Resolution Complexity of Random Constraint Satisfaction Problems: Another Half of the Story

Yong Gao, Joseph Culberson

Department of Computing Science, University of Alberta, Edmonton, Alberta, Canada, T6G 2E8

Abstract

Let $C_{n,m}^{2,k,t}$ be a random constraint satisfaction problem (CSP) on $n$ binary variables, where $m$ constraints are selected uniformly at random from all the possible $k$-ary constraints each of which contains exactly $t$ tuples of the values as its restrictions. We establish an upper bound on the constraint tightness threshold for $C_{n,m}^{2,k,t}$ to have an exponential resolution complexity. The upper bound partly answers the open problem regarding the CSP resolution complexity with the tightness between the existing upper and lower bounds [1].

1 Introduction

Phase transitions and threshold phenomena in NP complete problems have been extensively investigated. Many problems such as propositional satisfiability (SAT), graph coloring, and the constraint satisfaction problem (CSP), have been shown to have a solubility threshold under various random models. Over the past ten years, much attention has been paid to the identification of the exact value of the threshold and/or the upper and lower bounds for the threshold [2–4]. Recently, research interest started to switch to analytical investigation of the links between the solubility threshold phenomena and the algorithmic complexity of solving these NP complete problems.

In the study of the phase transitions of CSPs, many natural random models have been proposed, but not all of them exhibit a threshold. A detailed

Email addresses: ygao@cs.ualberta.ca (Yong Gao), joe@cs.ualberta.ca (Joseph Culberson).
discussion on the random CSP models and their limitations can be found in [5–7].

In this paper, we consider $C_{n,m}^{2,k,t}$, a random CSP model defined on $n$ binary variables, where $m$ constraints are selected uniformly at random from all the possible $k$-ary constraints each of which excludes exactly $t$ tuples of the values. In [6], it is shown that for any $t \geq 2^{k-1}$ and $m > 0$ such that $\frac{m}{n} = c$ is constant, $C_{n,m}^{2,k,t}$ is flawed in the sense that it is almost always trivially unsatisfiable and can be checked in linear time. In [1], Mitchell shows that for $0 < t < k - 1$, the resolution complexity of $C_{n,m}^{2,k,t}$ is almost surely exponential. A similar exponential complexity result has also been established in [8] under a different random CSP model. The main result of this paper is a set of tightness upper bounds for the threshold of an exponential complexity of $C_{n,m}^{2,k,t}$. These upper bounds partly answer the open problem regarding the CSP resolution complexity where the constraint tightness is between the existing upper and lower bounds [1,6].

In the study of the resolution complexity of SAT, there has been much interest in the necessary clause density at which unsatisfiable SAT instances can be recognized polynomially [9,10]. Currently, the best result shows that there are polynomial algorithms to certify unsatisfiable random $k$-SAT instances with at least $n^{k/2+o(1)}$ clauses [10]. Since a CSP on binary variables is naturally equivalent to a SAT problem, our result shows that $C_{n,m}^{2,k,t}$ is an alternative random SAT model in which instances with $O(n)$ clauses can be recognized as unsatisfiable polynomially.

The rest of the paper is organized as follows. In the next section, we introduce basic concepts related to CSPs, their random models, and the resolution complexity. In Section 3, we present our results together with some discussion. Section 4 is devoted to the proof of the results.

2 Preliminaries

Throughout this paper, we consider CSPs defined on variables each of which has $\mathcal{D} = \{0, 1\}$ as its domain. A k-ary relation over $\mathcal{D}$ is a map $R : \mathcal{D}^k \rightarrow \{0, 1\}$.

A CSP $C$ consists of a set of binary variables $X = \{x_1, \ldots, x_n\}$ and a set of constraints $(C_1, \ldots, C_m)$. A constraint $C$ of arity $k$ is specified by its constraint scope, a subset of $k$ variables $x$, and a $k$-ary relation $R_C$. Each tuple $a_C \in R_C^{-1}(0) \subset \mathcal{D}^k$ is called a restriction of the constraint. The set $R_C^{-1}(0)$, called the restriction set of the constraint, contains all the tuples that are not compatible with the scope variables of the constraint. A restriction is also called a nogood. We will call $|R_C^{-1}(0)|$ the constraint tightness of the constraint $C$. Associated
with a CSP is a constraint hypergraph with its vertices corresponding to the set of variables and its edges corresponding to the set of constraint scopes.

An assignment to the variables \( X = \{x_1, \cdots, x_n\} \) is a solution to the CSP if it satisfies all the relations associated with the set of constraints. A CSP is called satisfiable if there is at least one satisfying assignment. Throughout the rest of the paper, we assume that all the constraints of a CSP have the same scope size, and use the following notation:

1. \( n \), the number of variables;
2. \( m \), the number of constraints;
3. \( k \), the size of the constraint scope;
4. \( c = \frac{m}{n} \), the constraint density; and
5. \( t \), the constraint tightness of a constraint.

Consequently, the constraint hypergraph will always be \( k \)-uniform.

**Definition 1 (Random CSPs)** Let \( 0 < t < 2^k \) be an integer. In the random CSP model \( C_{n,m}^{2,k,t} \), a random CSP instance is constructed by first selecting a collection of \( m \) constraint scopes uniformly at random without replacement from the set of all the size-\( k \) subsets of variables, and then independently for each constraint scope, choosing a relation \( R \) over the scope variables uniformly from all the possible \( \left( \binom{2^k}{2} \right) \) relations.

