Charaktery a Diskrétní Fourierova transformace

Nejdůležitějším kvantovým algoritmem je *Diskrétní Fourierova transformace* (DFT). Důvody jsou dva:

- DFT je pro kvantové počítače exponenciálně rychlejší než pro počítače klasické;
- DFT umožňuje (mimo jiné) faktorizaci přirozených čísel.

Diskrétní Fourierova transformace se týká zobrazení z konečné komutativní grupy G do $\mathbb{C}$. Každé takové zobrazení f lze chápat jako vektor $(f(g_1), f(g_2), \ldots, f(g_n))$, kde $n = |G|$ a g_i jsou prvky G. Množina všech zobrazení tak tvoří vektorový prostor $\mathbb{C}^n$, přičemž bazí, ke které se uvedený zápis vztahuje, je báze charakteristických funkcí jednotlivých prvků, tedy funkcí $b_1, b_2, \ldots, b_n$ definovaných vztahem $b_i(g_j) = \delta_{ij}$.

DFT je přechod od "chronologického" zápisu funkce v této bázi, k zápisu v bázi tzv. *charakterů* grupy G, které vyjadřují "frekvenční" rozklad funkce. Pro porozumění DFT je proto třeba nejprve pojednat o charakterech konečných grup.

Nechť $(G, \cdot)$ je komutativní grupa. Každý grupový homomorfismus

$$\chi : (G, \cdot) \to (\mathbb{C}, \cdot)$$

se nazývá *charakter* grupy G. Dále budeme uvažovat pouze konečné grupy G.

Charaktery tvoří také grupu, s násobením definovaným

$$(\chi_1 \cdot \chi_2)(g) = \chi_1(g) \cdot \chi_2(g).$$

Jednotkovým prvkem této grupy charakterů je identická jednička, kterou značíme ε a nazýváme *triviálním* charakterem.

Věta. Nechť je X grupa charakterů konečné komutativní grupy G. Pak

$$X \cong G.$$

Důkaz. Protože je G konečná, musejí se všechny její prvky zobrazovat na jednotkovou kružnici. Přesněji, prvek g se musí zobrazovat na r-tou odmocninu z 1, kde r je řád prvku g. Máme tedy

$$\chi(g) = \exp\left[2\pi i \frac{k}{r}\right],$$

pro nějaké $k \in \mathbb{Z}_r$.

Nechť $\{h_1, \ldots, h_m\}$ je nějaká minimální množina generátorů grupy G, kde prvek h_j má řád r_j. Pak

$$G \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

a charakter χ je jednoznačně určen volbou

$$(k_1, \ldots, k_m) \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$$

tak, že

$$\chi(h_j) = \exp\left[2\pi i \frac{k_j}{r_j}\right].$$

Je snadné ověřit, že zobrazení $\chi \mapsto (k_1, \ldots, k_m)$ dává požadovaný isomorfismus. □

Vzhledem k tomu, že se pohybujeme na jednotkové kružnici, platí

$$\chi^{-1}(g) = \chi(g)^{-1} = \chi(g)^*.$$

Dále je užitečné si všimnout, že pro $g, h \in \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_m}$ platí

$$\chi_h(g) = \chi_g(h).$$

Obě strany rovnosti se totiž rovnají

$$(\diamond) \qquad \exp\left[2\pi i \sum_{j=1}^{m} \left(\frac{k_j \ell_j}{r_j}\right)\right],$$

kde $g = (k_1, k_2, \ldots, k_m)$ a $h = (\ell_1, \ell_2, \ldots, \ell_m)$.

Pro počítání s charaktery je klíčové následující tvrzení.

Lemma. Pro libovolný netriviální charakter χ grupy G platí

$$\sum_{g \in G} \chi(g) = 0.$$

Důkaz. Nechť je χ netriviální, a zvolme $h \in G$ tak, že $\chi(h) \neq 1$. Protože $g \mapsto hg$ je permutace grupy G, dostáváme

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \chi(h) \sum_{g \in G} \chi(g),$$

a tedy

$$\sum_{g \in G} \chi(g) = 0.$$

□

Následující tvrzení ukazuje, že charaktery jsou ortogonální množinou vzhledem ke standardnímu skalárnímu součinu (pracujeme tedy v Hilbertově prostoru $\mathbb{H}_n$, nikoli pouze v $\mathbb{C}_n$).

Lemma. Nechť χ_1 a χ_2 jsou dva různé charaktery grupy G. Pak platí

$$\sum_{g \in G} \chi_1(g)^* \chi_2(g) = 0.$$

Důkaz. Protože $\chi_1 \neq \chi_2$, je $\chi_1^* \chi_2 = \chi_1^{-1} \chi_2$ netriviální charakter, a tvrzení plyne z předchozího lemmatu. □

Norma každého charakteru χ je

$$\sqrt{\sum_{g \in G} \chi(g)^* \chi(g)} = \sqrt{n}.$$

Vidíme proto, že množina

$$\left(\frac{1}{\sqrt{n}}\chi_1, \frac{1}{\sqrt{n}}\chi_2, \ldots, \frac{1}{\sqrt{n}}\chi_n\right)$$

je ortonormální báze $\mathbb{H}_n$, které říkáme *báze charakterů*.

