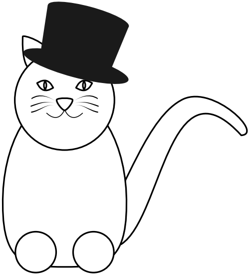
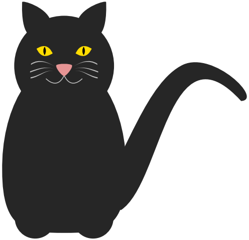
(Quantum) Codes and Correlations

Emina Soljanin, Rutgers





Acknowledgement

This presentation is based in part on joint work with

Michael Schleppy & **Nicolas Swanson**

Optimal Strategies for Winning Certain Cosset-Guessing Quantum Games

to appear in JSAIT https://arxiv.org/abs/2410.08160

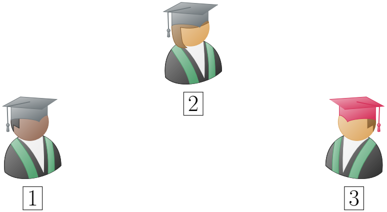
Funding:

NSF-FET Award # 2007203

NSF-GRF for Michael

A Hat Color Game – (Three) players and a Judge

The judge randomly picks one of the two hat colors for each player.



The players can see the hats of other players but not their own.

- Once they have had a chance to look at the other hats, the players must simultaneously guess the color of their own hats or pass.
- They win if there is at least one correct and no incorrect guess.
- The players can agree on a strategy in advance.
  Once the game starts, they cannot communicate.

What is the maximal winning probability? How can it be achieved?

Three Playing Strategies and their Winning Rates P_{win}

1. Each player guesses a randomly $\longleftrightarrow$ guesses a preselected color.
   $\longrightarrow P_{win} = 1/8$

2. One player guesses randomly and all other pass.
   $\longrightarrow P_{win} = 1/2$

3. A player offers a guess iff he sees two identical colors.
   The guess is the other color (not the one observed).

   Suppose colors are 0 & 1 and consider all color-assignment scenarios:

000	111	all speak
100	011	#1 speaks
010	101	#2 speaks
110	001	#3 speaks

   We see that $P_{win} = 3/4$.

Can we Extend the Strategy to n Players?

Some observations about the three player optimal strategy:

1. Players are given a random three-bit string s. Each sees a two bits.
2. They base their guesses on the strings in set $\boxed{C = \{000, 111\}}$.
3. If $s \in C$, all players speak up and all guesses are wrong.
4. For all $s \notin C$ at most one player speaks.
5. Any other three-bit string is one bit flip away from one of those in $\mathcal{C}$.
   $\implies$ at least on player speaks when $s \notin C$ and his guess is right.

Can we find a set C to use in the same way for n-bit strings?

The Hat Game with $n = 2^m - 1$ Players

An optimal strategy based on a length-n Hamming code

- Players treat a hat color configuration as a vector in $\mathbb{F}_2^n$:
$$(x_1, \dots, x_n) \in \mathbb{F}_2^n.$$
Each player gets his coordinate number.
- Each player checks if there is a unique bit value at his coordinate that would make the full vector a codeword.
- If yes, he guesses the opposite value. If no, he passes.

To prove this claim, we observe that Hamming codes are perfect and use some covering arguments.

$$P_{win} = \frac{n}{n+1}$$

An All or Nothing Game

A two-step modified game:

- In the first step, the players play the original game.
- In the second step, the players win only when each guesses correctly.

The players win only if they win the second round.

