Procesamiento Cuántico de Información

Ariel Bendersky¹

¹Departamento de Computación - FCEyN - Universidad de Buenos Aires

Burocracia

- Las clases van a ser grabadas a menos que alguien se oponga en este momento.
- Criterio de aprobación:
 - Un TP (licenciatura y doctorado).
 - Un seminario sobre el TP. Para doctorado, leer y contar algún trabajo que relacione lo visto con el tema de doctorado, dentro de lo posible.
- Criterio de promoción: Nota superior a 7 (la nota es una sola del TP y seminario).

- Formalismo.
- Algoritmos cuánticos y aplicaciones.
- No localidad.
- Artistas exclusivxs.
- Lo que ustedes manifiesten interés (dentro de lo posible y si queda tiempo).

- Formalismo.
- Algoritmos cuánticos y aplicaciones.
- No localidad.
- Artistas exclusivxs.
- Lo que ustedes manifiesten interés (dentro de lo posible y si queda tiempo).

- Formalismo.
- Algoritmos cuánticos y aplicaciones.
- No localidad.
- Artistas exclusivxs.
- Lo que ustedes manifiesten interés (dentro de lo posible y si queda tiempo).

- Formalismo.
- Algoritmos cuánticos y aplicaciones.
- No localidad.
- Artistas exclusivxs.
- Lo que ustedes manifiesten interés (dentro de lo posible y si queda tiempo).

- Formalismo.
- Algoritmos cuánticos y aplicaciones.
- No localidad.
- Artistas exclusivxs.
- Lo que ustedes manifiesten interés (dentro de lo posible y si queda tiempo).

Clase 1

Temas:

• Un poco de fenomenología e historia.

Objetivo:

- Causar confusión.
- Reconocer que el mundo cuántico es un lugar extraño, y que puede servir para procesamiento de información.

Historia

Historia

Hitos



1982 - Richard Feynman se da cuenta de que una computadora clásica es muy ineficiente para simular sistemas cuánticos. Propone usar sistemas cuánticos para simular otros sistemas cuánticos.

Hitos



1985 - David Deutsch define las máquinas de Turing cuánticas. Eso le da un marco teórico a la computación cuántica como la conocemos hasta hoy.

¿Para qué sirve?



Hitos



1994 - Peter Shor descubre un algoritmo cuántico eficiente para factorizar números naturales. Eso rompe los sistemas de criptografía más utilizados.

Un viaje al pasado. Breve historia de la luz.

- Siglo XVII. Newton propone la teoría corpuscular de la luz.
- Siglo XVII. Huygens propone la teoría ondulatoria de la luz.
- Siglo XIX. Young demuestra la naturaleza ondulatoria de la luz.
- Siglo XIX. Maxwell le da un marco teórico a la teoría ondulatoria.
- Siglo XX. Nace la cuántica. Vuelven los corpúsculos. Las ondas no se van.

Experimentos con pelotitas y un poco de interferencia

Pizarra

Fenomenología

Cada electrón sabe que hay varias puertas.

Más situaciones extrañas en el mundo cuántico

Experimentos de Stern-Gerlach. Ver pizarra.

- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de M sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0.$
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.



- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \dot{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0.$
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.



- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \vec{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0$.
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.



- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \vec{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0$.
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.

- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \vec{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0$.
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.

- Un electrón es un pequeño imán de momento magnético M.
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0), \ \hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \vec{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0$.
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.

- Un electrón es un pequeño imán de momento magnético \vec{M} .
- El experimento de Stern-Gerlach muestra que la proyección de \vec{M} en cualquier dirección es $\pm \frac{\hbar}{2}$.
- Consideremos las direcciones dadas por $\hat{n}_1 = (1, 0, 0)$, $\hat{n}_2 = (-1/2, \sqrt{3}/2, 0)$, $\hat{n}_3 = (-1/2, -\sqrt{3}/2, 0)$
- Quiero medir la suma de las proyecciones de \vec{M} sobre esos tres versores:
 - $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \pm \frac{\hbar}{2} \neq 0$.
 - Pero $\vec{M} \cdot \hat{n}_1 + \vec{M} \cdot \hat{n}_2 + \vec{M} \cdot \hat{n}_3 = \vec{M} \cdot (\hat{n}_1 + \hat{n}_2 + \hat{n}_3) = 0$
 - Absurdo.

