České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

VÝZKUMNÝ ÚKOL

Optimalizace kvantového vyhledávacího algoritmu

2008 Václav Potoček

Poděkování

Rád bych tímto poděkoval vedoucímu výzkumného úkolu, panu prof. Ing. Igoru Jexovi, DrSc., za spolupráci a především veškerou podporu k umožnění spolupráce s dalšími spoluautory této práce, Aurélem Gábrisem, Ph.D., a Tamásem Kissem, Ph.D.

Obsah

Úvod

Tato práce navazuje na mou bakalářskou práci [1] z roku 2007. V tomto textu jsou ve stručnosti zrekapitulována základní fakta z teorie kvantových algoritmů se specializací na vyhledávací algoritmy a kvantové náhodné procházky. Jsou vyzdviženy dva vyhledávací algoritmy, Groverův algoritmus a algoritmus vyhledávání na hyperkrychli pomocí náhodné procházky, důraz je pak kladen především na porovnání těchto dvou algoritmů, určených pro vyhledávání v nesetříděné databázi.

Cílem práce je pokračovat ve zjištění uvedeném v [1], které vysvětluje teoretickou podstatu nejvíce zřetelného rozdílu mezi oběma algoritmy. Ve spolupráci se spoluautory byly tyto výsledky zobecněny a rozšířeny a byly navrženy způsoby, jak využít těchto zjištění k vylepšení stávajícího algoritmu.

Výsledkem práce je rukopis článku [13], jehož aktuální verze je uvedena ve formě přílohy.

1. Kvantové algoritmy

Kvantové algoritmy jsou relativně novou oblastí výzkumu na pomezí fyziky, matematiky a informatiky. Tato analogie klasických algoritmů, využívající k provádění algoritmických úkonů postuláty kvantové mechaniky, ukázala možnost snížení charakteru časové složitosti řešení některých algoritmických úloh až o exponenciální faktor. Neexistuje však obecný postup, jak stávající algoritmus vylepšit pouze využitím kvantové mechaniky, naopak, objevy nových kvantových algoritmů, které mají tuto výhodu oproti svým klasickým protějškům, jsou velmi vzácné.

Ve skutečnosti byly dosud nalezeny pouze dvě hlavní aplikační oblasti, ve kterých mají kvantové algoritmy reálnou možnost projevit svůj potenciál. Většina současného výzkumu se soustředí na prohlubování znalostí o nich, ani tato práce není výjimkou. Zmíněné oblasti však mají velký praktický význam:

Fourierova transformace posloupností a hledání periodicity má hlavní využití pro faktorizaci velkých čísel, tedy algoritmického úkolu, jehož nekvantová složitost ještě nebyla podpořena důkazem, ale věří se, že žádný klasický algoritmus s polynomickou časovou složitostí neexistuje [2]. Díky Shorově algoritmu [3] je však s využitím kvantového algoritmu možno dosáhnout kvadratické časové složitosti.

Druhou hlavní oblastí, ve které se projevuje významná výhoda kvantových algoritmů nad klasickými, je *vyhledávání v nesetříděné databázi*. Ačkoliv je teoreticky dokázáno [4], že není možné dosáhnout exponenciálního urychlení oproti klasickému případu jako v případě Shorova algoritmu, vzhledem k povaze zadání může být i polynomické urychlení velice výhodné.

Existují dva hlavní limity kvantových algoritmů. Příklad teoretického limitu časové složitosti i v kvantovém algoritmu byl nastíněn v předchozím odstavci a setkáme se s ním v sekci 2. Důvodem, proč kvantové algoritmy nejsou dosud využívány ve větším měřítku, jsou však praktické limity jejich použitelnosti – současná experimentální fyzika čelí podstatným problémům v situacích, kdy je třeba spolehlivě ovládat větší kvantový systém a udržet v něm čistý stav po dobu delší než v řádu jednotek sekund.

