Belief propagation decoding of quantum channels by passing quantum messages

arXiv:1607.04833

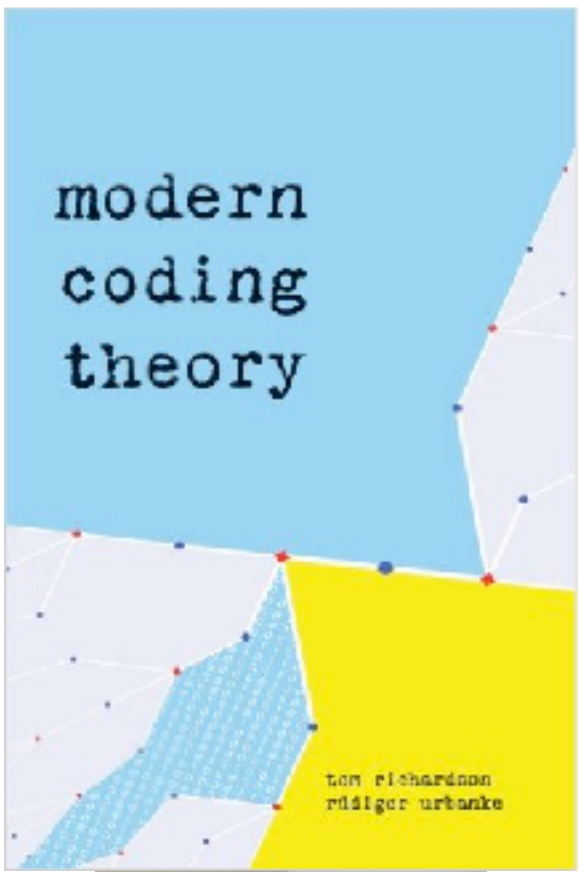
QIP 2017

lempelziv@flickr

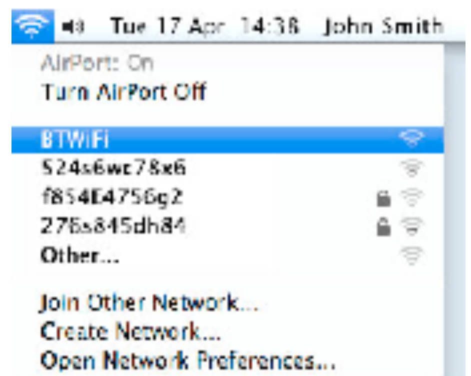
Joseph M. Renes

ETH zürich

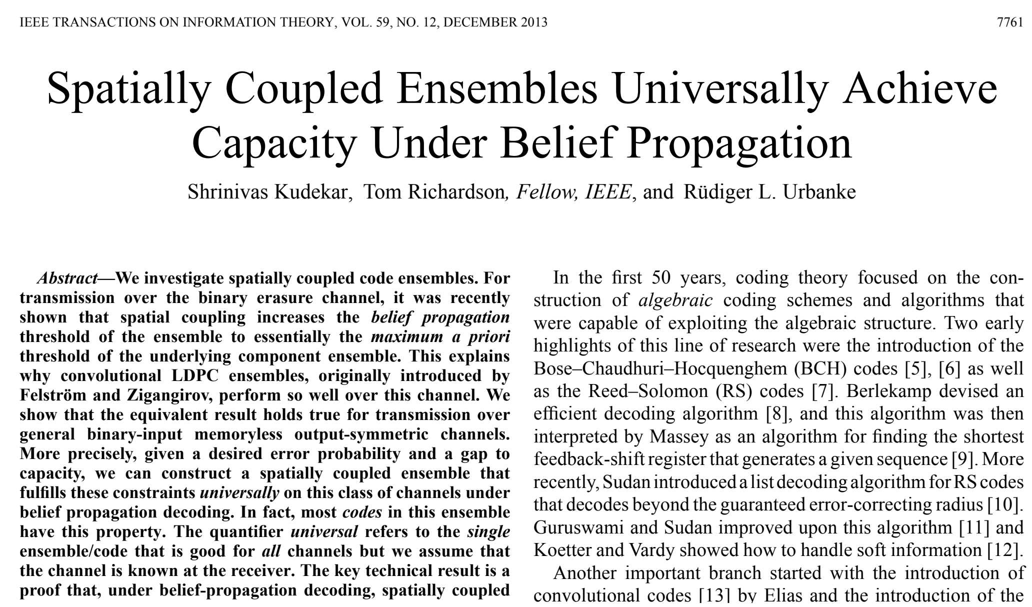
To do research in quantum information theory, pick a favorite text on classical information theory, open to a chapter, and translate the contents into quantum-mechanical language.



Based on belief propagation decoding



arXiv:1607.04833



IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 59, NO. 12, DECEMBER 2013 7761

Spatially Coupled Ensembles Universally Achieve Capacity Under Belief Propagation

