Group Coset Monogamy Games

and an Application to Device-Independent QKD

Eric Culf   Thomas Vidick   Victor V. Albert

arXiv2212.03935

QCRYPT 2023

College Park, Maryland
August 18th 2023

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

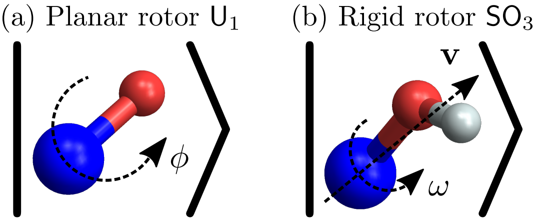
- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces

[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$

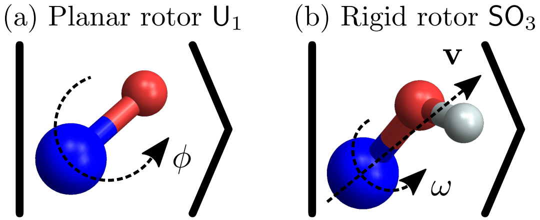
[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]



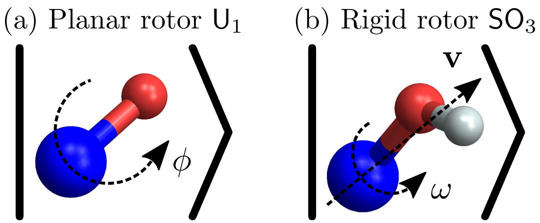
[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]
  - Optical modes: $G = \mathbb{R}^n$



[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]
  - Optical modes: $G = \mathbb{R}^n$



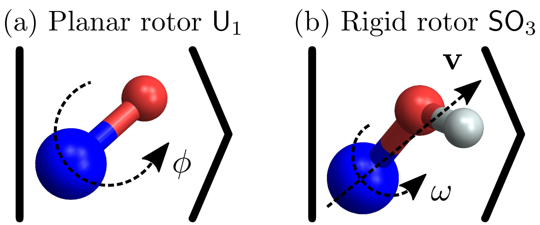
$$|\ H\ \rangle = \sqrt{\frac{1}{|H|}} \sum_{h \in H} |\ h\rangle$$

Subgroup $H \subseteq G$

[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

Coset States

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]
  - Optical modes: $G = \mathbb{R}^n$



Coset representative $g \in G$

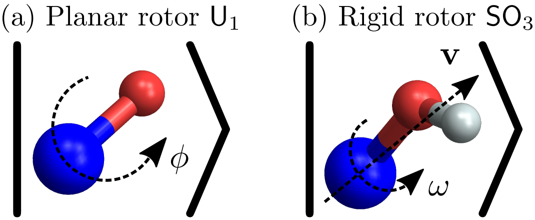
$$|gH\rangle = \sqrt{\frac{1}{|H|}} \sum_{h \in H} |gh\rangle$$

Subgroup $H \subseteq G$

[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

Coset States

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]
  - Optical modes: $G = \mathbb{R}^n$



Irreducible representation $\gamma : H \to \mathcal{U}(d_\gamma)$

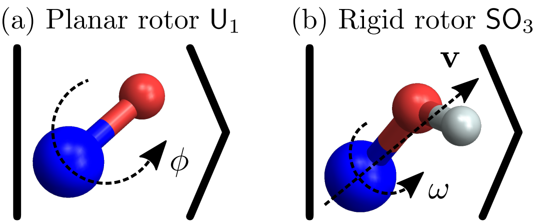
Coset representative $g \in G$

$$|gH^\gamma\rangle = \sqrt{\frac{1}{|H|}} \sum_{h \in H} \gamma(h) |gh\rangle$$

Subgroup $H \subseteq G$

[1] Albert, Covey, and Preskill, 2020, “Robust Encoding of a Qubit in a Molecule”.

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1 [1]
  - Optical modes: $G = \mathbb{R}^n$



Irreducible representation $\gamma : H \to \mathcal{U}(d_\gamma)$

Coset representative $g \in G$

$$|gH^\gamma_{m,n}\rangle = \sqrt{\frac{d_\gamma}{|H|}} \sum_{h \in H} \gamma_{m,n}(h) |gh\rangle$$

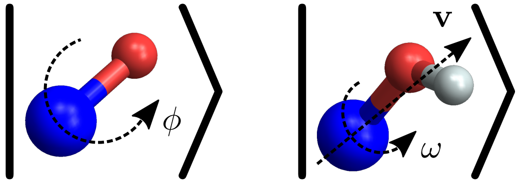
Subgroup $H \subseteq G$

Matrix indices $1 \leq m, n \leq d_\gamma$

[1] Albert, Covey, and Preskill, 2020, “Robust Encoding of a Qubit in a Molecule”.

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1[1]
  - Optical modes: $G = \mathbb{R}^n$

(a) Planar rotor U_1 (b) Rigid rotor SO_3



Irreducible representation $\gamma : H \to \mathcal{U}(d_\gamma)$

Coset representative $g \in G$

$$|gH^{\gamma}_{m,n}\rangle = \sqrt{\frac{d_\gamma}{|H|}} \sum_{h \in H} \gamma_{m,n}(h) |gh\rangle$$

Subgroup $H \subseteq G$

Matrix indices $1 \le m, n \le d_\gamma$

For each H, $|gH^{\gamma}_{m,n}\rangle$ forms orthonormal basis over $(gH, \gamma_{m,n}) \in G/H \times \hat{H}$

[1] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".

Various error-correcting codes have coset states as code and error words

[2] Calderbank and Shor, 1996, “Good quantum error-correcting codes exist”.
[3] Gottesman, Kitaev, and Preskill, 2001, “Encoding a qubit in an oscillator”.
[4] Albert, Covey, and Preskill, 2020, “Robust Encoding of a Qubit in a Molecule”.
[5] Braunstein, 1998, “Quantum error correction for communication with linear optics”.

Various error-correcting codes have coset states as code and error words

Code	G	$H \cong$

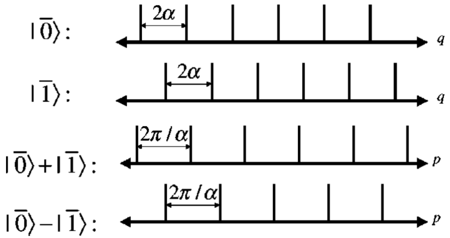
[2] Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5] Braunstein, 1998, "Quantum error correction for communication with linear optics".