Q: Is it better to play the modified or the original game?
A: The modified because the first round reveals the cosset $\implies P_{win} = 1$

Consider the standard array for the $[7, 4]$ Hamming code:

0000000	0000000	0001111	0110011	0111100	1010101	1011010	1100110	1101001	$\cdots$
1000000	1000000	1001111	1110011	1111100	0010101	0011010	0100110	0101001	$\cdots$
0100000	0100000	0101111	0010011	0011100	1110101	1111010	1000110	1001001	$\cdots$
0010000	0010000	0011111	0100011	0101100	1000101	1001010	1110110	1111001	$\cdots$
0001000	0001000	0000111	0111011	0110100	1011101	1010010	1101110	1100001	$\cdots$
0000100	0000100	0001011	0110111	0111000	1010001	1011110	1100010	1101101	$\cdots$
0000010	0000010	0001101	0110001	0111110	1010111	1011000	1100100	1101011	$\cdots$
0000001	0000001	0001110	0110010	0111101	1010100	1011011	1100111	1101000	$\cdots$

Some Hat Color Guessing Game Observations

Participants and Rules

- There is a challenger and cooperating players.
- The challenger
  - chooses a math object at random
  - reveals some information about the choice to each player s.t. the players jointly have all information
- The players
  - cannot communicate once the game begins
  - can devise a strategy before the game starts

The Optimal Strategy and Revealed Information

- No strategy can change individual guessing rates.
- The color configuration becomes known to everyone.

The optimal strategy correlates individual guesses.

QM foundations & non-local games?

What do we need to know to play quantum games?

How is quantum information **represented**

How is quantum information **processed**

How is classical information **extracted**

How is Quantum information represented?

Classical computers store and operate on **bits**. What about quantum?

What is a Qubit?

A qubit is a quantum computing/information counterpart to a bit.
Physically, a qubit is a two-level quantum system.
Mathematically, a qubit is a unit-norm column vector in $\mathbb{C}^2$.


$|\psi\rangle$ is Dirac's notation that indicates a column vector.

$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |0\rangle = \left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right] \;\; \& \;\; |1\rangle = \left[\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right], \quad \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$

$\langle\psi|$ is the Hermitian transpose of $|\psi\rangle$.

How are multiple qubits represented?

An n–qubit state $|\phi\rangle$ is a unit-norm vector in $\mathbb{C}^{\otimes n}$:

$$|\phi\rangle = \sum_{i_j \in \{0,1\}} \alpha_{i_0 i_1 \ldots i_{n-1}} |i_0 i_1 \ldots i_{n-1}\rangle, \quad \sum_{i_j \in \{0,1\}} |\alpha_{i_0 i_1 \ldots i_{n-1}}|^2 = 1$$

$|i_0 i_1 \ldots i_{n-1}\rangle$ is a shorthand notation for $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle$, a basis vector of $\mathbb{C}^{\otimes n}$ labeled by $i_0 i_1 \ldots i_{n-1} \in \mathbb{F}_2^n$.

 $(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$

In general, an n-qubit state is **any** unit-norm vector in $\mathbb{C}^{2^n}$, and thus it cannot always be expressed as a product of single qubit states.

How is quantum information processed?

Quantum Gates:

Action on an n-qubit state is described by a $2^n \times 2^n$ **unitary matrix** U.

U can be a Kronecker product of matrices of smaller dimensions, or not.

- For $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, we have

$$U |\psi\rangle = \alpha U |0\rangle + \beta U |1\rangle .$$

  Thus, we often describe U by its action on the basis vectors $|0\rangle$ & $|1\rangle$.

- When $U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1}$, then its action on the basis vector $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle \in \mathcal{H}_{2^n}$ is, by the mixed-product property,

$$U |i_0 i_1 \ldots i_{n-1}\rangle = \boxed{U_0|i_0\rangle} \otimes \boxed{U_1|i_1\rangle} \otimes \cdots \otimes \boxed{U_{n-1}|i_{n-1}\rangle}$$

  We say that U_j <u>acts locally</u> on $|i_j\rangle$.

Are there some standard gates?

The Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|0\rangle \; -\boxed{H}- \; (|0\rangle + |1\rangle)/\sqrt{2} = |+\rangle$$

$$|1\rangle \; -\boxed{H}- \; (|0\rangle - |1\rangle)/\sqrt{2} = |-\rangle$$

The Identity and the Pauli Matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad |0\rangle \; -\boxed{I}- \; |0\rangle \qquad |1\rangle \; -\boxed{I}- \; |1\rangle$$

$$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad |0\rangle \; -\boxed{Y}- \; i\,|1\rangle \qquad |1\rangle \; -\boxed{Y}- \; -i\,|0\rangle$$

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad |0\rangle \; -\boxed{X}- \; |1\rangle \qquad |1\rangle \; -\boxed{X}- \; |0\rangle$$

$$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad |0\rangle \; -\boxed{Z}- \; |0\rangle \qquad |1\rangle \; -\boxed{Z}- \; -|1\rangle$$

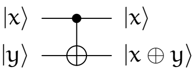
σ_X is often referred to as `NOT` or a bit-flip gate.

How about 2-qubit gates?

The two-qubit quantum gate known as XOR or CNOT:

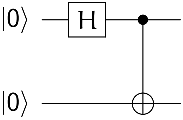
$\mathtt{CNOT} : |x, y\rangle \rightarrow |x, x \oplus y\rangle$

$x, y \in \{0, 1\}$



$$U_{\mathtt{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

We use the Hadamard and the CNOT gates to create entanglement:

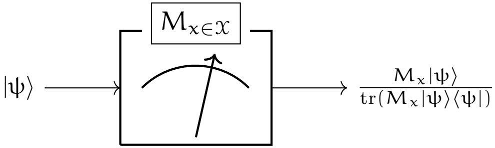


$$\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

How is classical information extracted?

We use measurements defined by a set of matrices $\{M_x\}_{x \in \mathcal{X}}$ that are

1. projectors (Hermitian and idempotent): $M_x = M_x^\dagger$ & $M_i^2 = M_x$,
2. pairwise orthogonal: $M_x M_y = \delta_{xy} M_x$
3. form a resolution of the identity: $\sum_{x \in \mathcal{X}} M_x = I$.



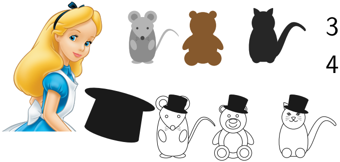
When measuring state $|\psi\rangle$:

- the only possible results are $x \in \mathcal{X}$
- result x occurs with probability $\mathrm{tr}\big(M_x|\psi\rangle\langle\psi|\big)$
- if we get result x, the output state is $\frac{M|\psi\rangle}{\mathrm{tr}(M_x|\psi\rangle\langle\psi|)}$

A High Level View of the Coset Guessing Game

ALICE

1) Randomly draws 3 math objects to prepare a multi-qubit state.



2) Transforms the state as Bob & Charlie request.

3) Sends half the qubits to Bob & half to Charlie.

4) Reveals objects $\#1$ to Bob and Charlie. 

BOB & CHARLIE

win if Bob identifies object $\#2$ and Charlie identifies object $\#3$.

Alice's Quantum State Preparation Recipe

The ingredients:

- $W \subseteq \mathbb{F}_2^n$ is a k-dimensional subspace of $\mathbb{F}_2^n$
- $G(n,k)$ is the set of all subspaces $W \subseteq \mathbb{F}_2^n$ of dimension k.
- $|W\rangle = \frac{1}{\sqrt{2^k}} \sum_{u \in W} |u\rangle$ is known as the subspace state.

Alice does the following:

1. Chooses $W \in G(2n, n)$, $x \in \mathbb{F}_2^{2n}$, and $z \in \mathbb{F}_2^{2n}$ uniformly at random.
2. Prepares the corresponding $2n$-qubit **coset state**:

$$|W_{x,z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{u \in W} (-1)^{z \cdot u} |x + u\rangle .$$

3. Sends the first n qubits of $|W_{x,z}\rangle$ to Bob and the rest to Charlie.
   (Bob & Charlie can request qubits from $\Phi(|W_{x,z}\rangle)$ but not in this talk.)
4. Reveals her choice of $|W\rangle$.

