3.1 Định nghĩa các hàm $\square_1^{\text{QP}}$

Định nghĩa theo lược đồ của chúng tôi dẫn đến một lớp hàm đặc biệt, gọi là $\square_1^{\text{QP}}$ (trong đó $\square$ được đọc là "square"), nắm bắt các hàm lượng tử tính được trong thời gian đa thức ánh xạ từ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$; lớp này gồm một tập nhỏ các hàm lượng tử khởi đầu và bốn quy tắc xây dựng đặc biệt: hợp thành, hoán đổi, phân nhánh và đệ quy lượng tử đa qubit. Định nghĩa 3.1 trình bày hình thức chính thức cho định nghĩa theo lược đồ của chúng tôi.

Sau đây, ta nói rằng một hàm lượng tử f từ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$ là bảo toàn số chiều nếu, với mọi trạng thái lượng tử $|\phi\rangle \in \mathcal{H}_\infty$ và mọi số $n \in \mathbb{N}^+, |\phi\rangle \in \mathcal{H}_{2^n}$ kéo theo $f(|\phi\rangle) \in \mathcal{H}_{2^n}$ (tức là $\ell(|\phi\rangle) = \ell(f(|\phi\rangle))$).

Định nghĩa 3.1 Gọi $\square_1^{\text{QP}}$ là tập hợp tất cả các hàm lượng tử thu được từ các hàm lượng tử khởi đầu trong Lược đồ I bằng một số hữu hạn lần (kể cả 0 lần) áp dụng các quy tắc xây dựng II-IV lên các hàm lượng tử đã được xây dựng trước đó, trong đó các Lược đồ I-IV được cho như sau. Gọi $|\phi\rangle$ là một trạng thái lượng tử bất kỳ trong $\mathcal{H}_\infty$.
I. Các hàm lượng tử khởi đầu. Cho $\theta \in [0, 2\pi) \cap \tilde{\mathbb{C}}$ và $a \in \{0, 1\}$.

1. $I(|\phi\rangle) = |\phi\rangle$. (đồng nhất)
2. $PHASE_\theta(|\phi\rangle) = |0\rangle\langle 0 \mid \phi\rangle + e^{i\theta}|1\rangle\langle 1 \mid \phi\rangle$. (dịch pha)
3. $ROT_\theta(|\phi\rangle) = \cos\theta|\phi\rangle + \sin\theta(|1\rangle\langle 0 \mid \phi\rangle - |0\rangle\langle 1 \mid \phi\rangle)$. (quay quanh trục xy với góc θ)
4. $NOT(|\phi\rangle) = |0\rangle\langle 1 \mid \phi\rangle + |1\rangle\langle 0 \mid \phi\rangle$. (phủ định)
5. $SWAP(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{a,b\in\{0,1\}} |ab\rangle\langle ba \mid \phi\rangle & \text{otherwise.} \end{cases}$ (hoán đổi 2 qubit)
6. $MEAS[a](|\phi\rangle) = |a\rangle\langle a \mid \phi\rangle$. (đo chiếu từng phần)
   II. Quy tắc hợp thành. Từ g và h, ta định nghĩa Compo $[g, h]$ như sau:

Compo $[g, h](|\phi\rangle) = g \circ h(|\phi\rangle)(= g(h(|\phi\rangle)))$.
III. Quy tắc phân nhánh. Từ g và h, ta định nghĩa Branch $[g, h]$ như sau:
(i) Branch $[g, h](|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) \leq 1$,
(ii) Branch $[g, h](|\phi\rangle) = |0\rangle \otimes g(\langle 0 \mid \phi\rangle) + |1\rangle \otimes h(\langle 1 \mid \phi\rangle)$ ngược lại.
IV. Quy tắc đệ quy lượng tử đa qubit. Từ g, h, p bảo toàn số chiều, và $k, t \in \mathbb{N}^+$, ta định nghĩa $kQ\,\text{Rec}_t\,[g, h, p \mid \mathcal{F}_k]$ như sau:
(i) $kQ\,\text{Rec}_t\,[g, h, p \mid \mathcal{F}_k]\,(|\phi\rangle) = g(|\phi\rangle)$ nếu $\ell(|\phi\rangle) \leq t$,
(ii) $kQRec_t\,[g, h, p \mid \mathcal{F}_k]\,(|\phi\rangle) = h\left(\sum_{s:|s|=k} |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)\right)$ ngược lại,
trong đó $|\psi_{p,\phi}\rangle = p(|\phi\rangle)$ và $\mathcal{F}_k = \{f_s\}_{s\in\{0,1\}^k} \subseteq \{kQ\,\text{Rec}_t\,[g, h, p \mid \mathcal{F}_k]\,, I\}$. Để nhấn mạnh " k," chúng tôi gọi quy tắc này là đệ quy lượng tử k-qubit. Trong trường hợp $k = 1$, để ngắn gọn ta viết $Q\,\text{Rec}_t\,[g, h, p \mid f_0, f_1]$ thay cho $1QRec_t\,[g, h, p \mid \{f_0, f_1\}]$.

Trong Lược đồ I, $PHASE_\theta$ và ROT_θ lần lượt tương ứng với các ma trận $Z_{2,\theta}$ và R_θ đã cho ở Mục 2.3. Sau này, chúng tôi sẽ lập luận rằng góc θ trong $PHASE_\theta$ và ROT_θ có thể cố định thành $\pi/4$. Hàm lượng tử MEAS gắn với phép đo chiếu từng phần, trong cơ sở tính toán $\{0, 1\}$, áp dụng lên qubit đầu tiên của $|\phi\rangle$ khi $\ell(|\phi\rangle) \geq 1$, và hiển nhiên suy ra rằng $\ell(\text{ MEAS }[i](|\phi\rangle)) \leq \ell(|\phi\rangle)$.

Trước khi đi xa hơn, để giúp người đọc hiểu hành vi của các hàm lượng tử khởi đầu liệt kê trong Lược đồ I, chúng tôi minh họa ngắn gọn cách các hàm này biến đổi các qustring cơ bản độ dài 3. Với các bit $a, b, c, d \in \{0, 1\}$ với $d \neq a$, ta có $I(|abc\rangle) = |abc\rangle, PHASE_\theta\left(|abc\rangle = e^{i\theta a}|abc\rangle, ROT_\theta(|abc\rangle) = \cos\theta|abc\rangle + (-1)^a \sin\theta|\bar{a}bc\rangle, NOT(|abc\rangle) = |\bar{a}bc\rangle, SWAP(|abc\rangle) = |bac\rangle, MEAS[a](|abc\rangle) = |abc\rangle$, và $MEAS[d](|abc\rangle) = \mathbf{0}$, trong đó $\bar{a} = 1 - a$.

Lược đồ IV là lõi của định nghĩa $\square_1^{\text{QP}}$. Quy tắc đệ quy chuẩn dùng để định nghĩa một hàm đệ quy nguyên thủy f từ hai hàm g và h có dạng: $f(0, x) = g(x)$ và $f(n+1, x) = h(n, x, f(n, x))$ với mọi $n \in \mathbb{N}$. Quy tắc này cần một bộ đếm nội bộ (ở vị trí đối số thứ nhất của f) để điều khiển số lần lặp áp dụng h. Tuy nhiên, trong Lược đồ IV, chúng tôi không dùng bộ đếm như vậy. Thay vào đó, chúng tôi dùng chiến lược chia để trị để chia một trạng thái lượng tử đã cho theo từng qubit. Ở mỗi bước quy nạp, chúng tôi xử lý các trạng thái lượng tử ngắn hơn k-qubit cho đến khi trạng thái lượng tử có độ dài không quá t. Chúng tôi muốn đưa ra hai ví dụ cụ thể về cách Lược đồ IV hoạt động trong các trường hợp $k = 1, 2$. Lưu ý rằng trong trường hợp $k = 1$, Lược đồ IV trở thành quy tắc đệ quy lượng tử 1-qubit (hay đơn qubit) được mô tả như sau:
(i') $QRec_t\left[g, h, p \mid f_0, f_1\right](|\phi\rangle) = g(|\phi\rangle)$ nếu $\ell(|\phi\rangle) \leq t$,
(ii') $QRec_t\left[g, h, p \mid f_0, f_1\right](|\phi\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{p,\phi}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{p,\phi}\rangle\right)\right)$
ngược lại, trong đó mỗi hàm f_0 và f_1 phải là I hoặc $Q\,\text{Rec}_t\left[g, h, p \mid f_0, f_1\right]$.

