

The Reverse Ising Problem

Isaac Martin

Summer 2023

Contents

1	Foundations	1
1.1	Circuits	1
1.2	The Reverse Ising Problem	2
1.3	Constraint Sets for Designing Ising Systems	3
1.4	Partial Ising Circuits	7
2	Boolean Circuits and Functions	8
3	Hierarchical Clustering	8
4	Pseudo-boolean optimization and polynomial fitting	8

1 Foundations

1.1 Circuits

Throughout this document we set $\Sigma = \{-1, 1\}$ to be the set of possible spins (Σ for spin) taken by a single vertex in an Ising graph. For any set X , we denote by Σ^X the set of all functions $\sigma : X \rightarrow \Sigma$ and note, by setting $n = |X|$, that Σ^X can equivalently be viewed as the set of n -tuples valued in $\{-1, 1\}$, $\Sigma^X \cong \{(\sigma_1, \dots, \sigma_n) \in \Sigma^n\}$ or as the set of binary strings of length n under the identification $\Sigma \leftrightarrow \{0, 1\}$. We first review a few elementary facts.

Proposition 1.1. Let X be any set.

- (a) If $\alpha : N \hookrightarrow X$ then we have a map $\text{res}_{XN} \Sigma^X \rightarrow \Sigma^N$ given $\text{res}_{XN}(\sigma) = \sigma \circ \alpha$. We denote $\text{res}_{XN}(\sigma) = \sigma|_N$.
- (b) If $N, M \subseteq X$ are disjoint, then $\Sigma^N \times \Sigma^M \cong \Sigma^{N \cup M}$.
- (c) If $N, M \subseteq X$ are not necessarily disjoint, then $\Sigma^N \times_{N \cap M} \Sigma^M \cong \Sigma^{N \cup M}$.

Proof.

- (a) Trivial; statement of fact.
- (b) This is a special case of (c).
- (c) The object $\Sigma^{N \cup M}$ fits into the following diagram

$$\begin{array}{ccc}
 \Sigma^{N \cup M} & \xrightarrow{\text{res}} & \Sigma^N \\
 \downarrow \text{res} & & \downarrow \text{res} \\
 \Sigma^M & \xrightarrow{\text{res}} & \Sigma^{N \cap M}
 \end{array}$$

where all maps are the appropriate restriction maps. In fact, $\Sigma^{N \cup M}$ together with restriction maps is the universal object of this diagram; suppose we have another object P with maps $q_1 : P \rightarrow \Sigma^M$ and $q_2 : P \rightarrow \Sigma^N$ making this commute. Then $\text{res}(q_1(p)) = \text{res}(q_2(p))$ so the map $u : P \rightarrow \Sigma^{N \cup M}$ given by

$$u(p)(x) = \begin{cases} q_1(p)(x) & x \in M \\ q_2(p)(x) & x \in N \end{cases}$$

is well defined on $M \cap N$. Hence $\Sigma^{N \cup M}$ is the pullback of Σ^M and Σ^N with restriction maps to $\Sigma^{N \cap M}$. □

Definition 1.2. A **circuit** is a tuple (N, M, f) where

- $N, M \subseteq X$ are arbitrary subsets of some universal set X and are almost always chosen so that $N \cap M = \emptyset$. Both N and M should be finite and we call their elements **input** and **output** spins respectively.
- $f : \Sigma^N \rightarrow \Sigma^M$ is an arbitrary function called the *logic* function.

We make special note of the scenarios in which N and M are not disjoint. Additionally, we define the following terminology.

- $A = X \setminus (N \cup M)$ is the **set of auxiliary spins** of X .
- Σ^X is the **spin space**, Σ^N is the **input space**, Σ^M the **output space** and Σ^A the **auxiliary space** of X . Elements of Σ^X are called **spin states**, elements of Σ^N **input states**, etc.
- $\mathcal{R}(f) = \{\sigma \in \Sigma^X \mid f(\sigma|_N) = \sigma|_M\}$ is the set of **correct** or **right** spin states.
- $\mathcal{W}(f) = \Sigma^X \setminus \mathcal{R}(f)$ is the set of **wrong** spin states.
- $\mathcal{L}(\sigma) = \mathcal{L}(\sigma|_N) = \{\sigma' \in \Sigma^X \mid \sigma'|_N = \sigma|_N\}$ is the **input level** of σ . It is useful to talk about the input level of both an input state $\sigma|_N$ and a full spin state σ , so we write $\mathcal{L}(\sigma)$ and $\mathcal{L}(\sigma|_N)$ to mean the same thing.

