양자정보의 측정에 대한 양자광학적 연구: 정보이득과 상태교란의 배타성

백소영*, 김윤호*

1. 양자측정

양자역학에서 양자상태의 측정에 대한 문제는 양자이론의 발전 과정에서 철학적 과학적 논쟁의 핵심주제가 되어 왔다. 고전역학과 달리, 양자역학에서는 측정이라는 행위 자체가 측정 대상의 양자상태를 교란시키는 역할을 한다 [1]. 양자측정의 방법에는 관측대상과 측정장치를 직접 연결하여 정보를 얻어내는 직접측정(direct measurement)과 간접적으로 정보를 얻어내는 간접측정(indirect measurement)이 있다. 직접 측정은 Heisenberg의 불확정성의 원리로 설명할 수 있는데 보다 많은 정보를 얻기위해 측정의 강도를 세게 할수록 측정되는 계의 양자상태는 더욱 심하게 교란된다 [2]. 간접측정의 경우 양자지우개(quantum eraser)를 예로 들 수 있는데 측정대상에 대한 양자정보를 양자얽힘(quantum entanglement)을 이용해 간접적으로 지움으로써 측정에 의한 직접적인 양자상태의 교란을 피할 수 있다 [3, 4].

양자측정을 통해서 얻는 정보의 양과 측정대상의 양자상태의 교란 사이에는 배타적인 관계식이 성립하는데 양자정보 연구의 초기에도 이러한 관계에 대한 구체적이고 정량적인 연구의 중요성은 알려져 있었다 [5]. 이러한 연구를 위해서는 먼저 양자측정의 두 가지 요소를 정의할 필요가 있다. 첫번째는 측정을 통해 얻는 정보를 어떻게 기술할 것인가이고 다음 문제는 측정후의 양자상태를 어떻게 기술할 것이냐는 문제이다. 또 양자측정에서 단일 양자계에 대한 한 번의 측정은 양자상태에 대한 아무런 정보도 주지 못함이 알려져 있으므로 이 문제를 의미있게 접근하기 위해서는 양자역학이 전제하고 있는 Born의 통계적 해석방법이 필요하다. 즉 양자상태에 대한 정보이득이란 가능한 많은 측정을 통해 특정 양자상태를 가질 확률이 특정 확률로 존재한다는 것을 통계적으로 기술할 수 있어야 한다는 것이다. 여기서 통계적 방법으로 정량화된 정보이득과 양자상태의 교란은 우리가 도달할 수 있는 양자측정의 한계치를 정의해준다.

양자측정에서 정보를 얻어내는 과정이 양자상태의 교란을 반드시 수반해야 한다면 양자측정시 우리가 사용해야 할 전략은 측정을 통해 최대한 많은 정보를 얻어내면서 최소한의 상태교란을 측정되는 계에 주는 것이다. 따라서 다양한 양자상태에 대해 최적의 양자측정 방법을 찾아내고 또 효율적으로 구현하는 것은 양자역학의 학문적 연구뿐만 아니라 양자정보분야의 발전에 필수적인 기초연구에 해당한다 [9, 10, 11]. 양자정보의 측정과정에서 나타나는

* 포항공과대학교 물리학과

정보이득과 상태교란의 배타성은 양자광학적인 시스템을 이용해 연구할 수 있는데 이 글에서는 양자정보의 측정에 대한 양자광학적 연구에 대해 간략히 소개하고자 한다.

2. Heisenberg 현미경

1927년 Heisenberg는 과학에서 필요한 모든 개념들은 그에 대응되는 실험설계가 있어야 의미를 가질 수 있다고 믿고 양자측정의 불확정성에 대한 사고 실험을 처음으로 선보인다. 그림 1은 Heisenberg가 제안한 정지해 있는 전자의 위치를 측정하기 위한 현미경이다. 직경 D와 초점거리 f를 가지는 렌즈를 이용해 현미경를 구성하고 전자는 렌즈의 초점에 놓여있다고 가정한다. 이때 왼쪽 방향에서 입사되는 광자는 전자와 충돌을 겪은 후 산란되고 현미경을 통해 이 산란되는 광자를 관측함으로써 전자의 위치를 알 수 있다. 파동이론에 따르면 현미경이 구별할 수 있는 전자의 위치의 정확도는 회절한계에 의해 다음과 같이 주어진다.

$$\Delta x = \lambda/(2\sin\theta). \tag{1}$$

따라서 파장이 짧은, 즉 에너지가 높은 광자를 이용할수록 전자의 위치를 보다 정확하게 측정할 수 있다.

하지만 에너지가 높은 광자를 이용할수록 광자는 전자와 충돌시 많은 운동량을 전자에게 전달하게 되고 전자는 필수불가결한 상태 변화를 겪어야 한다. 여기서 운동량 보전법칙을 이용하면 충돌후 전자가 얻게 되는 운동량의 불확정을 계산할 수 있다. 먼저 충돌전 전자는 정지해 있다고 가정하였으므로 전체계가 가지는 운동량은 초기 입사되는 광자가 가지는 운동량인 h/λ로 표현되며, 여기에서 h는 플랑크 상수이다. 충돌후 광자가 렌즈를 통해 관측되는 경우는 그림 1에서 광자가 2θ의 입체각 내에서 렌즈에 도달하는 경우로 이때 전자가 가질 수 있는 x 방향 운동량의 최대와 최소값은 다음과 같다.

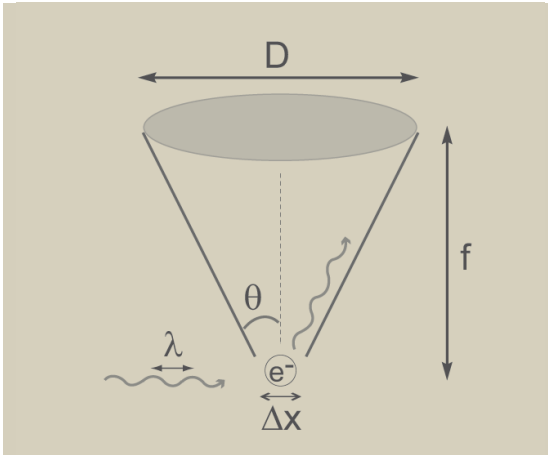

그림 1. Heisenberg 현미경의 개념도. *D*와 *f*는 각각 렌즈의 직경 및 촛점거리이다.

