Non-Standard Forms of Teaching Mathematics and Physics: Experimental and Modeling Approach

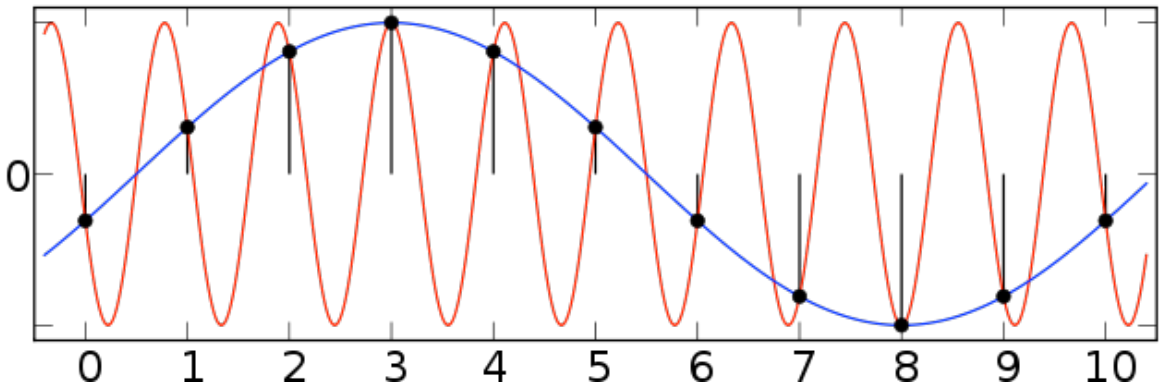
IPA HU-SRB/1203/221/024

Odabrane teme za radoznale srednjoškolce

Stefan Hačko

Department of Mathematics and Informatics

Faculty of Sciences, University of Novi Sad



University of Novi Sad
2015

The project is co-financed by the European Union

Sadržaj

1 Elementaran pristup dirihletovom integralu **4**
- 1.1 Uvod . . . 4
  - 1.1.1 Pregled rada . . . 4
  - 1.1.2 Osnovni pojmovi i definicije . . . 4
- 1.2 Nesvojstveni integral . . . 6
  - 1.2.1 Definicija i osnovne osobine . . . 7
  - 1.2.2 Konvergencija nesvojstvenog integrala . . . 8
- 1.3 Dirihleov integral . . . 9
  - 1.3.1 Definicija . . . 9
  - 1.3.2 Konvergencija Dirihleovog integrala . . . 9
  - 1.3.3 Vrednost dirihleovog integrala . . . 10
- 1.4 Zaključak . . . 14

2 Teorijski model kvantnog računara **16**
- 2.1 Uvod . . . 16
  - 2.1.1 Istorija kvantnih računara . . . 17
- 2.2 Matematički model kvantnog računara . . . 19
  - 2.2.1 Postulati kvantne mehanike . . . 19
  - 2.2.2 Teorijski model kvantnog računara . . . 22
- 2.3 Kvantni algoritmi . . . 29
  - 2.3.1 Kvantni algoritmi zasnovani na Furijevoj transformaciji 29
  - 2.3.2 Kvantni algoritmi za pretragu . . . 29
  - 2.3.3 Kvantna furijeva transformacija . . . 30
- 2.4 Zakljucak . . . 33
  - 2.4.1 Prednosti kvantnih računara . . . 33
  - 2.4.2 Problemi kvantnih računara . . . 33
  - 2.4.3 Budućnost kvantnih računara . . . 34

3 Teorema o uzorcima **35**
- 3.1 Uvod . . . 35
  - 3.1.1 Istorijski pregle . . . 35
  - 3.1.2 Pregled rada . . . 36
- 3.2 Osvnovni pojmovi i tvrđenja . . . 37
  - 3.2.1 Pred-Hilbertovi i Hilbertovi prostori . . . 37
  - 3.2.2 Furijeovi koeficijent . . . 38
  - 3.2.3 Trigonometrijski redovi Furijea . . . 40

3.2.4 Furijeova transformacija 42
3.3 Šenonova teorema 44
3.3.1 Poasonova formula 44
3.3.2 Dokaz Šenonove teoreme o uzorcima 45
3.3.3 Primene Šenonove teoreme 47
3.4 Aliasing 48
3.5 Zaključak 50

Deo 1

Elementaran pristup dirihletovom integralu

1.1 Uvod

1.1.1 Pregled rada

Ovaj rad je podeljen u tri dela. U uvodu su izložene osnovne definicije i teoreme, bez dokaza (za dokaze svih teorema pogledati [8]), vezane za odredjeni integral, koje su potrebne za dalje čitanje rada. U drugom delu rada u najkraćim crtama izloženo je proširivanje odredjenog integrala na nesvojstveni integral. U posledljem delu rada detaljno je izloženo izračunavanje Dirihleovog integrala elementarnim metodama.

1.1.2 Osnovni pojmovi i definicije

U ovom delu rada daćemo osnovne definicije i teoreme potrebne za dalje čitanje i razumevanje ovog rada.

Odredjeni integral

Definicija 1.1.1. Podela intervala $[a, b]$ je svaki konačan skup tačaka $x_i \in [a, b], i = 0, 1, \ldots, k$, takvih da je

$$a = x_0 < x_1 < \cdots < x_{k-1} < x_k = b.$$

Uvodimo oznaku

$$\mathcal{P} = \{x_i\}_{i=0}^{k}$$

Tačke x_i se nazivaju *deobne tačke*, svaki interval oblika $[x_{i-1}, x_i], i = 1, 2, \ldots, k$, *interval podele*, a njegova dužina se označava sa Δx_i.

Označimo sa

$$\delta_{\mathcal{P}} = \max\{\Delta x_i | i = 1, 2 \ldots, k\}.$$

Definicija 1.1.2. Neka je funkcija f definisana na intervalu $[a, b]$. Neka je $\mathcal{P} = \{x_i\}_{i=0}^{k}$ podela intervala $[a, b]$ i neka su c_i proizvoljno izabrana tačke tako

da važi

$$c_i \in [x_{i-1}, x_i], i = 1, 2, \ldots, k.$$

Suma

$$\sigma_{\mathcal{P}}(f) = \sigma_{\mathcal{P}}(f; c_1, c_2, \ldots, c_k) = \sum_{i=1}^{k} f(c_i) \cdot \delta x_i$$

se naziva **Rimanova integralna suma** funkcije f na intervalu $[a, b]$.

Definicija 1.1.3. Broj I je granična vrednost Rimanovih integralnih suma funkcije $f : [a, b] \to \mathbb{R}$, kad $\delta_{\mathcal{P}} \Rightarrow 0$, ako za svako $\epsilon > 0$ postoji $\delta = \delta(\epsilon) > 0$ tako da za svaku podelu $\mathcal{P} = \{x_i\}_{i=0}^{k}$ intervala $[a, b]$ za koju vazi $\delta_{\mathcal{P}} < \delta$ i svaki izbor tačaka $c_i \in [x_{i-1}, x_i], i = 1, 2, \ldots, k$ vazi da je

$$|\sum_{i=1}^{k} f(c_i) \cdot \Delta x_i - I| < \epsilon.$$

U tom slučaju pišemo $\lim_{\delta_{\mathcal{P}} \to 0} \sigma_{\mathcal{P}}(f) = I$ i kažemo da je funkcije f **Riman integrabilna** na intervalu $[a, b]$.

Broj I naziva se **Odredjeni integral** funkcije f i označava se sa

$$I = \int_a^b f(x)dx$$

Sledeca tvrdjenja blize odredjuju neke klase Riman integrabilnih funkcija.

Tvrdjenje 1.1.4 (Potreban uslov za Riman integrabilnost)**.** *Ako je funkcija f integrabilna na $[a, b]$ onda je ona i ograničena na $[a, b]$.*

Tvrdjenje 1.1.5. *Funkcija monotona ili neprekidna na [a,b], je i integrabilna na tom intervalu.*

Funkcije zadate preko odredjenog integrala

Uvedimo sada pojam funkcije zadate preko odredjenog integrala.

Definicija 1.1.6. Neka je funkcija f integrabilna na $[a, b]$, onda je ona integrabilna i na sakom podintevalu $[a, x]$ intevala $[a, b]$ (ref), pa svakom $x \in [a, b]$ mozemo dodeliti jedan broj, odredjeni integral funkcije f na intervalu $[a, x]$. Time je definisana funkcija

$$F(x) = \int_a^x f(t)dt.$$

Sledeca tvrdjenja daju osobine funkcije F.

Tvrdjenje 1.1.7. *Ako je funkcija f integrabilna na $[a, b]$ onda je funkcija F neprekidna na $[a, b]$.*

Tvrdjenje 1.1.8. *Neka je funkcija f integrabilna na $[a,b]$ i neprekidna u tački x_0. Tada he funkcija F diferencijabilna u tački x_0 i pri tome važi*

$$F'(x_0) = f(x_0)$$

.

Tvrdjenje 1.1.9. *Ako je funkcija f neprekidna na $[a,b]$ onda je*

$$F(x) = \int_a^x f(t)dt, x \in [a,b]$$

njena primitivna funkcija.

Izračunavanje odredjenog integrala

Sledeća teorema na daje vezu izmadju odredjenog i neodredjenog integrala i u velikome olaksava izračunavanje odredjenog integrala.

Teorema 1.1.10 (Osnovna teorema integralnog računa)**.** *Neka je funkcija f neprekidna na $[a,b]$*[1] *i neka je G bilo koja primitivna funkcija za f na $[a,b]$, tada je*

$$\int_a^b f(x)dx = G(b) - G(a) = G(x)\Big|_a^b \tag{1.1.1}$$

Jednakost 1.1.1 naziva se ***Njutn-Lajbnicova formula****.*

Dokaz. Funkcija

$$F(x) = \int_a^x f(t)dt, x \in [a,b]$$

je na osnovu 1.1.9 takodje jedna primitvan funkcija za f na $[a,b]$ te je za neko $c \in \mathbb{R}$

$$F(x) = G(x) + c, x \in [a,b]. \tag{1.1.2}$$

Iz $F(a) = 0$ zamenom u 1.1.2 dobija se da je $c = -G(a)$ te je

$$\int_a^x f(t)dt = G(x) - G(a)$$

Sada, za $x = b$, dobija se tražena formula. □

1.2 Nesvojstveni integral

Pojam Rimanovog integrala vezan je za ograničen interval $[a,b], a,b \in \mathbb{R}$. Sa druge strane znamo da neograničena funkcija nije Riman integrabilna. Ovo su osnovni razlozi za prosirenje pojma Rimanovog integrala, i prosirenje ćemo upravo vršiti u ta dva pravca.

[1] Ovaj uslov se može oslabiti ali posto ćemo se u radu baviti samo neprekidnim funkcijama koristićemo teoremu u ovom obliku.

1.2.1 Definicija i osnovne osobine

Definicija 1.2.1. Neka je $[a, \omega), \omega \in \mathbb{R} \cup \{+\infty\}$, interval na kome je definisana funkcija f integrabilna na svakom podintervalu $[a, b] \subset [a, \omega)$. Neka je dalje

$$F(b) = \int_a^b f(x)dx, b \in [a, \omega).$$

Granična vrednost

$$\lim_{b \to \omega - 0} F(b)$$

naziva se **nesvojstveni integral** funkcije f na $[a, \omega)$ i označava se sa

$$\int_a^\omega f(x)dx.$$

Ukoliko ova granična vrednost postoji u $\mathbb{R}$ kažemo da nesvojstveni integral **konvergira**, a u suprotnom da **divergira.** Ukoliko je $\omega = \pm\infty$ ili $f \notin \mathcal{R}[a, \omega], \omega \in \mathbb{R}$, tačka ω se naziva **tačka singulariteta** nesvojstvenog integrala.

Napomena 1.2.2. Analogno se definiše i $\int_\omega^a f(x)dx$ gde je $\omega \in \mathbb{R} \cup \{-\infty\}$.

Napomena 1.2.3. Ako su obe granice, recimo ω_1 i ω_2 tačke singulariteta, a drugih singulariteta u intervalu (ω_1, ω_2) nema, integral $\int_{\omega_1}^{\omega_2} f(x)dx$ konvergira ako i samo ako konvergiraju i $\int_{\omega_1}^a f(x)dx$ i $\int_a^{\omega_2} f(x)dx$ gde je $a \in (\omega_1, \omega_2)$ proizvoljna tačka.

Sledeće tvrdjenja nam daju osnovne osobine nesvojstvenog integrala. Dokaz sledi neposredno iz definicije i svojstva neprekidnih funkcija. U deljem tekstu predpostavimo da $\int_\omega^a f(x)dx$ i $\int_\omega^a g(x)dx$ konvergiraju.

Tvrdjenje 1.2.4. *Ako je $\omega \in \mathbb{R}$ i $f \in \mathcal{R}[a, \omega]$ onda je nesvojstveni integral jednak odredjenom integralu funkcije f na $[a, \omega]$.*

Tvrdjenje 1.2.5. *Ako $c \in [a, \omega]$ i drugih singulariteta nema, onda je*

$$\int_a^\omega f(x)dx = \int_a^c f(x)dx + \int_c^\omega f(x)dx.$$

Tvrdjenje 1.2.6. *Za proizvoljno $\alpha, \beta \in \mathbb{R}$ važi da je*

$$\int_a^\omega (\alpha f(x) + \beta g(x))dx = \alpha \int_a^\omega f(x)dx + \beta \int_a^\omega g(x)dx$$

Izračunavanje nesvojstvenog integrala

Sledeća teorema uvelikom olakšava izračunavanje neodredjenog integrala.

Teorema 1.2.7. *Ako je funkcija f neprekidna na $[a, \omega)$ i G bilo koja njena primitivna funkcija, onda je*

$$\int_a^\omega f(x)dx = \lim_{x\to\omega-0} G(x) - G(a) = G(x)\Big|_a^\omega$$

1.2.2 Konvergencija nesvojstvenog integrala

Sada ćemo razmotriti problem ispitivanje konvergencije nesvojstvenog integrala bez njegovog izračunavanja.

Teorema 1.2.8. *Neka je funkcija f nenegativna na $[a, \omega)$ i integrabilna na svakom podintervalu $[a, b] \subset [a, \omega)$. Nesvojstveni integral konvergira ako i samo ako postoji broj $M > 0$ takav da je za svako $b \in [a, \omega)$*

$$\int_a^\omega f(x)dx \leq M.$$

Označimo sa

$$I_1 = \int_a^\omega f(x)dx, I_2 = \int_a^\omega g(x)dx$$

Posledica 1.2.9. *Ako je*

$$0 \leq f(x) \leq g(x), x \in [a, \omega),$$

tada iz konvergencije integrala I_2 sledi konvergencija integrala I_1, a iz divergencije integrala I_1 sled divergencija integrala I_2.

Uvedimo sada pojam apsolutne konvergencije.

Definicija 1.2.10. Nesvojstveni integral $\int_a^\omega f(x)dx$ **apsolutno konvergira** ako konvergira integral $\int_a^\omega |f(x)|dx$. Za nesvojstveni integral kažemo da **uslovno konvergira** ako konvergira intgral $\int_a^\omega f(x)dx$, a ne konvergira apsolutno.

Tvrdjenje 1.2.11. *Ako nesvojstveni integral apsolutno konvergira onda on i konvergira.*

Primer 1. Dokazati konvergenciju nesvojstvenog integrala

$$\int_1^{+\infty} \frac{\cos x}{x^2}dx$$

Dokaz. Ispitajmo prvo apsolutnu konvergenciju integrala. Iz nejednakosti

$$\left|\frac{\cos x}{x^2}\right| \leq \frac{1}{x^2}, x \in [1, +\infty)$$

i teoreme 1.2.9 sledi njegova apsolutna konvergencija, a iz teoreme 1.2.11 sledi i njegova konvergencija. □

U nastavku rada bavićemo se izračunavanjem jednog konvergentnog nesvojstvenog integrala funkcije koja nema primitivnu funkciju u klasi elementarnih funkcija.

