2.2.2 Квантово търсене в масив от данни чрез алгоритъм на Гроувър

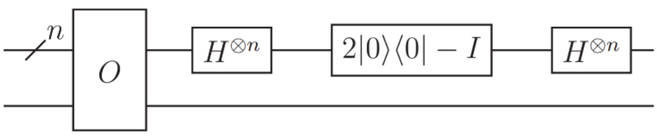
Търсенето в неподреден масив от данни е необходимо да бъде бързо и при класическите компютри се прилагат различни методологии за ускорение като техниките на паралелното програмиране. При квантовите компютри е възможно квадратично ускорение чрез алгоритъма на Гроувър[Wittek, 2014]. Той бива използван за реализацията на примерна система за препоръки в **Трета глава** на текущия научен труд. Целта е да се дефинира функция за търсения елемент, която да бъде върне резултат *истина* при успех. Алгоритъмът използва вътрешни извиквания към оракул, който определя стойността на функцията. След което трябва да се намери най-малкият възможен брой извиквания на оракула, определящи кои елементи са търсените. Нека съществува база-данни от $N = 2^n$ елемента, където $n = \log N$ бита служат за декларацията на всеки такъв. Извършва се начална инициализация, като се получава равно-претегленото суперпозиционно състояние $|\psi\rangle = \frac{1}{\sqrt{n}}\sum_{x=0}^{n-1}|x\rangle$ чрез трансформация на Адамар върху $|0\rangle^{\otimes n}$. Дефинира се *оператор на Гроувър G*, познат още като дифузен оператор на Гроувър. Той се състои от следните стъпки:

- извикване на оракул $\mathrm{O} = (-1)^{f(x)}$, където$f(x) = 1$, ако е решение;
- прилагане на трансформация на Адамар $\mathcal{H}^{\otimes n}$;
- прилагане на условно фазово отместване на състоянията, т.е. тези които не са $|0\rangle$, получават фаза -1: $|x\rangle \mapsto -(-1)^{\delta x0}|x\rangle$;
- повторно прилагане на трансформацията на Адамар.

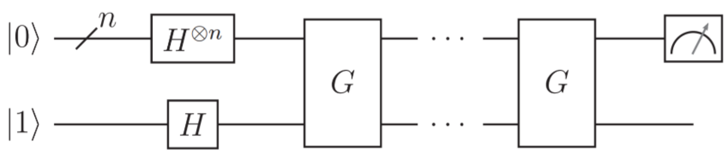
Когато стъпките са приложени заедно, се образува тъждеството:

$$(\mathcal{H}^{\otimes n}(2|0\rangle\langle 0| - \mathrm{I})\mathcal{H}^{\otimes n})O = (2|\psi\rangle\langle\psi| - \mathrm{I})\mathrm{O} \qquad (8.1)$$

Графично представяне на тази част от алгоритъма е представено на Фигура 12, както и итерациите при прилагане на оператора $O(\sqrt{N})$ пъти:

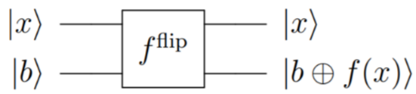


Фигура 12.1. Принципна квантова логическа схема на алгоритъм на Гроувър[Wittek, 2014].



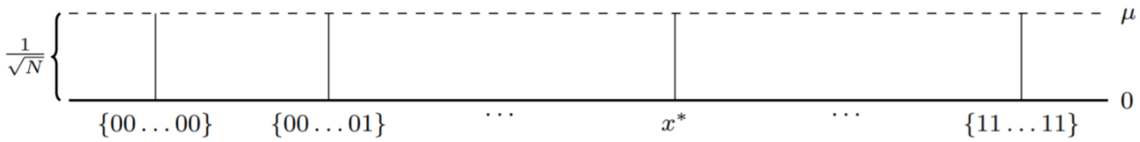
Фигура 12.2. Пълна квантова логическа схема за приложение на алгоритъма на Гровър[Wittek, 2014].

