Combinatorics, Probability and Computing (2007) 16, 5–28. © 2006 Cambridge University Press
doi:10.1017/S096354830600784X First published online 14 August 2006 Printed in the United Kingdom

Strong Refutation Heuristics for Random k-SAT

AMIN COJA-OGHLAN[1]†, ANDREAS GOERDT[2]
and ANDRÉ LANKA[2]

[1]Humboldt-Universität zu Berlin, Institut für Informatik,
Unter den Linden 6, 10099 Berlin, Germany
(e-mail: coja@informatik.hu-berlin.de)

[2]Technische Universität Chemnitz, Fakultät für Informatik
Straße der Nationen 62, 09107 Chemnitz, Germany
(e-mail: {goerdt,lanka}@informatik.tu-chemnitz.de)

Received 10 November 2004; revised 11 March 2005

A simple first moment argument shows that in a randomly chosen k-SAT formula with m clauses over n boolean variables, the fraction of satisfiable clauses is $1 - 2^{-k} + o(1)$ as $m/n \to \infty$ almost surely. In this paper, we deal with the corresponding algorithmic *strong refutation problem*: given a random k-SAT formula, can we find a *certificate* that the fraction of satisfiable clauses is $1 - 2^{-k} + o(1)$ in polynomial time? We present heuristics based on spectral techniques that in the case $k = 3$ and $m \geqslant \ln(n)^6 n^{3/2}$, and in the case $k = 4$ and $m \geqslant Cn^2$, find such certificates almost surely. In addition, we present heuristics for bounding the independence number (resp. the chromatic number) of random k-uniform hypergraphs from above (resp. from below) for $k = 3, 4$.

1. Introduction and results

1.1. Random k-SAT

Let $V = \{x_1, \ldots, x_n\}$ be a set of n propositional variables, and let $L = \{x_i, \bar{x}_i : i = 1, \ldots, n\}$ be the set of literals over V. A *k-clause* over V is a disjunction of k literals over V. Furthermore, the *k-SAT problem* is to decide whether for a given set φ of k-clauses there exists an assignment of the variables V that satisfies all clauses in φ. The k-SAT problem is well known to be NP-hard. In addition to the decision version, the optimization version *MAX k-SAT* – given a set φ of k-clauses, find an assignment that satisfies the maximum number of clauses – is of fundamental interest. Let OPT(φ) signify the maximum number of clauses of φ that can be satisfied simultaneously by any assignment. Then a result

† Research supported by the Deutsche Forschungsgemeinschaft (grant DFG FOR 413/1-1).

of Håstad [26] shows that it is NP-hard to approximate OPT(φ) within a factor of $1-2^{-k}+\varepsilon$ for any fixed $\varepsilon > 0$. Indeed, this hardness result is essentially best possible, as the expected fraction of clauses satisfied by a random assignment is $1-2^{-k}$. (Besides, an assignment that satisfies a $1-2^{-k}$ fraction of the clauses can also be constructed deterministically in polynomial time: see [5, pp. 223 *et seq*.].)

However, the NP-hardness result just shows that no polynomial time algorithm can achieve an approximation ratio of $1-2^{-k}+\varepsilon$ on *all* instances (unless P=NP). Therefore, it does not rule out the existence of efficient *heuristics* for k-SAT or MAX k-SAT that are successful on large/interesting classes of instances. From the point of view of heuristics, the satisfiability problem is interesting in two respects. On the one hand, one could ask for heuristics for *finding* a satisfying assignment. This problem has been studied, *e.g.*, by Flaxman [18], who has shown that in a rather general model of random satisfiable formulas a satisfying assignment can be found in polynomial time almost surely (see also [34] for an extension to semirandom formulas). On the other hand, in this paper we study heuristics for *refuting* k-SAT instances, *i.e.*, for *certifying* that no satisfying assignment exists. More precisely, we present *strong refutation heuristics* that do not only certify that there is no satisfying assignment, but even that the number of satisfiable clauses does not exceed the trivial $(1-2^{-k})$-fraction significantly. One motivation for studying this problem is the relationship between the existence of strong refutation heuristics for random formulas and approximation complexity pointed out by Feige [14].

In order to analyse a heuristic rigorously, we need to specify a model of input instances. Let $0 < p = p(n) < 1$. In this paper, we consider the following standard model $\mathrm{Form}_{n,k,p}$ of *random* instances of MAX k-SAT. The random formula $\mathrm{Form}_{n,k,p}$ is obtained by including each of the $(2n)^k$ possible k-clauses over the variables $V = \{x_1, \ldots, x_n\}$ with probability p independently; here we consider clauses as *ordered* k-tuples of literals, and we allow multiple occurrences of literals in a clause as well as tautological clauses containing both x and $\bar{x}$. Observe that the number of clauses occurring in $\mathrm{Form}_{n,k,p}$ is binomially distributed with mean $m = (2n)^k p$. We say that the random formula $\mathrm{Form}_{n,k,p}$ enjoys some property *almost surely*, or *with high probability* if the probability that the property holds tends to 1 as the number n of variables tends to infinity. Throughout, we apply the notions 'almost surely' and 'with high probability' to families of probability spaces different from $\mathrm{Form}_{n,k,p}$ in the same manner. (A couple of related though slightly different models of random k-SAT instances have been considered – *e.g.*, one could neglect the order of the literals in a clause, or forbid multiple occurrences of a variable in one clause – but the differences are merely of technical relevance.)

The combinatorial structure of random k-SAT formulas and, in particular, the question for which values of p there exist satisfying assignments, has attracted considerable attention. Friedgut [19] has shown that for each fixed k, $\mathrm{Form}_{n,k,p}$ exhibits a *sharp threshold behaviour*: there exist numbers $c_k = c_k(n) = O(1)$ such that $\mathrm{Form}_{n,k,p}$ is satisfiable almost surely if $m < (1-\varepsilon)c_k n$, whereas $\mathrm{Form}_{n,k,p}$ is unsatisfiable almost surely if $m > (1+\varepsilon)c_k n$. We refer to c_k as the *satisfiability threshold*. (Section 1.3 below contains some more detailed comments on the literature.) Furthermore, for any fixed truth value assignment a of V the number of clauses of $\mathrm{Form}_{n,k,p}$ that a satisfies is binomially distributed with parameters $\lambda = (2^k-1)\cdot n^k$ and p. Therefore, the number of clauses satisfied by a is

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

$(1+o(1))\lambda p$ almost surely as $m \to \infty$. In fact, a simple first moment argument shows that, almost surely, for *all* assignments b the number of clauses satisfied by b is $(1+o(1))\lambda p$ as $m/n \to \infty$. Hence, almost surely $\mathrm{OPT}(\mathrm{Form}_{n,k,p}) \sim (1-2^{-k})m$ as $m/n \to \infty$.

With respect to the computational complexity of refuting $\mathrm{Form}_{n,k,p}$, *i.e.*, finding a certificate that $\mathrm{Form}_{n,k,p}$ is unsatisfiable, the strongest previous results are based on spectral techniques. The first spectral heuristic for refuting $\mathrm{Form}_{n,k,p}$ has been suggested by Goerdt and Krivelevich [22], who show that the existence of a satisfying assignment of $\mathrm{Form}_{n,4,p}$ with $p \geqslant \ln(n)^7 n^{-2}$ can be refuted in polynomial time almost surely. Note that for $p = \ln(n)^7 n^{-2}$, the expected number of clauses is $m = 16\ln(n)^7 n^2$. Removing the polylogarithmic factor, Feige and Ofek [16] and (independently) Coja-Oghlan, Goerdt, Lanka, and Schädlich [10] have shown that spectral techniques can be used to refute $\mathrm{Form}_{n,4,p}$ almost surely if $p \geqslant Cn^{-2}$ for a sufficiently large constant $C > 0$. Moreover, Feige and Ofek [17] have given a sophisticated heuristic for refuting $\mathrm{Form}_{n,3,p}$ with $p \geqslant Cn^{-3/2}$ (*i.e.*, $m = 8Cn^{3/2}$). Their heuristic relies on extracting and refuting a 2-XOR formula consisting of $\Theta(n)$ clauses from the input 3-SAT formula. Moreover, refuting the 2-XOR formula essentially reduces to bounding the MAX CUT on a graph corresponding to the formula, which can be implemented efficiently via spectral techniques. The result of Feige and Ofek improves on previous work by Friedman and Goerdt [20], who have presented a heuristic that refutes $\mathrm{Form}_{n,3,p}$ almost surely if $p \geqslant n^{\varepsilon-3/2}$ for an arbitrarily small but constant $\varepsilon > 0$, and Goerdt and Lanka [23], who assume that $p \geqslant (\ln^7 n)n^{-3/2}$. We emphasize that in all of the above cases, the values of p to which the refutation heuristics apply exceed the threshold $p = 2^{-k}n^{1-k}c_k$ when $\mathrm{Form}_{n,k,p}$ actually becomes unsatisfiable almost surely by at least a factor of $n^{(k-2)/2}$.

The new aspect in the present paper is that we deal with *strong* refutation heuristics. That is, we present heuristics that on input $\mathrm{Form}_{n,k,p}$ almost surely certify that not more than a $(1-2^{-k}+\varepsilon)$-fraction of the clauses can be satisfied, for an arbitrarily small, but constant $\varepsilon > 0$. This aspect has not (at least not explicitly) been studied previously. In fact, the heuristics suggested so far [10, 16, 17, 20, 22, 23] only certify that every assignment leaves a $o(1)$-fraction of the clauses unsatisfied.

With respect to MAX 3-SAT, we have the following result.

Theorem 1.1. *Suppose that* $\ln(n)^6 n^{-3/2} \leqslant p = o(n^{-1})$. *There is a polynomial time algorithm* `3-Refute` *that satisfies the following two conditions.*

Correctness. *For any MAX* 3-*SAT instance* φ, *the output of* `3-Refute`(φ, p) *is an upper bound on the number of satisfiable clauses* $\mathrm{OPT}(\varphi)$.

Completeness. *If* $\varphi = \mathrm{Form}_{n,3,p}$, *then* `3-Refute`$(\varphi, p) \leqslant (7+o(1))n^3 p$ *almost surely.*

Since the number of clauses of $\mathrm{Form}_{n,3,p}$ is binomially distributed with mean $8n^3p$, $\mathrm{Form}_{n,3,p}$ has $(8+o(1))n^3p$ clauses almost surely. Therefore, `3-Refute` certifies almost surely that $\mathrm{Form}_{n,3,p}$ does not admit an assignment that satisfies more than a $\frac{7}{8}+o(1)$ fraction of the clauses. Note that the value of p required by Theorem 1.1 is by a factor of $\ln(n)^6$ larger than that required by the heuristic of Feige and Ofek [17]. However, since the heuristic suggested in [17] just refutes a suitably chosen subformula consisting of a

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

$o(1)$ fraction of the clauses (and ignores the remaining clauses), this heuristic does not provide strong refutation.

Moreover, the following result addresses MAX 4-SAT.

Theorem 1.2. *Suppose that $p \geqslant c_0 n^{-2}$ for a sufficiently large constant $c_0 > 0$. There is a polynomial time algorithm* `4-Refute` *that satisfies the following two conditions.*

Correctness. *For any MAX 4-SAT instance φ, the output of* `4-Refute`(φ, p) *is an upper bound on the number of satisfiable clauses* $\mathrm{OPT}(\varphi)$.