Shrinivas Kudekar, Tom Richardson, *Fellow, IEEE*, and Rüdiger L. Urbanke

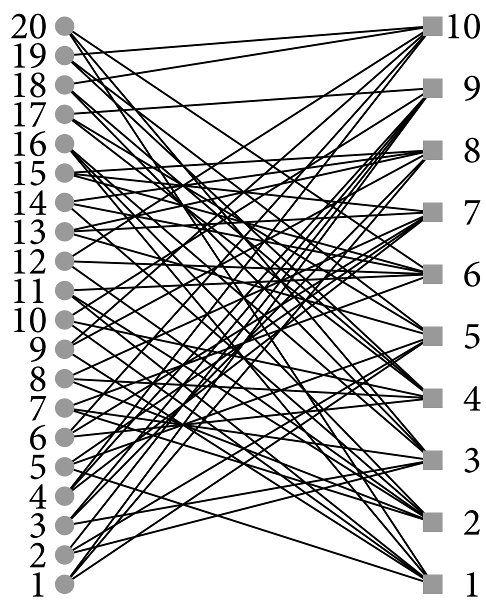
***Abstract*—We investigate spatially coupled code ensembles. For transmission over the binary erasure channel, it was recently shown that spatial coupling increases the *belief propagation* threshold of the ensemble to essentially the *maximum a priori* threshold of the underlying component ensemble. This explains why convolutional LDPC ensembles, originally introduced by Felström and Zigangirov, perform so well over this channel. We show that the equivalent result holds true for transmission over general binary-input memoryless output-symmetric channels. More precisely, given a desired error probability and a gap to capacity, we can construct a spatially coupled ensemble that fulfills these constraints *universally* on this class of channels under belief propagation decoding. In fact, most *codes* in this ensemble have this property. The quantifier *universal* refers to the *single* ensemble/code that is good for *all* channels but we assume that the channel is known at the receiver. The key technical result is a proof that, under belief-propagation decoding, spatially coupled**

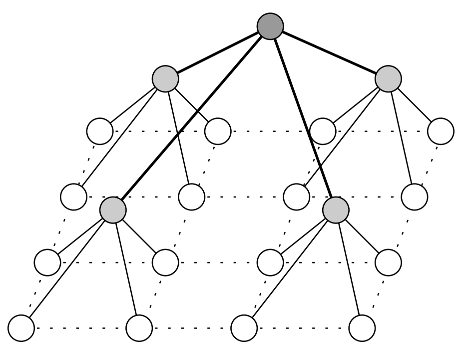
In the first 50 years, coding theory focused on the construction of *algebraic* coding schemes and algorithms that were capable of exploiting the algebraic structure. Two early highlights of this line of research were the introduction of the Bose–Chaudhuri–Hocquenghem (BCH) codes [5], [6] as well as the Reed–Solomon (RS) codes [7]. Berlekamp devised an efficient decoding algorithm [8], and this algorithm was then interpreted by Massey as an algorithm for finding the shortest feedback-shift register that generates a given sequence [9]. More recently, Sudan introduced a list decoding algorithm for RS codes that decodes beyond the guaranteed error-correcting radius [10]. Guruswami and Sudan improved upon this algorithm [11] and Koetter and Vardy showed how to handle soft information [12].

Another important branch started with the introduction of convolutional codes [13] by Elias and the introduction of the

Quantum belief propagation decoding?

Belief propagation: message passing algorithm for performing inference in a graphical model





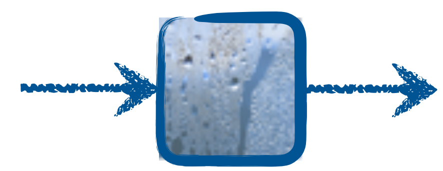
decoder infers channel input from output;
code can be described by a graphical model

early precursor: Bethe-Peierls approximation in statistical physics

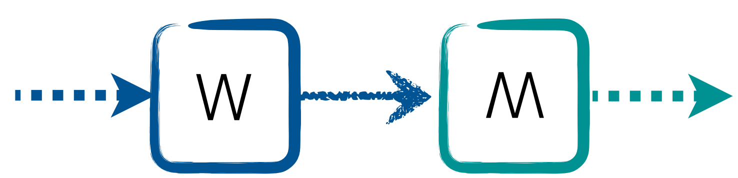
many applications in statistics and machine learning besides coding:

inference, optimization, constraint satisfaction

Quantum belief propagation decoding?

- Can use classical algorithm for usual stabilizer decoding
- Optimal for:  
- But not, e.g. amplitude damping 

Let’s consider CQ channels for simplicity



Need to infer channel input from quantum output

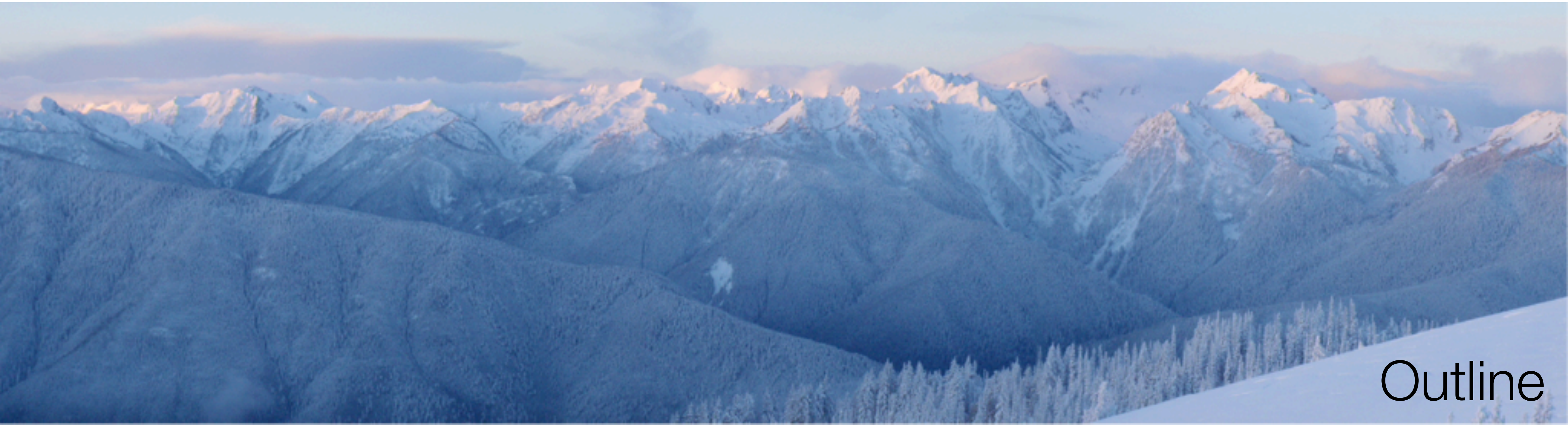
(not trying to compute marginals of quantum states)