$$\max(p_x) = \frac{h}{\lambda} + \frac{h\sin\theta}{\lambda'}, \tag{2}$$

$$\min(p_x) = \frac{h}{\lambda} - \frac{h\sin\theta}{\lambda''}. \tag{3}$$

광자의 파장이 전자와의 충돌에 의해 크게 변하지 않으므로 $\lambda \approx \lambda' \approx \lambda''$로 근사할 수 있고 따라서 전자의 x 방향 운동량의 불확정성은 다음과 같이 표현된다.

$$\Delta p_x \sim \frac{2h\sin\theta}{\lambda}. \tag{4}$$

식 (1)과 식 (4)으로부터 전자의 위치 및 운동량 측정의 불확정성의 최소값을 구할 수 있으며 이는 아래와 같다.

$$\Delta x \Delta p_x \sim h.$$

일반적인 양자측정은 이 최소값 보다 더 큰 불확정성을 줄 것으로 생각할 수 있으므로 위 식은 아래와 같이 표현될 수 있다.

$$\Delta x \Delta p_x \geq h. \tag{5}$$

식 (5)가 바로 잘 알려진 Heisenberg의 불확정성의 원리이며 전자의 위치 측정의 정확도가 높아질수록 측정 후 운동량 값의 불확정성이 더 커지는 것을 알 수 있다. Heisenberg의 불확정성의 원리는 일반적으로 서로 공액변수 관계에 있는 두 물리량의 측정의 정확도는 서로 배타적인 관계에 있음을 나타낸다.

3. 양자정보의 측정

3.1 양자정보의 기본단위 및 양자정보의 측정

고전적인 정보처리과정에서 사용하는 정보의 기본 단위인 비트는 0 또는 1의 값을 갖는다. 반면 양자역학의 핵심개념인 양자중첩을 이용하면 0과 1 두 개의 상태를 동시

양자정보의 측정에 대한 양자광학적 연구: 정보이득과 상태교란의 배타성

에 가질 수 있는 이차원 양자 상태 (양자비트 또는 qubit)를 만들 수 있으며 아래와 같이 표현한다.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \quad (6)$$

양자비트에 저장된 양자상태를 양자정보라고 하며 α와 β가 복소수이므로 양자비트는 그림 2에 표현된 Bloch 구(sphere) 표면의 모든 지점을 표현 가능한 벡터로 이해될 수 있다. 이와 비교할 때 고전비트는 Bloch 구의 남극($|1\rangle$) 또는 북극 ($|0\rangle$)만을 표현할 수 있다.

많은 수의 양자비트들을 이용하면 양자중첩 및 양자얽힘에 의해 동시에 여러 상태에 작용하는 병렬식 정보처리를 할 수 있어 기존의 디지털 컴퓨터보다 특정 연산을 훨씬 빨리 할 수 있는 양자 전산이 가능하다고 알려져 있다 [6]. 또한 고전적으로는 구현이 불가능한 양자암호(quantum cryptography) 및 양자전송(quantum teleportation) 등의 양자통신이 가능하다는 것도 최근 활발한 연구를 통해 알려져 있다 [7].

양자전산 및 양자통신을 위해서는 양자비트의 안정적인 구현과 제어가 필수적인데 최근 편광, 위상, 경로, 시간 등 단일광자의 다양한 자유도를 이용해 안정적인 양자비트를 구현하고 제어하는 연구가 많이 진행되고 있다 [8]. 단일광자기반의 양자비트는 양자통신 분야의 응용에 특히 적합하며 선형광학계(linear optical elements)를 이용한 양자전산이 가능하다는 것도 알려져 있어서 양자정보 실험연구의 중요한 부분을 차지한다 [6, 7].

양자정보의 측정이란 결국 양자비트의 양자상태를 측정하는 것이다. 앞서 소개한 Heisenberg의 불확정성의 원리

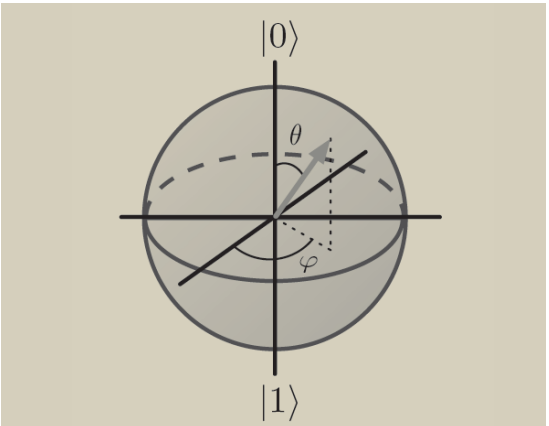

그림 2. Bloch 구(sphere). 양자비트는 Bloch 구 표면의 모든 지점을 표현할 수 있는 반면 고전비트는 남극(|1⟩) 또는 북극(|0⟩)만을 표현할 수 있다.

에 의하면 모든 양자측정에서 정보를 얻는과정은 측정대상의 교란을 야기한다. 따라서 양자정보를 잘 다루기 위해서는 양자비트의 측정에서 얻을 수 있는 정보이득(information gain)과 상태교란(state disturbance)을 정량화하고 이들 간의 균형관계에 대한 연구가 선행되어야 한다.

먼저 측정을 통한 정보이득을 어떻게 정량화 할 수 있는지 알아보자. 앞서 이야기 한 바와 같이 단일 양자계에 대한 한번의 측정은 양자상태에 대한 아무런 정보도 주지 못하며 No cloning theorem에 의해 임의의 양자상태를 완벽하게 복제하는 것은 불가능 하다. 양자비트의 양자상태를 완벽하게 파악하려면 동일하게 준비된 양자비트 앙상블(ensemble)에 대한 무한번의 측정을 통해 복소수인 α와 β를 알아내어야 하지만 이러한 측정은 불가능하다. 따라서 현실적으로 우리는 동일하게 준비된 유한한 갯수의 양자비트 앙상블에 대해 유한번의 측정을 함으로써 양자비트의 양자상태를 추정할 수 있다. 양자측정의 결과를 통해 추정(Guess)하는 상태를 ρ_G라고 한다면 측정을 통한 정보이득은 추정하는 상태가 측정 이전의 양자비트의 양자상태와 얼마나 닮았는지를 정량화하는 estimation fidelity G_ψ로 정의할 수 있으며 아래와 같다.

$$G_\psi = \langle\psi|\rho_G|\psi\rangle.$$

이 때 측정하는 양자비트를 Bloch 구 상에 존재하는 모든 가능한 pure state에 대해 고려하면 estimation fidelity의 평균값은 다음과 같이 주어진다.

$$G_{\mathrm{avg}} = \int G_\psi d\psi.$$

양자비트에 아무런 측정도 하지 않으면서 단순히 양자상태를 무작위 추정(random guess)을 할 경우에도 양자상태를 제대로 맞출 확률이 있으므로 정보이득을 정량화 할 수 있는데 이 경우 estimation fidelity는 1/2로 주어진다 [7]. 즉 양자비트에 대한 estimation fidelity의 최소값은 1/2이며 측정의 세기에 따라 이 값은 증가한다.

