

# 양자 프로그래밍 Quantum Programming

이광근  
프로그래밍 연구실  
ropas.snu.ac.kr  
서울대학교

# 전공: 프로그램 분석

- 프로그램 분석(program static analysis) = 실행전에 실행성질을 자동으로 안전하게 어림잡는 일반적인 방법
  - “실행전”: 프로그램을 돌리기 전에
  - “실행성질”: 실행중의 프로그램 성질
  - “자동으로”: 프로그램이 프로그램을 분석
  - “안전하게”: 모든 실제상황을 포섭
  - “어림잡는”: 군더더기가없을 순 없다
  - “일반적인”: 가능한 언어와 실행성질이 무제한

# 웬 양자 프로그래밍?

- 궁금
- 지금은 아마도 양자컴퓨터의 1930년대
  - 양자 프로그래밍 언어 및 프로그래밍 시스템?
  - 프로그래밍 언어/프로그램 분석 기술을 발판으로
- “통계적 프로그램 분석” “statistical static analysis”
  - 분석은 반드시 안전(sound)해야 한다?
    - 안전성을 포기하는 분석이 유용할 수도
    - 2시간 분석 후 “100% 확신하는 데, 버그 없다” 대신에
    - 2초 분석 후 “100% 확신하는 데, 버그 있거나 없다” 대신에
    - 2초 분석 후 “99% 확신하는 데, 버그 없다.”
  - 양자 프로그램의 의미(분석)는 근본적으로 확률적이다

# 양자 컴퓨터의 능력/성질

- 하나가 동시에 두 상태를 가질 수(superposition)
  - 한 비트가 0과 1을 동시에 가질 수 있다
  - n개의 비트가 한 순간 최대  $2^n$  개 상태를 가질 수 있다!
- 완벽한 블랙박스
  - 양자 데이터는 박스 안에
  - 외부에서는 연산 함수만 싸 준다
  - 외부에서 결과를 쳐다보려는 순간 중첩은 사라진다
- 두개가 완벽히 엮일 수(entanglement)
  - 한 비트가 0으로 관찰되면 다른 하나는 반드시 1로 관찰된다! 혹은 그 반대로.

# 수학적인 모델(1/4)

## Quantum State

- a quantum state = a vector in a Hilbert space (complex vector space  $\mathbb{C}^n$  for some  $n \in \mathbb{N}$ )
- quantum bit(qbit) state:
  - $a|0\rangle + b|1\rangle$  or vector  $(a, b)$
  - “amplitudes”  $a, b \in \mathbb{C}$  and  $|a|^2 + |b|^2 = 1$
  - $|a|^2$  and  $|b|^2$  are the probabilities for 0 and 1
- one-qbit state is a vector  $(a, b)$
- two-qbit state is a vector  $(a, b, c, d)$
- n-qbit state is a vector of length  $2^n$

# a one-qubit state

| states | amplitude    | probability |
|--------|--------------|-------------|
| 0      | $0.3 + 0.3i$ | 0.18        |
| 1      | $0.9 + 0.1i$ | 0.82        |

Above two states are superposed in one qubit with the probabilities.

$$\phi$$

“amplitude” denotes also the two square roots  $\pm \sqrt{0.18}$  the probability.

# a three-qbit state

| states | amplitude      | probability |
|--------|----------------|-------------|
| 000    | $0.37 + 0.04i$ | 0.14        |
| 001    | $0.11 + 0.18i$ | 0.04        |
| 010    | $0.09 + 0.31i$ | 0.10        |
| 011    | $0.30 + 0.30i$ | 0.18        |
| 100    | $0.40 + 0.01i$ | 0.16        |
| 101    | $0.35 + 0.43i$ | 0.31        |
| 110    | $0.09 + 0.12i$ | 0.02        |
| 111    | $0.15 + 0.16i$ | 0.05        |

Above 8 states are superposed  
in three qbits with the probabilities.

$$\phi\phi\phi$$

# quantum state = vector

- $q = a0 \oplus b1$  를 벡터  $(a,b)$  로 표현
- $q = a00 \oplus b01 \oplus c10 \oplus d11$  를 벡터  $(a,b,c,d)$  로 표현
- $q =$  크기가  $2, 2^2, 2^3, \dots$  인 벡터를



