Akadémiai Doktori Értekezés Tézisei

Ivanyos Gábor

Classical and quantum algorithms for algebraic problems

(Klasszikus és kvantum-számítógépes algoritmusok algebrai problémákra)

2007

1. Bevezetés

1.1. A vizsgált feladatok

Az értekezésben különféle algebrai problémák algoritmikus vonatkozásait tárgyaljuk. Ezen problémák egy jó része mátrixalgebrák, illetve modulusok struktúrájával kapcsolatos. Az ilyen feladatok maguktól értetődően adódnak például csoportok számítógépes reprezentációelméletében, de felvetődnek más struktúrákkal, például Lie-algebrákkal kapcsolatos számítások során is. Hatékony megoldásuk jelentős szerepet játszik például a GAP [13] és a MAGMA [2] számítógépes algebrai rendszerekben.

A mátrixalgebrás problémák mellett foglalkozunk olyan kérdésekkel is, mint véges kommutatív csoport szorzótáblájának tesztelése, mint kvantum-kapukészletek számítási erejének algoritmikus vizsgálhatósága, vagy mint az úgynevezett rejtett részcsoport problémája. Ez utóbbi közös általánosítása olyan feladatoknak, amelyek megoldásában a kvantumszámítógépekre tervezett algoritmusok exponenciálisan gyorsabbak az ismert klasszikus módszereknél és olyan érdekes problémáknak (például gráfok izomorfiájának eldöntése), amelyeknek bonyolultságát intenzíven vizsgálják.

1.2. Az alkalmazott módszerek

A dolgozatban kitüntetett szerepet játszanak a véletlent használó algoritmusok, de bemutatunk determinisztikus eljárásokat is, ezek között egy olyan eredménnyel, amely egy viszonylag egyszerű randomizált algoritmust helyettesít hatékony determinisztikus módszerrel. Ez utóbbival hozható párhuzamba az az eredményünk, amelyben egy – a kvantumos világban természetesen adódó – kvantumgépes módszert váltunk ki klasszikus randomizált algoritmussal egy kicsi többletinformáció elérhetőségének feltételezése mellett. A rejtett részcsoport problémakörében elért kvantumgépes eredményünkben az alapvető technikai összetevő egyfajta statisztikai döntési eljárás. A kapukészletek számítási erejével kapcsola-

tos módszerünk ugyanakkor mélyebb algebrai eredmények felhasználásán alapszik.

1.3. Az értekezés szerkezete

A disszertáció tíz fejezetből áll. Ezek közül az első a legfontosabb eredményeket foglalja össze, a második pedig a vizsgált problémák elméleti hátterét és a felhasznált algoritmikus módszereket tekinti át. Itt a többi témánál részletesebben tárgyaljuk azt a kvantumgép-modellt, amelyet a későbbiekben használunk.

Eredményeinket a hátralevő nyolc fejezetben mutatjuk be. Ezek közül öt foglalkozik mátrixalgebrákkal, illetve asszociatív algebrák feletti modulusokkal. Ebben a részben kitüntetett szerepet játszik a Jacobson-radikál, az algebra legbővebb nilpotens ideálja. Az utolsó három fejezetben kvantum-számítógépekkel kapcsolatos eredményeket mutatunk be.

2. A fő eredmények

2.1. Algoritmusok mátrixalgebrákra és modulusokra

Az eredmények első csoportja mátrixalgebrákkal és modulusokkal kapcsolatos algoritmikus problémákra vonatkozik. Az ilyen algoritmusok fontos szerepet játszanak a számítógépes matematika különböző területein. Már szó volt a számítógépes reprezentációelméletről és a Lie-algebrákkal kapcsolatos számításokról. Itt hadd említsünk még egy alkalmazási irányt. A mátrixalgebrás eljárások fontos építőkövei a [32] és a [22] dolgozatokban javasolt nemkommutatív számelméleti algoritmusoknak, amelyek váratlanul szerephez jutottak a többcsatornás kommunikációban újabban alkalmazott kódolási eljárásokban [20].

A mátrixalgebrákkal kapcsolatos korai algoritmikus jellegű eredmények közül itt L. E. Dickson 1923-ban megjelent művéből [5] a nulla karakterisztikájú alaptest fölötti algebrák radikáljának számításra kiválóan alkalmas karakterizációját említenénk. Algebrák struktúrájának kiszámí-

tására szolgáló *polinom idejű* módszerek első szisztematikus gyűjteménye Friedl Katalin és Rónyai Lajos 1983-as munkájában [12] lelhető fel. Azóta a tárház jelentős mértékben bővült, immár a gyakorlatban legfontosabb alaptestek feletti mátrixalgebrák legtöbb strukturális invariánsa kiszámolható polinom időben.