Results

arXiv:1607.04833

- BP decoder for pure state channel, tree codes
- Also works for polar codes:
  Efficient, capacity-achieving decoder for BPSK over lossy Bosonic channel
- And for quantum communication, part of conjugate basis decoder:
  Efficient, capacity-achieving decoder for amplitude damping

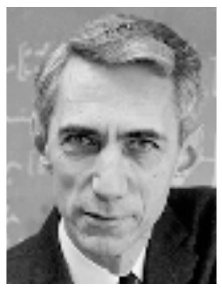
1. Coding setup
2. Factor graphs
3. Classical BP



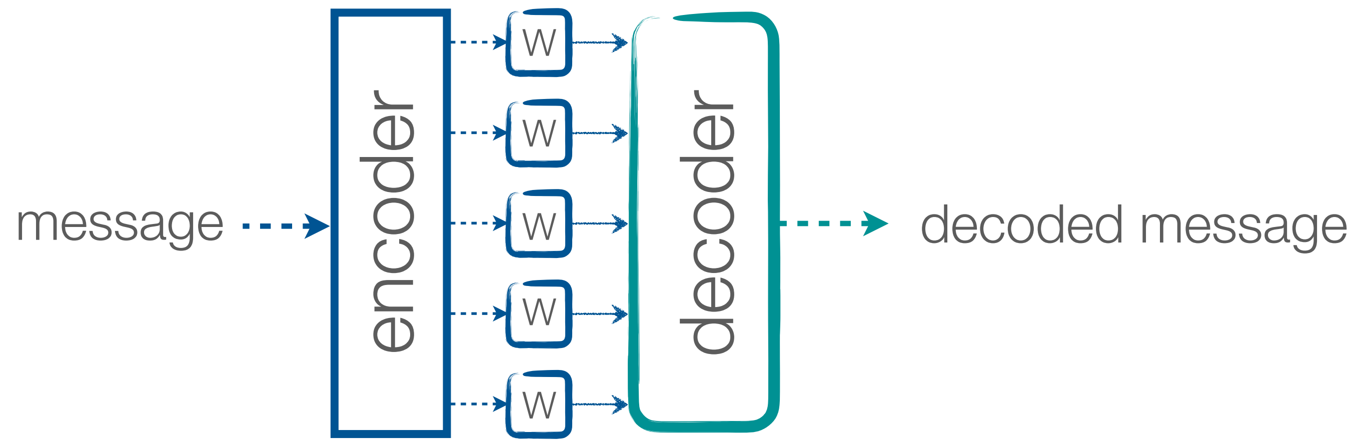
National Park Service

4. Quantum BP
5. Many open questions

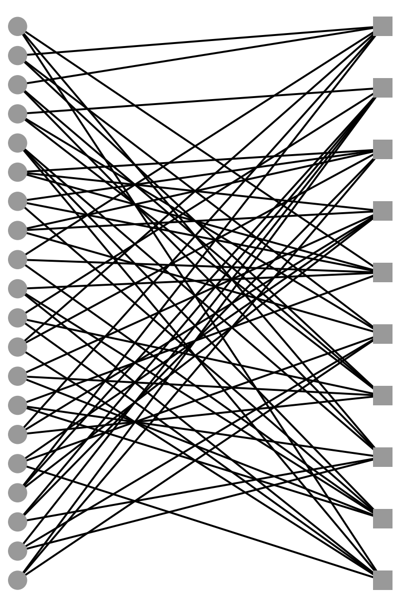
Coding setup



Shannon scenario: stochastic iid noise.
not adversarial; fault-free decoding



Linear code



bitwise decoding of random codeword

classically, marginalize joint distribution

$$P_{X_1^n Y_1^n = y_1^n} \to P_{X_i Y_1^n = y_1^n}$$

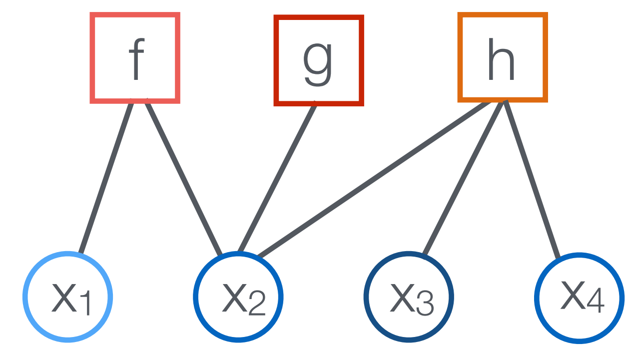
quantumly, perform Helstrom
measurement for each bit

