ĐẠI HỌC QUỐC GIA TPHCM

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

Bài tập 3

Đề tài: Vướng lượng tử & Các thuật toán truy vấn lượng tử

Môn học: Nhập môn Tính toán lượng tử

Sinh viên thực hiện:

Lưu Thượng Hồng (23122006)

Giáo viên hướng dẫn:

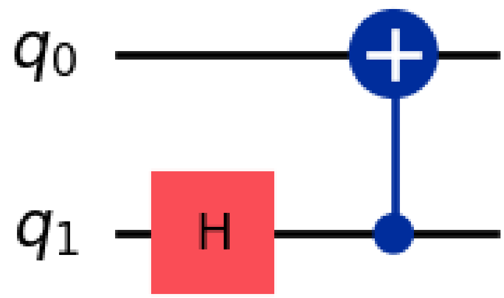
ThS. Vũ Quốc Hoàng

Ngày 3 tháng 12 năm 2025

Mục lục

1 Bài 1

Bài làm trong Jupyter Notebook



Hình 1: Mạch lượng tử tạo trạng thái Bell từ trạng thái cơ sở tính toán

```
# Tính toán
inputs = ["00", "01", "10", "11"]

for inp in inputs:
    qc = QuantumCircuit(2)

    # 1. Khởi tạo trạng thái đầu vào
    # Nếu bit là '1', ta dùng cổng X để lật |0> thành |1>
    if inp[0] == "1":
        qc.x(1)
    if inp[1] == "1":
        qc.x(0)

    # 2. Áp dụng mạch H + CNOT
    qc.h(1)  # H lên qubit 1
    qc.cx(1, 0)  # CNOT (control=1, target=0)

    # 3. Xem kết quả
    state = Statevector(qc)
    pretty_output = format_state(state)
```

```
    print(f"|{inp}>       | {pretty_output}")
```

Listing 1: "Cài đặt mạch lượng tử tạo trạng thái Bell trên Qiskit"

Kết quả:

Input	Output
$\|00\rangle$	$(0.707+0j)\|00\rangle + (0.707+0j)\|11\rangle$
$\|01\rangle$	$(0.707+0j)\|01\rangle + (0.707+0j)\|10\rangle$
$\|10\rangle$	$(0.707+0j)\|00\rangle + (-0.707+0j)\|11\rangle$
$\|11\rangle$	$(0.707+0j)\|01\rangle + (-0.707+0j)\|10\rangle$

Mạch lượng tử này chuyển đổi trạng thái cơ sở tính toán sang trạng thái Bell, tức là tạo ra sự vướng víu giữa hai qubit đầu vào.

2 Bài 2

2.1 Câu a

Một hàm logic là khả nghịch nếu nó là một song ánh.
Quan sát bảng ta thấy không có hàng nào trùng output, do đó hàm này là một song ánh và khả nghịch.

2.2 Câu b

Ta tìm hàm Boolean cho D, E, F theo A, B, C.

- F bằng 1 tại $(0,0,1), (0,1,1), (1,0,1), (1,1,0)$. Ta có biểu thức:

$$\begin{aligned} F &= \overline{A}\overline{B}C + \overline{A}BC + A\overline{B}C + AB\overline{C} \\ &= \overline{A}C + \overline{B}C + AB\overline{C} \\ &= AB \oplus C \end{aligned}$$