Z teorie kvantových algoritmů bude text této práce a článku [13] využívat především následující pojmy a fakta:

- stavovým prostorem kvantového algoritmu je jakýkoliv konečnědimenzionální komplexní Hilbertův prostor, nicméně nejčastěji jsou používány prostory získané jako tenzorový součin dvoudimenzionálních prostorů, odpovídajících jednotkám *qubitů*,
- výpočetní bází n-qubitového systému se nazývá tenzorový součin ortonormálních bází jednotlivých qubitů, úplné měření na takovém systému určí jeden vektor výpočetní báze či ekvivalentně n-bitový binární řetězec a způsobí kolaps stavu,
- úplné měření je možno provádět i na jednotlivých podsystémech (kvantových registrech),
- kvantová hradla jsou unitární operace působící na celém systému nebo na jeho podsystémech, existuje přitom základní množina jedno- a dvouqubitových kvantových hradel, z níž je možno zrealizovat hradlo odpovídající libovolné navržené unitární matici,
- pro libovolnou binární funkci n logických proměnných, již je možno popsat pomocí logických operací (hradel), je snadné sestavit takové kvantové hradlo, které pro každý stav z výpočetní

báze jednoho registru provádí v závislosti na funkční hodnotě dvě různé operace na jiném kvantovém registru,

– hradlo reprezentující binární funkci pak díky linearitě může zpracovat superpozici více vstupů, což je princip kvantového paralelizmu, měřením však není možné ze systému n qubitů získat více než n bitů klasické informace.

2. Vyhledávací algoritmy

Vyhledávací algoritmy jsou určeny k řešení úlohy vyhledat v jisté množině jeden prvek, který budeme nazývat označeným. Tento prvek bude určen binární rozhodovací funkcí, definovanou na prohledávané množině (databázi), která vrací hodnotu 1 pro označený prvek a 0 pro všechny ostatní. Tato funkce se v literatuře běžně označuje termínem orákulum (oracle).

Jestliže dotazy na orákulum (či jeho *volání*) jsou jedinou informací, na jejímž základě můžeme označený prvek vyhledat, nazývá se tato algoritmická úloha vyhledávání v nesetříděné databázi.

Díky povaze tohoto zadání neexistuje žádná optimální možnost, jak volit výběr pokusných prvků. Jakýkoliv klasický algoritmus má tedy stochastickou povahu s průměrným i maximálním počtem pokusů $O(N)$, kde N označuje velikost databáze.

Tato hodnotící funkce, závislost počtu dotazů na orákulum na velikosti databáze, by jistě byla rozhodujícím kritériem při porovnávání kvality různých vyhledávacích algoritmů. Otázkou tedy je, zda jsme s využitím kvantové paralelizace volání orákula schopni snížit takto definovanou časovou složitost pod lineární hranici.

Odpovědí je, že ano, dokonce je i známa další, kvantová hranice, kterou nemohou překročit ani kvantové algoritmy. Ve článku [4] je dokázáno, že optimální kvantový vyhledávací algoritmus má složitost $O(\sqrt{N})$. Je poskytnuta i odpovídající konstanta úměrnosti. V současnosti jsou známy dva hlavní způsoby kvantové implementace vyhledávacího algoritmu, které mají tento charakter. Oba předpokládají, že velikost databáze N je mocnina čísla 2, $N = 2^n$, v jiných případech je třeba databázi uměle zvětšit.

3. Groverův algoritmus

Groverův algoritmus, navržený v roce 1996 L. Groverem [5], je prvním a velice důležitým objevem v kategorii vyhledávacích algoritmů. Jeho důležitost spočívá především v ukázání konkrétní oblasti, kde kvantové algoritmy mohou dosahovat řádově lepšího výkonu než klasické.

Groverův algoritmus pracuje na Hilbertově prostoru $n + k$ qubitů, kde bázové stavy podsystému prvních n qubitů (hlavního registru) jsou identifikovány s jednotlivými prvky databáze. Ostatní qubity jsou určeny pouze jako pomocné pro kvantovou verzi orákula, bázovými stavy tedy obvykle nazýváme bázové stavy prvního podsystému.[1]

[1] Toto je umožněno faktem, že součástí kvantové verze orákula je nutně navrácení pomocných qubitů do původního stavu.

