

ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ENTROPİK BELİRSİZLİK BAĞINTILARI VE KUANTUM BİLİŞİM
KURAMINDAKİ BAZI UYGULAMALARI

Alptuğ ÖZDEMİR

FİZİK ANABİLİM DALI

ANKARA
2021

Her hakkı saklıdır

ÖZET

Yüksek Lisans Tezi

ENTROPİK BELİRSİZLİK BAĞINTILARI VE KUANTUM BİLİŞİM KURAMINDAKİ BAZI UYGULAMALARI

Alptuğ ÖZDEMİR

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Fizik Anabilim Dalı

Danışman: Prof. Dr. Abdullah VERÇİN

Entropik belirsizlik bağıntıları (EBB), uzun zaman önce Heisenberg belirsizlik bağıntılarına alternatif olarak ortaya atılmıştır. Son yıllarda ivme kazanan, yoğun çalışılan ve uygulama alanları oldukça geniş bir konudur. Belirsizliği nicelendirilen entropinin standart sapmayla yer değiştirmesi, bu bağıntıların özellikle kuantum kriptoloji, dolanıklık tanıklıkları, koherenslik ve kuantum diskord gibi bir çok konuya uygulanmasını sağlamıştır. Bilişim süreçlerinde, sisteme uygulanan uyumsuz (sıra değişmeyen) ölçümler arasında oluşan belirsizlikler için daha tutarlı ve sıkı (indirgenemez) alt sınırlar elde edilmesini sağlamıştır. Bu çalışmada öncelikle bir hafıza sistemine sahip olmayan sistemler için EBB ele alınmış, aynı zamanda bu bağıntıların tarihsel gelişimi incelenmiştir. Daha sonra bir hafıza sistemi varlığında bağıntıların nasıl geliştiği, elde edilen alt sınırların değişimleri ve kuantum korelasyonların uyumsuz ölçümler arasındaki belirsizlikler üzerine etkileri ele alınmıştır. Son olarak, bu bağıntıların bazı güncel uygulama alanları incelenmiştir.

Temmuz 2021, 88 sayfa

Anahtar Kelimeler: belirsizlik, entropi, ölçüm, kuantum bilişim, kuantum kriptografi, belirsizlik bağıntıları

ABSTRACT

Master Thesis

ENTROPIC UNCERTAINTY RELATIONS and SOME APPLICATIONS in QUANTUM INFORMATION THEORY

Alptuğ ÖZDEMİR

Ankara University
Graduate School of Natural and Applied Sciences
Department of Physics

Supervisor: Prof.Dr. Abdullah VERÇİN

Entropic uncertainty relations (EURs) have long been proposed as an alternative to Heisenberg uncertainty relations. In recent years, the subject has gained momentum, intensive study and application areas. With the replacement of entropy, quantifying the uncertainty, with standard deviation, these relations have been applied to many subjects such as quantum cryptology, entanglement witnessing, coherence and quantum discord. It has provided that more consistent and tight lower limits are obtained for the uncertainties between the measurement that will be applied to the system in the information processes. In this study, firstly, EURs are considered for systems that do not have a memory system, and the historical development of these relations is reviewed. Secondly, development of EURs, variations of lower bound and the effects of the quantum correlations on the uncertainties between incompatible measurements are discussed in the presence of a memory system. Finally, some current application areas of these relations are examined.

July 2021, 88 pages

Key Words: uncertainty, entropy, measurement, quantum information, quantum cryptography, uncertainty relations.

TEŞEKKÜR

Çalışmalarımı yönlendiren, araştırmalarımın her aşamasında bilgi, öneri ve desteklerini esirgemeyen, akademik alanda olduğu kadar hayat tecrübesi ile de her zaman ilerlediğim yola ışık tutan ve kendimi geliştirmeme fırsat tanıyan danışman hocam sayın Prof. Dr. Abdullah VERÇİN'e (Ankara Üniversitesi Fizik Anabilim Dalı), çalışmalarım süresince maddi ve manevi desteklerini esirgemeyen sayın Dr. Adem TÜRKMEN'e (Ordu Üniversitesi Fizik Anabilim Dalı) ve sevgili aileme en derin duygularıyla teşekkür ederim.

