



Kvantumalgoritmusok

Dr. Hannusch Carolin
hannusch.carolin@inf.unideb.hu

2026

- 1 Matematikai alapok I (Számelméleti alapok, algebrai alapismeretek, komplex számok, mátrix- és vektorszámítás, Dirac féle jelölés, vektortér)
- 2 Matematikai alapok II (Lineáris leképezések, belső szorzat, tenzor szorzat, operátorok)
- 3 Kvantum információ reprezentálása. Klasszikus állapotok, valószínűségi állapotok, kvantum állapotok. Determinisztikus és probabilisztikus algoritmusok, qubit operátorok
- 4 Kvantum áramkörök, ortogonális állapotok. Teleportáció és IBM Qiskit implementáció
- 5 Kvantum algoritmusok és kvantum komplexitás, Deutsch algoritmus, Deutsch-Józsa áramkör, Deutsch-Józsa algoritmus
- 6 Boole kapuk szimulációja, Boole áramkörök szimulációja

- 7 Simon algoritmus
- 8 Shor algoritmusai I (Faktorizálás, Kvantum Fourier transzformáció)
- 9 Shor algoritmusai II (Kvantum rendezés, kvantum diszkrét logaritmus algoritmus)
- 10 Kvantum keresés, kvantum számolás
- 11 HHL algoritmus, kvantum Fourier transzformáció
- 12 Kitekintés: Kvantum hibajavítás and kriptográfia
- 13 Kitekintés: Business and Machine Learning

- BUCHMANN, Johannes. Introduction to Quantum Algorithms. American Mathematical Society, 2024.
- IBM Quantum platform, Qiskit documentation:
<https://quantum.cloud.ibm.com/>
- REDDY, C. Kishor Kumar, et al. The Rise of Quantum Computing in Industry 6.0 Towards Sustainability. Springer Nature, 2024.
- LANDSBERG, Joseph M. Quantum Computation and Quantum Information: A Mathematical Perspective. American Mathematical Society, 2024.

Matematikai alapok I

Számelméleti alapismeretek

- $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
- $\mathbb{Z}_k = \{0, \dots, k-1\}$
- Legnagyobb közös osztó, relatív prím
- mod
- prímfaktorizáció (számelmélet alaptétele: minden szám felbontható egyértelműen prímszámok szorzatára)

Algebrai alapismeretek

- Halmazok, Descartes szorzat
- Polinomok (algebra alaptétele: $\mathbb{C}$ algebrailag zárt)
- csoport, gyűrű, test

Vektortér egy számtest felett: általában $\mathbb{R}$ vagy $\mathbb{C}$ felett

- 1 Két vektor összeadása is értelmezett.
- 2 Egy vektor skalárral (testbeli elemmel való) szorzata is értelmezett.

Vektorok, mátrixok

Egy $m \times n$ típusú mátrixnak van m sora és n oszlopa. Egy vektor egy $1 \times n$ mátrix.

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & & & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix}$$

Úgy is jelöljük: $A = (a_{i,j})$

Sorvektor:

$$v = (v_1, \dots, v_n)$$

Oszlopvektor:

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Transzponálás: Sorok $\leftrightarrow$ Oszlopok

Összeadás: Ugyanolyan típusú mátrixokat lehet összeadni, elemenként adunk össze, azaz

$$A + B = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ \vdots & & & \\ a_{m,1} & a_{m,2} & \dots & a_{m,n} \end{pmatrix} + \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ \vdots & & & \\ b_{m,1} & b_{m,2} & \dots & b_{m,n} \end{pmatrix} =$$
$$\begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} & \dots & a_{1,n} + b_{1,n} \\ \vdots & & & \\ a_{m,1} + b_{m,1} & a_{m,2} + b_{m,2} & \dots & a_{m,n} + b_{m,n} \end{pmatrix}$$

Szorzás: $m \times k$ típusú és $k \times n$ típusú mátrixot lehet szorozni, az eredmény egy $m \times n$ típusú mátrix

$$A \cdot B = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,k} \\ \vdots & & & \\ a_{m,1} & a_{m,2} & \dots & a_{m,k} \end{pmatrix} \cdot \begin{pmatrix} b_{1,1} & b_{1,2} & \dots & b_{1,n} \\ \vdots & & & \\ b_{k,1} & b_{k,2} & \dots & b_{k,n} \end{pmatrix} =$$
$$\begin{pmatrix} a_{1,1} \cdot b_{1,1} + a_{1,2} \cdot b_{2,1} + \dots + a_{1,n} \cdot b_{k,1} & \dots \\ \vdots & \\ a_{m,1} \cdot b_{1,1} + a_{m,2} \cdot b_{2,1} + \dots + a_{m,n} \cdot b_{k,1} & \dots \end{pmatrix}$$