Počátečním stavem Groverova algoritmu je taková superpozice bázových stavů, ve které má každý stejnou amplitudu.[2] Základní charakteristikou algoritmu pak je, že opakovanou aplikací dvou kvantových hradel, z nichž jedno odpovídá fázovému posunu řízenému výsledkem volání orákula, převede počáteční stav na stav, při němž úplné měření ve výpočetní bázi dá s velkou pravděpodobností výsledek odpovídající označenému vstupu. Tento postup byl později zobecněn i mimo rámec Groverova algoritmu pod názvem posilování amplitudy [6].

Optimální počet *iterací* (opakování aplikací těchto dvou hradel, a tedy přeneseně i volání orákula) závisí pouze na velikosti databáze a je určen analyticky:

$$t_f = \left[\frac{\pi}{4}\sqrt{N}\right],$$

kde hranaté závorky značí celou část čísla. Pravděpodobnost naměření vektoru odpovídajícího označenému stavu (pravděpodobnost úspěchu) po tomto počtu provedených iterací podléhá odhadu

$$P \geq 1 - \frac{1}{N}.$$

Pravděpodobnost úspěchu do dosažení uvedeného počtu iterací monotónně roste. Kdybychom však tento počet překročili, pravděpodobnost úspěchu by opět začala klesat až blízko k nule, odkud dále by se její vývoj periodicky opakoval. K tomuto závěru dojdeme přesnou analýzou vývoje stavu systému, která ukazuje, že tento stav se pohybuje pouze ve dvourozměrném reálném podprostoru celého stavového prostoru, jenž má ortonormální bázi tvořenou hledaným vektorem a jiným vektorem, který odpovídá nulové pravděpodobnosti úspěchu. Jedna iterace má geometrický význam rotace stavu v tomto podprostoru o konstantní úhel.

Analytický popis průběhu Groverova algoritmu platí s odpovídajícími úpravami přesně i v zobecnění, kdy umožníme více než jeden označený prvek databáze. Definici pravděpodobnosti úspěchu je pak třeba upravit na pravděpodobnost, že úplné měření na systému dá za výsledek stavový vektor, který odpovídá některému prvku množiny označených prvků. Ukazuje se, že tato pravděpodobnost je v každý okamžik rovnoměrně rozdělena mezi všechny označené vstupy.

Ukazuje se však, že pro aplikaci Groverova algoritmu v tomto zobecnění je potřebné předem znát počet označených prvků databáze, který označíme m. Vzorec pro optimální počet iterací je totiž třeba upravit na tvar

$$t_f = \left[\frac{\pi}{4}\sqrt{\frac{N}{m}}\right],$$

odhad pro pravděpodobnost úspěchu zůstává nezměněn. Algoritmus tedy v tomto případě proběhne v kratším čase, ovšem za cenu toho, že získáme pouze jeden prvek označené množiny vstupů. Pro zjištění dalších prvků je třeba fyzikální systém znovu uvést do počátečního stavu a algoritmus opakovat.

Na konec výčtu těchto základních vlastností Groverova algoritmu, které později postupně porovnáme s odpovídajícími vlastnostmi jiného vyhledávacího algoritmu, jímž se zabývá tento výzkumný úkol, uveďme, že dosažení jednotkové pravděpodobnosti úspěchu (pokud neuvažujeme

[2] Tohoto stavu je snadné dosáhnout z experimentálně přístupnějšího stavu, kdy všechny qubity jsou ve stavu $|0\rangle$: postačí postupně na každý aplikovat Hadamardovo hradlo. Jedná se tedy o faktorizovatelný stav.

chyby vnesené okolím) brání pouze omezení, že počet iterací je nutně celé číslo a geometricky odvozená hodnota se tedy musí zkreslit zaokrouhlením.[3] Toto tvrzení je i důvodem, proč větší databáze obecně umožňují dosažení lepší pravděpodobnosti úspěchu.

4. Kvantové náhodné procházení

Pro účely následujícího textu a přiloženého článku budeme potřebovat začlenit vsuvku o utvoření kvantové analogie k principu náhodných procházek, dobře známému příkladu aplikace matematické teorie Markovových procesů.

Tato analogie se nejsnáze zkonstruuje v případě náhodné procházky po vrcholech n-regulárního grafu. Pro její účely zavedeme Hilbertův prostor dimenze rovné počtu vrcholů grafu s ortonormální bází, jejíž vektory identifikujeme s jednotlivými možnými polohami chodce.

