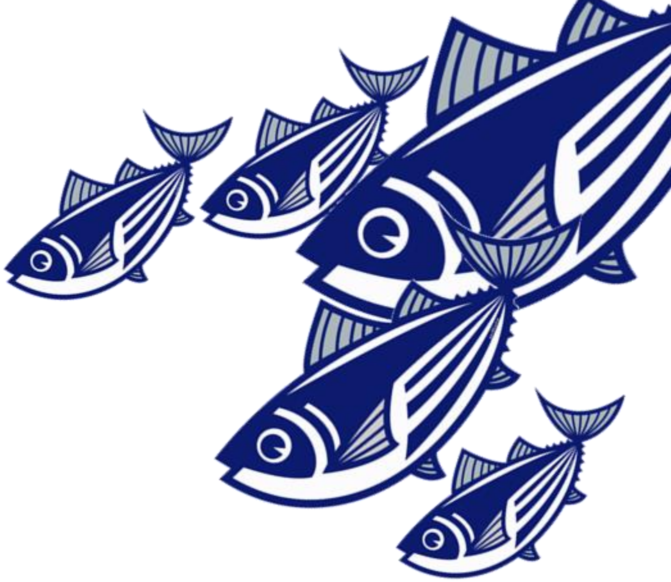


Unitary designs

- constructions and applications -

Yoshifumi Nakata

The University of Tokyo

UT-PSC
Photon Science Center of the University of Tokyo

さきがけ
PRESTO

@ 8th Quantum Theory & Technology Un-Official Meeting

Self-introduction

中田芳史

東京大学工学系　光量子科学研究センター: 特任研究員

□ 経歴：

- 2006 - 2008:　東京大学　修士課程（村尾研）
- 2008 - 2010:　青年海外協力隊　エチオピア
- 2008 - 2013:　東京大学　博士課程（村尾研）
- 2013 - 2015:　Leibniz University Hannover (Germany)
- 2015 - 2017:　Autonomous University of Barcelona (Spain)
- 2017 -　　　:　東京大学（特任研究員）
- 2018 -　　　:　京都大学基研（特定助教）

最近は「ユニタリ・デザイン」に
関連した研究

Outline

Intro. Random unitary in quantum information

1. Haar random unitary in QI
2. Unitary designs in QI

Part I. Constructing unitary designs

1. Unitary 2-designs
2. Unitary t-designs for general t

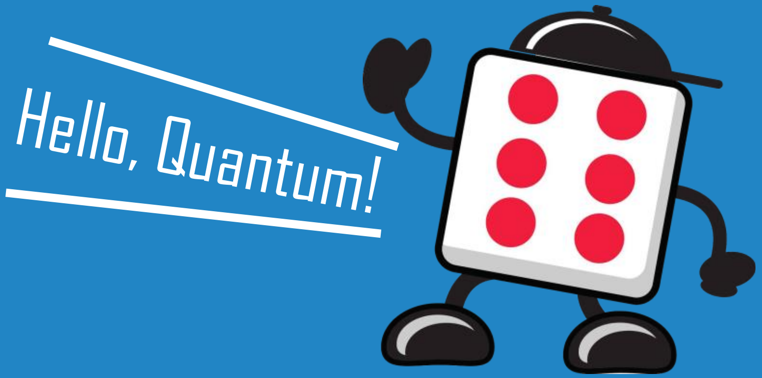
Part II. Applications of random unitary

1. Towards channel coding with symmetry-preserving unitary

Intro.

Random unitary in quantum information science

Randomness meets Quantum World!!



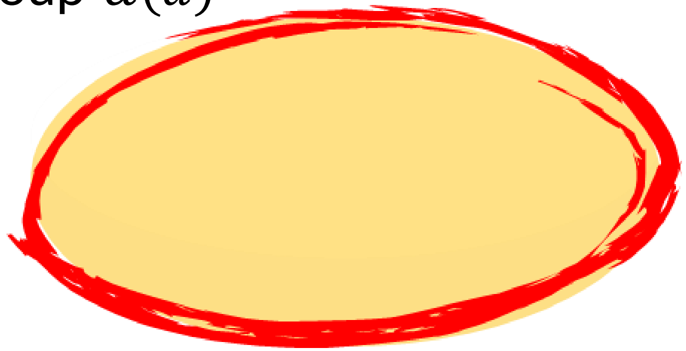
A Haar random unitary

A Haar random untiary is the unique unitarily invariant probability measure H on the unitary group $U(d)$. Namely,

(A) $\mu_{\mathsf{H}}(U(d)) = 1,$

(B) for any $V \in U(d)$ and any (Borel) set $\omega \subseteq U(d)$, $\mathsf{H}(V\omega) = \mathsf{H}(\omega V) = \mathsf{H}(\omega)$.

Unitary group $\mathcal{U}(d)$



A distribution of the Haar measure

Applications of a Haar random unitary

Haar random unitary is very useful in QIP and in fundamental physics.

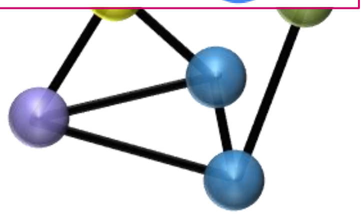
In QIP

1. Q. communication [Hayden et.al. ‘07]
2. Randomized benchmarking [Knill et.al. ‘08]
3. Q. sensing [Oszmaniec et.al. ‘16]
4. Q. comp. supremacy [Bouland et.al. ‘18]

In fundamental physics

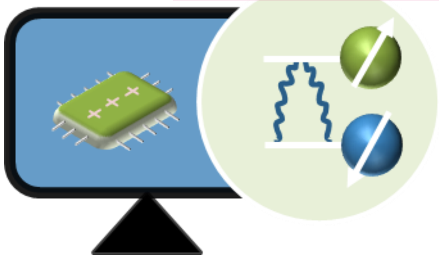
1. Disordered systems
2. Pre-thermalization [Reimann ‘16]
3. Q. black holes [Hayden&Preskill ‘07]
4. Q. chaos -OTOC- [Roberts&Yoshida ‘16]

