Katedra teoretické fyziky
Přírodovědecká fakulta
Univerzita Palackého

VYBRANÉ PARTIE SOUČASNÉ FYZIKY

Tomáš Opatrný a Lukáš Richterek

Olomouc 2005

Abstrakt

Tento text si klade za cíl seznámit čtenáře s vybranými partiemi současné fyziky. První část pojednává o základních představách moderní kosmologie, o nejdůležitějších vlastnostech Vesmíru a o možných scénářích jeho dalšího vývoje. Seznámení se základními principů by mělo čtenáře připravit a motivovat ke studiu další odborné literatury. Druhá oblast se týká kvantového zpracování informace. Dozvíme se tam o tom, proč nás velmi zajímá možnost sestrojení kvantového počítače, jak by takový počítač pracoval a k čemu by mohl být užitečný, co to je kvantová kryptografie a teleportace kvantových stavů. Náš text v žádném případě nepokrývá zvolená témata vyčerpávajícím způsobem, měl by spíše sloužit k základní orientaci a motivovat k hlubšímu studiu problémů, jimž se ostatní fyzikální kurzy na PřF UP věnují jen okrajově nebo vůbec. Od čtenáře – studenta předpokládáme základní znalost diferenciálního i integrálního počtu a fyzikálních pojmů na úrovni základního kurzu fyziky na PřF UP a též základní znalosti z kvantové teorie. Na několika místech se odvoláváme teorii relativity a na statistickou fyziku; znalost těchto disciplin popř. jejich matematického aparátu je pro čtenáře bezesporu výhodou.

Cílová skupina

Text je primárně určen jako doplněk k volitelnému předmětu „Vybrané kapitoly z fyziky“ pro 5. ročník učitelství všeobecně vzdělávacích předmětů kombinací, pro něž je fyzika jedním z aprobačních předmětů. Doufáme, že by mohl oslovit i ostatní zájemce o fyziku ať už z řad studentů UP či veřejnosti.

Obsah

Přílohy

Kapitola 1

Friedmannovy kosmologické modely

Studijní cíle: V této kapitole odvodíme základní rovnice popisující rozpínání (i případné smršťování) vesmíru. Ukážeme si vliv základních kosmologických parametrů na možný budoucí osud vesmíru, budeme diskutovat jejich měření i nejpravděpodobnější hodnoty.

Klíčová slova: Friedmannova rovnice, Hubbleův a decelerační parametr, hustotní parametr, kosmologická konstanta Λ, Hubbleovy diagramy, inflace.

Potřebný čas: 300 minut.

Otázky spojené s existencí, vlastnostmi našeho vesmíru i s postavením člověka v něm se vždy promítaly do základů lidské kultury, náboženských a filozofických směrů. Od dob Galileových a Newtonových se rozvíjí kosmologické teorie vycházející z fundamentálních fyzikálních zákonů, jež kladou důraz jak na přesné výpočty a předpovědi, tak především na konfrontaci se stále se zpřesňujícími pozorováními. V tomto smyslu je fyzikální kosmologie vědeckou, tj. vyvratitelnou teorií, v níž jsou naše představy a modely neustále korigovány, aby bylo dosaženo stále větší a lepší shody s tím, co v našem vesmíru pozorujeme.

Průvodce studiem

Naše chápaní vesmíru a jeho vývoje s neustále vyvíjí, jak po stránce teoretické, tak získáváním a zpracováním stále přesnějších experimentálních dat. V moderní kosmologii se doslova a do písmene uplatňuje celá fyzika – od fyziky mikrosvěta a kvantové teorie pole až po teorii relativity. Zde se budeme zabývat pouze základy relativistické kosmologie, základními pozorovanými vlastnostmi vesmíru a z nich vyplývajícími nejjednoduššími modely. Otázky týkající se raného a velmi raného vesmíru v prvních minutách po velkém třesku, inflační teorie a problematiky formování struktur najde čtenář v podrobnějších monografiích, např. [1.17, 1.23, 1.27, 1.30, 1.32].

Obr. 1.1: Galaxie v souhvězdí Andromedy známá pod označením z katalogu francouzského astronoma Charlese Messiera (1730-1817) jako M31, v NGC katalogu J.L.E. Dreyera (1852–1926) je uvedena pod číslem NGC 224 (oba katalogy jsou dnes k dispozici na internetových adresách `http://www.seds.org/messier/` resp. `http://www.seds.org/~spider/ngc/ngc.html`). Jedná se o superobří spirální galaxii typu Sb ve vzdálenosti více jak $2{\cdot}10^6$ ly, spolu s naší Galaxií je největší v naší místní skupině. Na obrázku vidíme také dvě satelitní trpasličí eliptické galaxie NGC 205 a NGC 221 (M32). Galaxie M31 představuje zvětšenou obdobu naší vlastní Galaxie s hmotností okolo $3{\cdot}10^9\,M_\odot$. Do místní skupiny Galaxií patří celkem asi 30 galaxií, z nichž nejznámější jsou satelity naší Mléčné dráhy – nepravidelné galaxie Velké a Malé Magellanovo mračno (LMC neboli Large Magellanic Cloud a SMC neboli Small Magellanic Cloud). Galaxie v místní skupině tvoří gravitačně vázaný systém a díky tomu se od sebe nevzdalují v důsledku rozpínání vesmíru (viz část 1.5), naopak lze předpokládat, že ve velmi vzdálené budoucnosti může dojít ke srážkám např. naší Galaxie a M31.

1.1 Základní východiska a principy relativistické kosmologie

Mikoláš Koperník (1473–1543)

V tomto textu se budeme zabývat společnými základy moderních kosmologických teorií, které můžeme shrnout označením *standardní kosmologický model*. Vychází ze dvou základních principů, *zobecněného Koperníkova principu* a *principu uniformity*. Jádro prvního tvoří tvrzení, že se nenalézáme ve středu vesmíru ani v jeho význačném bodě. V historickém kontextu jde o velmi důležitý myšlenkový zlom, neboť ve starověku i středověku byla právě Země považována za střed všehomíra, okolo něhož obíhala všechna ostatní tělesa. Průlom představoval heliocentrický model sluneční soustavy Mikoláše Koperníka z r. 1543, jenž zbavil Zemi „výsadního“ postavení.

Dnes víme, že z kosmologického hlediska není význačná ani naše Galaxie nebo kupa galaxií, dokonce i hmota, z níž jsou složena naše těla představuje pouze malou část v porovnání s převažujícím typem hmoty ve vesmíru.

Homogenita a izotropie na velkých vzdálenostech představují klíčové vlastnosti vesmíru!

„Princip uniformity“ nebo také „princip homogenity a izotropie“ tvrdí, že vesmír je ve velkých měřítkách homogenní a izotropní, tj. stejný ve všech místech a ve všech směrech. Je zřejmé, že např. v měřítkách naší sluneční soustavy, popř. naší Galaxie uvedený princip neplatí; ve Slunci popř. v jádru Galaxie je soustředěno mnohem více hmoty než na okraji. Homogenita a izotropie se projevuje až na velkých škálách o rozměrech řádově 10^3 Mpc, jak o tom svědčí výsledky řady pozorování (viz obr. 1.2–1.4)

O vlastnostech vesmíru vypovídají i zdánlivě triviální otázky; příkladem může být tzv. *Olbersův paradox*. Otázka „Jak to, že je noční obloha temná?“ byla poprvé zformulována Keplerem v roce 1610, diskutována Halleym a Cheseauxem v 18. století a zpopularizována německým lékařem a astronomem Heinrichem Wilhelmem Matthäusem Olbersem (objevitelem planetek Pallas a Vesta i komety 13P/Olbers) v r. 1826. Význam otázky vynikne k kontextu dobových filozofických představ, užitečné je i srovnání s odpovědí, které dává současná kosmologie. Pokud by vesmír byl nekonečný a obsahoval nekonečné množství rovnoměrně rozmístěných hvězd, pak by noční obloha měla být stejně jasná jako povrch Slunce. Zjednodušeně řečeno, v každém místě oblohy bychom nalezli svítící hvězdu.[1]

H. W. M. Olbers (1758–1840)

Olbersův paradox: i jednoduchá otázka vede k hlubšímu zamyšlení!

Možná řešení paradoxu jsou následující:

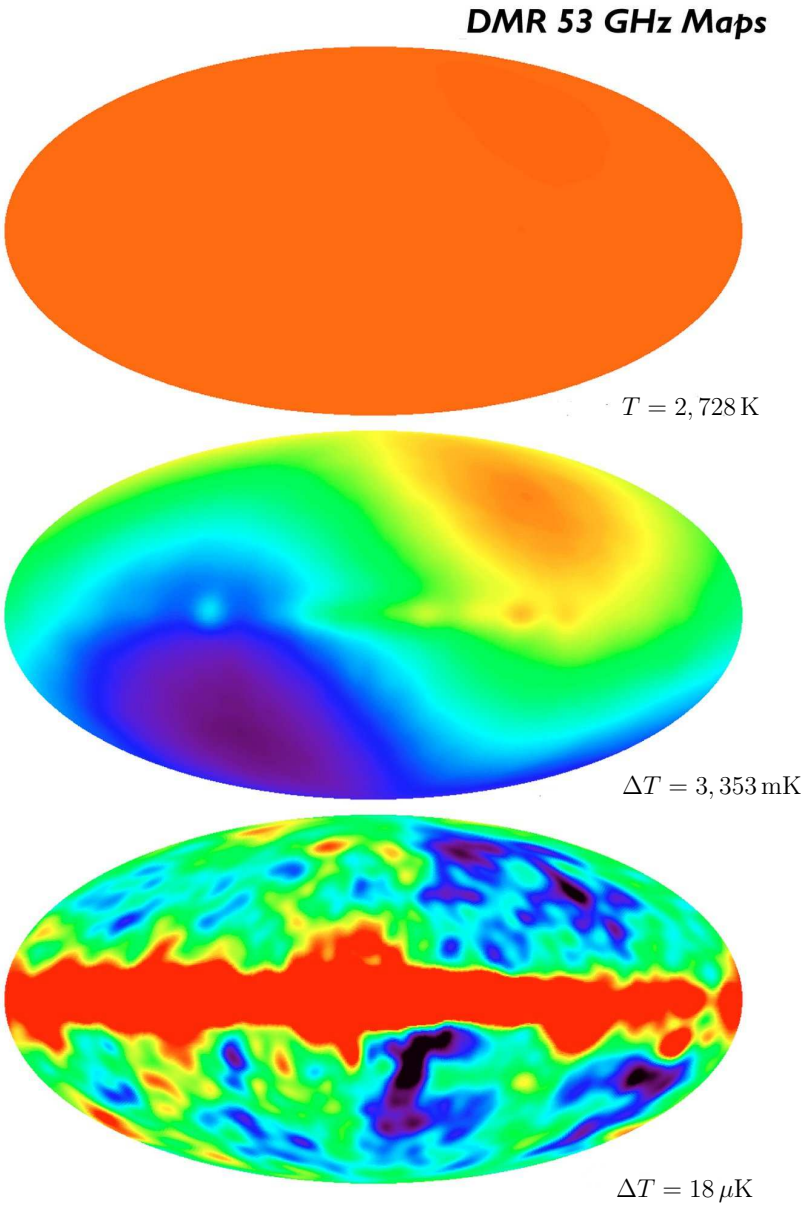
1. mezihvězdný prach nám brání vidět vzdálené hvězdy;
2. vesmír obsahuje pouze konečný počet hvězd;
3. hvězdy nejsou rozmístěny rovnoměrně
4. vesmír se rozpíná, světlo od nejvzdálenějších hvězd má takový rudý posuv, že je mimo oblast viditelného světla;
5. vesmír má konečné stáří, světlo od nejvzdálenějších objektů k nám ještě nedorazilo.

Z hlediska moderní kosmologie se nejvýznamněji se uplatňuje právě poslední možnost – vesmír existuje pouze konečnou dobu, podle nejnovějších odhadů asi $(13{,}7 \pm 0{,}2)$ miliard světelných let [1.5].

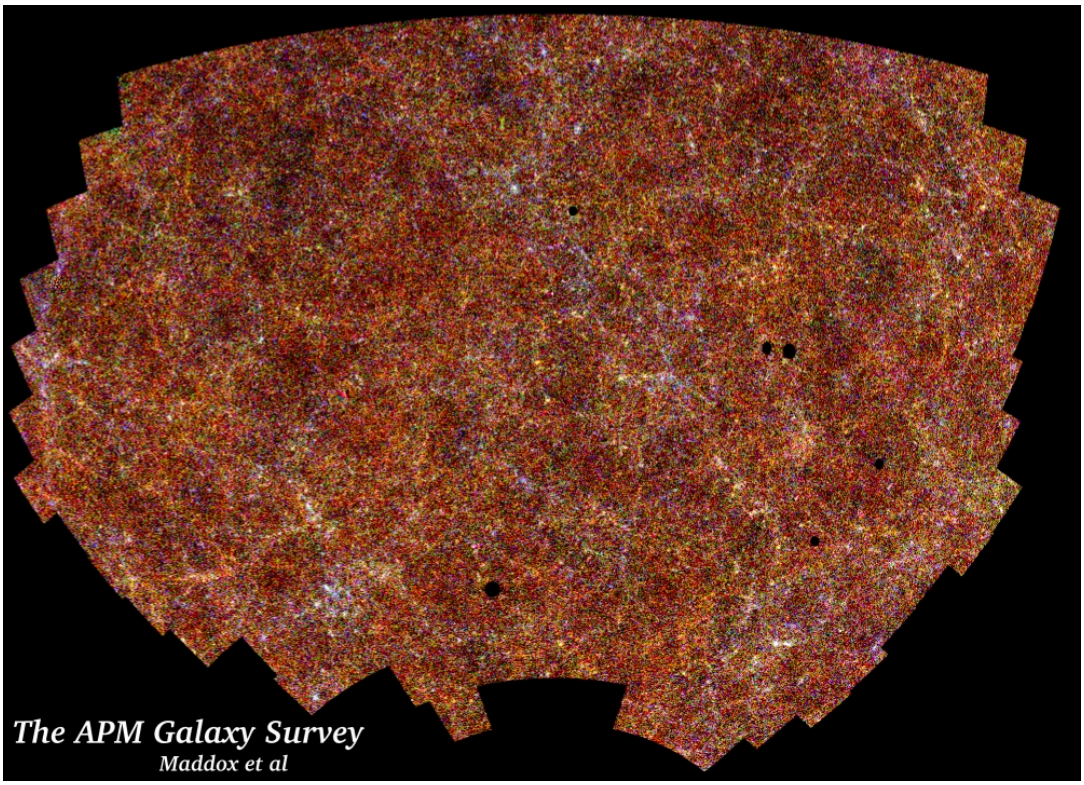
Shrnutí

Vesmír je ve velkých měřítkách homogenní a izotropní; svědčí o tom rozbory kosmického mikrovlnného záření a statistické sledování rozmístění galaxií v něm. Nejen z Olbersova paradoxu vyplývá, že vesmír netrvá „odjakživa“, ale pouze konečnou dobu.

[1] Přesnější formulace vychází s poznatku, že světelný tok od vzdálených zdrojů klesá se čtvercem jejich vzdálenosti od nás r, tj. s $1/r^2$, ale objem kulové vrstvy, v níž se hvězdy nacházejí je roven $4\pi r^2 \mathrm{d}r$, výsledný světelný tok z takové vrstvy tak nezávisí na její vzdálenosti; podrobnější diskusi lze najít např. v [1.40].



Obr. 1.2: Teplota kosmického mikrovlnného záření podle výsledků družice COBE, konkrétně její součásti DMR (Differential Microwave Radiometer). Tři mapy teploty záření pro různé rozsahy jsou vyneseny v galaktických souřadnicích, rovina naší Galaxie se nachází uprostřed. Horní mapa dokládá, že záření je vysoce homogenní s teplotou $T \approx 2{,}73\,\mathrm{K}$. Prostřední část ukazuje rozdíly v teplotě řádu mK. Zřetelná dipólová anizotropie odpovídá pohybu sluneční soustavy vůči kosmickému mikrovlnnému záření (jeho klidové soustavě). Pokud tuto anizotropii odečteme, získáme zbývající anizotropii řádu μK na dolní mapě, přičemž výrazný červený pruh uprostřed odpovídá záření z naší Galaxie; více obrázků a informací lze nalézt na `http://lambda.gsfc.nasa.gov/product/cobe/` a v [1.4]. Studium anizotropií mikrovlnného záření, jež jsou podle současných představ „otiskem“ fluktuací hustoty vesmíru v době vzniku mikrovlnného záření (tj. asi 300-400 000 let po velkém třesku), je považováno za klíč k pochopení vzniku pozorovaných struktur (galaxií). Poskytuje dosud nejpřesnější určení stáří vesmíru i dalších kosmologických parametrů – viz stránky projektu WMAP (Wilkinson Microwave Anisotropy Probe) `http://map.gsfc.nasa.gov/` nebo např. [1.37]



Obr. 1.3: Úhlové rozdělení galaxií podle projektu APM (Automated Plate Measuring, domovská stránka `http://www-astro.physics.ox.ac.uk/~wjs/apm_survey.html`) [1.24]. Zahrnuta je asi 1/4 oblohy rozdělená do menších čtverečku, jejichž barva odráží počet galaxií v každém z nich (čím světlejší, tím více). Vidíme, že na velkých škálách se počet galaxií v jednotlivých směrech neliší.

Pojmy k zapamatování

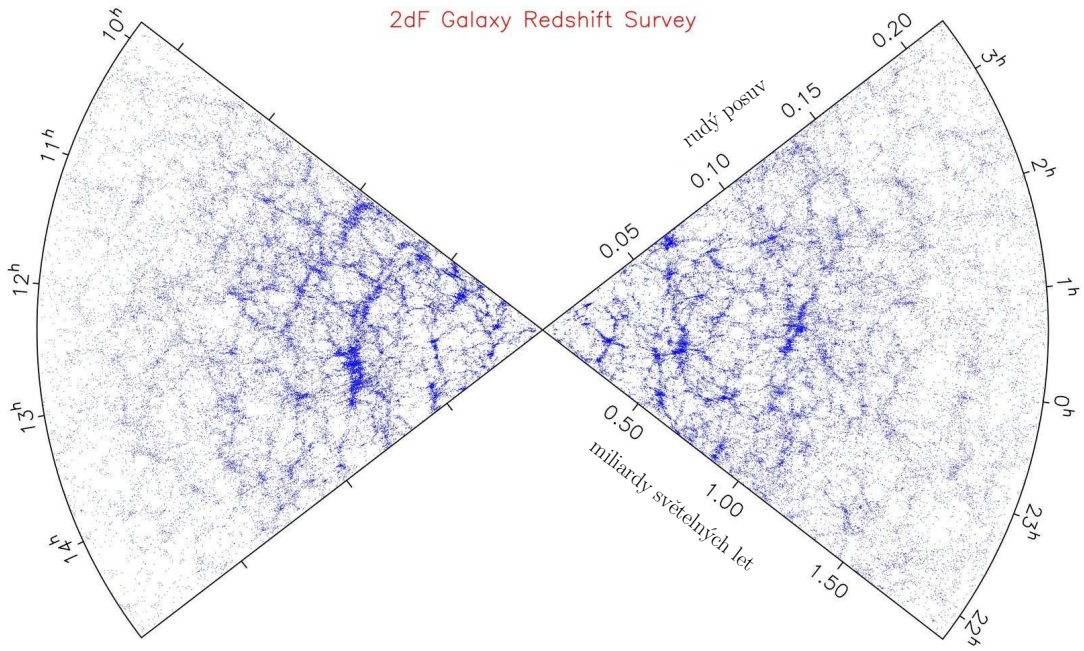
- Koperníkův princip
- princip homogenity
- princip uniformity
- Olbersův paradox

Kontrolní otázky

1. *Co rozumíme pod Koperníkovým principem?*
2. *Jaké nejstarší objekty v současné době ve vesmíru pozorujeme Hubbleovým teleskopem?*
3. *Jaké je přibližně stáří vesmíru?*

Cvičení

1. Naše Galaxie s hmotností $2{,}5{\cdot}10^{11}\,M_\odot$ a galaxie M 31 v souhvězdí Andromedy o hmotnosti $3{,}6{\cdot}10^{11}\,M_\odot$ jsou dvě největší galaxie v tzv. místní soustavě galaxií. Předpokládejme, že tvoří dvojnou soustavu a obíhají kolem společného hmotného středu po kruhových drahách. Určete velikost oběžné doby mezi nimi, jestliže vzdálenost mezi nimi je asi 700 kpc [1.38].



Obr. 1.4: 2dF Galaxy redshift survey ukazuje polohu 62 559 z celkového počtu 220 929 galaxií, u nichž byly určeny úhlové souřadnice a rudý posuv [1.9]. V souladu s Hubbleovým zákonem (1.5.1) je radiální vzdálenost galaxií určena rudým posuvem z. Zdánlivě galaxií v prostoru s rostoucí vzdáleností od nás ubývá, ale jde jen o výběrový efekt – ve velkých vzdálenostech můžeme pozorovat pouze nejzářivější objekty. Pro malé rudé posuvy, kde je počet galaxií zmapován důkladněji, vidíme zřetelně vláknovitou strukturu s uzly a mezerami. Homogenita vesmíru předpokládá, že rozmístění galaxií ve vzdálenějších oblastech musí být stejné. Více obrázků a informací lze nalézt na stránkách projektu `http://www.mso.anu.edu.au/2dFGRS/`.

Řešení

1. Podle 3. Keplerova zákona platí

$$\frac{a^3}{T^2} = \frac{G}{4\pi^2}\,(M_1 + M_2)\,,$$

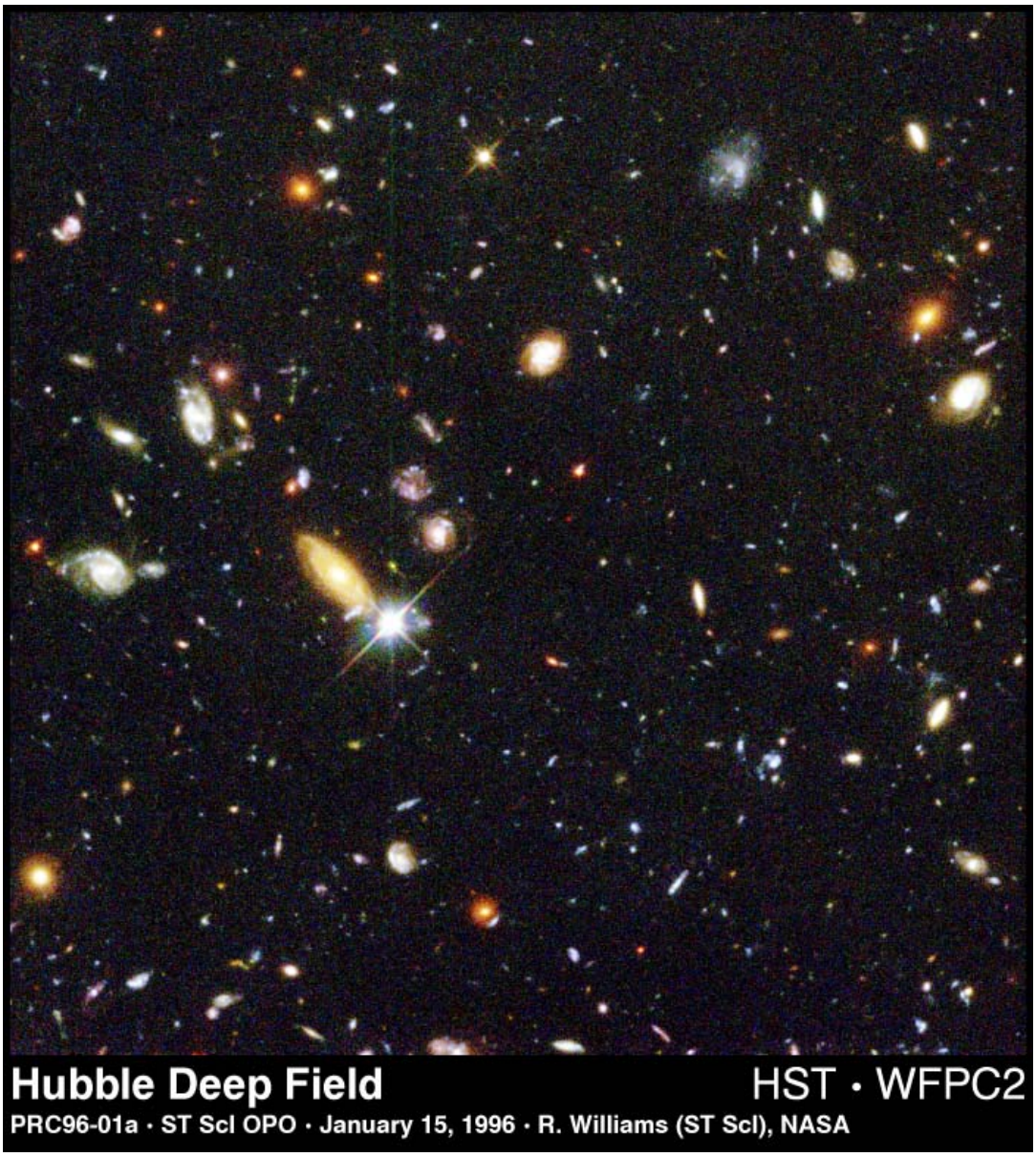
odkud

$$T = \sqrt{\frac{4\pi^2 a^3}{G\,(M_1 + M_2)}}.$$

Po dosazení v jednotkách SI $G = 6{,}67{\cdot}10^{-11}\,\mathrm{m^3{\cdot}kg{\cdot}^{-1}s^{-2}}$, $a = 700\,\mathrm{kpc} \approx 2{,}16{\cdot}10^{22}\,\mathrm{m}$, $M_1 \approx 4{,}975{\cdot}10^{41}\,\mathrm{kg}$ a $M_1 \approx 7{,}161{\cdot}10^{41}\,\mathrm{kg}$ vychází $T \approx 2{,}22{\cdot}10^{18}\,\mathrm{s} \approx 7{,}03{\cdot}10^{10}$ let. Galaxie oběhnou okolo společného hmotného středu asi za 70 miliard let.

Průvodce studiem

K plnému porozumění moderní kosmologii a korektnímu odvození rovnic, popisujících expanzi vesmíru je nezbytná znalost obecné teorie relativity. Avšak



Obr. 1.5: Pohled na velmi vzdálené galaxie Hubbleovým teleskopem označovaný jako „the Hubble deep field“. Snímek pokrývá malou část oblohy asi 30× menší než Měsíc, tak malou, že se v ní nachází pouze několik jasných hvězd z naší Galaxie. Naopak vidíme řadu galaxií v různých stadiích vývoje – od spirálních a eliptických, až po slabě zářící nepravidelné objekty, jejichž světlo bylo vysláno méně jak miliardu let po velkém třesku, tj. zhruba před 12–13 miliardami let, a které patří k nejstarším dosud pozorovaným objektům ve vesmíru. Vzhledem k homogenitě a izotropii lze i tento malý vzorek oblohy považovat za reprezentativní, typické rozmístění galaxií.

i čtenář, jenž se studiem Einsteinovy teorie dosud nezabýval, může řadu jevů odvodit a popsat na základě elementárnějších úvah vyžadujících znalosti na úrovni základního vysokoškolského kurzu fyziky. Potřebuje k tomu především

Friedmannovu rovnici (1.2.3) a rovnici pro práci vykonanou tlakem při rozpínání vesmíru. Zájemce o nástin plně relativistického odvození rovnic odkazujeme na následující podkapitolu 1.3.

1.2 Friedmannova rovnice

V této části vyjdeme z modelu Newtonovského vesmíru, v němž uvažujeme pouze nerelativistické pohyby a gravitace je chápána jako síla působící mezi hmotnými částicemi [1.19, 1.23]. Friedmannova rovnice (1.2.3) v tomto případě popisuje zachování celkové mechanické energie částice (galaxie) v průběhu vesmírné expanze. V relativistickém odvození namísto klasické hustoty hmotnosti musíme započítat hustotu energie v souladu se známou rovnicí ekvivalence hmotnosti a energie $E = mc^2$ a namísto gravitace jako síly uvažovat zakřivení prostoročasu, nicméně výsledek je formálně tentýž, bez jakýchkoli korekčních členů či přiblížení. Do hustoty energie však musíme započítat všechny její formy. K pochopení a správné interpretaci šíření světla v zakřiveném vesmíru (Hubbleovy diagramy, fotometrická vzdálenost apod. – viz část 1.10) se pak bez teorie relativity neobejdeme!

Východiskem našich úvah je zákon zachování energie.

Rozpínání vesmíru pozorujeme jako vzájemné vzdalování galaxií objevené Edwinem Hubblem (viz část 1.5). Náš newtonovský model si lze představit jako rozpínající se plyn, jehož „molekuly“ jsou celé galaxie (ty samy se nerozpínají). Gravitace naopak galaxie přitahuje k sobě a rozpínání zpomaluje. Zvolíme-li počátek souřadnic v „místě“ některé galaxie (např. naší), potom na galaxii ve vzdálenosti R působí pouze hmota obsažená v kouli o poloměru R (působení vnějších vrstev se vyruší, to je důležitá vlastnost gravitační i coulombovské síly v klasické fyzice), jejíž hmotnost $M = 4\pi R^3\varrho/3$, kde ϱ je hustota vesmírné „tekutiny“. Mechanická energie uvažované galaxie bude potom

$$E = \frac{1}{2}\,m\left(\frac{\mathrm{d}R}{\mathrm{d}t}\right)^2 - \frac{GMm}{R} = \frac{1}{2}\,m\left(\frac{\mathrm{d}R}{\mathrm{d}t}\right)^2 - \frac{4\pi}{3}\,m\varrho R^2.$$

Předpokládáme-li, že na galaxii působí ještě izotropní síla $F = \Lambda mc^2 R/3$, jíž odpovídá potenciální energie[2]

$$U = -\frac{1}{6}\,\Lambda mc^2 R^2,$$

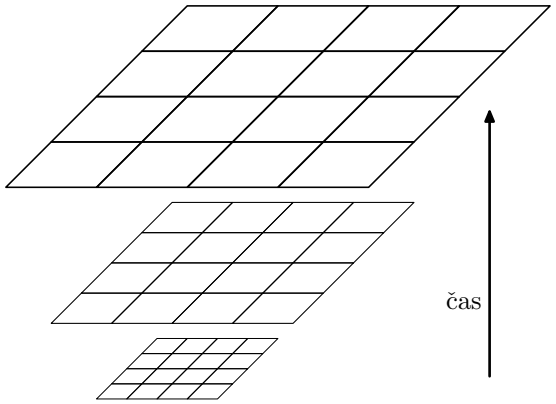
Podle nejnovějších pozorování musíme počítat s kosmologickou konstantou.

vychází celková energie dané galaxie

$$E = \frac{1}{2}\,m\left(\frac{\mathrm{d}R}{\mathrm{d}t}\right)^2 - \frac{1}{6}\,\Lambda mc^2 R^2 - \frac{4\pi}{3}\,m\varrho R^2. \tag{1.2.1}$$

Parametr Λ o rozměru m^{-2} nazýváme *kosmologickou konstantou* a standardně bývá interpretována jako vliv energie samotného vakua.

[2] V daném kontextu jde o *ad hoc* předpoklad; zavedení kosmologické konstanty přirozeně plyne z Einsteinových rovnic obecné teorie relativity (1.3.2) a v důsledku novějších pozorování (viz např. [1.5, 1.20]) o nutnosti zahrnout i tento člen dnes málokdo pochybuje.



Obr. 1.6: K zavedení „comoving“ souřadnic: souřadnicový systém je unášen expanzí, takže uvažovaný objekt zůstává stále ve zvoleném bodě souřadnicové sítě, ostatní body se od něj v důsledku rozpínání vzdalují.

Vzhledem k homogenitě a izotropii rozpínání je výhodné zavést tzv. *„comoving“ souřadnice*, které jsou „unášeny“ rozpínáním a pro zvolenou galaxii zůstávají po celou dobu konstantní. Zvětšování vzájemných vzdáleností je pak popsáno *expanzním faktorem* $a = a(t)$ závisejícím na čase (viz obr. 1.6). Pro skutečnou vzdálenost proto platí

Pro jednodušší popis zavádíme „comoving“ souřadnice a expanzní faktor.

$$\boldsymbol{R} = a(t)\boldsymbol{x} \tag{1.2.2}$$

a po dosazení do (1.2.1) získáváme

$$\frac{2E}{mx^2} = \left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 - \frac{1}{3}\,\Lambda c^2 a^2 - \frac{8\pi}{3}\,\varrho a^2.$$

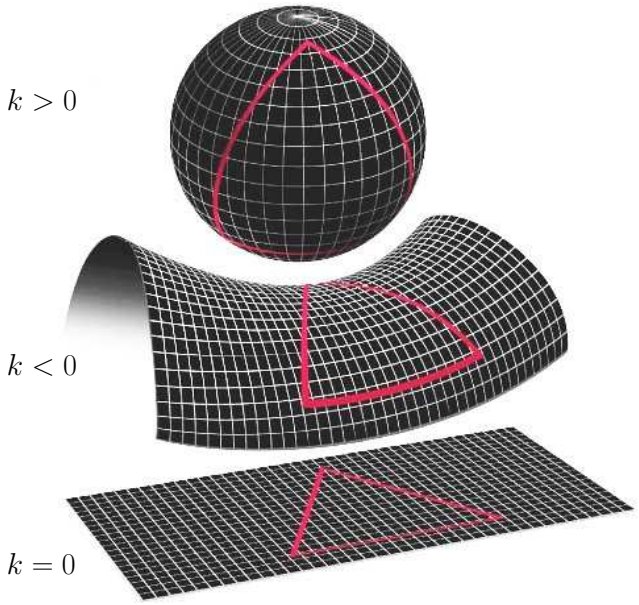
Jak energie E, hmotnost m i „comoving“ souřadnice x jsou v rámci našeho newtonovského modelu pro uvažovanou galaxii konstantami, použijeme-li ekvivalenci hmotnosti a energie $E = mc^2$, bude $2E/(mx^2) = 2c^2/x^2$. Výraz $2/x^2$ odráží geometrii vesmíru v „comoving“ souřadnicích a obvykle klademe $2/x^2 = -k$. Po dosazení do předcházející rovnice dospějeme k základní, tzv. *Friedmannově rovnici* popisující rozpínání vesmíru pomocí expanzního faktoru

Friedmannova rovnice

$$\frac{1}{a^2}\left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 = \frac{8\pi G}{3}\,\varrho + \frac{1}{3}\,\Lambda c^2 - \frac{kc^2}{a^2}. \tag{1.2.3}$$

Nazvána je po ruském matematikovi A. A. Friedmannovi[3], který v roce 1922 odvodil a předpověděl rozpínání vesmíru z Einsteinových rovnic obecné teorie relativity. Výše uvedené odvození dokazuje platnost rovnice (1.2.3) pro newtonovský model vesmíru, v rámci obecné teorie relativity lze dokázat (viz část 1.3) její platnost pro všechny homogenní izotropní kosmologické modely popsané metrickým tenzorem (1.3.1).