# 수학적인 모델(2/4)

## Quantum Entanglement

- 두개의 독립적인 qbit  $(a,b)$ 와  $(v,w)$ 가 합쳐지면 2-qbit 는
  - $(av, aw, bv, bw) = (a,b) \otimes (v,w)$
- 두개의 qbit이 완벽하게 엮였다는 것은, 그것들이 두개의 qbit으로 쪼개지지 못하는 경우를 말한다
  - $(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}) \neq (a,b) \otimes (v,w)$
  - 첫 qbit과 두번째 qbit은 항상 같도록 엮여있다.

# 수학적인 모델(3/4)

## Quantum Operations

- quantum state transitions = linear and unitary transformations  $T$

$$\begin{bmatrix} a \\ b \end{bmatrix} \mapsto T \begin{bmatrix} a \\ b \end{bmatrix}$$

- “linear”: operators are matrices
- “unitary”: the unit probability is preserved
- for  $n$ -qbit states, a quantum operator is a unitary  $2^n \times 2^n$  matrix over  $\mathbb{C}$

# basic quantum gates

N, Nc, H, Hc, V, Vc, W, Wc, X

– not, Hadamard, phase changes, controlled-ops, exchange

–  $H(1,0)$  = uniform superposition  $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$

– Nc  $((\frac{1}{\sqrt{2}} \otimes \frac{1}{\sqrt{2}} (1,0)))$  = entangled bits  
 $(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{i} \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\
 \begin{pmatrix} \text{Id} & 0 \\ 0 & N \end{pmatrix} \quad \begin{pmatrix} \text{Id} & 0 \\ 0 & H \end{pmatrix} \quad \begin{pmatrix} \text{Id} & 0 \\ 0 & V \end{pmatrix} \quad \begin{pmatrix} \text{Id} & 0 \\ 0 & W \end{pmatrix}$$

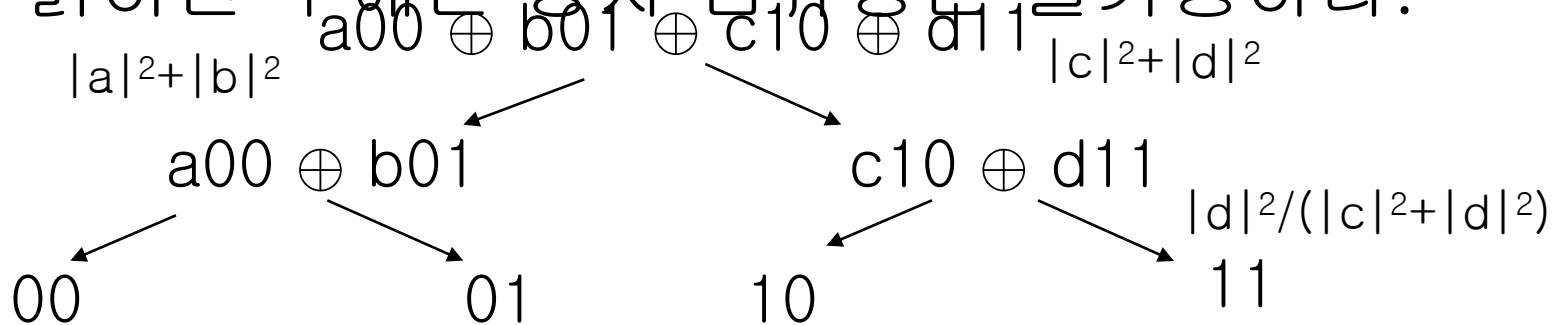
# compound quantum operations

- **initialize** to the uniform superposition of  $n$  qbits:  $(\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}))$
- phase **flips**:  $(a,b) \mapsto (a,b)$
- **entangle**:  $(\frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}})$
- **Fourier transform**: computing period
- an operation can be **simultaneously** applied to multiple qbits
- $H, Vc, X$  can make **any unitary transform**