Kvantová náhodná procházka (diskrétní v čase) vyžaduje však kromě tohoto *prostoru polohy*, který označíme $\mathcal{H}_S$, ještě n-dimenzionální Hilbertův prostor $\mathcal{H}_C = \mathbb{C}^n$, který nazýváme *prostor mince*. Toto označení má původ v popisu kvantové náhodné procházky po přímce [7]. V analogii s „klasickou“ náhodnou procházkou na přímce, kde si chodec vybírá svůj další směr hodem mince, touto „kvantovou mincí“ se hází působením vhodně zvoleného unitárního operátoru na prostoru $\mathcal{H}_C$. Kvantová mince si tímto principem uchovává svou předchozí hodnotu. Toto neintuitivní chování se ukazuje jako nevyhnutelné, pokud chceme získat více než pouze triviální výsledky [8].

Stavový prostor kvantové náhodné procházky je tenzorovým součinem $\mathcal{H}_C \otimes \mathcal{H}_S$, prvky jehož ortonormální báze $|d, x\rangle = |d\rangle|x\rangle$ budeme identifikovat s chodcem stojícím na poloze x, jehož mince právě ukazuje d-tou hodnotu z n možných. Předpokládejme, že v každém vrcholu jsou jednotlivé hrany z něj vedoucí označeny možnými hodnotami mince (stejná hrana nemusí mít stejné číslo při pohledu z obou konců), takže mince určuje, po které hraně má chodec v dalším kroku přejít.

Jedna iterace kvantové náhodné procházky, která slouží jako analogie jednoho kroku klasické náhodné procházky, je složena z *operátoru mince* C, který provádí unitární transformaci nad každou n-ticí amplitud bázových vektorů $|d, x\rangle$ pro pevné x, a *operátoru kroku* S, který na bázové vektory působí dle naznačené identifikace jako jeden krok ve směru určeném mincí za zachování jejího stavu. Z podmínky linearity obou operátorů pak dodefinujeme obraz libovolné superpozice.

Důležité je, že mince nebudeme uvažovat pouze tvaru $C_0 \otimes I$. Jestliže rozložíme identitu v tomto tenzorovém součinu dle vztahu

$$C = C_0 \otimes \sum_{x \in V} |x\rangle\langle x| = \sum_{x \in V} C_0 \otimes |x\rangle\langle x|,$$

(V jsme označili množinu vrcholů grafu), můžeme zadefinovat *mince závislé na poloze*

$$C = \sum_{x \in V} |x\rangle\langle x| \otimes C_0(x). \tag{1}$$

[3] Optimální hodnota bez omezení na celou část je však určena mírně komplikovanějším výrazem než $\frac{\pi}{4}\sqrt{N}$.

Taková mince ponechává obraz libovolného bázového vektoru $|d, x\rangle$ v lineárním obalu bázových vektorů se stejným x a tak splňuje podmínku uvedenou v minulé sekci. Snadno zjistíme, že unitarita C je ekvivalentní unitaritě $C(x)$ pro všechna $x \in V$.

Stejně jako v teorii Markovových procesů je možné kromě procesů diskrétních v čase (označovaných jako Markovovy řetězce) zavást i procesy vyvíjející se spojitě, je možné zadefinovat i kvantové náhodné procházky spojité v čase, jejichž časový vývoj je popsán Schrödingerovou rovnicí s vhodně zvoleným Hamiltoniánem. Tento druh kvantových náhodných procházek je popsán například v [9]. Zajímavé je zmínit, že tyto procházky uměle přidaný prostor mince nevyžadují. Pro účely tohoto textu je však nebudeme potřebovat zavádět.

5. SKW algoritmus

Tento algoritmus je znám pod zkratkou jmen tří autorů článku [10], ve kterém byl v roce 2002 představen. Je prvním kvantovým algoritmem, který využívá náhodné procházky k řešení algoritmické úlohy vyhledávání v nesetříděné databázi, a tak propojuje předchozí sekce.