Completeness. *If $\varphi = \mathrm{Form}_{n,4,p}$, then almost surely* `4-Refute`$(\varphi, p) \leqslant 15n^4 p + c_1 n^3 \sqrt{p}$, *where $c_1 > 0$ is a constant.*

As in the case of MAX 3-SAT, the number of clauses of $\mathrm{Form}_{n,4,p}$ follows a binomial distribution with mean $16n^4 p$, so that $\mathrm{Form}_{n,4,p}$ has $16n^4 p + o(n^3 \sqrt{p})$ clauses almost surely. Hence, `4-Refute` almost surely provides a certificate that not more than a

$$\frac{15n^4 p + c_1 n^3 \sqrt{p}}{16n^4 p + o(n^3 \sqrt{p})} = \frac{15}{16} + O\left(\frac{1}{n\sqrt{p}}\right)$$

fraction of the clauses can be satisfied. The second order term $O(\frac{1}{n\sqrt{p}})$ gets arbitrarily small as $n^2 p \geqslant c_0$ grows. Theorem 1.2 applies to the same range of p as the best previously known refutation heuristics [10, 16] for 4-SAT, but provides strong refutation.

Theorem 1.1 directly implies that for $\varphi = \mathrm{Form}_{n,3,p}$, $p \geqslant \ln(n)^6 n^{-3/2}$, $\mathrm{OPT}(\varphi)$ can be approximated within a factor of $1 - o(1)$ almost surely as follows. First, construct an assignment a that satisfies a $\frac{7}{8}$ fraction of the clauses; this can be done deterministically in polynomial time (*e.g.*, [5, pp. 223 et seq.]). Then, run `3-Refute` in order to (try to) certify that not more than a $\frac{7}{8} + o(1)$-fraction of the clauses can be satisfied. If `3-Refute` succeeds, which happens almost surely by Theorem 1.1, then the number of clauses satisfied by the assignment a is within a factor of $1 - o(1)$ from $\mathrm{OPT}(\varphi)$. Similarly, Theorem 1.2 implies that the number of satisfiable clauses of $\varphi = \mathrm{Form}_{n,k,p}$ can be approximated within a factor of $1 - O(\frac{1}{n\sqrt{p}})$ with high probability.

1.2. Hypergraph problems

The techniques that the algorithms `3-Refute` and `4-Refute` rely on yield heuristics for random instances of some coNP-hard hypergraph problems. Recall that a *k-uniform hypergraph* $H = (V, E)$ consists of a set $V = V(H)$ of vertices and a set $E = E(H)$ of edges. The edges are subsets of V of cardinality k. An *independent set* in H is a set $S \subset V(H)$ such that there is no edge $e \in E(H)$ with $e \subset S$. The *independence number* $\alpha(H)$ is the number of vertices in a maximum independent set. Moreover, H is called *κ-colourable* if there exists κ independent sets $S_1, \ldots, S_\kappa$ in H such that $S_1 \cup \cdots \cup S_\kappa = V(H)$. The *chromatic number* $\chi(H)$ is the least integer $\kappa \geqslant 1$ such that H is κ-colourable.

The NP-hardness of approximation results for graph colouring and the clique problem in graphs [15, 25] imply immediately that it is NP-hard to approximate the independence number (resp. the chromatic number) of k-uniform hypergraphs on n vertices within a factor of $n^{\varepsilon-1}$ (resp. $n^{1-\varepsilon}$), where $\varepsilon > 0$ is arbitrarily small but fixed. Therefore, we are interested in heuristics for estimating the independence number or the chromatic number

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

of *random* hypergraphs. As in the case of MAX k-SAT, two different issues arise. On the one hand, one could ask for heuristics that compute a lower bound on the independence number, or an upper bound on the chromatic number. For instance, a heuristic for finding a 2-colouring of a random 2-colourable hypergraph has been suggested by Chen and Frieze [7]. On the other hand, in this paper we deal with heuristics for upper-bounding the independence number, and lower-bounding the chromatic number.

In analogy with the $\mathrm{Form}_{n,k,p}$ model of random k-SAT instances, there is the $H_{n,k,p}$ model of random k-uniform hypergraphs: the vertex set of $H_{n,k,p}$ is $V = \{1, \ldots, n\}$, and each of the $\binom{n}{k}$ possible edges is present with probability $0 < p < 1$ independently. Krivelevich and Sudakov [30] have determined the probable value of the independence number and of the chromatic number of random hypergraphs: if $1 \ll d = k\binom{n-1}{k-1}p = o(n^{k-1})$, then

$$\chi(H_{n,k,p}) \sim \left(\frac{d}{k \ln d}\right)^{\frac{1}{k-1}} \text{ and } \alpha(H_{n,k,p}) \sim n\left(\frac{d}{k \ln d}\right)^{\frac{1}{1-k}} \text{ almost surely.} \tag{1.1}$$

Hence, in particular, if $d > \max\{C, (1+\varepsilon)kl^{k-1}\ln(kl^{k-1})\}$ for an arbitrarily small but fixed $\varepsilon > 0$ and a suitable constant $C > 0$, then $\chi(H_{n,k,p}) > l$ and $\alpha(H_{n,k,p}) < nl^{-1}$ almost surely.

The following results deal with the *algorithmic* problem of bounding the independence number of $H_{n,k,p}$ from above, or bounding the chromatic number of $H_{n,k,p}$ from below. (The proofs of Krivelevich and Sudakov [30] do not lead to polynomial time algorithms for these problems.)

Theorem 1.3. *Let $\varepsilon > 0$ be arbitrarily small but fixed. Suppose that $\ln(n)^6 \leqslant n^{3/2}p = o(n^{1/2})$. There is a randomized polynomial time algorithm* `3-Alpha` *that satisfies the following conditions.*

Correctness. *For any 3-uniform hypergraph H,* `3-Alpha`(H, p) *outputs an upper bound on $\alpha(H)$.*

Completeness. *Almost surely the random hypergraph $H = H_{n,3,p}$ enjoys the following property: the probability over the coin tosses of* `3-Alpha`(H, p) *of the event that* `3-Alpha`$(H, p) <$ *εn tends to 1 as $n \to \infty$.*

We abbreviate the completeness statement in Theorem 1.3 by simply saying that 'if $H = H_{n,3,p}$, then `3-Alpha`$(H, p) < \varepsilon n$ almost surely'. We use a similar terminology in the following results.

Theorem 1.4. *Let $1 \leqslant a \leqslant n$ be an integer. Suppose that $a^4 p \geqslant c_0 n^2$ for some sufficiently large constant $c_0 > 0$. There is a randomized polynomial time algorithm* `4-Alpha` *that satisfies the following conditions.*

Correctness. *For any 4-uniform hypergraph H,* `4-Alpha`(H, p) *outputs an upper bound on $\alpha(H)$.*

Completeness. *If $H = H_{n,4,p}$, then* `4-Alpha`$(H, p) < a$ *almost surely.*

Since $\alpha(H)\chi(H) \geqslant |V(H)|$ for all H, Theorem 1.4 yields an algorithm for lower-bounding the chromatic number immediately.

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Corollary 1.5. *Let $\kappa \geqslant 2$ be an integer. Suppose that $n^2p \geqslant c_0\kappa^4$ for some sufficiently large constant $c_0 > 0$. There is a randomized polynomial time algorithm* `4-RefuteCol` *that satisfies the following conditions.*

Correctness. *If H is a 4-uniform hypergraph, then* `4-RefuteCol`(H, p) *either outputs 'not κ-colourable' or 'fail'. If* `4-RefuteCol`(H, p) *answers 'not κ-colourable', then $\chi(H) > \kappa$.*
Completeness. *On input $H = H_{n,4,p}$,* `4-RefuteCol`(H, p) *outputs 'not κ-colourable' almost surely.*

1.3. Further related work

Quite a few papers deal with estimates on the satisfiability thresholds c_k (see Section 1.1). Using the second moment method and extending the work of Achlioptas and Moore [1], Achlioptas and Peres [3] have shown that $c_k = 2^k \ln(2) - O(k)$. In addition, Achlioptas, Peres and Naor [2] have derived rather precise estimates on the number of satisfiable clauses (above the threshold). The proofs are, however, non-algorithmic, *i.e.*, they do not lead to heuristics for finding good assignments or for refuting the existence of a satisfying assignment. The best current bounds on c_3 are $3.52 \leqslant c_3 \leqslant 4.52$ [24, 28, 13]. Furthermore, $7.91 \leqslant c_4 \leqslant 10.23$ [3, 29].

With respect to proof complexity, various types of resolution proofs for the non-existence of satisfying assignments have been investigated on $\mathrm{Form}_{n,k,m}$. Ben-Sasson [6] has shown that tree-like resolution proofs for refuting $\mathrm{Form}_{n,k,m}$ almost surely have size $\exp(\Omega(n/\Delta^{1/(k-2)+\varepsilon}))$, where $\Delta = m/n$ and $0 < \varepsilon < 1/2$ is an arbitrary constant. Hence, tree-like resolution proofs are of exponential length even if the number of clauses is $m = n^{k-1-\delta}$ ($\delta > 0$ arbitrarily small but constant). Furthermore, [6, Theorem 2.24] shows that general resolution proofs for the nonexistence of satisfying assignments almost surely have exponential size if $m \leqslant n^{k/2-\delta}$. We emphasize that resolution does not yield *strong* refutation.

Let $G_{n,p}$ denote the *binomial random graph* on n vertices, in which each of the $\binom{n}{2}$ possible edges is present with probability $0 < p < 1$ independently. Krivelevich and Vu [32] and Coja-Oghlan and Taraz [12, 9] have proved that using spectral techniques or semidefinite programming, one can certify that $\alpha(G_{n,p}) = O(\sqrt{n/p})$ in polynomial time almost surely. Hence, these algorithms can be used to refute that $\alpha(G_{n,p}) > \varepsilon n$ for a fixed $\varepsilon > 0$, provided that p is such that the expected number of edges is $\geqslant C\varepsilon^{-2}n$ for certain constant $C > 0$. Furthermore, building on [32, 11, 12], Coja-Oghlan has shown that using semidefinite programming, one can refute in polynomial time that $G_{n,p}$ is k-colourable if $np \geqslant Ck^2$.

1.4. Notation and preliminaries

If φ is a k-SAT instance, then $|\varphi|$ signifies the number of clauses in φ. Moreover, if $G = (U, E)$ is a graph and $S \subset U$, then $E_G(S) = \{e \in E : e \subset S\}$. Furthermore, if $S, T \subset U$, then $E_G(S, T) = \{\{s, t\} \in E : s \in S, t \in T\}$.

Let $V_1 = \{v_1, \ldots, v_n\}$ and $V_2 = \{w_1, \ldots, w_n\}$ be two disjoint sets of n vertices each. A graph $G = (V_1 \cup V_2, E)$ is (V_1, V_2)-*bipartite* if $e \cap V_1, e \cap V_2 \neq \emptyset$ for all $e \in E$. We let $B_{n,p}$ denote a *random bipartite graph* obtained by including each of the n^2 possible edges

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

$\{v_i, w_j\}$ with probability p independently. Hence, the expected number of edges of $B_{n,p}$ is n^2p.

Let $U = \{u_1, \ldots, u_n\}$ be a set, and let $k \geqslant 1$ be an integer. A *k-tuple system* is a pair $T = (U, S)$ where $S \subset U^k$. The difference between a hypergraph and a k-tuple system is that the edges of a hypergraph are unordered *sets* of k elements, whereas a k-tuple system consists of *ordered k-tuples*. For $0 < p < 1$, we obtain the *random k-tuple system* $T_{n,k,p}$ by including each possible k-tuple from U^k with probability p independently. Thus, the number of k-tuples occurring in $T_{n,k,p}$ is binomially distributed with mean $n^k p$.

