# Rejtett részcsoportok és kvantum-számítógépek

Ivanyos Gábor
MTA SZTAKI

2007. április 30.

## 1. Bevezetés

R. P. Feynmann vetette fel először azt az ötletet, hogy a kvantum-jelenségeket esetleg hatékony számításra fel lehet használni [6]. A kvantum-számítógép modelljeinek kidolgozása és néhány a kvantum-géppel a klasszikusnál hatékonyabban megoldható – játékos jellegű – feladat felfedezése után Shor publikálta az első – mindjárt kettő – igazán életszagú alkalmazást [26, 27]: az egészek törzstényezős felbontását elvégző, valamint a diszkrét logaritmust kiszámoló polinomidejű kvantum-algoritmusát.

Mindazok a számítási feladatok, amelyekre a mai napig a klasszikusnál exponenciálisan gyorsabb kvantum-algoritmust találtak, többé-kevésbé (véleményem szerint inkább többé, mint kevésbé) közel állnak az úgynevezett rejtett részcsoport problémájához. Ezzel a feladattal közös keretbe foglalhatók a Shor által megoldott problémák és még több más érdekes feladat is. Az előadáson a véges csoportok rejtett részcsoportjait kereső kvantum-algoritmusokból szeretnék ízelítőt adni.

A bevezető hátralevő részében röviden ismertetek egy – a többi fontos modellel polinomiálisan ekvivalens – kvantum-gépmodellt, majd definiálom a rejtett részcsoport problémáját és vázolom a legnépszerűbb speciális eseteit. A második részben tárgyalom a kommutatív csoportok rejtett részcsoportjainak megtalálására szolgáló standard kvantum-algoritmust. Az előadás végén a nemkommutatív csoportokban történő általam legérdekesebbnek gondolt próbálkozásokról szeretnék beszámolni.

### 1.1. Kvantum bitek és kvantum-áramkörök

Itt röviden ismertetek egy kvantum-gépmodellt, amely a többi szokásos modellel polinomiálisan ekvivalens. Bővebb háttéranyag található például a [25], [19] vagy a [11] könyvekben. Magyar nyelvű bevezető anyagot Nagy Benedek jegyzetének [24] ötödik fejezetében találhat az Olvasó.

A kvantum-áramkörök alapelemei a kvantum bitek. Egy kvantum bit egy lehetséges állapota

$$a|0\rangle + b|1\rangle,$$

ahol $a$ és $b$ komplex számok, amelyekre $|a|^2 + |b|^2 = 1$. Egy kvantum bit tehát a kétdimenziós $B$ komplex euklideszi tér (avagy Hilbert-tér) egységvektora. A $B$ tér kitüntetett bázisának elemeit jelöli $|0\rangle$ illetve $|1\rangle$. Ha a fenti állapotú kvantum bitet megfigyeljük (megmérjük), akkor a 0 bitet kapjuk $|a|^2$ valószínűséggel és az 1 bitet kapjuk $|b|^2$ valószínűséggel.

Egy $n$ kvantum bitből álló együttes (rendszer) egy lehetséges állapota a $2^n$ dimenziós komplex euklideszi tér egységvektora. Ha a kitüntetett ortonormált bázis elemeit az $n$ hosszú $0-1$ sorozatokkal (bitsorozatokkal) indexeljük, akkor a rendszer állapota az $n$ hosszú bitsorozatok egy komplex együtthatós lineáris kombinációja (kvantumos szakzsargonban: szuperpozíciója), ahol az együtthatók abszolút értékének négyzetösszege 1. Ha egy állapotot megmérünk, eredményként egy konkrét bitsorozatot kapunk. Minden egyes bitsorozat valószínűsége a megfelelő együttható abszolút értékének a négyzete. Gyakran célszerű az $n$ bites állapotok terét a $B$ tér $\mathbb{C}$ feletti $n$-edik tenzorhatványakét szemlélni.

A kvantum-számítógép által végrehajtható műveletek unitér transzformációk. Az elemi lépéseket az úgynevezett kvantum-kapuk szolgáltatják. Egy $k$ bites kvantum-kapu a $2^k$ dimenziós komplex euklideszi tér egy unitér transzformációja. Az $n > k$ esetben egy $n$ kvantum bites rendszer bármely $k$ kvantum bitjére "bedrótozhatunk" egy $k$ kvantum bites $U$ kaput. A drótozásnak megfelelő művelet matematikai definíciója a következő: Kiválasztunk az $n$ kvantum bit közül $k$ bitet (a sorrend is számít!), a $2^n$ dimenziós teret felbontjuk a $k$ kvantum bitnek megfelelő $2^k$ dimenziós $W$ tér és a maradék kvantum bitekből megfelelő $2^{n-k}$ dimenziós $W'$ tér tenzorszorzatára. A bedrótozott kapu által végrehajtott művelet az $U_W \otimes I_{W'}$ tenzorszorzat lesz, ahol $I_{W'}$ a $W'$ téren az identitás, $U_W$ pedig az $U$ transzformáció a $W$ téren (abban az értelemben, hogy a $k$ kvantum bit sorrendi kiválasztása egyben azonosítja a $W$ teret $k$ kvantum bites állapotok terével.)