1.3 Dirihleov integral

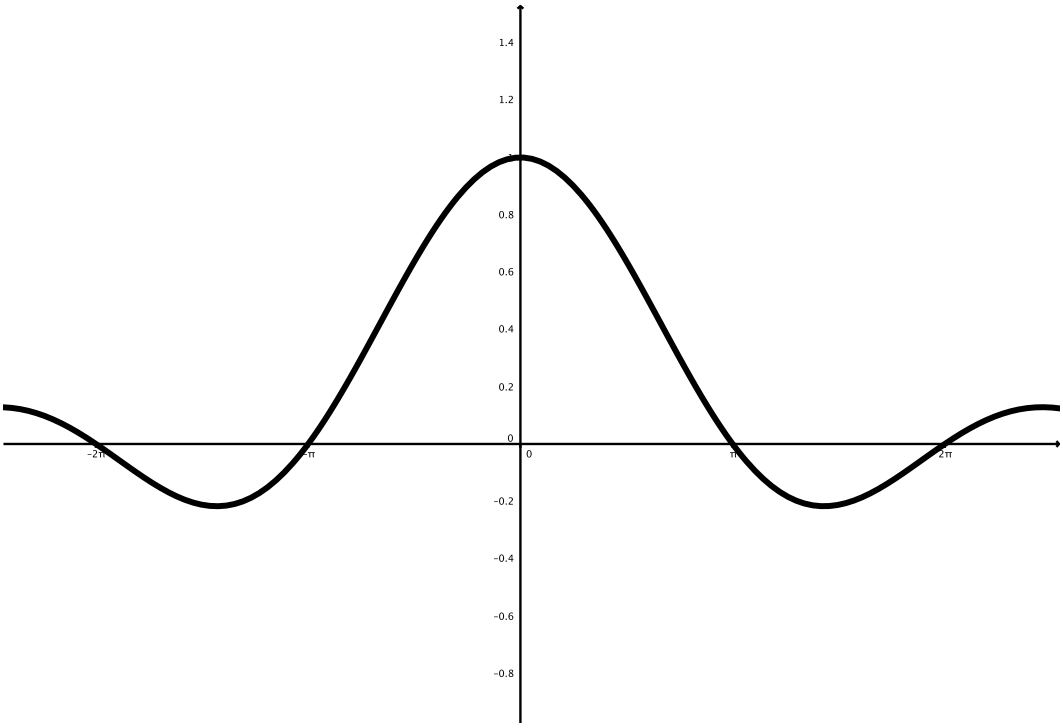
1.3.1 Definicija

U literaturi pod pojmom Dirihleov integral mogu se neći više različitih integrala od kojih je jedan dat sledećom definicijom.

Definicija 1.3.1. Dirihleov integral je nesvojstveni integral

$$\int_0^{+\infty} \frac{\sin x}{x} dx.$$

1.3.2 Konvergencija Dirihleovog integrala



Prikaz 1.1: Funkcija $\frac{\sin x}{x}$ u okolini tačke 0.

Dokažimo sledeće tvrdjenje.

Tvrdjenje 1.3.2. *Dirihlevo integral uslovno konvergira.*

Dokaz. Jedina tačka singulariteta je $+\infty$ (0 nije tačka singulariteta jer se funkcija $\frac{\sin x}{x}$ može neprekidno dodefinisati u 0) pa ispitajmo konvergenciju u okolini tačke singulariteta.

Parcijalnom integracijom se dobija

$$\int_1^{+\infty} \frac{\sin x}{x} dx = -\frac{\cos x}{x}\Big|_1^{+\infty} - \int_1^{+\infty} \frac{\cos x}{x^2} dx = \cos 1 - \int_1^{+\infty} \frac{\cos x}{x^2} dx.$$

Pošto iz primera 1 znamo da $\int_1^{+\infty} \frac{\cos x}{x^2} dx$ konvergira sledi da i Dirihleov integral konvergira.

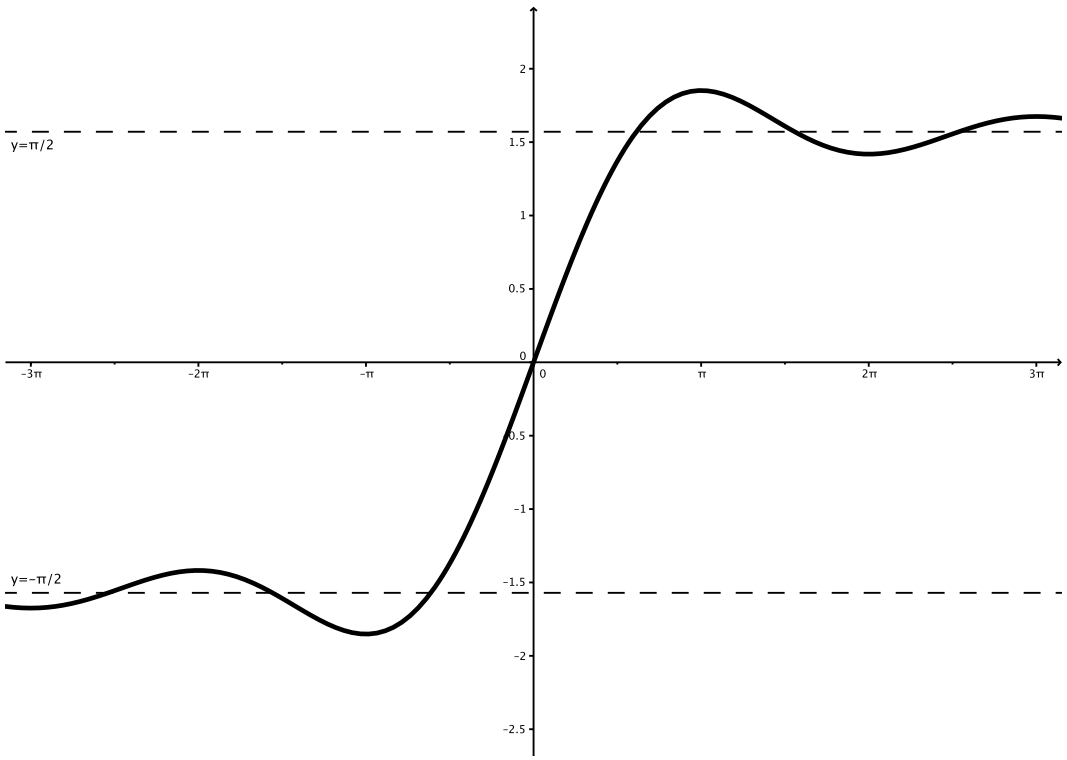
Pokažimo sada da Dirihleov integral ne konvergira i apsolutno.

Iz nejednakosti $|\sin x \geq \sin^2 x = \frac{1-\cos 2x}{2}$, za proizvoljno $b > 1$ sledi

$$\int_1^b \left|\frac{\sin x}{x}\right| dx \geq \frac{1}{2}\int_1^b \frac{dx}{x} - \frac{1}{2}\int_1^b \frac{\cos 2x}{x} dx$$

Iz neograničenosti desne strane ove nejednakosti ($\ln b \to +\infty, b \to +\infty$) sledi da je i leva starna neograničena pa iz teoreme 1.2.9 sledi da nesvojstveni integral $\int_1^b \left|\frac{\sin x}{x}\right| dx$ divergira što implicira da Dirihleov integral uslovno konvergira. □

1.3.3 Vrednost dirihleovog integrala



Prikaz 1.2: Grafik funkcije $g(x) = \int_0^x \frac{\sin t}{t} dt$

Pošto sada znamo da dirihleov integral konvergira, možemo sada izračunati njegovu vrednost.

Tvrdjenje 1.3.3. *Vrednost Dirihleovog integrala je* $\frac{\pi}{2}$*, tj.*

$$\int_0^{+\infty} \frac{\sin x}{x} dx = \frac{\pi}{2}.$$

Dokaz. Primetimo prvo da ne možemo primeniti Njutn-Lajbnicovu formulu za ovaj integral, pošto funkcija $\frac{\sin x}{x}$ nema primitivnu funkciju u klasi elementarnih funkcija.

Dokažimo prvo specijalan slučaj Riman-Lebegove leme.

Lema 1.3.4 (Riman-Lebeg)**.** *Ako je* f *neprekidna funkcija na* $[a, b]$*, onda je*

$$\lim_{\lambda \to \infty} \int_a^b f(t) \sin(\lambda t) dt = 0.$$

Dokaz. Neka je $n \in \mathbb{N}$ i $\mathcal{P} = \{t_0, t_1, \ldots, t_n\}$ ekvidistantna podela intervala $[a, b]$ za kou važi

$$a = t_0 < t_1 < \cdots < t_n = b$$
$$t_i - t_{i-1} = \frac{b-a}{n}$$

Onda važi

$$\begin{aligned} \int_a^b f(t) \sin \lambda dt = & \quad \sum_{i=1}^{n} \int_{t_{i-1}}^{t_i} f(t) \sin \lambda t dt \\ = & \quad \sum_{i=1}^{n} \int_{t_{i-1}}^{t_i} [f(t) - f(t_i)] \sin \lambda t dt + \sum_{i=1}^{n} f(t_i) \int_{t_{i-1}}^{t_i} \sin \lambda t dt \end{aligned}$$

Pošto je f neprekidna na $[a, b]$ ona je i uniformno neprekidna na $[a, b]$[2].

Neka je $\epsilon > 0$ proizvoljno dato.

Iz uniformne neprekidnosti funkcije f sledi da za to ϵ postoji $\delta > 0$ takvo da za sve x i y iz $[a, b]$

$$|x - y| < \delta \Rightarrow |f(x) - f(y)| < \frac{\epsilon}{2(b-a)}.$$

Ako je $n > \frac{b-a}{\delta}$, onda za svako t takvo da je $t_{i-1} \leq t \leq t_i, |t - t_i| \leq |t_i - t_{i-1}| = \frac{b-a}{n} \leq \delta, i = \{1, 2, \ldots, n\}$ imamo da je

$$|f(t) - f(t_i)| < \frac{\epsilon}{2(b-a)}.$$

[2]Sledi iz Kantorove teoreme o uniformnoj neprekidnosti

Konačno dobijamo

$$\begin{aligned}\left|\sum_{i=1}^{n}\int_{t_{i-1}}^{t_i}[f(t)-f(t_i)]\sin\lambda t dt\right| &\leq \sum_{i=1}^{n}\int_{t_{i-1}}^{t_i}|f(t)-f(t_i)|\cdot|\sin\lambda t|dt\\ &\leq \sum_{i=1}^{n}\int_{t_{i-1}}^{t_i}|[f(t)-f(t_i)|dt\\ &< \frac{\epsilon}{2(b-a)}\cdot(b-a)=\frac{\epsilon}{2}.\end{aligned}$$

Sa druge strane dobijamo

$$\begin{aligned}\left|\int_{t_{i-1}}^{t_i}\sin\lambda t dt\right| &= \left|-\frac{1}{\lambda}[\cos\lambda t_i-\cos\lambda t_{i-1}]\right|\\ &\leq \frac{|\cos\lambda t_i|+|\cos\lambda t_{i-1}|}{\lambda}\leq\frac{2}{\lambda}\end{aligned}$$

Pošto je funkcija f neprekidna na $[a,b]$ sledi da je ona i ograničena na $[a,b]$, tj. postoji broj $M>0$ takav da je $|f(x)|\leq M$, za sve $x\in[a,b]$. Imajućo ovo u vidu dobijamo

$$\begin{aligned}\left|\sum_{i=1}^{n}f(t_i)\int_{t_{i-1}}^{t_i}\sin\lambda t dt\right| &\leq M\sum_{i=1}^{n}\left|\int_{t_{i-1}}^{t_i}\sin\lambda t dt\right|\\ &\leq M\sum_{i=1}^{n}\frac{2}{\lambda}=\frac{2Mn}{\lambda}\end{aligned}$$

Izaberimo sada takvo λ da važi $\lambda>\frac{4Mn}{\epsilon}$. Za to λ važi.

$$\begin{aligned}\left|\int_a^b f(t)\sin(\lambda t)dt\right| &\leq \left|\sum_{i=1}^{n}\int_{t_{i-1}}^{t_i}[f(t)-f(t_i)]\sin\lambda t dt\right| \\ &\quad+\left|\sum_{i=1}^{n}f(t_i)\int_{t_{i-1}}^{t_i}\sin\lambda t dt\right|\\ &< \frac{\epsilon}{2}+\frac{2Mn}{\lambda}<\frac{\epsilon}{2}+\frac{\epsilon}{2}=\epsilon.\end{aligned}\tag{1.3.1}$$

Pošto je ϵ bulo proizvoljno seldi da je $\lim_{\lambda\to\infty}\int_a^b f(t)\sin(\lambda t)dt=0$. □

Sada želimo da zapišemo naš početni integral u obliku koji će nam dozvoliti da primenimo predhodnu lemu. Neka je c proizvoljan pozitivan broj. Uvedimo smenu $x=\lambda t, dx=\lambda dt$, dobijamo

$$\lim_{\lambda\to+\infty}\int_0^c\frac{\sin\lambda t}{t}dt=\lim_{\lambda c\to+\infty}\int_0^{\lambda c}\frac{\sin x}{x}dx=I\tag{1.3.2}$$

Odavde sledi da Dirihleov integral može biti zapisan kao granična vrednost

integrala na konačnom intervalu. Ali na prvi integral se lema ne može primeniti jer funkcija $f(t) = \frac{1}{t}$ nije neprekidna na intervalu $[0, c]$.

Pronadjimo funkciju g takvu da je funkcija f, koja je definisana sa

$$f(x) = \frac{1}{x} - \frac{1}{g(x)} = \frac{g(x) - x}{xg(x)}, x \neq 0,$$

bude neprekidna na zatvorenom intervalu $[0, c], c > 0$. Drugim rečima, mi zahtevamo da $\lim_{x\to 0} f(x)$ postoji i bude jednak $f(0)$. Pretpostavimo sada da $\lim_{x\to 0} g(x) = 0$ i $g'(x)$ postoji. Primenjujući Lopitalovo pravilo dobijamo

$$\lim_{x\to 0} f(x) = \lim_{x\to 0} \frac{g(x) - x}{xg(x)} = \lim_{x\to 0} \frac{g'(x) - 1}{g(x) + g'(x)x}.$$

Pretpostavimo sada da $\lim_{x\to 0} g'(x) = 1$ i da $g''(x)$ postoji, onda primenjujući ponovo Lopitalovo pravilo dobijamo

$$\lim_{x\to 0} f(x) = \lim_{x\to 0} \frac{g'(x) - 1}{g(x) + g'(x)x} = \lim_{x\to 0} \frac{g''(x)}{2g'(x) + g''(x)x}.$$

Ako još prtpostavimo da je i $\lim_{x\to 0} g''(x) = 0$, i primetimo da je f neprekidno, onda dobijamo

$$\lim_{x\to 0} f(x) = \lim_{x\to 0} \frac{g''(x)}{2} = 0 = f(0).$$

Iz predpostavki za funkciju g možemo još zaključiti da mora da važi i $\lim_{x\to 0} g(x) + g''(x) = 0$. Sve ove pretpostavke navode da je jedan ok kandidata za funkciju $g(t) = \sin t$. Neposrednom proverom se dobija da funkcija $\sin t$ zadovoljava sve tražene uslove. Definišimo funkciju

$$f(t) = \begin{cases} \frac{1}{t} - \frac{1}{\sin t} & , t > 0 \\ 0 & , t = 0 \end{cases}.$$

Iz diskusije gore, sledi da je f neprekidna na intervalu $[0, c]$, ako $0 \leq c < \pi$. Sada na funkciju f možemo primeniti lemu 1.3.4 i dobijamo[3]

$$\lim_{\lambda\to+\infty} \int_0^c \frac{\sin \lambda t}{t} dt = \lim_{\lambda\to+\infty} \int_0^c \frac{\sin \lambda t}{\sin t} dt. \tag{1.3.3}$$

Iz jednačine 1.3.2 znamo da je leva strana poslednje jednačine jednaka integralu kojeg želimo da izračunamo. Ako izračunamo izraz sa desne strane jednačine 1.3.3 i njegova vrednost bude jednaka sa $\frac{\pi}{2}$ dokazaćemo tvrdjenje. Primetimo još da umesto λ možemo staviti bilo koji izraz koji teži ka beskonačnosti.