The random CSP model \( C_{n,m}^{2,k,t} \) can be generalized to allow for a non-integer tightness \( t \) as follows. For an integer \( t \), the constraints are constructed as usual. For a non-integer \( t = t_0 + \alpha \), where \( t_0 \) is an integer and \( 0 < \alpha < 1 \), a constraint is constructed by selecting a random set of restrictions of size \( t_0 \) with probability \( 1 - \alpha \) and a random set of restrictions of size \( t_0 + 1 \) with probability \( \alpha \).

A resolution refutation for a CNF formula \( F \) is a sequence of clauses \( F_1, \cdots, F_s \) such that

1. each \( F_i \) is either a clause from \( F \) or a resolvent of two clauses preceding it; and
2. \( F_s \) is the empty clause.

The resolution complexity of an unsatisfiable CNF formula is the minimum number of clauses in any resolution refutation. The C-Res complexity of a CSP is defined to be the resolution complexity of an equivalent CNF encoding of the CSP ([1]). For CSPs on binary variables, the equivalent CNF encoding is straightforward since each constraint with a tightness \( t \) is equivalent to \( t \) CNF clauses defined on the same set of variables.
3 Main Results

In this section, we present our main results together with some discussions.

**Theorem 1** Let $C_{n,m}^{2,k,t}$ be a random CSP. Then, we have

$$\lim_{n \to \infty} \Pr\{C_{n,m}^{2,k,t} \text{ is satisfiable} \} = 0$$

if $c = \frac{m}{n}$ and $t$ satisfy one of the following

1. For $t = 2^{k-2} - 1 + \alpha$ with $0 < \alpha \leq 1$,

   $$c > \frac{\binom{2^k}{2^{k-2}}}{2k(k-1)\alpha};$$

2. For $t = 2^{k-2} + j + \alpha$ with $0 < \alpha \leq 1$ and $0 \leq j \leq 2^{k-1} - 2^{k-2} - 1$,

   $$c > \frac{1}{2k(k-1)} \left( \frac{\binom{2^k}{2^{k-2}}}{\binom{2^k}{2^{k-2}+j}} \right) (1 + \alpha \frac{2^{k-2}}{j+1})^{-1}.$$

The theorem is proved by showing that for any constraint tightness $t$ and constraint density $c$ satisfying (1) or (2), a random instance of $C_{n,m}^{2,k,t}$ asymptotically almost surely implies an unsatisfiable 2-SAT subproblem. The intuition is that a constraint $C$ with $t$ restrictions is equivalent to a $k$-CNF formula with $t$ clauses defined on exactly $k$ variables. If $t > 2^{k-2}$, there is a non-zero probability that these $t$ clauses imply a 2-clause. As a result, if there are enough constraints, we will get enough implied 2-clauses to form an unsatisfiable 2-CNF formula in a form called the criss-cross loop \(^1\). In fact, this situation has been shown to be true in a different context where the so-called NK landscape model is analyzed ([13]). An NK landscape defined on a set of $n$ variables can be viewed as a special random CSP consisting of exactly $n$ constraints \{\(C_1, \ldots, C_n\)\} such that for each $1 \leq i \leq n$, the constraint $C_i$ is defined on the variable $x_i$ and $(k - 1)$ other randomly selected variables.

Consider a constraint $C_i$, $1 \leq i \leq m$, of $C_{n,m}^{2,k,t}$. Let $C_i, |C_i| = t$, be the set of k-clauses that is equivalent to $C_i$ and let $F_i$ be the set of all the 2-clauses that can be derived from $C_i$. The proof of Theorem 1 indicates that the set of 2-clauses \{\(F_i, 1 \leq i \leq M = O(m)\)\} is unsatisfiable. Since the resolution complexity of an unsatisfiable 2-SAT problem is polynomial, we have

\(^1\) It should be noted that the implied 2-CNF clauses are not uniformly distributed and the resulting 2-CNF formula is not equivalent to a standard random 2-SAT. Consequently, the current result does not follow from the proof of the satisfiability threshold of the standard random 2-SAT [11,12].
Theorem 2 For any $t$ and $c = \frac{m}{n}$ satisfying the conditions in Theorem 1, the resolution complexity of $C_{n,m}^{2,k,t}$ is almost surely polynomial and a polynomial refutation can be obtained in polynomial time.

PROOF. The set of 2-clauses $F_i$ can be derived from the set of $k$-clauses $C_i$ as follows:

1. Let $D = C_i$;
2. Resolve all the pairs of clauses of the form $\{A, x\}$ and $\{A, \overline{x}\}$ in $D$, where $A$ is a clause of size larger than 2. Insert all the resolvents into $D$ and repeat this step until there are no more pairs of clauses in $D$ that can be resolved in this way.
3. Let $F_i$ be the set of all the 2-clauses in $D$.

