

Probabilistic analysis of LP decoding

Alexandros Dimakis

Joint work with
Costas Daskalakis
Richard Karp
Martin Wainwright
EECS/Statistics dept.
UC Berkeley

motivation

- Asymptotic behavior of message-passing decoders: well understood
- this work: finite-length analysis of LP decoding over BSC
- Similar behavior of LP and message passing decoders: shed light on non-asymptotic analysis for message passing.

outline

- LP decoding-Background
- Main Result
- LP decoding is a flow on hypergraphs
- Probabilistic analysis of random LDPC codes

LP decoding

- ML decoding can be written as a linear program:
- For a code \mathbf{C} define $\mathbf{Poly}(\mathbf{C})$ the convex hull of codewords.
- ML decoding: minimize negative log likelihood:

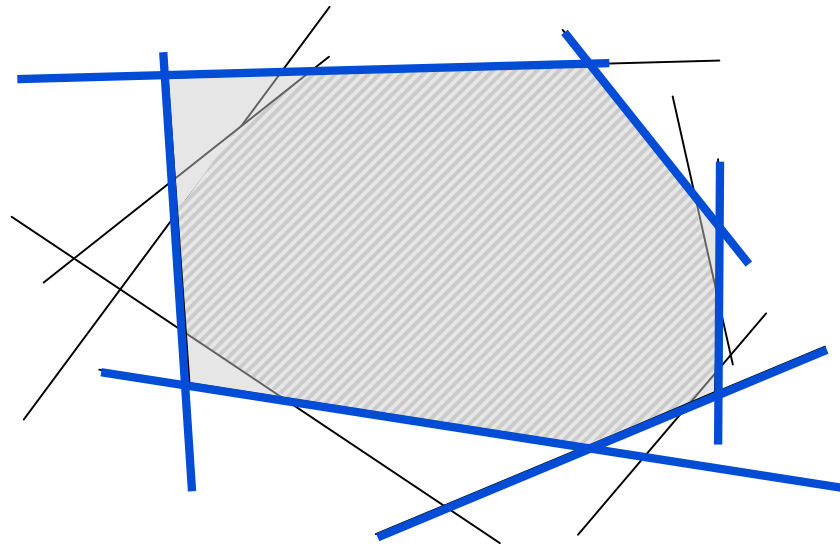
$$\gamma_i = \log\left(\frac{\Pr(r / u = 0)}{\Pr(r / u = 1)}\right)$$

- ML decoding can be written as

$$\begin{aligned} \min \gamma^T x \\ x \in \mathbf{Poly}(\mathbf{C}) \end{aligned}$$

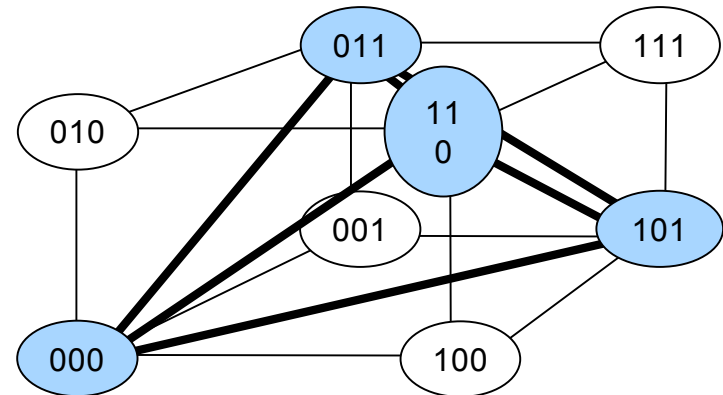
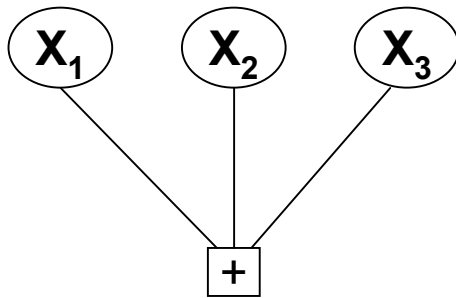
Relaxed polytope

