APLIKACE GEOMETRICKÝCH ALGEBER V KVANTOVÉM POČÍTÁNÍ

JAN MICHÁLEK

Abstrakt. Tato práce se zabývá využitím geometrických algeber v kvantovém počítání. Začíná definicí obecné Cliffordovy algebry a poté odvozuje specifickou komplexní geometrickou algebru, která je vhodná pro reprezentaci kvantových výpočtů. Tento přístup je porovnáván s tradiční metodou použití klasické maticové reprezentace. Analýzou a porovnáním těchto dvou metod si tato práce klade za cíl poskytnout poznatky o potenciálních výhodách použití geometrických algeber pro aplikace v kvantovém počítání.

Úvod

Kvantové počítání je relativně novým, i když velmi dynamickým oborem informatiky. Pro další rozvoj je nezbytné solidní matematické ukotvení. V současné době je nejběžnějším způsobem reprezentace kvantových stavů a operací takzvaný Diracův formalismus. Jedná se o elegantní nástroj, který nám pomáhá zvládnout všechny komplikace, které nám kvantové počítání přináší. Vede k maticové reprezentaci, kde jsou qubity chápány jako vektory a kvantov0 br8nz jako matice. Dimenze matic však s vyšším počtem vstupních qubitů roste a stává se výpočetně náročnější.

Tato práce se pokusí poskytnout alternativu. Bude ukázáno, že aparát geometrických algeber může být pro kvantové výpočty stejně vhodný a v některých konkrétních aplikacích dokonce výhodnější. Bude zavedena obecná Cliffordova algebra a odvozena speciální geometrická algebra. Kvantové stavy pak budou reprezentovány prvky geometrické algebry. Kvantové brány jsou také asociovány s prvky této algebry a to umožňuje přímou aplikaci a výpočty v rámci jedné algebraické struktury. Tento přístup bude porovnán s maticovou reprezentací na jednoduchých příkladech.

1. Algebraický základ

V teto kapitole jsou uvedeny a vysvětleny klíčové pojmy potřebné k pochopení prezentovaných konceptů.

2020 *MSC.* Primární 68Q12; Sekundární 15A66.

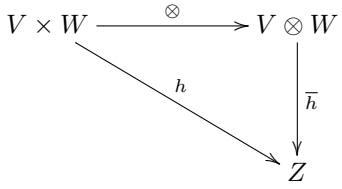
Klíčová slova. Cliffordova algebra, geometrická algebra, kvantové počítání.

Článek vznikl na základě bakalářské práce autora v oboru Matematické inženýrství na FSI VUT v Brně. Vedoucí práce byl Petr Vašík z Ústavu matematiky FSI VUT v Brně.

1.1. Tenzorové prostory

Tenzory jsou abstraktní objekty, které lze definovat několika způsoby. Nejprve představíme univerzální vlastnost, která nám dává omezení, která musí být vždy splněna. Tato definice však není konstruktivní. Proto uvedeme také alternativní definici tenzoru.

Definice 1.1 (Univerzální vlastnost)**.** Tenzorový součin dvou vektorových prostorů V a W, které jsou nad stejným polem K, je vektorový prostor $V \otimes W$ spolu s bilineárním zobrazením $\otimes : (\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} \otimes \mathbf{w}$, $\otimes : V \times W \to V \otimes W$, takovým, že pro každé bilineární zobrazení $h : V \times W \to Z$ existuje jednoznačné lineární zobrazení $\overline{h} : V \otimes W \to Z$, které splňuje $h = \overline{h} \circ \otimes$ (následující diagram komutuje).



Univerzální vlastnost by nám měla sloužit jako ověření, zda je daná konstrukce tenzorového součinu platná. Pokud platí univerzální vlastnost, pak je zkonstruovaný tenzorový součin správný.

Definice 1.2 (Tenzorový součin)**.** Mějme dva vektorové prostory V a W nad stejným polem K. Tenzorový součin $V \otimes W$ je vektorový prostor spolu s příslušným bilineárním zobrazením $V \times W \to V \otimes W$, které vezme prvky $\mathbf{v} \in V$ a $\mathbf{w} \in W$ a zobrazí je na prvek vektorového prostoru $V \otimes W$, $(\mathbf{v}, \mathbf{w}) \mapsto \mathbf{v} \otimes \mathbf{w}$.

Definice 1.3 (Dimenze tenzorového prostoru)**.** Mějme dva vektorové prostory V a W s $\dim V = n$ a $\dim W = m$. Pak tenzorový prostor $V \otimes W$ má dimenzi $\dim V \otimes W = mn$.

Jedním zvláště zajímavým příkladem tenzorového součinu je *Kroneckerův součin*. Je široce využíván v kvantovém počítání. Kroneckerův součin bere jako vstupní prvky dvě matice a jako výstup vytváří jinou matici s vyšší dimenzí.

Definice 1.4 (Kroneckerův součin)**.** Vezměme dvě matice A, B ve tvaru

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & \dots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \dots & b_{pq} \end{pmatrix}.$$

Pak jejich Kroneckerův součin, značený $C = A \otimes B$, má tvar

$$C = A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}. \tag{1.1}$$

1.2. Tenzorová algebra

Po zavedení tenzorových prostorů lze nyní zkonstruovat tenzorovou algebru.

Definice 1.5 (Tenzorová mocnina)**.** Nechť V je vektorový prostor nad polem K. Pro každé $k \in \mathbb{N}$ je definována k-tá tenzorová mocnina V jako tenzorový součin V k-krát sám se sebou:

$$T^k V = V^{\otimes k} = V \otimes V \otimes \cdots \otimes V.$$

Definice 1.6 (Tenzorová algebra)**.** Tenzorová algebra $T(V)$ je konstruována jako přímá suma $T^k V$ pro $k = 0, 1, 2, \ldots$, tj.

$$T(V) = \bigoplus_{k=0}^{\infty} T^k V = K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \cdots . \tag{1.2}$$

Pod $T^0 V$ je rozuměno základní pole K.

Definice 1.7 (Gradovaná algebra)**.** Algebra A nad polem K je nazývána gradovanou, pokud může být zapsána jako přímá suma $A = \oplus_{k=0}^{\infty} A^k$ vektorových prostorů nad K, takových že zobrazení násobení splňuje $A^k \times A^l \to A^{k+l}$.

Z definice tenzorové algebry je zřejmé, že tato algebra je gradovaná. Například skalár ($T^0 V$) je tenzor řádu 0 a má stupeň 0, vektor ($T^1 V$) je tenzor řádu 1 a má stupeň 1 a tak dále. Tato vlastnost tenzorové algebry umožňuje manipulaci s objekty různých stupňů v rámci jedné algebraické struktury.

1.3. Cliffordova algebra

Cliffordova algebra je značena $Cl(V, Q)$, kde V je vektorový prostor a Q je kvadratická forma definovaná na vektorovém prostoru V. Přesná definice pak může být zapsána následovně.

Definice 1.8 (Cliffordova algebra, [6])**.** Nechť V je n-rozměrný vektorový prostor nad základním polem K a Q je kvadratická forma na V. Cliffordova algebra je pak definována jako

$$T(V)/I(Q) = T(V)/(\mathbf{v} \otimes \mathbf{v} - Q(\mathbf{v})\mathbb{1})$$

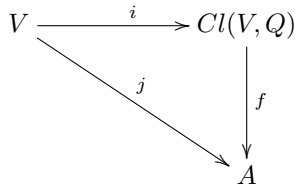
kde $T(V)$ je tenzorová algebra vektorového prostoru V, $I(Q)$ je oboustranný ideál generovaný kvadratickou formou Q a $\mathbb{1}$ je multiplikativní identita ve V.

Budeme se soustředit zejména na případy, kde základní pole K je $\mathbb{R}$ nebo $\mathbb{C}$. Cliffordova algebra má také některé zajímavé vlastnosti. Tato algebra je volná, unitární, asociativní a také gradovaná.

Alternativním způsobem popisu Cliffordovy algebry je *univerzální vlastnosti*. Tento přístup není konstruktivní, ale poskytuje dobrý kontext pro hlubší porozumění.

Definice 1.9 (Univerzální vlastnost Cliffordovy algebry)**.** Nechť V je vektorový prostor nad polem K, nechť A je unitární asociativní algebra s operací $\odot$. Nechť $Cl(V, Q)$ je Cliffordova algebra s operací $*$. Dále nechť i je lineární zobrazení i :

$V \to Cl(V,Q)$ splňující $i(\mathbf{v}) * i(\mathbf{v}) = Q(\mathbf{v})\mathbb{1}$ pro všechna $\mathbf{v} \in V$. Toto zobrazení je definováno pomocí **univerzální vlastnosti**: Pro libovolnou unitární asociativní algebru A nad K a libovolné lineární zobrazení $j : V \to A$, které splňuje $j(\mathbf{v}) \odot j(\mathbf{v}) = Q(\mathbf{v})\mathbb{1}_A$, kde $\mathbb{1}_A$ značí multiplikativní jednotku v A, pro všechna $\mathbf{v} \in V$, existuje jednoznačný algebraický homomorfismus $f : Cl(V,Q) \to A$, pro který platí, že následující diagram komutuje.



Komutováním je myšleno, $f \circ i = j$.

Vektorový prostor V je vybaven kvadratickou formou Q, a proto může být vytvořena ortogonální báze. S využitím symetrické bilineární formy asociované kvadratické formě Q můžeme psát: $\langle \mathbf{e}_i, \mathbf{e}_j \rangle = 0$ pro $i \neq j$ a $\langle \mathbf{e}_i, \mathbf{e}_i \rangle = Q(\mathbf{e}_i)$.

Často se setkáváme s Cliffordovými algebrami zapsanými ve formě $Cl_{p,q}(V,Q)$. Ty jsou nazývány p,q Cliffordovými algebrami. Nyní ukážeme obecný příklad vysvětlující význam koeficientů p, q, správně označovaných jako *signatura* Cliffordovy algebry.

