing method, and resolution-based method, the possibility and impossibility of average hardness of refutation was proven for some constraint satisfaction problems [50–53] and the MIS problem [54, 55]. Following this line, we fix the method of refutation to the linear programming relaxation with cutting planes [56], which is one of the standard and strong methods to solve the MIS problem, and show that refutation is impossible for the constructed specific instances. We first derive a lower bound on possible refutation for the constructed instances, and then show numerically and analytically that the true optimal value for these instances is strictly less than that.

2. Maximum independent set problem and characterization of hardness

We first explain the maximum independent set problem (MIS). For a given graph \( G \), an independendent set is a set of vertices which are not neighboring with each other on the graph (i.e. for any edge at least one of two end point vertices is not included in the set). The task of MIS is to find (one of) the largest independent set(s). For example, given the graph in the left of figure 1, the set of gray vertices in the right figure is one of the largest independent sets. The size of the largest independent set is called the independent number, which we denote by \( N^* \). We define independent ratio as \( N^*/N \), where \( N \) denotes the graph size (i.e. the number of vertices) of the given graph.

In the computational complexity language, the MIS problem is known to be NP-complete for the decision version formulation and NP-hard for the optimization version. The refutation, which we will describe in detail below, in MIS only exists in the optimization version, and therefore we are focusing on the NP-hardness of MIS in
this paper. Both NP-completeness and NP-hardness are very strong evidence for the
MIS problem to be impossible to solve with a polynomial time algorithm. From the
numerical side, simulations show that MIS for Erdős–Renyi random graphs with the
average degree larger than Napier’s constant $2.718\cdots$ is hard to compute efficiently on
average [15, 57, 58]. In other words, even the best known algorithms fail to solve MIS of
a random graph with high probability, if computation time is bounded by a polynomial
of the graph size $N$.

An exact algorithm for MIS should handle the following two tasks.

(i) *Searching*; to find an independent set with size $N^*$.

(ii) *Refuting*; to ensure that the size of all other independent sets are less than or
equal to $N^*$.

When we consider the large size limit, we can relax our result to allow $o(N)$ errors,
that is, the algorithm is regarded as succeeded if it finds an independent set with size
$N^* - o(N)$ and it refutes an independent set with size $N^* + o(N)$. We focus on the hard-
ness of the latter task, refutation. Suppose that an algorithm ensures that no set larger
than $N_{\text{refute}}$ is an independent set. Then, this algorithm succeeds in refutation if
\[
\lim_{N \to \infty} \frac{N_{\text{refute}} - N^*}{N^*} = 0
\]
is satisfied, and it fails to refute if
\[
\lim_{N \to \infty} \frac{N_{\text{refute}} - N^*}{N^*} > 0
\]
is satisfied. The main goal of this paper is to construct a graph sequence such that all
plausible algorithms explained below fail to refute even in the above relaxed sense.

It should be noted that we should not aim for a hardness proof regarding *any* type
of refutation, since that will imply $P \neq NP$, which is believed to be true but proof is cur-
rently out of reach. Thus, to discuss the hardness of computation in as general a way as
possible, we specify the method of refutation. In the next section, we provide a method
of refutation; linear programming relaxation with cutting planes.
3. Linear programming relaxation with cutting planes

We here introduce the method of refutation: linear programming (LP) relaxation with cutting planes [56]. Unlike integer programming, LP (where all arguments run in the real number) is tractable. Based on this fact, LP relaxation loosens the conditions on arguments \( x_i \in \{0, 1\} \) to \( 0 \leq x_i \leq 1 \), and solve this relaxed problem as an approximation or a bound of the original integer programming problem.

We first explain the idea of LP relaxation. We use symbols \( x_i \in \{0, 1\} \) \((i = 0, 1, \ldots, p - 1)\), where \( x_i = 1 \) \((x_i = 0)\) represents that the vertex \( i \) belongs \( (\) does not belong \) to the set. MIS can be expressed as the problem to find

\[
N^* = \max \left[ \sum_i x_i \right]
\]

under the constraints

\[
x_i + x_j \leq 1
\]

for all pairs of \((i, j)\) neighboring in the given graph. The basic idea of LP relaxation is to relax the condition \( x_i \in \{0, 1\} \) to \( 0 \leq x_i \leq 1 \). In other words, the LP problem is an optimization problem to find (3) with the solution space \( 0 \leq x_i \leq 1 \) under the constraint (4). A linear programming problem can be solved efficiently, which means that the relaxed linear problem of MIS with the same constraints (4) is tractable. Let \( x_i^{\text{LP}} \) be the solution (optimal assignment) of the relaxed MIS, and let \( N_{\text{LP}} := \sum_i x_i^{\text{LP}} \). Since \( N^* \leq N_{\text{LP}} \), the above LP relaxation serves as a refutation for any independent number larger than \( N_{\text{LP}} \).