Mint már említettük, eredményeink ezen csoportjában kitüntetett szerepet játszik az egyik fontos strukturális invariáns, a Jacobson-féle radikál (a rövidség kedvéért: radikál). Egy A asszociatív algebra $\mathrm{Rad}(A)$ radikálja A-nak a legnagyobb nilpotens ideálja. Különféle alaptestekre ismertek a Dickson-féle jellemzés általánosításán alapuló módszerek, amelyek a radikált (szemi-)lineáris egyenletrendszerek megoldásával számítják ki. Véges alaptestekre Rónyai Lajos adott először polinom idejű módszert [31], ennek W. Eberly készítette el egy a nem prímtest feletti algebrákra valamivel hatékonyabban működő változatát [8]. Véges testek transzcendens bővítései feletti algebrákra a [23] dolgozatban található módszer, amelyet differenciálalgebrában felmerülő problémák megoldására is lehet használni [14]. A legáltalánosabb p karakterisztikájú testek felett működő hatékony módszer a [3] dolgozatban található. A működéshez egy olyan kiegészítő eljárás szükséges, amely megoldja az alaptest felett az $a_1x_1^p + \ldots, a_mx_m^p = 0$ alakú – úgynevezett *p-szemilineáris* – egyenleteket.

Az [I01] dolgozat alapján készült rövid harmadik fejezetben a radikálszámítás egy alkalmazását mutatjuk be mátrixfélcsoportokra:

- Polinom időben eldönthető, hogy egy véges test konstans transzcendenciafokú bővítése feletti, generátorokkal adott mátrixfélcsoport véges-e.

Az [I99] cikken alapuló negyedik fejezet fő eredményeinek ismertetését egy kis kerülővel kezdjük. Említettük, hogy p karakterisztikában a [3] dolgozat módszere p-szemilineáris egyenletrendszerek megoldásán múlik. Az $x_1^p - ax_2^p = 0$ nemnulla megoldásainak a megtalálása nyilván az a

együttható p-edik gyökének kiszámításával egyenértékű. Gyökvonás márpedig csupán a testműveleteket használó algoritmussal nem lehetséges: egy testelem p-edik gyökének létezése általános alaptest felett algoritmikusan eldönthetetlen. Következésképpen – ahogy W. Eberly megmutatta [7] – kommutatív mátrixalgebrák radikáljának kiszámítására sincsen általános, csak a testműveleteket használó módszer. Ennek kapcsán azt sejtette, hogy nincs további nehézség a nemkommutatív esetben. A [3] dolgozat alapján az adódik, hogy a *kiszámíthatóság* szintjén tényleg ez a helyzet, de a módszer nem ad meg polinom idejű redukciót *egyetlen* kommutatív algebra radikáljának kiszámítására. Többek közt az ilyen visszavezetés létezésének kérdése kapcsán kezdtük el vizsgálni a radikál kiszámításának lehetséges alternatív (azaz *nem* a Dickson-féle jellemzés általánosításain alapuló) módszereit.

Párhuzamosan W. A. de Graaf egy, a nulla karakterisztikájú Lie-algebrák radikáljának kiszámítására szolgáló *praktikus* algoritmuson dolgozott [15], amely sebességében a gyakorlatban sokkal gyorsabbnak bizonyult a Dickson-féle jellemzéshez hasonló tételen alapuló "hagyományos" módszernél. W. A. de Graaf eljárása úgynevezett Cartan-részalgebrák kiszámításán (ld. [17]) alapul. Módszerének gyakorlatban mutatott sikeressége alapján arra jutottunk, hogy az asszociatív esetben bizonyos kommutatív részalgebrák (úgynevezett maximális tóruszok) hasznosak lehetnek. (Megjegyezzük, hogy asszociatív algebrák Lie-algebrájában a Cartan-részalgebrák a maximális tóruszok centralizátorai. Az sem mellékes, hogy maximális tóruszok determinisztikus polinom idejű algoritmussal találhatók [16], sőt, sokféle alaptest esetében véletlen elemek segítségével nagyon gyorsan kaphatók.) A negyedik fejezet egyik fő eredménye, hogy az új megközelítés megadja a keresett redukciót:

- Egy A mátrixalgebra radikáljának a kiszámítása determinisztikus polinom idejű algoritmussal visszavezethető egy olyan kommutatív algebra radikáljának a kiszámítására, amely faktora A egy részalgebrájának.

A bemenet olyan mátrixokból áll, amelyek generálják A-t. A kimene-

tet pedig olyan mátrixok alkotják, amelyek által generált ideál $\mathrm{Rad}(A)$. Ugyanez az eredmény (csak egy másik polinommal az időkorlátot illetően), ha a kimenetben és/vagy a bemenetben lineáris bázisokat követelünk meg. A bonyolultságot a végrehajtott testműveletek számában mérjük.