Google

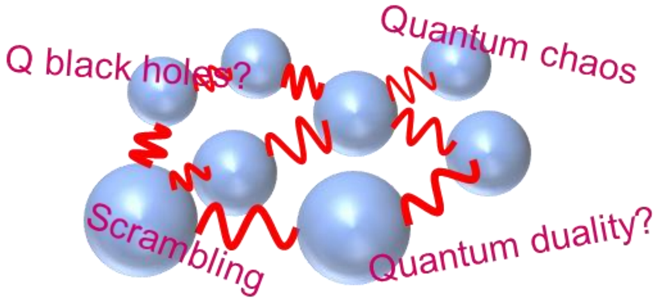


Quantum communication

IBM

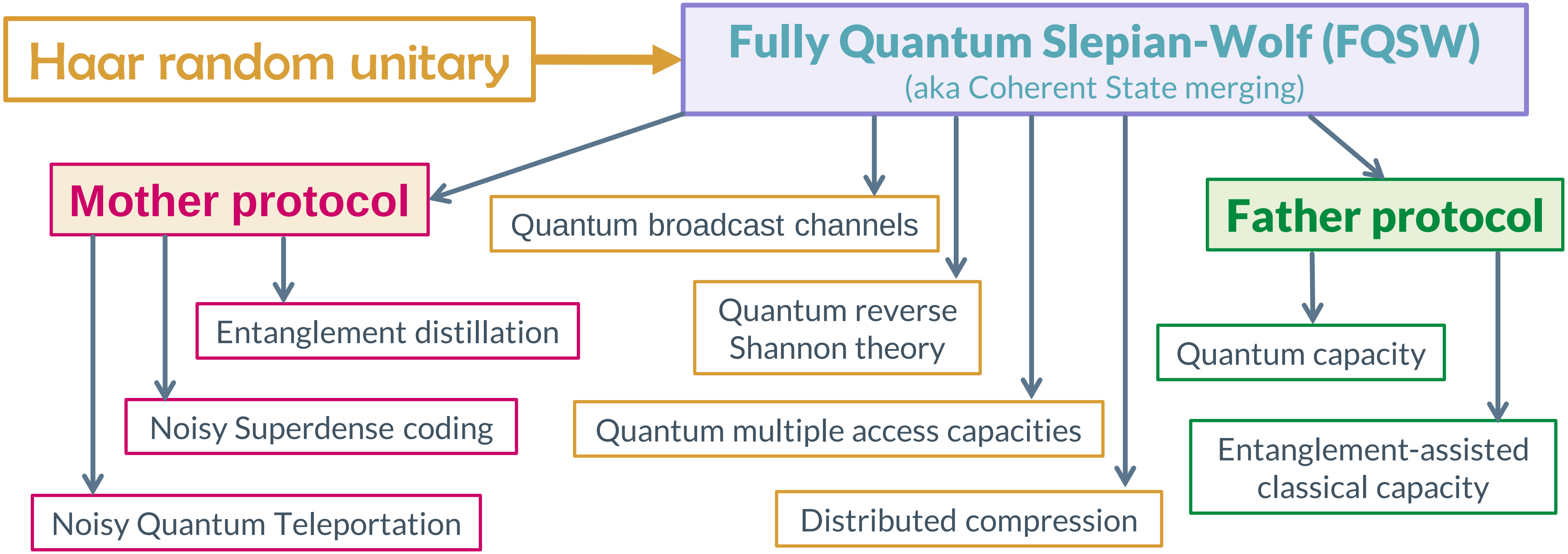


Quantum computation



Haar random in Q. communication

- Quantum communication
  - Two people want to communicate in a quantum manner.



Haar random unitary

Fully Quantum Slepian-Wolf (FQSW)
(aka Coherent State merging)

Mother protocol

Entanglement distillation

Noisy Superdense coding

Noisy Quantum Teleportation

Quantum broadcast channels

Quantum reverse Shannon theory

Quantum multiple access capacities

Distributed compression

Father protocol

Quantum capacity

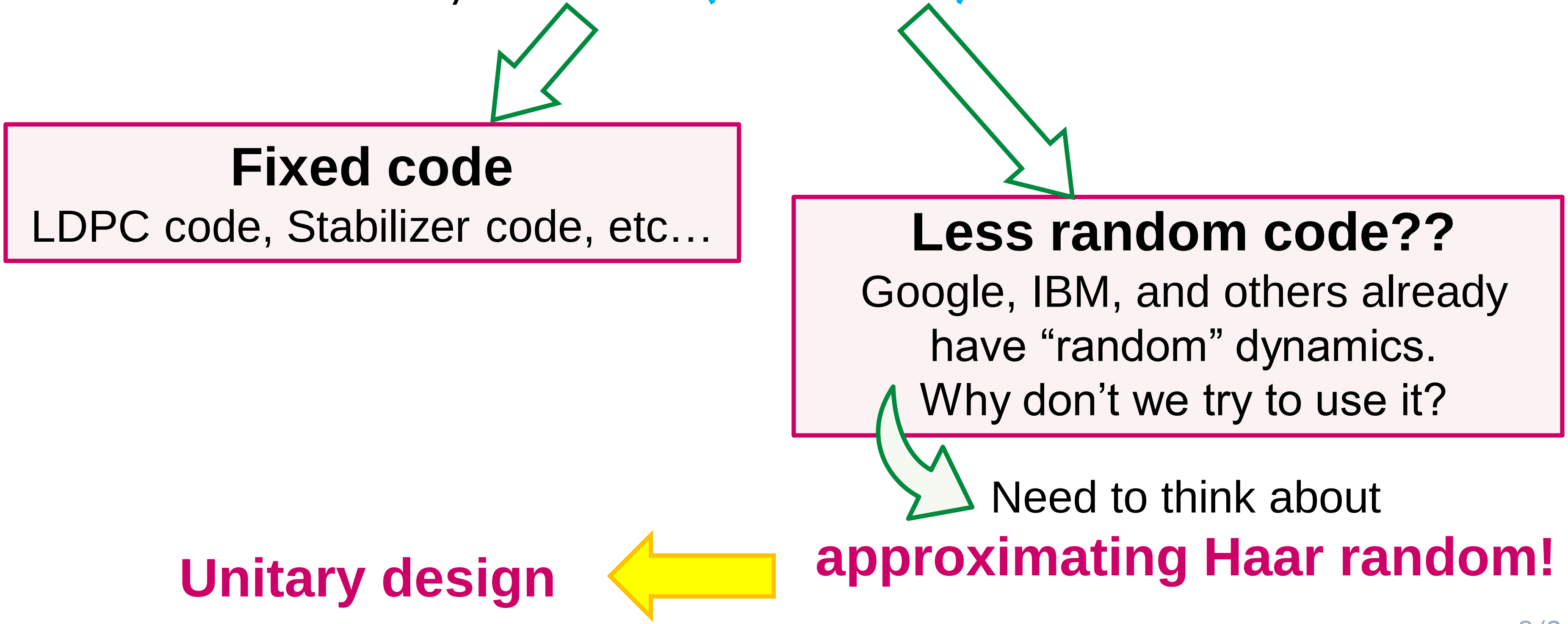
Entanglement-assisted classical capacity

See Hayden's tutorial talk in QIP2011

Family tree of information protocols

Haar random in Q. communication

- Quantum communication
  - Two people want to communicate in a quantum manner.
- **Haar** random unitary is a **random encoder**!!
  - It is extremely **inefficient (too random)**.



Fixed code

LDPC code, Stabilizer code, etc…

Less random code??

Google, IBM, and others already have “random” dynamics. Why don’t we try to use it?

Need to think about

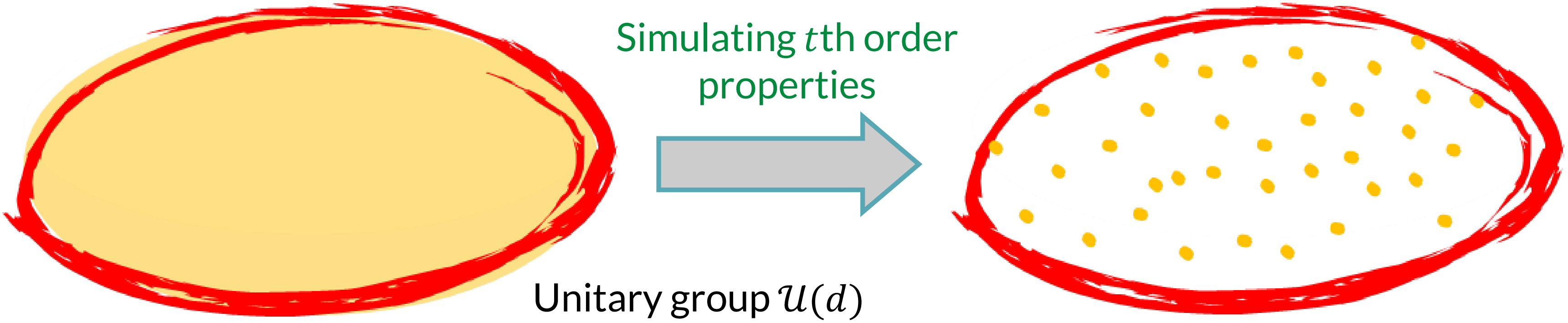
approximating Haar random!