Alice's Coset States for $n = 1$

There are three one-dimensional subspaces of $\mathbb{F}_2^2 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$:

$$W^{(1)} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \quad W^{(2)} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\} \quad W^{(3)} = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$$

There are four coset states for each of these sub spaces:

$$\begin{array}{lll}
\left|W^{(1)}_{00,00}\right\rangle = |0\rangle \otimes |+\rangle & \left|W^{(2)}_{00,00}\right\rangle = |+\rangle \otimes |0\rangle & \left|W^{(3)}_{00,00}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\
\left|W^{(1)}_{00,01}\right\rangle = |0\rangle \otimes |-\rangle & \left|W^{(2)}_{00,10}\right\rangle = |-\rangle \otimes |0\rangle & \left|W^{(3)}_{00,01}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \\
\left|W^{(1)}_{10,00}\right\rangle = |1\rangle \otimes |+\rangle & \left|W^{(2)}_{01,00}\right\rangle = |+\rangle \otimes |1\rangle & \left|W^{(3)}_{10,00}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \\
\left|W^{(1)}_{10,01}\right\rangle = |1\rangle \otimes |-\rangle & \left|W^{(2)}_{01,10}\right\rangle = |-\rangle \otimes |1\rangle & \left|W^{(3)}_{10,01}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)
\end{array}$$

NB: If we know the subspace $W^{(i)}$ and have both qubits, we can identify the coset state by measuring the qubits the basis corresponding to $W^{(i)}$.

However, Bob and Charlie have one qubit each.

Subspace & Coset States $\Longrightarrow$

1995–96: CSS quantum codes
Calderbank–Shor; Steane
Quantum codewords as superpositions

$\downarrow$

1990s–2000s: Hidden Subgroup Problem
Ettinger–Høyer–Knill and others
Coset states as carriers of hidden algebraic information

$\downarrow$

2012: Hidden-subspace quantum money
Aaronson–Christiano
Subspace states $|A\rangle = \frac{1}{\sqrt{|A|}} \sum_{a \in A} |a\rangle$ as cryptographic objects

$\downarrow$

2013: BB84 monogamy-of-entanglement games
Tomamichel–Fehr–Kaniewski–Wehner
Guessing complementary quantum measurement outcomes

$\downarrow$

2021: Hidden cosets and unclonable cryptography
Coladangelo–J. Liu–Q. Liu–Zhandry
Coset states $|A_{s,s'}\rangle = X^s Z^{s'} |A\rangle$ & the strong coset monogamy game

$\downarrow$

2021–22: Subspace-coset monogamy
Culf–Vidick
Proof of exponentially small simultaneous guessing probability

$\downarrow$

2022–23: Group coset monogamy games
Culf–Vidick–Albert
Extension to general groups and connections with CSS/GKP codes

$\downarrow$

2024: Optimal coset-guessing strategies
Schleppy–Soljanin–Swanson
Tight winning probability & explicit coding-based optimal strategy

$\downarrow$

2025–26: General (n, k) coset guessing
Schleppy–Soljanin
Winning rates as a function of subspace dimension/rate

Bob's & Charlie's Game

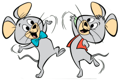
They play jointly but can talk only before the game starts.

Bob and Charlie

- get n qubits each of the $2n$-qubit coset state $|W_{x,z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{u \in W} (-1)^{z \cdot u} |x + u\rangle$.
- get the identity of W, e.g., Alice broadcasts a basis of W.
- can perform measurements (W-dependent) on their respective qubits

Bob guesses x based on his measurement result.

Chrlie guesses z based on his measurement result.



They win if each guesses correctly.

How does the winning probability p_{win} scale with n?

Cooking (up) Analogies

$$|W_{x,z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{u \in W} (-1)^{z \cdot u} |x + u\rangle.$$

Prior Results and Our Contributions

$p_{\text{win}} \to 0$ as $n \to \infty$

conjectured by Coladangelo, Liu, Liu, and Zhandry in 2021

proved by Culf and Vidick in 2022 with

- no claim to the derived probability-bound optimality
- techniques involving general operator inequalities by Tomamichel, Fehr, Kaniewski and Wehner, in 2013

This talk

- derives an **upper bound** on p_{win}
- shows how Bob & Charlie **can achieve** the bound asymptotically
- as a byproduct, derives a **circuit** to map $|0\rangle^{\otimes n}$ into

  $$|W_{x,z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{u \in W} (-1)^{z \cdot u} |x + u\rangle$$

  that uses only CNOTs and single-qubit gates.