Annak kedvéért, hogy megmutathassuk a kapcsolatot a következő két fejezet tartalmával, megemlítjük, hogy a fenti algoritmust megalapozó struktúratételek azt mondják ki, hogy $\mathrm{Rad}(A)$ felbomlik két lineáris alterének összegére, amelyekből az egyik a T maximális tórusz centralizátorának a radikálja által generált ideál, a másik pedig a kommutátorokból álló $[A, C]$ altér, ahol C a T tórusz azon elemeiből áll, amelyek centrálisak modulo $\mathrm{Rad}(A)$. A későbbiekben C-re mint T szemi-centrális részére és az $[A, C]$ altérre mint $\mathrm{Rad}(A)$ kommutátor-részére hivatkozunk. Természetesen ahhoz, hogy a C szemi-centrális részt $\mathrm{Rad}(A)$ előzetes ismerete nélkül kiszámítsuk, szükségünk van C egy alternatív jellemzésére. Egy ilyen jellemzést meg is adunk a dolgozatban.

Kidolgoztunk egy, a fent említett redukciós módszer elvi részein alapuló véletlent használó módszert is, amely olyan perfekt testek felett működik, amelyekben polinomok négyzetmentes részét hatékonyan ki lehet számítani. Az algoritmust egy kiegészített input modellel írtuk le: feltételeztünk egy olyan eljárás segítségét is, amely A-nak bizonyos algebrai értelemben vett "véletlen" elemeit állítja elő. A "véletlen" alatt azt értjük, hogy a eljárás által kiadott elemek jó eséllyel elkerülik rögzített alacsony fokú polinomok zérushelyeit. Megjegyezzük, hogy ez a feltétel közvetve azt is maga után vonja, hogy az alaptestnek "elég nagynak" kell lennie. Fordítva, ha az alaptest "elég nagy" és A-nak egy lineáris bázisa adott, akkor egy ilyen eljárás $O(n^4)$ időben implementálható elég nagy tartományból véletlenül választott együtthatókkal vett lineáris kombinációk segítségével. Ugyanakkor ha A-nak csak algebra generátorai állnak rendelkezésre, a később részletesebben is tárgyalandó MeatAxe [21] programrendszer véletlenelem-generátora néhány mátrixszorzás árán a gyakorlatban jól használható elemeket ad. Algoritmusunk eredménye egy olyan

rendszer, amely mint ideált generálja $\mathrm{Rad}(A)$-t. Egy ilyen rendszerből persze polinom időben kiszámolható $\mathrm{Rad}(A)$ egy lineáris bázisa is, de nagy dimenziós radikál esetén ez a polinom elég magas fokú. Ugyanakkor sok gyakorlati esetben tényleg elég ideál-generátorokat megadni. Randomizált algoritmusunk bonyolultságát itt az egyszerűség kedvéért abban a fontos speciális esetben ismertetjük, amikor a generátorok száma konstans.

- Tegyük fel, hogy K egy perfekt test és az $A \leq M_n(K)$ mártix-algebra m generátorral adott, ahol m konstans. Ekkor nagyjából $O(n^4)$ alapművelettel előállítható mátrixok egy olyan rendszere, amely által generált ideál éppen $\mathrm{Rad}(A)$.

Fent $M_n(K)$-val a szokásoknak megfelelően a K test elemeiből álló $n \times n$-es mátrixok alkotta algebrát jelöltük. Az eredmény pontos leírása az értekezésben Theorem 4.3 cím alatt szerepel. Az algoritmus Monte Carlo típusú, azaz kis valószínűséggel az output lehet hibás is. A hiba valószínűsége a szokásos módon – ismétléssel – exponenciálisan kicsivé tehető. A fenti hozzávetőleges ismertetésben a durva $O(n^4)$-es korlátból elhagytunk polilogaritmikus faktorokat. Elhanyagoltuk továbbá nagyjából $O(n)$ algebrai értelemeben vett véletlen elem előállításának és ugyanannyi polinom négyzetmentes részének a költségét. Az $O(n^4)$-es korlát polilogaritmikus faktor erejéig akkor igaz tehát, ha a K test felett a polinomok négyzetmentes része kiszámítható $O(n^3)$ művelettel és $O(n^3)$ művelettel nyerhetők "véletlen" elemek A -ból. Megjegyezzük, hogy nulla karakterisztikában vagy véges testek felett az előbbi feladat közel lineáris időben megoldható. Ha A bázisa is adott és a véletlen elemeket véletlen lineáris kombinációk képzésével állítjuk elő, akkor a módszer költsége (a legtöbb fontos alaptest felett) nagyjából $O(n^5)$. Az összehasonlítás kedvéért megjegyezzük, hogy 0 karakterisztikában a Dickson-féle jellemzésen alapuló módszer költsége tudomásunk szerint legalább n^6-os nagyságrendű.