Alptuğ ÖZDEMİR
Ankara, Temmuz 2021

İÇİNDEKİLER

TEZ ONAY SAYFASI

ETİK	i
ÖZET	ii
ABSTRACT	iii
TEŞEKKÜR	iv
SİMGELER DİZİNİ	vii
ŞEKİLLER DİZİNİ	ix
1. GİRİŞ	1
2. ÖN HAZIRLIK	6
2.1 Standart Sapma	6
2.1.1 Standart sapmanın sezgi karşıtı davranışları	7
2.2 Ölçüm	9
2.2.1 İzdüşüm işlemcileri	10
2.2.2 Pozitif-operatör değerli ölçü (POVM)	11
2.3 Entropi.	12
2.3.1 Klasik bilişimde entropi: Shannon entropisi	12
2.3.2 Kuantum bilişimde entropi: von Neumann entropisi	15
2.3.3 Rényi entropisi	17
3. BİR HAFIZA SİSTEMİ OLMADAN EBB	19
3.1 Shannon Entropisi ile EBB.	19
3.2 Rényi Entropisi ile EBB.	22
3.3 Daha Sıkı Bir Sınır: Kübitler	22
3.4 Daha Sıkı Bir Sınır: Saf Olmayan Durumlar	24
3.5 Daha Sıkı Bir Sınır: Keyfi boyutlar	26
3.6 POVM ile Keyfi Ölçümler	27
3.7 Çoğullama Yaklaşımı ve EBB.	29
3.8 Tahmin Oyunu	30
3.9 Çoklu Ölçüm Kümeleri.	31
4. BİR HAFIZA SİSTEMİ VARLIĞINDA EBB	34
4.1 Klasik ve Kuantum Hafıza	34
4.2 Koşullu Entropiler.	36
4.3 Klasik Hafıza Varlığında EBB	38
4.4 Kuantum Hafıza Varlığında EBB	39
4.4.1 İki-parçalı sistemler.	40
4.4.2 Üç parçalı sistemler.	42
4.4.3 Hafıza varlığında çoklu ölçüm kümeleri	45
4.5 Bilişim Dışarlama Prensibi.	45
4.6 Kuantum Kanal Yaklaşımı	46
4.7 Kuantum Hafıza Varlığında Tahmin Oyunu	47

5. UYGULAMALAR	51
5.1 Kuantum Anahtar Dağıtımı	51
5.2 Dolanıklık Tanıkları	53
5.2.1 Shannon entropik tanıkları	54
5.2.2 Diğer entropik tanıklar	55
5.3 Steering Eşitsizlikleri	56
5.4 Dalga-Parçacık İkiliği	57
5.5 Koherenslik	59
5.6 Diskord	60
5.7 Klasik Korelasyonların Kilitlenmesi	61
6. SONUÇ	62
KAYNAKLAR	64
EK 1 SHANNON ENTROPİSİNİN EN BÜYÜK DEĞERİ VE BA- ĞIL ENTROPİNİN POZİTİFLİĞİ	67
EK 2 RÉNYİ ENTROPİSİNİN MONOTONLUĞU ve LİMİTLERİ	70
EK 3 İKİ OLASILIĞIN ÇARPIMININ EN BÜYÜK DEĞERİ . .	73
EK 4 RİEZE-THORİN İÇ-UZANIM (İTERPOLASYON) TEOREMİ ve MU SINIRININ İSPATI	74
EK 5 HAFIZALI DURUMDA ÜÇ PARÇALI SİSTEMLER İÇİN EBB	77
EK 6 COLES - PİANİ SINIRI	80
EK 7 KARŞILIKLI YANSIZ BAZLAR	84
ÖZGEÇMİŞ	88