The bound \( N_{\text{LP}} \) can be improved by introducing cutting planes. If the given graph has an odd-length cycle \( i_1, i_2, \ldots, i_{2k+1} \), then we can add the constraints

\[
\sum_{j=1}^{2k+1} x_{i_j} \leq k,
\]

which we call a cutting plane. The LP problem with cutting planes is an optimization problem to find (3) with the solution space \( 0 \leq x_i \leq 1 \) under the constraints (4) and (5). Since the solution (optimal assignment) of the original problem (MIS) satisfies these cutting planes, we confirm that the LP problem with cutting planes is still a relaxed problem of the original MIS. We shall take all cutting planes induced by cycles in the given graph. We note that the graph sequence we will introduce has degree three, so the basic component of the graph besides trees are cycles. Denoting by \( x_i^{\text{LP-CP}} \) the solution (optimal assignment) of the LP problem with all possible cutting planes for cycles, we define

\[
N_{\text{LP-CP}} := \sum_i x_i^{\text{LP-CP}}.
\]

Obviously, \( N_{\text{LP-CP}} \leq N_{\text{LP}} \) holds by construction, and thus the refutation bound \( N^* \leq N_{\text{LP-CP}} \) is stronger than the previous bound, \( N^* \leq N_{\text{LP}} \).

As an example, in figure 2 we consider some cutting planes in the graph introduced in figure 1. The four cutting planes impose
respectively. In this graph, the refutation by LP relaxation reads $N^* \leq N_{LP} = 4$ (the assignment $x_i = 1/2$ for all $i$ satisfies all constraints), which is not a tight upper bound. On the other hand, the refutation by LP relaxation with cutting planes reads $N^* \leq N_{LP-CP} = 3$. Here, $N_{LP-CP} \leq 3$ is directly confirmed by the summation of (7) and (8), and $N_{LP-CP} \geq 3$ comes from the fact that the assignment $x_2 = x_6 = x_7 = 1$ and others to be zero satisfies all constraints. The upper bound $N^* \leq 3$ is tight, which means the success of refutation by LP relaxation with cutting planes in this graph.

In the context of relaxation problems, the ratio between the maximum size of the original problem, $N^*$, and that of the relaxed problem, $N_{LP}$ or $N_{LP-CP}$, is called integrality gap. The integrality gap $N_{LP}/N^*$ or $N_{LP-CP}/N^*$ is always larger than or equal to 1, and an algorithm employing relaxation is regarded as succeeding in refutation if and only if the integrality gap is equal to 1.

4. Construction of the graph sequence

We now construct a graph sequence of hard instances. The graph has $p$ vertices labeled as $\{0, 1, \ldots, p-1\}$ with a prime $p$. Each vertex $x$ is connected to $x \pm 1$ and $-x^{-1}$ (mod $p$). $x^{-1}$ (mod $p$) is uniquely defined as the integer which satisfies $x \cdot x^{-1} \equiv 1$ (mod $p$) when $p$ is prime. The exception is $x = 0$ where we set $0^{-1} = 0$, letting vertex 0 has a self loop. (If $-x^{-1} \equiv x \pm 1 \mod p$, we connect these two vertices with two edges.) We call this graph as inverse graph. The inverse graph with $p = 11$ is depicted in figure 3. This graph turns out to be a well-known example of an expander graph [59]. For a given set of vertices $S$ in a graph, we consider the ratio of the number of edges connecting in and out of $S$ to the number of vertices $|S|$. The expansion ratio of a graph $G$ is the maximum of the above ratio with respect to a set $S$ with $|S| \leq |G|/2$. The expander graphs are graph sequences with large expansion ratios, and thus random walks on them mix rapidly.
We shall show the following relations for the sequence of the inverse graphs:

\[
\lim_{N \to \infty} \frac{N_{LP-CP}}{N} = \frac{1}{2},
\]

\[
\lim_{N \to \infty} \frac{N^*}{N} < \frac{1}{2}.
\]

The first relation (11) shows that the refutation method based on LP relaxation with cutting planes only reproduces a trivial upper bound 1/2 in the large size limit. On the other hand, the last relation (12) shows that the independent ratio is strictly less than 1/2. Combining these relations, we conclude that any algorithm based on LP relaxation with cutting planes cannot solve MIS efficiently (i.e. we need a brute-force type search for refutation, which could take exponentially long time in general).

5. Demonstration of hardness

5.1. Lower bound on refutation obtained by linear programming relaxation with cutting planes

In this subsection, we show that the refutation bound obtained through LP relaxation with cutting planes converges to the trivial bound in the large \( N \) limit:

\[
\lim_{N \to \infty} \frac{N_{LP-CP}}{N} = \frac{1}{2}.
\]

This means that LP relaxation with cutting planes cannot refute the MIS on the inverse graph properly.