Ví dụ 1. Trước hết xét trường hợp $k = 1$. Trong ví dụ này, ta đặt $t = 1, g = NOT, h = SWAP$, và $p = NOT$, đồng thời viết ngắn gọn F cho $QRec_1\left[NOT, SWAP, NOT \mid f_0, f_1\right]$ với $f_0 = I$ và $f_1 = F$. Cần lưu ý rằng $\mathbf{0}$ là một đối tượng đặc biệt và theo Bổ đề 3.4 (1), ta có $g(\mathbf{0}) = \mathbf{0}$ với mọi hàm lượng tử g. Gọi $|\phi\rangle$ là một trạng thái lượng tử bất kỳ trong $\mathcal{H}_\infty$ được đưa vào F.
(1) Giả sử $|\phi\rangle$ có độ dài 1 và có dạng tổng quát $\alpha|0\rangle + \beta|1\rangle$. Theo Bổ đề 3.4(2), chỉ cần xét cơ sở tính toán $B_1 = \{|0\rangle, |1\rangle\}$. Vì $\ell(|\phi\rangle) \leq t$, kết quả của f trên các qubit cơ sở $|0\rangle$ và $|1\rangle$ được tính như sau.
(i) $F(|0\rangle) = g(|0\rangle) = NOT(|0\rangle) = |1\rangle$.
(ii) $F(|1\rangle) = g(|1\rangle) = NOT(|1\rangle) = |0\rangle$.

Hiển nhiên $F(\mathbf{0}) = \mathbf{0}$. Vì $|\phi\rangle$ là chồng chập dạng $\alpha|0\rangle + \beta|1\rangle$, các tính toán trên lập tức suy ra

$$F(|\phi\rangle) = F(\alpha|0\rangle + \beta|1\rangle) = NOT(\alpha|0\rangle + \beta|1\rangle) = \alpha NOT(|0\rangle) + \beta NOT(|1\rangle) = \alpha|1\rangle + \beta|0\rangle.$$

(2) Tiếp theo, giả sử $|\phi\rangle$ có độ dài 2. Trong trường hợp $|\phi\rangle$ là trạng thái lượng tử cơ sở $|00\rangle$ trong $B_2 = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, ta có $|\psi_{p,\phi}\rangle = |\psi_{NOT,00}\rangle = NOT(|00\rangle) = |10\rangle$. Tương tự, nếu $|\phi\rangle$ lần lượt là $|01\rangle, |10\rangle$, và $|11\rangle$, thì trạng thái lượng tử $|\psi_{p,\phi}\rangle$ tương ứng là $|11\rangle, |00\rangle$, và $|01\rangle$. Liên quan đến phép đo chiếu từng phần, suy ra rằng với mọi bit $a \in \{0, 1\}$, $\langle 1 \mid 1a\rangle = |a\rangle, \langle 0 \mid 0a\rangle = |a\rangle, \langle 1 \mid 0a\rangle = \mathbf{0}$, và $\langle 0 \mid 1a\rangle = \mathbf{0}$. Cũng lưu ý rằng $I(\mathbf{0}) = \mathbf{0}$. Dùng các đẳng thức này cùng với $F(|0\rangle) = |1\rangle$ và $F(|1\rangle) = |0\rangle$ thu được ở (1), ta có thể tính kết quả $F(|\phi\rangle)$ như sau.
(i) $F(|00\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,00}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,00}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 10\rangle) + |1\rangle \otimes F(\langle 1 \mid 10\rangle)) = h($
$I(\mathbf{0}) + |1\rangle \otimes F(|0\rangle)) = h(|1\rangle \otimes F(|0\rangle)) = SWAP(|1\rangle \otimes |1\rangle) = SWAP(|11\rangle) = |11\rangle$.

[1] Hình thức hiện tại của các Lược đồ I-IV hiệu chỉnh những sai khác do hình thức ban đầu trong bản tóm tắt mở rộng 39 gây ra.

(ii) $F(|10\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,10}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,10}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 00\rangle) + |1\rangle \otimes F(\langle 1 \mid 00\rangle)) = h$
$I(|0\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|0\rangle)) = SWAP(|0\rangle \otimes |0\rangle) = SWAP(|00\rangle) = |00\rangle$.
(iii) $F(|01\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,01}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,01}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 11\rangle) + |1\rangle \otimes F(\langle 1 \mid 11\rangle)) = h$
$I(\mathbf{0}) + |1\rangle \otimes F(|1\rangle)) = h(|1\rangle \otimes F(|1\rangle)) = SWAP(|1\rangle \otimes |0\rangle) = SWAP(|10\rangle) = |01\rangle$.
(iv) $F(|11\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,11}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,11}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 01\rangle) + |1\rangle \otimes F(\langle 1 \mid 01\rangle)) = h$
$I(|1\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|1\rangle)) = SWAP(|0\rangle \otimes |1\rangle) = SAWP(|01\rangle) = |10\rangle$.

Theo Bổ đề 3.4 (2), chẳng hạn khi $|\phi\rangle$ có dạng $\alpha|00\rangle + \beta|10\rangle$, ta được

$$F(|\phi\rangle) = F(\alpha|00\rangle + \beta|10\rangle) = \alpha F(|00\rangle) + \beta F(|10\rangle) = \alpha|11\rangle + \beta|00\rangle.$$

(3) Xét trường hợp độ dài của $|\phi\rangle$ là 3. Với cơ sở tính toán $B_3 = \{|000\rangle, |001\rangle, |010\rangle, \ldots, |111\rangle\}$, ta chỉ tính các kết quả $F(|\phi\rangle)$ cho đầu vào $|\phi\rangle$ thuộc $\{|001\rangle, |101\rangle\}$. Lưu ý rằng $|\psi_{NOT,001}\rangle = |101\rangle$ và $|\psi_{NOT,101}\rangle = |001\rangle$. Nhắc lại từ (1)-(2) rằng $F(|01\rangle) = |01\rangle$ và $F(\mathbf{0}) = \mathbf{0}$.
(i) $F(|001\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,001}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,001}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 101\rangle) + |1\rangle \otimes F(\langle 1 \mid 101\rangle))$
$I(\mathbf{0}) + |1\rangle \otimes F(|01\rangle)) = h(|1\rangle \otimes F(|01\rangle)) = SWAP(|1\rangle \otimes |01\rangle) = SAWP(|101\rangle) =$
$|011\rangle$.
(ii) $F(|101\rangle) = h\left(|0\rangle \otimes f_0\left(\langle 0 \mid \psi_{NOT,101}\rangle\right) + |1\rangle \otimes f_1\left(\langle 1 \mid \psi_{NOT,101}\rangle\right) = h(|0\rangle \otimes I(\langle 0 \mid 001\rangle) + |1\rangle \otimes F(\langle 1 \mid 001\rangle)$
$I(|01\rangle) + |1\rangle \otimes F(\mathbf{0})) = h(|0\rangle \otimes I(|01\rangle)) = SWAP(|0\rangle \otimes |01\rangle) = SAWP(|001\rangle) =$
$|001\rangle$.