not $\rho_{X_1^n B_1^n} \to \rho_{X_i B_1^n}$

Factor graphs

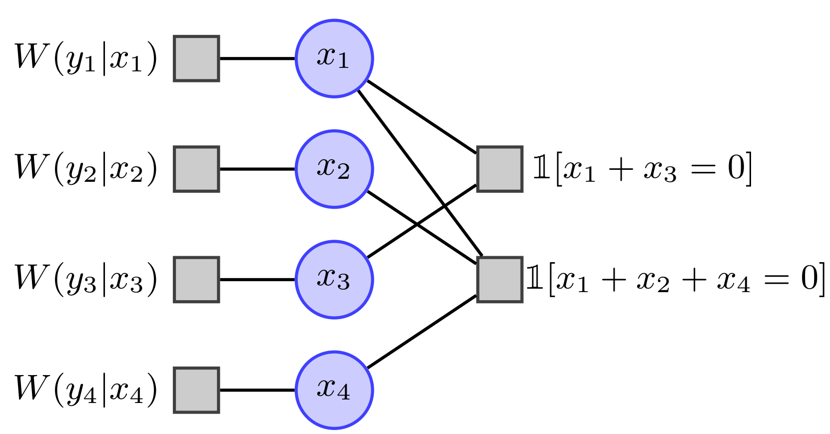
factorizeable joint probability

$$P(x_1, x_2, x_3, x_4) = \frac{1}{Z} f(x_1, x_2) g(x_2) h(x_2, x_3, x_4)$$



easier to compute marginals:

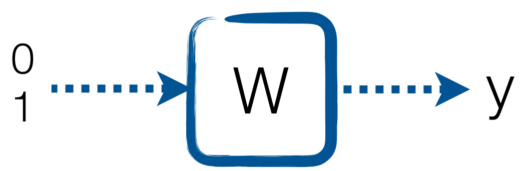
$$P(x_1) = \sum_{x_2, x_3, x_4} P(x_1, x_2, x_3, x_4) = \frac{1}{Z} \sum_{x_2} f(x_1, x_2) g(x_2) \Big(\sum_{x_3, x_4} h(x_2, x_3, x_4) \Big)$$



channel input & output distribution:

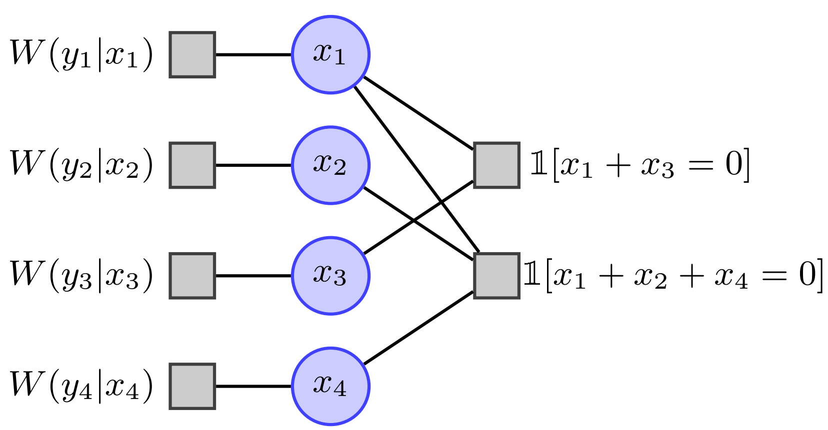
$$P_{X^n Y^n}(x_1^n, y_1^n) = \frac{1}{|C|} \mathbb{1}[x_1^n \in C] \prod_{j=1}^{n} W(y_j | x_j).$$

Classical BP decoding



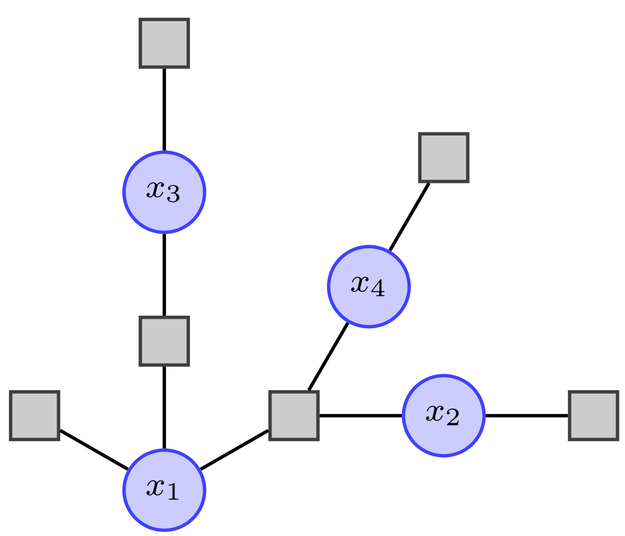
symmetric binary input channel:
only care about likelihood ratio

$$\ell(y) = \frac{W(y|1)}{W(y|0)}$$



$x_i \to y_1^n$ is a channel;
want $\ell(y_1^n)$

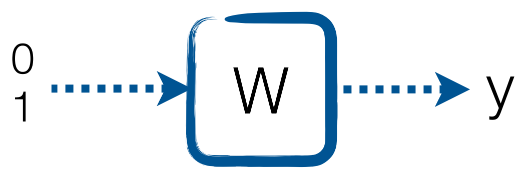
assume tree factor graph



for each node,
associate a channel to all its leaves

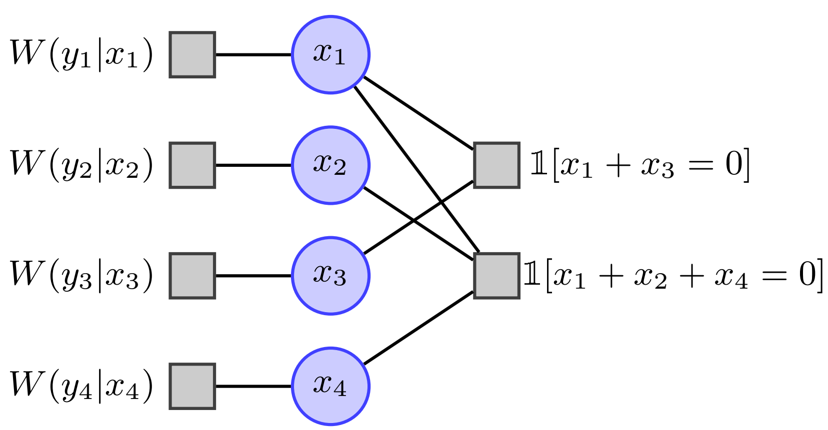
BP recursively computes $\ell(y_1^n)$
starting from the leaves