Unitary design

Unitary designs as approximating Haar

持続可能な高度量子技術開発に向けた
量子疑似ランダムネスの発展と応用
さきがけ PRESTO

- Random coding by unitary d
  - Nice applications of **NISQ** (Noisy-Intermediate-Scale-Quantum device).
  - **Quantum pseudo-randomness** in quantum computer
  - Nice insights to **fundamental physics** (chaos, blackholes, etc…)
- Unitary t-design is a set of unitaries that simulate up to the t-th order properties of Haar random unitary.



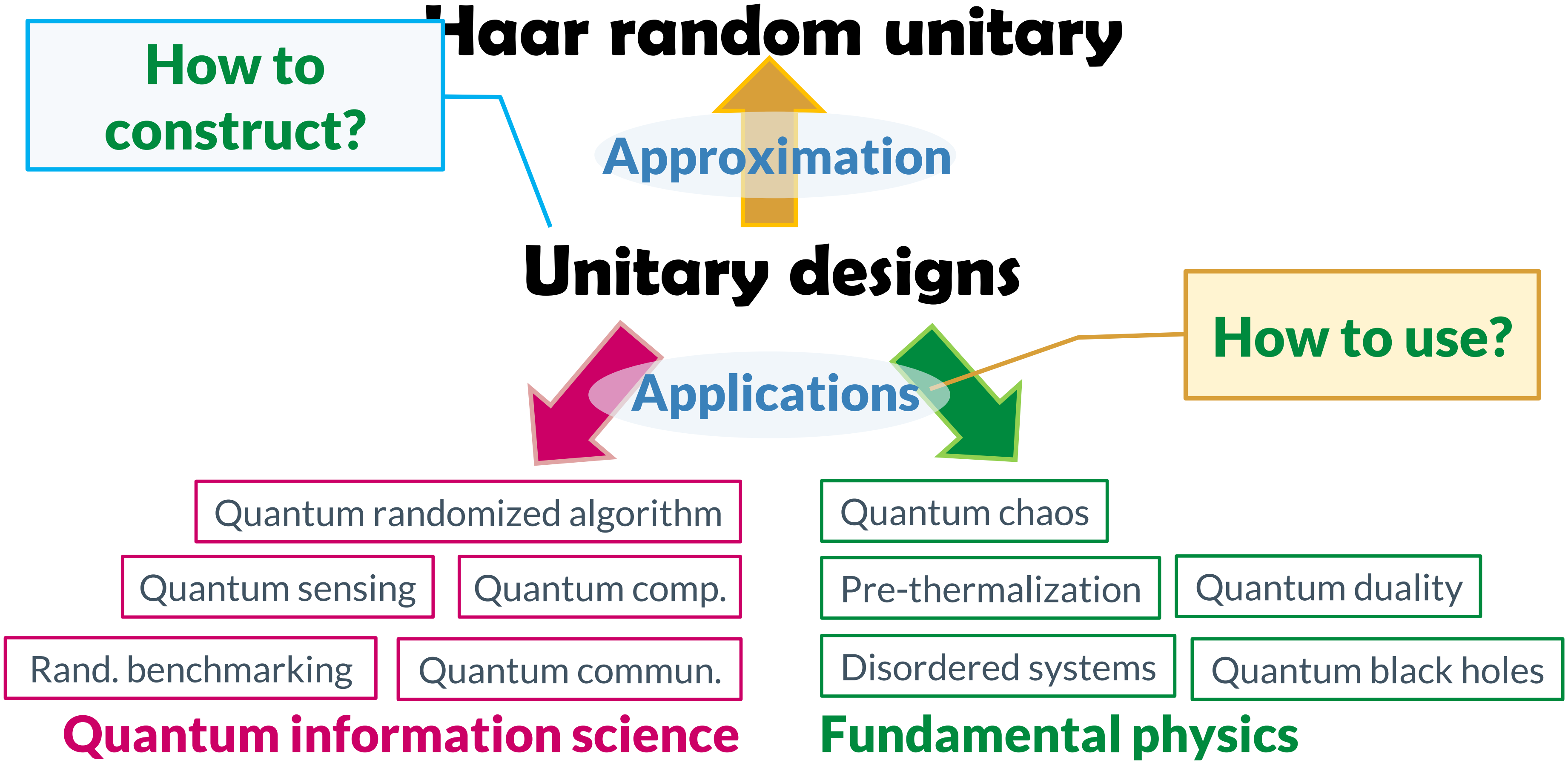
Simulating tth order properties

Unitary group $\mathcal{U}(d)$

A distribution of the Haar measure

A distribution of a unitary design

Unitary design meets QIP and fundamental physics



Haar random unitary

How to construct?

Approximation

Unitary designs

How to use?

Applications

- Quantum randomized algorithm
- Quantum sensing
- Quantum comp.
- Rand. benchmarking
- Quantum commun.

Quantum information science

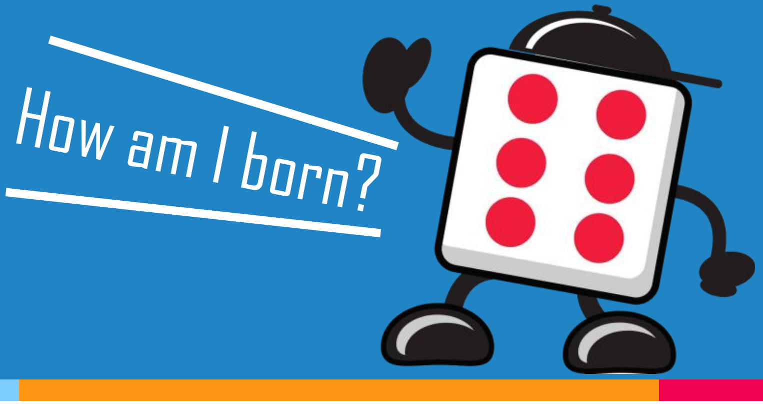
- Quantum chaos
- Pre-thermalization
- Quantum duality
- Disordered systems
- Quantum black holes

Fundamental physics

Part 1.

Constructing unitary designs

Generating quantum pseudo-randomness!



In collaboration with Hirche, Koashi, and Winter.

[1] YN, C. Hirche, C. Morgan, and A. Winter, JMP, 58, 052203 (2017).

[2] YN, C. Hirche, M. Koashi, and A. Winter, PRX, 7, 021006 (2017).

Short History of constructing designs

Approximate unitary design

An ϵ-approximate unitary t-design is a probability measure that simulates up to the tth order statistical moments of the Haar measure within an error ϵ.

Unitary t-design minimizes the frame potential of degree t.

