Constructing Hard Examples for Graph Isomorphism

Anuj Dawar

1 XOR Formulas

Fix a countable set $\mathcal{X}$ of Boolean variables. We use capital letters $X, Y, \ldots$ to range over this set. A 3-XOR-formula is a finite set of clauses, where each clause contains exactly 3 literals, each of which is either a variable X or a negated variable $\overline{X}$.

We say that a 3-XOR-formula φ is satisfiable if there is an assignment $T : \mathcal{X} \to \{0, 1\}$ of truth values to the variables $\mathcal{X}$ such that in each clause of φ, an *even* number of literals is made true.

Given a 3-XOR-formula φ, we can construct a system of linear equations over the two-element field $\mathbb{F}_2$. That is, for each clause C of φ we construct the equation $x + y + z = c$ where x, y, z are the variables occurring in the literals of C and c is 1 if an odd number of them appear negated and 0 otherwise. It is easily verified that this system of equations has a solution if, and only if, φ is satisfiable. Note that two distinct clauses may give rise to the same equation. Say that two clauses are *equivalent* if they give rise to the same equation.

2 k-local Consistency

We are interested in 3-XOR-formulas that are unsatisfiable but k-locally consistent, for suitable integer k. For our purposes, we define k-local consistency by means of the following pebble game, played by two players called Spoiler and Verifier. The game is played on a 3-XOR-formula φ with k pebbles $p_1, \ldots, p_k$. At each move Spoiler chooses a pebble p_i (either one that is already in play, or a fresh one) and places it on a variable X appearing in φ. In response, Duplicator has to choose a value from $\{0, 1\}$ for the variable X. If, as a result, there is a clause C such that all literals in C have pebbles on them and the assignment of values to them given by Duplicator results in C being unsatisfied, then Spoiler has won the game. Otherwise the game can continue. If Duplicator has a strategy to play the game forever without losing, we say that φ is k-locally consistent.

It is known (see for instance [1]) that k-local consistency has a close relationship with definability in the logic $\exists L^k_{\infty\omega}$—the existential positive fragment of the infinitary logic with k variables. In particular, the class of non k-locally consistent formulas is definable in this logic, while the class of unsatisfiable formulas is not. There are, for each k, unsatisfiable formulas that are k-locally consistent.

3 Random XOR Formula

For fixed positive integers m, n we write $F(m, n)$ for the set of all 3-XOR-formulas over the variables $X_1, \ldots, X_n$ containing exactly m inequivalent clauses. We also write $\mathcal{F}(m, n)$ for the

uniform probability distribution over $F(m,n)$. It is known that, for large enough values of m and n, with $m > n$, a random formula drawn from this distribution is unsatisfiable (see [7]).
Question 1: How large does n have to be to make the probability of unsatisfiability greater than $\frac{1}{2}$, say?
Experiment: Construct for some large values of n, random 3-XOR-formulas and run them through a SAT solver to check for satisfiability. Use this to build up a database of random unsatisfiable formulas.

Also, for any k there is a constant c_k such that, for sufficiently large m and n with $m > c_k n$, a random formula drawn from $\mathcal{F}(m,n)$ is k-locally consistent. This is proved for 3CNF-formulas in [1], but should also follow for 3-XOR-formulas from results in that paper and [3, 2].
Question 2: What is the value of c_k?
Question 3: How large does n have to be to make the probability of k-local consistency greater than $\frac{1}{2}$, say?

4 Homogeneous Systems of Equations

Thinking of a 3-XOR-formula as a system of equations, we say that it is *homogeneous* if the right hand side of each equation is 0. Note that a homogeneous system of equations is always satisfied by the constant 0 assignment. Say that a homogeneous system of equations is *uniquely satisfiable* if this is the only satisfying assignment to its variables.

Define $H(m,n)$ to be the set of all homogenous systems of equations with m clauses and n variables, and $\mathcal{H}(m,n)$ for the uniform probability distribution over this set.
Question 4: Is it the case that for some constant Δ, and sufficiently large m and n with $m > \Delta n$, a random system from $\mathcal{H}(m,n)$ is uniquely satisfiable? If so, what is the value of Δ? How large does n have to be to make the probability large enough?

Note that every homogeneous system is k-locally-consistent, because it is satisfiable. For the construction, we actually require a property stronger than k-local-consistency. Say that a formula φ in $F(m,n)$ is *strongly k-locally consistent* if for any variable X in $X_1,\ldots,X_n$ the formula $\varphi[X \leftarrow 1]$ obtained by fixing the value of the variable X to be 1 is k-locally-consistent.

It should be provable that, again, for any k there is a constant s_k such that, for sufficiently large m and n with $m > s_k n$, a random formula drawn from $\mathcal{F}(m,n)$ is strongly k-locally consistent. And the same should follow for $\mathcal{H}(m,n)$.
Question 5: What are the values of the parameters s_k and what are sufficiently large values of n for this to work?

We are especially interested in homogeneous systems that are uniquely satisfiable and strongly k-locally consistent.

5 Graph Construction

We give a construction of graphs from formulas that is inspired by those of Cai et al. [4] and the multipedes of [5].

For any 3-XOR-formula φ, we define a graph G_φ by the following construction. If φ has m inequivalent clauses and n variables, G_φ has a total of $4m + 2n + 3(n-1)$ vertices.