Classical BP decoding



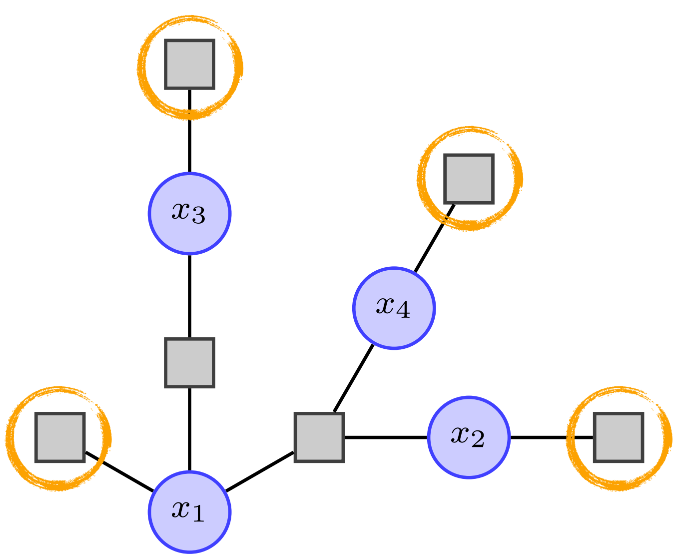
symmetric binary input channel:
only care about likelihood ratio

$$\ell(y) = \frac{W(y|1)}{W(y|0)}$$



$x_i \to y_1^n$ is a channel;
want $\ell(y_1^n)$

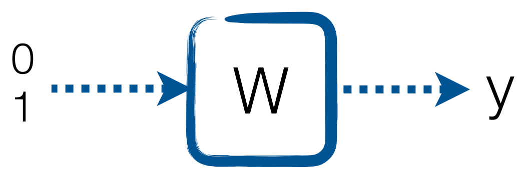
assume tree factor graph



for each node,
associate a channel to all its leaves

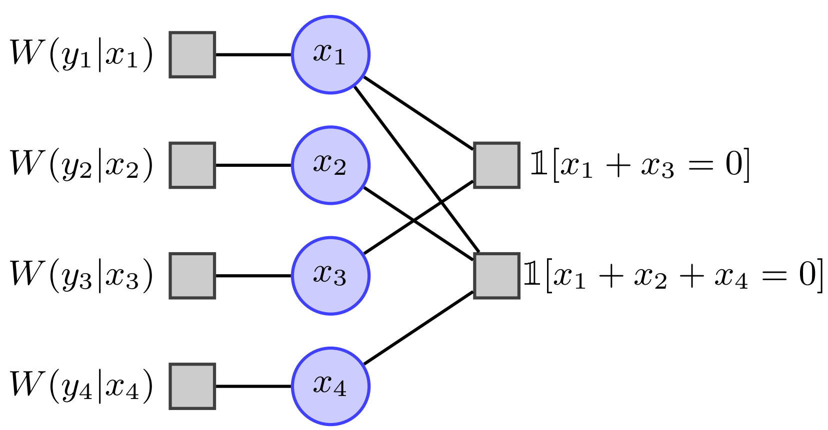
BP recursively computes $\ell(y_1^n)$
starting from the leaves

Classical BP decoding



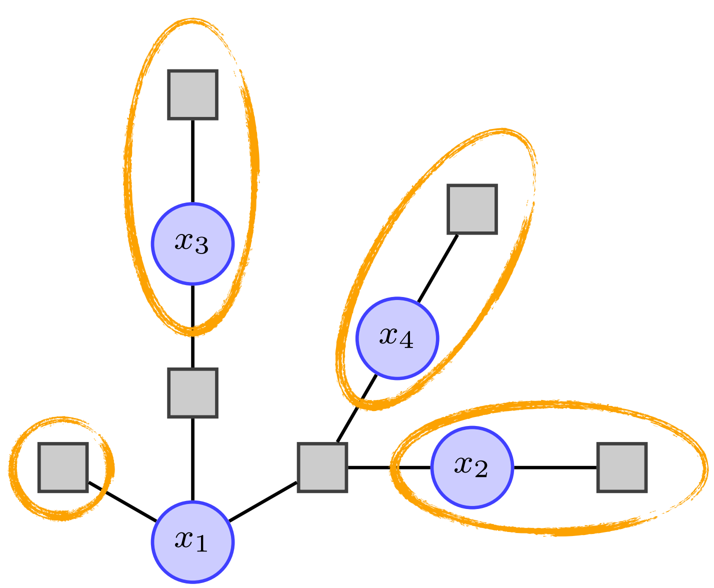
symmetric binary input channel:
only care about likelihood ratio