Various error-correcting codes have coset states as code and error words

Code	G	$H \cong$
CSS[2]	$\mathbb{Z}_2^n$	$\mathbb{Z}_2^k$

[2] Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5] Braunstein, 1998, "Quantum error correction for communication with linear optics".

Various error-correcting codes have coset states as code and error words

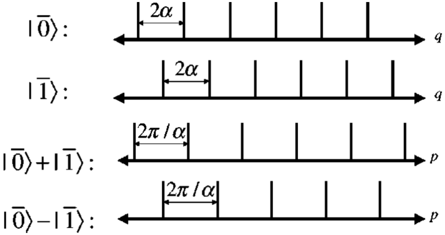


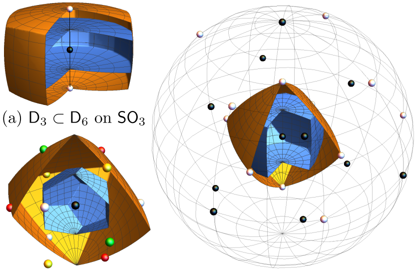
Code	G	$H \cong$
CSS[2]	$\mathbb{Z}_2^n$	$\mathbb{Z}_2^k$
GKP[3]	$\mathbb{R}$	$\mathbb{Z}$

[2] Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5] Braunstein, 1998, "Quantum error correction for communication with linear optics".

Various error-correcting codes have coset states as code and error words

Code	G	$H \cong$
CSS[2]	$\mathbb{Z}_2^n$	$\mathbb{Z}_2^k$
GKP[3]	$\mathbb{R}$	$\mathbb{Z}$
Molecular[4]	SO_3	point group





(a) $D_3 \subset D_6$ on SO_3

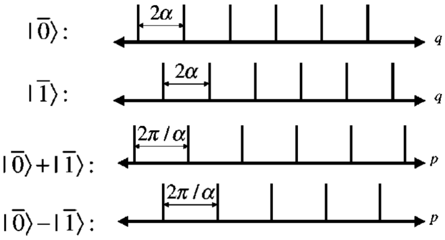
(c) $T \subset I$ on SO_3

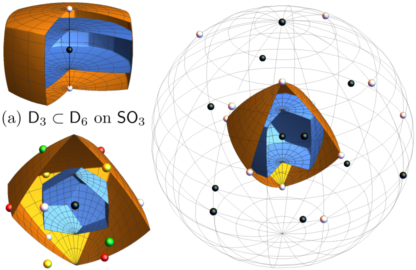
(b) $T \subset O$ on SO_3

[2] Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5] Braunstein, 1998, "Quantum error correction for communication with linear optics".

Various error-correcting codes have coset states as code and error words

Code	G	$H \cong$
CSS[2]	$\mathbb{Z}_2^n$	$\mathbb{Z}_2^k$
GKP[3]	$\mathbb{R}$	$\mathbb{Z}$
Molecular[4]	SO_3	point group
Analog CSS[5]	$\mathbb{R}^n$	$\mathbb{R}^k$





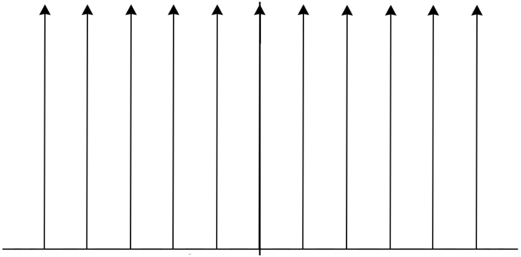
(a) $D_3 \subset D_6$ on SO_3

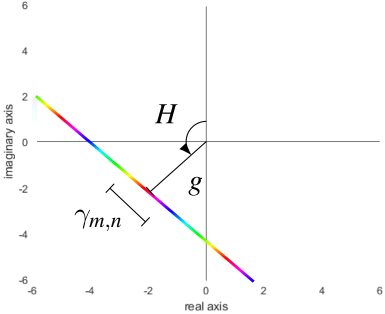
(c) $T \subset I$ on SO_3

(b) $T \subset O$ on SO_3

[2]Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3]Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4]Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5]Braunstein, 1998, "Quantum error correction for communication with linear optics".

- Coset states $|gH_{m,n}^{\gamma}\rangle$ are well-defined only for finite groups

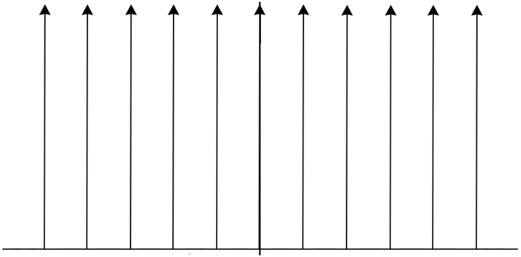




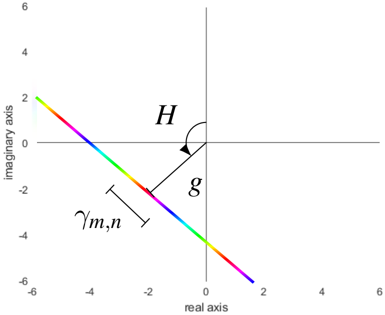
[6] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".

Coset States for Infinite Groups

- Coset states $|gH^{\gamma}_{m,n}\rangle$ are well-defined only for finite groups
- Definition can be modified for groups with 'nice' representation theory
  - **Compact:** Peter-Weyl theorem
  - **Abelian**: Fourier transform

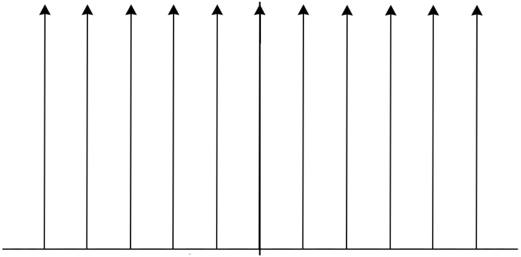


6

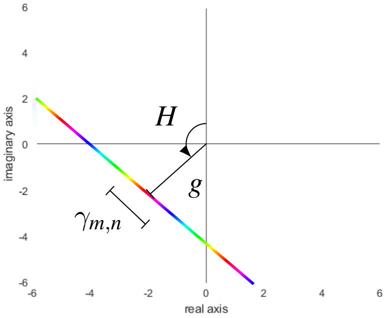


[6] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".