Az ötödik és hatodik fejezetekben a fenti módszerével közeli rokonságban álló alapelveken működő algoritmusokat ismertetünk *véges testek*

feletti algebrák radikáljának kiszámítására. Ezekben a fenti algebrai véletlen elemek konstruálhatósága helyett azt tesszük fel, hogy egy olyan segédeszköz áll rendelkezésre, amely az algebra véletlen elemeit adja az *uniform* (vagy legalábbis megközelítőleg uniform) eloszlás szerint.

Sok esetben – mint például a már érintőlegesen említett MeatAxe rendszer esetében – elegendő a radikál egy nemtriviális elemét előállítani. A MeatAxe egy széles körben elterjedt eljárásgyűjtemény véges testek feletti algebrák feletti modulusok kezelésére. A legfontosabb alkotóelem egyfajta konstruktív irreducibilitás-teszt, amely reducibilis modulusokban talál egy nemtriviális részmodulust. R. Parker eredeti módszere [30] a gyakorlatban kitűnően működik kis alaptestek esetén. D. F. Holt és S. Rees kidolgozott egy általánosabb esetben is hatékony, véletlen elemeket használó eljárást. Az új módszer elméletben is és a gyakorlatban is igen jól teljesít tetszőleges véges alaptest felett, kivéve néhány speciális szerkezetű algebraosztályt. Észrevettük, hogy ezekben a kedvezőtlen esetekben a radikál "kommutátor-része" (ld. fentebb) játszik jelentős szerepet. Az is kiderült, hogy a rossz esetekben egy primitív idempotenssel helyettesíteni lehet a maximális tórusz szemi-centrális részét. Primitív idempotens pedig igen jó eséllyel nyerhető véletlen elem karakterisztikus polinomjának felbontása segítségével. Ezt a gondolatmenetet az [IL00] dolgozat alapján készült ötödik fejezetben fejtjük ki részletesen. Az eredmény a következő:

- A Holt-Rees–féle MeatAxe eljárás lényeges lassulás nélkül kiegészíthető egy olyan algoritmussá, amely pozitív konstans valószínűséggel minden reducibilis modulusban talál egy valódi részmodulust.

A kiegészítéssel együtt a MeatAxe eljárás egy Las Vegas típusú algoritmussá válik. Egy Las Vegas típusú randomizált eljárás kis valószínűséggel lehet sikertelen, de sosem ad hibás kimenetet. Kicsit konkrétabban, a kiegészített MeatAxe pozitív konstans valószínűséggel vagy egy irreducibilitás-bizonyítást, vagy egy valódi részmodulust talál. Az ötödik

fejezetben leírt eljárást először a C-MeatAxe csomagban, majd később a GAP [13] és a MAGMA [2] rendszerekben is implementálták.

Algebrák radikáljának kiszámítására szolgáló, általános test felett működő módszerünkben a szűk keresztmetszetnek a maximális tórusz szemicentrális részének a kiszámítása bizonyult. Párhuzamosan W. Eberly és M. Giesbrecht javasolt egy igen gyors módszert véges testek feletti féligegyszerű (triviális radikállal rendelkező) algebrák felbontására [9]. Dolgozatukban ők is az algebra véletlen elemeinek konstruálhatóságát feltételezték. Felvetették, hogy ki lehet-e terjeszteni eljárásukat nemtriviális radikál esetére is. Az [I00] dolgozat alapján készült hatodik fejezetben egy ilyen kiterjesztéssel foglalkozunk. Eberly és Giesbrecht észrevette, hogy fő eszközük, a primitív idempotensek egy teljes ortogonális rendszerének hatékony konstruálhatóságára vonatkozó eredményük érvényes az általános esetben is. Ezen a nyomon indultunk el. Primitív idempotensek teljes ortogonális rendszere egy maximális *felhasadó* tórusznak felel meg. Módszerünk lényege az, hogy egy ilyen tórusznak a szemi-centrális része gyorsan megtalálható. A felhasznált eszközök segítségével ez után az eredeti célnál egy kicsit többet is el lehet érni: nemcsak a radikál, hanem egy Wedderburn-komplemens (a radikál szerinti faktorral izomorf részalgebra) is megkonstruálható hatékonyan. Eredményünk konstans sok generátorral megadott algebrák esetére nagy vonalakban a következő:

- Tegyük fel, hogy K egy véges test és az $A \leq M_n(K)$ algebra m generátorral adott, ahol m állandó. Ekkor nagyjából $O(n^3)$ műveletet felhasználó Las Vegas típusú módszerrel megtalálható mátrixoknak egy olyan rendszere, amely által generált algebra A-ban egy Wedderburn-komplemens, továbbá egy olyan rendszer is, amely által generált ideál A radikálja.

Megjegyezzük, hogy módszerünknek egy Monte Carlo típusú változata (ahol a válasz helyessége nem garantált) $O(n^3)$-nél valójában alacsonyabb bonyolultságú: polilogaritmikus számú mátrix összeszorzásának a költségével arányos, akárcsak Eberly és Giesbrecht eljárása.