Chẳng hạn nếu $|\phi\rangle$ có dạng $\alpha|001\rangle + \beta|101\rangle$, Bổ đề 3.4(2) kéo theo $F(|\phi\rangle) = F(\alpha|001\rangle + \beta|101\rangle) = \alpha F(|001\rangle) + \beta F(|101\rangle) = \alpha|011\rangle + \beta|001\rangle$.

Ví dụ 2. Ta xét một ví dụ khác cho trường hợp $k = 2$. Chẳng hạn đặt $t = 3, g = NOT, h = SWAP$, và $p = NOT$, ta viết F cho $2QRec_3\left[NOT, SWAP, NOT \mid f_{00}, f_{01}, f_{10}, f_{11}\right]$ với $f_{00} = I$, $f_{01} = NOT$, $f_{10} = F$, và $f_{11} = F$. Gọi $|\phi\rangle$ là một trạng thái lượng tử bất kỳ trong $\mathcal{H}_\infty$.
(1) Khi độ dài của $|\phi\rangle$ không quá 3, ta lập tức có $F(|\phi\rangle) = g(|\phi\rangle) = NOT(|\phi\rangle)$. Ví dụ, $F(|0\rangle) = |1\rangle, F(|10\rangle) = |00\rangle$, và $F(|101\rangle) = |001\rangle$.
(2) Giả sử độ dài của $|\phi\rangle$ là 4, xét các trạng thái lượng tử cơ sở trong $B_4 = \{|0000\rangle, |0001\rangle, |0010\rangle, \ldots, |1111\rangle\}$. Ở đây, ta chỉ tập trung vào hai trường hợp: $|\phi\rangle \in \{|0101\rangle, |1011\rangle\}$. Ta lưu ý rằng $|\psi_{NOT,0010}\rangle = NOT(|0010\rangle) = |1010\rangle$ và $|\psi_{NOT,1011}\rangle = NOT(|1011\rangle) = |0011\rangle$.
(i) $F(|0010\rangle) = h\left(|00\rangle \otimes f_{00}\left(\langle 00 \mid \psi_{NOT,0010}\rangle\right) + |01\rangle \otimes f_{01}\left(\langle 01 \mid \psi_{NOT,0010}\rangle\right) + |10\rangle \otimes f_{10}\left(\langle 10 \mid \psi_{NOT,0010}\rangle\right) +$
$h(|00\rangle \otimes I(\langle 00 \mid 1010\rangle) + |01\rangle \otimes NOT(\langle 01 \mid 1010\rangle) + |10\rangle \otimes F(\langle 10 \mid 1010\rangle) + |11\rangle \otimes$
$F(\langle 11 \mid 1010\rangle)) = h(|00\rangle \otimes I(\mathbf{0}) + |01\rangle \otimes NOT(\mathbf{0}) + |10\rangle \otimes F(|10\rangle) + |11\rangle \otimes F(\mathbf{0})) =$
$h(|10\rangle \otimes F(|10\rangle)) = SWAP(|10\rangle \otimes |00\rangle) = SWAP(|1000\rangle) = |0100\rangle$.
(ii) $F(|1101\rangle) = h\left(|00\rangle \otimes f_{00}\left(\langle 00 \mid \psi_{NOT,1101}\rangle\right) + |01\rangle \otimes f_{01}\left(\langle 01 \mid \psi_{NOT,1101}\rangle\right) + |10\rangle \otimes f_{10}\left(\langle 10 \mid \psi_{NOT,1101}\rangle\right) +$
$h(|00\rangle \otimes I(\langle 00 \mid 0101\rangle) + |01\rangle \otimes NOT(\langle 01 \mid 0101\rangle) + |10\rangle \otimes F(\langle 10 \mid 0101\rangle) + |11\rangle \otimes$
$F(\langle 11 \mid 0101\rangle)) = h(|00\rangle \otimes I(\mathbf{0}) + |01\rangle \otimes NOT(|01\rangle) + |10\rangle \otimes F(\mathbf{0}) + |11\rangle \otimes F(\mathbf{0})) =$
$h(|01\rangle \otimes NOT(|01\rangle)) = SWAP(|01\rangle \otimes |11\rangle) = SWAP(|0111\rangle) = |1011\rangle$.

3.2 Một lớp con của $\square_1^{\text{QP}}$ và các tính chất cơ bản

Trong sáu hàm lượng tử khởi đầu của Lược đồ I, MEAS có hành vi khá khác biệt. Nó có thể thay đổi chuẩn cũng như số chiều của các trạng thái lượng tử, và điều đó khiến nó về bản chất là không khả nghịch. Vì lý do này, trong thực hành thường có lợi khi giới

hạn sự chú ý vào một lớp con của $\square_1^{\text{QP}}$, gọi là $\widehat{\square_1^{\text{QP}}}$, lớp này cấm hoàn toàn việc sử dụng MEAS.

Định nghĩa 3.2 Ký hiệu $\widehat{\square_1^{\text{QP}}}$ chỉ lớp con của $\square_1^{\text{QP}}$ được định nghĩa bởi các Lược đồ I-IV ngoại trừ MEAS trong Lược đồ I.

Không dùng MEAS trong Lược đồ I, mọi hàm lượng tử f trong $\widehat{\square_1^{\text{QP}}}$ đều bảo toàn số chiều của đầu vào; nói cách khác, f thỏa mãn $\ell(f(|\phi\rangle)) = \ell(|\phi\rangle)$ với mọi đầu vào $|\phi\rangle \in \mathcal{H}_\infty$.

Tiếp theo, ta minh họa cách xây dựng các cổng đơn vị điển hình bằng định nghĩa theo lược đồ của chúng tôi.

Bổ đề 3.3 Các hàm sau thuộc $\widehat{\square_1^{\text{QP}}}$. Gọi $|\phi\rangle$ là một phần tử bất kỳ trong $\mathcal{H}_\infty$.

1. $\text{CNOT}(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \le 1, \\ |0\rangle\langle 0 \mid \phi\rangle + |1\rangle \otimes NOT(\langle 1 \mid \phi\rangle) & \text{otherwise.} \end{cases}$ (controlled-NOT)
2. $Z_{1,\theta}(|\theta\rangle) = e^{i\theta}|0\rangle\langle 0 \mid \phi\rangle + |1\rangle\langle 1 \mid \phi\rangle$.
3. $zROT_\phi(|\phi\rangle) = e^{i\theta}|0\rangle\langle 0 \mid \phi\rangle + e^{-i\theta}|1\rangle\langle 1 \mid \phi\rangle$. (quay quanh trục z)
4. $GPS_\theta(|\phi\rangle) = e^{i\theta}|\phi\rangle$. (dịch pha toàn cục)
5. $WH(|\phi\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (\langle 0 \mid \phi\rangle + \langle 1 \mid \phi\rangle) + \frac{1}{\sqrt{2}}|1\rangle \otimes (\langle 0 \mid \phi\rangle - \langle 1 \mid \phi\rangle)$. (biến đổi Walsh-Hadamard)
6. $\text{CPHASE}_\theta(|\phi\rangle) = \begin{cases} |\phi\rangle \\ \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} \left(|0\rangle\langle b \mid \phi\rangle + e^{i\theta b}|1\rangle\langle b \mid \phi\rangle\right) \end{cases}$ if $\ell(|\phi\rangle) \le 1$, (controlled-PHASE)

Chứng minh. Chỉ cần xây dựng từng hàm lượng tử trong bổ đề từ các hàm lượng tử khởi đầu và bằng cách áp dụng các quy tắc xây dựng. Các hàm đích này được xây dựng như sau. (1) CNOT = Branch $[I, NOT]$. Lưu ý rằng khi $\ell(|\phi\rangle) \le 1$, Lược đồ III (i) suy ra $\text{CNOT}(|\phi\rangle) = |\phi\rangle$, khớp với Mục 1 của $CNOT$. (2) $Z_{1,\theta} = NOT \circ PHASE_\theta \circ NOT$. (3) $zROT_\theta = Z_{1,\theta} \circ PHASE_{-\theta}$. (4) $GPS_\theta = Z_{1,\theta} \circ PHASE_\theta$. (5) $WH = \text{ROT}_{\frac{\pi}{4}} \circ NOT$. (6) $CPHASE_\theta = \text{Branch}[WH, f]$, trong đó $f = \text{Branch}\,[I, GPS_\theta] \circ WH \circ NOT$.

