1. Bevezetés

Klasszikusnak nevezzük – a kvantumos ellentéteként – 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 színképek) 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" színképek leírása) hatására viszont már formálódott a *kettős* fizikai világkép: 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 elmélethez 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 elméletről 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 világkép keretei

[1] A gyakori kvantum- előtagot jobbára 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 struktúrái 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 titkosírás-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. Ismertetem 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 ellenőrízhetők. 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 utolsó sorban ajánlom Geszti magyar nyelvű modern q-mechanika tankönyvét [60], külön q-információ-elméleti függelékkel.