양자 컴퓨팅 및 정보의 기초 (M1522.002500)

- Lecturer: 김태현 (taehyun@snu.ac.kr, 301-407)
- 강의 조교 (TA)
  - 전형준 (ijshj10@gmail.com, 301-416)
  - 정다운 (realacornzet@gmail.com, 301-451-1)
- 일정
  - 수업 시간: 월, 수 5~6:15pm / 302-509 (온라인 수업 기간에는 사전에 동영상을 촬영해서 올리고, 가끔씩 정규 수업 시간을 zoom을 통한 Q&A 세션으로 활용할 예정임. Q&A 세션은 매번 정규 시간에 있는 것이 아니라, 일주일에 한번 정도 0.5~1시간 정도 진행할 예정이고, 실제 진행하는 시간은 별도로 공지할 예정임)
  - Office hour: 수요일 7~8pm / 301-407 (온라인 수업 기간에는 zoom 을 활용해서 온라인으로 면담 가능하니, 사전에 예약을 해주기 바람.)
- 교재
  - 주교재: "Quantum computation and quantum information", Michael A. Nielsen & Isaac L. Chuang, Cambridge University Press (2010)
  - 부교재: "Principles of Quantum Mechanics", Ramamurti Shankar, 2nd ed. Plenum Press (1994)
- Course homepage: ETL
- 성적
  - 중간고사 2회 (각 25%) , 기말고사 1회 (30%) , 과제 10%, 출석 5%, 태도 5% (공식적인 사유로 출석이 불가능할 경우에는 정다운 학생(TA)에게 사유서를 제출하기 바랍니다.)
  - 대학원생은 학부생과는 별도의 기준으로 학점을 부여할 예정임.
  - 대학원생은 일반 과제 및 시험 이외에 이 분야의 대표적인 논문 1~2개를 요약한 review term paper (3~4장 분량)를 제출해야 하고, 별도의 시간을 정해 따로 발표하는 시간을 가질 예정임. 이 경우 중간 고사의 비중은 각 20%씩이고, term paper 및 발표가 10%를 차지할 예정임.

강의 Scripting 작업 지원자 모집

- 이번 학기 전체 강의는 동영상 녹화 후 다음 학기에 SNUON에 올라갈 예정임
- 매번 강의 후, 녹화된 동영상을 보면서 강의 내용을 typing할 지원자 모집 (해당 강의 녹화 후 약 3주 이내)
- 한 학생이 여러 강의를 입력하는 것을 지원해도 되고, 한 학생이 1 강의만 입력해도 됨.
- 말로 한 것과 칠판에 적은 수식 등도 같이 입력해야 되나, 해당 강의 자료 powerpoint파일을 제공할 예정이므로 수식 입력에 대한 큰 부담은 없을 것으로 예상됨
- 혜택
  - 학기말에 한 강의 (최대 75분)당 8만원의 수당 지급 예정
  - 한 강의 입력당 1회 결석을 상쇄해 줄 예정임

Tentative schedule for the class

- [Week 1] Review of linear algebra
- [Week 2] Review of linear algebra
- [Week 3] Introduction to quantum mechanics
- [Week 4] Summary of computer science and quantum circuits
- [Week 5] Quantum circuits, 1st mid-term exam
- [Week 6] Quantum algorithms
- [Week 7] Quantum algorithms
- [Week 8] Quantum programming language
- [Week 9] Quantum cryptography, 2nd mid-term exam
- [Week 10] Advanced quantum theory - POVM, Density matrix, Partial trace, etc.
- [Week 11] Review of computation and information theory
- [Week 12] Quantum error correction code
- [Week 13] Final exam
- [Week 14] Physical implementation of quantum information processing
- [Week 15] Physical implementation of quantum information processing

Linear Vector Spaces

- **Definition 1**: A ***linear vector space*** V is a collection of objects $|1\rangle, |2\rangle, \ldots, |V\rangle, \ldots |W\rangle, \ldots$ called vectors, for which the following two operations are well-defined:
  1. Vector addition: $|V\rangle + |W\rangle$
  2. Multiplication by scalars $a, b, \ldots,$ denoted by $a|V\rangle$
  - Closure: the result of these operation belongs to the space, $|V\rangle + |W\rangle \in V$
  - Scalar multiplication is distributive in both the vectors and scalars: $a(|V\rangle + |W\rangle) = a|V\rangle + a|W\rangle,\ \ (a+b)|V\rangle = a|V\rangle + b|V\rangle$
  - Scalar multiplication is associative: $a(b|V\rangle) = (ab)|V\rangle$
  - Addition is commutative: $|V\rangle + |W\rangle = |W\rangle + |V\rangle$
  - Addition is associative: $|V\rangle + (|W\rangle + |Z\rangle) = (|V\rangle + |W\rangle) + |Z\rangle$
  - There exists a null vector $|0\rangle$ obeying $|V\rangle + |0\rangle = |V\rangle$
  - For every vector $|V\rangle$, there exists an inverse under addition, $|-V\rangle$ such that $|V\rangle + |-V\rangle = |0\rangle$
  - For every vector $|V\rangle$, $1|V\rangle = |V\rangle$
- **Definition 2**: The numbers $a, b, \ldots,$ are called the ***field*** over which the vector space is defined.
  - If the field are complex, we have a complex vector space.