Vì mọi hàm $\square_1^{\text{QP}}$-function f được xây dựng bằng cách áp dụng các Lược đồ I-IV, một lần áp dụng một trong các lược đồ được xem là một bước cơ bản của quá trình xây dựng để sinh ra f. Điều này giúp ta định nghĩa độ phức tạp mô tả của f là số lần tối thiểu dùng các lược đồ đó để xây dựng f. Ví dụ, mọi hàm khởi đầu đều có độ phức tạp mô tả bằng 1 vì chỉ dùng Lược đồ I một lần. Như đã minh họa trong chứng minh Bổ đề 3.3, các hàm lượng tử $CNOT, Z_{1,\theta}$, và WH có độ phức tạp mô tả nhiều nhất là 3, còn $zROT_\theta$ và GPS_θ nhiều nhất là 4, trong khi $CPHASE_\theta$ có độ phức tạp mô tả nhiều nhất là 15. Thước đo độ phức tạp này là thiết yếu khi chứng minh, chẳng hạn, Bổ đề 3.4 vì bổ đề sẽ được chứng minh bằng quy nạp theo độ phức tạp mô tả của hàm lượng tử đích. Ở Mục 6.2, chúng tôi sẽ thảo luận ngắn về thước đo độ phức tạp này cho nghiên cứu tương lai.

Các tính chất nền tảng của các hàm $\widehat{\square_1^{\text{QP}}}$ được nêu trong bổ đề sau. Một hàm lượng tử từ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$ được gọi là bảo toàn chuẩn nếu $\|f(|\phi\rangle)\| = \||\phi\rangle\|$ đúng với mọi trạng thái lượng tử $|\phi\rangle$ trong $\mathcal{H}_\infty$.

Bổ đề 3.4 Cho f là một hàm lượng tử bất kỳ trong $\widehat{\square_1^{\text{QP}}}$ và cho $|\phi\rangle, |\psi\rangle \in \mathcal{H}_\infty$ cùng $\alpha \in \mathbb{C}$.

1. $f(\mathbf{0}) = \mathbf{0}$, trong đó $\mathbf{0}$ là vectơ không.
2. $f(|\phi\rangle + |\psi\rangle) = f(|\phi\rangle) + f(|\psi\rangle)$.
3. $f(\alpha|\phi\rangle) = \alpha \cdot f(|\phi\rangle)$.
4. f bảo toàn số chiều và bảo toàn chuẩn.

Chứng minh. Gọi f là một hàm $\widehat{\square_1^{\text{QP}}}$ bất kỳ, gọi $|\phi\rangle, |\psi\rangle \in \mathcal{H}_\infty$, và gọi $\alpha \in \mathbb{C}$ cùng $\theta \in [0, 2\pi)$ là các hằng số. Như đã nói trước đó, ta chứng minh bổ đề bằng quy nạp theo độ phức tạp mô tả của f. Nếu f là một trong các hàm lượng tử khởi đầu của Lược đồ I, thì dễ kiểm tra rằng nó thỏa các Điều kiện $1-4$ của bổ đề. Đặc biệt, khi $|\phi\rangle$ là vectơ không $\mathbf{0}$, tất cả các biểu thức $e^{i\theta}|\phi\rangle, \cos\theta|\phi\rangle, \sin\theta|\phi\rangle, \langle 0 \mid \phi\rangle, \langle 1 \mid \phi\rangle$, và $\langle ba \mid \phi\rangle$ dùng trong Lược đồ I đều là $\mathbf{0}$; do đó, $|b\rangle \otimes \langle 1 \mid \phi\rangle$ và $|b\rangle \otimes \langle 0 \mid \phi\rangle$ cũng là $\mathbf{0}$ với mỗi bit $b \in \{0,1\}$. Vì vậy Điều kiện 1 được chứng minh.

Trong các Lược đồ II-IV, ta xét Lược đồ IV vì các lược đồ còn lại dễ chứng minh thỏa Điều kiện 1-4. Gọi g, h, và p là các hàm lượng tử trong $\widehat{\square_1^{\text{QP}}}$ và giả sử p bảo toàn số chiều. Theo giả thuyết quy nạp, giả sử g, h, và p thỏa Điều kiện $1-4$. Để dễ đọc, ta viết f cho $kQRec_t\left[g, h, p \mid \mathcal{F}_k\right]$. Trong phần sau, ta chỉ tập trung vào Điều kiện 2 và 4 vì các điều kiện còn lại dễ kiểm tra. Lập luận của ta sẽ dùng quy nạp theo độ dài đầu vào $|\phi\rangle$ đưa vào f.

(i) Mục tiêu là chứng minh f thỏa Điều kiện 2. Trước hết, xét trường hợp $\ell(|\phi\rangle) \leq t$. Khi đó suy ra $f(|\phi\rangle + |\xi\rangle) = g(|\phi\rangle + |\xi\rangle) = g(|\phi\rangle) + g(|\xi\rangle)$ vì giả sử g thỏa Điều kiện 2. Tiếp theo xét trường hợp $\ell(|\phi\rangle) > t$. Từ định nghĩa của f, ta có $f(|\phi\rangle + |\xi\rangle) = h\left(\sum_{s:|s|=k} |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi,\xi}\rangle\right)\right)$, trong đó $|\psi_{p,\phi,\xi}\rangle = p(|\phi\rangle + |\xi\rangle)$. Do $p(|\phi\rangle + |\xi\rangle) = p(|\phi\rangle) + p(|\xi\rangle)$ theo giả thuyết quy nạp, ta kết luận $\langle s \mid \psi_{p,\phi,\xi}\rangle = \langle s \mid \psi_{p,\phi}\rangle + \langle s \mid \psi_{p,\xi}\rangle$ với mỗi xâu $s \in \{0,1\}^k$. Theo giả thuyết quy nạp, suy ra $f_s\left(\langle s \mid \psi_{p,\phi,\xi}\rangle\right) = f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right) + f_s\left(\langle s \mid \psi_{p,\xi}\rangle\right)$, dẫn đến đẳng thức $|s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi,\xi}\rangle\right) = |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right) + |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\xi}\rangle\right)$. Dùng Điều kiện 2 cho h, ta thu được $h\left(\sum_{s:|s|=k} |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi,\xi}\rangle\right)\right) = \sum_{s:|s|=k} h(|s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)) + \sum_{s:|s|=k} h\left(|s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\xi}\rangle\right)\right)$. Từ đó kết luận $f(|\phi\rangle + |\xi\rangle) = f(|\phi\rangle) + f(|\xi\rangle)$.