At this point it is worth remarking that this object (N, M, f) in no way carries the data of an Ising system. An Ising system is a collection of spins with connections between them, together with a fixed quadratic Hamiltonian which predicts the dynamics of the system. What we have defined has no Hamiltonian, no notion of dynamics and no real semblance of a graph structure; it has only a function which specifies a desired output to each input and a lot of extra space $(X \setminus (N \cup M))$ with which to begin adding additional structure. An abstract circuit, as defined, is nothing other than a skeleton for an Ising system we wish to design.

1.2 The Reverse Ising Problem

Definition 1.3. An **Ising system** is a pair (X, H) , often referred to as simply X , where

- $X \subseteq \mathbb{N}$ is a set whose elements are called **spins**,
- $H \in \mathbb{R}[X]$ is a 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 .

An Ising system is inherently probabilistic. The probability that an Ising system X is in state $\sigma \in \Sigma^X$ is given by the **configuration probability**

$$P_\beta = \frac{e^{-\beta H(\sigma)}}{Z_\beta}$$

where $\beta = (k_B T)^{-1} \geq 0$ is inverse temperature, k_B is the Boltzmann constant and the normalization constant Z_β is the partition function $Z_\beta = \sum_{\sigma \in \Sigma^G} e^{-\beta H(\sigma)}$. Notice that probability is maximized whenever the Hamiltonian is minimized, hence low energy states are more probable than high energy states.

With this in mind, for an Ising system with (X, H) with X finite and a subset $U \subseteq X$, we define the **minimizer with respect to U** to be the function $m_U : \Sigma^U \rightarrow \Sigma^X$ defined

$$f_U(\tau) = \arg \min_{\sigma \in \Sigma^X, \sigma|_U = \tau} H(\sigma).$$

It answers the question: “if the states of U are held fixed, then what is the most likely state of X ?” We likewise define the **minimizer logic** of U to be the function $f_U : \Sigma^U \rightarrow \Sigma^{U^c}$ given $f_U(\tau) = m_U(\tau)|_{U^c}$.

We would like to design Ising systems 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 $f : \Sigma^N \rightarrow \Sigma^M$ 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,

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

Definition 1.4. Fix an abstract circuit (N, M, f) . We say that an Ising system (X, H) **solves** (N, M, f) (in that it solves the reverse Ising problem on (N, M, f)) if for each $\sigma \in \Sigma^X$

$$\tau = \arg \min_{\sigma' \in \mathcal{L}(\sigma)} H(\sigma') \implies \tau \in \mathcal{R}(f).$$

In other words, a choice of Hamiltonian H for X solves the circuit if the minimizer of the Hamiltonian among all states with matching input states has as its output component the correct output as specified by the circuit logic f .

1.3 Constraint Sets for Designing Ising Systems

Let us first consider the simplest case of a circuit (N, M, f) with $X = N \cup M$ and N and M disjoint.

Lemma 1.5. The circuit X is solvable with an Ising system if and only if there exists a Hamiltonian H such that for all $s \in \Sigma^N$ and $t \neq f(s)$ $H(s, t) > H(s, f(s))$.

Proof. Obvious, is essentially the definition of the Ising system solvability. □

It is not hard to find examples of circuits which are not solvable, for instance, the naive XOR circuit with $|X| = 3$ is not solvable with an Ising system.

For the remainder of this section, suppose that $X = N \cup M \cup A$ is a finite set and N , M , and A are all disjoint. We call elements of this extra set A **auxiliary spins**.

Proposition 1.6. Let $X \subseteq \mathbb{N}$ be infinite and N, M be finite disjoint subsets. For any choice of f_X , 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 $\text{ham} : \Sigma^X \rightarrow \mathbb{R}$ defined

$$\text{ham}(\sigma) = d(\sigma, \mathcal{L}(\sigma|_N))$$

where d is hamming distance, write it as a multilinear polynomial, add auxiliary variables to reduce to a quadratic using, for instance, Rosenberg reduction. \square

The task of finding an Ising system which solves some abstract circuit (N, M, f) can thus be thought of as finding a sufficiently large cardinality for A and then solving a mixed non-linear optimization problem to find valid a valid quadratic Hamiltonian together with auxiliary states which occur at the desired minimizers of input levels. The following lemma demonstrates one way one might attempt to solve an abstract circuit with auxiliaries.