Let $v \geqslant 1$ be an integer. We let J_v denote an $v \times v$ matrix with *all* entries equal to 1. Furthermore, $\vec{1}_v$ denotes the vector with all v entries equal to 1. We omit the index v if it is clear from the context. Furthermore, if A is a matrix, then $\|A\| = \sup_{\|\xi\|=1} \|A\xi\|$ signifies the norm of A. Here $\|\eta\| = \sqrt{\eta_1^2 + \cdots + \eta_v^2}$ signifies the l_2-norm of a vector $\eta \in \mathbb{R}^v$. We recommend [33] as a reference to all further notions and results from linear algebra.

We frequently apply the following Chernoff bounds on the tails of a binomially distributed random variable X with mean μ (see [27, pp. 26–28] for proofs):

$$\text{if } t > 0, \text{ then } \mathbf{P}(X \geqslant \mu + t) \leqslant \exp\left(-\frac{t^2}{2(\mu + t/3)}\right) \tag{1.2}$$

$$\text{and } \mathbf{P}(X \leqslant \mu - t) \leqslant \exp\left(-\frac{t^2}{2\mu}\right); \tag{1.3}$$

$$\text{if } t \geqslant 7\mu, \text{ then } \mathbf{P}(X > t) \leqslant \exp(-t). \tag{1.4}$$

1.5. Techniques and outline

The heuristics for Theorems 1.1–1.4 are based on heuristics for certifying that certain random k-tuple systems have ‘low discrepancy’. Roughly speaking, we say that a random k-tuple system $T = (U, E)$ has ‘low discrepancy’ if for *all* set $S \subset U$ the number $|E \cap S^k|$ of tuples spanned by S is approximately $(|S| \cdot |U|^{-1})^k \cdot |E|$ (see Section 3.1 for a precise definition). Now, on the one hand, a standard first moment argument shows that if $T = T_{n,k,p}$ is a random k-tuple system such that $n^{k-1}p \gg 1$, then T has low discrepancy almost surely. However, on the other hand, *certifying* that a random k-tuple system has low discrepancy seems to be an algorithmic challenge. Indeed, the main technical contributions of this paper are heuristics for certifying almost surely that a 3-tuple system $T_{n,3,p}$ (resp. 4-tuple system $T_{n,4,p}$) with $p \geqslant n^{-3/2} \ln^6 n$ (resp. $p \gg n^{-2}$) has low discrepancy.

To see the connection between refuting a random k-SAT instance strongly and certifying low discrepancy, let $\varphi = \text{Form}_{n,k,p}$ be a random formula over the propositional variables $V = \{x_1, \ldots, x_n\}$. Let $L = \{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$ be the set of literals. Then we can define a k-tuple system $T = T(\varphi) = (L, E)$ as follows: the k-tuple $(l_1, \ldots, l_k)$ is present in E if and only if the clause $l_1 \vee \cdots \vee l_k$ occurs in φ. Clearly, as $\varphi = \text{Form}_{n,k,p}$ is a random formula, $T = T_{2n,k,p}$ is a random k-tuple system. Now consider any truth value assignment a. Let $F_a \subset L$ be the set of literals set to false. Then $|F_a| = n$. Therefore, if T has low discrepancy, then the number of k-tuples $e \in E \cap F_a^k$ is $(1 + o(1))2^{-k}|E|$, and each such k-tuple e corresponds to a clause that evaluates to false under the assignment a. Thus, if T has low discrepancy, then any assignment leaves a $(1 + o(1))2^{-k}$-fraction of the clauses

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

unsatisfied. Hence, if we can certify almost surely that a random k-tuple system has low discrepancy, then we can refute $\mathrm{Form}_{n,k,p}$ strongly.

In Section 2 we carry out the above approach for random 4-SAT, and Section 3 deals with the strong refutation heuristic for random 3-SAT. Moreover, in Section 4 we apply the techniques developed in Sections 2 and 3 to bound the independence number of random hypergraphs (Theorems 1.3 and 1.4).

Let us finally sketch how the heuristics for certifying that a random k-tuple system T has low discrepancy work. First, let $T = T_{n,4,p}$, $p \geqslant Cn^{-2}$. In order to certify that T has low discrepancy, we construct a bipartite auxiliary graph G. If the graph G has low discrepancy in a certain sense (see Section 2.1), then the random 4-tuple system T is of low discrepancy as well. Furthermore, using spectral techniques, we can almost surely certify that G has low discrepancy. More precisely, we set up a matrix M that is related to the adjacency matrix of G; if the norm of M is considerably smaller than the average degree of G, which happens to be the case almost surely, then G has low discrepancy. Moreover, to certify that a random 3-tuple system $T = T_{n,3,p}$, $p \geqslant \ln^6 n^{-3/2}$, has low discrepancy, we construct a certain bipartite auxiliary graph B and in addition a matrix $\mathbf{A}$. Loosely speaking, almost surely we have that both B has low discrepancy and $\mathbf{A}$ has norm $\leqslant n^{3/2+o(1)}p$, and in this case, T has low discrepancy (see Section 3.1 for details).

There are only few references on certifying that a k-tuple system (or, equivalently, a k-uniform hypergraph) has low discrepancy. For instance, Chung [8] addresses the discrepancy problem on k-tuple systems with $\geqslant n^{k-1}$ tuples, *i.e.*, for rather 'dense' k-tuple systems. By comparison, in order to obtain the strong refutation heuristics for Theorems 1.1 and 1.2, we need to certify low discrepancy on random k-tuple systems with an expected number of $n^{\frac{k}{2}+o(1)}$ tuples ($k = 3, 4$). To this end, we extend the techniques from Coja-Oghlan, Goerdt, Lanka, and Schädlich [10], and Goerdt and Lanka [23] considerably ([10, 23] do not address the issue of *strong* refutation). Furthermore, we consider it as a significant aspect of the present work that both the proofs and the algorithms are much simpler than those in [10, 23]. For instance, in order to refute a random 4-SAT formula, [10, Section 2] combines somewhat intricate spectral methods with the use of approximation algorithms for NP-hard problems such as MAX CUT or MIN BISECTION. By contrast, the heuristic presented in this paper just computes the eigenvalues of one auxiliary matrix (see Section 2).

2. A strong refutation heuristic for random 4-SAT

In Section 2.2 we present the heuristic for Theorem 1.2. The main tool is a procedure for certifying that a random bipartite graph is of low discrepancy.

2.1. Discrepancy of random bipartite graphs

Throughout, we let $V_1 = \{v_1, \ldots, v_n\}$, $V_2 = \{w_1, \ldots, w_n\}$ be two disjoint sets of n vertices. Let G be a (V_1, V_2)-bipartite graph, and let $0 \leqslant p \leqslant 1$. We say that G has *low p-discrepancy* if, for all sets $S_i \subset V_i$, $i = 1, 2$, we have

$$||S_1||S_2|p - |E_G(S_1, S_2)|| \leqslant c_1\sqrt{|S_1||S_2|np} + n\exp(-np/c_1), \tag{2.1}$$

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

where $c_1 > 0$ denotes some sufficiently large constant. The aim in this section is to establish the following proposition.

Proposition 2.1. *Suppose that $np \geqslant c_0$ for some sufficiently large constant $c_0 > 0$. There is a polynomial time algorithm* `BipDisc` *and a constant $c_1 > 0$ such that the following two conditions hold.*

Correctness. *Let G be a (V_1, V_2)-bipartite graph. Then* `BipDisc`(G, p) *either outputs 'low discrepancy' or 'fail'. If* `BipDisc`(G, p) *outputs 'low discrepancy', G has low p-discrepancy.*
Completeness. `BipDisc`$(B_{n,p}, p)$ *outputs 'low discrepancy' almost surely.*

Suppose that $np = d > c_0$, let $G = B_{n,p}$, and let $S_i \subset V_i$ be subsets of cardinality $\Omega(n)$ $(i = 1, 2)$. Further, assume that `BipDisc`(G, p) outputs 'low discrepancy'. Note that the expected number of S_1-S_2-edges is $|S_1| \cdot |S_2| \cdot p = \Omega(nd)$. By comparison, the term on the right-hand side of (2.1) is $c_1\sqrt{|S_1||S_1|np} + n\exp(-np/c_1) \leqslant O(n\sqrt{d})$. Hence, if d is sufficiently large, then (2.1) entails that $E_G(S_1, S_2)$ is in fact approximately equal to its expectation $|S_1||S_2|p$ for *all* S_1, S_2.

The procedure `BipDisc` is based on computing the norm of a certain auxiliary matrix. Given a (V_1, V_2)-bipartite graph $B = (V_1 \cup V_2, E)$, we let $A = A(B) = (a_{ij})_{i,j=1,\dots,n}$ be the matrix with entries $a_{ij} = 1$ if $\{v_i, w_j\} \in E$, and $a_{ij} = 0$ if $\{v_i, w_j\} \notin E$. Further, we set $M(B, p) = pJ - A(B)$. On input B and p, $\|M(B, p)\|$ can be computed in polynomial time within any numerical precision (*e.g.*, by computing the largest eigenvalue of the positive semidefinite matrix $M(B, p)^T M(B, p)$, where $M(B, p)^T$ denotes the transpose of $M(B, p)$). The next lemma shows what $\|M(B, p)\|$ has to do with discrepancy.

Lemma 2.2. *Let B be a (V_1, V_2)-bipartite graph. Then for any two sets $S_i \subset V_i$, $i = 1, 2$, we have $||E_B(S_1, S_2)| - |S_1||S_2|p| \leqslant \sqrt{|S_1||S_2|} \cdot \|M(B, p)\|$.*

Proof. Let $M = M(B, p)$. Moreover, let $\xi_i = (\xi_i^{(v)})_{v\in V_i}$ be the characteristic vector of S_i, that is, $\xi_i^{(v)} = 1$ if $v \in S_i$, and $\xi_i^{(v)} = 0$ otherwise $(v \in V_i)$. Then $\|\xi_i\| = \sqrt{|S_i|}$, $\langle pJ\xi_2, \xi_1\rangle = p|S_1||S_2|$, and $\langle A\xi_2, \xi_1\rangle = |E_B(S_1, S_2)|$. Therefore,

$$||S_1||S_2|p - |E_B(S_1, S_2)|| = |\langle M\xi_2, \xi_1\rangle| \leqslant \|M\| \cdot \|\xi_1\| \cdot \|\xi_2\| = \sqrt{|S_1||S_2|} \cdot \|M\|,$$

as claimed. □

In the case $np \geqslant \ln(n)^7$, one can show that $\|M(B_{n,p})\| \leqslant O(\sqrt{np})$ almost surely (via the 'trace method' from [21]). Hence, in this case, Lemma 2.2 implies that we could certify (2.1) almost surely just by computing $\|M(B_{n,p})\|$. In the case $np = O(1)$, however, $\|M(B_{n,p})\| = \Theta(\sqrt{\ln n}) \gg \sqrt{np}$ almost surely, *i.e.*, $\|M(B_{n,p})\|$ is too large to give the bound (2.1); the reason is that almost surely there occur vertices of degree $\Theta(\ln n)$ in $B_{n,p}$ (see [31] for more details). Following an idea of Alon and Kahale [4], we avoid this problem by removing all edges that are incident with vertices whose degree is too high (at least $10np$, say).

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Lemma 2.3. *Suppose that $c_0 \leqslant np$ for a sufficiently large constant $c_0 > 0$. Let $G = B_{n,p}$, and let S be the set of all vertices that have degree $> 10np$ in G. Then there are constants $c_2, c_3, c_4 > 0$ such that the following three statements hold almost surely.*

(1) $|S| \leqslant n\exp(-c_2 np)$.
(2) *The number of edges of G incident with at least one vertex in S is* $\leqslant c_3 n^2 p \exp(-c_2 np)$.
(3) *Let G' be the graph obtained from G by deleting all edges that are incident with a vertex in S. Then $\|M(G',p)\| \leqslant c_4\sqrt{np}$.*

We shall prove Lemma 2.3 in Section 2.3. Finally, the algorithm for certifying that $B_{n,p}$ has low discrepancy is as follows.

