

Diósi Lajos

Bevezetés a kvantuminformáció-elméletbe

– az elméleti fizika oldaláról

Diósi Lajos

Bevezetés a kvantum-
információ-elméletbe
– az elméleti fizika oldaláról



A könyv a Magyar Tudományos Akadémia támogatásával készült.



© Diósi Lajos, Typotex, Budapest, 2017
Engedély nélkül semmilyen formában nem másolható!

ISBN 978 963 279 978 0

Témakör: *fizika*

Kedves Olvasó!
Köszönjük, hogy kínálatunkból választott olvasnivalót!
Újabb kiadványainkról és akcióinkról a www.typotex.hu
és a [facebook.com/typotexkiado](https://www.facebook.com/typotexkiado) oldalakon értesülhet.

Kiadja a Typotex Elektronikus Kiadó Kft.
Felelős vezető: Votisky Zsuzsa
Főszerkesztő: Horváth Balázs
Műszaki szerkesztő: Erő Zsuzsa
A borítót készítette: Szalay Éva
Készült a Kódex Könyvgyártó Kft. nyomdájában
Felelős vezető: Marosi Attila

Előszó

A kvantuminformáció gyorsan fejlődő kutatási terület. Új intézetek, laboratóriumok keletkeztek világszerte egyedi kvantumrendszerek vizsgálatára, vezérlésére, mely különleges és komplex matematikai, fizikai és technikai feladat. A kvantumtechnológiák ígért előnye is felvillanyozta a területet, melyet nemrég még marginálisnak tartottak. Korábban számos alapvető kvantumtulajdonság csak egyedi rendszerek statisztikus sokaságán lett bizonyítva, egyedi rendszeren sohasem. A kvantum-szuperpozíció redukciója, bomlása vagy felélédeése anélkül szerepelt tankönyveinkben egyedi rendszereken illusztrálva, hogy egyedi rendszeren valaha is kísérletileg tanúsítva lett volna. Mára azonban a fiatal generáció ezeket a kvantumelméleti és kísérleti alapokat az anyatejjel szívhatja magába.

2001-től fogva tavaszi szemesztereken adtam elő választható tárgyként végzős és végzett fizikusoknak az Eötvös Loránd Tudományegyetemen. A tizenkét előadás nem fedhette le a kvantuminformáció minden standard fejezetét. Vezérelveim az elméleti fizikuséi voltak, és a meggyőződés a fizika egységében. Tisztes egyensúlyt értem el a kvantuminformációs törzsanyag és azt az elméleti fizika épületéhez kötő fejezetek között. A szöveg nem kíván speciális matematikai ismereteket, csupán a komplex vektorterek és a valószínűség-számítás elméleti alapjait. Tökéletes olvasóm lesz, aki előzőleg kvantumelméleti alaptanulmányokat folytatott. Akik készek sokszorosan több időt fordítani kvantuminformációs tudásszerzésre, azoknak kimerítő monográfiák állnak rendelkezésükre – jobbára angolul.

A Springernél két angol nyelvű kiadást (2007, 2011) megélt, másodsorra kissé bővített, de még mindig vékony kötet két célt is megvalósít a mostani magyar kiadással. Közvetlenebbül éri el a magyar nyelvű fizikus és matematikus közösséget, egyetemi hallgatóságot a kvantuminformatica modern tudománya. Támogatja, csiszolja a magyar szaknyelvet, hisz a kvantuminformatica számtalan új – mára meggyökeresedett – angol szakkifejezést, szaknyelvi fordulatot teremtett, ezek magyar megfelelői tankönyvben honosíthatók meg legkönnyebben.

Javaslom a vékony könyvet fizikusoknak, matematikusoknak és mindenkinek, aki az elméleti fizika integráló megközelítésében érdekelt. Persze nem lenne fölösleges egy második vékony könyv: „Bevezető a kvantuminformáció-elméletbe – a kísérleti fizika oldaláról” ...

