CCST9077 notes

T1

preview video

- types of information
    - difference: disorder (thermodynamics)VS order(biology, gene)
- same? connection?
    - only need probability(some randomness) to define information
    - getting rid of all the external things, e.g. language
    - Challenge: all theories are based on some laws, but how come we derive these basic laws?
        - information can be the one concept to close these problems
        - closed reasoning
- information is superior
    - physics: start with laws → derive everything
    - but where does a law come from (infinite regression)
    - answer: information
        - capable of explaining itself
- Why not spontaneous generation of information
    - not faith/ god/ religion
    - infinite regression ⇒ more complex
    - might never get there, but follow the scientific method
    - make sense for oneself
- socially generated construct: emotion/ free will/aesthetic/ love ⇒ no idea
    - quantum physics: grey between black and white
    - probability: something genuinely random
- human information
    - meaningful information: different context
- Are we immortal
    - copy/ ethical issue?
- important phase of development
    - information consistently being created
    - emphasis, explain using a set of only a few rules
    - hope

L2

MOORE'S LAW: #transistors doubles/ 2 year

- summarise, observation
- intel: integrated electronics
- 3nm: r of atoms ~0.1nm, of hair ~50,000nm
- End of Moore's law?
  - new approach: quantum mechanics (state of the atom)⇒ new type of computers
  - • new units of information: qubits instead of bits
  • new ways to transmit information: quantum communication
  • new way to process information: quantum information processing
  Intro to quantum information
- ball in box
    - definite states
    - superposition states → probability

      > scientific method: hypothesis → experiments

    - H1: fluid
    - H2: The ball is either on the left or on the right, but we do not know where it is
        - shake the box: swap classic superposition
- Qubits
  uniqueness of quantum information processing
- no cloning: cannot copy the state of qubits
- cannot be stored in bits

L1

- What made information technology possible 2+2
- What is information
    - everyday
    - general
- Why is information important (forecast + decision making)
- quantifying information (measuring the amount of information)
    - find out the sequence: by asking questions
- bits (what?>>>unit significance?)
- information processing (bg+3)
    - development 3+4+2+next
    - storage
        - df (store into physical object)
        - physical realisation (encode into the property of the object)
        - compression (prior knowledge)
    - transmission
        - df (move place to place)
        - physical realization(encode, decode, traveling object)

        - special case: storage
    - computation
        - df(input, output, basic operation)
        - physical realization(physical interact)
- information revolution
- it from bit(everything in the universe is made of information)
- Can everything be reduced to information

L2

- Moore's law(what? significance? not law of nature; quantify)

> scientific method (hypotheses+experiment)

- ball in box
    - superposition states
    - state collapse (experiment: change the state of the system)
    - Hype1: superposition state ⇒ always L
    - Hype2: classic state, but we don't know which ⇒ can be R
    - magic shake(L → super; super → L)
    - result: always L
- qubits: 2 alternative states+quantum superposition, significance
- quantum information (no cloning + no stored into bits)
    - bits → qubits
- quantum information processing
    - magic shake, open
- it from qubits (everything in the universe made of qubits)

L3

> linearly polarised photon as qubits

- entanglement
    - bell state (know relation, don't know exact which ⇐ dependence) (new state; not either both L or both R)
    - whole vs part
- spooky action at a distance
    - message transfer no faster than light ⇒ no message transfer
- steering
  - **measurement on A** force B to acquire a **definite quantum state**
  - **choice of A's measurement** determines **possible states of B**

> no faster than light communication
> B don't know A's choice of steering or not? -- e.g. H from +45/-45/H

L4

- EPR paper
    - property(independent of measurement)
    - reality(local, cannot be affected by another system?)
    - Bell state (incomplete description of reality)
- Bell's theorem (complete)
    - realism (reality independent of measurement)
    - locality (independent of others)
    - local realistic: (complete description of reality) +locality
- Violation of Bell inequality
- True randomness
- device-independent random number generation