Algorithm 1. BipDisc(G, p)
Input: A (V_1, V_2)-bipartite graph $G = (V_1 \cup V_2, E)$, a number $0 \leqslant p \leqslant 1$.
Output: Either 'low discrepancy' or 'fail'.

1. Let S be the set of all vertices of degree $> 10np$ in G. If $|S| > n\exp(-c_2 np)$, then output 'fail' and halt; here $c_2 > 0$ is a sufficiently small constant (see Lemma 2.3).
2. Let $E_S = \{e \in E : e \cap S \neq \emptyset\}$. If $|E_S| > c_3 n^2 p \exp(-c_2 np)$, where $c_3 > 0$ is a sufficiently large constant, then halt with output 'fail'.
3. Let G' be the graph obtained from G by deleting all edges in E_S. Let $M = M(G', p)$. If $\|M\| > c_4\sqrt{np}$ for a certain constant c_4, then output 'fail' and halt.
4. Output 'G has low discrepancy'.

Proof of Proposition 2.1. Let $S_i \subset V_i$ for $i = 1, 2$. If BipDisc(G, p) answers 'low discrepancy', then, by Lemma 2.2,

$$||E_G(S_1 \setminus S, S_2 \setminus S)| - |S_1 \setminus S||S_2 \setminus S|p| \leqslant c_4\sqrt{|S_1||S_2|np}. \tag{2.2}$$

Moreover, because of step 2,

$$|E_G(S_1, S_2)| - |E_G(S_1 \setminus S, S_2 \setminus S)| \leqslant c_3 n^2 p \exp(-c_2 np). \tag{2.3}$$

Finally, due to step 1

$$\begin{aligned} |S_1||S_2|p - |S_1 \setminus S||S_2 \setminus S|p &\leqslant (|S_1| + |S_2|)|S|p \leqslant 2np \cdot |S| \\ &\leqslant 2n^2 p \exp(-c_2 np) \leqslant n\exp(-c_2 np/2). \end{aligned} \tag{2.4}$$

Combining (2.2)–(2.4), we conclude that (2.1) holds, provided that c_1 is chosen large enough. Finally, Lemma 2.3 implies that BipDisc$(B_{n,p}, p)$ outputs 'low discrepancy' almost surely. □

2.2. The refutation heuristic

Let $V = \{x_1, \ldots, x_n\}$ be a set of n propositional variables, and let $L = \{x_1, \bar{x}_1, \ldots, x_n, \bar{x}_n\}$ be the set of the $2n$ literals over V. Moreover, assume that $n^2 p \geqslant c_0$ for a sufficiently large constant c_0.

Let φ be a set of 4-clauses over V. To employ the procedure BipDisc from Section 2.1, we construct a bipartite graph $G = G(\varphi)$ from φ as follows. G is a (V_1, V_2)-bipartite

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

graph, where $V_i = L \times L \times \{i\}$, *i.e.*, V_1, V_2 are disjoint copies of $L \times L$. For each clause $l_1 \vee l_2 \vee l_3 \vee l_4$ of φ, we include the edge $\{(l_1, l_2, 1), (l_3, l_4, 2)\}$ in G, where $l_1, l_2, l_3, l_4 \in L$. That is, the edges of G are obtained by 'splitting the clauses of φ in the middle'. Thus, each V_i has $4n^2$ vertices, and the edges of G are in one-to-one correspondence with the clauses of φ. The algorithm for Theorem 1.2 is as follows.

```
Algorithm 2. 4-Refute($\varphi, p$)
Input: A set $\varphi$ of 4-clauses over $V$, and a number $0 \leqslant p \leqslant 1$.
Output: An upper bound on the number of satisfiable clauses.
1. If $|\varphi| > 16n^4 p + n^3\sqrt{p}$, then return $|\varphi|$ and halt.
2. Construct the graph $G = G(\varphi)$ as above. If BipDisc($G, p$) answers 'fail', then return
   $|\varphi|$ and halt.
3. Return $15n^4 p + c_1 n^3\sqrt{p}$, where $c_1$ is a sufficiently large constant.
```

We first prove that 4-Refute outputs an upper bound on the number of satisfiable clauses; recall that for a 4-SAT formula, $\mathrm{OPT}(\varphi)$ signifies the maximum number of clauses that can be satisfied simultaneously.

Lemma 2.4. *There is a constant $c_1' > 0$ such that the following holds. Let φ be a set of* 4-*clauses such that* BipDisc($G(\varphi), p$) *answers 'low discrepancy'. Then* $|\varphi| - \mathrm{OPT}(\varphi) \geqslant n^4 p - c_1' n^3\sqrt{p}$.

Proof. Consider an assignment that sets the literals $T \subset L$ to true, and $F = L \setminus T$ to false. Clearly, $|T| = |F| = n$. We shall bound the number of edges of $G = G(\varphi)$ that correspond to unsatisfied clauses. Invoking Proposition 2.1, we get

$$|E_G(F \times F \times \{1\}, F \times F \times \{2\})| \geqslant |F|^4 p - c_1'' n^3\sqrt{p} - 4n^2 \exp(-4n^2 p / c_1'') \geqslant n^4 p - c_1' n^3\sqrt{p},$$

where c_1', c_1'' are suitable constants. Hence, there are at least $n^4 p - c_1' n^3\sqrt{p}$ unsatisfied clauses. □

Proof of Theorem 1.2. By Lemma 2.4, the output of 4-Refute(φ, p) is always an upper bound on the number of satisfiable clauses, provided that the constant c_1 is chosen sufficiently large. Since $|\mathrm{Form}_{n,4,p}|$ is binomially distributed with mean $16n^4 p$, the Chernoff bounds (1.2) and (1.3) yield that the total number of clauses in $\mathrm{Form}_{n,4,p}$ is $\leqslant 16n^4 p + o(n^3\sqrt{p})$ almost surely. Hence, the probability that step 1 of 4-Refute outputs $|\varphi|$ is $o(1)$. Further, the completeness of BipDisc($\mathrm{Form}_{n,4,p}, p$) (see Proposition 2.1) implies that the probability that step 2 of 4-Refute($\mathrm{Form}_{n,4,p}, p$) answers 'fail' is $o(1)$ as well. □

2.3. Proof of Lemma 2.3

Given a (V_1, V_2)-bipartite graph G, we let G' be the graph obtained from G by deleting all edges that are incident with vertices of degree $> 10np$ in G. Furthermore, we let $A' = A(G')$ be the $n \times n$-matrix whose ijth entry is 1 if v_i, w_j are adjacent in G', and 0 otherwise. We need the following lemma from [10, Lemma 45], whose proof is based on spectral considerations from [4].

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Lemma 2.5. *There are constants $c_0, c > 0$ such that the following holds. Suppose that $np \geqslant c_0$. Then $G = B_{n,p}$ enjoys the following three properties almost surely.*

(1) *Let S be the set of all vertices that have degree $> 10np$ in G. Then $|S| \leqslant n\exp(-np/c)$.*
(2) *For all unit vectors $\xi \perp \vec{1}$ we have $\|A'\xi\| \leqslant c\sqrt{np}$.*
(3) $\|A'\vec{1} - np\vec{1}\| \leqslant cn\sqrt{p}$.

Proof of Lemma 2.3. Let $G = B_{n,p}$, where $np \geqslant c_0$ for a sufficiently large constant $c_0 > 0$. Let S be the set of all vertices that have degree $> 10np$ in G. Our goal is to establish that the following three statements hold almost surely.

(1) $|S| \leqslant n\exp(-c_2np)$.
(2) The number of edges of G incident with at least one vertex in S is $\leqslant c_3n^2p\exp(-c_2np)$.
(3) Let G' be the graph obtained from G by deleting all edges that are incident with a vertex in S. Then $\|M(G', p)\| \leqslant c_4\sqrt{np}$.

Here $c_2, c_3, c_4 > 0$ denote suitable constants.

Part (1) of Lemma 2.5 shows immediately that the first property is satisfied almost surely, if $0 < c_2 < 1$ is a sufficiently small constant.

With respect to the second property, fix a set S' consisting of $s = n\exp(-c_2np)$ vertices. Then the number of edges that are incident with S' is bounded from above by a binomially distributed random variable with mean $snp = n^2p\exp(-c_2np)$. Hence, by the Chernoff bound (1.4), $\mathbf{P}(S'$ is incident with $> 10snp$ edges$) \leqslant \exp(-10snp)$. Therefore, the expected number of sets $S' \subset V$ of cardinality s such that S' is incident with $> 10snp$ edges is

$$\begin{aligned}&\leqslant \binom{n}{s}\exp(-10snp) \leqslant \left(\frac{\mathrm{e}n}{s}\right)^s\exp(-10snp)\\ &\leqslant \exp(s(1-(10-c_2)np)) \leqslant \exp(-8snp) = o(1),\end{aligned}$$

because $0 < c_2 < 1$. Consequently, almost surely there is no such set S'. Hence, in particular S is incident with at most $c_3n^2p\exp(-c_2np)$ edges almost surely, if $c_3 \geqslant 10$.

Finally, we establish that part (3) of Lemma 2.3 holds almost surely. Let $e = \|\vec{1}\|^{-1} \cdot \vec{1} = n^{-1/2} \cdot \vec{1}$. By Lemma 2.5, almost surely we have

$$\|A'\xi\| = O(\sqrt{np}) \text{ for all unit vectors } \xi \perp \vec{1}, \tag{2.5}$$

$$\|A'e - npe\| = O(\sqrt{np}). \tag{2.6}$$

Let $M = M(G', p) = pJ - A'$. Let $\xi \perp \vec{1}$ be a unit vector. Then $J\xi = 0$, whence (2.5) yields

$$\|M\xi\| = \|A'\xi\| = O(\sqrt{np}). \tag{2.7}$$

Moreover, by (2.6),

$$\|Me\| = \|npe - A'e\| = O(\sqrt{np}). \tag{2.8}$$

Finally, let η be a unit vector. Then we have a decomposition $\eta = \alpha e + \beta\xi$, where $\alpha^2 + \beta^2 = 1$ and $\xi \perp \vec{1}$ is a unit vector. Combining (2.7) and (2.8), we conclude that $\|M\eta\| \leqslant \|M\xi\| + \|Me\| = O(\sqrt{np})$. Consequently, $\|M\| = O(\sqrt{np})$. □

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Remark. Instead of Lemma 2.5, we could also use the spectral considerations from Feige and Ofek [16] to prove Lemma 2.3.

3. A strong refutation heuristic for random 3-SAT

While our refutation heuristic for 4-SAT is based on checking that a certain bipartite graph has low discrepancy, the heuristic for 3-SAT needs a procedure for certifying low discrepancy of triple systems. This procedure is the content of Section 3.1. Then, in Section 3.2, we show how to employ the procedure in order to refute random 3-SAT instances strongly.

3.1. Discrepancy in triple systems

Let $T = (V, S)$ be a triple system, where $|V| = n$. For $W_1, W_2, W_3 \subset V$ we let

$$(W_1, W_2, W_3)_T = S \cap (W_1 \times W_2 \times W_3).$$

We say that T has *low* ε*-discrepancy* if, for all sets $X \subseteq V$ of cardinality $\varepsilon n \leqslant |X| \leqslant (1-\varepsilon)n$, we have $|(X,X,X)_T| = (|X| \cdot n^{-1})^3 \cdot |S| + o(|S|)$.

