A. Appendix

A.1. Alternative Construction

We consider a related construction where we generate each row independently by fixing exactly t randomly chosen elements to 1. In contrast, the previous construction has on average nf non-zero elements per row, but the number can vary. We can use an analysis similar to the one for Theorem 3, the main difference being that we need to substitute $r^{(w,f)}(0,0)$ with

$$z^{(w,f)}(0,0) = \left(\sum_{\text{even } \ell}^{\min(w,t)} \frac{\binom{w}{\ell}\binom{L-w}{t-\ell}}{\binom{L}{t}} \right)^m .$$

Then we can obtain a closed form expression for ϵ by again looking at the worst-case distribution of the neighbors in terms of Hamming distance w.

A.2. Proofs

Proof of Proposition 2. Let $i^* = \log_2 |S|$ and $2^{\hat{i}-1}$ be the output of $\mathcal{A}$. We will show that $\hat{i}$ is within $[\lfloor i^* \rfloor, \lfloor i^* \rfloor + 2]$ with probability at least 3/4.

Fix any $i \leq i^*$. Then $\mathrm{E}[|h_t^{-1}(0) \cap S|] = |S|/2^i \geq 1$. Weak $(\mu^2, 4)$-concentration implies that $\Pr[|h_t^{-1}(0) \cap S| = 0] \leq 1/4$. Chernoff bound applied to the T underlying independent 0-1 indicator random variables then implies that a majority of the T sets will be empty with probability at most $\exp(-T/8)$. It follows that with probability at least $(1 - \exp(-T/8))^{i^*} \geq (1 - \exp(-T/8))^n \geq 1 - n\exp(-T/8)$, the majority of the T sets for *all* $i \leq i^*$ will simultaneously be non-empty. Thus, for $T \geq 8\ln(8n)$, we have that with probability at least 7/8, all $i \leq i^*$ will behave correctly.

Fix any $i \geq i^*+2$. Here we can simply use Markov's inequality to infer that $\Pr[|h_t^{-1}(0) \cap S| \geq 1] \leq 1/4$. From the same Chernoff bound based argument as above, it follows that for $T \geq 8\ln(8n)$, with probability at least 7/8, all $i \geq i^* + 2$ will behave correctly.

By union bound, it follows that the output $2^{\hat{i}-1}$ of $\mathcal{A}$ will be in the range $[2^{\lfloor i^* \rfloor - 1}, 2^{\lfloor i^* \rfloor + 1}]$ with probability at least $1 - 1/8 - 1/8 = 3/4$. □

Proof of Proposition 3. From Chebychev's inequality, $\Pr[|X - \mu| \geq \sqrt{\delta}\sigma] \leq \delta$, which implies the claimed strong correlation. For showing the desired weak correlation, we use Cantelli's one-sided inequalities. For the first case, $\Pr[X \leq \mu - \sqrt{\delta - 1}\sigma] \leq 1/(1 + (\delta - 1)) = 1/\delta$. The second case works similarly. □

Proof of Proposition 4. From Chernoff's bound, $\Pr[X \leq \mu + \sqrt{k}] = \Pr[X \leq (1 + \frac{\sqrt{k}}{\mu})\mu] \leq \exp(-\frac{k}{3\mu})$. Thus, $k \geq (3\ln\delta)\mu$ suffices to bound this probability by $1/\delta$. The other side, $\Pr[X \leq \mu - \sqrt{k}]$, similarly leads to $k \geq (2\ln\delta)\mu$ as the condition to bound the probability by $1/\delta$. Combining the two, we get the desired result for weak concentration. The result for strong concentration follows by using the union bound to obtain $\exp(-\frac{k}{3\mu}) + \exp(-\frac{k}{2\mu})$, which is less than $\exp(-\frac{k}{c\mu})$ for any $c > 3$. □

Proof of Proposition 5. This follows from observing that pairwise independence implies $\sigma^2 = |S|/2^m(1 - 1/2^m) < \mu$ and then applying Prop. 3. □