Notes:

L5_cryptography

- one-time pad: 1(flip) 0(remain)
    - secure
        - length(key) == length(message)
        - random
        - no recycle
- quantum key distribution (QKD)
    - E91 protocol: pair of entangled quantum
        - Bell state, announce measurement, check result
        - Observation in between must have an influence
    - BB84 protocol: single quantum
        - steps: preparation(A) ⇒ measurement(B) ⇒ shifting(public discussion) ⇒ detection
        - shifting: AB with different measurement ⇒ collapse at B → dismiss this bit
        - detection: AB same measurement, 50% Eve chooses the wrong measurement ⇒ qubit collapses to the other state ⇒ change the B's observation result → select random sample bits to test correctness

L6_computer

- quantum computing **(why speed up/ where does power come from? → superposition + inference)**

> Deutsch's game

    - simulation (nature itself)

> quantum in **superposition** to attempt computational problem **in parallel**
> ⇒ defeat RSA cryptosystem???

    - HHL (linear equation → quantum-enhanced ML/ AI) (exponential)
    - Grover (search in unstructured database) (quadratic)

> initialization(magic shake many qubits in different superposition)
> ⇒ parallel computing(superposition)
> ⇒ **merging superposition(another magic shake) (inference: cancel/ amplified)**
> ⇒ measurement

    - Shor's (factorization)(exponential) e.g. cybersecurity
- limitation
    - hard to build
    - no Pf: exponential speed up
    - at most exponential speed up (⇐ energy consumption is exponential)
    - general scientific problem
- advantage
    - ideal: no heat ⇒ less heat dissipation ⇒ higher speed& energy cost
    - now: energy-demanding, but one-off (when amount scales up)
- challenge of implementation
    - correction of error ⇒ add redundancy ⇒ more qubits
    - isolation(sensitive to noise), control(interact with qubits), temperature, academic...
- quantum supremacy
    - simulating probability distribution
    - sampling (Jiuzhang)
- future

L7_sensor

- precision limit (fundamental limit)

> precision(repeated/ close to each other) accuracy(close to true value

    - **Heisenberg's uncertainty** : ~~measure position and velocity simutaneouslu with high precision~~ (condition: Heisenberg's microscope)
        - more precision ⇒ more energy, more uncertainty about velocity
        - end of Moore's law, limit in measuring time/ rotation/ ...
- **quantum sensor (single)**

> object(size), superposition, inference

    - Rayleigh's criterion
        - classic: shorter wave length, larger lens
        - quantum: closer!
    - cold atom sensor
        - GPS-free navigation (measuring acceleration & orientation of space, ultra-precise)
        - Gravimeters (general relativity: gravity stronger ⇒ time slower)
        - atomic clock: (latest: nuclear clock)
            - constant vibration frequency of atoms
            - cold atom ⇒ stable
    - magnetic sensor: NV centers
    - medical: detect COVID RNA, imaging of tumor cells
- **quantum-enhanced scaling (entanglement)**
    - classic scaling: √**N** ⇐ N together
    - Quantum Scaling: **N**, Heisenberg scaling, (even with noise: e.g.**N^(3/4)**)
        - GPS: global network of clock ⇒ precision in time ⇒ precision in space
        - squeezed light (positive quantum sensing) 压缩光
        - spin-squeezed atom (rubidium) 自旋压缩原子
        - nuclear magnetic resonance 核磁共振
- application
    - **Quantum-Enhanced LIGO** (Gravitational wave detection)
    - GPS
    - radar
    - microscope
- commercialization

Midterm write-up

logistics

comments, organize them, combine ideas in video and lectures
format: follow up interview/ another scientist who counter some ideas/ time traveller
remark:

- creativity and originallity
- quantum concepts (superposition, entanglement, etc) are concerned, **you are required to describe and explain them using the "magic box" language** (cf. Lectures 1-4) of this course. Please also add references to the origin (e.g., Lecture 3, p 4-5).
- **a brief statement on the usage of AI** (e.g., "AI has been used to polish the write-up and correct grammar mistakes.").
- plagarism

video

- why EPR pairs is alternative model for cryptography
    - Einstine ⇒ Bell
    - defining locality, reality
- why quantum algorithm is not a growing branch of quantum information today

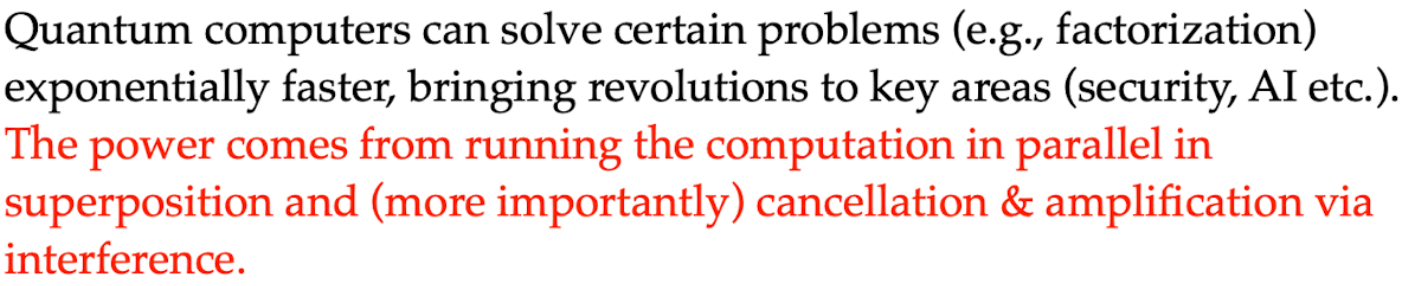
    - "it might be wrong to expect quantum computers to better than classical computer in solving classical and well-defined questions "
    - entirely new class of algorithms, only for quantum not classic ones
      e.g. are 2 quantum entangled
      ⇒ data structure is define under quantum structure
    - quantum simulation
      e.g. biology, photosynthesis, non-trivil, why energy transfer is sufficient? what is the mechanism ⇒ quantum simulation, what is the important factor ⇒ crucial for solar cell technology
      ⇒ presentation of such question is under quantum structure
      e.g.
    - computation becomes exponentially difficult when particles increases
- predictions for the next five years
    - development of tools and techniques ⇒ control nature
        - better quantum communication,
        - quantum cryptography, device independent cryptography
        - quantum computing/ others (apart from quantum simulation)
          e.g. more accurate clock
    - really explore quantum technology: see the potential
        - harness entanglement, superposition
    - imagine going to the past and interviewing a computer scientist like Charles Babbage
      - speculate the usage and impact of this machine: he will not imagine
      ⇒ probably much more ten years later

write-up

setup: I'm a time traveller from 2025 to 2015, who is studying basic quantum computing knowledge. I would like to follow up some question that explains quantum application mentioned in the interview, and share the exciting development in quantum technology in the "following 10 years".

format: **story(some narration)** / third party narration/ first angle? (time traveller, scientist)

- mechanism of cryptography model using EPR pairs: **E91 protocol**
    - quantum entanglement
    - Bell state
    - perform same measurement
- some deficiency of E91 protocol?
- "it might be wrong to expect quantum computers to better than classical computer in solving classical and well-defined questions "
    - correct: quantum simulation, new types of computing algorithm
    - more exciting: classic questions that classical computers might not solve due to exponentially growing complexity (exponentially speed up) ⇒ improve efficiency (exponentially faster)



- future prospect:
    - better quantum communication
    - device independent cryptography
    - quantum computing technology into daily life
- summarize/ ending: lay the foundation, 》》value

A Glimpse Forward: A Conversation Across Time with Professor Artur Ekert

The tutorial room was buzzing with the usual pre-class chatter. Our tutor loaded the week's material - "Today we're watching a classic interview with quantum cryptography pioneer Artur Ekert, recorded back in 2015..." As the video began, something strange happened. The tutor's voice faded into a distant echo. The students around me seemed to dissolve into haze. Only Ekert's image on screen grew sharper, more vivid, until I realized I wasn't watching a recording anymore - I was there, in 2015, standing at the back of the actual interview venue.