(ii) Ta muốn chứng minh f thỏa Điều kiện 4. Theo giả thuyết quy nạp, với mọi $s \in \{0,1\}^k$, ta có $\|f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)\| = \|\langle s \mid \psi_{p,\phi}\rangle\|$ và $\|h(|\phi\rangle)\| = \||\phi\rangle\|$. Các đẳng thức này suy ra $\|f(|\phi\rangle)\|^2 = \|h\left(\sum_{s:|s|=k} |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)\right)\|^2 = \|\sum_{s:|s|=k} |s\rangle \otimes f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)\|^2 = \sum_{s:|s|=k} \| f_s\left(\langle s \mid \psi_{p,\phi}\rangle\right)\|^2$ bằng $\sum_{s:|s|=k} \|\langle s \mid \psi_{p,\phi}\rangle\|^2$. Hạng cuối cùng trùng với $\| |\psi_{p,\phi}\rangle \|^2$, mà bằng $\|p(|\phi\rangle)\|^2$. Điều này suy ra Điều kiện 4 vì $\|p(|\phi\rangle)\| = \||\phi\rangle\|$.

Bổ đề 3.4(4) chỉ ra rằng mọi hàm trong $\widehat{\square_1^{\text{QP}}}$ cũng đóng vai trò là các hàm ánh xạ từ Φ_∞ đến Φ_∞ thay vì từ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$.

Cho một hàm lượng tử g bảo toàn số chiều và bảo toàn chuẩn, nghịch đảo của g là một hàm lượng tử duy nhất f thỏa điều kiện rằng với mọi $|\phi\rangle \in \mathcal{H}_\infty$, $f \circ g(|\phi\rangle) = g \circ f(|\phi\rangle) = |\phi\rangle$. Hàm lượng tử đặc biệt này được ký hiệu là g^{-1}.

Mệnh đề tiếp theo đảm bảo rằng $\widehat{\square_1^{\text{QP}}}$ đóng dưới phép "nghịch đảo" vì $\widehat{\square_1^{\text{QP}}}$ không chứa MEAS.

Mệnh đề 3.5 Với mọi hàm lượng tử $g \in \widehat{\square_1^{\text{QP}}}$, g^{-1} tồn tại và thuộc $\widehat{\square_1^{\text{QP}}}$.

Chứng minh. Ta chứng minh mệnh đề này bằng quy nạp theo độ phức tạp mô tả của g đã nêu ở trên. Nếu g là một trong các hàm lượng tử khởi đầu, ta định nghĩa nghịch đảo của nó g^{-1} như sau: $I^{-1} = I, PHASE_\theta^{-1} = PHASE_{-\theta}, ROT_\theta^{-1} = ROT_{-\theta}, NOT^{-1} = NOT$, và $SWAP^{-1} = SWAP$. Nếu g được tạo từ một hoặc nhiều hàm lượng tử khác bằng một trong các quy tắc xây dựng, thì nghịch đảo của nó được định nghĩa là: Compo$[g,h]^{-1}$ = Compo $\left[h^{-1}, g^{-1}\right]$, Branch$[g,h]^{-1}$ = Branch $\left[g^{-1}, h^{-1}\right]$, và $kQRec_t\left[g,h,p \mid \{f_s\}_{s\in\{0,1\}^k}\right]^{-1} = kQRec_t\left[g^{-1}, p^{-1}, h^{-1} \mid \left\{f_s^{-1}\right\}_{s\in\{0,1\}^k}\right]$.

Việc chúng tôi chọn các Lược đồ I-IV được thúc đẩy bởi một tập cổng lượng tử phổ dụng cụ thể. Lưu ý rằng một lựa chọn khác về các hàm lượng tử khởi đầu và quy tắc xây dựng có thể dẫn đến một tập hàm $\square_1^{\text{QP}}$ khác. Lược đồ I dùng góc "tùy ý" θ trong $[0, 2\pi) \cap \widetilde{\mathbb{C}}$ để đưa vào $PHASE_\theta$ và ROT_θ; tuy nhiên, ta có thể giới hạn θ về giá trị duy nhất $\frac{\pi}{4}$ vì $PHASE_\theta$ và ROT_θ với giá trị tùy ý $\theta \in [0, 2\pi)$ có thể được xấp xỉ với độ chính xác mong muốn bằng WH và $Z_{2,\frac{\pi}{4}}$. Phần cuối này xuất phát từ thực tế là mọi toán tử đơn vị đơn qubit đều có thể được xấp xỉ đến độ chính xác bất kỳ từ các cổng lượng tử WH và $Z_{2,\frac{\pi}{4}}$ 6 (xem thêm 25). Để thảo luận thêm về lựa chọn các lược đồ, xem Mục 6.1.

3.3 Xây dựng các hàm lượng tử phức tạp hơn

Trước khi trình bày định lý chính (Định lý 4.1), chúng tôi muốn chuẩn bị các hàm lượng tử hữu ích và các quy tắc xây dựng mới suy ra trực tiếp từ các Lược đồ I-IV. Các hàm lượng tử và quy tắc xây dựng này sẽ được dùng cho chứng minh bổ đề then chốt của chúng tôi (Bổ đề 4.3), bổ đề hỗ trợ định lý chính.

Với mỗi $k \in \mathbb{N}^+$, ta giả sử thứ tự từ điển chuẩn $<$ trên $\{0,1\}^k$ và mọi phần tử trong $\{0,1\}^k$ được liệt kê theo từ điển là $s_1 < s_2 < \cdots < s_{2^k}$. Ví dụ, khi $k = 2$, ta có $00 < 01 < 10 < 11$. Với mỗi xâu $s \in \{0,1\}^n$, s^R ký hiệu xâu đảo của s; tức là $s^R = s_n s_{n-1} \cdots s_2 s_1$ nếu $s = s_1 s_2 \cdots s_{n-1} s_n$. Ta mở rộng khái niệm này cho trạng thái lượng tử như sau. Cho trạng thái lượng tử $|\phi\rangle \in \mathcal{H}_{2^n}$, xâu đảo của $|\phi\rangle$, ký hiệu $\left|\phi^R\right\rangle$, có dạng $\sum_{s:|s|=n}\langle s \mid \phi\rangle \otimes \left|s^R\right\rangle$, trong đó $\langle s \mid \phi\rangle$ chỉ là một vô hướng. Chẳng hạn, nếu $|\phi\rangle = \alpha|01\rangle + \beta|10\rangle$, thì $\left|\phi^R\right\rangle = \alpha|10\rangle + \beta|01\rangle$.

Bổ đề 3.6 Cho $k \in \mathbb{N}$ với $k \geq 2$, cho $g, h \in \widehat{\square_1^{\text{QP}}}$, và cho $\mathcal{G}_k = \left\{g_s \mid s \in \{0,1\}^k\right\}$ là một tập các hàm $\widehat{\square_1^{\text{QP}}}$. Các hàm lượng tử sau đều thuộc $\widehat{\square_1^{\text{QP}}}$. Bổ đề cũng đúng nếu thay $\widehat{\square_1^{\text{QP}}}$ bằng $\square_1^{\text{QP}}$.

Gọi $|\phi\rangle$ là một trạng thái lượng tử bất kỳ trong $\mathcal{H}_\infty$.

1. Compo $[\mathcal{G}_k]\left(|\phi\rangle\right) = g_{s_1} \circ g_{s_2} \circ \cdots \circ g_{s_{2^k}}\left(|\phi\rangle\right)$. (hợp thành nhiều hàm)

2. Switch $_k[g,h](|\phi\rangle) = g(|\phi\rangle)$ nếu $\ell(|\phi\rangle) < k$ và Switch $_k[g,h](|\phi\rangle) = h(|\phi\rangle)$ ngược lại. (chuyển mạch)

3. $LENGTH_k[g](|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) < k$ và $LENGTH_k[g](|\phi\rangle) = g(|\phi\rangle)$ ngược lại.

4. REMOVE $E_k(|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) < k$ và REMOVE $E_k(|\phi\rangle) = \sum_{s:|s|=k}\langle s \mid \phi\rangle \otimes |s\rangle$ ngược lại.

5. $REP_k(|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) < k$ và $REP_k(|\phi\rangle) = \sum_{s:|s|=n-k}\langle s \mid \phi\rangle \otimes |s\rangle$ ngược lại.