Dokažimo sledeći identitet

$$1 + 2\cos 2t + 2\cos 4t + \cdots + 2\cos 2nt = \frac{\sin(2n+1)t}{\sin t} \tag{1.3.4}$$

[3]Primenom aditivnosti nesvojstvenog integrala i osobina limesa.

Iz identiteta $\sin a - \sin b = 2\sin\left(\frac{a-b}{2}\right)\cos\left(\frac{a+b}{2}\right)$ dobijamo

$$\sin(2k+1)t - sin(2k-1)t = 2\sin t\cos(2kt).$$

Na kraju dobijamo,

$$\begin{aligned} 1+2\cos 2t+2\cos 4t+\cdots+2\cos 2nt &= 1+ \frac{1}{\sin t}\left[\sum_{k=1}^{n}\sin(2k+1)t-\sin(2k-1)t\right] \\ &= 1+\frac{1}{\sin t}[\sin(2n+1)t-\sin t] \\ &= \frac{\sin(2n+1)t}{\sin t.} \end{aligned}$$

U jednačini 1.3.3 λ možemo zameniti izrazom $2n+1$, zato što $2n+1 \to +\infty$, kada $n \to +\infty$. Pošto jednačina 1.3.3 važi za sve $c \in [0,\pi)$ možemo integraliti obe strane jednačine 1.3.4 na intervalu $[0, \frac{\pi}{2}]$, pa dobijamo

$$\begin{aligned} \int_0^{\frac{\pi}{2}} \frac{\sin(2n+1)t}{\sin t}dt &= \int_0^{\frac{\pi}{2}}(1+2\cos 2t+2\cos 4t+\cdots+2\cos 2nt)dt \\ &= \frac{\pi}{2}+\left[\sin 2t+\frac{\sin 4t}{2}+\cdots+\frac{\sin 2nt}{n}\right]_0^{\frac{\pi}{2}} \\ &= \frac{\pi}{2}. \end{aligned}$$

Iz 1.3.3 za $c = \frac{\pi}{2}$ dobijamo

$$\lim_{\lambda\to+\infty}\int_0^{\frac{\pi}{2}}\frac{\sin\lambda t}{t}dt = \lim_{\lambda\to+\infty}\int_0^{\frac{\pi}{2}}\frac{\sin\lambda t}{\sin t}dt = \lim_{n\to+\infty}\int_0^{\frac{\pi}{2}}\frac{\sin(2n+1)t}{\sin t}dt = \frac{\pi}{2}.$$

Konačno iz jednačine 1.3.2 imamo

$$\int_0^{\infty}\frac{\sin x}{x}dx = I = \lim_{\lambda\to+\infty}\int_0^{\frac{\pi}{2}}\frac{\sin\lambda t}{t}dt = \frac{\pi}{2},$$

što je i trebalo pokazati. □

1.4 Zaključak

U ovom radu izloženo je jedno od mogućih rešenje Dirigleovog integrala. Pri rešavanju ovog integrala korušćene su samo teoreme i metode realne analize funkcija jedne promenjive, što pokazuje da se i elementarnim metodama mogu rešiti veoma kompleksni problemi. Ovim radom želeo bih da podstaknem mlade studente, koji se još nisu susretali sa kompleksnom i furijevom analizom, da traže elementarne metode za rešavanjem sličnih problema, izračunavanje nesvojstevnih integrala funkcija koje nemaju primitivnu funkciju u klasi elementarnih funkcija.

Za druge metode rešavanja ovog integrala pogledati [3].

Deo 2

Teorijski model kvantnog računara

2.1 Uvod

Počeci računarstva datiraju vekovima unazad i sežu do starih Vavilonaca oko 1750. godine pre nove ere (p.n.e.). Vavilonci su razvili za svoje vreme veoma sofisticirane ideje o tačno definisanim koracima ka ostvarivanju zadatog cilja, što je bila osnova za definisanje koncepta koji je početkom 19. veka dobio naziv „Algoritam" [18].

Prva primena algoritama u računarskim tehnologijama u obliku strogih matematičkih definicija - formalizma [18] bila je 1936. godine. Matematičar Alan Tjuring (Alan Turing) objavio je rad u kome daje detaljan apstraktni opis onoga što je danas poznato kao „Tjuringova mašina." [28] Tjuringova mašina je hipotetička računarska mašina koja služi da odredi da li se neki matematički problem može rešiti korišćenjem nekog od ponudjenih algoritama. Suštinski, Tjuringova mašina je merni instrument za testiranje odredjenih algoritama, u praksi, u odnosu na konačni broj tačno definisanih koraka. Po principu ekvivalencije ako neki matematički problem ima definisan algoritam koji vodi ka rešenju, Tjuringova mašina će ga takodje uspešno rešiti. Iako se čini jednostavnim, model Tjuringove mašine predstavlja najopštiji matematički oblik računanja.

Na osnovu koncepta Tjuringove mašine konstruisani su prvi računari sa vakumskim cevima kao osnovnim komponentama. Iako su predstavljali revolucionaran pronalazak za svoju epohu, računari sa cevima su imali ozbiljne nedostatke u svakodnevnoj primeni. Bili su glomazni, trošili su veliku količinu energije, pregrevali se i često se kvarili. Prekretnica u konstrukciji računara došla je sa razvojem prvog tranzistora 1947. godine. Tranzistori u računarima su pronašli široku primenu i zamenili vakumske cevi. Računari postaju manji, troše manje energije i pouzdaniji su u svakodnevnom radu.

Gordon Mur (Gordon Moore) je 1965. godine pretpostavio da će se računarska moć svakih 18 do 24 meseca udvostručiti [17]. Praksa je dokazala Murovu smelu pretpostavku tako da je ta tvrdnja postala poznata kao „Murov zakon" (Moore's law). Od šezdesetih godina prošlog veka pa sve do danas ovaj zakon se ispostavio približno tačnim. 1973. godine kada je proizveden Intelov

8008 mikroprocesor zasnovan na tranzistorskoj tehnologiji pa do 2008. godine performanse računara su uvećane za 2^{23} odnosno preko osam miliona puta!

Većina eksperata smatra da se Murov zakon može održati najkasnije do kraja 2020. godine. Prognoza naučnika o vremenskim ograničenjima Murovog zakona zasniva se na činjenici da smanjenjem veličine komponenata mikroprocesora ispod sopstvene De Broljevske (De Brolil) talasne dužine, kvantni efekti utiču na stabilnost rada procesora. Naime, Hajzenbergova relacija neodredjenosti ukazuje da u odredjenom kritičnom momentu smanjivanja fizičkih karakteristika komponente dolazi do ispoljavanja talasnih svojstava čestice te se gube korpuskularna svojstva čestica i samim tim osnovne karakteristike i funkcije procesora [12].

Jedno od mogućih rešenja ovog problema i mogućnost da se Murov zakon održi pronalazimo u teoriji kvantnih računara.

2.1.1 Istorija kvantnih računara

Krajem 19. veka Lord Kelvin je izjavio:„ Na vedrom nebu fizike pojavila su se dva tamna oblaka koja najavljuju buru u svetu fizike" [13]. Naime, pojavljuju se problemi vezani za strukturu materije- atome i problemi elektromagnetnog zračenja tela na koje Njutnova mehanika, Maksvelova elektrodinamika i klasična termodinamika ne mogu dati teorijsko rešenje. Max Plank (Max Planc) 1900. godine predlaže rešenje elektromagnetnog zračenja tela uvodeći pojam „kvant energije". Kvant energije je najmanja promena energije koje telo moze da emituje ili apsorbuje i iznosi:

$$E = h\nu \tag{2.1.1}$$

gde je E energija kvanta zračenja, h Plankova konstanta i ν frekvencija zračenja. Ova, na prvi pogled jednostavna, pretpostavka je jedan od osnovnih temelja moderne kvantne mehanike. Suštinski, kvantna mehanika je matematički alat ili skup pravila za modeliranje teorija u fizici. Metaforički možemo reći:

> *Kvantna mehanika je za fizičku teoriju ono što je operativni sistem računara za računarski program.*[19, str. 2]

Kvantna mehanika opisuje ponašanje kvantnih sistema. Kvantni sistem je svaki sistem čestica koji se podvrgava zakonima kvantne mehanike. Sedamdesetih godina prošlog veka, sa razvojem računara, fizičari su pokušavali da kvantne sisteme simulišu na računarima, ali sa malo uspeha. Naime, za sistem od N čestica potrebno je 2^{n} podataka da bi se on uspešno računarski predstavio [6]. To znači da sa porastom broja čestica količina memorije potrebna za predstavljanje sistema eksponencijalno raste, a samim tim i vreme obrade podataka. Prve simulacije kvantnih sistema na računarima bile su spore, neefikasne i mogle su se primeniti na sisteme sa malim brojem čestica.

Ova svojstva kvantnih sistema u svrhe modeliranja mašina za računanje prvi je iskoristio fizičar Ričard Fejnman (Richard Feynman) 1981. godine

[6] kada je predložio prvi teorijski model kvantnog računara. Kvantni računar je kvantno mehanički sistem koji obradjuje informacije koristeći zakone kvantne mehanike. Fajnmen je pretpostavio da bi takav sistem omogućio eksponencijalno ubrzanje simulacije kvantno mehaničkih sistema i eksponencijalno ubrzanje pojedinih algoritama iz klasičnog računarstva.

Iste godine, Tomaso Tofoli (Tomasso Toffoli) predložio je univerzalni skup kvantnih operacija sa kojima bi se mogao simulirati svaki algoritam za kvantni računar. Iako je Tofolijev matematički alat bio razvijen, naučnici toga doba nisu uspevali da pronadju kvantne algoritme za kvantne računare koji su bili efikasniji od onih za klasične računare. Zbog toga u naučnom svetu nije bilo mnogo interesovanja za fizičko implementiranje kvantnih računara.

Prekretnica u razvoju kvantnih računara došla je sa Piterom Šorom (Peter Shor) 1995. godine osmislivši kvantni algoritam za rastavljanje velikih brojeva na proste faktore- faktorisanje brojeva.Šorov algoritam bi faktorisanje izvršavao eksponencijalno brže nego klasični algoritam [24]. Ovo svojstvo kvantnog računara moguće je koristiti za dešifrovanje kodova koji imaju široku primenu digitalnim komunikacijama. Kao i uvek, kada su inovacije iz oblasti kriptografije trebale da se implementiraju, Američka vojska počinje da ulaže velike svote novca u istraživanja fizičkih implementacija kvantnih računara.

Lov Grover (Lov Grover) 1996. godine osmislio je kvantni algoritam koji u nesortiranoj bazi od N podataka moze da pronadje traženi u podatak u $\sqrt{n}$ koraka, istu operaciju klasični računar izvrši u N koraka [11]. Nakon Groverovog pronalaska Američka kompanija International Buissenes Machines (IBM) zajedno sa naučnicima univerziteta Stanford i Massachusetts Institute of Technology (MIT) 1998. godine uspešno su izvršili Groverov algoritam na kvantnom računaru koji radi na 3 bita kvantnih podataka- Qbit-a. Iako je 3 qubita veoma mala količina informacija to je dokaz da kvantni računari mogu biti fizički konstruisani.

Fizičke implementacije kvantnih računara je veoma teško ostvariti. Trenutno ne postoje tehnološke metode koje bi efikasno zaštitile kvantne sisteme od spoljašnjih uticaja [22]. Praktično, i veoma slab intenzitet kosmičkog zračenja moze da poremeti sistem kvantnog računara [22]. Zbog toga fizičke implementacije kvantnih računara nisu postigle uspehe kolike i teorijski model. Trenutno najsofiticiraniji fizički model kvantnog računara konstruisan je početkom 2011 godine i vrši operacije na 14 Qbita [16].

2.2 Matematički model kvantnog računara

Kvantni računar je kvantno mehanički sistem koji obradjuje informacije koristeći zakone kvantne mehanike. Za opisivanje stanja kvantnog računara koristi se vektorsko prikazivanje kvantnog sistema koju je uveo fizičar Pol Dirak (Paul Dirac). U osnovi ovog načina predstavljanja podataka leži linearna algebra, sa razlikom u obeležavanju vektora. Vektor u Dirakovom načinu prestavljanja podataka ima oznaku:

$$\overrightarrow{v} = |v\rangle \,. \tag{2.2.1}$$

Paulijeve matrice

U kvantnom računarstvu postoje četiri matrice koje se veoma često koriste i nazivaju se *Paulijeve matrice*, a ime su dobile po fizičaru Volfgangu Paujiju (Wolfgang Pauli). To su matrice veličine 2 sa 2 i u zavisnosti od autora drugačije se obeležavaju. Paulijeve matrice i neke od načina obeležavanja možete videti u prikazu 2.1.

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Prikaz 2.1: Paulijeve matrice i njihova obelezavanja

2.2.1 Postulati kvantne mehanike

Kvantna mehanika je matematički alat za razvijanje fizičkih teorija. Sama po sebi kvantna mehanika ne odrdjuje fizičke zakone kojima se neki sistem podvrgava, ali ona daje matematičke alate i koncepte za razvijanje takvih zakona. U ovom delu rada biće izloženi neki od postulata kvantne mehanike koji su bitni za proučavanje kvantnih računara. Ovi postulati daju vezu izmedju fizičkog sveta i matematičkog formalizma kvantne mehanike.

U stručnoj literaturi u zavisnosti od autora javljaju se različite formulacije postulata kvantne mehanike u okviru ovog rada biće izloženi postulati kvantne mehanike koji se javljaju u knjigama [19] i [5]. Postulati koji su ovde izloženi neposredno su povezani sa radom kvantnih računara i principe njihovog rada i nisu jedini postulati kvantne mehanike.

Prostor stanja

Prvi postulat kvantne mehanike definiše prostor u kome su matematičke formule kvantne mehanike primenjive.

Postulat 1. *Za svaki izolovani fizički sistem postoji kompleksan vektorski prostor sa unutrašnjim proizvodom (Hilbertov prostor*[1]*), tj. postoji* prostor stanja *sistema. Sistem je u potpunosti opisan njegovim* vektorom stanja $|\psi\rangle$[2]*,koji je jediničnivektor u prostoru stanja.*

Uzmimo u obzir najjednostavniji kvantni sistem *qbit*. Qubit ima dvodimenzionalni prostor stanja i njegovi ortonormalni bazisni vektori su $|0\rangle$ i $|1\rangle$. Onda vektor stanja možemo zapisati kao linearnu kombinaciju

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.2.2}$$

vektora $|0\rangle$ i $|1\rangle$, gde su a i b kompleksni brojevi. Uslov da $|\psi\rangle$ mora biti jediničan vektor znači da mora biti ispunjen i uslov $|a|^2 + |b|^2 = 1$. Taj uslov se još naziva i *uslov normalizacije*.

Evolucija sistema

Način opisivanja promene vektora stanja $|\psi\rangle$ sa vremenom, dat je sledećim posutlatom.