# 수학적인 모델(4/4)

## Measurement

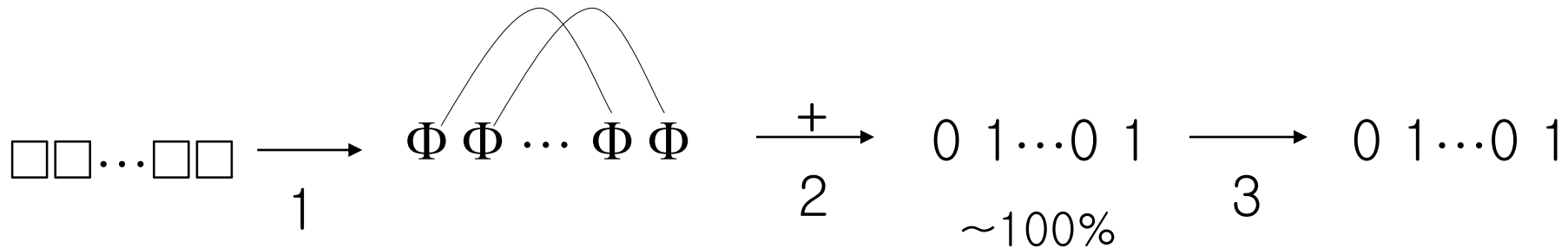
- 양자비트 값을 읽는 순간 중첩된 것 중에 하나만 관찰된다.
  - 중첩된 모든 것을 관찰할 순 없다
  - 확률에 따라 하나만 볼 수 있다
- 엮여있는 양자비트는 짝의 관찰 결과에 따라 엮인다
- 읽혀진 후에는 양자 컴퓨팅을 불가능하다.



# 양자 프로그래밍 스텝

## Steps in Quantum Programming

1. **initialize** qbits: superposition, entanglement, etc.
2. **transform** by unitary operations
3. **measure**



# 양자 컴퓨터 후보들

- NMR on molecules in solution
- quantum dots on surface
- laser acting on floating ions in vacuum
- molecular magnets

# 양자 컴퓨터의 계산이론

- **사실**: 양자컴퓨터는 확률적인 계산만한다.
- $QP =$  양자컴퓨터가 효과적으로 풀 수 있는 문제의 집합
- **추측**:  $QP \cap NP\text{-완결} = \{\}$ 
  - 즉, 양자컴퓨터는  $NP\text{-완결}$ 문제를  $P\text{-시간}$ 에 풀 수는 없을게다
  - 양자컴퓨터 + 비선형연산자 라면 몰라도
- **사실**: 양자컴퓨터때문에 계산가능한 함수가 더 늘지는 않는다.
  - 양자-계산가능  $\Rightarrow$  튜링-계산가능
  - 끝나요-문제는 양자컴퓨터로도 못 푼다
  - 처치-튜링 논제는 아직도 살아있다



# 양자 알고리즘 vs 확률적 알고리즘

## quantum algm vs randomized algm

- 양자 알고리즘은 확률뿐 아니라 위상 phase까지 운용할 수 있다
- 확률: one-qbit state  $(a,b)$  has 0 with prob.  $|a|^2$ , or 1 with prob.  $|b|^2$
- 위상: two one-qbit state  $(a,b)$  and  $(\overline{a},\overline{b})$  has the same prob. dist. but opposite phases.
- $\overline{a_1 + a_2 i} = a_1 - a_2 i$

# 양자계산 알고리즘 1

## 양자탐색 quantum search(1/2)

- data: (A,10), (B,11), (C,01), (D,00), unordered
- goal: search who is 01
- algorithm
  1. **uniformly** superpose 2 qbits such that every entry has prob  $\frac{1}{4}$  with positive amplitude  $\frac{1}{2}$
  2. **reverse phase**: beam pulses to reverse matched entry's phase, from  $\frac{1}{2}$  to  $-\frac{1}{2}$
  3. **trim**: beam pulses to set each entry's amplitude as the reverse difference from the average
    - amplitude  $\frac{1}{2}$  becomes (  $\frac{1}{4} - \frac{1}{4} = 0$  )
    - amplitude  $-\frac{1}{2}$  becomes (  $\frac{1}{4} + \frac{3}{4} = 1$  )
  4. **measure!** 01 is read.

time complexity: we repeat steps 2-3  $O(\sqrt{N})$  times.