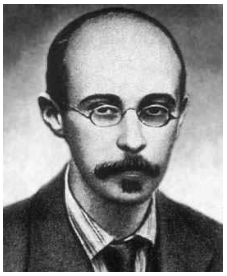
[3]V české literatuře se setkáme se dvěma různými přepisy jeho jména: s fonetickým ruským transkriptem „Fridman“ a nebo s podobou obvyklou v anglosaské literatuře, kterou používáme v textu. Friedmannova maminka, profesionální pianistka, se za svobodna jmenovala Ludmila Vojáčková [1.13].



Obr. 1.7: Dvourozměrné analogie různých geometrií vesmíru v závislosti na hodnotách parametru k (opraveno podle http://map.gsfc.nasa.gov/m_uni/uni_101shape.html).

Průvodce studiem

Friedmannova rovnice určuje změnu expanzního faktoru s časem, tj. „rychlost“ rozpínání. Každodenní zkušenost nám napovídá, že k popisu běžných pohybů potřebujeme znát i zrychlení, tj. druhou derivaci expanzního faktoru podle času – pouze s Friedmannovou rovnicí zcela určitě nevystačíme. I když zavedení konstant k a *Lambda* ve Friedmannově rovnici můžeme chápat formálně, mají svůj fyzikální význam. Těmto otázkám se budeme věnovat ve zbytku podkapitoly.



A. A. Friedmann (1888–1925)

Parametr k s rozměrem m^{-2} charakterizuje konstantní křivost vesmíru a po vhodném přeškálování souřadnic lze uvažovat pouze tři hodnoty $k = 0, \pm 1$; potom už jde o parametr bezrozměrný a s takovým budeme nadále pracovat [1.17]. Hodnota $k = 0$ odpovídá nekonečnému *plochému* vesmíru, v němž platí zákony eukleidovské geometrie (součet úhlu v trojúhelníku je roven 180°, obvod kruhu je roven $2\pi r$). Hodnota $k = 1$ odpovídá *uzavřenému* konečnému vesmíru, jehož geometrie je podobná geometrii kulové plochy (lze jej v principu „obejít dokola“, součet úhlů v trojúhelníku je větší než 180°, obvod kruhu menší než $2\pi r$). Konečně hodnota $k = -1$ odpovídá nekonečnému *otevřenému* vesmíru, jehož geometrie je podobná geometrii sedlové plochy (součet úhlů v trojúhelníku je menší než 180°, obvod kruhu větší než $2\pi r$); dvourozměrné analogie zmíněných geometrií vesmíru jsou znázorněny na obr. 1.7. V současné době nelze s jistotou říci, jakou geometrii náš vesmír má, zda je přesně plochý, jak jej vnímáme z běžné každodenní zkušenosti (kdy běžně používáme uvedené vzorce eukleidovské geometrie), nebo je na velkých škálách zakřiven. Víme, že

Parametr k určuje geometrii vesmíru: buď je otevřený, plochý nebo uzavřený.

se jeho geometrie od Euklidovy liší jen velmi málo, což teoreticky vysvětlujeme pomocí mechanismu inflace (viz část 1.7). Podrobnější rozbor topologie našeho vesmíru v závislosti na parametru k lze nalézt např. v [1.15, 1.17, 1.27, 1.32].

Druhou rovnici popisující expanzi vesmíru získáme z práce, kterou přitom hmota – „plyn galaxií“ – vykoná. V části 1.4 ukážeme, že různé formy energie, jež mohou být ve vesmíru obsaženy, přispívají k tlaku „plynu“ rozdílně a vedou k odlišné závislosti hustoty energie ϱ na čase. Uvažujme kouli o objemu V, jejíž objem se změní o $\mathrm{d}V$. Energie obsažená v tomto objemu bude

$$E = \frac{4\pi}{3}\,\varrho c^2 R^3.$$

Považujeme-li rozpínání za adiabatické (nedodáváme žádnou vnější energii), musí podle 1. věty termodynamické platit

$$\mathrm{d}E + p\,\mathrm{d}V = 0 \qquad \text{neboli} \qquad \frac{\mathrm{d}E}{\mathrm{d}t} + p\,\frac{\mathrm{d}V}{\mathrm{d}t} = 0.$$

Dosadíme-li postupně

$$\begin{aligned}\frac{\mathrm{d}E}{\mathrm{d}t} &= 4\pi\varrho c^2 R^2\,\frac{\mathrm{d}R}{\mathrm{d}t} + \frac{4\pi}{3}\,c^2 R^3\,\frac{\mathrm{d}\varrho}{\mathrm{d}t},\\ \frac{\mathrm{d}V}{\mathrm{d}t} &= 4\pi R^2\,\frac{\mathrm{d}R}{\mathrm{d}t}\end{aligned}$$

a přejdeme ke „comoving“ souřadnicím (1.2.2), dospějeme k další důležité rovnici pro změnu hustoty energie s časem

Další důležitá rovnice určuje změnu hustoty vesmíru s časem.

$$\frac{\mathrm{d}\varrho}{\mathrm{d}t} + \frac{3}{a}\frac{\mathrm{d}a}{\mathrm{d}t}\left(\varrho + \frac{p}{c^2}\right) = 0. \tag{1.2.4}$$

Ke změně hustoty energie přispívá jednak zvětšení objemu (člen $\mathrm{d}a/\mathrm{d}t$, jednak práce vykonaná při expanzi tlakem p, jež se v našem newtonovském modelu mění na gravitační potenciální energii.

Derivujeme-li Friedmannovu rovnici (1.2.3) podle času, získáme

$$2\,\frac{1}{a}\,\frac{\mathrm{d}a}{\mathrm{d}t}\,\frac{1}{a^2}\left[a\,\frac{\mathrm{d}^2a}{\mathrm{d}t^2} - \left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2\right] = \frac{8\pi G}{3}\,\frac{\mathrm{d}\varrho}{\mathrm{d}t} + \frac{2kc^2}{a^3}\,\frac{\mathrm{d}a}{\mathrm{d}t},$$

po dosazení za $\mathrm{d}\varrho/\mathrm{d}t$ z (1.2.4) dále

$$\frac{1}{a}\,\frac{\mathrm{d}^2a}{\mathrm{d}t^2} - \left(\frac{1}{a}\,\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 = -\,4\pi G\left(\varrho + \frac{p}{c^2}\right) + \frac{kc^2}{a^2}$$

a odečtením Friedmanovy rovnice (1.2.3) druhou základní rovnici popisující „zrychlení“ rozpínání vesmíru

Třetí a poslední ze stěžejních rovnic určuje „zrychlení“ kosmologické expanze.

$$\frac{1}{a}\,\frac{\mathrm{d}^2a}{\mathrm{d}t^2} = -\frac{4\pi G}{3}\,\left(\varrho + \frac{3p}{c^2}\right) + \frac{1}{3}\,\Lambda c^2. \tag{1.2.5}$$

Vidíme, že v rozporu s intuitivním předpokladem, že tlak „plynu galaxií“ se podílí na rozpínání vesmíru, přispívá naopak ke zpomalení expanze podobně jako $\Lambda < 0$. Naopak $\Lambda > 0$ přispívá ke zrychlení expanze. Tlak p skutečně nemůže vyvolávat rozpínání vesmíru, neboť v homogenním vesmíru nemohou existovat tlakové síly (vyžadovaly by gradient tlaku.

Při konkrétních výpočtech se neobejdeme bez stavové rovnice.

K řešení získaných rovnic je ještě zapotřebí znát závislost tlaku na hustotě $p = p(\varrho)$. Závisí na typu materiálu (energie) a nazýváme ji *stavovou rovnicí*. S nejdůležitějšími případy (z kosmologického hlediska) stavových rovnic se setkáme v části 1.4.

Shrnutí

Friedmannova rovnice (1.2.3), rovnice pro časovou změnu hustoty energie (1.2.4) a z nich vyplývající rovnice (1.2.5) popisují rozpínání vesmíru prostřednictvím změny expanzního faktoru $a(t)$ s časem. K jejich řešení potřebujeme znát ještě stavovou rovnici, tj, závislost tlaku na hustotě charakterizující typ materiálu (energie) vyplňující vesmír. Geometrie vesmíru se liší v závislosti na parametru k a mohou nastat 3 případy: plochý, otevřený a uzavřený vesmír.

Pojmy k zapamatování

- comoving souřadnice
- kosmologická konstanta
- Friedmannova rovnice
- stavová rovnice
- plochý, uzavřený a otevřený vesmír

Kontrolní otázky

1. *Jak závisí geometrie vesmíru na parametru k?*
2. *Uveďte příklady vzorců eukleidovské geometrie, které v zakřiveném prostoru neplatí.*
3. *Jakou geometrii má náš vesmír?*
4. *Jakou závislost udává stavová rovnice?*
5. *Čím se vyznačují „comoving“ souřadnice?*
6. *Jaká vliv má kosmologická konstanta Λ na rozpínání vesmíru?*

Průvodce studiem

Pro čtenáře obeznámeného se základy obecné teorie relativity v následující kapitole naznačíme, jak lze rovnice (1.2.3) a (1.2.5) odvodit z Einsteinových rovnic aplikovaných na homogenní izotropní vesmír. Ostatní čtenáři mohou tuto část při prvním čtení přeskočit, neboť její prostudování není nezbytně nutné k pochopení dalšího výkladu. Dále se budeme odvolávat pouze na Robertsonovu-Walkerovu metriku (1.3.1).

1.3 Robertsonova-Walkerova metrika

V obecné teorii relativity je základní veličinou popisující geometrii prostoročasu metrický tenzor $g_{\mu\nu}$. Lze ukázat (viz např. [1.15, 1.27]), že předpoklad homogenity a izotropie splňuje *Robertsonova-Walkerova metrika*

Robertsonova-Walkerova metrika popisuje prostoročas s konstantní křivostí.

$$\mathrm{d}s^2 = -c^2\mathrm{d}t^2 + a(t)^2\left[\frac{\mathrm{d}r^2}{1-kr^2} + r^2\left(\mathrm{d}\vartheta^2 + \sin^2\vartheta\,\mathrm{d}\varphi^2\right)\right], \tag{1.3.1}$$

pro kterou v „comoving“ souřadnicích $x^0 = ct$, $x^1 = r$, $x^2 = \vartheta$ a $x^3 = \varphi$ má metrický tenzor tvar

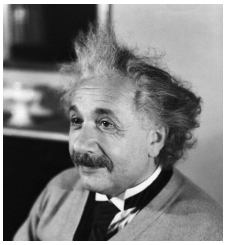
$$g_{\mu\nu} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & a(t)^2/(1-kr^2) & 0 & 0 \\ 0 & 0 & a(t)^2 r^2 & 0 \\ 0 & 0 & 0 & a(t)^2 r^2 \sin^2\vartheta \end{pmatrix}.$$

Parametr $k = \pm 1{,}0$ zavedený v předcházející podkapitole 1.2 charakterizuje křivost prostoročasu, jež v důsledku homogenity a izotropie musí být konstantní. Obsah vesmíru modelujeme ideální tekutinou s tenzorem energie hybnosti (viz např. [1.16, 1.17, 1.26, 1.30])

$$T_{\mu\nu} = \left(\varrho + \frac{p}{c^2}\right) u_\mu u_\nu + g_{\mu\nu} p.$$

V klidové soustavě tekutiny pro složky čtyřrychlosti platí $u_0 = -c$, $u_r = u_\vartheta = u_\varphi = 0$, takže

$$T_{\mu\nu} = \begin{pmatrix} \varrho c^2 & 0 & 0 & 0 \\ 0 & pa(t)^2/(1-kr^2) & 0 & 0 \\ 0 & 0 & pa^2 r^2 & 0 \\ 0 & 0 & 0 & pa^2 r^2 \sin^2\varphi \end{pmatrix}.$$



Albert Einstein (1879–1955)

Po dosazení do *Einsteinových rovnic* obecné teorie relativity (viz např. [1.6, 1.15, 1.25, 1.36])

$$G_{\mu\nu} + \Lambda g_{\mu\nu} = \frac{8\pi G}{c^4} T_{\mu\nu} \tag{1.3.2}$$

získáme dvě nezávislé rovnice

Řešení Einsteinových rovnic vypočtené pro Robertsonovu-Walkerovu metriku.

$$\begin{aligned} \frac{3}{a^2}\left[\left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 + kc^2\right] - \Lambda c^2 &= 8\pi G\varrho, \\ -\frac{1}{a^2}\left[kc^2 + 2a\frac{\mathrm{d}^2 a}{\mathrm{d}t^2} + \left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2\right] + \Lambda c^2 &= 8\pi G\frac{p}{c^2}. \end{aligned}$$

První z nich dává přímo *Friedmanovu rovnici* (1.2.3), z druhé odečtením (1.2.3) pak získáme (1.2.5). Konečně z relativistického zákona lokálního zachování energie-hybnosti[4]

$$\sum_\nu \nabla_\nu T^{\mu\nu} = 0,$$

[4] Zákon musíme skutečně chápat v lokálním smyslu, protože pokud se zakřivení prostoročasu mění, energie nezůstává konstantní, ale odpovídajícím způsobem se mění; příkladem může být energie mikrovlnného záření, která v důsledku rozpínání vesmíru klesá (viz vztah (1.4.4)). V plochém prostoročase speciální teorie relativity ovšem zákon zachování platí globálně [1.15].

kde ∇_ν značí kovariantní derivaci, obdržíme přímo (1.2.4).

Zdůrazněme ještě jednou, že obecná teorie relativity dává hlubší a konzistentnější odvození rovnic, které jsme v části 1.2 získali pomocí newtonovského kosmologického modelu. Moderní relativistická kosmologie představuje jednu z nejúspěšnějších a nejzajímavějších aplikací Einsteinovy teorie relativity.

Shrnutí

Homogenní izotropní vesmír s konstantní křivostí je v „comoving“ sférických souřadnicích popsán Robertsonovou-Walkerovou metrikou (1.3.1). Zakřivení prostoru ovlivňuje šíření světelných signálů.

Pojmy k zapamatování

- Robertsonova-Walkerova metrika

Kontrolní otázky

1. Jak lze jednoduše zdůvodnit, že křivost vesmíru musí být konstantní?

Průvodce studiem

Na konci části 1.2 jsme se zmínili o významu stavové rovnice: charakterizuje typ materiálu, kterým je v našem modelu vesmír vyplněn a který určuje jeho rozpínání. V následující podkapitole probereme nejdůležitější příklady stavových rovnic a jim odpovídajících druhů energie.

1.4 Hustota a tlak

Tlak tekutiny v kosmologickém modelu závisí na typu materiálu, jímž je vesmír zaplněn. V zásadě může jít o běžnou hmotu, záření, vakuum, popř. o jejich kombinaci (což je samozřejmě nejrealističtější model); s každým z těchto typů energie je spojen jiný tlak.

Vztah $p = p(\varrho)$ mezi tlakem a hustotou popisuje *stavová rovnice*. Dosazením za p do (1.2.4) pak pro každý typ materiálu získáme předpis, jak se jeho hustota mění s časem. Stavová rovnice má pro uvažované typy energie tvar

Stavová rovnice v kosmologii není vůbec složitá!

$$p = w\varrho c^2. \tag{1.4.1}$$

Dosazením do rovnice (1.2.4) a integrací získáváme závislost

$$\varrho \propto \frac{1}{a^{3+3w}}. \tag{1.4.2}$$

Hmotu, tj. materiál z něhož se skládají i naše těla, popisujeme v kosmologickém měřítku jako tzv. *prach*. Srážky galaxií jsou odlišné od srážek molekul v plynu a

nevytvářejí žádný tlak, proto $w_\mathrm{m} = 0$.[5] Pro závislost hustoty energie hmoty ϱ_m na čase pak podle (1.4.2) vychází

Závislost hustoty hmoty na čase odpovídá změně objemu.

$$\varrho_\mathrm{m} \propto \frac{1}{a^3}; \tag{1.4.3}$$

hustota energie v kouli o poloměru $a(t)$ zůstává konstantní, neboť

$$\frac{\mathrm{d}}{\mathrm{d}}\left(\varrho_\mathrm{m} a^3\right) = 0.$$

Vidíme, že hustota energie hmoty – prachu klesá pouze v důsledku rozpínání vesmíru.

Stavovou rovnici pro záření (ideální „plyn“ tvořený z fotonů) lze odvodit z následující úvahy: uvažujme fotony s hybností $\boldsymbol{p}$, jež se odrážejí od rovinné stěny s plochou A postavenou kolmo na osu x. Při odrazu od stěny se změní složka hybnosti fotonu p_x na $-p_x$, ostatní složky zůstanou stejné. Průměrná síla, kterou působí fotony na stěnu, je dána změnou jejich hybnosti v uvažovaném časovém intervalu, tj. $2p_x$ násobek počtu fotonů, které v tomto intervalu do stěny narazí. Uvažujeme-li fotony s různými hybnostmi $\boldsymbol{p}$ a uvědomíme-li si, že v průměru se pouze polovina pohybuje v kladném směru osy x (polovina v opačném) a tlak je určen podílem síly a plochy, na kterou síla působí, pro tlak na stěnu A vychází

$$p_\gamma = \frac{1}{2}\, 2\, \overline{p_x v_x}\, n_\gamma,$$

kde n_γ je počet fotonů v jednotkovém objemu (koncentrace) a čárkou „nad“ značíme střední časovou hodnotu příslušného výrazu. Fotony se pohybují rychlostí c a pohyby ve směru os x, y i z jsou stejně pravděpodobné, takže v průměru se ve směru osy x pohybuje pouze 1/3 z jejich celkového počtu, takže

$$p_\gamma = \frac{1}{3}\, c\, |\boldsymbol{p}|\, n_\gamma.$$

Připomeňme, že energie E_γ fotonu o vlnové délce λ je rovna

$$E_\gamma = h\, \frac{c}{\lambda} = c\, |\boldsymbol{p}|\,,$$

kde h je Planckova konstanta. Pro záření tak dostáváme stavovou rovnici[6]

S zářením je spojen nenulový tlak!

$$p_\gamma = \frac{1}{3}\, \varrho_\gamma c^2$$

tj. $w_\gamma = 1/3$. Dosazením do (1.4.2) obdržíme

Hustota záření s časem klesá rychleji než hustota prachu.

$$\varrho_\gamma \propto \frac{1}{a^4}. \tag{1.4.4}$$

[5] Srážky galaxií znamenají v podstatě jejich prostoupení, nikoli odraz pružných „kuliček“; výsledkem jsou – v závislosti na hmotnosti interagujících galaxií - většinou různé nepravidelné galaxie nebo galaktický kanibalismus – pohlcení jedné galaxie druhou.

[6] Přesné odvození stavové rovnice ideálního fotonového plynu lze nalézt ve většině učebnic statistické fyziky, např. [1.10, 1.18, 1.21, 1.22]

Hustota energie záření tak klesá rychleji než hustota hmoty podle rovnice (1.4.3), protože se nejenom mění počet fotonů v jednotkovém objemu v důsledku rozpínání vesmíru, ale navíc se mění i jejich energie v důsledku rudého posuvu popsaného v části 1.6. Ze statistického rozboru záření černého tělesa popsaného Planckovým zákonem a Wienovým posunovacím zákonem (viz např. [1.10, 1.18, 1.21, 1.22]) plyne, že nejvíce energie připadá na fotony s energií $E \approx 2{,}8\, k_B T$ a střední energie fotonů záření při teplotě T je $\overline{E} \approx 2{,}7\, k_B T$. Při rozpínání vesmíru pak vlnová délka λ, energie fotonu E a rovnovážná teplota záření T závisejí na expanzním faktoru $a(t)$

$$\lambda \propto a(t), \qquad E \propto \frac{1}{\lambda} \propto \frac{1}{a(t)}, \qquad T \propto \overline{E} \propto \frac{1}{a}.$$

Počet fotonů se přitom zachovává, takže jejich počet n_γ v objemové jednotce musí při rozpínání klesat

$$n_\gamma \propto \frac{1}{a(t)^3},$$

zatímco energie fotonů v této jednotce se mění podle vztahu (1.4.4)

$$\varrho_\gamma = n_\gamma \overline{E} \propto T^4$$

v souladu se Stefanovým-Boltzmannovým zákonem.

Konečně hustota energie vakua se s časem nemění, tj.

Hustoty vakua na čase nezávisí: vakuum je prostě vakuum!

$$\frac{\mathrm{d}\varrho_\mathrm{v}}{\mathrm{d}t} = 0, \tag{1.4.5}$$

tudíž

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(\varrho_\mathrm{v} a^3\right) = \varrho_\mathrm{v} \frac{\mathrm{d}a^3}{\mathrm{d}t}.$$

Z rovnice (1.2.4) pak vychází

Stavová rovnice vakua nám ukazuje, že energie vakua je spojena s tlakem.

$$p_\mathrm{v} = -\varrho_\mathrm{v} c^2$$

neboli $w_\mathrm{v} = -1$. Výsledek je v souladu s požadavkem, že hustota energie vakua musí být stejná pro všechny pozorovatele, tj. invariantní pro vzhledem k Lorentzově transformaci speciální teorie relativity. V homogenním vesmíru musí být konstantní v prostoru, a kombinace časové i prostorové derivace v Lorentzových transformacích vyžaduje, aby nezávisela ani na čase (důkaz invariantnosti a odpovídající tvar tenzoru energie-hybnosti vakua lze nalézt např. v [1.19]).

V poslední době byla předložena řada hypotéz, předpokládajících, že vesmír obsahuje speciální látku zvanou „*quintessence*“, pro niž $w < -1/3$, popř. závisí na čase. Důvodem je snaha vysvětlit zrychlující se rozpínání vesmíru, jež by existence takové – dosud experimentálně neprokázané – formy hmoty vysvětlovala.

Zda existuje „quintessence“ nebo jde o pouhou spekulaci nelze dnes ještě rozhodnout.

Ze závislostí (1.4.3), (1.4.4) a (1.4.5) vyplývá, že vzájemný poměr jednotlivých druhů energie se s časem mění. Hustota energie záření klesá rychleji, než hustota energie hmoty; v raných stádiích vývoje vesmíru proto bylo dominantní záření. Je-li vakuum nositelem energie, bude v někdy v budoucnu dominantní právě vakuum. V současné době jsme v etapě rozpínání vesmíru, kde je dominantní nebo alespoň velmi významnou složkou „prach“ (chladná hmota).

Jiná dominantní energie má za následek jinou závislost expanzního faktoru na $a(t)$ na čase. Kvalitativní rozdíl můžeme demonstrovat na nejjednodušším modelu s $k = 0$ i $\Lambda = 0$. Friedmannova rovnice (1.2.3) se potom zjednoduší na

$$\left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 \propto \varrho a^2.$$

Pro prach po dosazení z (1.4.3) s počáteční podmínkou $a(t = 0 = 0$ vychází

$$\frac{\mathrm{d}a}{\mathrm{d}t} \propto \frac{1}{a^{1/2}} \qquad \Longrightarrow a \propto t^{2/3}; \tag{1.4.6}$$

podobně pro záření podle (1.4.4)

$$\frac{\mathrm{d}a}{\mathrm{d}t} \propto \frac{1}{a} \qquad \Longrightarrow \qquad a \propto t^{1/2} \tag{1.4.7}$$

a pro vakuum v souladu s (1.4.5)

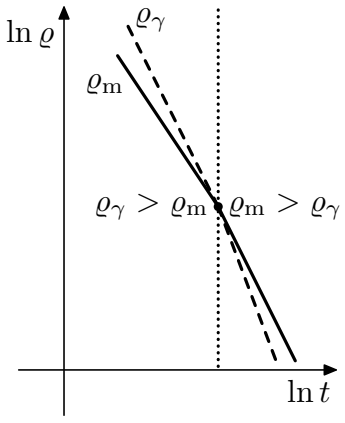
$$\frac{\mathrm{d}a}{\mathrm{d}t} \propto a \qquad \Longrightarrow \qquad a \propto \exp\left(Ht\right), \tag{1.4.8}$$

kde H je Hubbleův parametr definovaný vztahem (1.5.2), v tomto případě je konstantní. Exponenciální rozpínání způsobené energií vakua nazýváme *inflací*. Ve skutečném vesmíru se uplatňují všechny zmíněné složky, ale v různých fázích vývoje různou měrou. Na počátku vývoje prošel fází dominantního záření, nyní dominuje prach a v daleké budoucnosti bude pravděpodobně rozhodující energie vakua. Přechod mezi érami dominantního záření a dominantního prachu pro model s $k = 0$ a $\Lambda = 0$ je znázorněn na obr. 1.8.

Inflací rozumíme rychlé a obrovské rozpínání vesmíru způsobené energií vakua.

Shrnutí

Vesmír je naplněn různými typy energie, z nichž nejvýznamnější vliv na jeho expanzi mají chladná hmota (prach), záření a energie vakua. Jejich vzájemné zastoupení se s časem mění; v dávné minulosti prošel vesmír érou dominantního záření, nyní se nachází ve stavu dominantního prachu a ve vzdálené budoucnosti pravděpodobně bude dominovat energie vakua. Předpokládá se, že energie vakua dominovala i v krátkém časovém intervalu (řádově $t = 10^{-34}$ s po velkém třesku). Tuto fázi označujeme jako inflace a vesmír se během ní exponenciálně zvětšil.



Obr. 1.8: Éry dominantního záření a prachu

Pojmy k zapamatování

- quintessence
- inflace

Kontrolní otázky

1. *Co se kromě rozpínání vesmíru podílí na změně energie záření?*
2. *Jaké typy energie dominovaly v různých fázích vývoje vesmíru?*
3. *K čemu dochází ve fázi vývoje zvané inflace?*

Úkoly k textu

1. Dokažte, že pokud ve vesmíru dominuje energie popsaná obecnou stavovou rovnicí (1.4.1), bude při $k = 0$ a $\Lambda = 0$ expanzní faktor záviset na čase podle vztahu
$$a \propto t^{2/(3+3w)}.$$
Ověřte, že rovnice (1.4.6), (1.4.7) i (1.4.8) jsou speciálními případy získané závislosti.

2. Ukažte, že pokud $k = 0$ a rozpínání vesmíru u ovlivňuje pouze prach s hustotou energie $\varrho_{\mathrm{m}} > 0$ a vakuum s hustotou energie $\varrho_{\mathrm{v}} > 0$, potom (viz [1.31])
$$a^{3/2} \propto \sinh\left(\sqrt{6\pi G\varrho_{\mathrm{v}}}t\right).$$

Průvodce studiem

Po odvození základních rovnic můžeme nyní přistoupit k podrobnější diskusi vlastností našich matematických modelů a jejich konfrontaci s výsledky pozorování reálného vesmíru. V následující podkapitole se zaměříme na ústřední pozorovanou skutečnost, která ve své době překvapila i samotného Einsteina: náš vesmír se rozpíná...

1.5 Hubbleův zákon

Označíme-li $\boldsymbol{v}$ rychlost, jíž se od nás vzdaluje galaxie ve vzdálenosti $\boldsymbol{d} = a(t)\boldsymbol{r}$, kde $\boldsymbol{r}$ reprezentuje „comoving“ souřadnice, lze psát

$$\boldsymbol{v} = \frac{\mathrm{d}\boldsymbol{d}}{\mathrm{d}t} = \frac{\mathrm{d}a}{\mathrm{d}t}\,\boldsymbol{r} = \frac{1}{a}\,\frac{\mathrm{d}a}{\mathrm{d}t}\,\boldsymbol{d}$$

neboli

$$\boldsymbol{v} = H\boldsymbol{d}, \tag{1.5.1}$$

kde jsme zavedli časově proměnný parametr

$$H = H(t) = \frac{1}{a}\,\frac{\mathrm{d}a}{\mathrm{d}t}. \tag{1.5.2}$$

Hubbleův zákon: jednoduchý vztah mezi rychlostí a vzdáleností.

Vztah (1.5.1) nazýváme *Hubbleovým zákonem* a parametr $H(t)$ definovaný rovnicí (1.5.2) *Hubbleovým parametrem*. Současná hodnotu parametru $H_0 = H(t_0)$ představuje jeden z důležitých observačních údajů – *Hubbleovu konstantu*[7]. Jednoduchý vztah (1.5.1) vyjadřuje skutečnost, že čím je od nás objekt dále, tím se od nás více vzdaluje a tím je světlo, které od objektu přichází, posunuto k delším vlnovým délkám; vzhledem k proměnnosti Hubbleova parametru $H(t)$ s časem však nejde o přímou úměru. Hubbleův zákon představuje přímý experimentální důkaz o rozpínání našeho vesmíru a poprvé byl ověřen Edwinem Powellem Hubblem v roce 1929 pomocí 100-palcového dalekohledu observatoře na Mt. Wilsonu v USA. Většinou počítáme s hodnotou Hubbleovy konstanty

E. P. Hubble (1889 - 1953)

$$H_0 = 100\,h\,\mathrm{km{\cdot}s^{-1}{\cdot}Mpc,^{-1}} \qquad \text{kde} \qquad h \in 0{,}55 - 0{,}75. \tag{1.5.3}$$

Bezrozměrný parametr h, odrážející neurčitost v současném měření Hubbleovy konstanty, slouží jako „měřítko mapy“ pro kosmologické vzdálenosti, proto bývá výhodné pracovat s poměrnými veličinami, v nichž se vykrátí (Hubbleův parametr (1.5.2), decelerační parametr (1.7.7)). Ze studia anizotropií kosmického mikrovlnného záření vychází hodnota $h = 0{,}71 \pm 0{,}04$ [1.5], k podobným výsledkům konvergují i další nezávislá pozorování [1.12].

Hubbleova konstanta je současnou hodnotou Hubbleova parametru.

I když se Hubbleova konstanta tradičně udává v $\mathrm{km{\cdot}s^{-1}{\cdot}M^{-1}pc}$, v soustavě SI má rozměr $\mathrm{s^{-1}}$. Její převrácenou hodnotu nazýváme *Hubbleovým časem* t_H . V miliardách let (Gyr) vychází

$$t_\mathrm{H} = \frac{1}{H_0} = 9{,}78\,h^{-1}\,\mathrm{Gyr}. \tag{1.5.4}$$

Hubbleův čas představuje hrubý odhad stáří vesmíru – tak dlouho by trval, pokud by se po celou dobu rozpínal rovnoměrně (srovnejte se vztahem (1.7.9)).

Hubbleův čas představuje hrubý odhad stáří vesmíru.

Shrnutí

Rychlost, s jakou se od nás vzdalují galaxie, se zvětšuje s jejich vzdáleností od nás podle Hubbleova zákona (1.5.1). Hubbleův parametr vystupující v této rovnici jako koeficient úměrnosti závisí obecně na čase. Jeho současnou hodnotu nazýváme Hubbleovou konstantou a patří k nejdůležitějším experimentálním údajům o našem vesmíru. Její převrácená hodnota se nazývá Hubbleovým časem a slouží jako hrubý odhad stáří vesmíru.

Pojmy k zapamatování

- Hubbleův zákon
- Hubbleův parametr
- Hubbleova konstanta
- Hubbleův čas

[7] V kosmologii obvykle indexem „0“ značíme současné hodnoty veličin.

Kontrolní otázky

1. *Jaká je podle současných pozorování hodnota Hubbleovy konstanty?*
2. *Za jakých podmínek by stáří vesmíru bylo rovno Hubbleovu času?*

Cvičení

1. Najděte závislost $H = H(t)$ Hubbleova parametru na čase pro éru dominantního záření a dominantního prachu s využitím rovnic (1.4.7) a (1.4.6). Uvažujte nejjednodušší případ plochého vesmíru $k = 0$ bez energie vakua $\Lambda = 0$.

Řešení

1. Z rovnic (1.2.3) a (1.4.3) pro éru dominantního prachu plyne

$$H^2 = \frac{1}{a^2}\left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 \propto \frac{1}{a^3}$$

neboli

$$\sqrt{a}\,\mathrm{d}a \propto \mathrm{d}t.$$

Integrací s počáteční podmínkou $a(t=0) = 0$ pak vychází

$$a^{3/2} \propto t \qquad \Longrightarrow \qquad a \propto t^{2/3}.$$

Označíme-li konstantu úměrnosti K, bude

$$a = Kt^{2/3}, \quad a_0 = Kt^{2/3}, \quad \Longrightarrow \qquad a = a_0\left(\frac{t}{t_0}\right)^{2/3},$$

kde indexem 0 značíme současné hodnoty. Dosazením posledního výrazu do (1.5.2) vychází

$$H = \frac{2}{3t},$$

konkrétně $H_0 = 2/(3t_0)$. Obráceně pak pro stáří takového vesmíru vychází

$$t_0 = \frac{2}{3H_0} = \frac{2}{3}\,t_{\mathrm{H}},$$

kde $t_{\mathrm{H}} = 1/H_0$ je Hubbleův čas.
Pro model s dominantním zářením se výchozí rovnice změní na

$$H^2 = \frac{1}{a^2}\left(\frac{\mathrm{d}a}{\mathrm{d}t}\right)^2 \propto \frac{1}{a^4}$$

resp.

$$a\,\mathrm{d}a \propto \mathrm{d}t.$$

Analogickým způsobem pak odvodíme

$$a = a_0\left(\frac{t}{t_0}\right)^{1/2}, \qquad H = \frac{1}{2t}.$$

Průvodce studiem

V části 1.4 jsme viděli, že hustota energie záření při expanzi vesmíru klesá rychleji než hustota prachu a tudíž i rychleji, než by odpovídalo pouhému zvětšení objemu. Proč tomu tak je? V následující podkapitole odhalíme příčinu: při rozpínání vesmíru se mění vlnová délka (a tím samozřejmě i frekvence) světelných signálů. V kombinaci s výše popsaným Hubbleovým zákonem to znamená, že čím je pozorovaná galaxie od nás dále, tím je změna vlnové délky větší. Připomeňme, že pozorování galaxií je zároveň výletem do jejich minulosti, neboť na překonání vzdálenosti od nich k nám potřebuje světlo jistý čas (viz část 1.9).