Postulat 2. *Evolucija* zatvorenog *kvantnog sistema opisana je* unitarnom transformacijom. *Stanje $|\psi\rangle$ sistema u trenutku t_1 povezano je sa stanjem $|\psi'\rangle$ sistema u trenutku t_2 unitarnim operatorom U koji zavisi samo od trenutaka t_1 i t_2,*

$$|\psi'\rangle = U\,|\psi\rangle \tag{2.2.3}$$

Kvantna mehanika ne daje odgovor na pitanje koji unitarni operator opisuje realni fizički sistem ali ona garantuje da takav operator postoji. Za sistem jednog qbita, koji je najvažniji sistem za rad kvantnog računara, pokazano je da *svaki* unitarni operator može biti fizički realizovan [19, str. 81].

Postulat 2 zahteva da kvantni sistem bude zatvoren, što znači da kvantni sistem koji želimo da proučavamo mora biti izolovan od spoljnih uticaja, tj. ne sme biti u interakciji sa drugim sistemima. Suštinski svi sistemi, osim Univerzuma kao celine, su na nekom nivou u interakciji sa drugim sistemima. Praktično gledano, postulat 2 je do odredjene granice dobra aproksimacija pojedinih sistema, medju kojima je i sistem qbita [19, str. 82].

Postulat 2 opisuje vezu dva kvantna stanja u dva različita vremenska trenutka, tj. opisuje sistem u diskretnom vremenu. Ovaj način opisivanja pogodan je teoretsko proučavanje kvantnog računara, ali za proučavanje fizičkih osobina kvantnog računara potrebno je ovaj postulat proširiti na sledeći način.

Postulat 3. *Vremenska evolucija zatvorenog kvantnog sistema opisana je Šredingerovom jednačinom (Schrödinger equation):*

$$i\hbar\frac{d\,|\psi\rangle}{dt} = \hat{H}\,|\psi\rangle\,, \tag{2.2.4}$$

[1]Hilbertov prostor je generalizacija prostora $\mathbb{C}^n$

[2]U opštem slučaju vektor stanja je rešenje Šredingerove jedančine

gde je $\hbar$ Dirakova konstanta, i imaginaran jedinica, a operator $\hat{H}$ je Hamiltonijan[3] *zatvorenog sistema.*

U ovom delu rada dok budemo proučavali teorijski model računara pozivaćemo se samo na postulat 2, a za fizički opis kvantnog računara pozivaćemo se na postulat 3.

Kvantno merenje

Prethodna dva postulata daju opis evolucije zatvorenog sistema koji nije u interakciji sa bilo kojim drugim sistemom, ali mora postojati trenutak u evoluciji sistema kada spoljašnji fizički sistem- posmatrač dolazi u kontakt sa tim sistemom. Ovaj postupak se zove kvantno merenje i neophodan je da bi se utvrdilo ponašanje sistema. Kada posmatrač stupi u kontakt sa zatvorenim kvantnim sistemom on prestaje da bude zatvoren i za njega više ne važe postulati 2 i 3. U okviru ovog rada neće biti izložen detaljan matematički opis kvantnog merenja već samo neophodni koncepti kvantnog merenja neposredno važni za razumevanje kvantnih računara.

Posmatrajmo sistem qbita koji ima 2 moguća stanja $|0\rangle$ i $|1\rangle$. Za ovaj sistem važi princip superpozicije, pa vektor stanja $|\psi\rangle$ je linearna kombinacija

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle \tag{2.2.5}$$

vektora $|0\rangle$ i $|1\rangle$, a a i b su kompleksni brojevi. Ako izvršimo merenje ovog sistema, posmatrač dodje u kontakt sa sistemom, onda dolazi do „kolapsa" superpozicije i posmatrač opaža da je sistem u stanju $|0\rangle$ ili stanju $|1\rangle$. Verovatnoća opažanja sistema u stanju $|0\rangle$ ili $|1\rangle$ data je kvadratom modula kompleksnog broja a ili b.

Detaljan matematički opis kvantnog merenja izložen je u [19, str. 84-86].

Složeni sistem čestica

Način dobijanja prostora stanja složenog sistema od prostora stanja jednostavnih sistema dat je sledećim postulatom.

Postulat 4. *Ako je Hilbertov prostor $\mathbb{H}_1$ prostor stanja sistema S_1, a Hilbertov prostor $\mathbb{H}_n$ prostor stanja sistema S_n, onda prostor stanja složenog sistema $S_1+\cdots+S_n$ je tenzorski proizvod Hilbertovih prostora $\mathbb{H}_1$ do $\mathbb{H}_n$, $\mathbb{H}_1\otimes\cdots\otimes\mathbb{H}_n$.*

Navedimo jedan jednostavan primer primene ovog postulata. Ako je $|A\rangle$ stanje sistema A i $|B\rangle$ stanje sistema B, onda odgovarajuće stanje u složenom sistemu $A+B$ odgovara vektoru stanja $|A\rangle\otimes|B\rangle$ ili kraće $|AB\rangle$. Rad svakog kvantnog računara koji obradjuje informacije na više od jednog qbita zasniva se na ovom postulatu.

[3]Hamiltonijan je operator koji predstavlja ukupnu energiju zatvorenog sistema

2.2.2 Teorijski model kvantnog računara

Do sada su bili izloženi postulati kvantne mehanike koji su neposredno važni za proučavanje kvantnih računara i dalje diskusije će se zasnivati na tim postulatima. Postulat 1 definiše prostor stanja koji se koristi za opisivanje zatvorenog kvantnog sistema. Postulati 2 i 3 govore da dinamika zatvorenog kvantnog sistema opisana je Šredingerovom jednačinom, a samim tim i unitarnom evolucijom. Kvantno merenje daje odgovor na pitanje kako iz kvantnog sistema dobiti odredjene informacije, a postulat 4 objašnjava kako prostore stanja kombinovati da bi se dobio složeni kvantni sistem. Svaki od uslova ovih postulata mora biti ispunjen da bi se kvantni računara uspešno mogao teorijski predstaviti.

U ovom delu rada objasnićemo dva vodeća koncepta u svetu kvantnih računara. Prvi je fundamentalni modela kvantnog računara, kvantni računar zasnovan na principu kvantnih kola (Quantum Circuit Computer) i u radu biće izložen detaljan opis njegovog rada. Drugi koncept govori o postojanju malog skupa kvantnih operacija koje su *univerzalne*, to znači da svako kvantno kolo može biti predstavljeno preko tih operacija.

Qbit

Bit (Binary Digit) je fundamentalni koncept klasičnog računarstva i klasične informacije. Analogno tome u kvantnom računarstvu fundamentalni koncept je kvantni bit ili kraće qbit (Quantum Binary Digit). Qubit je *matematički objekat* koji ima osobine kvantnog sistema i on je osnovna jedinica kvantne informacije.

Analogno stanjima 0 i 1 klasičnog bita, za stanja qbita uzimaju se stanja $|0\rangle$ i $|1\rangle$. Osnovna razlika izmedju klasičnog bita i qubita je u tome što qbit ne mora da se nalazi samo u diskretnim stanjima $|0\rangle$ i $|1\rangle$ već može da se nadje u superpoziciji tih stanja:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{2.2.6}$$

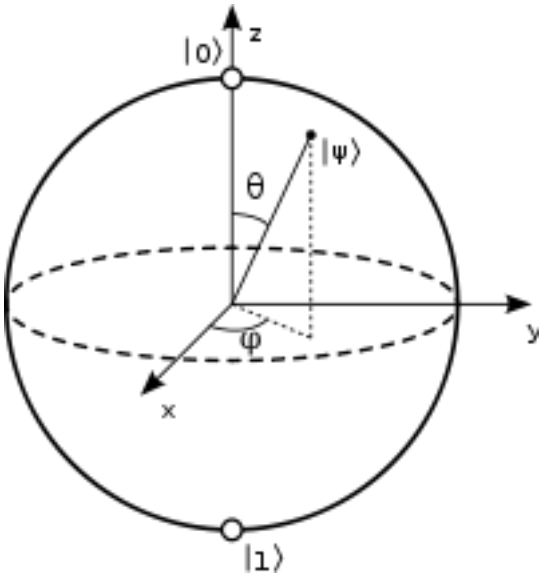
Brojevi α i β su kompleksni brojevi i nazivaju se *amplitude*, a specijalna stanja $|0\rangle$ i $|1\rangle$ zovu se *računarska bazisna stanja* i ona formiraju ortonormalne bazise vektorskog prostora u kom se qbit nalazi.

Za razliku od klasičnog bita, gde u svakom trenutku možemo odrediti da li se bit nalazi u stanju 0 ili 1 (proces očitavanja memorije), da bi odredili stanje qbita moramo izvršiti kvantno merenje. Kvantnim merenjem dolazi do kolpsa superpozicije i opažamo qbit u jednom od diskretnih stanja $|0\rangle$ ili $|1\rangle$. Kvantnim merenjem možemo dobiti stanje $|0\rangle$ sa verovatnoćom $|\alpha|^2$ ili stanje $|1\rangle$ sa verovatnoćom $|\beta|^2$. Tokodje mora biti ispunjen uslov normalizacije $|\alpha|^2 + |\beta|^2 = 1$, jer zbir svih verovatnoća mora biti 1 (100%). Geometrijski to predstavljamo kao jedinični vektor u dvodimenzionalnom prostoru.

Geometrijski qbit može biti predstavljen na sledeći način. Pošto je $|\alpha|^2 + |\beta|^2 = 1$ onda se jednačina 2.2.6 može zapisati kao

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\,. \tag{2.2.7}$$

Brojevi θ i φ su realni brojevi i definišu tačku na jediničnoj trodimenzionalnoj sferi, prikaz **??**. Ova sfera se još naziva i Blok sfera (Bloch sphere). Na Blok sferi postoji beskonačno mnogo tačaka, ali to ne znači da na jednom qbitu može biti skladišteno beskonačno mnogo podataka. Naime posle kvantnog merenja qbit može se može naći samo u stanju 0 ili 1 što znači da qbit može da skladišti istu količinu informacija kao i klasičan bit. Ovu predpostavku Aleksandar Holevo je dokazao 1973. godine i poznata je kao Holevova teorema (Holevo's theorem)[29].



Prikaz 2.2: Blok sfera

Sistem više qbita

Pretpostavimo da imamo sistem od dva qbita. Ako bi to bila dva klasična bita onda bi imali četiri moguća stanja, 00, 01, 10 i 11, u kojima se oni mogu naći. Analogno tome, dva kvantna bita imaju četiri računarska bazisna stanja sa oznakama $|00\rangle$, $|01\rangle$, $|10\rangle$ i $|11\rangle$. Par qubita takodje može biti u superpoziciji ova četiri stanja, gde je svakom računarskom bazisnom stanju dodeljen kompleksni koeficijent- amplituda, tako da vektor stanja je opisan sledećom formulom:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,. \tag{2.2.8}$$

Slično slučaju jednog qbita, verovatnoća merenja kvantnog bita u stanju $|x\rangle$ ($x \in \{00, 01, 10, 11\}$) je $|\alpha_x|^2$. Uslov da zbir verovatnoća mora biti jedan dat je uslovom noramlizacije

$$\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1 \tag{2.2.9}$$

gde $\{0,1\}^2$ označava „skup svih stringova dužine dva čiji znakovi mogu biti 1 ili 0." U sistemu 2 qbita možemo vršiti merenje i samo na jednom qbitu.

Uzmimo primer da vršimo merenje na prvom qbitu, onda verovatnoća da se qbit nalazi u stanju $|0\rangle$ je $|\alpha_{00}|^2 + |\alpha_{01}|^2$, a stanje posle merenja je

$$|\psi'\rangle = \frac{\alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}, \tag{2.2.10}$$

gde je $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ faktor renormalizacije.

Generalno možemo posmatrati sistem od n qbita. Onda računarska bazisna stanja sistema su oblika $|x_1 x_2 \dots x_n\rangle$, a broj računarska bazisna stanja je 2^n, a samim tim to je i broj amplituda. Za $n = 500$ broj amplituda premašio bi broj atoma u kosmosu, a pokušaj da se takav broj qbita predstavi na klasično računaru je nemoguć. Iz toga sledi da je moguće simulirati samo kvantne računare sa malim brojem qbita.

Jedno-qubitne kvantne kapije

Promene na kvantnim stanjima qbita mogu biti opisane jezikom *kvantnog računarstva*. Analogno klasičnim računarima koji su izgradjeni od *električnih kola* koja se sastoje iz *provodnika* i *logičkih kapija*, kvantni računari izgradjeni su od *kvantnih kola* koja *sadrže provodnike* i *elementarne kvantne kapije*. U klasičnim kolima provodnici prenose informacije, dok logičke kapije manipulišu tim informacijama.

Uzmimo primer jedne klasične logičke kapije koja izvršava operacije na jednom bitu. Jedini pripadnik ove klase je logička NE kapija, čije su operacije definisane *tablicom istinitosnih vrednosti*, u kojoj $0 \to 1$ i $1 \to 0$, tj. stanja 1 i 0 su obrnuta.

Analogno klasičnoj NE kapiji definiše se kvantna NE kapija koja stanje

$$\alpha\,|0\rangle + \beta\,|1\rangle \tag{2.2.11}$$

linearno preslikava u stanje u kojem su uloge bazisa $|0\rangle$ i $|1\rangle$ obrnute,

$$\alpha\,|1\rangle + \beta\,|0\rangle\,. \tag{2.2.12}$$

Linearnost kvantnih kapija sledi iz generalnih svojstava kvantne mehanike i linearnost mora biti zadržana u svim operacijama nad kvantnim bitima. U slučaju da kvantne kapije ne deluju linearno na qbite to bi moglo dovesti do paradoksa kao što su putovanje kroz vreme, komunikacije brže od svetlosti i kršenja drugog zakona termodinamike.

Kvantnu NE kapiju možemo predstaviti i pomoću matrice čija svojstva slede direktno iz linearnosti kvantnih kapija. Definišimo matricu X, koja predstavlja kvantnu NE kapiju, na sledeći način:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.2.13}$$

Stanje $\alpha\,|0\rangle + \beta\,|1\rangle$ predstavimo matričnim oblikom

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix}, \tag{2.2.14}$$

gde prvi red predstavlja amplitudu koja odgovara stanju $|0\rangle$, a drugi red odgovara stanju $|1\rangle$, onda izlaz kvantne NE kapije definisan je na sledeći način:

$$X\begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \begin{bmatrix}\beta\\ \alpha\end{bmatrix}. \tag{2.2.15}$$

Kvantne kapije koje deluju na jedan qbit predstavljaju se matricama veličine 2×2. Da bi neka matrica predstavljala kvantnu kapiju jedini uslov koji mora ispuniti je unitarnosti. Matrica U je *unitarna* ako i samo ako

$$U^\dagger U = I, \tag{2.2.16}$$

gde je $U^\dagger$ adjungovana matrica U, a I jedinična matrica. Unitarnost garantuje da će uslov normalizacije biti očuvan pre i posle primene kvantne kapije.

Za razliku od klasičnog računarstva gde postoji samo jedna ne-trivijalna logička kapija- NE kapija za jedan bit, u kvantnom računarstvu postoji mnoštvo ne-trivijalnih kvantnih kapija za jedan qbit. Dve veoma važne kvantne logičke kapije koje će mo u radu često koristiti su Z kapija:

$$Z \equiv \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \tag{2.2.17}$$

koja stanje $|0\rangle$ ne menja, a stanju $|1\rangle$ menja znak u $-\,|1\rangle$, i Adamardova kapija (Hadamard gate):

$$H \equiv \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}. \tag{2.2.18}$$

Adamardova kapija deluje isto kao i „kvadratni koren NE" kapije, tako što stanje $|0\rangle$ prebacuje u stanje $(|0\rangle + |1\rangle)/\sqrt{2}$, „pola puta" izmedju $|0\rangle$ i $|1\rangle$, a stanje $|1\rangle$ prebacuje u stanje $(|0\rangle - |1\rangle)/\sqrt{2}$, „pola puta" izmedju $|0\rangle$ i $|1\rangle$. Adamardova kapija je jedna od najvažnijih i najkorisnijih kapija u kvantnom računarstvu.