We first calculate a lower bound of \( N_{LP-CP} \). Let \( s_i \) be the length of the shortest odd-length cycle which contains the vertex \( i \). (We note that the outer circumferential \( N \) (odd-length) cycle contains all vertices, which guarantees that \( s_i \) is well-defined.) Then, by setting
all constraints including cutting planes are satisfied. Since $N_{\text{LP-CP}}$ is the maximum of\[\sum_i x_i,\]

(14)

A crucial property of the inverse graph is that the number of small odd-length cycles in this graph is rigorously bounded. To explain this, we introduce a symbol sequence to describe a directed path. A single directed jump from $x$ to $x+1$, $x-1$, $-x^{-1}$ is denoted by $+$, $-$, $R$, respectively, and a directed path from a given initial vertex is written as a sequence of symbols \{+$,-,R$\}. For example, a directed path $2 \to 3 \to 7 \to 6 \to 5 \to 4 \to 8$ in figure 3 is expressed as the sequence \[+[+R--R]\] with the initial vertex 2. A cycle can be regarded as a directed path with the same initial and final state $x$. By choosing a proper initial state $x$ and a proper direction, any cycle can be described in the form of \[+[+\cdots R]\] without loss of generality. We refer to such a sequence as cycle sequence.

As an example, let us consider a 5-cycle described by \[[++R-R]\] (see figure 4). By construction, the initial state of this cycle $x$ is the solution of\[\frac{1}{x+2} - 1 \equiv x \mod p.\]

(16)

The left hand side is $(x+2)/(x+3)$, which means that this equation is quadratic and thus it has at most two solutions. This means that the inverse graph contains at most two 5-cycles expressed as \[[++R-R]\]. For any cycle sequence, the corresponding equation has at most two solutions, and hence the cycle described by this cycle sequence appears at most twice in a given inverse graph. The exact number of cycles described by a particular cycle sequence in a given inverse graph could be obtained by calculating the quadratic residue [60]. (For example, (16) is transformed into a quadratic equation $y^2 \equiv 3 \mod p$ with $y = x+2$, which has two solutions for $p \equiv 1, 11 \mod 12$ and no solution for $p \equiv 5, 7 \mod 12$. See also appendix)

We now evaluate the upper bound of the number of short odd-length cycles. Noting that the pairs $++, --$ and $RR$ do not appear in cycle sequences, the number of cycle sequences \[+[+\cdots R]\] with length $2k+1$ is bounded above by $2^{2k-1}$. This directly implies that $2k+1$ cycles appear in the inverse graph for any $p$ at most $2 \cdot 2^{2k-1} = 2^{2k}$ times. Hence, in any graph, the number of vertices contained by odd-length cycles with length less than $2k'$ is bounded above by a constant, $a(k') := \sum_{k=1}^{k'-1} (2k+1)2^{2k}$, which is independent of $p$. In other words, short odd-length cycles cover only a small fraction of vertices for large $p$.

Recalling the fact that the number of cycles with length $2k+1$ is at most $2^{2k}$ and the function $(s-1)/2s$ is monotonically increasing with respect to $s$, the right-hand side of (15) is bounded below by
for any $k'$. For a given $\epsilon > 0$, we define $k'$ as

$$k' \geq \frac{1}{2} \left( \frac{1}{\epsilon} - 1 \right),$$

which is equivalent to

$$\frac{k'}{2k' + 1} \geq \frac{1}{2} - \frac{\epsilon}{2}.$$  

(19)

We also take sufficiently large $N$ as

$$N = p \geq p' := a(k') + \frac{a(k') - 2b(k') + 2}{\epsilon}$$

(20)

with $b(k') := \sum_{k=1}^{k'-1} k2^{2k}$, which directly implies

$$b(k') \geq \frac{a(k') - \epsilon(N - a(k'))}{2} + 1.$$  

(21)

Then, we have the bound for $N_{\text{LP-CP}}$:

$$N_{\text{LP-CP}} \geq \sum_{k=1}^{k'-1} (2k + 1)2^{2k} \frac{k}{2k + 1} + (N - a(k')) \frac{k'}{2k' + 1}$$

$$= b(k') + k' \cdot \frac{N - a(k')}{2k' + 1}$$

$$\geq \frac{N}{2} - \varepsilon N + \varepsilon a(k') + 1$$

$$\geq N \left( \frac{1}{2} - \varepsilon \right).$$  

(22)
Since $\varepsilon$ is arbitrary and $N_{\text{LP-CP}}/N \leq 1/2$, we have (13).

5.2. Upper bound on independent ratio

We next show two arguments, one analytical and the other numerical, that the true independent ratio is strictly less than half. First, we exactly compute the independent ratio of the inverse graph up to $p = 311$, using a refined brute force search algorithm [58]. We remark that the computation time by this algorithm increases exponentially with the size $p$. The obtained results are shown in figure 5, where the independent ratio is plotted against the system size $N = p$. The plot suggests that although the independent ratio fluctuates, it converges to a value around 0.46, which is strictly less than half.