1.6 Šíření světla ve Friedmannových modelech

Při popisu šíření světelných signálů musíme vzít v úvahu geometrii vesmíru charakterizovanou metrickým tenzorem. Studujme pro jednoduchost radiální šíření světelných signálů v Robertsonově-Walkerově prostoročase (1.3.1). Světlo se podle obecné teorie relativity šíří po nulových geodetických čarách, pro něž platí $\mathrm{d}s^2 = 0$, pro čistě radiální pohyb ze zdroje o souřadnici $r = r_\mathrm{e}$ k pozorovateli o souřadnici $r = r_0$ jsou navíc ϑ i φ konstantní, tj. $\mathrm{d}\vartheta = \mathrm{d}\varphi = 0$. Dosazením do (1.3.1) získáme

Pro šíření světelných signálů položíme v (1.3.1) $\mathrm{d}s = 0$.

$$\frac{c\mathrm{d}t}{a(t)} = \pm\frac{\mathrm{d}r}{\sqrt{1-kr^2}},$$

kde kladné resp záporné znaménko odpovídá fotonům šířícím se ve směru rostoucího resp. klesajícího r. Po integraci dostáváme

$$\int_{t_\mathrm{e}}^{t_0}\frac{c\mathrm{d}t}{a(t)} = \pm\int_{r_\mathrm{e}}^{r_0}\frac{\mathrm{d}r}{\sqrt{1-kr^2}}. \tag{1.6.1}$$

Označíme-li periody v místě vyslání a zachycení signálu po řadě T_e a T_0 a jim odpovídající vlnové délky $\lambda_\mathrm{e} = cT_\mathrm{e}$ a $\lambda_0 = cT_0$, bude pro signál emitovaný v čase $t_\mathrm{e} + T_\mathrm{e}$ analogicky platit

$$\int_{t_\mathrm{e}+T_\mathrm{e}}^{t_0+T_0}\frac{c\mathrm{d}t}{a(t)} = \pm\int_{r_\mathrm{e}}^{r_0}\frac{\mathrm{d}r}{\sqrt{1-kr^2}}. \tag{1.6.2}$$

Vzhledem k tomu, že r je „comoving“ souřadnicí, která se nemění s časem, budou na čase nezávislé pravé strany rovnic (1.6.1) a (1.6.2), musí být proto rovny i jejich levé strany

$$\int_{t_\mathrm{e}+T_\mathrm{e}}^{t_0+T_0}\frac{c\mathrm{d}t}{a(t)} = \int_{t_\mathrm{e}}^{t_0}\frac{c\mathrm{d}t}{a(t)}.$$

S využitím vlastností mezí určitých integrálů po úpravě dostáváme

$$\int_{t_\mathrm{e}+T_\mathrm{e}}^{t_\mathrm{e}}\frac{c\mathrm{d}t}{a(t)} + \int_{t_\mathrm{e}}^{t_0}\frac{c\mathrm{d}t}{a(t)} + \int_{t_0}^{t_0+T_0}\frac{c\mathrm{d}t}{a(t)} = \int_{t_\mathrm{e}}^{t_0}\frac{c\mathrm{d}t}{a(t)},$$

$$\int_{t_0}^{t_0+T_0} \frac{c\mathrm{d}t}{a(t)} = \int_{t_\mathrm{e}}^{t_\mathrm{e}+T_\mathrm{e}} \frac{c\mathrm{d}t}{a(t)}.$$

V malých časových intervalech odpovídajících periodě světelných vln T_e a T_0 lze pokládat expanzní faktor $a(t)$ za konstantní, tudíž

Vlnová délka λ je úměrná expanznímu faktoru a.

$$\frac{cT_0}{a(t_0)} = \frac{cT_\mathrm{e}}{a(t_\mathrm{e})}, \qquad \text{neboli} \qquad \frac{\lambda_0}{a(t_0)} = \frac{\lambda_\mathrm{e}}{a(t_\mathrm{e})}.$$

Vlnová délka světla se mění úměrně s expanzním faktorem. Protože $a(t)$ s časem roste, zvětšuje se i vlnová délka směrem k červenému konci spektra. V praxi charakterizujeme změnu vlnové délky nejčastěji tzv. *rudým posuvem* z definovaným vztahem

Změnu vlnové délky vyjadřuje rudý posuv.

$$z = \frac{\lambda_0 - \lambda_\mathrm{e}}{\lambda_\mathrm{e}} \tag{1.6.3}$$

neboli

$$1 + z = \frac{\lambda_0}{\lambda_\mathrm{e}} = \frac{a(t_0)}{a(t_\mathrm{e})}. \tag{1.6.4}$$

Příklady spekter galaxií s různými rudými posuvy jsou na obr. 1.9.

Naměření rudého posuvu vzdálených galaxií je přímým důkazem rozpínání našeho vesmíru. Např. signál, pro který naměříme $z = 1$, byl vyslán v čase t_e, kdy $a(t_\mathrm{e}) = a(t_0)/2$, tj. vesmír měl poloviční velikost než dnes. Nejjednodušší vysvětlení rudého posuvu předpokládá, že se vlnová délka světla zvětšuje spolu s vesmírem (obr. 1.10). Nabízí se i vysvětlení, že jde vlastně o dopplerovský posun způsobený vzdalováním zdrojů světla v důsledku rozpínání vesmíru. Odvozený vzorec pro rudý posuv z (1.6.4) je v souladu se vztahem pro Dopplerův posuv ve speciální teorii relativity pouze v prázdném prostoru, prakticky pro dostatečně blízké zdroje ($z = v/c \ll 1$). V zakřiveném prostoročase je korektní zavedení relativní rychlosti zdroje a pozorovatele komplikovanější. Obecně relativistický výpočet v [1.28] dokazuje, že kosmologický rudý posuv lze skutečně interpretovat jako dopplerovský, i když v literatuře není na tuto otázku jednotný názor.

Shrnutí

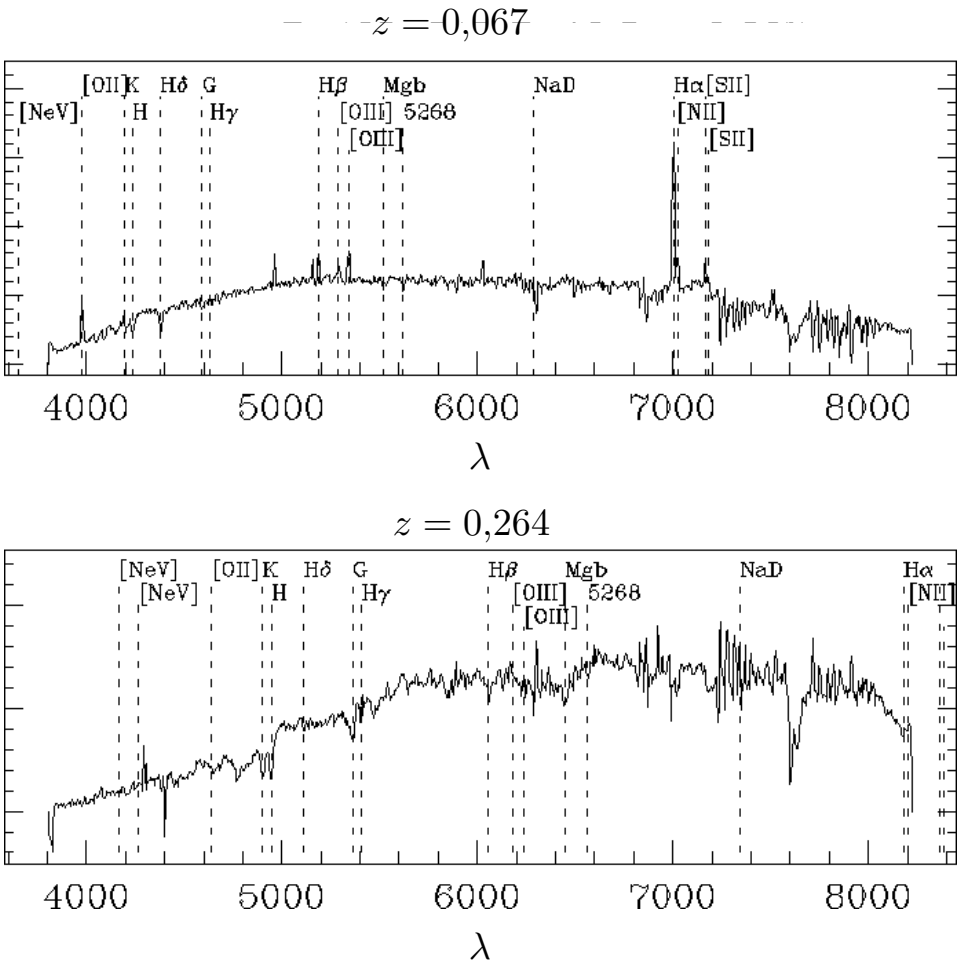
Šíření světla odráží geometrii prostoročasu. V rozpínajícím se homogenním a izotropním vesmíru roste vlnová délka světla úměrně velikosti vesmíru. Mírou změny vlnové délky je rudý posuv spektrálních čar.

Pojmy k zapamatování

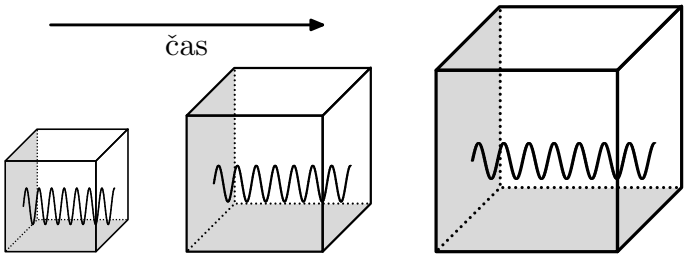
- rudý posuv

Kontrolní otázky

1. *Dokážete na základě definice rudého posuvu vysvětlit modrý posuv?*
2. *Pro které objekty ve vesmíru můžeme naměřit rudý a modrý posuv?*
3. *Jaké je vysvětlení kosmologického rudého posuvu?*



Obr. 1.9: Příklady spekter dvou galaxií s různými rudými posuvy. Vlnová délka je udávána v angströmech, 1 Å = 0,1 nm. Vyznačeny jsou i typické spektrální čáry; všimněme si různé polohy těchto čar jež odráží různý rudý posuv. Svislá osa znázorňuje relativní světelný tok připadající na jednotlivé části spektra. Upraveno podle [1.8].



Obr. 1.10: K vysvětlení rudého posuvu: vlnová délka fotonu se „rozpíná“ s vesmírem jako u fotonu v uzavřené krabici

Cvičení

1. Jaký rudý posuv naměříme u galaxií patřících do kupy galaxií v souhvězdí Panny, vzdalují-li se od nás rychlostí asi $1\,000\,\mathrm{km{\cdot}s^{-1}}$? Rychlost světla je přibližně $300\,000\,\mathrm{km{\cdot}s^{-1}}$ [1.39].

2. Které z emisních čar v následující tabulce můžeme z povrchu Země pozorovat v optickém oboru spektra u kvasaru s následujícím rudým posuvem:
   a) $z = 0{,}1$,
   b) $z = 1$,
   c) $z = 4$.

   Tabulka hlavních emisních čar u aktivních galaxií a kvasarů [1.38]:

L_α	121,6 nm
N V	124,0 nm
C IV	154,9 nm
C III	190,9 nm
Mg II	279,8 nm
O II	372,7 nm
Ne III	386,8 nm
H_δ	410,2 nm
H_γ	434,1 nm

Řešení

1. Pro dané hodnoty $v = 1\,000\,\mathrm{km{\cdot}s^{-1}}$, $c = 300\,000\,\mathrm{km{\cdot}s^{-1}}$, tedy $v/c = 1/300 \approx 0{,}0033 \ll 1$. Rychlost je dostatečně malá, takže můžeme použít přibližný vztah

$$z \approx \frac{v}{c} \approx 0{,}0033.$$

2. Označme $z_a = 0{,}1$, $z_b = 1$ a $z_c = 4$ rudé posuvy. Viditelné světlo má vlnové délky v intervalu $I_0 = \langle 400\,\mathrm{nm}, 780\,\mathrm{nm}\rangle$. Podle (1.6.3) platí

$$z = \frac{\lambda_0}{\lambda_\mathrm{e}} - 1,$$

   kde λ_0 je vlnová délka pozorovaná na zemi a λ_e vlnová délka světla vyzářeného kvazarem. Zřejmě

$$\lambda_\mathrm{e} = \frac{\lambda_0}{1+z}.$$

   Přepočítejme podle posledního vztahu intervaly vlnových délek, v nichž může být při daných rudých posuvech vyzářeno světlo, aby jeho vlnová délka λ_0 na Zemi zapadala do intervalu viditelného světla:
   a) $I_{za} = I_0/(1+z_a) = \langle 363{,}6\,\mathrm{nm}, 709{,}1\,\mathrm{nm}\rangle$,
   b) $I_{zb} = I_0/(1+z_b) = \langle 200{,}0\,\mathrm{nm}, 390{,}0\,\mathrm{nm}\rangle$,
   c) $I_{zc} = I_0/(1+z_c) = \langle 80{,}0\,\mathrm{nm}, 156{,}0\,\mathrm{nm}\rangle$.

   Porovnáním získaných intervalů se zadanou tabulkou zjistíme, že viditelné budou spektrální čáry
   a) O II, Ne III, H_δ a H_γ,
   b) Mg II, O II a Ne III,
   c) L_α, N V a C IV.

Průvodce studiem

Známe již klíčové rovnice (1.2.3)–(1.2.5) a přirozeně se ptáme: jaká byla minulost a jaká může být daleká budoucnost právě našeho jedinečného vesmíru? Zdaleka ne všechny parametry vystupující ve zmíněných rovnicích umíme snadno určit – vždyť už v části 1.5 jsme viděli, že Hubbleova konstanta není známa s velkou přesností. Pro řadu úloh je výhodnější pracovat s bezrozměrnými, tzv. observačními parametry, jejichž hodnoty lze určit přímo z pozorování. Zavedení těchto veličin je věnována následující podkapitola.

1.7 Observační parametry vesmíru

Ze všech Friedmannových modelů je nejjednodušší případ s $k = 0$ a $\Lambda = 0$. Odpovídá mu nekonečný vesmír s eukleidovskou geometrií, který se bude neustále rozpínat. Z Friedmannovy rovnice (1.2.3) pro hustotu vesmíru v tomto modelu dostáváme

Kritická hustota určuje hustotu plochého vesmíru obsahujícího pouze prach.

$$\varrho_{\mathrm{c}} = \frac{3H^2}{8\pi G} \tag{1.7.1}$$

označovanou jako *kritická hustota*. Vzhledem k tomu, že Hubbleův parametr H se mění s časem, není ani hodnota kritické hustoty neměnná. Pro současnou hodnotu (1.5.3) dostáváme

$$\varrho_{\mathrm{c0}} = \frac{3H_0^2}{8\pi G} = 1{,}88\, h^2{\cdot}10^{-26}\,\mathrm{kg{\cdot}m^{-3}} = 2{,}78\, h^{-1}{\cdot}10^{11}\, M_{\otimes}/\left(h^{-1}\mathrm{Mpc}\right). \tag{1.7.2}$$

Vidíme, že ačkoli v běžně užívaných jednotkách jde o hustotu velmi malou, je *průměrná* hustota našeho vesmíru této hodnotě velmi blízká, i když lokálně (např. v našem těle, na Zemi, ve Sluneční soustavě) může být mnohem větší. Galaxie totiž obsahují miliardy hvězd a jejich hmotnost se pohybuje okolo 10^{11}–10^{12} hmotností Slunce $M_{\odot}$ a 1 Mpc je zároveň typickou mezigalaktickou vzdáleností. Jsou i další argumenty, např. *inflační modely*, podle nichž se hustota našeho vesmíru od ϱ_{c0} liší jen velmi málo.

Hustotní parametry udávají poměr hustot vůči ϱ_{c}.

Pro jednotlivé druhy energie (prach, záření i vakuum) můžeme zavést hustotní parametr prachu

$$\Omega_{\mathrm{m}}(t) = \frac{\varrho_{\mathrm{m}}}{\varrho_{\mathrm{c}}}, \tag{1.7.3}$$

záření

$$\Omega_{\gamma}(t) = \frac{\varrho_{\gamma}}{\varrho_{\mathrm{c}}} \tag{1.7.4}$$

nebo vakua

$$\Omega_{\mathrm{v}}(t) = \frac{\varrho_{\mathrm{v}}}{\varrho_{\mathrm{c}}} = \frac{8\pi G\varrho_{\mathrm{v}}}{3H^2} = \frac{\Lambda c^2}{3H^2}. \tag{1.7.5}$$

Protože prach i záření hrají v dynamice kosmologických modelů obdobnou úlohu a jednu z těchto složek považujeme většinou za dominantní (po většinu doby expanze

je to právě prach), budeme jejich součet nadále označovat jako Ω_m. Dosazením do Friedmannovy rovnice (1.2.3) vychází

$$\frac{kc^2}{H^2a^2} = \Omega_\mathrm{m} + \Omega_\mathrm{v} - 1. \tag{1.7.6}$$

Vidíme, že pokud má mít vesmír plochou eukleidovskou geometrii $k = 0$, musí být splněno

$$\Omega_\mathrm{m} + \Omega_\mathrm{v} = 1.$$

Inflace je jednou z možností jak vysvětlit, proč je náš vesmír (téměř) plochý.

Pokud se rozpínání vesmíru zpomaluje, potom se součin $H^2a^2 = (\mathrm{d}a/\mathrm{d}t)^2$ zmenšuje a zlomek na levé straně rovnice (1.7.6) zvětšuje. Je-li odchylka $\Omega_\mathrm{m} + \Omega_\mathrm{v}$ od 1 nyní malá, musela být v minulosti ještě mnohem, mnohem menší, hovoříme o tzv. *problému plochosti vesmíru*: jako to, že je geometrie vesmíru vyladěna tak blízko k eukleidovské? Tato skutečnost je jednou z motivací k předpokladu, že vesmír ve velmi raném stadiu prošel fází tzv. *inflace*, prudkého rozpínání s $H \approx$ konst., kdy se hodnota zlomku zmenšila úměrně $1/a^2$ a vesmír se stal (téměř) plochým. Potvrzuje to i rozbor anizotropií mikrovlnného záření s výsledkem $\Omega_\mathrm{m} + \Omega_\mathrm{v} = 1{,}02 \pm 0{,}02$ [1.5].

Decelerační parametr charakterizuje rozpínání vesmíru na větších vzdálenostech.

Důležitou charakteristikou expanze vesmíru je kromě rychlosti rozpínání, jejíž mírou je Hubbleova konstanta, také „zrychlení“. Až do 90-tých let minulého století se předpokládalo, že expanze se bude vždy zpomalovat, namísto akcelerace bylo proto přirozenější zavést veličinu zvanou *decelerační parametr* q definovaný vztahem

$$q = -\frac{\dfrac{\mathrm{d}^2a}{\mathrm{d}t^2}\, a}{\left(\dfrac{\mathrm{d}a}{\mathrm{d}t}\right)^2}. \tag{1.7.7}$$

Dosazením do (1.2.5) s využitím (1.7.3)–(1.7.5) pak vychází

$$q = \frac{\Omega_\mathrm{m}}{2} - \Omega_\mathrm{v}. \tag{1.7.8}$$

Zřejmě pokud $\Omega_\mathrm{m}/2 - \Omega_\mathrm{v} = 0$, rozpínání probíhá s konstantní rychlostí, pro $q > 0$ se zpomaluje a pro $q < 0$ se zrychluje.

Rozvineme-li vztah pro expanzní faktor $a(t)$ v Taylorovu řadu okolo současného stáří vesmíru $t = t_0$, dostáváme

$$a(t) = a(t_0) + \left.\frac{\mathrm{d}a}{\mathrm{d}t}\right|_{t_0} (t - t_0) + \left.\frac{\mathrm{d}^2a}{\mathrm{d}t^2}\right|_{t_0} (t - t_0)^2 + \dots$$

a pro rudý posuv objektu, od něhož bylo světlo vysláno z čase t podle (1.6.4) vychází

$$\frac{1}{1+z} = \frac{a(t)}{a(t_0)} = 1 + H_0\,(t - t_0) - \frac{q_0}{2} H_0^2\,(t - t_0)^2 + \dots,$$

kde $H_0 = H(t_0)$, $q_0 = q(t_0)$ představují současné hodnoty Hubbleova a deceleračního parametru.

Z Friedmannovy rovnice (1.7.6) pak lze vyjádřit současnou hodnotu expanzního faktoru

$$a_0 = \frac{c}{H_0}\sqrt{\frac{k}{\Omega_{\mathrm{m0}} + \Omega_{\mathrm{v0}} - 1}}.$$

V případě plochého vesmíru $k = 0$ vychází neurčitý výraz $0/0$, pro který z limitního chování obdržíme tzv. *Hubbleovu délku*

$$d_{\mathrm{H}} = ct_{\mathrm{H}} = \frac{c}{H_0} \approx 2\,998\,h^{-1}\,\mathrm{Mpc}, \tag{1.7.9}$$

Hubbleova délka představuje hrubý odhad velikosti pozorovaného vesmíru.

která odpovídá dráze, kterou urazí světlo za Hubbleův čas (1.5.4) v plochém vesmíru. Přibližně tak charakterizuje velikost pozorovaného vesmíru, tj. oblasti, z níž můžeme zachytit světelné (i jakékoli jiné) signály.

Shrnutí

Kritickou hustotou nazýváme hustotu plochého homogenního vesmíru s nulovou energií vakua. Hustotu všech typů energie pak s výhodou vyjadřujeme poměrem k této kritické hustotě pomocí hustotních parametrů. Spolu s deceleračním parametrem, popisujícím zrychlování resp. zpomalování expanze, představují další důležité měřitelné charakteristiky vesmíru.

Pojmy k zapamatování

- hustotní parametr
- decelerační parametr
- Hubbleova délka

Kontrolní otázky

1. *Jaký vztah musí splňovat hustotní parametry pro plochý vesmír?*
2. *Jak moc se liší celková hustota vesmíru od kritické a jakým procesem to umí moderní kosmologie vysvětlit?*
3. *Jaký je význam deceleračního parametru?*
4. *Jaký má význam Hubbleova délka?*

Cvičení

1. Kolika nukleonům v m^3 odpovídá kritická hustota vesmíru pro hodnotu Hubbleovy konstanty $H_0 = 71\,\mathrm{km{\cdot}s^{-1}{\cdot}Mpc}$ [1.39]?

Úkoly k textu

1. Ukažte, že je-li v nějakém čase $\Omega = \Omega_{\mathrm{m}} + \Omega_{\mathrm{v}} = 1$, potom se Ω s časem nemění.
2. Jaká podmínka musí být splněna, aby hustotní parametr vakua Ω_{v} byl konstantní a nezávisel na čase?
3. Předpokládejme, že v určitém čase je v rovnici (1.7.8) $q = 0$. Co musí být splněno, aby decelerační parametr zůstal nulový?

Řešení

1. Kritickou hustotu určíme ze vztahu (1.7.1) dosazením za příslušné konstanty $H0 = 71\,\mathrm{km{\cdot}s^{-1}{\cdot}Mpc} = 2{,}30{\cdot}10^{-18}\,\mathrm{s^{-1}}$ a $G = 6{,}67{\cdot}10^{-11}\,\mathrm{m^3{\cdot}kg{\cdot}^{-1}s^{2-1}}$. Je-li hmotnost jednoho nukleonu (protonu nebo neutronu) $m_\mathrm{u} \approx 1{,}66{\cdot}10^{-27}\,\mathrm{kg}$ (tzv. hmotnostní atomová jednotka), bude odpovídající počet nukleonů v $\mathrm{m^{3-1}}$

$$n = \frac{3H_0^2}{8\pi G m_\mathrm{u}} \approx 5{,}7.$$

Kritická hustota odpovídá necelým šesti nukleonům v $1\,\mathrm{m^3}$.

Průvodce studiem

Jedna z ústředních otázek kosmologie zní: bude se náš vesmír stále rozpínat nebo se někdy v budoucnu smrští zpět do stavu podobného jako na počátku? Odpověď dávají hodnoty hustotních parametrů, jejichž přesné určení představuje výzvu mnoha experimentálním projektům (Boomerang, 2dF Galaxy Redshift Survey, Sloan Digital Sky Survey, Supernova Cosmology Project, Wilkinson Anisotropy Probe). Konktrétní možnosti vývoje vesmíru v závislosti na obsahu množství hmoty a energie vakua diskutujeme v následující části.

1.8 Budoucnost vesmíru

Moderní kosmologie předpokládá, že vesmír se rozpíná z velmi horkého, superhustého stavu, označovaného jako *velký třesk* nebo anglicky „Big Bang“ Jednou ze zajímavých otázek, které můžeme zkoumat je, zda rozpínání vesmíru bude trvat věčně nebo zda se zastaví, vesmír dosáhne maximálního rozměru a poté se začne znovu smršťovat a skončí „*velkým křachem*“ (anglicky „Big Crunch“). Různé případy, jež mohou nastat, přehledně znázorňujeme v rovině Ω_m a Ω_v (záření, které dominovalo krátkou dobu na počátku vesmíru neuvažujeme). Rozpínání se zřejmě zastaví, pokud $\mathrm{d}^2a/\mathrm{d}t^2 < 0$ (neboli $q > 0$) a tato podmínka zůstává splněna, dokud $\mathrm{d}a/\mathrm{d}t = 0$ (resp. $H = 0$). Podle (1.7.8) tato situace vždy nastane pro $\Omega_\mathrm{v} < 0$, neboť potom

$$q = \frac{\Omega_\mathrm{m}}{2} - \Omega_\mathrm{v} > 0$$

a ve Friedmannově rovnici (1.7.6) lze nalézt a, pro něž $H = 0$.

Je-li $\Omega_\mathrm{v} < 0$, expanze se jednou změní ve smršťování.

Jestliže $\Omega_\mathrm{m} \leqq 1$, potom se rozpínání zastaví pro $\Omega_\mathrm{v} < 0$, ale nikoli pro $\Omega_\mathrm{v} = 0$. Protože kladná hodnota Ω_v zvětšuje jak $\mathrm{d}^2a/\mathrm{d}t^2$, tak $\mathrm{d}a/\mathrm{d}t$, vidíme, že v tomto případě se rozpínání ve smršťování také nezmění.

Konečně při $\Omega_\mathrm{m} \geqq 1$ také existuje maximální hodnota Ω_v, při které se rozpínání ještě zastaví a přejde v kontrakci (viz obr. 1.11). V tomto limitním případě dospěje vesmír do stavu, kdy $q = 0$ i $H = 0$, který odpovídá tzv. *Einsteinovu statickému*

vesmíru[8] (v němž by tyto podmínky platily po celou dobu). Úpravou Friedmanovy rovnice (1.7.6) se započtením závislostí hustoty energie prachu na expanzním faktoru (1.4.3)–(1.4.5) lze psát

Při $\Omega_\mathrm{v} > 0$ je teoretických možností více, dokonce i nerozpínající se Einsteinův statický vesmír.

$$H^2 = H_0^2\Omega_{\mathrm{m}0}\,\frac{a_0^3}{a^3} + H_0^2\Omega_{\mathrm{v}0} - \frac{kc^2}{a^2}.$$

Z této rovnice lze pro $t = t_0$ vyjádřit

$$kc^2 = H_0^2 a_0^2\,(\Omega_{\mathrm{m}0} + \Omega_{\mathrm{v}0} - 1)$$

a dosadit zpět, čímž dostaneme

$$\frac{H^2}{H_0^2} = \Omega_{\mathrm{m}0}\left(\frac{a_0^3}{a^3} - \frac{a_0^2}{a^2}\right) + \Omega_{\mathrm{v}0}\left(1 - \frac{a_0^2}{a^2}\right) + \frac{a_0^2}{a^2} = 0. \tag{1.8.1}$$

Podobně podmínka $q = 0$ podle (1.7.8) dává

$$\Omega_{\mathrm{v}0} = 4\Omega_{\mathrm{m}0}\left(\frac{a_0}{2a}\right)^3.$$

Dosazením do (1.8.1) a zavedením substituce $a = a_0/(2x)$ dospějeme ke kubické rovnici

$$4x^3 - 3x + 1 - \frac{1}{\Omega_{\mathrm{m}0}} = 0. \tag{1.8.2}$$

Podle definice $x < 1$, rovnici proto lze řešit pomocí goniometrické substituce $x = \cos\beta$. S využitím vzorce (viz např. [1.35])

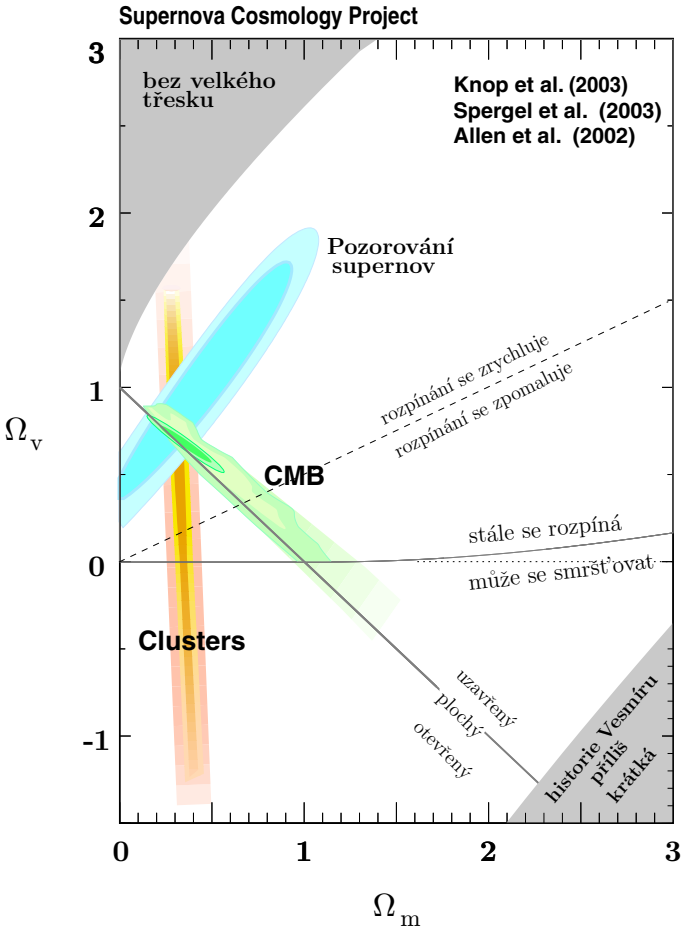
$$\cos 3\beta = 4\cos^3\beta - 3\cos\beta$$

obdržíme z (1.8.2) postupně

$$\begin{aligned}
\cos 3\beta &= -\left(1 - \frac{1}{\Omega_{\mathrm{m}0}}\right),\\
\cos(3\beta - \pi) &= 1 - \frac{1}{\Omega_{\mathrm{m}0}},\\
x &= \cos\left[\frac{1}{3}\arccos\left(1 - \frac{1}{\Omega_{\mathrm{m}0}}\right) + \frac{\pi}{3}\right],\\
\Omega_{\mathrm{v}0} &= 4\Omega_{\mathrm{m}0}x^3 = 4\Omega_{\mathrm{m}0}\cos^3\left[\frac{1}{3}\arccos\left(1 - \frac{1}{\Omega_{\mathrm{m}0}}\right) + \frac{\pi}{3}\right].
\end{aligned} \tag{1.8.3}$$

Poslední závislost (ve zvětšeném měřítku) je také vykreslena na 1.11. Podrobnější rozbor této problematiky lze nalézt např. v [1.11].

[8] Kosmologická konstanta Λ byla Einsteinem zavedena právě proto, aby získal statický, nerozpínající se model vesmíru. Po Hubbleových pozorováních, která rozpínání vesmíru prokázala, označil Einstein zavedení Λ jako jeden ze svých největších omylů, dnes se však zdá být omylem velmi inspirujícím...



Obr. 1.11: Znázornění výsledků tří různých nezávislých měření v rovině parametrů Ω_{m0} a Ω_{v0}: pozorování vzdálených supernov [1.20], kosmického mikrovlnného záření (CMB) [1.37] a studia rozložení hmoty ve skupinách galaxií [1.1]. Vidíme, že pozorování konvergují k hodnotám $\Omega_{m0} = 0{,}3$ a $\Omega_{v0} = 0{,}7$. Upraveno podle [1.33].

Shrnutí

Budoucnost vesmíru – věčné rozpínání versus budoucí smršťování, zrychlování versus zpomalování expanze – lze jednoznačně předpovědět v závislosti na hodnotách hustotních parametrů hmoty a vakua. Pro jejich současné nejpravděpodobnější hodnoty se vesmír bude stále rychleji rozpínat.

Pojmy k zapamatování

- velký třesk
- velký křach
- Einsteinův statický vesmír

Kontrolní otázky

1. *Jaké jsou nejpravděpodobnější hodnoty hustotních parametrů Ω_{m0} a Ω_{v0}?*
2. *Co z těchto hodnot plyne pro budoucnost Vesmíru?*

Úkoly k textu

1. Ověřte, že pokud $\Omega_{m0} = 54/28$, potom z rovnice (1.8.2) vychází $\Omega_{v0}/\Omega_{m0} = 1/54$.

2. Ukažte, že pokud $\Omega_{\mathrm{m0}} - 1 \ll 1$, potom aproximací rovnice (1.8.3) získáme

$$\Omega_{\mathrm{v0}} = \frac{4\Omega_{\mathrm{m0}}}{27}\left(1 - \frac{1}{\Omega_{\mathrm{m0}}}\right)^3,$$

tj. stejný výsledek, jako kdybychom v rovnici (1.8.2) zanedbali kubický člen.