Egy $n$ kvantum bites kvantum-áramkör egy rögzített kapukészletből vett, a fent leírt módon bedrótozott kapuk sorozata. A lépésszám a sorozat hossza, a végrehajtott művelet pedig a fent részletezett transzformációk szorzata. Feltesszük, hogy a kapukészlet, amiből dolgozunk, az összes lehetséges 1 és 2 kvantum bites unitér transzformációból áll. Polinomiális lassulás erejéig ez a modell ekvivalens azzal, mintha az összes lehetséges legfeljebb $k$ kvantum bites kapukból építkeznénk valamely konstans $k$-ra.

Véges kapukészlettel is dolgozhatunk. Ha olyan véges 2 kvantum bites készletet veszünk, amely az $U_4$ unitér csoportnak (pontosabban, a $PU_4$ projektív változatnak) egy sűrű részcsoportját adják, minden $\epsilon > 0$-ra tetszőleges 4 dimenziós unitér transzformáció $\epsilon$ hibával megközelíthető $\log(1/\epsilon)$-ban polinomiális számú transzformáció szorzatával az adott készletből. Ezt felhasználva egy $\ell$ hosszú, a tág készletből vett kapukból épített áramkör 1 százalékos hibával megközelíthető $\ell$-ben polinom sok, a szűkebb készletből vett kapu felhasználásával. Ennek gyakorlati jelentősége az, hogy amennyiben az állapotokon a kvantum "program" lefuttatása után mérést végzünk, közel az "ideális" kapukészletéhez azonos eloszlást kapunk.

Egy kvantum programból a véletlent használó algoritmusokhoz hasonló jellegű eljárást nyerünk, ha egy konkrét "bemenő" bitsorozatra (pontosabban az

annak megfelelő báziselemre) futtatjuk le, majd az eredményre mérést alkalmazunk. A fent vázolt közelítés így gyakorlati értelmet nyer, hiszen két – operátor normában – közeli transzformáció utáni mérés megközelítőleg azonos eloszlást eredményez.

Egyes modellek megengednek a számolás közbeni mérési műveleteket is. Ezek a fent vázolt modellel szintén polinomiálisan ekvivalensek. Idő és hely hiányában ezek részletezésére nem térünk ki.

Noha kvantum-áramkörrel csak unitér – következésképpen invertálható – transzformációk hajthatók végre, a modell ténylegesen nem gyengébb a klasszikus Boole-áramkör modellnél. Valóban, a bitsorozatokon értelmezett $x \mapsto f(x)$ függvényt az $(x, y) \mapsto (x, f(x) \oplus y)$ leképezéssel helyettesíthetjük. (Itt $y$ az összes olyan hosszú bitsorozaton fut végig, ahány bitbe $f(x)$ belefér és $\oplus$ a bitenkénti kizáró vagy művelet.) Utóbbi művelet immár a megfelelő hosszú kétrészes bitsorozatok egy permutációja és így a kvantum-állapotok unitér transzformációjává terjed ki. A reverzibilis számításokra vonatkozó korai eredmények szerint minden Boole-áramkörrel hatékonyan kiszámítható $f$ függvényre az $(x, y) \mapsto (x, f(x) \oplus y)$ leképezés is hatékonyan számítható 3-bites úgynevezett Toffoli-kapuk segítségével.

A fentiek alapján, ha egy $f$ függvény polinom időben számolható klasszikus algoritmussal, akkor polinom hosszúságú kvantum-áramkörrel megvalósítható egy olyan transzformáció, amely tetszőleges

$$\sum_x a_x |x\rangle |0\rangle$$

alakú állapotból a

$$\sum_x a_x |x\rangle |f(x)\rangle$$

állapotot hozza létre. Szavakban: kvantum-géppel bármely klasszikusan hatékonyan számolható függvény szuperpozícióban is hatékonyan számolható. Ez a kvantum-géppel való hatékony számolások egyik legfontosabb – noha eléggé kézenfekvő – eszköze.

## 1.2. Rejtett részcsoportok

Legyen $G$ egy csoport és $f$ egy $G$-t az $\ell$ hosszú bitsorozatok $S$ halmazába képező függvény valamely $\ell$ pozitív egész számra. Azt mondjuk, hogy az $f$ függvény a $H \leq G$ részcsoportot *rejti*, ha $f(x) = f(y)$ akkor és csak akkor teljesül, ha $x$ és $y$ a $H$ részcsoportnak ugyanazon baloldali mellékosztályába esik. Más szavakkal az $f$ függvény konstans értéket vesz fel a $H$ részcsoport baloldali mellékosztályain, de a különböző mellékosztályokon felvett értékek különbözők.