양자측정에서 관심있는 또하나의 요소는 측정에 의한 상태변화 즉 양자비트의 변화이다. 측정에 의해 교란된 양자상태를 ρ_F로 정의하면 측정 전과 측정 후의 양자비트의 닮은 정도는 operation fidelity F_ψ로 정의할 수 있고 아래와 같다.

$$F_\psi = \langle\psi|\rho_F|\psi\rangle.$$

그리고 operation fidelity의 모든 양자상태에 대한 평균값은 다음과 같이 주어진다.

$$F_{\text{avg}} = \int F_\psi d\psi.$$

Operation fidelity가 1에 가까울 경우 측정 후의 양자상태가 측정 이전의 양자상태와 비슷하다는 것을 뜻하므로 측정을 통한 상태교란이 별로 없었음을 의미한다.

3.2 정보이득과 상태교란의 균형관계

Heisenberg 현미경의 경우와 같이 양자비트에 대한 측정에서도 정보를 많이 얻기 위한 측정은 더 많은 상태교란을 수반할 수 밖에 없다. 그림 3은 양자측정을 통해 얻을 수 있는 두 물리량인 estimation fidelity (G)와 operation fidelity (F)의 배타성에 대해 간략히 묘사하고 있다. G와 F의 상관관계는 d-차원의 양자상태에 대해 이론적인 연구가 이루어 졌고 2차원 양자상태인 양자비트의 경우 G와 F의 상관관계는 아래와 같다 [13].

$$F_{\text{avg}} \le \frac{2}{3} + \frac{\sqrt{1-(6G_{\text{avg}}-3)^2}}{3}. \qquad (7)$$

위의 estimation fidelity (G)와 operation fidelity (F)의 관계식에서 최소교란양자측정(Minimum disturbance quantum measurement)을 등호가 성립하는 경우로 정의하며 이는 특정 정보이득의 값(G)에서 F가 최대가 되는 (즉 상태교란이 최소인) 양자측정에 해당된다.

그렇다면 최소교란양자측정을 통해 우리가 얻을 수 있는 정보이득의 최소와 최대값은 어떻게 정해질까? 정보이득이 최소가 되는 경우는 측정을 하지 않는 경우 또는 정보를 전혀 얻어낼 수 없는 측정을 하는 경우이다. 이때 양자비트의 상태를 $|0\rangle$ 또는 $|1\rangle$로 무작위로(random) 추정할 수 밖에 없으므로 그 경우 추정한 양자상태가 측정전의 양자상태와 일치할 확률은 1/2로 예상할 수 있다. 그렇다면 앞서 정의된 estimation fidelity가 과연 이 예상값과 일치하는지를 알아보자. 양자비트의 상태를 0으로 (또는 1) 추정한다고 가정하면 식 (6)의 양자비트에 대한 estimation fidelity는 $G_\psi = |\langle 0|\psi\rangle|^2 = |\alpha|^2$ (또는 $|\beta|^2$)이다. 이를 모든 가능한 양자비트의 pure state 대해 평균하면 Gavg = 1/2이므로 앞의 예상값과 일치함을 알 수 있다. 이러한 정보를 전혀 얻어낼 수 없는 측정은 상태를 교란시키지 않기때문에 operation fidelity는 1의 값을 가진다.

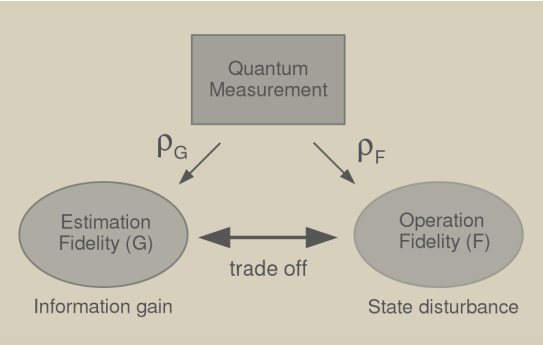

그림 3. 양자측정에서 정보이득(information gain)과 상태교란(state disturbance) 의 배타적관계. 측정을 통해 추정한 양자상태는 ρ_G 이며 측정 후 교란된 양자상태는 ρ_F 이다.

이번에는 매우 강한 측정을 하는 경우를 상상해보자. 양자상태를 computational basis인 $|0\rangle$과 $|1\rangle$로 투영측정(projection measurement)하는 경우 식 (6)의 양자비트는 $|0\rangle$ 또는 $|1\rangle$로 완전히 투영(projection 또는 collapse)되는데 이를 von Neumann 측정이라 한다. 이 경우, 식 (6)의 양자비트가 기저상태 $|0\rangle$ 으로 투영될 때 우리는 양자비트의 상태를 $|0\rangle$으로 추정해야 하고 이 때의 확률은 $P_0 = |\alpha|^2$ 이다. 또 기저상태 $|1\rangle$로 투영될때에는 $P_1 = |\beta|^2$의 확률로 양자비트의 상태를 $|1\rangle$로 추정해야 한다. 따라서 측정을 통해 추정하는 양자상태 ρ_G 를 아래와 같이 정의할 수 있다.

$$\rho_G = P_0|0\rangle\langle 0| + P_1|1\rangle\langle 1|.$$

이로부터 estimation fidelity G_ψ 를 아래와 같이 구할 수 있으며

$$G_\psi = P_0|\langle 0|\psi\rangle|^2 + P_1|\langle 1|\psi\rangle|^2 = |\alpha|^4 + |\beta|^4,$$

양자비트의 pure state에 대한 평균값은 Gavg = 2/3 이다 [7]. 따라서 식 (7)이 등호를 만족할 조건, 즉 최소교란양자측정의 조건으로부터 von Neumann 측정에서의 operation fidelity Favg = 2/3가 되며 이것이 최소교란양자측정에서 F가 가지는 최소값이 된다.