Jak už bylo řečeno na začátku, Diskrétní Fourierova transformace je převod zobrazení $f : G \to \mathbb{C}$ ze zápisu v bázi charakteristických funkcí do zápisu v bázi charakterů. Protože jsou obě báze ortonormální, jedná se o unitární zobrazení. Matice DFT je tedy inverzní matice k matici přechodu od kanonické bázi k bázi charakterů. Protože inverzní matice unitární matice je matice adjungovaná, máme

$$[\mathrm{DFT}]_{k,\ell} = \frac{1}{\sqrt{n}} \chi_{g_k}(g_\ell)^*,$$

kde $g_1, g_2, \ldots, g_n$ je nějaké očíslování prvků grupy G. Díky výše dokázané záměnnosti indexů jsou DFT a DFT^{-1} komplexně sdružené a pro zjednodušení zápisu se obvykle uvažuje inverzní transformace IFT (ušetříme tím znaménka minus v exponentu).

Kvantový rozklad Diskrétní Fourierovy transformace

Kvantová ralizace Diskrétní Fourierovy transformace spočívá v konstrukci obvodu, který počítá operátor DFT, tedy v rozkladu DFT na malé operátory.

Výše jsme definovali DFT pro obecnou grupu G. Nejdůležitější a nejobvyklejší je DFT pro cyklickou grupu $(\mathbb{Z}_N, +)$ a není-li řečeno výslovně jinak, rozumí se označením DFT právě tento případ.

Pro ilustraci a procvičení ovšem provedeme nejprve DFT na grupě $(\mathbb{Z}_2^m, +)$. Máme $M = 2^m$ a k-tý bázový prvek $\mathbb{H}_M$ budeme jako obvykle zapisovat $|k\rangle = |k_1 k_2 \ldots k_m\rangle$, kde $k_1 k_2 \ldots k_m$ je binární zápis k. Budeme také přirozeně předpokládat, že očíslování grupy $\mathbb{Z}_2^m$ tomuto zápisu odpovídá, že tedy k-tý prvek je právě $(k_1, k_2, \ldots, k_m)$.

Podle $(\diamond)$ pak máme

$$[\mathrm{DFT}]_{k,\ell} = \frac{1}{\sqrt{2^m}} \exp\left[2\pi i \sum_{j=1}^{m} \frac{k_j \ell_j}{2}\right] = \frac{1}{\sqrt{2^m}} (-1)^{\sum_{j=1}^m k_j \ell_j} = \frac{1}{\sqrt{2^m}} (-1)^{k \cdot \ell}.$$

To je ovšem matice, kterou známe již z Deutschova-Jozsova algoritmu; nad $\mathbb{Z}_2^m$ dostáváme snadný rozklad

$$\mathrm{DFT} = H^{\otimes m}.$$

Obraťme se nyní k případu $(\mathbb{Z}_M, +)$. Využijeme poznámku na konci předchozího oddílu a budeme rozkládat IFT, kde

$$[\mathrm{IFT}]_{k,\ell} = \frac{1}{\sqrt{M}} \exp\left[2\pi i \frac{k\ell}{M}\right].$$

Obvod je vždy definován na bázových prvcích. Chceme tedy sestrojit obvod, který vstup $|k\rangle = |k_1\rangle|k_2\rangle \cdots |k_m\rangle$ zobrazí takto:

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{\ell=0}^{M-1} \exp\left[2\pi i \frac{k\ell}{M}\right] |\ell\rangle,$$

což po rozkladu

$$|\ell\rangle = \bigotimes_{j=1}^{m} |\ell_j\rangle, \qquad \frac{\ell}{M} = \sum_{j=1}^{m} \frac{\ell_j}{2^j}$$

dává

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{\ell_1=0}^{1} \sum_{\ell_2=0}^{1} \cdots \sum_{\ell_m=0}^{1} \bigotimes_{j=1}^{m} \exp\left[2\pi i \frac{k}{2^j} \ell_j\right] |\ell_j\rangle.$$

To můžeme rozložit jako součin m dvou členných součtů

$$|k\rangle \mapsto \frac{1}{\sqrt{M}} \bigotimes_{j=1}^{m} \sum_{\ell_j=0}^{1} \exp\left[2\pi i \frac{k}{2^j} \ell_j\right] |\ell_j\rangle = \bigotimes_{j=1}^{m} \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left[2\pi i \frac{k}{2^j}\right] |1\rangle\right).$$

Faktor u $|1\rangle$ rozepíšeme:

$$\exp\left[2\pi i\frac{k}{2^j}\right] = \exp\left[2\pi i\frac{\sum_{t=1}^{m} 2^{m-t}k_t}{2^j}\right] = \exp\left[2\pi i\sum_{t=1}^{m} 2^{(m-t-j)}k_t\right]$$

a z periodicity exponenciely dostáváme

$$\exp\left[2\pi i\frac{k}{2^j}\right] = \exp\left[2\pi i\sum_{t=m-j+1}^{m} 2^{(m-t-j)}k_t\right]$$