6. $SWAP_k(|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) < 2k$ và $SWAP_k(|\phi\rangle) = \sum_{s:|s|=k}\sum_{t:|t|=k}|st\rangle\langle ts \mid \phi\rangle$ ngược lại.

7. REVERSE$(|\phi\rangle) = \left|\phi^R\right\rangle$.

8. Branch$_k$ $[\mathcal{G}_k]$ $(|\phi\rangle) = |\phi\rangle$ nếu $\ell(|\phi\rangle) < k$ và Branch$_k$ $[\mathcal{G}_k]$ $(|\phi\rangle) = \sum_{s:|s|=k}|s\rangle \otimes g_s(\langle s \mid \phi\rangle)$ ngược lại.

9. RevBranch $_k$ $[\mathcal{G}_k]$ $(|\phi\rangle) = |\phi\rangle$ if $\ell(|\phi\rangle) < k$ and RevBranch $_k$ $[\mathcal{G}_k]$ $(|\phi\rangle) = \sum_{s:|s|=k} g_s\left(\sum_{u:|u|=n-k}\langle us \mid \phi\rangle \otimes |u\rangle\right) \otimes |s\rangle$ otherwise, trong đó $n = \ell(|\phi\rangle)$.
Sự khác nhau giữa $REMOVE_k$ và REP_k khá tinh tế nhưng $REMOVE_k$ dời k qubit đầu của đầu vào xuống cuối, còn REP_k dời k qubit cuối lên đầu. Chẳng hạn với các qustring cơ bản độ dài 4, ta có $REP_1(|a_1a_2a_3a_4\rangle) = |a_4a_1a_2a_3\rangle$ và $REMOVE_1(|a_1a_2a_3a_4\rangle) = |a_2a_3a_4a_1\rangle$. Tương tự, Branch$_k$ $[\mathcal{G}_k]$ áp dụng mỗi g_s trong $\mathcal{G}_k$ lên trạng thái lượng tử thu được từ $|\phi\rangle$ bằng cách loại bỏ k qubit đầu, trong khi RevBranch $_k$ $[\mathcal{G}_k]$ áp dụng g_s lên trạng thái lượng tử thu được bằng cách loại bỏ k qubit cuối, bất cứ khi nào $k \leq \ell(|\phi\rangle)$. Ví dụ, nếu $\mathcal{G}_k = \{h\}_{s\in\{0,1\}^k}$ cho một hàm lượng tử đơn h, thì với mọi xâu $s \in \{0,1\}^k$, ta có Branch$_k$ $[\mathcal{G}_k]$ $(|s\rangle|\phi\rangle) = |s\rangle\otimes h(|\phi\rangle)$ và RevBranch$_k$ $[\mathcal{G}_k]$ $(|\phi\rangle|s\rangle) = h(|\phi\rangle)\otimes|s\rangle$.

Chứng minh Bổ đề 3.6, Cho $k \in \mathbb{N}^+, g \in \widehat{\square_1^{\text{QP}}}$, và $\mathcal{G}_k = \left\{g_s \mid s \in \{0,1\}^k\right\} \subseteq \widehat{\square_1^{\text{QP}}}$. Với mỗi chỉ số $i \in [k]$, gọi s_i là phần tử thứ i theo thứ tự từ điển của $\{0,1\}^k$.

1. Trước hết đặt $f_{2^k} = g_{s_{2^k}}$ và định nghĩa quy nạp $f_{i-1} = \text{Compo}\left[g_{s_{i-1}}, f_i\right]$ với mọi chỉ số $i \in \left[2, 2^k\right]_{\mathbb{Z}}$ để thu được $f_1 = \text{Compo}\,[\mathcal{G}_k]$. Hàm lượng tử nhận được f_1 hiển nhiên thuộc $\widehat{\square_1^{\text{QP}}}$ vì k là hằng số cố định độc lập với đầu vào của f_1.

2. Đây là một trường hợp đặc biệt của quy tắc đệ quy lượng tử đơn qubit (hay quy tắc đệ quy lượng tử 1-qubit), trong đó $t = k-1, p = I$, và $f_0 = f_1 = I$. Vì vậy, Switch $[g,h]$ thuộc $\widehat{\square_1^{\text{QP}}}$.

3. Vì $LENGTH_k[g] =$ Switch $_k[I,g], LENGTH_k$ thuộc $\widehat{\square_1^{\text{QP}}}$.

4. Ta bắt đầu với trường hợp $k = 1$. Hàm lượng tử cần tìm $REMOVE_1$ được định nghĩa là

$$\text{REMOVE}_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ \sum_{a\in\{0,1\}} |a\rangle \otimes \text{REMOV } E_1 \left(\langle a \mid \psi_{SWAP,\phi}\rangle\right) & \text{otherwise }, \end{cases}$$

Chính thức hơn, ta đặt $REMOVE_1 = QRec_1\left[I, I, SWAP \mid REMOVE_1, REMOVE_1\right]$. Với trường hợp $k = 2$, ta định nghĩa $REMOVE_2 = REMOVE_1 \circ REMOVE_1$. Với mỗi chỉ số $k \geq 3, REMOVE_k$ được thu được như sau. Gọi h'_k là k phép hợp thành của $REMOVE_1$ và định nghĩa $REMOVE_k$ là $LENGTH_k\left[h'_k\right]$. Ta lưu ý rằng $LENGTH_k$ là cần thiết trong định nghĩa vì h'_k không được đảm bảo bằng $REMOVE_k$ khi $\ell(|\phi\rangle) \leq k - 1$.
5) Trước tiên, ta định nghĩa REP_1 là $REP_1 = QRec_1\left[I, SWAP, I \mid REP_1, REP_1\right]$, tức là,

$$REP_1(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1 \\ \sum_{a\in\{0,1\}} SWAP\left(|a\rangle \otimes REP_1(\langle a \mid \phi\rangle)\right) & \text{otherwise.} \end{cases}$$

Hiển nhiên, REP_1 thuộc $\widehat{\square_1^{\text{QP}}}$. Với chỉ số tổng quát $k > 1$, ta định nghĩa REP_k theo cách sau. Trước hết đặt h'_k là k phép hợp thành của REP_1. Cuối cùng đặt $REP_k = LENGTH_k\left[h'_k\right]$.
6) Trước hết ta hiện thực một hàm lượng tử $SWAP_{i,i+j}$, hoán đổi qubit thứ i và qubit thứ $(i+j)$ của mọi đầu vào. Mục tiêu này đạt được bằng cách xây dựng quy nạp $SWAP_{i,i+j}$ như sau. Ban đầu đặt $SWAP_{i,i+1} = REP_{i-1} \circ SWAP \circ REMOVE_{i-1}$. Với mọi chỉ số $j \in [k - i]$, định nghĩa $SWAP_{i,i+j} = SWAP_{i+j-1,i+j} \circ SWAP_{i,i+j-1} \circ SWAP_{i+j-1,i+j}$. Sau đó đặt $g = SWAP_{k,2k} \circ SWAP_{k-1,2k-1} \circ \cdots \circ SWAP_{2,k+2} \circ SWAP_{1,k+1}$. Cuối cùng, chỉ cần định nghĩa $SWAP_k$ là $LENGTH_{2k}[g]$.
7) Hàm lượng tử cần tìm REVERSE có thể được định nghĩa là REVERSE = QRec $_1$ [I , REMOV E_1, I | REVERSE, REVERSE], tức là,

$$REVERSE(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1 \\ REMOVE_1\left(\sum_{a\in\{0,1\}}(|a\rangle \otimes REVERSE(\langle a \mid \phi\rangle))\right) & \text{otherwise.} \end{cases}$$

