

THE REVERSE ISING PROBLEM

ISAAC MARTIN

1. FOUNDATIONS

Definition 1.1. Let $\Sigma = \{-1, +1\}$. An **Ising circuit** is a pair (G, f) where G is a finite set with a partition $G = N \cup M$ and f is a function $f : \Sigma^N \rightarrow \Sigma^M$. For convenience we always assume $N = \{1, \dots, n\}$ and $M = \{n+1, \dots, n+m\}$.

Partial Ising Circuits.

Definition 1.2. As always, let $\Sigma = \{-1, +1\}$ and let (G, f) be an Ising circuit with $G = N \cup M$. An **Ising subcircuit** of (G, f) is some pair (G', f') such that $G' = N \cup M'$ with $M' \subset M$ and f' agrees with f on the M' coordinates; i.e. there is some function $g : \Sigma^N \rightarrow \Sigma^{M \setminus M'}$ such that $f = f' \times g$.

Definition 1.3. Let $\Sigma = \{-1, +1\}$ and let (G, f) be an Ising circuit with further decompositions of the output space into $M = M_1 \cup M_2$ and the logic into $f = f_1 \times f_2$. We say that (G, f) is *partially solvable* with respect to M_2 if there exists some Hamiltonian such that

$$(s, f_1(s), f_2(s)) < (s, f_1(s), t)$$

for all $s \in \Sigma^N$ and $f_2(s) \neq t \in \Sigma^{M_2}$.

Proposition 1.4. Let (G, f) be an Ising circuit with subcircuit $(N \cup M_1, f_1)$, and set $M_2 = M \setminus M_1$. If the subcircuit $(G_1 = N \cup M_1, f_1)$ is solvable and (G, f) is partially solvable with respect to M_2 then (G, f) is solvable.

Proof. Suppose (G_1, f_1) is solvable with Hamiltonian H_1 and (G, f) is partially solvable by Hamiltonian H_2 . By definition this means

$$H_1(s, f_1(s)) < H_1(s, r) \quad \text{for all } s \in \Sigma^N \text{ and } f_1(s) \neq r \in \Sigma^{M_1}$$

and

$$H_2(s, f_1(s), f_2(s)) < H_2(s, f_1(s), t) \quad \text{for all } s \in \Sigma^N \text{ and } f_2(s) \neq t \in \Sigma^{M_2}.$$

Define $H_\lambda(s, r, t) = H_2(s, r, t) + \lambda H_1(s, r)$. By definition, H_λ is a Hamiltonian which solves (G, f) if and only if for all $(r, t) \neq (f_1(s), f_2(s))$,

$$\begin{aligned} H_\lambda(s, r, t) > H_\lambda(s, f_1(s), f_2(s)) &\iff H_\lambda(s, r, t) - H_\lambda(s, f_1(s), f_2(s)) > 0 \\ &\iff H_2(s, r, t) - H_2(s, f_1(s), f_2(s)) + \lambda(H_1(s, r) - H_1(s, f_1(s))) > 0 \\ &\iff H_2(s, r, t) - H_2(s, f_1(s), f_2(s)) > \lambda(H_1(s, f_1(s)) - H_1(s, r)). \end{aligned}$$

Set $\alpha = \max_{s,r} (H_1(s, f_1(s)) - H_1(s, r))$ and $\beta = \min_{s,r,t} (H_2(s, r, t) - H_2(s, f_1(s), f_2(s)))$. Then any choice of λ such that $\beta > \lambda\alpha$ will ensure the above inequality is satisfied for all $s, r \neq f_1(s)$ and $t \neq f_2(s)$. \square

Remark 1.5. The converse of Proposition 1.4 is false; solvability of (G, f) does not necessarily imply the solvability of its subcircuits.

Remark 1.6. Decomposing an Ising circuit G into $G_1 = N \cup M_1$ and $G_2 = N \cup M_2$ seems dual to the addition of auxiliary spins A to circuit $G_1 = N \cup M_1$, however, the two processes are distinct in a subtle way. Solving an Ising circuit G through the addition of auxiliary spins A and an auxiliary array $g : \Sigma^N \rightarrow \Sigma^A$ results in a constraint set

$$(s, f(s), g(s)) < (s, t, a) \text{ for all } s \in \Sigma^N \text{ and } f(s) \neq t \in \Sigma^M,$$

for a total of $2^N(2^{M+A} - 2^A)$ constraints. However, solving $G = N \cup M_1 \cup M_2$ requires satisfying the constraints

$$(s, f_1(s), f_2(s)) < (s, r, t) \text{ for all } s \in \Sigma^N \text{ and } (f_1(s), f_2(s)) \neq (r, t) \in \Sigma^{M_1} \times \Sigma^{M_2},$$

for a total of $2^N(2^{M_1+M_2} - 1)$ constraints. **Circuits with auxiliaries care only about correctness in the output component, whereas circuits with decomposed output spaces require correctness in all output components. Auxiliary spins are therefore not the same as output spins.**

These remarks notwithstanding, Proposition 1.4 is a powerful tool for solving Ising circuits. For instance, suppose we have an algorithm `PartialSolve` which takes as input (G, M_2) where

- $G = N \cup M_1 \cup M_2$ is an ising circuit
- (G, M_1) is a solvable subcircuit

and returns an Ising circuit G' which is partially solvable with respect to M_2 . Such an algorithm can be achieved using an auxiliary solve, for instance. We can then solve *any* Ising circuit by

Algorithm 1: RecursivePartialSolve

Input: Ising Circuit $(G = N \cup M, f)$ with decomposition $M = M_1 \cup \dots \cup M_k$.