- Coset states $|gH^{\gamma}_{m,n}\rangle$ are well-defined only for finite groups
- Definition can be modified for groups with 'nice' representation theory
  - **Compact:** Peter-Weyl theorem
  - **Abelian**: Fourier transform
- Sums $\sum_{h\in H}$ become Haar integrals $\int_H d_H h$

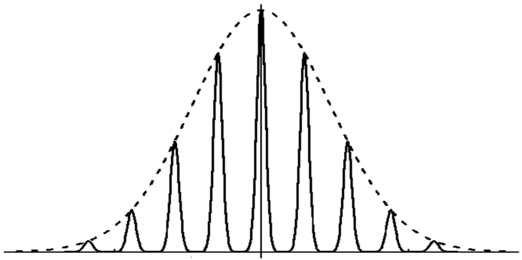


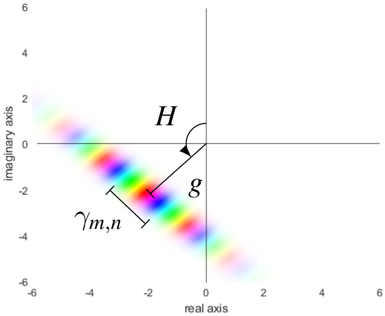
[6]



[6] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".

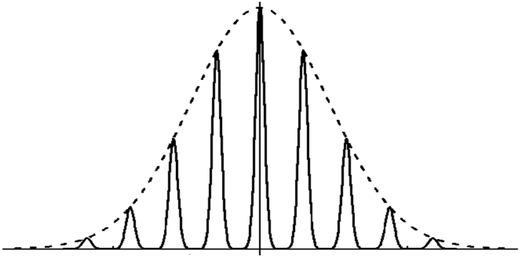
- Coset states $|gH_{m,n}^{\gamma}\rangle$ are well-defined only for finite groups
- Definition can be modified for groups with ‘nice’ representation theory
  - **Compact:** Peter-Weyl theorem
  - **Abelian**: Fourier transform
- Sums $\sum_{h\in H}$ become Haar integrals $\int_H d_H h$
- We need to replace Dirac deltas with Gaussians (damping)

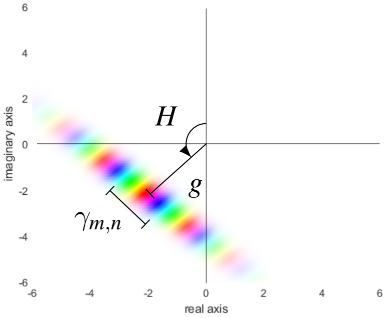

[6]



[6] Gottesman, Kitaev, and Preskill, 2001, “Encoding a qubit in an oscillator”.

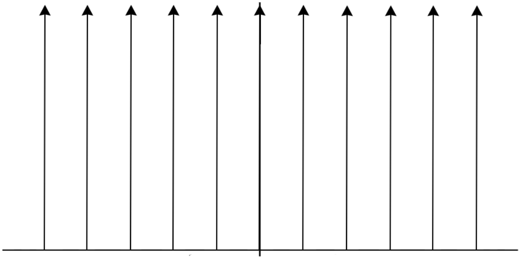
- Coset states $|gH^{\gamma}_{m,n}\rangle$ are well-defined only for finite groups
- Definition can be modified for groups with 'nice' representation theory
  - **Compact:** Peter-Weyl theorem
  - **Abelian**: Fourier transform
- Sums $\sum_{h\in H}$ become Haar integrals $\int_H d_H h$
- We need to replace Dirac deltas with Gaussians (damping)
- Preserves states but harder to work with rigorously

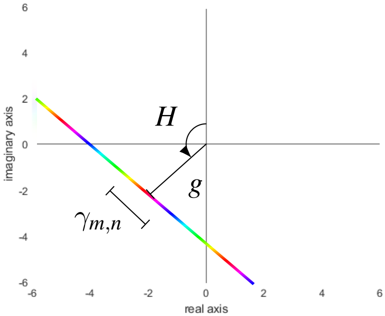

[6]



[6] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".

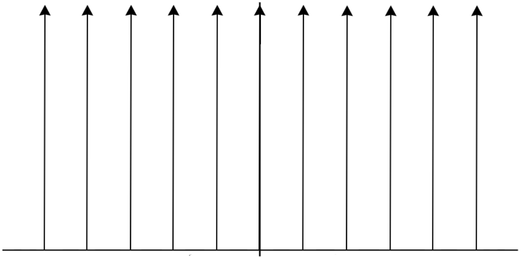
- Alternate approach: Generalise only measurement

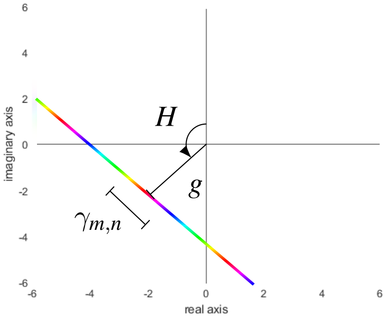




- Alternate approach: Generalise only measurement
- Measurement in basis of coset states becomes operator-valued measure

$$A^H : \mathscr{B}(G/H \times \hat{H}) \to \mathcal{B}(L^2(G)) \quad \text{satisfying} \quad \mathrm{Tr}(A^H(E)\rho) = \Pr[(gH, \gamma_{m,n}) \in E]$$

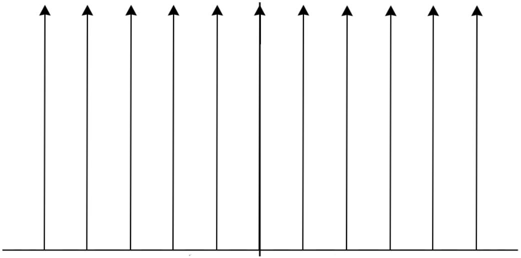


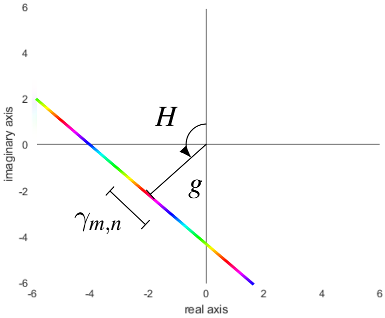


- Alternate approach: Generalise only measurement
- Measurement in basis of coset states becomes operator-valued measure

$$A^H : \mathscr{B}(G/H \times \hat{H}) \to \mathcal{B}(L^2(G)) \quad \text{satisfying} \quad \mathrm{Tr}(A^H(E)\rho) = \Pr[(gH, \gamma_{m,n}) \in E]$$