A mátrixalgebrákkal és modulusokkal foglalkozó fejezetek közül az utolsóban, a [CIK97] dolgozat egyes részei alapján készült rövid hetedik fejezetben egy egyszerű feladat megoldására mutatunk determinisztikus polinom idejű módszert. A feladat modulusok izomorfiájának konstruktív változata: döntsük el, hogy két modulus izomorf-e, és ha igen, adjunk is meg izomorfizmust. Ha az alaptest elég nagy, a feladatra egyszerű randomizált módszer adódik: ha a két modulus izomorf, akkor egy véletlenül választott morfizmus az egyikből a másikba valójában izomorfizmus lesz. Itt az izgalmas kérdés az, hogy helyettesíthető-e a véletlent használó módszer polinom idejű determinisztikussal. Megmutatjuk, hogy a legtöbb fontos alaptest felett igen:

- Tegyük fel, hogy K egy olyan test, amely feletti mátrixalgebrák radikáljának kiszámítására polinom idejű determinisztikus algoritmus van. Ekkor K-algebrák feletti modulusok konstruktív izomorfizmusproblémájára is van polinom idejű determinisztikus módszer.

Látható, hogy ebben a fejezetben is fontos szerepet kap a radikál kiszámítása. Itt történetesen azért, mert a fejezet fő technikai eszköze, a ciklikus modulusok generátorát előállító determinisztikus algoritmus általában nem működik a nem-féligegyszerű esetben. Megjegyezzük továbbá, hogy a vizsgált feladat speciális esete az először J. Edmonds által [10] felvetett és azóta is sokat vizsgált kérdésnek: létezik-e hatékony determinisztikus módszer maximális rangú mátrix keresésére mátrixok lineáris tereiben. A feladat gazdag és tartalmas kombinatorikai kapcsolataival foglalkozik Lovász László cikke [28]. Domokos Mátyás a problémával közeli rokonságban álló invariánselméleti eredményeket ért el a [6] és egyes azt követő publikációiban.

2.2. Kvantum-számítógépekkel kapcsolatos eredmények

R. P. Feynmann vetette fel először azt az ötletet, hogy a kvantumjelenségeket esetleg hatékony számításra fel lehet használni [11]. A kvantum-számítógép modelljeinek kidolgozása és néhány a kvantum-

géppel a klasszikusnál hatékonyabban megoldható – játékos jellegű – feladat felfedezése után P. Shor publikálta 1994-ben az első két igazán életszagú alkalmazást [33, 34]: az egészek törzstényezős felbontását elvégző, valamint a diszkrét logaritmust kiszámoló polinomidejű kvantumalgoritmusát. Nem sokkal Shor eredményeinek bemutatását követően jelent meg L. Grover kvantumgépes algoritmusa [18], amellyel egy n elemű adatbázisban $\sqrt{n}$ lekérdezéssel lehet keresni. Ezek az eredmények jelentős lökést adtak a kvantum-számítógépek fizikai megvalósítására irányuló próbálkozásoknak, és felkeltették az érdeklődést a számítási problémák kvantum-számítógépes algoritmikus bonyolultsága iránt is. A dolgozat utolsó három fejezetében ilyen területeket érintő eredményeket mutatunk be.

Az [I07] dolgozat alapján készült nyolcadik fejezet összekapcsolja az értekezés reprezentációelméleti részét a kvantumgépekkel kapcsolatos problémákkal. Itt azonban algebrák reprezentációi helyett csoportok reprezentációit tekintjük. Önmagában a bemutatott algoritmus nem nehéz, a helyességének az igazolása viszont nagyon is az. A vizsgált algoritmikus kérdés tulajdonképpen kvantumgépek fizikai megvalósításával kapcsolatos: annak eldönthetősége, hogy eszközök – úgynevezett kvantum kapuk – egy adott készlete alkalmas-e arra, hogy általános kvantum-számítógépet építhessünk belőle.

Valamivel részletesebben, egy n kvantum bites kapu egy unitér transzformáció az n kvantum bit állapotait magában foglaló 2^n dimenziós komplex euklideszi téren. Egy n bites kapu $N(N-1)\cdots(N-n+1)$ féleképpen csatlakoztatható $N \geq n$ bitre, így ennyiféleképpen fogható fel N kvantum bites kapuként. Azt mondjuk, hogy n kvantum bites kapuk egy készlete *N-univerzális*, ha a készletbeli kapuk összes N-bitre való csatlakoztatásából nyert készlet a 2^N dimenziós téren ható unitér csoportnak egy sűrű részcsoportját generálja. Ez annak felel meg, hogy minden N bites transzformáció tetszőleges pontossággal megközelíthető a készletből vett kapukból álló eszköz segítségével. Valamivel pontosabban: Itt a sűrűséget projektív értelemben – tehát modulo a skalármátrixok – kell te-

kinteni, ugyanis egyenértékűnek számítanak az olyan kvantum-állapotok, amelyek egymás skalárszorosai.