We provide another analytic argument supporting our claim. Let $A$ be the $N \times N$ normalized adjacency matrix of a $d$-regular graph, where $A_{ij} = 1/d$ if there is an edge between the vertices $i$ and $j$ in the graph and $A_{ij} = 0$ otherwise. We set $A_{ii} = 0$ except $i = 0$, where we set $A_{00} = 1/3$ to reflect the existence of the self loop. We denote the eigenvalues of $A$ with decreasing order by $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$. If the graph is $d$-regular, it is known that $\lambda_1 = 1$, $\lambda_N \geq -1$ and the equality holds if and only if the graph is bipartite [61]. In addition, the independent ratio of a $d$-regular graph is bounded above by the smallest eigenvalue, which is called Hoffman’s bound [61]:

$$\frac{N^*}{N} \leq \frac{-\lambda_N}{1 - \lambda_N}. \quad (23)$$

(We note that although the inverse graph has a self loop, we can easily extend Hoffman’s bound to such graphs, which is demonstrated in appendix B.) Thus, obtaining a good lower bound of $\lambda_N$, we have a good bound of the independent ratio. It is noteworthy that the second largest eigenvalue in the absolute sense $\lambda := \max(\lambda_2, -\lambda_N)$ characterizes the speed of mixing through random walks on the graph. The larger the gap $1 - \lambda$ is, the quicker the probability distribution equilibrates. For example, a review paper on

Figure 5. Exactly computed independent ratio for the inverse graph from $p = 11$ to $p = 311$. Two dotted lines show the average value of the data, either using all of it or only the latter half. Both of the error bars do not exceed 0.48, and becomes smaller for the latter half, which strongly suggests a convergence to a value strictly less than 0.5.
the expander graph [59] shows that the inverse graph satisfies $\lambda < 1 - 10^{-4}$ for large
$N$. This relation suggests that the independent ratio for sufficiently large $N$ is strictly
less than half:

$$\frac{N^*}{N} \leq 0.499975 < 0.5.$$  \hspace{1cm} (24)

While a tighter bound of $\lambda_N$ should give us a better bound on the independent ratio,
this already suffices for our argument.

6. Discussion

We explicitly constructed hard instances (an infinite sequence of graphs) of the maxi-
mum independent set problem (MIS). For this graph, the linear programming relax-
ation with cutting planes only provides the upper bound of the independent ratio as
$1/2$, while the true independent ratio is strictly less than $1/2$. This difference implies
that the hardness stems from not local but global structures of the graph. To our best
knowledge, this is the first explicit deterministic construction of a hard instance in
optimization problems.

We here remark that although we specify the method of refutation to LP relax-
ation with cutting planes, the hardness result appears to apply to other algorithms. In
fact, for the case of random graphs some other well-known algorithms including belief
propagation and leaf removal fail to solve the MIS at the same point as that for the LP
relaxation (without cutting planes) [57, 62]. Presuming from this fact, we expect that
other algorithms also fail to solve the MIS for the inverse graph.

It is noteworthy that the inverse graph shares various properties with $K$-regular
random graphs with $K \geq 3$, which are considered to be typically hard for MIS because
it is in the replica-symmetry-breaking (RSB) phase [27]. For instance, it is known that
regular random graphs are expander graphs [59] and have few short cycles [63] with
high probability. The expected independent ratio of 3-regular random graphs is almost
surely larger than $6\ln(2/3) - 2 \simeq 0.4328$ [64, 65] and smaller than 0.458 [66], which is
close to the numerical result of the inverse graph, which is also almost 3-regular. These
facts lead us to anticipate that the introduced inverse graph shares the typical prop-
erties of random graphs, which are hard instances of MIS. The Erdős–Renyi random
graph for average degree larger than Napier’s constant $e$ is known to be in the RSB
phase for the cutting-plane method [56], and the complex energy landscape of the RSB
phase gives us an intuitive reason why the problem is hard. We can expect that the
inverse graph is effectively in the RSB phase, similarly to a random 3-regular graph.

It is reasonable to expect that some other expander graphs which have explicit
constructions [59] are also concrete typical hard instances. Recent studies on computa-
tional hardness from the viewpoint of statistical mechanics have paid much attention
to the connection between the energy landscape of the solution space and the hardness
of problems [24, 25, 28–30, 34], which also resulted in inspiring efficient algorithms
[67–71]. Furthermore, a concrete example of a hard instance will help our investi-
gation of the deep structure of computational hardness and serve as a benchmark for
analytical evaluation of algorithms. Some examples of promising research directions based on our results are to discover the hidden global structure causing computational hardness, and to analyze the replica symmetry breaking in systems without quenched disorder (randomness). These studies should lead to further understanding of various phenomena beyond randomized models.

Acknowledgments

We thank Koji Hukushima, Yoshiyuki Kabashima, Tomoyuki Obuchi, and Satoshi Takabe for fruitful discussions. NS was supported by JSPS Grants-in-Aid for Scientific Research Grant No. JP19K14615.

Appendix A. Table of presence or absence of short cycles with odd length

The table A1 shows which type of cycle appears in particular inverse graphs. The table is read as follows. For example, the number of the 7-cycle described by the cycle sequence [+++ + + + R] is equal to the number of solutions of the equation $y^2 \equiv 2 \mod p$, which is two if $p \equiv 1, 7 \mod 8$ and is none if $p \equiv 3, 5 \mod 8$. In contrast, the 7-cycle described by the cycle sequence [+++ + R + R] always exists uniquely, and the initial vertex of this sequence is always $x = -2$. Here, the equation corresponding to this sequence as (16) is not a quadratic equation but a simple first-degree polynomial equation. In some cases, this equation has no solution for any $p$, which occurs, for example, for the 7-cycle described by the cycle sequence [+++ R + R – R].