SİMGELER DİZİNİ

$\hat{q}, \hat{p}$	Sırasıyla konum ve momentum işlemcileri
X, Y, Z, M	Gözlenebilirler (ölçüm işlemcileri)
Θ	Ölçüm kümesi
K^k, L^l	Alice'nin ölçüm kümesinin elemanları
$\sigma(X)$	X değişkeni için standart sapma
$[,]$	Sıra değişim (komütasyon) bağıntısı
$\{ , \}$	Anti-sıra değişim (anti-komütasyon) bağıntısı
$(\cdot)^T$	Transpoz işlemi
$ \psi\rangle$	Durum vektörü
ρ	Yoğunluk işlemcileri (matrisleri)
$\tilde{\rho}$	Genişletilmiş uzaydaki yoğunluk işlemcisi (matrisi)
P_i	İzdüşüm işlemcileri (von Neumann ölçümleri)
E_m	POVM elemanları olan pozitif işlemciler
ρ_{AB}	Alt sistemleri A ve B olan iki parçalı bir sistemin yoğunluk işlemcisi
ρ_A, ρ_B	İki parçalı sistemin indirgenmiş yoğunluk işlemcileri
$\sigma_X, \sigma_Y, \sigma_Z$	Pauli işlemcileri (matrisleri)
$ x\rangle, z\rangle$	Bazlar
F	Fourier dönüşümü
Tr	İz işlemi
$ 0\rangle, +\rangle$	Spin-yukarı durumu (Sırasıyla σ_Z ve σ_X için)
$ 1\rangle, -\rangle$	Spin-aşağı durumu (Sırasıyla σ_Z ve σ_X için)
$ \phi^\pm\rangle, \psi^\pm\rangle$	Bell (veya EPR) durumları
U_k, U_l	Üniter dönüşüm işlemcileri (matrisleri)
$\mathbb{1}$	Birim işlemci (birim matris)
d	Çalışılan uzayın boyutu
$\mathcal{H}, \mathcal{K}$	Hilbert uzayı
$\tilde{\mathcal{H}}, \tilde{\mathcal{K}}$	Genişletilmiş Hilbert uzayı
$B(\mathcal{H}^d)$	Hilbert uzayı $\mathcal{H}^d$ 'de tanımlı çizgisel dönüşümlerin uzayı
$\mathbb{C}^d$	d boyutlu kompleks vektör uzayı
$\mathbb{R}^d$	d boyutlu gerçel vektör uzayı
$\ \mathbf{x}\ _p$	Operatör p-norm
$ A $	A kümesinin kardinalitesi
$p(x)$	Çıktıları x olan rasgele bir X değişkeni için olasılık
$p(x, y)$	Çıktıları x ve y olan rasgele X ve Y değişkenleri için bileşik olasılık
$p(x y)$	y 'nin verilmesi durumunda x 'in koşullu olasılığı
$p_Q(q)$	Gaussiyen olasılık dağılımı
$p_{tahm}(X)$	En yüksek tahmin olasılığı
$p_{\text{çarp}}(X)$	Çarpışma olasılığı
p_{tahm}^{pg}	Oldukça iyi tahmin olasılığı
$H(X)$	Shannon entropisi
$H(XY)$	Bileşik sistemin Shannon entropisi
$H(X Y)$	Koşullu Shannon entropisi
$I(X; Y)$	Klasik karşılıklı bilişim

$h(Q)$	Diferansiyel entropi
$h_{bin}(X)$	İkili (<i>binary</i>) entropi
$S(\rho)$	ρ yoğunluk işlemcisinin kuantum (von Neumann) entropisi
$S(\rho_{AB})$	İki parçalı bir AB sisteminin kuantum entropisi
$S(A B)$	Kuantum koşullu entropi ($S(A B) = S(AB) - S(A)$)
$I(A; B)$	Kuantum karşılıklı bilişim ($I(A; B) = S(A) + S(B) - S(AB)$)
$D(\rho \sigma)$	Kuantum bağıl entropi
$H_\alpha(X)$	Rényi entropisi
$H_\infty(X)$	Min entropi
$H_2(X)$	Çarpışma entropisi
c	Çakışma matrisinin en büyük elemanı
$F(\rho, \sigma)$	Öz uygunluk (<i>fidelity</i>)
$\mathcal{E}, \mathcal{F}, \mathcal{X}, \mathcal{Z}$	Kuantum kanallar
I_{coh}	Koherent bilişim
$\chi(\mathcal{E}, X)$	Holevo niceliği
$D_A(\rho_{AB})$	Kuantum diskord
$J_A(\rho_{AB})$	En büyük klasik karşılıklı bilişim miktarı
E_X, E_Z	Hata işlemcileri
E_D	Damıtılabilir dolanıklık
$\mathcal{V}, \mathcal{P}, \mathcal{D}$	Işığın dalga-parçacık tahmin edilebilirliği
$\Phi(Z, \rho)$	Koherent durumların damıtılma miktarı
q_D	Deutsch Sınırı
q_{MU}	Maasen-Uffink Sınırı
q_{CP}	Coles-Piani Sınırı
q_{SR}	Sanchez-Ruiz Sınırı
r_H	Hall üst sınırı
r_{CP}	Coles Piani üst sınırı
$\mathbf{p}, \mathbf{q}, \mathbf{w}$	Olasılık vektörleri