Nechť $K = \mathbb{R}$ je základní pole pro vektorový prostor $V = \operatorname{span}\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ vybavený kvadratickou formou $Q(\alpha_1\mathbf{v}_1 + \cdots + \alpha_n\mathbf{v}_n)$, kde $\alpha \in \mathbb{R}$. Formu můžeme zapsat následujícím způsobem:

$$\begin{pmatrix}\alpha_1 & \ldots & \alpha_n\end{pmatrix} A \begin{pmatrix}\alpha_1 \\ \vdots \\ \alpha_n\end{pmatrix},$$

kde uvažujeme α_i jako koeficienty vektoru $\mathbf{v}$ zapsaného v bázi, a A značí matici odpovídající dané kvadratické formě.

Protože víme, že matice A je symetrická, $A = A^T$, z definice kvadratické formy plyne, že A je *ortogonálně diagonalizovatelná*:

$$U^T A U = \Lambda = \begin{pmatrix}\lambda_1 & & \\ & \ddots & \\ & & \lambda_n\end{pmatrix}.$$

Nyní je báze změněna vzhledem k diagonalizaci, $V = \operatorname{span}\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$. Kvadratická forma je nyní přepsána do tvaru

$$Q(\beta_1\mathbf{x}_1 + \cdots + \beta_n\mathbf{x}_n) = \lambda_1\beta_1^2 + \cdots + \lambda_n\beta_n^2, \quad \beta_i \in \mathbb{R}.$$

To znamená, že můžeme jednoduše psát $Q(\mathbf{x}_i) = \lambda_i$, odkud odvodíme $\mathbf{x}_i^2 = \lambda_i$.

Podívejme se nyní detailně čemu může být λ_i rovno. Možnosti se rozpadnou do tří neizomorfních případů:

$$\lambda_i = \begin{cases} 1, \\ 0, \\ -1. \end{cases}$$

Lze ukázat, že jiné případy, například 2, jsou izomorfní buď s 1 nebo -1.

Shrnutí všech poznatků a informací je následující. Nechť A je Cliffordova algebra $A \cong Cl(V, Q)$ s n generátory, pak vektorový prostor V a kvadratická forma Q mohou být zapsány následovně (kvadratická forma je již ortogonalizována s nenulovými prvky na diagonále):

$$V = \operatorname{span}\{\mathbf{x}_1, \ldots, \mathbf{x}_p, \mathbf{y}_1, \ldots, \mathbf{y}_q, \mathbf{z}_1, \ldots, \mathbf{z}_r\}, \quad p+q+r = n,$$

$$Q(\alpha_1\mathbf{x}_1 + \cdots + \alpha_p\mathbf{x}_p + \beta_1\mathbf{y}_1 + \cdots + \beta_q\mathbf{y}_q + \gamma_1\mathbf{z}_1 + \cdots + \gamma_r\mathbf{z}_r), \quad \alpha_i, \beta_i, \gamma_i \in \mathbb{R}.$$

Pro každé $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ nyní platí, již dříve popsaný, speciální případ:

$$\mathbf{x}_i^2 = 1, \quad \mathbf{y}_i^2 = -1, \quad \mathbf{z}_i^2 = 0.$$

V této práci se budeme zajímat o algebry, kde $r = 0$. Koeficienty p, q lze nyní snadno vysvětlit. Počet prvků v bázi, jejichž druhá mocnina je 1, je koeficient p, a počet prvků v bázi, jejichž druhá mocnina je -1, je koeficient q. Konkrétní algebra je potom zapsána se svou signaturou:

$$Cl_{p,q}(V, Q).$$

1.4. Vnější algebra

Vnější algebra, známá také jako Grassmannova algebra, se používá zejména v geometrii při studiu ploch, objemů a objektů vyšší dimenze. Využívá vnější součin.

Definice 1.10 (Vnější algebra)**.** Nechť V je n-rozměrný vektorový prostor nad základním polem K a I je ideál generovaný $(\mathbf{u}\otimes\mathbf{u})$. Vnější algebrou pak rozumíme:

$$T(V)/(\mathbf{u} \otimes \mathbf{u}),$$

což se obvykle značí jako $\bigwedge(V)$.

Na této algebře je definován tzv. vnější součin, v angličtině známý jako *wedge product*, viz [6].

Definice 1.11 (Vnější součin)**.** Nechť V je vektorový prostor nad základním polem K. Potom zobrazení $\bigwedge : V \times V \to V \otimes V$ se nazývá *vnější součin*, jestliže má následující vlastnosti:

(A1) *Antisymetrie*:

$$\mathbf{u} \wedge \mathbf{v} = -\mathbf{v} \wedge \mathbf{u},$$

(A2) *Škálování*:

$$(\alpha\mathbf{u}) \wedge \mathbf{v} = \alpha(\mathbf{u} \wedge \mathbf{v}),$$

(A3) *Distributivita*:

$$\mathbf{u} \wedge (\mathbf{v} + \mathbf{w}) = (\mathbf{u} \wedge \mathbf{v}) + (\mathbf{u} \wedge \mathbf{w})$$

pro všechna $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ a $\alpha \in K$.

Tato definice může být rozšířena na $\bigwedge : V \times \cdots \times V \to V^{\otimes k}$, čímž se přidá asociativita. Lineární kombinace součinů dvou vektorů $\mathbf{u} \wedge \mathbf{v}$ se nazývá *bivektor*, podobně lineární kombinace součinů tří vektorů se nazývá *trivektor* a lineární kombinace součinů k vektorů se nazývá *k-vektor*. Lineární kombinace smíšených k-vektorů se nazývá *multivektor*. Budeme také používat termín *blade*. Blade k-třídy se skládá z vnějšího součinu k vektorů. Bivektor lze chápat jako orientovanou rovinu a trivektor jako orientovaný objem.

Definice 1.12 (Vnější mocnina)**.** k-tá vnější mocnina, $\bigwedge^k(V)$, je definována jako vektorový podprostor $\bigwedge(V)$ generovaný prvky ve tvaru $\mathbf{x}_1 \wedge \mathbf{x}_2 \wedge \cdots \wedge \mathbf{x}_k$, kde $\mathbf{x}_i \in V$.

1.5. Bra-Ket notace

Při práci s vektory bude použita bra-ket notace. Tato notace je často využívána v kvantovém počítání k popisu kvantových stavů. Poskytuje způsob, jak popsat vektor $\mathbf{v}$ v komplexním vektorovém prostoru. *Ket* je označován jako $|a\rangle$, a *bra* je označován jako $\langle a|$.

Použití bra-ket notace je efektivnější než zápis vektorů do sloupců či řádků a umožňuje snadnější manipulaci s vektory. *Bra* reprezentuje sloupcový vektor a *ket* vznikne jeho transpozicí a komplexním sdružením:

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}, \qquad \langle a| = \begin{pmatrix} {a_1}^* & {a_2}^* & \dots & {a_n}^* \end{pmatrix}.$$

Obecně lze psát: $\langle a|^\dagger = |a\rangle$, $|a\rangle^\dagger = \langle a|$, kde symbol † je používán pro označení konjugované transpozice.

Vnitřní součin dvou vektorů je pak zapsán ve tvaru $\langle a||b\rangle$, což se zkracuje na $\langle a|b\rangle$.

2. Kvantové počítání

2.1. Qubit

Qubit je základní jednotkou v kvantové informatice a liší se od klasického bitu, který má pouze dva možné stavy - 0 nebo 1. Qubit totiž může existovat v superpozici obou stavů. To znamená, že qubit může uchovávat nejen 0 nebo 1, ale všechny možné kombinace těchto stavů současně. To otevírá široké spektrum možností pro zpracování a ukládání informací způsoby, které klasické bity neumožňují. Tato zvýšená flexibilita má však svou protiváhu. Hlavní výzvou v kvantovém počítání je najít způsoby, jak pomocí matematického aparátu reprezentovat a manipulovat s těmito superpozicemi. Další výzvou je navrhnout a sestavit hardware, které by tyto výpočty mohl efektivně implementovat.

Pro reprezentaci qubitů budou definovány dva ortonormální bázové stavy. Budou značeny $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ a $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$. Tyto dva stavy jsou většinou nazývány výpočetní bází.

Obecný kvantový stav je ztotožněn s normalizovaným vektorem, generovaným z ortonormální výpočetní báze v dvoudimenzionálním prostoru. Jak jsme již dříve zmínili, qubit je kombinací, v našem případě lineární kombinací, základních stavů a může být napsán následujícím způsobem:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\\beta\end{pmatrix}, \tag{2.1}$$

kde koeficienty α a β jsou komplexní čísla.

Koeficienty α a β jsou správně nazývány *pravděpodobnostní amplitudy*. Pokud změříme daný qubit, pravděpodobnosti získání výsledků $|0\rangle$ nebo $|1\rangle$ jsou $|\alpha|^2$ případně $|\beta|^2$. Druhý axiom pravděpodobnosti nám dává omezení $|\alpha|^2 + |\beta|^2 = 1$, které musí vždy platit. Koeficienty α a β jsou komplexní čísla a právě kvůli tomu má qubit čtyři stupně volnosti. Existuje více způsobů, jak se vyrovnat s tím, že pracujeme s objektem, který má čtyři stupně volnosti. Dají se také nalézt způsoby, jak qubit vhodně vizualizovat.

2.2. Blochova sféra

Elegantním způsobem reprezentace qubitů je Blochova sféra.