그렇다면 측정을 하지않는 경우와 가장 강한 측정을 하는 사이의 측정은 어떻게 이해할 수 있을까? 이 경우, 양자비트는 computational basis $|0\rangle$과 $|1\rangle$이 아닌 직교하지 않는 두 기저상태를 이용해서 측정되며 이는 Positive

Operator Valued Measurement (POVM)로 이해할 수 있다. 이 경우 정보이득과 상태교란은 측정을 하지 않는 경우와 von Neumann 측정을 하는 경우의 사이값을 가지게 된다. 위의 예제들로로부터 측정을 하지는 않는 경우보다 측정을 하는 경우, 그리고 보다 강한 측정을 할수록 측정을 통한 정보이득은 늘어나지만 상태교란은 더욱 심해짐을 정량적으로 확인할 수 있다.

4. 최소교란양자측정

지금까지 정보이득과 상태교란의 정량화를 통해 최소교란양자측정의 조건을 얻을 수 있었다. 지금부터는 이를 실험적으로 구현하기 위한 실제적인 방법에 대해 알아보자. 최소교란양자측정의 실험적 구현을 위해서는 양자회로(quantum circuit)를 설계할 수 있어야 하므로 먼저 양자회로에 대해 간단히 살펴보도록 하겠다.

4.1 양자회로

고전컴퓨터의 정보처리과정이 전자회로로 구현되듯, 양자컴퓨터를 구현하기 위해서는 그에 해당하는 양자회로를 설계할 필요가 있다. 양자회로의 기본 구성 요소는 wire와 하나의 양자비트에 작용하는 단일 양자게이트 (quantum gate), 여러개의 양자비트에 작용하는 다중양자게이트가 있다 [12]. 양자회로에서 wire는 고전 컴퓨터의 wire처럼 물리적인 wire일 필요는 없으며 시간의 경과나 양자비트의 진행경로를 의미한다.

양자비트가 양자정보를 운반하는 수단이라면 양자게이트는 단일 양자비트의 정보를 바꾸거나 여러개의 양자비트간의 정보를 교류하는 정보처리 과정에 사용된다. 식 (6)에서 정의된 양자비트를 행렬 $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$로 표현하면 단일 양자비트에 작용하는 임의의 양자게이트 U는 2 × 2 행렬로 표현된다. 행렬 연산자가 작용한 후 양자비트의 상태를 $\alpha'|0\rangle+\beta'|1\rangle$라 하면 연산 전후 각각의 양자비트의 규격화 조건 $|\alpha|^2+|\beta|^2 = 1$ 및 $|\alpha'|^2+|\beta'|^2 = 1$ 은 임의의 양자게이트 U가 반드시 $U^\dagger U = 1$의 조건을 만족해야 함을 의미하며 따라서 양자게이트는 반드시 유니터리 행렬로 표현될 수 있어야 한다. 이 유니터리 조건은 양자게이트의 유일한 구속조건이므로 모든 유니터리 행렬은 원칙적으로 양자게이트로 작동할 수 있다.

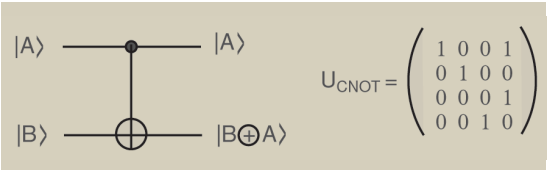

그림 4. 양자비트 |A⟩와 |B⟩ 사이에 작용하는 Controlled-Not (CNOT) 게이트. CNOT 게이트와 단일 양자비트 게이트들을 이용하면 임의의 양자연산이 가능하다.

대표적인 단일 양자게이트로는 X-게이트, Z-게이트, Hadamard-게이트가 있으며 아래와 같이 표현된다.

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}. \quad (8)$$

X-게이트는 $|0\rangle$ ($|1\rangle$)에 있던 양자상태를 $|1\rangle$ ($|0\rangle$)로 바꾸는 역할을 하는 bit-flip 게이트이며 식 (6)의 양자비트가 X-게이트 연산을 겪으면 $\alpha|1\rangle + \beta|0\rangle$상태로 변환된다. Z-게이트는 1의 상태만 선택적으로 부호를 바꾸어 $\alpha|0\rangle - \beta|1\rangle$로 만드는 phase gate이다. Hadamard-게이트는 $|0\rangle$ 또는 $|1\rangle$의 양자비트를 $|0\rangle$과 $|1\rangle$의 양자중첩상태로 만들어 내는 역할을 한다. 따라서 식 (6)의 양자비트는 $\alpha(|0\rangle + |1\rangle)/\sqrt{2} + \beta(|0\rangle - |1\rangle)/\sqrt{2}$ 로 변환된다.

여러개의 양자비트에 작용하는 다중 양자게이트 중 가장 널리 알려진 것에는 두개의 양자비트 사이에 작용하는 controlled-NOT (CNOT) 게이트가 있다. CNOT 게이트는 하나의 양자비트의 상태에 따라 다른 양자비트의 상태를 바꾸거나 그대로 두는 연산이다. 그림 4는 CNOT에 해당하는 양자회로와 행렬연산을 보여준다. 두 개의 양자비트중 $|A\rangle$는 제어양자비트(control quantum bit)로 $|B\rangle$는 표적 양자비트(target quantum bit)로 정의한다. 제어양자비트가 $|0\rangle$일때 표적양자비트는 원래 상태를 유지하고 제어양자비트가 $|1\rangle$일때만 표적양자비트의 상태는 $|0\rangle$ ($|1\rangle$)에서 $|1\rangle$ ($|0\rangle$)로 바뀐다.

Hadamard 게이트를 이용해 양자중첩상태를 만들어 내듯 CNOT 양자게이트를 이용하면 독립적이었던 두 양자비트간에 얽힘상태를 만들어 낼 수 있다. 예를 들어, 제어양자비트를 $|A\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, 표적양자비트를 $|B\rangle = |0\rangle$으로 정의하면 두 양자비트간의 CNOT 연산은 다음과 같은 얽힘 양자상태를 생성한다.

$$(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}. \quad (9)$$

두 양자 비트의 얽힘상태란 전체상태가 더이상 두 양자비트의 단순한 곱으로, 즉 $|A'\rangle \bigotimes |B'\rangle$ 의 형태로 표현될 수 없음을 의미한다. 얽힘상태에 있는 두 양자비트는 공간적으로 멀리 분리되어도 하나의 양자비트가 $|0\rangle$ 또는 $|1\rangle$의 기저 상태로 측정되는 순간 나머지 양자비트의 상태도 $|0\rangle$ 또는 $|1\rangle$ 로 결정되는 즉, 양자비트 A에 대한 측정이 양자비트 B의 결정에 동시에 영향을 주는 비국소적인 성질을 가진다. 이러한 비국소성은 양자역학의 근원적인 검증은 물론 얽힘광원을 이용한 양자암호, 양자통신, 양자전산 등을 가능하게 하는 중요한 양자역학적 성질로 알려져 있다.