Фазовото отместване по-горе всъщност възниква от проблема, че достъпването на квантова база-данни би било еквивалентно на това при класическите компютри, но образуващият се оракул няма да бъде валиден квантов гейт. Причината се основава на факта, че този квантов гейт притежава n-битов входен интерфейс и еднобитов изходен. Освен това гейтът нито е унитарен, нито е реверсивен. Решението, което се използва основно, е третата стъпка от оператора на Гроувър. В [Wright, 2015] е предложен алтернативен подход чрез f^{flip} гейт, където се използва допълнителен $|b\rangle$ бит за изход. Квантова логическа схема на тази операция е показана на Фигура 13:



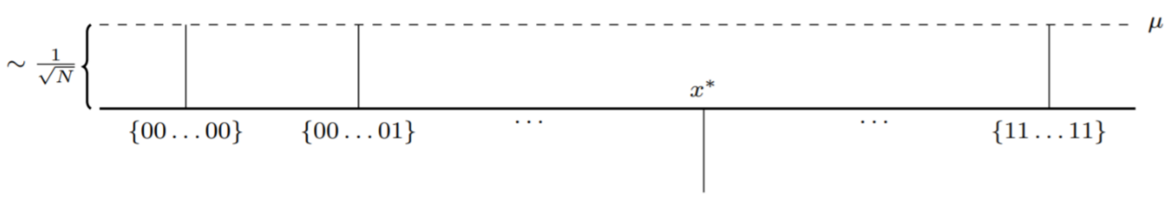
Фигура 13. Принципна логическа схема на квантов f^{flip} гейт[Wright, 2015].

Което и да е от двете решения, ще доведе до желания ефект, а именно да *изпъкнат* елементите, които отговарят на входния критерий, т.е. да са решения на задачата. Графичното обяснение отново е взаимствано от [Wright, 2015], но дава точна представа за събитията при итерациите на Гроувър. Нека всички амплитуди след първоначалната инициализация биват изобразени чрез бар-графи, както се вижда на Фигура 14.1.



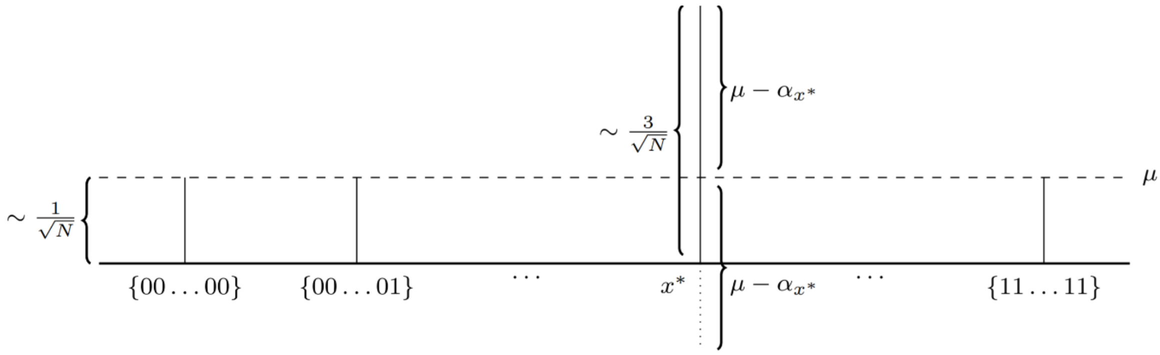
Фигура 14.1. Начални амплитуди, където μ е средната им стойност.

Прилага се трета стъпка от оператора на Гроувър и *търсеният* елемент x^*, който все още не е дефиниран като такъв от самия алгоритъм, обръща амплитудата си заради състоянието $-\frac{1}{\sqrt{N}}|x^*\rangle + \sum_{x\epsilon\{0,1\}^n;x\neq x^*}\frac{1}{\sqrt{N}}|x\rangle$. Това явление е показано на Фигура 14.2.