A kapcsolódó számítási problémában, a rejtett részcsoport problémájában feltesszük még, hogy $x$ bement esetén az $f(x)$ függvényérték hatékony algoritmussal kiszámíthatók, vagy – egy transzparansebb megfogalmazásban – egy orákulum azonnal megadja $f(x)$-et. (Kvantum-számítógépes esetben az orákulumról azt feltételezzük, hogy olyan unitér transzformáció, amely a $|x\rangle|0\rangle$ állapotot a $|x\rangle|f(x)\rangle$ állapotba viszi. Itt a kiinduló állapot második részében a

$|0\rangle$ alatt egy $\ell$ hosszú csupa nullából álló bitsorozatot értünk.) A feladat az $f$ függvény által rejtett $H$ részcsoport kiszámítása. Lássunk részcsoportot rejtő függvényre három fontos példát.

**Csoportelem rendje és egészek faktorizációja.** Legyen $A$ egy véges csoport és $a$ egy elem az $A$ csoportból. Tegyük fel, hogy az $A$ csoport elemei $\ell$ hosszú bitsorozatokkal vannak kódolva. Így $A$ azonosítható az $S$ halmaz egy részhalmazával. Legyen $G$ az egész számok $\mathbb{Z}$ csoportja és $f : G \to S$ az $f(z) = a^z$ képlettel megadható függvény. Ekkor $f$ az $m\mathbb{Z}$ részcsoportot rejti, ahol $m$ az $a$ eleme rendje. Ebben a példában tehát a rejtett részcsoport meghatározása egyenértékű az $a$ elem rendjének kiszámításával. Megjegyezzük, hogy ha $a$ és $a^{-1}$ is adott, akkor az $a^z$ hatvány az iterált négyzetre emelés módszerével (más néven gyors hatványozással) $O(\log |z|)$ darab $A$-beli szorzás segítségével számolható.

Alkalmazásként tekintsük azt az esetet, amikor $n$ egy páratlan egész szám és $A$ a modulo $n$ vett redukált maradékosztályok multiplikatív csoportja. Ebben a csoportban a rend számítása egy olyan eszköz, amelynek segítségével a következő hatékony véletlent használó algoritmus adható az $n$ szám egy valódi osztójának megadására. Feltesszük, hogy $n$ nem egyetlen prímszám hatványa. (Egyszerű próbálkozással tudunk valódi osztót találni olyan számhoz, amely egy másik pozitív egész szám valahanyadik hatványa.) Választunk egy véletlen 1 és $n-1$ közé eső $a$ egész számot, és kiszámoljuk a villámgyors euklideszi algoritmussal $a$ és $n$ legnagyobb közös osztóját. Ha ez a közös osztó nem 1, nyertünk egy valódi osztót. Megmutatjuk, hogy a fennmaradó eseteknek legalább a felében szintén tudunk gyorsan valódi osztót találni. Jelöljük egy $n$-hez relatív prím $a$ szám modulo $n$ vett multiplikatív rendjét $o(a)$-val. Az $n$-re vonatkozó feltevésből könnyen adódik, hogy egy véletlenül választott $n$-hez relatív prím $a$ számra legalább $1/2$ valószínűséggel $o(a)$ páros és $a^{o(a)/2}$ maradéka modulo $n$ nem $-1$. Ezért a $b = a^{o(a)/2}$ modulo $n$ vett maradékosztály (gyors hatványozással történő) kiszámítása után azt kapjuk, hogy a $b^2$ szám $n$-nel osztva 1 maradékot ad, ugyanakkor $b$ maradéka modulo $n$ se nem 1 se nem $-1$. Másképpen fogalmazva, az $n$ szám osztója a $b^2 - 1 = (b+1)(b-1)$ szorzatnak, de nem osztója egyik tényezőnek sem. Így $n$-nek egy valódi osztóját nyerjük, ha az euklideszi algoritmussal kiszámítjuk mondjuk $b-1$ és $n$ legnagyobb közös osztóját.