4.2 최소교란양자측정을 위한 양자회로

앞에서 알아본 양자회로의 기본요소들을 이용해서 양자비트의 최소교란양자측정을 구현하기 위한 양자회로에 대해 알아보자. 그림 5는 참고문헌 [14]에서 제안된 최소교란양자측정의 양자회로이다. 측정하고자 하는 임의의 양자비트를 시스템 양자비트 $|\psi\rangle_s$로 정의하자. 최소교란양자측정의 기본 아이디어는 모르는 양자상태 $|\psi\rangle_s$를 측정하기 위해 보조 양자비트(ancilla qubit)를 도입하고 이들의 얽힘상태를 생성하는 것이다. 이후 보조 양자비트를 측정하여 시스템 양자비트에 대한 정보를 얻어낼 수 있으며, 이 때 측정의 세기에 따른 정보이득과 상태교란을 앞서 정의된 estimation fidelity (G)와 operation fidelity (F)로 정량화한다. 주어진 양자회로에서 구한 F와 G가 식 (7)의 등호를 만족할 때 제안된 양자회로가 시스템 양자비트에 대한 최소교란양자측정을 구현하는 양자회로로 동작함을 확인할 수 있다.

양자회로에서는 먼저 사용되는 양자상태의 초기화과정이 필요한다. 측정하고자 하는 임의의 시스템 양자비트는

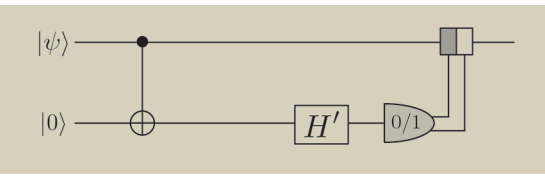

그림 5. 양자비트 $|\psi\rangle$에 대한 최소교란양자측정을 위한 양자회로. 보조양자비트(ancilla)를 도입하여 $|0\rangle$로 초기화한다.

$|\psi\rangle_s = \alpha|0\rangle_s + \beta|1\rangle_s$로 주어지며 이 때 이 양자비트는 규격화 조건 $|\alpha|^2 + |\beta|^2 = 1$을 만족해야 한다. 양자비트의 최소교란양자측정을 위해 보조양자비트(ancilla qubit)를 도입하고 이 보조양자비트는 $|0\rangle_a$ 으로 초기화하였다.

최소교란양자측정을 위한 양자회로는 다음과 같다. 먼저 두 양자비트의 얽힘상태를 생성하기 위해 CNOT 게이트를 가한다. 그 결과 $|\psi\rangle_s \otimes |0\rangle_a$ 의 초기 상태는 아래와 같은 얽힘상태로 변화된다.

$$\alpha|0\rangle_s|0\rangle_a + \beta|1\rangle_s|1\rangle_a$$

다음으로는 보조양자비트에 Hadamard-like 양자게이트를 가한다. 이는 Hadamard 게이트의 닮은꼴로 $H' = \begin{pmatrix} t & r \\ r & -t \end{pmatrix}$의 형태를 띤다. 여기서 t와 r은 규격화 조건 $|t|^2 + |r|^2 = 1$을 만족해야하고 $|t| \geq |r|$을 가정한다. 이후 두 양자비트의 전체상태는 다음과 같이 주어진다.

$$(\alpha t|0\rangle_s + \beta r|1\rangle_s)|0\rangle_a + (\alpha r|0\rangle_s - \beta t|1\rangle_s)|1\rangle_a. \quad (10)$$

보조양자비트의 측정결과에 따라 시스템양자비트의 양자상태를 추정해야 하므로 지금부터 보조양자비트의 측정값이 0이냐 1이냐에 따라 시스템 양자비트의 상태를 $|0\rangle$ 또는 $|1\rangle$에 있는 것으로 추정하기로 약속하자. 먼저 식 (10)에서 $t = r$인 경우 시스템 양자비트는 보조양자비트의 측정결과에 따라 같은 확률로 다른 양자상태에 있게 된다. 보조 양자비트의 측정값이 0일 경우 시스템 양자비트는 원래의 양자상태와 같게되며 보조 양자비트의 측정값이 1일 경우 Z-양자게이트를 시스템 양자비트에 작용함으로써 원래 상태를 완전히 회복할 수 있다. 보조양자비트에 대한 양자측정은 0과 1을 무작위로 (random) 측정결과로 내놓게 되므로 시스템양자비트에 대한 아무런 의미있는 정보도 추정할 수 없게 되며 이는 결국 시스템 양자비트의 양자상태가 전혀 교란되지 않을 것임을 의미한다. 만약 $t \neq r$인 경우 보조양자비트에 대한 측정결과를 이용해 시스템양자비트의 양자상태를 추정할 수 있지만 시스템 양자비트는 더이상 측정이전의 양자상태를 완전히 회복할 수 없게 된다. 이 때 t와 r값은 측정의 세기를 결정하며 측정이 강할수록 정보이득은 증가하고 상태교란은 심해진다.

그렇다면 지금부터 그림 5의 양자회로가 최소교란양자

측정을 만족하는지를 이론적으로 검토해보자. 식 (10)로부터 보조양자비트의 측정값이 0일 확률은 $P_0 = |\alpha|^2 t^2 + |\beta|^2 r^2$이고 1일 확률은 $P_1 = |\alpha|^2 r^2 + |\beta|^2 t^2$임을 알 수 있다. 따라서 측정후 시스템 양자비트의 상태를 0 또는 1로 추정할 확률은 각각 P_0와 P_1이 된다. 그 결과 측정으로부터 추정할 수 있는 시스템 양자비트의 상태는 아래와 같다.

$$\rho_G = P_0|0\rangle_{ss}\langle 0| + P_1|1\rangle_{ss}\langle 1|.$$

이때 시스템 양자비트 $|\psi\rangle_s$에 대한 estimation fidelity는 $G_\psi = {}_s\langle\psi|\rho_G|\psi\rangle_s$이고 이를 Bloch 구 상의 모든 pure state 양자비트에 대해 평균하면 그 값은 다음과 같다.

$$G_{\mathrm{avg}} = \int G_\psi d\psi = \frac{1}{3}(t^2 + 1). \qquad (11)$$

다음으로 측정후의 상태교란을 정량화하는 operation fidelity (F)를 구해보자. 보조양자비트를 측정한 후의 교란된 시스템 양자비트의 상태는 아래와 같다.