Budapest, 2017. szeptember

Diósi Lajos

Tartalomjegyzék

1. Bevezetés	1
2. A klasszikus fizika alapjai	5
2.1. Állapottér, mozgásegyenlet	5
2.2. Művelet, keverés, szelekció	6
2.3. A nemszelektív műveletek linearitása	7
2.4. Mérések	8
2.4.1. Projektív mérés	8
2.4.2. Nemprojektív mérés	9
2.4.3. Gyenge mérés, időben folytonos mérés	10
2.5. Összetett rendszerek	11
2.6. Kollektív rendszer	13
2.7. Kétállapotú rendszer (bit)	13
Problémák, gyakorlatok	14
3. Féligklasszikus – féligkvantum fizika	15
Problémák, gyakorlatok	16
4. A kvantumfizika alapjai	19
4.1. Állapottér, szuperpozíció, mozgásegyenlet	19
4.2. Művelet, keverés, szelekció	20
4.3. Nemszelektív műveletek linearitása	21
4.4. Mérések	22
4.4.1. Projektív mérés	23
4.4.2. Nemprojektív mérés	24
4.4.3. Gyenge mérés, időben folytonos mérés	25
4.4.4. Kompatibilis fizikai mennyiségek	27
4.4.5. Mérés tiszta állapotban	27
4.5. Összetett rendszerek	28
4.6. Kollektív rendszer	30
Problémák, gyakorlatok	30

5. Kétállapotú kvantumrendszer: qubit reprezentációk	33
5.1. Számítási reprezentáció	33
5.2. Pauli-reprezentáció	34
5.2.1. Állapottér	34
5.2.2. Forgatási invariancia	35
5.2.3. Sűrűségmátrix	36
5.2.4. Mozgásegyenlet	36
5.2.5. Fizikai mennyiségek, mérés	37
5.3. Ismeretlen qubit, Alice és Bob	38
5.4. Számítási és Pauli-reprezentáció kapcsolata	38
5.5. Fock-reprezentáció	39
Problémák, gyakorlatok	40
6. Egy-qubit eljárások	41
6.1. Egy-qubit műveletek	41
6.1.1. Logikai műveletek	41
6.1.2. Depolarizáció, repolarizáció, tükrözés	42
6.2. Állapotpreparáció, állapotmeghatározás	43
6.2.1. Ismert állapot preparációja, keverés	44
6.2.2. Ismeretlen állapot meghatározása sokaságon	45
6.2.3. Egyetlen állapot meghatározása: klónozhatatlanság	46
6.2.4. Két állapot hűsége	46
6.2.5. Közelítő állapotmeghatározás és klónozás	47
6.3. Két nemortogonális állapot megkülönböztethetlensége	47
6.3.1. Megkülönböztetés projektív méréssel	48
6.3.2. Megkülönböztetés nemprojektív méréssel	48
6.4. A klónozhatatlanság és megkülönböztethetlenség alkalmazásai	49
6.4.1. Kvantumbankjegy	49
6.4.2. Titkos kvantumkulcs, kvantumkriptográfia	50
Problémák, gyakorlatok	52
7. Összetett kvantumrendszer, tiszta állapot	55
7.1. Kétrésű összetett rendszerek	55
7.1.1. Schmidt-felbontás	55
7.1.2. Állapottisztítás	56
7.1.3. Összefonódásmérték	57
7.1.4. Összefonódás és lokális műveletek	58
7.1.5. Két-qubit tiszta állapot összefonódása	59
7.1.6. Maximális összefonódások átválthatósága	60
7.2. Kvantumkorrelációk története	61
7.2.1. EPR, Einstein-nemlokalitás 1935	61
7.2.2. Egy nemlétező lineáris művelet 1955	62
7.2.3. Bell-nemlokalitás 1964	64
7.3. Kvantumkorrelációk alkalmazása	66
7.3.1. Szupersűrű kódolás	66
7.3.2. Teleportáció	67
Problémák, gyakorlatok	68