Proposition 3.1. *Let $\varepsilon > 0$ be constant, and suppose that $\ln^6 n \leqslant n^{3/2}p = o(n^{1/2})$. There is a polynomial time algorithm* $\texttt{TripleDisc}_\varepsilon$ *that satisfies the following conditions.*

Correctness. *For each triple system $T = (V,S)$ the output of* $\texttt{TripleDisc}_\varepsilon(T,p)$ *is either 'low discrepancy' or 'fail'. If the output is 'low discrepancy', then T has low ε-discrepancy.*
Completeness. *The output of* $\texttt{TripleDisc}_\varepsilon(T_{n,3,p},p)$ *is 'low discrepancy' almost surely.*

To certify that the triple system $T = (V,S)$ has low discrepancy, the algorithm $\texttt{TripleDisc}_\varepsilon$ constructs a *bipartite projection graph* $B_{12} = (V_1 \cup V_2, E)$. The vertex sets of B_{12} are $V_i = V \times \{i\}$, and the edge $\{(x,1),(y,2)\}$ is present in B_{12} if and only if there is a $z \in V$ such that $(x,y,z) \in S$. Thus, if $T = T_{n,3,p}$, then each V_1-V_2-edge occurs in B_{12} with probability $p' = 1-(1-p)^n \sim pn$ independently of all other edges, so that B_{12} is distributed as the random bipartite graph $B_{n,p'}$.

In order to certify that the triple system $T = (V,S)$ has low discrepancy, it is, however, *not* sufficient to check that the projection graph B_{12} is of low discrepancy. Therefore, in addition to the projection graph, we consider the matrix $\mathbf{A}(T,p)$ defined as follows. For $0 < p < 1$ and $b_1, b_2, z \in V$ we let

$$B_{b_1b_2z} = B_{b_1b_2z}(T,p) = \begin{cases} -1 & \text{if } (b_1,b_2,z) \in S, \\ p/(1-p) & \text{otherwise.} \end{cases} \tag{3.1}$$

Then the $n^2 \times n^2$-matrix $\mathbf{A} = \mathbf{A}(T,p) = (\mathbf{a}_{b_1c_1,b_2c_2})_{(b_1,c_1),(b_2,c_2)\in V^2}$ is given by

$$\mathbf{a}_{b_1c_1,b_2c_2} = \begin{cases} \sum_{z\in V}(B_{b_1b_2z} \cdot B_{c_1c_2z} + B_{b_2b_1z} \cdot B_{c_2c_1z}) & \text{if } (b_1,b_2) \neq (c_1,c_2), \\ 0 & \text{if } (b_1,b_2) = (c_1,c_2). \end{cases} \tag{3.2}$$

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Remark. Given a triple system T, we could define its 'product graph' $P = (V \times V, E_P)$, where $\{(b_1, c_1), (b_2, c_2)\} \in E_P$ if and only if

$$(b_1, b_2) \neq (c_1, c_2) \wedge (\exists z \in V : ((b_1, b_2, z), (c_1, c_2, z) \in T) \vee ((b_2, b_1, z), (c_2, c_1, z) \in T)).$$

The definition of P is directed by the refutation heuristic from [20]. If we had constructed the matrix $\mathbf{A}$ as in (3.2) but with $B_{b_1b_2z} = 1$ if $(b_1, b_2, z) \in S$ and $B_{b_1b_2z} = 0$ if $(b_1, b_2, z) \notin S$, then $\mathbf{A}$ would essentially be the adjacency matrix of P. However, the definition (3.1) of the $B_{b_1b_2z}$ s has been adjusted so that $\mathrm{E}(B_{b_1b_2z}) = 0$. This adaptation will be of technical significance in the proof of Lemma 3.3 below.

If $T = (V, S)$ is a triple system, $x \in V$, and $i \in \{1, 2, 3\}$, then the *degree of x in slot i* is

$$d_{x,i} = d_{x,i}(T) = |\{(z_1, z_2, z_3) \in S : z_i = x\}|.$$

We say that T is *asymptotically regular* if $d_{x,i} = (1 + o(1))n^{-1}|S|$ for all x, i. Equipped with these definitions, we can state the following sufficient condition for T having low discrepancy.

Lemma 3.2. *Suppose that $\ln^6 n \leqslant f = n^{3/2}p = o(n^{1/2})$ and let $\varepsilon > 0$ be a constant. If $T = (V, S)$ with $|V| = n$ is a triple system that satisfies the following four conditions, then T has low ε-discrepancy.*

(1) $|S| = (1 + o(1))f \cdot n^{3/2}$.

(2) *T is asymptotically regular.*

(3) *The projection graph $B_{12} = (V_1 \cup V_2, E)$ of T satisfies $|E| = |S| + o(|S|)$ and has low p'-discrepancy (see (2.1)).*

(4) *We have $\|\mathbf{A}(T, p)\| \leqslant f \cdot \ln^5 n$.*

The proof of Lemma 3.2 can be found in Section 3.3.

Algorithm 3. $\texttt{TripleDisc}_\varepsilon(S, p)$

Input: A triple system $T = (V, E)$, a number $0 < p < 1$.

Output: Either 'low discrepancy' or 'fail'.

1. Check whether conditions (1), (2) and (4) in Lemma 3.2 hold. If not, halt with output 'fail'.
2. If $\texttt{BipDisc}(B_{12}, p')$ answers 'low discrepancy', then output 'low discrepancy'. Otherwise output 'fail'.

In order to prove that $\texttt{TripleDisc}_\varepsilon$ is complete, we need the following lemma, which we shall prove in Section 3.4.

Lemma 3.3. *Suppose that $\ln(n)^6 \leqslant f = n^{3/2}p = o(n^{1/2})$. Then $\|\mathbf{A}(T_{n,3,p}, p)\| \leqslant f \cdot \ln^5 n$ almost surely.*

Proof of Proposition 3.1. The correctness of $\texttt{TripleDisc}_\varepsilon$ follows from Lemma 3.2 immediately. In order to prove the completeness, let us first observe that the random triple

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

system $T = (V, S) = T_{n,3,p}$ satisfies conditions (1) and (2) in Lemma 3.2 almost surely. Indeed, $|S|$ is binomially distributed with mean n^3p, so that the Chernoff bounds (1.2) and (1.3) imply that $|S| \sim n^3p$ almost surely. Moreover, for each $x \in V$ and each $i \in \{1, 2, 3\}$, $d_{x,i}(T)$ is binomially distributed with mean n^2p. Hence, by the Chernoff bound (1.2),

$$\mathbf{P}(|d_{x,i} - n^2p| > n\sqrt{p}\ln n) \leqslant \exp\left(-\Omega\left(\frac{n^2p\ln^2 n}{n^2p + n\sqrt{p}\ln n}\right)\right) \leqslant \exp(-\Omega(\ln^2 n)) \leqslant n^{-2}.$$

Therefore, by the union bound we have $|d_{x,i} - n^2p| \leqslant n\sqrt{p}\ln n = o(n^2p)$ for all $x \in V$ and all $i \in \{1, 2, 3\}$ almost surely.

Furthermore, the bipartite graph $B_{12} = (V_1 \cup V_2, E)$ satisfies $|E| \leqslant |S|$ by construction. Moreover, if there occur two edges $e_1 = (x, y, z_1), e_2 = (x, y, z_2) \in S$, $z_1 \neq z_2$, whose first two components coincide, then e_1, e_2 get mapped to the same edge of B_{12}. However, since the expected number of edges $e_1 = (x, y, z_1) \in S$ such that there exists $e_1 \neq e_2 = (x, y, z_2) \in S$ is $o(|S|)$, we conclude that $|E| \sim |S|$ almost surely.

Since $p' \sim np \gg n^{-1}$, Proposition 2.1 entails that $\texttt{BipDisc}(B_{12}, p')$ answers 'low discrepancy' almost surely and thus certifies that condition (3) in Lemma 3.2 holds. Finally, due to Lemma 3.3, condition (4) in Lemma 3.2 holds almost surely. □

Remark. The techniques behind $\texttt{TripleDisc}_\varepsilon$ can be adapted easily to obtain an algorithm that certifies further related discrepancy properties. For example, a variation of $\texttt{TripleDisc}_\varepsilon$ can be used to certify that all triples (X_1, X_2, X_3) of subsets of V of cardinalities $|X_i| = \alpha_i n$, $\varepsilon \leqslant \alpha_i \leqslant 1 - \varepsilon$, satisfy $|(X_1, X_2, X_3)_T| \sim \alpha_1 \cdot \alpha_2 \cdot \alpha_3 \cdot |S|$. Since our refutation heuristics do not rely on this more general discrepancy concept, we omit the details.

3.2. The refutation heuristic

Let φ be a set of 3-clauses over the variable set $V = \{x_1, \ldots, x_n\}$. Let $L = \{x_i, \bar{x}_i : 1 \leqslant i \leqslant n\}$ be the set of literals over V. To apply the procedure $\texttt{TripleDisc}_\varepsilon$ from Section 3.1, we construct a triple system $T = (L, S) = T(\varphi)$ in the natural way: the triple (l_1, l_2, l_3) is in S if and only if the clause $l_1 \vee l_2 \vee l_3$ occurs in φ. Thus, the clauses in φ and the triples in S are in one-to-one correspondence. Moreover, if $\varphi = \mathrm{Form}_{n,3,p}$ is a random 3-SAT instance, then $T(\varphi) = T_{2n,3,p}$ is a random triple system.

Algorithm 4. $\texttt{3-Refute}(\varphi, p)$

Input: A set φ of 3-clauses over V, and a number $0 < p < 1$.

Output: An upper bound on the number of satisfiable clauses.

1. Compute the triple system $T = T(\varphi)$ and run $\texttt{TripleDisc}_{1/2}(T, p)$. If the output is 'fail', then return $|\varphi|$ and halt.
2. Return $(7 + o(1))n^3p$.

Proof of Theorem 1.1. Let φ be a 3-SAT instance, and consider an assignment a of the variables V that sets a set $T_a \subset L$ of literals to true, and a set $F_a = L \setminus T_a$ of literals to false. Then $|T_a| = |F_a| = n$. In order to prove that $\texttt{3-Refute}$ is correct, assume that

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

$\texttt{TripleDisc}_{1/2}(T,p)$ does not fail. We need to show that the assignment a does not satisfy more than $(7+o(1))n^3$ clauses. Indeed, if $\texttt{TripleDisc}_{1/2}(T,p)$ answers 'low discrepancy', then the correctness of $\texttt{TripleDisc}_\varepsilon$ (see Proposition 3.1) implies that $|\varphi| \sim 8n^3p$, and $(F_a,F_a,F_a)_T \sim \frac{1}{8}(2n)^3p$. Hence, the assignment a satisfies at most $(7+o(1))n^3p$ clauses. Finally, the completeness of 3-`Refute` is an immediate consequence of the completeness of $\texttt{TripleDisc}_{1/2}$ established in Proposition 3.1. □

3.3. Proof of Lemma 3.2

Let $T=(V,S)$ be a triple system with $|V|=n$ that satisfies the assumptions of Lemma 3.2. Let $\ln^6 n \leqslant f = n^{3/2}p = o(n^{1/2})$. Moreover, let $B_{12}=(V_1\cup V_2, E)$ be the bipartite projection graph, and set $s=n^3p\sim|S|\sim|E|$. Let X be an arbitrary subset of V such that $\alpha=|X|n^{-1}$ satisfies $\varepsilon\leqslant\alpha\leqslant 1-\varepsilon$, and set $Y=V\setminus X$. Moreover, for each $z\in V$ let

$$M_z=(X,X,\{z\})_T, \quad \text{and set}$$
$$M=\{(B,C)\in S\times S : B,C\in M_z \quad \text{for some} \quad z\in V, \quad \text{and} \quad B\neq C\}.$$

Thus, M consists of ordered pairs $((b_1,b_2,z),(c_1,c_2,z))\in S\times S$, where $(b_1,b_2)\neq(c_1,c_2)$ and $b_1,b_2,c_1,c_2\in X$. Furthermore, let $m=|M|$ and $m_z=|M_z|$. We proceed in two steps.