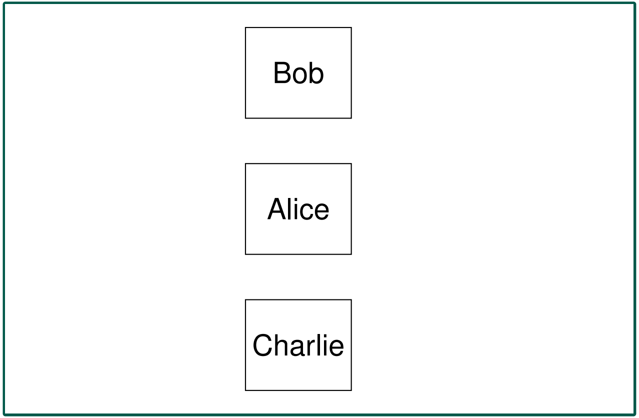
- Intuitively $A^H(E) = \int_E |gH^{\gamma}_{m,n}\rangle\langle gH^{\gamma}_{m,n}|\, d(gH, \gamma_{m,n})$





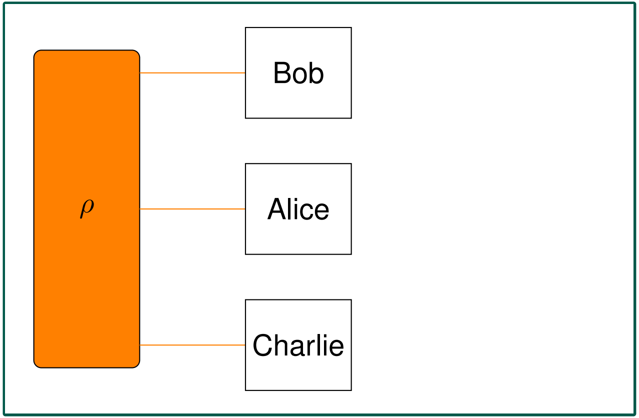
Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

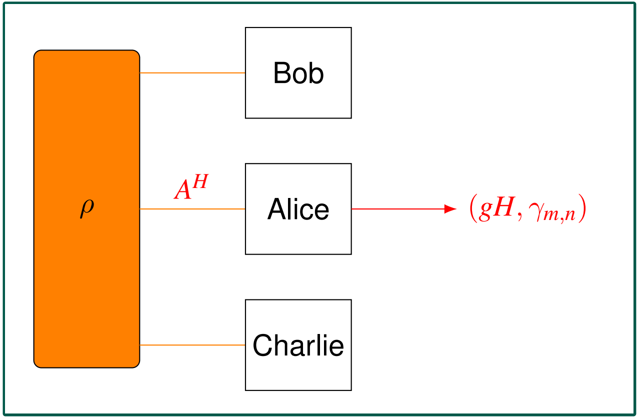
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, “Hidden Cosets and Applications to Unclonable Cryptography”.



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state

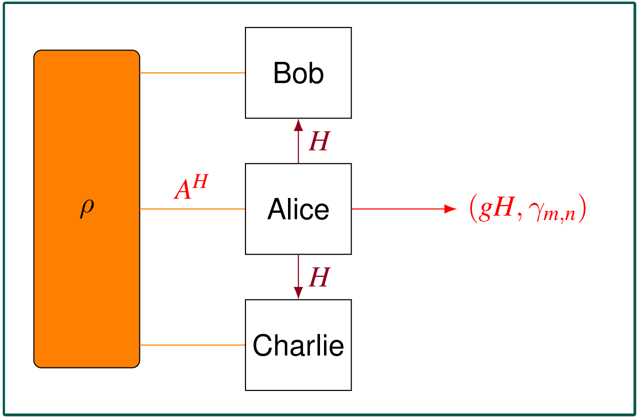
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H

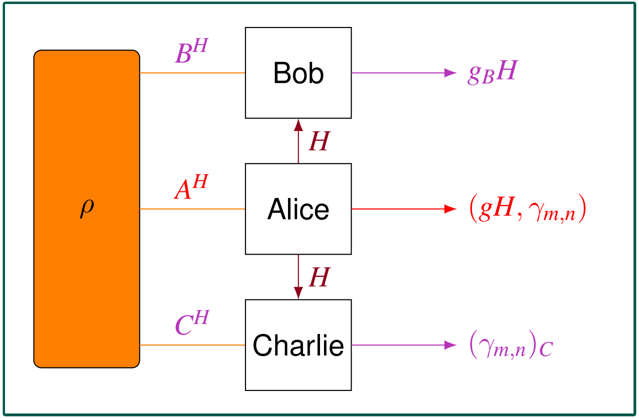
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, “Hidden Cosets and Applications to Unclonable Cryptography”.



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H
3. Alice sends H to Bob and Charlie.

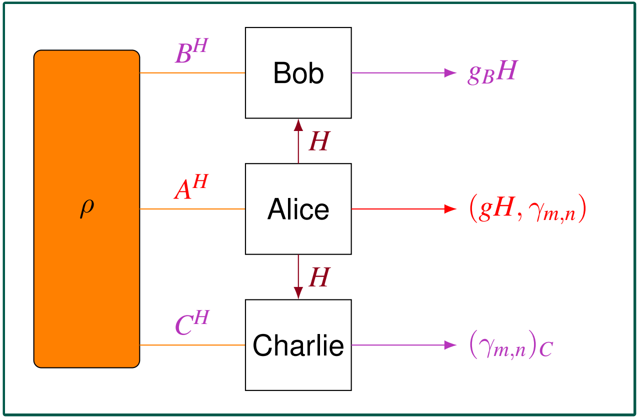
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H
3. Alice sends H to Bob and Charlie.
4. Bob guesses gH, Charlie guesses $\gamma_{m,n}$

[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".