Lemma 1.7. The circuit X is solvable with an Ising system if and only if there exists a function $g : \Sigma^N \rightarrow \Sigma^M$ and a Hamiltonian H such that for all $\sigma \in \Sigma^N$, $\eta \in \Sigma^A$ and $f(\sigma) \neq \eta \in \Sigma^M$, $H(\sigma, \eta) > H(\sigma, f(\sigma), g(\sigma))$.

The image of the function g is called the **auxiliary array** of X . If we fix a specific spin $a \in A$, then the set $\{g(\sigma)_a\}_{\sigma \in \Sigma^N}$ is called the *auxiliary vector* of a .

Proof. Again, obvious. \square

A solution to a circuit employing Lemma 1.7 consists of two parts: obtaining a feasible auxiliary array g and identifying choices of Hamiltonians such that the constraints in Lemma 1.7 are all satisfied. Although it is always possible, choosing a feasible g is quite difficult, and doing so in such a way that minimizes the cardinality of A is even harder. If a feasible g is known, solving for H is a linear programming problem; however, because the number of constraints in Lemma 1.7 grows exponentially in N , M and A , for problems on the order of $|X| \approx 100$ there is no computer on earth that can actually solve the LP-problem as stated.

Definition 1.8 (Constraint Sets for Reverse Ising). Let (N, M, f) be an abstract circuit with $X = N \cup M \cup A$ and N, M, A all disjoint. We say that an Ising system (X, H) together with a choice $g : \Sigma^N \rightarrow \Sigma^A$ of auxiliary array satisfies

- **Weak Constraints** if for all $\sigma_N \in \Sigma^N$ and $\sigma_M \neq f(\sigma_N)$

$$H(\sigma_N, \sigma_M, \sigma_A) > H(\sigma_N, f(\sigma_N), g(\sigma_N)).$$

There are $2^{M+A} - 2^A$ constraints per input level, $2^N(2^{M+A} - 2^A)$ total.

- **Full Constraints** if for all $\sigma_N \in \Sigma^N$ and $\sigma_M \neq f(\sigma_N)$ or $\sigma_A \neq g(\sigma_N)$

$$H(\sigma_N, \sigma_M, \sigma_A) > H(\sigma_N, f(\sigma_N), g(\sigma_N)).$$

There are $2^{M+A} - 1$ constraints per input level, $2^N(2^{M+A} - 1)$ total.

- **Threshold Constraints with respect to F** if for some function $F : \Sigma^N \times \Sigma^M \rightarrow \Sigma^A$

$$H(\sigma_N, \sigma_M, F(\sigma_N, \sigma_M)) > H(\sigma_N, f(\sigma_N), F(\sigma_N, f(\sigma_N))).$$

There are $2^M - 1$ constraints per input level or $2^N(2^M - 1)$ constraints total.

Lemma 1.9. Let (N, M, f) be an abstract circuit with $X = N \cup M \cup A$ and all N, M and A disjoint. This circuit is solved by an Ising system (X, H) if and only if there is an auxiliary array $g : \Sigma^N \rightarrow \Sigma^A$ such that H satisfies full constraints.

Proof. The reverse implication is clear, as ever constraint in Lemma 1.7 is a constraint in Lemma ??.

For the forward implication, suppose (N, M, f) is solved by an Ising system (X, H) . Defining g to be the auxiliary component of the minimizer with respect to N , $g(\sigma_N) = m_N(\sigma_N)|_A$, does the trick. \square

Lemma 1.10. Let (N, M, f) again be an abstract circuit. There exists an Ising system which solves this circuit if and only if there is some function $F : \Sigma^N \times \Sigma^M \rightarrow \Sigma^A$ such that both

- (a) the new circuit $(N \cup M, A, F)$ is solvable by an Ising system with Hamiltonian R with the following additional property:

$$R(\sigma_N, \sigma_M, F(\sigma_N, \sigma_M)) \geq R(\sigma_N, f(\sigma_N), F(\sigma_N, f(\sigma_N))) \quad (\dagger)$$

for all σ_N and σ_M . We call this the **weak neutralizability condition**. (If the inequality is instead an equality, we call this the **strong neutralizability condition**. Likewise, if such an Ising system (X, R) exists, we correspondingly say that F is weakly neutralizable or strongly neutralizable.)

- (b) there is an Ising system (X, H) which satisfies threshold constraints with respect to F .