Since the number of constraints is $m = cn$, it takes linear time to run the above procedure for all the constraints, and the length of the resulting sequence of clauses is also linear in $n$. □

Table 1
Ranges of tightness with different complexity

<table>
<thead>
<tr>
<th>Scope Size</th>
<th>Resolution Complexity of $C_{n,m}^{2,k,t}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>$2^{\Omega(n)}$ ([1])</td>
</tr>
<tr>
<td>4</td>
<td>[1, 2]</td>
</tr>
<tr>
<td>5</td>
<td>[1, 3]</td>
</tr>
<tr>
<td>$k$</td>
<td>$[1, k-2]$</td>
</tr>
</tbody>
</table>

From Theorems 1 and 2, we can see that for a given tightness $2^{k-2} - 1 < t < 2^{k-1}$, the resolution complexity for the random CSP $C_{n,m}^{2,k,t}$ is polynomial if the constraint density is larger than a certain value. This partly answers the open problem regarding the resolution complexity of random CSP inside the constraint tightness interval $k - 2 < t < 2^{k-1}$ ([1]). For $k = 3$, $c > \frac{7}{3}$, and integer tightness $t$, our results actually show that $t = 2$ is the exact tightness threshold for the exponential resolution complexity. Table 1 shows the current status of the tightness interval of different resolution complexity. The first and the last columns are from [1].

See Molloy and Salavatipour [14] for more recent results on the resolution complexity of random CSP on non-binary variables with the constraint tightness in the range specified in the columns “Unknown” and “Poly. for some $c$” in Table 1. 
The existence of upper bounds characterized by unsatisfiable 2-SAT subproblems raises concerns that $C_{n,m}^{2,k,t}$ might be still flawed even if the tightness $t$ is less than $2^{k-1}$. However, this is not the case. Using a random hypergraph argument and the fact that a 2-clause cycle is satisfiable, it can be shown that for any fixed $t \leq 2^{k-1} - 1$, $C_{n,m}^{2,k,t}$ does have a phase transition with a threshold lower bounded by $\frac{1}{k(k-1)}$.

**Theorem 3** For any fixed $t \leq 2^{k-1} - 1$ and $c = \frac{m}{n} < \frac{1}{k(k-1)}$, $C_{n,m}^{2,k,t}$ is asymptotically almost surely satisfiable.

![Fig. 1. The upper bound $u(t)$ for the threshold $c_3(t)$ as a function of tightness $t$. Left figure: the function itself. Right figure the derivative of the function.](image)

Having established that $C_{n,m}^{2,k,t}$ has a phase transition, it is obvious that the tightness $t$ serves almost the same role as the parameter $p$ in the $(2+p)$-SAT [15] to model the gradual changing from the first order transition to the second order transition. For each fixed constraint tightness $1 \leq t \leq 2^{k-1} - 1$, let $c_k(t)$ be the constraint density threshold of the satisfiability transition. When $t = 1$, we get the k-SAT model, and hence, $c_k(1)$ is exactly the k-SAT threshold. As $t$ gradually increases, $c_k(t)$ decreases to a limit value larger than or equal to $\frac{1}{k(k-1)}$, continuously or discontinuously. Theorems 1 and 2 indicate that for random CSPs, it is possible to have different types of easy-hard complexity pattern if we can pick an appropriate constraint tightness and constraint density relation. The property of the threshold as a function of the constraint tightness and the constraint density deserves further investigation, and the behavior of the upper bounds in Theorem 1, as depicted in Figure 1, is suggestive.
4 Proof of the Results

4.1 Proof of Theorem 1

First, we need some definitions that will be used to characterize CSP subproblems that imply unsatisfiable 2-SAT problems.

Definition 2 (k-Criss-Cross Loop) Let \( p > 0 \) be an integer and \( V = \{v_0, v_1, \ldots, v_{3p}\} \subset X = \{x_1, \ldots, x_n\} \) be a subset of variables. A k-criss-cross loop \((k\text{-cc-loop}) \mathcal{L}(V, E)\) is a \( k \)-uniform hypergraph on \( X \) whose hyperedges \( E = \{E_1, \ldots, E_{3p+2}\} \) form two cycles \( \mathcal{E}_1 = \{E_1, \ldots, E_{p+1}\} \) and \( \mathcal{E}_2 = \{E_{p+2}, \ldots, E_{3p+2}\} \) such that

1. \( E_1 \cap E_{p+1} \cap E_{p+2} \cap E_{3p+2} = \{v_0\}; \)
2. \( E_i \cap E_{i+1} = \{v_i\}, \forall 1 \leq i \leq p; \)
3. \( E_i \cap E_{i+1} = \{v_{i-1}\}, \forall p+2 \leq i \leq 3p+1; \) and
4. \( \forall 1 \leq i \leq 3p+2, |E_i \setminus V| = k-2, \) and \( \{E_i \setminus V, 1 \leq i \leq 3p+2\} \) are mutually disjoint.

We call the variables in \( V \) the cyclic variables (or cyclic vertices) of the \( k \)-cc-loop. The variable \( v_0 \) is called the special variable of the \( k \)-cc-loop.

![Fig. 2. An illustration of a k-cc-loop. Only the cyclic variables \( v_i, 1 \leq i \leq 3p \), are shown. Each hyper-edge \( E_i \) contains two cyclic variables from \( V \) and \( (k-2) \) variables from \( X \setminus V \).](image)

In a k-cc-loop, there are exactly two cycles that touch at the special vertex \( v_0 \). This type of construct was first proposed by Franco in [9] and can be viewed as a generalization to the notion of simple cycles used in the study of the phase transition of random 2-SAT [11,12]. The difference between the k-cc-loop defined in Definition 2 and those used in [9,11,12] is that the former is defined on variables while the latter are defined on literals.

