Лекція 4: Унітарні базиси, Суперщільне кодування та Телепортація

1. Унітарні базиси

Якщо H це скінченновимірний гільбертів простір (розмірності d), то на $L(H)$ теж існує структура гільбертового простору. У якості скалярного добутку береться добуток Гільберта-Шмідта:

$$\forall A, B \in L(H) \ : \ (A, B) = \mathrm{Tr}(B^\dagger A) = \mathrm{Tr}(AB^\dagger).$$

В літературі зазвичай вводять позначення $|A\rangle\rangle$ в контексті цього, і тоді пишуть $\langle\langle B|A\rangle\rangle = (A, B) = \mathrm{Tr}(B^\dagger A)$.

Більше того, існує явна ізометрія між $L(H)$ та $H \otimes H$, яку можна задати як

$$|A\rangle\rangle = \sum_i A|i\rangle \otimes |i\rangle = (A \otimes I) \sum_i |i\rangle|i\rangle,$$

або, що те саме,

$$A = \sum_{ij} a_{ij} |i\rangle\langle j| \quad \longleftrightarrow \quad |A\rangle\rangle = \sum_{ij} a_{ij} |i\rangle|j\rangle.$$

Виявляється, що в $L(H)$ існують **унітарні базиси**, тобто набори унітарних операторів $\{U_i, i = 1, 2, .., d^2\}$, таких що

$$\mathrm{Tr}(U_i^\dagger U_j) = d \cdot \delta_{ij}$$

Типовий приклад це унітарний базис породжений операторами "зсуву" та "часів" (інколи їх називають операторами трансляції та повороту).

Оператор (циклічного) зсуву визначається як

$$\forall k \ : \ S|k\rangle = |k+1\rangle,$$

де $|d\rangle \coloneqq |0\rangle$. Оператор часів визначається як

$$\forall k \ : \ C|k\rangle = w^k |k\rangle, \quad w = e^{\frac{2\pi i}{d}}$$

Твердження *Набір з d^2 операторів $\{W_{kl} = C^k S^l\}, k, l \in [0, .., d-1]$, є унітарним базисом.*

Це неважко перевірити використовуючи що

$$S^d = I, \quad C^d = I, \quad CS = wSC.$$

Стан $\frac{1}{\sqrt{d}} \sum_i |i\rangle|i\rangle \in H \otimes H$ є максимально сплутаним (інколи їх називають EPR-станами).

Для унітарного A стан $\frac{1}{\sqrt{d}} \sum_i A|i\rangle \otimes |i\rangle$ також є максимально сплутаним.

Наслідок 1 *У $H \otimes H$ існує базис, що складається з максимально сплутаних станів:*

$$|\Psi_{kl}\rangle = \frac{1}{\sqrt{d}} \sum_i W_{kl} |i\rangle \otimes |i\rangle$$

2. Суперщільне кодування

Нехай є двоє учасників A та B і один хоче повідомити іншому якусь класичну інформацію за допомогою пересилання одної фізичної квантової системи. Яку максимальну кількість інформації можна передати, якщо квантова система розмірності d?

Учасник A може закодовути число з набору $\{0, 1, .., d-1\}$ за допомогою стану $|i\rangle \in H$. Отримавши цей стан, учасник B може визначити закодоване число провівши вимірювання, шо відповідає розкладу $I = \sum_i |i\rangle\langle i|$. Тобто можна передати $\log_2(d)$ біт класичної інформації.

Теорема Холево строго доводить, що передати більше неможливо.

Але, якщо учасники розподілили між собою сплутаний стан, то вони можуть використати його для передачі більшої кількості інформації.

Твердження *(Суперщільне кодування)*

Якщо двоє учасників A та B розподілили між собою максимально сплутаний стан (у розмірності $d \times d$), то один учасник може повідомити іншому $log_2(d^2) = 2log_2(d)$ класичних бітів інформації передавши свою квантову частинку (розмірності d).

Доведення. Нехай учасники A та B мають доступ до чистого максимально сплутаного стану

$$\frac{1}{\sqrt{d}} \sum_i |i\rangle_A \otimes |i\rangle_B \in H_A \otimes H_B,$$

який фізично розподілили між собою.

Тоді, учасник A кодує пару чисел (k, l) з множини $[0, 1, ..., d-1]^2$ (тобто $log_2(d^2)$ біт інформації) застосуванням оператору W_{kl} на своїй частниці та фізично передаючи її до B.

Після отримання частинки від A учасник B буде мати доступ до стану

$$|\Psi_{kl}\rangle = \frac{1}{\sqrt{d}} \sum_i W_{kl} |i\rangle_A \otimes |i\rangle_B$$

на усій системі. Але ж всі такі стани утворюють базис на $H_A \otimes H_B$, тому учасник B може застосувати відповідне вимірювання, щоб визначити числа k, l.

3. Квантова телепортація

В деякому сенсі квантова телепортація це процес, обернений до суперщільного кодування. Наша ціль – передати від учасника A до учасника B квантовий стан в розмірності d за допомогою пересилання $2\log_2(d)$ біт класичної інформації (без пересилання фізичної квантової системи).