(quantum cryptography: Unpacking EPR Pairs & The E91 Protocol) "Professor Ekert", I began, " about those 'spooky' EPR pairs...Could you explain how Einstein's philosophical concern, 'entanglement', become the foundation for your cryptography model E91 Protocol? "

"Let's use a 'magic box' example to explain it. Normally, a single magic box can be in a superposition state, like the ball being both 'left' and 'right' at once until you open it (Lecture 2, p20-26). But **entanglement** involves two boxes. Imagine we have a special source that produces pairs of boxes in what we call a **Bell state** (Lecture 3, p11-12). In this state, you cannot describe the state of one box independently of the other. The two boxes are a single, connected system. If Alice and Bob each take one box from an entangled pair to distant locations, and they both open their boxes (a measurement), they will always find their balls on the same side. If Alice sees 'left', Bob's will be 'left'. If she sees 'right', his will be 'right'. This perfect correlation happens instantly, no matter the distance. This is the 'spooky action at a distance' that so troubled Einstein, but countless experiments have confirmed it's real (Lecture 4, p33-35).

"So in your E91 protocol, this is how you create a secret key?"

"Precisely. In E91, the source sends entangled box pairs to Alice and Bob. To establish a shared secret bit, they both perform the same type of 'magic shake'—a specific way of manipulating the box before opening it, which corresponds to choosing a **measurement basis (Lecture 2, p30-31).** Because of the entanglement, their outcomes—'left' or 'right'—will be identical. They can agree, for instance, that 'left' is 0 and 'right' is 1. This shared, random sequence of 0s and 1s becomes their secret key."

"But what if an eavesdropper(Eve) intercepts the boxes? Could she mimic the entanglement?"

"The answer is no, and this is the core of its security. The No-Cloning property of quantum (Lecture 2, p49-53) prevents Eve from copying a magic box. Her only option is to intercept and measure Bob's box herself. But the moment she performs her **'magic shake,' she collapses the entanglement (Lecture 3, p36)**, destroying the quantum correlation. This sabotage is detectable. In the E91 protocol, Alice and Bob randomly use different types of 'magic shakes' (measurements). Later, they perform a Bell test (Lecture 4, p28-30) by comparing their choices for a subset of boxes.With entanglement, their results will show correlations so strong that they violate a Bell inequality—something impossible in a classical world. If Eve has intervened, the entanglement is broken, and their results will meekly obey the classical limit of the inequality, instantly revealing her presence."

(Quantum Computing's True Potential) "You mentioned that quantum computers's most significant impact(in general) is. creating completely a new class of questions to solved and algorithm as method. Could you elaborate?"

"For example, simulating molecules for drug discovery. Classically, tracking each particle's state requires **exponential resources (Lecture 6, p6)**. But with qubits in **superposition (Lecture 2, p20-26)**, a quantum computer explores all possibilities at once. It's like using a magic box that tests all paths in a maze simultaneously."

"In the following decade, Professor, your vision is reality. Companies now use quantum simulators to design new materials, and quantum machine learning is unlocking patterns in data that were previously invisible."

“However, you also stated that: ‘It might be wrong to expect quantum computers to better than classical computer in solving classical and well-defined problems. I understand your caution, but looking from the future, we've found the situation to be quite different.”

"Oh? Please continue."

