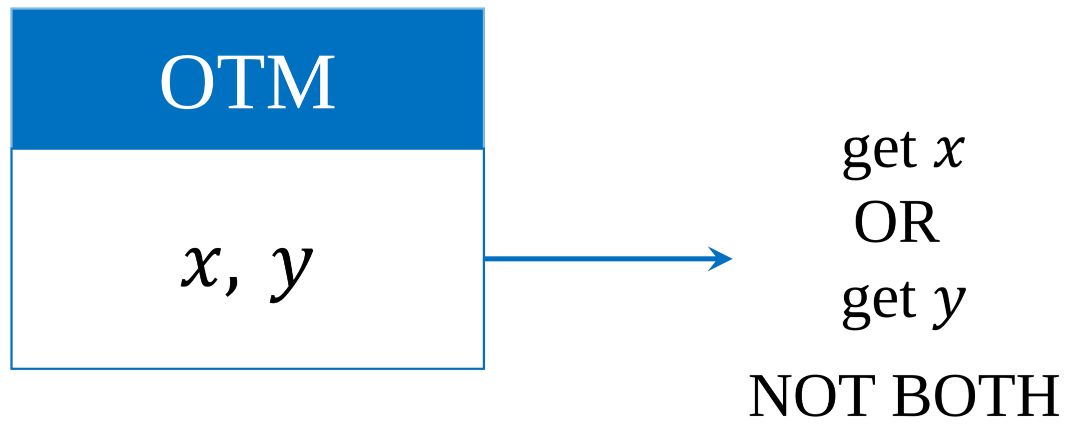
One-time memory from isolated Majorana islands

Sourav Kundu†, Ben Reichardt

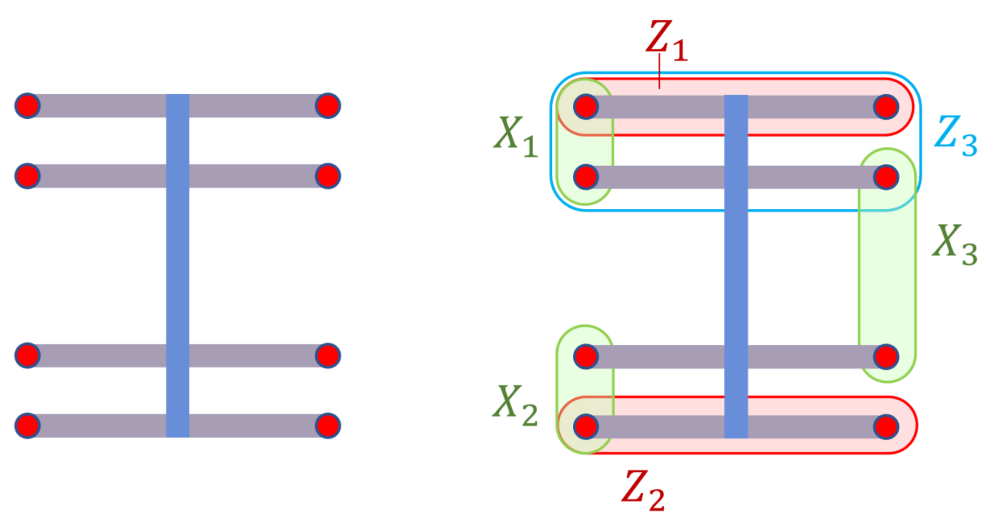
† Email: souravku@usc.edu, Zoom: 8966571313

One-time memory (OTM)

An ideal one-time memory stores two bits x and y. Bob can choose to read either x or y, but not both.



