양자 사후 추론을 쉽게 잘 이용할 수 있게 하기

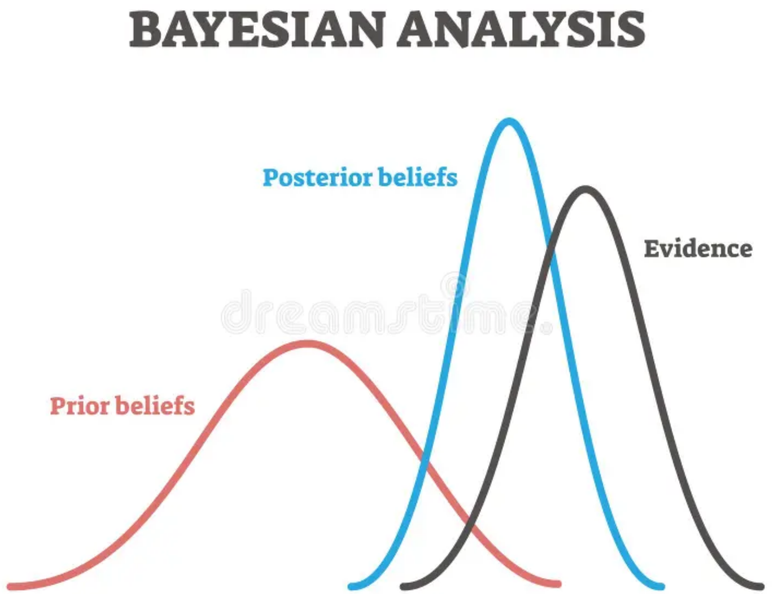
전승민, 류석영

SIGPL Summer School 2026

사후 기댓값 추론은 흔히 필요한 문제

$$\mathbb{E}[X \mid e] = \sum_{x} P(X = x \mid e) \cdot x$$

- **확률 모델에서, “사건 e 발생시 X의 기댓값은?”**
  - 예 1: 날씨가 흐릴 때, 비가 올 확률은?
  - 예 2: 사고가 발생했을 때, 예상 지연 시간은?
- 공학, 과학, 의료 등 여러 분야에서 흔히 필요



양자컴퓨터로 가속 가능

$\mathbb{E}[X \mid e]$를 오차 ϵ 이내로 근사하고 싶다”

필요 샘플 수:

	e 발생확률		
고전	$P(e)^{-1}$	$\times$	ϵ^{-2}
양자	$\sqrt{P(e)^{-1}}$	$\times$	$\sqrt{\epsilon^{-2}}$

제곱근으로 감소

예: $P(e) = 0.01, \epsilon = 0.01$ → 고전은 1M개, 양자는 1K개 샘플 필요

Quantum rejection sampling (Ozols et al, TOCT’13)

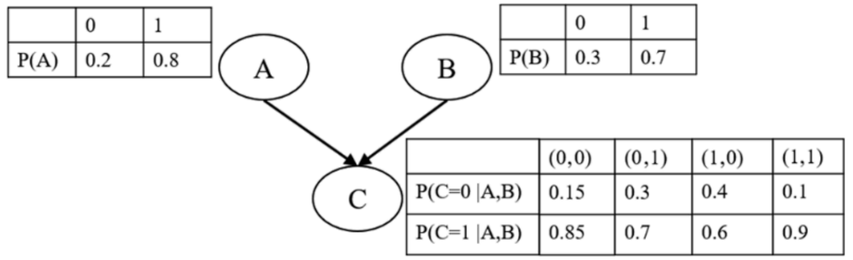
Quantum speedup of Monte Carlo methods (Montanaro, PRSA’15)

그러나, 이론을 실적용하기 어려움

기대: $\sqrt{P(e)^{-1}} \times \sqrt{\epsilon^{-2}}$ 개 샘플로, → $\tilde{\mathbb{E}}[X \mid e]$