- ❑ A more precise definition:

For a set of unitaries $\mathcal{U} = \{p_i, U_i\}_{i=1}^{K}$, define the *frame* potential of degree t, by

$$F_t(\mathcal{U}) = \sum_{i,j=1}^{K} p_i p_j \left|\mathrm{Tr}[U_i U_j^\dagger]\right|^{2t}$$

Then, $\mathcal{U} = \{p_i, U_i\}_{i=1}^{K}$ is an ϵ-approximate unitary t-design if

$$F_t(\mathcal{U}) = F_t^{\mathrm{Haar}} + \epsilon.$$

- ➢ Indeed, the average over Haar measure is the minimum, which is $t!$ if $d \geq t$.

Short History of constructing designs

Approximate unitary design

An ϵ-approximate unitary t-design is a probability measure that simulates up to the tth order statistical moments of the Haar measure within an error ϵ.

☐ Two approaches

1. Use a subgroup of the unitary group → Clifford group

✓Beautiful analyses are possible!!	☠ Quantum circuits??
✓Exact unitary designs!!	☠ Up to 2- (or 3-)designs.

2. Use a “random” quantum circuits

✓Works for general t-design.	☠Not exact designs.
✓Quantum circuits are given.	☠Case-by-case analyses….

Short History of constructing designs

Approximate unitary design

An ϵ-approximate unitary t-design is a probability measure that
simulates up to the tth o of
within an error ϵ.

BHH12
Googleによる実験
(超伝導qubit:≈49 qubits?)
[S. Boixo, Nature Physics, 2018]

NHKW17
中国・カナダによる実験
(NMR: 12 qubits)
[J. Li, arXiv, 2018]

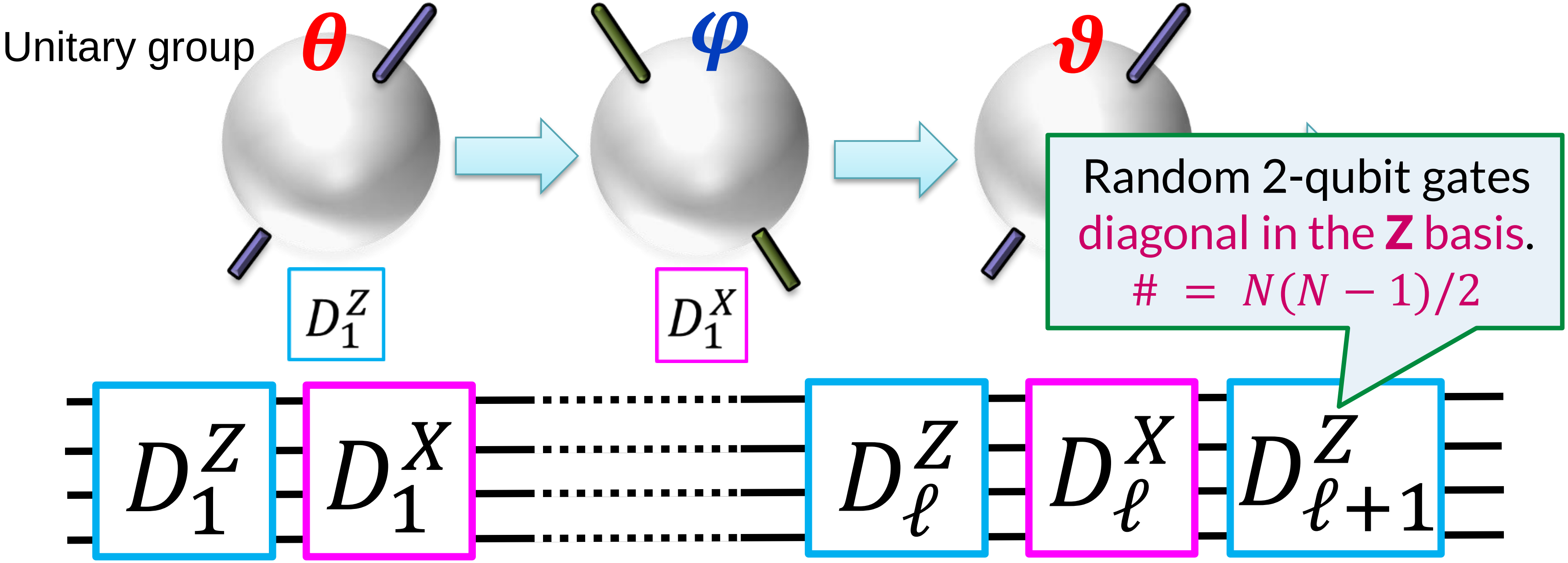
❑ “Random” circuits co

	HL09	BHH12	NHKW17
		ircuits	Hadamard gates + random diagonal gates
		n of iltonian	Combinatorics
# of gates	$O(t^3N^3)$ [Brodsky & Hoory ’13]	$O(t^{10}N^2)$	$\Theta(tN^2)$
Works for	$t = O(N/\log N)$	$t = O(\mathrm{poly}(N))$	$t = o(\sqrt{N})$

HM18
\# of gates
= $O(\mathrm{poly}(t)N^{1+1/D})$ for any $D < \log N$.

Constructing designs by NHKW17

❑ The idea is to use random diagonal unitaries in X and Z bases.



Random 2-qubit gates
diagonal in the **Z** basis.
$\# = N(N-1)/2$

- Each D_i^W are independently chosen.
- If $\ell \geq t + \frac{1}{N}\log_2 1/\epsilon$, this forms an ϵ-approximate unitary t-design.
- $\approx tN^2$ gates are used in the construction

Short History of constructing designs

Approximate unitary design

An ϵ-approximate unitary t-design is a probability measure that simulates up to the tth o of within an error ϵ.

- ❑ "Random" circuits co

BHH12
Googleによる実験
(超伝導qubit:≈49 qubits?)
[S. Boixo, Nature Physics, 2018]

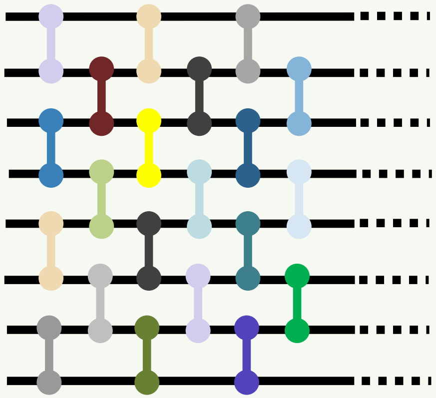
NHKW17
中国・カナダによる実験
(NMR: 12 qubits)
[J. Li, arXiv, 2018]

	HL09	BHH12	NHKW17
		ircuits	Hadamard gates + random diagonal gates
		n of iltonian	Combinatorics
# of gates	$O(t^3N^3)$ [Brodsky & Hoory '13]	$O(t^{10}N^2)$	$\Theta(tN^2)$
Works for	$t = O(N/\log N)$	$t = O(\mathrm{poly}(N))$	$t = o(\sqrt{N})$

HM18
# of gates
$= O(\mathrm{poly}(t)N^{1+1/D})$ for any $D < \log N$.