- Unfortunately, **$\text{Poly}(\mathbf{C})$** cannot be described efficiently (ML decoding is NP-hard)
- However suggests a way to approximate: Relax the polytope:



How to relax

- Every check c_j in the code defines a local codeword polytope $LCP(c_j)$:



$$\sum_{i \in (N(j) \setminus S)} x_i + \sum_{i \in S} (1 - x_i) \geq 1 \quad \text{Forbidden Set Inequalities} \quad 0 \leq x_i \leq 1 \quad \text{Box Inequalities}$$

$$P = \bigcap_{\forall j} LCP(c_j)$$

Facts and questions

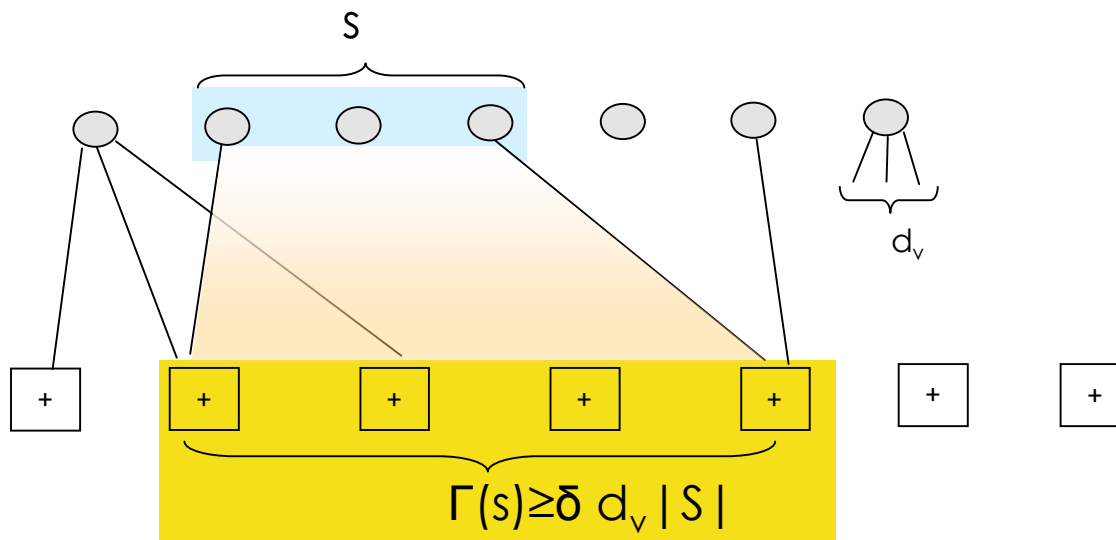
- The relaxed polytope P , contains all codewords plus fractional vertices (**pseudocodewords**)
- If optimization yields integral point, it is the ML codeword (**ML certificate**) (Feldman et al)
- Similar performance with message-passing decoders but can be **analyzed for finite blocklengths**. (errors occur due to near-pseudocodewords)
- How many errors can be corrected?
(hopefully a big constant fraction of n)

outline

- LP decoding-Background
- Main Result
- LP decoding is a flow on hypergraphs
- Probabilistic analysis on random LDPC codes

(λ, δ) -expander graphs

The Tanner graph of a code is an (λ, δ) -expander:



If for every set S , such that $|S| \leq \lambda n$,

$$\Gamma(S) \geq \delta d_v |S|$$

Best previously known result

- If the code is a (λ, δ) -expander, (for suitable λ, δ)
- LP decoding can correct **any** $c_1 n$ or less bit flips.
- For rate=1/2, $c_1=0.00017$
- Worst case analysis, **adversarial** bit flips

Feldman, Malkin, Servedio, Stein and Wainwright, IT Transactions 2006

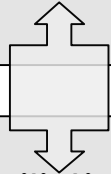
our main result

- **Theorem:** For a random, left regular LDPC code, LP decoding can correct $c_2 n$ **random** bit flips, w.h.p.
- For rate=1/2, $c_2=0.002$
- Average case-probabilistic analysis
- Finite blocklength: Our technique yields error probability bounds for any finite n .

