Конструкция на Ozawa от статиите

[1998-O1] Ozawa M, On the Halting Problem for Quantum Turing Machines, 1066 (1998) 174-183

[1998-O2] Ozawa M, Quantum Nondemolition Monitoring of Universal Quantum Computers, Phys. Rev. Lett., Vol.80, No.3 (1998) 631-634

[2000-O] Ozawa M, Quantum Turing Machines: Local Transition, Preparation, Measurement, and Halting, Quantum Communication, Computing, and Measurement 2, Edts. Kumar et al. (2000) 241-248

[2000-NO] Nishimura H, Ozawa M, Quantum Oracles and Computational Complexity, 1166 2000 207-215

[2001-ON] Ozawa M, Nishimura H, Local Transition Functions of Quantum Turing Machines, Theoret. Informatics Appl. 34 (2000) 379–402

[2002-O] Ozawa M, Halting of Quantum Turing Machines, C.S. Calude et al. (Eds.): UMC 2002, LNCS 2509 (2002) 58-65

[2002-NO] Nishimura H, Ozawa M, Computational complexity of uniform quantum circuit families and quantum Turing machines, Theoretical Computer Science 276 (2002) 147–181

0. Техническа Лема (стандартна)

Нека $\mathcal{H}$ - хилбертово пространство,

U - унитарен оператор в $\mathcal{H}$,

Π - ортогонален проектор в $\mathcal{H}$ (проектира върху $\Pi\mathcal{H}$).

$\Pi^\perp = \uparrow - \Pi$ - ортогонален проектор върху ортогоналното допълнение $(\Pi\mathcal{H})^\perp = \Pi^\perp\mathcal{H}$ (така, $\mathcal{H} = \Pi\mathcal{H} \oplus \Pi^\perp\mathcal{H}$).

Да разгледаме следните условия

(1) $\Pi\mathcal{H}$ е U-инвариантно, т.е., $U(\Pi\mathcal{H}) \subseteq \Pi\mathcal{H}$;

(2) $\Pi^\perp\mathcal{H}$ е U-инвариантно;

(3) $U(\Pi\mathcal{H}) = \Pi\mathcal{H}$;

(4) $\Pi U = U\Pi$;

(5) $\Pi U \Pi = U\Pi$;

(6) $\Pi^\perp U \Pi^\perp = \Pi^\perp U$.

Тогава: (1) $\Leftrightarrow$ (5) $\Leftrightarrow$ (6);

(1) & (2) $\Leftrightarrow$ (3) $\Leftrightarrow$ (4).

Доказателство. (1) $\Rightarrow$ (5)) $\Pi U \Pi\Psi = U\Pi\Psi$ за $\forall \Psi \in \mathcal{H}$.

($\Pi U \Pi\Psi \in \Pi\mathcal{H}$; $U\Pi\Psi \in U(\Pi\mathcal{H}) \subseteq \Pi\mathcal{H}$)

(5) $\Rightarrow$ (1))

$\Psi \in \Pi\mathcal{H} \Rightarrow \Psi = \Pi\Psi. \Rightarrow U\Psi = U\Pi\Psi.$

$\Rightarrow \Pi(U\Psi) = U\Psi$, понеже $\Pi U\Psi = \Pi U \Pi\Psi = U\Pi\Psi = U\Psi.$

$\Rightarrow U\Psi \in \Pi\mathcal{H}$

(5) $\Rightarrow$ (6)) $\Pi^\perp U = \Pi^\perp U(\Pi + \Pi^\perp) = \Pi^\perp U\Pi + \Pi^\perp U \Pi^\perp$

$\Pi^\perp U\Pi = \Pi^\perp \Pi U \Pi$, $\Pi^\perp\Pi = 0$

$\Pi^\perp U \Pi^\perp = \Pi^\perp U \Pi^\perp \Pi$, $\Pi^\perp\Pi = 0$

(6) $\Rightarrow$ (5)) $U\Pi = (\Pi + \Pi^\perp)U\Pi = \Pi U\Pi + \Pi^\perp U\Pi$

$(3) \Rightarrow (1)\,\&\,(2)$) $(3) \Rightarrow (1)$ - очевидно. $(3) \Rightarrow (2)$ - понеже

$$\Psi \perp \Pi\mathcal{H} \;\Rightarrow\; U\Psi \perp U(\Pi\mathcal{H}) = \Pi\mathcal{H}.$$

$(1)\,\&\,(2) \Rightarrow (3)$) Защо $U(\Pi\mathcal{H}) \supseteq \Pi\mathcal{H}$? $\Leftrightarrow$ (2)

$$\Pi^\perp\mathcal{H} = (\Pi\mathcal{H})^\perp \supseteq U(\Pi\mathcal{H})^\perp = U(\Pi^\perp\mathcal{H}) \overset{\downarrow}{=} \Pi^\perp\mathcal{H}$$

$(1)\,\&\,(2) \Rightarrow (4)$) Имаме:

(1) $\Rightarrow \Pi U \Pi = U\Pi$.