Tulajdonságok

- Az összeadás kommutatív: $A + B = B + A$
- A szorzás nem kommutatív: $A \cdot B \neq B \cdot A$ általában
- négyzetes mátrix: ugyanannyi sora van mint oszlopa
- I_n -nel jelöljük az n -dimenziós egységmátrixot:

$$I_n = \begin{pmatrix} 1 & \dots & 0 \\ 0 & 1 & \dots \\ \vdots & & \\ 0 & \dots & 1 \end{pmatrix}$$

- Ha $A^{-1}A = AA^{-1} = I$, akkor A^{-1} az A mátrix inverze.

Kérdések és feladatok

- ① Asszociatív az összeadás a mátrixok körében?
- ② A szorzás?
- ③ Disztributív?

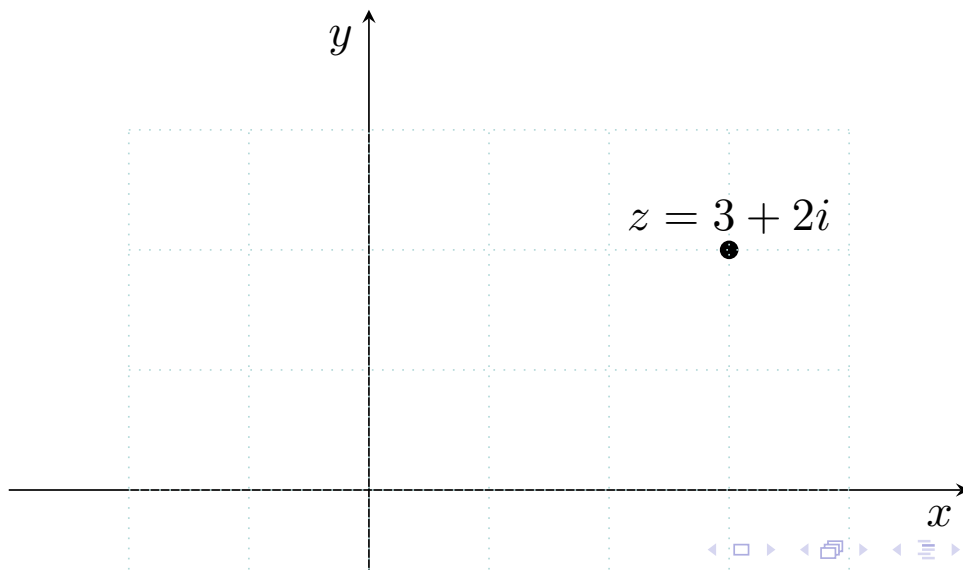
Komplex számok

$$\mathbb{R}^2 = \mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}$$

$$i^2 = -1$$

Legyen $z = x + yi$. Ekkor x a valós rész, jelölés $Re(z) = x$ és y a képzetes rész, jelölés $Im(z) = y$.