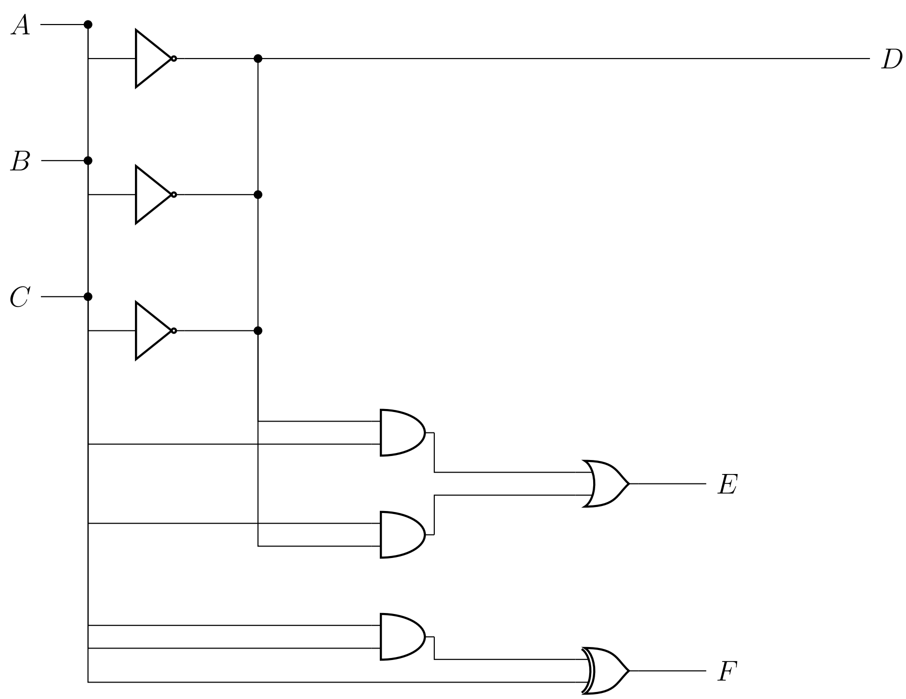
- E bằng 1 tại $(0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 1, 0)$. Ta có biểu thức:

$$\begin{aligned} E &= \overline{A}B\overline{C} + \overline{A}BC + A\overline{B}\overline{C} + AB\overline{C} \\ &= \overline{A}B + A\overline{C} \end{aligned}$$

- D bằng 1 tại $(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1)$. Ta có biểu thức:

$$\begin{aligned} D &= \overline{A}\overline{B}\overline{C} + \overline{A}\overline{B}C + \overline{A}B\overline{C} + \overline{A}BC \\ &= \overline{A} \end{aligned}$$

Ta có mạch logic:



2.3 Câu c

Dựa trên các hàm Boolean đã rút gọn ở câu b:

- $D = \overline{A}$
- $E = \overline{A}B + A\overline{C}$
- $F = AB \oplus C$

Ta thiết kế mạch lượng tử sử dụng 3 qubit đầu vào $|A\rangle, |B\rangle, |C\rangle$ (ký hiệu q_0, q_1, q_2) và 3 qubit đầu ra $|D\rangle, |E\rangle, |F\rangle$ (ký hiệu q_3, q_4, q_5) được khởi tạo ở trạng thái $|0\rangle$.
Quy trình thực hiện trên mạch (sử dụng các cổng X, CNOT, Toffoli):

1. **Tính F:** Sử dụng cổng Toffoli với điều khiển q_0, q_1 lên q_5 (tạo AB), sau đó dùng CNOT từ q_2 lên q_5 (tạo $AB \oplus C$).