Definition 3 (Reducible k-cc-loop) Let \( \mathcal{L}(V, E) \) be a k-cc-loop where \( V = \{v_0, v_1, \ldots, v_{3p}\} \) and \( E = \{E_1, \ldots, E_{3p+2}\} \). A sequence of constraints \( \mathcal{C} = \{C_1, \ldots, C_{3p+2}\} \) is said to be a reducible k-cc-loop on \( \mathcal{L}(V, E) \) if
Each $C_i$ has $E_i$ as its constraint scope;
(2) Each $C_i$ implies a 2-CNF clause defined on two cyclic variables in $E_i$
such that the resulting set of 2-CNF clauses is of the form

\[
\begin{align*}
  u_0 \lor u_1, & \quad \overline{u}_1 \lor u_2, \quad \overline{u}_2 \lor u_3, \quad \cdots, \quad \overline{u}_{p-1} \lor u_p, \quad \overline{u}_p \lor u_0; \\
  \overline{u}_0 \lor u_{p+1}, & \quad u_{p+1} \lor u_{p+2}, \quad u_{p+2} \lor u_{p+3}, \quad \cdots, \quad u_{3p-1} \lor u_{3p}, \quad u_{3p} \lor \overline{u}_0,
\end{align*}
\]

where $u_i$ is a literal of the variable $v_i$.

We call the above 2-CNF formula a contradictory bi-cycle on the k-cc-loop $L(V, E)$.

In the following, we assume that $l = 3p + 2 = o(n)$.

**Lemma 1** Let $C^{2,k,t}_{n,m}, c = \frac{m}{n}$ be a random CSP. Let $L(V, E)$ be a k-cc-loop
where $V = \{v_0, v_1, \ldots, v_{3p}\}$ is the sequence of cyclic variables and $E = \{E_1, \ldots, E_l\}$
is the sequence of hyperedges. The probability that $C^{2,k,t}_{n,m}$ contains a reducible
k-cc-loop on $L(V, E)$ is

\[
\left(\frac{2rck!}{n^{k-1}}\right)^l \Theta(1),
\]

where $r$ is such that

(1) For $t = 2^{k-2} - 1 + \alpha$ with $0 < \alpha < 1$,

\[
r = \frac{1}{\left(2^{k-2}\right)} \left(1 + 2^{k-2} \alpha\right),
\]

(2) For $t = 2^{k-2} + j + \alpha$ with $0 \leq \alpha < 1$ and $0 \leq j \leq 2^{k-1} - 2^{k-2} - 1$,

\[
r = \left(\frac{2^{k-2} + j}{2^{k-2}}\right) \left(1 + \alpha \frac{2^{k-2}}{j+1}\right).
\]

**PROOF.** Let $N = \binom{n}{k}$ be the number of possible hyperedges. Let $C = \{C_1, C_2, \ldots, C_l\}$
be a sequence of constraints where each constraint $C_i$ has
the hyperedge $E_i$ as its scope. Then the probability that $C^{2,k,t}_{n,m}, c = \frac{m}{n}$, contains
the constraints $C = \{C_1, C_2, \ldots, C_l\}$ is

\[
\frac{1}{\binom{N}{cn}} \left(\frac{N-l}{cn-l}\right)^l \left(\frac{cn}{N}\right)^l \Theta(1) = \left(\frac{ck!}{n^{k-1}}\right)^l \Theta(1).
\]

Let $C$ be a constraint that has $v_i$ and $v_j$ as two of its scope variables. Given
a literal $u_i$ of the variable $v_i$ and a literal $u_j$ of the variable $v_j$, we calculate
the probability that $C$ implies the clause $u_i \lor u_j$. Here we give the details for
the case of \( t = 2^k - 2^k + 2 + \alpha \) with \( 0 \leq \alpha < 1 \) and \( 0 \leq j \leq 2^k - 2^k - 2 - 1 \). The case of \( t = 2^k - 1 + \alpha \) can be handled similarly.

Recall that a constraint contains a restriction set of size \( t = 2^k - 2^k + 2 + \alpha \) with probability \( 1 - \alpha \) and of size \( t = 2^k - 2^k + 1 + \alpha \) with probability \( \alpha \). As we are dealing with constraints over binary variables, it is easy to see that the constraint \( C \) implies the clause \( u_i \lor u_j \) if and only if the set of restrictions contains the set of \( 2^k \) binary vectors \((u_i, u_j, \ast)\) with \( \ast \) being any binary vector in \( \{0, 1\}^{k-2} \). Therefore, the probability that \( C \) implies the clause \( u_i \lor u_j \) is

\[
\begin{align*}
  r &= \frac{\binom{2^k - 2^k - 2}{j}}{\binom{2^k}{2^k}} (1 - \alpha) + \frac{\binom{2^k - 2^k - 1}{j+1}}{\binom{2^k}{2^k}} \alpha \\
  &= \frac{\binom{2^k - 2^k + j}{2^k}}{\binom{2^k}{2^k}} (1 + \alpha \frac{2^k - j}{j+1}). \quad (4)
\end{align*}
\]

As the constraint relations of the constraints are determined independently, the probability that the sequence of constraints \( C = \{C_1, C_2, \ldots, C_l\} \) implies the 2-CNF contradictory bicycle defined by a literal sequence \((u_0, u_1, \cdots, u_{l-2})\) is \( r^l \).