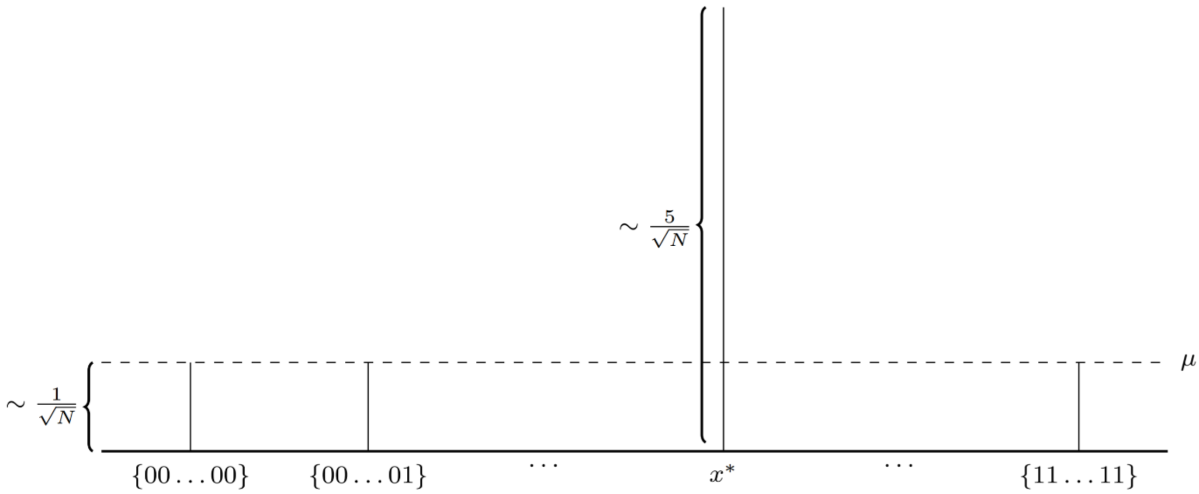
Фигура 14.2. Първи белези за намиране на търсения елемент.

Самият дифузен гейт изпълнява следното свързване: $\sum_{x\in\{0,1\}} a_x\,|x\rangle \mapsto \sum_{x\in\{0,1\}^n}(2\mu - a_x)\,|x\rangle$, т.е. следващото прехвърляне ще бъде спрямо средната стойност, както е показано на Фигура 14.3.



Фигура 14.3. Увеличена амплитуда на търсения елемент.

Аналогично, изпълнението на операциите от Фигура 14.2 и Фигура 14.3 ще се повтаря $O(\sqrt{N})$ брой пъти, като всеки път амплитудата на търсения елемент ще нараства, както е показано на Фигура 14.4.



Фигура 14.4. Видимо нарастване на амплитудата на търсения елемент и възможно доближаване до край на процеса на итерациите.

Важна забележка е, че всъщност амплитудата a_{x^*} не може да стане по-голяма от 1. Нейното увеличение ще се забави постепенно и по-късно ще се обърне. Всъщност, това от което се нуждае една система, е видима разлика между амплитудите на търсените елементи и останалите. Целта е да не се достига намаляване на амплитудата.

Подробно математическо представяне на алгоритъма на Гроувър може да бъде разгледано в [Тончев, 2017]. Тази техника също стъпва и на очакването, че основното ускорение се дължи на квантовото сплитане. Подробно са разгледани множество анализи относно този феномен при алгоритъма на Гроувър в [Qu et al, 2015]. Както стана въпрос по-горе, анализът на алгоритъма се базира на приложението на оракула към общото суперпозиционно състояние, т.е. от гледна точка на статично измерване. Както е разгледано в [Тончев, 2017], n-кюбит състояния, който се получават след последователно прилагане на итерации G, имат следната форма:

$$\left|\psi_k{}^G\right\rangle \equiv \frac{\cos\left[(2k+1)^{\theta}/_2\right]}{\sqrt{2^n}\cos\left(^{\theta}/_2\right)}\sum_{x\in f^{-1}(0)}|x\rangle + \frac{\sin\left[(2k+1)^{\theta}/_2\right]}{\sqrt{2^n}\sin\left(^{\theta}/_2\right)}\sum_{x\in f^{-1}(1)}|x\rangle, \tag{8.2}$$

$$\left|\psi_k{}^O\right\rangle \equiv \frac{\cos\left[((2(k-1)+1)^{\theta}/_2\right]}{\sqrt{2^n}\cos\left(^{\theta}/_2\right)}\sum_{x\in f^{-1}(0)}|x\rangle + \frac{\sin\left[((2(k-1)+1)^{\theta}/_2\right]}{\sqrt{2^n}\sin\left(^{\theta}/_2\right)}\sum_{x\in f^{-1}(1)}|x\rangle. \tag{8.3}$$

