Ismerd meg!

Gondolatok az általános relativitás elméletről

GÖRBE EZ A MI VILÁGUNK. Tessék ezt nekem elhinni, még akkor is, ha furcsának hangzik. Bolyai és Lobacsevszkij ugyan már megsejtette, Rieman le is írta a geometriáját, de aki igazán megtalálta és meg is magyarázta az okait és következményeit, az Albert Einstein volt.
Ő, az ún. Általános Relativitás „egyszerű" tenzor egyenletével egy új „görbe" (görbült) világot teremtett itt és most, valamint mindenütt és mindenkor a világegyetemben.

a) $$R_{ik} - \frac{1}{2} g_{ik} R = \chi T_{ik}$$

az *i*, és *k* ko – vagy kontra – variáns indexek

míg:

b) R_{ik} egy 10 tagú görbületi tenzor (az ún. Ricci tenzor), a tér szerkezetét pedig a g_{ik} metrikus tenzor adja, valamint

c) $R = R_{ik} g^{ik}$, míg χ (kappa) egy univerzális állandó, és T_{ik} az energia-impulzus tenzor.

Ugyanakkor nagyon kérem önöket ne is próbálják megoldani a fenti a.), b.) ,c.) együttest, (egyenletrendszert) mert már sokan megpróbálták és mind különböző megoldást találtak.

Hogy melyik a helyes? Talán mindegyik, vagy egyik sem?

Ha még emlékeznek, a FIRKA 2004-2005/6-os számában írt rövid gondolataimra, tudhatják, hogy a válaszom igen is és nem is, mert a mi világunk nemcsak „görbe" de „bizonytalan" is, rendezett és rendezetlen is, kaotikus és áttekinthető is ugyanakkor, és egyszerre mindenütt, szóval nem determinált hanem probabilisztikus, azaz sem nem „igen" sem nem „nem", hanem mindig csak „LEHETSÉGES" (Ezt a kijelentést talán Einstein nem is írná alá, de hát tévedni emberi dolog). Persze az is lehet, hogy ÉN TÉVEDEK!!!

Az 1905-ben publikált „Speciális Relativitás" dolgozatában Einstein bevezette a 4-dimenziós világot.

Ez a „Világ", hogy úgy mondjam, „sima" (lapos) volt. A 3 tér-dimenzió: előttem és mögöttem, tőlem jobbra és balra, valamint fölöttem és alattam egyenes vonalakat feltételezett. A 4-ik dimenzió: az „Idő" pedig egyenletesen folyt a múltból a jövő felé. Ezek egyesítése adta a kompakt 4-dimenziós világot.

De 1915-re mindez megváltozott. A közbeeső 10 év alatt Einsteint gyötörte a kérdés, hogy mi okozza az általános gravitációt? Miért esett az alma a fáról Newton fejére, és nem fordítva, a fejéről a fára? Persze a newtoni alma mese valóban egy „nyári kacsa", de ha nem is esett az alma Newton fejére, mégis csak *le esett* és nem a földről *mászott fel a fára.* Vajon miért? tette fel magának a kérdést Einstein. Egyáltalán mi okozza a testek közötti kölcsönös vonzást (itt nem a mágneses vonzásra gondolunk, hanem a newtoni általános vonzásra) és miért nem a kölcsönös taszítást?

A választ 1915. november 25-én adta meg, amely az 1916. március 20-án, az Annalen der Physics-ben publikált dolgozatában található. Lényege az, hogy a 4-dimenziós világ nem „sima", hanem „görbe" azaz „GÖRBÜLT". Elméletét először az 1919. május 29-én bekövetkezett Napfogyatkozás során igazolták kísérletileg. A Royal Astronomical Society, Sir Arthur Eddington által vezetett kutatócsoportjának kísérleti megfigyeléseit, eredményeit és a várható következményeit, a fénysugár görbült térben való elhajlását, a Royal Society 1919. november 6-i ülésén publikálták. Ekkor végre a világ is felfigyelt Albert Einsteinre.

Az Általános Relativitáselmélet további kísérleti igazolásai közé tartozik a Merkur perihelium mozgásának pontos kiszámítása, a fény-spektrumban előálló ún. vörös-eltolódás. Ezekre most itt nem térhetünk ki részletesebben.

A relativitás-elvével foglalkozó szakemberek véleménye megoszlik arról, hogy mi is az, ami az általános elmélet alapjául szolgál. Az egyik oldal az ún. ekvivalencia-elvet vallja magáénak, a másik pedig esküszik a 4 dimenziós tér geometriai görbületére.

Én úgy találom, hogy mind a két félnek van valami igaza. Az ekvivalencia-elvet vallók inkább Newtonhoz nyúlnak vissza, míg a görbületet hangsúlyozók Bolyai-Lobacsevszkij és Riemann munkáját tekintik alapvetőnek. Én az utóbbiakhoz tartozom, de itt kötelességem megemlíteni a másik tábor alaptételét is.