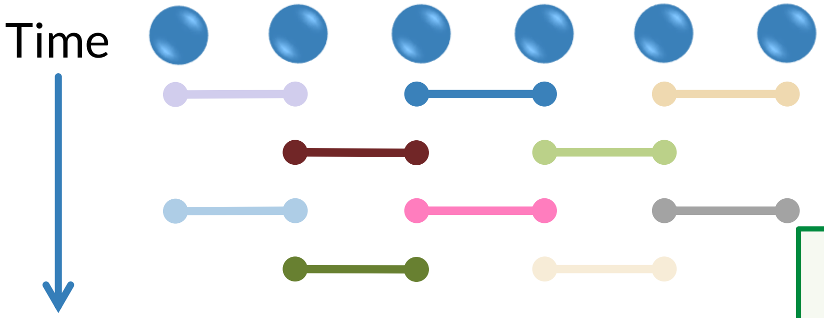
Constructing designs by HM18

Construction by BHH12



- ☐ The idea is to apply random 2-qubit gates on nearest-neighbor qubits.
- ☐ Mapped to a Hamiltonian gap problem.
- ☐ After $\approx t^{10}N^2$ gates, it becomes an approximate unitary t-design.
  - – The t-dependence may not be optimal.

Qubits



- ☐ 1-dimensional geometry.

D-dimensional geometry.

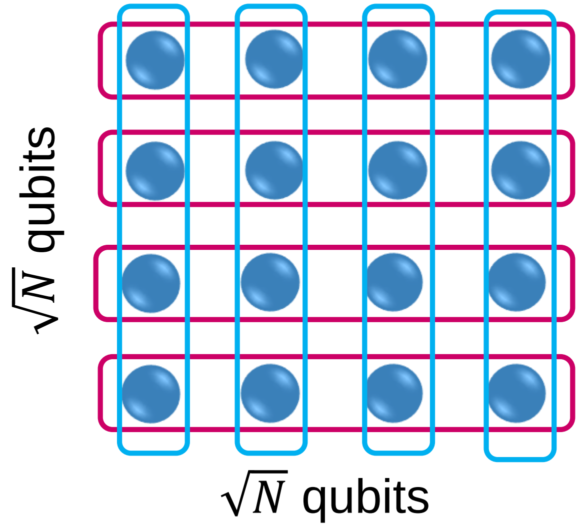
HM18

# of gates

= $O(\mathrm{poly}(t)N^{1+1/D})$ for any $D < \log N$.

Constructing designs by HM18

Qubits on 2-dim lattice



1. Apply random gates in one direction to make a design in each row.
   - $\approx t^{10}(\sqrt{N})^2$ gates per each row [BHH12].
   - There exists $\sqrt{N}$ rows.

   ⇨ $\approx t^{10}N^{3/2}$ gates.
2. Do the same in another direction.

   ⇨ $\approx t^{10}N^{3/2}$ gates.
3. Repeat 1 and 2, $\mathrm{poly}(t)$ times.

This forms an approximate unitary t-design, where # of gates = $O(\mathrm{poly}(t)N^{3/2})$.

Note: can be generalized to any $D \in \mathbb{N}$

Surprising!

Is this method applicable to **any** constructions??
e.g.) NHKW17

Optimality of the constructions

HM18

# of gates = $O(\mathrm{poly}(t)N^{1+1/D})$ for any $D < \log N$.

Theorem

At least $\approx tN$ quantum gates are needed to generate a unitary design.

If $\mathcal{U} = \{U_i\}_{i=1}^{K}$ is a unitary t-design,

$$t! = \sum_{i,j=1}^{K} p_i p_j \left|\mathrm{Tr}[U_i U_j^\dagger]\right|^{2t} \geq \sum_{i=1}^{K} p_i^2 \left|\mathrm{Tr}[U_i U_i^\dagger]\right|^{2t} \geq 2^{2tN}/K.$$

$$\boxed{K \geq 2^{2tN}/t!.}$$

If each gate is chosen from s different gates and the # of gates is L, $K = s^L$.

$$\boxed{L \gtrsim 2tN - t\log t.}$$

Is it possible to achieve this bound? If not, better bound?

Summary and open questions about constructing designs

	# of local unitaries	It works for
Harrow and Low, 2009	$O(t^3N^4)$	$t = O(N/\log N))$
Brandao, Horodecki, and Harrow, 2012	$O(t^{10}N^2)$	$t =$O(poly(N))
Nakata, Hirche, Koashi, and Winter, 2017	$O(tN^2)$	$t = o(N^{1/2})$
Harrow, and Mehraban, 2018	$O(\text{poly}(t)N^{1+1/D})$	$t = \text{poly}(N)$

❑ Several constructions for approximate t-designs for general t.

- Is the bound ($\approx tN$) achievable?
- In design theory, a t-design has several "types".

Not all "types" are needed in QIP.

❑ What about exact ones?

- In some applications, we need exact ones, e.g. RB.
- For 2-designs, use Clifford circuits [CLLW2015].
- For general t, how to construct exact ones?

Exact ones for any t [Okuda, and YN, in prep],
but $\mathrm{O}(10^6)$ gates to make 4-designs on 2 qubits…

Part 2.

Applications of unitary designs

Let's use Quantum pseudo-randomness!

In collaboration with Wakakuwa, and Koashi.

[1] E. Wakakuwa, and YN, in preparation.

[2] YN, E. Wakakuwa, and M. Koashi, in preparation.

[3] E. Wakakuwa, YN, and M. Koashi, in preparation.

Applications of a Haar random unitary

Haar random unitary is very useful in QIP and in fundamental physics.

In QIP

1. Q. communication [Hayden et.al. '07]
2. Randomized benchmarking [Knill et.al. '08]
3. Q. sensing [Oszmaniec et.al. '16]
4. Q. comp. supremacy [Bouland et.al. '18]

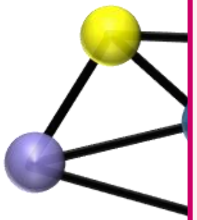
In fundamental physics

1. Disordered systems
2. Pre-thermalization [Reimann '16]
3. Q. black holes [Hayden&Preskill '07]
4. Q. chaos -OTOC- [Roberts&Yoshida '16]

Physical systems often have **symmetries**!

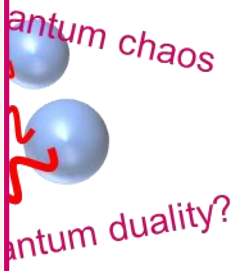
QIP with symmetry restrictions??