Kısaltmalar:

CPTP	Tamamen pozitif ve iz koruyan (<i>Completely positive and trace preserving</i>)
EBB	Entropik belirsizlik bağıntıları
EPR	Einstein-Podolski-Rosen
KYB	Karşılıklı yansız bazlar
KYLK	Karşılıklı yansız $s \times s$ Latin kareleri
MU	Maasen-Uffink
QKD	Kuantum anahtar dağıtımı (<i>Quantum key distribution</i>)
POVM	Pozitif operatör-değerli ölçü (<i>Positive operator-valued measure</i>)

ŞEKİLLER DİZİNİ

Şekil 2.1	A sistemi	8
Şekil 2.2	B sistemi.	8
Şekil 4.1	Klasik hafıza; bir madeni para ile bir spin-1/2 parçacığı arasında klasik korelasyonlar olarak gibi tasvir edilebilir. (Coles v.d 2017)	34
Şekil 4.2	Kuantum hafıza; bir elektronun spininin X ve Z bileşenlerinin başka bir elektronun spininin X ve Z bileşenleri ile korelasyon halinde olması gibi tasvir edilebilir. Böylece sağdaki elektron bir kuantum hafıza, kuantum yan bilişim olur.	35
Şekil 5.1	Belirtilmiş çizgilerin altın kalan bölgeler dolanıklığın mevcut olduğu bölgeler olarak görülmektedir. (Coles v.d 2017)	54
Şekil 5.2	Tek foton için Mach-Zender interferometresi. Fotonun aldığı yol Z 'nin bazıları $\{ 0\rangle, 1\rangle\}$ ile etiketlenmiştir. E ise fotonun çevresini temsil etmektedir. Bir faz ϕ alt kola uygulanmış ve fotonun alabileceği iki yol ikinci ışın ayırıcıya (<i>beam splitter</i>) gelmektedir. En son olarak gelen foton dedektörler D_0 veya D_1 'den birinde tespit edilir (Coles v.d 2017).	57
Şekil 7 .1	3×3 karşılıklı yansız Latin kareleri	85

1. GİRİŞ

Kuantum mekaniğinin uygulamaları, kuramın keşfinin ilk yıllarından bu zamana kadar bir çok alana yayılmış ve teknolojiye önemli ölçüde nüfuz etmiştir. Klasik mekanik gibi kuantum mekaniği de kendi bilişim kuramına evrilmiş ve bilim insanları bunun üzerine yıllar boyunca sürecektir tartışmalar, üzerine düşünülmesi gereken problemler, kullanılabilir teknolojiler ortaya koymuştur. Günümüzde *Kuantum Bilişim Kuramı* (*Quantum information theory*) artık teorik fiziğin bir konusu olduğu kadar deneysel fiziğin de öncü alanlarından biri haline gelmiştir. Devletler, üniversiteler, enstitüler ve hatta özel şirketler bu teknolojileri üretebilmek için büyük bir yarış içine girmiş, bunun sonucu olarak da bu kuramın ürünleri kullanılabilir olmaya başlamıştır.

Ancak ulaşılan teknolojiler ve kullanılan deney aletleri ne kadar gelişirse gelişsin, kuantum mekaniğinin doğası gereği sıra değişmeyen (uyuşumsuz, komüte etmeyen) gözlenebilirler arasında belirsizlik olduğu bilinmektedir. Bu, Heisenberg (1927) tarafından ortaya konulan ve kendi adıyla bilinen *Heisenberg belirsizlik bağıntıları* ile şöyle ifade edilir: Eğer bir parçacığın konumu yüksek doğrulukla belirlenmek istenirse, momentumundaki belirsizlik o kadar artar veya tam tersi. Matematiksel olarak kabaca;