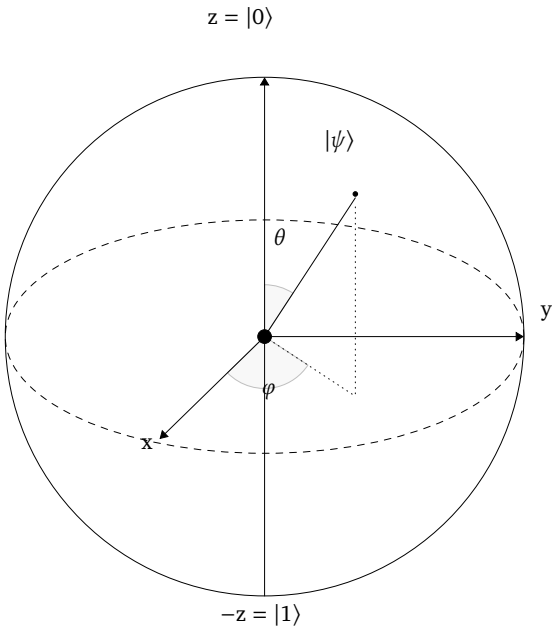
Vraťme se ke vztahu (2.1), můžeme vidět, že k popsání jednoho qubitu je potřeba kombinace dvou základních stavů. Také víme, že koeficienty α a β jsou komplexní čísla. Každý daný stav tak může být popsán čtyřmi reálnými čísly. Takový systém by bylo obtížné vizualizovat.

Ovšem vzhledem k tomu, že jsme identifikovali kvantové stavy s komplexními vektory, kde koeficienty jsou pravděpodobnostní amplitudy, můžeme nyní zavést *fázi*. Fáze je úhel mezi reálnou a imaginární složkou komplexního vektoru. Ve skutečnosti existují dva druhy fází. *Relativní fáze* se týká fázového rozdílu mezi dvěma pravděpodobnostními amplitudami. Je to míra toho, jak se amplitudy vzájemně ovlivňují. *Globální fáze* se týká celkové fáze kvantového stavu. Je to společný fázový faktor, který ovlivňuje všechny pravděpodobnostní amplitudy ve stavu. Zdůrazněme však, že globální fáze neovlivňuje pravděpodobnosti měření konkrétního výsledku. Navíc globální fáze nemá fyzikální význam, protože se zruší při výpočtu pravděpodobností. To znamená, že jeden stupeň volnosti lze odstranit. Pokud vezmeme v úvahu omezení dané druhým axiomem pravděpodobnosti, zbavíme se dalšího stupně volnosti. To nás vede k systému se dvěma stupni volnosti.

Jak již název napovídá, k reprezentaci qubitu bude použita sféra. A protože máme dva stupně volnosti, lze efektivně využít sférických souřadnic. Obecný qubit lze pak zapsat následujícím způsobem:

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{\mathrm{i}\phi}\sin(\theta/2)|1\rangle = \cos(\theta/2)|0\rangle + (\cos\phi + \mathrm{i}\sin\phi)\sin(\phi/2)|1\rangle,$$

kde $0 \leq \theta \leq \pi$ a $0 \leq \phi \leq 2\pi$.



Obrázek 2.1. Blochova sféra.

Při vhodném výběru parametrů θ a ϕ lze každý stav jednoznačně popsat, viz Obrázek 2.1. Přesněji řečeno platí jednoznačná korespondence mezi kvantovými stavy (reprezentovanými qubity) a body na sféře. Je důležité si uvědomit, že qubit má podobu dvourozměrného vektoru. Volba báze je zcela libovolná. V této práci jsme od začátku pracovali s $|0\rangle$ a $|1\rangle$. Tyto stavy lze ztotožnit se severním a jižním pólem naší sféry. Nicméně každý pár dvou protilehlých bodů je ortogonální, jejich vnitřní součin je nulový. Mohou tedy sloužit jako ortogonální báze. Z praktických důvodů se však budeme držet volby $|0\rangle$ a $|1\rangle$.

Stavy $|0\rangle$ a $|1\rangle$ jsou umístěny na z-ové ose. Nyní se podívejme blíže na x-ovou a y-ovou osu. Mají svůj vlastní pár protilehlých bodů. Na x-ové ose obvykle hovoříme o $|+\rangle$, $|-\rangle$, a na y-ové ose o $|i\rangle$, $|-i\rangle$. Tyto páry také mohou tvořit bázi, jak jsme již dříve uvedli. Jelikož byla zvolena báze $|0\rangle$, $|1\rangle$, vyjádříme nyní tyto páry bodů v této bázi a dostaneme

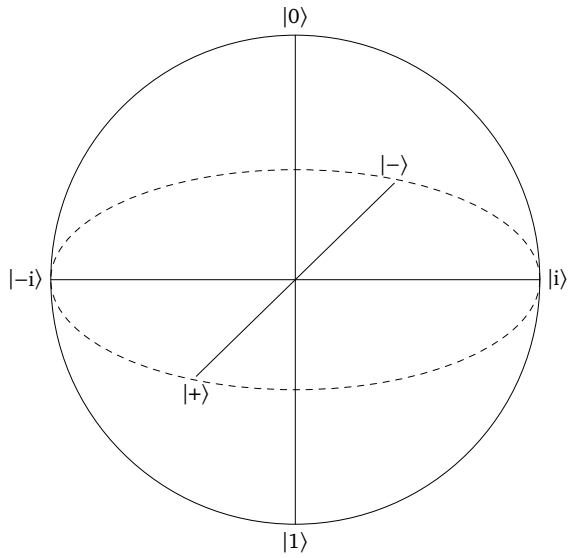
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

a

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).$$

Tyto body jsou poté vizualizovány na sféře, viz Obrázek 2.2.

Pokusíme se pochopit klasický bit z tohoto nového pohledu. Bylo řečeno, že bit může nabývat pouze dvou hodnot, 0 a 1. Může tedy být buď na severním pólu nebo



Obrázek 2.2. Blochova sféra – osy.

na jižním pólu naší sféry a nikde jinde. Qubit může zaujmout libovolnou pozici na sféře, zatímco klasický bit si musí vybrat mezi dvěma protilehlými body, které jsou zvoleny jako báze. Zde je jasně vidět obrovská variabilita, kterou poskytuje použití qubitů pro výpočty.

2.3. Multi qubity

Qubity byly spojeny se stavovými vektory a stavový vektor o dimenzi 2 byl použit pro reprezentaci jednoho qubitu. K reprezentaci multi qubitů stačí zvýšit dimenzi vektoru. Jeden qubit je reprezentován 2-dimenzionálním vektorem, dva qubity jsou reprezentovány 4-dimenzionálním vektorem a n-qubit je reprezentován 2^n-dimenzionálním vektorem. Dimenze také určuje, kolik bázových vektorů je potřeba. Podívejme se na příklad dvou qubitů a jak je zde stavový vektor konstruován.

$$|a\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = \begin{pmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{pmatrix}.$$

Připomeňme si, že koeficienty a_{ij} jsou *pravděpodobnostní amplitudy*. Kvadrát koeficientu $|a_{ij}|^2$ je pravděpodobnost změření stavu $|ij\rangle$.

Druhý axiom pravděpodobnosti musí platit i zde a proto dospíváme k následující normalizační podmínce:

$$|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1.$$

Stejná konstrukce bude použita pro n-qubity. Normalizační podmínka musí vždy platit.

Pro dva oddělené qubity definujeme *kolektivní stav* pomocí Kroneckerova součinu, viz vztah (1.1). K reprezentaci kolektivního stavu také použijeme stavový vektor. Dimenze stavového vektoru je 2^n, kde n je počet qubitů, které popisujeme. Podívejme se na příklad, jak je kolektivní stav dvou qubitů získán

$$|a\rangle = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} b_0 \\ a_1 \end{pmatrix},$$

$$|ba\rangle = |b\rangle \otimes |a\rangle = \begin{pmatrix} b_0 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \\ b_1 \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} b_0 a_0 \\ b_0 a_1 \\ b_1 a_0 \\ b_1 a_1 \end{pmatrix}.$$

Vstupem byly dva qubity a použili jsme Kroneckerův součin k sestavení stavového vektoru reprezentujícího kolektivní stav. Konečný stavový vektor má dimenzi 4. Bylo řečeno, že stavový vektor popisující kolektivní stav má dimenzi 2^n. Vzali jsme dva qubity, tedy 2^2, což je vskutku 4.

2.4. Měření

Uvedli jsme, že qubit může získat nejen hodnoty 0 a 1, ale všechny jejich kombinace. Avšak po provedení měření je qubit změřen buď na pozici odpovídající 0 nebo na pozici odpovídající 1. Je důležité objasnit, v jaké bázi se měření provádí. Stejný qubit můžeme měřit v různých bazích a získat různé výsledky. Měření v bázi $|0\rangle, |1\rangle$ dává možné výsledky $|0\rangle$ $|1\rangle$. Ale pokud změníme bázi například na $|+\rangle, |-\rangle$, pak jsou možné výsledky $|+\rangle$ a $|-\rangle$. Volba báze je klíčová pro správný výklad měření. Budeme se držet báze $|0\rangle$, $|1\rangle$.

Ve skutečnosti je poměrně jednoduché spočítat pravděpodobnost výsledků pro libovolný qubit. Výpočet vnitřního součinu mezi bázovým stavem a stavovým vektorem reprezentujícím qubit dává pravděpodobnost, že qubit skončí v konkrétním bázovém stavu. Přesněji řečeno, druhá mocnina této hodnoty je požadovaná pravděpodobnost. Vezměme si například obecný vektor $|\psi\rangle$ a podívejme se, jak získat pravděpodobnosti změření v bázových stavech $|0\rangle$, $|1\rangle$,

$$p(|0\rangle) = |\langle 0|\psi\rangle|^2, \qquad p(|1\rangle) = |\langle 1|\psi\rangle|^2.$$

3. Kvantové brány

Identifikovali jsme qubit se stavovým vektorem a nyní ho můžeme transformovat. Transformace qubitu je ve své podstatě pouze rotací na Blochově sféře. V klasické informatice pracují výpočty s logickými bránami. Tyto brány berou jako vstup jeden nebo více bitů, provádí operace definované matematickou logikou a jako výstup vracá opět bit nebo více bitů.

Pro smysluplné kvantové počítání je nutné zavést tyto logické brány. Blochova sféra je velmi užitečná pro vizualizaci toho, jak fungují brány na konkrétním qubitu. Pro brány na více qubitech bude použito tensorového součinu.