8. Általános kvantumműveletek	71
8.1. Teljesen pozitív leképezések	71
8.2. Redukált dinamikák	72
8.3. Közvetett mérés	73
8.4. Nemprojektív mérés közvetett mérésből	75
8.5. Összefonódás és LOCC	76
8.6. Nyitott kvantumrendszer: master-egyenlet	76
8.7. Kvantumcsatornák	77
Problémák, gyakorlatok	77
9. Klasszikus információelmélet	79
9.1. Shannon-entrópia, matematikai tulajdonságok	79
9.2. Üzenetek	80
9.3. Adattömörítés	80
9.4. Kölcsönös információ	82
9.5. Csatornkapacitás	82
9.6. Optimális kódok	83
9.7. Kriptográfia és információelmélet	84
9.8. Entrópiusan irreverzibilis műveletek	84
Problémák, gyakorlatok	85
10. Kvantuminformáció-elmélet	87
10.1. Von Neumann-entrópia, matematikai tulajdonságok	87
10.2. Üzenetek	88
10.3. Adattömörítés	89
10.4. Elérhető kvantuminformáció	91
10.5. Összefonódás: a kvantumkommunikáció erőforrása	92
10.6. Összefonódás koncentrációja (desztilláció)	93
10.7. Összefonódás hígítása	94
10.8. Entrópiusan irreverzibilis műveletek	95
Problémák, gyakorlatok	96
11. Kvantumszámítógép	99
11.1. Párhuzamos kvantumszámítás	99
11.2. Aritmetikai függvény kiszámítása	100
11.3. Orákulumprobléma: az első kvantumalgoritmus	101
11.4. Keresési kvantumalgoritmus	103
11.5. Fourier-algoritmus	104
11.6. Perióduskereső kvantumalgoritmus	105
11.7. Hibajavítás	107
11.8. Kvantumkapuk, kvantumkörök	109
Problémák, gyakorlatok	111

12. Qubit-termodinamika	113
12.1. Termális qubit	113
12.2. Ideális qubitgáz	114
12.3. Informatikai és termodinamikai entrópiák	115
12.4. Kvantumtermalizáció	116
12.5. Kvantumhűtőgép	117
12.6. Termális qubit külső munkával	118
12.7. Kvantum-Carnot-körfolyamat	120
Problémák, gyakorlatok	121
Függelék	123
F.1. Bevezetés	123
F.2. A hőtartály, ütközések	124
F.3. Egy kecses irreverzibilis művelet	125
F.4. Új matematikai sejtés a relatív kvantumentrópiára	126
Feladatmegoldások	127
Irodalomjegyzék	143
Tárgymutató	145

