Phase Transition Behavior of Cardinality and XOR Constraints

Yash Pote – NUS
Saurabh Joshi – IIT-Hyderabad
Kuldeep S. Meel – (NUS) National University of Singapore

The Problem

Linear Equations (in mod 2)— $O(n^3)$

Instance: A uniformly random matrix $A \in \{0,1\}^{m \times n}$, a random vector $b \in \{0,1\}^m$.

Question: Is there a vector $x \in \{0,1\}^n$, such that $Ax = b$.

$$\mathrm{A} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \qquad \mathrm{b} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\mathrm{x} = \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

The Problem

CARD-XOR – NP-Complete

Instance: A uniformly random matrix $A \in \{0,1\}^{m \times n}$, a random vector $b \in \{0,1\}^m$, and an integer $w > 0$.

Question: Is there a vector $x \in \{0,1\}^n$, of Hamming weight $\leq w$, such that $Ax = b$.

$$A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad b = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad w = 1$$

$$x = \left\{ \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

Where do you find CARD-XOR

Determining the satisfiability of CARD-XOR formulas is of importance in:

- Model Counting
- Discrete Integration
- Approximate Inference

Where do you find CARD-XOR

Determining the satisfiability of CARD-XOR formulas is of importance in:

- Model Counting
- Discrete Integration
- Approximate Inference

- Central problem in coding theory where it is known as Maximum Likelihood Decoding.
- The hardness of breaking the LPN cryptosystem.

Why call it CARD-XOR

We encode the:

- Hamming Weight Constraint as a Cardinality Constraint
- Matrix Equation as a system of XORs

Hence CARD-XOR.

Encoding into CNF

- We have a set of n Boolean variables.
  $\{x_1, x_2 ... x_n\} = \{0, 1 ... 0\}$
- A cardinality constraint counts the number of variables set to 1 (True) in an assignment.

The Encoding

Cardinality Constraints

A cardinality constraint may be defined over boolean variables by

$$\sum_{i=1}^{n} x_i \triangleright w$$

- $w \in \mathbb{Z}$
- $\triangleright \in \{\leq, \geq, =\}$

Example: $x_1 + x_2 + x_3 + x_4 \leq 5$.
Notice that these are just extensions of the usual clause constraints,

- *clause* $:\geq,\ w = 1$
- **cardinality**: $\geq,\ w \geq 1$

XORs

- Linear equations in mod 2 are just XORs.
- $A = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{bmatrix} \quad x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \quad b = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Is:

$$\begin{aligned} x_1 \oplus \quad\quad x_3 &= 0 \\ x_2 \oplus x_3 &= 1 \end{aligned}$$

Putting both encodings together, we get a Cardinality-XOR (CARD-XOR) formula.

The CARD-XOR problem

The CARD-XOR constraint

Instance: $\mathbf{m}$ random XOR constraints, and an integer $w > 0$.
Question: Is there a vector $x \in \{0, 1\}^n$ of cardinality $\leq w$, such that it satisfies the XORs?

The CARD-XOR problem

The CARD-XOR constraint

Instance: **m** random XOR constraints, and an integer $w > 0$.
Question: Is there a vector $x \in \{0, 1\}^n$ of cardinality $\leq w$, such that it satisfies the XORs?

Now we will look at some properties of these constraints—

What are Phase Transitions

- Sudden sharp transformation from one state to another at a certain point.
- In our case, we see a sudden change in satisfiability on varying the parameters **m** (number of XORs) and **w** (cardinality).
- This kind of analysis originates from statistical physics where we see similar discontinuities in behavior in large systems when some thermodynamic variable is varied.
  Ex. States of matter – Ice, water and vapor.

What are Phase Transitions

- Sudden sharp transformation from one state to another at a certain point.
- In our case, we see a sudden change in satisfiability on varying the parameters **m** (number of XORs) and **w** (cardinality).

- Behaviour observed in many randomly generated problem instances.
  - NP-Complete - k-CNF($k > 2$), Graph Coloring, CNF-XOR...