3.1. Brány na qubitu

Brány na qubitu berou jako vstup jeden qubit reprezentovaný stavovým vektorem, aplikují operátor a dávají jako výstup jiný stavový vektor

$$M|\psi\rangle \to |\psi'\rangle. \tag{3.1}$$

Můžeme vidět, že operátor M změní náš stavový vektor na jiný. Z lineární algebry je dobře známo, že matice se používají k transformaci vektorů. Matice tedy budou reprezentovat kvantové brány.

Tyto matice musí být unitární, protože norma vektoru musí být zachována.

Definice 3.1 (Unitární matice)**.** Invertibilní čtvercová matice se nazývá *unitární*, když její komplexně sdružená transpozice A^* je také její inverzní matice, $AA^* = A^*A = I$, kde I je jednotková matice.

Existuje nekonečně mnoho způsobů, jak napsat obecný tvar operátoru M. Jeden z možných tvarů je následující:

$$M(\phi, \theta, \lambda) = \begin{pmatrix} \cos(\theta/2) & -e^{\mathrm{i}\lambda}\sin(\theta/2) \\ \mathrm{e}^{\mathrm{i}\phi}\sin(\theta/2) & \mathrm{e}^{\mathrm{i}(\phi+\lambda)}\cos(\theta/2) \end{pmatrix}.$$

Tento tvar je však nepraktický a zbytečně složitý. Proto bude definována množina základních matic a požadovaný operátor bude poté získán kombinací těchto matic. S relativně malou množinou bázových matic lze získat libovolnou požadovanou matici. Navíc součin dvou unitárních matic je také unitární matice. Zvolené matice budou násobeny, vytvoří novou matici, která bude reprezentovat operátor. Stavový vektor je pak násoben konečnou maticí a tím se provede transformace.

Protože jsme zavedli Blochovu sféru pro reprezentaci qubitů, můžeme si představit transformace jako rotace na Blochově sféře. Pokud je splněna podmínka unitarity matice, zůstává stavový vektor na sféře a jen se kolem ní otáčí.

3.1.1. NOT brány. Základní logickou bránou v klasické informatice je NOT brána. Přepisuje hodnotu bitu na opačnou možnost. Bit s hodnotou 0 resp. 1 je změněn na 1 resp. 0. Situace u qubitů je trochu složitější. Jelikož qubit může nabývat libovolné hodnoty na Blochově sféře, nemůže být NOT brána tak snadno definována.

Začněme nejjednodušším příkladem. Pokud je qubit na severním pólu Blochovy sféry, což reprezentuje hodnotu $|0\rangle$, pak by NOT brána měla změnit jeho hodnotu na $|1\rangle$. Toho lze dosáhnout rotací stavového vektoru kolem x-ové nebo y-ové osy. Když je NOT brána aplikována na stavový vektor, jeho hodnota je změněna na hodnotu portilehlého bodu. Matice, které tuto transformaci provádějí, se ne vždy dají snadno nalézt. Prozatím bude stačit definovat rotace kolem osy x, y a z:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

3.1.2. Hadamardova brána. Možná nejdůležitější bránou v kvantovém počítání je takzvaná Hadamardova brána. Zaujímá zvláštní pozici v množině elementárních matic. Na první pohled nemusí být zřejmé, proč je tato matice tak zásadní. Její důležitost bude vysvětlena později, nyní bude poskytnuta pouze definice. Když Hadamardova brána působí na stavový vektor, otáčí vektor kolem osy $(x - z)$. Forma matice reprezentující Hadamardovu bránu je následující:

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

3.1.3. Fázová brána. Fázová brána slouží k otáčení stavového vektoru kolem osy z. Jako parametr přijímá reálné číslo ϕ, které určuje úhel otočení. Forma matice je následující:

$$P = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\phi} \end{pmatrix}.$$

Parametr ϕ můžeme měnit a získáme tak tzv. rodinu fázových bran.

3.2. Brány pro multi qubity

Brány pro multi qubity jsou klíčovým prvkem kvantového počítání, protože umožňují provádět operace na více qubitech současně. Stejně jako u bran pro jednotlivé qubity i u bran pro multi qubity se spoléhá na matematické operace s maticemi pro transformaci stavových vektorů. Nicméně matice používané pro multi qubitové brány jsou mnohem větší, s rozměry závislými na počtu vstupních qubitů. Rozměr matice brány pro multi qubit je roven $2^n \times 2^n$, kde n je počet vstupních qubitů. Tyto matice musí splňovat stejné vlastnosti jako matice pro jednotlivé qubity a jejich konstrukce vyžaduje pečlivé zvážení toho, jak brána působí na bázové stavy.

Pro ilustraci tohoto konceptu můžeme zmínit některé běžné příklady bran pro multi qubity. Například existují 2-qubitové brány jako je CNOT (Controlled NOT) brána, SWAP brána a CZ brána (controlled phase gate). Kromě toho existují 3-qubitové brány, jako je Toffoliho brána (také známá jako CCNOT brána). Je důležité poznamenat, že tyto brány jsou jen několika příklady z mnoha možných bran pro multi qubity a volba konkrétní brány bude záviset na požadovaném účelu daného výpočetního systému. Nicméně porozumění základům toho, jak tyto brány fungují a jak ovlivňují stavové vektory, je klíčovým krokem při návrhu efektivních kvantových obvodů.

3.2.1. CNOT brána. Controlled-NOT brána je nejpoužívanější bránou pro multi qubity. Přijímá dva qubity jako vstup, zkontroluje hodnotu prvního qubitu nazývaného *controlled qubit*, a pokud je 1, obrátí hodnotu druhého qubitu nazývaného *target qubit*. Podívejme se, jak brána působí na bázové stavy:

$$\mathrm{CNOT}|00\rangle = |00\rangle, \quad \mathrm{CNOT}|01\rangle = |01\rangle, \quad \mathrm{CNOT}|10\rangle = |11\rangle, \quad \mathrm{CNOT}|11\rangle = |10\rangle.$$

Matice reprezentující CNOT bránu má následující formu:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

První dva řádky odpovídají případům, kdy je controlled qubit ve stavu $|0\rangle$ a proto se nic nemění. Třetí a čtvrtý řádek odpovídá situaci, kdy je controlled qubit ve stavu $|1\rangle$ a tedy se hodnota target qubitu obrátí.

3.2.2. SWAP brána. SWAP brána je velmi jednoduchá. Jednoduše prohodí stavy dvou qubitů. Nemá vliv na stavy $|00\rangle$, $|11\rangle$, ale ovlivňuje stavy $|10\rangle$, $|01\rangle$. Matice, která ji reprezentuje je následující:

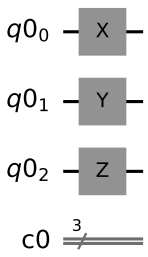
$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

3.2.3. CZ brána. Také nazývaná Controlled-Z brána provádí rotaci kolem osy z, pokud je první qubit (controlled qubit) roven 1. Má například vliv na stav $|11\rangle$, který je poté změněn na $-|11\rangle$. Obecná forma je následující:

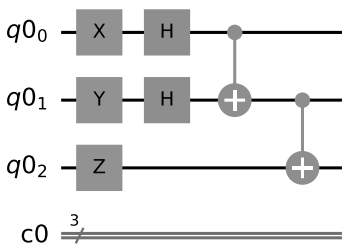
$$\text{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

3.3. Kvantový obvod

Nyní můžeme začít s konstrukcemi kvantových obvodů. Budeme používat nástroj Qiskit [11]. Podívejme se na příklad na Obrázku 3.1.



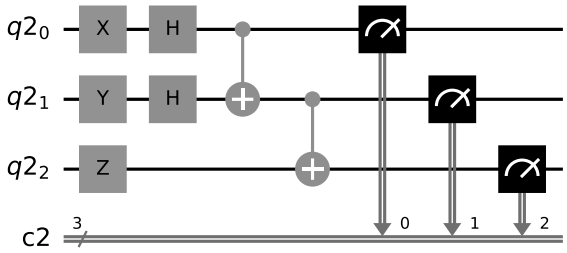
Obrázek 3.1. Základní brány.



Obrázek 3.2. Hadamardova brána a C-NOT brána.

Tento obvod bere jako vstup tři qubity. Každý z nich je uložen na samostatném vlákně. Tyto vlákna budou označeny jako $q0_i$ a budou použity k uložení qubitů. Zajímá nás pouze dolní index i a nula ve výrazech pro qubity pro nás nemá žádný

zvláštní význam. Klasické bity jsou také použity v obvodech. Používají se k uložení hodnoty získané z měření qubitu. Jsou označeny jako $c0$ a spojeny do jednoho vlákna, aby se ušetřilo místo a obvody byly srozumitelnější. Můžeme vidět, že na kvantových drátech jsou již kvantové brány, konkrétně brány X, Y a Z. Tyto brány působí na konkrétní qubity. Nyní mohou být přidány další brány, například Hadamardova brána a C-NOT brána, viz Obrázek 3.2. Všimněme si, že C-NOT brána je brána 2-qubitová, což znamená, že má jako vstup dva qubity. Posledním krokem k funkčnímu obvodu je přidání měření. Zde jsou klasické bity užitečné. Měření je umístěno na vlákno s qubitem a výsledek je uložen do klasického bitu. Protože existují pouze dvě možnosti, jak měření může skončit, je možné tuto hodnotu uložit do klasického bitu. Na Obrázku 3.3 je vidět, jak je měření prováděno a kde jsou výsledky uloženy.



Obrázek 3.3. Měření.

Tento obvod nemá žádný konkrétní účel, ale může sloužit jako příklad. V následující kapitole bude ukázáno, jak můžeme tyto obvody reprezentovat pomocí geometrických algeber.

4. Geometrické algebry v kvantovém počítání

Myšlenka implementace geometrických algeber (GA) v kvantovém počítání (QC) spočívá ve speciálním způsobu reprezentace qubitů. Jednotlivé qubity jsou asociovány s prvky GA a stejně tak i kvantové brány jsou asociovány s prvky GA. Díky tomu se nám otevírá cesta pro přímou implementaci. Jednotlivé transformace qubitů pomocí kvantových bran se dají repreznotovat jako součin prvků, které reprezentují kvantový stav a kvantovou bránu.