$$\rho_F = |\psi_0'\rangle_{ss}\langle\psi_0'| + |\psi_1'\rangle_{ss}\langle\psi_1'|.$$

여기서 $|\psi_0'\rangle_s = \alpha t|0\rangle_s + \beta r|1\rangle_s$이고 $|\psi_1'\rangle_s - \alpha r|0\rangle_s + \beta t|1\rangle_s$이다. 따라서 측정 후의 양자비트가 측정전의 양자비트와 얼마나 닮았는지를 의미하는 operation fidelity는 $F_\psi = {}_s\langle\psi|\rho_F|\psi\rangle_s$로 구해진다. 이를 마찬가지로 Bloch 구 상의 모든 pure state 양자비트에 대해 평균하면 그 결과는 다음과 같다.

$$F_{\mathrm{avg}} = \int F_\psi d\psi = \frac{2}{3}(1 + tr). \qquad (12)$$

여기서 $t = r = 1/\sqrt{2}$인 경우는 시스템 양자비트의 상태를 무작위로 추정하는 경우에 해당하므로 Favg = 1로 주어져 상태교란이 전혀 없음을 확인할 수 있다. 마지막으로 앞의 식 (11)와 식 (12)을 이용해 Favg와 Gavg사이에 다음의 균형관계가 성립함을 확인할 수 있다.

$$F_{\mathrm{avg}} = \frac{2}{3} + \frac{\sqrt{1 - (6G_{\mathrm{avg}} - 3)^2}}{3}. \qquad (13)$$

이는 식 (7)의 등호에 해당하는 조건으로 제안하는 양자회로가 최소교란양자측정의 조건을 잘 만족함을 의미한다.

5. 단일광자 양자비트에 대한 최소교란양자측정

지금까지 모든 일반적인 양자비트에 대해 적용 가능한 최소교란양자측정 회로에 대한 아이디어를 소개하였다. 이번 장에서는 앞장에서 소개한 최소교란양자측정을 단일광자 양자비트에 대해 구현하는 실험을 소개한다.

5.1 단일광자 양자비트 생성

단일광자 기반의 양자비트는 양자통신, 양자전산 등 양자정보분야의 다양한 실험연구에 유용하게 사용될 수 있다. 단일광자 양자비트를 구현하기 위해서는 단일광자의 편광, 위상, 경로, 시간 등의 자유도를 제어하고 측정할 수 있어야 한다. 본 연구에서는 자발매개하향변환(Spontaneous parametric downconversion: SPDC)과정을 이용한 Heralded single-photon source (HSPS)를 이용하여 단일광자를 구현하였고 편광상태를 이용하여 단일광자 양자비트를 구현하였다.

먼저 HSPS를 간단히 기술하면 아래와 같다. 2차 비선형 결정에 주파수 ω_p의 에너지를 가지는 펌프광원이 주입되면 에너지와 운동량 보존을 만족하는 범위에서 주파수 ω_1과 ω_2를 가지는 광자쌍이 SPDC 과정을 통해 생성되며 이 광자쌍의 양자상태는 아래와 같다.

$$|\Psi\rangle = \int d\omega_1 d\omega_2 S(\omega_1, \omega_2)|\omega_1, \omega_2\rangle \qquad (14)$$

여기서 $|S(\omega_1, \omega_2)|^2$는 ω_1, ω_2의 광자 2개가 동시에 생성될 확률을 의미한다 [15]. 두 광자의 에너지는 $\omega_1 + \omega_2 = \omega_p$를 항상 만족하므로 생성된 광자쌍의 에너지 및 생성시간은 서로 얽힘상태에 있다. SPDC 광자쌍은 항상 동시에 생성되므로 두 개의 광자중 하나를 검출기로 바로 보내 트리거(trigger) 신호로 사용하면 짝을 이루는 나머지 광자에 대해 조건부적으로 단일광자 상태를 만드는 것이 가능하며 이를 heralded single-photon source (HSPS)라고 부른다. SPDC 과정에 기반한 HSPS는 광자의 파장과 선폭제어가 쉽고 진행방향이 잘 정의되며 오랜시간 안정적으로 유지되기 때문에 효과적인 단광자 광원으로 널리 쓰이고 있다 [16, 17, 18].

그림 6은 최소교란양자측정을 실험적으로 구현하기 위

한 장치도이다. SPDC 과정으로 생긴 광자쌍에서 하나의 광자는 트리거 신호로 사용하고 나머지 광자는 최소교란 측정을 위한 양자비트로 사용한다. 양자비트를 생성하기 위해 단광자의 편광상태를 이용하였다. 생성된 단광자를 광섬유 편광 조절판(fiber polarization controller, FPC)과 편광판(polarizer, Pol)을 통과시켜 초기 편광상태를 수직 편광으로 정의해준다. 이후 파장판(wave plate, WP)을 이용해 시스템 양자비트 $|\psi\rangle_s = \alpha|H\rangle_s + \beta|V\rangle_s$ 를 준비한다.

앞에서 제안된 최소교란양자측정을 구현하기 위해서 보조양자비트가 필요한데 본 실험에서는 시스템 양자비트로 사용된 단광자의 또 다른 자유도인 경로(path)를 보조양자비트로 도입하였다. 따라서 단광자가 어느 경로로 진행하느냐에 따라 보조양자비트의 값이 $|0\rangle$ 또는 $|1\rangle$로 정해지고 두 경로를 동시에 지날 확률이 있을 때 보조양자비트는 $|0\rangle$과 $|1\rangle$의 중첩상태로 표현된다. 그림 6에서 각 경로에 표시된 0과 1이 보조 양자비트의 값을 의미한다. 파장판을 통과한 단일광자를 경로 0으로 보냄으로써 보조 양자비트의상태는 $|0\rangle$으로 초기화 되었다. 이로써 두 양자비트의 전체 상태는 $|\psi\rangle_s \otimes |0\rangle_a$ 로 초기화된다.