$$\ell(y) = \frac{W(y|1)}{W(y|0)}$$



$x_i \to y_1^n$ is a channel;
want $\ell(y_1^n)$

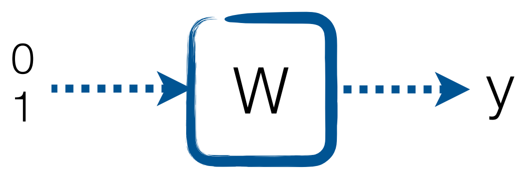
assume tree factor graph



for each node,
associate a channel to all its leaves

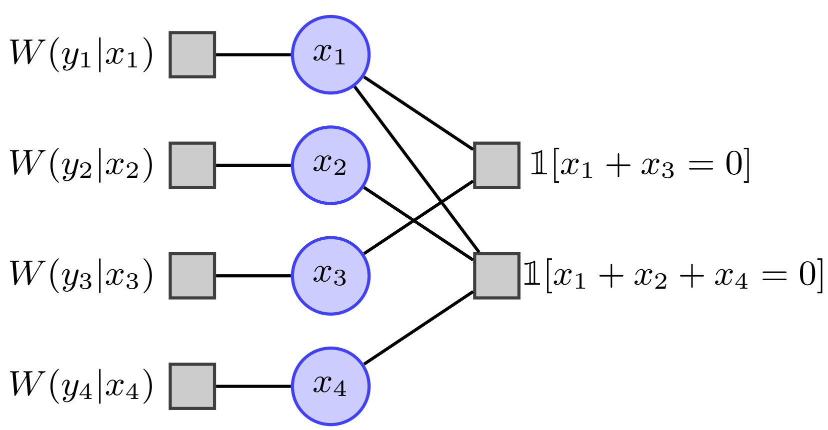
BP recursively computes $\ell(y_1^n)$
starting from the leaves

Classical BP decoding



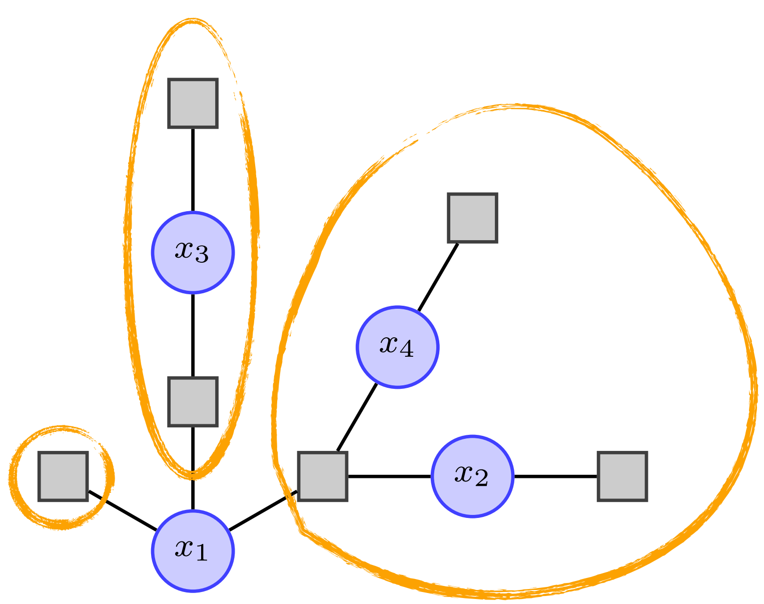
symmetric binary input channel:
only care about likelihood ratio

$$\ell(y) = \frac{W(y|1)}{W(y|0)}$$



$x_i \to y_1^n$ is a channel;
want $\ell(y_1^n)$

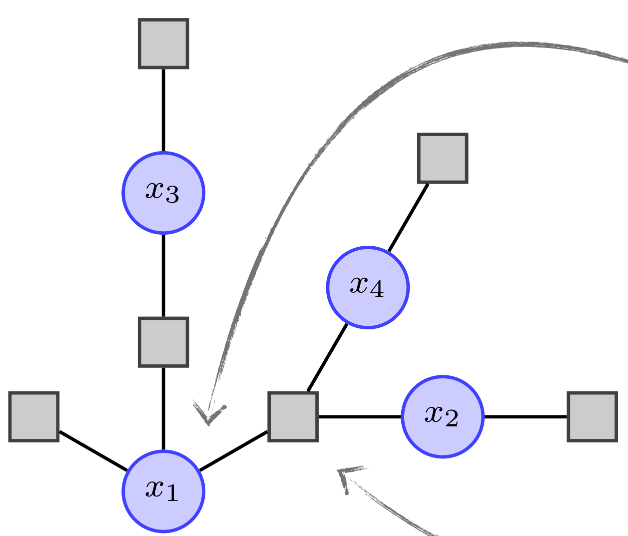
assume tree factor graph



for each node,
associate a channel to all its leaves

BP recursively computes $\ell(y_1^n)$
starting from the leaves

Classical BP decoding



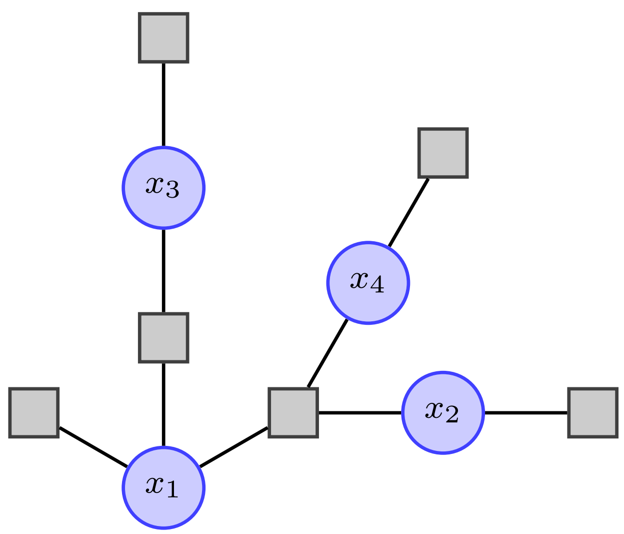
BP rules specify two kinds of channel convolution

$W \circledast W'$	$W_0 \otimes W'_0$ $W_1 \otimes W'_1$	Variable node
$W \boxast W'$	$1/2(W_0 \otimes W'_0 + W_1 \otimes W'_1)$ $1/2(W_0 \otimes W'_1 + W_1 \otimes W'_0)$	Check node

- BP finds exact marginals on trees
- Can run algorithm for all codeword bits concurrently
- Also works on loopy LDPC factor graphs


Barefoot Jake

Quantum BP decoding



Now the outputs are quantum, no likelihood function

Want to perform Helstrom measurement

Can we combine Helstrom measurements along the branches?

