How to refute random nonsatisfiable formulas

Uriel Feige
Weizmann Institute

Part of this work was done at Microsoft Research
3CNF formulas

\((x_1 \lor x_2 \lor \neg x_3) \land (x_2 \lor \neg x_4 \lor x_5) \land \cdots\)

n variables,
m clauses,
3 literals per clause.
**Satisfiable** if some assignment satisfies at least one literal in every clause.
Algorithmic tasks

Accept only satisfiable formulas.

- NP-complete.
- Witness for satisfiability – a satisfying assignment.

Accept only non-satisfiable formulas.

- coNP-complete.
- No witnesses for non-satisfiable formulas, unless NP=coNP.
Average case complexity

Want algorithms that work well on typical instances.

Want to discover distributions on which problems are hard (e.g., for cryptography).

Average case complexity of refutation relates to worse case complexity of approximation.
Average Case Refutation

- **Deterministic:** polytime algorithm that aborts on all satisfiable formulas, and accepts most* nonsatisfiable formulas.
- **Nondeterministic:** polysize witnesses that can be checked in polynomial time, never exist for satisfiable formulas, and exist for most* nonsatisfiable formulas.

* from a given distribution.
Satisfaction versus refutation

For worst case complexity, deterministic algorithms for satisfiability are equivalent to deterministic algorithms for refutation.

For average case complexity, no such equivalence is known.
Random 3CNF

\[(x_1 \lor x_2 \lor \bar{x}_3) \land (x_2 \lor \bar{x}_4 \lor x_5) \land \cdots\]

\(n\) variables, \(m\) clauses, 3 literals per clause.

Clauses chosen independently at random. Random formula of density \(d\).

\(m = dn\).
Density threshold [Friedgut 1999]
Challenge

Refute dense formulas. Gets more difficult closer to threshold.

(Proof: suffices to refute a sufficiently large prefix of a very dense random formula.)
Refutation by approximation

When $m \gg n$, every assignment satisfies roughly $7m/8$ clauses of a random formula. An algorithm for approximating max 3SAT within a ratio strictly better than $7/8$ would refute most dense 3SAT formulas. Unfortunately, approximating max 3SAT (in the worst case) beyond $7/8$ is NP-hard [Hastad 2001].
Turning the argument around

What if refuting random 3SAT is hard?
Would imply hardness of approximation:
• Max 3SAT beyond 7/8 (PCP + Fourier).
• Min bisection, dense k-subgraph, bipartite clique, 2-catalog segmentation, treewidth, etc.

A good rule of thumb. Most of its predictions (with weaker constants) can be proved assuming NP not in subexponential time [Khot 2006].
State of the art

Current best refutation algorithms are based on spectral techniques [Goerdt and Krivelevich 2001].

Deterministic refutation, \( d > n^{0.5} \) [Feige and Ofek 2005].

Nondeterministic refutation, \( d > n^{0.4} \) [Feige, Kim, Ofek 2006].
In this talk

Random polarity formula of density $d$.

An adversary chooses an arbitrary 3CNF formula with $dn$ clauses.

The polarity of each literal is flipped independently at random with probability $1/2$.

Algorithm needs to refute the new formula.
Refutation arithmetic

In an assignment, fraction of clauses in which 1, 2 or 3 literals are satisfied will be denoted by \( a, b \) and \( c \) respectively.

For refutation, need to show that for every assignment \( a + b + c < 1 \).
Statistics on literals

Majority vote assignment satisfies the largest number of literals.
For random polarity, satisfies \( 3m/2 + O(n\sqrt{d}) \) literals.

Hence, can certify that:

\[
a + 2b + 3c \leq \frac{3}{2} + \Omega(1/\sqrt{d})
\]
Pairs of literals

Construct an $n$ by $n$ symmetric matrix $M$. Every clause contributes to six entries.

$$x_1 \lor x_2 \lor x_4$$

\[
\begin{array}{cc}
-1 & +1 \\
-1 & +1 \\
+1 & +1 \\
\end{array}
\]
Discrepancy (cut norm)

Maximize $x^T My$ over all § 1 vectors $x$ and $y$.

For indicator vector of an assignment, $x=y$, $\text{disc} = (8a + 8b - 6)m$. (3NAE)

For random polarity, the expected contribution of a clause is 0. Hence, w.h.p.

$$\text{disc} \leq O(\sqrt{n} \sqrt{m}) = O(m / \sqrt{d})$$
Bounding the cut norm

The Grothendieck constant: a semidefinite programming relaxation approximates the cut norm within a constant factor [Alon and Naor, 2006].

Hence can certify that:

\[ 2a + 2b \leq \frac{3}{2} + O(1/\sqrt{d}) \]
Max 3LIN2

Assignment that satisfies in as many clauses as possible an odd number of literals (either one or three literals).

Namely, clauses are satisfied as 3XOR, or equivalently, as 3LIN2, linear equation mod 2 over 3 variables.

In LIN2 negation of a variable is equivalent to flipping the right hand side.
Max 3LIN2

\[ X_1 + X_2 + X_3 = 1 \pmod{2} \]
\[ X_2 + X_3 + X_4 = 1 \pmod{2} \]
\[ X_1 + X_6 + X_7 = 0 \pmod{2} \]

...

Satisfiability: in P.
Maximization: inapproximable [Hastad 2001].
Even subsystems

A subset of the equations that contains every variable an even number of times.

Observation: inconsistent if right hand side is 1 in an odd number of equations.

Observation: 3LIN nonsatisfiable iff it has an inconsistent even subsystem (proof: Gaussian elimination).