5.2 최소교란양자측정의 회로의 구현

최소교란양자측정의 다음 단계는 시스템 양자비트와 보조양자비트 사이에 CNOT 게이트를 작용시켜 얽힘상태를 만드는 것이다. 단일광자의 편광과 경로를 이용한 두 양자비트간의 CNOT 게이트는 편광빔분할기(polarizing beam splitter, PBS)를 이용해 구현가능하다. 편광 분할기는 수직편광은 반사시키고 수평 편광은 통과시키므로 편광 분할기를 통과한 후 단일광자의 양자상태는 시스템 양자비트(편광)와 보조양자비트(경로)간의 얽힘상태로 주어지며 아래와 같다.

$$\alpha|H\rangle_s|0\rangle_a + \beta|V\rangle_s|1\rangle_a.$$

CNOT게이트의 다음 단계로 Hadamard-like 양자게이트를 보조 양자비트에 작용하여야 하는데 이는 제어가능한 t와 r값을 가지는 가변 빔분할기(variable beam splitter, VBS)를 포함한 Mach-Zehnder 간섭계를 이용해 구현 가능하다. 가변 빔분할기는 경로 0과 1에 놓인 반파장판과 편광분할기로 구성되며 반파장판의 광축을 각각 φ 와 $\varphi + \pi/4$ 를 놓았을 때 H′의 변수는 $t = \cos 2\varphi$ 와 $r = \sin 2\varphi$ 로 정의된다. 따라서 반파장판의 각도를 조절하여 양자측정의 세기를 제어하는 것이 가능하다.

마지막으로 시스템 양자비트의 양자상태를 추정하는 방법은 다음과 같다. 가변 빔분할기의 출력 모드에서 단광자가 경로 0에서 검출될 때 보조양자비트의 상태는 0일 것이며 이 경우 시스템 양자비트는 $|0\rangle$ 즉, 수평 ($|H\rangle$) 편광상태에 있다고 추정하기로 앞에서 약속하였다. 이 때 경로 0으로 가는 시스템 양자비트의 실제 상태는 $\alpha t|H\rangle + \beta r|V\rangle$이다. 이는 초기 상태 $\alpha|H\rangle + \beta|V\rangle$와 다르므로 보조양자비트에 대한 측정이 곧 시스템 양자비트에 상태교란을 일으킴을 의미한다(실험적으로 보조양자비트에 대한 측정은 단일광자가 출력모드 0 또는 출력모드 1에서 검출되는 것을 의미한다).

마찬가지로 출력모드 1에서 단일광자가 검출되는 경우 시스템 양자비트는 $|1\rangle$ 즉, 수직 ($|V\rangle$) 편광상태에 있는 것으로 추정하며 실제 편광 상태는 $\beta t|H\rangle + \alpha r|V\rangle$ 가 된다. 이 경우, 시스템 양자비트의 양자상태를 측정 전의 상태와 유사하게 만들기 위해 X-게이트를 가하도록 한다. X-게이트는 광축이 수직과 45도를 이루는 반파장판을 이용해 구현 가능하다.

교란된 양자상태가 원래의 양자상태와 얼마나 비슷한지를 실험적으로 알아보기 위해 파장판, 편광 빔분할기, 단광자 검출기로 구성된 편광분석 장치를 이용해 시스템 양자비트의 양자상태를 측정한다. 각 출력모드 $\imath$ ($\imath$ = 0, 1)에서 시스템 양자비트를 초기 상태인 $|\psi\rangle$ 와 그에 수직

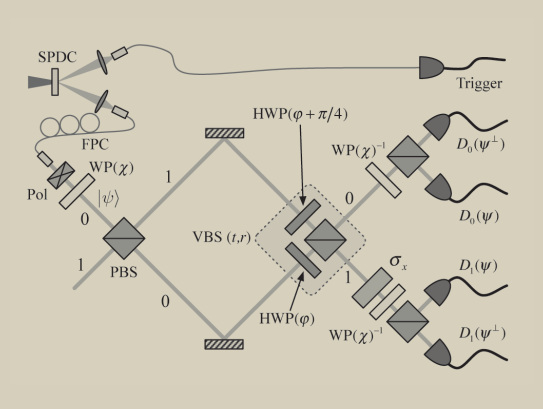

그림 6. 단일광자 양자비트에 대한 최소교란양자측정 실험장치. 첫번째 PBS는 시스템양자비트(편광)와 보조양자비트(경로)간의 CNOT 게이트에 해당하며 이들 양자비트간의 얽힘상태를 생성한다. VBS는 보조양자비트에 대한 H′ 게이트에 해당한다.

한 기저상태인 $|\psi^{\perp}\rangle$로 투영측정하며 그 결과를 단광자 검출기 $D_i(\psi)$와 $D_i(\psi^{\perp})$로 기록한다. 시스템 양자비트의 상태교란이 전혀 없다면 원칙적으로 단광자는 항상 $D_i(\psi)$ 검출기에서 측정될 것이다. 하지만 정보이득에 따른 상태교란이 있는 경우, 즉 $t \neq r$ 의 경우, $D_i(\psi^{\perp})$에서도 단광자가 검출될 것이며 이를 이용하여 정보이득과 상태교란의 상관관계를 실험적으로 연구할 수 있다.

5.3 *F*-*G* 값의 실험적인 정량화

그림 6의 실험장치가 단일광자 양자비트에 대해 최소교란양자측정을 잘 구현하는지를 확인하기 위해서는 operation fidelity와 estimation fidelity를 실험값으로 정량화하고 이들간의 균형관계를 구해야 한다.

최소교란측정의 균형관계를 알아보기 위해서는 측정의 세기를 변화시키며 operation fidelity와 estimation fidelity를 구해야 하는데 이를 위해 가변 빔분할기에 들어있는 파장판의 각도 φ 를 22.5°에서 0°까지 단계적으로 변화시키면서 실험을 하였다. 파장판의 각도 $\varphi = 22.5°$인 경우 $t = r = 1/\sqrt{2}$ 이므로 H'은 Hadamard 게이트로 작동하고 이 경우가 시스템 양자비트의 상태를 무작위로 추정하는 경우에 해당한다. 반면 $\varphi = 0°$의 경우는 von Neumann측정에 해당하며 정보이득과 상태교란 모두가 가장 큰 측정이 된다.