# 양자 탐색 quantum search(2/2)

suppose we search entry of 101

input qubits

amplitude  $+\frac{1}{2\sqrt{2}}$

A 011

B 001

C 110

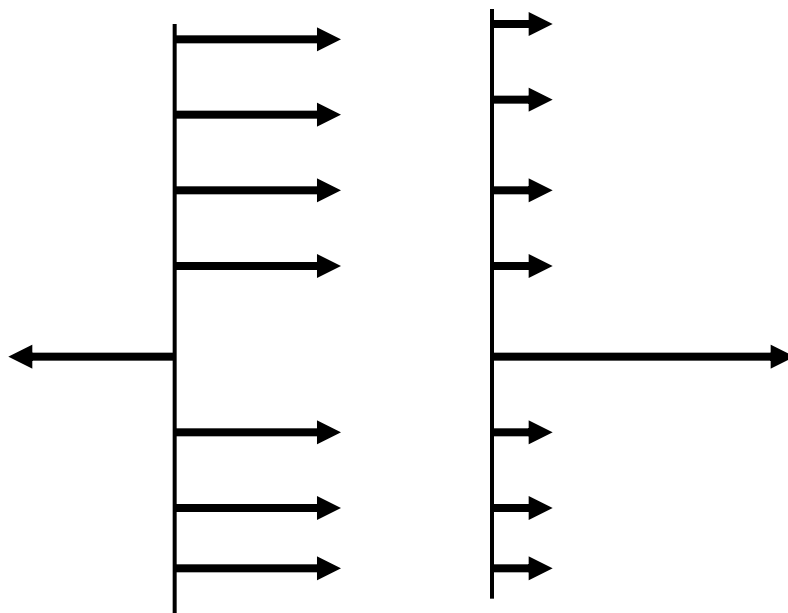
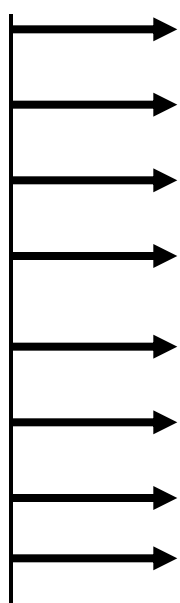
D 000

E 101

F 010

G 111

H 100



prob. 1/8

( reverse phase ; trim )  $\sqrt{N}$

# 양자계산 알고리즘 2

## 양자 인수분해(1/2)

- to factorize  $N$ : known in mathematics
  - choose a random  $r < N$
  - $r^1 \bmod N, r^2 \bmod N, r^3 \bmod N, \dots$
  - period length  $p$  of the above sequence
  - $\gcd(r^{p/2}+1, N), \gcd(r^{p/2}-1, N)$  are prime factors with high prob.