**Diszkrét logaritmus.** Legyen most $a$ és $b$ az $A$ kommutatív csoport két eleme. Tegyük fel, hogy $b$ az $a$ elemnek valamilyen $a^t$ hatványával egyezik meg. A feladat, hogy keressünk egy ilyen $t$ számot. Világos, hogy $t$ modulo az $a$ elem $o(a)$ rendje egyértelműen meghatározott. Az egyszerűség kedvéért feltesszük, hogy ismerjük az $o(a)$ és az $o(b)$ számokat. (Például kiszámítottuk a fenti rendszámoló algoritmussal.) Világos, hogy $o(b)$ az $o(a)$ számnak egy osztója. Legyen $G$ a $\mathbb{Z}_{o(a)} \times \mathbb{Z}_{o(b)}$ direkt szorzat és $f$ az a függvény, amelyre $f(x,y) = a^x \cdot b^{-y}$. Ahogy előbb, itt is feltesszük, hogy $A$ elemei $\ell$ hosszú bitsorozatokkal vannak ábrázolva. Az $f(x,y)$ értéket itt is a gyors hatványozás segítségével számolhatjuk. Könnyen látható, hogy az $f$ függvény a $(tu, u)$ párokból álló részcsoportot rejti,

ahol $u$ a modulo $o(a)$ vett maradékokon fut végig és a második koordinátában szereplő $u$-t modulo $o(b)$ kell érteni.

**Gráfok automorfizmusai és az izomorfizmus-probléma.** Legyen $\Gamma$ egy (irányítatlan, egyszerű) gráf $n$ csúccsal és $G$ az $S_n$ szimmetrikus csoport. Egy $\pi \in G$ permutációra legyen $\Gamma^\pi$ az a gráf, amelynek egy $\{a, b\}$ csúcspár akkor és csak akkor éle, ha $\{\pi(a), \pi(b)\}$ éle az eredeti $\Gamma$ gráfnak. Ekkor az $f(\pi) = \Gamma^\pi$ függvény által rejtett részcsoport a $\Gamma$ gráf automorfizmuscsoportja. Tehát ebben az esetben a rejtett részcsoport meghatározása nem más, mint a gráf automorfizmuscsoportjának kiszámítása.

Gráfok izomorfiája az autmorfizmuscsoport-probléma megoldásával a következő kézenfekvő módszerrel dönthető el. Legyen $\Gamma_1$ és $\Gamma_2$ két gráf. Az egyszerűség kedvéért feltesszük, hogy mindkét gráf összefüggő. Ha nem ugyanakkora az automorfizmuscsoportjuk, akkor nyilván nem izomorfak. Ha ugyanakkora, akkor tekintsük a két gráf diszjunkt egyesítését. Ha a két gráf nem izomorf, akkor az egyesített gráf automorfizmuscsoportja a komponensek automorfizmuscsoprtjainak direkt szorzata. Ha viszont a két gráf izomorf, akkor ez a direkt szorzat az egyesítés automorfozmuscsoprtjában egy 2 indexű részcsoport.

Az első két főleg kriptográfiai alkalmazásaik miatt fontos példára Shor javasolt polinomidejű kvantum-algoritmust [26, 27], jelentős lökést adva a kvantum-számítógépek építésére törekvő próbálkozásoknak. A következő fejezetben bemutatjuk, hogyan lehet véges kommutatív csoportok rejtett részcsoportjait polinom időben megtalálni kvantum-számítógéppel. A módszer alapvetően Shor algoritmusának egy kézenfekvő általánosítása. A harmadik példára – gráfok izomorfizmusának problémájára – azonban jelenleg nem ismert a legjobb klasszikus módszereket megverő kvantum-algoritmus. Ugyanakkor ez a példa a nemkommutatív rejtett részcsoport problémakörében folyó vizsgálatok legfontosabb motiváló tényezője.

## 2. Kommutatív csoportok rejtett részcsoportjai

Ebben a fejezetben vázoljuk azt a kvantum-algoritmust, amellyel kommutatív csoportok rejtett részcsoportjait lehet megtalálni. A módszert hasonló általánosságban először Kitaev írta le [18]. Az alapvető eszköz az úgynevezett kvantum Fourier-transzformáció, amely lényegében a széles körűen alkalmazott klasszikus diszkrét Fourier-transzformáció kvantum-számítógépes megfelelője.

Véges csoportokkal kapcsolatos kvantum-algoritmusok többségénél kulcsfontosságú műveleti terep a csoportalgebra, mégpedig úgy szemlélve, hogy a csoportalgebra elemei a csoportelemek szuperpozíciói. Tehát a kitüntetett ortonormált bázist a csoportelemekből alkotják. [1]

[1] Noha a csoportalgebra általában nem 2-hatvány dimenziós, tehát nem felel meg teljesen pontosan a bevezetőben tárgyalt térnek, de $G$ elemeinek bitsorozatokkal történő kódolása segítségével beágyazható ilyen térbe.

Legyen $G$ egy véges kommutatív csoport és jelölje $\widehat{G}$ a $G$ csoport lineáris karaktereinek csoportját. A $G$ csoport Fourier-transzformációja az a leképezés, amelynél a $g \in G$ báziselem (avagy a kvantum-számítások körében népszerű jelölésrendszerben a $|g\rangle$ állapot) képe a

$$\frac{1}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \chi(g)|\chi\rangle$$

állapot. Ez utóbbi a $\widehat{G}$ karaktercsoport algebrájának eleme. Szokás rögzíteni $G$ egy bázisának segítségével $G$ és $\widehat{G}$ között egy megfeleltetést (dualitást) és így a Fourier-transzformációt a csoportalgebra önmagára történő unitér leképezésének tekinteni.