Proof technique

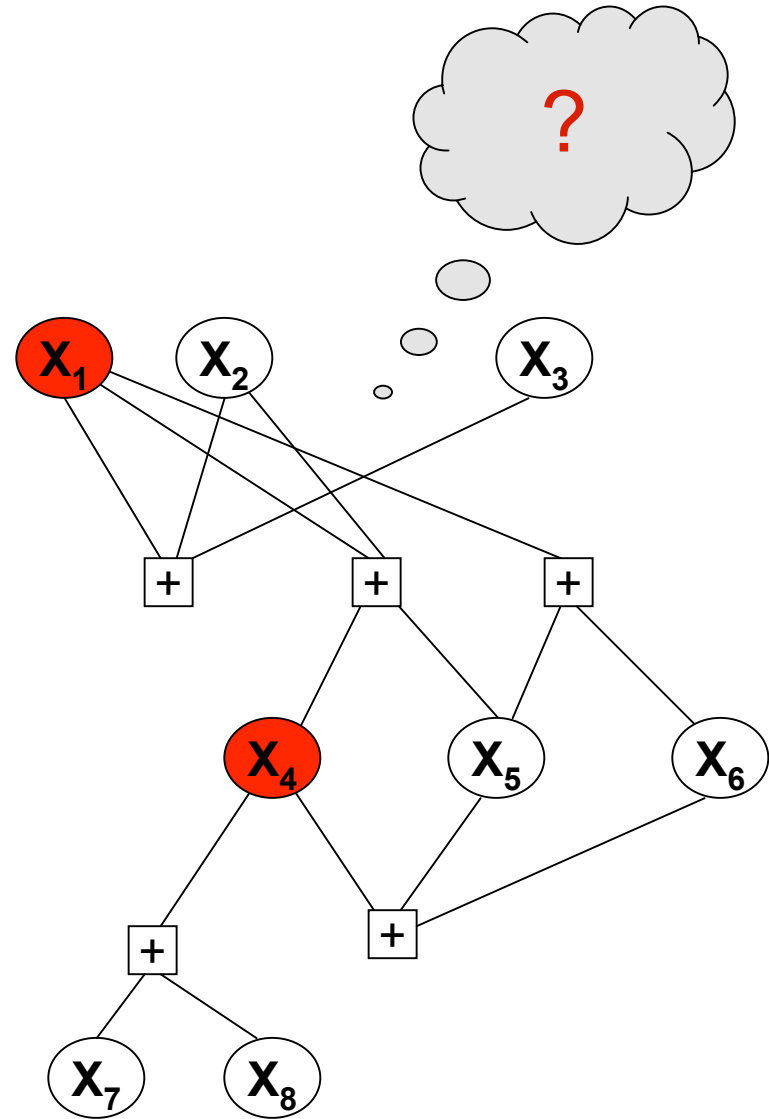
1. Valid Hyperflow

For specific Tanner graph and flipped bits, find a way to see if LP decoder succeeds