Postoji beskonačno mnogo unitarnih matrica, a samim tim i beskonačno mnogo jedno-qbitnih kvantnih kapija, ali je pokazano [19, str. 174] da se svaka jedno-qbitna kvantna kapija može predstaviti na sledeći način:

$$U = e^{i\alpha}\begin{bmatrix}e^{-i\beta/2} & 0\\ 0 & e^{i\beta/2}\end{bmatrix}\begin{bmatrix}\cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2}\\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2}\end{bmatrix}\begin{bmatrix}e^{-i\delta/2} & 0\\ 0 & e^{i\delta/2}\end{bmatrix}, \tag{2.2.19}$$

gde su α, β, γ i δ realni brojevi.

Više-qbitne kvantne kapije

U klasičnom računarstvu jedna od često korištenih logičkih kapija je ekskluzivana-ili kapija ili XOR kapija. Analogno njoj u kvantnom računarstvu javlja se *kontrolisana*-NE ili CNOT kapija. Ova kapija ima dva ulazna qbita, *kontrolni* qbit i *ciljni* qbit. Rad CNOT kapije je opisan na sledeći način. Ako je kontrolni qbit u stanju 0, onda se na ciljnom qbitu ne vrše promene, a ako je kontrolni qbit u stanju 1, onda se ciljnom qbitu stanja obrnu,

$$|00\rangle \to |00\rangle\,; |01\rangle \to |01\rangle\,; |10\rangle \to |11\rangle\,; |11\rangle \to |10\rangle\,. \tag{2.2.20}$$

Drugi način predstavljanja CNOT kapije jeste generalizacija XOR kapije, pošto se dejstvo CNOT kapije može predstaviti kao $|A, B\rangle \to |A, B \oplus A\rangle$, gde je $\oplus$ oznaka sabiranje po modulu dva[4], a to je ista funkcija koju vrši i XOR kapija. Još jedan način da se CNOT kapija predstavi jeste pomoću matrice:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.2.21}$$

Generalno da bi se matrično predstavila kvantna kapija koja deluje na n qbita potrebna je $n \times n$ matrica. Takva matrica mora biti unitarna da bi se očuvao uslov normalizacije.

Pokazano je da se svaka kvantna operacija može predstaviti pomoću univerzalne kvantne kapije 2.2.19 i CNOT kapije [19, str. 191-195].

Bitna razlika izmedju kvantnih i klasičnih logičkih kapija jeste *reverzabilnost*. Naime ako uzmemo bilo koju klasičnu logičku kapiju, na osnovu stanja njenog izlaza ne možemo odrediti stanja na njenom izlazu što znači da je takva operacija *ireverzabilna*. Odlika kvantnih kapije je u tome što za proizvoljunu kvantnu kapiju uvek na osnovu stanja na njenom izlazu možemo rekonstruisati stanje na njenom ulazu. Reverzabilnost kvantnih kapija direktno sledi iz unitarnosti kvantnih kapija [19, str. 21].

Kvantna kola

U klasičnom računarstvu spajanjem jednostavnih logičkih kapija provodnicima dobijaju se *logička kola*. Analogno tome, u kvantnom računarstvu spajanjem kvantnih kapija provodnicima dobijamo kvantna kola.

Uzmimo u obzir jednostavno kvantno kolo, sastavljeno od tri kvantne kapije, koje vrši zamenu dva qbita, prikaz **??**. Ovo kolo se čita sa levo na desno. Svaka linija u kolu predstavlja *provodnik* u kvanotnom kolu. Provodnik ne mora da predstavlja fizičku žicu, on može da predstavlja promenu vremena ili česticu koja se kreće u prostoru. Ako nije drugačije naznačeno smatra se da su početna stanja svakog qbita $|0\rangle$. Kolo u prikazu **??** zamenjuje stanja bita

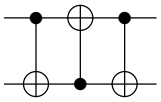
[4] $p \oplus q = (p \wedge \neg q) \vee (\neg p \wedge q)$

na sledeći način:

$$\begin{aligned} |a,b\rangle &\to |a, a\oplus b\rangle \\ &\to |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\to |b, (a\oplus b)\oplus b\rangle = |b,a\rangle\,. \end{aligned} \tag{2.2.22}$$

Treba naglasiti da nije moguće napraviti kopiju qbita, [19, str. 24-25]

Osnovne standardne oznake koje se koriste u kvantnim kolima detaljno su objašnjene u [19, str. xxiv]. Pomoću tih kola može se predstaviti svaki kvantni algoritam što implicira da su ta kola *univerzalna*.



Prikaz 2.3: Kvantno kolo za zamenu dva qbita

Belovo stanje

Uzmimo u obzir slučaj kvantnog kola predstavljenog u prikazu 2.4, koje je sastavnjeno od Adamardove kapije praćene CNOT kapijom. Na primer, Adamardova kapija ulaz $|00\rangle$ prevodi u stanje $(|0\rangle + |1\rangle)/\sqrt{2}$ i onda CNOT kapija daje izlazno stanje $(|00\rangle + |11\rangle)/\sqrt{2}$. Drugim rečima Adamardova transformacija prvo gornji qbit prevodi u superpoziciju stanja, zatim taj qbit deluje kao kontrolni qbit CNOT kapije, na kraju ciljni qbit je invertovan samo ako je kontrolni qbit 1. Izlazna stanja su

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; \tag{2.2.23}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}; \tag{2.2.24}$$

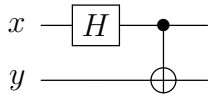
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \tag{2.2.25}$$

$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.2.26}$$

Ova stanja su poznata pod imenima *Belova stanja* (Bell states), *EPR* stanja ili ponekad *EPR* parovi. Naziv EPR stanja izveden je od prvih slova imena naučnika koji su prvi ukazali na postojanje ovakvih stanja- Ajnštajn (Einstein), Podolski (Podolsky), Rozen (Rosen), a naziv Belova stanja dat je u čast naučniku Džonu Belu (John S. Bell). Ustaljene oznake $|\beta_{00}\rangle\,, |\beta_{01}\rangle\,, |\beta_{10}\rangle\,, |\beta_{11}\rangle$ mogu se objasniti sledećom formulom

$$|\beta_{xy}\rangle \equiv \frac{|0,y\rangle + (-1)^x\,|1,\bar{y}\rangle}{\sqrt{2}}, \tag{2.2.27}$$

gde je $\bar{y}$ negacija od y.



Prikaz 2.4: Kvantno kolo za dobijanje Belovog stanja

2.3 Kvantni algoritmi

Analogno algoritmu iz klasičnog računarstva *kvantni algoritam* se definiše kao konačan skup koraka za izračunavanje nekog računarskog problema na kvantnom računaru. Kvantni algoritmi su podeljeni na tri grupe. Prvu čine algoritmi zasnovani na kvantnoj verziji *Furijeve transformacije*. Šorov algoritam za faktorisanje brojeva je jedan od algoritama iz te grupe. Drugu grupu čine kvantni algoritmi za pretragu, kao na primer *Groverov algoritam*. Treća grupa su algoritmi za kvantne simulacij. U okviru ovog rada zadržaćemo se samo na prve dve grupe algoritama.

2.3.1 Kvantni algoritmi zasnovani na Furijevoj transformaciji

Diskretna Furijeva transformacija obično je predstavljena kao transformacija skupa $x_0, \ldots, x_{N-1}$ N kompleksnih brojeva u skup kompleksnih brojeva $y_0, y_1, \ldots, y_{N-1}$ definisana da formulom:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \tag{2.3.1}$$

Ova transformacija je veoma korisna u mnogim granama nauke, pa i u kvantnom računarstvu, jer problem trnsformisan Furijevom transformacijom češće je lakši nego ne transformisani. Jednačina 2.3.1 može biti proširena da bi se dobila kvantna verzija ove transformacije.

Definišimo linearnu transformaciju U na n qbita koja bazisno stanje $|j\rangle$, gde je $0 \leq j \leq 2^n - 1$, transformiše na sledeći način:

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \,. \tag{2.3.2}$$

Pokazuje se da je ova transformacija unitarna [19, str. 37].

Na klasčnom računaru za izvršavanje brze Furijeve transformacije potrebno je $N \log N = n2^n$ koraka da bi se faktorisalo $N = 2^n$ brojeva. Kvantni računar istu transformaciju izvrši u $\log^2 N = n^2$ koraka, što je eksponencijalna ušteda. Pokazalo se da se ova transformacija može se koristiti za efikasno transformisanje vektora stanja razloženog od 2^n kompleksnih brojeva.

Najvažnija primena ove transformacije je u eksponencijalnom ubrzavanju faktorisanja velikih prirodnih brojeva. Detaljniji opis ove transformacije i njenih primena dat je u delu rada 2.3.3.

2.3.2 Kvantni algoritmi za pretragu

Sasvim drugačiju klasu algoritama čine kvantni algoritmi za pretragu koje je osmislio Lov Grover (Lov Grover). Kvantni algoritmi za pretragu rešavaju sledeću vrstu problema: Za dati prostor veličine N, bez predhodnog uvida u

strukturu prostora pretrage, pronaći elemenat sa odredjenim karakteristikama. Klasično ovaj problem se rešava u N koraka, ali je Grover pokazao da kvantni računar može pronaći traženi elemenat u $\sqrt{N}$ koraka.

Ovaj algoritam daje samo kvadratno ubrzanje, u odnosu na eksponencijalno ubrzanje kod furijeve transformacije, ali postoje veliki interesi za njegovo implementiranje jer mnogi problemi u računarstvu zasnivaju se na pretrazi nekog prostora.

2.3.3 Kvantna furijeva transformacija

Najznačajnije otkriće u svetu kvantnih računara jeste mogućnost rešavanja odredjenog računarskog problema na kvantnom računaru efikasnije nego na klasičnom. Jedan od tih problema je faktorisanje prirodnih brojeva na proste faktore. Naime, na klasičnom računaru za faktorisanje n-bitnog prirodnog broja potrebno je oko $e^{n^{1/3}\log^{2/3} n}$ koraka, što znači da vreme izračunavanje eksponencijalno raste sa porastom broja. Za razliku od klasičnog računara, kvantni računar isti račun odradi u oko $n^2 \log n \log\log n$ koraka. Iz ovoga sledi da je kvantni računar za neke probleme eksponencijalno brži u odnosu na klasični.

Faktorisanje brojeva na kvantnom računaru izvršava se zahvaljujući *kvantnoj Furijevoj transformaciji*. U ovom delu rada izložićemo neke od njenih osnovnih osobina, kao i algoritam za njeno izračunavanje.

Transformacija

U odeljku 2.3.1 definisali smo diskretnu Furijevu transformaciju i kvantnu Furijevu transformaciju. Ova transformacija može se predstaviti i u obliku proizvoda i iz tog oblika se izvodi kvantno kolo za izvršavanje kvantne furijeve transformacije.

Uzmimo da je $N = 2^n$, gde je n neki prirodan broj, i bazisna stanja $|0\rangle, \ldots, |2^n - 1\rangle$ su računarska stanja n qbitnog kvantnog računara. Stanje $|j\rangle$ može se predstaviti binarnom reprezentacjom gde je $j = j_1 j_2 \ldots j_n$, tj. formalno $j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$. Uz pomoć elementarnih pravila algebre jednačina 2.3.2 se može predstaviti u sledećem obliku [19, str. 218]:

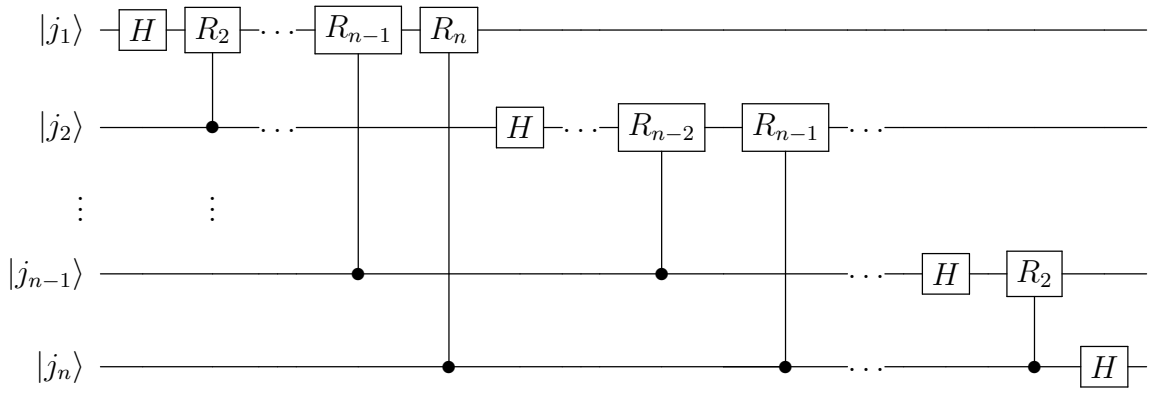
$$|j_1 j_2 \ldots j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)\ldots(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)}{2^{n/2}} \tag{2.3.3}$$

Ovaj oblik kvantne Furijeve transformacije često se u literaturi koristi i kao definicija ove transformacije i koristan je za konstruisanje kvantnog kola za efikasno izračunavanje kvantne Furijeve transformacije, dokazivanje njene unitarnosti i razvijanje algoritama zasnovanih na njoj.

Na prikazu 2.5 dato je efikasno kolo za izračunavanje kvantne furijeve transformacije. Kapija R_k je unitarna transformacija data sledećom matricom:

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}. \tag{2.3.4}$$

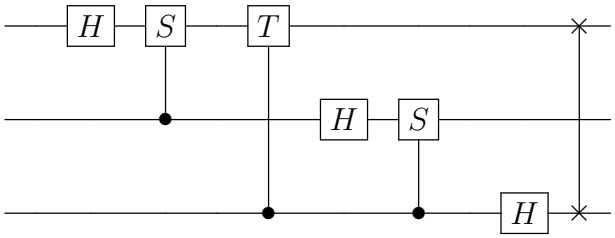
Detaljna analiza ovog kola data je u [19, str. 218-219].



Prikaz 2.5: Efikasno kvantno kolo za kvantnu Furijevu transformaciju

Furijeva transformacija za tri qbita

Pogledajmo kvantno kolo kvantne Furijeve transformacije za tri qubita:



Kapije S i T su redom faza i $\pi/8$ kapije. Ova transformacija se može predstaviti i unitarnom matricom:

$$\frac{1}{\sqrt{8}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}, \tag{2.3.5}$$

gde je $\omega = e^{2\pi i/8} = \sqrt{i}$.

Performanse

Pogledajmo koliko je kvantnih kapija potrebno da bi se izvršila kvantna Furijeva transformacija. Operacija počinje sa Adamarovom kapijom i $n-1$ uslovljenih rotacija na prvom qbitu- ukupno n operacija. Zatim na drugom qbitu se

izvrši Adamarova transformacija praćena sa $n-2$ uslovljenih rotacija- ukupno $n-1$ kvantnih kapija. Nastavljajući ovo na svim qbitima vidimo da je potrebno $n+(n-1)+(n-2)+\cdots+1 = n(n+1)/2$ kvantnih kapija. Sa druge strane, klasičnom računaru za izvršavanje *brze Furijeve transformacije* potrebno je $n2^n$ logičkih kapija, što znači da kvantni računar daje eksponencijalno ubrzanje u odnosu na klasični računar.

Ova osobina kvantnog računara mogla bi se koristiti za prepoznavanje i upravljanje glasom i faktorisanje velikih brojeva.

