Grover implementazione

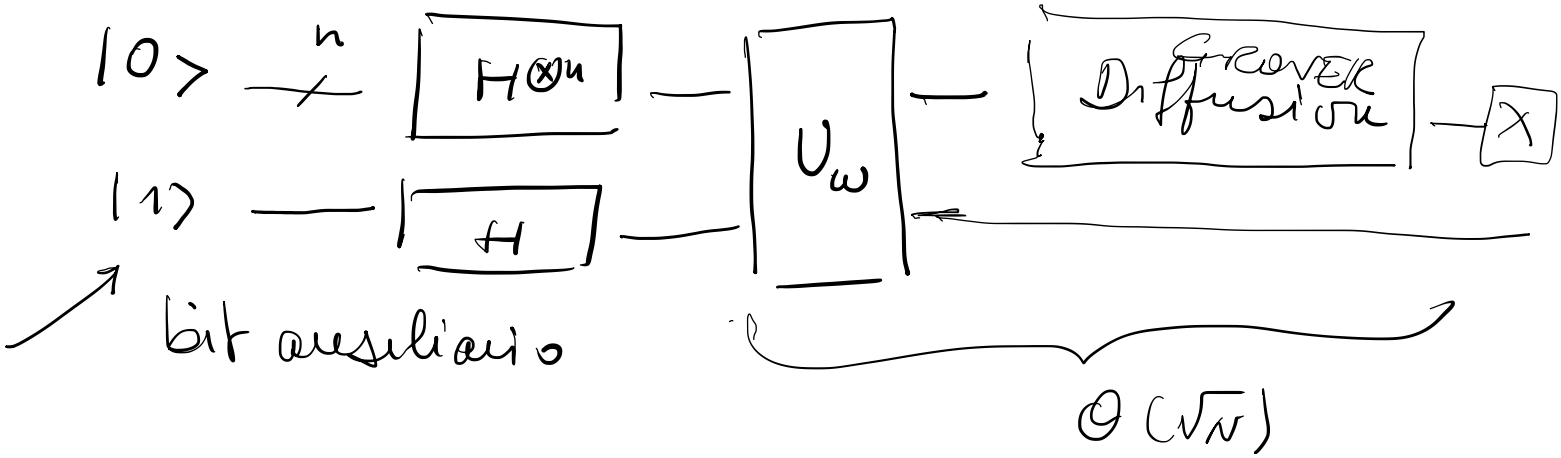
Trovare 1 elemento w dato

$f: \{0,1\}^n \to \{0,1\}$ $\quad f(w)=1 \quad f(x)=0 \; x \neq w$

Black-box $\quad |j\rangle_n |y\rangle_1 \to |j\rangle |y \oplus f(j)\rangle$

oppure $U_\omega(|j\rangle) = (-1)^{f(j)} |j\rangle$.

Circuito



G. Diffusion

$$H^{\otimes n}(2|0\rangle\langle 0|^{\otimes n} - I^{\otimes n})H^{\otimes n}$$

1. Dobbiamo "cambiare segno" allo stato $|w\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.
Le black box si occupa di questo.

2. Operare con operatore di diffusione che effettua un'inversione rispetto alla media. (solo sui primi n bits).

$$\sum \alpha_j |j\rangle \longrightarrow \sum_j \left(2\left(\sum_k \frac{\alpha_k}{2^n}\right) - \alpha_j\right)|j\rangle$$

la matrice

$$W = \frac{2}{2^n} \cdot \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - I^{\otimes n}$$

rappresenta questa azione

Ricordiamo che se $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

allora

$$H^{\otimes q} = \frac{1}{\sqrt{2}} \begin{pmatrix} H^{\otimes q-1} & H^{\otimes q-1} \\ H^{\otimes q-1} & -H^{\otimes q-1} \end{pmatrix}$$

e quindi

$$H^{\otimes n}_{jk} = \frac{1}{\sqrt{2^n}} (-1)^{j \cdot k}$$ ← prodotto scalare $j, k \in \{0,1\}^n$

se allora definiamo $R = \begin{pmatrix} 2 & 0 \cdots & 0 \\ 0 & & \\ \vdots & & 0 \end{pmatrix}$

si ha

$$\left(H^{\otimes n} \cdot R\, H^{\otimes n}\right)_{jk} = \left(H^{\otimes n}\right)_{j0} R_{00} \left(H^{\otimes n}\right)_{0k}$$

$$= \frac{2}{2^n}$$

dato che $R_{jk} = 0 \quad j,k \neq 0$

Da cui

$$W = H^{\otimes n} R + I^{\otimes n} - I^{\otimes n} = \quad \leftarrow H^{\otimes n} \cdot H^{\otimes n}$$

$$= H^{\otimes n} \left(R - I^{\otimes n} \right) H^{\otimes n} =$$

$$= H^{\otimes n} \underbrace{\mathrm{diag}(1, -1, \ldots, -1)}_{\text{"}F} H^{\otimes n}$$

Come costruire F?

L'effetto di F è cambiare il segno del coefficiente di ogni stato $|j\rangle$ della base tranne $|0\rangle$!

Invece di F proviamo costruire
$-F$ che cambia il segno a
$|0\rangle$ e lascia gli altri $|j\rangle$
invariati. Tanto le matrici
di F e $-F$ è un cambiamento
di fase globale e quindi
implementano la stessa operazione.

Abbiamo il gate $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

quindi $CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$ (su
2 qubits) quindi proviamo a
costruire un gate che

che cambia il segno di $|-1\rangle$
e lascia gli altri invariati.

Indichiamo con $C^{n-1}Z$

il gate che applicato a
n qubits applica Z all'ennesimo
se gli altri sono tutti $|1\rangle$.