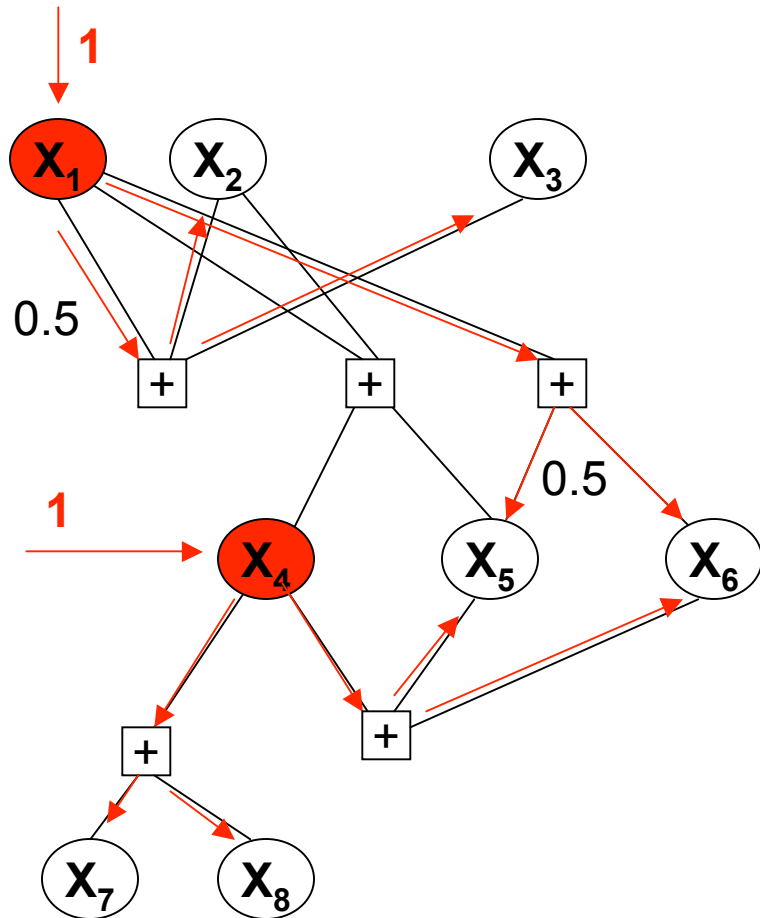


2. Probabilistic analysis

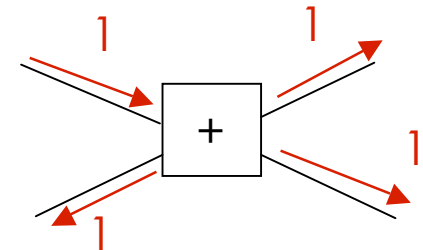
Show that for random code and random bit-errors, a valid hyperflow exists with high probability



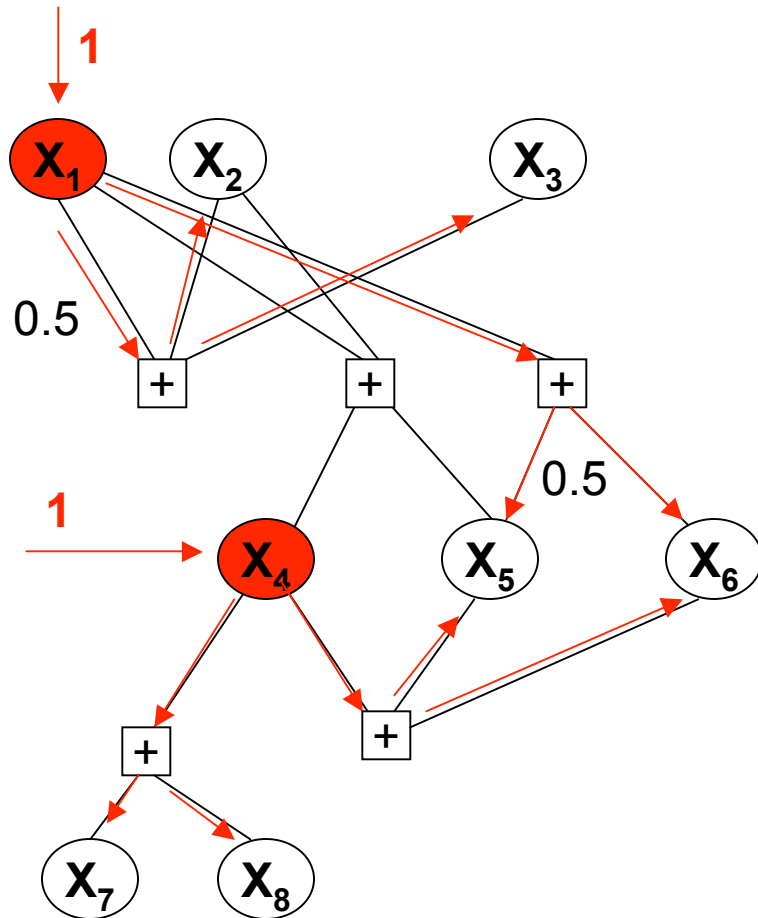
LP decoding is a flow on hypergraphs



- How to show that LP decoding corrects these errors?
- Incoming flow of 1 for each flipped bit
- Unflipped bits can absorb up to 1 unit of flow
- Checks **reproduce** the flow=hyperedges