Szimbólumok, jelölések, rövidítések

$\{ , \}$	Poisson-zárójel, antikommutátor	\circ	kompozíció
$[,]$	kommutátor	\times	Descartes-szorzat
$\langle \rangle$	várhatóérték	\otimes	tenzorszorzat
\hat{O}	mátrix	tr	nyom
\hat{O}^\dagger	adjungált mátrix	tr _A	parciális nyom
\oplus	moduló összegzés	log	bináris logaritmus
x, y, \dots	fázistérpontok	\hat{x}	qubit hermitikus mátrix
Γ	fázistér	$ x\rangle$	számítási bázisvektor
$\rho(x)$	fázistéreloszlás, klasszikus állapot	$ \uparrow\rangle, \downarrow\rangle$	spin-fel, spin-le bázis
x, y, \dots	bináris számok	$\mathbf{n}, \mathbf{m}, \dots$	Bloch-egységvektorok
$x_1 x_2 \dots x_n$	bináris sor	$ \mathbf{n}\rangle$	qubit állapotvektor
$\rho(x)$	diszkrét klasszikus állapot	\mathbf{s}	qubit polarizációvektor
\mathcal{M}	művelet	$\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$	Pauli-mátrixok
\mathcal{T}	polarizációtükrözés	$\hat{\sigma}$	Pauli-mátrixok vektora
\mathcal{I}	egységművelet	$\mathbf{a}, \mathbf{b}, \boldsymbol{\alpha}, \dots$	valóstérbeli vektorok
\mathcal{L}	Lindblad-generátor	\mathbf{ab}	valós skalárszorzat
$A(x), A(x)$	klasszikus fizikai mennyiség	\hat{a}, \hat{a}^\dagger	keltő, elnyelő mátrix
$H(x)$	Hamilton-függvény	X, Y, Z	1-qubit Pauli-kapuk
P	indikátor függvény	H	Hadamard-kapu
$\Pi(x), \Pi(x)$	klasszikus effektus	$T(\varphi)$	fáziskapu
\mathcal{H}	Hilbert-tér	cNOT	vezérelt NOT
d	vektortér dimenzió	F	hűség
$ \psi\rangle, \varphi\rangle, \dots$	állapotvektorok	E	összefonódás mérték
$\langle\psi , \langle\varphi , \dots$	adjungált állapotvektorok	$S(\rho), S(p)$	Shannon-entrópia
$\langle\psi \varphi\rangle$	komplex skalárszorzat	$S(\hat{\rho})$	von-Neumann-entrópia
$\langle\psi \hat{O} \varphi\rangle$	mátrixelem	$S(\rho' \ \rho), S(\hat{\rho}' \ \hat{\rho})$	relatív entrópia
$\hat{\rho}$	sűrűségmátrix, kvantumállapot	$ \Psi^\pm\rangle, \Phi^\pm\rangle$	Bell-bázisvektorok
\hat{A}	kvantumfizikai mennyiség	\hat{M}_n	Kraus-mátrixok
\hat{H}	hamilton	$ n; E\rangle$	környezeti bázisvektor
\hat{P}	hermitikus projektor	X, Y, \dots	klasszikus üzenet
\hat{I}	egységmátrix	$H(X), H(Y)$	Shannon-entrópia
\hat{U}	unitér leképezés	$H(X Y)$	feltételes Shannon-entrópia
$\hat{\Pi}$	kvantumeffektus	$I(X:Y)$	kölcsönös információ
p	valószínűség	C	csatornkapacitás
w	súly keverékben	$\rho(x y)$	feltételes eloszlás
		$\rho(y x)$	átviteli valószínűség /függvény
T	hőmérséklet	Q	hőmennyiség
E	energia	S_{th}	termodinamikai entrópia
W	munka		
q-	kvantum-		
LO	lokális művelet	LOCC	lokális művelet és klasszikus kommunikáció

1. Bevezetés

Klasszikusnak nevezzük – a kvantumos ellentétéként – azokat az alapvető fizikai dinamikai jelenségeket és elméleteiket, amelyek a XIX. század végéig a makroszkopikus világ tanulmányozása útján váltak ismertté. Galilei, Newton, Maxwell egymásra épülő eredményeinek egyik legtömörebb megfogalmazása a klasszikus kanonikus dinamika volt. Ugyanekkorra a mikrovilág atomi szerkezetének hipotézise is elfogadottá vált. A klasszikus dinamikát az atomi szabadsági fokokra kiterjesztve bizonyos, makroszinten is jelentkező mikroszkopikus jelenségeket pontosan meg lehetett magyarázni. Ez közvetett, de elegendő bizonyítékot szolgáltatott az atomi szerkezetre. A mikrovilág más jelenségei (pl. a „vonalas” atomi színeképek) azonban ellenálltak a klasszikus elmélet természetes kiterjesztésének a mikroszkopikus szabadsági fokokra. Planck, Einstein, Bohr, Sommerfeld munkái nyomán kialakult a klasszikus elméletnek egy egyszerű megszorítása. Ez a naiv *kvantált* klasszikus elmélet képes volt a mikroszkopikus szabadsági fokok stacionárius állapotainak nemfolytonos (diszkrét) spektrumát leírni. A stacionárius állapotok közötti átmenetek részletes dinamikáját azonban az elmélet nem tartalmazza. A sikerek (pl. a „vonalas” színeképek leírása) hatására viszont már formálódott a *kettős* fizikai világgép: mikroszkopikus szabadsági fokokra más törvényszerűségek érvényesek, mint a makroszkopikusokra. Schrödinger, Heisenberg, Born, Jordan működése nyomán kialakult a *kvantumelmélet*¹, mely a mikroszkopikus szabadsági fokok teljes és a tapasztalatokkal tökéletesen egyező leírását adja. Ez a q-elmélet már nem egyszerűen a klasszikus elmélet kvantált változata volt, hanem egy attól teljesen idegen szerkezetű új formalizmus, melyet kifejezetten a mikroszkopikus szabadsági fokokra alkalmaztak. A makroszkopikus szabadsági fokokra viszont továbbra is a klasszikus elmülethez ragaszkodtak.