Viszonylag egyszerűen igazolható, hogy $N \geq \max\{2, n\}$-re az N-univerzalitás egy N-ben monoton tulajdonság. Tehát ha egy $n > 1$ kvantum bites készlet N-univerzális valamely $N \geq n$-re, akkor N'-univerzális minden $N' > N$-re is. Ez alapján $n > 1$ esetén egy n kvantum bites kapukészletet univerzálisnak nevezünk, ha létezik olyan $N > n$, melyre a készlet N-univerzális. Az univerzalitás egyfajta *végső soron* való alkalmasságot jelent általános kvantum-számítógép építésére. Adott N-re az N-univerzalitás tesztelése eldönthető a generált csoport Zariski-lezártjának kiszámítása útján, például H. Derksen, E. Jeandel és P. Koiran módszerével [4]. Ebből – hacsak nem tudunk valamilyen korlátot adni a legkisebb olyan N-re, amelyre egy univerzális kapukészlet már N-univerzális – nem következik azonnal, hogy az univerzalitás algoritmikusan eldönthető. A nyolcadik fejezet fő eredménye szerint azonban megadható egy ilyen korlát:

- Ha egy n kvantum bites kapukészlet univerzális, akkor már N-univerzális bármely $N \geq 255n$-re. Következésképpen az univerzalitás algoritmikusan eldönthető tulajdonság.

Megközelítésünkből valójában az is adódik, hogy egy m elemű készletre az N-univerzalitás eldönthető egy $m \cdot 2^{O(N)}$ egyenletből álló $2^{O(N)}$-változós homogén lineáris egyenletrendszer segítségével. Sűrű reprezentáció esetén, azaz ha az input a kapukat leíró mátrixok $m \cdot 2^{2n}$ eleméből áll, $N = 255n$-re az egyenletrendszer mérete még mindig polinomiális n-ben, igaz, nagyon nagy kitevővel. A korlát bizonyítása egyrészt R. Guralnick és P. H. Tiep egy, a véges csoportok reprezentációelmélete területéről való 2005-ös, a véges egyszerű csoportok osztályozását falhasználó eredményét [19], másrészt D. Lazard nulldimenziós ideálok Hilbert-függvényének regularitására vonatkozó korlátját [27] használja fel. Figyelemre méltó, hogy a véges egyszerű csoportok osztályozása szerepet játszik egy ilyen, látszatra numerikus jellegű problémánál.

A kilencedik fejezetben az [FIMSS03] dolgozat egyes eredményei, illetve az [FIMSS03] függelékében megjelent módszert alaposabban kifejtő [I07pre] cikk alapján egy olyan kvantum-algoritmust mutatunk be, amely rejtett részcsoportokat talál feloldható csoportok egy bizonyos osztályában.

Mindazok a számítási feladatok, amelyekre a mai napig a klasszikusnál exponenciálisan gyorsabb kvantum-algoritmust találtak, többé-kevésbé közel állnak az úgynevezett rejtett részcsoport problémájához. Ezzel a feladattal közös keretbe foglalhatók a Shor által megoldott problémák – diszkrét logaritmus számítása, továbbá egészek multiplikatív rendjének kiszámítása modulo összetett számok (ez utóbbi a faktorizációban szerepet játszó eszköz) – és még több más érdekes feladat is. Közelebbről, a rejtett részcsoport problémája a következő. Tegyük fel, hogy – egy hatékony kiértékelő algoritmus vagy egy orákulum segítségével – adott egy, a G véges csoporton értelmezett f függvény, amelyre az teljesül, hogy van G-nek egy olyan H részcsoportja (a *rejtett részcsoport*), amelyre az igaz, hogy az $f(x)$ és az $f(y)$ értékek akkor és csak akkor egyenlők, ha $xH = yH$ (szavakban: x és y a H részcsoportnak ugyanabba a baloldali mellékosztályába esik). A feladat a H részcsoport meghatározása, lehetőleg az ábrázolási méretben (azaz $\log|G|$-ben) polinom időben. Míg kommutatív csoportokra tényleg létezik polinom idejű megoldás ld. [26, 29], a nemkommutatív csoportok esete jelenleg is intenzíven vizsgált terület (nem kis részt azért, mert például gráfok izomorfizmusának kérdése is felfogható természetes módon egy rejtett részcsoport-problémaként a szimmetrikus csoportban). Az intenzív erőfeszítések ellenére az összes csoport, amelyre jelenleg polinom idejű kvantum-algoritmus ismert rejtett részcsoportok megdatálására igen közel áll ahhoz, hogy kommutatív legyen. Ilyen csoportok egy viszonylag széles osztályára mutatunk be módszert a kilencedik fejezetben.