Small even subsystem: at most $n^\epsilon$ equations.
Decomposition

Improving over [Naor and Versraete 2005]:

**Theorem:** every 3LIN2 system with at least $cn\sqrt{n \log \log n}$ equations has a small even subsystem. Moreover, it can be found efficiently.

**Corollary:** can efficiently find at least $n^{3/2} - \varepsilon$ disjoint even subsystems.
Random polarity 3LIN2

Arbitrary instance:

\[
\begin{align*}
X_1 + X_2 + X_3 &= 1 \pmod 2 \\
X_2 + X_3 + X_4 &= 1 \pmod 2 \\
X_1 + X_6 + X_7 &= 0 \pmod 2 \\
X_8 + X_2 + X_3 &= 1 \pmod 2 \\
X_2 + X_7 + X_4 &= 1 \pmod 2 \\
X_1 + X_6 + X_9 &= 0 \pmod 2
\end{align*}
\]
Random polarity 3LIN2

Random polarity variant:

\[ X_1 + X_2 + X_3 = 1 \pmod{2} \]
\[ X_2 + X_3 + X_4 = 0 \pmod{2} \]
\[ X_1 + X_6 + X_7 = 1 \pmod{2} \]
\[ X_8 + X_2 + X_3 = 1 \pmod{2} \]
\[ X_2 + X_7 + X_4 = 0 \pmod{2} \]
\[ X_1 + X_6 + X_9 = 0 \pmod{2} \]
Random polarity even subsystems

Every even subsystem becomes inconsistent with probability $1/2$.

**Corollary:** in a random polarity 3LIN2 system of size $cn \sqrt{n \log \log n}$, one can almost surely efficiently find $n^{3/2-\varepsilon}$ disjoint inconsistent subsystems. Hence can certify that:

$$a + c \leq 1 - n^{-\varepsilon}$$
Doing the refutation arithmetic

Majority vote \[ a + 2b + 3c \leq 3/2 + O(1/\sqrt{d}) \]

Discrepancy \[ 2a + 2b \leq 3/2 + O(1/\sqrt{d}) \]

Even subsystems \[ a + c \leq 1 - n^{-\epsilon} \]

Summing up \[ 4(a + b + c) < 4 \quad \text{Q.E.D.} \]
Summary so far

Random polarity 3CNF model.
Refutation algorithms at densities

\[ c \sqrt{n \log \log n} \]

Combination of algorithmic tools (SDP) and extremal hypergraph theory.
Smoothed model

An adversary chooses an arbitrary 3CNF formula with $d_n$ clauses.
The polarity of each literal is flipped independently at random with probability $\varepsilon$.
Algorithm needs to refute the new formula.

Small but significant change to random polarity model, even when $\varepsilon = 0.49$. 
Previous refutation arithmetic

Majority vote \[ a + 2b + 3c \leq 3/2 + O(1/\sqrt{d}) \]

Discrepancy \[ 2a + 2b \leq 3/2 + O(1/\sqrt{d}) \]

Even subsystems \[ a + c \leq 1 - n^{-\varepsilon} \]

Summing up \[ 4(a + b + c) < 4 \quad \text{Q.E.D.} \]
What goes wrong?

Majority vote: \[ a + 2b + 3c \leq \frac{3}{2} + O(1) \]

Discrepancy: \[ 2a + 2b \leq \frac{3}{2} + O(1) \]

Even subsystems: \[ a + c \leq 1 - n^{-\epsilon} \]

Summing up: \[ 4(a + b + c) < 4 + O(1) \]
What can we hope for?

An $\varepsilon$-smoothed 3CNF formula with $m$ clauses contains a random polarity subformula with $\varepsilon^3m$ clauses. Find this subformula, and apply to it the random polarity algorithm. Will require an overhead of $\varepsilon^{-3}$ in density.

**Problem:** how can we find this subformula?
What we actually do

Break formula into two unequal parts.
In the smaller part, just look for inconsistent subsystems.
Append to the smaller part additional clauses from the larger part, so as to make the resulting formula have a balanced majority vote assignment and low discrepancy.
This can be done using LP with SDP as a separation oracle, followed by randomized rounding.
The result

\( \varepsilon \)-smoothed 3CNF model.

Refutation algorithms at densities

\[ c \varepsilon^{-2} \sqrt{n \log \log n} \]

Somewhat better dependency on \( \varepsilon \) than our initial hope.
Where do we stand?

Models: random, random polarity, and $\varepsilon$-smoothed.

Refutation arithmetic reduces refuting 3SAT to strongly refuting max-3LIN2 (with overhead of $\varepsilon^{-2}$ in the density).

Need to show that at least $\Omega(n\sqrt{d})$ equations are unsatisfiable.
Strong refutation of max-3LIN2

Approach: even subsystems of size $O(\sqrt{d})$. For arbitrary formulas (random polarity), even subsystems exist and can be found efficiently when $d > \sqrt{n \log \log n}$.

For random formulas, even subsystems exist when $d > n^{0.4}$ [Feige, Kim, Ofek 2006] but can be found efficiently only when $d > n^{0.5}$. 
Refutation densities

Random 3CNF:
Deterministic refutation, $d > n^{0.5}$ [Feige and Ofek 2005].
Nondeterministic refutation, $d > n^{0.4}$ [Feige, Kim, Ofek 2006].

$\epsilon$-smoothed 3CNF:
Deterministic refutation, $d > \epsilon^{-2} \sqrt{n \log\log n}$. 