Egy kockacukor tömegközépponti mozgása makroszkopikus szabadsági fok. Egy atomé mikroszkopikus. A kockacukorra klasszikus elméletet, az atomra kvantumelméletet kell használnunk. Nincs azonban éles határ arra, mikortól kell egyik elmületről a másikra váltani. Továbbá nyilvánvaló, hogy a kockacukor klasszikus tömegközépponti mozgását az őt alkotó atomok kvantumos mozgásából is le kell tudni vezetni. Ezért a klasszikus és q-elmélet között egy sajátos egymásra utaltság van, amelynek a fenti dichotómiára konzisztens megoldást kell adnia. A q-elmélet Neumann János szerinti „axiomatikus” megfogalmazása a kettős fizikai világgép keretei

¹ A gyakori kvantum- előtagot jobbra a q- előtaggal fogjuk rövidíteni.

között a mikrovilág teljes, a makrovilág klasszikus elméletével összhangban maradó leírását adja.

Tegyünk egy kitérőt a kettős világkép alternatívájáról. Eszerint minden makroszkopikus jelenség visszavezethető mikroszkopikusok összeségére. Ilyen módon tehát a világmindenség alapvető fizikai elmélete a q-elmélet lehetne, a makroszkopikus jelenségek klasszikus dinamikája pedig ebből határesetként volna levezethető. A jelenlegi q-elmélet azonban nem áll meg a saját lábán. Hivatkozik eredendően makroszkopikus rendszerekre is, ezért klasszikus fizikát is igényel. Az egész fizikai világra önmagában érvényes (univerzális) q-elmélet a mintegy fél évszázad óta tartó elméleti erőfeszítések ellenére ma még nincs elfogadva.

Ezért a kurzus során a kettős fizikai világkép keretein belül maradunk. A Neumann-féle „axiomatikus” q-elméletet fogjuk használni. Az elmélet bizarr strukturái és tulajdonságai között történetileg a diszkrétség (kvantáltság) volt az első, nevét is innen kapta. Az évtizedek során további meglepő tulajdonságokra is fény derült. „Divattá” vált paradox tulajdonságokat levezetni a q-elméletben. A paradox jóslatoknak van egy külön vonulata (Einstein–Podolski–Rosen, Bell) amelyik elkülönített q-rendszerek közötti korrelációkra épül, olyanokra, amelyek sohasem létezhetnének klasszikusan. Egy másik sarkalatos paradoxon pedig a q-állapot másolhatatlansága, tehát az, hogy a lehetséges másolatok hűsége alapvetően és erősen korlátozott lesz.

A paradoxonok szerepe eleinte a q-elmélet jobb megismerése volt. Megtudtuk, melyek a q-rendszerek legfőbb *differencia specifikái* a makrorendszerekhez képest. Az eredetileg paradox kvantáltság következményeit viszonylag jól értjük, és a hasznát (lásd pl. félvezetők, szupravezetés, szuperfolyékonyság) is értékelni tudjuk a klasszikus fizikához képest. Az 1900-as évek végére a *q-korrelációkkal* kapcsolatos paradoxonok kerültek előtérbe. Ezek hasznát fokozatosan derítjük fel. A kulcsszó: *információ!* A q-elméletből következő q-korrelációk a klasszikus információkezelés lehetőségeit nagy mértékben kitágítják, ideértve az információ tárolását, kódolását, továbbítását, titkosítását, védelmét, feldolgozását, miként algoritmusokat, játékstratégiákat is. Mindez tárgyát képezi a tág értelemben vett q-információ-elméletnek. Kurzusunk csupán az alapelemeket tárgyalja, bevezető szinten.