Proof of Proposition 6. The first two observations are straightforward. For the third, let S and T be sets with $|T| = |S|+1$. Given $y_1, y_2 \in \{0,1\}^m$, let $f(x_1, x_2)$ denote $P[H(x_1) = y_1, H(x_2) = y_2]$. Then

$$\begin{aligned} \sum_{x,y \in T, x \neq y} f(x,y) &= \frac{1}{|T| - 2} \sum_{z \in T} \sum_{x,y \in T \setminus \{z\}, x \neq y} f(x,y) \\ &\leq \frac{1}{|T| - 2} \sum_{z \in T} |S|(|S| - 1)\frac{\epsilon}{2^m} \\ &= \frac{|T|}{|T| - 2}|S|(|S| - 1)\frac{\epsilon}{2^m} \leq |T|(|T| - 1)\frac{\epsilon}{2^m} \end{aligned}$$

This finishes the proof. □

Proof of Lemma 1. By Theorem 3, the hash functions $h^i_{A,b}$ from $\mathcal{H}^{f*}$ in the inner loop at iteration i are $(\epsilon, 2^{i+2})$-AU, with $\epsilon < \frac{31}{5(2^{i+2}-1)}$ by construction.

Let $S = \{\sigma_1, \sigma_2, \cdots, \sigma_{2^{i+2}}\}$, $X = |\left(h^i_{A,b}\right)^{-1}(\mathbf{0}) \cap S|$. Notice $|S| = 2^{i+2}$ and $\mathrm{E}[X] = 2^{i+2}/2^i = 4$.

By by Corollary 1 and Theorem 2, X is weakly $(\mu^2, 9/4)$-concentrated.

Then by weak concentration

$$\begin{aligned} \Pr[w_i \geq b_{i+2}] &= \Pr[w_i \geq w(\sigma_{2^{i+2}})] \geq \Pr[X \geq 1] \\ &= 1 - \Pr[X \leq 0] \geq 1 - 4/9 = 5/9 \end{aligned}$$

Similarly, we have from Markov's inequality

$\Pr[w_i \leq b_{i-2}] \geq 3/4 \geq 5/9$.

Finally, using Chernoff inequality (since $w_i^1, \cdots, w_i^T$ are i.i.d. realizations of w_i)

$$\Pr\left[M_i \leq b_{i-2}\right] \geq 1 - \exp(-\alpha' T) \quad (3)$$
$$\Pr\left[M_i \geq b_{i+2}\right] \geq 1 - \exp(-\alpha' T) \quad (4)$$

where $\alpha' = 2(5/9 - 1/2)^2$, which gives the desired result

$$\Pr\left[b_{i+2} \le M_i \le b_{i-2}\right] \ge 1 - 2\exp(\alpha' T) \\ = 1 - \exp(-\alpha^* T)$$

where $\alpha^* = \ln 2\alpha' = 2(5/9 - 1/2)^2 \ln 2 > 0.0042$ $\square$

A.3. Additional Experiments

We report additional experimental results for mixed interaction Ising grids in Figure 4 with the same setup as in Section 7 but with external field 1.0 rather than 0.1.

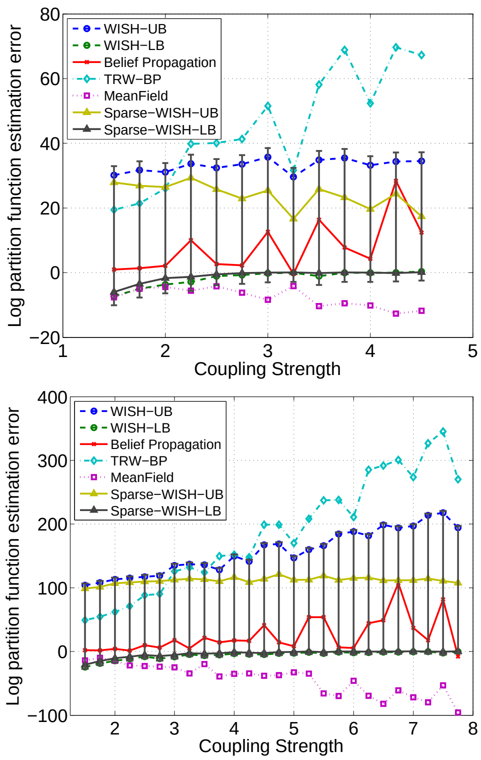

Figure 4. Results on Ising grids with mixed interactions. Top: Mixed 10×10. Field 1.0. Bottom: Mixed 15×15. Field 1.0.