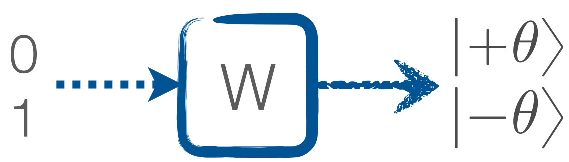
Can we "repackage" the outputs as with likelihood?

Try the simplest case: pure state outputs

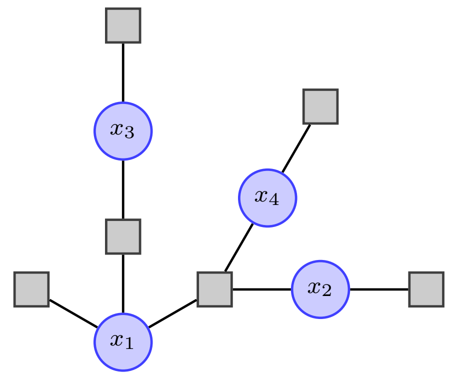
$$\langle +\theta | -\theta \rangle = \cos\theta$$

optimal measurement is σ_x

Quantum BP decoding



$\langle +\theta | -\theta \rangle = \cos\theta$



$W \circledast W'$	$W_0 \otimes W_0'$ $W_1 \otimes W_1'$
$W \boxast W'$	$1/2(W_0 \otimes W_0' + W_1 \otimes W_1')$ $1/2(W_0 \otimes W_1' + W_1 \otimes W_0')$

$\circledast$ convolution yields pure states: repackage in a single qubit with $U_{\circledast}(\theta, \theta')$

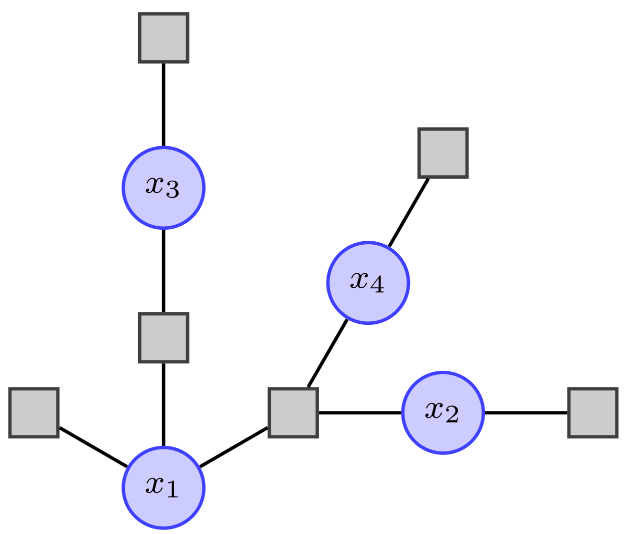
$$|+\theta\rangle \otimes |+\theta'\rangle \quad |-\theta\rangle \otimes |-\theta'\rangle \longrightarrow |\pm\theta^{\circledast}\rangle \quad \cos\theta^{\circledast} = \cos\theta\cos\theta'$$

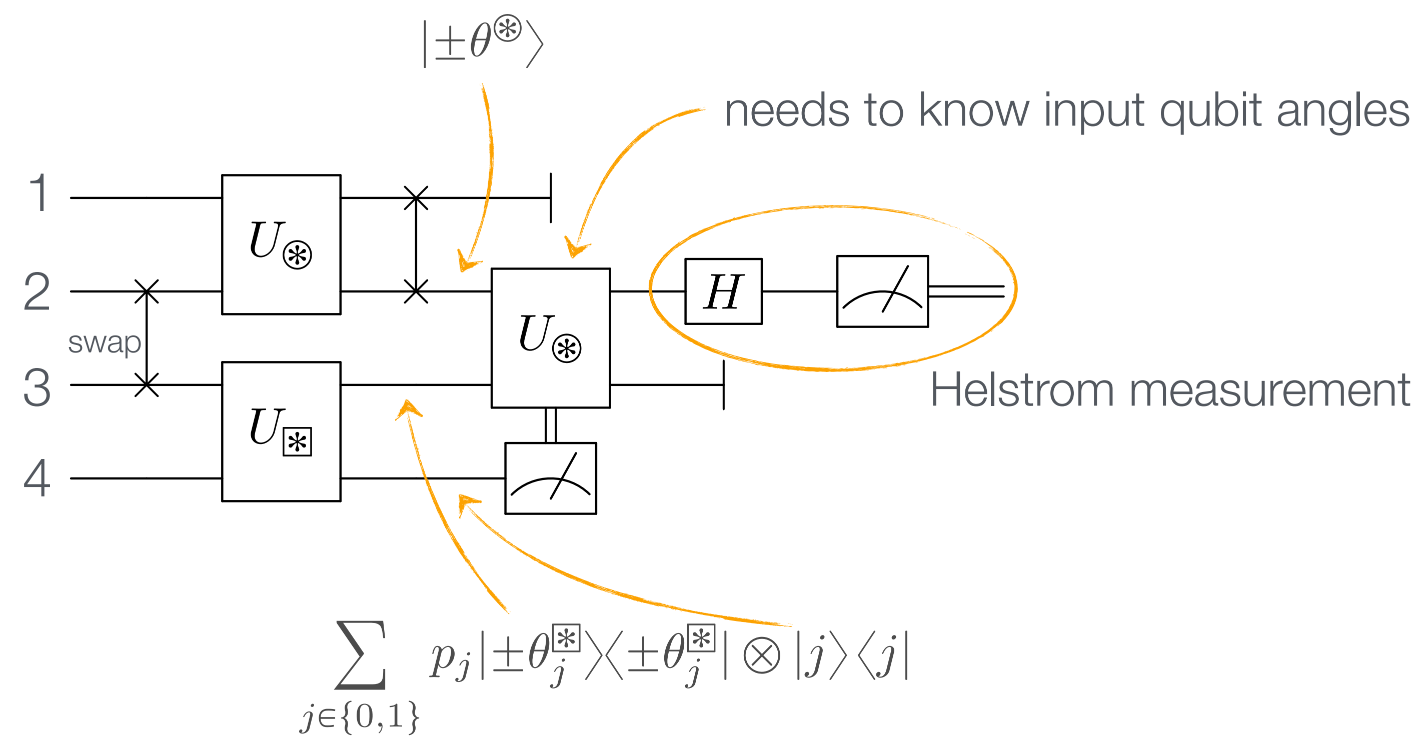
$\boxast$ convolution gives a *heralded* mixture of pure states!