In this table, we leave some columns for quadratic residues of composite numbers blank, because the conditions for the solutions to have two/no solutions are relatively complicated. The explicit conditions for those cases could be obtained in the following way.

We here briefly explain a mathematical background behind this calculation. We first introduce the Legendre’s symbol for a prime $p$ and an integer $a$ which are relatively prime:

$$\left( \frac{a}{p} \right) := \begin{cases} 1 & : y^2 \equiv a \mod p \text{ has two solutions} \\ -1 & : y^2 \equiv a \mod p \text{ has no solution.} \end{cases} \quad (A.1)$$

The Legendre’s symbol satisfies the following relation

$$\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right), \quad (A.2)$$

which could be used to calculate the conditions of composite quadratic residues having two/no solutions. This relation says that $y^2 \equiv ab \mod p$ has two solutions if and only if (i) both $y^2 \equiv a \mod p$ and $y^2 \equiv b \mod p$ have two solutions, or (ii) both $y^2 \equiv a \mod p$ and $y^2 \equiv b \mod p$ have no solution. For example, $y^2 \equiv 15 \mod p$ has two solutions if and only if (i) both $p \equiv 1, 11 \mod 12$ and $p \equiv 1, 4 \mod 5$ hold, or (ii) both $p \equiv 5, 7 \mod 12$ and $p \equiv 2, 3 \mod 5$ hold.

To calculate the quadratic residue of primes, we employ the quadratic reciprocity
### Constructing concrete hard instances of the maximum independent set problem

Table A1. A table of possible odd-length cycles with length up to 9. In the others column, we use the following abbreviation: A: \( x = -1 \) is a unique solution for any \( p \). B: \( x = -2 \) is a unique solution for any \( p \). N: no solution for any \( p \).

| Length | Sequence | Equation | Two solutions | No solution | Others |
|--------|----------|----------|---------------|-------------|--------|
| 3      | ++R      | \( y^2 \equiv 3 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) | A      |
|        | +++ + R  | \( y^2 \equiv -1 \mod p \) | \( p \equiv 1 \mod 4 \) | \( p \equiv 3 \mod 4 \) |        |
| 5      | +++R - R | \( y^2 \equiv 3 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++R + R | \( y^2 \equiv 2 \mod p \) | \( p \equiv 1, 7 \mod 8 \) | \( p \equiv 3, 5 \mod 8 \) |        |
| 7      | +++ + R + R | \( y^2 \equiv 15 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + R - R | \( y^2 \equiv 1 \mod 4 \) | \( p \equiv 3 \mod 4 \) | \( N \) |        |
|        | +++ + R + + R | \( y^2 \equiv 3 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) | \( N \) |
|        | +++ + R - - R | \( y^2 \equiv 3 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) | \( N \) |
| 9      | +++ + +++ + R | \( y^2 \equiv 15 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 1 \mod 4 \) | \( p \equiv 3 \mod 4 \) | \( N \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 6 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 2 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 6 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 2 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |
|        | +++ + +++ + R | \( y^2 \equiv 6 \mod p \) | \( p \equiv 1, 11 \mod 12 \) | \( p \equiv 5, 7 \mod 12 \) |        |

https://doi.org/10.1088/1742-5468/ab409d
and the following two supplementary laws
\[
\begin{align*}
\left( \frac{-1}{p} \right) &= (-1)^{\frac{p-1}{2}}, \quad \text{(A.4)} \\
\left( \frac{2}{p} \right) &= (-1)^{\frac{p^2-1}{8}}.
\end{align*}
\]

We list the conditions for quadratic residues of small primes and the special case \(-1\) below.

| Quadratic equation | Two solutions | No solution |
|--------------------|--------------|-------------|
| \(y^2 \equiv -1 \mod p\) | \(p \equiv 1 \mod 4\) | \(p \equiv 3 \mod 4\) |
| \(y^2 \equiv 2 \mod p\) | \(p \equiv 1, 7 \mod 8\) | \(p \equiv 3, 5 \mod 8\) |
| \(y^2 \equiv 3 \mod p\) | \(p \equiv 1, 11 \mod 12\) | \(p \equiv 5, 7 \mod 12\) |
| \(y^2 \equiv 5 \mod p\) | \(p \equiv 1, 4 \mod 5\) | \(p \equiv 2, 3 \mod 5\) |
| \(y^2 \equiv 7 \mod p\) | \(p \equiv 1, 3, 9, 19, 25, 27 \mod 28\) | \(p \equiv 5, 11, 13, 15, 17, 23 \mod 28\) |

**Appendix B. Hoffman’s bound for graphs with a self loop**

In the main part, we derive the bound on independent number by applying Hoffman’s bound. However, the original version of Hoffman’s bound applies only to regular graphs without self loop, while the inverse graph has a single self loop, which implies that our derivation is not fully justified. In this appendix, by following the proof of Hoffman’s bound in detail [61] we extend it to graphs with a single loop and complete our proof of the upper bound of the independent number.