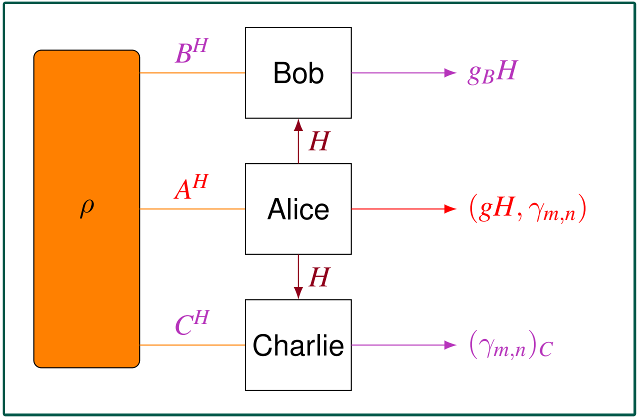


Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H
3. Alice sends H to Bob and Charlie.
4. Bob guesses gH, Charlie guesses $\gamma_{m,n}$
5. Bob and Charlie win if guesses are up to allowed errors E, F

[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".

Monogamy-of-Entanglement Games from Coset States



Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

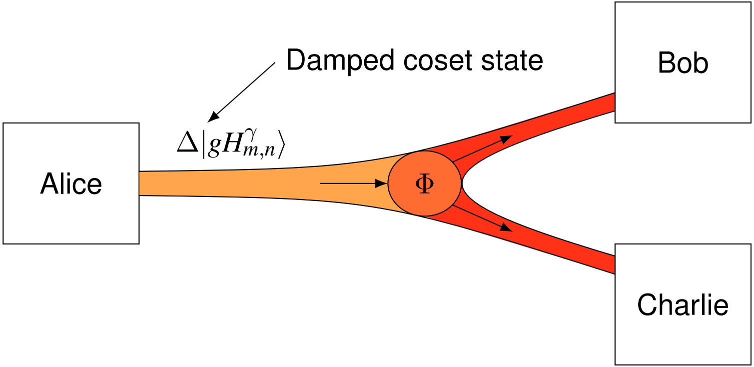
1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H
3. Alice sends H to Bob and Charlie.
4. Bob guesses gH, Charlie guesses $\gamma_{m,n}$
5. Bob and Charlie win if guesses are up to allowed errors E, F

Theorem

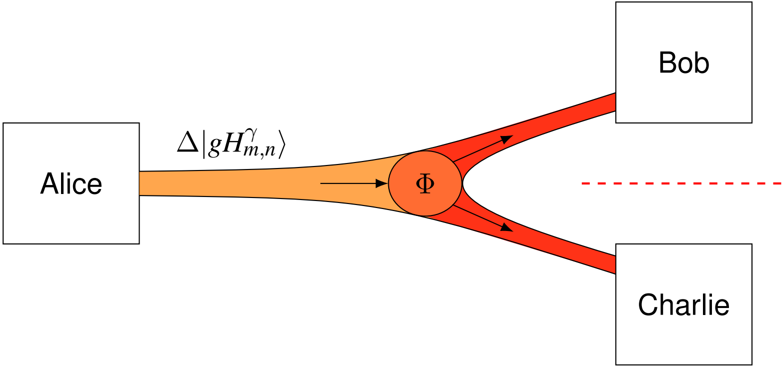
$$\mathfrak{w}_{\mathsf{G}}(\mathsf{S}) \leq \mathop{\mathbb{E}}_{i} \sup_{H \in \mathcal{S}, \gamma \in \mathrm{Irr}(H), g \in G} \sqrt{d_\gamma \mu_H(H \cap E g \pi_i(H)) \mu_{\hat{H}}(F)}$$

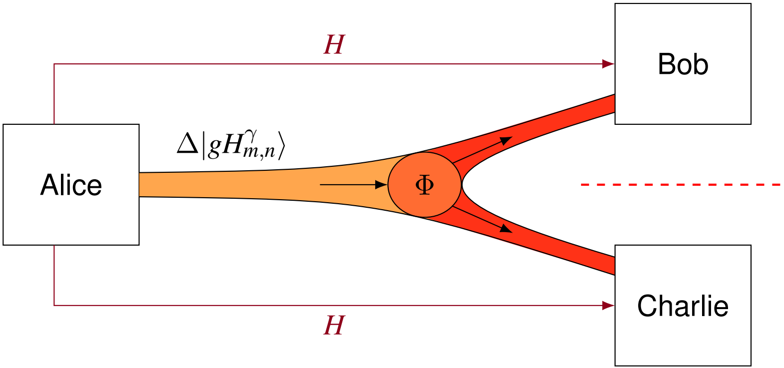
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, "Hidden Cosets and Applications to Unclonable Cryptography".