Step 1. We establish that

$$m\sim\alpha^4f^2n^2=\alpha^4s^2/n \tag{3.3}$$

implies

$$|(X,X,X)_T|\sim\alpha^3s. \tag{3.4}$$

Step 2. We prove (3.3).

With respect to the first step, note that

$$|(X,X,V)_T|\sim E_{B_{12}}(X\times\{1\},X\times\{2\})\sim\alpha^2s \tag{3.5}$$

because B_{12} is of low p'-discrepancy and $|E|\sim|S|$. Moreover, (3.5) yields

$$\sum_{z\in V}m_z=\sum_{z\in V}|(X,X,\{z\})_T|=|(X,X,V)_T|\sim\alpha^2s. \tag{3.6}$$

Therefore,

$$\begin{aligned} m&=\sum_{z\in V}m_z(m_z-1)\\ &=\sum_{z\in V}m_z^2-\sum_{z\in V}m_z=\sum_{z\in X}m_z^2+\sum_{z\in Y}m_z^2-\alpha^2s(1+o(1)). \end{aligned} \tag{3.7}$$

Furthermore, since the sum $\sum_{z\in X}m_z^2$ subject to the condition $\sum_{z\in X}m_z=|(X,X,X)_T|$ is minimized when each term equals the arithmetic mean $|(X,X,X)_T|/\alpha n$ of all αn terms, we have

$$\sum_{z\in X}m_z^2\geqslant\alpha n\left(\frac{|(X,X,X)_T|}{\alpha n}\right)^2=\frac{|(X,X,X)_T|^2}{\alpha n}. \tag{3.8}$$

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Since $|(X,X,Y)_T| = |(X,X,V)_T| - |(X,X,X)_T|$, we get in the same way that

$$\sum_{z\in Y} m_z^2 \geqslant (1-\alpha)n\left(\frac{|(X,X,Y)_T|}{(1-\alpha)n}\right)^2 = \frac{(|(X,X,V)_T| - |(X,X,X)_T|)^2}{(1-\alpha)n}. \tag{3.9}$$

Now let δ be such that $|(X,X,X)_T| = (\alpha^3+\delta)s$. We shall prove that $\delta = o(1)$. Invoking (3.3), we get

$$\begin{aligned}\alpha^4 f^2 n^2 \sim m &= \sum_{z\in X} m_z^2 + \sum_{z\in Y} m_z^2 - (1+o(1))\alpha^2 s \quad \text{(by (3.7))}\\ &\geqslant \frac{|(X,X,X)_T|^2}{\alpha n} + \frac{(|(X,X,V)_T| - |(X,X,X)_T|)^2}{(1-\alpha)n}\\ &\qquad\qquad - (1+o(1))\alpha^2 s \quad \text{(by (3.8), (3.9))}\\ &\sim \frac{((\alpha^3+\delta)s)^2}{\alpha n} + \frac{(\alpha^2 s - (\alpha^3+\delta)s)^2}{(1-\alpha)n} - \alpha^2 s \quad \text{(using (3.5))}.\end{aligned}$$

Dividing both sides of the preceding estimate by $s^2/n = f^2n^2$, we get

$$\begin{aligned}\alpha^4 &\geqslant \frac{(\alpha^3+\delta)^2}{\alpha} + \frac{(\alpha^2(1-\alpha)-\delta)^2}{1-\alpha} - o(1)\\ &= \alpha^5 + 2\delta\alpha^2 + \frac{\delta^2}{\alpha} + \alpha^4(1-\alpha) - 2\alpha^2\delta + \frac{\delta^2}{1-\alpha} - o(1)\\ &= \frac{\delta^2}{\alpha} + \alpha^4 + \frac{\delta^2}{1-\alpha} - o(1).\end{aligned}$$

As $\varepsilon \leqslant \alpha \leqslant 1-\varepsilon$, we conclude that $\delta = o(1)$. Thus, we get $|(X,X,X)_T| \sim \alpha^3 s(1+o(1))$, thereby proving (3.4).

We are left to show (3.3). Let χ be the characteristic vector of $X\times X$, that is $\chi \in \{0,1\}^{n^2} = \{0,1\}^{V\times V}$ is 1 in each coordinate corresponding to an element of $X\times X$, and 0 otherwise. As $\|\chi\|^2 = |X\times X| = \alpha^2 n^2$ we conclude that $|\langle\chi,\mathbf{A}\chi\rangle| \leqslant \alpha^2n^2\cdot\|\mathbf{A}\|$, where $\mathbf{A} = \mathbf{A}(T,p)$. Hence, plugging in the definition of $\mathbf{A}$, we get

$$\begin{aligned}\alpha^2n^2\|\mathbf{A}\| \geqslant |\langle\chi,\mathbf{A}\chi\rangle| &= \left|\sum_{(b_1,b_2)\in X\times X}\ \sum_{(c_1,c_2)\in X\times X} \mathbf{a}_{b_1c_1,b_2c_2}\right|\\ &= \left|\sum_{\substack{(b_1,b_2,c_1,c_2)\in X^4\\(b_1,b_2)\neq(c_1,c_2)}}\ \sum_{z\in V}(B_{b_1b_2z}\cdot B_{c_1c_2z} + B_{b_2b_1z}\cdot B_{c_2c_1z})\right|\\ &= 2\cdot\left|\sum_{\substack{(b_1,b_2,c_1,c_2)\in X^4\\(b_1,b_2)\neq(c_1,c_2)}}\ \sum_{z\in V} B_{b_1b_2z}\cdot B_{c_1c_2z}\right|.\end{aligned} \tag{3.10}$$

We shall prove below that

$$\beta = \sum_{\substack{(b_1,b_2,c_1,c_2)\in X^4\\(b_1,b_2)\neq(c_1,c_2)}}\ \sum_{z\in V} B_{b_1b_2z}\cdot B_{c_1c_2z} = m - (1+o(1))\alpha^4n^2f^2. \tag{3.11}$$

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Combining (3.10) and (3.11), we get $2 \cdot |m - (1+o(1))\alpha^4 n^2 f^2| \leqslant \alpha^2 n^2 \|\mathbf{A}\|$. Since

$$\begin{aligned}\|\mathbf{A}\| &\leqslant f \ln^5 n && \text{(by condition (4) of Lemma 3.2)}\\ &= o(f^2) && \text{(by the assumption that } f \geqslant \ln^6 n\text{)},\end{aligned}$$

we conclude that $m \sim \alpha^4 n^2 f^2$, thereby proving (3.3).

To prove (3.11), we observe that the sum β consists of the following terms.

(a) $\sum_{z\in V} m_z(m_z - 1) = m$-times the term 1.
This accounts for the cases when $(b_1, b_2, z), (c_1, c_2, z) \in S$, so that $B_{b_1 b_2 z} = B_{c_1 c_2 z} = -1$.

(b) $2 \cdot \sum_{z\in V} m_z(\alpha^2 n^2 - m_z)$-times the term $-p/(1-p)$.
This accounts for those cases when $(b_1, b_2, z) \in S$ and $(c_1, c_2, z) \notin S$ or *vice versa*. In these cases one 'B-factor' is -1 and the other is $p/(1-p)$. Note that $|X \times X| = \alpha^2 n^2$, and that we have $\alpha^2 n^2 - m_z$ triples $(b_1, b_2, z) \notin S$ with $b_1, b_2 \in X$.

(c) $\sum_{z\in V}(\alpha^2 n^2 - m_z)\cdot(\alpha^2 n^2 - m_z - 1)$-times the term $(p/(1-p))^2$.
This accounts for those cases when $(b_1, b_2, z), (c_1, c_2, z) \notin S$.

By the assumption $s \sim f n^{3/2}$ and (3.6), we get

$$\sum_{z\in V} m_z = |(X, X, V)_T| \sim \alpha^2 f n^{3/2}. \tag{3.12}$$

Hence, as $1 - p \sim 1$ and $m_z \leqslant s = O(f n^{3/2}) = o(n^2)$, we obtain the following estimate on the terms as in (b):

$$\begin{aligned}-2\cdot\sum_{z\in V} m_z(\alpha^2 n^2 - m_z)\cdot\frac{p}{1-p} &\sim -2\cdot\sum_{z\in V} m_z(\alpha^2 n^2)\cdot p \sim -2\alpha^2 n^2 p \cdot \sum_{z\in V} m_z\\ &\sim -2\alpha^2 n^{1/2} f \cdot \alpha^2 f n^{3/2} \quad \text{(by (3.12))}\\ &\sim -2\alpha^4 f^2 n^2.\end{aligned}$$

With respect to the terms in (c), we get

$$\begin{aligned}\sum_{z\in V}(\alpha^2 n^2 - m_z)\cdot(\alpha^2 n^2 - m_z - 1)\left(\frac{p}{1-p}\right)^2 &\sim \sum_{z\in V} \alpha^4 n^4 \cdot p^2\\ &\sim \sum_{z\in V} \alpha^4 n^4 f^2 n^{-3} \sim \alpha^4 n^2 f^2.\end{aligned}$$

Consequently, the sum over all three types (a)–(c) is $m - \alpha^4 f^2 n^2 \cdot (1 + o(1))$, which implies (3.11).

3.4. Proof of Lemma 3.3

The proof of Lemma 3.3 is based on the trace method from [21]. Let $T = (V, S) = T_{n,3,p}$. Since every possible triple is present in S with probability p, the definition of $B_{b_1 b_2 z}$ entails that

$$\mathrm{E}(B_{b_1 b_2 z}) = p\cdot(-1) + (1-p)\cdot\frac{p}{1-p} = -p + p = 0 \text{ for all } b_1, b_2, z \in V. \tag{3.13}$$

Let $\lambda_1 \geqslant \cdots \geqslant \lambda_{n^2}$ be the eigenvalues of $\mathbf{A} = \mathbf{A}(T, p)$, and let $\lambda = \|\mathbf{A}\| = \max\{\lambda_1, -\lambda_{n^2}\}$ signify the spectral radius of $\mathbf{A}$. Further, recall that the trace of a matrix, which is defined

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

as the sum of the elements on the main diagonal, equals the sum of the eigenvalues (see [33]). Consequently,

$$\text{Trace}[\mathbf{A}] = \sum_{(b_1,c_2)\in V\times V} \mathbf{a}_{b_1c_2,b_1c_2} = \sum_{i=1}^{n^2} \lambda_i,$$

$$\text{Trace}[\mathbf{A}^k] = \sum_{i=1}^{n^2} \lambda_i^k \quad \text{for any integer } k \geqslant 1.$$

As all eigenvalues of $\mathbf{A}$ are real, for even k we obtain

$$\lambda^k \leqslant \sum_{i=1}^{n^2} \lambda_i^k = \text{Trace}[\mathbf{A}^k].$$

In particular, $\mathrm{E}(\lambda^k) \leqslant \mathrm{E}(\text{Trace}[\mathbf{A}^k])$. We shall prove below that there exists an even $k = k(n)$ such that

$$\mathrm{E}(\text{Trace}[\mathbf{A}^k]) \leqslant (\ln^4 n \cdot f)^k. \tag{3.14}$$