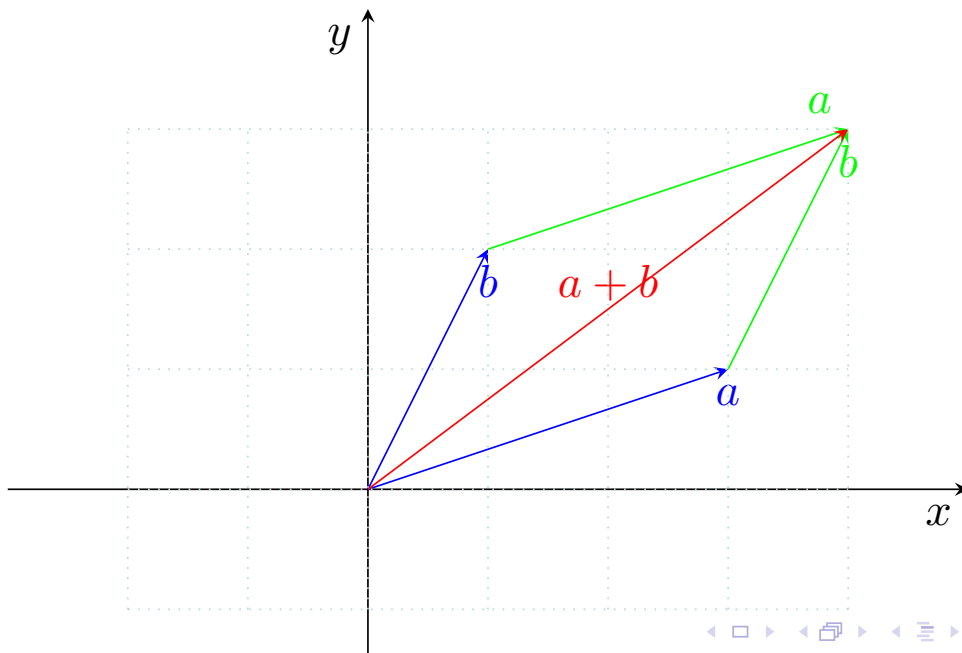
Ábrázolása



Aritmetika

- $(a + bi) + (c + di) = (a + c) + (b + d)i$
- $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$
- Ha $z = a + bi$, akkor z konjugáltja $\bar{z} = a - bi$
- Ha $z = a + bi$ akkor z abszolút értéke $|z| = \sqrt{a^2 + b^2}$

Geometriai összeadás



Feladatok I

- ➊ Rajzoljuk le az S halmazt derékszögű koordinátarendszerben!
 - ➊ $S = \{z \in \mathbb{C} \mid 0 \leq \operatorname{Im}(z) \leq 5\}$
 - ➋ $S = \{z \in \mathbb{C} \mid 0 \leq \operatorname{Im}(z) \leq 5, -1 \leq \operatorname{Re}(z) \leq 3\}$
 - ➌ $S = \{z \in \mathbb{C} \mid \operatorname{Im}(z)^2 + \operatorname{Re}(z)^2 \leq 1\}$
- ➋ Legyen $z_1 = 3 + 4i, z_2 = -5 - i, z_3 = 6 + i, z_4 = -2 + 2i$.
 - ➊ Számoljuk ki a $z_1 + z_2, z_2 - z_3, z_2 z_3 z_4, z_1 z_4$ számokat!
 - ➋ Mennyi z_1 abszolút értéke?
 - ➌ Melyik komplex szám z_4 konjugáltja?
- ➌ Ugyanannyi $z_1 z_2$ mint $z_2 z_1$? Ez mindig így van?

Feladatok II

① Legyen $A = \begin{pmatrix} 1 & 2 & 3 \\ -2 & 0 & 2 \\ 6 & 4 & -1 \end{pmatrix}$, $B = \begin{pmatrix} 8 & -2 & 1 & 2 \\ -2 & 5 & 0 & -3 \\ 1 & 1 & -1 & 1 \end{pmatrix}$, és

$$C = \begin{pmatrix} 3 & 2 & 1 \\ -2 & 1 & 1 \\ 3 & 4 & -1 \end{pmatrix}.$$

- ① Milyen összegeket lehet képezni ezekből a mátrixokból?
- ② Számoljuk ki az $A \cdot B$, $B \cdot A$, $A \cdot C$ és $C \cdot A$ mátrixot!

② Legyen $M = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 0 & 2 \\ 4 & 3 & -1 \end{pmatrix}$ és $v = (1, 2, 3)$.

- ① Milyen szorzatot lehet az M mátrixból és a v vektorból képezni?
- ② Írjuk fel M^T -t és v^T -t!

Legyen X egy esemény. Annak a valószínűsége, hogy az X esemény bekövetkezik, legyen p . Jelölés:

$$P(X) = p.$$

Példák

- Jelölje X egy szabályos éremmel való dobást. Ekkor $P(X = \text{fej}) = 0,5$.
- Jelölje X egy szabályos dobókockával való dobást. Ekkor $P(X = 6) = \frac{1}{6}$.

Állapotok

Tegyük fel, hogy X véges számú állapotban lehet egy adott időpontban. Ekkor az állapotok halmazát Σ -val jelöljük.

Példák

- ❶ X egy bit, akkor $\Sigma = \{0, 1\}$.
- ❷ X egy szabályos érme, akkor $\Sigma = \{\text{fej}, \text{írás}\}$.
- ❸ X egy fényfűzér, akkor $\Sigma = \{\text{ki}, \text{be}, \text{villogó}\}$.
- ❹ X egy szabályos kocka, akkor $\Sigma = \{1, 2, 3, 4, 5, 6\}$.

Dirac féle jelölés

Legyen Σ egy állapothalmaz. Ekkor jelöljük $|\alpha\rangle$ -val azt az oszlopvektort, melynek 1 van azon a helyen, amely $\alpha \in \Sigma$ -hoz tartozik. Tehát ha pl. $\Sigma = \{0, 1\}$, akkor

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \text{ és } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Példa: Legyen $\Sigma = \{\nabla, \triangle, \square\}$ és a következő rendezést használjuk $\nabla, \triangle, \square$.

Ekkor

$$|\nabla\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |\triangle\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \text{ és } |\square\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$