Output: Ising circuit $G' = G \cup A$ solving G with auxiliary spins A .

```

1  $i = 1$   $G' = N \cup M_i$ .
2 while  $i \neq k$  do
3    $i = i + 1$ 
4    $G' = G' \cup M_i$ 
5    $G' = \text{PartialSolve}(G')$ 
```

Since G' is always solvable, the full circuit G (together with the auxiliary spins accrued by the solves of G') is solvable if and only if G' is solvable with respect to $M_{i+1} \cup \dots \cup M_k$, due to Proposition 1.4. By the time `RecursivePartialSolve` terminates, G' will be a solution to G with auxiliaries.

The advantage of using this algorithm over an auxiliary solve is that each iteration of *PartialSolve* only has to operate over $|2^N \times (2^{M_2} - 1)|$ many constraints.

2. HIERARCHICAL CLUSTERING

A choice of “auxiliary array” can be thought of as a function $a : \Sigma^N \rightarrow \Sigma^A$ which assigns an auxiliary state to each input state. The collection of germs of this function partitions Σ^N into subsets of inputs which share the same auxiliary state. To be clear, we’re talking about the partition

$$\{a^{-1}(\alpha)\}_{\alpha \in \Sigma^A}$$

of input spin space. If the choice of auxiliary array a makes the Ising circuit feasible, then we say a solves the Ising circuit.

This simple observation motivates a simple question: *can a partition of Σ^N be found such that it matches the partition produced by some feasible auxiliary array using only the logic of the Ising circuit?* Producing such a partition is a clustering problem on input spinspace.

3. PSEUDO-BOOLEAN OPTIMIZATION AND POLYNOMIAL FITTING

A pseudo boolean function (PBF) is any function $f : \{0, 1\} \rightarrow \mathbb{R}$. It is a well known fact that any such PBF can be uniquely represented by a multilinear polynomial in n variables [pseudo-boolean optimization Boros, Hammer]; that is, a polynomial

$$g(x_1, \dots, x_n) = \sum_{S \subset [n]} a_S \prod_{j \in S} x_j$$

with $a_S \in \mathbb{R}$ which equals f pointwise on $\{0, 1\}^n$. To be clear, here S iterates over all subsets of $[n] = \{1, \dots, n\}$.

It is another well-known fact that the optimization of any pseudo-boolean function can be reduced in polynomial time to an optimization problem on a quadratic polynomial. The original method for accomplishing this was first written by Rosenberg, and since then a reputable zoo of alternative algorithms have been introduced. Most methods share the same basic idea: reduce degree ≥ 3 monomial terms appearing in the polynomial g by introducing auxiliary variables subject to constraints.

<copy Rosenberg algorithm from Boros, Hammer pg 168>

Theorem 3.1. *Let f be a multilinear polynomial in n variables. There exists an algorithm *REDUCE* which produces a multilinear polynomial g in $n + a$ variables such that*

$$\min_{(\mathbf{x}, \mathbf{a}) \in \mathbb{B}^n \times \mathbb{B}^a} g(\mathbf{x}, \mathbf{a}) = \min_{\mathbf{x} \in \mathbb{B}^n} f(\mathbf{x})$$

and if $(\mathbf{x}, \mathbf{a}) = \arg \min_{(\mathbf{x}, \mathbf{a}) \in \mathbb{B}^n \times \mathbb{B}^a} g(\mathbf{x}, \mathbf{a})$ then $\mathbf{x} = \arg \min_{\mathbf{x} \in \mathbb{B}^n} f(\mathbf{x})$.

Boros Hammer Pseudo Boolean Optimization 2002. □

We need a slightly stronger statement however.

Theorem 3.2. *Let $f : \Sigma^N \rightarrow \Sigma^M$ be a circuit. Then there exists an Ising circuit with auxiliary spins given by Hamiltonian H which solves f .*

Proof. Fix $G = N \cup M$ and consider the hamming objective function $\text{ham} : \Sigma^N \times \Sigma^M \rightarrow \mathbb{R}$ defined

$$\text{ham}(s, t) = d(t, f(s))$$

where $d(t, f(s))$ is the Hamming distance between t and the correct output $f(s)$. Then there exists some multilinear polynomial g in $|G|$ variables which recovers ham pointwise. We now apply Rosenberg reduction to g and set H equal to the terminal quadratic polynomial we obtain. All that remains to show is that on any input level s the output which minimizes H is $f(s)$.

Fix an input s and suppose that the minimizer of $g^k(s, \cdot)$ has output coordinates $f(s)$. To obtain g^{k+1} we replace some pair $x_i x_j$ by x_{k+1} and add the expression $M(x_i x_j - 2x_i x_{k+1} - 2x_j x_{k+1} + 3x_{k+1})$. Observe that this expression is zero if $x_i x_j = x_{k+1}$ and is strictly positive otherwise. It follows that $g^k(\mathbf{x}) = g^{k+1}(\mathbf{x}, x_{k+1})$ if $x_{k+1} = x_i x_j$ and $g^k(\mathbf{x}) < g^{k+1}(\mathbf{x}, x_{k+1})$ if $x_{k+1} \neq x_i x_j$. Hence the minimizer of g^{k+1} on input level s also has the correct output coordinates, and inductively, we conclude that H is an Ising Hamiltonian reproducing the circuit f . □