Since both of the positive and negative literals of the special variable \( v_0 \) have to appear in a 2-CNF contradictory bicycle, there are \( 2^{l-2} \) ways to select the literal sequences to form the contradictory bi-cyle. Since the constraint tightness \( t \) is less than \( 2^k - 1 \), the events that the sequence of constraints \( C \) implies 2-CNF contradictory bi-cycles formed by different literal sequences are pair-wise disjoint. It follows that the probability for the sequence of constraints \( C \) to be a reducible k-cc-loop is

\[
  r^l 2^{l-2}. \quad (5)
\]

The lemma is proved by combining (3), (4), and (5). \( \Box \)

**Lemma 2** For any \( 2^k - 1 < t < 2^k - 1 \), the expected number of k-cc-loops on which the random CSP \( C_{n,m}^{2,k,t} \), \( c = \frac{m}{n} \), contains a reducible k-cc-loop is

\[
  \frac{1}{4n} (2rck(k-1))^l \Theta(1)
\]

where \( r \) is the same as in Lemma 1.

**PROOF.** Let \( V = \{v_0, v_1, \cdots, v_{2p}\} \) be a sequence of variables and \( L(V, E) \) be the k-cc-loop defined on \( V \).
From lemma 1, the probability that the CSP contains a reducible k-cc-loop on the k-cc-loop $L(V, E)$ is

$$\left(\frac{2rck!}{n^{k-1}}\right)^l \Theta(1)$$

The total number of k-cc-loops is

$$\binom{n}{l-1}(l-1)! \prod_{i=0}^{l-1} \binom{n-l+1-(k-2)i}{k-2}$$

$$= \binom{n}{l-1}(l-1)! \frac{1}{((k-2)!)^l} \frac{(n-l+1)!}{(n-l+1-l(k-2))!}$$

$$= n^{l(k-1)} \frac{1}{((k-2)!)^l} \Theta(1)$$

where the term $\prod_{i=0}^{l-1} \binom{n-l+1-(k-2)i}{k-2}$ is the total number of ways to choose the variables for $E_i \setminus V$ for each hyperedge $E_i$ in $E$. \(\square\)

**Proof of Theorem 1.** Assume that $2^{k-1}-1 < t < 2^{k-1}$ and $c = \frac{m}{n} > 0$ satisfy one of the two conditions in Theorem 1. Let $p = \ln^2 n$ so that $l = \Theta(1) \ln^2 n$. Let $A_l$ be the number of k-cc-loops on which $C_2^{2,k,t}$ contains a reducible k-cc-loop. To prove the theorem, it suffices to show that

$$\lim_n P \{ A_l > 0 \} = 1. \quad (6)$$

Lemma 2 tells us that the expectation $\mathcal{E}[A_l]$ of $A_l$ satisfies

$$\lim_{n \to \infty} \mathcal{E}[A_l] = \infty.$$  

In order to use the second-moment method to establish (6), we claim that the variance $\text{var}(A_l)$ of $A_l$ satisfies

$$\text{var}(A_l) = O(\mathcal{E}[A_l]^2).$$

For a k-cc-loop $L(V, E)$ defined on $V$, let $I_{L}$ be the indicator function of the event that $C_2^{2,k,t}$ contains a reducible k-cc-loop on $L(V, E)$. Then, $A_l = \sum_{L} I_{L}$ where the sum is over all the possible k-cc-loops. Given two k-cc-loops $L$ and $M$, we write $L \sim M$ if $L$ and $M$ share some hyperedges. Since $\mathcal{E}[I_{L}I_{M}] = \mathcal{E}[I_{L}]\mathcal{E}[I_{M}] = 0$ whenever the two k-cc-loops $L$ and $M$ do not share any
hyperedges, we have

\[ var(A_l) = \sum_{\mathcal{L}} var(I_L) + \sum_{\mathcal{L} \sim \mathcal{M}} (\mathcal{E}[I_L I_M] - \mathcal{E}[I_L] \mathcal{E}[I_M]). \]

By the proof of lemma 2,

\[ \mathcal{E}^2[A_l] = \left( \frac{1}{4n} (2rck(k - 1))^l \right)^2 O(1). \]

Since

\[ \sum_{\mathcal{L}} var(I_L) = \sum_{\mathcal{L}} \mathcal{E}[I_L] (1 - \mathcal{E}[I_L]) = o(\mathcal{E}^2[A_l]), \]

it is enough to show that

\[ \sum_{\mathcal{L} \sim \mathcal{M}} \mathcal{E}[I_L I_M] = o(\mathcal{E}^2[A_l]). \tag{7} \]

Assume that \( \mathcal{L}_1 \) and \( \mathcal{L}_2 \) share \( q \) hyper-edges. Similar to the proof of lemma 1, we have

\[ \mathcal{E}[I_{\mathcal{L}_1} | I_{\mathcal{L}_2}] \leq \frac{1}{(N - l)} \left( \frac{N - 2l + q}{c n - 2l + q} \right)^{l-q} 2^{l-q-2} \]

\[ = \left( \frac{2rck!}{n^{k-1}} \right)^{l-q} O(1) \tag{8} \]

Therefore,

\[ \mathcal{E}[I_{\mathcal{L}_1} I_{\mathcal{L}_2}] = \mathcal{E}[I_{\mathcal{L}_1} | I_{\mathcal{L}_2}] \mathcal{E}[I_{\mathcal{L}_2}] = \left( \frac{2rck!}{n^{k-1}} \right)^{2l-q} O(1). \tag{9} \]

To prove (7), we need to count the number of pairs of \( k \)-cc-loops sharing \( q \) hyper-edges. The following concepts about the cyclic variables in a \( k \)-cc-loop are required. Let \( \mathcal{L} \) be a \( k \)-cc-loop and \( S \) be a set of hyper-edges in \( \mathcal{L} \). We call a cyclic variable appearing in \( \mathcal{L} \)

(1) \textit{fixed} if it belongs to at least two hyper-edges in \( S \);

(2) \textit{limited} if it belongs to one hyper-edge in \( S \); and

(3) \textit{free} if it does not appear in any edges in \( S \).