(2) $\Rightarrow \Pi^\perp U \Pi^\perp = U\Pi^\perp$, т.е., $(\hat{1} - \Pi)U(\hat{1} - \Pi) = U(\hat{1} - \Pi)$

$$\Pi U = U\Pi \;\Leftarrow\; \cancel{U} - U\Pi - \cancel{U\Pi} + \cancel{\Pi U \Pi} = \cancel{U} - U\Pi$$

$(4) \Rightarrow (1)\,\&\,(2)$)

$\Pi U = U\Pi \;\Rightarrow\; \Pi U \Pi = U\Pi^2 = U\Pi. \Rightarrow (1).$

$\hookrightarrow \Pi^\perp U = U\Pi^\perp \Rightarrow \Pi^\perp U \Pi^\perp = U\Pi^\perp. \Rightarrow (2).$ □

(Контра)пример. а) (1) $\not\Rightarrow$ (2).

Нека $e_n \in \mathcal{H}$ за $n \in \mathbb{Z}$ е ортонормиран базис

Нека $Ue_n := e_{n+1}$, $\Pi\mathcal{H} := \overline{\mathrm{Span}\{e_n \mid n \geq 0\}}$

Тогава $U(\Pi\mathcal{H}) = \overline{\mathrm{Span}\{e_n \mid n \geq 1\}} \subseteq \overline{\mathrm{Span}\{e_n \mid n \geq 0\}} = \Pi\mathcal{H}$

Но $(\Pi\mathcal{H})^\perp = \Pi^\perp\mathcal{H} = \overline{\mathrm{Span}\{e_n \mid n < 0\}}$ и

$U(\Pi^\perp\mathcal{H}) = \overline{\mathrm{Span}\{e_n \mid n < 1\}} \not\subseteq \overline{\mathrm{Span}\{e_n \mid n < 0\}}$.

б) Но ако $\mathcal{H}$ е крайно-мерно, то (1) - (6) са еквивалентни:

понеже U е унитарен, то $\mathrm{Ker}\, U = 0$; тогава

$$\dim \Pi\mathcal{H} = \dim U(\Pi\mathcal{H}) \text{ и } U(\Pi\mathcal{H}) \subseteq \Pi\mathcal{H}$$

$$\Rightarrow U(\Pi\mathcal{H}) = \Pi\mathcal{H}$$

тоест, (1) $\Rightarrow$ (3).

Означение Когато $\mathcal{H}_1 \subseteq \mathcal{H}$ е U инвариантно, т.е., $U\mathcal{H}_1 \subseteq \mathcal{H}_1$

то ще пишем $\mathcal{H}_1$ (инв.) U

Възможно е: U (унит.) $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_1^{\perp}$, U (инв.) $\mathcal{H}_1$, U (инв.) $\mathcal{H}_1^{\perp}$

1. **Имаме** P - ортогонален проектор - "стоп-индикатор";
Q - ортогонален проектор - "(част от) изходни данни";
U - унитарен оператор - "изчислителна еволюция".

Предполагане: а) $PQ = QP$ - ортогонален проектор за "стоп-индикатор" & "(част от) изходни данни".

б) $U(PQ\mathcal{H}) \subseteq PQ\mathcal{H}$
$U(PQ^{\perp}\mathcal{H}) \subseteq PQ^{\perp}\mathcal{H}$
} при установени стоп-индикатор и изходни данни те повече не се променят от U

$\Rightarrow U(P\mathcal{H}) \subseteq P\mathcal{H}$, понеже $P\mathcal{H} = PQ\mathcal{H} \oplus PQ^{\perp}\mathcal{H}$.

Обща картина:

U (инв.) $P\mathcal{H}$ $\oplus$ U (инв.) $P^{\perp}\mathcal{H}$

U (унит.) $\mathcal{H} = PQ\mathcal{H} \oplus PQ^{\perp}\mathcal{H} \oplus P^{\perp}Q\mathcal{H} \oplus P^{\perp}Q^{\perp}\mathcal{H}$

(инв.) U, (инв.) U, (инв.) U, (инв.) U

2. Следствие ("тождества на Ozawa")

а) $PQU = UPQ + PQUP^{\perp}$, като

$UPQ\mathcal{H} \perp PQUP^{\perp}\mathcal{H}$

б) $PQU^n = U^nPQ + U^{n-1}PQUP^{\perp} + U^{n-2}PQ(UP^{\perp})^2 + \cdots$
$+ UPQ(UP^{\perp})^{n-1} + PQ(UP^{\perp})^n$

като $U^nPQ\mathcal{H}, U^{n-1}PQUP^{\perp}\mathcal{H}, U^{n-2}PQ(UP^{\perp})^2, \ldots,$
$UPQ(UP^{\perp})^{n-1}\mathcal{H}, PQ(UP^{\perp})^n$
са взаимно ортогонални