¿Qué nos dice esto?

Medir es mucho más que revelar un valor predeterminado. La medición, de alguna manera, genera el resultado que muestra. El proceso de medición es una característica muy particular del mundo cuántico.

Siguen las cosas extrañas

No localidad

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Ley de Betteridge: Todo título que termina con un signo de pregunta puede responderse con la palabra no.
- Conclusión: "While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."
- Traducción: Cuánticos, dejen de chamuyar y construyan una teoría razonable.

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Ley de Betteridge: Todo título que termina con un signo de pregunta puede responderse con la palabra no.
- Conclusión: "While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."
- Traducción: Cuánticos, dejen de chamuyar y construyan una teoría razonable.

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Ley de Betteridge: Todo título que termina con un signo de pregunta puede responderse con la palabra no.
- Conclusión: "While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."
- Traducción: Cuánticos, dejen de chamuyar y construyan una teoría razonable.

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Ley de Betteridge: Todo título que termina con un signo de pregunta puede responderse con la palabra no.
- Conclusión: "While we have thus shown that the wave function does not provide a complete description of the physical reality, we left open the question of whether or not such a description exists. We believe, however, that such a theory is possible."
- Traducción: Cuánticos, dejen de chamuyar y construyan una teoría razonable.

Bohr (1935)

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Del abstract: It is shown that a certain "criterion of physical reality" formulated in a recent article with the above title by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena.
- Traducción: ¿Chamuyo? Mirá quién habla.

Bohr (1935)

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Del abstract: It is shown that a certain "criterion of physical reality" formulated in a recent article with the above title by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena.
- Traducción: ¿Chamuyo? Mirá quién habla.

Bohr (1935)

- Título: Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
- Del abstract: It is shown that a certain "criterion of physical reality" formulated in a recent article with the above title by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena.
- Traducción: ¿Chamuyo? Mirá quién habla.

29 años de discusión pero pocos argumentos después...

- Título: On the Einstein-Podoslky-Rosen paradox
- Resumen: ¡Bohr! ¡Einstein! ¡No discutan! Se me ocurre una manera de distinguir experimentalmente quién tiene razón.
- Nacen las desigualdades de Bell para determinar si la naturaleza es local o no local.

29 años de discusión pero pocos argumentos después...

- Título: On the Einstein-Podoslky-Rosen paradox
- Resumen: ¡Bohr! ¡Einstein! ¡No discutan! Se me ocurre una manera de distinguir experimentalmente quién tiene razón.
- Nacen las desigualdades de Bell para determinar si la naturaleza es local o no local.

29 años de discusión pero pocos argumentos después...

- Título: On the Einstein-Podoslky-Rosen paradox
- Resumen: ¡Bohr! ¡Einstein! ¡No discutan! Se me ocurre una manera de distinguir experimentalmente quién tiene razón.
- Nacen las desigualdades de Bell para determinar si la naturaleza es local o no local.

29 años de discusión pero pocos argumentos después...

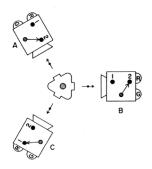
- Título: On the Einstein-Podoslky-Rosen paradox
- Resumen: ¡Bohr! ¡Einstein! ¡No discutan! Se me ocurre una manera de distinguir experimentalmente quién tiene razón.
- Nacen las desigualdades de Bell para determinar si la naturaleza es local o no local.

Un poco de historia

- 1982 Aspect, Dalibard y Roger hacen el primer experimento y muestran que la naturaleza es no local. Pero el experimento tiene algunos errores (loopholes).
- 24 de Agosto de 2015 B. Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson. Primer experimento loophole-free (?).

Un poco de historia

- 1982 Aspect, Dalibard y Roger hacen el primer experimento y muestran que la naturaleza es no local. Pero el experimento tiene algunos errores (loopholes).
- 24 de Agosto de 2015 B. Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D.J. Twitchen, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson. Primer experimento loophole-free (?).