Důvodem, proč k již vyřešené úloze kvantového vyhledávání přistupovat s pomocí kvantových náhodných procházek, je fakt, že ve fyzikálních implementacích kvantového algoritmu může být výrazně snazší i spolehlivější využívat pouze operace, které působí na množství invariantních podprostorů malých dimenzí, jako jsou operace C a S. To je rozdíl oproti hradlům použitým v Groverově algoritmu, která „mixují“ dohromady amplitudy všech bázových stavů současně.

SKW algoritmus je také znám jako algoritmus vyhledávání na hyperkrychli. Prvky databáze, jejíž velikost je stejně jako v Groverově algoritmu omezena na mocniny dvojky, totiž identifikuje s vrcholy hyperkrychle,[4] a tak jinak nesetříděné databázi přidává strukturu grafu bez jakékoliv souvislosti s označeným prvkem.

V literatuře je možno nalézt popisy dalších vyhledávacích algoritmů, které využívají kvantové náhodné procházení na jiných grafech [11], ty však leží mimo rámec této práce.

Jak bylo zmíněno výše, SKW algoritmus je algoritmem využívajícím kvantovou náhodnou procházku. Jeho stavový prostor je tedy tenzorovým součinem prostoru pozice, který odpovídá stavovému prostoru n qubitů, s prostorem mince $\mathbb{C}^n$ a pomocným stavovým prostorem dalších qubitů potřebných pro orákulum. Poslední zmíněný prostor se opět neuvažuje a za stavový prostor se považuje součin $\mathcal{H}_C \otimes \mathcal{H}_S$.

Samotný SKW algoritmus pak má podobné rámcové rozčlenění průběhu jako Groverův algoritmus. Počáteční stav je stav, kde všechny bázové stavy $|d, x\rangle$ mají shodnou amplitudu.[5] Po předem daný počet iterací se na prostoru nechá probíhat kvantová náhodná procházka, jejíž mince je závislá na poloze ve smyslu vzorce (1), kde volba $C_0(x)$ je určena výsledkem volání orákula. Po předem daném počtu iterací se procházka ukončí a provede se úplné měření na prostoru polohy. Toto měření určuje jednoznačně jeden prvek databáze, který je s velkou pravděpodobností označeným prvkem.

[4] Snadno nahlédneme, že n-rozměrná hyperkrychle je n-regulární graf s $N = 2^n$ vrcholy.

[5] Jedná se opět o faktorizovatelný stav. Poznamenejme však, že pokud i $n = \log_2 N$ není mocninou dvojky, dosažení potřebného stavu registru mince vyžaduje konstrukci nestandardního kvantového hradla a může být složité.

Autoři SKW ve svém článku uvádějí, podobně jako Grover, matematický popis vývoje stavu v průběhu algoritmu. Jestliže probereme všechny vlastnosti Groverova algoritmu vyzdvižené v sekci 3, nalezneme s SKW mnoho podobných vlastností, ale i některé důležité rozdíly. Hlavní odlišností však je, že výpočty v SKW algoritmu jsou přibližné (jedná se o asymptotické odhady).

Prvním rozdílem podstatným pro výpočet je skutečnost, že nejmenší invariantní podprostor stavového prostoru SKW algoritmu, obsahující výchozí stav, má dimenzi $2n$, zatímco u Groverova algoritmu je dvourozměrný. Existuje však vektor s velkým překryvem s hledaným stavem takový, že stavový vektor se (za předpokladu dostatečné velikosti databáze) během průběhu odchýlí jen zanedbatelně od lineárního obalu výchozího stavu a tohoto vektoru. Je tedy možno říci, že tvrzení, že stavový vektor se pohybuje pouze ve dvourozměrném podprostoru, je asymptotické.

Doporučený počet iterací SKW algoritmu je určen přibližným vzorcem

$$t_f = \left[\frac{\pi}{\sqrt{8}} \sqrt{N} \right],$$

což oproti Groverově algoritmu větší o faktor $\sqrt{2}$. Po tomto počtu iterací je pravděpodobnost úspěchu odhadnuta asymptotickým vzorcem

$$P \geq \frac{1}{2} - O(1/n).$$

Tento vzorec má podobnou interpretaci jako v sekci 3: čím větší je databáze, tím lepší je zaručeno utlumení pravděpodobnosti chyby. Vykazuje však pomalejší konvergenci s rostoucí velikostí databáze, pouze dle převrácené hodnoty $n = \log_2 N$, navíc se tato závislost udává pouze v O-notaci. Hlavní a nejvíce zřetelný rozdíl je však v tom, že limitní hodnota pravděpodobnosti není 1, ale pouze 1/2. Pravděpodobnosti vyšší než tato hranice jsou ve výchozím znění algoritmu nedosažitelné.