Průvodce studiem

Již v souvislosti s rudým posuvem jsme připomínali, že pozorování vesmíru je cestou do minulosti. Zejména u velmi vzdálených objektů je důležité určit dobu, kterou jejich světlo potřebovalo k uražení vzdálenosti k nám. Pozorujeme-li dnes objekty, jejichž světlo bylo vyzářeno před 10 a více miliardami let (viz obr. 1.5), získáváme konkrétnější představu o formování galaxií, formování prvních hvězd apod. Díky rozpínání vesmíru a možné křivosti jeho geometrie však určování časů a vzdáleností není jednoduché. Nejpraktičtější je najít jejich vztah k experimentálně dobře definovaným veličinám: rudému posuvu z a hustotním parametrům.

1.9 Stáří pozorovaných objektů

V této části odvodíme vztah mezi rudým posuvem z světla vyslaného vzdálenou galaxií a časem t, který světelný signál potřeboval k překonání vzdálenosti k nám. Určování vzdálenosti pozorovaných objektů se pak budeme věnovat v následující podkapitole 1.10. Obě veličiny musí odrážet geometrii vesmíru a nutně proto závisejí na hustotě hmoty Ω_{m} (prachu popř. záření) i hustotě vakuové energie Ω_v.

Vyjdeme ze zavedení Hubbleova parametru (1.5.2), jež přepíšeme do tvaru

Vyjádříme změnu času v závislosti na expanzním faktoru...

$$\mathrm{d}t = \frac{1}{H}\,\frac{\mathrm{d}a}{a}. \tag{1.9.1}$$

Ze vztahu (1.8.1) dále plyne

$$H = H_0\sqrt{\Omega_{\mathrm{m0}}\left(\frac{a_0^3}{a^3} - \frac{a_0^2}{a^2}\right) + \Omega_{\mathrm{v0}}\left(1 - \frac{a_0^2}{a^2}\right) + \frac{a_0^2}{a^2}}$$

a z definice rudého posuvu (1.6.4) také

...a expanzní faktor v závislosti na rudém posuvu.

$$a = \frac{a_0}{1+z}, \qquad \mathrm{d}a = -\frac{a_0}{(1+z)^2}\,\mathrm{d}z,$$

kde a_0 značí současnou hodnotu expanzního faktoru. Označíme-li rudý posuv pozorované galaxie z_{e} a expanzní faktor v čase vyslání světla a_{e}, po dosazení do (1.9.1)

obdržíme [1.7]

$$\Delta t = t_0 - t_\mathrm{e} = \frac{1}{H_0}\int\limits_{a_\mathrm{e}}^{a_0} \frac{\mathrm{d}a}{a\sqrt{\Omega_{\mathrm{m}0}\left(\frac{a_0^3}{a^3}-\frac{a_0^2}{a^2}\right)+\Omega_{\mathrm{v}0}\left(1-\frac{a_0^2}{a^2}\right)+\frac{a_0^2}{a^2}}} = \tag{1.9.2}$$

$$= \frac{1}{H_0}\int\limits_{0}^{z_\mathrm{e}} \frac{\mathrm{d}z}{(1+z)\sqrt{\Omega_{\mathrm{m}0}(1+z)^3+\Omega_{\mathrm{v}0}+(1-\Omega_{\mathrm{m}0}-\Omega_{\mathrm{v}0})(1+z)^2}}.$$

Pokud bychom započítali i hustotu záření, která klesá s a podle vztahu (1.4.4) a je popsána hustotním faktorem Ω_γ, analogickými úvahami odvodíme

$$\Delta t = \frac{1}{H_0}\int\limits_{0}^{z_\mathrm{e}} \frac{\mathrm{d}z}{(1+z)\sqrt{\Omega_{\mathrm{m}0}(1+z)^3+\Omega_{\gamma 0}(1+z)^4+\Omega_{\mathrm{v}0}+(1-\Omega_0)(1+z)^2}}, \tag{1.9.3}$$

kde jsme označili $\Omega_0 = \Omega_{\mathrm{m}0} + \Omega_{\gamma 0} + \Omega_{\mathrm{v}0}$ současnou hodnotu celkového hustotního faktoru zahrnujícího všechny formy energie [1.30].

Protože $1+z>0$, bude $\Omega_{\mathrm{m}0}(1+z)^3 > \Omega_{\mathrm{m}0}(1+z)^2$ a $\Omega_{\mathrm{v}0} < \Omega_{\mathrm{v}0}(1+z)^2$, větší $\Omega_{\mathrm{m}0}$ vede ke zkrácení Δt, naopak větší kladné $\Omega_{\mathrm{v}0}$ má za následek větší Δt. Kvalitativně tak můžeme posoudit vliv jednotlivých forem energie na stáří samotného vesmíru, jež je extrapolací uvedeného vztahu. Numerický model vývoje expanzního faktoru v závislosti na čase pro plochý vesmír (tj. $\Omega_0 = 1$) je znázorněn na obr. 1.12.

Shrnutí

Čas, za který k nám doputovalo světlo ze vzdálených objektů, stejně jako stáří samotného vesmíru závisejí na zastoupení jednotlivých forem energie.

Kontrolní otázky

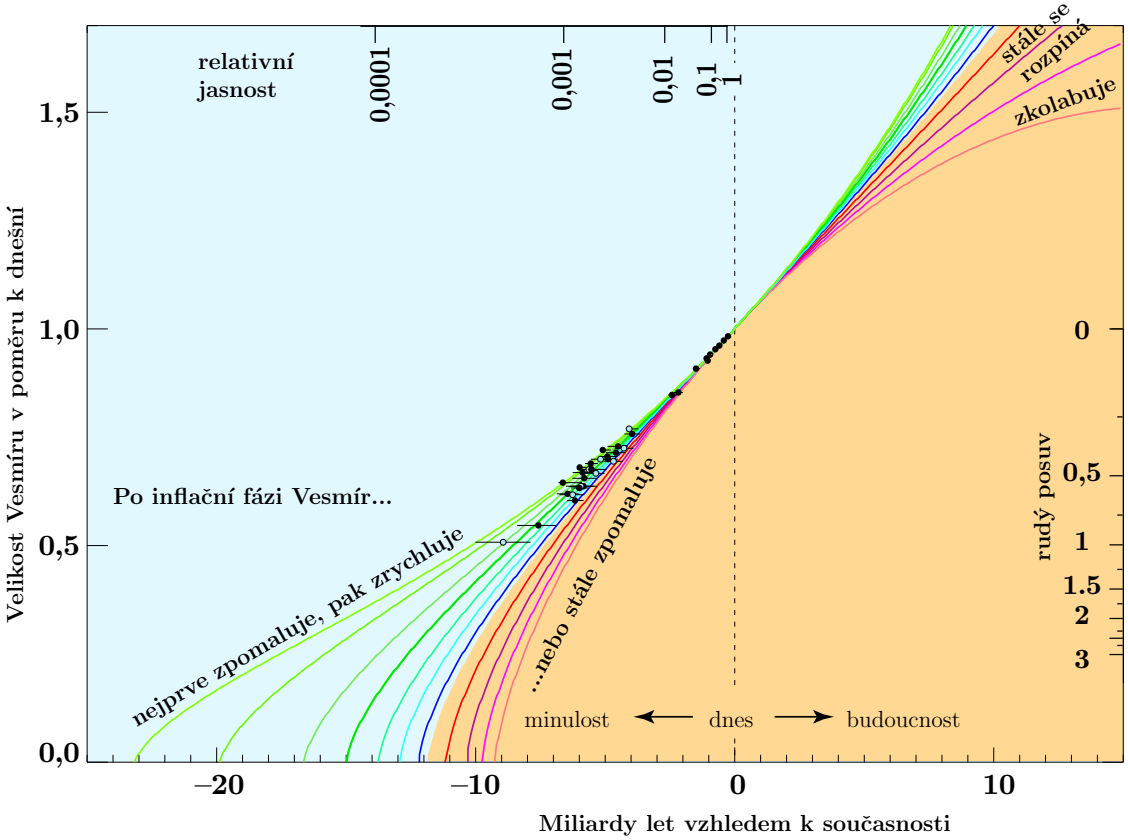
1. *Jaký má vliv přítomnost hmoty na stáří vesmíru?*
2. *Jak může stáří vesmíru ovlivnit energie kosmologická konstanta?*

Cvičení

1. Ukažte, že pokud by vesmír obsahoval pouze energii vakua $0 < \Omega_{\mathrm{v}0} < 1$, potom z rovnice (1.9.2) s počáteční podmínkou $a(t=0)=0$ získáme rovnici

$$a = a_0\sqrt{\frac{1-\Omega_{\mathrm{v}0}}{\Omega_{\mathrm{v}0}}}\,\sinh\left(\sqrt{\Omega_{\mathrm{v}0}}H_0 t\right).$$

   Vyšetřete limitní případy $\Omega_{\mathrm{v}0}\to 0$ a $\Omega_{\mathrm{v}0}\to 1$.



Obr. 1.12: Rekonstrukce a možné předpovědi rozpínání (popř. budoucího smršťování) vesmíru z výsledků měření vzdálených supernov (data znázorněná černými body) pro plochý vesmír s eukleidovskou geometrií. Současná hodnota expanzního faktoru je přeškálována na hodnotu $a_0 = 1$, takže $a = 1/(1+z)$. Křivky v oblasti s modrým pozadím představují modely, u nichž převáží vliv kosmologické konstanty a rozpínání se bude zrychlovat. Křivky v oblasti se žlutým pozadím odpovídají modelům, u nichž se rozpínání bude zpomalovat, u posledních dvou modelů nakonec dojde ke zpětnému smršťování. Upraveno podle [1.33].

Řešení

1. Z rovnice (1.9.2) při $\Omega_{\mathrm{m}0} = 0$ plyne

$$H_0 \,\mathrm{d}t = \frac{\mathrm{d}a}{a\sqrt{\Omega_{\mathrm{v}0}\left(1 - \dfrac{a_0^2}{a^2}\right) + \dfrac{a_0^2}{a^2}}}$$

nebo – zavedeme-li proměnnou $u = a/a_0$

$$H_0 \,\mathrm{d}t = \frac{\mathrm{d}u}{\sqrt{1 - \Omega_{\mathrm{v}0} + \Omega_{\mathrm{v}0} u^2}}.$$

Vzhledem k počátečním podmínkám v zadání úlohy můžeme psát

$$\int_0^t H_0 \,\mathrm{d}t = \int_0^u \frac{\mathrm{d}u}{\sqrt{1 - \Omega_{\mathrm{v}0} + \Omega_{\mathrm{v}0} u^2}},$$

což vede k výsledku

$$H_0\, t = \frac{1}{\sqrt{\Omega_{\mathrm{v}0}}}\ \mathrm{argsinh}\left(\frac{\sqrt{\Omega_{\mathrm{v}0}}\, u}{\sqrt{1-\Omega_{\mathrm{v}0}}}\right) = \frac{1}{\sqrt{\Omega_{\mathrm{v}0}}}\ \mathrm{argsinh}\left(\frac{\sqrt{\Omega_{\mathrm{v}0}}}{\sqrt{1-\Omega_{\mathrm{v}0}}}\,\frac{a}{a_0}\right).$$

Obrácená závislost potom má tvar ze zadání úlohy

$$a = a_0 \sqrt{\frac{1-\Omega_{\mathrm{v}0}}{\Omega_{\mathrm{v}0}}}\ \sinh\left(\sqrt{\Omega_{\mathrm{v}0}} H_0 t\right).$$

Zřejmě pokud $\Omega_{\mathrm{v}0} \to 0$,

$$\sinh\left(\sqrt{\Omega_{\mathrm{v}0}} H_0 t\right) \approx \sqrt{\Omega_{\mathrm{v}0}} H_0 t$$

a $a \to a_0 H_0 t$, naopak pokud $\Omega_{\mathrm{v}0} \to 1$, potom

$$t \propto \mathrm{argsinh}\left(\frac{\sqrt{\Omega_{\mathrm{v}0}}}{\sqrt{1-\Omega_{\mathrm{v}0}}}\,\frac{a}{a_0}\right) \to \infty.$$

Takový model vesmíru by existoval nekonečně dlouho a nezačínal by velkým třeskem (viz levá horní část obr. 1.11).

Průvodce studiem

Pracujeme-li v astronomii s jednotkou světelný rok (1 ly), chápeme ji jako vzdálenost uraženou světlem ve vakuu za jeden rok. Na první pohled by mělo stačit vynásobit pravou stranu rovnice (1.9.3) rychlostí světla ve vakuu c a zjistili bychom vzdálenost objektu s příslušným rudým posuvem. Jenže přesně vzato tak jednoduché to není! Protože náš vesmír nemá geometrii příliš odlišnou od Euklidovy, pro bližší galaxie a přibližně to sice platí a někdy je dokonce takový odhad i postačující. Chceme-li však studovat Hubbleovy diagramy a zkoumat, jakým hustotním parametrům odpovídají, musíme se tímto problémem zabývat detailněji.

1.10 Fotometrická vzdálenost a Hubbleovy diagramy

Hubbleovy diagramy znázorňují závislost vzdálenosti pozorovaného objektu, resp. jeho hvězdné velikosti, na rudém posuvu z a poskytují detailnější obraz vlastností vesmíru na velkých vzdálenostech. Zpočátku, ve 30-ých letech 20. století přesně odpovídaly Hubbleovu zákonu (1.5.1) s konstantním Hubbleovým parametrem H. Novější data získaná např. v rámci „Supernova cosmology project“ [1.20, 1.33] zahrnují pozorování mnohem vzdálenějších objektů a ukazují, že rozpínání vesmíru se skutečně s časem mění.

Rychlost, z jakou se od nás vzdalují daleké galaxie určujeme z rudého posuvu spektrálních čar (viz část 1.6). Zatímco rudý posuv je možné změřit s poměrně vysokou přesností, mezigalaktické vzdálenosti musíme určovat nepřímo. Nejčastěji se využívá fotometrických zákonů: skutečnosti, že intenzita osvětlení (obecně ozáření) nějaké plochy klesá se čtvercem její vzdálenosti od zdroje. Pokud bychom znali svítivost vzdáleného zdroje, potom bychom změřením světelného výkonu dopadajícího do našich měřicích přístrojů mohli určit jeho vzdálenost. K takovým měřením se používají tzv. *standardní svíčky* („standard candles“), tj. objekty, jejichž absolutní svítivost určujeme z jiných, nezávislých fyzikálních vlastností (viz obr. 1.13). Vlivem rozpínání vesmíru a možnému zakřivení jeho geometrie se takto určená, tzv. *fotometrická vzdálenost*, liší od pouhého součinu $c\Delta t$, kde Δt je dáno vztahem (1.9.3) nalezeným v předcházející podkapitole 1.9.

Standardní svíčky jsou „kalibrované“ zdroje, u nichž známe (nebo předpokládáme) jejich skutečný zářivý výkon.

V praxi nejčastěji měříme fotometrickou vzdálenost.

Pro šíření signálu z (1.6.1) získáváme [1.15, 1.30]

$$\int_{t_\mathrm{e}}^{t_0} \frac{c\mathrm{d}t}{a(t)} = \int_0^{r_\mathrm{e}} \frac{\mathrm{d}r}{\sqrt{1-kr^2}} = \chi. \tag{1.10.1}$$

Analogickými úvahami jako při odvození (1.9.3) vypočítáme integrál na levé straně

$$\chi = \frac{c}{a_0 H_0} \int_0^{z_\mathrm{e}} \frac{\mathrm{d}z}{\sqrt{\Omega_{\mathrm{m}0}\,(1+z)^3 + \Omega_{\gamma 0}\,(1+z)^4 + \Omega_{\mathrm{v}0} + (1-\Omega_0)\,(1+z)^2}} \tag{1.10.2}$$

Integrál na pravé straně (1.10.1) dává různé výsledky pro různé hodnoty k, což odráží vliv geometrie vesmíru na šíření světelných signálů [1.15, 1.19]

$$\begin{array}{ll} r_\mathrm{e} = \sin\chi & \text{pro } k = 1, \\ r_\mathrm{e} = \chi & \text{pro } k = 0, \\ r_\mathrm{e} = \sinh\chi & \text{pro } k = -1. \end{array} \tag{1.10.3}$$

Označíme-li L absolutní svítivost zdroje (celkový vyzářený výkon) a $\mathcal{F}$ jeho zdánlivou svítivost (zářivý tok, tj. výkon záření dopadající v místě pozorovatele na jednotkovou plochu kolmou na směr šíření záření), potom v plochém prostoru pro fotometrickou vzdálenost d_L platí [1.15, 1.17]

$$\mathcal{F} = \frac{L}{4\pi d_\mathrm{L}^2} \tag{1.10.4}$$

Zavedení fotometrické vzdálenosti odráží pokles zářivého toku se čtvercem vzdálenosti od zdroje.

Nachází-li se zdroj v místě s „comoving“ souřadnicí r_e a vyšle signál v čase t_e, dopadne světlo v současnosti (tj. v čase t_0) na plochu

$$S = 4\pi a_0^2 r_\mathrm{e}^2;$$

r_e je přitom obecně dáno vztahy (1.10.3). V důsledku kosmologického rudého posuvu (1.6.4) však bude energie každého fotonu namísto hc/λ_e rovna $hc/\lambda_0 = hc/[\lambda_\mathrm{e}\,(1+z)]$. Díky poklesu frekvence záření fotony vyzářené v intervalu Δt_e dopadnou do místa pozorování v intervalu

$$\Delta t_0 = \Delta t_\mathrm{e}\,(1+z)$$

Obr. 1.13: Supernova 1994Dna okraji galaxie NGC 4526 je příkladem supernovy typu Ia, jejichž kulminační jasnost převýší svítivost celého jádra galaxie; proto lze supernovy pozorovat i ve velkých vzdálenostech. V tomto případě se z kosmologického hlediska díváme „za humna“ přibližně 20 Mpc. Supernovy typu Ia jsou příkladem standardních svíček, u nichž byla empiricky zjištěna závislost mezi kulminační svítivostí a dobou poklesu jasnosti [1.33].

Pro zářivý tok v místě pozorování pak vychází

$$\mathcal{F} = \frac{L}{4\pi a_0^2 r_\mathrm{e}^2 \left(1+z\right)^2}$$

a srovnáním s (1.10.4) pro fotometrickou vzdálenost odvodíme

$$d_\mathrm{L} = r_\mathrm{e} a_0 \left(1+z\right), \tag{1.10.5}$$

Fotometrická vzdálenost závisí na současné velikosti vesmíru a rudém posuvu pozorované galaxie.

kde za r_e opět musíme dosadit z (1.10.3) a (1.10.2).

Pro malé rudé posuvy přibližně do hodnoty $z \approx 0{,}4$ vystačíme s užitečnou aproximací. Rozvineme-li expanzní faktor $a(t)$ v Taylorovu řadu v okolí současné hodnoty

$a(t_0)$

$$a(t) \approx a(t_0) + \left.\frac{\mathrm{d}a}{\mathrm{d}t}\right|_0 (t - t_0) + \left.\frac{\mathrm{d}^2 a}{\mathrm{d}t^2}\right|_0 (t - t_0)^2 + \ldots$$

a dosadíme podle (1.5.2) a (1.7.7)

$$a(t) \approx a(t_0) \left[1 + H_0 (t - t_0) - \frac{1}{2} q_0 H_0^2 (t - t_0)^2 + \ldots\right]$$

S použitím (1.10.5) pak dospějeme ke vztahům [1.17]

$$d_\mathrm{L} = \frac{c}{H_0} \left[z + \frac{1}{2} (1 - q_0) z^2 + \ldots\right]$$

respektive

$$z = \frac{H_0}{c} \left[d_\mathrm{L} + \frac{1}{2} (1 + q_0) \frac{H_0}{c} d_\mathrm{L}^2 + \ldots\right].$$

U členů vyšších řádů se již projevuje zakřivení geometrie a situace je mnohem komplikovanější [1.17]. Pro malé $z \approx v/c$ pak v 1. přiblížení dostáváme Hubbleův zákon (1.5.1). Dodejme, že Edwin Hubble při svých měřeních z roku 1929 pozoroval galaxie se $z \approx 0{,}003$.

V praktické astronomii se častěji užívají historicky zavedené magnitudy.

Při samotných pozorováních pracujeme obvykle namísto fotometrické vzdálenosti s historicky zavedenými hvězdnými velikostmi neboli *magnitudami*, i když v případě kosmologie nejde o pozorování hvězd, nýbrž galaxií. Magnitudy byly zavedeny již ve starověku Ptolemaiem a Hipparchem a odrážejí zkušenost, že naše fyziologické vjemy jsou úměrné logaritmu intenzity podnětu (dnes se však už pouze na lidské smysly zdaleka nespoléháme). *Absolutní hvězdná velikost (magnituda)* M je definována vztahem

$$M = -2{,}5 \log_{10} \left(\frac{L}{L_\odot}\right) + 4{,}74, \tag{1.10.6}$$

kde $L_\odot = 3{,}85{\cdot}10^{26}\,\mathrm{W}$ je zářivý výkon Slunce, *relativní hvězdná velikost (magnituda)* pak

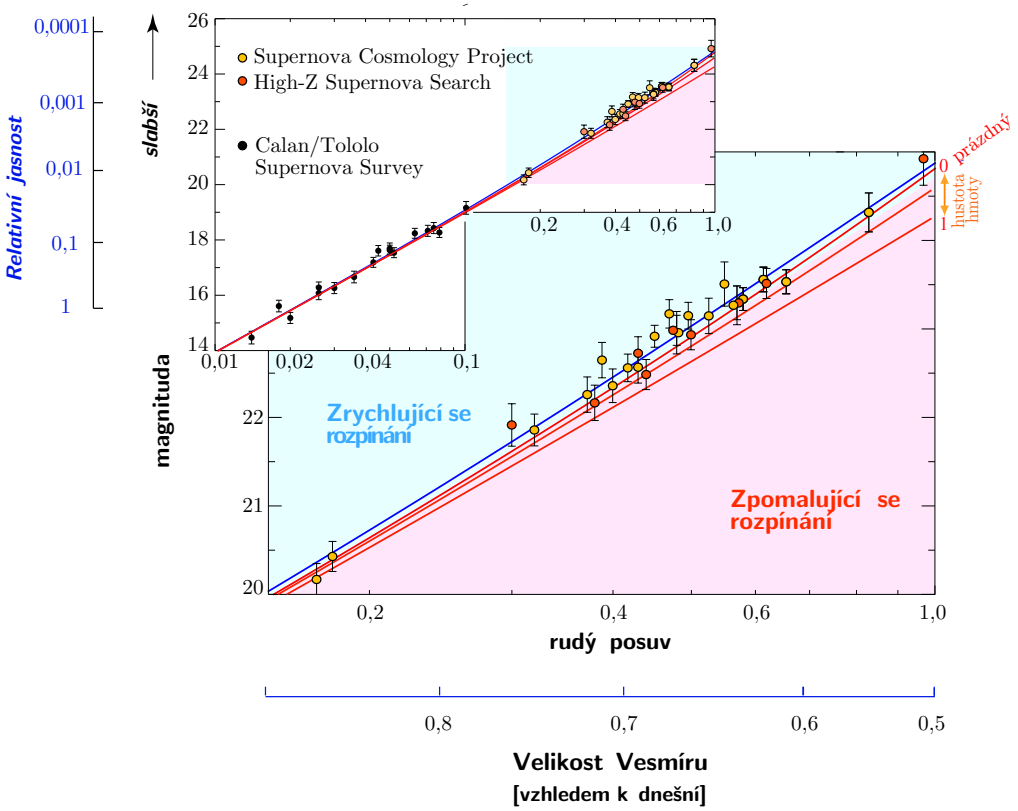
$$m = -2{,}5 \log_{10} \left(\frac{\mathcal{F}}{\mathcal{F}_{\odot\,\mathrm{v}\,10\,\mathrm{pc}}}\right) + 4{,}74,$$

kde $\mathcal{F}_{\odot\,\mathrm{v}\,10\,\mathrm{pc}} = 3{,}21{\cdot}10^{-10}\,\mathrm{W{\cdot}m^{-2}}$ je zářivý výkon Slunce, který by dopadal na jednotku plochy, pokud by se nacházelo ve vzdálenosti 10 pc. Obecně je proto zdánlivá magnituda objektu rovna jeho absolutní magnitudě, kterou by měl ve vzdálenosti 10 pc od nás. Rozdíl

Fotometrickou vzdálenost pak nahrazujeme modulem vzdálenosti.

$$m - M = 5 \log_{10} \left(\frac{d_\mathrm{L}}{10\,\mathrm{pc}}\right)$$

nazývaný *modulem vzdálenosti* je astronomickým vyjádřením vztahu (1.10.4). Příklad závislosti magnitudy na rudém posuvu pro vzdálené supernovy je na obr. 1.14.



Obr. 1.14: Příklad Hubbleova diagramu, tj. závislosti pozorované magnitudy na rudém posuvu z, odpovídající datům získaným pozorováním supernov typu Ia. Pro $z = 0{,}1$ (odpovídá vzdálenosti asi 10^9 ly se začínají křivky lišit v závislosti na předpokládaných hodnotách hustotních parametrů Ω_{m0} a Ω_{v0}. Červené křivky odpovídají modelům bez kosmologické konstanty $\Omega_{v0} = 0$, a hodnotám $\Omega_{m0} = 1$ až $\Omega_{m0} = 0$ (prázdný vesmír). Naměřeným datům nejlépe odpovídá modrá křivka s hodnotami $\Omega_{m0} \approx 0{,}3$ a $\Omega_{v0} \approx 2\Omega_{m0}$, což podle rovnice (1.7.8) znamená, že se rozpínání vesmíru v současné době zrychluje. Upraveno podle [1.33].

Shrnutí

Vlastnosti vesmíru na velkých vzdálenostech dobře charakterizují Hubbleovy diagramy, tj. závislosti vzdálenosti galaxií na rudém posuvu. Měření vzdáleností představuje v kosmologii velký problém, většinou pracujeme s tzv. fotometrickou vzdáleností, při samotných pozorováních i s hvězdnou velikostí neboli magnitudou. Také z Hubbleových diagramů pro supernovy ve vzdálených galaxiích vyplývá, že rozpínání vesmíru se v současné době zrychluje.

Pojmy k zapamatování

- Hubbleův diagram
- standardní svíčky
- fotometrická vzdálenost
- hvězdná velikost (magnituda)
- modul vzdálenosti

Kontrolní otázky

1. *Jakou závislost představují Hubbleovy diagramy?*
2. *Jak zavádíme absolutní a relativní magnitudu?*

Cvičení

1. Ve spektru kvasaru 3C 273 je emisní čára vodíku H_β o laboratorní vlnové délce 486,1 nm posunuta o 77,8 nm směrem k dlouhovlnnému konci spektra. Určete
   a) vzdálenost kvasaru,
   b) lineární rozměru kvasaru, jestliže jeho úhlový průměr činí 0,24″,
   c) velikost výtrysku z kvasaru, jehož úhlová velikost je 19,5″,
   d) zářivý výkon kvasaru, jestliže absolutní bolometrická hvězdná velikost je -25 mag [1.38].
2. Zářivý výkon kvasarů dosahuje 10^{40} W. Fyzikální podstata procesů umožnujících uvolňování tak obrovské energie není dosud definitivně objasněna. Vypočtěte, jaké množství hmoty v jednotkách $M_\odot$ za rok by se muselo přeměnit, aby pokrylo tento výkon
   a) při termonukleární reakci s účinností $\eta = 0{,}01$,
   b) při akreci na černou díru s účinností $\eta = 0{,}2$ [1.38].
3. Šířka čáry H_β ve spektru jádra seyfertovské galaxie je zhruba 3 nm. jaké jsou charakteristické rychlosti pohybu mračen plynu v jádře takové galaxie [1.38]?
4. Rádiový zdroj v jádře aktivní galaxie má úhlovou velikost 0,001″, kosmologický rudý posuv je $z = 0{,}5$. Odhadněte lineární rozměry zdroje v pc [1.38]. Uvažujte Hubbleovu konstantu $H_0 = 71\,\mathrm{km{\cdot}s^{-1}{\cdot}M^{-1}pc}$.

Řešení

1. a) Ze zadání $\lambda = 486{,}1$ nm, $\Delta\lambda = 77{,}8$ nm, $z = \Delta\lambda/\lambda \approx 0{,}16$. Můžeme proto použít přibližný vztah $z \approx v/c$, neboli $v = cz$. Z Hubbleova zákona (1.5.1) $v \approx H_0 d$ a konečně
   $$d = \frac{v}{H_0} = \frac{cz}{H_0} = \frac{\Delta\lambda c}{\lambda H_0},$$
   což pro $H_0 \approx 71\,\mathrm{km{\cdot}s^{-1}{\cdot}Mpc^{-1}}$ dává $d \approx 674$ Mpc.
   b) Pro úhel $\alpha = 0{,}24'' \approx 1{,}16{\cdot}10^{-6}$ rad vychází lineární rozměr
   $$l_\alpha = d\alpha \approx 782\,\mathrm{pc}.$$
   c) Analogicky pro úhel $\beta = 19{,}5'' \approx 9{,}45{\cdot}10^{-5}$ rad vyjde
   $$l_\beta = d\beta \approx 63{,}7\,\mathrm{kpc}.$$
   d) Z rovnice (1.10.6), kde položíme $M = -25$ odvodíme
   $$L = 10^{(4{,}74-M)/2{,}5}\,L_\odot = 10^{1{,}9-0{,}4M}\,L_\odot$$
   po dosazení zářivého výkonu Slunce $L_\odot = 3{,}85{\cdot}10^{26}$ W vychází zářivý výkon kvasaru $L = 3{,}03{\cdot}10^{38}$ W.

2. Vyjdeme z Einsteinova vztahu mezi hmotností a energií $E = Lt = \eta \Delta m c^2$, odkud dostáváme
   a) $\Delta m_1 = \dfrac{Lt}{\eta c^2} = 3{,}53{\cdot}10^{32}\,\mathrm{kg} \approx 177\,M_\odot$,
   b) $\Delta m_2 = \dfrac{Lt}{\eta c^2} = 1{,}76{\cdot}10^{31}\,\mathrm{kg} \approx 9\,M_\odot$.

3. Ze zadání plyne $2\Delta\lambda = 3\,\mathrm{nm}$, vlnová délka čáry $H_\beta = 486{,}1\,\mathrm{nm}$. Koeficient 2 u $\Delta\lambda$ vyjadřuje skutečnost, že plyn se pohybuje jak směrem k nám, tak od nás, pohyb v jednom směru tak statisticky zodpovídá za polovinu rozmazání spektrální čáry. Podle vztahu (1.6.3) dále platí

$$z = \frac{\Delta\lambda}{\lambda} \approx 0{,}0062 \ll 1.$$

   Můžeme proto opět použít přibližný vztah $z \approx v/c$ a pro $c \approx 3{\cdot}10^8\,\mathrm{m{\cdot}s^{-1}}$ vychází

$$v = c\,z = c\,\frac{\Delta\lambda}{\lambda} \approx 9{,}23{\cdot}10^5\,\mathrm{m{\cdot}s^{-1}}.$$

4. Vzhledem k velké hodnotě rudého posuvu musíme použít relativistický vztah

$$1 + z = \sqrt{\frac{1 + \dfrac{v}{c}}{1 - \dfrac{v}{c}}}.$$

   V kombinaci s Hubbleovým zákonem (1.5.1) $v \approx H_0 r$ a vlastnosti úhlů v radiánech $d \approx \alpha r$ (přesná rovnost by platila v plochém prostoru) vychází

$$d \approx \alpha\,\frac{v}{H_0} = \frac{\alpha c}{H_0}\,\frac{(1+z)^2 - 1}{(1+z)^2 + 1}.$$

   Pro zadané hodnoty $\alpha = 0{,}001'' = 4{,}85{\cdot}10^{-9}\,\mathrm{rad}$, $c = 2{,}99{\cdot}10^5\,\mathrm{km{\cdot}s^{-1}}$, $z = 0{,}5$ a $H_0 = 71\,\mathrm{km{\cdot}s^{-1}{\cdot}M^{-1}pc}$ pod dosazení obdržíme

$$d \approx 7{,}86{\cdot}10^{-6}\,\mathrm{Mpc} = 7{,}86\,\mathrm{pc}.$$

1.11 Závěr

V této kapitole jsme nastínili základní představy moderní relativistické kosmologie, základní scénáře možného vývoje vesmíru i výsledky nejnovějších měření jeho základních observačních parametrů. V následujících letech můžeme očekávat další, přesnější a důkladnější pozorování, která bezpochyby naše porozumění vesmíru prohloubí a přinesou i nejedno překvapení. Čtenáře s hlubším zájmem o tuto problematiku můžeme odkázat na mnoho zajímavých monografií: od populárních [1.2, 1.3, 1.13, 1.14, 1.34, 1.39] až po odborné [1.17, 1.27, 1.29, 1.30, 1.32, 1.38]. Řečeno slovy amerického nositele Nobelovy ceny S. Weinberga: „úsilí pochopit vesmír je jednou z velmi mála věcí, která zvedá lidský život trochu nad úroveň frašky a dává mu něco z krásy tragédie“ [1.39].

Literatura ke kapitole 1

[1.1] Allen S.W., Schmidt R.W., Fabian A.C.: „Cosmological constraints from the X-ray gas mass fraction in relaxed lensing clusters observed with Chandra“. *Mon. Not. Roy. Astron. Soc.* **334** (2002), L11. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0205007.

[1.2] Barrow J.D.: *Teorie všeho*. Mladá fronta, Praha 1999.

[1.3] Barrow J.D.: *Teorie ničeho*. Mladá fronta, Praha 2005.

[1.4] Bennett C.L., Banday A.J., Gorski K.M. a kol.: „Four-Year COBE DMR Cosmic Microwave Background Observations: Maps and Basic Results“. *Astrophys. J.* **464** (1996), L1–L4. URL: http://adsabs.harvard.edu/cgi-bin/nph-bib_query?bibcode=1996ApJ...464L...1B&db_key=AST.