NOTA Se $n=2$

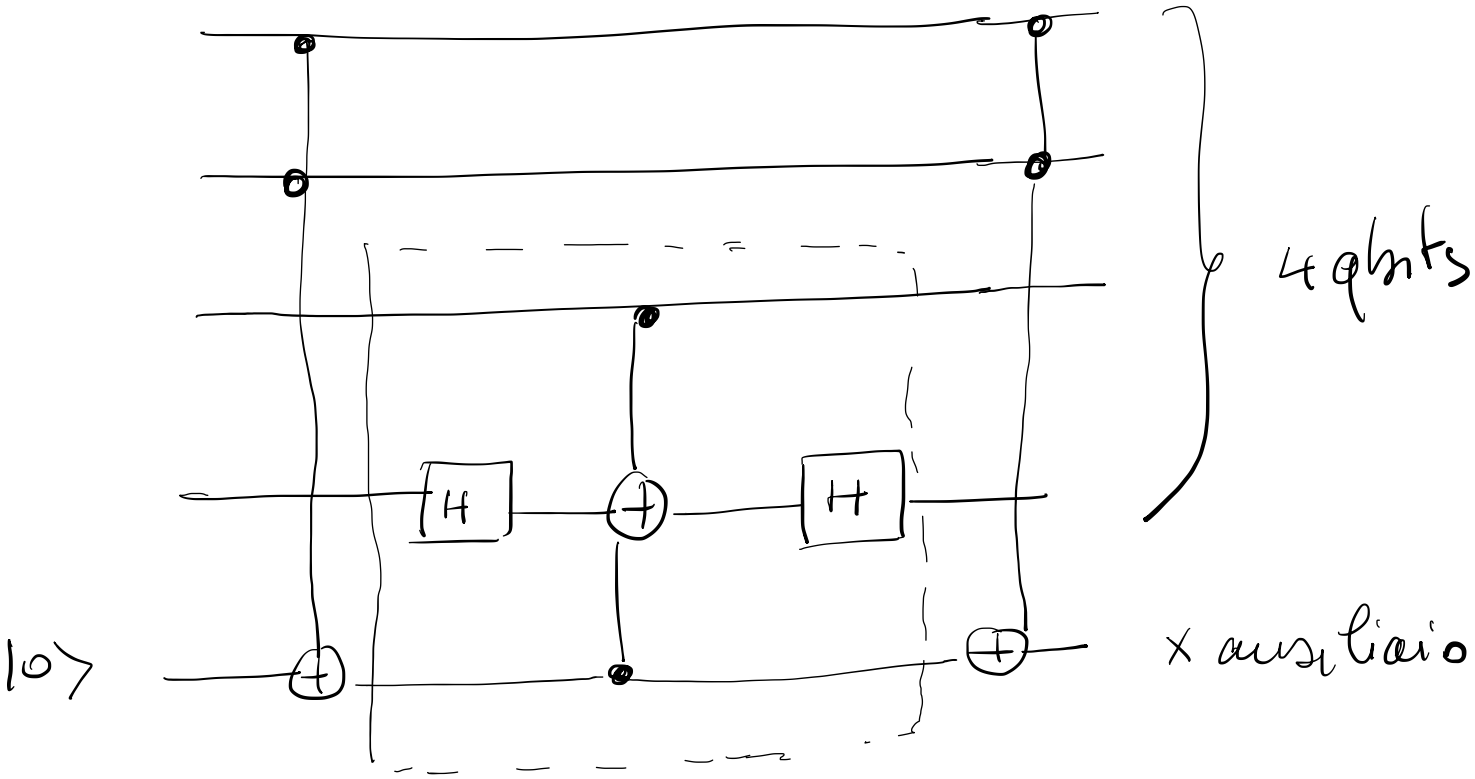
Così se abbiamo $C^{n-1}Z$

$$F = X^{\otimes n}\left(C^{n-1}Z\right)X^{\otimes n}$$

Ci sono molti modi per costruire $C^{n-1}Z$. Un modo:

- implementare $C^{n-2}X$ e CZ

Es. $n=4$ C^3Z



Per concludere ricordiamo che il numero ottimale di iterazioni è

$$k \simeq \frac{\pi}{4}\sqrt{2^n}$$

Vediamo ora come implementare un circuito che trova f t.c

$$f(5) = 1 \quad e \quad f(x) \neq 0$$

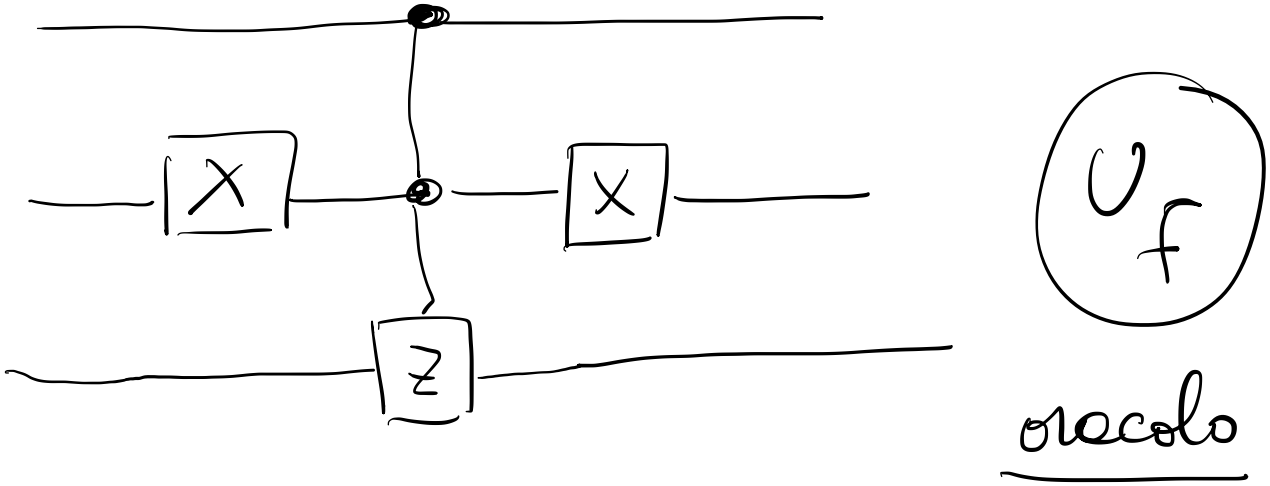
$0 \leq x \leq 7$.