Linear Vector Spaces

- The previous definitions imply
  - $|0\rangle$ is unique
  - $0|V\rangle = |0\rangle$
  - $|-V\rangle = -|V\rangle$
  - $|-V\rangle$ is the unique additive inverse of $|V\rangle$
- $|V\rangle$: ket
- $\langle V|$: bra
- Verify that all the above definitions are satisfied by the typical spatial vectors shaped like arrows.
- Examples of vector space
  - All 2x2 matrices
  - All functions $f(x)$ defined in an interval $0 \leq x \leq L$.
  - All periodic function obeying $f(0) = f(L)$

Linear Vector Spaces

- **Definition 3**: The set of vectors $(|1\rangle, |2\rangle, \dots, |n\rangle)$ is said to be ***linearly independent*** if the only set of a_i's satisfying $\sum_{i=1}^{n} a_i |i\rangle = |0\rangle$ is trivial one with all $a_i = 0$ and none of $|1\rangle, |2\rangle, \dots, |n\rangle$ is multiple of $|0\rangle$. If the set of vectors is not linearly independent, we say they are ***linearly dependent***.
- **Definition 4**: A vector space has ***dimension n*** if it can accommodate a maximum of n linearly independent vectors. It will be denoted by $V^n(R)$ if the field is real, and by $V^n(C)$ if the field is complex.
- What is the dimension of 2x2 matrices?
- **Theorem 1**: Any vector $|V\rangle$ in an n-dimensional space can be written as a linear combination of n linearly independent vectors $|1\rangle, |2\rangle, \dots, |n\rangle$.

From Chap. 1 of "Principles of Quantum Mechanics", Ramamurti Shankar, 2nd ed. Plenum Press (1994)

Linear Vector Spaces

- **Definition 5**: A set of n linearly independent vectors in an n-dimensional space is called a ***basis***.
- We can write $|V\rangle = \sum_{i=1}^{n} v_i |i\rangle$
- **Definition 6**: The coefficients of expansion v_i of a vector in terms of a linearly independent basis ($|i\rangle$) are called the **components of the vector in *that basis***.
- **Theorem 2**: the above expansion is unique.

Inner Product Spaces

- Properties of inner product for the case of arrow vector
  - $\vec{A} \cdot \vec{B} = A_x B_x + A_y B_y + A_z B_z$
  - $\vec{A} \cdot \vec{B} = \vec{B} \cdot \vec{A}$ (symmetry)
  - $\vec{A} \cdot \vec{A} \geq 0$, 0 iff $\vec{A} = 0$ (positive semidefinite)
  - $\vec{A} \cdot \left(b\vec{B} + c\vec{C}\right) = b\vec{A} \cdot \vec{B} + c\vec{A} \cdot \vec{C}$ (linearity)
- Generalized requirement for inner product
  - The result is a number (generally a complex)
  - $\langle V|W\rangle = \langle W|V\rangle^*$ (skew-symmetry)
  - $\langle V|V\rangle \geq 0$, 0 iff $|V\rangle = |0\rangle$ (positive semidefinite)
  - $\langle V|(a|W\rangle + b|Z\rangle) = a\langle V|W\rangle + b\langle V|Z\rangle$ (linearity in ket)
- **Definition 7**: A vector space with an inner product is called an ***inner product space***

Properties of Inner Product

- Generalized requirement for inner product
  - The result is a number (generally a complex)
  - $\langle V|W\rangle = \langle W|V\rangle^*$ (skew-symmetry)
  - $\langle V|V\rangle \geq 0$, 0 iff $|V\rangle = |0\rangle$ (positive semidefinite)
  - $\langle V|(a|W\rangle + b|Z\rangle) = a\langle V|W\rangle + b\langle V|Z\rangle$ (linearity in ket)

- Does the following inner product satisfy the requirements?
  - $\vec{A} \cdot \vec{B} = A_x B_x + A_y B_y$
  - $\vec{A} \cdot \vec{B} = A_x (B_x + B_y + B_z)$
  - $\vec{A} \cdot \vec{B} = A_x B_x + 2A_y B_y + 3A_z B_z$
  - $\vec{A} \cdot \vec{B} = A_x^2 B_x^2 + A_y B_y + A_z B_z$

From Chap. 1 of "Principles of Quantum Mechanics", Ramamurti Shankar, 2nd ed. Plenum Press (1994)