$$\sigma(\hat{q})\sigma(\hat{p}) \sim h, \quad (1.1)$$

şeklinde yazılabilir. Burada, $\hat{q}$ ve $\hat{p}$ işlemcileri sırasıyla konum ve momentum işlemcileri, $\sigma(\hat{q})$ ve $\sigma(\hat{p})$ sırasıyla konum ve momentumdaki belirsizlikler (standart sapmalar) ve h , Planck sabitidir. Kennard (1927) ve Weyl (1928), belirsizlik bağıntılarının aşağıdaki eşitsizlik formunu ortaya koymuşlardır,

$$\sigma(\hat{q})\sigma(\hat{p}) \geq \hbar/2. \quad (1.2)$$

Robertson (1929), bu bağıntıları sadece konum ve momentum için değil bütün sıra değişmeyen gözlenebilirler için bir genellemesi olduğunu göstermiştir,

$$\sigma(X)\sigma(Z) \geq \frac{1}{2}|\langle\psi|[X, Z]|\psi\rangle|. \quad (1.3)$$

Daha sonra, Schrödinger (1930) şunu göstermiştir,

$$\sigma(X)\sigma(Z) \geq \sqrt{\left(\frac{1}{2}\langle\{X, Z\}\rangle - \langle X\rangle\langle Z\rangle\right)^2 + \left(\frac{1}{2i}\langle[X, Z]\rangle\right)^2}. \quad (1.4)$$

Bu çalışmalardan sonra belirsizlik bağıntıları üzerine Heisenberg'in orijinal fikri kalıcı olmuş ve çalışmalar daha genel, güçlü ve sıkı (parametrelere göre değişmeyen, indirgenemez, *tight*) bir alt sınır bulmaya yönelik olmuştur. Ancak standart sapma, sezgi karşıtı (*counterintuitive*) davranışlar göstermektedir. Bu iddaa Bölüm 2'de incelenecektir. Elde edilen bağıntıların sağ tarafının gözlenebilirliğe göre değişken olması da daha kullanışlı belirsizlik ölçülerinin gerekliliğini doğurmuştur.

Everett (1957), bu konu ile ilgili bilim dünyasına “Belirsizliği nasıl ölçebiliriz?” sorusunu yöneltmiş, Hirschmann (1957) cevap olarak Shannon'un ünlü *Komünikasyon'un Matematiksel Bir Temeli* (1948) isimli makalesinde ele aldığı, belirsizliğin bir ölçüsü olan entropiyi önermiş ve Entropik Belirsizlik Bağıntıları'nın (EBB) ilk formunu ortaya koymuştur. Daha sonra Białynicki-Birula ve Mycielski (1975), EBB ile Heisenberg belirsizlik bağıntılarının ilişkili olduğunu göstermiştir. Bir gaussiyen olasılık dağılımı differansiyel entropiyi maksimize eder¹ ve çalışmalarında aşağıdaki sonuca ulaşmışlardır²,

$$h(\hat{q}) + h(\hat{p}) \geq \log(e\pi\hbar). \quad (1.5)$$

$h(\hat{q})$ diferansiyel entropi şöyle tanımlanır,

$$h(\hat{q}) := \int p_{\hat{q}}(q) \log(p_{\hat{q}}(q)) dq. \quad (1.6)$$

Gaussiyen olasılık dağılımı ise şöyle ifade edilir,

$$p_{\hat{q}}(q) = \frac{1}{\sqrt{2\pi\sigma(\hat{q})^2}} \exp\left(\frac{-(q - \bar{q})^2}{2\sigma(\hat{q})^2}\right). \quad (1.7)$$

Burada $\bar{q}$ konumun beklenen değerini tanımlamaktadır ve benzer bir dağılım fonksiyonu momentum için de yazılabilir. Gaussiyen dağılımlar sürekli olasılık dağılımlarıdır, yani $p_{\hat{q}}(q) \geq 0$ ve $\int p_{\hat{q}}(q) dq = 1$ şartlarını sağlarlar. Dağılım içerisinde yer alan varyans (standart sapmanın karesi, $\sigma(\hat{q})^2$) terimi ise orijinal belirsizlik bağıntıları ile

¹Lagrange çarpanları yöntemi kullanılarak görülebilir.