- Si sólo un detector está en 1, siempre hay un número impar de luces rojas.
- Si los tres detectores están en 1, nunca se observa un número impar de luces rojas.



Se puede pensar cada partícula como instrucciones sobre qué debe hacer el detector en cada caso.

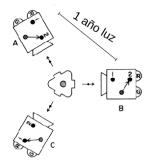
$$\begin{pmatrix} RGR \\ GGG \end{pmatrix}$$

Enumerando todas las posibilidades se ve que esas dos reglas no se pueden cumplir nunca.

- Si las tres partículas están en un estado cuántico particular, y los detectores miden ciertas propiedades cuánticas de las partículas, sí se puede construir esa máquina.
- Qué raro... o no tanto. Si los detectores pudieran hablarse entre ellos no habría nada sorprendente (si cada detector sabe qué midieron los otros).
- Evitemos que se hablen, aunque no sepamos muy bien qué mecanismo usa la naturaleza para que se hablen.

- Si las tres partículas están en un estado cuántico particular, y los detectores miden ciertas propiedades cuánticas de las partículas, sí se puede construir esa máquina.
- Qué raro... o no tanto. Si los detectores pudieran hablarse entre ellos no habría nada sorprendente (si cada detector sabe qué midieron los otros).
- Evitemos que se hablen, aunque no sepamos muy bien qué mecanismo usa la naturaleza para que se hablen.

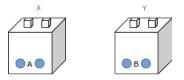
- Si las tres partículas están en un estado cuántico particular, y los detectores miden ciertas propiedades cuánticas de las partículas, sí se puede construir esa máquina.
- Qué raro... o no tanto. Si los detectores pudieran hablarse entre ellos no habría nada sorprendente (si cada detector sabe qué midieron los otros).
- Evitemos que se hablen, aunque no sepamos muy bien qué mecanismo usa la naturaleza para que se hablen.



La decisión de qué medir se toma a último minuto.

Sigue ocurriendo lo mismo. Los detectores parecen saber lo que pasó en los otros detectores: La mecánica cuántica es *no local*. Y se puede probar experimentalmente si la naturaleza se comporta así o no.

CHSH - Clauser, Horne, Shimony, Holt (1969)



Después de muchos experimentos miramos P(AB|XY). Toda teoría local obedece:

$$|E(00) + E(01) + E(10) - E(11)| \le 2$$

con E(ij) = P(00|ij) + P(11|ij) - P(01|ij) - P(10|ij) La cuántica permite llegar a $2\sqrt{2}$. Otra prueba de que es no local.

Localidad

P(AB|XY) es local si y sólo si puede escribirse como:

$$P(AB|XY) = \sum_{\lambda} \rho_{\lambda} P_{a}^{\lambda}(A|X) P_{b}^{\lambda}(B|Y)$$

Físicamente quiere decir que Alice y Bob comparten un dado (tienen un dado que cada vez que lo tiran les da el mismo resultado a ambos), y después hacen cosas locales.

No localidad

Si no se puede escribir así, es no local. Equivalentemente, es no local si viola una desigualdad de Bell.

Localidad

P(AB|XY) es local si y sólo si puede escribirse como:

$$P(AB|XY) = \sum_{\lambda} \rho_{\lambda} P_{a}^{\lambda}(A|X) P_{b}^{\lambda}(B|Y)$$

Físicamente quiere decir que Alice y Bob comparten un dado (tienen un dado que cada vez que lo tiran les da el mismo resultado a ambos), y después hacen cosas locales.

No localidad

Si no se puede escribir así, es no local. Equivalentemente, es no local si viola una desigualdad de Bell.

No señalización

Una distribución es no señalizante (Non signaling) si no sirve para transmitir información de manera instantánea.

Para eso, los marginales deben ser independientes de la otra parte (lo que hace Alice no afecta la estadística de Bob y viceversa).

$$\sum_{a} P(aB|0Y) = \sum_{a} P(aB|1Y)$$

$$\sum_b P(Ab|X0) = \sum_b P(Ab|X1)$$

No son lo mismo

Localidad ⇒ No señalización No señalización ⇒ Localidad

Einstein duerme en paz

Hay distribuciones que no son locales pero tampoco señalizan. La cuántica admite algunas de esas distribuciones de probabilidad multipartitas, pero no admite señalización.