Pro názornost zápisu bude užitečné rozšířit binární zápis i za „desetinnou“, resp. spíše „polovinnou“ čárku a psát

$$0, a_1a_2\cdots = \sum_j \frac{a_j}{2^j}.$$

Pak lze IFT vyjádřit takto:

$$|k\rangle \mapsto \frac{|0\rangle + \exp\left[2\pi i(0,k_m)\right]|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}} \otimes \cdots$$
$$\otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_2\cdots k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + \exp\left[2\pi i(0,k_1\cdots k_{m-1}k_m)\right]|1\rangle}{\sqrt{2}}.$$

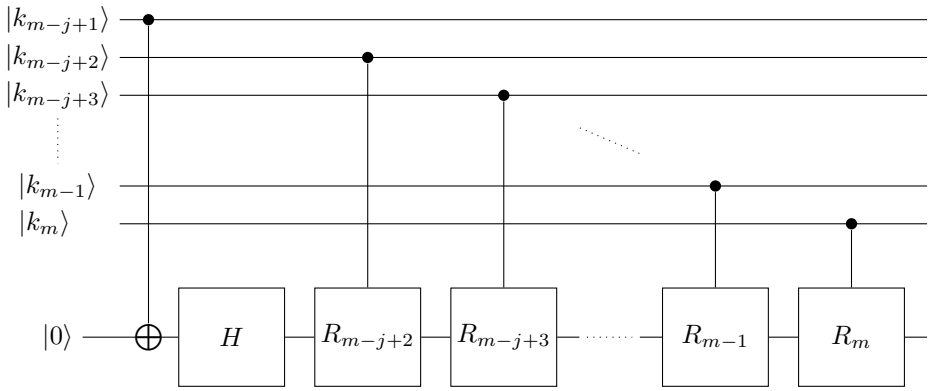
Zkonstruovat obvod, který IFT počítá už není těžké. Všimněme si nejprve, že

$$\frac{|0\rangle + \exp\left[2\pi i(0,a)\right]|1\rangle}{\sqrt{2}} = H|a\rangle,$$

kde H je Hadamardův operátor. Dále budeme potřebovat matice relativního fázového posunu

$$R_t = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^t} \end{pmatrix},$$

které budeme aplikovat kontrolované bitem na t-té pozici za “desetinnou” čárkou. Konstrukce j-tého kubitu výstupu vypadá nyní takto:



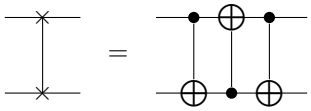
Stačí tedy použít m pomocných kubitů, na počátku ve stavu $|0\rangle$, jako výstupní registr transformace.

Je ovšem také možné pomocné kubity ušetřit, pokud si všimneme, že první kubit vstupu je potřeba pouze pro výpočet n-tého kubitu výstupu, druhý kubit vstupu pouze pro výpočet posledních dvou kubitů výstupu atd. Díky tomu můžeme začít

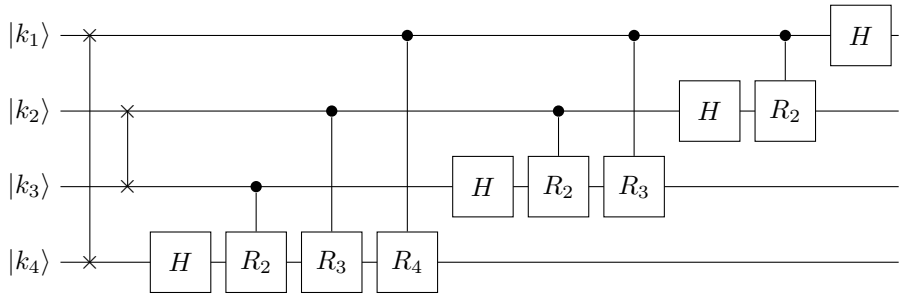
konstrukcí posledního kubitu výstupu v prvním kubitu vstupu, a takto postupně odzadu konstruovat v j-tém vstupním kubitu j-tý výstupní počítáno odzadu.

Dostaneme tedy Fourierovu tranformaci "vzhůru nohama", což jistě není vážný problém. Pokud bychom chtěli i tuto nepřesnost odstranit, stačí na začátku obrátit pořadí vstupních kubitů pomocí $\left\lfloor \frac{m}{2} \right\rfloor$ transpozic. Transpozice bázových kubitů je samozřejmě unitární (jako každá permutace), značí se

a není těžké ověřit, že platí



Celková podoba obvodu IFT pro $\mathbb{Z}_{2^4}$ je znázorněna na následujícím obrázku.



Je zřejmé, že složitost algoritmu (počet hradel) je $\mathcal{O}(m^2) = \mathcal{O}(\log^2 M)$. Nejrychlejší klasický algoritmus, tzv. *rychlá Fourierova transformace*, má přitom složitost $\mathcal{O}(M \log M)$. V tomto případě přinášejí tedy kvantové počítače exponenciální zrychlení.