Bob's and Charlie's Measurements

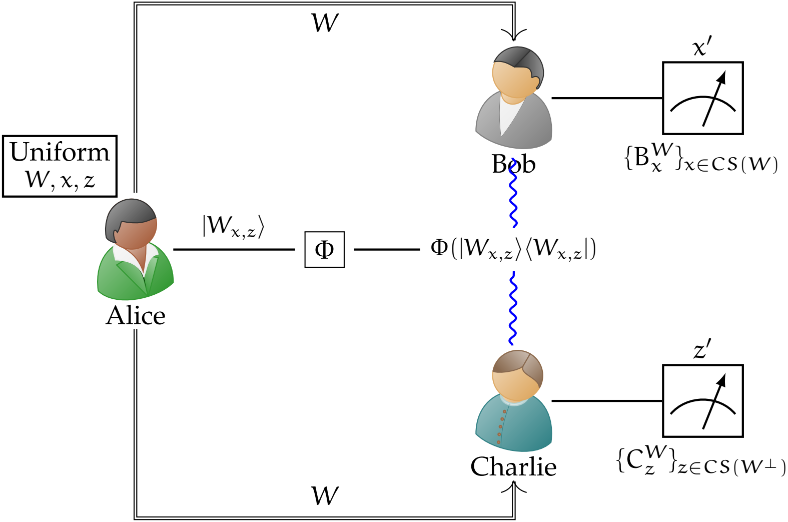
Bob and Charlie

- get n qubits each of the $2n$-qubit coset state $|W_{x,z}\rangle = \frac{1}{\sqrt{2^n}} \sum_{u \in W} (-1)^{z \cdot u} |x+u\rangle$.
- get the identity of W, e.g., Alice broadcasts a basis of W.
- can perform measurements (W-dependent) on their respective qubits

Some observations & notation:

- $x + x' \in W$ & $z + z' \in W^{\perp} \implies W_{x,z} = W_{x',z'}$.
  (x, x' are in the same coset of W and z, z' are in the same coset of $W^{\perp}$.)
- $CS(V)$ denotes a set of coset representatives of a subspace $V \subset \mathbb{F}_2^n$.
- $\{B_x^W\}_{x \in CS(W)}$ is Bob's & $\{C_z^W\}_{z \in CS(W^{\perp})}$ is Charlie's POVM for W.
- Given W, x, z, Bob's guesses $\hat{x}$ and Charlie's guesses $\hat{z}$ wp
  $$p(\hat{x}, \hat{z}|W, x, z) = \mathrm{Tr}\left[(B_{\hat{x}}^W \otimes C_{\hat{z}}^W) |W_{x,z}\rangle \langle W_{x,z}|\right]$$

A Coset Guessing Game Diagram



Bob&Charlie's Winning Probability

Given W, x, z, Bob's guesses $\hat{x}$ and Charlie's guesses $\hat{z}$ wp

$$p(\hat{x}, \hat{z}|W, x, z) = \mathrm{Tr}\left[(B^W_{\hat{x}} \otimes C^W_{\hat{z}}) |W_{x,z}\rangle \langle W_{x,z}|\right]$$

$\Longrightarrow$

Bob and Charlie win wp $p_{\text{win}}(W) = \sum_{x,z} p(x,z) p(x,z|W,x,z)$

Bound the joint probability by a marginal!

We will explain how Bob & Charlie can play to ensure such correlations.

Theorem – An achievable bound on the winning probability:

$$p_{\text{win}} \overset{\dagger}{\leqslant} \frac{1}{\binom{2n}{n}_2} \sum_{k=0}^{n} 2^{k^2} \binom{n}{k}_2^2 \left(\frac{1}{2}\right)^k \overset{*}{\doteq} \Theta\left(\frac{1}{2^n}\right)$$

† follows from, some operators (in)equalities, and subspace counting.
∗ follows from some (Gaussian) binomial (in)equalities .