4.1. Geometrická algebra

Nyní definujeme vhodný aparát GA pro účely QC. V první kapitole byly diskutovány a obecně definovány základní algebraické pojmy. Tyto definice budou nyní mírně upraveny pro konkrétní účely. Začneme s případem reálné GA. Abychom mohli správně definovat GA, musí být zaveden nový pojem nazývaný *geometrický součin*, viz [3, 4]. Geometrický součin je kombinací vnitřního a vnějšího součinu. Mějme reálný vektorový prostor $\mathbb{R}^n$. Vektorový prostor má ortonormální bázi $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$. Je také vybaven bilineárním formou B se signaturou (p, q).

$$B(\mathbf{e}_i, \mathbf{e}_j) = \begin{cases} 1, & \text{je-li } i = j = 1, \dots, p, \\ -1, & \text{je-li } i = j = p+1, \dots, m, \\ 0, & \text{je-li } i \neq j. \end{cases} \tag{4.1}$$

Všimněme si, že bilineární forma B je symetrická. Proto lze definovat k ní asociovanou kvadratickou formu Q. Vztah je následující:

$$B(\mathbf{a}, \mathbf{b}) = \frac{1}{2}\big(Q(\mathbf{a}+\mathbf{b}) - Q(\mathbf{a}) - Q(\mathbf{b})\big). \tag{4.2}$$

Definice 4.1. V případě vektorového prostoru $\mathbb{R}^n$ s bilineární formou B je vnitřní součin definován jako

$$\mathbf{e}_i \cdot \mathbf{e}_j = B(\mathbf{e}_i, \mathbf{e}_j).$$

Pro definici vnějšího součinu použijeme definici z vnější algebry, Definice 1.11. Sečtení těchto dvou součinů vede k tzv. geometrickému součinu, viz [8].

Definice 4.2 (Geometrický součin)**.** Geometrický součin, označovaný jako $\mathbf{e}_i\mathbf{e}_j$, dvou bázových vektorů je kombinací vnitřního a vnějšího součinu

$$\mathbf{e}_i\mathbf{e}_j = \mathbf{e}_i \cdot \mathbf{e}_j + \mathbf{e}_i \wedge \mathbf{e}_j.$$

Je důležité si všimnout všech užitečných vlastností, které geometrický součin má. Tyto vlastnosti budou široce využívány, protože nám umožňují zjednodušit výpočty.

Poznámka. Vzhledem k tomu, že vnitřní součin dvou ortonormálních prvků je roven nule, viz (4.1), redukuje se geometrický součin dvou ortonormálních prvků na jejich vnější součin,

$$\mathbf{e}_i\mathbf{e}_j = \mathbf{e}_i \wedge \mathbf{e}_j.$$

Podobné chování má také vnější součin. V případě bázových prvků víme, že vnější součin prvku se sebou samým je roven nule. Proto můžeme odvodit, že geometrický součin dvou ortonormálních bázových prvků se redukuje na vnitřní součin, který je buď plus nebo mínus jedna,

$$\mathbf{e}_i\mathbf{e}_i = \mathbf{e}_i \cdot \mathbf{e}_i = \begin{cases} 1, & \text{pokud } i = j = 1, \dots, p, \\ -1, & \text{pokud } i = j = p+1, \dots, m. \end{cases}$$

Tyto definice jsou nyní rozšířeny na obecný stupeň r bladu. Pro vnitřní součin dostaneme tvar

$$\mathbf{e}_j \cdot \mathbf{e}_A = \sum_{k=1}^{r} (-1)^k B(\mathbf{e}_j, \mathbf{e}_{i_k}) \mathbf{e}_{A\setminus\{i_k\}}.$$

Pro vnější součin získáme

$$\mathbf{e}_j \wedge \mathbf{e}_A = \begin{cases} \mathbf{e}_j \wedge \mathbf{e}_{i_1} \wedge \cdots \wedge \mathbf{e}_{i_r}, & \text{pokud } j \notin A, \\ 0 & \text{pokud } j \in A. \end{cases}$$

A pro geometrický součin jednoduše definujeme

$$\mathbf{e}_i\mathbf{e}_A = \mathbf{e}_j \cdot \mathbf{e}_A + \mathbf{e}_j \wedge \mathbf{e}_A.$$

Zkonstruovaná algebra se nazývá reálná geometrická algebra s přislušným geometrickým součinem, který se také nazývá Cliffordův součin. Obvykle je značena jako $\mathbb{G}_{p,q}$. Tato algebra je ve skutečnosti dobře známou Cliffordovou algebrou, viz Definice 1.8. Kvadratická forma, která generuje ideál, je ta asociovaná s bilineární formou (4.2). S vědomím toho, že zkonstruovaná geometrická algebra je ve skutečnosti Cliffordova algebra, můžeme využít všechny vlastnosti, které Cliffordova algebra má. Tato algebra je asociativní a také volná, což znamená, že ji lze generovat z bázových prvků pomocí geometrického součinu.

Vnitřní a vnější součin lze považovat za symetrický a antisymetrický součin, $\mathbf{a} \cdot \mathbf{b} = \frac{1}{2}(\mathbf{ab} + \mathbf{ba})$ a $\mathbf{a} \wedge \mathbf{b} = \frac{1}{2}(\mathbf{ab} - \mathbf{ba})$. Tyto vlastnosti lze odvodit přímo z definice těchto operací a poté jsou zapsány ve formě geometrického součinu.

4.2. Komplexifikace

Tato kapitola využívá mnoho definic z [5]. Rozšiřuje tyto koncepty, propojuje je s již definovanými a poskytuje příklady pro lepší porozumění.

Abychom mohli reprezentovat komplexní povahu qubitů, je nutné zavést komplexní čísla. Nastavení základního pole na $\mathbb{C}$ ale samo o sobě nestačí, protože potřebujeme komplexní chování přenést přímo do algebry. Toho lze dosáhnout definicí speciální ortogonální lineární transformace a také nastavením báze vektorového prostoru na sudý. Uvažujme lineární ortogonální transformaci $J : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$ takovou, že $J^2 = -1$, kde 1 je identita. Akce J na ortonormální bázi $(\mathbf{e}_1, \ldots, \mathbf{e}_{2n})$ je následující, viz [5]:

$$J(\mathbf{e}_j) = -\mathbf{e}_{j+n}, \quad J(\mathbf{e}_{j+n}) = \mathbf{e}_j,$$

kde $j = 1, \ldots, n$. S použitím J nyní představíme novou transformovanou bázi, která se v kontextu QC ukazuje býti velmi praktickou, viz [5].

Definice 4.3. Wittova báze je tvaru

$$\begin{aligned} f_j &= \frac{1}{2}(1 + iJ)(\mathbf{e}_j) = \frac{1}{2}(\mathbf{e}_j - i\mathbf{e}_{j+n}), \quad j = 1, \ldots, n, \\ f_j^\dagger &= \frac{1}{2}(1 - iJ)(\mathbf{e}_j) = \frac{1}{2}(\mathbf{e}_j + i\mathbf{e}_{j+n}), \quad j = 1, \ldots, n. \end{aligned}$$

Tato definice je zvláště elegantní, protože můžeme ověřit, že pro každé $j = 1, \ldots, n$ platí $f_j^2 = 0$ a $f_j^{\dagger 2} = 0$. Skutečně,

$$\begin{aligned} f^2 &= \frac{1}{2}(\mathbf{e}_j - i\mathbf{e}_{j+n})\frac{1}{2}(\mathbf{e}_j - i\mathbf{e}_{j+n}) \\ &= \frac{1}{4}(\mathbf{e}_j^2 - i\mathbf{e}_j\mathbf{e}_{j+n} - i\mathbf{e}_{j+n}\mathbf{e}_j + i^2\mathbf{e}_{j+n}^2) \\ &= \frac{1}{4}(1 - i\mathbf{e}_j\mathbf{e}_{j+n} + i\mathbf{e}_j\mathbf{e}_{j+n} - 1) = \frac{1}{4}(0) = 0. \end{aligned} \tag{4.3}$$

Volba tohoto konkrétního f, $f^\dagger$ je také motivována skutečností, že jsou splněny jak Grassmanovy tak dualní identity:

$$\begin{aligned} ff^\dagger + f^\dagger f &= 1, \\ f_j f_k + f_k f_j = f_j^\dagger f_k^\dagger + f_k^\dagger f_j^\dagger, &\quad j,k = 1,\dots,n, \\ f_j f_k^\dagger + f_k^\dagger f_j &= \delta_{jk}, \quad j,k = 1,\dots,n, \end{aligned} \tag{4.4}$$

kde symbol δ_{jk} je Kroneckerovo delta.