$n = 3$ # passi ottimale $k \simeq 2.2$

$\Rightarrow \boxed{k = 2.}$

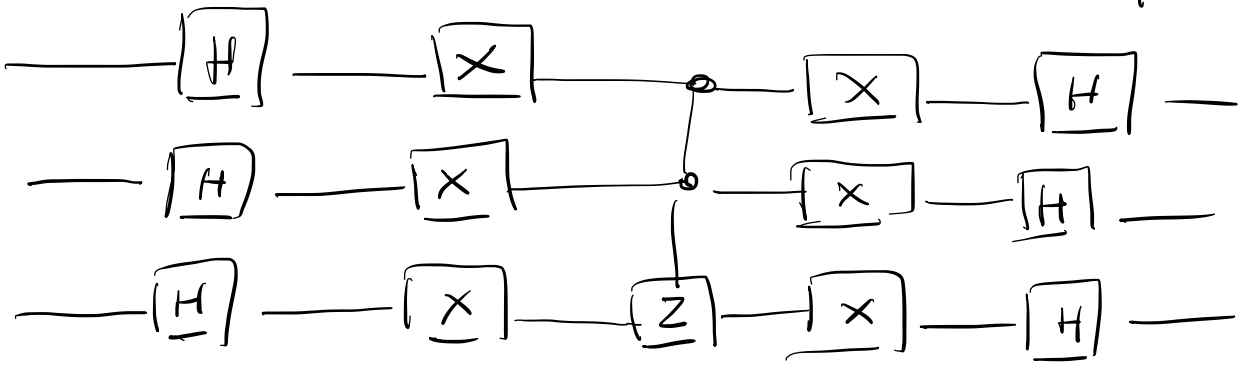
Scriviamo U_f -

Vogliamo che cambi il segno a 101 - Quindi se usiamo C^2Z, che cambia il segno se tutti 1



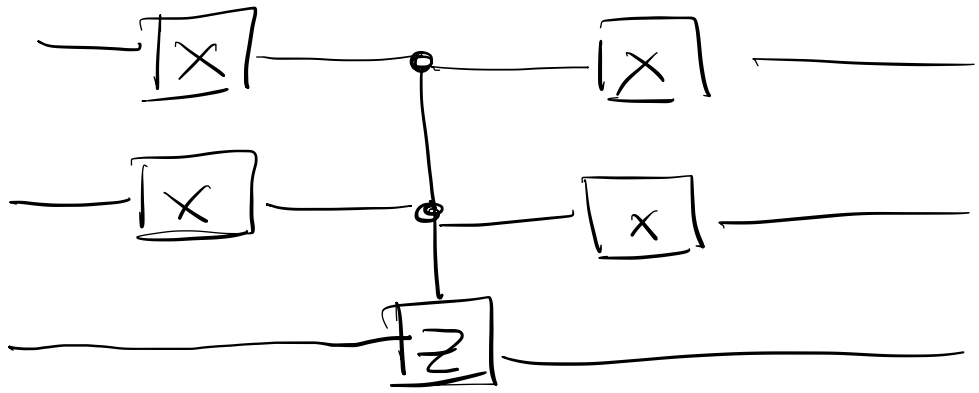
oracolo

Diffusione $H^{\otimes 3} F H^{\otimes 3} = H^{\otimes 3} \underbrace{X^{\otimes 3} C^2 Z X^{\otimes 3}}_{F} H^{\otimes 3}$



Se vogliamo $f(001) = 1$

U_f -



. . .

Esempi Grover 1 volta

2 volte

3 volte

Confronta i risultati.

—

Esempio (E-1-3-SAT).

Problema:

Data $\bigwedge_{1}^{m} C_k$ su n variabili booleane, $x_1, \ldots, x_n$, con 3 letterali per clausola $C_1, \ldots, C_m$ dove una clausola è composta di OR e not.

Determinare se esiste un assegnamento di x_1, x_2, x_3 tale che ogni C_i ha esattamente 1 letterale vero

Es $(x_1 \nabla x_2 \nabla \neg x_3)$ (LG110)

Possibili assegnamenti con 1 solo vero.

101, 011, 000,

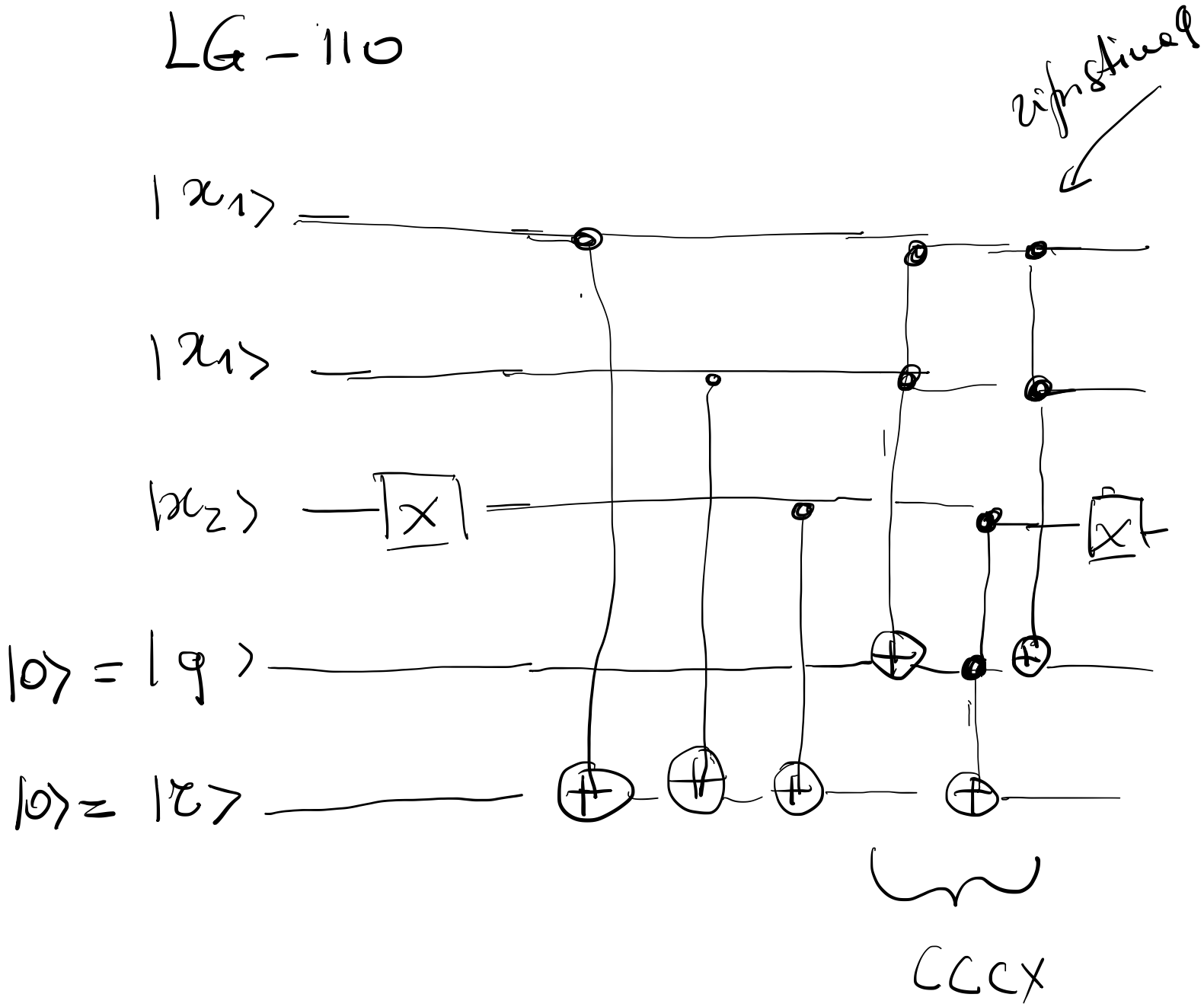
Chiediamo LG-110

Il gate che riconosce che esiste 1 solo assegnamento vero per $x_1 \nabla x_2 \nabla \neg x_3$.