➡ **Quantum Communication**
with symmetry-preserving coding



Quant
communication

computation



Random unitary with a symmetry

- So far, Haar random unitaries on $\mathcal{H}_N^S = (\mathbb{C}^2)^{\otimes N}$.
- Physical systems often have a symmetry.
  - Rotational symmetry, U(1) symmetry, etc…
  - Tensor product representation of a group G.
  - Irreducible decomposition:

Hilbert space invariant under any action of G.

$$\mathcal{H}_N^S = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r})^{\oplus m_j} \Rightarrow \mathcal{H}_N^S = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r} \otimes \underline{\underline{\mathcal{H}_j^{S_m}}})$$

multiplicity

multiplicity $\dim(\mathcal{H}_j^R) = m_j$

e.g.) Spin-spin coupling (spin-1/2 × 3): $\mathcal{H} = 4 \oplus \underbrace{2 \oplus 2}$

4-dimensional irrep. $(\dim \mathcal{H}_1^{S_r} = 4, \dim \mathcal{H}_1^{S_m} = 1)$

2-dim. irreps with multiplicity 2. $(\dim \mathcal{H}_2^{S_r} = 2, \dim \mathcal{H}_2^{S_m} = 2)$

Random unitary with a symmetry

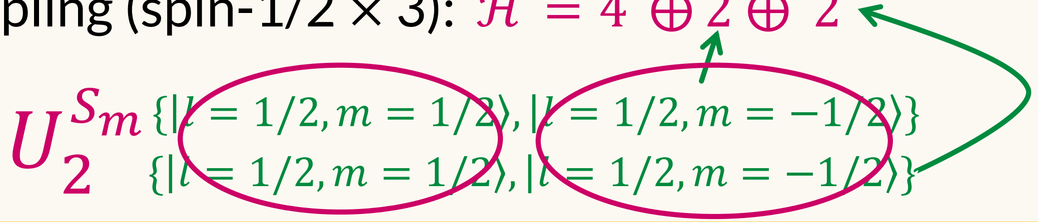
- So far, Haar random unitaries on $\mathcal{H}_N^S = (\mathbb{C}^2)^{\otimes N}$.
- Physical systems often have a symmetry.
  - Rotational symmetry, U(1) symmetry, etc…
  - Tensor product representation of a group G.
  - Irreducible decomposition:

Hilbert space invariant under any action of G.

$$\mathcal{H}_N^S = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r})^{\oplus m_j} \Rightarrow \mathcal{H}_N^S = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r} \otimes \mathcal{H}_j^{S_m})$$

- "*Symmetry-preserving*" random unitaries.
  - $U = \bigoplus_{j=1}^{J} (I_j^{S_r} \otimes U_j^{S_m})$, where $U_j^{S_m}$ is the Haar on $\mathcal{H}_j^{S_m}$.

e.g.) Spin-spin coupling (spin-1/2 × 3): $\mathcal{H} = 4 \oplus 2 \oplus 2$



$$U_2^{S_m} \begin{matrix} \{|l = 1/2, m = 1/2\rangle, |l = 1/2, m = -1/2\rangle\} \\ \{|l = 1/2, m = 1/2\rangle, |l = 1/2, m = -1/2\rangle\} \end{matrix}$$

Why symmetry-preserving R.U.?

Symmetry-preserving random unitary (a group G is given)

$U = \bigoplus_{j=1}^{J} (I_j^{S_r} \otimes U_j^{S_m})$, where $U_j^{S_m}$ is the Haar on $\mathcal{H}_j^{S_m}$.

Decoupling-type theorem

One of the most important theorems in QIP

[1] E. Wakakuwa, and YN, in preparation.

Quantum Communication

with symmetry restriction

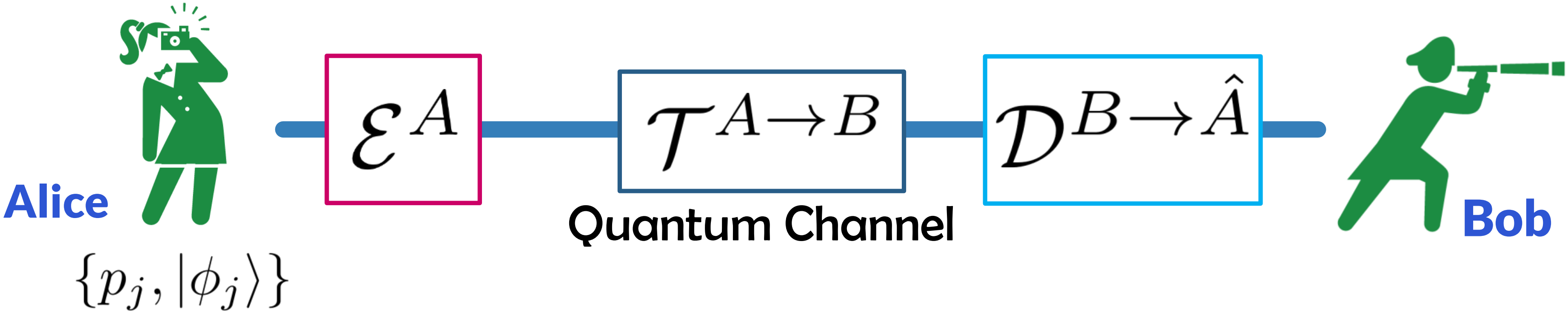
[2] YN, E. Wakakuwa, and M. Koashi, in prep.

"Hybrid" communication

quantum and classical

[3] E. Wakakuwa, YN, and M. Koashi, on going.

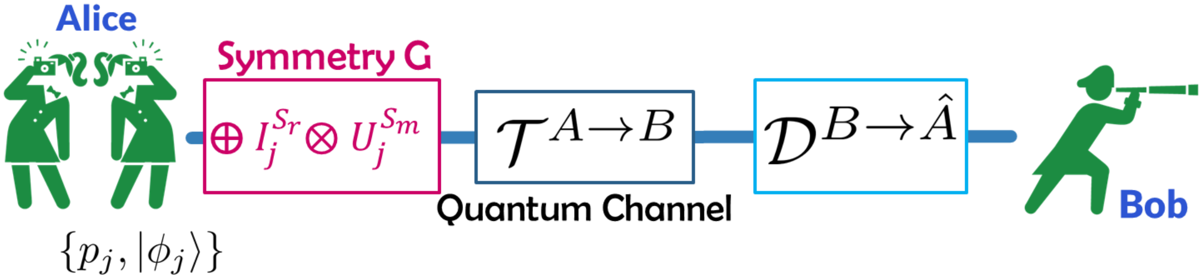
Quantum Communication with symmetry-preserving coding



- Limited to symmetry-preserving unitary encoding!
  - A group G is acting on the system A.
  - The $\mathcal{E}^A$ should be in the form of $U = \bigoplus (I_j^{S_r} \otimes U_j^{S_m})$.
- In general, full information cannot be reliably transmitted.

What information can be transmitted reliably at what rate?

Quantum Communication with symmetry-preserving coding



What information can be transmitted reliably at what rate?

$$\mathcal{H}_N = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r} \otimes \mathcal{H}_j^{S_m})$$

Hopeless to transmit?
(no encoding)

Classical info Is reliably **transmitted**!

Quantum info cannot!

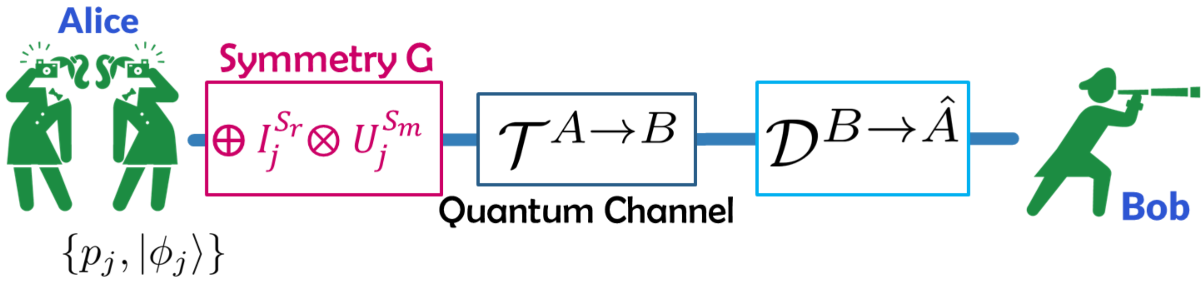
Hopeless to transmit
(no encoding)

In general, **cannot** be transmitted!