Toto důležité zjištění znamená, že po průběhu algoritmu je nezbytné provést kontrolní dosazení nalezeného prvku do orákula. Jestliže dá orákulum negativní výsledek, je třeba stav systému znovu inicializovat a nechat celý algoritmus opakovat.

Průběh pravděpodobnosti úspěchu v závislosti na počtu iterací před měřením vykazuje, opět pro dostatečně velká N, stejnou oscilující závislost jako v Groverově algoritmu. Při menších velikostech databáze (význam tohoto slova je subjektivní, ale pro dobré srovnání jím rozumějme například $n \leq 5$) se však projeví nezanedbatelné korekce vůči zmíněnému dvourozměrnému podprostoru a k přibližně harmonickému průběhu se přidá zvlnění, které vede k poruchám monotonie růstu a poklesu pravděpodobnosti až k poruchám periodicity průběhu.

Fundamentální a nevyhnutelnou odchylkou od harmonického průběhu je, že pravděpodobnost úspěchu se mění jen s každou druhou iterací. Toto pozorování má velmi úzký vztah s tvrzením, že náhodná procházka po hyperkrychli (a mnoha jiných grafech) je Markovovým řetězcem s periodou 2 [12].[6]

Zobecnění SKW algoritmu na případ více označených prvků není v současné literatuře popsáno. Zčásti se mu věnuje přiložený článek [13], ve kterém na základě numerických výsledků

[6] Stejné abstraktní odůvodnění je pak použitelné pro vysvětlení snížené limitní pravděpodobnosti. Bez odkazu na Markovovy řetězce je pak vyjádřeno v přiloženém článku zavedením sudého a lichého podprostoru a rovnicemi (14).

pozorujeme zcela stejnou změnu ve vzorci pro optimální počet iterací: nahrazení N za podíl N/m. Podobně jako v Groverově algoritmu po tomto počtu iterací získáme informaci pouze o jednom náhodném označeném prvku. Drobné rozdíly oproti Groverově algoritmu spočívají v tom, že

- skutečný počet iterací, po kterém je pravděpodobnost úspěchu nejvyšší, vykazuje slabou závislost na vzájemné poloze a symetrii rozložení označených prvků na hyperkrychli a
- pravděpodobnost obecně není rozložena mezi označené prvky rovnoměrně. Tato vlastnost není v článku explicitně zmíněna. Součástí některých prováděných numerických simulací bylo počítání standardní odchylky, které kromě speciálně symetrických rozložení dávalo nenulové výsledky.

6. Optimalizace SKW algoritmu

SKW algoritmus se nabízí jako možná náhrada Groverova algoritmu. Vykazuje však několik rozdílů, z nichž některé jsou silnými argumenty v jeho neprospěch, zvláště pak, že limitní dosažitelná pravděpodobnost úspěchu v jednom běhu algoritmu je 1/2 namísto 1. To znamená, že kontrolní ověření výsledku dá s mnohem větší pravděpodobností negativní výsledek a algoritmus je třeba opakovat. Pravděpodobnost úspěchu je sice možno zvýšit libovolně blízko jistotě po $O(1)$ opakováních algoritmu, kde tento počet pro velká N je přibližně

$$r_\varepsilon = -\lceil \log_2 \varepsilon \rceil,$$

kde ε je hranice, pod kterou chceme snížit pravděpodobnost chyby, tento počet však v žádném případě nemůže soupeřit s odpovídající hodnotou v případě Groverova algoritmu. Dalším rozdílem, přestože menšího významu, je počet dotazů na orákulum, který je v případě SKW větší oproti Groverově algoritmu faktorem $\sqrt{2}$.

