# Ph/CS 219C

**Exercises**
**Due: Thursday 21 May 2026**

### 3.1 Belief propagation on a line and on a cycle.

Consider the Tanner graph of a 3-bit repetition code. The three variable nodes are denoted 1, 2, 3. There are also two check nodes denoted $a$, $b$. The graph has four edges. Check $a$ is connected by edges to variables 1 and 2; check $b$ is connected by edges to variables 2 and 3. For variable $i$, $e_i$ indicates whether that variable has an error or not ($e_i = 1$ for an error and $e_i = 0$ for no error). The syndrome bits at the check nodes are denoted by $s_a$, $s_b$. For example, $s_a = 1$ indicates that the pair $(e_1, e_2)$ is either $(1, 0)$ or $(0, 1)$, and $s_a = 0$ indicates that $(e_1, e_2)$ is either $(0, 0)$ or $(1, 1)$. We consider independent noise acting on the three variables, but with distinct prior distributions given by $\psi_i(e_i)$, where $i = 1, 2, 3$.

*a*) Suppose $(s_a, s_b) = (1, 0)$. Find the global joint probability distribution for the three variables $P(e_1, e_2, e_3)$ and derive from this joint distribution the marginal distributions $P_i(e_i)$ for each of the three variables. Write these marginals as log likelihood ratios defined by

$$L_i^{\text{true}} = \ln\left(\frac{P_i(0)}{P_i(1)}\right), \tag{1}$$

expressed in terms of the prior log likelihood ratios

$$L_i^{\text{prior}} = \ln\left(\frac{\psi_i(0)}{\psi_i(1)}\right). \tag{2}$$

When the Tanner graph is a tree (i.e., contains no closed loops, as is true in this case), belief propagation is guaranteed to converge to the true marginal distributions. In the first round of BP, each variable sends its prior log likelihood ratio to its neighboring checks. Subsequently, in even-numbered rounds checks pass messages to their variable neighbors, and in odd-numbered rounds variables pass messages to neighboring checks, following rules described in class (and in the lecture notes).

*b*) Write out explicitly the messages sent in each round, up to the point where the protocol converges (after which messages sent by check and by variables no longer change). After how many rounds is convergence achieved?

*c*) Verify that the true marginal distributions $L_i^{\text{true}}$ are reached when BP converges.

Consider now the Tanner graph of a 3-bit repetition code with three check nodes instead of two. The additional check node $c$ is connected by edges to variables 3 and 1.

*d*) Suppose that the check bits are $(s_a, s_b, s_c) = (1, 1, 0)$. Assuming the same prior distributions as before, find the global joint distribution for the three variables, and express the corresponding log likelihood ratios $L_i^{\text{true}}$ in terms of the prior log likelihood ratios $L_i^{\text{prior}}$.

*e*) Does BP converge to the true marginals in this case?

### 3.2 Correcting erasure errors in the toric code

Consider erasure errors in a classical linear error-correcting code with code length $n$. If there is a unique error supported on the erased set of bits that could have caused the observed error, then this error can be found in $O(n^3)$ time using Gaussian elimination. The same applies to the $X$ or $Z$ error correction in a quantum CSS code. In the toric code, though, erasure correction can be achieved much more efficiently, requiring only $O(n)$ time.

Consider correction of $Z$ errors in the unrotated toric code – qubits are on edges and checks are on vertices of a square lattice. Suppose that a known subset of the qubits is erased and no non-erasure errors occur. Each erased qubit is replaced by a maximally mixed qubit; hence for the erased qubits $Z$ errors occur with probability $1/2$. The syndrome is measured and is fully supported on vertices that are contained in erased edges. We are to apply $Z$ to a subset of the erased qubits until the syndrome becomes trivial, ideally without inducing a logical error in the process.

*a*) Suppose that the erased edges form a connected tree (with no closed loops). Describe a decoding procedure that yields a trivial syndrome after a number of steps that is no larger than the size of the erased set. **Hint:** Construct a decoder that acts only on the erased set, starting at the leaves of the tree.

*b*) Using your decoder, what is the probability of a decoding error?

For a graph with constant degree and $n$ vertices, a *spanning forest* can be constructed by an $O(n)$-time classical algorithm. A spanning forest of a graph $G = (V, E)$ is a subgraph $F = (V, E')$ such that: (1) $F$ contains all vertices of $G$. (2) $F$ contains no closed loops.(3) Two vertices are connected in $F$ if and only if they are connected in $G$.