For each clause C of φ, let $C_1 = C$ and let C_2, C_3, C_4 be the three clauses equivalent to C obtained by negating exactly two of the literals of C. We then have a vertex in G_φ for each of these clauses. Also, for each variable X in φ, we have two vertices X^0 and X^1. In addition, for each i with $1 \leq i < n$ we have three vertices i_l, i_r, i_s.

The edges are described as follows. For each clause C, if the literal X occurs in C, we have an edge from C to X^1 and if the literal $\overline{X}$ occurs in C, we have an edge from C to X^0. There is an edge between X^0 and X^1. For each i we also have the edges: (i_l, i_r), (i_r, i_s) and (i_l, X_i^0), (i_l, X_i^1), (i_r, X_{i+1}^0) and (i_r, X_{i+1}^1).

Recall that we say that a graph G is *rigid* if it has no non-trivial automorphisms.

Proposition 1. *If φ is homogeneous, then it is uniquely satisfiable if, and only if, G_φ is rigid.*

Proof. Letα be any automorphism of G_φ. Note that every clause vertex C has degree 3. Every variable vertex X^0 or X^1 has degree at least 4. Every vertex i_s has degree 1. Thus, each of the following sets is fixed (set-wise) by α:

- the set $S = \{i_s \mid 1 \leq i < n\}$: this is the set of vertices of degree 1;
- the set $R = \{i_r \mid 1 \leq i < n\}$: this is the set of vertices adjacent to a vertex in S;
- the set of clause vertices $\mathcal{C}$: this is the set of vertices of degree 3 that are not within distance 2 of a vertex in S;
- the set of variable vertices $\mathcal{X}$: this is the set of neighbours of $\mathcal{C}$; and
- the set $L = \{i_l \mid 1 \leq i < n\}$: this is everything else.

Indeed, we can say more. Each of the sets S, L and R is fixed *pointwise* by α. If this were not so, there would be some i, j with $i < j$ such that $\alpha(i_s) = j_s$ (since the set S is fixed). Then, $\alpha(i_r) = j_r$ (since these are the sole nieghbours), $\alpha(\{X_i^0, X_i^1\}) = \{X_j^0, X_j^1\}$ (since these are the only neighbours in $\mathcal{X}$ of i_r and j_r respectively), and so $\alpha((i+1)_l) = (j+1)_l$ and $\alpha((i+1)_r) = (j+1)_r$. Proceeding by induction, we have for all k $\alpha((i+k)_r) = (j+k)_r$. Taking k large enough so that $j + k > n$, we get a contradiction.

It also follows that, for each variable X, $\alpha(\{X^0, X^1\}) = \{X^0, X^1\}$. That is, α either fixes each of the two vertices or it interchanges them. Note that if α fixes all the variable vertices, then it is the identity everywhere, since no two vertices in $\mathcal{C}$ have the same neighbours in $\mathcal{X}$. Let T be the assignment that maps X to 0 if α is the identity on $\{X^0, X^1\}$ and 1 otherwise. We now check that T satisfies φ.

In the other direction, suppose there is a truth assignment T that satisfies φ, we can show that the map on $\mathcal{X}$ that exchanges the vertices X^0 and X^1 just in case $T(X) = 1$ and is the identity everywhere else on $\mathcal{X}$ can be extended to an automorphism of G_φ. $\square$

Note and Extension: The role of the vertices i_l, i_r, i_s is just to eliminate automorphisms based on a permutation of the variables. Perhaps we don't need them if we can prove that a random formula does not admit such automorphisms anyway.

6 C^k-rigidity

C^k is the fragment of first-order logic where we allow counting quantifiers: $\exists^i x\varphi$ means that there exist at least i distinct elements x satisfying φ, but each formula has at most k distinct variables.

For a graph G and a vertex $v \in V(G)$, the C^k-type of (G, v) is the collection of all C^k formulas $\varphi(x)$ in one free variable such that $G \models \varphi[v]$. We write $u \equiv^k v$ to indicate that (G, u) and (G, v) have the same C^k-type. This equivalence relation is characterized by the bijection game of Hella [6]. We say that a graph is C^k-rigid if no two vertices have the same C^k-type. The Hella bijection game can be used to establish the following.

Proposition 2. *If φ is strongly k-locally consistent, then for any variable X occuring in it, $X^0 \equiv^k X^1$ in G_φ.*

It is also known that equivalence in C^{k+1} is the same as indistinguishability in the k-dimensional Weisfeiler-Leman algorithm for graph isomorphism. This is a significant generalization of the method of vertex refinement.

Hence, if φ is a homogeneous system of equations that is strongly k-locally consistent, then G_φ is rigid but not C^k-rigid. Such graphs should be hard for Traces. Moreover, choosing φ at random from the distribution $H(m, n)$ for suitably large values of m and n should ensure that φ has both these properties with high probability.

References

[1] A. Atserias. On sufficient conditions for unsatisfiability of random formulas. *J. ACM*, 51:281–311, 2004.

[2] A. Atserias and V. Dalmau. A combinatorial characterization of resolution width. *J. Comput. Syst. Sci.*, 74:323–334, 2008.

[3] E. Ben-Sasson and A. Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48:149–169, 2001.

[4] J-Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.

[5] Y. Gurevich and S. Shelah. On rigid structures. *Journal of Symbolic Logic*, 61:549–562, 1996.

[6] L. Hella. Logical hierarchies in PTIME. *Information and Computation*, 129:1–19, 1996.

[7] B. Pittel and G. B. Sorkin. The satisfiability threshold for k-xorsat. *Combinatorics, Probability & Computing*, 25:236–268, 2016.