První otázkou je, čím je rozdíl v dosažitelné pravděpodobnosti úspěchu způsoben, tedy, pokud možno, jak je zbytek pravděpodobnosti rozložen mezi další vrcholy kromě označeného. Dalším krokem pak je najít způsob, jak případně tuto informaci využít k lokalizaci označeného vrcholu a tak tuto pravděpodobnost v důsledku přidat k pravděpodobnosti úspěchu.

Přiložený článek [13] poskytuje odpověď na obě tyto otázky. Ukazuje, že je skutečně možno SKW algoritmus optimalizovat přiblížením jeho vlastností ke Groverově algoritmu a tím i k teoretické ideální hranici. Článek navrhuje několik možných způsobů, jak SKW algoritmus pozměnit pro dosažení tohoto cíle. V případech, kdy umožníme i silnější zásahy do samotného rámce SKW algoritmu, je možno dosáhnout nejen pravděpodobnosti úspěchu $1 - O(1/n)$, ale i snížení počtu potřebných iterací na hodnotu stejnou jako v Groverově algoritmu.

Považujeme tento výsledek za užitečný z hlediska možné realizace kvantového algoritmu pro řešení skutečné úlohy, ale i za podstatný z teoretického hlediska: propojuje významně dva algoritmy, které k řešení stejné algoritmické úlohy používají dva zdánlivě nepříbuzné způsoby.[7]

[7] Na Groverův algoritmus je možno pohlížet jako na podobně utvořenou náhodnou procházku na úplném grafu nade všemi prvky databáze, což tento rozdíl zmenšuje. SKW algoritmus však používá náhodnou procházku na regulárním grafu exponenciálně menšího řádu.

Závěr

Ve článku [13] se nám podařilo nalézt několik reálně využitelných strategií určených pro zvýšení pravděpodobnosti úspěchu v SKW algoritmu nad hranici jedné poloviny. Různé strategie vyžadují zásahy do různých částí průběhu algoritmu (kromě nejslabší, první uvedené varianty) a přinášejí podobný výsledek využitím odlišných principů. Poslední dvě uvedené varianty kromě zvýšení pravděpodobnosti úspěchu ještě dosáhnou konečného stavu s menší časovou složitostí a tak ještě více přibližují vlastnosti upraveného SKW algoritmu Groverově algoritmu, který je velice blízký teoretické optimální hranici.

Článek byl v době odevzdání výzkumného úkolu zaslán do časopisu Physical Review A. V aktuální verzi je k dispozici na internetové službě arXiv [13].

Použitá literatura

[1] Potoček, V. *Quantum Algorithms.* Praha, 2007. 72 s. Bakalářská práce na Fakultě jaderné a fyzikálně inženýrské Českého vysokého učení technického v Praze

[2] Nielsen, M. A., Chuang, I. L. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000. 676 s.

[3] Shor, P. W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* arXiv:quant-ph/9508027v2

[4] Boyer, M., Brassard, G., Høyer, P., Tapp, A. *Tight bounds on quantum searching.* arXiv: :quant-ph/9605034v1

[5] Grover, L. K. *A fast quantum mechanical algorithm for database search.* arXiv:quant-ph/ /9605043

[6] Brassard, G., Høyer, P., Mosca, M., Tapp, A. *Quantum Amplitude Amplification and Estimation.* arXiv:quant-ph/0005055v1

[7] Ambainis, A. *Quantum walks and their algorithmic applications.* arXiv:quant-ph/0403120

[8] Meyer, D. A. *On the absence of homogenous scalar unitary cellular automata.* arXiv:quant-ph/9604011v2

[9] Kempe, J. *Quantum random walks – an introductory overview.* Contemporary Physics, 44, s. 307–327, 2003

[10] Shenvi, N., Kempe, J., Whaley, K. *Quantum Random Walk Search Algorithm.* arXiv:quant-ph/0210064

[11] Childs, A. M., Goldstone, J. *Spatial search by quantum walk.* arXiv:quant-ph/0306054v2

[12] Wikipedia, the free encyclopedia. *Markov chain.* <http://en.wikipedia.org/wiki/Markov_ _chain> [rev. 23. 6. 2008, cit. 24. 6. 2008]

[13] Potoček, V. *Optimized quantum random-walk search algorithms.* arXiv:quant-ph/0805.4347 [quant-ph]