2. **Tính E:**

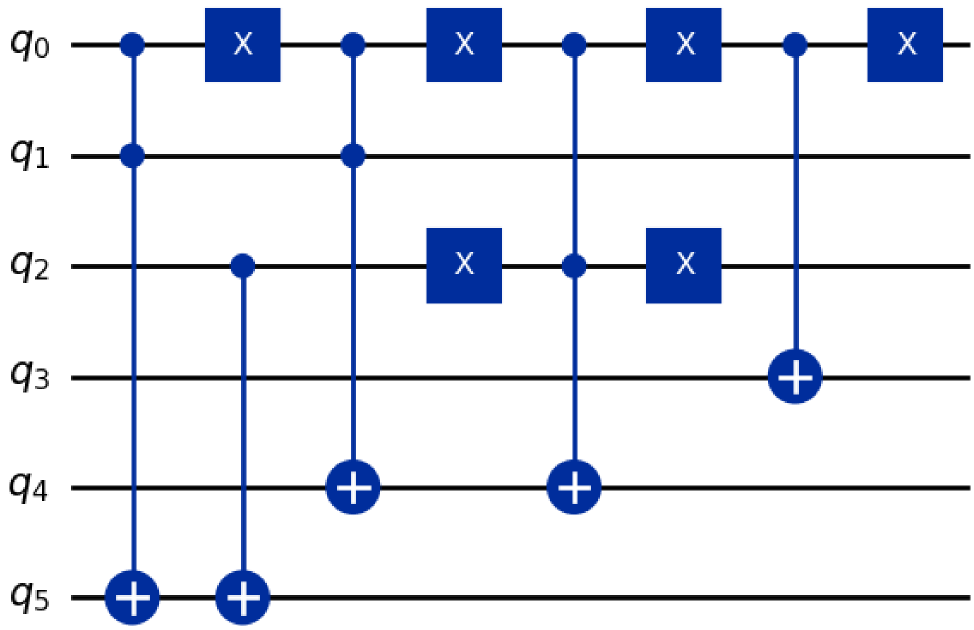
    - Tính $\overline{A}B$: Áp dụng $X(q_0)$, sau đó $Toffoli(q_0, q_1, q_4)$. Sau đó áp dụng $X(q_0)$ để trả lại trạng thái A.
    - Tính $A\overline{C}$: Áp dụng $X(q_2)$, sau đó $Toffoli(q_0, q_2, q_4)$. Sau đó áp dụng $X(q_2)$ để trả lại trạng thái C.

3. **Tính D:** Áp dụng $X(q_0)$, sau đó $CNOT(q_0, q_3)$. Cuối cùng áp dụng $X(q_0)$ để trả lại trạng thái A ban đầu.

```
# 3 qubit đầu vào (0, 1, 2) và 3 qubit đầu ra (3, 4, 5)
qc = QuantumCircuit(6)

# 1. Tính F = AB XOR C trên qubit 5
qc.ccx(0, 1, 5)  # Toffoli(A, B, F) -> F = AB
qc.cx(2, 5)  # CNOT(C, F) -> F = AB XOR C

# 2. Tính E = (NOT A)B + A(NOT C) trên qubit 4
# Phần 1: (NOT A)B
qc.x(0)  # NOT A
qc.ccx(0, 1, 4)  # Toffoli(NOT A, B, E) -> E = (NOT A)B
qc.x(0)  # Quay lại A ban đầu

# Phần 2: A(NOT C)
qc.x(2)  # NOT C
qc.ccx(0, 2, 4)  # Toffoli(A, NOT C, E) -> E = (NOT A)B + A(NOT C)
qc.x(2)  # Quay lại C ban đầu

# 3. Tính D = NOT A trên qubit 3
qc.x(0)  # NOT A
```

```
qc.cx(0, 3)  # CNOT(A, D) -> D = NOT A
qc.x(0)  # Quay lại A ban đầu
```

Listing 2: "Cài đặt mạch lượng tử cho hàm f trên Qiskit"



Hình 2: Mạch lượng tử thực hiện hàm $f(A, B, C) = (D, E, F)$

2.4 Câu d

Trạng thái đầu vào là:

$$|\psi\rangle_{in} = \frac{1}{\sqrt{3}}(|000\rangle + |100\rangle + |111\rangle)$$

Ta xác định đầu ra cho từng thành phần cơ sở dựa trên hàm f:

- Với $|000\rangle$ $(A = 0, B = 0, C = 0)$:
  - $D = \overline{0} = 1$
  - $E = \overline{0} \cdot 0 + 0 \cdot \overline{0} = 0$
  - $F = 0 \cdot 0 \oplus 0 = 0$
  - Kết quả: $|100\rangle$

- Với $|100\rangle$ $(A = 1, B = 0, C = 0)$:
  - $D = \overline{1} = 0$
  - $E = \overline{1} \cdot 0 + 1 \cdot \overline{0} = 1$
  - $F = 1 \cdot 0 \oplus 0 = 0$
  - Kết quả: $|010\rangle$
- Với $|111\rangle$ $(A = 1, B = 1, C = 1)$:
  - $D = \overline{1} = 0$
  - $E = \overline{1} \cdot 1 + 1 \cdot \overline{1} = 0$
  - $F = 1 \cdot 1 \oplus 1 = 0$
  - Kết quả: $|000\rangle$

Vậy trạng thái đầu ra của hệ 3 qubit chứa giá trị (D, E, F) là:

$$|\psi\rangle_{out} = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |000\rangle)$$

Kiểm tra lại bằng mạch lượng tử trên Qiskit đã cho kết quả đúng như trên (xem trong notebook).