—

Alle

LG - 110



$\Rightarrow |r\rangle = 1 \quad (=) \quad 1!$ bl.

Come fare per risolvere?

1. ORACOLO

usiamo 8 qbits:

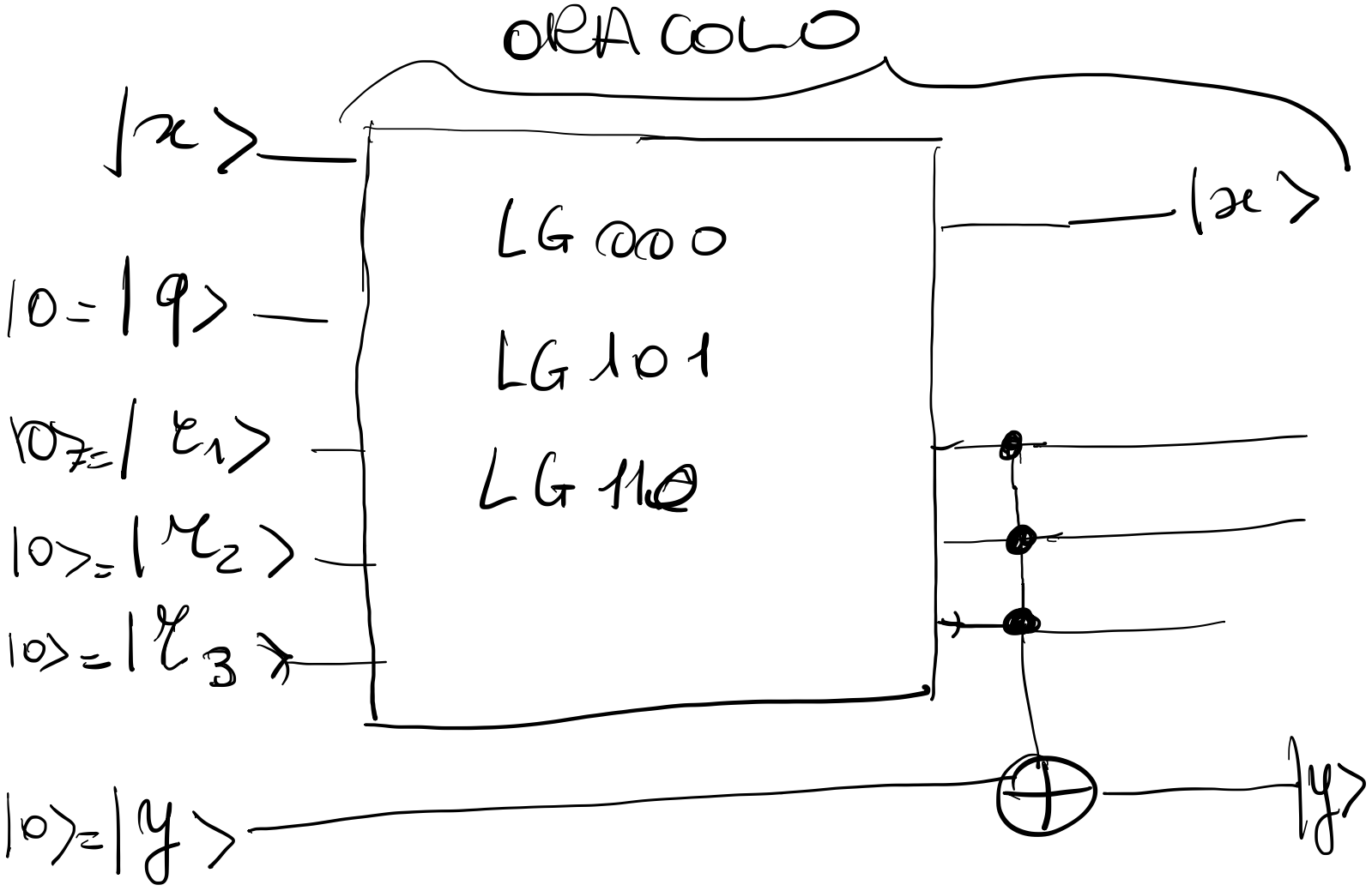
- 3 input
- 1 ancilla
- 3 per memorizzare la validità delle 3 formule
- 1 per valore oracolo