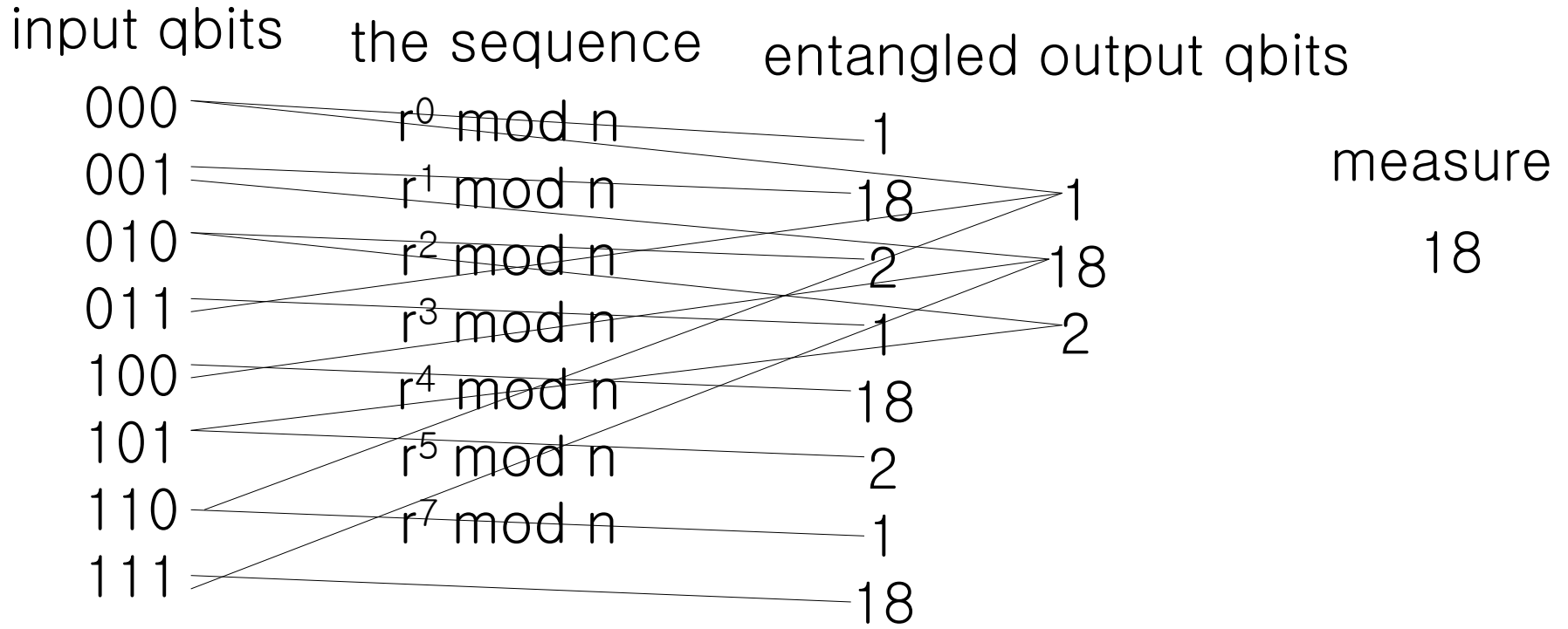
$$N = 15, r = 7$$

$$7, 4, 13, 1, 7, 4, 13, 1, 7, 4, 13, 1, 7, \dots$$

$$p = 4$$

$$\gcd(7^2+1, 15) = 5, \gcd(7^2-1, 15) = 3$$

# 양자 인수분해 (2/2)



001      get the period

100                      3                      then compute the gcd's

111

input after the measure

# Quantum Programming Language

## 현재수준(1/2)

```
 $C ::= \text{let bit } b = 0 \text{ in } C$   
|  $\text{let qbit } q = 0 \text{ in } C$   
|  $b = 0 \mid b = 1$   
|  $q_1 \cdots q_n^* = U$   
|  $\text{skip} \mid C; C$   
|  $\text{if } b \text{ then } C \text{ else } C$   
|  $\text{measure } q \text{ then } C \text{ else } C$   
|  $\text{while } b \text{ do } C$ 
```

from [Selinger 2003] with some touch

# Quantum Programming Language

## 현재수준 (2/2)

- mathematical semantics: denotational
  - semantics of loops by limits in ordered space
- static type system
  - primitive, simple: Pascal-like
  - no compound data types

# Language and Static Analysis Issues

- no compound/algebraic quantum data type yet
  - superposition of multiple list
  - `qtype qlist = qNIL | qCONS of int * qlist`
  - `qCONS(2,qCONS(1,qNIL))` means the superposition of `[]`, `[1]`, and `[1, 2]`.
- no high-level construct for the unitary transformation  $U$  yet
- need static checks for
  - is  $U$  unitary transformation?
  - any duplicate quantum data?
    - copying quantum data is impossible



# 자료

- *A Shortcut Through Time*, George Johnson, 2003
- “Towards a Quantum Programming Language”, Peter Selinger, 2003
- “Quantum Programming in QCL”, Bernhard Omer, 2000
- “Quantum Programming”, Paolo Zuliani, 2001
- “Quantum computer”, from Wikipedia
- “There’s Plenty of Room at the Bottom”, Richard Feynman, 1959
- “A fast quantum mechanical algorithm for database search”, Lov Grover, 1996
- “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, Peter Shor, 1995
- 기타 인터넷 자료들