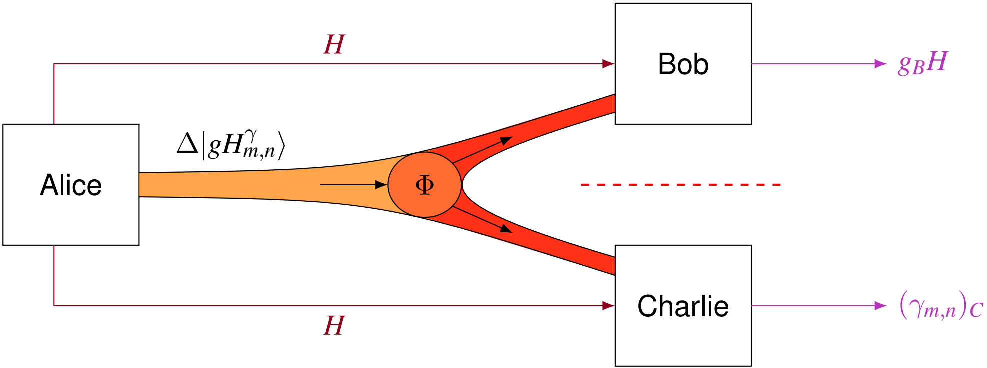
Prepare-and-Measure Version

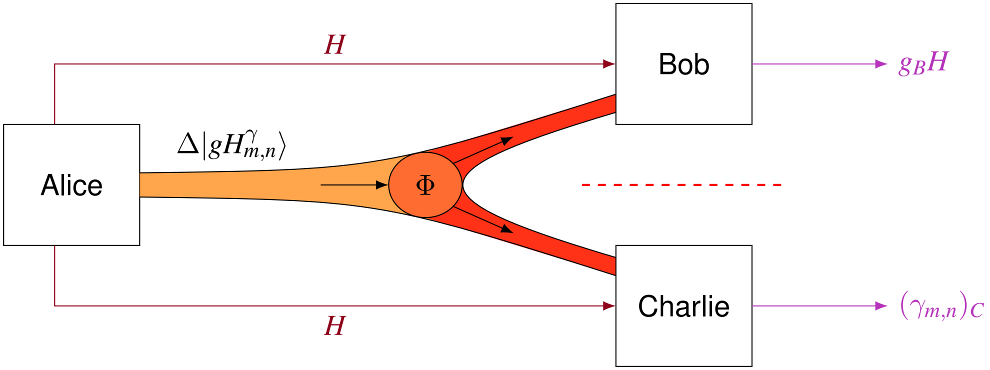

Damped coset state
Bob
Alice
$\Delta|gH^{\gamma}_{m,n}\rangle$
Φ
Charlie

Prepare-and-Measure Version



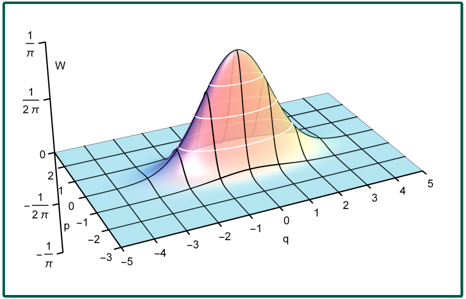

H
Bob
$\Delta|gH^{\gamma}_{m,n}\rangle$
Alice
Φ
Charlie
H


H
Bob
$g_B H$
Alice
$\Delta|gH^{\gamma}_{m,n}\rangle$
Φ
Charlie
$(\gamma_{m,n})_C$
H



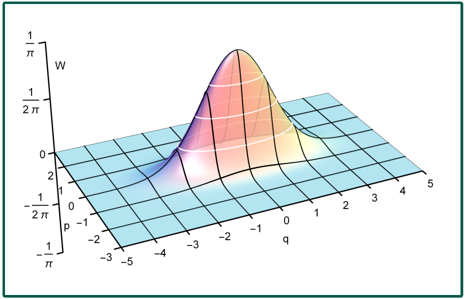
The same bound on the winning probability holds!

- Monogamy properties can be used to construct one-sided device-independent QKD[8]



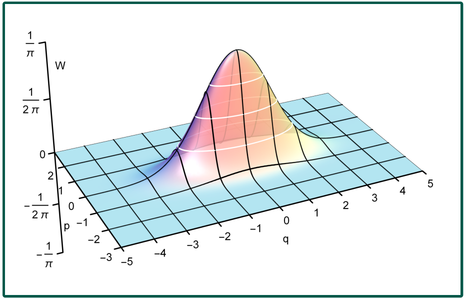
[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, “A monogamy-of-entanglement game with applications to device-independent quantum cryptography”.

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".

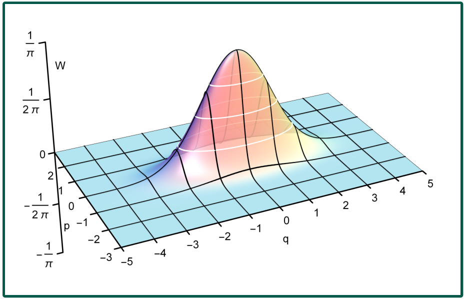
- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, “A monogamy-of-entanglement game with applications to device-independent quantum cryptography”.

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

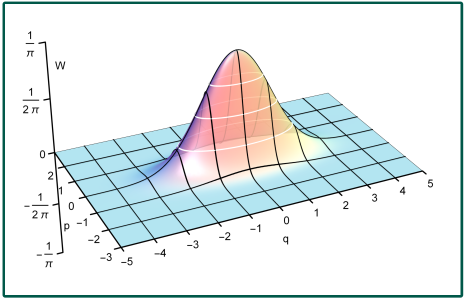
- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

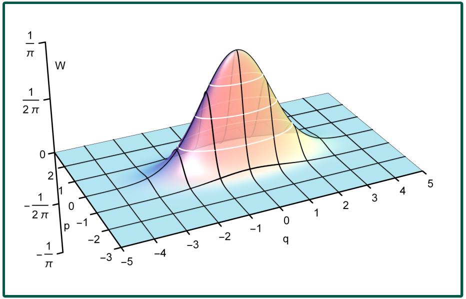
- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$
- We can identify $\mathbb{R}^n/P \cong P^\perp$, $\hat{P} \cong P$



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

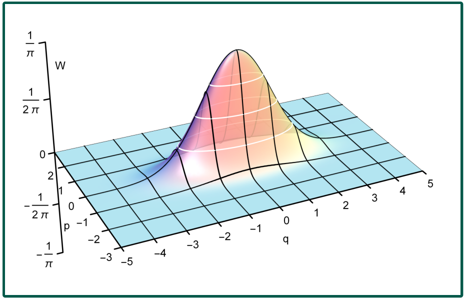
- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$
- We can identify $\mathbb{R}^n/P \cong P^\perp$, $\hat{P} \cong P$
- Intuitively, coset states are position/momentum eigenstates $|q + P^{\gamma_p}\rangle = \int_P e^{2\pi i p\cdot x}|x+q\rangle dx$.



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

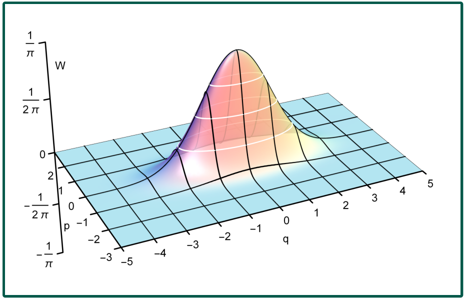
- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$
- We can identify $\mathbb{R}^n/P \cong P^\perp$, $\hat{P} \cong P$
- Intuitively, coset states are position/momentum eigenstates $|q + P^{\gamma_p}\rangle = \int_P e^{2\pi i p\cdot x}|x + q\rangle dx$.
- Measurement is homodyne detection



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$
- We can identify $\mathbb{R}^n / P \cong P^\perp$, $\hat{P} \cong P$
- Intuitively, coset states are position/momentum eigenstates $|q + P^{\gamma_p}\rangle = \int_P e^{2\pi i p \cdot x} |x + q\rangle dx$.
- Measurement is homodyne detection
- Damped coset states are squeezed states



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, “A monogamy-of-entanglement game with applications to device-independent quantum cryptography”.

Open Questions

- Is it possible to make the QKD protocol more practical?

Open Questions

- Is it possible to make the QKD protocol more practical?
- Can monogamy-of-entanglement be used to show DIQKD properties of coherent state protocols?