2.4 Zakljucak

U uvodnom delu rada postavili smo pitanje: "Da li će Murov zakon važiti i do kraja ove decenije." Pretpostavke većine naučnika ne idu u prilog Murovog zakona. Naime, od kraja šezdesetih godina do sada tehnologija proizvodnje poluprovodničkih elemenata, a samim tim i računara, suštinski se nije menjala. Tokom godina, proizvodjači integrisanih kola samo su smanjivali dimenzije poluprovodnika, ne menjajući njihov način rada, što je dovelo da same granice *iscrpljivanja* materijala. Poslednji Intelov[5] skok sa 34 nm[6] tehnologije na 22 nm tehnologiju proizvodnje mikroprocesora smatra možda jednim od poslednjih udvostručavanja računarske moći. Teorijski, zakoni kvantne mehanike i kvantni efekti ne *dopuštaju* procesorske tehnologije manje od 10 nm.

Rešenje ovog problema je napuštanje klasičnih poluprovodničkih tehnologija i istraživanje novih računarskih metoda. Kao što je već ranije rečeno jedno od teorijskih rešenja ovog problema, a samim tim garancija za održanje Murovog zakona, jesu kvantni računari. U praksi, kvantni računari bi koristili kvantne efekte, koji su smetnja rada klasičnih računara, za brže i efikasnije rešavanje računarskih problema. Smatra se da bi kvantni računari doneli, dugo očekivani, eksponencijalni skok u brzini obrade podataka.

2.4.1 Prednosti kvantnih računara

U odeljku rada "Kvantni algoritmi" već je bilo reči o kvantnim algoritmima koji omogućavaju eksponencijalno ubrzavanje odredjenih računarskih problema. Upravo zbog toga, vojska, policija i druge bezbednosne službe ulažu velike svote novca u razvoj kvantnih računara. Uz pomoć kvantnih računara sadašnji klasični *kriptografski* kodovi sa lakoćom be se mogli dešifrovati. Takodje znatno ubrzanje bi dobili i algoritmi za pretragu baza podataka što ubrzao proces identifikacije odredjenih osoba.

Sa druge strane, komercijalni korisnici sa implementacijom kvantnog računara dobili bi veoma visok stepen privatnosti podataka. Za razliku od klasične kriptografije, *kvantna kriptografija* daje metode za enkripciju podakaka koje su skoro nemoguće za dešifrovanje od strane neovlašćenog lica.

Drugi značajan aspekt kvantnog računarstva su *kvantne mreže*. Kvantna mreža je spoj dva ili više računara koji razmenjuju resurse za rešavanje računarskog problema. Implementiranje kvantnih mreža omogućilo bi bržu, efikasniju i sigurniju komunikaciju na globalnom nivou.

U preseku, kvantni računari su brži, efikasniji i sigurniji u odnosu na klasične računare.

2.4.2 Problemi kvantnih računara

Kvantno računarstvo i kvantna informatika su relativno mlade naučne discipline, intenzivno se proučavaju tek tridesetak godina. Upravo zbog toga,

[5]Vodeći proizvodjač mikroprocesora u svetu

[6]Veličina tranzistora

javljaju se problemi koji do sada nisu rešeni.

Prvi problem koji se javlja vezan je za kvantne algoritme. Naime, sredinom devedesetih godina prošlog veka došlo je do ogromnog skoka u kvantnoj informatici sa pronalaskom Šorovog algoritma za faktorisanje brojeva. Kao što je već bilo reči, ovaj algoritam eksponencijalno ubrzava faktorisanje brojeva u odnosu na klasični računar. Smatralo se da će se ubrzo posle ovog pronalaska pronaći i druge klase kvantnih algoritama koji potvrdjuju računarsku nadmoć kvantnih računara u odnosu na klasične. Ako pogledamo period od pronalaska Šorovog algoritma do danas možemo videti da nije došlo do značajnog teorijskog napretka na polju kvantne informatike. Do danas teorija kvantnih algoritama još nije dovoljno istražena i razjašnjena [25].

Drugi veliki problem jesu fizička ostvarenja kvantnih računara. Praktično, dva osnovna problema koja se javljaju su izolovanje sistema od spoljašnje sredine i pristup tako izilovanom sistemu. Sa današnjim tehnološkim mogućnostima nije moguće u isto vreme rešiti oba problema. Tehnologija izolovanja sistema još uvek nije dovoljno napredovala da može da izoluje kvantni sistem od dekoherencije na više od par sekundi, što kvantne računare u današnjoj fazi razvoja čini nepraktičnim.

Današnji kvantni računari su ostvarivi samo u laboratorijskim uslovima i više su dokaz koncepta nego praktične, komercijalne mašine za računanje.

2.4.3 Budućnost kvantnih računara

Gledano danas, kvantni računari deluju kao naučna fantastika. I ako postoje mnogi dokazi da su kvantni računari realno ostvarivi niko ne može da garantuje njihovu masovnu upotrebu u daljoj budućnosti. Veliki preokret u kvantnom računaru uslovljen je pronalaskom materijala i tehnologija koji mogu izolovati kvantne sisteme u praktično neograničenim vremenskim periodima.

Sa druge strane kvantni računari nisu jedini koncept u trci za održanje Murovog zakona. Pokazano je da DNK računari, molekularni računari i drugi različiti bio računari takodje se mogu koristiti za efikasniju i bržu obradu podataka nego na klasičnim računarima.

Po meni, pre nego što uspemo da ostvarimo masovnu proizvodnju kvantnih računara potrebo je da razvijemo dublje teorijsko razumevanje kvantnih računara, a i same kvantne mehanike. Smatram da je u skoroj budućnosti potreban veliki skok u tehnologiji izrade materijala, koji bi unapredio razvoj kvantnih računara. Potrebno je pronaći materijale koji efikasno mogu zaštititi kvantni sistem od dekoherencije.

Za mene drugi veoma bitan faktor za budućnost kvantnih računara jeste edukacija. Mnogi njudi u današnjem društvu nisu upućeni u svet kvantnih računara i smatraju ga konceptom naučnofantastičnih knjiga i filmova, a samim tim i nerealnim. Potrebno je ljude upoznati sa konceptom kvantnih računara da bi on bio prihvaćen kao budućnost računarstva.

Ja lično smatram da kvantni računari jesu budućnost računarstva i da će oni relativno brzo biti fizički ostvareni.[15].

Deo 3

Teorema o uzorcima

3.1 Uvod

U 21. veku, svakodnevni život je nezamisliv bez uređaja čija se funkcija zasniva na obradi digitalnih signala. Ti uređaji su postali svakodnevnica i njihova pristupačnost kao da nema granica. Princip rada zasniva se na prevođenju ananogne stvarnosti u digitalne zapise na različitim elektronskim medijima, kako po obliku tako i po sadržaju. Zbog kompleksnosti i postavljanja sve viših standarda od strane korisnika, kao da postoji gornji limit mogućnosti ovih uređaja. Još krajem prošlog veka, informatičari su bili ponosni na činjenicu: da se auto industrija razvijala tempom kao informatičke tehnologije, danas bi Rolls Royce koštao jedan dolar. Kompleksnost prevođenja analognog u digitalni signal, kao da vraća cenu digitalizacije ka početnoj ceni Rolls Royce-a.

3.1.1 Istorijski pregle

Teorema o uzorcima[1] je implicirana u radu Harry Nyqist-a 1928 [20], ali se Nyqist u radu eksplicitno ne bavi problemom uzorkovanja i rekonstrukcije signala. Otprilike u isto vreme, Karl Küpfmüller je doobio sličan rezultat.

Teoremu o uzorcima, koja je suštinski dualno tvrđenje onom koje je Nyqist dobio, dokazao je Claude E. Shannon 1949. u radu [23]. Slične rezultate su dobili i V. A. Kotelnikov, 1933, E. T. Whittaker 1915, i D. Gabor 1946. [7].

Teorema o uzorcima se u literaturi može naći pod različitim nazivima: Teorema o uzorcima, Shannon-ova teorema o uzorcima, Nyquist-ova teorema o ozorcima, Nyquist-Shannon-ova teorema o uzorcima, itd. Kako se Nyquist-ovo ime našlo uz ovu teoremu nije još u potpunosti jasno. Pojam „Nyquist Sampling Theorem" (Nyquist-ova teorema o uzorcima) prvi put se pojavljuje 1959, u knjizi njegovog poslodavca, kompanije *Bell Labs* [2]. Prvi put, ova teorema, se sreće kao „Shannon Sampling Theorem" (Shannon-ova teorema o uzorcima) 1954. u knjizi [10].

U ovom radu mi ćemo koristiti naziv Šenonova teorema o uzorcima.

[1] Eng. Sampling Theorem

3.1.2 Pregled rada

Rad je podeljen u pet celina. Prva je uvod i kratak istorijski osvrt na ljude koji su doprineli dokazu ove teoreme. U drugom delu dajemo kratak pregled osnovnih pojmova i tvrđenja neophodnih za uspešno praćenje dokaza Šenonove teoreme. Tvrđenja će biti data bez dokaza, za dokaze pogledati [27]. U trećem delu bavimo se dokazom Šenonove teoreme (dajemo i dokaz Poasonove formule) i primenom te teoreme. Četvrta celina bavi se problemom aliasinga. Na kraju, u petom delu dat je zaključak u kome se osvrćemo na implikacije Šenonove toereme u razvoju informatičkih tehonologija.

3.2 Osvnovni pojmovi i tvrđenja

U ovom delu rada dajemo kratak pregled pred-Hilbertovih i Hilbertovih prostora, definišemo Furejeove koeficijente, trigonometrijske Furijeove redove i Furijeovu transformaciju i dajemo njihove osnovne osobine, bez dokaza. Smatramo da je čitalac upoznat sa pojmovima norme, metrike, vektorskog prostora, konvergencije, itd. (inače pogledati [27]).

3.2.1 Pred-Hilbertovi i Hilbertovi prostori

Prvo uvodimo pojam Hilbertovog prostora.

Definicija 3.2.1. Neka je dat vektorski prostor X nad poljem $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Preslikavanje $(\cdot,\cdot) : X \times X \to \mathbb{F}$ se naziva skalarni (unutrašnji proizvod) ako važe sledeći uslovi:

1. $(x,x) \geq 0, \forall x \in X$ i $(x,x) = 0$ akko $x = 0$;
2. $(\alpha x + \beta y, z) = \alpha(x,z) + \beta(y,z), \forall x,y,z \in X, \forall \alpha,\beta \in \mathbb{F}$;
3. $(x,y) = \overline{(y,z)}, \forall x,y \in X$.

Uređen par $X, (\cdot,\cdot)$ se naziva *pred-Hilbertov prostor*.

Pred-Hilbertov prostor koji je kolmpletan, tj. svaki Košijev niz je konvergentan, naziva se *Hilbertov* prostor.

Sada definišemo ortonormiran sistem vektora.

Definicija 3.2.2. Neka je $(X, (\cdot,\cdot))$ pred-Hilbertov prostor i $x, y \in X$. Elementi x i y su *ortogonalni* ako važi $(x,y) = 0$. Vektor čija je norma jednaka jedinici je *normiran vektor*.

Ortogonalana sistem (ili ortogonalan skup) je skup nenula vektora u kojem su svaka dva vektora ortogonalna. Ortogonalan skup vektora u kome je svaki vektor i normiran je *ortonormiran sistem*.

Primetimo da ako imamo ortonormiran skup vektora $E = \{e_k : k \in I\}$ i pred-Hilbertovom prostoru, tada za svako $i,k \in I$ važi:

$$(e_i, e_k) = \begin{cases} 0 & i \neq k, \\ 1 & i = k. \end{cases}$$

Lako se pokazuje da ortogonalan sistem čine linearno nezavnisni vektori. Od velikog značaja je i sledeće tvrđenje.

Teorema 3.2.3. *Svaki konačno dimenzionalni pred-Hilbertov prostor ima ortonormiranu bazu.*

U dokazu ove teoreme daje se Gram-Šmitov-postupak normalizacije. Radoznalog čitaoca upućujemo na [27]. Sledeće tvrđenje nam pokazuje „moć" i značaj ortonormiranog sistema.

Teorema 3.2.4. *Neka je $(X, (\cdot,\cdot))$ pred-Hilbertov prostor i neka je dat ortonormiran skup vektora $\{e_1, \ldots, e_n\}$. Ako je vektor $x \in X$ definisan sa:*

$$x = \sum_{k=1}^{n} x_k e_k,$$

onda je $x_k = (x, e_k), k = 1, 2, \ldots, n$.

Sada definišemo potpuno ortonormiran sistem i dajemo potreban i dovoljan uslov da neki skup vektora bude potpuno ortonormiran. Ovi sistemi vektora su, kao što ćemo videti u nastavku rada, ključni za pručavanje Furijeovih redova.

Definicija 3.2.5. Ortonormiran sistem $E = \{e_k \in X : k \in I\}$ je *potpuno ortonormiran sistem* u pred-Hilbertovom prostoru $(X, (\cdot,\cdot))$ akko za proizvoljan ortonormiran sistem $\overline{E}$ važi

$$E \subseteq \overline{E} \Rightarrow E = \overline{E}.$$

Teorema 3.2.6. *Neka je $(X, (\cdot,\cdot))$ pred-Hilbertov prostor. Skup:*

$$E = \{e_k \in X : k \in I\}$$

je potpuno ortonormiran sistem akko za svaki element $x \in X$ važi:

$$(x, e_k) = 0, \forall k \in I \Rightarrow x = 0.$$

3.2.2 Furijeovi koeficijent

U ovom delu definišemo furijeove koeficijente za neki vektor x iz pred-Hilbertovog prostora i dajemo vezu koeficijenata i samog vektora.

Definicija 3.2.7. Neka je $(X, (\cdot,\cdot))$ pred-Hilbertov prostor, $x \in X$ i neka je $E = \{e_k \in X : k \in I\}$ potpuno ortonormiran sistem u X. Brojevi $x_k = (x, e_k), k \in I$, nazivaju se *Furijeovi koeficijenti* vektora x.

Zanimljivo je, a i od velikog značaja je sledeće tvrđenje, njegov dokaz se može naći u [21].

Teorema 3.2.8. *Neka je $(X, (\cdot,\cdot))$ pred-Hilbertov prostor. Tada je skup Furijeovog koeficijenta $\{x_k \neq 0 : k \in I\}$ prebrojiv skup za svaki vektor $x \in X$.*

Sledeći rezultat je poznat kao Beselove nejednakost.

Teorema 3.2.9. *Neka je $X, (\cdot,\cdot)$ pred-Hilbertov prostor. Ako je*

$$\{x_{k_j} \neq 0 : j \in \mathbb{N}\}$$

skup nenula Furijeovih koeficijenata zadatog vektora $x \in X$, onda važi Beselova nejednakost:

$$\sum_{j=1}^{\infty} |x_{k_j}|^2 \neq \|x\|^2.$$

Od fundamentalnog značaja za dalji rad nam je sledeća teorema.

Teorema 3.2.10. *Neka je $(X, (\cdot,\cdot))$ Hilbertov prostor, $E = \{e_\alpha | \alpha \in I\}$ potpuno ortonormiran sistem i neka je $x \in X$. Tada je:*

$$x = \sum_{k=1}^{\infty} x_k e_k, \tag{3.2.1}$$

pri čemu su $\{x_k | k \in \mathbb{N}\}$ Furijeovi koeficijenti vektora $x \in X$, različiti od nule, a e_k elementi potpunog ortonormiranog sistema, indeksirani na odgovarajuć način, tj. tako da važi $x_k = (x, e_k)$.

Takođe važi i Parsevalova jednakost:

$$\|x\|^2 = \sum_{k=1}^{\infty} |x_k|^2.$$

Sada dajemo primer vektorskog prostora nad poljem realnih brojeva sa potpuno ortonormiranim sistemom.