[1.5] Bennett C.L. a kol.: „First Year Wilkinson Microwave Anisotropy Probe (WMAP) Observations: Preliminary Maps and Basic Results“. *Astrophys. J. Suppl.* **148** (2003), 1–27. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0302207.

[1.6] Carroll S.M.: *Spacetime and Geometry: An Introduction to General Relativity*. Addison-Wesley 2003. ArXiv: http://xxx.lanl.gov/abs/gr-qc/9712019.

[1.7] Carroll S.M., Press W.H., Turner E.L.: „The cosmological constant“. *Annual Rev. Astron. Astrophys.* **30** (1992), 499–542. URL: http://adsabs.harvard.edu/cgi-bin/nph-bib_query?bibcode=1992ARA%26A..30..499C&db_key=AST.

[1.8] Colless M., Boyle B.: „Redshift Surveys with 2dF“. (1997). ArXiv: http://xxx.lanl.gov/abs/astro-ph/9710268.

[1.9] Colless M. a kol. (The 2DFGRS): „The 2dF Galaxy Redshift Survey: Spectra and redshifts“. *Mon. Not. Roy. Astron. Soc.* **328** (2001), 1039. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0106498 URL: http://www.mso.anu.edu.au/2dFGRS/.

[1.10] Čulík F., Noga M.: *Úvod do štatistickej fyziky a termodynamiky*. Alfa, Bratislava 1982.

[1.11] Felten J.E., Isaacman R.: „Scale factors $R(t)$ and critical values of the cosmological constant Λ in Friedman universes“. *Rev. Mod. Phys.* **58**(3) (1986), 689–698.

[1.12] Freedman W.L. a kol.: „Final Results from the Hubble Space Telescope Key Project to Measure the Hubble Constant“. *Astrophys. J.* **553** (2001), 47–72. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0012376.

[1.13] Gygar J.: *Vesmírná zastavení*. Pyramida, Praha 1990.

[1.14] Gygar J.: *Vesmír jaký je*. Mladá fronta, Praha 1997.

[1.15] Hartle J.B.: *Gravity: An Introduction to Einstein's Relativity*. Addison Wesley, San Francisco 2003.

[1.16] Horský J., Bartoň S.: *Relativistický vesmír*. Ando Publishing, Brno 1997.

[1.17] Horský J., Novotný J., Štefaník M.: *Úvod do fyzikální kosmologie*. Academia, Praha 2004.

[1.18] Janků V.: *Základy statistické fyziky*. UP, Olomouc 1983.

[1.19] Jordan T.F.: „Cosmology calculation almost without general realtivity“. *Am. J. Phys.* **73**(7) (2005), 653–662. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0309756.

[1.20] Knop R.A. a kol. (The Supernova Cosmology Project): „New Constraints on Ω_M, Ω_Λ, and w from an Independent Set of Eleven High-Redshift Supernovae Observed with HST“. *Astrophys. J.* **598** (2003), 102–137. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0309368.

[1.21] Kvasnica J.: *Statistická fyzika*. Academia, Praha 1983 a 1998.

[1.22] Ландау, Л.Д., Лифшиц, Е.М.: *Статистическая физика Часть 1*. Наука, Москва 1976.

[1.23] Liddle A.R.: *An Introduction to modern Cosmology*. John Wiley & Sons Ltd, Chichester 1999.

[1.24] Maddox S.J., Efstathiou G., Sutherland W.J.: „The APM Galaxy Survey - Part Two - Photometric Corrections“. *Mon. Not. Roy. Astron. Soc.* **246** (1990), 433–457. URL: http://adsabs.harvard.edu/cgi-bin/nph-bib_query?bibcode=1990MNRAS.246..433M&db_key=AST.

[1.25] Misner C.W., Thorne K.S., Wheeler J.A.: *Gravitation*. W. H. Freeman &, San Francisco 1973.

[1.26] Møller C.: *The Theory of Relativity*. Clarendon Press, Oxford 1962.

[1.27] Narlikar J.V.: *Introduction to Cosmology*. Cambridge University Press, Cambridge 1993.

[1.28] Narlikar J.V.: „Spectral shifts in general relativity“. *Am. J. Phys.* **62**(10) (1994), 903–907.

[1.29] Padmanabhan T.: *Cosmology and Astrophysics Through Problems*. Cambridge University Press, Cambridge 1996.

[1.30] Peacock J.A.: *Cosmological Physics*. Cambridge University Press, Cambridge 1999.

[1.31] Peebles P.J.E.: „Tests of cosmological models constrained by inflation“. *Astrophys. J.* **284** (1984), 439–444. URL: http://adsabs.harvard.edu/cgi-bin/nph-bib_query?bibcode=1984ApJ...284..439P&db_key=AST.

[1.32] Peebles P.J.E.: *Principles of physical cosmology*. Princeton University Press, New Jersey 1993.

[1.33] Perlmutter S.: „Supernovae, Dark Energy, and the Accelerating Universe“. *Physics Today* **56**(4) (2003), 53–60. URL: http://panisse.lbl.gov/.

[1.34] Rees M.: *Náš neobyčejný vesmír*. Dokořán, Praha 2002.

[1.35] Rektorys K. a kol.: *Přehled užité matematiky I, II*. SNTL, Praha 1988.

[1.36] Schutz B.: *Gravity from the ground up*. Cambridge University Press, Cambridge 2003. URL: http://www.gravityfromthegroundup.org/.

[1.37] Spergel D.N. a kol. (WMAP): „First Year Wilkinson Microwave Anisotropy Probe (WMAP) Observations: Determination of Cosmological Parameters“. *Astrophys. J. Suppl.* **148** (2003), 175. ArXiv: http://xxx.lanl.gov/abs/astro-ph/0302209.

[1.38] Štefl V., Krtička J.: *Úlohy z astrofyziky*. PřF MU, Brno 2000.

[1.39] Weinberg S.: *První tři minuty*. Mladá fronta, Praha 1998.

[1.40] Wesson P.S.: „Olbers's paradox and the spectral intensity of the extragalactic background light“. *Astrophys. J.* **367** (1991), 399–406. URL: http://adsabs.harvard.edu/cgi-bin/nph-bib_query?bibcode=1991ApJ...367..399W&db_key=AST.

Kapitola 2

Základy kvantové informace

Studijní cíle: Dozvíme se proč se lidé začali zabývat otázkami kvantové informace a komunikace, co to jsou qubity a kvantová hradla, jaký je princip kvantového počítače a k čemu by mohl být dobrý, jak funguje kvantová kryptografie či kvantová teleportace.

Klíčová slova: Kvantový bit, qubit, kvantové hradlo, kvantový počítač, kvantově provázané stavy.

Potřebný čas: 450 minut.

2.1 Úvod a něco z historie

2.1.1 Moorův zákon

Naše výpočetní možnosti neustále rostou. Kvantitativně to vystihuje tzv. Moorův zákon: množství tranzistorů které dokážeme umístit na jeden čip se zdvojnásobí zhruba každý rok a půl. Toto pravidlo v ještě optimističtější podobě - zdvojnásobení každý rok - formuloval Gordon Moore, spoluzakladatel firmy Intel roku 1965. Napsal tehdy, že tento trend bylo možné pozorovat několik dosavadních roků a předpověděl, že ještě pár let by to tak mělo jít dál. Za deset let bychom se prý měli dostat z tehdejších šedesáti tranzistorů na neuvěřitelných šedesát tisíc. Moore svůj odhad později zmírnil na zdvojnásobení každé dva roky, ale sám neočekával platnost vyřčeného pravidla po delší dobu než nějakých deset či patnáct let. Uplynulo čtyřicet let a jak si můžeme ověřit, exponenciální nárůst počtu tranzistorů se nezastavil. Například roku 1989 obsahoval mikroprocesor Intel486 1,2 milionů tranzistorů, roku 2004 udává Intel pro svůj Itanium mikroprocesor 590 milionů tranzistorů. To je téměř devět zdvojnásobení během patnácti let, čili zdvojnásobení každý rok a osm měsíců.

Jednoho dne se ale rostoucí exponenciála musí zastavit. Velikost atomu je jistě principiální překážka - tranzistor může být sotva menší než jeden atom. Nejspíše ale ještě dříve narazíme na jiné těžkosti - snad to bude naše schopnost odvádět odpadní teplo, možná to budou ekonomické bariéry. Kdy se dnešní exploze zastaví? Bude trvat ještě deset nebo patnáct let? Ať už ji zastaví cokoliv, ještě několit roků bude vývoj v různých oblastech fyziky pomáhat v udržení platnosti Moorova zákona. Ale na věky to zřejmě nepůjde.

2.1.2 Limity výpočetních možností

Kvantově mechanické modely

I když je růst možností výpočetní techniky impozantní, existují problémy, se kterými si naše počítače sotva kdy poradí. Jedním z nich je numerické modelování větších kvantově mechanických systémů. Problémem je již pouhé zadání stavu do paměti počítače. Zatímco v klasické fyzice je stav popsán zadáním polohy a hybnosti (tedy dvou vektorů) pro každou částici, v kvantové mechanice se stav popisuje pomocí vlnové funkce. Tato funkce má tolik argumentů, kolik stupnů volnosti má celý systém.

Představme si jednu částici, pohybující se v jednom rozměru. Klasická fyzika potřebuje na popis jejího stavu dvě reálná čísla (polohu a hybnost), kvantová fyzika musí zadat komplexní číslo pro každý bod. Rekněme, že pro numerickou simulaci si vystačíme s rozdělením úsečky, podél které se částice pohybuje, na 100 dílků. Ve sto bodech musíme zadat hodnotu vlnové funkce - tedy její reálnou a imaginární část. Předpokládejme, že pro každou z nich nám stačí přesnost daná pamětí jednoho bytu - čili 8 bitů, tedy přesnost omezená na zhruba tři platné číslice. Pro jednu dimenzi tedy potřebujeme zhruba 200 bytů. Buďme velkorysí a řekněme, že se spokojíme jen se 100 byty. Pokud uvažujeme dvourozměrný pohyb částice, musíme zadat její vlnovou funkci na síti 100×100 bodů. Při požadované přesnosti to znamená 10 tisíc bytů, což je stále hravě zvládnutelné. Pro třírozměrný pohyb je to $100^3 = 10^6$, tedy milion bytů. Stále je to řešitelné i na běžném notebooku. Uvažujme ale nyní dvě částice v třírozměrném prostoru. Konfigurační prostor tohoto systému je šestirozměrný a na jeho popis už potřebujeme $100^6 = 10^{12}$ bytů, tedy zhruba terabyte. Naše počítače už dostávají zabrat. Zajímá nás kvantověmechanický problém tří interagujících částic ve třech rozměrech (třeba elektrony v atomu lithia)? Pro numerickou simulaci potřebujeme $100^9 = 10^{18}$ bytů a to je již nad naše možnosti.

Podobně se do problémů dostaneme i při studování mnohem jednodušších systémů - například spinů elektronů. Spin elektronu (jeho vnitřní moment hybnosti) může nabývat jen dvou projekcí do každého směru. Rekněme, že měříme průmět spinu do osy z: můžeme dostat hodnotu buď $+\hbar$ nebo $-\hbar$. Každá z těchto dvou hodnot odpovídá možnému stavu spinu. Tyto stavy si můžeme označit jako $|\uparrow\rangle$ a $|\downarrow\rangle$. Kromě toho se však podle zákonů kvantové mechaniky každý spin může nacházet v libovolné superpozici těchto dvou stavů, tedy ve stavu $|\psi\rangle = \alpha|\uparrow\rangle + \beta|\downarrow\rangle$, kde α a β jsou dvě komplexní čísla splnující $|\alpha|^2 + |\beta^2| = 1$ (o významu těchto čísel a jejich vlivu na výsledky měření se dozvíme více v následujících kapitolách). Zadání těchto dvou čísel definuje stav jednoho spinu. Pokud budeme mít za úkol popsat stav dvou spinů, musíme zadat čtyři koeficienty v superpozici

$$|\psi\rangle = \alpha_1|\uparrow\uparrow\rangle + \alpha_2|\uparrow\downarrow\rangle + \alpha_3|\downarrow\uparrow\rangle + \alpha_4|\downarrow\downarrow\rangle. \tag{2.1.1}$$

Při celkovém počtu N spinů to představuje 2^N koeficientů. Možnost numerického modelování interagujících spinů (což je důležité například pro studium magnetických vlastností látek) tak velice rychle klesá s počtem uvažovaných spinů.

Průvodce studiem

Trochu to připomíná pověst o vynálezci šachu. Když se ho král zeptal, jakou odměnu si žádá za autorství tak úžasné hry, vynálezce si prý řekl o pár zrnek obilí. Na první políčko šachovnice nechť král položí jedno zrnko, na druhé dvě, na třetí čtyři a na každé další dvojnásobný počet toho, co bylo na předchozím políčku. Na celou šachovnici by to představovalo $2^{64} - 1$ zrnek. Ačkoliv se na první pohled mohlo zdát, že se jedná o směšně malou odměnu, mohl ji král stěží splnit. Výsledné množství řádově tisíckrát přesahuje současnou roční světovou produkci pšenice.

K podobné beznaději přijdeme při snahách modelovat kvantově mechanický vývoj systémů složených z více částic. Sice můžeme dostat řadu užitečných výsledků použitím různých aproximací a zjednodušujících předpokladů, na sledování libovolného stavu ale naše možnosti nestačí.

„Složité“ problémy

Kromě modelování kvantově mechanických systémů zná matematika řadu úloh, které se s rostoucím vstupem stávají stále hůře řešitelné tak, že velmi rychle přesáhnou možnosti i těch nejlepších počítačů. Typickým příkladem je problém obchodního cestujícího: máme zadáno N měst, která se mají navštívit. V jakém pořadí městy projedeme, aby byla uražená cesta nejkratší? Další příklad by se dal popsat jako úkol ubytovat N studentů ve čtyřlůžkových pokojích na kolejích s tím, že každý student uvede několik požadavků s kým nesnese, aby byl na pokoji. Důležitou úlohou, jejíž složitosti vděčíme za bezpečný přenos dat, je faktorizace velkých čísel. Pokud budete mít za úkol rozložit na prvočinitele číslo 119, budete za chvilku hotovi, ale u čísla 16637 už to půjde déle. S rostoucím počtem číslic se tento problém rychle stane neřešitelným i pro naše počítače. Kódování pomocí velkých čísel, kde klíč představuje znalost jejich prvočinitelů, je základem některých dnešních kryptografických systémů (o principu tzv. RSA kódu se můžeme dočíst v příloze B).

2.1.3 Ať počítá kvantový systém!

Kvantové superpozice

Skepse nad nemožností využít naše počítače k simulaci kvantových systémů se ale dá obrátit. V osmdesátých letech s tímto nápadem přišel Richard Feynman (nositel Nobelovy ceny za fyziku z roku 1965 za kvantovou elektrodynamiku a autor vynikajících „Feynmanových přednášek z fyziky“ [2.1]). Každý počítač je konec konců fyzikální systém a počítání je fyzikální proces. Všechny dosavadní počítače však k reprezentaci číslic a jejich zpracování využívají pouze zákony klasické fyziky (to, že děje uvnitř tranzistoru atd. jsou ve své podstatě kvantové, tu nehraje roli). Pokud

bychom ale využili všech možností, které nám dává kvantová mechanika, vypadalo by počítání podstatně jinak.

V „klasickém“ počítači (tedy v tom, který pracuje na základě klasické fyziky) může být každý bit ve stavu 0 nebo 1. Soubor N bitů odpovídá 2^N možnostem, v jakých stavech tento soubor může být. Pokud bychom však využili kvantové mechaniky, víme, že podle principu superpozice se každý systém může nacházet v libovolné superpozici jakýchkoliv jiných přípustných stavů. S N kvantovými bity můžeme tedy pracovat s mnohem více než s 2^N stavy—máme k dispozici i jakoukoliv jejich superpozici.

Průvodce studiem

Princip superpozice je jedním ze základních principů kvantové fyziky: pokud může být systém v jednom stavu nebo ve druhém, může být i v jakékoliv superpozici těchto stavů. Erwin Schrödinger, jeden ze zakladatelů kvantové fyziky dospěl k názoru, že z tohoto principu vyplývají důsledky, které se příčí zdavému rozumu—a už málem chtěl kvantovou fyziku zavrhnout. Například radioaktivní jádro může dojít po určité době do superpozice stavů „nerozpadlé jádro“ a „nové jádro a alfa částice“. Jenže alfa částice může spustit řetězec reakcí v Geiger-Müllerově počítači, proudový impuls pak může spustit pekelný stroj, který rozbije ampuli s jedem a jed usmrtí kočku. Pokud může být atom v superpozici stavů (tj. *zároveň* v jednom i druhém stavu), může být v takové superpozici i sama kočka—živá a mrtvá zároveň—a to je podezřelé!

Uvažujme například pouhé dva bity. Jejich hodnoty si můžeme označit jako (0,0), (0,1), (1,0) a (1,1), případně v desítkové soustavě jako 0, 1, 2 a 3. V kvantové fyzice by těmto hodnotám odpovídaly například orientace dvojic spinů, které odpovídají stavům označeným jako $|0\rangle$, $|1\rangle$, $|2\rangle$ a $|3\rangle$. Kromě těchto stavů však kvantově mechanický systém může být v mnoha jiných stavech, například

$$\begin{aligned}
|\psi_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle, \\
|\psi_2\rangle &= \frac{1}{2}|1\rangle + i\frac{\sqrt{3}}{2}|2\rangle, \\
|\psi_3\rangle &= \frac{1}{2}\left(0\rangle + |1\rangle + i|2\rangle - |3\rangle\right), \\
|\psi_4\rangle &= \frac{1}{2}\left(0\rangle - |1\rangle + |2\rangle - |3\rangle\right), \\
&\dots
\end{aligned}$$

Snadno si představíme, že možností, do jakého stavu náš systém umístit, s rostoucím počtem bitů rychle přibývá. Můžeme toho ale nějak využít pro naše počítání?

Deutschova úloha

Nebylo příliš jednoduché najít konkrétní příklad, kdy by vývoj kvantového systému mohl představovat výpočetní algoritmus, který by byl efektivnější, než stan-

dardní algoritmy. Jedním z nich je tzv. Deutschova úloha. Předpokládejme, že kolega má v počítači zadanou funkci proměnné $x \in \{0,1\}$, která může nabývat hodnot 0 nebo 1. Celkem existují čtyři takové funkce: $f_1(x) = 0$, $f_2(x) = 1$, $f_3(x) = x$ a $f_4(x) = 1 - x$. My zatím nevíme, o kterou funkci se jedná, můžeme ale do ní dosazovat a ptát se na výsledek. Řekněme, že máme odpovědět ano či ne na otázku, zda je zadaná funkce konstantní. Pokud bychom měli takovouto funkci naprogramovanou v běžném počítači, museli bychom do ní dosazovat celkem dvakrát. Když však budeme kódovat informaci pomocí kvantových stavů a využijeme principu superpozice, stačí pouze jediné dosazení.

Shorova faktorizace

Ačkoliv po Deutschově úloze přišlo ještě několik dalších jednoduchých schémat, kde byl kvantový přístup efektivnější než s klasickými algoritmy, nějakou dobu to byly spíše jen teoretické hříčky, u nichž nelze očekávat nějakou praktickou aplikaci. Přelom nastal roku 1994, kdy Peter Shor z telekomunikačních laboratoří AT&T publikoval algoritmus, který by na kvantovém počítači dokázal efektivně faktorizovat velká čísla (internetově přístupná verze viz [2.4]). Realizace takového algoritmu by měla zásadní dopad na bezpečnost přenosu kódovaných informací, protože běžně užívané kódy jsou založeny na složitosti faktorizace velkých čísel. Jak takový algoritmus funguje se dozvíme v kapitolách 2.4 a 2.5.

Groverovo vyhledávání

Jiným příkladem efektivity kvantového zpracování informace je Groverův vyhledávací algoritmus. Ve svém článku z roku 1997 nazvaném „Kvantová mechanika pomáhá hledat jehlu v kupce sena“ [2.6] přišel L. K. Grover z Bellových laboratoří s efektivním postupem vyhledávání v rozsáhlých databázích. Představme si, že neznámá kráska nám zanechala své telefonní číslo a my si nemůžeme vzpomenout na její jméno. Můžeme vzít telefonní seznam a probírat jedno číslo po druhém. Kolik záznamů musíme přečíst, než padneme na ten správný? Sice můžeme mít štěstí a být úspěšní hned napoprvé, můžeme však být smolaři a z N záznamů projít všechny. V průměru však budeme muset číst $N/2$-krát. Groverův kvantový algoritmus umožňuje, aby se počat čtení omezil na řádově $\sqrt{N}$. Tedy pokud má seznam milión položek, nemusíme jich přečíst 500 000, ale stačí jen zhruba tisíc. O principu Groverova algoritmu se dozvíme v kapitole 2.6.

Modelování kvantových systémů

Zajímavým výsledkem je i nalezený způsob, jak kvantovým počítačem modelovat evoluci kvantových systémů. Přesněji řečeno, jakým způsobem z elementárních kvantových „procesorů“ sestavit předem zadaný evoluční operátor popisující zkoumaný kvantový systém.

2.1.4 Problémy konstrukce kvantového počítače

Křehkost kvantových bitů

Jakkoliv nalezené kvantové algoritmy vypadají slibně, zásadní problém spočívá v tom, jak takový počítač fyzicky sestrojit. Kvantové bity (zvané *qubity*) jsou buď velmi citlivé na rušivé vlivy okolí, anebo je značně obtížné je přinutit, aby spolu navzájem „mluvily“. První problém lze ilustrovat na tomto příkladu: bit může být realizován třeba jako jeden ze dvou spinových stavů nějakého atomu drženého v pasti (může jít například o iont udržovaný na svém místě vhodným elektrickým polem, nebo neutrální atom zachycený v tzv. optické mřížce, stojaté vlně tvořené interferujícími laserovými svazky). Řekněme, že pokud spin valenčního elektronu míří dolů, znamená to logickou nulu, zatímco spin mířící vzhůru znamená logickou jedničku. Potřebujeme připravit a udržet qubit ve stavu $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Elektron však mění svůj spin pod vlivem vnějšího magnetického pole—a to může být způseobeno třeba okolními atomy. Bez naší kontroly tak může dojít třeba k tomu, že se nula překlopí na jedničku a naopak. Pokud takovémuto překlápění nějak zabráníme, stále ještě snadno může docházet k fázovým posuvům: vstupní superpozice se změní na $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$, kde φ je nějaká neznámá fáze, daná konkrétní interakcí atomu s okolím. Výsledný stav qubitu je tedy odlišný od vstupního a na výstup z počítače se pak v žádném případě nemůžeme spolehnout. Musíme tedy hledat způsob jak systém qubitů co nejlépe izolovat od okolí, případně jak korigovat drobné chyby, které se v průběhu času vyskytly. Oba přístupy jsou dnes v centru intenzivního vědeckého výzkumu.

Průvodce studiem

V křehkosti kvantových superpozic spočívá jedna z odpovědí, proč nepozorujeme „Schrödingerovy kočky“, tedy superpozice různých stavů (živý a zároveň mrtvý) u makroskopických objektů. Vlivem i nepatrné interakce s okolím (například místnost s kočkou opustí jediný foton) se systém dostává do jednoho z mnoha „normálních“ stavů. Uchování neporušených superpozic mnohaqubitových stavů (mnoho qubitů je skoro makroskopický objekt) je pak jednou z hlavních výzev pro realizaci kvantového počítače.

Nesnadná interakce mezi qubity

Některé systémy kvantových bitů jsou naopak poměrně robustní. Ač se to nezdá, patří k nim třeba světlo. Qubit můžeme realizovat pomocí polarizace jediného fotonu. Pokud bude elektrické pole horizontálně letícího fotonu kmitat vodorovně ($\leftrightarrow$), bude to znamenat logickou nulu, svislé kmitání ($\updownarrow$) bude znamenat jedničku. V průhledném prostředí se takový foton může šířit na veliké vzdálenosti aniž by se jeho polarizační stav nějak narušil. Problém však je přinutit fotony interagovat: jak dosáhnout toho, aby polarizační stav jednoho fotonu ovlivnil polarizaci druhého fotonu? Něco takového je ale nezbytně nutné, pokud bychom chtěli postavit „fotonový

kvantový počítač“ s polarizačními qubity. I zde je spousta zajímavých otázek, které čekají na své vyřešení.

2.1.5 Jiné aplikace kvantové informatiky

Kvantová kryptografie

Ačkoliv by kvantové počítače mohly představovat určitou hrozbu pro naše soukromí (rychlá faktorizace velkých čísel by znamenala snadné rozluštění kódovaných zpráv), přináší jiné odvětví kvantové informatiky naopak možnost jak dosáhnout bezpečného přenosu utajovaných dat. Využívá se tu principiální nemožnosti spolehlivě rozlišovat mezi neortogonálními kvantovými stavy a toho, že měření kvantový stav obecně narušuje. Základem kvantové kryptografie je distribuce tajného klíče mezi dvěma vzdálenými partnery tak, aby nikdo jiný klíč nemohl znát. Jakmile dvě strany klíč znají (je to v podstatě náhodná posloupnost nul a jedniček), stačí jej přičíst k binárně kódované zprávě. Takto zašifrovaný vzkaz se pak vnějšímu pozorovateli jeví jako zcela chaotická změť nul a jedniček bez jakýchkoliv vnitřních korelací, které by se daly využít k získání nějaké užitečné informace.

Tajný klíč se dá předat například posláním řady qubitů. Jak uvidíme později, je přitom zapotřebí náhodně měnit bázi, v jaké se nuly a jedničky kódují do kvantových stavů. Pokud by nějaký špión chtěl předávaný klíč odposlechnout, musel by přitom do systému vnést takový šum, že by byl snadno odhalitelný.

Kvantová kryptografie je z oblastí kvantové informatiky pravděpodobně nejblíže komerčnímu využití. Jako ukázku jejích možností provedl vědecký tým prof. Antona Zeilingera z vídeňské univerzity první skutečnou bankovní transakci na jaře roku 2004: slabounkým proudem fotonů proběhla platba mezi vídeňskou radnicí a pobočkou místní banky. O kvantové kryptografii bude pojednávat kapitola 2.7.

Kvantová teleportace

Ve sci-fi příbězích funguje teleportace tak, že cestující je ve startovní stanici rozebrán na své nejmenší součástky - řekněme atomy, informace o těchto atomech je poslána světelným či jiným elektromagnetickým zářením do cílové stanice, kde je pak cestující z odpovídajících součástek opět poskládán dohromady. Kvantová teleportace znamená podobnou přepravu kvantových stavů. Systém ve startovní stanici se nachází v nějakém neznámém kvantovém stavu. Pokud bychom tento stav změřili a zjištěnou informaci poslali do cílové stanice, mohli bychom tam připravit jiný systém ve stejném stavu. Problém je ovšem v tom, že nelze určit stav kvantového systému měřením na jediném exempláři. Pokud bychom totiž změřili jednu fyzikální veličinu, řekněme polohu nějaké částice, zničíme tím informaci o konjugované veličině, v našem případě o její hybnosti. Mohli bychom se snažit operovat v rámci Heisenbergových relací neurčitosti a měřit obě veličiny současně za cenu snížení přesnosti. Představme si například harmonický oscilátor o (úhlové) frekvenci ω připravený v nějakém (pro nás neznámém) koherentním stavu. Pokud bychom se

pokusili změřit jeho polohu a hybnost a výsledné hodnoty použít k přípravě stavu jiného harmonického oscilátoru, byl by takto vytvořený stav podobný originálu, ale obsahoval by přidaný šum. Množství šumu by odpovídalo fluktuacím termálního stavu o střední energii jednoho energetického kvanta $\hbar\omega$, kde $\hbar = 1{,}055 \times 10^{-34}$ Js je Planckova konstanta h dělená 2π. Čistší výsledek nám kvantová mechanika s tímto protokolem nedovolí.

Tento problém se však dá překonat, pokud by výchozí a cílová stanice sdílely předem připravený kvantově provázaný stav. To je zvláštní stav systému, který se skládá ze dvou (či více) odlehlých podsystémů. Můžeme pak měřit určité kombinované veličiny systému, jehož stav se má teleportovat a provázaného podsystému ve výchozí stanici. Mohou to být například součet poloh a rozdíl hybností - operátory těchto veličin navzájem komutují a lze je tedy měřit současně s libovolnou přesností. Výsledné hodnoty pošleme do cílové stanice, kde se na jejich základě působí na tamní podsystém - operátor jej přesune a „šťouchne“ do něj tak, aby se přesným způsobem změnila jeho poloha a hybnost. Na konci celé této operace bude stav vstupního systému zničen, ale v cílové stanici bude připraven stav totožný s tím, jaký byl původně ve výchozí stanici. Takováto „kvantová teleportace“ byla nedávno experimentálně realizována na optických pulsech, přičemž teleportované veličiny byly jednak proměnné odpovídající intenzitě elektrického pole světelného svazku (analogické poloze a hybnosti mechanického systému), ale i polarizační proměnné analogické spinu. V tomto druhém případě dává měření kombinovaného systému ve výchozí stanici dva bity informace (jeden ze čtyř stavů systému složeného ze dvou spinů 1/2), které se pošlou do cílové stanice tak, aby tam mohl být zrekonstruován teleportovaný qubit. O teleportaci kvantových stavů qubitu se dozvíme více v kapitole 2.9

Husté kódování

Teleportací „naruby“ by se mohlo nazývat husté kódování, kdy dvě komunikující strany (řekněme Alice a Bob) na počátku sdílejí kvantově provázané dvojice systémů. Pokud chce Alice poslat nějakou zprávu Bobovi, bude mu předávat qubity - například fotony s vhodnou polarizací. Při vhodné manipulaci pak s každým qubitem předá dva bity informace, tedy dvakrát tolik, než co by umožňovalo posílání qubitů bez sdílených provázaných stavů.

Klonování

Operací, kterou nám kvantová mechanika nedovolí provádět dokonale, je přesné kopírování kvantových stavů, někdy nazývané klonování. To, co je v počítačích naprosto běžnou a nezbytnou součástí mnoha algoritmů, tedy zkopírování dat z jednoho registru do druhého, s qubity učinit nelze. Plyne to z principu superpozice: představme si zařízení, které do prázdného registru x kopíruje informaci o hodnotách 0, 1 z registru y, tedy $|0\rangle_x|0\rangle_y \rightarrow |0\rangle_x|0\rangle_y$ a $|0\rangle_x|1\rangle_y \rightarrow |1\rangle_x|1\rangle_y$. Pokud by však qubit v registru y byl nějakou superpozicí stavů $|0\rangle$ a $|1\rangle$, třeba $a|0\rangle_y + b|1\rangle_y$, byl by pak výsledný stav obou registrů $a|0\rangle_x|0\rangle_y + b|1\rangle_x|1\rangle_y$, což je něco jiného, než dvě kopie původního stavu, tedy $(a|0\rangle_x + b|1\rangle_x)(a|0\rangle_y + b|1\rangle_y)$. Nemožnost přesně

kopírovat kvantovou informaci nám dovoluje spolehnout se na kvantovou kryptografii. Nicméně můžeme kvantové stavy klonovat alespoň přibližně s tím, že kopírování vnáší do soustavy jistý šum. Jak zvolit optimální klonovací strategii? Jaké ohrožení soukromí by pak takovéto klonování představovalo? Jak skombinovat teleportaci s klonováním pro „kvantové faxování“ či „teleklonování“? To jsou některé z mnoha otázek, které dnes kvantová informatika řeší a které jsou podstatné pro případnou kvantovou komunikaci. Motivací je umožnit výměnu dat mezi kvantovými počítači i mezi vzdálenými stranami, které chtějí sdílet tajný kryptografický klíč a potřebují zamezit vlivu ztrát, které jsou podstatné při přenosu na větší vzdálenosti.

Shrnutí

Kvantová informatika využívá kódování informace pomocí kvantových stavů různých fyzikálních systémů. Důležitým aspektem je zde hlavně princip superpozice stavů. Kvantový počítač by měl být schopen efektivně řešit některé problémy, které by na klasických počítačích trvaly příliš dlouho. Jedná se například o faktorizaci velkých čísel, vyhledávání v rozsáhlých databázích nebo modelování časového vývoje kvantových systémů. Kvantová kryptografie slouží k bezpečnému předávání tajného klíče. K dalším aplikacím kvantové informatiky patří husté kódování či teleportace kvantových stavů.

Pojmy k zapamatování

- Moorův zákon,
- superpozice kvantových stavů,
- qubit,
- kvantový počítač,
- kvantová kryptografie,
- kvantová teleportace.

Kontrolní otázky

1. *Jakým způsobem rostou nároky na paměť počítače v závislosti na velikosti systému při modelování kvantových stavů?*
2. *Proč je zajímavá otázka jak efektivně faktorizovat velká čísla?*
3. *Jaké jsou hlavní překážky pro postavení kvantového počítače?*
4. *Proč lidé považují kvantovou kryptografii za bezpečnou?*

Úkoly k textu

1. Předpokládejme, že Moorův zákon bude platit ještě neomezenou dobu a že například každý rok a půl se zdvojnásobí velikost paměti, kterou mají naše počítače k dispozici. Řekněme, že jsme nyní schopni uložit 10 GB v paměti počítače pro popis fyzikálního stavu. Za jak dlouho bychom pak byli schopni uložit informaci o klasickém mikrostavu jednoho molu plynu, jestliže pro popis stavu jedné molekuly potřebujeme 5 bytů informace?

2. Řekněme, že na zadání jedné amplitudy pravděpodobnosti potřebujeme 5 bytů informace, a že chceme popsat kvantový stav soustavy spinů, z nichž každý má dvě možné projekce. Kolikaspinový systém můžeme popsat za dnešních podmínek (jako v předchozí úloze) a kolikaspinový systém bude možné popsat poté, co půjde do paměti našeho počítače uložit informaci o klasickém mikrostavu jednoho molu částic?