실험에서는 시스템 양자비트를 $|\psi\rangle_s$로 초기화하고 4개의 검출기 $D_i(\psi)$, $D_i(\psi^{\perp})$와 트리거 검출기의 동시계수를 주어진 시간 동안 측정한다. 각 검출기의 동시계수 $N_i(\psi)$, $N_i(\psi^{\perp})$로부터 규격화된 동시계수 $n_i(\psi) = N_i(\psi)/N_{tot}$를 구할 수 있고 이를 이용해 operation fidelity $F_\psi = \langle\psi|\rho_F|\psi\rangle = n_0(\psi) + n_1(\psi)$와 estimation fidelity $G_\psi = \langle\psi|\rho_G|\psi\rangle = P_0|\langle H|\psi\rangle|^2 + P_1|\langle V|\psi\rangle|^2$를 구한다. 여기서 $P_i = n_i(\psi) + n_i(\psi^{\perp})$로 정의된다. Operation fidelity와 estimation fidelity의 평균값을 구하기 위해서는 F_ψ와 G_ψ를 Bloch 구상에 모든 pure state 상태에 대해 평균해야 한다. 실험적으로 무한개의 양자상태에 대해 측정을 하는 것은 불가능하나 Bloch 구 표면에 모든 6개 대표 양자상태인 $|H\rangle, |V\rangle, |L\rangle = |H\rangle + i|V\rangle, |R\rangle = |H\rangle - i|V\rangle, |D\rangle = |H\rangle + |V\rangle, |A\rangle = |H\rangle - |V\rangle$에 대해 평균을 할 경우 모든 pure state에 대한 평균과 동일한 값을 준다는 것이 알려져 있다. 따라서 실험에서는 위의 6개 대표 양자상태에 대한 F_ψ와 G_ψ 값을 이용해 *G*avg와 *F*avg를 구하였다. 이 실험의 결과는 그림 7에 나타나 있으며 본 측정장치가 단일광자 양자비트에 대해 최소교란양자측정을 구현함을 보여준다.

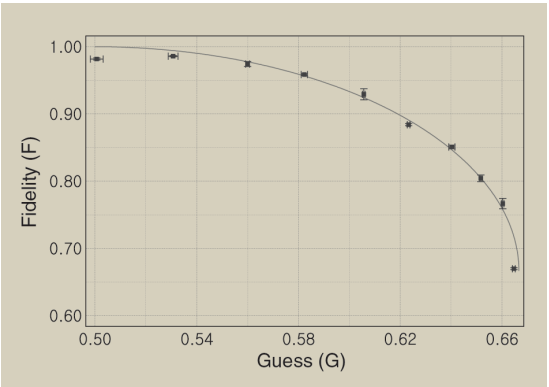

그림 7. *F*와 *G*의 균형관계. 실험으로 얻은 Gavg와 Favg가 이론적인 값(실선)에 잘 근사함을 확인할 수 있다.

6. 결론

이 글에서는 양자역학에서 양자측정이 무엇을 의미하는지를 되돌아 보았고 양자측정이 최근 많이 연구되고 있는 양자정보에 어떠한 영향을 미치는지를 간단히 소개하였다. 특히 양자정보의 기본단위인 양자비트에 대해 측정을 통해 얻게 되는 정보이득과 양자상태의 교란과의 상관관계를 보였고 최소교란양자측정이라는 개념을 소개하였다. 또 최소교란양자측정을 구현하는 일반적인 양자회로를 보였고 단일광자 양자비트에 대해 최소교란양자측정을 어떻게 구현할 수 있는지를 자세히 설명하였다. 이 글에서 소개한 단일광자 양자비트에 대한 최소교란양자측정은 선형광학계를 사용하였고 이론적인 성공확률이 100%이므로 양자통신 및 양자암호 분야의 연구에 응용될 수 있을 것으로 생각한다 [19]. 또 d- 차원의 양자상태에 대해 확장가능할 것으로 예상하고 있다.

최소교란양자측정은 양자역학의 기본원리인 불확정성원리를 양자정보의 관점에서 새롭게 조명할 수 있게 해주며 측정 즉, 정보이득의 한계를 측정에 의한 양자상태교란 및 양자상태의 차원(dimension)과 연관지어준다. 뿐만 아니라 최소교란양자측정은 측정에 의한 정보이득과 상태교

란과의 관계를 정량화 해주기 때문에 많은 수의 양자비트를 이용한 양자정보 실험 및 이론 연구에 유용하게 사용될 수 있을 것으로 생각한다.

참 고 문 헌

[1] A. Peres, Quantum Theory: Concepts and Methods (Kluwer, Dordrecht, 1995).
[2] W. Heisenberg, The Physical Principles of the Quantum Theory (Dover, New York, 1930).
[3] M.O. Scully and K. Drühl, Phys. Rev. A 25, 2208 (1982).
[4] Y.-H. Kim et al., Phys. Rev. Lett. 84, 1 (2000).
[5] W.K. Wooters and W.H. Zurek, Phys. Rev. D 19, 473 (1979); L.S. Bartell, ibid., 21, 1698(1980); B.-G. Englert, Phys. Rev. Lett. 77, 2154 (1996); P.D.D. Schwindt, P.G. Kwiat, and B.-G. Englert, Phys. Rev. A 60, 4285 (1999).
[6] E. Knill, R. Laamme, and G. J.Milburn, Opt. Express, Nature (London) 409, 46 (2001).
[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[8] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Rev. Mod.Phys. 79, 135 (2007).
[9] S. Massar and S. Popescu, Phys. Rev. Lett. 74, 1259 (1995).
[10] D. Bruss and C. Macchiavello, Phys. Lett. A 253, 149 (1999).
[11] C.A. Fuchs and A. Peres, Phys. Rev. A 53, 2038 (1996).
[12] M.A. Nielsen and I.L. Chuang, Quantum Computation and Quantum Information (Cambridge, 2000).
[13] K. Banaszek, Phys. Rev. Lett. 86, 1366 (2001).
[14] S.-Y. Baek, Y.W. Cheong, Y.-H. Kim, Phys. Rev. A 77, 060308(R) (2008).
[15] S.-Y. Baek and Y.-H. Kim, Phys. Rev. A 77, 043807 (2008).
[16] S.-Y. Baek and Y.-H. Kim, Phys. Rev. A 78, 013816 (2008).
[17] C.K. Hong and L. Mandel, Phys. Rev. Lett. 56, 58 (1986).
[18] S.-Y. Baek, O. Kwon, and Y.-H. Kim, Phys. Rev. A 77, 013829 (2008).
[19] F. Sciarrino, M. Ricci, F. De Martini, R. Filip, and L. Mista, Phys. Rev. Lett. 96, 020408(2006).

약 력

백소영

2004년 포항공과대학교 학사과정을 졸업하고 현재까지 포항공과대학교에서 박사과정을 밟고 있으며 2010년 2월 박사학위 수여예정이다.

E-mail : simply@postech.ac.kr

약 력

김윤호

2001년 Univ of Maryland, Baltimore County에서 양자광학 실험으로 박사학위를 받은 후 2004년까지 Oak Ridge National Laboratory에서 Eugene P. Wigner Fellow로 근무하였다. 현재 포항공과대학교 물리학과에 재직중이다.

E-mail : yoonho@postech.ac.kr