Se una combinazione è valida $LG \longrightarrow |x\rangle|1\rangle$

Calcoliamo tutte e

poi controlliamo che i risultati siano tutti 1

ossia CCCX



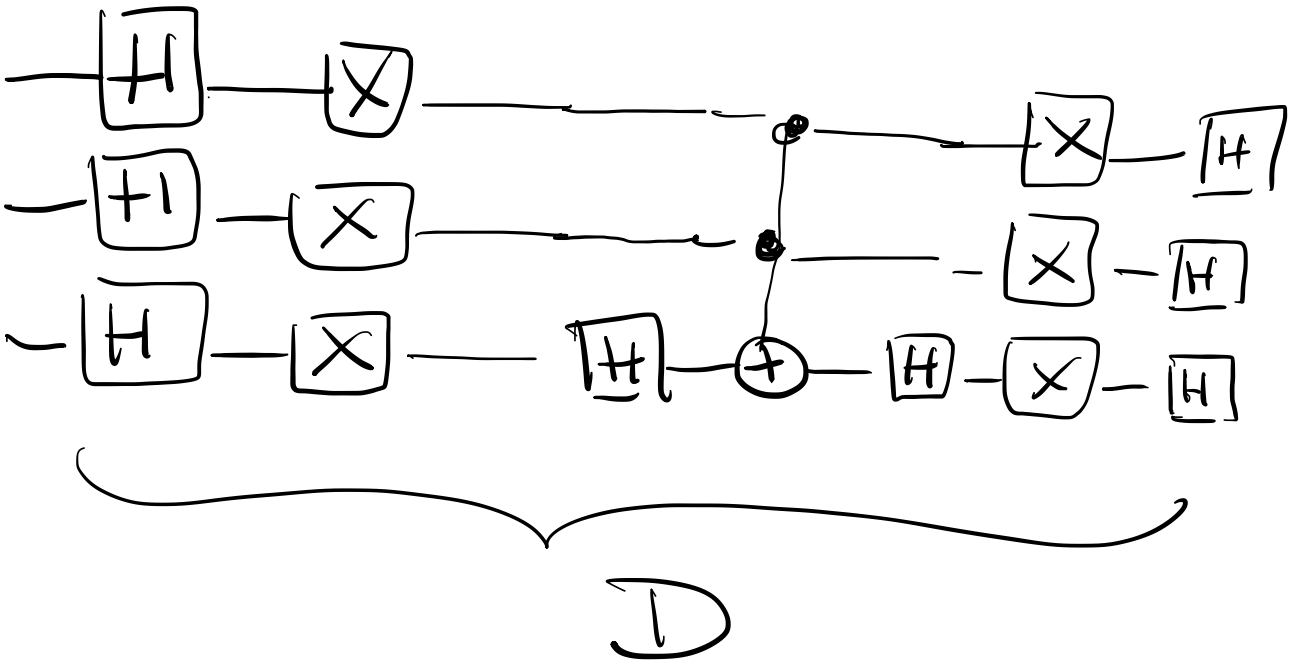
Ci basta sapere $|x\rangle$ e $|y\rangle$

$$O(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$$

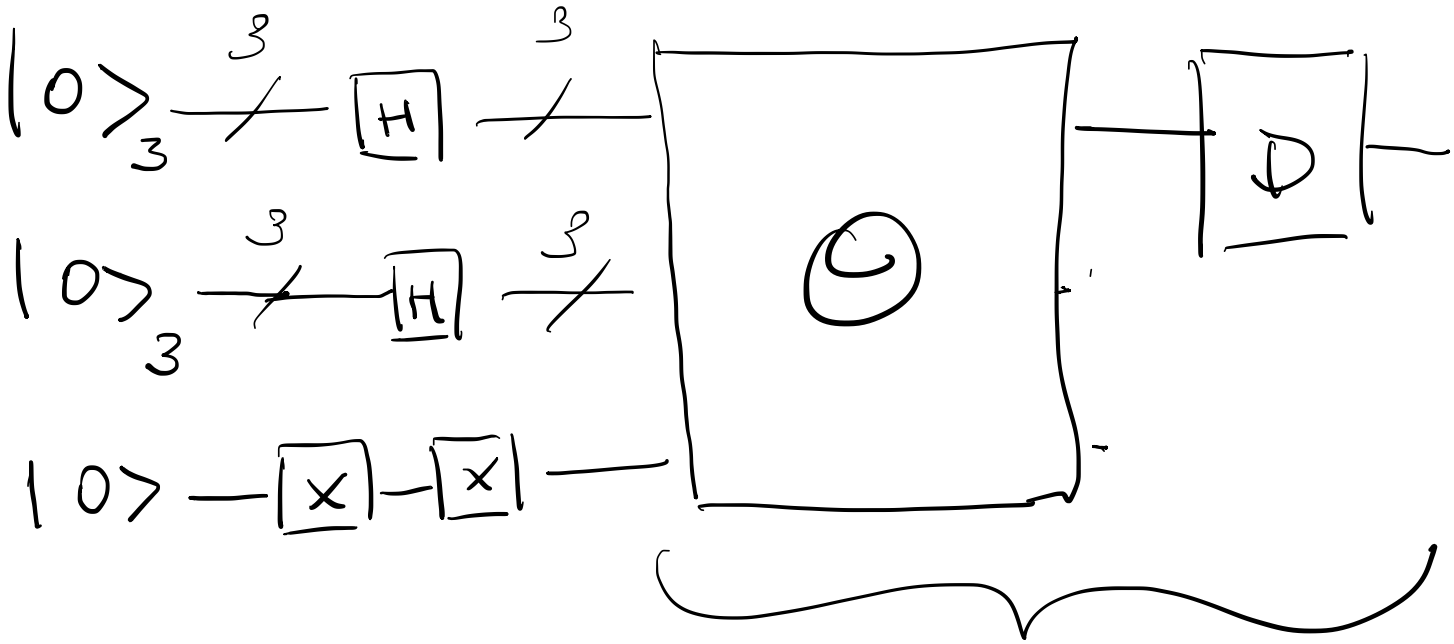
Attenzione: tutti i valori che non servono vanno ripristinati al valore iniziale!

A questo punto diffusione

$$W = H^{\otimes 3} X^{\otimes 3} C^3_Z X^{\otimes 3} H^{\otimes 3}$$



In definitiva



Ripetere 2 volte per $N = 3$. !

Esempio -

LCSAT 3-1G 1 Grover

LCSAT3-2G 2 Grover

Altra applicazione - (MQ)

Trovare le soluzioni di un sistema di eq. polinomiali quadratiche su $\mathbb{F}_2$

Per ora limitiamoci a:

2 equazioni in 3 variabili di grado 2 e supponiamo che esiste una sola soluzione.

Problema 1. Un sistema di equazioni quadratiche su F_2 è dato da un "cubo" $(\lambda_{ij}^{(k)})$ su F_2 e un vettore $(v_1 \dots v_n) \in F_2^n$. Vogliamo trovare $(x_1, \dots, x_n) \in F_2^n$ t.c.

$$\sum_{1 \le i,j \le n} \lambda_{ij}^{(k)} x_i x_j = v_k$$

Problema 2 Diciamo che un sistema è in forma "conveniente" se è dato da un "cubo" $(\lambda_{ij}^{(k)})$ con $\lambda_{ij}^{(k)} = 0$ se $i > j$. Inoltre $v = (1, \dots, 1)$.

Ogni sistema si può ricondurre

a un sistema equivalente con

$n+1$ equazioni e $n+1$ variabili

che è in forma canonica.

Basta definire

$$\lambda'^{(k)}_{ij} = \begin{cases} \lambda^{(k)}_{ij} & i=j \le n \\ \lambda^{(k)}_{ij} + \lambda^{(k)}_{ji} & 1<j<n \\ 1+v_k & i=j=n+1 \\ 0 & \text{altrimenti} \end{cases}$$

$$\lambda'^{(n+1)}_{ij} = \begin{cases} 1 & i=j=n+1 \\ 0 & \text{altrimenti} \end{cases}$$

Costruiamo un oracolo. (Si può fare meglio).