*c*) Describe a decoder for the toric code that runs in $O(n)$ time.

*d*) Suppose the erased set contains no homologically nontrivial loops. What is the probability of a decoding error?

*e*) Suppose the erased set contains one or more homologically nontrivial loops. What is the probability of a decoding error?

*f*) Is your decoder optimal? That is, does it achieve the lowest possible probability of a decoding error for any possible erased set of qubits?

### 3.3 Toom's rule in a two-dimensional classical repetition code

Toom's rule is a decoder for the 2D classical repetition code. Suppose data bits reside on the plaquettes of a square lattice. Each syndrome bit, residing on an edge, records the parity of two data bits that share that edge. In each decoding step, every data bit observes the syndrome bits on its northern and eastern edges, and flips itself if both those syndrome bits are nontrivial.

A set of data bits with errors can be decomposed as a union of disjoint connected "droplets." A set of data bits forms a connected droplet if, for any two plaquettes $P_i$ and $P_j$ in the set, there exists a sequence of plaquettes beginning with $P_i$ and ending with $P_j$ such that each consecutive pair of plaquettes in the sequence shares an edge. Repeatedly applying Toom's rule can gradually "erode" the droplet, eventually removing it completely, hence correcting all the bit-flip errors that had been contained inside the droplet.

*a*) On the 2D plane, consider a set of droplets that are all completely contained within a rectangle which has side length $L$ in the north-south direction and side length $W$ in the east-west direction. Let $T(L, W)$ denote the maximum number of Toom's rule steps that suffice to complete erode all droplets in the rectangle. What is $T(L, W)$?

*b*) What is the minimum-weight error (minimal number of flipped plaquettes) contained inside the rectangle for which $T(L, W)$ steps are required to fully erode all droplets?

*c*) For a connected droplet with $N$ errors, what is the maximum number $T(N)$ of steps needed to erode the droplet completely?

*d*) What droplet shapes require $T(N)$ steps to erode completely? How many such shapes are there?

*e*) Consider the 2D repetition code on an $L \times W$ torus (periodic boundary conditions). Are there now droplets that fail to erode? What is the lowest weight droplet that fails to erode?

### 3.4 A CNOT gadget constructed from measurements

Verify the circuit identity shown in Fig. 1. Here $\mathcal{M}_\sigma$ represents measurement of the Pauli operator $\sigma$, $|+\rangle$ is the eigenstate of $X$ with eigenvalue $+1$, and $\sigma_1$, $\sigma_2$ on the right-hand side of the equation are single-qubit Pauli operators that depend on the outcomes of the four measurements in the circuit on the left-hand side. What are $\sigma_1$ and $\sigma_2$? **Hint**: Check that Pauli operators propagate through the circuit as they do through a CNOT gate:

$$\text{CNOT}: \quad XI \to XX\ , \quad IX \to IX\ , \quad ZI \to ZI\ , \quad IZ \to ZZ\ ,$$

(where the first qubit is the control qubit and the second qubit is the target qubit of the CNOT) except for minus signs that depend on the measurement outcomes, and note that the minus signs can be removed by choosing $\sigma_1$ and $\sigma_2$ appropriately.

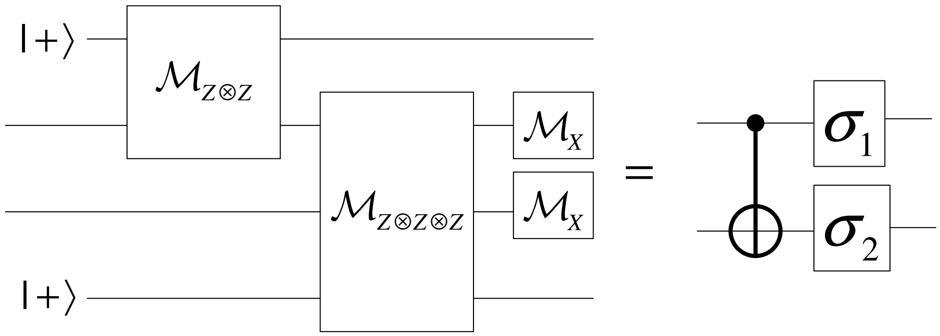


Figure 1: A measurement-based CNOT gadget.

Though it is a bit more complicated than the measurement-based CNOT gadget constructed in class, this gadget has an advantageous feature: the Pauli operators that are measured nondestructively are $Z$-type operators. In some experimental settings these are easier to measure than operators that are $X$-type or of mixed type.