3 Bài 3

Theo **Định lý không nhân bản (No-Cloning Theorem)**, ta không thể sao chép một trạng thái lượng tử *bất kỳ chưa biết*. Tuy nhiên, $|\Phi^+\rangle$ là một trạng thái *đã biết* (trạng thái Bell). Do đó, việc "sao chép" ở đây được hiểu là chuẩn bị (prepare) một trạng thái giống hệt như vậy trên một cặp qubit khác độc lập.

Trạng thái Bell $|\Phi^+\rangle$ được định nghĩa là:

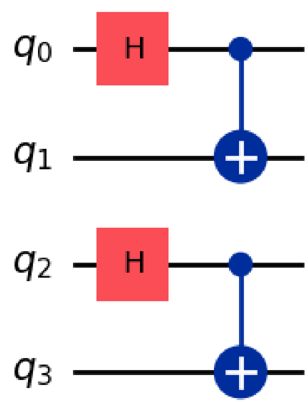
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Mạch tạo trạng thái này bao gồm một cổng Hadamard (H) tác động lên qubit điều khiển và một cổng CNOT tác động lên qubit mục tiêu. Để tạo ra hai bản sao, ta thực hiện quy trình này trên hai cặp qubit riêng biệt (ví dụ: cặp q_0, q_1 và cặp q_2, q_3).

Trạng thái kỳ vọng của hệ 4 qubit là tích tensor của hai trạng thái Bell:

$$\begin{aligned}|\Psi\rangle &= |\Phi^+\rangle_{23} \otimes |\Phi^+\rangle_{01}\\ &= \left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] \otimes \left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right]\\ &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)\end{aligned}$$

Mạch lượng tử:



Hình 3: Mạch lượng tử tạo hai bản sao của trạng thái Bell $|\Phi^+\rangle$

Kiểm tra kết quả trên Qiskit cho thấy trạng thái đầu ra đúng như kỳ vọng:

$$|\Psi\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$$

- Cặp bit thấp (q_1q_0) nhận giá trị 00 hoặc 11, tương ứng với trạng thái $|\Phi^+\rangle$.
- Cặp bit cao (q_3q_2) nhận giá trị 00 hoặc 11, cũng tương ứng với trạng thái $|\Phi^+\rangle$.
- Sự xuất hiện của các tổ hợp chéo (ví dụ $|00\rangle_{23}|11\rangle_{01}$) cho thấy hai cặp này độc lập với nhau.

Như vậy, ta đã tạo thành công bản sao của trạng thái $|\Phi^+\rangle$.

4 Bài 4

Giả sử Alice và Bob chia sẻ cặp qubit vướng víu ở trạng thái:

$$|\Phi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{1}$$

4.1 Câu a

Giao thức Mã đậm đặc

Mục tiêu: Alice gửi 2 bit cổ điển b_1b_0 cho Bob bằng cách tác động cổng lượng tử lên qubit A và gửi nó cho Bob.

Quy trình:

1. Alice áp dụng cổng U lên qubit A dựa trên 2 bit cần gửi.
2. Alice gửi qubit A cho Bob.
3. Bob thực hiện phép đo trong cơ sở Bell trên hệ 2 qubit.

Bảng quy ước mã hóa và giải mã:

Tin nhắn (b_1b_0)	**Cổng Alice** (U_A)	**Trạng thái hệ** ($\|\psi\rangle_{AB}$) $(U_A \otimes I)\|\Phi^-\rangle$	**Kết quả đo của Bob** (Trạng thái Bell)
00	I	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$
01	X	$-\|\Psi^-\rangle$	$\|\Psi^-\rangle$
10	Z	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$
11	ZX	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$

Bảng 1: Giao thức Mã đậm đặc với e-bit $|\Phi^-\rangle$

4.2 Câu b

Dịch chuyển lượng tử

Mục tiêu: Alice muốn chuyển trạng thái $|\psi\rangle_Q = \alpha|0\rangle + \beta|1\rangle$ cho Bob.