²Daha kesin ifade edilirse, logaritma fonksiyonu boyutsuz olmalı ve formülasyon içerisinde konum ve momentum ölçekleri $I_{\hat{q}}$ ve $I_{\hat{p}}$ yer almalıdır. Ancak sadelik açısından burada belirtilmemiştir.

EBB'yi birbirine bağlamaktadır.

Daha sonra Deutsch (1982), sıra-değişmeyen işlemciler için ayrık olasılık dağılımları ve Shannon entropisini kullanarak aşağıdaki sonuca ulaşmıştır:

$$H(X) + H(Z) \geq -2 \log \left(\frac{1+c}{2} \right). \quad (1.8)$$

Burada, X ve Z sıra değişmeyen iki işlemci ve $H(X)$ ve $H(Z)$ sırasıyla X ve Z 'nin Shannon entropileridir (Bknz (2.20)). $c = \max_{X,Z} |\langle x|z \rangle|^2$ olup, $|x\rangle$ ve $|z\rangle$ sırasıyla X ve Z 'nin özbazlarını temsil etmektedir.

Maasen ve Uffink (1986) sıra değişmeyen herhangi iki gözlenebilir için EBB'nin aşağıdaki formunu ortaya koymuştur,

$$H(X) + H(Z) \geq \log \frac{1}{c}. \quad (1.9)$$

Alt sınırın en büyük değeri, gözlenebilirlerin baz kümeleri *karşılıklı yansız bazların* bir kümesi yani $c = \max_{X,Z} |\langle x|z \rangle|^2 = 1/d$ olduğunda elde edilir. Burada d , çalışılan Hilbert uzayı $\mathcal{H}^d$ 'nin boyutudur. (1.9) bağıntısı entropi temelli belirsizlik bağıntılarının kullanışlı bir formu olmuş ve bilişim kuramı içerisinde rol oynamasını sağlamıştır.

Entropi, bilişim kuramında oldukça sık kullanılan bir niceliktir. Bilginin kodlanması, işlenmesi, iletilmesi, okunması ve depolanması gibi süreçlerde anahtar rol üstlenir. Bu süreçlerdeki ölçüm kaynaklı oluşabilecek belirsizliklerin alt sınırının bilinmesi avantajdır ve bu avantaj EBB ile sağlanabilir. Ayrıca kuantum rasgelelik, kuantum anahtar dağıtımı, dolanıklık tanıkları, dalga-parçacık ikililiği, koherenslik, kuantum diskord, steering, klasik korelasyonların kilitlenmesi gibi farklı alanlarda uygulamaları bulunmaktadır.

Bu bağıntının rağbet görmesinin en büyük nedenlerinden birisi de durum bağımsız bir alt sınır vermesidir. (1.3) ve (1.4) bağıntılarının sağ tarafı durum bağlı olup, her gözlenebilir çifti ve (veya) her $|\psi\rangle$ durum vektörü için alt sınırlar değişmektedir. Bu tartışmalar da Bölüm.2'de ele alınmıştır. MU sınırı ise başlangıç durumundan bağımsız bir sonuçtur.

Heisenberg bağıntısında olduğu gibi, (1.9)'un sağ tarafının geliştirilebileceği ve farklı

durumlar için daha güçlü alt sınırların olabileceği gösterilmiştir. Yine durum bağımsız, işlemcilere göre değişmeyen ve MU sınırından daha güçlü alt sınırlar elde edilebileceği, Bölüm.3'te ele alınacaktır.

İlerleyen yıllarda bu bağıntıların aslında başlangıç durum bağımsız olmadığı ortaya çıkmıştır. Berta vd. (2010) kuantum hafıza varlığında (ölçüm yapılan sistemle korelasyon halinde bulunan başka bir sistem, *side information*) EBB'yi inceleyerek aşağıdaki başlangıç durumuna bağlı formu elde etmişlerdir; İki parçalı bir sistem için bu bağıntı şöyle ifade edilebilir:

$$H(X|B) + H(Z|B) \geq \log \frac{1}{c} + S(A|B). \quad (1.10)$$

Burada, $H(X|B)$ ($H(Z|B)$) koşullu Shannon entropisi ve $S(A|B)$ koşullu von Neumann entropisidir. Bu iki entropinin arasındaki en önemli fark, koşullu Shannon entropisi her zaman pozitif değerler alırken, koşullu von Neumann entropi negatif değerler alabilir ve negatif değerler dolanıklığa bir işaret olarak görülür (Nielsen ve Chuang 2011 Syf. 514). En küçük değeri $-\log d$ olur ve bu durumda sistemlerin en dolanık durumdan olduğu söylenir. Bu durumda (1.10)'nun sağ taraf aşık olur ve iki parçalı en dolanık halde bulunan bir sistem üzerinde yapılacak ölçümlerde belirsizliğin sıfıra indirgenebileceği sonucu ortaya çıkmaktadır. Fotonlar üzerinde yapılan deneylerle bu çalışmanın doğruluğu gösterilmiştir (Li v.d 2011). Bu bağıntıya Bölüm.4'te yer verilecektir.

Pati v.d (2012), (1.10)'un sağ tarafına kuantum diskordun da ($D_A(\rho_{AB})$) eklenebileceğini göstermişlerdir,

$$H(X|B) + H(Z|B) \geq \log \frac{1}{c} + S(A|B) + \max [0, D_A(\rho_{AB}) - J_A(\rho_{AB})]. \quad (1.11)$$

Burada, $J_A(\rho_{AB}) = \max_X I(X; B)$ olarak tanımlanır ve ölçümden sonraki klasik karşılıklı bilişim miktarının en büyük değeridir. Bu bağıntı da Bölüm.4'te ele alınacaktır.

EBB'nin özellikle kuantum kriptoloji alanında geniş kullanım alanları vardır ve kuantum güvenlik protokolleri ile yüzde yüz güvenlik sağlanabileceğini ispatlamak için kullanılmaktadır. Sistemler ilgili bilişim elde etmeye çalışan kulak misafirlerinin

(*eavesdroppers*) hiçbir zaman tam olarak bilişim elde edemeyeceği EBB ile gösterilebilir. Tek ve çok parçalı sistemler için geliştirilen ve bir düşünce deneyi olan *tahmin oyunları* bu bağıntıların ve kuantum kriptolojideki uygulamalarının anlaşılması açısından ele alınacaktır.

Bu çalışmada ön hazırlık olarak standart sapmanın sezgi karşısı davranışları tartışılacak, sonra Shannon, von Neumann ve Rényi entropileri incelenecektir. Ayrıca bu kısımda ölçüm konusu da kısaca ele alınacaktır. Daha sonra, bir hafıza sistemi olmadan EBB, bir hafıza sistemi varlığında EBB ve kuantum bilişim kuramındaki bazı uygulamaları incelenecektir. Ekler kısmında ise tez içinde ele alınan, ancak hesap olarak uzun olan bazı gerekli bilgiler ve yine bu çalışma için gerekli görülen bazı konular incelenmiştir.

2. ÖN HAZIRLIK

EBB'yi incelemeden önce, standart sapmanın sezgi karşısı (mantığa aykırı) davranışlarından ve bilişim kuramı içerisindeki kullanışsızlığından bahsedilecek, sonra bilişimsel entropi konusu incelenecektir. Ayrıca, bütün entropik belirsizlik bağıntıları ölçüme dayanan bağıntılar olduğu için, kuantum mekaniğinde *ölçüm* kavramı de ele alınacaktır.

2.1 Standart Sapma

Kuantum mekaniğinde, Hilbert uzayı $\mathcal{H}^d$ üzerinde tanımlı çizgisel dönüşümlerin (işlemcilerin) uzayı $B(\mathcal{H}^d)$ ile gösterilirse, $X \in B(\mathcal{H}^d)$ olmak üzere, Hermite-sel bir X işlemcisinin $|\psi\rangle$ durumunda beklenen değerinden ne kadar sapma olabileceği standart sapma ile nicelendirilir. En genel ifade ile X 'in $|\psi\rangle$ durumundaki, $\langle\psi|X|\psi\rangle = \langle X\rangle$, beklenen değerinden farkının karesinin ortalamasına *varyans*, bu değer kareköküne de *standart sapma* veya *kare-ortalama karekök sapma* denir. Standart sapma $\sigma(X)$ ile gösterilir ve şöyle tanımlanır:

$$\sigma(X) = \sqrt{\langle(X - \langle X\rangle)^2\rangle} = \sqrt{\langle X^2\rangle - \langle X\rangle^2}. \quad (2.1)$$