Definiamo

$$y_i^{(k)} = \sum_{1 \le j \le n} \lambda_{ij}^{(k)} x_j$$

$$E^{(k)} = \sum_{1 \le i \le n} x_i y_i^{(k)}$$

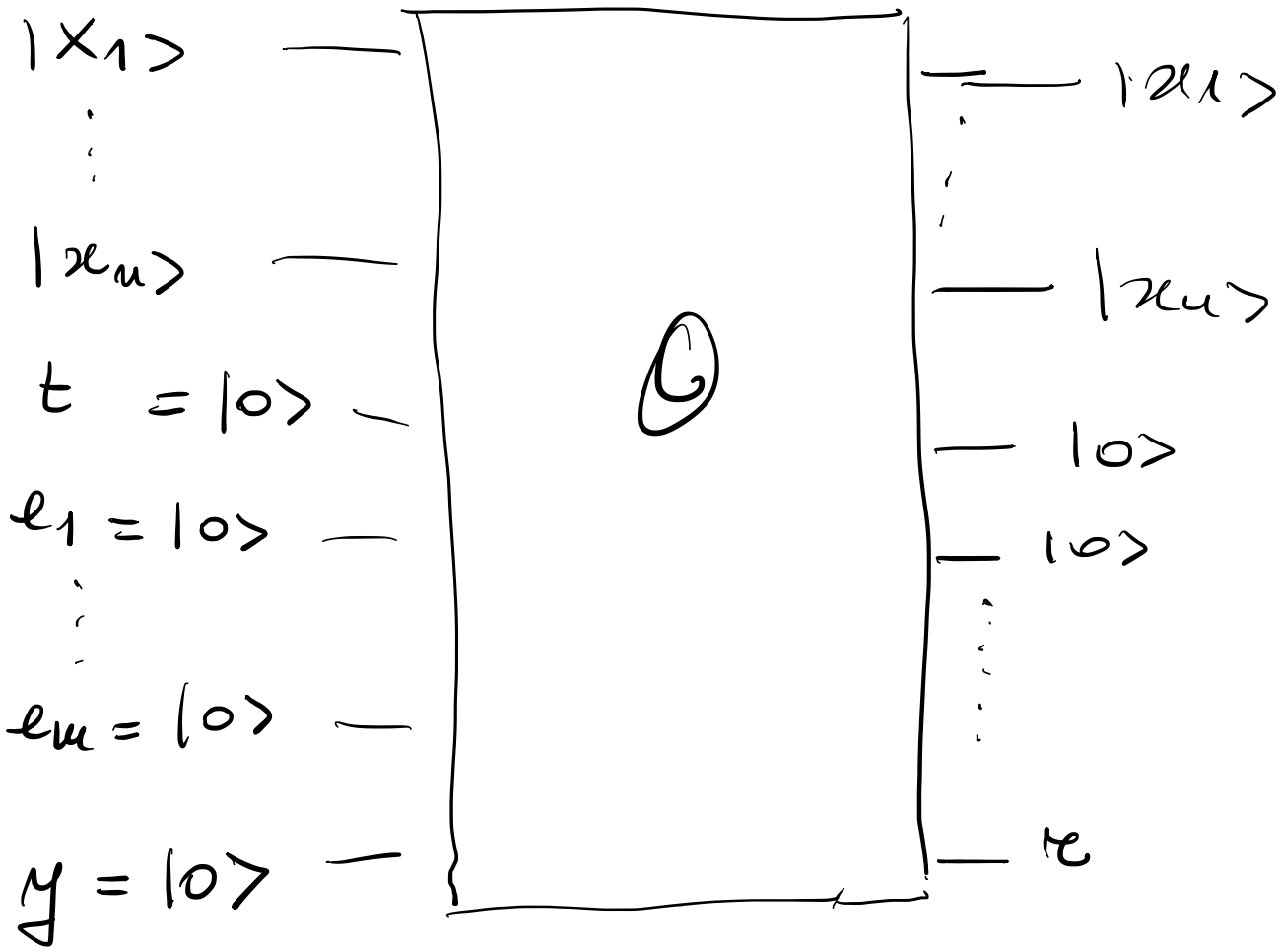
Così (x_i) è soluzione $\iff E^{(k)} = 1 \ \forall k$

Es.

$$\begin{cases} x_1(1 + x_2 + x_3) + x_2 x_3 = 1 \\ x_1(1 + x_3) = 1 \end{cases}$$