Primer 2. Neka je $L^2([0, 2\pi])$ vektorski prostor nad poljem $\mathbb{R}$ čiji su selementi po delovima neprekidne funkcije $f : [0, 2\pi] \to \mathbb{R}$ za koje važi:

$$\|f\| := \left(\int_0^{2\pi} |f(x)|^2 \right)^{1/2} < \infty.$$

Sa

$$(f, g) = \int_0^{2\pi} f(t)g(t)dt, \quad f, g \in L^2([0, 2\pi])$$

definisan je skalarni proizvod i $(L^2([0, 2\pi]), (\cdot,\cdot))$ je Hilbertov prostor. Može se pokazati da je

$$\left\{ \frac{1}{\sqrt{2\pi}}, \frac{1}{\sqrt{\pi}} \sin nt, \frac{1}{\sqrt{\pi}} \cos nt | n \in \mathbb{N} \right\}.$$

Takođ, biće nam važan i primer vektorskog prostora nad poljem kompleksnih brojeva sa potpuno ortonormiranim sistemom.

Primer 3. Neka je $L^2([0, 2\pi])$ vektorski prostor nad poljem $\mathbb{C}$ čiji su selementi

po delovima neprekidne funkcije $f : [0, 2\pi] \to \mathbb{C}$ za koje važi:

$$\|f\| := \left(\int_0^{2\pi} |f(t)|^2 dt \right)^{\frac{1}{2}} = \left(\int_0^{2\pi} |f(t)\overline{f}(t)| dt \right)^{\frac{1}{2}} < \infty.$$

Može se pokazati da je:

$$(f, g) = \int_0^{2\pi} f(t)\overline{g}(t)dt, f, g \in L^2([0, 2\pi]),$$

skalarni proizvod i da je $(L^2([0, 2\pi]), (\cdot, \cdot))$ je Hilbertov prostor. Takođe može se dokazati da je

$$\left\{ \frac{e^{ikt}}{\sqrt{2\pi}} : k \in \mathbb{Z} \right\}$$

potpuno ortonormiran sistem. Za svaku funkcijeu $f \in L^2([0, 2\pi])$ Furijeovi koeficijenti dati su sa:

$$f_k = \frac{1}{\sqrt{2\pi}} \int_0^{2\pi} f(t)e^{-ikt} dt,$$

i pri tome je

$$f(t) = \frac{1}{\sqrt{2\pi}} \sum_{k=-\infty}^{\infty} f_k e^{-ikt}, t \in [0, 2\pi].$$

3.2.3 Trigonometrijski redovi Furijea

U ovom delu kratko se nastavljamo na priču iz primera 1 i dajemo definiciju trigonometrijskog reda Furijea (direktna posledica primera 1).

Definicija 3.2.11. Neka je $f(x)$ funkcija s periodom 2π, koja na intervalu $[-\pi, \pi]$ ima konačan broj tačaka prekida prve vrste. *Trigonometrijski red Furijea* funkcije f dat je sa:

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos nx + b_n \sin nx),$$

pri čemu su Furijeovi koeficijenti dati sa:

$$a_0 = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)dx,$$

$$a_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos nxdx, \quad n \in \mathbb{N},$$

$$b_n = \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin nxdx, \quad n \in \mathbb{N}.$$

Ako imamo funkciju sam periodom $2l$, lako se pokazuje da furijeov red ima sledeći oblik:

$$f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty}\left(a_n \cos\frac{n\pi x}{l} + b_n \sin\frac{n\pi x}{l}\right),$$

gde je

$$a_0 = \frac{1}{l}\int_{-l}^{l} f(x)dx,$$

$$a_n = \frac{1}{l}\int_{-l}^{l} f(x)\cos\frac{n\pi x}{l}dx, \quad n \in \mathbb{N},$$

$$b_n = \frac{1}{l}\int_{-l}^{l} f(x)\sin\frac{n\pi x}{l}dx, \quad n \in \mathbb{N}.$$

Za razvijanje funkcija u kosinusne i sinusne redove pogledati [27]. Sada navodimo još neke teoreme koje će nam biti neophodne za dokaz Šenonove toereme.

Teorema 3.2.12 (O uniformnoj konvergenciji)**.** *Ako je f neprekidna na intervalu $[-\pi, \pi]$ i važi $f(-\pi) = f(\pi)$ i ako je f' po delovima neprekidna, onda Furijeov red funkcije f uniformno konvergira ka f na $[pi, \pi]$.*

Iz ove teoreme sledi da Furijeove redove smemo, pod datim uslovima, diferencirati „član po član". O integraciji „član po član" nam govori sledeća teorema.

Teorema 3.2.13. *Ako je funkcija f po delovima neprekidna na $[-\pi, \pi]$ onda njen Furijeov red možemo integraliti „član po član".*

O jedinstvenosti razvoja u Furijeov red govori nam sledeća teorema:

Teorema 3.2.14. *Ako su Furijeovi redovi funkcija f, g (po delovima neprekidne na $[-\pi, \pi]$) jednaki, tada važi $f(x) = g(x)$ osim u konačnom broju tačaka.*

3.2.4 Furijeova transformacija

Furijeov red se koristi u analizi funkcija definisanih na konačnom intervalu ili periodičnih funkcija na celom $\mathbb{R}$, iz potrebe da se pručavaju aperiodične funkcije definisane na celom $\mathbb{R}$ uvodimo pojam Furijeove transformacije.

Ako se $t \in \mathbb{R}$ interpretira kao vreme, a $\omega \in \mathbb{R}$ kao frekvncija, za zadat signal $f(t)$, definiše se nova funkcija $F(\omega)$, pri čemu je $f(t)$ vremenski opis, a $F(\omega)$ frekvencijski opis datog signala. Funkcija $F(\omega)$ naziva se Furijeova transformacija.

Prvo uvodimo oznaku $G(\mathbb{R})$ za familiju funkcija $f : \mathbb{R} \to \mathbb{C}$ koje su po delovima neprekidne i apsolutno integrabilne.

Definicija 3.2.15. Neka je data funkcija $f \in G(\mathbb{R})$. *Furijeova transformacija funkcije* f je definisana nesvojstvenim integralom:

$$F(f)(\omega) := \frac{1}{2\pi} \int_{-\infty}^{+\infty} f(x) e^{-i\omega x} dx.$$

Osnovne osobine Furijeove transformacije date su sledećom teoremom.

Teorema 3.2.16. *Za svaku funkciju $f \in G(\mathbb{R})$ važi:*

1. *$F(\omega)$ je definisano za svako $\omega \in \mathbb{R}$,*
2. *$F(\omega)$ je neprekidna funkcija na $\mathbb{R}$,*
3. *$\lim_{\omega \to +\infty} = 0$.*

Trivijalno se proverava linearnost za Furijeovu transformaciju. Sada dajemo tablicu osnovnih Furijeovih transformacija:

Osobina	**Funkcija**	**Furijeova transformacija**
	$f(x)$	$F(f)(\omega)$
Izvod	$f'(x)$	$i\omega F(f)(\omega)$
Izvod reda $p \in \mathbb{N}$	$f^{(p)}(x)$	$(i\omega)^p F(f)(\omega)$
Translacija	$f(x-t)$	$e^{-it\omega} F(f)(\omega)$
Modulacija	$e^{i\xi x} f(x)$	$F(f)(\omega - \xi)$
Dilatacija ($a \neq 0$)	$f(x/a)$	$\lvert a \rvert F(f)(a\omega)$
Konvolucija	$(f_1 * f_2)(t)$	$1/2\pi F(f_1)(\omega) F(f_2)(\omega)$
Množenje	$(f_1 \cdot f_2)(t)$	$(F(f_1) * F(f_2))(\omega)$
Množenje polinomom	$x^p f(x)$	$i^p F(f)^{(p)}(\omega)$

Evo jednog primera koji će nam kasnije biti od koristi:

Primer 4. Neka je data funkcija:

$$f(x) = \begin{cases} 1 & a \leq x \leq b, \\ 0 & \text{inače}, \end{cases}$$

$a, b \in \mathbb{R}$, tj. karakteristična funkcija intervala $[a, b]$, imamo da važi:

$$F(f)(\omega) = \frac{1}{2\pi} \int_{-\infty}^{\infty} f(x) e^{-i\omega x} dx = \frac{1}{2\pi} \int_{a}^{b} e^{-i\omega x} dx$$
$$= \frac{e^{-i\omega a} - e^{-i\omega b}}{2\pi i \omega}.$$

Specijalno, za $a = -b, b > 0$ dobija se:

$$F(f)(\omega) = \frac{\sin \omega b}{\omega \pi}.$$

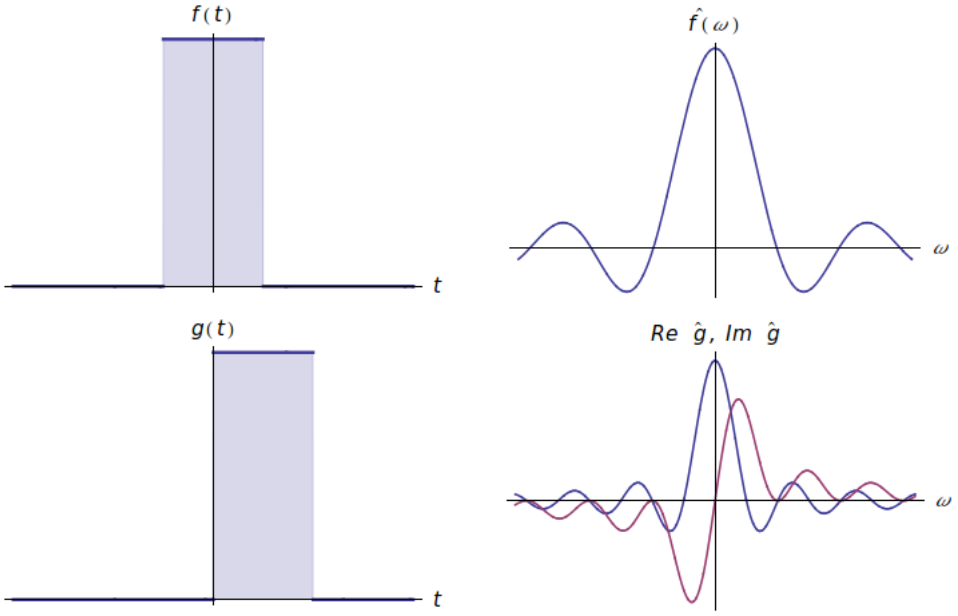
Takođe imamo i sledeću teoremu, koja nam u kombinaciji sa predhodim primermo daje značajnu činjenicu, koju ćemo koristiti u dokazu Šenonove teoreme.

Teorema 3.2.17. *Ako je $F(f)(\omega) \in G(\mathbb{R})$, tada je:*

$$F(F(f)(\omega))(x) = \frac{1}{2\pi} f(-x).$$

Sada dobijamo:

$$F(2\sin(a\omega)/\omega)(x) = 2\pi F(\sin(a\omega)/(\pi\omega))(x) = 2\pi F(F(\chi_a)(\omega))(x) = \chi_a \tag{3.2.2}$$



Prikaz 3.1: Grafik funkcije i njene Furijeove transformacije iz primera 3.

3.3 Šenonova teorema

U ovom delu prvo dajemo dokaz Poasonove formule, a zatim dokazujemo Šenenovu teoremu.

3.3.1 Poasonova formula

Poasonova formula daje elegantnu vezu između Furijeovih redova i Furijeove transformacije. Ona se zasniva na zanimljivom triku periodizacije. Naime, ako je f apsolutno integrabilna funkcija i neka je dato $L > 0$, tada je:

$$\sum_{n=-\infty}^{\infty} f(x + nL),$$

periodična funkcija sa periodom L. Poasonova formula je data sledećom teoremom:

Teorema 3.3.1. *Neka je data funkcija f takva da je:*

$$|f(x)| \leq C(1 + |x|)^{-p}, \quad |F(f)(\omega)| \leq C(1 + |\omega|)^{-p}, \quad \forall x, \omega \in \mathbb{R},$$

za neke konstante $p > 1$ i $C > 0$. Tada, za svako $L > 0$ važi:

$$\sum_{n=-\infty}^{\infty} f(x + nL) = \frac{2\pi}{L} \sum_{n=-\infty}^{\infty} F\left(\frac{2\pi n}{L}\right) e^{2\pi i n x/L}, x \in \mathbb{R}.$$

Formula važi tačkasto za sve $x \in \mathbb{R}$ i obe sume su apsolutno konvergentne.

Dokaz. Primetimo prvo da oba reda apsolutno tačkasto konvergiraju za svako $x \in \mathbb{R}$ (direktna posledica uslova i poredbenog kriterijuma konvergencije). Preostaje samo da se pokaže jednakost.

Ako je funkcija $g(x)$ periodična sa periodom $L > 0$, njen Furijeov red u kompleksnom obliku glasi

$$\sum_{n=-\infty}^{\infty} c_n e^{2\pi i n x/L},$$

gde je:

$$c_n = \frac{1}{L} \int_0^L g(x) e^{-2\pi i n x/L} dx, \quad n \in \mathbb{N}.$$

Prema tome, za $g(x) = \sum_{n=-\infty}^{\infty} f(x+nL)$ važi:

$$\begin{aligned} c_n &= \frac{1}{L}\int_0^L \sum_{k=-\infty}^{\infty} f(x+kL)e^{-2\pi inx/L}dx \\ &= \frac{1}{L}\sum_{k=-\infty}^{\infty}\int_0^L f(x+kL)e^{-2\pi inx/L}dx \\ &= \frac{1}{L}\sum_{k=-\infty}^{\infty}\int_{kL}^{(k+1)L} f(y)e^{-2\pi iny/L}e^{2\pi ink}dy \\ &= \frac{1}{L}\int_{-\infty}^{\infty} f(y)e^{-2\pi iny/L}dy \\ &= \frac{2\pi}{L}F\left(\frac{2\pi n}{L}\right), \quad n \in \mathbb{N}, \end{aligned}$$

jer je $e^{-2piink} = 1, \forall n, k \in \mathbb{N}$. U drugoj jednakosti smo koristili pretpostavke o funkciji f i Vajerštrasov kriterijum o uniformnoj konvergenciji da bi razmenili granične procese. Na osnovu jedinstvenosti razvoja u Furijeov red, tvrđenje sledi. □

Na sličan način se može pokazati da, ako je F Furijeova transformacija funkcije f i ako važe uslovi predhodne teoreme, važi sledeća formula:

$$\sum_{n=-\infty}^{\infty} F(\omega - n\omega_s) = \frac{1}{2\pi}T\sum_{n=-\infty}^{\infty} f(nT)e^{-inT\omega}, \omega \in \mathbb{R}, \tag{3.3.1}$$

pri čemu je $T = \frac{2\pi}{\omega_s}$, a $\omega_s > 0$ zadata konstanta.

3.3.2 Dokaz Šenonove teoreme o uzorcima

Prvo definišemo vremenski ograničene funkcije i funkcije ograničenog opsega.

Definicija 3.3.2. Za signal (funkciju) f kažemo da je vremenski ograničena ako postoji konstanta M takva da je $f(x) = 0$ za svako $|x| \geq M$. Funkcija $f \in G(\mathbb{R})$ je ograničenog opsega ako postoji konstanta L takva da je $F(f)(\omega) = 0$ za svako $|\omega| > L$.

Funkcije ograničenog opsega mogu se rakonstruisati iz svojih uzoraka (poznatih vrednosti u diskretnom nizu tačaka) na sledeći način.

Teorema 3.3.3 (Šenonova teorema o uzorcima)**.** *Neka je $f \in G(\mathbb{R})$ i neka za njenu Furijeovu transformaciju važi $F(f)(\omega) = 0$, za svako $|\omega| > L$. Tada za*

svako $\omega_s > 2L$ *važi:*

$$f(x) = \sum_{n=-\infty}^{\infty} f(nT) \frac{2\sin(\omega_s(x-nT)/2)}{\omega_s(x-nT)}, x \in \mathbb{R},$$

pri čemu je $T = \frac{2\pi}{\omega_s}$.