Group Coset Monogamy Games

and an Application to Device-Independent QKD

Eric Culf   Thomas Vidick   Victor V. Albert

arXiv2212.03935

QCRYPT 2023

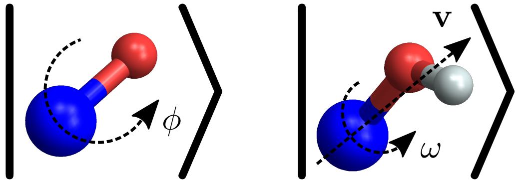
College Park, Maryland
August 18th 2023

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Coset States

- Group Hilbert spaces $L^2(G)$ often naturally represent quantum spaces
  - Qubits: $G = \mathbb{Z}_2^n$
  - Rotational symmetries: $G = \mathrm{SO}_3$ or U_1 [1]
  - Optical modes: $G = \mathbb{R}^n$

(a) Planar rotor U_1 (b) Rigid rotor SO_3



Irreducible representation $\gamma : H \to \mathcal{U}(d_\gamma)$

Coset representative $g \in G$

$$|gH^{\gamma}_{m,n}\rangle = \sqrt{\frac{d_\gamma}{|H|}} \sum_{h \in H} \gamma_{m,n}(h) |gh\rangle$$

Subgroup $H \subseteq G$

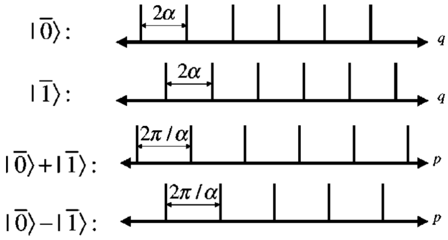
Matrix indices $1 \leq m, n \leq d_\gamma$

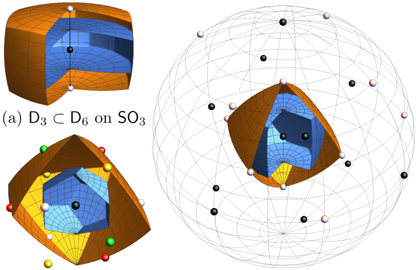
For each H, $|gH^{\gamma}_{m,n}\rangle$ forms orthonormal basis over $(gH, \gamma_{m,n}) \in G/H \times \hat{H}$

[1] Albert, Covey, and Preskill, 2020, “Robust Encoding of a Qubit in a Molecule”.

Various error-correcting codes have coset states as code and error words

Code	G	$H \cong$
CSS[2]	$\mathbb{Z}_2^n$	$\mathbb{Z}_2^k$
GKP[3]	$\mathbb{R}$	$\mathbb{Z}$
Molecular[4]	SO_3	point group
Analog CSS[5]	$\mathbb{R}^n$	$\mathbb{R}^k$





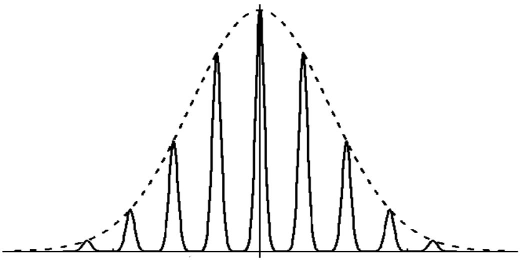
(a) $\mathrm{D}_3 \subset \mathrm{D}_6$ on SO_3

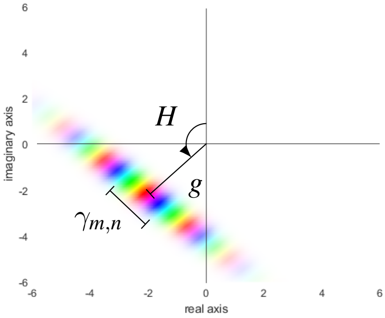
(c) $\mathrm{T} \subset \mathrm{I}$ on SO_3

(b) $\mathrm{T} \subset \mathrm{O}$ on SO_3

[2] Calderbank and Shor, 1996, "Good quantum error-correcting codes exist".
[3] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".
[4] Albert, Covey, and Preskill, 2020, "Robust Encoding of a Qubit in a Molecule".
[5] Braunstein, 1998, "Quantum error correction for communication with linear optics".

- Coset states $|gH^{\gamma}_{m,n}\rangle$ are well-defined only for finite groups
- Definition can be modified for groups with 'nice' representation theory
  - **Compact:** Peter-Weyl theorem
  - **Abelian**: Fourier transform
- Sums $\sum_{h\in H}$ become Haar integrals $\int_H d_H h$
- We need to replace Dirac deltas with Gaussians (damping)
- Preserves states but harder to work with rigorously

 [6]

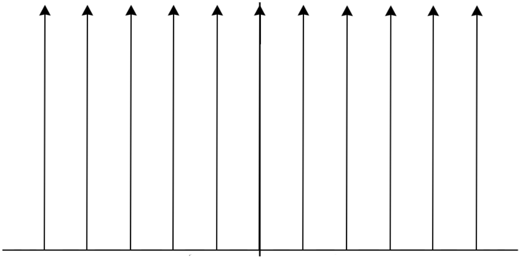


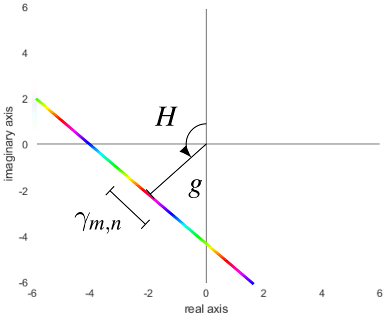
[6] Gottesman, Kitaev, and Preskill, 2001, "Encoding a qubit in an oscillator".