- Kvantum-számítógéppel polinom időben megoldható a rejtett részcsoport problémája olyan véges, konstans feloldható hosszúságú csoportokban, amelyeknek a kommutátor részcsoportja konstans

exponensű.

Megjegyezzük, hogy 2003-ban, amikor az [FIMSS03] dolgozat megjelent, a fent említett osztály tartalmazta majdnem az összes ismert polinom idejű rejtett részcsoportkeresővel rendelkező csoportot. Jelenleg az említésre érdemes kivételek bizonyos olyan nilpotens csoportok, amelyeknek a kommutátor részcsoportja már kommutatív, ld [1, 24, 25]. Az eljárásban alkalmazott módszer egy, a rejtett részcsoport problémájának alkalmasan megválasztott általánosításán alapuló indukció, ahol az indukciós lépés voltaképpen az általánosított Reed-Muller–kódok elvén működő statisztikai döntés.

Az értekezés utolsó, tizedik fejezete az [FIS05] dolgozat bizonyos részei alapján készült. Az eredmény a hetedik fejezet algoritmusával hozható párhuzamba. Ott egy véletlent használó klasszikus algoritmust váltottunk ki hatékony determinisztikussal, itt egy kvantum-algoritmussal viszonylag egyszerűen megoldható feladatban keressük azt, hogy hatékony megoldásához mennyi szükséges a kvantum-számítógép erejéből. Megmutatjuk, hogy a kvantum-algoritmus kiváltható polinom idejű klasszikus randomizált módszerrel, feltéve, hogy kezünkben van egy csoportelemek rendjének többszörösét kiszámoló eljárás. Tehát a kvantum-gép erejéből valójában valamivel kevesebbet is elég használni, mint Shor nevezetes algoritmusa.

- Egy véges halmazon adott bináris műveleti tábláról a tábla méretének *logaritmusában* polinom idejű klasszikus randomizált módszerrel tesztelhető, hogy egy adott számot osztó exponensű kommutatív csoport szorzótáblája-e. A tesztelő algoritmusokkal szemben szokásosan támasztott követelmények szerint az algoritmus mindig elfogadja a megfelelő csoportok szorzótábláit és nagy valószínűséggel elutasítja azokat, amelyek "távol" állnak egy megfelelő csoport szorzótáblájától.

A fent alkalmazott távolság egyfajta *szerkesztési* (az átírás mellett törlést és beszúrást is megengedő) távolság relatív változata. Megjegyezzük,

hogy a hasonló feladatokra korábban ismert legjobb tesztelő módszerek enyhén szublineárisak voltak a táblázat méretében, tehát ezekhez képest exponenciális gyorsulást sikerült elérni.

Az értekezés alapjául szolgáló publikációk

[CIK97] A. Chistov, G. Ivanyos, M. Karpinski, Polynomial time algorithms for modules over finite dimensional algebras, *Proc. 1997 ISSAC, 68–74.*

[FIMSS03] K. Friedl, G. Ivanyos, F. Magniez, M. Santha, P. Sen, Hidden translation and orbit coset in quantum computing, *Proc. 35th ACM STOC, 1–9, 2003.*

[FIS05] K. Friedl, G. Ivanyos, M. Santha, Efficient testing of groups, *Proc. 37th ACM STOC, 157–166, 2005.*

[I99] G. Ivanyos, Finding the radical of matrix algebras using Fitting decompositions, Journal of Pure and Applied Algebra 139, 159-182, 1999.

[I00] G. Ivanyos, Fast randomized algorithms for the structure of matrix algebras over finite fields, *Proc. 2000 ISSAC, 175–183.*

[I01] G. Ivanyos, Deciding finiteness for matrix semigroups over function fields over finite fields, *Israel Journal of Mathematics 124, 185–188, 2001.*

[I07] G. Ivanyos, Deciding universality of quantum gates, *Journal of Algebra 310, 49–56, 2007.*

[I07pre] G. Ivanyos, On solving random systems of linear disequations, *Submitted. Preprint: arXiv:0704.2988 [quant-ph], 2007.*

[IL00] G. Ivanyos, K. Lux, Treating the exceptional cases of the MeatAxe, *Experimental Mathematics 9, 373–381, 2000.*

Egyéb hivatkozások

[1] D. Bacon, A. Childs, and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. *Proc. 46th IEEE FOCS, 469–478, 2005.*

[2] J. J. Cannon, W. Bosma (Eds.) Handbook of Magma Functions, *Edition 2.13, 2006, (http://magma.maths.usyd.edu.au/magma).*

[3] A. M. Cohen, G. Ivanyos, D. B. Wales, Finding the radical of an algebra of linear transformations, *Journal of Pure and Applied Algebra 117–118, 177–193 1997.*

[4] H. Derksen, E. Jeandel, P. Koiran, Quantum automata and algebraic groups, *J. Symb. Comp. 39, 357–371, 2005.*