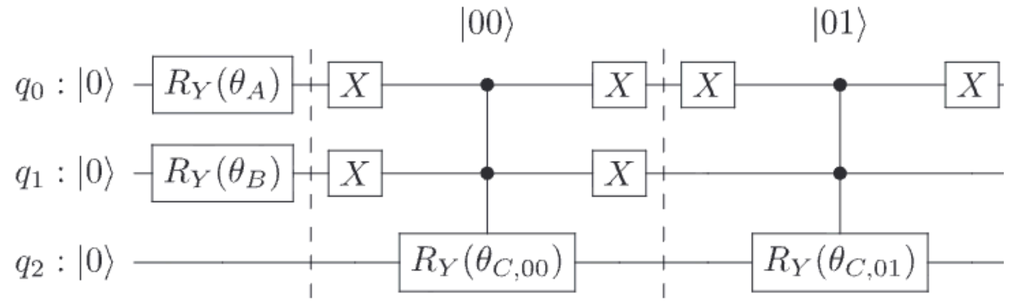
필요부품: (1) 확률분포를 표현하는 양자회로, (2) $P(e)$ 값

- (1), (2) 둘 다 다룬 사례는 없음
- (1)만을 Bayesian network (BN)로 다루는 방법들: **양자이득은 절반, 사용성과 효율도 낮음**



확률모델을 표현하는 BN

컴파일



Quantum inference on Bayesian networks (Low, Chuang, PRA'14)

해결책: 확률적 프로그래밍 언어를 양자로 연결

사후 기댓값 문제

Q: 두 부품 중 적어도 하나가 고장났을 때, 평균 몇 개 고장?

$$\mathbb{E}[F_1 + F_2 \mid F_1 + F_2 \geq 1]?$$

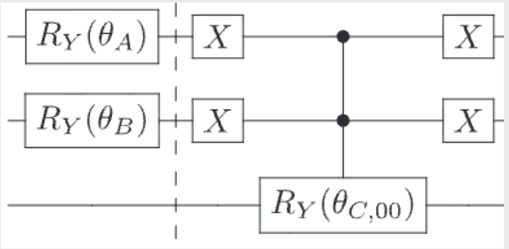


확률적 프로그램

```
F1 ~ Bernoulli(0.5);
F2 ~ Bernoulli(0.5);
observe(F1 || F2);
return F1 + F2;
```



양자회로, P(e) 분석결과



$$P(F_1 + F_2 \geq 1) = 3/4$$

양자이론과 연결

$$\tilde{\mathbb{E}}[F_1 + F_2 \mid F_1 + F_2 \geq 1] = 4/3$$

기대: 쉽고 효율적이고 제대로 된 첫 end-to-end

사후 기댓값 문제

Q: 두 부품 중 적어도 하나가 고장났을 때, 평균 몇 개 고장?

$$\mathbb{E}[F_1 + F_2 | F_1 + F_2 \geq 1]?$$

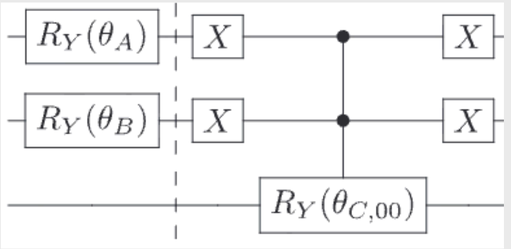


확률적 프로그램

```
F1 ~ Bernoulli(0.5);
F2 ~ Bernoulli(0.5);
observe(F1 || F2);
return F1 + F2;
```



양자회로, P(e) 분석결과



$$P(F_1 + F_2 \geq 1) = 3/4$$

사용 쉬움

다양한 확률모델, 사건을 고수준으로 쉽게 작성 가능

컴파일 효율 높음

BN 기반과 다르게, 고수준 연산 회로 (곱셈 등)를 적극 사용

양자이론과 연결

양자이득 전부 취함

$$P(e)^{-1}\epsilon^{-2} \rightarrow P(e)^{-1/2}\epsilon^{-1}$$

$$\tilde{\mathbb{E}}[F_1 + F_2 | F_1 + F_2 \geq 1] = 4/3$$

양자 사후 추론을 쉽게 잘 이용할 수 있게 하기

- 배경: 사후 기댓값 추론은 중요, 이를 위한 양자가속 이론이 있음
- 문제: 기존의 BN 기반 방법들은 양자 이론을 실적용하기 불충분
  - 두 개의 양자 이론 중 하나만 적용 가능
  - 그마저도 사용성, 컴파일 효율 부족
- 해결책: 확률적 프로그래밍 언어로부터 고수준 컴파일
  - 기대 1: 고수준 연산식을 그대로 양자회로로 변환 => 사용성, 컴파일 효율
  - **기대 2: 고수준 정보로부터 P(e)를 분석 => 두 양자이론 모두 적용 가능 (Main TODO)**