We start from a theorem on matrices. Consider a \(2 \times 2\) block matrix
\[
X := \begin{pmatrix} X^{[1,1]} & X^{[1,2]} \\ X^{[2,1]} & X^{[2,2]} \end{pmatrix},
\]
where two diagonal block matrices \(X^{[1,1]}\) and \(X^{[2,2]}\) are respectively \(n \times n\) and \(m \times m\) square matrices. We also introduce the quotient matrix of \(X\) defined as
\[
C := \begin{pmatrix} \frac{1}{n} \sum_{i=1}^{n} \sum_{j=1}^{n} X_{i,j}^{[1,1]} & \frac{1}{n} \sum_{i=1}^{n} \sum_{j=1}^{m} X_{i,j}^{[1,2]} \\ \frac{1}{m} \sum_{i=1}^{m} \sum_{j=1}^{n} X_{i,j}^{[2,1]} & \frac{1}{m} \sum_{i=1}^{m} \sum_{j=1}^{m} X_{i,j}^{[2,2]} \end{pmatrix},
\]
where \(X_{i,j}^{[1,1]}\) represents the \((i, j)\)-component of the matrix \(X^{[1,1]}\), and \(X_{i,j}^{[1,2]}\), \(X_{i,j}^{[2,1]}\), and \(X_{i,j}^{[2,2]}\) are defined in a similar manner. Let \(\eta_1 \geq \eta_2 \geq \cdots \geq \eta_{n+m}\) be eigenvalues of \(X\) in descending order, and \(\theta_1 \geq \theta_2\) be two eigenvalues of \(C\). Then, the interlacing technique, or the Higman–Sims technique, suggests that if \(X\) is symmetric, then the following inequality is satisfied [61]:

\[\text{https://doi.org/10.1088/1742-5468/ab409d}\]
\[ \eta_1 \geq \theta_1 \geq \theta_2 \geq \eta_{n+m}. \quad (B.3) \]

This inequality serves as our starting point.

We now go back to our original problem. Let \( G \) be the inverse graph (with a self loop) with size \( N \) and \( L \) be one of the largest independent set of this graph. The size of \( L \) is denoted by \( N^* = |L| \). We reorder the label of vertices such that the vertices in \( L \) have labels in \( 1 \leq i \leq N^* \) and those not in \( L \) have labels in \( N^* + 1 \leq i \leq N \). We set \( X \) the normalized adjacency matrix of the inverse graph (with a self loop), and set \( n = N^* \), \( m = N - N^* \). Note that the vertex with a self loop has a reordered label larger than \( n = N^* \) because any independent set does not contain vertices with self loops. Then, the quotient matrix of \( X \) becomes

\[ C = \begin{pmatrix} 0 & \frac{N^*}{N - N^*} & 1 \\ \frac{N^*}{N - N^*} & 1 - \frac{N^*}{N - N^*} & \frac{1}{3(N - N^*)} \end{pmatrix}. \quad (B.4) \]

Here, if the graph is fully 3-regular without self loop, then the \((2,2)\)-component of \( C \) is replaced to \( 1 - \frac{N^*}{N - N^*} \) (the third term is removed).

The smaller eigenvalue of \( C \) is

\[ \theta_2 = \frac{1}{2} \left[ 1 - \frac{N^*}{N - N^*} - \frac{1}{3(N - N^*)} \right. \]
\[ \left. - \sqrt{\left( 1 - \frac{N^*}{N - N^*} - \frac{1}{3(N - N^*)} \right)^2 + 4 \frac{N^*}{N - N^*}} \right], \quad (B.5) \]

while we know that the minimum eigenvalue of \( X \) is strictly larger than \(-1\):

\[ \eta_N \geq -1 + x \quad (B.6) \]

with \( x \geq 10^{-4} \) [59]. The inequality \( \theta_2 \geq \eta_N \) introduced in (B.3) reads

\[ \frac{N^*}{N} \leq 1 - \frac{1}{2 - x - \frac{1}{3(2-x)(N-N^*)}} \leq 1 - \frac{1}{2 - x} < 0.499975 < 0.5, \quad (B.7) \]

which is the desired result.

References

[1] Arora S and Barak B 2009 Computational Complexity: a Modern Approach (Cambridge: Cambridge University Press)
[2] Bogdanov A and Trevisan L 2006 Average-case complexity Found. Treat Theor. Comput. Sci. 2 1
[3] Lipton R J 1989 New directions in testing Distrib. Comput. Cryptogr. 2 191
[4] Ajtai M 1996 Generating hard instances of lattice problems Proc. of the 28th Annual ACM Symp. on Theory of Computing p 99
[5] Regev O 2009 On lattices, learning with errors, random linear codes, and cryptography J. ACM 56 34
[6] Daniely A, Linial N and Shalev-Shwartz S 2014 From average case complexity to improper learning complexity Proc. of the 46th Annual ACM Symp. on Theory of Computing p 441
[7] Wang T, Berthet Q and Plan Y 2016 Average-case hardness of RIP certification (arXiv:1605.09646)
[8] Mézard M and Parisi G 1985 Replicas and optimization J. Phys. Lett. 46 771–8
[9] Mézard M and Parisi G 1986 A replica analysis of the travelling salesman problem J. Phys. France 47 1285–96

https://doi.org/10.1088/1742-5468/ab409d
Constructing concrete hard instances of the maximum independent set problem