Щодо вимірювання сплутаного стану

Нехай задано чистий сплутаний стан $|\phi\rangle$ на $H_1 \otimes H_2$:

$$|\phi\rangle = \frac{1}{\sqrt{d}} \sum_i \alpha_i |i\rangle |\psi_i\rangle.$$

І нехай ми проводимо локальне вимірювання першої системи, яке задано проекторами $P_i = |i\rangle\langle i|$. Новий стан на $H_1 \otimes H_2$ у випадку "i" буде

$$\frac{(P_i \otimes I)|\phi\rangle}{||(P_i \otimes I)|\phi\rangle||} = \frac{\alpha_i}{|\alpha_i|} |i\rangle|\psi_i\rangle \cong |i\rangle|\psi_i\rangle$$

І хоча не знаючі результат вимірювання редукований стан другої системи не зміниться, він, очевидно, зміниться на $|\psi_i\rangle$ коли ми дізнаємося результат "i".

Тобто, в деякому сенсі ми змінюємо квантовий стан другої системи передавши результат вимірювання "i", тобто передавши класичну інформацію.

Але це ще не телепортація.

Для телепортації розглянемо наступне.

Нехай учасники розділили максимально сплутаний стан

$$\frac{1}{\sqrt{d}}\sum_i |i\rangle_A \otimes |i\rangle_B \in H_A \otimes H_B.$$

І нехай учасник A має також чистий стан $|\phi\rangle_C \in H_C$, який хоче передати. Можна вважати, що вся система перебуває у стані

$$|\text{start}\rangle = |\phi\rangle_C \otimes \frac{1}{\sqrt{d}}\sum_i |i\rangle_A \otimes |i\rangle_B =$$

$$= \frac{1}{\sqrt{d}}\sum_i |\phi\rangle_C \otimes |i\rangle_A \otimes |i\rangle_B \in H_C \otimes H_A \otimes H_B.$$

Формально ми би могли застосувати унітраний оператор перестановки $\text{SWAP}_{CB} \in L(H_C \otimes H_B)$, який можна визначити через

$$\forall i, j : \text{SWAP}_{CB}|i\rangle_C|j\rangle_B = |j\rangle_C|i\rangle_B.$$

В результаті ми би отримали стан

$$|\text{end}\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle_C \otimes |i\rangle_A \otimes |\phi\rangle_B = \big(\frac{1}{\sqrt{d}}\sum_i |i\rangle_C \otimes |i\rangle_A\big) \otimes |\phi\rangle_B.$$

Але на практиці це неможливо бо системи C та B розділені між учасниками.

Теорема

Для будь-якого унітарного базису $\{W_{kl}\}$ *та* $\forall|\phi\rangle_C \in H_C$ *виконується:*

$$|\phi\rangle_C \otimes \frac{1}{\sqrt{d}}\sum_i |i\rangle_A|i\rangle_B =$$

$$= \frac{1}{d}\sum_{kl}\big(\frac{1}{\sqrt{d}}\sum_i W_{kl}|i\rangle_C|i\rangle_A\big) \otimes W_{kl}^{-1}|\phi\rangle_B$$

$$= \frac{1}{d}\sum_{kl}|\Psi_{kl}\rangle_{CA} \otimes W_{kl}^{-1}|\phi\rangle_B$$

Доведення.

Помножимо обидва вирази зліва на $\langle\Psi_{pq}| \otimes \langle r|$.

Для правого виразу маємо

$$\langle\Psi_{pq}| \otimes \langle r| \cdot \frac{1}{d}\sum_{kl}|\Psi_{kl}\rangle_{CA} \otimes W_{kl}^{-1}|\phi\rangle_B = \frac{1}{d}\langle r|W_{pq}^{-1}|\phi\rangle.$$

Для лівого виразу

$$\langle\Psi_{pq}| \otimes \langle r| \cdot |\phi\rangle_C \otimes \frac{1}{\sqrt{d}}\sum_i |i\rangle_A|i\rangle_B =$$

$$= \frac{1}{\sqrt{d}}\sum_j \langle j|W_{pq}^{-1} \otimes \langle j| \otimes \langle r| \cdot \frac{1}{\sqrt{d}}\sum_i |\phi\rangle_C|i\rangle_A|i\rangle_B =$$

$$= \frac{1}{d}\sum_i \langle i|W_{pq}^{-1}|\phi\rangle \otimes \langle r|i\rangle =$$

$$= \frac{1}{d}\langle r|W_{pq}^{-1}|\phi\rangle.$$

Використовуючи це твердження протокол телепортації полягає у наступному. Учасник A проводить вимірювання в системі $H_C \otimes H_A$, яке відповідає розкладу за базисом $\{ \frac{1}{\sqrt{d}}\sum_i W_{kl}|i\rangle_C|i\rangle_A \}$. В результаті визначаються числа k, l, які передаються учаснику B. Участник B застосовує оператор W_{kl} до свого стану, в результаті чого отримує стан $|\phi\rangle$.

Зауваження *Насправді, в точності такий же протокол підходить і для телепортації змішаного стану.*