Octon Majorana islands



Karzig et al. [1] propose that islands of superconducting nanowires correspond to qubits. An "octon" island with 8 **Majorana zero modes** corresponds to 3 qubits

Properties:

- Only can measure parity of any 2 MZMs
- The island has overall even parity
- Two operators commute if they intersect on even number of MZMs (Z_1 and Z_3), else anticommute

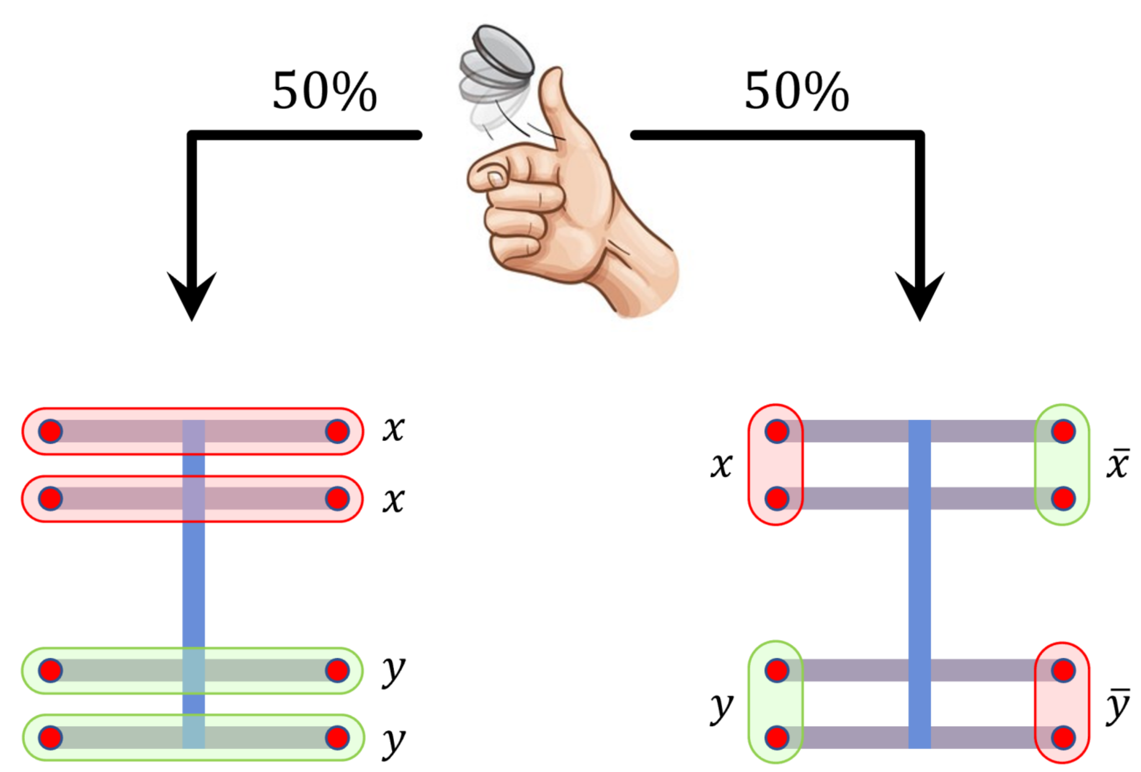
Claim: Octon is imperfect OTM

$$\mathbb{P}(\text{get } x) = 1 \qquad \mathbb{P}(\text{get } y) = \frac{3}{4}$$

OR

$$\mathbb{P}(\text{get } x) = \frac{3}{4} \qquad \mathbb{P}(\text{get } y) = 1$$

Store 2 bits in octon OTM



Alice randomly chooses the Z basis (left) or the X basis (right) to store bits x and y.

Read bit from octon OTM

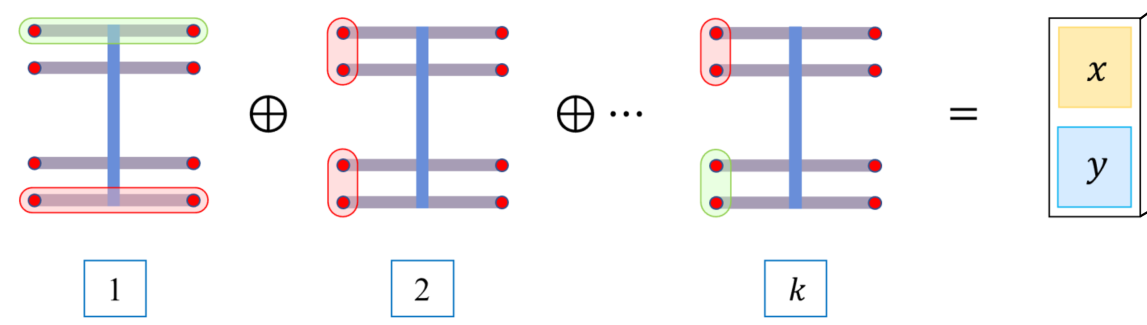
Suppose Bob wants bit x (stored in top four MZMs)

He measures parity of bottom four MZMs in either X or Z basis, by measuring the 2 vertical operators or the 2 horizontal operators. If the bottom has even parity, he reads bit x from the horizontal operator. If it has odd parity, he reads bit x from the vertical operator.