A Fourier-transzformáció $\log |G|$-ben polinomiális lépésszámú kvantum-algoritmussal tetszőleges pontossággal megközelíthető. Az implementációról itt annyit jegyeznénk meg, hogy mivel direkt szorzat Fourier-transzformációja a komponensek Fourier-transzformációinak a tenzorszorzata, így az igazi faladat ciklikus csoportok Fourier transzformációjának megvalósítása. Ez 2-hatvány rendű csoportokra a klasszikus gyors Fourier transzformációhoz hasonló trükkel megy, az általános esetben a közelítés 2-hatványrendű Fourier transzformációk segítségével történik.

A rejtett részcsoportot megtaláló kvantum-algoritmus a következő. Kiindulunk az

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|0\rangle$$

állapotból, ahol a második részben $|0\rangle$ valójában egy $\ell$ hosszú csupa nullából álló bitsorozat. Erre az állapotra alkalmazva az orákulumot az

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle|f(g)\rangle$$

állapotot kapjuk. Legyen $g_1, \ldots, g_{|G:H|}$ egy $H$ rejtett részcsoport mellékosztályai szerinti reprezentánsrendszer. Átcsoportosítjuk a fenti összeget a második részben szereplő érték szerint:

$$\frac{1}{\sqrt{|G|}} \sum_{i=1}^{|G:H|} \sum_{h \in H} |g_i h\rangle|f(g_i)\rangle.$$

Ha alkalmazzuk a $G$ csoport Fourier transzformációját, az

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \sum_{i=1}^{|G:H|} \sum_{h \in H} \chi(g_i h)|\chi\rangle|f(g_i)\rangle$$

állapotot kapjuk. Ebben az összegben rögzített $i$-re és $\chi$-re a $|\chi\rangle|f(g_i\rangle$ báziselem együtthatója

$$\frac{\chi(g_i)}{|G|} \sum_{h \in H} \chi(h).$$

Itt használtuk azt is, hogy $\chi(g_i h) = \chi(g_i)\chi(h)$. A $H$ részcsoport karaktareire vonatkozó ortogonalitási relációkat alkalmazva azt kapjuk, hogy ez az együtthatók

$$\begin{array}{ll} 0 & \text{ha } \chi_{|H} \neq 1_H \text{ és} \\ \frac{\chi(g_i)}{|G:H|}, & \text{ha } \chi_{|H} = 1_H. \end{array}$$

Mármost, ha mérést alkalmazunk, 0 lesz a valószínűsége, hogy a $\chi$ karaktert találjuk az első részben minden olyan $\chi$ karakterre, amelyre $\chi_{|H} \neq 1_H$ és egyaránt $\frac{1}{|G:H|}$ az olyan karakterekre, amelyekre $\chi_{|H} \neq 1_H$. Az eljárást $N = O(\log |G|)$-szer ismételve nagy valószínűséggel olyan $\chi_1, \ldots, \chi_N$ karaktereket kapunk, amelyek a $H^\perp = \{\chi \in \widehat{G} | \chi_{|H} = 1_H\}$ csoport egy generátorrendszerét alkotják. Ha tényleg ez következik be, akkor a $H$ részcsoport a $G$ csoport $H$ azon elemeiből áll, amelyekre $\chi_1(h) = 1, \ldots, \chi_N(h) = 1$. Ezek a feltételek lényegében egy lineáris egyenletrendszerrel egyenértékűek a $G$ csoportban. Az egyenletrendszer klasszikus determinisztikus polinomidejű algoritmussal megoldható.

# 3. Nemkommutatív próbálkozások

Ebben a részben röviden áttekintjük a nemkommutatív csoportok rejtett részcsoportjainak megkeresésére irányuló legígéretesebb módszereket, kitérve néhány, a módszerek korlátaira vonatkozó eredményre is.

## 3.1. A standard Fourier-módszer

Kézenfekvőnek tűnik a kommutatív csoportoknál bevált módszert alkalmazni a nemkommutatív esetben is. Akárcsak a kommutatív esetben, az első menetben itt is a rejtő függvényt kiszámoló orákulomut alkalmazzuk a csoportelemek szuperpozíciójára. A következő lépésben a Fourier-transzformációnak a lentebb részletezendő nemkommutatív általánosítását alkalmazzuk, majd az eredményt megfigyeljük. Ezt a módszert standard Fourier-módszernek vagy röviden standard módszernek hívják hívják.