Доказателство. а) $PQUPQ^{\perp} = 0$: понеже $PQ^{\perp}\mathcal{H} \perp PQ\mathcal{H}$
и U - унитарен

$U(PQ^{\perp}\mathcal{H}) \perp U(PQ\mathcal{H}) \subseteq PQ\mathcal{H}$

$\Rightarrow 0 = PQUPQ^{\perp} = PQUP(\hat{1}-Q) = PQUP - PQUPQ$
$= PQUP - UPQ$

$\Rightarrow PQU = PQU(P+P^{\perp}) = \underbrace{PQUP}_{UPQ} + PQUP^{\perp}$

$UPQ\mathcal{H} \perp PQUP^{\perp}\mathcal{H}$, понеже

$\langle UPQ\mathcal{H} \mid PQUP^{\perp}\mathcal{H} \rangle$
$= \langle \underbrace{PQUPQ\mathcal{H}}_{UPQ} \mid \cancel{U}P^{\perp}\mathcal{H} \rangle$
$= 0$

б) $P^\perp U^k = P^\perp U U^{k-1} = P^\perp U P^\perp U^{k-1} = \dots = P^\perp (UP^\perp)^{k-1}$

$$PQU^n = PQUU^{n-1} = UPQU^{n-1} + PQUP^\perp U^{n-1}$$
$$= UPQU^{n-1} + PQ(UP^\perp)^n$$
$$= UPQUU^{n-2} + PQ(UP^\perp)^n$$
$$= U^2PQU^{n-2} + UPQUP^\perp U^{n-2} + PQ(UP^\perp)^n$$
$$= U^2PQU^{n-2} + UPQ(UP^\perp)^{n-1} + PQ(UP^\perp)^n$$
$$= \dots = U^nPQ + U^{n-1}PQUP^\perp + U^{n-2}PQ(UP^\perp)^2 + \dots$$
$$+ UPQ(UP^\perp)^{n-1} + PQ(UP^\perp)^n$$

като $U^nPQ\mathcal{H}, U^{n-1}PQUP^\perp\mathcal{H}, U^{n-2}PQ(UP^\perp)^2, \dots,$
$UPQ(UP^\perp)^{n-1}\mathcal{H}, PQ(UP^\perp)^n$

са взаимно ортогонални

защото на всяка стъпка от индукцията възниква разбиване $U^k PQUU^{n-k-1}\mathcal{H}$

унитарен $UPQ + PQUP^\perp$

взаимно ортогонални според а)

□

Забележка Ако $k = k_1 + k_2 + \dots + k_m$

то $P^\perp U^k = P^\perp U^{k_1} P^\perp U^{k_2} \dots P^\perp U^{k_m}$

3. Интерпретация

$$\|PQU^nP\Psi\|^2 = \|U^nPQ\Psi\|^2 = \|U^{n-1}PQUP^\perp\Psi\|^2$$

$$\|PQU^n\Psi\|^2 = \|PQ\Psi\|^2 + \|PQUP^\perp\Psi\|^2 + \cdots + \|PQ(UP^\perp)^n\Psi\|^2$$

вероятността за индикатор за спиране и краен резултат след n стъпки без мониторинг

$$= \sum_{k=0}^{n}$$

вероятността за индикатор за спиране и краен резултат за k стъпки с мониторинг на всяка стъпка

$$\|PQ(UP^\perp)^k\Psi\|^2 = \|U^{n-k}PQ(UP^\perp)^k\Psi\|^2$$

за $k_1 + \cdots + k_m = k-1$

$$\equiv \|PQUP^\perp U^{k_1} P^\perp U^{k_2} \ldots P^\perp U^{k_m}\Psi\|^2$$

- вероятността стоп-индикатора да сработи **точно** на k-тата стъпка, независимо дали е бил постоянен мониторинга

4. Обръщане хода на времето

U^* (унит.) $\mathcal{H} = PQ\mathcal{H} \oplus PQ^\perp\mathcal{H} \oplus P^\perp Q\mathcal{H} \oplus P^\perp Q^\perp\mathcal{H}$

$P\mathcal{H} \oplus P^\perp\mathcal{H}$

U^* (инв.) $P\mathcal{H}$; U^* (инв.) $P^\perp\mathcal{H}$

$PQ\mathcal{H}$: U^* (инв.) U ; $PQ^\perp\mathcal{H}$: U^* (инв.) U ; $P^\perp Q\mathcal{H}$: U^* (инв.) U ; $P^\perp Q^\perp\mathcal{H}$: U^* (инв.) U

защото към Лема 0 мога да добавя, че

$$\Pi U\Pi = U\Pi \iff \Pi U^*\Pi = \Pi U^*$$
$$\iff \Pi^\perp U\Pi^\perp = \Pi^\perp U \iff \Pi^\perp U^*\Pi^\perp = U^*\Pi^\perp$$