Per vedere se $\underline{x}$ è soluzione

Definiamo



ossia $n+m+2$ registri e

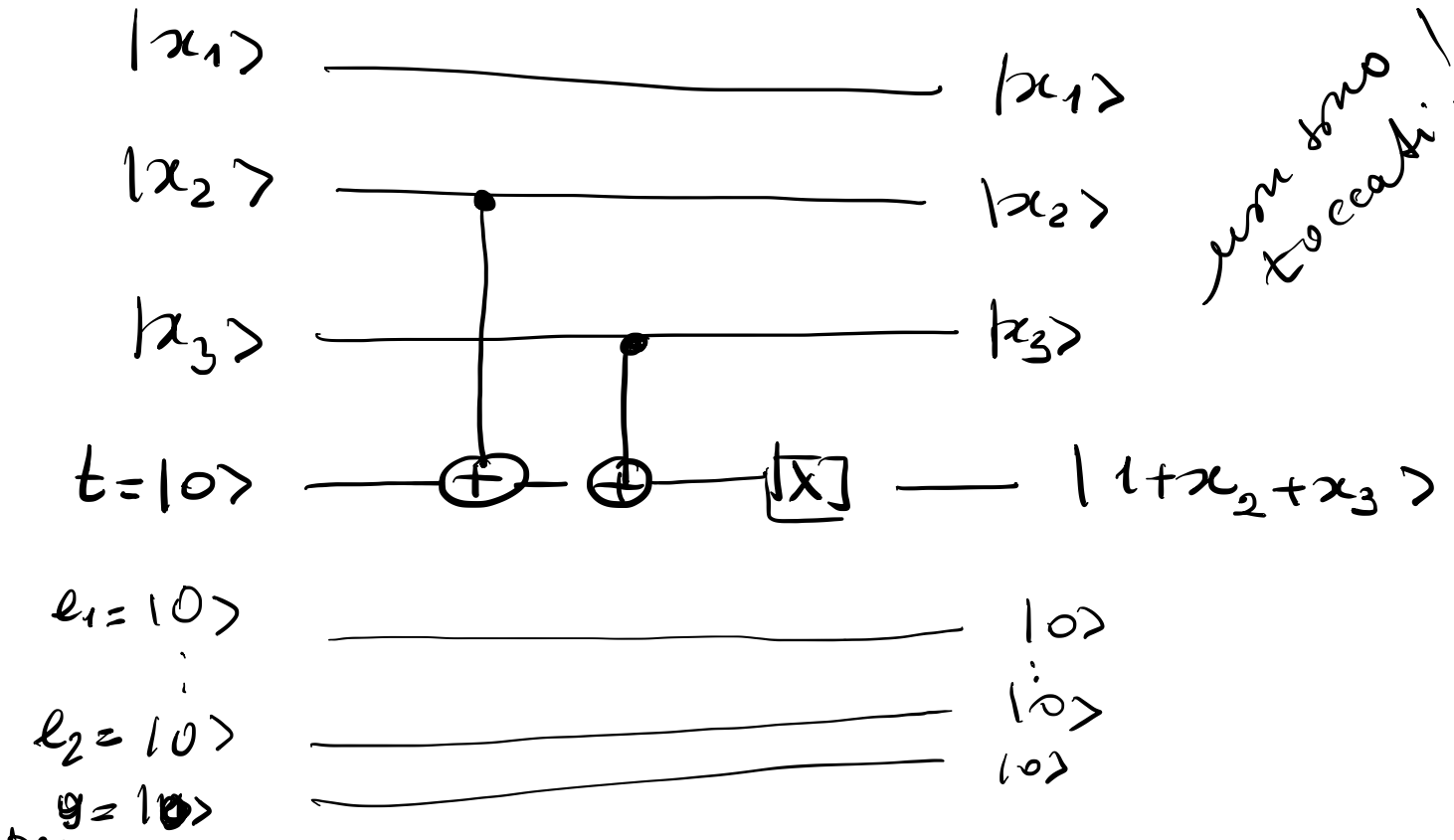
$r = |1\rangle$ se $\underline{x}$ è soluzione

$r = |0\rangle$ altrimenti

Oss. $1 + z = \overline{z}$, quindi

per ottenere in uscita $y_1^{(1)}$ in t.

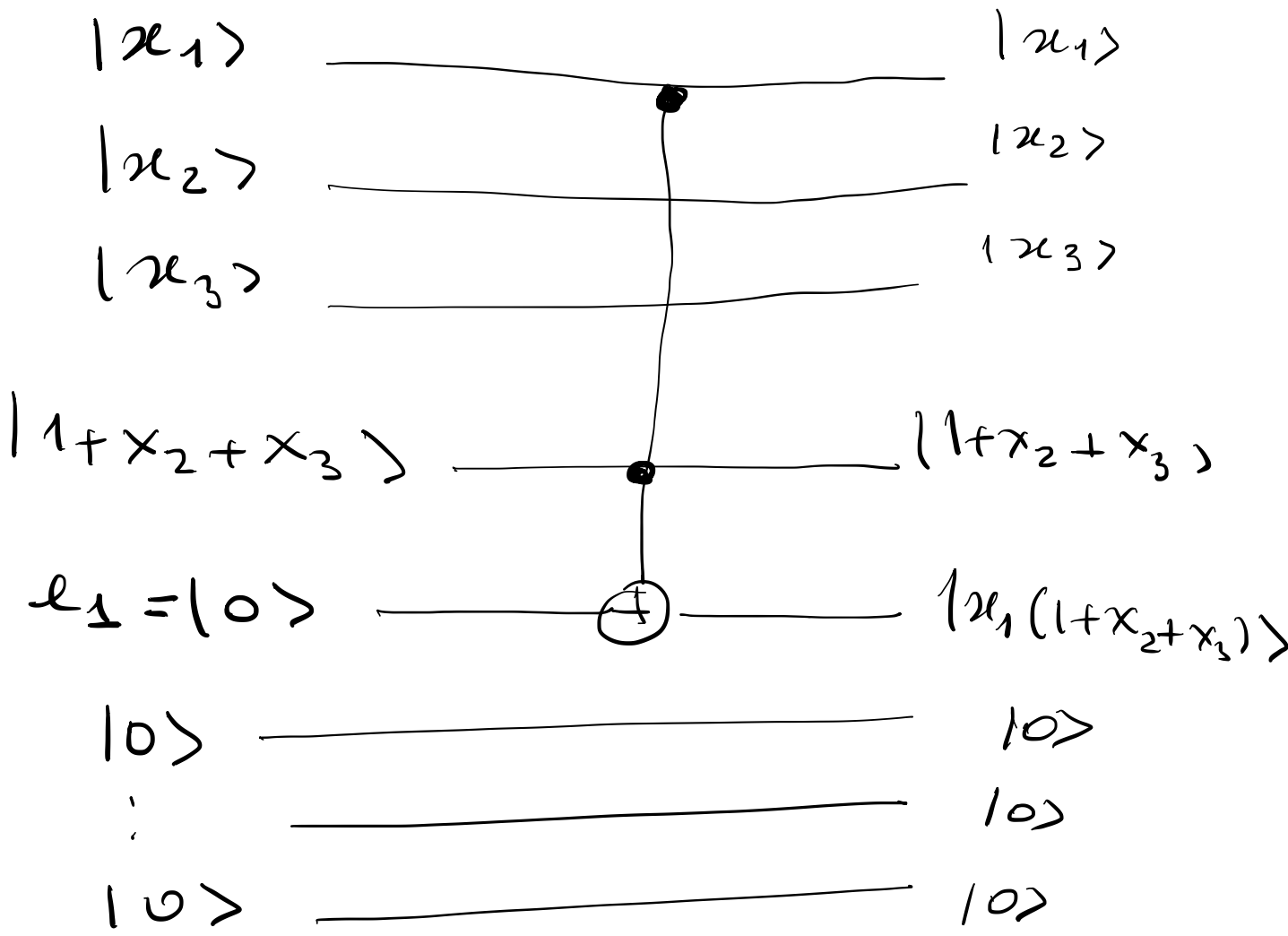
Vediamo l'esempio



non sono toccati!