[5] L. E. Dickson, Algebras and Their Arithmetics, *The University of Chicago Press, Chicago, 1923.*

[6] M. Domokos, Relative invariants of 3×3 matrix triples, *Linear and Multilinear Algebra 47, 175–190, 2000.*

[7] W. M. Eberly, Computations for Algebras and Group Representations, *PhD. thesis, Dept. of Computer Science, University of Toronto, 1989.*

[8] W. M. Eberly, Decomposition of algebras over finite fields and number fields, *Computational Complexity 1, 179–206, 1991.*

[9] W. M. Eberly, M. W. Giesbrecht, Efficient decomposition of associative algebras over finite fields, *J. Symb. Comp. 37, 35–81, 2004.*

[10] J. Edmonds, System of distinct representatives and linear algebra, *Journal of Research of the National Bureau of Standards 718, 241–245, 1967.*

[11] R. P. Feynmann. Simulating physics with computers. *J. Theor. Physics 21, 467–488, 1982.*

[12] K. Friedl, L. Rónyai, Polynomial time solution of some problems in computational algebra, *Proc. 17th ACM STOC, 153–162, 1985.*

[13] The GAP Group, GAP – Groups, Algorithms, and Programming, *Version 4.4.9, 2006 (http://www.gap-system.org)*

[14] M. Gisbrecht, Y. Zhang, Factoring and decomposing ore polynomials over $F_q(t)$, *Proc. 2003 ISSAC, 127-134, 2003.*

[15] W. A. de Graaf, Using Cartan subalgebras to calculate nilradicals and Levi subalgebras of Lie algebras, *J. Pure and Applied Algebra 139, 25–39, 1999.*

[16] W. A. de Graaf, G. Ivanyos, Finding maximal tori and splitting elements in matrix algebras, *In: F. van Oysteayen, M. Saorin (eds), Interaction between Ring Theory and Representations of Algebras, Lecture Notes in Pure and Applied Mathematics 210, Marcel Dekker, 95–105, 2000.*

[17] W. A. de Graaf, G. Ivanyos, L. Rónyai, Computing Cartan subalgebras of Lie algebras, *Applicable Algebra in Engineering, Communication and Computing 7, 71–90, 1996.*

[18] L. Grover, A fast quatum mechanical algorithms for datebase search, *Proc. 28th ACM STOC, 212–219, 1996.*

[19] R. M. Guralnick, P. H. Tiep, Decompositions of small tensor powers and Larsen's conjecture, *Represent. Theory 9, 138–208, 2005.*

[20] C. Hollanti, J. Lahtonen, K. Ranto, R. Vehkalahti, On the densest MIMO lattices from cyclic division algebras, *Prepint arXiv:cs/0703052v1 [cs.IT], 2007.*

[21] D. F. Holt, S. Rees, Testing modules for irreducibility. *J. Austral. Math. Soc. Ser. A 57, 1–16, 1994.*

[22] G. Ivanyos, L. Rónyai, Finding maximal orders in semisimple algebras over $\mathbf{Q}$, *Computational Complexity 3, 245–261, 1993.*

[23] G. Ivanyos, L. Rónyai, Á. Szántó, Decomposition of algebras over $F_q(X_1, \ldots, X_m)$, *Applicable Algebra in Engineering, Communication and Computing 5, 71–90, 1994.*

[24] G. Ivanyos, L. Sanselme, M. Santha, An efficient quantum algorithm for the hidden subgroup problem in extraspecial groups, *Proc. STACS 2007, Springer LNCS Vol. 4393, 586–597, 2007.*

[25] G. Ivanyos, L. Sanselme, M. Santha, An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups *Preprint arXiv:0707.1260 [quant-ph], 2007.*

[26] A. Kitaev. Quantum measurements and the Abelian Stabilizer Problem. *Technical report arXiv:/quant-ph/9511026, 1995.*

[27] D. Lazard, Résolution des systèmes d'équations algébriques, *Theoret. Comput. Sci. 15, 77–110, 1981*

[28] L. Lovász, Singular spaces of matrices and their application in combinatorics, *Bulletin of the Brazilian Mathematical Society 20, 87–99, 1989.*

[29] M. Mosca, Quantum Computer Algorithms, *PhD Thesis, University of Oxford, 1999.*

[30] R. A. Parker, The computer calculation of modular characters (the Meat-Axe). *In: Computational Group Theory, Academic Press, 267–274, 1984.*

[31] L. Rónyai, Computing the structure of finite algebras, *J. Symbolic Computation 9, 355–373, 1990.*

[32] L. Rónyai, Algorithmic properties of maximal orders in simple algebras over **Q**, *Computational Complexity* 2, (1992a), 225–243.

[33] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. *Proc. 25th IEEE FOCS, 124–134, 1994.*

[34] P. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. on Computing 26, 1484–1509, 1997.*