La no localidad es más barata que la comunicación

Con comunicación se puede simular no localidad. Con no localidad no se puede simular comunicación.

No son lo mismo

Localidad ⇒ No señalización No señalización ⇒ Localidad

Einstein duerme en paz

Hay distribuciones que no son locales pero tampoco señalizan. La cuántica admite algunas de esas distribuciones de probabilidad multipartitas, pero no admite señalización.

La no localidad es más barata que la comunicación

Con comunicación se puede simular no localidad. Con no localidad no se puede simular comunicación.

No son lo mismo

Localidad ⇒ No señalización No señalización ⇒ Localidad

Einstein duerme en paz

Hay distribuciones que no son locales pero tampoco señalizan. La cuántica admite algunas de esas distribuciones de probabilidad multipartitas, pero no admite señalización.

La no localidad es más barata que la comunicación

Con comunicación se puede simular no localidad. Con no localidad no se puede simular comunicación.

Usos

Distribución de claves

Distribución de claves

Las cajas de CHSH pueden usarse para hacer distribución de claves aleatorias (Alice y Bob reciben claves aleatorias pero iguales).

Criptografía

Eso les permite hacer criptografía intrínsecamente segura.

Es device independent

No depende de la mecánica cuántica, sólo de la no localidad. Si descubrimos que la naturaleza no era cuántica pero sí era no local, esto sigue funcionando.

Distribución de claves

Distribución de claves

Las cajas de CHSH pueden usarse para hacer distribución de claves aleatorias (Alice y Bob reciben claves aleatorias pero iguales).

Criptografía

Eso les permite hacer criptografía intrínsecamente segura.

Es device independent

No depende de la mecánica cuántica, sólo de la no localidad. Si descubrimos que la naturaleza no era cuántica pero sí era no local, esto sigue funcionando.

Distribución de claves

Distribución de claves

Las cajas de CHSH pueden usarse para hacer distribución de claves aleatorias (Alice y Bob reciben claves aleatorias pero iguales).

Criptografía

Eso les permite hacer criptografía intrínsecamente segura.

Es device independent

No depende de la mecánica cuántica, sólo de la no localidad. Si descubrimos que la naturaleza no era cuántica pero sí era no local, esto sigue funcionando.

Communication complexity

El problema

Quiero calcular una función f(A, B) con A y B n-uplas binarias. Alice tiene A y Bob tiene B. ; Cuanta información tiene que envíar Alice a Bob para que calcule f?

La no localidad cuántica ayuda en algunos casos.

Communication complexity

El problema

Quiero calcular una función f(A, B) con A y B n-uplas binarias. Alice tiene A y Bob tiene B. ¿Cuanta información tiene que envíar Alice a Bob para que calcule f?

No localidad

La no localidad cuántica ayuda en algunos casos.

Listo por hoy

Hoy vimos:

- El mundo cuántico es un lugar extraño.
- Los objetos cuánticos están en más de un lugar a la vez (superposición).
- Medir no es revelar un valor preestablecido.
- Hay correlaciones no locales que sirven para muchas tareas.

Tarea para el hogar

Los ejercicios que voy a dar no son requisito de aprobación ni se entregan. No son muchos, ni van a ser en todas las clases, pero si no los hacen se les va a hacer muy cuesta arriba seguir la materia.

Tarea para el hogar

Repasar:

 Matrices complejas. Matrices hermíticas (o hermitianas), matrices unitarias. Autovalores y autovectores. Producto tensorial.

Ejercicio:

• Considere las matrices de Pauli definidas por:

$$\sigma_{\mathsf{x}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_{\mathsf{y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_{\mathsf{z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

- Encuentre los autovalores y autovectores de cada una.
- Sea $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. Encuentre los autovalores y autovectores de $\vec{\sigma} \cdot \hat{n}$ para \hat{n} un versor genérico. (Notar que $\vec{\sigma} \cdot \hat{n} = n_x \sigma_x + n_y \sigma_y + n_z \sigma_z$).