

Let's summarize what we've learned about random classical LDPC codes.

Take a random (Δ_B, Δ_C) classical LDPC code: $3 \leq \Delta_B < \Delta_C$.

$$\Rightarrow k = n \left(1 - \frac{\Delta_B}{\Delta_C}\right) \text{ (+1 if } \Delta_B \text{ even)} \Rightarrow \text{"constant rate"}$$

i.e. only finite physical bit overhead needed for each logical bit

Linear confinement: $|Hx| \geq \eta |x|$ if $|x| \leq \alpha n$

$\Rightarrow$ code distance $d > \alpha n \Rightarrow$ "asymptotically good"

These codes have remarkable statistical physics properties that we explore.

The quantum generalizations of these LDPC codes often exhibit same phenomena but derivations are more involved, so we'll do it for classical case.

Consider thermal (Gibbs) state of classical code:

$$P_\beta(x) = \frac{1}{Z(\beta)} e^{-\beta |Hx|} \quad \text{so energy} = \# \text{ of violated checks.}$$

Thm: Take Δ_B odd. Then w.h.p.

$$Z(\beta) = 2^k (1 + e^{-\beta})^{n-k} \Rightarrow \text{no "thermodynamic phase transition" at finite } T$$

Up to overall prefactor this matches 1d Ising model!

Proof: Similar to what we saw for 2d surface code.

$$\text{Write: } Z(\beta) = \sum_{x \in \mathbb{F}_2^n} e^{-\beta |Hx|}$$

$$\nwarrow \text{decompose } \mathbb{F}_2^n = \mathbb{F}_2^k \oplus \mathbb{F}_2^{n-k}$$

(logical) (independent checks)

$$Z(\beta) = \sum_{l \in \mathbb{F}_2^k} \sum_{s \in \mathbb{F}_2^{n-k}} e^{-\beta |s + 0 \cdot l|} = \sum_{l, s} e^{-\beta |s|}$$

errors that flip exactly one check logical codeword shift by

$$= \sum_s 2^k e^{-\beta |s|} = 2^k (1 + e^{-\beta})^{n-k}$$

So we might be worried that this means random codes are not self-correcting. However linear confinement also leads to:

Thm: For $\beta > \beta_c \leftarrow O(1)$, Gibbs sampler protects logical info for $t_{\text{mem}} \gtrsim \exp(c \cdot n)$ for $O(1) c$.

Proof: Apply same bottleneck theorem as in 2d Ising:

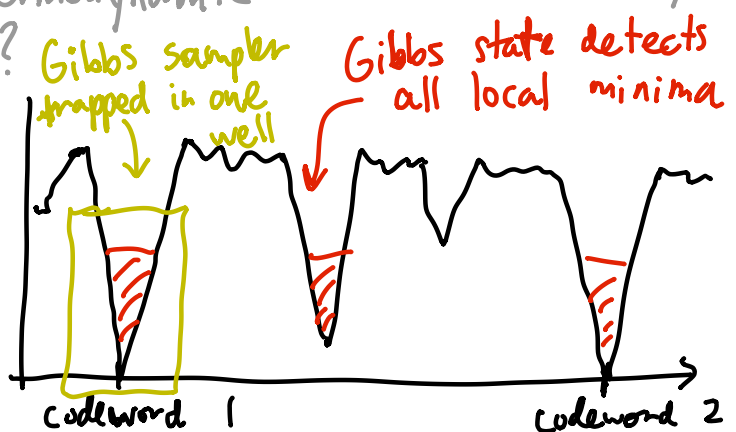
let $B = \{x : |x| = \frac{\alpha n}{2}\}$ linear confinement Scale
 let $A = \{x : |x| < \frac{\alpha n}{2}\}$ put factor $1/2$ to make sure $< d/2$ errors $\Rightarrow$ correctable
 call these "decodable"
 $P_\beta(A) > P_\beta(\{000\dots\}) = \frac{e^{-\beta \cdot 0}}{Z(\beta)}$ lower bound on $|Hx|$
 $P_\beta(B) = \frac{1}{Z(\beta)} \sum_{x \in B} e^{-\beta |Hx|} < \frac{1}{Z(\beta)} 2^n e^{-\beta \cdot \eta \alpha n / 2}$
crude bound on # of sites in B

$\Rightarrow \frac{P_\beta(B)}{P_\beta(A \cup B)} < (2e^{-\beta \eta \alpha / 2})^n$ is exponentially small if
 $\beta > \beta_c = \frac{2}{\eta \alpha} \log 2$ note this is a bound on the true transition temperature
 $\hookrightarrow t_{\text{mem}} \gtrsim \frac{P_\beta(A \cup B)}{P_\beta(B)}$ under single bit-flip dynamics QED

One can thicken bottleneck if there are multi-bit flip errors, same general philosophy holds!

