# Jeszcze o algebrze obliczeń kwantowych,

## czyli artykuł dla Koneserów Macierzy

*Maciej ZDANOWICZ**

*Instytut Matematyki, Wydział Matematyki, Informatyki i Mechaniki, Uniwersytet Warszawski

W poniższym artykule postaramy się przybliżyć Czytelnikowi niektóre podstawowe pojęcia algebry wieloliniowej nad liczbami zespolonymi, która jest podstawą rozważań w kwantowej teorii obliczeń. Bez zbędnej zwłoki przystąpimy od razu do konkretów.

**Stany i bramki kwantowe.** Stanem komputera kwantowego obsługującego $n$ tak zwanych kubitów jest jakiś wektor długości 1 z $\mathbb{C}^{2^n}$. Wykorzystując bardzo sugestywną notację Paula Diraca stan $s$ w takim komputerze może być zapisany w postaci

$$s = \sum_{(b_1 \ldots b_n) \in \{0,1\}^n} s_{b_1,\ldots,b_n} \cdot |b_1 \ldots b_n\rangle, \qquad \text{dla} \quad s_{b_1,\ldots,b_n} \in \mathbb{C}.$$

Intuicyjnie, możemy sobie więc wyobrażać, że pamięć komputera jest niedeterministyczna i znajduje się w stanie $(b_1 \ldots b_n)$ z prawdopodobieństwem $|s_{b_1,\ldots,b_n}|^2$. Warto zwrócić uwagę, że przy tej uproszczonej interpretacji pomijamy istotną informację pochodzącą od zespolonego *skierowania* współrzędnych stanu $s$.

Zespolona ściągawka:
$|a+bi| = \sqrt{a^2+b^2}$,
długość $\|c\|$ wektora $c = (c_1, \ldots, c_n)$ wynosi $\sqrt{|c_1|^2 + \ldots |c_n|^2}$,
$\overline{a+bi} = a - bi$.

Przystąpimy teraz do krótkiej analizy dostępnych operacji na komputerze kwantowym, które odpowiadają odwracalnym operatorom $M$ zachowującym długości wektorów (czyli dla każdego $\phi$ ma być $\|M\phi\| = \|\phi\|$). Operacje te nazywamy *operatorami unitarnymi.* Dla liczby naturalnej $N$ przez $U(N)$ oznaczać będziemy grupę przekształceń unitarnych przestrzeni $\mathbb{C}^N$. Jak łatwo się przekonać (zachęcamy do próby udowodnienia tego faktu) grupa ta może być utożsamiona ze zbiorem macierzy $U$ rozmiaru $N \times N$ spełniających równość $U \cdot U^\dagger = I_N$, gdzie $I_N$ jest macierzą przekształcenia identycznościowego, a operacja $U \mapsto U^\dagger$ przyporządkowuje macierzy $[u_{ij}]$ macierz $[\overline{u_{ji}}]$, np:

$$\frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}^\dagger = \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} \quad \text{oraz} \quad \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1-i & 1+i \\ 1+i & 1-i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

**Iloczyn tensorowy.** W celu zwięzłego zapisu bramek kwantowych dużych rozmiarów wykorzystuje się operację tak zwanego iloczynu tensorowego. *Iloczynem tensorowym* przestrzeni wektorowych $V$ i $W$, oznaczanym $V \otimes W$, nazwiemy przestrzeń generowaną przez elementy $v \otimes w$, dla $v \in V$ i $w \in W$, spełniające liniowe zależności

$$(av + bv') \otimes w = av \otimes w + bv' \otimes w$$
$$v \otimes (aw + bw') = av \otimes w + bv \otimes w'$$

dla $v' \in V$, $w' \in W$ i $a, b \in \mathbb{C}$. Można wykazać, że dla ustalonych baz $v_1, \ldots, v_n$ i $w_1, \ldots, w_m$ bazą przestrzeni $V \otimes W$ są elementy $v_i \otimes w_j$.

Powyższe zależności oznaczają, że $\mathbb{C}^{2^n} \otimes \mathbb{C}^{2^m}$ może być utożsamione z przestrzenią $\mathbb{C}^{2^{n+m}}$ za pomocą przyporządkowania określonego w bazach Diraca przy użyciu formuły $|b_1 \ldots b_n\rangle \otimes |b'_1 \ldots b'_n\rangle \mapsto |b_1 \ldots b_n b'_1 \ldots b'_m\rangle$.

Operacja iloczynu tensorowego może być również wykonana na operatorach $\phi\colon V \to V$ i $\xi\colon W \to W$. Jest ona oznaczana przez $\phi \otimes \xi$ i zdefiniowana za pomocą formuły

$$(\phi \otimes \xi)(v \otimes w) = \phi(v) \otimes \xi(w).$$

Intuicyjnie, każdy z operatorów w iloczynie tensorowym działa „niezależnie" na mniejszym podzbiorze współrzędnych.

Okazuje się (ponownie zachęcamy do próby samodzielnego udowodnienia tego faktu), że jeżeli $\phi$ i $\xi$ zadane są odpowiednio przez macierze $A = [a_{ij}]$ oraz $B = [b_{km}]$ to $\phi \otimes \xi$ zadane jest przez macierz $A \otimes B$ zdefiniowaną następująco:

$$A \otimes B = \begin{bmatrix} a_{11}\begin{bmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{bmatrix} & \ldots & a_{1n}\begin{bmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{bmatrix} \\ \vdots & \ddots & \vdots \\ a_{n1}\begin{bmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{bmatrix} & \ldots & a_{nn}\begin{bmatrix} b_{11} & \ldots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{nn} \end{bmatrix} \end{bmatrix}.$$

Na przykład:

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$