Az ekvivalencia-elve így hangzik: A tehetetlenségi és a gravitációs erőtér teljes mértékben azonos egymással, közöttük nincs semmi különbség, az egész csak interpretáció kérdése.

Én szeretnék mélyebbre hatolni, mert életem munkája alapján ezt sejtem az igazi Einsteini követelménynek.

És végül is mi az hogy „gravitáció", mit értünk gravitációs-erőtér alatt?

Tessék elképzelni egy szorosan kifeszített fehér lepedőt, amelynek a közepébe bele esik egy nagy tömegű test. Minden más apró tárgy a lepedőn a nagy tömegű test felé fog „gurulni"(más szóval a közepén levő nagy tömegű test magához „vonzza" az apróbbakat). Miért ?

Talán a nagyobbik tömeg egy belső (intrinsec) tulajdonsággal rendelkezik, amit vonzó erőnek nevezhetünk, vagy mert a lepedő begörbült a nagy tömegű test körül és ez okozza a „gurulást" ?

A válasz erre nem is olyan egyszerű. De talán könnyebben megközelíthető, ha a lepedőre egy másik ugyanolyan nagy tömegű testet ejtünk mint az első volt, attól pár centiméternyi távolságra. (Itt szándékosan elhallgattam a centiméterek számát, okom erre Eötvös Loránd örökké híressé vált inga kísérlete a tömegek kölcsönös „vonzásának" igazolására).

Nos, merre fognak most „gurulni" az apróbb testek?

A választ Einstein adja meg. *Minden* test körül a 4-dimenziós tér-idő görbült.

Sőt ennél még tovább megyünk. Nincs is olyan önállóan létező valami a Világűrben mint a tér és az idő. Az anyagi testek létezése hozza őket létre. És mindegyik test saját görbült tér-idő-vel rendelkezik. Hogy az apróbb testek ilyenkor merre „gurulnak" az az egyes tér-idők relatív görbültségétől függ.

A fenebb leírt Einsteini tenzor-egyenlet minden megoldása ezt sugallja. És a kísérletek ezt „bizonyítják".

A gyakorlat pedig valóban ezt igazolja.

De az egyenletek bizonyos megoldásai másik két kérdést is tisztáznak.(az egyes megoldások lényegében abban különböznek, hogy milyen értéket adunk az χ állandónak. Erre Einstein nem adott határozott választ.).

Az egyik kérdés a taszítással kapcsolatos. Ha egymás közelében több anyagi test létezik, gondoljunk például a Világegyetem rengeteg Galaxisára (Tejútrendszerére) és milliárdnyi égitestére, akkor az egyes tér-idők görbültségének relatív volta szabja meg a vonzás vagy taszítás dominálását. A mai mérések például a Világegyetem tágulására utalnak, azaz a kölcsönös taszítás mutatkozik dominánsnak. Egyes elméletek szerint ebben az ún. sötét tömegek is szerepet játszhatnak. E feltételezésnek a szépséghibája, hogy ilyen sötét tömegeket még senki sem talált.

A másik kérdés, amit a fenti tenzor-egyenletek sugallnak, a „zárt és véges" vagy „nyitott és végtelen" Világegyetem kérdése.

Ennek a kérdésnek a megválaszolása szintén az χ állandó értékétől függ és mindkét lehetőséget nyitva tartja. Az eddigi mérések a nyitott, végtelen és táguló Világegyetemet sugallják, de ezt nem tekinthetjük végleges válasznak.

Van ugyanis egy harmadik lehetőség is, az ún. „pulzáló" Világegyetem, amely hol tágul, hol szűkül. De ennek tárgyalására itt nem térhetünk ki.

E cikk keretében még két kérdést szeretnék érinteni. A sokszoros Világegyetemek kérdését, és az idő kimagasló szerepét az elmélet továbbfejlesztésében.

A fent említett a, b, c, tenzor-egyenletek egyes megoldásai, mint azt már Einstein is előre látta, lehetővé teszik bizonyos „lyukak" felbukkanását a görbült tér-idő néhány pontján. Ezek az ún. Einstein-Rosen hidak, ha elég mélyek, „wormholok"-at (giliszta-lyukakat, alagutakat) képeznek, amelyeken keresztül lehet bújni, és eljutni egy a mienkkel párhuzamos másik Világegyetembe. Mivel az ilyen lyukak száma egyelőre megszámlálhatatlan (de feltehetően nagyon sok), fennáll annak a lehetősége, hogy a mienkkel nagyon sok párhuzamos Világegyetem létezhet.

Az elmélet szépséghibája egyelőre az, hogy ezek a „fekete lyukak", amelyek létezése már bizonyított, mindent elnyelnek és onnan még semmi (és persze senki) nem jött vissza a mi világunkba, hogy beszámoljon az alagút másik oldalán levő, azaz a mienkkel párhuzamos Világegyetemekről.