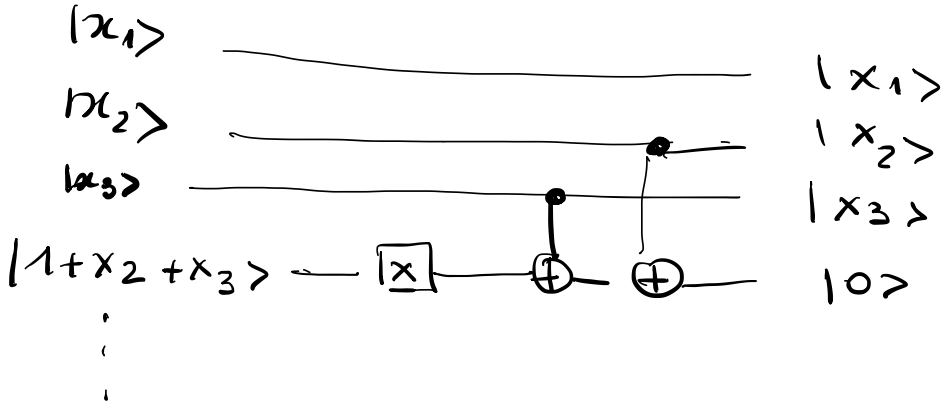
per aggiungere $x_2 x_3$ usiamo un Toffoli

$T(x_1, t, e_1)$



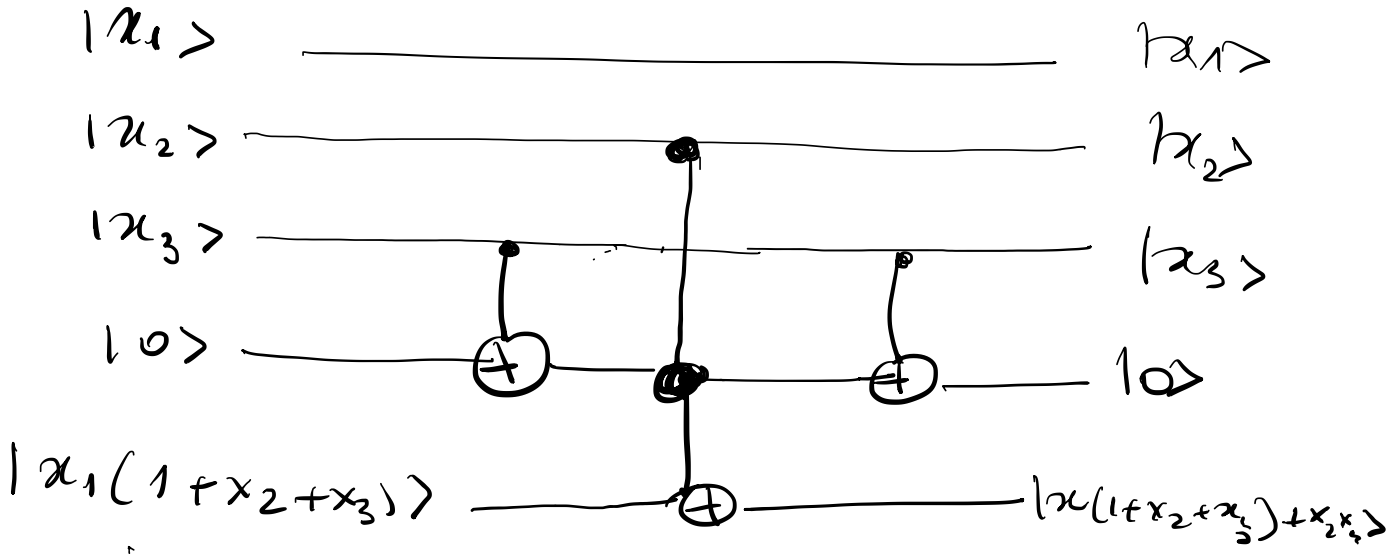
Poi bisogna "ristinare" (t)

basta applicare a ritroso le trasformazioni fatte per mettere $y_1^{(1)}$ in t

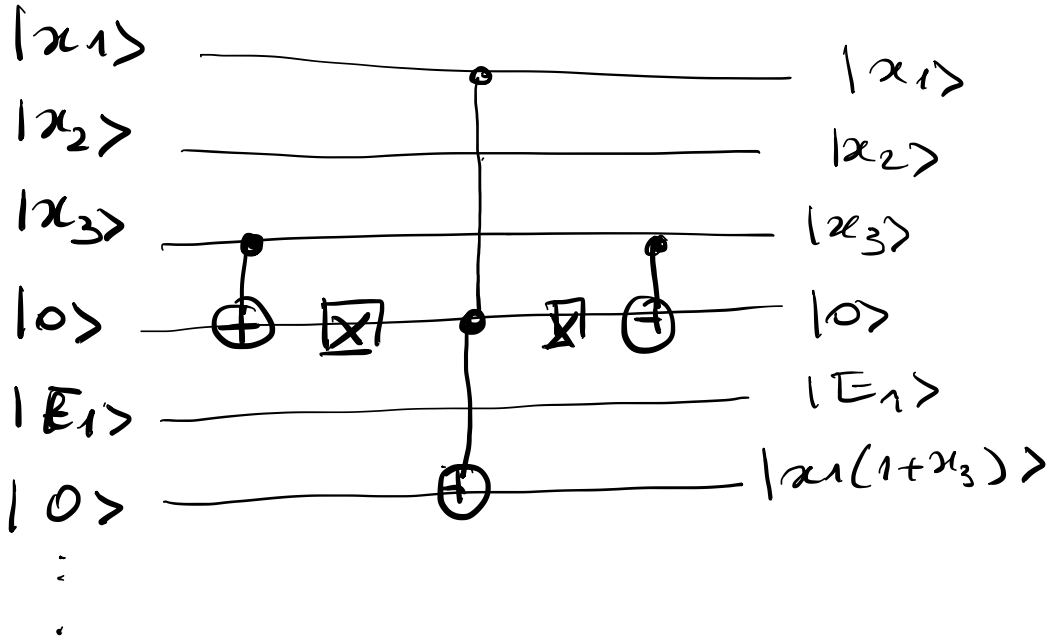


Poi aggiungiamo $y_2^{(1)} = x_2 x_3$

a e_1



Continuiamo con le altre equazioni per ottenere $x_1(1+x_3)$ in e_2 usiamo



Alla fine $|y>1$ se tenevi gli $|E_1\rangle = |1\rangle$ - Possiamo usare un m. qubits Toffoli.
Fatto l'oracolo basta applicare l'operatore di diffusione di G.

Esempio

QE-2