Maybe **possible** to transmit

Reliably **transmitted!**

Quantum Communication with symmetry-preserving coding



What information can be transmitted reliably at what rate?

$$\mathcal{H}_N = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r} \otimes \mathcal{H}_j^{S_m})$$

Classical info Is reliably **transmitted**!

Reliably **transmitted!**

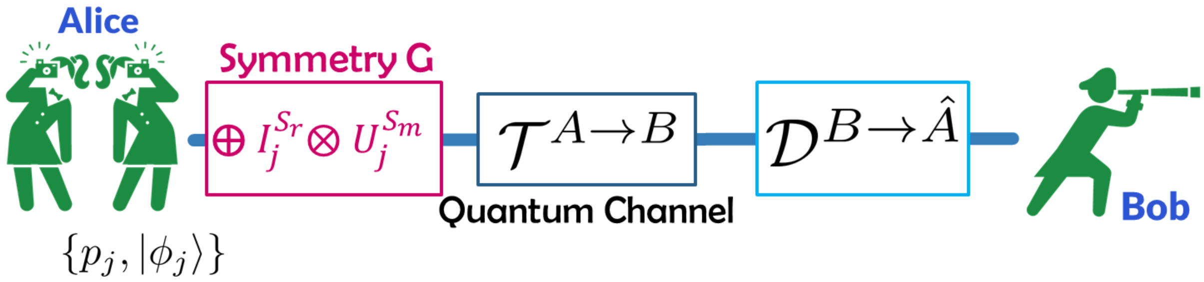
From the information of what random code $U_j^{S_m}$ is u ,

Bob can guess j.

(although j is NOT transmitted through hannel)

At what rate??

Quantum Communication with symmetry-preserving coding



What information can be transmitted reliably at what rate?

$$\mathcal{H}_N = \bigoplus_{j=1}^{J} (\mathcal{H}_j^{S_r} \otimes \mathcal{H}_j^{S_m})$$

Classical info Is reliably **transmitted**!

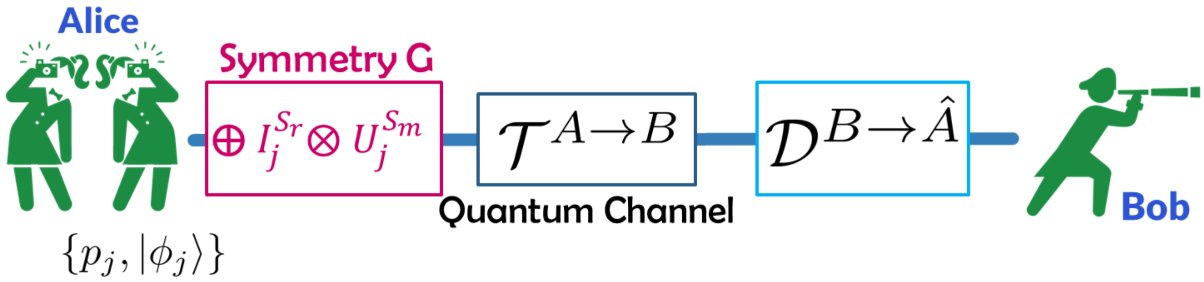
Reliably **transmitted!**

At what rate??

$$H_{\min}(S_m * S'_m|RE)_\Gamma \gg 1$$

$$\Gamma^{S_m * S'_m RE} := d_S \langle\Omega|^{S_r S'_r} \begin{pmatrix} \frac{1}{m_1}\Psi_{11}^{S_r S_m R} \otimes \bar{\tau}_{11}^{S'_r S'_m E} & \cdots & \frac{1}{\sqrt{m_1 m_J}}\Psi_{1J}^{S_r S_m R} \otimes \bar{\tau}_{1J}^{S'_r S'_m E} \\ \vdots & & \vdots \\ \frac{1}{\sqrt{m_J m_1}}\Psi_{J1}^{S_r S_m R} \otimes \bar{\tau}_{J1}^{S'_r S'_m E} & \cdots & \frac{1}{m_J}\Psi_{JJ}^{S_r S_m R} \otimes \bar{\tau}_{JJ}^{S'_r S'_m E} \end{pmatrix} |\Omega\rangle^{S_r S'_r}$$

Quantum Communication with symmetry-preserving coding



What information can be transmitted reliably at what rate?

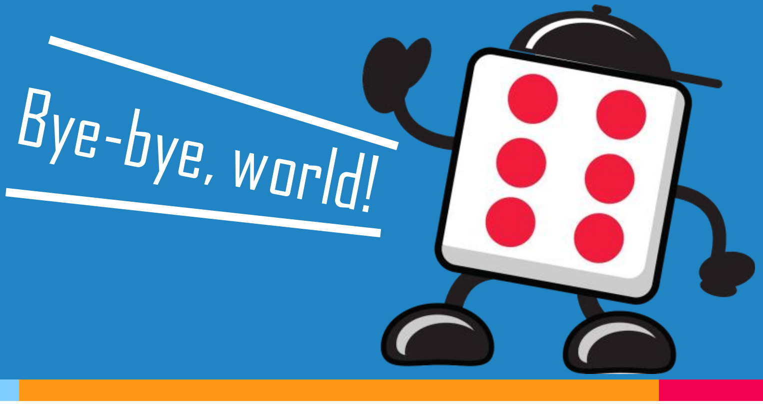
☐ Open problems:

1. Converse (not easy even in the i.i.d. limit)?
   - Asymptotic limit of the entropy?? $H_{\min}(S_m * S'_m|RE)_\Gamma$
2. What happens if we consider symmetry-preserving operations, not only unitary?
3. How to implement symmetry-preserving unitary??