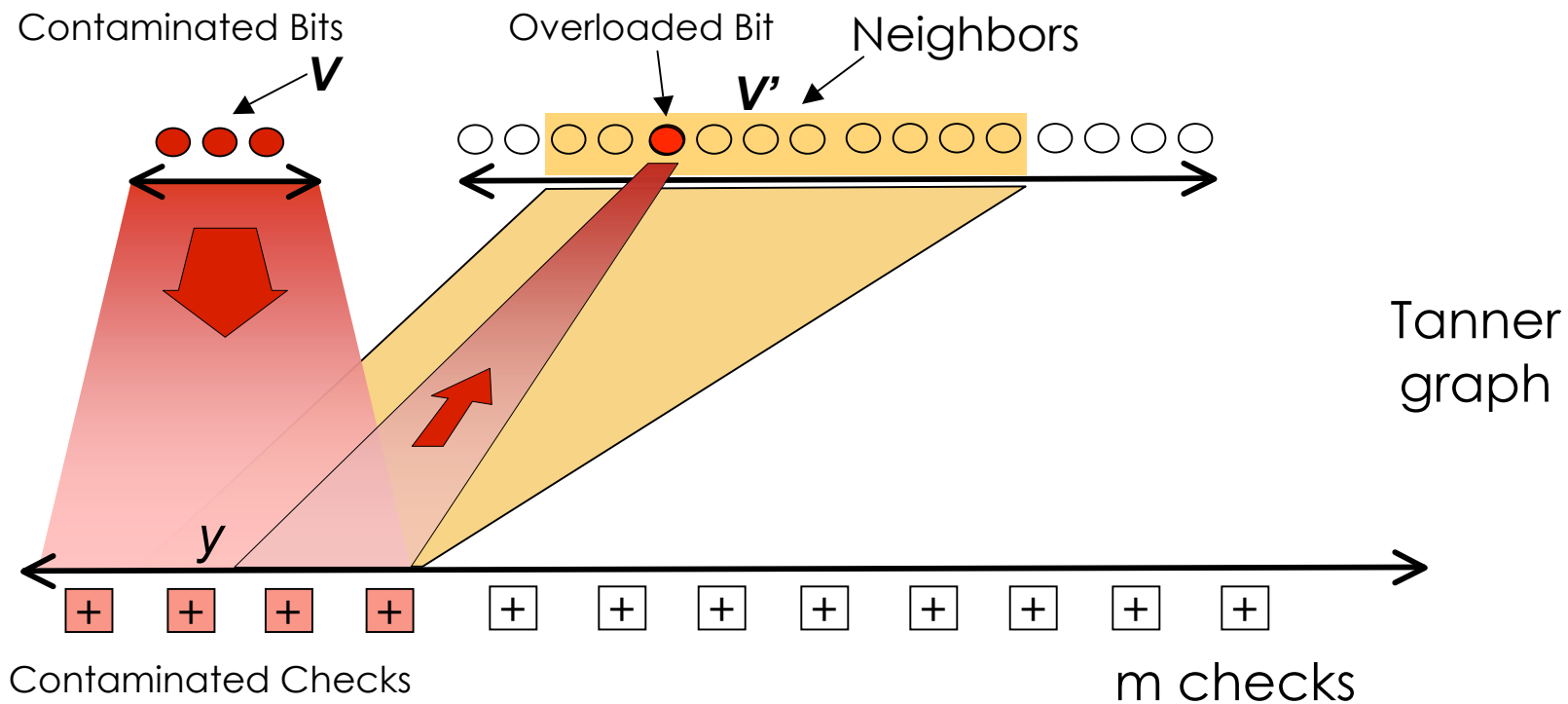
LP decoding is a flow on hypergraphs



- **Theorem:** LP decoding succeeds if there exists a **valid hyperflow** from the flipped to the unflipped bits on the Tanner graph
- Proof by **LP duality** and bounding.
- **Valid hyperflow witness** extends the dual witness of Feldman et al.

