[thm]Note

The Reverse Ising Problem

Isaac Martin and Andrew Moore

University of Texas at Austin

July 26, 2023

Circuits

For the rest of this presentation fix X to be an index set and let $\Sigma = \{-1,1\}$ or $\{0,1\}$. We can switch between $\{0,1\}$ and $\{-1,1\}$ conventions by the change of variables $x \mapsto 2x-1$. A **circuit** is a tuple (N, M, f) where

- $N, M \subseteq X$ are arbitrary finite disjoint subsets of X. We call N the collection of *input* indices or vertices and M the collection of *output* indices/vertices.
- $f : \Sigma^N \longrightarrow \Sigma^M$ is an arbitrary function – the *logic* of the circuit.

Note Σ^N is the collection of functions $N \longrightarrow \Sigma$ and is isomorphic to $\overbrace{\Sigma \times \ldots \times \Sigma}^{|N| \text{ times}}$. Σ^N is the *input spinspace* and Σ^M is the *output spinspace*.

Ising Systems

An **Ising system** is a pair (X, H), often referred to as simply X, where

- X is the set from the previous slide, often a subset of $\mathbb{N}$
- $H \in \mathbb{R}[X]$ is a multilinear quadratic polynomial called the *Hamiltonian* of X.

The **state space** of X is Σ^X. An Ising system X in state $\sigma \in \Sigma^X$ has energy $H(\sigma)$ given by evaluating the Hamiltonian at σ.

Solving Circuits with Ising Systems

We would like to design Ising systems (X,H) with the following features:

(1) A subset $N \subseteq X$ of spins whose state can be fixed

(2) A subset $M \subseteq X$ whose states vary freely with dynamics

(3) For a choice $\sigma_N \in \Sigma^N$, the most likely spin state in $\sigma_M \in \Sigma^M$ is $f(\sigma_N)$, where $f : \Sigma^N \to \Sigma^M$ is some function.

Stated another way, given an abstract circuit (N,M,f), we want to design Ising systems such that for every choice of input state $\sigma|_N$, the state σ' which minimizes energy among all states matching σ in input is a correct spin state. That is,

$$\arg\min_{\sigma' \in \mathcal{L}(\sigma)} H(\sigma') \in \mathcal{R}(f) \text{ for all } \sigma \in \Sigma^X.$$

In this situation we say that (X,H) *solves* the circuit (N,M,f).

More terminology

We often let $A = X \setminus (N \cup M)$ be the set of **auxiliary** spins.

For each input spin state $\sigma \in \Sigma^N$ we call $\{\sigma\} \times \Sigma^{M \cup A}$ the *input level* of σ. This is verbally useful – an Ising system (X, H) solves a circuit (N, M, f) if the correct output $f(\sigma)$ is the minimizer of its input level.

Examples

AND

XOR

Dynamics and our Goal

We are only interested in finding Ising systems such that the correct answer of each input minimizes the Hamiltonian on its input level. This does *not* necessarily yield good dynamics, but it is a necessary condition for good dynamics to be present.

Our Goal: Find robust methods for algorithmically finding Ising systems which solve arbitrary circuits. Work on dynamics later.

XOR is the first example of a circuit which is infeasible without auxiliaries. This is common – an Ising Hamiltonian only has access to quadratic terms and is hence not especially expressive.

What would a **higher degree Hamiltonian** look like?

All Circuits are Solvable via Higher Degree Hamiltonians

Proposition 2.1

Any circuit (N, M, f) can be solved without auxiliaries by a multilinear polynomial H of high enough degree.

Key Fact: Any pseudo boolean function $f : \Sigma^X \to \mathbb{R}$ can be uniquely represented by a multilinear polynomial [1].

Proof:

Rosenberg Reduction

These higher degree Hamiltonians can actually be reduced to quadratic polynomials at the cost of adding auxiliary variables using **Rosenberg reduction.**

Observation: For $x, y, z \in \{0, 1\}$ the following equivalences hold:

$xy = z$ iff $xy - 2xz - 2yz + 3z = 0$

$xy \neq z$ iff $xy - 2xz - 2yz + 3z > 0$.

Rosenberg reduction works by replacing products with new auxiliary variables and penalizing “incorrect” values of the new variables.

Example: Let $f(x_1, x_2, x_3) = x_1x_2x_3$. This has minimum value at $x_1 = x_2 = x_3 = 0$.

Full Rosenberg Algorithm

REDUCEMIN(f)

Input: A pseudo-Boolean function f given by its multi-linear polynomial form (1).

Initialize: Set $M \stackrel{\text{def}}{=} 1 + 2\sum_{S \subseteq \mathbf{V}} |c_S|$, $m = n$, and $f^n = f$.

Loop: While there exists a subset $S^* \subseteq \mathbf{V}$ for which $|S^*| > 2$ and $c_{S^*} \neq 0$ repeat:

1. Choose two elements i and j from S^* and update
   $c_{\{i,j\}} = c_{\{i,j\}} + M$, set
   $c_{\{i,m+1\}} = c_{\{j,m+1\}} = -2M$ and
   $c_{\{m+1\}} = 3M$, and
   for all subsets $S \supseteq \{i,j\}$ with $c_S \neq 0$ define
   $c_{(S \setminus \{i,j\}) \cup \{m+1\}} = c_S$ and set $c_S = 0$.
2. Define $f^{m+1}(x_1, \ldots, x_{m+1}) = \sum_{S \subseteq \mathbf{V}} c_S \prod_{k \in S} x_k$, and set $m = m + 1$.

Output: Set $g = f^m$.

All circuits solvable with auxiliaries

Proposition 2.2

Let $X \subseteq \mathbb{N}$ be infinite and N, M be finite disjoint subsets. For any choice of f, the circuit (N, M, f) is solvable with an Ising system. Since $|X| > |N \cup M|$ in this case, we sometimes say that X is **solvable with auxiliary spins**.

Notice that this lemma says nothing about the *number* of auxiliary spins needed to solve a circuit; in general, it can be quite large.

Proof. Take the hamming objective function $\mathrm{ham} : \Sigma^{N \cup M} \longrightarrow \mathbb{R}$ defined to be the hamming distance from σ to the (unique) correct spin state whose N coordinates match those of σ:

$$\mathrm{ham}(\sigma) = d(\sigma_M, f(\sigma_N)).$$

This has minimum value 0 obtained precisely at spins with correct output coordinates. It is also a pseudo-boolean function and hence can be written uniquely as a multilinear polynomial. Add auxiliary variables until the degree of this polynomial is 2 using, for instance, Rosenberg reduction. The obtained quadratic will be an Ising Hamiltonian in $|N \cup M \cup A|$ variables where A is the set of auxiliary variables added during the reduction step. □

References

[1] Peter L. Hammer Endre Boros. "Pseudo-Boolean optimization". In: Discrete Applied Mathematics 123 (2002), pp. 155–225. DOI: 10.1016/S0166-218X(01)00341-9.