Řešení

1. Jeden mol je $\sim 6 \times 10^{23}$ částic, pro popis stavu potřebujeme $\sim 3 \times 10^{24}$ bytů informace, tedy asi 3×10^{14} krát víc, než máme k dispozici. Protože $3 \times 10^{14} \approx 2^{48}$, musíme celkem 48krát zdvojnásobit naši paměťovou kapacitu, na což bychom při stálé platnosti Moorova zákona potřebovali asi 72 let.
2. Na kvantový popis N-spinového systému musíme zadat 2^N amplitud a tedy potřebujeme 5×2^N bytů paměti. K dispozici máme zatím 10^{10} bytů, což je zhruba 5×2^{31}, takže můžeme popsat stav systému s asi 31 spiny. Z předchozí úlohy víme, že pro popis klasického mikrostavu jednoho molu potřebujeme 48krát zdvojnásobit naši paměťovou kapacitu. Každé zdvojnásobení paměťové kapacity nám umožní zvýšit počet popisovaných spinů o jeden, takže nakonec bychom mohli pracovat s asi 79 spiny.

2.2 Kvantové bity neboli qubity

2.2.1 Co je to qubit

Za kvantový bit můžeme považovat libovolný fyzikální systém, u nějž jsou ve hře dva vzájemně ortogonální kvantové stavy. Z matematického hlediska tyto stavy odpovídají dvěma ortogonálním vektorům v Hilbertově prostoru. Fyzikálně to jsou například dvě ortogonální polarizace fotonu, dva vibrační stavy harmonického oscilátoru (třeba iontu v iontové pasti), dva spinové stavy atomu nebo iontu, případně stav fotonu, který se může nacházet ve dvou cestách nějakého interferometru. Mohou to být i dvě různé hodnoty proudu v supravodivém interferenčním zařízení SQUID (Superconducting QUantum Interference Device), případně dvě hodnoty náboje na supravodivém ostrůvku odděleném od jiných supravodičů tenkou bariérou z nesupravodivého materiálu—tzv. Josephsonovým spojem.

Při volbě dvou bázových ortogonálních stavů dvoustavového systému máme velkou volnost: pokud jde o polarizace fotonu, může to být vertikální a horizontální polarizace, nebo polarizace 45° šikmo vzhůru a šikmo dolů, nebo levotočivá a pravotočivá kruhová polarizace, případně jakákoliv jiná dvojice lineárně či elipticky polarizovaných stavů. Je dobré si připomenout, že pokud si zvolíme nějakou bázovou dvojici stavů, jakýkoliv jiný stav je možné vyjádřit jako jejich superpozici. Například

pravotočivě polarizovaný foton ve stavu $|R\rangle$ a levotočivě polarizovaný foton ve stavu $|L\rangle$ lze vyjádřit pomocí vertikální polarizace $|\updownarrow\rangle$ a horizontální polarizace $|\leftrightarrow\rangle$ jako

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|\updownarrow\rangle + i|\leftrightarrow\rangle\right), \tag{2.2.1}$$

$$|L\rangle = \frac{1}{\sqrt{2}}\left(i|\updownarrow\rangle + |\leftrightarrow\rangle\right). \tag{2.2.2}$$

Pro bázové stavy přitom platí podmínka ortonormality, tedy skalární součin vektoru se sebou samým je jednička a skalární součin s druhým (ortogonálním) vektorem je nula,

$$\langle\updownarrow|\updownarrow\rangle = 1, \tag{2.2.3}$$

$$\langle\updownarrow|\leftrightarrow\rangle = 0, \tag{2.2.4}$$

$$\langle\leftrightarrow|\updownarrow\rangle = 0, \tag{2.2.5}$$

$$\langle\leftrightarrow|\leftrightarrow\rangle = 1. \tag{2.2.6}$$

Průvodce studiem

Volba vhodné báze je důležitým krokem: může nám velice usnadnit některé výpočty, nebo může být vhodná pro fyzikální implementaci. Pokud pracujeme například se spiny atomů, které se nacházejí v magnetickém poli, je vhodné volit za bázové stavy ty, které mají definovanou projekci spinu do směru magnetického pole: bázové stavy se pak „nehýbou“. Pokud bychom zvolili jiný směr než magnetické pole, systém by v daném bázovém stavu nezůstal a osciloval by mezi různými bázovými stavy.

Jakmile máme zvolenou bázi, můžeme si její dva vektory označit jako $|0\rangle$ a $|1\rangle$ a každý stav systému vyjádřit jako jejich superpozici $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, kde α a β jsou komplexní čísla splňující $|\alpha|^2 + |\beta|^2 = 1$. Těmto komplexním číslů říkáme často *amplitudy*. Pokud bychom chtěli vyjádřit stav $|\psi\rangle$ pomocí jiné báze, dané vektory $|u\rangle$ a $|v\rangle$, můžeme psát $|\psi\rangle = \tilde{\alpha}|u\rangle + \tilde{\beta}|v\rangle$. Vztah mezi dvojicí amplitud $\tilde{\alpha}$, $\tilde{\beta}$ a α, β je dán skalárními součiny mezi vektory báze $|0\rangle$, $|1\rangle$ a vektory báze $|u\rangle$, $|v\rangle$. Vynásobíme-li vektor $|\psi\rangle$ zleva bázovými vektory $|u\rangle$ a $|v\rangle$, dostaneme

$$\langle u|\psi\rangle = \tilde{\alpha}\langle u|u\rangle + \tilde{\beta}\langle u|v\rangle = \tilde{\alpha} = \alpha\langle u|0\rangle + \beta\langle u|1\rangle, \tag{2.2.7}$$

$$\langle v|\psi\rangle = \tilde{\alpha}\langle v|u\rangle + \tilde{\beta}\langle v|v\rangle = \tilde{\beta} = \alpha\langle v|0\rangle + \beta\langle v|1\rangle, \tag{2.2.8}$$

což lze psát v maticovém tvaru

$$\begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{2.2.9}$$

kde matice U daná vztahy

$$U = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} = \begin{pmatrix} \langle u|0\rangle & \langle u|1\rangle \\ \langle v|0\rangle & \langle v|1\rangle \end{pmatrix}, \tag{2.2.10}$$

se nazývá matice přechodu od báze $|0\rangle$, $|1\rangle$ k bázi $|u\rangle$, $|v\rangle$.

2.2.2 Měření kvantových bitů

Měření je v kvantové fyzice svou povahou nedeterministické, to znamená, že často není principiálně možné ze známého stavu předpovědět výsledek měření, ale jen pravděpodobnosti, s jakými ten který výsledek může nastat. Tím, jakou veličinu budeme měřit (např. průmět spinu elektronu do osy x, nebo kruhovou polarizaci fotonu) určujeme bázi, do které se bude stavový vektor promítat. Druhé mocniny absolutních hodnot amplitud u jednotlivých bázových stavů jsou rovny pravděpodobnostem, s jakými zjistíme příslušný výsledek.

Průvodce studiem

Za tuto tzv. „statistickou interpretaci“ vlnové funkce dostal Max Born v roce 1954 Nobelovu cenu. Poprvé se objevila v jeho článku z roku 1926, kde se zabývá myšlenkou, že nově vzniklá kvantová mechanika je vhodná i pro popis nestacionárních dějů, například srážek částic. V článku je věta říkající, že nalezená vlnová funkce Φ (zkoumal tam srážku elektronu s atomem) může mít pouze jednu interpretaci, a to pravděpodobnost, že se odražený elektron šíří daným směrem. Pod čarou se pak objevuje poznámka doplněná při korektuře: „Přesnější úvaha ukazuje, že pravděpodobnost je úměrná kvadrátu Φ.“ Dva řádečky a Nobelova cena z toho—tomu říkám efektivita práce!

Pokud uvažujeme například foton ve stavu $|\psi\rangle = \frac{1}{2}|R\rangle - i\frac{\sqrt{3}}{2}|L\rangle$ a měříme kruhovou polarizaci fotonu, zjistíme s pravděpodobností $|\frac{1}{2}|^2 = 1/4$ pravotočivou a s pravděpodobností $|i\frac{\sqrt{3}}{2}|^2$ 3/4 levotočivou polarizaci. Pokud bychom měli stav fotonu zadán jako lineárně polarizovaný ve svislém směru $|\updownarrow\rangle$, převedením do báze kruhových polarizací zjistíme, že $|\updownarrow\rangle = \frac{1}{\sqrt{2}}|R\rangle - \frac{i}{\sqrt{2}}|L\rangle$ a tím pádem každou z kruhových polarizací bychom naměřili s pravděpodobností 1/2.

Je třeba zdůraznit, že ačkoliv qubit může být v nekonečně mnoha různých stavech, jeho měřením nikdy nedostaneme víc než jeden bit informace: jednu ze dvou možných odpovědí.

Pokud uvažujeme systém o více qubitech, měření na jednom qubitu může ovlivnit stav zbývajícího systému. Představme si například dva qubity připravené ve stavu

$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle \tag{2.2.11}$$

a měříme stav prvního qubitu v bázi $|0\rangle$, $|1\rangle$. Stav daný rovnicí (2.2.11) si můžeme přepsat do tvaru

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2.2.12}$$

Měření na prvním qubitu nám dá výsledek $|0\rangle$ nebo $|1\rangle$, každý s pravděpodobností 1/2. Pokud bude výsledek 0, bude druhý qubit ve stavu $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, pokud bude výsledek 1, změní se stav druhého qubitu na $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Pokud

bychom tedy nyní měřili stav druhého qubitu v bázi dané stavy $|+\rangle$ a $|-\rangle$, dostali bychom jednoznačný výsledek určený tím, co bylo naměřeno na prvním qubitu. Na druhé straně, pokud bychom druhý qubit měřili v bázi $|0\rangle$ a $|1\rangle$, byl by výsledek zcela náhodný: s pravděpodobností 1/2 bychom dostali 0 a s pravděpodobností 1/2 bychom dostali 1.

Stav z rovnice (2.2.11) však lze přepsat i ve tvaru

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\right] \otimes |0\rangle + \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right] \otimes |1\rangle \\ &= \frac{1}{\sqrt{2}}|+\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|-\rangle \otimes |1\rangle. \end{aligned} \tag{2.2.13}$$

To znamená, že pokud budeme měřit první qubit v bázi $|+\rangle$ a $|-\rangle$, dostane se podle výsledku druhý qubit buď do stavu $|0\rangle$ nebo $|1\rangle$. Pokud pak měříme stav druhého qubitu v bázi $|0\rangle$, $|1\rangle$, bude výsledek jednoznačně určený z měření na prvním qubitu. Pokud bychom však měřili druhý qubit v bázi $|+\rangle$ a $|-\rangle$, bude výsledek zcela náhodný.

Stav z rovnice(2.2.11) má zajímavé korelační vlastnostmi mezi dvěma qubity; takovému stavu se říká *kvantově provázaný,* neboli *entanglovaný.* Takovéto stavy mají velký význam pro přenos kvantové informace, více se o nich dozvíme v kapitole 2.8.

Shrnutí

Qubit čili kvantový bit je libovolný systém s dvěma ortogonálními stavy, například spin elektronu či polarizace fotonu. Qubit může nést jeden bit informace, může však být připraven v libovolné superpozici bázových stavů. Měření na qubitu nese všechny rysy kvantového měření: výsledek může být buď předpověditelný nebo náhodný, podle zvolené báze. Měřením však původní kvantový stav zaniká a systém (pokud není též detekcí zničen jako foton při fotodetekci) je připraven ve zcela novém kvantovém stavu.

Pojmy k zapamatování

- Qubit,
- báze,
- kvantové měření.

Kontrolní otázky

1. *Kolik bitů informace můžete předat kolegovi, jestliže mu dáte jeden qubit?*
2. *Kolik bázových stavů má systém složený z pěti qubitů?*
3. *S jakými pravděpodobnostmi bychom dostali jednotlivé výsledky, pokud bychom stav z předchozí úlohy měřili v bázi $|+\rangle$ a $|-\rangle$?*

Úkoly k textu

1. Qubit je připraven ve stavu $\frac{i}{\sqrt{3}}|0\rangle - \sqrt{\frac{2}{3}}|1\rangle$. Provedeme na něm měření v bázi $|0\rangle$, $|1\rangle$. S jakými pravděpodobnostmi dostaneme jednotlivé výsledky?
2. S jakými pravděpodobnostmi bychom dostali jednotlivé výsledky, pokud bychom stav z předchozí úlohy měřili v bázi $|+\rangle$ a $|-\rangle$?

Řešení

1. $|0\rangle$ s pravděpodobností 1/3 a $|1\rangle$ s pravděpodobností 2/3.
2. $|+\rangle$ i $|-\rangle$ s pravděpodobností 1/2.

2.3 Kvantová hradla

Pro funkci kvantového počítače je nezbytné, abychom dokázali s qubity manipulovat. Transformace qubitů probíhá v hradlech—to jsou zařízení, ve kterých dochází k nějaké jasně definované změně kvantového stavu qubitu.

2.3.1 Reverzibilita kvantového počítání

Každá transformace qubitů odpovídá evoluci kvantového stavu nějakého fyzikálního systému. Pokud je celý systém izolovaný od svého okolí, je takováto transformace popsána unitárním operátorem, tedy operátorem U, pro který platí $UU^\dagger = = U^\dagger U = I$, kde I je jednotkový operátor. Pro maximální využití výhod kvantového počítání je zapotřebí pracovat právě s unitárními transformacemi. Protože každý unitární operátor lze invertovat (inverzním operátorem k U je jeho hermitovsky sdružený operátor $U^\dagger$), je možné každou operaci v kvantovém počítači obrátit a nechat ji běžet nazpět. To je velký rozdíl oproti práci klasických počítačů, který však s sebou přináší určité komplikace.

Průvodce studiem

Reverzibilním počítáním se zabývali teoretici i na základě klasické fyziky: Fredkin a Toffoli v osmdesátých letech přišli s balistickým modelem reverzibilního počítače. Ten je tvořen soustavou kulečníkových koulí (jejichž přítomnost či nepřítomnost kóduje binární čísla) a překážek tvořících hradla. Koule se pohybují beze ztrát energie podle Newtonových zákonů a narážejí do překážek a do sebe navzájem. Výsledek „výpočtu“ pak odečteme z poloh koulí na konci jejich dráhy. Protože srážkové děje v klasické fyzice mohou probíhat oběma směry, můžeme nechat takovýto počítač „běžet zpět“, aby z výsledných dat udělal data vstupní.

FANAOUT: kopírování

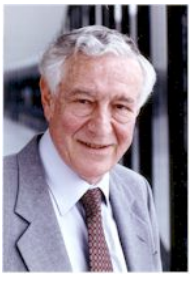
Operace FANOUT (tedy „rozfouknutí“) vytváří dvě kopie vstupního bitu. Aby tato operace mohla být unitární, znamená to, že velikost vstupu musí být rovna velikosti výstupu (měřeno dimenzí Hilbertova prostoru vstupního a výstupního stavu). Protože na výstupu jsou dva bity, musí být vstupní bit doplněn dalším pomocným bitem, který je nastaven na nějakou pevnou hodnotu. Příklad realizace FANOUT ukážeme v odstavci 2.3.4.

Operaci FANOUT můžeme pro kvantové počítání sestrojit, nicméně je třeba si uvědomit, že nám dovoluje pouze vytvořit z bitu 0 dva nulové bity, případně z bitu 1 dva bity o hodnotě 1. Nemůžeme však „klonovat“ kvantové stavy, tedy vytvářet kopie libovolných superpozic—viz odstavec 2.1.5.

Nulování

Operace, která by z libovolné vstupní hodnoty vytvořila nulu, neboli jakýkoliv vstupní stav transformovala na $|0\rangle$, není unitární. Znamená to tedy, že obecně nemůžeme v kvantovém počítači vynulovat nepotřebné bity a volné registry použít pro ukládání užitečných dat. Pomoci si můžeme pouze tehdy, pokud máme dvě (či více) kopií nějakého bitu. V tomto případě můžeme použít inverzi k operaci FANOUT a ze dvou kopií vytvořit jedinou s tím, že jeden bit se vynuluje.

Pro vynulování poslední kopie daného bitu (o neznámé hodnotě) však nemůžeme použít unitární transformaci. Takovéto operaci by odpovídalo „stlačování“ fázového prostoru nebo snižování dimenze Hilbertova prostoru našeho fyzikálního systému. Z termodynamického hlediska by to odpovídalo poklesu entropie systému. Podle druhého termodynamického zákona však entropie izolovaného systému klesat nemůže, entropie se můžeme zbavit pouze tím, že ji předáme nějakému jinému fyzikálnímu systému. Pokud budeme předávat tuto entropii okolí, které je v termodynamické rovnováze při teplotě T, může se jeho entropie zvýšit o ΔS pouze tehdy, pokud mu dodáme energii (ve formě tepla) $T\Delta S$. Při nulování neznámého bitu se entropie daného registru sníží o $k_B \ln 2$, kde $k_B = 1{,}38 \times 10^{-23}$ J/K je Boltzmannova konstanta. Proč? Neznámý bit nabývá hodnoty 0 s pravděpodobností 1/2 a hodnoty 1 také s pravděpodobností 1/2. Entropie takového registru je tedy $S_1 = -k_B \sum_n p_n \ln p_n = -k_B[\frac{1}{2}\ln\frac{1}{2} + \frac{1}{2}\ln\frac{1}{2}] = k_B \ln 2$. Bit s hodnotou 0 odpovídá systému s nulovou entropií: $p_0 = 1$ a $p_1 = 0$, tedy $S_1 = 0$. Celkem tedy entropie registru poklesne o $\Delta S = k_B \ln 2$. Předáme-li takovou entropii do okolí o teplotě T, musíme disipovat teplo $k_B T \ln 2$.



Rolf Landauer (1927 - 1999) z IBM, největší přínos má ve zkoumání fyzikálních mezí pro naše výpočetní možnosti.

Tomuto tvrzení se říká *Landauerův princip:* pro vynulování neznámého bitu je nutno disipovat alespoň $k_B T \ln 2$ tepla. V současných počítačích se disipuje mnohem více tepla (bity v nich nejsou kódovány pomocí dvou kvantových stavů elementárních „dvoustavových“ systémů, ale pomocí stavů mnohem větších objektů). Landauerův princip udává určitou mez pro minimální disipaci tepla, ke které se můžeme blížit, pokud naše počítače budou v maximální míře pracovat s reverzibilními kroky.

Průvodce studiem

Landauerův princip se ukazuje také jako konečné rozluštění záhady Maxwellova démona. Maxwell uvažoval inteligentní bytůstku, která by oddělovala v rozdělené nádobě s plynem rychlé molekuly od pomalejších: po čase by tak v jedné části byla vyšší teplota než ve druhé. To by nám pak umožňovalo zapojit mezi obě části tepelný stroj, který by část tepla přeměnit na užitečnou práci. To je ale proti druhému termodynamickému zákonu. Někde asi musí být chyba - a přes stovku let a řadu falešných stop trvalo, než fyzikové zjistili kde: při každém měření rychlosti molekul Maxwellův démon zaplňuje svoji paměť. Až svou paměť zaplní úplně, bude ji muset vynulovat. Ale na to musí podle Landauerova principu disipovat energii (znehodnotit ji na teplo). Znehodnocené energie bude nakonec přinejmenším tolik, kolik jsme získali užitečné práce.

Pro kvantové počítání to znamená, že pokud ireverzibilní kroky nepřicházejí v úvahu (například pro ztrátu koherence), musíme mít v zásobě dostatek volných bitů, do kterých se v průběhu výpočtů odkládá „odpad“.

2.3.2 Jednobitová hradla

Hradla I, X, Y a Z

Nejjednoduššímm typem hradel jsou taková, která mění stav jediného qubitu. Ta zcela nejjednodušší, označená jako operátory I, X, Y a Z transformují qubity následujícím způsobem:

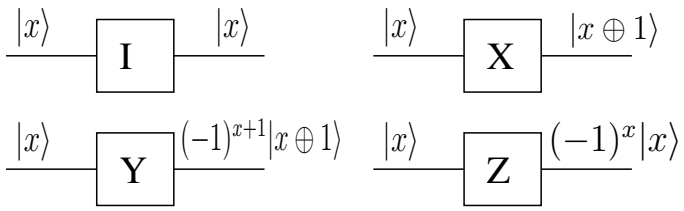
$$\begin{aligned} I: \quad & |0\rangle \rightarrow |0\rangle, \\ & |1\rangle \rightarrow |1\rangle, \qquad (2.3.1) \\ X: \quad & |0\rangle \rightarrow |1\rangle, \\ & |1\rangle \rightarrow |0\rangle, \qquad (2.3.2) \\ Y: \quad & |0\rangle \rightarrow -|1\rangle, \\ & |1\rangle \rightarrow |0\rangle, \qquad (2.3.3) \\ Z: \quad & |0\rangle \rightarrow |0\rangle, \\ & |1\rangle \rightarrow -|1\rangle. \qquad (2.3.4) \end{aligned}$$

Tyto transformace lze také vyjádřit pomocí matic jako

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

Transformace I je identita a „hradlo“ tu má triviální funkci, hradlo X je negace, hradlo Z představuje fázový posuv o π radiánů a hradlo $Y = ZX$ je kombinací

posledních dvou. Uvedená hradla se někdy znázorňují pomocí symbolů na obr. 2.1. Na schématu může proměnná x nabývat hodnot 0 a 1, přičemž součet $\oplus$ se definuje jako $0 \oplus 0 = 1 \oplus 1 = 0$ a $0 \oplus 1 = 1 \oplus 0 = 1$.



Obr. 2.1: Schéma jednobitových hradel I, X, Y a Z.

Hadamardovo hradlo

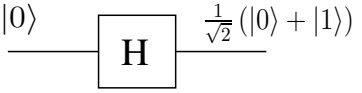
Tuto čtveřici jednobitových transformací je třeba doplnit o hradlo, připravující superpozici bázových stavů podle předpisu

$$\begin{aligned} H: \qquad |0\rangle &\rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\ |1\rangle &\rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right), \end{aligned} \tag{2.3.5}$$

což lze vyjádřit pomocí matice

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.3.6}$$

Toto je takzvaná *Hadamardova transformace*. Její schéma, spolu s působením na qubit ve stavu $|0\rangle$ je na obr. 2.2. Algebraicky můžeme Hadamardovu transformaci vyjádřit též jako $H|x\rangle = \frac{1}{\sqrt{2}}[(-1)^x|x\rangle + |x \oplus 1\rangle)$.



Obr. 2.2: Působení Hadamardovy transformace na nulový qubit.

Obzvláště důležitou aplikací této transformace je vytváření mnohabitových stavů, pokud operátor H působí na každý z N vynulovaných bitů:

$$\begin{aligned} (H \otimes H \otimes \ldots \otimes H)|00\ldots0\rangle &= \frac{1}{\sqrt{2^N}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \ldots \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{\sqrt{2^N}} \sum_{x=0}^{2^N-1} |x\rangle, \end{aligned} \tag{2.3.7}$$

kde $|x\rangle$ jsou N-bitové stavy a x probíhá všechny hodnoty čísel od 0 do $2^N - 1$ v binárním tvaru. Takovéto Hadamardově transformaci aplikované na Nqubitů se říká *Walshova,* případně *Walshova-Hadamardova* transformace. Aplikací Walshovy transformace připravujeme vstupní registr v superpozici všech možných čísel od 0 do $2^N - 1$, přičemž každé číslo tu vystupuje se stejnou vahou.

Fázový posuv

Zobecněním hradla Z na libovolné úhly je fázový posuv o hodnotu ϕ, který můžeme vyjádřit transformací

$$\begin{aligned} Z(\phi): \qquad |0\rangle &\rightarrow |0\rangle, \\ |1\rangle &\rightarrow e^{i\phi}|1\rangle, \end{aligned} \tag{2.3.8}$$

případně pomocí matice jako

$$Z(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

Rotace qubitu

Zobecněním hradel I a Y je rotace qubitu o úhel θ, daná maticí

$$U(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}. \tag{2.3.9}$$

Jak si můžeme ověřit, pro $\theta = 0$ dostáváme $U(0) = I$ a pro $\theta = \pi$ dostáváme $U(\pi) = Y$.

2.3.3 Dvoubitová hradla

Řízená negace CNOT

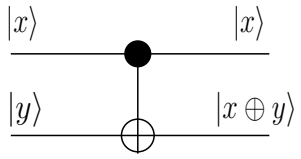
Aby mohl kvantový počítač fungovat, je nutné, aby mohl jeden bit ovlivňovat druhý. Operací, která patří k těm nejdůležitějším, je kontrolovaná (řízená) negace, zvaná CNOT (controlled not): podle toho, v jakém stavu je první qubit, se druhý qubit buď nezmění, nebo se neguje. Formálně ji můžeme popsat jako

$$\begin{aligned} \mathrm{CNOT}: \qquad |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle, \end{aligned} \tag{2.3.10}$$

případně pomocí matice

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.3.11}$$

Schéma hradla CNOT je na obrázku 2.3.



Obr. 2.3: Schéma hradla CNOT.

Řízený fázový posuv

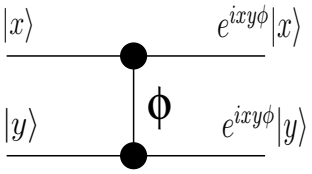
Jiným příkladem dvoubitového hradla je řízený fázový posuv: fáze stavu se změní pouze tehdy, když oba qubity budou nabývat hodnotu 1:

$$\begin{aligned} B(\phi): \quad & |00\rangle \rightarrow |00\rangle \\ & |01\rangle \rightarrow |01\rangle \\ & |10\rangle \rightarrow |10\rangle \\ & |11\rangle \rightarrow e^{i\phi}|11\rangle, \end{aligned} \tag{2.3.12}$$

případně pomocí matice

$$B(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}, \tag{2.3.13}$$

což odpovídá schématu na obr. 2.4.

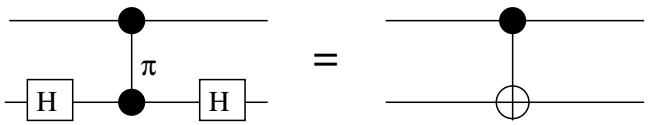


Obr. 2.4: Schéma řízeného fázového posuvu.

Pro kvantové počítání nejdůležitějším případem řízeného fázového posuvu je takový, který odpovídá hodnotě $\phi = \pi$, tedy matici

$$B(\pi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \tag{2.3.14}$$

Jak se můžeme přesvědčit, lze z tohoto hradla a pomocí jednobitových Hadamardových hradel sestavit hradlo CNOT, což odpovídá obr. 2.5.

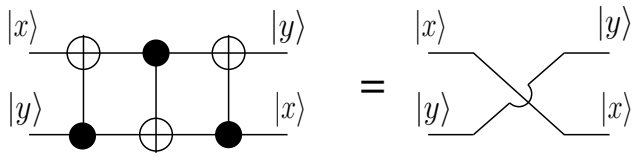


Obr. 2.5: Řízená negace sestavená ze dvou Hadamardových hradel a řízeného fázového posuvu.

2.3.4 Kombinace kvantových hradel

Hradlo SWAP

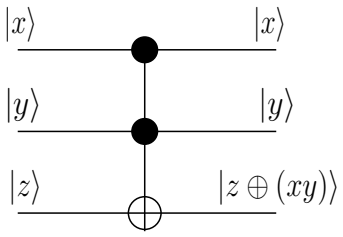
Řetězením jednobitových a dvoubitových kvantových hradel můžeme získávat další kvantové obvody—některé velmi jednoduché, jiné komplikovanější. Například ze tří hradel CNOT můžeme sestrojit hradlo SWAP, tedy výměnu bitu mezi dvěma registry, viz obr. 2.6.



Obr. 2.6: Výměna bitu mezi registry pomocí tří hradel CNOT.

Toffoliho hradlo

Toffoliho hradlo je tříbitové hradlo a patří k těm nejdůležitějším pro kvantové výpočty. Jedná se o negaci řízenou dvěma vstupními bity: právě tehdy, když oba řídící bity nabývají hodnotu 1, překlopí se hodnota řízeného bitu. Schématicky znázorňujeme Toffoliho hradlo jako na obrázku 2.7. Symbolicky můžeme zapsat funkci



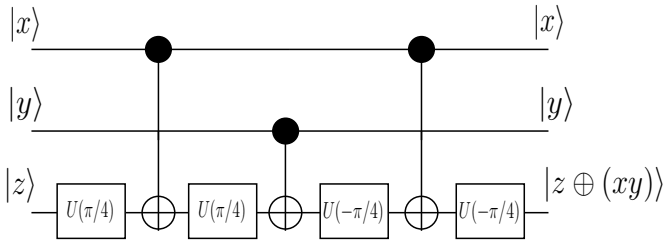
Obr. 2.7: Toffoliho hradlo překlápí bit z právě tehdy když oba bity x a y nabývají hodnoty 1.

Toffoliho hradla vztahem $(x,y,z) \rightarrow (x,y,z \otimes (xy))$. Pokud na jeden vstupní bit přivádíme pevně danou hodnotu, chová se Toffoliho hradlo jako dvoubitové hradlo, pokud na dva vstupní bity přivedeme pevné hodnoty, můžeme dostat hradla transformující

jediný bit. Přitom o jaké hradlo půjde, můžeme zvolit výběrem vstupních bitů:

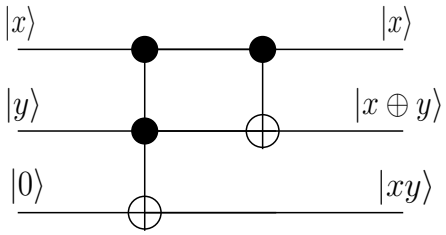
$$z \otimes (xy) = \begin{cases} xy & \text{pro } z = 0 \quad \text{(AND)} \\ x \oplus z & \text{pro } y = 1 \quad \text{(CNOT)} \\ \overline{x} & \text{pro } y = z = 1 \quad \text{(NOT)} \\ x & \text{pro } y = 1,\ z = 0 \quad \text{(FANOUT)} \end{cases} \tag{2.3.15}$$

Kvantové Toffoliho hradlo lze sestrojit pomocí řízených negací a jednobitových hradel, příklad je na obrázku 2.8.



Obr. 2.8: Toffoliho hradlo sestrojené pomocí tří hradel CNOT a čtyř hradel rotujících qubit o úhel $\pi/4$. (Ve skutečnosti přidává tento obvod v některých případech k řízenému bitu fázový posun, ten je však v případě potřeby snadno odstranitelný.)

Z Toffoliho hradel a z řízené negace lze sestavit například sčítací obvod, jak ukazuje obr. 2.9. V něm zůstává první bit x nezměněn, druhý bit nese na výstupu



Obr. 2.9: Kvantový sčítací obvod pro dva qubity sestavený z Toffoliho hradla a řízené negace.

hodnotu součtu bitů x a y modulo 2, $x \oplus y$, a třetí bit slouží jako přenos: jsou-li oba vstupní bity rovny jedné, je jejich součet (modulo 2) 0 a „jedna jde dál“. Řetězením dvoubitových sčítacích hradel pak můžeme sestavit hradlo sčítající libovolně velká vstupní čísla. Podobným způsobem pak můžeme konstruovat řadu dalších matematických operací.

Průvodce studiem

Poznamenejme, že pro sestavení univerzálního klasického počítače potřebujeme jako stavební kameny několik typů elementárních hradel, vždy však mezi nimi bude alespoň jedno tříbitové hradlo—např. Toffoliho. U kvantových obvodů však pro univerzální obvod vystačíme s jedno- a dvoubitovými hradly: díky možnosti vytvářet superpozice stavů z nich lze sestrojit Toffoliho hradlo, jak jsme ukázali na obr. 2.8. Něco takového u klasických obvodů není možné.

2.3.5 Kvantová Fourierova transformace

Mezi ostatními funkcemi vytvořenými z elementárních hradel patří k nejdůležitějším Fourierova transformace, která z N-bitového kvantového stavu $|x\rangle$ vytváří superpozici

$$F : |x\rangle \rightarrow \frac{1}{2^{N/2}} \sum_{y=0}^{2^N-1} \exp\left(i\frac{2\pi xy}{2^N}\right)|y\rangle. \tag{2.3.16}$$

Všimněme si, že tato transformace přeměňuje každý bázový stav (tedy každý stav odpovídající nějakému binárnímu číslu) v superpozici všech bázových stavů, zastoupených se stejnou vahou. Chová se tedy podobně jako Walshova-Hadamardova transformace, kromě triviálního případu $N = 1$ však působí odlišně. Konkrétně pro $N = 2$ dostáváme pro Fourierovu transformaci

$$\begin{aligned}
F : |00\rangle &\rightarrow \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right), \\
|01\rangle &\rightarrow \frac{1}{2}\left(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle\right), \\
|10\rangle &\rightarrow \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right), \\
|11\rangle &\rightarrow \frac{1}{2}\left(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle\right),
\end{aligned} \tag{2.3.17}$$

zatímco Walshova-Hadamardova transformace působí jako

$$\begin{aligned}
H : |00\rangle &\rightarrow \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right), \\
|01\rangle &\rightarrow \frac{1}{2}\left(|00\rangle - |01\rangle + |10\rangle - |11\rangle\right), \\
|10\rangle &\rightarrow \frac{1}{2}\left(|00\rangle + |01\rangle - |10\rangle - |11\rangle\right), \\
|11\rangle &\rightarrow \frac{1}{2}\left(|00\rangle - |01\rangle - |10\rangle + |11\rangle\right).
\end{aligned} \tag{2.3.18}$$

Průvodce studiem

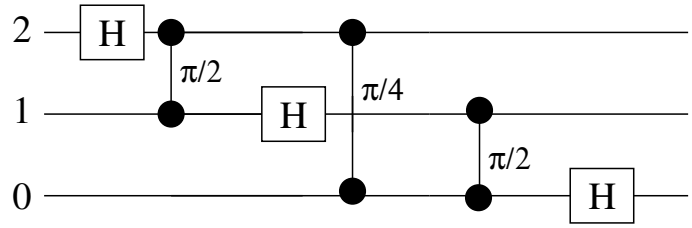
Ve fyzice hraje Fourierova transformace velmi důležitou roli, zjednodušeně můžeme říci, že nás informuje o tom, jak jsou v dané funkci (nebo signálu) zastoupeny různé frekvence. Rozklad světelného svazku hranolem do spektrálních komponent je svým způsobem fyzikální implementace Fourierovy transformace. V řadě případů je jednodušší pracovat „ve frekvenční oblasti“ spíše než přímo s časovým průběhem. Kvantová Fourierova transformace je v jistém ohledu analogií takovéhoto spektrálního rozkladu pro rozklad nějakého stavu do různých bází.