Dokaz. Neka je za dato $a \in \mathbb{R}$, sa χ_a je označena karakteristična funkcija intervala $[-a, a]$, tj:

$$\chi_a(x) = \begin{cases} 1 & -a \leq x \leq a, \\ 0 & \text{inače.} \end{cases}$$

Neka je sada $\omega_s > 2L$ i neka je

$$F_s(\omega) = \sum_{n=-\infty}^{\infty} F(\omega - n\omega_s),$$

tada je F_s periodična funkcija sa periodom ω_s i važi:

$$F(\omega) = F_s(\omega)\chi_{\frac{\omega_s}{2}}.$$

Na osnovu jedinstvenosti Furijeove transformacije, dovoljno je da se pokaže da je

$$F\left(\sum_{n=-\infty}^{\infty} f(nT) \frac{2\sin(\omega_s(x-nT)/2)}{\omega_s(x-nT)}\right)(\omega) = F_s(\omega)\chi_{\frac{\omega_s}{2}}.$$

Iz (3.2.2) lako se dobija da važi:

$$F\left(\frac{2\pi\sin(\omega_s x/2)}{\omega_s x/2}\right)(\omega) = T\chi_{\frac{\omega_s}{2}}(\omega).$$

Prema tome, iz formule za translaciju Furijeove transformacije dobijamo:

$$F\left(f(nT)\frac{2\sin(\omega_s(x-nT)/2)}{\omega_s(x-nT)}\right)(\omega) = T\chi_{\frac{\omega_s}{2}}(\omega)e^{-in\omega T}.$$

Na kraju dobijamo:

$$\begin{aligned} F\left(\sum_{n=-\infty}^{\infty} f(nT)\frac{2\sin(\omega_s(x-nT)/2)}{\omega_s(x-nT)}\right)(\omega) &= \frac{T}{2\pi}\sum_{n=-\infty}^{\infty} f(nT)e^{-in\omega T}\chi_{\frac{\omega_s}{2}}(\omega) \\ &= \sum_{n=-\infty}^{\infty} F(\omega - n\omega_s)\chi_{\frac{\omega_s}{2}}(\omega) = F_s(\omega)\chi_{\frac{\omega_s}{2}}(\omega) = F(\omega), \end{aligned}$$

gde je u predposlednjoj jednakosti korišćeno (3.3.1). □

3.3.3 Primene Šenonove teoreme

Iz predhodne teoreme dobijamo da, ako imamo funkciju f ograničenog opsega (sa frekvencijom L) onda je u potpunosti određena svojim vrednostima (uzorcima) u nizu ravnomerno raspoređenih tačaka sa rastojanjem manjim od π/L. Teorema nam daje i odgovor kako da funkciju rekonstruišemo. Direktno dobijamo da ako je f ograničenog opsega L onda učestalost uzimanja uzorka ω_s, mora biti veća od $2L$. Ova frekvnecija se naziva *Najkvistova frekvencija.*

Uzorkovanje audio signala

Sa pojavom digitalne elektronike nametnulo se pitanje kako analogan audio sgnal pretvoriti u digitalan zapis. Odgovor na ovo pitanje upravo je dala Šenonova teorema o uzorcima. Naime, kako je obseg ljudskog sluha 20 000 Herca, doovoljno je sigal prpustiti kroz odgovarajući niskopropusni filter, na taj način dobijamo signal ogrničenog opsega (sa frekvencijom L=20 000) i tada ga uzorkovati Najkvistovom frekvencijom od 40 000 Herca. Današnji industrijski standard frekvencije uzorkovanja audio signaza za CD je 44 000 Hz. U nekim slučajevima ova frekvencija je drastično viša, iako su eksperimenti pokazali da čovek ni u kom slučaju ne registruje ultrazvučne talase, postoje slučajevi kada ultrazvučni talasi imaju značajan uticaj na niže frenvcije zvuka. Sledeća tabela daje primere nekih industrijskih standarda za frekvenciju uzorkovanja.

Frekvncija (Hz)	**Upotreba**
8 000	Telefonski signal
32 000	Bežični mikrofoni
44 100	Audio CD, MP3, VHS
48 000	Profesionalna audio oprema
96 000	DVD-Audio, BD-ROM (Blu-ray)
192 000	DVD-Audio, BD-ROM

Ostale primene

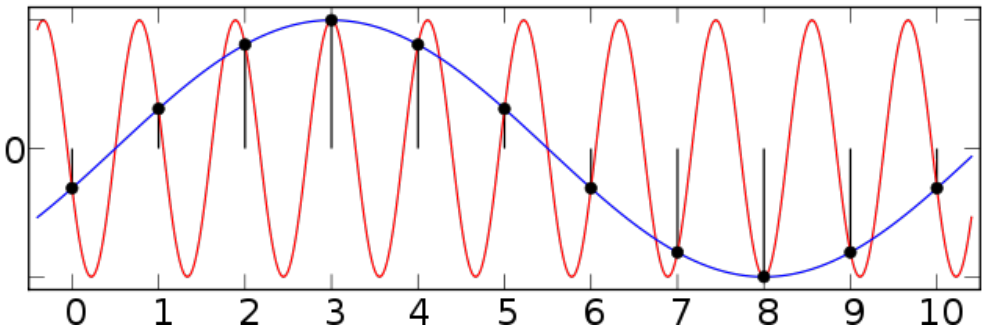
Teorija uzorkovanja se koristi u svakom pretvaranju analognog u digitalni signal. Neka polja primen su: Obrada i skladištenje fotografija, uzorkovanje video signala, 3D uzorkovanje[2] (uzorkovanje 3D fotografija ljudskog tela nastale putem X-zraka ili magnetne rezonance),...

Primetimo još jednu zanimljivu činjenicu. Šenonova teorema na daje samo dovoljan uslov za potpunu rekonstrukciju signala, naime, ona nam kaže da ako uzorkujemo Najkvistovom frekvencijom, onda možemo u potpunosti rekonstruisati signal. Prirodno se nameće pitanje, ako uzorkujemo frekvencijom manjom od Najkvistove, da li je tada rekonstrukcija signala moguća i da li je ona jednoznačna?

[2]eng. 3D Sampling

3.4 Aliasing

U ovom delu dajemo odgovor na pitanje, šta semože dogoditi ako signal uzorkujemo frekvencijom manjom od Njakvistove? Pogledajmo sledeći primer, slika 2.



Prikaz 3.2: Dva signala koja odgovaraju istom uzorku

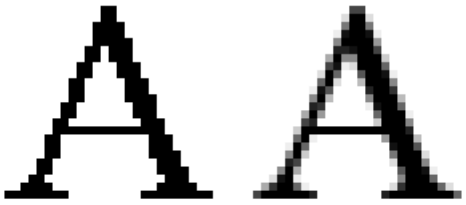
Vidimo da ako se signal uzorkuje frekvencijom manjom od Najkvistove može da se desi da jednom nizu uzoraka odgovara više različitih signala.

Ova pojava preklapanja frekvencija naziva se *aliasing* i u tom slučaju originalni signal ne može da se rekonstruiše na jedinstven način.

Da bi se aliasing sprečio postoje dve stvari koje se mogu učinit:

- Povećati frekvenciju uzorkovanja;
- Koristiti antialiasing filtere.

Antialiasing filter je filter koji ograničava opseg frekvencija signala, pre njegovog uzorkovanja, tako da novodobijeni signal zadovoljava uslove Šenonove teoreme. Teorija dozvoljava postojanje takvih filtera, ali je problem u njihovoj konstrukciji. Naime, nije moguće konstruisati idealan filter, pa dolazi do takozvanog curenja visokih frekvencija. Sledeća slika daje primer delovanja antialiasing filtera u operativnom sistemu Windows 7.

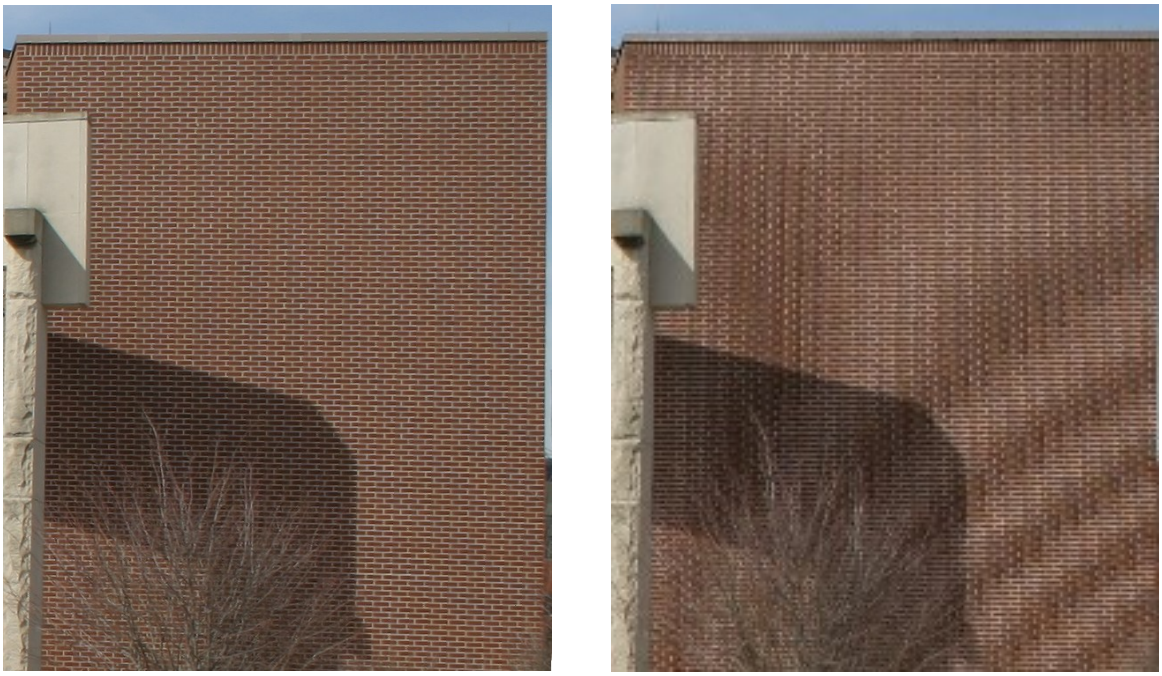


Prikaz 3.3: Dejstvo antialiasing filtera (desno)

Postoje dve vrste aliasinga:

1. Vremenski aliasing
2. Prostorni aliasing

Vremenski aliasing se javlja u uzorkovanju vremensko zavisnih signala, npr. audio signal. Jedan takav primer videli smo na početku ovog dela. Prostorni aliasing se se javlja pri prostornom uzorkovanju signala. Sledeće slike su neki primeri prostornog aliasinga.



Prikaz 3.4: Prostorni aliasing

3.5 Zaključak

Ostaje nam još da odgovorimo na pitanje, kako kompleksnost prevođenja analognog u digitalni signal može da utiče na cenu digitalnih uređaja? Kao što smo tokom rada videli, da bi analogan signal preveli u digitalni, moramo ga uzorkovati bar Najkvistovom frekvencijom (dva puta opseg signala), ako želimo da ga u potpunosti jednoznačno rekonstruišemo.

Korisnici zahtevaju sve veći i veći kvalitet zvuka, slike i videa. Gledano to kroz proces digitalizacije, zahteva se da se digitalizuju signali sve šireg opsega. To implicira više Najkvistove frekvencije uzorkovanja, a samim tim i više podataka za obradu i skladištenje. Današnja elektronika već zaostaje za zahtevima digitalizacije kompleksnih signala. Jedan primer je uzorkovanje 3D snimaka ljudskog tela. Pacjenti u aparatu za magnetnu rezonancu moraju da provedu od 15 do 90 minuta[3], upravo zbog toga što računar ne može u kratkom roku da uzorkuje, obradi i skladišti signal.

Elektronika bazirana na siliciumskim komponentama je skoro dostigla svoj maksimum i pitanje je da li je ona uopšte efikasno rešenje problema konverzije analognog u digitalni signal. Efikasno rešenje ovog problema verovatno leži u nekoj drugoj, nama možda još nepoznatoj tehnologiji, koja kada se pojavi na tržištu sigurno neće biti jeftina.

[3] http://www.nhs.uk/conditions/mri-scan/Pages/How-is-it-performed.aspx

Literatura

[1] D. Adnadjević and Z. Kadelburg. *Matematička analiza I.* Naučna knjiga, 1989.

[2] Bell Telephone Laboratories. *Transmission systems for communications.* New York, 1959.

[3] Guo Chen. A treatment of the dirichlet integral via the methodes of real analysis. 2009.

[4] Richard Courant. *Differential and integral calculus.* Wiley classics library. Interscience Publishers, New York, wiley classics library ed edition, 1988.

[5] Richard P. Feynman, Robert B. Leighton, and Matthew Sands. *The Feynman Lectures on Physics including Feynman's Tips on Physics: The Definitive and Extended Edition.* Addison Wesley, 2 edition, August 2005.

[6] Richard Phillips Feynman. *Feynman Lectures on Computation.* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1998.

[7] D. Gabor. Theory of communication. *Journal of the Institution of Electrical Engineers - Part I: General*, 94(73):58–, January 1947.

[8] L. Gajić. *Predavanja iz analize I.* Prirodno-matematički fakultet, Departman za matematiku i informatiku, 2006.

[9] Ljiljana Gajić. *Predavanja iz uvoda u analizu.* Prirodno-matematički fakultet, Departman za matematiku i informatiku, 2004.

[10] Truman S. Gray. *Applied electronics: a first course in electronics, electron tubes, and associated circuits.* Wiley, New York, 1954.

[11] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, 79:325–328, Jul 1997.

[12] W. Heisenberg. *The Physical Principles of the Quantum Theory.* Physics and chemistry. Dover Publications, 1949.

[13] W.T. Kelvin and Royal Institution of Great Britain. Weekly Evening Meeting. *Nineteenth century clouds over the dynamical theory of heat and light.* S.n, 1900.

[14] A. N. Kolmogorov and S. V. Fomin. *Introductory real analysis*. Dover Publications, New York, rev. english ed edition, 1975.

[15] Konjovic M. *Anksioznost i panika*. Naklada Slap, 2008.

[16] Thomas Monz, Philipp Schindler, Julio T. Barreiro, Michael Chwalla, Daniel Nigg, William A. Coish, Maximilian Harlander, Wolfgang Hänsel, Markus Hennrich, and Rainer Blatt. 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, 106:130506, Mar 2011.

[17] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 38(8), April 1965.

[18] Yiannis N. Moschovakis. What is an algorithm?, 2000.

[19] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[20] H Nyquist. Certain topics in telegraph transmission theory. *Proceedings of the IEEE*, 90(2):280–305, 2002.

[21] Hadžić Olga Pilipović Stevan. *Uvod u funkcionalnu analizu*. Univerzitet u Novom Sadu, Novi Sad, 1996.

[22] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Rev. Mod. Phys.*, 76:1267–1305, Feb 2005.

[23] C. E. Shannon. Communication in the presence of noise. *Proc. Institute of Radio Engineers*, 37, 1949.

[24] Peter W. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.Sci.Statist.Comput.*, 26:1484, 1997.

[25] Peter W. Shor. Progress in quantum algorithms, 2005.

[26] Michael Spivak. *Calculus*. Publish or Perish, Houston, Tex., 2008.

[27] Nenad Teofanov. *Predavanja iz primenjene analize*. Zavod za udzbenike - Beograd, 2011.

[28] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936.

[29] M. M. Wilde. From Classical to Quantum Shannon Theory. *ArXiv e-prints*, June 2011.