How is it possible to have no thermodynamic transitions and yet have a dynamical transition??

Claim: at least for $\Delta_B \geq 5$, LDPC has complex energy landscape w/ many deep local minima!



Recall: by taking α suitably small, we can find

$$|Hx| \geq \eta|x| \text{ for any } 0 \leq \eta < \frac{\Delta_B - 2}{2}$$

Prop: if $\eta > 1$, fraction of states **near any codeword** is exponentially small.

$$\uparrow \min_{y \in \ker(H)} |x - y|$$

Proof: let's sum over Gibbs weight of all states constrained by

linear confinement: $Z_{LC}(\beta) \leq \sum_{\substack{\text{pick codeword} \\ \text{sum over all } x \text{ with } |x| \leq \alpha n}} 2^k \sum_{j=0}^{\lfloor \alpha n \rfloor} \binom{n}{j} e^{-\beta \cdot \eta j}$

$$\Rightarrow Z_{LC}(\beta) < 2^k \sum_{j=0}^n \binom{n}{j} (e^{-\beta \eta})^j = 2^k (1 + e^{-\beta \eta})^n$$

Now take $\eta > 1$, which is possible if $\frac{\Delta_B - 1}{2} > 1$ or $\Delta_B \geq 5$.

Gibbs weight near codewords is $\frac{Z_{LC}(\beta)}{Z(\beta)} < \left(\frac{1 + e^{-\beta \eta}}{1 + e^{-\beta}} \right)^{n(n+1)/2}$

ratio $< 1 \Rightarrow$ exponentially small

Where's most of the weight in the Gibbs state?

Recall: no redundant check $\Rightarrow$ exist 2^k x w/ every syndrome s :

$$s = Hx$$

Now take $|s|=1$ (only a single violated check)

Can't come from a small error! (since $\eta > 1$)

$$\hookrightarrow |Hx| \geq \eta|x| > |x|$$

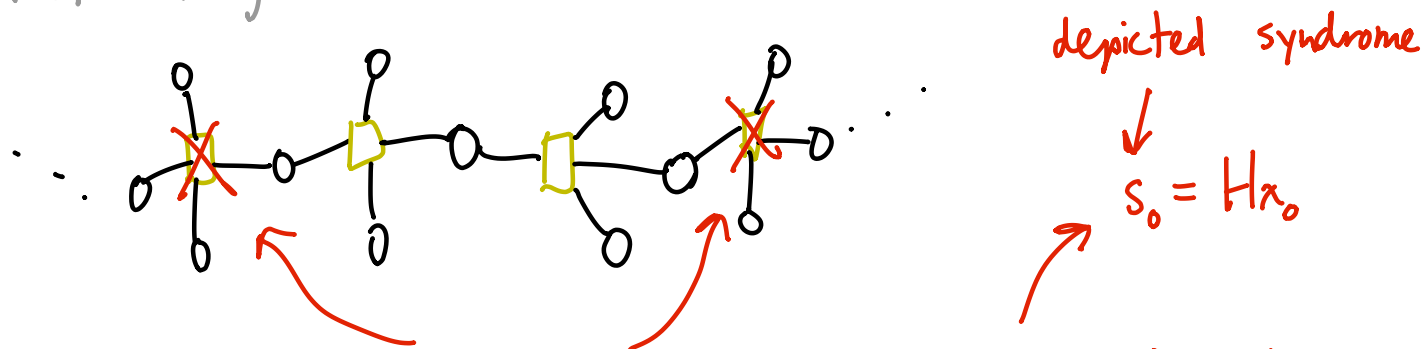
and no $x \neq 0$ obeys $1 > |x|$

So $|s|=1$ syndrome must come from extensive error!

$$\Rightarrow s = Hx \text{ w/ } |x| > \alpha n.$$

enormous error, almost but not quite a codeword!

We can actually construct exponentially many more of these error configs that are far from all codewords..



consider configuration where all violated checks sufficiently far apart
either violate check or not at each place $\Rightarrow$ exponentially many errors

Why can't this syndrome be created by a small error?

Try to remove w/ small error?

$$|H(x+x_0)| \geq |Hx| - |Hx_0| \geq \eta|x| - |s_0|$$

To flip each check violated in s_0 we must flip ≥ 1 bit next to each check so $|x| \geq |s_0| \Rightarrow |H(x+x_0)| \geq (\eta-1)|s_0| > 0$.

Argument fails if $|x| > \alpha n$ so no linear confinement $\Rightarrow$
 s_0 created by large error!

On homework you will explore further the constraints on energy landscape near these sparse syndromes created from large errors.
We can still give a quick argument that many such wells are deep local minima...

Suppose large error x_0 creates sparse syndrome s_0 .