How can we achieve the bound?

Ideas Under a CSS-Coding Lens

CSS(C_1, C_2) **with** $C_1 = \mathbb{F}_2^n$ **&** $C_2 = W$ **would**

1. see $|W\rangle$ as the image of $|0\rangle^{\otimes n}$
2. see coset states as error states: $|W_{x,z}\rangle = X_{\mathsf{Supp}(x)} Z_{\mathsf{Supp}(z)} |W\rangle$
3. pick minimum-weight coset representatives x & z for decoding

We will jointly

1. devise an encoding circuit N to map $|0\rangle^{\otimes n}$ into $|W\rangle$:
   $|W\rangle = N \cdot |0\rangle^{\otimes n}$
2. pick coset representatives x & z such that
   a) $\mathsf{Supp}(x) \cap \mathsf{Supp}(z) = \emptyset$
   b) $|W_{x,z}\rangle = X_{\mathsf{Supp}(x)} Z_{\mathsf{Supp}(z)} \cdot N \cdot |0\rangle^{\otimes n} = N\,|x + z\rangle$

Encoding Circuits for Subspace States

We can map $|0\rangle^{\otimes n}$ into subspace states by two and one qubit gates.

Lemma: A circuit for $|\mathrm{Span}(v_i)\rangle$

Consider $v_i \in \mathbb{F}_2^n$ with the support S_i and the leftmost 1 at index i. Then

$$\frac{1}{\sqrt{2}}\left(|0\rangle + |v_i\rangle\right) = \mathrm{CNOT}_{i,B_i}\, H_i \cdot |0\rangle^{\otimes n}.$$

- H_i denotes a Hadamard gate on the i-th qubit
- CNOT_{i,B_i} denotes a composition of CNOT gates which have i as the control qubit and the target qubits indices range over $B_i \coloneqq S_i \setminus \{i\}$.

Moreover, given vector $v_j \in \mathbb{F}_2^n$ s.t. $j \neq S_i$ & $i \neq S_i$ we can obtain $|\mathrm{Span}(v_i, v_j)\rangle$ by applying only CNOT and H gates to $|0\rangle^{\otimes n}$:

$$|0\rangle^{\otimes n} \overset{\mathrm{CNOT}_{i,B_i}\, H_i}{\mapsto} \frac{1}{\sqrt{2}}\left(|0\rangle + |v_i\rangle\right) \overset{\mathrm{CNOT}_{j,B_j}\, H_j}{\mapsto} \frac{1}{2}\left(|0\rangle + |v_j\rangle + |v_i\rangle + |v_i + v_j\rangle\right)$$

Subspace States Encoding & Cosset Representatives

Theorem – Mapping $|0\rangle^{\otimes n}$ into $|W\rangle$:

Consider $W \subset \mathbb{F}_2^n$ & its generator matrix A in reduced row echelon form. Let I denote the pivot column indices & $\mathrm{J} = \{(\mathrm{i},\mathrm{j}) : \mathrm{i} \in \mathrm{I}, \mathrm{j} \in \mathrm{I}^c, A_{\mathrm{ij}} = 1\}$. Then

$$|W\rangle = \mathrm{CNOT}_\mathrm{J}\, \mathrm{H}_\mathrm{I}\, |0\rangle^{\otimes n}$$

Proof: The form of A allows us to use the lemmas.

Moreover,
$\langle e_i \rangle_{i \in I^c}$ is a W-cosets transversal & $\langle e_i \rangle_{i \in I}$ is a $W^\perp$-cosets transversal.

The supports of coset representatives of W and $W^\perp$ are disjoint.

Selecting Coset Representatives –  An Example

CF. coset leaders

Consider a $[5, 2]$ code generator matrix:

$$A_{\mathtt{win}} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

A standard array for this code is

00000	01101	10110	11011
10000	11101	00110	01011
01000	00101	11110	10011
00100	01001	10010	11111
00010	01111	10100	11001
00001	01100	10111	11010
11000	10101	01110	00011
10001	11100	00111	01010

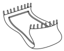
Bob's $CS(W)$ will use the highlighted strings as coset representatives.