Egy véges nemkommutatív $G$ csoport Fourier-transzformációja az az unitér leképezés, amelynél a $g$ csoportelem képe

$$\sum_{\rho \in \widehat{G}} \sum_{i,j=1}^{d_\rho} \frac{\sqrt{d_\rho}}{\sqrt{|G|}} \sum_{i,j=1}^{d_\rho} \rho(g)_{ij} |\rho, i, j\rangle,$$

ahol $\widehat{G}$ a $G$ csoport komplex irreducibilis mátrixreprezentációnak egy unitér reprezentánsrendszere és adott $\rho$ reprezentációra $d_\rho$ a dimenziót, $\rho(g)_{ij}$ pedig a $g$ elem az képének $i$-edik sor és $j$-edik oszlop kereszteződésében álló eleme. A képtér kitüntetett ortonormált báziselemeinek jelölésére szolgálnak a $|\rho, i, j\rangle$ szimbólumok (úgynevezett "mátrixelemek")). Elég sok nemkommutatív csoportra ismert hatékony kvantum Fourier-transzformáció [21], köztük a szimmetrikus csoportra is [2].

Sajnos a transzformáció függ attól, hogy az ekvivalencia-osztályokból milyen mátrixreprezentációt választunk (azaz a megfelelő modulusban milyen bázist választunk). A gyenge standard Fourier-módszer csak a $\rho$ reprezentációnevet figyeli meg (tehát az $i, j$ indexeket ignorálja), vagyis itt nem jelenik meg a fenti esetlegesség. Annak a valószínűsége, hogy éppen a $\rho$ reprezentációt mérjük az eljárás során

$$\frac{d_\rho}{|G|} \sum_{h \in H} \chi_\rho(h).$$

Ha a $H$ részcsoport normálosztó, akkor ez a valószínűség 0 minden olyan $\rho$-ra, amelynek $H$ nincs a magjában. A $H$-t magjukban tartalmazó reprezentációk valószínűsége "eléggé egyenletes" ahhoz, hogy $H$-t nagy valószínűséggel meg lehessen határozni az eljárás viszonylag kis számú ismétlése után [9, 8]. Kicsit általánosabban: a gyenge Fourier-módszerrel egy rejtett részcsoport úgynevezett normális magját (a benne levő legnagyobb normálosztót) polinom időben meg lehet találni [8] – feltéve, hogy a csoport kvantum Fourier-transzformációját hatékonyan el tudjuk végezni. Ez utóbbi feltételt nagy Lie típusú egyszerű csoportokat kompozíciófaktorként nem tartalmazó csoportokban meg lehet kerülni [12] Babai László és R. Beals egy csoportok struktúrájának kiszámítására kidolgozott algoritmusának [3] trükkösen alkalmazott kvantumos implementációjával.

A standard Fourier-módszer erős változatában az eredményesség függ az irreducibilis modulusok bázisának megválasztásától. Meglehetősen nehéz feladatnak tűnik a legjobb bázis megválasztása: megmutatható [8], hogy ha a csoport "eléggé" nemkommutatív és a rejtett részcsoport "eléggé" kicsi, akkor véletlen bázis választása esetén nem igazán nyerünk többletinformációt a gyenge változathoz képest. Sőt, a merev gráfok izomorfizmusának problémájához kapcsolódó rejtett részcsoportprobléma hatékony megoldására az erős standard Fourier-módszer semmilyen bázissal sem használható [23].

Egy kicsit részletesebben térünk ki egy, a gyenge standard módszer korlátaira vonatkozó eredményre. Az eredményhez vezető munka szép példája a mély csoportelméleti eszközök alkalmazásának. Kempe és Shalev 2004-ben a szimmetrikus csoportok azon részcsoportjait próbálta meghatározni, amelyeket a gyenge standard módszerrel rejtett részcsoportként a triviális részcsoporttól hatékonyan meg lehet különböztetni [17]. (Általában a $H_1$ és $H_2$ részcsoport polinom idejű megkülönböztetése alatt itt olyan $\log |G|$-ben polinom idejű kvantumalgoritmust értünk, amely minden olyan $f$ függvényre, amely vagy a $H_1$ vagy a $H_2$ részcsoportot rejti, nagy valószínűséggel helyesen dönt.) Nevezzük ebben a dolgozatban a triviálistól ilyen értelemben hatékonyan megkülönböztethető csoportokat röviden megkülönböztethetőnek.

Kempe és Shalev azt sejtették, hogy éppen azok a permutációcsoportok a megkülönböztethetők, amelyek tartalmaznak olyan nem identikus permutációt, amely csak konstans sok elemet mozgat. Mivel összesen is csak polinom sok ilyen permutáció van, az ezeken történő kimerítő kereséssel a részcsoport klasszikus módszerrel is megkülönböztethető a triviálistól. Érdemes megjegyezni, hogy egy $H$ permutációcsoportban az $1 \neq h \in H$ permutáció által mozgatott elemek számának minimuma $H$ minimális fokszámaként ismert és jelentős szerepet játszik

a permutációcsoportok vizsgálatában ősidőktől fogva [14, 15].