Add any error x w/ $|x| = \alpha n$:

$$|H(x+x_0)| \geq \eta \alpha n - |Hx_0| = \eta \alpha n - |s_0| \gtrsim n \quad \text{if } |s_0| < \eta \alpha n (1 - o(1))$$

e.g. take $|s_0| \leq \frac{1}{6} \eta \alpha n \Rightarrow$ free energy bottleneck

$$e^{-\beta F_{\text{bn}}} < 2^n e^{-\beta \eta \alpha n / 6} \quad \text{for correctable errors (relative to } x_0 \text{).}$$

The physical picture that's emerging for codes is then:

Gibbs state has measure concentration:

$$P_\beta(A) \approx \sum_{\text{"well } a"} p_a P_\beta^{(a)}(A)$$

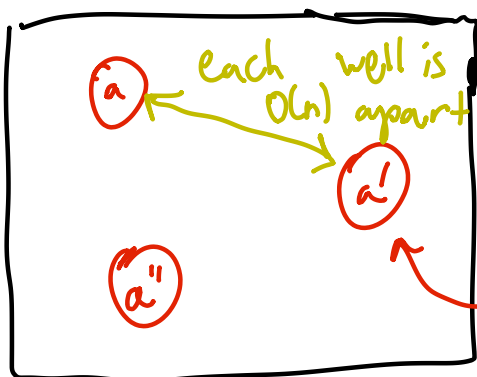
any subset of bitstrings $\hookrightarrow$ well $\Rightarrow$ "local min" w/ free energy bottleneck

$$\text{where } p_a = \frac{\sum_{x \text{ near } a} e^{-\beta |Hx|}}{\sum_{\text{all } x} e^{-\beta |Hx|}} =: \frac{Z_a}{Z}$$

simple choice of cutoff

$$\text{and } P_\beta^{(a)}(x) = \frac{e^{-\beta |Hx|}}{Z_a} \cdot \begin{cases} 1 \\ 0 \end{cases} \quad \begin{matrix} |Hx| \leq \frac{1}{6} \eta \alpha n \\ \text{else} \end{matrix}$$

measure concentration:



Gibbs measure concentrates in disjoint pieces

Linear confinement implies if $|Hx| \leq \frac{1}{6} \eta \alpha n$
 $\eta(|x+x'|) \leq |H(x+x')| \leq \frac{\eta \alpha}{3} n$

$\hookrightarrow$ if $|x+x'| < \alpha n \Rightarrow$ wells at least $\frac{\alpha n}{3}$ apart

2^k of these "a" are related by symmetry:

$$x_0 \rightarrow x_0 + y \quad \hookrightarrow y \in \ker(H)$$

Most replicas related by large non-codeword errors! e.g.

$$x_{0,a'} = x_{0,a} + \underbrace{x_{0,a''}}_{\leftarrow \text{large error w/ small, non-zero syndrome.}}$$

In physics literature this is often called
RSB = replica symmetry breaking (replica $\Rightarrow$ one realization of system.
RSB $\Rightarrow$ ergodicity broken)

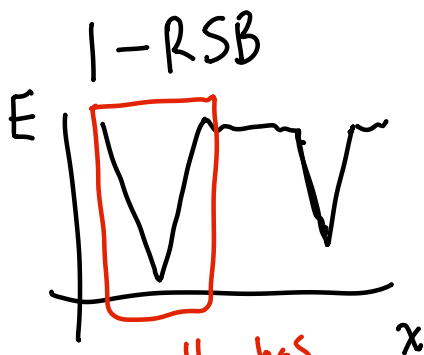
This is a very common feature of "spin glasses" $\nearrow$ can't minimize all terms simultaneously

usually disordered and frustrated:

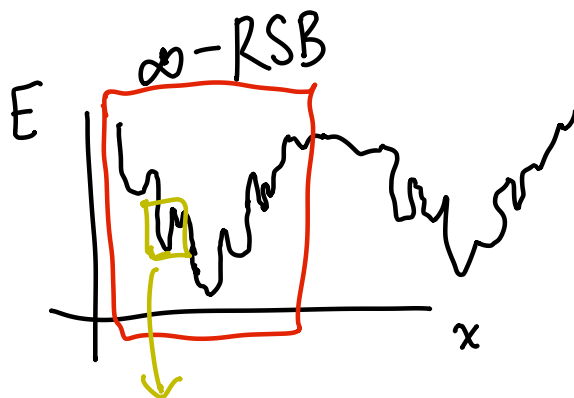
LDPC code does not have frustration but still has RSB.

$$E = \frac{1}{2} s_1 s_2 - \frac{1}{6} s_1 s_3 - \frac{2}{3} s_2 s_3$$

There are 2 types of RSB that arise commonly in physics...



each well has clear local minimum



"minima within minima" $\rightarrow$
"repeatedly broken replica symmetry"

HW6 will argue why LDPC codes are usually expected to be 1-RSB.