Jednoduchým způsobem, jak zkonstruovat bázi celé Cliffordovy algebry $\mathbb{C}_{2n}$, je použití geometrického součinu. Můžeme použít Grassmannovy blady Wittových prvků. Konstrukce je následující;

$$\begin{aligned} f_j f_k &= f_j \cdot f_k + f_j \wedge f_k = f_j \wedge f_k \\ f_j^\dagger f_k^\dagger &= f_j^\dagger \cdot f_k^\dagger + f_j \dagger \wedge f_k^\dagger = f_j^\dagger \wedge f_k^\dagger \\ f_j f_k^\dagger &= f_j \cdot f_k^\dagger + f_j \wedge f_k^\dagger = \frac{1}{2}\delta_{jk} + f_j \wedge f_k^\dagger \end{aligned} \tag{4.5}$$

Pro rozšíření Wittovy báze na celou algebru $\mathbb{C}_{2n}$ stačí vzít 2^{2n} možných geometrických součinů

$$(f_1)^{i_1}(f_1^\dagger)^{j_1}\dots(f_n)^{i_n}(f_n^\dagger)^{j_n}, \quad i_k, j_k \in \{0,1\} \text{ pro } k = 1,\dots,n.$$

4.3. Qubit v GA

Jak jsme již dříve zmínili, qubit bude reprezentován prvkem ležícím v komplexní Cliffordově algebře $\mathbb{C}_2$. Můžeme použít Wittovy bázové vektory $(f, f^\dagger)$ k vytvoření báze pro komplexní Cliffordovu algebru. Bázi lze následně zapsat ve tvaru $(1, f, f^\dagger, ff^\dagger)$. Předtím, než identifikujeme qubit s konkrétním prvkem, zmiňme podrobněji vlastnosti této algebry. Volba báze nás vede k dvěma primitivním idempotentům v této algebře, konkrétně $I = ff^\dagger$ a $K = f^\dagger f$. Konvence v oblasti fyziky, do kterých zde nebudeme do detailu zabíhat, nám pro použití určují idempotent I. S touto volbou lze dospět k následující reprezentaci stavů $|0\rangle$ a $|1\rangle$ u qubitu:

$$|0\rangle = I = ff^\dagger, \qquad |1\rangle = f^\dagger I = f^\dagger ff^\dagger = (1 - ff^\dagger)f^\dagger = f^\dagger.$$

Nyní můžeme přejít k definici qubitu, viz vztah (2.1), a použít naši reprezentaci stavů $|0\rangle$ a $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha ff^\dagger + \beta f^\dagger = (\alpha + \beta f^\dagger)I.$$

4.4. Brány v GA

Po zbytek této práce budeme držet tuto reprezentaci stavů $|0\rangle$ a $|1\rangle$. Nyní můžeme přistoupit ke konstrukci bran. Základní brány lze snadno získat s ohledem na jejich účinek na bázové stavy. K odlišení mezi maticovou reprezentací a GA reprezentací budeme používat různou notaci, viz [5]:

$$\begin{aligned} \text{X-brána:} &\quad \lambda_X = f^\dagger + f, \\ \text{Y-brána:} &\quad \lambda_Y = if^\dagger - if, \\ \text{Z-brána:} &\quad \lambda_Z = ff^\dagger - f^\dagger f, \end{aligned}$$

Uvedli jsme formu Z-brány v GA. Víme však, že Z-brána je pouze speciálním případem obecnější fázové brány. V jazyce GA má tato brána následující tvar, viz [5]:

$$\text{Fázová brána:} \quad \lambda_P = ff^\dagger - e^{i\phi} f^\dagger f.$$

Konkrétní fázové brány, o kterých jsme dříve mluvili, se získávají obdobným způsobem. Parametr ϕ se mění a vznikají různé brány. A při volbě $\phi = \pi$ dostáváme Z-bránu. Poslední důležitou branou, která nebyla zmíněna, je Hadamardova brána. Její konstrukce není intuitivní, proto přecházíme rovnou ke konečnému tvaru, viz [5]:

$$\lambda_H = \frac{1}{\sqrt{2}}\left(ff^\dagger - f^\dagger f + f + f^\dagger\right).$$

Všechny základní brány jsou zadefinovány a lze dojít k závěru, že každou bránu lze zapsat jako

$$\lambda = aff^\dagger + bf + cf^\dagger + df^\dagger f,$$

kde $a, b, c, d \in \mathbb{C}$ tak, že platí $a^2 + c^2 = b^2 + d^2 = 1$ a $\overline{b}a + \overline{d}c = 0$.

Tyto omezení zřetelně připomínají podmínky, které jsme specifikovali při definování obecné matice pro reprezentaci kvantové brány při maticové reprezentaci. Není to náhoda a také to ukazuje ekvivalenci mezi těmito dvěma typy reprezentace. Můžeme dokonce vyjádřit vztah

$$aff^\dagger + bf + cf^\dagger + df^\dagger f \longleftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

4.5. Multi qubity a jejich brány v GA

Připomeňme si nejprve, že pro bázi komplexní algebry $\mathbb{C}_{2n}$ používáme prvky $(f_1, f_1^\dagger, \ldots, f_n, f_n^\dagger)$ a s nimi konstruujeme 2^{2n} kombinací jejich geometrického součinu. To vede k dvěma primitivním idempotentům I a K. Idempotent I bude opět použit

$$I = I_1 \ldots I_n = f_1 f_1^\dagger \ldots f_n f_n^\dagger,$$

kde $I_i = f_i f_i^\dagger$.

Nyní bude zavedena definice obecného n-qubitu. Realizace je provedena v prostoru dimenze $N = 2^{2n}$ s ortonormální bází

$$|i_1 \ldots i_n\rangle = (f_1^\dagger)^{i_1} \ldots (f_n^\dagger)^{i_n} I,$$

kde $i_1, \ldots, i_n \in \{0, 1\}$.

Následujícím krokem je zkonstruování bran pro multi qubity. Základní brány budou zapsány ve formě matice. Brány reprezentující matice jsou obvykle řídké. Proto není obtížné zapsat matici ve formě sumy, ve které má každá matice pouze jednu nenulovou hodnotu:

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Každá matice v sumě je nyní zapsána ve formě vnějšího součinu. A vnější součin lze velmi jednoduše přepsat do GA. Také víme, že stav $\langle i_1 i_2|$ je pouze hermitovskou konjugací stavu $|i_1 i_2\rangle$. Proto můžeme odvodit

$$\begin{aligned} |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| & \\ &= II^\dagger + f_2^\dagger II^\dagger f_2 + f_1^\dagger f_2^\dagger II f_1 + f_1^\dagger II^\dagger f_2 f_1 \\ &= I + f_2^\dagger I f_2 + f_1^\dagger f_2^\dagger I f_1 + f_1^\dagger I f_2 f_1 \\ &= f_1 f_1^\dagger f_2 f_2^\dagger + f_1 f_1^\dagger f_2^\dagger f_2 - f_1^\dagger f_1 f_2^\dagger - f_1^\dagger f_1 f_2 \\ &= f_1 f_1^\dagger - f_1^\dagger f_1 (f_2^\dagger + f_2) \end{aligned}$$

Forma ostatních bran pro více qubitů je získána stejným způsobem. Tedy

$$\begin{aligned} \lambda_{CNOT} &= f_1 f_1^\dagger - f_1^\dagger f_1 (f_2^\dagger + f_2), \\ \lambda_{CZ} &= f_1 f_1^\dagger + f_1^\dagger f_1 (f_2 f_2^\dagger - f_2^\dagger f_2), \\ \lambda_{SWAP} &= f_1 f_1^\dagger f_2 f_2^\dagger + f_1^\dagger f_1 f_2^\dagger f_2 + f_1^\dagger f_2 - f_1 f_2^\dagger. \end{aligned} \tag{4.6}$$

Tato konstrukce lze použít pro libovolnou bránu. Maticová reprezentace je zapsána ve formě vnějšího součinu a pak převedena do GA.

4.6. Paralelní brány

Podobně jako v maticové reprezentaci i v GA reprezentaci je třeba vyřešit, jak reprezentovat paralelní brány působící na multi qubity. Řešením bude použití tenzorového součinu.

Definice 4.4 (Tenzorový součin bran)**.** Tenzorový součin $\lambda_1 \otimes \cdots \otimes \lambda_n$, kde $\lambda_k \in \left\{ f_k f_k^\dagger, f_k^\dagger f_k, f_k, f_k^\dagger \right\}$ pro každé $k = 1, \ldots, n$, je reprezentován geometrickým součinem $(-1)^s \lambda_1 \ldots \lambda_n$, kde znaménko je určeno kardinalitou množin S_i, tak že $s = \sum_i |S_i|$, kde

$$S_i = \left\{ l < i : \lambda_l = f_l \text{ nebo } \lambda_l = f_l^\dagger f_l \right\} \text{ v případě, že } \lambda_i = f_i \text{ nebo } \lambda_i = f_i^\dagger.$$

4.7. Měření

Poslední věcí, kterou je třeba zavést, je měření. Pro výpočet pravděpodobnosti určitého výsledku v maticové reprezentaci jsme pouze provedli vnitřní součin určitého výsledku s transformovaným qubitem. A druhá mocnina tohoto vnitřního součinu byla konkrétní pravděpodobností. V GA se použije takzvaná skalární projekce, označovaná jako $[\,\cdot\,]_0$. Skalární projekce vezme pouze skalární část multivektoru. Můžeme pro ní použít následující vzorec

$$\langle \rho | \psi \rangle = 2^n \left[\rho^\dagger \psi \right]_0,$$

kde n je počet qubitů. Tento faktor je třeba zavést kvůli našemu výběru báze a kvůli spinorové povaze reprezentace, kterou zde nebudeme diskutovat podrobněji. Podívejme se na příklad, jak tato skalární projekce funguje:

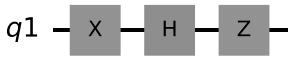
$$\langle 0|1\rangle = 2^1\left[ff^\dagger f^\dagger\right]_0 = 0, \qquad \langle 0|0\rangle = 2^1\left[ff^\dagger\right]_0 = 1$$

Výsledky jsou dle očekávání. Připomeňme pouze, že $ff^\dagger = \frac{1}{2} + f \wedge f^\dagger$ a tedy $\left[ff^\dagger\right]_0 = \frac{1}{2}$.

4.8. Příklad obvodu

V této kapitole si ukážeme některé jednoduché příklady, jak reprezentovat kvantové obvody v GA. Začneme příkladem sériového sestavení bran, kde se nesetkáme s tenzorovým součinem. Vždy budeme porovnávat maticovou reprezentaci a GA reprezentaci.

Příklad 4.5 (Sériové sestavení bran)**.** První příklad ukazuje obvod, kde jsou všechny brány umístěny na jedno vlákno, jak lze vidět na Obrázku 4.1.



Obrázek 4.1. Sériové sestavení bran.