[10] Fu Y and Anderson P W 1986 Application of statistical mechanics to NP-complete problems in combinatorial optimisation J. Phys. A: Math. Gen. 19 1605
[11] Cheeseman P C, Kanefsky B and Taylor W M 1991 Where the really hard problems are JICAI 91 331
[12] Mitchell D, Selman B and Levesque H 1992 Hard and easy distributions of SAT problems AAAI 92 459
[13] Kirkpatrick S and Selman B 1994 Critical behavior in the satisfiability of random boolean expressions Science 264 1297
[14] Monasson R, Zecchina R, Kirkpatrick S, Selman B and Troyansky L 1999 Determining computational complexity from characteristic ‘phase transitions’ Nature 400 133
[15] Weigt M and Hartmann A K 2000 Number of guards needed by a museum: a phase transition in vertex covering of random graphs Phys. Rev. Lett. 84 6118
[16] Hartmann A K and Weigt M 2005 Phase Transitions in Combinatorial Optimization Problems: Basics, Algorithms and Statistical Mechanics (New York: Wiley)
[17] Friedgut E 1999 Sharp thresholds of graph properties, and the k-sat problem J. Am. Math. Soc. 12 1017
[18] Achlioptas D and Peres Y 2004 The threshold for random k-SAT is 2k log 2 – O(k) J. Am. Math. Soc. 17 947
[19] Achlioptas D, Naor A and Peres Y 2005 Rigorous location of phase transitions in hard optimization problems Nature 435 759
[20] Ding J, Sly A and Sun N 2015 Proof of the satisfiability conjecture for large k Proc. of the 47th annual ACM Symp. on Theory of Computing p 59
[21] Monasson R and Zecchina R 1997 Statistical mechanics of the random K-satisfiability model Phys. Rev. E 56 1357
[22] Ricci-Tersenghi F, Weigt M and Zecchina R 2001 Simplest random K-satisfiability problem Phys. Rev. E 63 026702
[23] Zhou H 2005 Long-range frustration in a spin-glass model of the vertex-cover problem Phys. Rev. Lett. 94 217203
[24] Krzakala F, Montanari A, Ricci-Tersenghi F, Semerjian G and Zdeborová L 2007 Gibbs states and the set of solutions of random constraint satisfaction problems Proc. Natl Acad. Sci. 104 10318
[25] Zdeborová L and Krzakala F 2007 Phase transitions in the coloring of random graphs Phys. Rev. E 76 031131
[26] Li K, Ma H and Zhou H 2009 From one solution of a 3-satisfiability formula to a solution cluster: Frozen variables and entropy Phys. Rev. E 79 031102
[27] Zhang P, Zeng Y and Zhou H 2009 Stability analysis on the finite-temperature replica-symmetric and first-step replica-symmetry-broken cavity solutions of the random vertex cover problem Phys. Rev. E 80 021122
[28] Zdeborová L 2009 Statistical physics of hard optimization problems Acta Phys. Slovaca 59 169
[29] Zdeborová L and Krzakala F 2010 Generalization of the cavity method for adiabatic evolution of Gibbs states Phys. Rev. B 81 224205
[30] Braunstein A, Dall’Asta L, Semerjian G and Zdeborová L 2016 The large deviations of the whitening process in random constraint satisfaction problems J. Stat. Mech. P053401
[31] Mézard M and Montanari A 2009 Information, Physics, and Computation (Oxford: Oxford University Press)
[32] Mézard M, Mora T and Zecchina R 2005 Clustering of solutions in the random satisfiability problem Phys. Rev. Lett. 94 197205
[33] Achlioptas D and Ricci-Tersenghi F 2006 On the solution-space geometry of random constraint satisfaction problems Proc. ACM 2006 130
[34] Achlioptas D and Coja-Oghlan A 2008 Algorithmic barriers from phase transitions Found. Comput. Sci. 2008 793
[35] Bayati M, Gamarnik D and Tetali P 2010 Combinatorial approach to the interpolation method and scaling limits in sparse random graphs Proc. of the 42nd ACM Symp. p 105
[36] Coja-Oghlan A and Efthymiou C 2015 On independent sets in random graphs Random Struct. Algorithms 43 476
[37] Gamarnik D and Sudan M 2017 Limits of local algorithms over sparse random graphs Ann. Probab. 45 2353–76
[38] Diestel R 1997 Graph Theory (Berlin: Springer)
[39] Alon N and Spencer J H 2008 The Probabilistic Method (New York: Wiley)
[40] Horie A and Watanabe O 1997 Hard instance generation for SAT Int. Symp. on Algorithms and Computation (Berlin: Springer)
[41] Barthel W, Hartmann A K, Leone M, Ricci-Tersenghi F, Weigt M and Zecchina R 2002 Hiding solutions in random satisfiability problems: a statistical mechanics approach Phys. Rev. Lett. 88 188701
[42] Xu K, Boussemart F, Henery F and Lecoutre C 2007 Random constraint satisfaction: Easy generation of hard (satisfiable) instances Artif. Intell. 171 514