Az Általanos Relativitáselméleteben az időnek különleges szerepe van, és erre szeretnék ezen ismertetés végén kissé részletesebben kitérni.

Mi általában az időt mint egy folyamatosan folyó (valóban egy folyóhoz hasonlóan) a múltból a jövőbe simán haladó fogalomként regisztráljuk. De amint egy valódi folyóban a felszínen simának tűnő víz ömlése valójában az egyes molekulák össze-vissza ugrándozó mozgásából tevődik össze, úgy az idő folyása sem sima. Ezt a Kvantumelmélet probabilisztikus hozzáállásával oldja meg. A fotonok, mint a fénysugár legkisebb részecskéi (más szóval a fény-kvantumok), duális (kettős) tulajdonsággal rendelkeznek, akárcsak a tér és anyag minden más elemi részecskéje. Részecskéknek lehet őket tekinteni, de ugyanakkor hullám tulajdonságaik is vannak, tehát rezegnek, azaz frekvenciájuk van. Hogyan egyeztethető össze e probabilisztikus, azaz a valószínűség elvén alapuló nézet az általános relativitás 4-dimenziós görbült, de determinált (biztos és nem valószínű) tér-idő felfogásával. Ez a helyzet igen nagy fejfájást okozott Einsteinnak, aki életének utolsó 35 évében megpróbálta a két nézőpontot egymásba fűzni, és ez sem neki sem másnak eddig nem sikerült.

És ma sem állunk közelebb a megoldáshoz. A determinált és valószínű, a határozott és bizonytalan, együttes megközelítése a valóságnak, egyelőre elkerüli a modern tudomány művelőit.

A legújabb kutatások (String and Super-string), elméletek a részecske-hullám heisenbergi dualitását apró görbült húrocskák rezgésével próbálják helyettesíteni, hogy az említett mikro-világ és makro-világ remélt egységes világ-elméletet létrehozzák.

Ennek az elméletnek eddig legalább három szépséghibája van.

1. Kísérletileg még senki sem mutatta ki a húrocskák létezését.
2. Az elmélet legalább 13 dimenziós tér-időt feltételez,(ami ugyan matematikailag nem lehetetlen, de a fizikai szemlélettel nehezen egyeztethető össze),
3. Még így sem sikerült az egységes világ-elméletet létrehozni.

Soraimat azzal zárom, amire a már fentebb említett FIRKA cikkemet építettem. A mi világunk nemcsak görbe, de valószínűtlen is. Nincs határozott (determinált) valóság, csak a valószínű, probabilisztikus hozzáállás visz közelebb a megoldáshoz.

Gondolkodjunk ezeken a kérdéseken, és akkor világunk nemcsak egységesebbé, de *EMBERIBBÉ* is válik.

Weiszmann Endre
a City University of New York professzora

A nyilvános kulcsú kriptográfia egy lehetséges alkalmazása

I. rész

Bevezetés

Napjainkban a világhálón az e-kereskedelem egy gyorsan fejlődő és terjedő terület. De több különbség van a valós és az internet kereskedelem között, és a legalapvetőbb kérdések a biztonságot és megbízhatóságot jelentik. Mikor egy fogyasztó belép az üzletbe bizonyos javakat vásárolni, bizonyítja személyazonosságát, és megjelöl egy fizetési módszert. De az interneten mindketten, mind a vevő mind az eladó nehézségekkel bír azonosságának bizonyításakor. Hogyan tudja az eladó meggyőzni a vevőt, hogy átadjon fontos információkat? Hogyan tudja biztosítani magát az eladó egy valódi rendelésről? Hogyan lehet rájönni, hogy egy hívatlan harmadik lemásolja vagy módosítja az üzlet lebonyolításához szükséges információkat? Ezek a kérdések és még sok más ehhez hasonló kérdés képezi az interneten való kereskedelem problémáit.

Annak érdekében, hogy biztonságos e-kereskedelmi alkalmazásokat építhetsünk, szükségünk van a biztonsági igények meghatározására. Szükség van az alábbi négy nagy követelmény teljesítésére, egy biztonságos e-kereskedelem váza esetén:

- *bizalmasság (confidentiality):* az információk megvédése mindenki elől, a címzetten kívül
- jogosultság vizsgálat (authentication), hitelesség (certification): lehetőség bizonyos személy bizonyítására
- *sértetlenség (integrity):* gondoskodni a jogosulatlan információ változtatás lehetetlenségéről
- *(le)tagadhatatlanság (non-repudiation):* megakadályozni egy entitást, hogy előző elkötelezettségét vagy tettét letagadja

Az általánosan használt módszer az adatok bizalmasságának megőrzése érdekében a kriptográfia. De ahogy ezt az elkövetkezőkben meglátjuk, a hagyományos kriptográfiával a hitelességet, sértetlenséget és letagadhatatlanságot lehetetlen kivitelezni, biztosítani. A nyilvános kulcsú kriptográfia az első igazából forradalmi előrelépés ezen elvárások