Thus, he always obtains bit x perfectly. But bit y is lost if he chose the wrong basis to get parity of bottom.

$$\mathbb{P}(\text{get } y) = \frac{3}{4}$$

Octon cluster → Better OTM



A cluster of k octons is equivalent to a nearly perfect OTM. One bit is given by XOR of the top bits of all k octons, and the other bit is given by XOR of bottom bits of all k octons. If we want to correctly output one bit (say x), the other bit y can be read with probability

$$\mathbb{P}(\text{get } y) = \frac{1}{2} + \frac{1}{2^{k+1}}$$

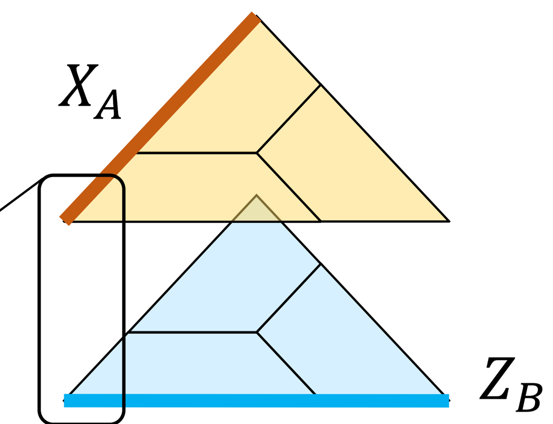
Error correction on OTM

What about MZM faults?

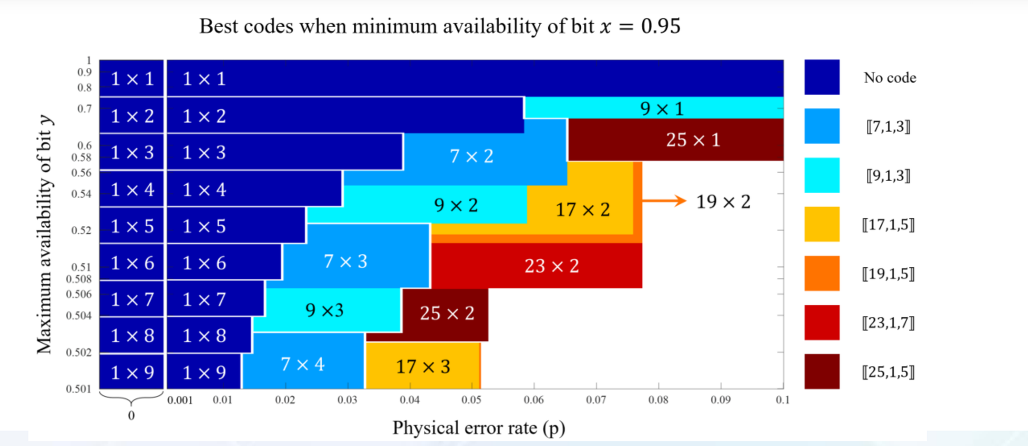
We choose a CSS code and obtain two classical codes A and B from it.

- In top layer, code A corresponds to the X stabilizers and logical operator X_A.
- In bottom layer, code B corresponds to Z stabilizers and logical operator Z_B.
- All stabilizer equivalents of X_A and Z_B intersect.

Thus, we can store the two classical bits as the parity of logical operators X_A and Z_B. Obtaining parity of one logical operator reduces probability of getting the other one.



Conclusion



References

1. T. Karzig et al., PRB 95, 235305 (2017)
2. S. Goldwasser et al., Crypto 2008, 39