A 2.–4. fejezetek összefoglalják a klasszikus, a félklasszikus és a q-fizikát. A 2. és 4. fejezet egymásnak mintegy tükörképe. Igyekeztem a klasszikus és a q-elmélet között létező párhuzamokat maximálisan kiaknázni, és csak a jelen kontextusban lényeges eltéréseket elkülöníteni. Ez utóbbiak például: a q-állapotok korlátozott megismerhetősége egyfelől, és általánosabb korrelációik másfelől. Az 5. fejezet az absztrakt kétállapotú q-rendszer – a qubit – jólismert elméletét közli. A 6. fejezet egyqubites q-információs eljárásokat és két alkalmazást ismertet: a bankjegy és a titkosítás-kulcs másolásvédelmét. A 7. fejezetet az összetett q-rendszereknek szenteltem. Ismertetem a q-korrelációk (másnéven összefonódás) elméletét, betekintést adok három elméleti előzménybe, végül két q-információs alkalmazást mutatok: a szupersűrű kódolást és a teleportációt. A 8. fejezet bevezet a q-műveletek modern elméletébe. A 9.-10. fejezetek kezdetben megint egymás tükörképei. A klasszikus és q-információ elméleti alapjai, a Shannon, illetve a Neumann entrópiákra épülve, párhuzamosan mutathatók be. Igaz ez még az adattömörítés klasszikus és kvantumos elméleteire is. A 10. fejezetben viszont külön rész foglalkozik a csak kvantumosan

létező összefonódás informatikai erőforrás jellegével. A 11. fejezet egyszerű bevezetést ad a q-információ kvintesszenciáját jelentő q-algoritmusok témájába. Ismeretemet a q-számítógép ötletéhez vezető koncepciót. Két, röviden tanítható nevezetes q-algoritmus, az orákulum és a keresési probléma mellett nehezebbek is helyet kapnak. A 12. fejezet önálló bevezetés a qubit q-termodinamikába. A Függelék eseti témája a termodinamikai és informatikai entrópiák intuitív azonosítása, ennek produktív erejéről szól.

Minden fejezetet Problémák, gyakorlatok rövid válogatása zár. Bizonyos mértékig ezek hivatottak kárpótolni az olvasót a főszöveg lakonikusságáért. A főszöveg olykor hiányzó vagy szűkszavú bizonyításai és magyarázatai itt még felbukkanhatnak. Így nyerhető további benyomás, hogyan lehetne származtatni és alkalmazni a gazdaságos főszövegbe tömörített ismereteket.

Részletesebb tudásra Nielsen és Chuang monográfiája ajánlható [1], ez mindmáig alapvető referencia, egyetemben Preskillével [2], illetve a Bouwmeester, Ekert és Zeilinger szerkesztette kötettel [3]. Bizonyos tételek, illetve módszerek, pl. a 10. és 11. fejezetben az [1] vagy [2] munkákat követik és ott közvetlenül ellenőrizhetőek. A bibliográfia folytatása [4]–[10] tankönyvek olyan hagyományos területekről, mint például a klasszikus és q-fizika, ezek szükségesek a q-információs tanulmányokhoz. Egy-egy hasznos összefoglaló szerepel a q-kriptográfiáról [11], illetve q-számítógépről [12] is. A bibliográfia további része szerény válogatás az idetartozó eredeti publikációkból. A magyar kiadásban megemlítem magyar szerzők monográfiáit, Imre és Balázs angol nyelvű munkáját a q-információ mérnöki megközelítéséről [58], Petz szintén angol matematikai művét q-információról [59], és nem utolsósorban ajánlom Geszti magyar nyelvű modern q-mechanika tankönyvét [60], külön q-információ-elméleti függelékkal.