Constructing a valid hyperflow

Existence of a (d_v, δ) - **generalized matching**:



Each flipped bit matched with δ checks + no overloaded bits \Rightarrow

Generalized matching \Rightarrow Yields a **valid hyperflow**.

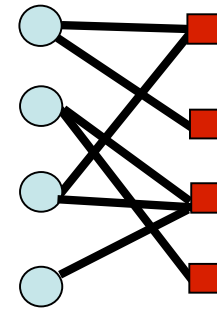
Hall's Theorem

Classical:

Bipartite Graph: n boys, m girls ($n \leq m$) :

There exists a matching for boys \Leftrightarrow

every subset of $i \leq n$ boys knows at least i girls (expands)



Generalized

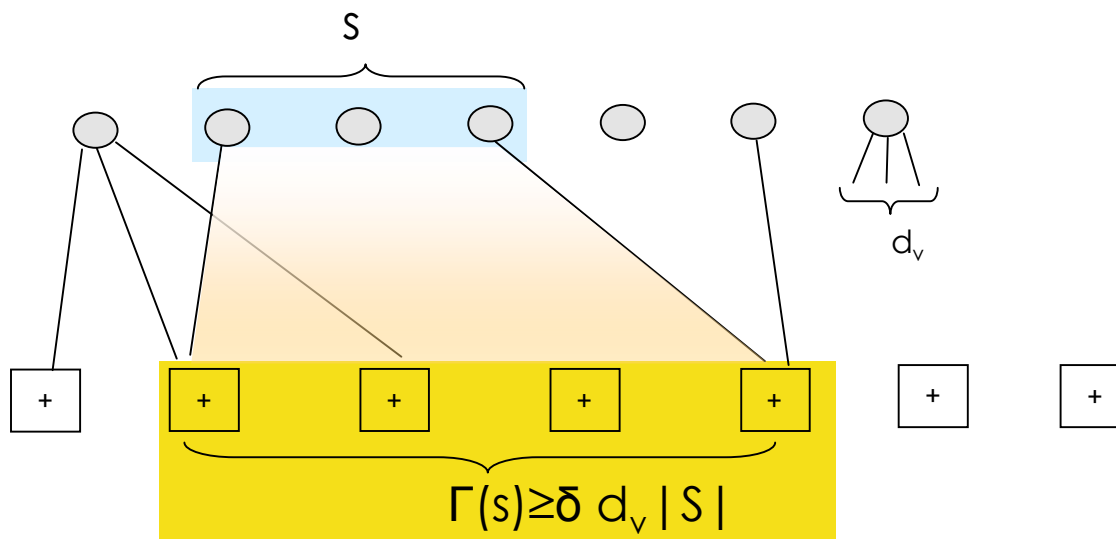
Bipartite Graph: n boys, m girls ($n \leq \delta m$):

There exists a δ -matching for boys \Leftrightarrow

every subset of $i \leq n$ boys knows at least δi girls (expands more)

Probabilistic expanders

The Tanner graph of a code is a (λ, δ) -probabilistic expander:



If for **almost** every set S , such that $|S| \leq \lambda n$,

$$\Gamma(S) \geq \delta d_v |S|$$

Yields **much higher** λ than standard (worst case) expanders
(Concept might be useful more generally in coding theory)

Connecting the pieces of the proof

1. A **random LDPC** will be a **probabilistic expander** w.h.p. (much larger expansion than standard expanders)

Proof by delicate interleaving of martingale concentrations and first moment method

2. A **probabilistic expander** will have a **generalized matching**

Proof by using the concentrations and Generalized Hall's theorem

3. A **generalized matching** guarantees that a **valid hyperflow** exists

Proof by constructing a hyperflow on the matching

4. A **valid hyperflow** is a witness for **LP decoding success**.

Proof by linear programming duality and symmetry of the relaxed polytope.



Conclusions and future work

- Presented average case, finite blocklength analysis. Deal with circles and finite graphs explicitly. Improves the known result by a factor of 10.
- There is still gap to capacity and asymptotic threshold bounds.
- Connections with message-passing: We can show that for trees min-sum is computing the hyperflow exactly. In general?