https://doi.org/10.1088/1742-5468/ab409d
[43] Jia H, Moore C and Strain D 2007 Generating hard satisfiable formulas by hiding solutions deceptively J. Artif. Intel. Res. 28 107
[44] Hen I, Job J, Albash T, Rønnow T F, Troyer M and Lidar D A 2015 Probing for quantum speedup in spin-glass problems with planted solutions Phys. Rev. A 92 042325
[45] Katzgraber H G, Hamze F, Zhu Z, Ochoa A J and Munoz-Bauza H 2015 Seeking quantum speedup through spin glasses: the good, the bad, and the ugly Phys. Rev. X 5 031026
[46] Marshall J, Martin-Mayor V and Hen I 2016 Practical engineering of hard spin-glass instances Phys. Rev. A 94 012320
[47] Takabe S, Hukushima K and Hartmann A K 2018 Large-deviation properties of linear-programming computational hardness of the vertex cover problem (arXiv:1802.02550)
[48] Feige U 2002 Relations between average case complexity and approximation complexity Proc. of the 34th Annual ACM Symp. on Theory of Computing p 534
[49] Alekhnovich M 2011 More on average case versus approximation complexity Comput. Complexity 20 755
[50] Barak B and Moitra A 2015 Tensor prediction, rademacher complexity and random 3-XOR CoRR (arXiv:1501.06521)
[51] Allen S R, O’Donnell R and Witmer D 2015 How to refute a random CSP IEEE 56th Annual Symp. Foundations of Computer Science p 689
[52] Kothari P K, Mori R, O’Donnell R and Witmer D 2017 Sum of squares lower bounds for refuting any CSP (arXiv:1701.04521)
[53] Deshpande Y, Montanari A, O’Donnell R, Schramm T and Sen S 2018 The threshold for SDP-refutation of random regular NAE-3SAT (arXiv:1804.05230)
[54] Chvátal V 1977 Determining the stability number of a graph SIAM J. Comput. 6 643
[55] Beame P, Impagliazzo R and Sabharwal A 2007 The resolution complexity of independent sets and vertex covers in random graphs Comput. Complex 16 245
[56] Dewenter T and Hartmann A K 2012 Phase transition for cutting-plane approach to vertex-cover problem Phys. Rev. E 86 041128
[57] Takabe S and Hukushima K 2014 Typical behavior of the linear programming method for combinatorial optimization problems: a statistical-mechanical perspective J. Phys. Soc. Japan 83 043801
[58] Takahashi J, Takabe S and Hukushima K 2017 An exact algorithm exhibiting RS-RSB/Easy-Hard correspondence for the maximum independent set problem J. Phys. Soc. Japan 86 073001
[59] Hoory S, Linial N and Wigderson A 2006 Expander graphs and their applications Bull. Am. Math. Soc. 43 439
[60] Coppel W A 2006 Number Theory: an Introduction to Mathematics (Berlin: Springer)
[61] Brouwer A E and Haemers W H 2012 Spectra of Graphs (New York: Springer)
[62] Takabe S and Hukushima K 2016 Typical performance of approximation algorithms for NP-hard problems J. Stat. Mech. 113401
[63] Wormald N C 1981 The asymptotic distribution of short cycles in random regular graphs J. Comb. Theory B 31 168
[64] Frieze A and Suen S 1994 On the independence number of random cubic graphs Random Struct. Algorithms 5 649
[65] Wormald N C 1995 Differential equations for random processes and random graphs Ann. Appl. Prob. 5 1217
[66] Dall’Astana L, Pin P and Ramezanpour A 2005 Statistical mechanics of maximal independent sets Phys. Rev. E 80 061136
[67] Mézard M, Parisi G and Zecchina R 2002 Analytic and algorithmic solution of random satisfiability problems Science 297 812
[68] Mézard M and Zecchina R 2002 Random K-satisfiability problem: from an analytic solution to an efficient algorithm Phys. Rev. E 66 056126
[69] Montanari A, Ricci-Tersenghi F and Semerjian G 2007 Solving constraint satisfaction problems through belief propagation-guided decimation (arXiv:0709.1667) (Proc. of the 45th Allerton Conf. p 352)
[70] Marino R, Parisi G and Ricci-Tersenghi F 2016 The backtracking survey propagation algorithm for solving random K-SAT problems Nat. Commun. 7 12996
[71] Baldassi C, Borgs C, Chayes J T, Ingrosso A, Lucibello C, Saglietti L and Zecchina R 2016 Unreasonable effectiveness of learning neural networks: From accessible states and robust ensembles to basic algorithmic schemes Proc. Natl Acad. Sci. 113 E7655

https://doi.org/10.1088/1742-5468/ab409d