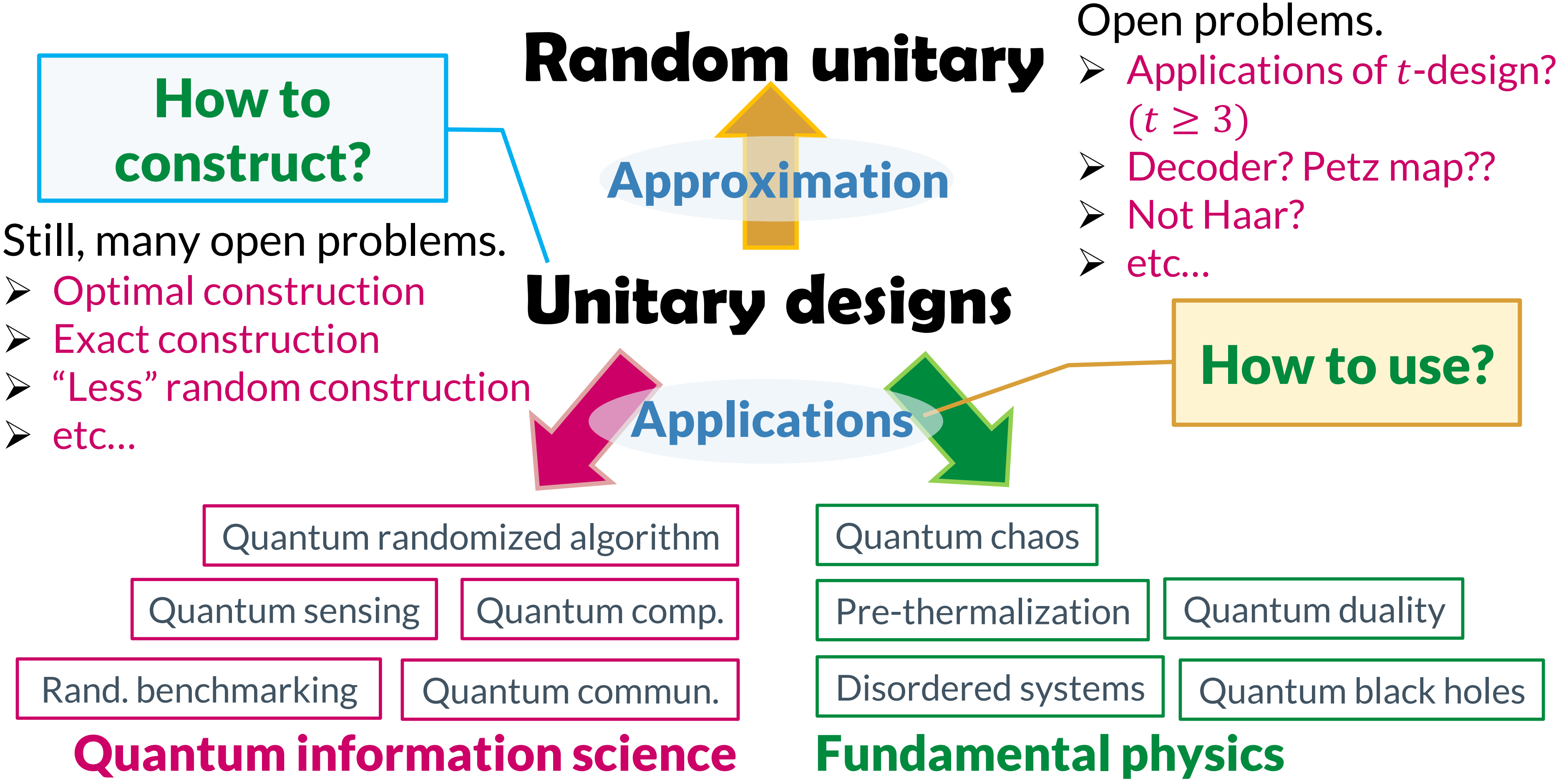
Part 3.

Summary

O-Shi-Ma-i



Unitary design meets QIP and fundamental physics



How to construct?

Still, many open problems.

- Optimal construction
- Exact construction
- “Less” random construction
- etc…

Random unitary

Approximation

Unitary designs

Applications

Open problems.

- Applications of t-design? $(t \geq 3)$
- Decoder? Petz map??
- Not Haar?
- etc…

How to use?

Quantum randomized algorithm

Quantum sensing

Quantum comp.

Rand. benchmarking

Quantum commun.

Quantum information science

Quantum chaos

Pre-thermalization

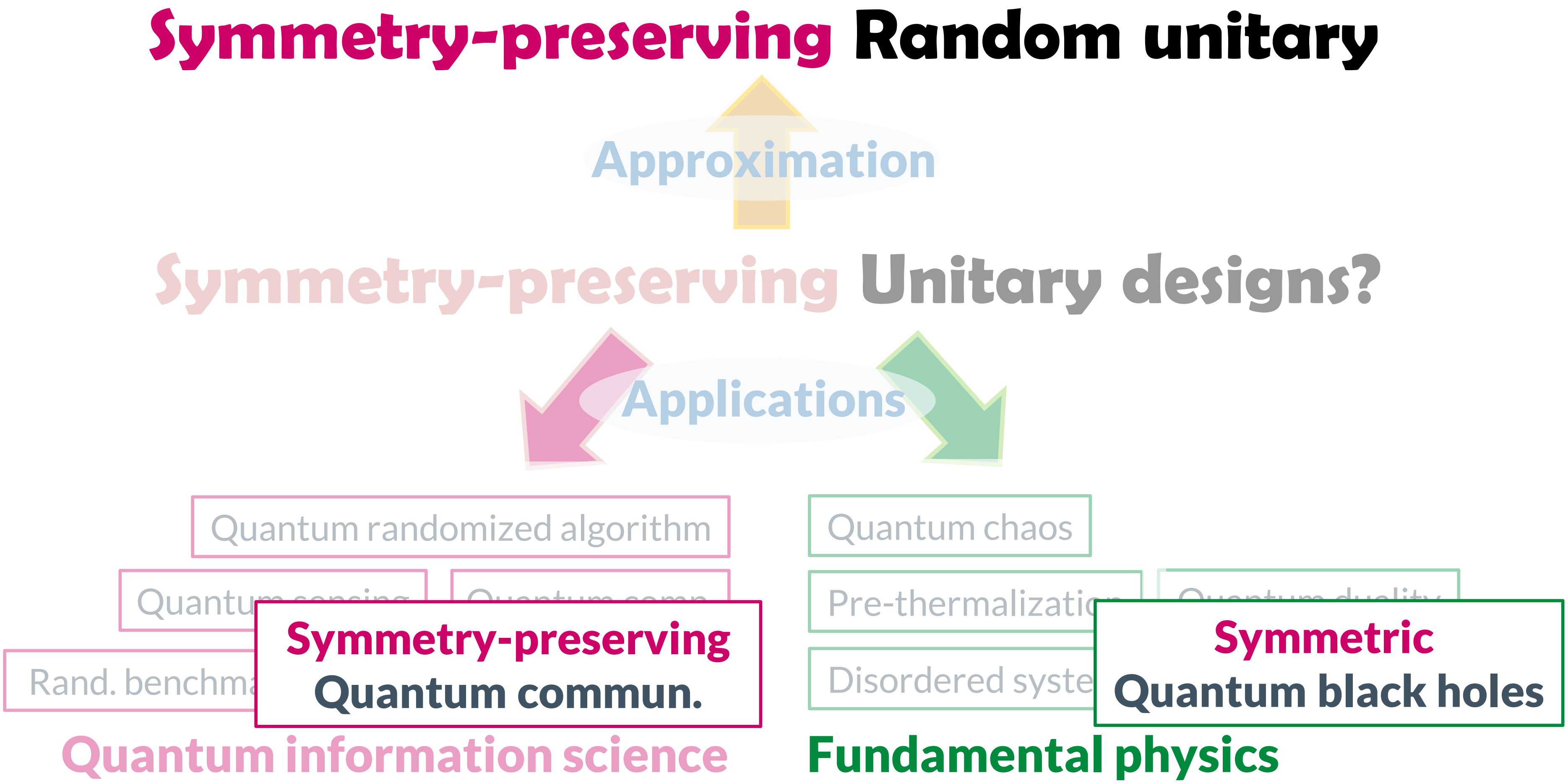
Quantum duality

Disordered systems

Quantum black holes

Fundamental physics

Possible future direction: symmetry



Symmetry-preserving Random unitary

Approximation

Symmetry-preserving Unitary designs?

Applications

Quantum randomized algorithm

Quantum sensing

Quantum comp

Rand. benchma

Symmetry-preserving Quantum commun.

Quantum information science

Quantum chaos

Pre-thermalizatio

Quantum duality

Disordered syste

Symmetric Quantum black holes

Fundamental physics

Thank you

また来年お会いしましょう！