Then Markov's inequality yields the assertion of the lemma:

$$\begin{aligned}\mathbf{P}(\lambda \geqslant \ln^5 n \cdot f) &= \mathbf{P}(\lambda^k \geqslant (\ln^5 n \cdot f)^k)\\ &\leqslant \frac{\mathrm{E}(\lambda^k)}{(\ln^5 n \cdot f)^k} \leqslant \frac{\mathrm{E}(\text{Trace}[\mathbf{A}^k])}{(\ln^5 n \cdot f)^k} \leqslant \frac{(\ln^4 n \cdot f)^k}{(\ln^5 n \cdot f)^k} = o(1).\end{aligned}$$

Thus, the remaining task is to establish (3.14). Let $k > 1$ be an even integer (which we shall specify below). A direct computation yields

$$\text{Trace}[\mathbf{A}^k] = \sum_{b_1=1}^{n}\sum_{c_1=1}^{n}\cdots\sum_{b_k=1}^{n}\sum_{c_k=1}^{n} \mathbf{a}_{b_1c_1,b_2c_2}\cdot \mathbf{a}_{b_2c_2,b_3c_3}\cdots \mathbf{a}_{b_kc_k,b_1c_1}. \tag{3.15}$$

If there is some $1 \leqslant i < k$ such that $(b_i, b_{i+1}) = (c_i, c_{i+1})$, or if $(b_k, b_1) = (c_k, c_1)$, then the entire product $\mathbf{a}_{b_1c_1,b_2c_2}\cdot \mathbf{a}_{b_2c_2,b_3c_3}\cdots \mathbf{a}_{b_kc_k,b_1c_1}$ vanishes, due to the definition of the $\mathbf{a}$s. Therefore, we omit these terms tacitly from now on, *i.e.*, we assume that

$$(b_i, b_{i+1}) \neq (c_i, c_{i+1}) \text{ for all } 1 \leqslant i < k, \text{ and } (b_k, b_1) \neq (c_k, c_1). \tag{3.16}$$

Expanding the $\mathbf{a}$s in (3.15), we get

$$\begin{aligned}\text{Trace}[\mathbf{A}^k] &= \sum_{b_1,\dots,b_k}\sum_{c_1,\dots,c_k}\left(\sum_{z_1\in V}(B_{b_1b_2z_1}\cdot B_{c_1c_2z_1} + B_{b_2b_1z_1}\cdot B_{c_2c_1z_1})\right)\times\cdots\\ &\qquad\times\left(\sum_{z_k\in V}(B_{b_kb_1z_k}\cdot B_{c_kc_1z_k} + B_{b_1b_kz_k}\cdot B_{c_1c_kz_k})\right)\\ &= \sum_{b_1,\dots,b_k}\sum_{c_1,\dots,c_k}\sum_{z_1,\dots,z_k}(B_{b_1b_2z_1}\cdot B_{c_1c_2z_1} + B_{b_2b_1z_1}\cdot B_{c_2c_1z_1})\times\cdots\\ &\qquad\times(B_{b_kb_1z_k}\cdot B_{c_kc_1z_k} + B_{b_1b_kz_k}\cdot B_{c_1c_kz_k}).\end{aligned}$$

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

Moreover, expanding the products, we obtain a sum $\sum_{j=1}^{2^k} X_j$, where each X_j is of the form

$$X_j = X_j(b_1,\ldots,b_k,c_1,\ldots,c_k,z_1,\ldots,z_k) = B_{\beta_1}\cdot B_{\gamma_1}\cdot B_{\beta_2}\cdot B_{\gamma_2}\cdot\ldots\cdot B_{\beta_k}\cdot B_{\gamma_k}. \tag{3.17}$$

Here we either have $\beta_i = (b_i,b_{i+1},z_i)$ and $\gamma_i = (c_i,c_{i+1},z_i)$, or $\beta_i = (b_{i+1},b_i,z_i)$ and $\gamma_i = (c_{i+1},c_i,z_i)$ for $1 \leqslant i < k$. Analogously, either $\beta_k = (b_k,b_1,z_k)$ and $\gamma_k = (c_k,c_1,z_k)$, or $\beta_k = (b_1,b_k,z_k)$ and $\gamma_k = (c_1,c_k,z_k,)$. Note that we may assume that $\beta_i \neq \gamma_i$ for all $i \in \{1,\ldots,k\}$, because by (3.16) the other terms do not contribute to the sum (3.15). Thus, we get

$$\mathrm{Trace}[\mathbf{A}^k] = \sum_{b_1,\ldots,b_k}\sum_{c_1,\ldots,c_k}\sum_{z_1,\ldots,z_k}\sum_{j=1}^{2^k} X_j(b_1,\ldots,b_k,c_1\ldots,c_k,z_1,\ldots,z_k).$$

Now, we reorder the above summation over terms containing exactly b different b_is and c_is and exactly z different z_is. As a notational convenience, we set

$$\mathscr{B} = (b_1,\ldots,b_k,c_1,\ldots,c_k) \text{ and } \mathscr{Z} = (z_1,\ldots,z_k).$$

Moreover, we let $\#\mathscr{B} = |\{b_1,\ldots,b_k,c_1,\ldots,c_k\}|$ signify the number of distinct b_is and c_is occurring in $\mathscr{B}$, and we let $\#\mathscr{Z} = |\{z_1,\ldots,z_k\}|$ denote the number of distinct z_is occurring in $\mathscr{Z}$. Then our goal is to show that

$$\mathrm{E}(\mathrm{Trace}[\mathbf{A}^k]) = \sum_{b=1}^{2k}\sum_{z=1}^{k}\sum_{\substack{\mathscr{B}\\ \#\mathscr{B}=b}}\sum_{\substack{\mathscr{Z}\\ \#\mathscr{Z}=z}}\sum_{j=1}^{2^k}\mathrm{E}(X_j(\mathscr{B},\mathscr{Z})) \leqslant (\ln^4 n\cdot f)^k.$$

We claim that

$$\mathrm{E}(\mathrm{Trace}[\mathbf{A}^k]) = \sum_{b=1}^{k+2}\sum_{z=1}^{k/2}\sum_{\substack{\mathscr{B}\\ \#\mathscr{B}=b}}\sum_{\substack{\mathscr{Z}\\ \#\mathscr{Z}=z}}\sum_{j=1}^{2^k}\mathrm{E}(X_j(\mathscr{B},\mathscr{Z})). \tag{3.18}$$

In fact, fix a $\mathscr{B}$ with $\#\mathscr{B} = b$, and a $\mathscr{Z}$ with $\#\mathscr{Z} = z$, and let

$$X_j = X_j(\mathscr{B},\mathscr{Z}) = B_{\beta_1}\cdot B_{\gamma_1}\cdots B_{\beta_k}\cdot B_{\gamma_k}$$

be a term of the sum corresponding to $\mathscr{B}$ and $\mathscr{Z}$. In order to prove (3.18), we show that if $z > k/2$ or $b > k+2$, then there exists a factor B_δ inside X_j which occurs only once. Then $\mathrm{E}(X_j) = 0$ by (3.13), because B_δ is independent of the remaining factors in X_j.

Assume that all factors B_δ occur at least twice. Then going along the product (3.17) from the left to the right, there are exactly z places where an element of $\mathscr{Z}$ occurs for the first time. At each such place, we get two new 'B-factors', which do not occur to the left in X_j. Thus, there are at least $2z$ different 'B-factors' in X_j. If each of these $2z$ 'B-factors' occurs at least twice in X_j, then $2k \geqslant 4z$, *i.e.*, $z \leqslant k/2$.

Furthermore, if we go through the expression (3.17) from the left to the right, then the first two 'B-factors' use at most four elements of $\mathscr{B}$ for the first time. Moreover, all the remaining 'B-factors' use at most two elements of $\mathscr{B}$ for the first time, because two indices in each 'B-factor' are determined by its predecessor. Thus, in addition to the first two 'B-factors', we need at least $b-4$ different 'B-factors' to use up all the elements of

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

$\mathscr{B}$. Hence, altogether there are at least $2 + (b - 4) = b - 2$ different 'B-factors'. Therefore, if each 'B-factor' occurs at least twice in X_j, then $2(b-2) \leqslant 2k$, *i.e.*, $b \leqslant k+2$. Thus, we have established (3.18).

Let B_α be a factor which occurs exactly $r \geqslant 2$ times in X_j. Then since we assume that $p \leqslant \frac{1}{2}$,

$$\mathrm{E}(B_\alpha^r) = p \cdot (-1)^r + (1-p) \cdot \left(\frac{p}{1-p}\right)^r \leqslant p + \frac{p^r}{(1-p)^{r-1}} \leqslant 2p.$$

As we have at least $\max\{2z, b-2\}$ different 'B-factors' in X_j, we obtain the estimate

$$\mathrm{E}(X_j) \leqslant (2p)^{\max\{2z,b-2\}},$$

where the right-hand side only depends on b and z. Therefore, we just need to show that

$$\sum_{b=1}^{k+2} \sum_{z=1}^{k/2} \sum_{\substack{\mathscr{B} \\ \#\mathscr{B}=b}} \sum_{\substack{\mathscr{Z} \\ \#\mathscr{Z}=z}} 2^k \cdot (2p)^{\max\{2z,b-2\}} \leqslant (\ln^4 n \cdot f)^k. \tag{3.19}$$

Given b, each $\mathscr{B}$ with $\#\mathscr{B} = b$ can be obtained by first picking a subset of b elements from V and then placing these elements into the $2k$ possible places; thus, there are at most $n^b b^{2k}$ ways to choose $\mathscr{B}$. Moreover, as we can assume $b \leqslant 2k$, we get $n^b b^{2k} \leqslant n^b (2k)^{2k}$. Similarly, we can bound the number of sequences $\mathscr{Z}$ with $\#\mathscr{Z} = z$ by $n^z z^k$, and since $z \leqslant k$, we get $n^z z^k \leqslant n^z k^k$. Therefore,

$$\sum_{b=1}^{k+2} \sum_{z=1}^{k/2} \sum_{\substack{\mathscr{B} \\ \#\mathscr{B}=b}} \sum_{\substack{\mathscr{Z} \\ \#\mathscr{Z}=z}} 2^k \cdot (2p)^{\max\{2z,b-2\}} \leqslant \sum_{b=1}^{k+2} \sum_{z=1}^{k/2} 2^{3k} \cdot n^{b+z} \cdot k^{3k} \cdot (2p)^{\max\{2z,b-2\}}.$$

As a next step, we estimate $n^{b+z} \cdot (2p)^{\max\{2z,b-2\}}$. If $2z > b-2$, then $b \leqslant 2z+1$, so that

$$n^{b+z} \cdot (2p)^{\max\{2z,b-2\}} \leqslant n^{3z+1} (2p)^{2z} = n^{3z+1} (2fn^{-3/2})^{2z} = n(2f)^{2z}.$$

On the other hand, if $b - 2 \geqslant 2z$, then $z \leqslant b/2 - 1$, whence

$$n^{b+z} \cdot (2p)^{\max\{2z,b-2\}} \leqslant n^{b+b/2-1} (2p)^{b-2} = n^{b+b/2-1} (2fn^{-3/2})^{b-2} = n^2 (2f)^{b-2}.$$

Furthermore, as $b \leqslant k+2$ and $z \leqslant k/2$, we have $\max\{2z, b-2\} \leqslant k$. Thus, in order to prove (3.19), we just need to show that

$$\sum_{b=1}^{k+2} \sum_{z=1}^{k/2} 2^{3k} \cdot k^{3k} \cdot n^2 \cdot (2f)^k \leqslant (\ln^4 n \cdot f)^k. \tag{3.20}$$

Let k as the smallest even integer $\geqslant \ln n$. Then, for n sufficiently large, we get

$$\sum_{b=1}^{k+2} \sum_{z=1}^{k/2} 2^{3k} \cdot k^{3k} \cdot n^2 \cdot (2f)^k \leqslant (k+2) \cdot (k/2) \cdot 2^{4k} \cdot k^{3k} \cdot n^2 \cdot f^k \leqslant (\ln^4 n)^k \cdot f^k,$$

which yields (3.20) and thus completes the proof.