Тук $\left|\psi_k{}^G\right\rangle$ са състоянията от итерациите на Гроувър, а $\left|\psi_k{}^O\right\rangle$ са същите итерационни състояния, но след оценка на сложността O, т.е. трансформирани към състояния на оракула. $|x\rangle$ представя основните изчислими състояния на n-кюбита, $f(x)$ е булевата функция, която осъществява преобразуването $\{0,1\}^n \longrightarrow \{0,1\}$. Както беше описано по-горе, тя става равна на единица, тогава и само тогава, когато x е едно от решенията на проблема за търсене. Очевидно е, че описаните по-горе състояния са във формата:

$$|\psi_2\rangle \equiv a\sum_{x\in f^{-1}(0)}|x\rangle + b\sum_{x\in f^{-1}(1)}|x\rangle, \tag{9.1}$$

където $a, b \in \mathbb{R}$ и $a^2|f^{-1}(0)| + b^2|f^{-1}(1)| = 1$. Такъв тип състояния се назовават като n-кюбитови *реални двустойностни състояния*. С тяхната помощ в [Qu et al, 2015] е анализирана качествено и количествено динамиката на сплитанията при изпълнението на алгоритъма на Гроувър. Нека $|\psi\rangle$ е чисто квантово състояние от n квантови бита. Ако то може да бъде разписано като тензорно произведение на чисти квантови състояния от k отделни подсистеми, тогава $|\psi\rangle$ се нарича *k-делимо*. За множество от такива състояния S_k, може да се дефинира $\delta(|\psi\rangle) \equiv k$, наречена *делима свобода*. Също така $\delta(|\psi\rangle) = n$ тогава и само тогава, когато $|\psi\rangle \in S_n$ – това състояние се нарича *напълно делимо*. Ако $\delta(|\psi\rangle) = 1$, тогава $|\psi^n\rangle$ се нарича *напълно сплетено* състояние. Ако $n \geq 3$ и $\delta(|\psi\rangle) \in \{2, 3, \ldots, n-1\}$, тогава $|\psi\rangle$ е *частично делимо състояние*. С цел улеснение, може да се приеме, че $n \geq 3$ е винаги изпълнено. По-долу е описана теорема за измерване на сплитането, доказана в [Qu et al, 2015].

Теорема 1: Нека $|f^{-1}(1)| \notin 0{,}2^n$, $a \neq -b$ и $a.b \neq 0$. Тогава:

- $|\psi_2\rangle$ е напълно делимо тогава и само тогава, когато $|f^{-1}(1)| = 2^{n-1}$ и $|\psi_2\rangle$ е представено във формите: $\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes(n-1)} \otimes\sqrt{2^{n-1}}(a|0\rangle + b|1\rangle)$ и $\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes(n-1)} \otimes\sqrt{2^{n-1}}(b|0\rangle + a|1\rangle)$;
- Ако $|f^{-1}(1)|$ е нечетно, то $|\psi_2\rangle$ е напълно сплетено;

- Ако $|f^{-1}(1)| = 2^q(2p+1)$, където $p \in \mathbb{N}$ и $q \in \mathbb{Z}^+$, $|\psi_2\rangle$ е напълно сплетено или k-делимо при $k \geq 2$. Ако $|\psi_2\rangle$ е k-делимо, тогава $k \leq q+1$ и приема формата $\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right]^{\otimes(k-1)} \otimes \sqrt{2^{n-1}}(a\sum_{x\in S}|x\rangle + b\sum_{x\in T}|x\rangle)$, където $S \cup T = 0{,}1^{n-k+1}$ и $S \cap T = \Phi$, а $|T| = 2^{q-k+1}(2p+1)$.