Začneme s maticovou reprezentací. Všechny matice se vynásobí a získáme matici reprezentující obvod

$$M = ZHX = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}. \tag{4.7}$$

Pro libovolný qubit nyní můžeme spočítat pravděpodobnost, že qubit skončí v konkrétním bázovém stavu. Qubit je vynásoben maticí obvodu, a poté se provede vnitřní součin s konkrétním bázovým stavem. Budeme používat bázové qubity $|\psi\rangle = |0\rangle$ a $|\rho\rangle = |1\rangle$. Spočítáme transformovaný qubit a pak provedeme vnitřní součin s bázovým stavem pro získání pravděpodobností:

$$|\psi'\rangle = M|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\ 1\end{pmatrix},$$

$$|\rho'\rangle = M|\rho\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix},$$

$$p(|0\rangle) = |\langle 0|\psi'\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}-1\\ 1\end{pmatrix}\right|^2 = \left|-\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

$$p(|1\rangle) = |\langle 1|\psi'\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}-1\\ 1\end{pmatrix}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

$$p(|0\rangle) = |\langle 0|\rho'\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

$$p(|1\rangle) = |\langle 1|\rho'\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\end{pmatrix}\begin{pmatrix}1\\1\end{pmatrix}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}\,.$$

Pro oba vektory je součet pravděpodobností roven 1. Omezení dáno druhým axiomem pravděpodobnosti je splněno, a můžeme dospět k závěru, že naše výpočty jsou správné:

$$p(|0\rangle) + p(|1\rangle) = \frac{1}{2} + \frac{1}{2} = 1.$$

Nyní si ukážme alternativu. Obvod bude reprezentován pomocí aparátu GA. Pak

$$\begin{aligned}
\lambda_M = \lambda_Z\lambda_H\lambda_X &= (ff^\dagger - f^\dagger f)\frac{1}{\sqrt{2}}(ff^\dagger - f^\dagger f + f + f^\dagger)(f^\dagger + f)\\
&= \frac{1}{\sqrt{2}}(ff^\dagger ff^\dagger - ff^\dagger f^\dagger f + ff^\dagger f + ff^\dagger f^\dagger)(f^\dagger + f)\\
&= \frac{1}{\sqrt{2}}(ff^\dagger + f + f^\dagger f - f^\dagger)(f^\dagger + f)\\
&= \frac{1}{\sqrt{2}}(ff^\dagger f^\dagger + ff^\dagger f + ff^\dagger + ff = f^\dagger ff^\dagger + f^\dagger ff - f^\dagger f^\dagger - f^\dagger f)\\
&= \frac{1}{\sqrt{2}}(f^\dagger - f^\dagger f + f + ff^\dagger).
\end{aligned}$$

Tento výraz může být považován za ekvivalent k finální matici získané v maticové reprezentaci. Nyní budou spočteny transformované qubity:

$$\begin{aligned}
|\psi'\rangle = \lambda_M|\psi\rangle &= \frac{1}{\sqrt{2}}(f^\dagger - f^\dagger f + f + ff^\dagger)(ff^\dagger)\\
&= \frac{1}{\sqrt{2}}(f^\dagger ff^\dagger - f^\dagger fff^\dagger + fff^\dagger + ff^\dagger ff^\dagger)\\
&= \frac{1}{\sqrt{2}}(f^\dagger + ff^\dagger),
\end{aligned}$$

$$\begin{aligned}
|\rho'\rangle = \lambda_M|\rho\rangle &= \frac{1}{\sqrt{2}}(f^\dagger - f^\dagger f + f + ff^\dagger)f^\dagger\\
&= \frac{1}{\sqrt{2}}(f^\dagger f^\dagger - f^\dagger ff^\dagger + ff^\dagger + ff^\dagger f^\dagger)\\
&= \frac{1}{\sqrt{2}}(ff^\dagger - f^\dagger).
\end{aligned}$$

Můžeme přistoupit k výpočtu pravděpodobnosti změření qubitů v konkrétních bázových stavech:

$$\begin{aligned}
p(|0\rangle) = |\langle 0|\psi'\rangle|^2 &= \left|2\left[ff^\dagger\frac{1}{\sqrt{2}}(f^\dagger + ff^\dagger)\right]_0\right|^2 = \left|\frac{2}{\sqrt{2}}\left[ff^\dagger f^\dagger + ff^\dagger ff^\dagger\right]_0\right|^2\\
&= \left|\frac{2}{\sqrt{2}}\left[ff^\dagger\right]_0\right|^2 = \left|\frac{2}{\sqrt{2}}\frac{1}{2}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}\,.
\end{aligned}$$

Ostatní pravděpodobnosti jsou spočteny stejným způsobem a proto je ukázána pouze zkrácená verze:

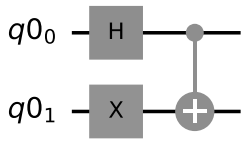
$$p(|1\rangle) = |\langle 1|\psi'\rangle|^2 = \left|2\left[f\frac{1}{\sqrt{2}}(f^\dagger + ff^\dagger)\right]_0\right|^2 = \frac{1}{2},$$

$$p(|0\rangle) = |\langle 0|\rho'\rangle|^2 = \left|2\left[ff^\dagger\frac{1}{\sqrt{2}}(ff^\dagger - f^\dagger)\right]_0\right|^2 = \frac{1}{2},$$

$$p(|1\rangle) = |\langle 1|\rho'\rangle|^2 = \left|2\left[f\frac{1}{\sqrt{2}}(ff^\dagger - f^\dagger)\right]_0\right|^2 = \frac{1}{2}.$$

Nyní můžeme ověřit, že součet pravděpodobností je pro oba vektory 1. Pravděpodobnosti spočítané pomocí GA reprezentace jsou stejné jako pravděpodobnosti spočítané pomocí maticové reprezentace. GA reprezentace se ukazuje jako korektní.

Příklad 4.6 (Paralelní sestavení bran)**.** V tomto příkladu je zkoumáno chování paralelního sestaveního bran. Na jednom vlákně je Hadamardova brána a na druhém X-brána. Poté je použita CNOT brána, přičemž první qubit je controlled qubitem, viz Obrázek 4.2.



Obrázek 4.2. Obvod s CNOT bránou.

Nejprve bude ukázána maticová reprezentace. Bude proveden tenzorový součin Hadamardovy brány a X-brány. Forma CNOT brány je známá, viz rovnice 4.6:

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

a

$$H \otimes X = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & -1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$

Finálni matice je získána součinem CNOT brány s $H \otimes X$, tj.

$$M = \mathrm{CNOT}(H \otimes X) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$
$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Ukážeme si účinek obvodu na dvou příkladech qubitů, a to konkrétně na $\psi = |00\rangle$ a $\rho = |01\rangle$:

$$|\psi'\rangle = M|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

$$|\rho'\rangle = M|\rho\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Získali jsme transformované qubity a můžeme provést měření:

$$p(|00\rangle) = |\langle 00|\psi'\rangle|^2 = \left| \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right|^2 = 0,$$

$$p(|01\rangle) = |\langle 01|\psi'\rangle|^2 = \left| \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2},$$

$$p(|10\rangle) = |\langle 01|\psi'\rangle|^2 = \left| \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$p(|11\rangle) = |\langle 11|\psi'\rangle|^2 = \left| \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right|^2 = 0.$$

Měření druhého qubitu bude zkráceno.

$$p(|00\rangle) = |\langle 00|\rho'\rangle|^2 = \frac{1}{2}, \qquad p(|01\rangle) = |\langle 01|\rho'\rangle|^2 = 0,$$
$$p(|10\rangle) = |\langle 10|\rho'\rangle|^2 = 0, \qquad p(|11\rangle) = |\langle 11|\rho'\rangle|^2 = \frac{1}{2}.$$

Jedndoduše lze ověřit že součet pravděpodobností je 1 pro oba případy.

Tentýž obvod je nyní realizován ve formě GA. Je proveden tenzorový součin Hadamardovy brány a X-brány. Forma CNOT hradla je známa, viz (4.6). Proto

$$\begin{aligned}\lambda_{HX} =& \lambda_H \otimes \lambda_X = \frac{1}{\sqrt{2}}\big(f_1 f_1^\dagger - f_1^\dagger f_1 + f_1 + f_1^\dagger\big)\big(f_2^\dagger + f_2\big),\\ =& \frac{1}{\sqrt{2}}\big(f_1 f_1^\dagger f_2^\dagger + f_1 f_1^\dagger f_2 + f_1^\dagger f_1 f_2^\dagger + f_1^\dagger f_1 f_2 - f_1 f_2^\dagger - f_1 f_2 + f_1^\dagger f_2^\dagger + f_1^\dagger f_2\big)\end{aligned}$$

$$\lambda_{CNOT} = f_1 f_1^\dagger - f_1^\dagger f_1 f_2^\dagger - f_1^\dagger f_1 f_2\,.$$

Konečná reprezentace obvodu je získána jednoduše vynásobením výrazů λ_{HX} a λ_{CNOT}. S využitím pravidel uvedených v (4.3), (4.4) a (4.5) můžeme zjednodušit na finální tvar

$$\begin{aligned}\lambda_M &= \lambda_{CNOT}\lambda_{HX}\\ &= \frac{1}{\sqrt{2}}\Big(f_1 f_1^\dagger f_2^\dagger + f_1 f_1^\dagger f_2 - f_1 f_2^\dagger - f_1 f_2 - f_1^\dagger f_1 f_2^\dagger f_2 + f_1^\dagger f_2^\dagger f_2\\ &\quad + f_1^\dagger f_1 f_2 f_2^\dagger + f_1^\dagger f_2 f_2^\dagger\Big).\end{aligned}$$