A Representation of Coset States

Theorem – Mapping $|0\rangle^{\otimes n}$ into $|W\rangle$:

Consider $W \subset \mathbb{F}_2^n$ & its generator matrix A in reduced row echelon form. Let I denote the pivot column indices & $\mathrm{J} = \{(i,j) : i \in \mathrm{I}, j \in \mathrm{I}^c, A_{ij} = 1\}$, $\langle e_i \rangle_{i \in \mathrm{I}^c}$ be W-coset representatives & $\langle e_i \rangle_{i \in \mathrm{I}}$ $W^{\perp}$-coset representatives. Then

$$|W_{x,z}\rangle = \mathsf{CNOT}_{\mathrm{J}}\, \mathrm{H}_{\mathrm{I}}\, |x + z\rangle$$

Proof:  

We use the following relations:

1. $|W_{x,z}\rangle = \mathrm{X}_{\mathsf{Supp}(x)} \mathrm{Z}_{\mathsf{Supp}(z)} |W\rangle = \mathrm{X}_{\mathsf{Supp}(x)} \mathrm{Z}_{\mathsf{Supp}(z)}\, \mathsf{CNOT}_{\mathrm{J}}\, \mathrm{H}_{\mathrm{I}}\, |0\rangle^{\otimes n}$
2. $(\mathrm{I} \otimes \mathrm{X})\, \mathsf{CNOT} = \mathsf{CNOT}(\mathrm{I} \otimes \mathrm{X})$ and $(\mathrm{Z} \otimes \mathrm{I})\, \mathsf{CNOT} = \mathsf{CNOT}(\mathrm{Z} \otimes \mathrm{I})$
   CNOT control bits are in $\mathsf{Supp}(CS(W^{\perp}))$, target bits are in $\mathsf{Supp}(CS(W))$
3. $\mathrm{ZH} = \mathrm{HX}$

$|W_{x,z}\rangle = \mathrm{CNOT}_J\, H_I\, |x+z\rangle$ & $\mathrm{Supp}(x) \cap \mathrm{Supp}(z) = \emptyset$ – Implications

Depending on J, there are two cases for CNOT gate inputs:

1. all CNOT gates operate <u>locally</u> on Bob's and Charlie's qubits.
2. some CNOT gates <u>straddle</u> Bob's and Charlie's qubits, which implies entanglement between Bob's and Charlie's qubits.

Case #1 – All CNOT gates are local:

$\Longrightarrow$ Bob and Charlie can/will locally invert all CNOT and H actions.

$\Longrightarrow$ Bob will have the first n qubits of $|x+z\rangle$, Charlie the second n.

$\Longrightarrow$ The rest of the game is classical.

A Classical Game and Correlations

- Each bit in $x + z$ is either an x or a z bit since $\mathrm{Supp}(x) \cap \mathrm{Supp}(z) = \emptyset$.
- Bob needs x and Charlie needs z bits but they are scrambled in $x + z$.

An Example:

$$x + z = \underbrace{z_1 z_2 x_3}_{\text{Bob's}} \quad \underbrace{x_4 x_5 z_6}_{\text{Charlie's}}.$$

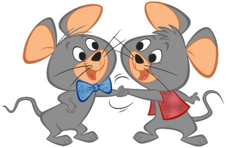
$\Longrightarrow$

Bob and Charlie can do little about their individual error rates,
BUT they can make them **entirely correlated**, as follows:

1. Bob reads off the x bits he has (those on his side in I)
   Charlie reads off the z bits he has (those on his side in I^c).
2. Bob assigns the values of z bits he has to the x bits he is missing.
   Charlie assigns the values of x bits he has to the z bits he is missing.

$\Longrightarrow$ Bob is right iff Charle is right.

The Epilogue



The shared quantum state only correlates individual guesses.

The optimal strategy

- turns the quantum correlations into the classical.
- does not improve the individual rates of correct guessing.