Vypišme ještě explicitně kvantovou Fourierovu transformaci pro tříbitové stavy:

F :

$$
\begin{aligned}
|000\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\right), \\
|001\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + e^{i\frac{\pi}{4}}|001\rangle + i|010\rangle + e^{i\frac{3\pi}{4}}|011\rangle - |100\rangle + e^{-i\frac{3\pi}{4}}|101\rangle - i|110\rangle + e^{-i\frac{\pi}{4}}|111\rangle\right), \\
|010\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + i|001\rangle - |010\rangle - i|011\rangle + |100\rangle + i|101\rangle - |110\rangle - i|111\rangle\right), \\
|011\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + e^{i\frac{3\pi}{4}}|001\rangle - i|010\rangle + e^{i\frac{\pi}{4}}|011\rangle - |100\rangle + e^{-i\frac{\pi}{4}}|101\rangle + i|110\rangle + e^{-i\frac{3\pi}{4}}|111\rangle\right), \\
|100\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle\right), \\
|101\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + e^{-i\frac{3\pi}{4}}|001\rangle + i|010\rangle + e^{i\frac{\pi}{4}}|011\rangle - |100\rangle + e^{i\frac{\pi}{4}}|101\rangle - i|110\rangle + e^{i\frac{3\pi}{4}}|111\rangle\right), \\
|110\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle - i|001\rangle - |010\rangle + i|011\rangle + |100\rangle - i|101\rangle - |110\rangle + i|111\rangle\right), \\
|111\rangle &\rightarrow \frac{1}{\sqrt{8}}\left(|000\rangle + e^{i\frac{-\pi}{4}}|001\rangle - i|010\rangle + e^{-i\frac{3\pi}{4}}|011\rangle - |100\rangle + e^{-i\frac{3\pi}{4}}|101\rangle + i|110\rangle + e^{i\frac{\pi}{4}}|111\rangle\right).
\end{aligned}
\tag{2.3.19}
$$

Hradlo vytvářející takovouto transformaci lze sestrojit z jednobitových Hadamardových hradel a z dvoubitových hradel řízeného fázového posuvu o úhly $\pi/2$ a $\pi/4$, jak je vidět z obrázku 2.10. Pro sestrojení vícebitové Fourierovy transformace bychom



Obr. 2.10: Kvantový obvod vytvářející Fourierovu transformaci na třech vstupních bitech. Konečný výsledek je třeba ještě bitově invertovat (nebo bity číst v opačném pořadí), což je triviální operace.

postupovali induktivně: pro přidávání dalšího bitu bychom napojili příslušný registr hradlem řízeného fázového posuvu na všechny předchozí registry a na závěr připojili hradlo Hadamardovy transformace. Přitom fázový posuv mezi k-tým a j-tým bitem je $\phi = \pi/2^{|k-j|}$.

Shrnutí

Při zpracování kvantové informace se musí brát v potaz reverzibilita kvantových transformací. Některé operace, které běžně provádějí naše počítače, jsou ireverzibilní a při kvantovém zpracování informace je třeba je vhodně modifikovat. Kvantová hradla provádějí transformace stavů qubitů. Nejjednodušší hradla transformují jednobitové stavy, u vícebitových hradel hodnoty jednoho či více bitů ovlivňují jiné bity. K nejdůležitějším jednobitovým hradlům patří ty, které realizují fázový posuv, rotace a Hadamardovu transformaci. Nejdůležitější dvoubitová hradla realizují řízenou negaci a řízený fázový posuv. Kombinací jednobitových a dvoubitových hradel

lze získat složitější kvantové obvody. Toffoliho hradlo, které může posloužit jako základní kámen pro sčítací obvody, lze sestrojit kombinací hradel řízené negace a jednobitových rotací. Ze sčítacích obvodů pak můžeme, podobně jako v klasické informatice sestavit obvod realizující komplikovanější funkce. Kromě toho patří k nejdůležitějším mnohobitovým obvodům ten, kterým se uskutečňuje kvantová Fourierova transformace.

Pojmy k zapamatování

- Reverzibilita, operace FANOUT, mazání informace, Landauerův princip,
- jednobitová hradla: fázový posuv, rotace, Hadamardova transformace,
- Walshova-Hadamardova transformace,
- dvoubitová hradla: řízená negace a řízený fázový posuv,
- vícebitová hradla: Toffoliho hradlo, sčítací obvod, kvantová Fourierova transformace

Kontrolní otázky

1. *Jak vypadají matice popisující Hadamardovu transformaci, fázový posuv o $\pi/4$ a negaci jednoho qubitu?*
2. *Jak vypadají matice popisující dvoubitovou Walshovu-Hadamardovu transformaci, řízenou negaci, řízený fázový posuv a Fourierovu transformaci?*

Úkoly k textu

1. Uvažujte dvoubitové hradlo řízeného fázového posuvu $B(\pi)$. Na jeho vstup přivedeme stav $\Psi^- = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$. Jak bude vypadat výstupní stav? Jak by se změnil tímto hradlem stav stav $\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?
2. Uvažujme dvoubitové hradlo, které je sestavené takto: první bit projde Hadamardovou transformací, následuje řízený fázový posuv $B(\pi)$ a poté druhý bit projde Hadamardovou transformací. Jak se změní vstupní stav $\Psi^- = = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$?

Řešení

1. $\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \rightarrow \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle)$ (stav Ψ^- se nezmění), $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ (stav Φ^+ se změní na Φ^-).
2. Výsledný stav bude $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |1\rangle$.

2.4 Shorův algoritmus: nalezení periody diskrétní funkce

Peter W. Shor z AT&T laboratoří, objevitel kvantového algoritmu pro faktorizaci čísel.

Jsme-li schopni pomocí jednoduchých kvantových hradel realizovat výpočet nějaké funkce (například pomocí sčítacích obvodů a podobně) a pokud máme sestro-

jený obvod pro kvantovou Fourierovu transformaci, můžeme tímto zařízením zjistit, zda je zadaná funkce periodická a jakou má periodu. Postup je následující. Nejprve připravíme N vstupních bitů v superpozici všech stavů,

$$|0\rangle \to \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle. \tag{2.4.1}$$

Toho nejsnáze dosáhneme Walshovou-Hadamardovou transformací (viz rovnice (2.3.7)), tedy použitím jednoho Hadamardova hradla pro každý vstupní, původně vynulovaný bit. Poté aplikujeme obvod „počítající" funkci f, $|x;0\rangle \to |x;f(x)\rangle$:

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x;0\rangle \to \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x;f(x)\rangle. \tag{2.4.2}$$

Protože jsme měli na vstupu superpozici všech 2^N bázových stavů, je jediným průchodem přes posloupnost hradel vypočítána funkce f pro všech 2^N hodnot jejího argumentu. Toto je krok, který nám klasické počítače neumožní.

Nyní na vstupní bity x aplikujeme kvantovou Fourierovu transformaci (viz odst. 2.3.5). Stav se tak změní

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x;f(x)\rangle \to \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} \sum_{y=0}^{2^N-1} \exp\left(i\frac{2\pi xy}{2^N}\right) |y;f(x)\rangle. \tag{2.4.3}$$

Předpokládejme nyní, že funkce f má periodu r, tedy $f(x+r) = f(x)$. Tím pádem můžeme stav $|f(x)\rangle$ „vytknout" a výraz $\sum_{x=0}^{2^N-1} \exp\left(i\frac{2\pi xy}{2^N}\right) |f(x)\rangle$ psát jako

$$\begin{aligned} \sum_{x=0}^{2^N-1} \exp\left(i\frac{2\pi xy}{2^N}\right) |f(x)\rangle &= \sum_{x=0}^{r-1} |f(x)\rangle \sum_n \exp\left(i\frac{2\pi(x+nr)y}{2^N}\right) \\ &= \sum_{x=0}^{r-1} \exp\left(i\frac{2\pi xy}{2^N}\right) |f(x)\rangle \sum_n \exp\left(i\frac{2\pi nry}{2^N}\right) \end{aligned} \tag{2.4.4}$$

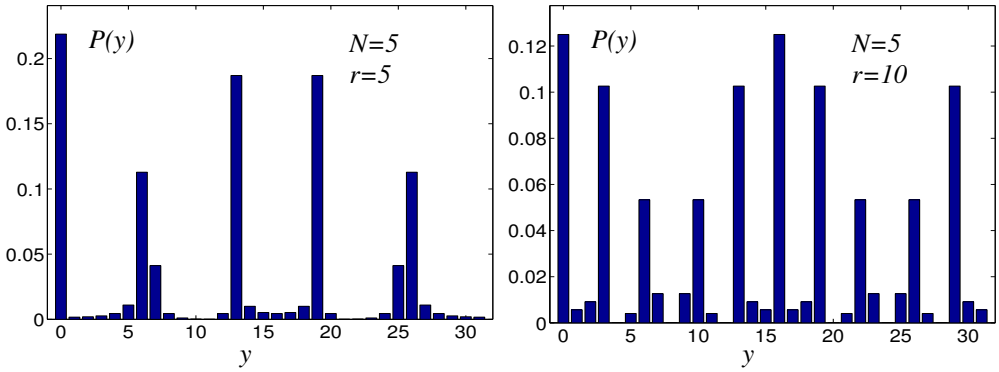
kde sčítání přes n probíhá od 0 do $[(2^N - 1 - x)/r]$ a výraz $[z]$ znamená celou část čísla z. Výsledný stav z (2.4.3) lze tedy zapsat ve tvaru

$$\frac{1}{2^{N/2}} \sum_{y=0}^{2^N-1} |y\rangle \sum_{x=0}^{r-1} \exp\left(i\frac{2\pi xy}{2^N}\right) |f(x)\rangle \sum_n \exp\left(i\frac{2\pi nry}{2^N}\right). \tag{2.4.5}$$

Suma na konci tohoto výrazu nabývá velkých hodnot pouze tehdy, když je příslušná exponenciála přibližně rovna 1 nezávisle na n, tedy pokud y nabývá hodnot blízkých

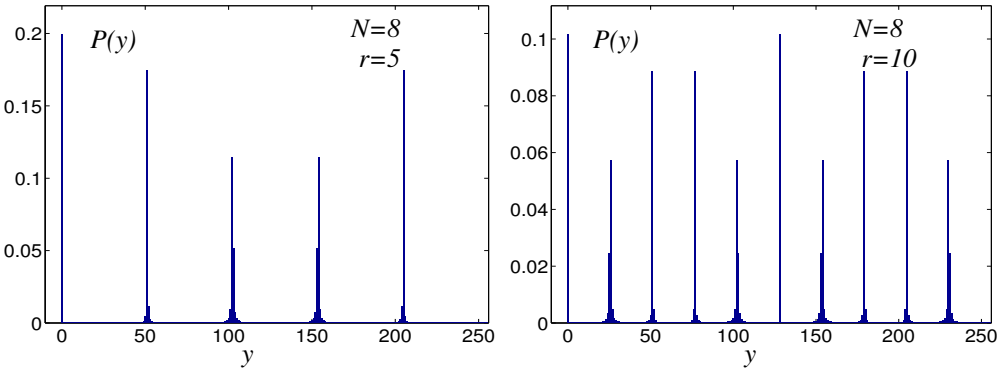
$$y \approx \frac{2^N}{r} m, \tag{2.4.6}$$

kde m je nějaké celé číslo. Pro jiné hodnoty mají příspěvky $\exp\left(i\frac{2\pi nry}{2^N}\right)$ pro různé hodnoty n různé fáze a interferencí se buď úplně nebo částečně vyruší.



Obr. 2.11: Pravděpodobnosti detekce pětibitového ($N = 5$) stavu $|y\rangle$ v případě, že funkce $f(x)$ má periodu $r = 5$ a $r = 10$.

Pokud nyní provedeme měření na vstupním registru, výsledkem bude nějaká hodnota y z intervalu mezi 0 a $2^N - 1$. Ovšem hodnoty y, pro které se příspěvky exponenciál v sumě v (2.4.5) vyruší, nastanou s téměř nulovou pravděpodobností. S největší pravděpodobností naměříme některou z hodnot y, pro kterou je splněn vztah (2.4.6). Průběh těchto pravděpodobností je ilustrován na obr. 2.11 a 2.12. Z naměřené hodnoty y a vztahu (2.4.6) pak můžeme tipovat jaká je perioda r; dosazením několika málo argumentů do funkce f si pak můžeme správnost tipu ověřit.



Obr. 2.12: Pravděpodobnosti detekce osmibitového ($N = 8$) stavu $|y\rangle$ v případě, že funkce $f(x)$ má periodu $r = 5$ a $r = 10$.

Průvodce studiem

Je dobré si uvědomit několik skutečností:

1. Kvantové počítání je „pravděpodobnostní“: výsledek měření je náhodný, i tak nám však poskytuje cennou informaci. Pokud bychom se snažili zjistit periodu funkce f na klasickém počítači, museli bychom funkční hodnotu spočítat mnohokrát, řádově $\sim 2^N$-krát. Při kvantovém počítání stačí několik málo dosazení do funkce realizované pomocí kvantových hradel a poté dosazení vytipovaných hodnot do funkce počítané na klasickém počítači.

2. Je zajímavé, že poté, co jsme kvantově napočítali hodnoty funkce f, $\sum_x |x,0\rangle \rightarrow \sum_x |x,f(x)\rangle$, již registr s funkčními hodnotami $|f(x)\rangle$ nepotřebujeme a můžeme jej vymazat. Vše zajímavé se nyní odehrává již jen v „nedotčeném“ registru argumentů $|x\rangle$! To je důsledek použití superpozice bázových stavů na vstupu.

Shrnutí

Pro nalezení periody nějaké diskrétní funkce nejprve připravíme superpozici stavů odpovídajících všem vstupním argumentům, pak tento stav použijeme jako argument pro výpočet funkce f a poté provedeme výpočet kvantové Fourierovy transformace na registru agrumentů. Nakonec změříme hodnotu v registru argumentů (zatímco stav v registru funkčních hodnot můžeme zcela ignorovat) a z ní se pokusíme vytipovat hledanou periodu. Správnost tipu pak ověříme přímým dosazením do funkce. Protože těchto úkonů je mnohem méně, než kolik bychom museli učinit při $\sim 2^N$-násobném dosazování do funkce, představuje tento algoritmus podstatnou úsporu při hledání periody.

Pojmy k zapamatování

- registr argumentů,
- registr funkčních hodnot,
- kvantová Fourierova transformace,
- měření stavu

2.5 Faktorizace čísel

Předešlé výsledky mají velký význam pro efektivní faktorizaci velkých čísel. To by nám umožnilo efektivně luštit tzv RSA kryptografický kód, (viz příloha B). Předpokládejme, že hodláme faktorizovat číslo $\mathcal{N}$. Bude nám stačit nalézt jediný faktor, což redukuje úlohu na jednodušší případ. Můžeme postupovat následujícím způsobem:

1. Zvolíme číslo z a ověříme u něj, že je nesoudělné s $\mathcal{N}$. To lze velmi snadno tzv. Euklidovým algoritmem. Pokud je číslo z soudělné s $\mathcal{N}$, máme první faktor čísla $\mathcal{N}$—největší společný dělitel $\mathcal{N}$ a z.
2. Na kvantovém obvodu sestrojíme funkci $f(x) = z^x (\mathrm{mod}\mathcal{N})$. Tuto funkci si můžeme zapsat jako posloupnost

x	0	1	2	…	$r-1$	r	$r+1$	$r+2$	…	$2r$	$2r+1$	…
$f(x)$	1	z	z^2	…	z^{r-1}	z^r	z^{r+1}	z^{r+2}	…	z^{2r}	z^{2r+1}	…
$f(x)$	1	z	z^2	…	z^{r-1}	1	z	z^2	…	1	z	…

   Druhý řádek je tu psán jako posloupnost mocnin, které je však třeba brát modulo $\mathcal{N}$. Ve třetím řádku jsou již zapsány funkční hodnoty tak, že je zřejmé, že funkce je periodická s periodou r: číslo r je prvním netriviálním exponentem, pro který platí $z^r (\mathrm{mod}\mathcal{N}) = 1$.

3. Pomocí kvantového algoritmu (viz předchozí kapitola) nalezneme hodnotu periody r. Pokud je toto číslo sudé, pokračujeme k bodu 4, pokud není, vrátíme se k bodu 1 a volíme novou hodnotu z. (Při každém opakování máme 50% šanci dostat sudý výsledek, takže takovýchto opakování nebude mnoho.)
4. Po nalezení sudého r můžeme vztah $z^r (\mathrm{mod} \mathcal{N}) = 1$ přepsat ve tvaru

$$\begin{aligned} \left(z^{r/2}\right)^2 - 1 &= 0 (\mathrm{mod} \mathcal{N}), \\ \left(z^{r/2}+1\right)\left(z^{r/2}-1\right) &= 0 (\mathrm{mod} \mathcal{N}). \end{aligned} \tag{2.5.1}$$

   To znamená, že součin na levé straně rovnice (2.5.1) je násobkem čísla $\mathcal{N}$ a tudíž buď $\left(z^{r/2}+1\right)$ nebo $\left(z^{r/2}-1\right)$ (případně obě čísla) má společného dělitele s $\mathcal{N}$.
5. Nakonec Euklidovým nalezneme společného dělitele $\left(z^{r/2}+1\right)$ a $\mathcal{N}$, případně společného dělitele $\left(z^{r/2}-1\right)$ a $\mathcal{N}$. Toto číslo tedy řeší náš problém.

Průvodce studiem

V roce 1977 byla vypsána cena 100 dolarů pro toho, kdo dokáže faktorizovat číslo $N = 114\,381\,625\,757\,888\,867\,669\,235\,779\,976\,146\,612\,010\,218\,296\,721\,242\,362\,562\,561\,842\,935\,706\,935\,245\,733\,897\,830\,597\,123\,563\,958\,705\,058\,989\,075\,147\,599\,290\,026\,879\,543\,541$. Řešení přišlo až v roce 1994, kdy 600-členný tým, který spojil síly svých výpočetních prostředků ohlásil výsledek: $N = pq$, kde $q = 3\,490\,529\,510\,847\,650\,949\,147\,849\,619\,903\,898\,133\,417\,764\,638\,493\,387\,843\,990\,820\,577$ a $p = 32\,769\,132\,993\,266\,709\,549\,961\,988\,190\,834\,461\,413\,177\,642\,967\,992\,942\,539\,798\,288\,533$.

Pro ilustraci si zkusme tímto postupem faktorizovat číslo 15. Jako číslo z si zvolme třeba 7. Jako posloupnost funkčních hodnot $f(x) = 7^x (\mathrm{mod}\ 15)$ pak dostáváme

x	0	1	2	3	4	5	6	7	8	9	10	...
$f(x)$	1	7	4	13	1	7	4	13	1	7	4	...

Je vidět, že perioda funkce $f(x)$ je $r = 4$, což je sudé číslo. Můžeme tedy psát

$$\begin{aligned} \left(7^{4/2}+1\right)\left(7^{4/2}-1\right) &= 0 (\mathrm{mod}\ 15), \\ 50 \times 48 &= 0 (\mathrm{mod}\ 15). \end{aligned} \tag{2.5.2}$$

Tedy buď 50 nebo 48 musí mít s číslem 15 společného dělitele. Jak vidíme (nebo ověříme Euklidovým algoritmem), největší společný dělitel čísel 50 a 15 je 5 a tedy 5 je dělitelem čísla 15.

Zkusme si ještě faktorizovat číslo 391. Za číslo z si zvolme například 4. Pro posloupnost funkčních hodnot $f(x) = 4^x (\mathrm{mod}\ 391)$ je pak již výhodné využít počítače. Dostáváme pak

x	0	1	2	3	4	5	6	...	42	43	44	45	...
$f(x)$	1	4	16	64	256	242	186	...	220	98	1	4	...

Perioda funkce $f(x)$ je tedy $r = 44$, což je opět sudé číslo. Můžeme tedy psát

$$\begin{aligned} \left(4^{22}+1\right)\left(4^{22}-1\right) &= 0(\text{mod } 391), \\ 17\ 592\ 186\ 044\ 417 \times 17\ 592\ 186\ 044\ 415 &= 0(\text{mod } 391). \end{aligned} \tag{2.5.3}$$

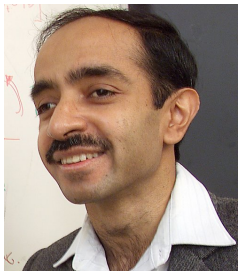
Euklidovým algoritmem zjistíme, že čísla 17 592 186 044 417 a 391 jsou nesoudělná, kdežto čísla 17 592 186 044 415 a 391 mají společného dělitele 23. Číslo 23 je tedy jedním z hledaných dělitelů a číslo 391 lze faktorizovat jako $391 = 23 \times 17$.

Shrnutí

Efektivní faktorizace velkých čísel je podstatná pro luštění kryptografického RSA kódu. Pro nalezení dělitelů čísla $\mathcal{N}$ zvolíme s ním nesoudělné číslo z a nalezneme periodu funkce $f(x) = z^x(\text{mod}\mathcal{N})$ jako nějaké sudé číslo r. Kvantový počítač je v tomto kroku mnohem efektivnější než klasické počítače. Z periody r pak snadno zjistíme alespoň jednoho dělitele čísla $\mathcal{N}$.

2.6 Groverův algoritmus: vyhledávání v neuspořádaných seznamech

2.6.1 Popis algoritmu



Lov Grover z Bellových laboratoří, autor kvantového vyhledávacího algoritmu.

Groverův algoritmus pomáhá vyhledat v nesetříděném seznamu o délce $\mathcal{N}$ číslo x, které splňuje předem zadanou podmínku. Předpokládejme, že N je číslo splňující $2^N \geqq \mathcal{N}$ a nechť U_p je kvantový obvod, který dává jako výstup odpověď, zda vstup splňuje naši podmínku,

$$U_p : |x;0\rangle \rightarrow |x,P(x)\rangle, \tag{2.6.1}$$

kde

$$P(x) = \begin{cases} 1 & \text{pokud } x \text{ splňuje podmínku} \\ 0 & \text{pokud } x \text{ nesplňuje podmínku} \end{cases} \tag{2.6.2}$$

Registr pro funkční hodnoty tedy může být pouze jednobitový. Kvantové vyhledávání probíhá takto:

1. Vstupní registr připravíme v superpozici všech bázových stavů (například z vynulovaného registru pomocí Walshovy-Hadamardovy transformace),

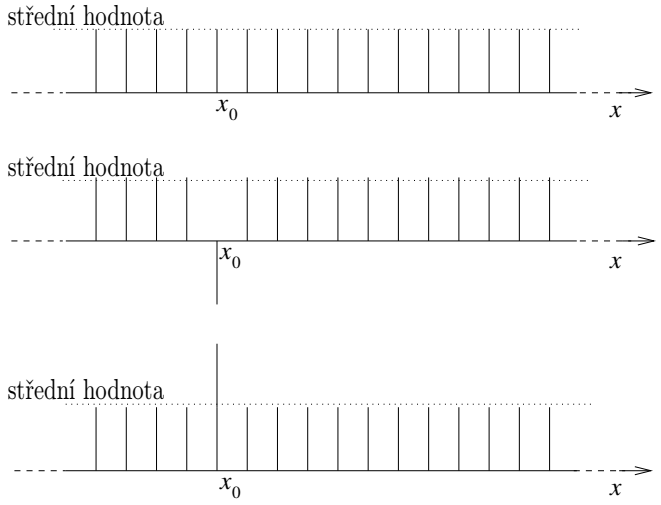
$$|0\rangle \rightarrow \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x\rangle. \tag{2.6.3}$$

2. Na takto připravený vstupní stav aplikujeme kvantový obvod U_p, získáme tak stav

$$\frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} |x;P(x)\rangle. \tag{2.6.4}$$

Znamená to, že pokud je na výstupu registru pro funkční hodnotu jednička, musí být v registru pro argument funkce hodnota, která splňuje naši podmínku, nazvěme ji x_0. Pokud bychom tedy provedli měření na registru pro funkční hodnotu a získali hodnotu 1, měření na registru pro x by nám dalo hledané číslo x_0. Problém však je, že výsledek 1 na registru pro funkční hodnotu získáme s mizivě malou pravděpodobností $\sim 1/2^N$. Groverův trik spočívá v transformaci kvantového stavu z rovnice(2.6.4) tak, aby vzrostla velikost amplitudy pravděpodobnosti pro stav $|x_0; 1\rangle$. To se děje následujícím způsobem:

3. Provedeme transformaci stavu, která změní amplitudu a_j na $-a_j$ u těch bázových stavů $|x_j\rangle$, pro které $P(x_j) = 1$.
4. Transformujeme stav tak, že se amplitudy pravděpodobnosti „překlápí“ kolem střední hodnoty amplitud. Tyto dva kroky jsou znázorněny na obr. 2.13.



Obr. 2.13: Překlápění amplitud v Groverově vyhledávacím algoritmu.

5. Posloupnost operací - aplikace operátoru $U_p \rightarrow$ překlopení amplitudy a_j na $-a_j$ $\rightarrow$ překlopení amplitud kolem jejich střední hodnoty opakujeme $\frac{\pi}{4}2^{N/2}$-krát.
6. V registru pro argumenty funkce provedeme měření a odečteme výsledek.

2.6.2 Překlápění kolem střední hodnoty amplitud

Abychom mohli aplikovat Groverův algoritmus, musíme dokázat pomocí základních kvantových hradel sestavit obvody překlápějící amplitudy pravděpodobností. Pro překlápění amplitud kolem jejich střední hodnoty potřebujeme zajistit transformaci

$$\sum_{k=0}^{2^N-1} a_k|x_k\rangle \rightarrow \sum_{k=0}^{2^N-1} (2A - a_k)|x_k\rangle, \tag{2.6.5}$$

kde A označuje střední hodnotu amplitud a_k. Tato operace odpovídá matici $2^N \times 2^N$

$$D = \begin{pmatrix} 2^{1-N}-1 & 2^{1-N} & \dots & 2^{1-N} \\ 2^{1-N} & 2^{1-N}-1 & \dots & 2^{1-N} \\ \dots & \dots & \dots & \dots \\ 2^{1-N} & 2^{1-N} & \dots & 2^{1-N}-1 \end{pmatrix}. \tag{2.6.6}$$

Protože platí, že $DD^\dagger = I$, je matice D unitární a může odpovídat nějakému vývoji kvantových stavů. Naším úkolem je nyní ukázat, že tuto matici lze efektivně implementovat pomocí nepříliš vysokého počtu elementárních hradel (jejich počet by měl být úměrný N a ne dimenzi matice 2^N).

Grover ukázal, že matici D lze zapsat ve tvaru $D = WRW$, kde W je Walshova-Hadamardova transformace a R je fázový posuv o π u jediného bitu,

$$R = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & -1 \end{pmatrix}. \tag{2.6.7}$$

Je užitečné si napsat matici R jako $R = R' - I$, kde

$$R' = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}. \tag{2.6.8}$$

Protože WRW je $W(R'-I)W = WR'W - I$ a jak si můžeme ověřit, platí

$$WR'W = \begin{pmatrix} 2^{1-N} & 2^{1-N} & \dots & 2^{1-N} \\ 2^{1-N} & 2^{1-N} & \dots & 2^{1-N} \\ \dots & \dots & \dots & \dots \\ 2^{1-N} & 2^{1-N} & \dots & 2^{1-N} \end{pmatrix}. \tag{2.6.9}$$

Tím pádem je $WR'W - I = D$. Překlápění amplitud kolem střední hodnoty lze tedy dosáhnout aplikací dvou Walshových transformací a fázovým posuvem u jednoho bitu.

2.6.3 Překlopení znaménka amplitudy

Abychom dokázali překlopit znaménko u té amplitudy, která přísluší stavu splňujícímu podmínku $P(x) = 1$, uvažujeme operátor U_p působící obecně $U_p : |x; b\rangle \rightarrow |x; b \oplus P(x)\rangle$. Aplikujeme nyní U_p na superpozici $|\psi\rangle = \frac{1}{2^{N/2}} \sum_{x=0}^{2^N-1} \alpha_x |x\rangle$ a qubit b ve stavu $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Rozdělme nyní množinu všech x na dvě podmnožiny: $X_0 = \{x|P(x) = 0\}$ a $X_1 = \{x|P(x) = 1\}$ a nechme působit operátor U_p na $|\psi; b\rangle$:

$$U_p|\psi; b\rangle = \frac{1}{2^{(N+1)/2}} U_p \left(\sum_{x\in X_0} \alpha_x |x,0\rangle + \sum_{x\in X_1} \alpha_x |x,0\rangle - \sum_{x\in X_0} \alpha_x |x,1\rangle - \sum_{x\in X_1} \alpha_x |x,1\rangle \right)$$

$$
\begin{aligned}
&= \frac{1}{2^{(N+1)/2}} \left(\sum_{x \in X_0} \alpha_x |x,0 \oplus 0\rangle + \sum_{x \in X_1} \alpha_x |x,0 \oplus 1\rangle - \sum_{x \in X_0} \alpha_x |x,1 \oplus 0\rangle - \sum_{x \in X_1} \alpha_x |x,1 \oplus 1\rangle \right) \\
&= \frac{1}{2^{(N+1)/2}} \left(\sum_{x \in X_0} \alpha_x |x,0\rangle + \sum_{x \in X_1} \alpha_x |x,1\rangle - \sum_{x \in X_0} \alpha_x |x,1\rangle - \sum_{x \in X_1} \alpha_x |x,0\rangle \right) \\
&= \frac{1}{2^{N/2}} \left(\sum_{x \in X_0} \alpha_x |x\rangle - \sum_{x \in X_0} \alpha_x |x,\rangle \right) |b\rangle. \qquad (2.6.10)
\end{aligned}
$$

Vidíme, že stav $|b\rangle$ zůstane nezměněn, ale v registru pro argument funkce dojde k překlopení znaménka u těch amplitud, pro které je $P(x) = 1$.

Shrnutí

Groverův algoritmus umožňuje efektivně zjistit, který argument x splňuje podmínku $P(x) = 1$. Pokud tímto argumentem může být libovolné číslo z 2^N, museli bychom při klasickém vyhledávání dosazovat do funkčního vztahu průměrně 2^{N-1}-krát. Groverův algoritmus vyžaduje pouze $\frac{\pi}{4}2^{N/2}$-násobné dosazení. Tento algoritmus je možné implementovat pomocí kombinací Walshových-Hadamardových transformací, jednobitových fázových posuvů a kvantového obvodu realizujícího testování podmínky $P(x)$.

Pojmy k zapamatování

- Překlápění amplitud kolem střední hodnoty,
- překlápění znaménka amplitudy hledaného stavu,
- efektivní vyhledávání.

2.7 Kvantová kryptografie

Charles Bennett z IBM, jeden z objevitelů kvantové kryptografie.

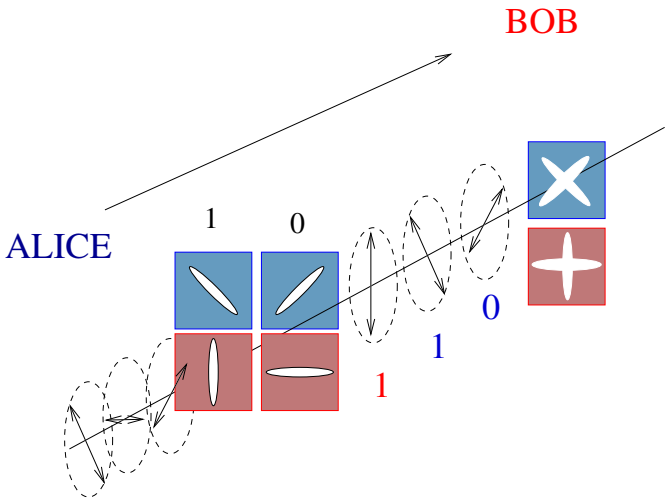
Ačkoliv by kvantové počítače mohly znamenat určitou hrozbu pro naše soukromí, přináší jiné odvětví kvantové informatiky naopak možnost, jak dosáhnout bezpečného přenosu utajovaných zpráv. Využívá se tu principiální nemožnosti spolehlivě rozlišovat mezi neortogonálními kvantovými stavy a toho, že měření kvantový stav obecně narušuje. Základem kvantové kryptografie je distribuce tajného klíče mezi dvěma vzdálenými partnery tak, aby nikdo jiný klíč nemohl znát. Jakmile dvě strany klíč znají (je to v podstatě náhodná posloupnost nul a jedniček), stačí jej přičíst k binárně kódované zprávě. Takto zašifrovaná zpráva se pak vnějšímu pozorovateli jeví jako zcela náhodná posloupnost nul a jedniček bez jakýchkoliv vnitřních korelací, které by se daly využít k získání nějaké užitečné informace.

Průvodce studiem

Sdílejí-li dvě strany zcela náhodnou, tajnou posloupnost čísel, může ji vysílající strana přičíst ke své zprávě (zapsané pomocí číslic) a přijímající strana pak

od šifrované zprávy odečíst. Tímto způsobem lze předat tajnou zprávu, aniž by z ní někdo nepovolaný mohl zjistit cokoliv rozumného. Problém je, že takovýto klíč můžeme použít pouze jednou: při opakovaném použití lze v předávaných zprávách najít korelace, které by mohly vést k „prosáknutí“ citlivých informací ven. Možnost předávat tajný klíč jako velmi dlouhou posloupnost náhodných čísel je tedy zcela podstatná.

2.7.1 Distribuce klíče



Obr. 2.14: Schéma kvantové kryptografie, protokol BB84.