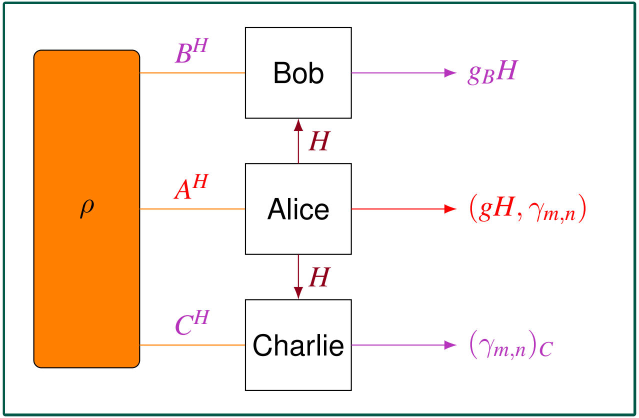
- Alternate approach: Generalise only measurement
- Measurement in basis of coset states becomes operator-valued measure

$$A^H : \mathscr{B}(G/H \times \hat{H}) \to \mathcal{B}(L^2(G)) \quad \text{satisfying} \quad \mathrm{Tr}(A^H(E)\rho) = \Pr[(gH, \gamma_{m,n}) \in E]$$

- Intuitively $A^H(E) = \int_E |gH^{\gamma}_{m,n}\rangle\langle gH^{\gamma}_{m,n}| \, d(gH, \gamma_{m,n})$







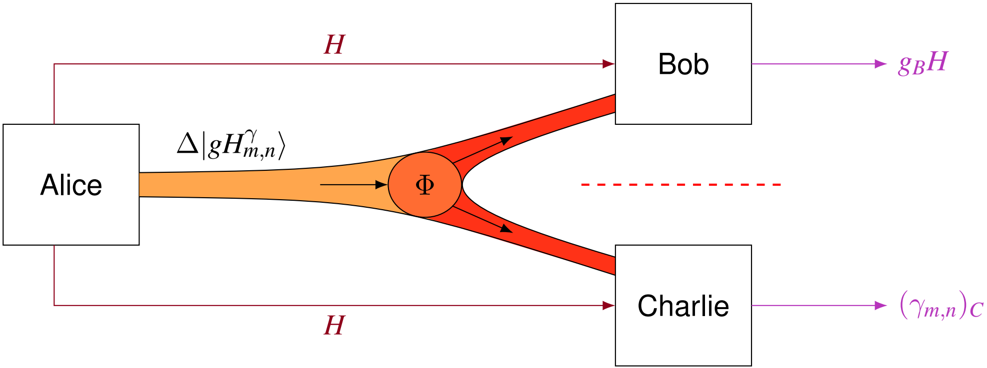
Generalises game of Coladangelo, Liu, Liu, and Zhandry[7]

1. Bob and Charlie prepare shared state
2. Alice samples subgroup H from a finite set $\mathcal{S}$ and measures with A^H
3. Alice sends H to Bob and Charlie.
4. Bob guesses gH, Charlie guesses $\gamma_{m,n}$
5. Bob and Charlie win if guesses are up to allowed errors E, F

Theorem

$$\mathfrak{w}_{\mathtt{G}}(\mathtt{S}) \leq \mathop{\mathbb{E}}_{i} \sup_{H \in \mathcal{S}, \gamma \in \mathsf{Irr}(H), g \in G} \sqrt{d_\gamma \mu_H(H \cap E g \pi_i(H)) \mu_{\hat{H}}(F)}$$

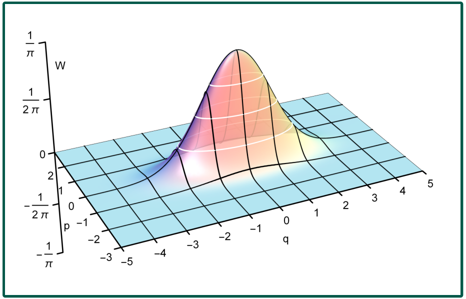
[7] Coladangelo, Liu, Liu, and Zhandry, 2021, “Hidden Cosets and Applications to Unclonable Cryptography”.



The same bound on the winning probability holds!

- Monogamy properties can be used to construct one-sided device-independent QKD[8]
- Using infinite-dimensional group spaces, we can work with continuous-variable states
- Putting these together should give continuous-variable one-sided DIQKD

- Group $G = \mathbb{R}^n$, subgroups are subspaces $P = \mathrm{span}\{e_{i_1}, \ldots, e_{i_{n/2}}\}$
- We can identify $\mathbb{R}^n/P \cong P^\perp$, $\hat{P} \cong P$
- Intuitively, coset states are position/momentum eigenstates $|q + P^{\gamma_p}\rangle = \int_P e^{2\pi i p \cdot x} |x + q\rangle dx$.
- Measurement is homodyne detection
- Damped coset states are squeezed states



[8] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, “A monogamy-of-entanglement game with applications to device-independent quantum cryptography”.

- Is it possible to make the QKD protocol more practical?
- Can monogamy-of-entanglement be used to show DIQKD properties of coherent state protocols?

Abelian case:

$$\langle\phi|A^H(E)|\psi\rangle = \int_E \overline{(\mathcal{F}_H|\phi\circ g\rangle)(\gamma)}(\mathcal{F}_H|\psi\circ g\rangle)(\gamma)d_{G/H\times\hat{H}}(gH,\gamma),$$

where $\mathcal{F}_H$ is the group Fourier transform $(\mathcal{F}_H|\psi\rangle)(\gamma) = \int_H \psi(h)\overline{\gamma(h)}dh$.

Compact case:

$$\langle\phi|A^H(E)|\psi\rangle = \sum_{\gamma_{m,n}} d_\gamma \int_{E_{\gamma_{m,n}}} \langle\phi\circ[g],\gamma_{m,n}\rangle_H\langle\gamma_{m,n},\psi\circ[g]\rangle_H d[g],$$

where $[g]$ is a fixed representative of gH, $\langle\psi,\phi\rangle_H = \int_H \overline{\psi(h)}\phi(h)d_H h$, and $d[g]$ is the induced Haar measure on the symmetric space of classes.

Overlap Lemma[9]

Let $P^1, \ldots, P^N$ be positive operators and $\pi_1, \ldots, \pi_N$ be mutually orthogonal permutations. Then,

$$\left\|\sum_i P^i\right\| \leq \sum_i \max_j \left\|\sqrt{P^j}\sqrt{P^{\pi_i(j)}}\right\|$$

Lemma

For $H, K \leq G$, $E \subseteq G$, $F \subseteq \hat{G}$, $q \in G$, $\gamma_{m,n} \in \hat{G}$. If G compact,

$$\left\|A^H(G/H \times \{\gamma_{m,n}\})A^K(EqK/K \times \hat{K})\right\| \leq \sup_{g \in G} \sqrt{d_\gamma \mu_H(H \cap gEK)}$$

If G abelian,

$$\left\|A^H(G/H \times F\gamma_{m,n})A^K(EqK/K \times \hat{K})\right\| \leq \sup_{g \in G} \sqrt{\mu_H(H \cap gEK)\mu_{\hat{H}}(F)}$$

[9] Tomamichel, Fehr, Kaniewski, and Wehner, 2013, "A monogamy-of-entanglement game with applications to device-independent quantum cryptography".