Write \( A_q \) for the total number of pairs of \( k \)-cc-loops sharing \( q \) hyperedges and \( A_q(S) \) for the total number of pairs of \( k \)-cc-loops sharing a given set \( S \) of \( q \) hyperedges. We need to consider two different cases depending on the structure of the set of shared hyperedges \( S \): (1) \( S \) is connected; and (2) \( S \) has
$h \geq 2$ connected components. In each of the cases, we also need to distinguish how many of the 4 special hyperedges, i.e., the hyperedges that contain the special variable $v_0$, are shared.

Fig. 3. An illustration of a set of $q = 6$ shared hyper-edges that form a hyper-tree containing three hyper-path branches. The variable $v$ appears in 3 hyper-edges. There are 4 fixed cyclic variables, 3 limited cyclic variables.

**Case 1: (The set of shared hyperedges $S$ is connected)** Let $q = |S|$. We consider three situations:

1. **(Each variable that appears in $S$ is incident to at most two hyperedges of $S$.)** In this case, $S$ is a hyper-path, and consequently any k-cc-loop that contains $S$ will have $q - 1$ fixed cyclic variables, 2 limited cyclic variables, and $(l - 1 - (q - 1) - 2)$ free cyclic variables. Therefore, the total number of pairs of k-cc-loops containing $S$ is

$$A_q(S) \leq l^2 \frac{(l-1-(q-1)-2) \left(\begin{array}{c} n \\ k-2 \end{array}\right)^2}{((k-2)!)^2(l-q)O(1)}$$

$$= \frac{l^2(n^{l-q}-2n^{(k-2)(l-q)})^2}{((k-2)!)^2l^{(l-q)}}O(1)$$

$$= \frac{l^2}{n^4((k-2)!)^2l^{(l-q)}}n^{2(k-1)(l-q)}O(1).$$

where the term $l$ is for the number of possible positions of $S$ in a k-cc-loop. As the number of possible hyper-paths with $q$ hyper-edges is less than

$$H = \binom{n}{q-1}(q-1)!\left(\binom{n}{k-1}\right)^2\left(\binom{n}{k-2}\right)^{q-2} = nn^{(k-1)q}1 \frac{1}{((k-2)!)^q}O(1),$$

the total number of pairs of k-cc-loops sharing $q$ hyperedges that form a hyper-path is less than

$$A_q(S) \cdot H \leq \frac{l^2}{n^4((k-2)!)^2l^{(l-q)}}n^{2(k-1)q}n^{-(k-1)q}O(1).$$

2. **(One variable $v$ appears in three or four hyper-edges in $S$; The other variables are incident to at most two hyper-edges of $S$; And $q = |S| <
In this case, $S$ is a hyper-tree consisting of three or four hyper-path branches that join at the special variable $v$, as shown in Figure 3.

If the degree of $v$ in $S$ is 3, then any k-cc-loop that contains $S$ will have $q - 2$ fixed cyclic variables, 3 limited cyclic variables, and $l - 1 - (q - 2) - 3$ free cyclic variables. Since the special variable $v$ appears in $S$, the position of $S$ in a k-cc-loop containing $S$ is fixed. It follows that the number of pairs of k-cc-loops that share $S$ is

$$A_q(S) \leq \left( k^3 n^{l-1-(q-2)-3} \binom{n}{k-2} \right)^2 \frac{1}{n^4((k-2)!)^2} n^{2(k-1)(l-q)} O(1).$$

(13)

The total number of such $S$, hyper-trees consisting of 3 hyper-path branches that join at special variables, is at most

$$H = \binom{n}{q-2} (q-2)! \binom{n}{k-1}^3 \binom{n}{k-2}^{q-3} = n^{q-2} n^{(k-2)(q-3)} n^{3(k-1)} O(1) = n n^{(k-1)q} \frac{1}{((k-2)!)^q} O(1).$$

Then, the total number of pairs of k-cc-loops whose shared hyper-edges form a hyper-tree consisting of three hyper-path branches that join at a special variable is at most

$$\frac{1}{n^3((k-2)!)^2} n^{2(k-1)q} n^{-(k-1)q} O(1).$$

(14)

Similar calculations show that the total number of pairs of k-cc-loops whose shared hyper-edges form a hyper-tree of four hyper-path branches that join at a special variable is less than (14).