A sejtést Kempe és Shalev 2004-ben fontos speciális esetekre, nevezetesen kisméretű, illetve primitív permutációcsoportra igazolta. A primitív esetben a bizonyítás a véges egyszerű csoportok osztályozására támaszkodó eredményeket használ. A megkülönböztethető primitív permutációcsoportok kizárólag az $A_n$ alternáló és az $S_n$ szimmetrikus csoport. Később Pyber László csatlakozásával sikerült a sejtést – ugyancsak az osztályozáson múló mély eredményeket felhasználva – teljes mértékben igazolniuk [16].

Az alábbi vázlatos gondolatmenet érzékelteti az összefüggést a megkülönböztethetetlenség és a minimális fokszám között. Ha egy tetszőleges $G$ csoport $H$ részcsoportja megkülönböztethető, akkor a gyenge standard Fourier-módszert alkalmazva a $H$-t illetve a triviális részcsoportot rejtő függvényre a karaktereken kapott eloszlások $L_1$-távolsága csak polinomiálisan lehet kicsi. Ez a távolság

$$D_H = \sum_{\rho \in \widehat{G}} \frac{d_\rho}{|G|} | \sum_{1 \neq h \in H} \chi_\rho(h). |$$

A következő – elemi úton bizonyítható – becsléssel meg lehet szabadulni a karakterektől:

$$D_h \leq \sum_{1 \neq h \in H} \frac{1}{\sqrt{|h^G|}},$$

ahol $h^G$ a $h$ elem $G$-beli konjugáltjainak a halmazát jelöli. Esetünkben, ahol $G = S_n$, egy permutáció konjugáltjainak a száma elég jól becsülhető a mozgatott elemek számának segítségével: egy $k$ elemet mozgató permutáció konjugáltjainak a száma legalább $k!/(2^{\frac{k}{2}}(k/2)!)$.

A standard Fourier módszer erős változatával hatékonyan meg lehet találni az $AGL_1(p)$ affin csoport bizonyos elég nagy rejtett részcsoportjait [22]. Úgy tűnik azonban, hogy sokkal többet nem lehet ezzel a módszerrel elérni: bebizonyították [23], hogy önmagában alkalmatlan gráfok izomorfiájának hatékony eldöntésére.

## 3.2. További hatékony rejtett részcsoport algoritmusok

A rejtett részcsoport probléma úgynevezett lekérdezési bonyolultsága polinomiális, elegendő az orákulumot $\log(G)$-ben polinom sok szuperpozícióra meghívni. A kapott állapotokból az orákulumot tovább már nem használó, de exponenciális idejű kvantum-algoritmussal megtalálható a rejtett részcsoport [5]. Ez az eredmény azt mutatja, hogy nincs könnyű dolga annak, aki a probléma nehézségét szeretné igazolni.

Ugyanakkor az összes olyan $G$ csoport, amelyben jelenlegi ismereteink szerint minden rejtett részcsoport $\log|G|$-ben polinomidejű kvantum-algoritmussal hatékonyan megtalálható "majdnem" kommutatív. A dolgozatot néhány fontosabb ilyen speciális eset tárgyalásával zárjuk.

A $D_n$ diéder csoport igen közel áll a ciklikushoz. Egy, a $D_n$-ben rejtett 2 rendű részcsoportokat hatékonyan (azaz $\log n$-ben polinom időben) megtaláló

módszer fontos rekurziós eszköz lenne a feloldatható csoportok rejtett részcsoportproblémájának megtámadásához. Sajnos a legjobb $D_n$-re ismert módszer [20] időigénye $2^{O(\sqrt{\log n})}$. Megjegyezzük, hogy ez a módszer tekinthető az első igazán tudatos úgynevezett többregiszteres technikának. Az ilyen algoritmusok sok részből álló összefonódott (entangled) állapotokkal dolgoznak, szemben a standard Fourier-módszerrel, amely egy nagyobb lépése egyrészes állapotra alkalmaz megfelelő unitér transzformáció után mérést, és ilyen lépéseket ismétel. Megmutatták, hogy a rejtett részcsoportot hatékonyan meghatározó esetleges általános algoritmus csakis sokregiszteres lehet [10]. Igaz ez a gráfok izomorfiájánál releváns speciális esetben is.