Нека $\chi(|\psi\rangle)$ е максималното число на Шмид[1] за *n*-кюбитовото чисто квантово състояние $|\psi\rangle$ върху всичките възможни бичастични разделения A: B на *n* квантови бита:

$$\chi(|\psi\rangle) \equiv \max_{A} rank[tr_B(|\psi\rangle\langle\psi|)], \tag{9.2}$$

където са изпълнени следните свойства:

- $\chi(|\psi\rangle) \in \{1,2,\dots,2^{[n/2]}\}$ при $\chi(|\psi\rangle) = 1$ тогава и само тогава, когато то е напълно делимо;
- $\chi(|\psi\rangle) \otimes \chi(|\psi'\rangle) = \chi(|\psi\rangle).\chi(|\psi'\rangle)$;
- $\chi(|\psi\rangle)$ намалява при локални и стохастични локални операции и класическа комуникация[2]. Сплитането се измерва с: $E_\chi(|\psi\rangle \equiv \log_2(\chi(\psi\rangle))$, което е всъщност функцията, измерващата количеството сплитане в квантово състояние, наречена още *сплетен монотон* при локални и стохастични локални операции и класическа комуникация.

Връщайки се към алгоритъма на Гроувър, може да се види, че първоначалното състояние $|0\rangle^{\otimes n}$ е напълно делимо и $\chi = 1$. След гейта на Адамар, приложен на първите *n* квантови бита, се получава състояние $|\psi_0{}^G\rangle$, което също е напълно делимо. След което се разглеждат уравненията (8) и за успешно изпълнение се счита намерено решение с вероятност $\varepsilon \epsilon \left[\frac{1}{2}, 1\right]$. Важно разглеждане би било многочастичното сплитане при описание динамиката на алгоритъма на Гроувър за $|f^{-1}(1)| \geq 2^{n-1}, R = 0 - R$ е индекс на итерациите. Това неравенство означава, че не съществува нито едно решение, което да е намерено с вероятност поне $\frac{1}{2}$. В [Qu et al, 2015] са доказани следните теореми**:**

Теорема 2: Нека $|f^{-1}(1)|$ е нечетно, тогава:

- всички $|\psi_1{}^O\rangle, |\psi_1{}^G\rangle, \dots, |\psi_{R-1}{}^O\rangle, |\psi_{R-1}{}^G\rangle$ и $|\psi_R{}^O\rangle$ са напълно сплетени;
- ако $\cos\left[(2R+1)\,\theta/2\right] \neq 0$, тогава $|\psi_R{}^G\rangle$ е напълно сплетено. В противен случай е напълно сплетено или частично делимо, но не и напълно делимо.

---

[1] Бел. прев. от англ. Schmidt rank, Schmidt number - число или ранг на Шмид. Не бива да се бърка с безмерната величина от механика на флуидите, изразяваща отношението между кинематичния вискозитет и масовия коефициент.

[2] Има се предвид LOCC и SLOCC.

Теорема 3: Нека $|f^{-1}(1)| = 2^q(2p+1)$, където $p \in \mathbb{N}$ и $q \in \mathbb{Z}^+$, тогава:

- ако $|\psi_1^O\rangle$ е напълно сплетено, тогава всички състояния на итерациите са също напълно сплетени;
- ако $\cos\left[(2R+1)\,{}^{\theta}/_{2}\right] \neq 0$, тогава $\left|\psi_R{}^G\right\rangle$ е напълно сплетено;

От трите теореми, посочени по-горе, следва фактът, че за повечето инстанции $\left|\psi_1{}^O\right\rangle$ е напълно сплетено, както и състоянията на итерациите. С други думи, дори изпълнението на алгоритъма на Гроувър е почти изпълнено със сплетени състояния. Научният труд на [Qu et al, 2015] показва, че при това обстоятелство максималните числа на Шмид за състоянията на итерациите са с еднакъв диапазон. По-точно, ако $|f^{-1}(1)| = 2^{\delta(|\psi_1^O\rangle)-1}$, всички максимални числа на Шмид при състоянията на итерациите ще бъдат равни на 2.