(3) (One variable $v$ appears in three or more hyper-edges in $S$; The other variables are incident to at most two hyper-edges of $S$; And $q = |S| \geq p + 3$). In this case, in addition to the cases where the shared hyperedges form a hyper-path or a hyper-tree consisting of hyper-path branches, we need to consider the situation where $S$ forms a unicycle. If $S$ forms a unicycle, then any k-cc-loop that contains $S$ should have $q - 1$ fixed cyclic variables and at least 1 limited cyclic variable. The total number of k-cc-loop pairs sharing a set $S$ of hyper-edges that form a unicycle is at most

$$\frac{1}{n^2((k-2)!)^2} n^{2(k-1)q} n^{-(k-1)q} O(1).$$

(15)
Case 2: (The set $S$ of shared hyperedges form $h \geq 2$ connected components)

In this case, the total number of sets of shared hyperedges is more than that in Case 1. But this is compensated for by the decreasing of free cyclic variables. In the following, we discuss in detail the case where these $h$ components are all hyper-paths. Other cases can be handled similarly. Let $h_1$ be the number of components in $S$ that are isolated hyper-edges, $h_2$ be the number of components in $S$ that contain 2 hyper-edges, and $h_3 = h - h_1 - h_2$ be the number of components in $S$ that are hyper-paths of length greater than 2. There are $2h_1 + 2h_2 + 2h_3$ limited cyclic variables, $h_2 + ((q - h_1 - 2h_2) - h_3)$ fixed cyclic variables, and consequently $l - 1 - q - h$ free cyclic variables. Thus, the number of pairs of $k$-cc-loops that share $S$ is at most

$$A_q(S) = \left( \binom{n}{k-2} \right)^{l-h} \binom{n}{k-2}^{l-q} \left( \frac{n}{k-2} \right)^{l-q} O(1)$$

$$= \left( \frac{p^2k^4}{n^2} \right)^{h} \frac{1}{n^2} \frac{n^{2(k-1)(l-q)}}{((k-2)!)^{2(l-q)}} O(1).$$

(16)

For the total number $H$ of hyper-edge sets that form $h$ hyper-path components, note that there are $(h_2 + ((q - h_1 - 2h_2) - h_3)) = q - h$ cyclic variables that are non-endpoints of the hyper-path components. Once these $q - h$ variables are fixed, there are at most $n^{qh_1}$ ways to choose the single-edge components, $n^{2(k-1)h_2}$ ways to choose the hyper-edges for the hyper-path components whose length is 2, and $n^{2(k-1)h_3} \binom{n}{k-2}^{q-h_1-2h_2-2h_3}$ ways to choose the interior hyper-edges for the hyper-paths whose length is greater than 2. Therefore, the total number of hyper-edge sets of size $q$ that form $h$ hyper-path components is at most

$$n^{q-h} n^{kh_1+2(k-1)(h_2+h_3)-k(h_1+2h_2+2h_3)+2(h_1+2h_2+2h_3)+(k-2)q} \frac{1}{((k-2)!)^{q-h}}$$

$$= n^{q-h} n^{2h_1+2h_2+2h_3+(k-2)q} \frac{1}{((k-2)!)^{q-h}}$$

$$= n^{h} n^{(k-1)q} \frac{1}{((k-2)!)^{q-h}}.$$

It follows that the total number of pairs of $k$-cc-loops sharing $q$ hyper-edges that form $h$ hyper-path components is at most

$$\left( \frac{p^2k^4}{(k-2)!} \right)^{h} \frac{1}{n^{h+2(k-1)q} n^{(k-1)q}} \frac{1}{((k-2)!)^{2l-q}}.$$
Since $h \geq 2$ and $l = O(ln^2(n))$, we conclude that the total number of pairs of k-cc-loops sharing $q$ hyper-edges that form $h$ hyper-path components is less than Case 1, formula (12).

In summary, the number of pairs of k-cc-loops sharing a set of hyper-edges that form $h$, $h \geq 1$, components is dominated by the case of $h = 1$. Therefore, the total number of pairs of k-cc-loops sharing a set of $q$ hyper-edges can be bounded as follows:

$$A_q \leq \begin{cases} 
\frac{l^2}{n^3((k-2))^{2l-q}} n^{2(k-1)!} n^{-(k-1)q} O(l), \text{ if } q \leq p + 2 \\
\frac{l^2}{n^3((k-2))^{2l-q}} n^{2(k-1)!} n^{-(k-1)q} O(l), \text{ if } q > p + 2,
\end{cases}$$

(17)

where the term “$O(l)$” is a result of summing over all the ways in which the $q$ hyper-edges are shared, i.e., the number of components and the structures of the components. Based on formulas (10) and (17), we have

$$\sum_{L \sim M} E[I_L I_M] = \sum_{q=1}^{p+1} \left( \frac{2rck!}{n^{k-1}} \right)^{2l-q} A_q$$

$$= \frac{1}{n^3} (2rck(k-1))^{2l} \sum_{q=1}^{p+1} (2rck(k-1))^{-q}$$

$$+ O(l) \frac{1}{n^2} (2rck(k-1))^{2l} \sum_{q=p+2}^{l} (2rck(k-1))^{-q}$$

$$= E^2(A_l) \frac{O(l^3)}{n} \sum_{q=1}^{p+1} (2rck(k-1))^{-q} + E^2(A_l) O(l) \sum_{q=p+2}^{l} (2rck(k-1))^{-q}$$

$$= E^2(A_l) \left( \frac{O(l^3)}{n} + O(l)(2rck(k-1))^{-(p+2)} \right)$$

$$= O(E^2(A_l)),$$

where the last two equations are because of the assumptions that $2rck(k-1) > 1$ and $l = 3p + 2 = \Theta(ln^2n)$. This establishes the formula (7) and thus, proves the theorem. □
4.2 Proof of Theorem 3

The proof of Theorem 3 is based on the concepts and results of hyper-trees and unicycles in random hypergraphs.