Quy trình:

1. Alice thực hiện cổng $CNOT$ lên cặp (Q, A) (với Q là điều khiển) và cổng $Hadamard$ lên Q.
2. Alice đo hệ (Q, A) trong cơ sở tính toán, nhận được 2 bit cổ điển z, x.

3. Alice gửi 2 bit này cho Bob.

4. Bob áp dụng cổng khôi phục lên qubit B để thu được $|\psi\rangle$.

Bảng quy ước khôi phục trạng thái: Do e-bit là $|\Phi^-\rangle$, trạng thái Bob nhận được sẽ sai khác so với giao thức chuẩn. Bob cần áp dụng các cổng sau để đưa qubit về đúng trạng thái $|\psi\rangle$:

Kết quả đo của Alice (z, x)	**Trạng thái tại Bob** (Trước khi khôi phục)	**Cổng Bob cần thực hiện** (U_{Bob})
00	$Z\|\psi\rangle$	**Z**
01	$XZ\|\psi\rangle$	**XZ**
10	$\|\psi\rangle$	**I**
11	$-X\|\psi\rangle$	**X**

Bảng 2: Bảng khôi phục cho Dịch chuyển lượng tử với e-bit $|\Phi^-\rangle$

5 Bài 5

Cho hàm $f : \mathbb{B}^2 \to \mathbb{B}$ với $f(x, y) = x \oplus y$.

5.1 Câu a

Oracle lượng tử U_f hoạt động trên 3 qubit theo quy tắc:

$$U_f|x, y\rangle|z\rangle = |x, y\rangle|z \oplus f(x, y)\rangle = |x, y\rangle|z \oplus x \oplus y\rangle$$

Để thực hiện phép toán này, ta sử dụng hai cổng CNOT:

- $CNOT(x, z)$ thực hiện $|z\rangle \to |z \oplus x\rangle$.
- $CNOT(y, z)$ thực hiện $|z \oplus x\rangle \to |z \oplus x \oplus y\rangle$.

Vậy U_f bao gồm hai cổng CNOT với qubit điều khiển lần lượt là x, y và qubit mục tiêu là z.

5.2 Câu b

Oracle pha Z_f hoạt động trên 2 qubit theo quy tắc:

$$Z_f|x, y\rangle = (-1)^{f(x,y)}|x, y\rangle = (-1)^{x \oplus y}|x, y\rangle$$

Ta có tính chất $(-1)^{x \oplus y} = (-1)^x \cdot (-1)^y$. Điều này tương đương với việc áp dụng cổng Z lên qubit x và cổng Z lên qubit y. Vậy $Z_f = Z \otimes Z$.

5.3 Câu c

Trạng thái đầu vào:

$$|+\rangle^{\otimes 2} = |+\rangle|+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Với Oracle lượng tử U_f (sử dụng thêm qubit ancilla $|-\rangle$ để tạo hiệu ứng phase kickback):

$$U_f(|+\rangle|+\rangle|-\rangle) = Z_f|+\rangle|+\rangle$$

Kết quả trên 2 qubit đầu vào sẽ tương tự như tác động của Z_f.