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

4. Hypergraph problems

The heuristics for Theorems 1.3 and 1.4 make use of the techniques from Sections 2 and 3. In order to apply these techniques directly, we transform random k-uniform hypergraphs into random k-tuple systems. We describe this transformation in Section 4.1. Then, we describe the algorithms for Theorem 1.4 and Theorem 1.3 in Sections 4.2 and 4.3.

4.1. From random hypergraphs to random k-tuple systems

Let $k \in \{3,4\}$, let $0 < p < 1$, and let $H = (V,E)$ be a k-uniform hypergraph. To transform H into a k-tuple system $T_p(H)$, we use the following randomized procedure. For each edge $e = \{y_1,\dots,y_k\} \in E$, let $T(e)$ be the set of the $k!$ possible ordered tuples that can be obtained from $y_1,\dots,y_k$. Letting $p_0 = 1-(1-p)^{1/k!}$, we choose the set $\emptyset \neq X_e \subset T(e)$ of k-tuples that we include into $T_p(H)$ to represent e according to the distribution

$$\mathbf{P}(X_e \text{ is chosen}) = p_0^{|X_e|}(1-p_0)^{k!-|X_e|}p^{-1}.$$

Thus, each edge $e \in E$ gives rise to at least one tuple in $T_p(H)$. The choice of the sets X_e is independent for all $e \in E$. Furthermore, we include each tuple $(x_1,\dots,x_k) \in V^k$ such that $|\{x_1,\dots,x_k\}| < k$ into $T_p(H)$ with probability p_0 independently.

Lemma 4.1. *The k-tuple system $T_p(H_{n,k,p})$ is distributed as a random k-tuple system T_{n,k,p_0}.*

Proof. This is a straightforward computation. □

4.2. Bounding the independence number of random 4-uniform hypergraphs

The heuristic 4-`Alpha` for Theorem 1.4 employs the procedure `BipDisc` from Section 2.1.

Algorithm 5. 4-`Alpha`(H,p)

Input: A 4-uniform hypergraph $H=(V,E)$, $V=\{1,\dots,n\}$, and a number $0<p<1$.
Output: An upper bound on $\alpha(H)$.

1. Construct $T = T_p(H)$ (see Section 4.1). Furthermore, let $V_i = V \times V \times \{i\}$ for $i = 1,2$, and construct a (V_1,V_2)-bipartite graph B as follows: include the edge $\{(v_1,v_2,1),(v_3,v_4,2)\}$ into B if and only if $(v_1,v_2,v_3,v_4) \in T$.
2. Let $p_0 = 1-(1-p)^{1/24}$. If `BipDisc`(B,p_0) answers ‘fail’, then return $|V|$. Otherwise, return $Cn^{1/2}p^{-1/4}$, where C is a sufficiently large constant.

Proof of Theorem 1.4. The completeness of 4-`Alpha` is an immediate consequence of Proposition 2.1. To prove the correctness, assume that there is an independent set I in H such that $a = |I| > n^{1/2}p^{-1/4}$. Let I_1,I_2,I_3,I_4 be disjoint subsets of I such that $|I_j| = a/4$ for $j = 1,2,3,4$. Then $E_B(I_1 \times I_2 \times \{1\}, I_3 \times I_4 \times \{2\}) = \emptyset$. Hence, if `BipDisc`$(B,p_0)$ outputs ‘low discrepancy’, then (2.1) implies that

$$\left(\frac{a}{4}\right)^4 p_0 \leqslant c_1\left(\frac{a}{4}\right)^2 n\sqrt{p_0} + n^2\exp(-n^2p_0/c_1) \leqslant \frac{c_1}{8}a^2n\sqrt{p_0},$$

where c_1 denotes a sufficiently large constant. Since $p_0 \geqslant \frac{p}{24}$, we get $a^2 \leqslant 32c_1n(p/24)^{-1/2}$. Hence, $a \leqslant Cn^{1/2}p^{-1/4}$ for a certain constant C. □

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press

4.3. Bounding the independence number of random 3-uniform hypergraphs

Let $\varepsilon > 0$ be an arbitrarily small but fixed number. The following algorithm tries to certify that the independence number of the 3-uniform hypergraph H is $\leqslant \varepsilon n$.

Algorithm 6. `3-Alpha`(H, p)

Input: A 3-uniform hypergraph $H = (V, E)$ with vertex set $V = \{1, \ldots, n\}$, and a number $0 < p < 1$.

Output: An upper bound on $\alpha(H)$.

1. Construct the triple system $T = T_p(H)$ (see Section 4.1). Let $p_0 = 1 - (1-p)^{1/6}$ and $Q = \{(x, y, z) \in T : |\{x, y, z\}| < 3\}$. If $|Q| > 4n^2 p_0$, then halt with output $|V|$.
2. If `TripleDisc`$_{\varepsilon/2}(T, p_0)$ answers 'fail', then return $|V|$. Otherwise, return εn.

Proof of Theorem 1.3. Note that $|Q|$ has binomial distribution with mean $(3 + o(1))n^2 p_0$. Hence, the Chernoff bound (1.2) implies that $|Q| \leqslant 4n^2 p_0$ almost surely. Thus, the completeness of `3-Alpha` follows from Proposition 3.1.

To prove the correctness, suppose that `3-Alpha`(H, p) outputs εn. Furthermore, assume for contradiction that H has an independent set I of cardinality εn. As `TripleDisc`$_{\varepsilon/2}(T, p)$ answers 'low discrepancy', the correctness of `TripleDisc`$_\varepsilon$ (see Proposition 3.1) implies that $|T| \sim n^3 p_0$, and that

$$|(I, I, I)_T| \sim |I|^3 p = \varepsilon^3 n^3 p_0.$$

However, as I is an independent set in H, we obtain the contradiction $|(I, I, I)_T| \leqslant |Q| \leqslant 4n^2 p_0 = o(n^3 p_0)$, thereby proving the correctness of `3-Alpha`. □

Acknowledgement

We are grateful to Uri Feige for helpful discussions.

References

[1] Achlioptas, D. and Moore, C. (2002) The asymptotic order of the k-SAT threshold. In *Proc. 43rd FOCS*, pp. 779–788.

[2] Achlioptas, D., Naor, A. and Peres, Y. (2003) The fraction of satisfiable clauses in a typical formula. In *Proc. 44th FOCS*, pp. 362–370.

[3] Achlioptas, D. and Peres, Y. (2003) The threshold for random k-SAT is $2^k \ln 2 - O(k)$. In *Proc. 35th STOC*, pp. 223–231.

[4] Alon, N. and Kahale, N. (1997) A spectral technique for coloring random 3-colorable graphs. *SIAM J. Comput.* **26** 1733–1748.

[5] Alon, N. and Spencer, J. (1991) *The Probabilistic Method*, Wiley.

[6] Ben-Sasson, E. (2001) Expansion in proof complexity. PhD thesis, Harvard University.

[7] Chen, H. and Frieze, A. (1996) Coloring bipartite hypergraphs. In *Proc. 5th IPCO*, pp. 345–358.

[8] Chung, F. K. R. and Graham, R. L. (1992) Cohomological aspects of hypergraphs. *Trans. Amer. Math. Soc.* **334** 365–388.

[9] Coja-Oghlan, A. (2005) The Lovász number of random graphs. *Combin. Probab. Comput.* **14** 439–465.

[10] Coja-Oghlan, A., Goerdt, A., Lanka, A. and Schädlich, F. (2004) Techniques from combinatorial approximation algorithms yield efficient algorithms for random $2k$-SAT. *Theoret. Comput. Sci.* **329** 1–45.

[11] Coja-Oghlan, A., Moore, C. and Sanwalani, V. (2003) MAX k-CUT and approximating the chromatic number of random graphs. In *Proc. 30th ICALP*, pp. 200–211.

[12] Coja-Oghlan, A. and Taraz, A. (2004) Exact and approximative algorithms for coloring $G(n, p)$. *Random Struct. Alg.* **24** 259–278.

[13] Dubois, O., Boufkhad, Y. and Mandler, J. (2000) Typical random 3-SAT formulae and the satisfiability threshold. In *Proc. 11th SODA*, pp. 126–127.

[14] Feige, U. (2002) Relations between average case complexity and approximation complexity. In *Proc. 24th STOC*, pp. 534–543.

[15] Feige, U. and Kilian, J. (1998) Zero knowledge and the chromatic number. *J. Comput. Syst. Sci.* **57** 187–199.

[16] Feige, U. and Ofek, E. (2003) Spectral techniques applied to sparse random graphs. Report MCS03-01, Weizmann Institute of Science.

[17] Feige, U. and Ofek, E. (2004) Easily refutable subformulas of large random 3CNF formulas. *Random Struct. Alg.* 27 (2005) 251–275.

[18] Flaxman, A. (2003) A spectral technique for random satisfiable 3CNF formulas. In *Proc. 14th SODA*, pp. 357–363.

[19] Friedgut, E. (1999) Necessary and sufficient conditions for sharp thresholds of graph properties and the k-SAT problem. *J. Amer. Math. Soc.* **12** 1017–1054.

[20] Friedman, J. and Goerdt, A. (2001) Recognizing more unsatisfiable random 3-Sat instances efficiently. In *Proc. 28th ICALP*, pp. 310–321.

[21] Füredi, Z. and Komlós, J. (1981) The eigenvalues of random symmetric matrices. *Combinatorica* **1** 233–241.

[22] Goerdt, A. and Krivelevich, M. (2001) Efficient recognition of random unsatisfiable k-SAT instances by spectral methods. In *Proc. 18th STACS*, pp. 294–304.

[23] Goerdt, A. and Lanka, A. (2003) Recognizing more random unsatisfiable 3-SAT instances efficiently. *Electron. Notes in Discrete Math.* **16**.

[24] Hajiaghayi, M. T. and Sorkin G. B. (2003) The satisfiability threshold of random 3-SAT is at least 3.52. IBM Research Report RC22942.

[25] Håstad, J. (1999) Clique is hard to approximate within $n^{1-\varepsilon}$. *Acta Mathematica* **182** 105–142.

[26] Håstad, J. (2001) Some optimal inapproximability results. *J. Assoc. Comput. Mach.* **48** 798–859.

[27] Janson, S., Łuczak, T. and Ruciński, A. (2000) *Random Graphs*, Wiley.

[28] Kaporis, A. C., Kirousis, L. M. and Lalas, E. G. (2003) Selecting complementary pairs of literals. *Electron. Notes in Discrete Math.* **16**.

[29] Kirousis, L., Kranakis, E., Krizanc, D. and Stamatiou, Y. (1998) Approximating the unsatisfiability threshold of random formulas. *Random Struct. Alg.* **12** 253–269.

[30] Krivelevich, M. and Sudakov, B. (1998) The chromatic numbers of random hypergraphs. *Random Struct. Alg.* **12** 381–403.

[31] Krivelevich, M. and Sudakov, B. (2003) The largest eigenvalue of sparse random graphs. *Combin. Probab. Comput.* **12** 61–72.

[32] Krivelevich, M. and Vu, V. H. (2002) Approximating the independence number and the chromatic number in expected polynomial time. *J. Combin. Optim.* **6** 143–155.

[33] Strang, G. (1988) *Linear Algebra and its Applications*, Harcourt Brace Jovanovich.

[34] Vilenchik, D. (2004) Finding a satisfying assignment for random satisfiable 3CNF formulas. MSc thesis, Weizmann Institute of Science.

https://doi.org/10.1017/S096354830600784X Published online by Cambridge University Press