**Definition 4** ([16]) Let $G$ be a $k$-uniform hypergraph with $r$ vertices and $s$ edges. The excess of $G$ is defined to be

$$ex(G) = (k - 1)s - r.$$ 

Generalizing the concepts of trees and cycles in graphs, we call a connected hypergraph $G$ (1) a hyper-tree if $ex(G) = -1$; (2) unicyclic if $ex(G) = 0$.

Consider the random $k$-uniform constraint hypergraph $G(n, m)$ associated with $C_{n, cn}^{2, k, t}$. From [16], for $c < \frac{1}{k(k - 1)}$, $G(n, m)$ almost surely consists of hyper-trees and unicyclic components. In this case, an instance of the random CSP is satisfiable if and only if the subproblems corresponding to the components of the constraint hypergraph are all satisfiable. A subproblem corresponding to a hyper-tree is satisfiable [5]. In the following, we prove that a subproblem corresponding to a unicyclic component is also satisfiable if the tightness of the constraint is less than $2^{k-1}$. We break up the task into three lemmas.

**Lemma 3** For any uncyclic $k$-uniform hypergraph $G$ with the edge set $E = (E_1, \cdots, E_t)$, we have

$$|E_i \cap E_j| \leq 2, \forall 1 \leq i, j \leq t.$$ 

**PROOF.** Assume that $a = |E_i \cap E_j| > 2$ and let

$$G' = (V, E - \{E_i\}).$$

Notice that $G'$ has at most $k - a + 1$ connected components $\{G_1, \cdots, G_{k-a+1}\}$. Since a connected hypergraph has at least an excess of -1, we have

$$ex(G) = ex(G_1) + \cdots + ex(G_{k-a+1}) + (k - 1) \geq a - 2 > 0.$$ 

A contradiction to the unicyclicity of $G$.

Due to Lemma 3, we only need to consider unicycles in which edges have at most size 2 intersection.

**Lemma 4** Let $C$ be a CSP such that

(1) Its constraint graph $G(V, E)$ is unicyclic ;
(2) The tightness $t$ is less than $2^{k-1}$; and

(3) There are a pair of hyper-edges $E_i$ and $E_j$ with $|E_i \cap E_j| = 2$.

Then, $C$ is satisfiable.

**PROOF.** Let $G' = (V, E - \{E_i\})$. Since $|E_i \cap E_j| = 2$, there should be exactly $k-1$ connected components in $G'$ such that (1) one of the components contains the intersection $E_i \cap E_j$, and each of the rest of the components contains exactly one vertex from $E_i - E_j$; and (2) each of the connected components has an excess of -1. Otherwise, $G'$ would have an excess larger than 0. The satisfiability of the CSP can be shown by first satisfying the constraint corresponding to the hyper-edge $E_i$ and then satisfy other constraints. This is possible because for the tightness $t < 2^{k-1}$, there is always at least one assignment that satisfies $E_i$ and $E_j$ simultaneously. \[\square\]

Now, we are in a position to deal with the situation where hyper-edges have an intersection with a size of at most 1.

**Lemma 5** Let $C$ be a CSP such that

(1) Its constraint graph $G(V, E)$ is unicyclic;

(2) The tightness $t$ is less than $2^{k-1}$; and

(3) For any pair of hyper-edges $E_i$ and $E_j$, we have with $|E_i \cap E_j| \leq 1$.

Then, $C$ is satisfiable.

**PROOF.** In this case, the constraint hypergraph $G(V, E)$ contains one cycle $F = (F_1, \cdots, F_l)$ of the form

$$|F_i \cap F_{i+1}| = 1, \quad 1 \leq i \leq l - 1, \quad |F_i \cap F_1| = 1.$$

and some additional hyper-tree branches attached to the cycle. If there is a partial assignment to the variables satisfying the constraints in the cycle, then we can always extend it to satisfy the hyper-tree branches. To see there exists such a partial assignment, let $y_i = F_i \cap F_{i+1}$ and $y_n = F_n \cap F_1$. Consider the two possible assignments 0 and 1 to $y_1$. If we assign $y_1 = 0$ or 1, we can find assignments to $y_i, 2 \leq i \leq n - 1$ to satisfy $F_1, \cdots, F_{n-1}$. Assume that $y_n$ is forced to take the value $a_0$ for the assignment $y_1 = 0$ and $a_1$ for the assignment $y_1 = 1$. Since there are at most $2^{k-1} - 1$ restrictions to the variables in $E_1$, we know at least one of the pairs $(y_1 = 0, y_n = a_0)$ and $(y_1 = 1, y_n = a_1)$ can satisfy the constraint corresponding to $F_1$. This shows the existence of a partial assignment that satisfies the constraints corresponding to the cycle hyper-edges. \[\square\]
Postscript

The results first appeared in [17]. At the time of submission we learned that our upper bound (Theorem 1) has been independently verified and extended, using a different proof technique, to include a matching lower bound. See [14].

Acknowledgements

The authors are grateful to the anonymous reviewers whose comments help improve the presentation of the paper significantly.

References


[8] K. Xu, W. Li, Many hard examples in exact phase transitions with applications to generating hard satisfiable instances, personal communication.