unitary $U_{\boxast}$ gives $\sum_{j\in\{0,1\}} p_j \, |j\rangle\langle j| \otimes |\pm\theta_j^{\boxast}\rangle\langle \pm\theta_j^{\boxast}|$

$$p_0 = \tfrac{1}{2}(1 + \cos\theta\cos\theta') \qquad \cos\theta_0^{\boxast} = \frac{\cos\theta + \cos\theta'}{1 + \cos\theta\cos\theta'} \qquad \cos\theta_1^{\boxast} = \frac{\cos\theta - \cos\theta'}{1 - \cos\theta\cos\theta'}$$

Quantum BP decoding



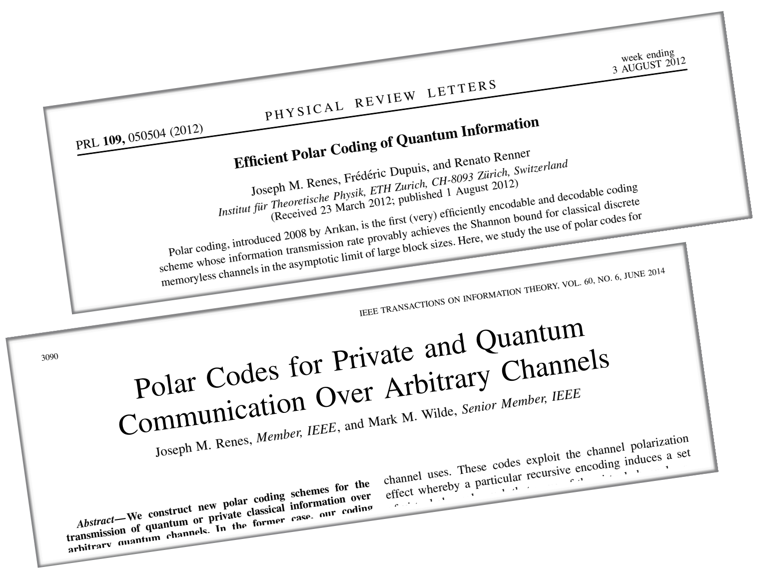


- pass qubits and some classical bits: “sufficient statistic”
- decode all codeword bits sequentially, unwinding each time
- $O(n^2)$ implementation of all Helstrom measurements

Quantum BP & polar codes

Variable and check convolutions = “better” and “worse” synth channels

Polar decoder has tree structure (for message not codeword bits, tho)


PRL **109**, 050504 (2012) PHYSICAL REVIEW LETTERS week ending 3 AUGUST 2012

Efficient Polar Coding of Quantum Information

Joseph M. Renes, Frédéric Dupuis, and Renato Renner

Institut für Theoretische Physik, ETH Zurich, CH-8093 Zürich, Switzerland

(Received 23 March 2012; published 1 August 2012)

Polar coding, introduced 2008 by Arıkan, is the first (very) efficiently encodable and decodable coding scheme whose information transmission rate provably achieves the Shannon bound for classical discrete memoryless channels in the asymptotic limit of large block sizes. Here, we study the use of polar codes for

3090 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 60, NO. 6, JUNE 2014

Polar Codes for Private and Quantum Communication Over Arbitrary Channels

Joseph M. Renes, *Member, IEEE*, and Mark M. Wilde, *Senior Member, IEEE*

Abstract—**We construct new polar coding schemes for the transmission of quantum or private classical information over arbitrary quantum channels. In the former case, our coding**

channel uses. These codes exploit the channel polarization effect whereby a particular recursive encoding induces a set

Quantum polar decoder uses polar decoder
for classical amplitude and phase info

 : amplitude = classical Z channel,
phase = pure state channel

O(n^2) decoder for capacity-achieving quantum polar code for amplitude damping

Open

oldsloat.blogspot

Questions

Open

other channels? e.g. classical coding for amplitude damping?

loops? spatially-coupled LDPC codes?

- use density matrix BP? need sufficient statistics, local tree to global
- relation to tensor networks?
- junction-tree algorithm?

Viterbi decoder (blockwise decoder)?

fully quantum version?

other tasks besides decoding?

Questions