Proof. Throughout this proof let σ, ω and η denote elements in Σ^N , Σ^M and Σ^A respectively. Suppose first that the circuit (N, M, f) is solvable by an Ising system (X, H) . Define $F : \Sigma^N \times \Sigma^M \rightarrow \Sigma^A$ to be the auxiliary component of the minimizer with respect to $N \cup M$:

$$F(\sigma, \omega) = m_{N \cup M}(\sigma, \omega)|_A := \arg \min_{\eta \in \Sigma^A} H(\sigma, \omega, \eta).$$

By definition of F , the circuit $(N \cup M, A, F)$ is solvable by the Ising system (X, H) . Furthermore, since H satisfies the weak constraints, for some value of $\eta' \in \Sigma^A$ we have that

$$H(\sigma, \omega, \eta) > H(\sigma, f(\sigma), \eta') \geq H(\sigma, f(\sigma), F(\sigma, f(\sigma)))$$

for all $\eta \neq \eta'$ where the second from the definition of F . Thus, in particular, it satisfies the weak neutralizability condition.

Since (X, H) solves the circuit (N, M, f) , by Lemma 1.7 we have that

$$H(\sigma, \omega, \eta) > H(\sigma, f(\sigma), F(\sigma, f(\sigma)))$$

for all $\omega \neq f(\sigma)$, and all η so in particular,

$$H(\sigma, \omega, F(\sigma, \omega)) > H(\sigma, f(\sigma), F(\sigma, f(\sigma)))$$

Thus (X, H) satisfies the threshold constraints with respect to F .

Now suppose that F is an arbitrary function such that $(N \cup M, A, F)$ is an abstract circuit solvable by an Ising system (X, R) whose Hamiltonian R satisfies (\dagger) and that (X, S) is an Ising system with Hamiltonian S which satisfies the threshold constraints with respect to F . Consider the family of Ising Hamiltonians $H_\lambda = S + \lambda R$ parameterized by λ . We show that for sufficiently large λ , H_λ , (X, H_λ) together with auxiliary array $g(\sigma) = F(\sigma, f(\sigma))$ satisfies the weak constraints and hence solves the circuit (N, M, f) .

Fix σ and $\omega \neq f(\sigma)$, and consider first the case that $\eta = F(\sigma, \omega)$. Then

$$\begin{aligned} H_\lambda(\sigma, \omega, \eta) - H_\lambda(\sigma, f(\sigma), g(\sigma)) &> 0 \\ \iff S(\sigma, \omega, \eta) - S(\sigma, f(\sigma), g(\sigma)) + \lambda(R(\sigma, \omega, \eta) - R(\sigma, f(\sigma), g(\sigma))) &> 0 \\ \iff S(\sigma, \omega, F(\sigma, \omega)) - S(\sigma, f(\sigma), F(\sigma, f(\sigma))) + \lambda R(\sigma, \omega, F(\sigma, \omega)) - \lambda R(\sigma, f(\sigma), F(\sigma, f(\sigma))) &> 0 \\ \iff S(\sigma, \omega, F(\sigma, \omega)) - S(\sigma, f(\sigma), F(\sigma, f(\sigma))) &> 0. \end{aligned}$$

The final condition in the above chain of bi-conditionals holds irrespective of the value of λ since S satisfies the threshold constraints. Now suppose that $\eta \neq F(\sigma, \omega)$. Set

$$\alpha = \min_{\substack{\omega \in \Sigma^M \\ \omega \neq f(\sigma)}} R(\sigma, \omega, \eta) - R(\sigma, f(\sigma), F(\sigma, f(\sigma))),$$

noting that by (\dagger) , the assumption that (X, R) solves $(N \cup M, A, F)$ and because $\eta \neq \omega$ we have

$$R(\sigma, \omega, \eta) > R(\sigma, \omega, F(\sigma, \omega)) \geq R(\sigma, f(\sigma), g(\sigma))$$

which in turn implies that $\alpha > 0$. Additionally set

$$\beta = \max_{\sigma \in \Sigma^G} S(\sigma, f(\sigma), F(\sigma, f(\sigma))) - S(\sigma, \omega, \eta).$$

Then

$$\begin{aligned} H_\lambda(\sigma, \omega, \eta) - H_\lambda(\sigma, f(\sigma), F(\sigma, f(\sigma))) &> 0 \\ \iff \\ S(\sigma, \omega, \eta) - S(\sigma, f(\sigma), F(\sigma, f(\sigma))) \\ + \lambda R(\sigma, \omega, \eta) - \lambda R(\sigma, f(\sigma), F(\sigma, f(\sigma))) &> 0 \\ \iff \\ \lambda &> \frac{S(\sigma, f(\sigma), F(\sigma, f(\sigma))) - S(\sigma, \omega, \eta)}{R(\sigma, \omega, \eta) - R(\sigma, f(\sigma), F(\sigma, f(\sigma)))}. \end{aligned}$$

Choosing $\lambda > \beta/\alpha$ ensures this is satisfied for all $\sigma \in \Sigma^X$. \square

The following theorem summarizes our results up to this point.