Všimněme si, že v maticové reprezentaci má finální matice 8 nenulových prvků. Výraz v GA reprezentaci má také 8 prvků. Pro ověření správnosti vypočítáme pravděpodobnosti výsledků měření pro qubity $\psi = |00\rangle$ a $\rho = |01\rangle$:

$$\begin{aligned}|\psi'\rangle = \lambda_M|\psi\rangle = \frac{1}{\sqrt{2}}\Big(&f_1 f_1^\dagger f_2^\dagger + f_1 f_1^\dagger f_2 - f_1 f_2^\dagger - f_1 f_2 - f_1^\dagger f_1 f_2^\dagger f_2 + f_1^\dagger f_2^\dagger f_2\\ &+ f_1^\dagger f_1 f_2 f_2^\dagger + f_1^\dagger f_2 f_2^\dagger\Big)\Big(f_1 f_1^\dagger f_2 f_2^\dagger\Big) = \frac{1}{\sqrt{2}}\Big(f_1 f_1^\dagger f_2^\dagger + f_1^\dagger f_2 f_2^\dagger\Big),\end{aligned}$$

$$\begin{aligned}|\rho'\rangle = \lambda_M|\rho\rangle = \frac{1}{\sqrt{2}}\Big(&f_1 f_1^\dagger f_2^\dagger + f_1 f_1^\dagger f_2 - f_1 f_2^\dagger - f_1 f_2 - f_1^\dagger f_1 f_2^\dagger f_2 + f_1^\dagger f_2^\dagger f_2\\ &+ f_1^\dagger f_1 f_2 f_2^\dagger + f_1^\dagger f_2 f_2^\dagger\Big)\Big(f_1 f_1^\dagger f_2 f_2^\dagger\Big) = \frac{1}{\sqrt{2}}\Big(f_1 f_1^\dagger f_2 f_2^\dagger + f_1^\dagger f_2^\dagger\Big).\end{aligned}$$

K výpočtu pravděpodobností jednotlivých výsledků použijeme skalární projekci. Je důležité změnit člen před skalární projekcí. Tento příklad pracuje se dvěma qubity, proto změníma na $2^n = 2^2 = 4$ a dostaneme

$$\begin{aligned}p(|00\rangle) = |\langle 00|\psi'\rangle|^2 &= \left|4\left[f_1 f_1^\dagger f_2 f_2^\dagger \frac{1}{\sqrt{2}}\big(f_1 f_1^\dagger f_2^\dagger + f_1^\dagger f_2 f_2^\dagger\big)\right]_0\right|^2\\ &= \left|\frac{4}{\sqrt{2}}\,[0]_0\right|^2 = 0,\end{aligned}$$

$$p(|01\rangle) = |\langle 00|\psi'\rangle|^2 = \left|4\left[f_1 f_1^\dagger f_2 \frac{1}{\sqrt{2}}\left(f_1 f_1^\dagger f_2^\dagger + f_1^\dagger f_2 f^\dagger 2\right)\right]_0\right|^2$$
$$= \left|\frac{4}{\sqrt{2}}\left[f_1 f_1^\dagger f_2 f_2^\dagger\right]_0\right|^2 = \left|\frac{4}{\sqrt{2}}\frac{1}{4}\right|^2 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}\,,$$

$$p(|10\rangle) = |\langle 10|\psi'\rangle|^2 = \frac{1}{2}\,,$$

$$p(|11\rangle) = |\langle 11|\psi'\rangle|^2 = 0.$$

Součet všech pravděpodobností je 1, což je správně. Nyní můžeme porovnat výsledky s těmi získanými pomocí maticové reprezentace. Všechny pravděpodobnosti jsou stejné. Pro druhý multi qubit je postup analogický a ukázány jsou pouze konečné pravděpodobnosti:

$$p(|00\rangle) = |\langle 00|\rho'\rangle|^2 = \frac{1}{2}\,, \qquad p(|01\rangle) = |\langle 01|\rho'\rangle|^2 = 0,$$
$$p(|10\rangle) = |\langle 10|\rho'\rangle|^2 = 0, \qquad p(|11\rangle) = |\langle 11|\rho'\rangle|^2 = \frac{1}{2}\,.$$

V případě druhého multi qubitu je součet pravděpodobnosti také 1. Jsou stejné jako v maticové reprezentaci, a lze tedy dospět k závěru, že reprezentace pomocí GA je ve všech směrech správná a funkční.

Je zřejmé, že s vyšším počtem vstupních qubitů se rozměr matic exponenciálně zvětšuje. Výpočet se stává velmi náročným, protože pracujeme s obrovskými maticemi. Reprezentace v GA je velmi intuitivní a umožňuje mnoho zjednodušení během výpočtu. Počet prvků reprezentujících kvantové stavy nebo kvantové brány se také zvětšuje, ale obvykle se výraz během výpočtu zjednoduší a mnoho prvků zcela vypadne. Je také třeba poznamenat, že geometrický součin některých prvků v GA je roven 0. Toto vlastnost zjednodušuje výpočet a také šetří spoustu paměti.

Největší problém s GA reprezentací je ten, že neexistuje žádný software pro přímou implementaci. GAALOPWeb nabízí některé možnosti, ale s mnoha omezeními. Při vhodné implementací lze pomocí GA realizovat QC velmi efektivně. Ekvivalence maticové a GA reprezentace také umožňuje použití vhodnější reprezentace pro konkrétní problém.

5. Shrnutí

V první kapitole se definují klíčové pojmy z algebry a jsou dány do patřičného kontextu. Obecně je popsán tenzorový součin a tenzorové prostory. Je odvozena Cliffordova algebra a diskutovány všechny její důležité vlastnosti, [6].

Druhá kapitola začíná definicí qubitu. Zdůrazněn je rozdíl mezi klasickým bitem a qubitem. Abychom mohli řešit problém s vizualizací qubitu, snížíme počet stupňů volnosti na dva a poté přepíšeme definici qubitu do sférických souřadnic. To umožní definovat tzv. Blochovu sféru, která se používá k vizualizaci různých qubitů a jejich transformací. Definice qubitu je rozšířena na multi qubity pomocí Kroneckerova součinu. V jednoduchosti je také popsáno, jak se provádí měření. Tato kapitola je založena na znalostech získaných z [2, 7, 13].

Další kapitola ukazuje, jak odvodit obecnou kvantovou bránu a jaké vlastnosti musí splňovat. Jsou definovány základní brány a demonstrován jejich účinek na konkrétní qubity. Definice brány pro jeden qubit je rozšířena na bránu pro multi qubity pomocí Kroneckerova součinu.

Hlavní část práce aplikuje znalosti a konstruuje aparát geometrické algebry (GA) vhodné pro kvantové výpočty (QC). Začínáme definicí GA nad reálnými čísly. Zvláštní pozornost je věnována geometrickému součinu, kterým je tato algebra vybavena. Tento součin hraje klíčovou roli po celou práci, a proto je pečlivě odvozen z vnitřního a vnějšího součinu. Jsou zdůrazněny důležité vlastnosti geometrického součinu. Abychom však mohli správně reprezentovat qubity v GA, musíme do naší definice zahrnout i komplexní čísla. Nastavení základního pole na komplexní čísla nestačí, protože komplexní chování musí být přeneseno přímo do algebry. Proto je představena ortogonální lineární transformace. Báze zkonstruovaná pomocí této transformace se nazývá Wittova báze a hraje velmi důležitou roli. Jsou zkoumámy důležité vlastnosti Wittovy báze pro účely dalších výpočtů. Další užitečné informace k této konstrukci GA lze nalézt v [5].

S vhodným aparátem GA můžeme přejít k definici qubitu. Klíčovým konceptem je identifikovat qubity s prvky GA. Je popsána obecná definice qubitu a poté rozšířena na multi qubity. Kvantové brány jsou také identifikovány s prvky GA, což umožňuje výpočet v rámci jedné algebraické struktury. Je prozkoumán vztah mezi maticovou a GA reprezentací. Poté je pečlivě odvozena forma kvantových bran zapsaných v GA. Je ukázán univerzální způsob, jak sestavit libovolnou bránu pro multi qubity. Stručně diskutujeme také to, jak provádět měření v GA.

Povedlo se sestavit aparát GA, který umožňuje intuitivní a přímočarý výpočet. Všechny získané výsledky potvrdily správnost tohoto přístupu. Elegantní definice báze umožňuje mnoho zjednodušení během výpočtu, což ho dělá rychlejším a potenciálně i méně náročným na pamět. Maticová reprezentace má problém se zvyšujícím se rozměrem matic. Tento růst je exponenciální a i pro malý počet qubitů může být výpočet velmi náročný. Rozměr výrazů reprezentujících kvantové brány v GA také roste, ale není tak dramatický a často se dá zjednodušit. Největším problémem je samotná implementace GA. Komplexní čísla jsou obtížně reprezentovatelná a v současné době neexistuje žádný software vhodný pro výpočty v GA. GAALOPWeb nabízí alternativu, ale pracuje s GA nad reálnými čísly a používá trochu odlišný přístup.

Reference

[1] M. E. Browne: *Schaum's outlines physics for engineering and science*, McGraw-Hill, New York, 2010.

[2] F. De Lima Marquezino, et al.: *A primer on quantum computing*, SpringerBriefs in Computer Science, 2019.

[3] L. Dorst, D. H. F. Fontijne, S. Mann: *Geometric algebra for computer science: an object-oriented approach to geometry*, Morgan Kaufmann Publishers, 2007.

[4] D. Hildenbrand: *Introduction to geometric algebra computing*, Chapman and Hall/CRC, 2018.

[5] J. Hrdina, A. Návrat. P.Vašík: *Quantum computing based on complex Clifford algebras*, 2022, online https://doi.org/10.1007/s1128-022-03648-w.

[6] M. S. Lane, G. Birkhoff: *Algebra*, American Mathematical Society, Providence, 1999.
[7] M. A. Nielsen, I. L. CHUANG: *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2010.
[8] C. Perwass: *Geometric algebra with applications in engineering*, Springer, 2009.
[9] L. Procházka: *Inverzní kinematika robotického ramene s předepsanou trajektorií efektoru pomocí geometrické algebry*, Bakalářská práce, Vysoké učení technické v Brně, Fakulta strojního inženýrství, Brno, 2022.
[10] E. M. Purcell, D. Morin: *Electricity and magnetism*, Cambridge University Press, Cambridge, 2018.
[11] Open-source quantum development, online https://qiskit.org/, accessed Apr 28, 2023.
[12] J. Rue, S. Xambo: *Mathematical essentials of quantum computing*, Lecture notes UPC, online https://web.mat.upc.edu/sebastia.xambo/QC/qc.pdf.
[13] *Theory of computing*, ACM Press, New York, 1993.

Jan Michálek, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: 228579@vutbr.cz