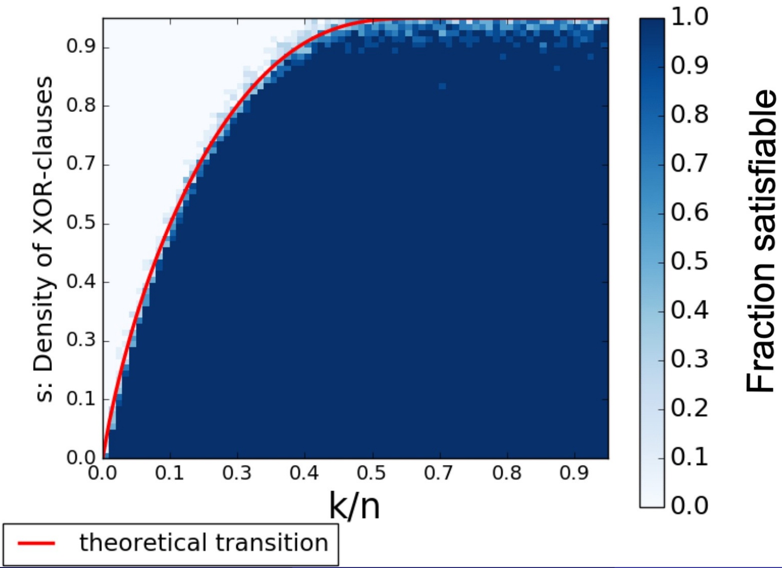
What are Phase Transitions

- Sudden sharp transformation from one state to another at a certain point.
- In our case, we see a sudden change in satisfiability on varying the parameters **m** (number of XORs) and **w** (cardinality).
- Behaviour observed in many randomly generated problem instances.
  - NP-Complete - k-CNF($k > 2$), Graph Coloring, CNF-XOR...
  - P - XORSAT, Arc-Consistency (AC3)...
  - PSPACE - QSAT, Modal K...
- Interestingly the complexity of solving the problem is also seen to peak at the same parameter thresholds, independent of the algorithm used.

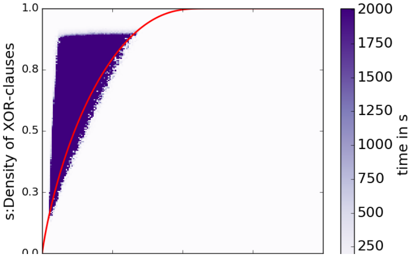
Showing the Phase Transition – Proof Sketch

- Step 1: We know the exact number of solutions of a cardinality constraint .$\#F = \sum_{i=0}^{w} \binom{n}{i}$.
- Step 2 : We can estimate what fraction of these solutions also satisfy m random XOR formulas.
  It is 2^{-m}.
- Step 3: The Phase transition is where #solutions goes to 0 w.h.p. It is $\#F \times 2^{-m}$.

Theoretical bounds and Experimental Verification

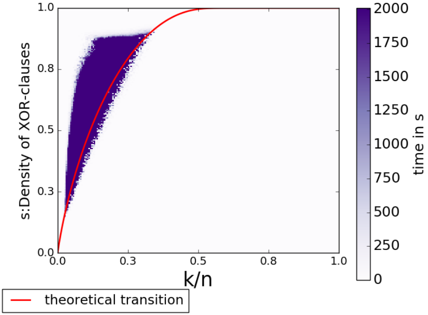


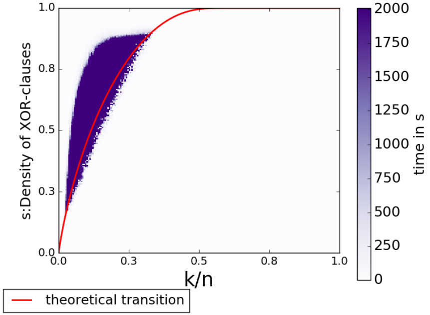
Insights from the runtime behavior of a State-of-the-Art SAT Solver



Encodings Don't Matter

1. Adder (Not Arc-Consistent)
2. BDD
3. Cardinality Networks





Branching Heuristics Do

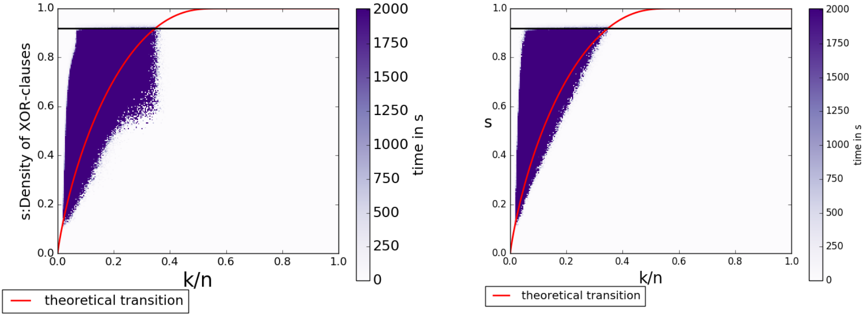


Figure: Polarity Caching vs. Always False

Future Exploration

- Extend study to pseudo boolean constraints, which are more general.

Pseudo-Boolean Constraints

A (linear) PB constraint may be defined over boolean variables by

$$\sum_i a_i . l_i \triangleright d$$

with

- $a_i, d \in \mathbb{Z}$
- $l_i \in \{x_i, \overline{x_i}\}, x_i \in \mathbb{B}$
- $\triangleright \in \{>, <, \leq, \geq, =\}$

Example: $3x_1 - 10x_2 + 2\overline{x_3} + x_4 \leq 5$

Thanks for your attention!
Any questions?

CryptoMiniSat

- We use only CryptoMiniSat for evaluation as it is optimized for CNF-XOR formulas, via tightly integrated Gauss-Jordan elimination and SAT solving.
- Alternate methods could be SMT solvers(z3) or PB solvers(OpenWBO, MiniSAT+), but no dedicated support for handling PB+XOR.
- To the best of our knowledge, there do not exist specialized solvers that can handle CNF-PB-XOR formulas efficiently.