8. Lưu ý rằng khi $k = 2$, Branch$_k$ $[\mathcal{G}_k]$ trùng với Branch và do đó thuộc $\widehat{\square_1^{\text{QP}}}$. Từ đây giả sử $k \geq 3$. Với mỗi xâu $s \in \{0,1\}^k$, đặt $g_s^{(0)} = g_s$. Với mỗi chỉ số $i \in \mathbb{N}$ thỏa $i < k$ và mỗi xâu $s \in \{0,1\}^*$ với $|s| = k - i - 1$, ta định nghĩa quy nạp $g_s^{(i+1)}$ là Branch $\left[g_{s0}^{(i)}, g_{s1}^{(i)}\right]$, tức là,

$$g_s^{(i+1)}(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle \leq 1, \\ |0\rangle \otimes g_{s0}^{(i)}(\langle 0 \mid \phi\rangle) + |1\rangle \otimes g_{s1}^{(i)}(\langle 1 \mid \phi\rangle) & \text{otherwise .} \end{cases}$$

Cuối cùng, ta đặt Branch$_k$ $[\mathcal{G}_k] = g_\lambda^{(k)}$, trong đó λ là xâu rỗng.
9) Giả sử $k \geq 2$, đặt RevBranch$_k$ $\left[\{g_s\}_{s\in\{0,1\}^k}\right]$ = REMOVE $E_k \circ$Branch$_k$ $\left[\{g_s\}_{s\in\{0,1\}^k}\right] \circ$ REP_k.

Bổ đề kế tiếp cho thấy ta có thể mở rộng mọi song ánh cổ điển trên $\{0,1\}^k$ thành hàm $\widehat{\square_1^{\text{QP}}}$ liên kết của nó, hàm này hành xử đúng hệt song ánh đó trên k bit đầu của đầu vào.

Bổ đề 3.7 Cho k là một hằng trong $\mathbb{N}^+$. Với mọi song ánh f từ $\{0,1\}^k$ đến $\{0,1\}^k$, tồn tại một hàm $\square_1^{\text{QP}}$ g_f sao cho, với mọi trạng thái lượng tử $|\phi\rangle \in \mathcal{H}_\infty$,

$$g_f(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq k-1, \\ \sum_{s\in\{0,1\}^k} |f(s)\rangle\langle s \mid \phi\rangle & \text{otherwise .} \end{cases}$$

Chứng minh. Cho một song ánh f trên $\{0,1\}^k$, chỉ cần chỉ ra tồn tại hàm $\widehat{\square_1^{\text{QP}}}$ h thỏa $h(|s\rangle|\phi\rangle) = |f(s)\rangle|\phi\rangle$ với mọi xâu $s \in \{0,1\}^k$ và mọi trạng thái lượng tử $|\phi\rangle \in \mathcal{H}_\infty$, vì g_f được thu từ h chỉ bằng cách đặt $g_f = LENGTH_k[h]$. Lưu ý rằng nếu $h \in \widehat{\square_1^{\text{QP}}}, h(\mathbf{0}) = \mathbf{0}$ khiến $g_f(\mathbf{0})$ bằng $\mathbf{0}$.

Một song ánh trên $\{0,1\}^k$ về bản chất là một hoán vị trên $\{s_1, s_2, \ldots, s_{2^k}\}$, trong đó mỗi s_i là xâu thứ i theo thứ tự từ điển trong $\{0,1\}^k$, và do đó có thể biểu diễn thành tích của một số hữu hạn phép hoán vị đổi chỗ, mỗi phép đổi chỗ hoán đổi hai số phân biệt. Việc này có thể thực hiện bằng cách áp dụng hợp thành nhiều lần của các $SWAP_{i,i+j}$ tương ứng, được định nghĩa trong chứng minh Bổ đề 3.6(6). Do đó, h thuộc $\widehat{\square_1^{\text{QP}}}$.

Cho một trạng thái lượng tử $|\phi\rangle$, ta có thể đồng thời áp dụng một hàm lượng tử f lên k qubit đầu của $|\phi\rangle$ và một hàm lượng tử khác g lên phần còn lại.

Bổ đề 3.8 Với $f, g \in \widehat{\square_1^{\text{QP}}}$ và $k \in \mathbb{N}^+$, hàm lượng tử $f^{\leq k} \otimes g$, được định nghĩa bởi

$$\left(f^{\leq k} \otimes g\right)(|\phi\rangle) = \begin{cases} f(|\phi\rangle) & \text{if } \ell(|\phi\rangle) \leq k \\ \sum_{s\in\{0,1\}^k} f(|s\rangle) \otimes g(\langle s \mid \phi\rangle) & \text{otherwise} \end{cases}$$

thuộc $\widehat{\square_1^{\text{QP}}}$. Ta ký hiệu g này là Skip $[f]$.

Chứng minh. Cho hàm lượng tử f, ta giới hạn việc áp dụng f lên k qubit cuối của mọi đầu vào $|\phi\rangle$ bằng cách đặt $f' = QRec_k\,[f, I, I \mid f_0, f_1]$, trong đó f_0 và f_1 đều là f'. Suy ra $f'(|\phi\rangle|s\rangle) = |\phi\rangle \otimes f(|s\rangle)$ với mọi $|\phi\rangle \in \mathcal{H}_\infty$ và $s \in \{0,1\}^k$.

Đặt $h = REP_k \circ f' \circ REMOVE_k$. Hàm lượng tử này h thỏa $h(|s\rangle|\phi\rangle) = f(|s\rangle) \otimes |\phi\rangle$ với mọi $s \in \{0,1\}^k$. Sau đó ta định nghĩa $\mathcal{G}_k = \{g_s\}_{s\in\{0,1\}^k}$ với $g_s = g$ cho mọi xâu $s \in \{0,1\}^k$ và đặt $g' = h \circ \text{Branch}_k\,[\mathcal{G}_k]$. Khi đó suy ra hàm lượng tử cần tìm $f^{\leq k} \otimes g$ bằng $\text{Switch}_{k+1}\,[f, g']$.

Tiếp theo, ta trình bày Bổ đề 3.9, hữu ích cho chứng minh bổ đề then chốt của chúng tôi (Bổ đề 4.3) ở Mục 5. Bổ đề này cho phép ta bỏ qua, trước khi áp dụng một hàm lượng tử cho trước, một số lượng tùy ý các số 0 cho đến khi đọc được một số lượng cố định các số 1.

Bổ đề 3.9 Cho f là một hàm lượng tử trong $\widehat{\square_1^{\text{QP}}}$ và cho k là một hằng trong $\mathbb{N}^+$. Tồn tại một hàm lượng tử g trong $\widehat{\square_1^{\text{QP}}}$ sao cho $g\left(\left|0^m 1^k\right\rangle \otimes |\phi\rangle\right) = \left|0^m 1^k\right\rangle \otimes f(|\phi\rangle)$ và $g\left(\left|0^{m+1}\right\rangle\right) = \left|0^{m+1}\right\rangle$ với mọi số $m \in \mathbb{N}$ và mọi trạng thái lượng tử $|\phi\rangle \in \mathcal{H}_\infty$. Bổ đề cũng đúng khi thay $\widehat{\square_1^{\text{QP}}}$ bằng $\square_1^{\text{QP}}$.