Jak se takovýto bezpečný klíč distribuuje? Uveďme si pro příklad princip kódu nazvaného BB84 podle jeho autorů Charlese Bennetta a Gilese Brassarda a roku, ve kterém byl publikován. Dvě komunikující strany, zvané tradičně Alice a Bob chtějí sdílet tajný klíč, viz obr. 2.14. Alice posílá Bobovi posloupnost qubitů, které kódují bity ve dvou možných bázích. Pro jednoduchost si představme různé lineární polarizace fotonů: ty mohou být orientovány buď vodorovně (stav $|\leftrightarrow\rangle$, což bude označovat hodnotu bitu 0) nebo svisle (stav $|\updownarrow\rangle$, což označuje hodnotu bitu 1). Toto odpovídá „červené“ bázi „$\oplus$“ na obr. 2.14. Alice však využije i kódování v jiné bázi: foton může být lineárně polarizován ve směru +45 stupňů (stav $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle + |\leftrightarrow\rangle)$ což bude znamenat bit 0) nebo ve směru −45 stupňů (stav $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\updownarrow\rangle - |\leftrightarrow\rangle)$, což znamená hodnotu bitu 1). Toto odpovídá „modré“ bázi „$\otimes$“ na obr. 2.14. Alice náhodně přepíná báze, ve kterých bity kóduje a také hodnoty bitů jsou zcela náhodné. Fotony zaslané Bobovi tedy mohou tvořit posloupnost jako:

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...
$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	...
1	1	1	0	0	1	0	0	0	1	1	0	...

Bob měří polarizace fotonů, které k němu přichází. Protože však neví, v jaké bázi

Alice kódovala, náhodně přepíná svůj detektor tak, aby rozlišoval buď mezi horizontální a vertikální polarizací (báze „$\oplus$“), nebo mezi polarizací ve směru $+45$ stupňů a -45 stupňů (báze „$\otimes$“). Připomeňme, že podle zákonů kvantové fyziky je výsledek měření zcela náhodný, pokud Bob měří v jiné bázi, než v jaké Alice kódovala svůj bit. Jestliže tedy Alice poslala foton $|\nwarrow\rangle$ a Bob měřil v bázi „$\oplus$“, dostane se stejnou pravděpodobností výsledek $|\updownarrow\rangle$ jako $|\leftrightarrow\rangle$. Předpokládejme, že posloupnost bází, ve kterých Bob měřil je (ve vztahu k výše uvedeným Aliciným stavům)

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...
$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\updownarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	...
1	1	1	0	0	1	0	0	0	1	1	0	...
$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	...

Bobovy naměřené hodnoty pak mohou být například

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...
$\|\nwarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nwarrow\rangle$	$\|\updownarrow\rangle$	$\|\updownarrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\leftrightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$	$\|\leftrightarrow\rangle$	...
1	1	0	1	1	1	1	0	0	0	1	0	...

Ve druhém, šestém, devátém, jedenáctém a dvanáctém případě měl Bob stejnou bázi jako Alice a musí tedy získat stejnou polarizaci, jakou Alice posílala. V ostatních případech je naproti tomu výsledek Bobova měření zcela náhodný. Bob nyní Alici sdělí, jaké báze pro svá měření používal (ne však výsledky měření) a Alice mu odpoví, ve kterých případech použila stejnou bázi jako Bob. Komunikující strany nyní vědí, kdy mohou očekávat stejné polarizace fotonů, přiřadí jim odpovídající hodnoty bitů a ostatní data zahodí. Pro náš příklad jsou tedy ponechané polarizace ty, které odpovídají fotonům číslo 2, 6, 9, 11 a 12, tedy $|\nwarrow\rangle$, $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nwarrow\rangle$ a $|\leftrightarrow\rangle$, což představuje hodnoty bitů „1,1,0,1,0“. Tato čísla mohou představovat začátek klíče, sdíleného Alicí a Bobem.

Giles Brassard z univerzity v Montrealu, jeden z objevitelů kvantové kryptografie.

2.7.2 Odhalení narušitele

Co když se však někdo pokoušel tuto komunikaci odposlechnout a získat nějakou znalost o klíči? Nějaký narušitel (nebo narušitelka - eavesdropper, většinou pojmenovaná Eva) zachytává fotony vyslané Alicí, proměří je a pošle Bobovi. Řekněme, že Eva zná všechny detaily komunikace mezi Alicí a Bobem a ví, že fotony mohou přilétat s některou ze čtyř lineárních polarizací $|\updownarrow\rangle$, $|\leftrightarrow\rangle$, $|\nwarrow\rangle$ a $|\nearrow\rangle$. Nemůže však vědět, pro kterou polarizaci se rozhodla Alice v každém jednotlivém případě. Co kdyby se Eva rozhodla detekovat polarizace a náhodně při tom střídat báze? Představme si například Evinu posloupnost bází

1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...
$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	...

Její naměřené hodnoty mohou být například

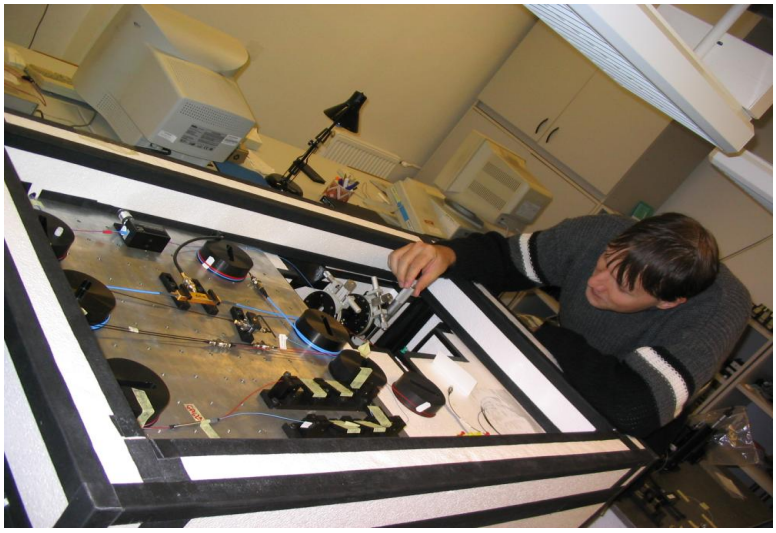
1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	...
$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	...
$\lvert\nearrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\updownarrow\rangle$	$\lvert\leftrightarrow\rangle$	...

Ve třetím, šestém, sedmém, osmém, desátém a dvanáctém případě to byla stejná báze jako u Alice a musí tedy získat stejnou polarizaci, ostatní hodnoty jsou náhodné. Fotony s polarizacemi odpovídajícími Eviným datům nyní putují k Bobovi. U šestého a dvanáctého fotonu mají Alice, Eva i Bob stejnou bázi, takže budou mít i stejné naměřené hodnoty polarizace. U druhého, devátého a jedenáctého fotonu jsou báze Alice a Boba stejné, Eva má však báze odlišné. Foton, který přijde Bobovi, bude dávat zcela náhodnou hodnotu polarizace. Ač měli Bob a Alice stejné báze, mohou u daného fotonu pozorovat různé polarizace - a to je podezřelé! Nesoulad mezi vysílanými a naměřenými hodnotami v případech, kdy Alice i Bob měli stejné báze je znakem toho, že narušitel mohl být na drátě. V praxi to znamená, že komunikující strany obětují část dat (řekněme tisíc bitů z celkového počtu deset tisíc) na jejich porovnání. V případě shody mohou Alice a Bob předpokládat, že jejich komunikaci nikdo nenarušil a ty bity, u nichž měli stejnou bázi, použijí jako tajný klíč. To, že by Eva měla štěstí a podařilo se jí odposlechout výměnu dat, aniž by Alice a Bob zjistili nějakou neshodu, je velice malá, v našem případě 2^{-250}. Pokud se budou některé z kontrolních bitů lišit, znamená to možnost narušení soukromí a Alice a Bob přestanou komunikovat. Poznamenejme, že bezpečnost kvantové kryptografie je mimo jiné založena na nemožnosti klonování kvantových stavů.

2.7.3 Rozvoj kvantové kryptografie

Náš příklad ilustroval kryptografický princip na základě polarizovaných fotonů. Existuje řada jiných návrhů, využívajících dalších vlastností světla. Je možné kódovat qubity pomocí interferometrické fáze, pomocí intenzity světelných pulsů, či pomocí prostorových módů, v nichž se pulsy šíří. Výzkum v této oblasti je velice intenzivní a kvantová kryptografie má zatím ze všech odvětví kvantové informatiky nejblíž ke komerčnímu využití. Z řady mezinárodních projektů, které v této oblasti působí, jmenujme například IST QuComm, financovaný z Pátého rámcového programu EU, jehož řešitel prof. Anders Karlsson získal roku 2004 Descartovu cenu (udělovala se v Praze), projekt SECOQC, jehož cílem je vyvinout funkční prototyp komerčně využitelného kryptografického spojení, či projekt COVAQIAL, soustředící se na využití spojitých proměnných pro kvantovou komunikaci.

Na posledních dvou jmenovaných projektech se podílí i Univerzita Palackého v Olomouci. K jejím důležitým výsledkům patří i jedno z prvních experimentálně fungujících kryptografických zařízení, které může sloužit i jako systém pro vzájemnou identifikaci komunikujících stran. To je v podstatě kombinace kryptografického systému na distribuci tajného klíče, spojeného s identifikační procedurou pro rozpoznání komunikujících stran [2.7]. Jako qubity tu fungovaly slabé nanosekundové pulsy, cestující optickým vláknem, přičemž informace se nekódovala do jejich polarizace, ale do jejich načasování: Alice svůj puls vláknovým děličem rozdělí na dvě části, z nichž jedna projde delší trasu než druhá, a poté je opět vláknovým děličem spojí (snímek



Obr. 2.15: Kvantová kryptografie v Olomouci: Dr. Haderka dolaďuje „Alici“, vysílající část kryptografického vláknového interferometru.

z laboratoře je na obr. 2.15). Tyto dvě trasy tak fungují jako dvě ramena Machova - Zehnderova interferometru, jejichž vzájemnou fázi můžeme nastavovat. Pokud je puls slabý tak, že obsahuje maximálně jediný foton, bude po průchodu takovýmto interferometrem ve stavu odpovídajícím superpozici dvou možných stavů: „foton vepředu“ (prošel kratším ramenem) a „foton vzadu“ (zdržel se v delším rameni). Tyto dvě možnosti spolu s jejich libovolnými superpozicemi představují qubit, s jehož detekcí se musí vypořádat Bob - tedy přijímací stanice. K detekci mu poslouží podobný interferometr, jako má Alice, přičemž nastavení fáze tu hraje roli výběru báze. Obě stanice spojovalo vlákno o celkové délce 0,5 km a zařízení bylo schopné vygenerovat zhruba 6 kilobitů klíče za sekundu.

Průvodce studiem

V dnešní době již fungují vláknové kryptografy na vzdálenost několika desítek kilometrů se současným rekordem cca 120 km. Důvodem, proč je těžké dostat se dále, jsou absorpční ztráty: narozdíl od běžné optické komunikace je nelze kompenzovat zesilovači, protože ty by do systému vnesly podobný šum, jako případný narušitel. Nicméně i tato vzdálenost může přinést zajímavé aplikace, např. pro komunikaci mezi bankami větší aglomerace. Připomeňme, že první bankovní transakce na bázi kvantové kryptografie proběhla na jaře roku 2004 mezi vídeňskou radnicí a pobočkou místní banky - své schopnosti tu demonstrovala skupina prof. Antona Zeilingera z vídeňské univerzity. Druhou možností je posílat fotony volným prostorem. Za vhodných atmosférických podmínek tak lze komunikovat pomocí fotonů šířících se vzduchem několik desítek kilometrů. Na delší vzdálenosti se však můžeme dostat, pokud foton část své cesty urazí vzduchoprázdným prostorem - pro kryptografickou komunikaci pak bude nutné využít družicového systému.

Shrnutí

Kvantová kryptografie umožňuje dvěma stranám sdílet tajný klíč. Je založena na výměně kvantových stavů a jejich měření. U protokolu BB84 Alice posílá Bobovi bity kódované pomocí stavů ve dvou různých bázích, Bob na těchto stavech provádí měření. Jak Alice, tak i Bob své báze náhodně mění. Po zaslání všech stavů se strany vzájemně informují o bázích, které použily pro každý stav. Jako součást klíče použijí bity z těch případů, u kterých se jejich báze shodovaly. Pro kontrolu se u části takovýchto bitů informují, zda se skutečně hodnoty bitů shodují. Pokud by se nějaký narušitel pokoušel vysílané stavy zachytit a proměřit, projevilo by se to tím, že některé z kontrolních bitů by se neshodovaly.

Pojmy k zapamatování

- Protokol BB84,
- kryptografický klíč
- střídání bází
- kvantové měření

2.8 Kvantová provázanost

Důležitým aspektem kvantové informatiky je existence tzv. entanglovaných, neboli kvantově provázaných stavů. (Jako kuriozitu je poprvé zmínil Erwin Schrödinger, který je pojmenoval „verschraenkte Zustände“, v angličtině se objevují pod názvem „entangled states“.) Jedná se o stavy systému, skládajícího se ze dvou či více navzájem odlehlých podsystémů. Vlastnosti těchto podsystémů (představme si například systém dvou fotonů, šířících se opačnými směry) mohou být vzájemně korelované. Pokud je celý systém v kvantově provázaném stavu, budou vzájemně korelované různé páry veličin, a to tak, že korelací je více, než by nám dovolovaly úvahy na základě klasické fyziky (přesněji řečeno, korelace mezi měřeními na dvou kvantových podsystémech mohou narušovat tzv. Bellovy nerovnosti). Pro ilustraci uvažujme například dva fotony A a B v kvantovém stavu

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|\updownarrow\rangle_A | \leftrightarrow\rangle_B - |\leftrightarrow\rangle_A | \updownarrow\rangle_B \right). \tag{2.8.1}$$

Pokud bychom měřili polarizaci jediného fotonu, dostali bychom zcela náhodnou hodnotu. Polarizace každého fotonu je ovšem vždy přesně opačná, než má jeho partner: pokud u fotonu A naměříme vertikální polarizaci, bude mít foton B s jistotou horizontální polarizaci a naopak. A neplatí to jen pro měření v bázi vertikální a horizontální polarizace. Zkusme pro ilustraci převést stav $|\psi\rangle$ do báze kruhových polarizací. Ze vztahů (2.2.1) a (2.2.2) zjistíme, že stavy $|\leftrightarrow\rangle$ a $|\updownarrow\rangle$ mohou být zapsány ve tvaru

$$|\updownarrow\rangle = \frac{1}{\sqrt{2}} \left(|R\rangle - i|L\rangle \right), \tag{2.8.2}$$

$$|\leftrightarrow\rangle = \frac{1}{\sqrt{2}} \left(-i|R\rangle + |L\rangle \right). \tag{2.8.3}$$

Stav $|\psi\rangle$ tedy můžeme psát jako

$$\begin{aligned} |\psi\rangle &= \frac{1}{2\sqrt{2}}\left[(|R\rangle_A - i|L\rangle_A)\,(-i|R\rangle_B + |L\rangle_B)\right. \\ &\quad \left. -\,(-i|R\rangle_A + |L\rangle_A)\,(|R\rangle_B - i|L\rangle_B)\right] \\ &= \frac{1}{\sqrt{2}}\left(|R\rangle_A|L\rangle_B - |L\rangle_A|R\rangle_B\right). \end{aligned} \tag{2.8.4}$$

Znamená to tedy, že pokud je foton A pravotočivě polarizovaný, bude foton B levotočivý a naopak. Kdykoliv ale zjistíme, že foton A měl horizontální polarizaci, bude foton B vertikálně polarizovaný. Jak je to možné, když přece lineární polarizace fotonu znamená, že se foton bude chovat zcela náhodně při průchodu analyzátorem detekujícím kruhovou polarizaci? Dá se uvažovat, že si každý foton s sebou nese jakousi ukrytou informaci, která rozhoduje o tom, jak na který analyzátor reagovat a je to jen naše neznalost, díky které považujeme chování fotonu za „náhodné“? John S. Bell roku 1964 ukázal, že pokud by takovéto „lokální skryté proměnné“ existovaly, musely by statistiky měření různých veličin splňovat určité nerovnosti. Kvantová mechanika však předpovídá možnost narušení Bellových nerovností a řada experimentů jí dává zapravdu. Plyne z toho, že existenci lokálních skrytých proměnných musíme nejspíš ze svých úvah o přírodě vyloučit.

Stav $|\psi\rangle$, nazývaný singlet, je typickým příkladem „entanglovaného“, tedy kvantově provázaného stavu. Je ale nutné si uvědomit, že ne všechny korelace odpovídají kvantové provázanosti. Představme si, že nám nějaký zdroj posílá dvojice fotonů, které budou s 50% pravděpodobností ve stavu $|\updownarrow\rangle_A|\leftrightarrow\rangle_B$ a s 50% pravděpodobností ve stavu $|\leftrightarrow\rangle_A|\updownarrow\rangle_B$. V kvantovém formalismu by to odpovídalo matici hustoty

$$\varrho = \frac{1}{2}|\updownarrow\rangle_A\langle\updownarrow| \otimes |\leftrightarrow\rangle_B\langle\leftrightarrow| + \frac{1}{2}|\leftrightarrow\rangle_A\langle\leftrightarrow| \otimes |\updownarrow\rangle_B\langle\updownarrow|. \tag{2.8.5}$$

I v tomto případě jsou lineární polarizace obou fotonů korelované: pokud u fotonu A zjistíme vertikální polarizaci, bude foton B s jistotou polarizován horizontálně a naopak. Narozdíl od předchozího případu se stavem $|\psi\rangle$, u stavu ϱ však nebudeme pozorovat žádné korelace mezi kruhovými polarizacemi obou fotonů. Matice hustoty ϱ z rovnice (2.8.5) neodpovídá kvantově provázanému stavu.

Přesněji se kvantová provázanost definuje takto: jakýkoliv kvantový stav dvou podsystémů A a B lze popsat maticí hustoty ϱ_{AB}. Pokud je možné tuto matici hustoty zapsat jako součet

$$\varrho_{AB} = \sum_k p_k \varrho_A^{(k)} \varrho_B^{(k)}, \tag{2.8.6}$$

kde $0 < p_k \leqq 1$ a $\varrho_A^{(k)}$ jsou matice hustoty podsystému A a $\varrho_B^{(k)}$ jsou matice hustoty podsystému B, nazývá se stav ϱ_{AB} *faktorizovatelný*. Pokud neexistuje žádná možnost, jak matici hustoty ϱ_{AB} zapsat ve tvaru (2.8.6), je příslušný stav kvantově provázaný.

V kvantové informatice se často pracuje s kvantově provázanými stavy dvou qubitů. Je proto velmi užitečné zavést pro dvoubitové systémy bázi, jejíž všechny

stavy jsou kvantově provázané. Jedná se o takzvanou *Bellovu bázi*:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \tag{2.8.7}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \tag{2.8.8}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \tag{2.8.9}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{2.8.10}$$

Jak se můžeme přesvědčit, singletní stav z našeho příkladu odpovídá Bellovu stavu $|\Psi^-\rangle$.

Průvodce studiem

Příroda nám někdy poskytuje zdroj entanglovaných stavů. Příkladem může být frekvenční konverze fotonů v nelineárních krystalech: z jednoho fotonu o frekvenci ω se mohou stát dva fotony s nižšími frekvencemi ω_1 a ω_2, pro něž platí $\omega_1 + \omega_2 = \omega$. Tyto dva nové fotony jsou v kvantově provázaném stavu. Často ale bývá problém, jak dva původně nezávislé fotony (například přilétající ze dvou různých zdrojů) přivést do vzájemně kvantově provázaného stavu.

Korelace u kvantově provázaných stavů svědčí o tom, že příroda se chová podstatně jinak, než by odpovídalo naší běžné intuici, z určitého pohledu to vypadá, jakoby výsledek měření na jednom podsystému okamžitě (nadsvětelnou rychlostí) ovlivnil chování jiných částí systému. Zároveň však toto „nadsvětelné“ ovlivnění má takový charakter, že ho nelze bezprostředně využít k předání informace: informace sama se může šířit maximálně rychlostí světla ve vakuu. Tyto vlastnosti kvantových systémů daly příčinu k mnoha filosofickým diskusím o tom, co vlastně znamená kvantový stav, zda odpovídá nějaké realitě nebo spíš naší subjektivní znalosti a co vlastně „za tím vším“ je. Ale v poslední době se spíše lidé snaží zjistit, jak by se tyto podivuhodné vlastnosti přírody daly prakticky využít. Například Artur Ekert roku 1991 zjistil, že provázané stavy by byly vynikajícím prostředkem pro kryptografii (jeho protokol E91 je odlišný od výše uvedeného protokolu BB84). Kromě toho budou kvantově provázané stavy důležité pro chod kvantových počítačů a již dnes jsou základem dalších zajímavých procesů: kvantové teleportace, hustého kódování a dalších.

Shrnutí

Kvantová provázanost (entanglement) je vlastnost stavů systémů, které jsou složené ze dvou (nebo více) podsystémů a měření na nich vykazují určitý typ korelací. Kvantově provázané stavy jsou takové, které nejsou faktorizovatelné—jejich matice hustoty nelze přepsat do tvaru konvexní sumy součinů matic hustoty jednotlivých podsystémů. Kvantově provázané stavy mohou narušovat tzv. Bellovy nerovnosti,

zatímco faktorizovatelné stavy nikoliv. U stavů dvou qubitů se často používají kvantově provázané stavy tvořící tzv. Bellovu bázi.

Pojmy k zapamatování

- Faktorizovatelný stav,
- Bellova báze,
- singlet,
- kvantová provázanost.

Cvičení

1. Dokažte, že Bellovy stavy tvoří ortonormální systém stavů dvou qubitů.
2. Najděte unitární matici, která permutuje Bellovy stavy $|\Phi^+\rangle \to |\Phi^-\rangle \to |\Psi^+\rangle \to |\Psi^-\rangle \to |\Phi^+\rangle$

2.9 Kvantová teleportace

Jednou z aplikací kvantové provázanosti je kvantová teleportace. Předpokládejme, že Alice má nějaký systém—pro jednoduchost předpokládejme qubit—v neznámém kvantovém stavu. Sama tento stav nepotřebuje, ale ráda by ho neporušený předala Bobovi, který je na vzdáleném místě a nelze mu qubit předat fyzicky. Alice si však s Bobem může telefonovat. Jak tento problém vyřešit?

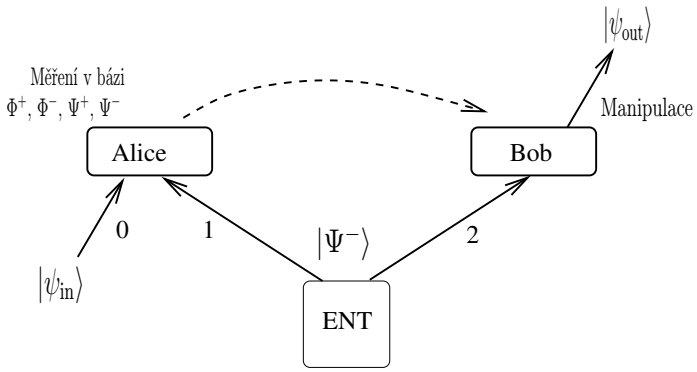
Jako první myšlenka nás může napadnout, že Alice jednoduše změří svůj qubit, výsledek zatelefonuje Bobovi a ten si svůj qubit připraví v tomto stavu. Ovšem něco takového nám kvantová mechanika nedovolí. Alice může měřit svůj qubit jen v jediné bázi a pokud takové měření provede, nutně musí přijít o veškerou informaci, která mohla být zakódovaná v jiné bázi. Předpokládejme například, že Alice má svůj qubit ve stavu $\frac{1}{2}|0\rangle + i\frac{\sqrt{3}}{2}|1\rangle$. Pokud by Alice svůj qubit změřila v bázi $|0\rangle$, $|1\rangle$, dostala by buď jedničku nebo (s menší pravděpodobností) nulu, ale nemohla by zjistit žádnou informaci o fázi mezi těmito dvěma stavy.

Předpokládejme ale navíc, že Alice s Bobem již sdílejí nějaký kvantově provázaný stav, například singlet $|\Psi^-\rangle$. V tomto případě může Alice Bobovi svůj stav *teleportovat*. Pro popis teleportace nám poslouží obr. 2.16. Pro odlišení si označme Alicin vstupní systém 0 a systémy, které nesou provázaný stav jako 1 (tento systém bude mít Alice) a 2 (bude mít Bob). Předpokládejme, že Alicin qubit je ve stavu $\alpha|0\rangle_0 + \beta|1\rangle_0$. Na počátku je tedy celý tříčásticový systém ve stavu

$$|\psi\rangle_{012} = (\alpha|0\rangle_0 + \beta|1\rangle_0)\frac{1}{\sqrt{2}}\left(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2\right). \tag{2.9.1}$$

Teleportace pak probíhá následujícím způsobem:

1. Alice provede měření na kombinovaném systému 0 a 1 v Bellově bázi. Tím získá výsledek, který je buď Φ^+, Φ^-, Ψ^+, nebo Ψ^-. Její vstupní stav je tímto měřením zlikvidován a navíc nemůže o tomto stavu již nic zjistit ani z výsledku měření: v každém z Bellových stavů je totiž stejně zastoupen jak stav $|0\rangle_0$ tak i stav $|1\rangle_0$.



Obr. 2.16: Kvantová teleportace jednoho qubitu. Alice má qubit v nějakém neznámém stavu $|\psi_{\text{in}}\rangle$ a chce ho předat Bobovi, aniž by ho mohla fyzicky poslat. Může k tomu využít sdílený kvantově provázaný stav.

2. Alice výsledek měření zatelefonuje Bobovi (v podstatě mu předá jen dva bity informace).
3. Bob podle výsledku měření provede jednu ze čtyř možných transformací na svém systému 2. Poté je systém 2 ve stejném kvantovém stavu, v jakém byl systém 0 na počátku.

Proč tomu tak je zjistíme, když budeme působit na stav (2.9.1) projekčními operátory Bellových stavů, což odpovídá měření v Bellově bázi:

$$|\Phi^+\rangle_{01}\langle\Phi^+|\psi\rangle_{012} = |\Phi^+\rangle_{01}(\alpha|1\rangle_2 - \beta|0\rangle_2), \tag{2.9.2}$$
$$|\Phi^-\rangle_{01}\langle\Phi^-|\psi\rangle_{012} = |\Phi^+\rangle_{01}(\alpha|1\rangle_2 + \beta|0\rangle_2), \tag{2.9.3}$$
$$|\Psi^+\rangle_{01}\langle\Psi^+|\psi\rangle_{012} = |\Psi^+\rangle_{01}(\beta|1\rangle_2 - \alpha|0\rangle_2), \tag{2.9.4}$$
$$|\Psi^-\rangle_{01}\langle\Psi^-|\psi\rangle_{012} = |\Psi^-\rangle_{01}(\beta|1\rangle_2 + \alpha|0\rangle_2). \tag{2.9.5}$$

Znamená to tedy, že pokud Alice zjistí stav Ψ^-, nebude Bob dělat se svým qubitem nic a jeho stav bude roven vstupnímu stavu na Alicině qubitu. Pokud Alice zjistí stav Ψ^+, bude muset Bob fázově posunout amplitudu u stavu $|0\rangle_2$ o π. Pokud Alice zjistí některý ze stavů Φ, bude muset Bob rotovat svůj qubit mezi bázovými stavy $|0\rangle_2$ a $|1\rangle_2$ a případně i provést fázový posuv. Každopádně po některé z těchto jednoduchých operací bude výstupní stav Bobova qubitu roven vstupnímu stavu qubitu u Alice, a to aniž se kdokoliv mohl tuto hodnotu stavu dozvědět.

Shrnutí

Kvantová teleportace je předávání kvantového stavu z jednoho systému na druhý—vzdálený. Využívá se při ní sdíleného kvantově provázaného stavu a klasické komunikace. Alice provede měření v Bellově bázi na vstupním stavu a její částí sdíleného provázaného stavu. Tím se ovšem vstupní stav zničí. Výsledek měření předá Alice Bobovi a ten na jeho základě provede transformaci na své části sdíleného provázaného stavu. Tím původně zničený vstupní stav nově vznikne na Bobově podsystému.

Kontrolní otázky

1. Jaké hradlo by měl použít Bob na svůj qubit, pokud Alice naměřila stav $|\Psi^+\rangle_{01}$?

2.10 Závěr

Kvantová informatika si získává místo jak ve fyzikálních, tak v matematických oblastech. Po matematické stránce jsou nejzajímavější možné nové algoritmy a protokoly zpracování kvantové informace. Z fyzikálního hlediska je pak nejdůležitějším problémem jejich konkrétní implementace. Tento text by měl sloužit jako základní orientace pro ty, kdo by se chtěli některým otázkám kvantové informatiky věnovat. Případný zájemce najde další informace buď v původní literatuře (např. [2.4, 2.6]), v přehledových článcích (k vynikajícím patří Braunsteinův [2.5]) nebo v monografiích (např.[2.3, 2.2]).

Literatura ke kapitole 2

[2.1] Feynman R.P., Leighton R.B., Sands M.: *Feynmanovy přednášky z fyziky.* Fragment, Havlíčkův Brod 2002.

[2.2] Dušek M.: *Koncepční otázky kvantové teorie.* Vydavatelství Univerzity Palackého, Olomouc 2002.

[2.3] Gruska J.: *Quantum computing.* McGraw-Hill, London 1999.

[2.4] Shor P.W.: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* http://www.arxiv.org/abs/quant-ph/9508027

[2.5] Braunstein S.L.: *Quantum computation.* http://www-users.cs.york.ac.uk/~schmuel/comp/comp.html

[2.6] Grover, L.K.: *Quantum mechanics helps in searching for a needle in a haystack.* Phys. Rev. Letters **79,** 325-328, 1997. http://www.arxiv.org/abs/quant-ph/9706033

[2.7] Dušek, M., Haderka, O., Hendrych, M., Myška, R.: *Quantum identification system.* Physical Review A **60,** p. 149, 1999. http://optics.upol.cz/dusek/clanky/pra60-149.pdf

Přílohy

Příloha A

Fyzikální konstanty a jednotky použité v textu

V přehledné tabulce uvádíme fyzikální konstanty a jednotky použité v textu spolu s jejich hodnotami v soustavě SI.

Boltzmannova konstanta	$k_B = 1{,}380\,662 \cdot 10^{-23}\,\mathrm{J{\cdot}K^{-1}}$
hmotnost Slunce	$M_\odot = 1{,}989 \cdot 10^{30}\mathrm{kg}$
gravitační konstanta	$G = 6{,}672\,0 \cdot 10^{-11}\mathrm{N{\cdot}m^2{\cdot}kg^{-2}}$
parsek	$1\,\mathrm{pc} = 3{,}085\,977\,56 \cdot 10^{16}\,\mathrm{m}$
Planckova konstanta	$h = 6{,}626\,176 \cdot 10^{-34}\,\mathrm{J{\cdot}s}$
rychlost světla ve vakuu	$c = 2{,}997\,924\,580 \cdot 10^{8}\,\mathrm{m{\cdot}s^{-1}}$
světelný rok	$1\,\mathrm{ly} = 9{,}460\,528\,3 \cdot 10^{15}\,\mathrm{m}$

Příloha B

RSA kryptografický kód

RSA kód je nazván podle svých objevitelů, kterými jsou Ronald Rivest, Adi Shamir a Leonard Adleman. Funguje následujícím způsobem. Předpokládejme, že dva účastníci—Alice a Bob spolu chtějí bezpečným způsobem komunikovat. Alice bude přijímat od Boba zprávy, které nikdo kromě Alice nedokáže rozluštit.

1. Alice zvolí dvě velká prvočísla p a q a vynásobí je, takže dostane číslo $\mathcal{N} = pq$. Pro ilustraci tu ale pracujme s malými prvočísly, zvolme si třeba $p = 17$ a $q = 11$, takže $\mathcal{N} = 17 \times 11 = 187$.
2. Alice dále vybere číslo e, které je nesoudělné jak s $(p-1)$ tak s $(q-1)$. V našem příkladu tedy hledáme číslo nesoudělné s 16 a 10. Zvolme $e = 7$.
3. Alice dále najde číslo d, které splňuje podmínku

$$e \times d = 1 (\text{mod } (p-1)(q-1)). \tag{2.0.1}$$

   V našem případě tedy hledáme číslo d splňující $7d = 1 (\text{mod } 16 \times 10)$, tedy $7d = = 1 (\text{mod } 160)$. Jak si můžeme ověřit, hledané číslo je $d = 23$.
4. Alice může komukoliv sdělit čísla $\mathcal{N}$ a e, která budou sloužit jako její *veřejný klíč*, ale čísla p, q a d si ponechá v tajnosti.Čísla $\mathcal{N}$ a d Alici slouží jako její *soukromý klíč*.
5. Pro zakódování zprávy musí Bob nejprve konvertovat posílaný text na číslo—například pomocí ASCII kódu. Zprávě (zatím nezašifrované) tak odpovídá číslo M. Šifrování se děje předpisem

$$C = M^e (\text{mod } \mathcal{N}). \tag{2.0.2}$$

   Šifrovanou zprávou je tedy číslo C. Pro ilustraci předpokládejme, že Bob chce Alici poslat písmeno X, které v ASCII kódu odpovídá číslu 88. Tedy $M = 88$ a

$$C = 88^7 (\text{mod } 187) = 894\ 432 (\text{mod } 187) = 11. \tag{2.0.3}$$

6. Bob pošle šifrovanou zprávu C Alici.
7. Alice může zprávu rozšifrovat pomocí svého soukromého klíče vztahem

$$M = C^d (\text{mod } \mathcal{N}). \tag{2.0.4}$$

   V našem případě to tedy znamená

$$M = 11^{23} (\text{mod } 187) = 88. \tag{2.0.5}$$

Veřejným klíčem může kdokoliv zašifrovat zprávu, kterou chce poslat Alici. Zašifrovanou zprávu ale může rozluštit jen ten, kdo má soukromý klíč. Aby někdo mohl ze znalosti veřejného klíče získat soukromý klíč, musel by dokázat faktorizovat číslo $\mathcal{N}$, tedy najít jeho činitele p a q. To je ovšem s rostoucí velikostí $\mathcal{N}$ výpočetně velice náročné, na klasických počítačích doba výpočtu roste exponenciálně s počtem číslic čísla $\mathcal{N}$. Kvantový počítač by však dokázal číslo $\mathcal{N}$ faktorizovat v čase, který roste jen polynomicky s počtem číslic $\mathcal{N}$.

Rejstřík