"The key lies in how we 'redefine' these problems. Take prime factorization - it's one of the most classical mathematical puzzles. Yet in 1994, Peter Shor conceived an algorithm that uses **quantum superposition and interference** - much like what we call the **'magic shake' (Lecture 2, p30-31) as you mentioned before** and **'constructive/destructive interference' (Lecture 6, p37)** - transforming what was nearly impossible for classical computers into a feasible task for quantum machines. Isn't this a complete of how we approach a classical problem? "

"Then consider solving systems of linear equations, the foundation of countless scientific computations. The **HHL algorithm****(Lecture6)** demonstrates quantum's exponential advantage under specific conditions. Even where we don't have exponential speedup, algorithms like Grover's search providing quadratic acceleration can still fundamentally change the game rules across multiple industries."

"So we've come to see that quantum computing's value lies precisely in providing us with a completely new 'toolbox,' allowing us to re-examine and solve those 'classical' challenges that once stumped conventional computers. It's not a universal solution, but it's actively redrawing the boundaries between 'possible' and 'impossible'."

(Future prospect) "You speak with such conviction about these developments. Tell me, how have these quantum tools actually evolved? What have we built?"
"What started in laboratories has now reached orbit, Professor. China's Micius satellite has transformed quantum key distribution from theory to global infrastructure. We're now sending entangled photons through space, creating hack-proof channels that span continents." I paused, watching his eyes widen. "It's like your E91 protocol scaled to the heavens – we're performing Bell tests between ground stations and satellites." (Lecture 5, p56-59)

"Even more remarkably, your prediction of device-independent cryptography becomes reality. We've built random number generators where we don't need to trust the devices themselves – the violation of Bell inequalities guarantees their security. Your theoretical framework has become practical assurance." (Lecture 5, p59)

"That’s amazing. I said that quantum computing will be seeing great development inthe following years. I’m always hoping that my work could benifit the public, so is how quantum technologies influenced daily life. ”

“While full-scale quantum computers are still emerging, quantum sensors are already revolutionizing everything from navigation to medicine. They're enhancing GPS accuracy, detecting diseases through ultra-sensitive magnetic imaging, and yes – even Samsung phones now use quantum-random encryption." (Lecture 5, p62)

(Closing) The words felt both impossible and inevitable. "Professor, I must confess something extraordinary. I'm not from this time. I traveled here from 2025, from a world where your theoretical seeds have grown into forests of innovation."
He leaned back slowly, the papers on his desk forgotten. A profound smile spread across his face, touching the corners of his eyes. "So," he said softly, "the trees we planted have truly borne fruit." He gazed out the window momentarily, as if seeing across time itself. "I always believed entanglement was more than just a puzzle to solve – it was nature's way of showing us a new language. To hear that we've learned to speak it... that students like you are having this conversation a decade from now..." He turned back, his expression radiant with wonder. "This is beyond anything I dared imagine."

As I prepared to return to my time, I reflected on the tapestry of progress: from Einstein’s skepticism to Bell’s inequalities, from Ekert’s E91 protocol to global quantum networks. Each scientist built upon the last, often without knowing how their 'pure' research would transform the world. Standing in 2015, Ekert saw the potential—but even he couldn’t foresee that in just ten years, quantum technologies would leap from labs into our daily lives. Time has a way of turning theoretical 'magic boxes' into engines of revolution.

Remark:Purpose:

1. To understand Ekert's insights on quantum cryptography and computation using the "magic box" framework from your lectures.
2. To reveal how his 2015 predictions unfolded by 2025.

Key ideas from lectures weaved in:

Lecture 2: Magic boxes, superposition, measurement collapse.

Lecture 3: Entanglement, Bell states, spooky action.

Lecture 4: CHSH game, Bell inequalities, true randomness.

Lecture 5: E91/BB84 protocols, device-independent crypto, QKD networks.

Lecture 6: Quantum simulation, exponential speedup, quantum supremacy.

AI Usage Statement

"AI was used to refine grammar and enhance narrative flow. "