Chứng minh. Cho $k \geq 2$. Với hàm lượng tử $f \in \widehat{\square_1^{\text{QP}}}$, trước hết ta mở rộng f thành f' sao cho $f'\left(\left|1^{k-1}\right\rangle |\phi\rangle\right) = \left|1^{k-1}\right\rangle \otimes f(|\phi\rangle)$ với mọi $|\phi\rangle \in \mathcal{H}_\infty$ và $f'\left(\left|0^{m+1}\right\rangle\right) =$

$\left|0^{m+1}\right\rangle$ với mọi $m \in \mathbb{N}$. Hàm lượng tử f' này có thể thu được theo quy nạp như sau. Ta đặt $f_{k-1} = \text{Branch}[I, f], f_i = \text{Branch}\,[I, f_{i+1}]$ với mỗi $i \in [k-2]$, và
cuối cùng định nghĩa f' là f_1. Khi $k = 1$, ta đơn giản đặt $f' = f$. Hàm lượng tử cần tìm g trong bổ đề phải thỏa

$$g(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) \leq 1, \\ |0\rangle \otimes f'(g(\langle 0 \mid \phi\rangle)) + |1\rangle\langle 1 \mid \phi\rangle & \text{otherwise .} \end{cases}$$

Hàm g này được định nghĩa hình thức là $g = QRec_1\left[I, \text{Branch}\left[f', I\right], I \mid g, I\right]$. Điều này hoàn tất chứng minh.
Trong khuôn khổ của chúng tôi, có thể xây dựng một dạng "hạn chế" của biến đổi Fourier lượng tử (QFT). Cho xâu nhị phân $s = s_1 s_2 \cdots s_k$ độ dài k với $s_i \in \{0, 1\}$, ta ký hiệu $num(s)$ là số nguyên có dạng $\sum_{i=1}^{k} s_i 2^{k-i}$. Chẳng hạn, $\text{num}(011) = 1 \cdot 2^1 + 1 \cdot 2^0 = 5$ và $\text{num}(1010) = 1 \cdot 2^3 + 1 \cdot 2^1 = 10$. Hơn nữa, gọi $\omega_k = e^{2\pi i/2^k}$, trong đó $i = \sqrt{-1}$.

Bổ đề 3.10 Cho k là một hằng cố định bất kỳ trong $\mathbb{N}^+$. Biến đổi Fourier lượng tử k-qubit sau thuộc $\widehat{\square_1^{\text{QP}}}$. Với mọi phần tử $|\phi\rangle$ trong $\mathcal{H}_\infty$, gọi

$$F_k(|\phi\rangle) = \begin{cases} |\phi\rangle & \text{if } \ell(|\phi\rangle) < k \\ \frac{1}{2^{k/2}} \sum_{t:|t|=k} \sum_{s:|s|=k} \omega_k^{\text{num }(s)\text{ num }(t)} |s\rangle\langle t \mid \phi\rangle & \text{otherwise} \end{cases}$$

Chứng minh. Khi $k = 1, F_1$ trùng với WH và do đó F_1 thuộc $\widehat{\square_1^{\text{QP}}}$ theo Bổ đề 3.3. Tiếp theo, giả sử $k \geq 2$. Đã biết rằng, với mọi $x_1, x_2, \ldots, x_k \in \{0, 1\}$,

$$F_k\left(|x_1 x_2 \cdots x_k\rangle\right) = \frac{1}{2^{k/2}} \left(|0\rangle + \omega_1^{x_k}|1\rangle\right) \left(|0\rangle + \omega_1^{x_{k-1}} \omega_2^{x_k}|1\rangle\right) \cdots \left(|0\rangle + \prod_{i=1}^{k} \omega_i^{x_i}|1\rangle\right). \tag{1}$$

Về sự kiện này và chứng minh của nó, xem chẳng hạn 25.
Hãy nhắc lại hàm lượng tử đặc biệt $SWAP_{i,i+j}$ trong chứng minh Bổ đề 3.6(6), hàm này hoán đổi giữa qubit thứ i và qubit thứ j. Dùng $CPHASE_\theta$, với mọi cặp chỉ số i, j thỏa $i < j$, ta định nghĩa $CPHASE_\theta^{(i,j)}$ là $SWAP_{1,i} \circ SWAP_{2,j} \circ CPHASE_\theta \circ SWAP_{2,j} \circ SWAP_{1,i}$, trong đó ta áp dụng $CPHASE_\theta$ lên qubit thứ i và qubit thứ j. Trước hết ta muốn xây dựng $G_k^{(1)} = F_k \circ REVERSE$, hàm này hoạt động tương tự F_k nhưng nhận $\left|\phi^R\right\rangle$ làm đầu vào. Để đạt mục tiêu đó, ta định nghĩa quy nạp $\left\{G_j^{(i)}\right\}_{i,j \in \mathbb{N}^+}$ như sau. Ban đầu đặt $G_0^{(i)} = I$ với mọi $i \in \mathbb{N}^+$. Tiếp theo, định nghĩa $G_1^{(i)}$ là $G_1^{(i)} = H$ nếu $i = 1$, và $G_1^{(i)} = REP_{i-1} \circ H \circ REMOVE_{i-1}$ ngược lại. Với mọi chỉ số $k \geq 2, G_k^{(i)}$ được định nghĩa là $G_{k-1}^{(i)} \circ CPHASE_{\frac{\pi}{2^{k-1}}}^{(i,i+k-1)} \circ \left(G_{k-2}^{(i)}\right)^{-1} \circ G_{k-1}^{(i+1)}$. Không khó để chỉ ra rằng $G_k^{(1)}$ trùng với $F_k \circ REVERSE$ theo Eqn. (1).

Vì $G_k^{(1)} = F_k \circ REVERSE$, chỉ cần định nghĩa F_k là $G_k^{(1)} \circ REVERSE$.
Dạng QFT tổng quát, trong đó k không bị giới hạn là một hằng số cụ thể, sẽ được bàn ở Mục 6.1 liên hệ với lựa chọn các Lược đồ I-IV tạo thành lớp hàm $\square_1^{\text{QP}}$.

4 Các đóng góp chính

Trong Mục 3.1, chúng tôi đã giới thiệu các hàm $\Box_1^{\mathrm{QP}}$ và các hàm $\widehat{\Box_1^{\mathrm{QP}}}$ ánh xạ từ $\mathcal{H}_\infty$ đến $\mathcal{H}_\infty$ bằng cách áp dụng các Lược đồ I-IV hữu hạn lần. Định lý chính của chúng tôi (Định lý 4.1) khẳng định rằng $\Box_1^{\mathrm{QP}}$ có thể đặc trưng chính xác mọi hàm trong FBQP ánh xạ từ $\{0,1\}^*$ đến $\{0,1\}^*$, và do đó đặc trưng mọi ngôn ngữ trong BQP trên $\{0,1\}$ bằng cách đồng nhất ngôn ngữ với hàm đặc trưng tương ứng của nó. Định lý này sẽ được chứng minh bằng hai bổ đề then chốt, Bổ đề 4.244 .3 .

4.1 Một đặc trưng mới của FBQP

Mục tiêu của chúng tôi là chứng minh sức mạnh của các hàm $\Box_1^{\mathrm{QP}}$ (và do đó của các hàm $\widehat{\Box_1^{\mathrm{QP}}}$) bằng cách chỉ ra trong Định lý 4.1 rằng các hàm $\Box_1^{\mathrm{QP}}$ (cũng như các hàm $\widehat{\Box_1^{\mathrm{QP}}}$) đặc trưng chính xác các hàm FBQP trên $\{0,1\}^*$. Để làm điều này, không may là có hai khó khăn lớn cần vượt qua.

Khó khăn thứ nhất nảy sinh khi xử lý các ký hiệu băng của QTM chỉ bằng qubit. Lưu ý rằng các QTM làm việc trên bảng chữ cái đầu vào không nhị phân đã được biết là có thể mô phỏng bằng các QTM nhận bảng chữ cái đầu vào nhị phân $\{0,1\}$. Ngay cả khi ta giảm thành công kích thước bảng chữ cái đầu vào xuống 2, trên thực tế, mô phỏng các QTM như vậy vẫn phải đòi hỏi xử lý đúng các ký hiệu băng không nhị phân, đặc biệt là ký hiệu phân biệt