Với Oracle pha Z_f:

$$\begin{aligned}
Z_f|+\rangle|+\rangle &= (Z \otimes Z)\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\
&= \frac{1}{2}(Z|0\rangle Z|0\rangle + Z|0\rangle Z|1\rangle + Z|1\rangle Z|0\rangle + Z|1\rangle Z|1\rangle) \\
&= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\
&= \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\
&= |-\rangle|-\rangle
\end{aligned}$$

5.4 Câu d: Kiểm tra trên Qiskit

```
# 1. Khởi tạo mạch 2 qubit
qc = QuantumCircuit(2)

# 2. Tạo trạng thái đầu vào |+>|+>
qc.h([0, 1])

# 3. Áp dụng Oracle pha Z_f cho hàm XOR
# Lý thuyết: (-1)^(x XOR y) = (-1)^x * (-1)^y => Cổng Z trên cả 2 qubit
qc.z(0)
qc.z(1)
```

```python

# 4. Hiển thị kết quả
state = Statevector(qc)
pretty_output = format_state(state)
print(f"Trạng thái cuối cùng sau Oracle pha Z_f: | {pretty_output}")
```

Listing 3: "Kiểm tra Oracle pha trên Qiskit"

Kết quả mô phỏng cho thấy trạng thái đầu ra là $|-\rangle|-\rangle$, khớp với tính toán lý thuyết.

6 Bài 6

Yêu cầu: Vẽ mạch và kiểm tra thuật toán Deutsch-Jozsa cho hàm f_1 và f_2.

Phân tích hàm: Dựa vào bảng giá trị:

- Hàm $f_1(x_1, x_0)$: $f(00) = 1, f(01) = 1, f(10) = 1, f(11) = 1$. $\Rightarrow f_1$ là **Hàm Hằng** (Constant), $f_1(x) = 1$.
- Hàm $f_2(x_1, x_0)$: $f(00) = 0, f(01) = 0, f(10) = 1, f(11) = 1$. $\Rightarrow f_2(x) = x_1$ (phụ thuộc vào bit cao). Đây là **Hàm Cân bằng** (Balanced).

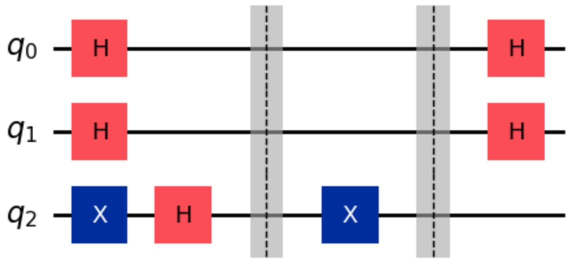
Thiết kế Oracle:

- Oracle U_{f_1}: Đảo bit output (hoặc không làm gì nếu dùng phase kickback với $|-\rangle$ thì chỉ cần thêm dấu trừ toàn cục). Để đơn giản, ta có thể dùng cổng X lên qubit ancilla.
- Oracle U_{f_2}: $f_2(x) = x_1$, nên ta dùng cổng CNOT với điều khiển là qubit x_1 và mục tiêu là qubit ancilla.

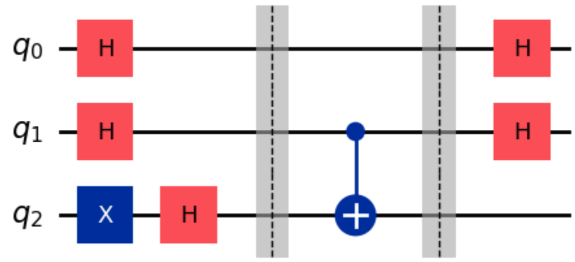
Quy trình thuật toán Deutsch-Jozsa:

1. Khởi tạo 2 qubit input ở trạng thái $|0\rangle$ và 1 qubit ancilla ở trạng thái $|1\rangle$.
2. Áp dụng cổng H lên tất cả các qubit.
3. Áp dụng Oracle U_f.
4. Áp dụng cổng H lên 2 qubit input.
5. Đo 2 qubit input.

Vẽ mạch cho cả hai hàm:



Hình 4: Mạch Deutsch-Jozsa cho f_1



Hình 5: Mạch Deutsch-Jozsa cho f_2

Kết quả thực nghiệm: (*kết quả trong notebook*)

- Hàm f_1: Kết quả đo '00' (xác suất 100%) $\rightarrow$ Kết luận: Hàm Hằng (Đúng).
- Hàm f_2: Kết quả đo '10' (xác suất 100%) $\rightarrow$ Kết luận: Hàm Cân bằng (Đúng).