Theorem 1.11. *Let (N, M, f) be an abstract circuit. Then the following are equivalent.*

- (i) *There exists an Ising system (X, H) which solves (N, M, f) .*
- (ii) *There exists an Ising system (X, H) which satisfies the weak constraints of f .*
- (iii) *There exists an Ising system (X, H) which satisfies the full constraints of f .*
- (iv) *There exists a function $F : \Sigma^N \times \Sigma^M \rightarrow \Sigma^A$, an Ising system (X, S) satisfying the threshold constraints with respect to F and an Ising system (X, R) which solves the circuit $(N \cup M, A, F)$ and has the weak neutralizability property.*

Proof. Lemma 1.7 proves $(i) \Leftrightarrow (ii)$, Lemma 1.9 proves $(i) \Leftrightarrow (iii)$ and Lemma 1.10 proves $(ii) \Leftrightarrow (iv)$. \square

Remark 1.12. Of these four equivalences, (iv) is perhaps the most opaque. One might wonder what utility it actually buys, especially since the assumption that R has the weak neutralizability condition and solves the circuit $(N \cup M, A, F)$ is awfully close to simply demanding that R satisfies the weak constraints of f . The Hamiltonian S appears only to be used to “fix” the places where R fails to satisfy the strong inequality version of the weak neutralizability condition. All of this begs the question: how is this ever useful?

1. **Threshold constraints do not scale exponentially in A .** Both the weak and full constraints grow exponentially in A , but the constraint matrices of the threshold constraints always have a fixed number of rows and only grow columnwise on the order of $\mathcal{O}(A^2)$.
2. **Good choices of F are known.** If F depends only on a few spins, then cooking up reasonable Hamiltonians R becomes far easier. See examples 1.13 and 1.14.
3. **Improvements to F can be made iteratively.** If a function $F_1 : \Sigma^N \times \Sigma^M \rightarrow \Sigma^{A_1}$ is weakly neutralizable and $F_2 : \Sigma^N \times \Sigma^{M \cup A_1} \rightarrow \Sigma^{A_2}$ is weakly neutralizable, then the composite function

$$F(\sigma, \omega) = (F_1(\sigma, \omega), F_2(\sigma, \omega, F_1(\sigma, \omega))) \in \Sigma^{A_1 \cup A_2}$$

is also strongly neutralizable. This means the threshold constraint approach to the reverse Ising problem lends itself well to iterative methods. In particular, due to the observation that the solvability of a boolean circuit by an Ising system is equivalent to linear separability, we can attach auxiliary spins one at a time (see Section 2).

Example 1.13. Suppose $F : \Sigma^N \times \Sigma^M \rightarrow \Sigma^A$ is constant in the Σ^M component. Then any Ising system (X, R) which solves the circuit $(N \cup M, A, R)$ is weakly neutralizable.

Example 1.14. Let $(\{a, b\}, \{c\}, AND)$ be the 1-bit AND circuit. Then there exists an Ising system $(\{a, b, c\}, R)$ which solves the circuit and is strongly neutralizable.

1.4 Partial Ising Circuits

Definition 1.15. 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 1.16. 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 1.17. 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 1.18. The converse of Proposition 1.17 is false; solvability of (G, f) does not necessarily imply the solvability of its subcircuits.

Remark 1.19. 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

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

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

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

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 1.17 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 1.17. 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 Boolean Circuits and Functions

In this section we consider abstract circuits (N, M, f) where $|M| = 1$. We start with some definitions

Proposition 2.1. Let (N, y, f) be an abstract circuit with one output – i.e. let f be a boolean function. There exists an Ising system (X, H) with $X = N \cup y$ if and only if the set of true vectors $T = f^{-1}(1)$ is linearly separable from the set of false vectors $F = X \setminus T = f^{-1}(-1)$.

Proof. View the set Σ^N as a set of tuples consisting of $+1/-1$ in each entry with every data point labeled \square

3 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.

4 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

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

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 4.1. *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 4.2. *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 . □