Érdekességként megjegyezzük, hogy $D_n$ diéder csoportra van egy olyan egyregiszteres technika [4], amelynek kvantum része polinomidejű és utána egy exponenciális idejű klasszikus módszerrel lehet e rejtett részcsoportot megtalálni. A $\mathbb{Z}_p^n \rtimes \mathbb{Z}_2$ csoport esetére, ahol $p$ egy prímszám viszont sikerült olyan egyregiszteres módszert találni, amely $n$-ben polinom, $p$-ben pedig exponenciális időben működik [7]. Ennek az algoritmusnak egy változatát ráadásul indukciós lépésként lehet használni feloldható csoportokban. Az eredmény egy polinom idejű – végső soron sokregiszteres – módszer olyan konstans feloldható hosszúságú $G$ csoportokra, ahol $G'$ konstans exponensű. Viszonylag kevés kivétellel az összes csoport, amelyben tetszőleges rejtett részcsoport a jelenleg ismert módszerekkel polinomidőben megtalálható, lényegében ilyen tulajdonságú.

Az egyik legszebb friss többregiszteres módszer $p^3$ rendű – a fenti osztályba nem tartozó – nemkommutatív csoportokban oldja meg a rejtett részcsoport problémáját polinomidőben [1]. Az algoritmus egy, a szakirodalomból ismert közel optimális mérés meghatározásán és hatékony implementációján alapul. Az eredményt – gyökeresen különböző módszerrel – a közelmúltban sikerült kiterjeszteni extraspeciálias csoportokra [13]. Az eljárás alapötlete az, hogy adott reprezentációkat automorfizmusokkal kombinálva a tenzorszorzatukat alkalmasan be lehet "hangolni". Úgy tűnik, a módszer kiterjeszthető tetszőleges 2 osztályú nilpotens csoportra.

# Hivatkozások


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

[2] R. Beals. Quantum computation of Fourier transforms over symmetric groups. In *Proc. 29th ACM STOC*, pages 48–53, 1997.

[3] R. Beals and L. Babai. Las Vegas algorithms for matrix groups. In *Proc. 34th IEEE FOCS*, pages 427–436, 1993.

[4] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. *Adv. in Appl. Math.*, 25(3), pages 239–251, 2000.

[5] M. Ettinger, P. Hoyer, and E. Knill. The quantum query complexity of the hidden subgroup problem is polynomial, *Inform. Proc, Letters*, 91(1), pages 43–48. 2004.

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

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

[8] M. Grigni, L. Schulman, M. Vazirani, and U. Vazirani. Quantum mechanical algorithms for the nonabelian Hidden Subgroup Problem. In *Proc. 33rd ACM STOC*, pages 68–74, 2001.

[9] S. Hallgren, A. Russell, and A. Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proc. 32nd ACM STOC*, pages 627–635, 2000.

[10] S. Hallgren, C. Moore, M. Rötteler, A. Russel, and P. Sen. Limitations of quantum coset states for graph isomorphism. In *Proc. 38th ACM STOC,* pages 604–617, 2006.

[11] M. Hirvensalo. *Quantum Computing*. Springer, 2001.

[12] G. Ivanyos, F. Magniez, and M. Santha. Efficient quantum algorithms for some instances of the non-Abelian hidden subgroup problem. *Int. J. of Foundations of Computer Science* 14(5), pages 723–739, 2003.

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

[14] C. Jordan. Sur la limite de transitivité des groupes non alternés. *Bull. Soc. Math. France,* 1, pages 40–71, 1873.

[15] C. Jordan. Sur la limite de degré des groupes primitifs qui conitennent une substitition donnée. *J. Reine Angew. Math.,* 79, pages 248–285. 1875.

[16] J. Kempe, L. Pyber, and A. Shalev. Permutation groups, minimal degrees and quantum computing. *Preprint quant-ph/0607204,* 2006.

[17] J. Kempe and A. Shalev. The hidden subgroup problem and permutation group theory. In *Proc. 16th ACM-SIAM SODA*, pages 1118–1125, 2005.

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

[19] A. Kitaev, A. Shen, and M. Vyalyi. Classical and quantum computation. In *Graduate Studies in Mathematics*, volume 47. American Mathematical Society, 2002.

[20] G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comp.* 35(1), pages 170–188,2005

[21] C. Moore, D. Rockmore, and A. Russell. Generic quantum Fourier transforms. In *Proc. 15th ACM-SIAM SODA*, pages 778–787, 2004.

[22] C. Moore, D. Rockmore, A. Russell, and L. Schulman. The power of basis selection in Fourier sampling: hidden subgroup problems in affine groups. In *Proc. 15th ACM-SIAM SODA*, pages 1113–1122, 2004.

[23] C. Moore, A. Russell, and L. Schulman. The Symmetric Group Defies Strong Fourier Sampling. In *Proc. 46th IEEE FOCS,* pages 479–490, 2005.

[24] B. Nagy. *Új elvű számítógépek.* Egytetemi jegyzet. Mobidiák, Debrecen 2005.

[25] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

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

[27] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26(5), pages 1484–1509, 1997.