Bir X gözlenebilirinin (veya sürekli bir X rasgele değişkenin) bir $p_X(x)$ olasılık dağılımı için standart sapma aşağıdaki gibi de ifade edilebilir,

$$\sigma(X) = \left[\int (X - \langle X\rangle)^2 p_X(x) dx \right]^{1/2}. \quad (2.2)$$

İntegral değişkeni dx bütün uzay üzerinden integral alındığını göstermektedir: Sonlu çıktıları olan bir rasgele X değişkeni için yukarıdaki integral bir sonlu toplamla değiştirilmelidir.

Heisenberg tarafından belirsizliğin bir ölçüsü olarak kullanılan standart sapma, halleri tarafından da kullanılmıştır. Ancak, hesaplardaki sezgi karşısı davranışları alternatif belirsizlik ölçülerinin aranmasına neden olmuştur.

2.1.1 Standart sapmanın sezgi karşısı davranışları

Laboratuvarda elde edilen sonuçlar ile beklenen değerler her zaman aynı olmayabilir ve sapma miktarını hesaplayabilmek deney sonuçları açısından önemlidir. Ancak standart sapma tutarlı davranışları sergilememekte ve belirsizliği nicelendirmesi sorgulanmaktadır. Aşağıdaki örnekler bu konu hakkındaki şüpheleri destekleyecek şekilde seçilmiştir.

Örnek 2.1 z -spin açısal momentumu, $m_z \in \{1, 0, -1\}$ olan spin-1 parçacıklar (bozonlar) ele alınsın. S_z işlemcisi ve durum vektörlerinin matris gösterimleri şu şekildedir,

$$S_z = \hbar \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}; |1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, |0\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, |-1\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}. \quad (2.3)$$

Bir parçacığın $|\psi_1\rangle = \sqrt{\frac{1}{3}}(|1\rangle + |0\rangle + |-1\rangle)$ gibi bütün durumların bir süperpozisyonu olan bir saf kuantum durumunda bulunduğu ve bulunma olasılıkları eşit ve $p_z = 1/3$ olduğu varsayalım. S_z ve S_z^2 'nin beklenen değerleri ve $\sigma(S_z)$ hesaplanırsa,

$$\langle\psi_1|S_z|\psi_1\rangle = 0, \quad \langle\psi_1|S_z^2|\psi_1\rangle = \frac{2}{3} \quad \text{ve} \quad \sigma(S_z) = \sqrt{\langle S_z^2 \rangle - \langle S_z \rangle^2} = \sqrt{\frac{2}{3}}, \quad (2.4)$$

çıkarm¹. İkinci adımda, sistem hakkında bilgi edinildiği düşünölsün ve $|0\rangle$ olma olasılığı $p_z(0) = 0$ varsayalım. Yeni olasılık dağılımı $p_z(1) = p_z(-1) = 1/2$ olur ve durum vektörü $|\psi_2\rangle = \sqrt{\frac{1}{2}}(|1\rangle + |-1\rangle)$ şeklinde ifade edilebilir. Bu durumda yeniden hesaplama yapılırsa,

$$\langle\psi_2|S_z|\psi_2\rangle = 0, \quad \langle\psi_2|S_z^2|\psi_2\rangle = 1 \quad \text{ve} \quad \sigma(S_z) = \sqrt{\langle S_z^2 \rangle - \langle S_z \rangle^2} = 1, \quad (2.5)$$

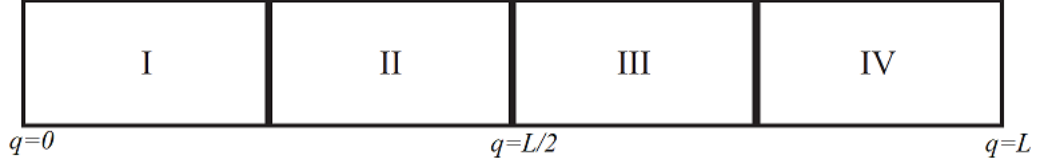
elde edilir. Burada spin bileşenlerinin olasılık değerleri arttığı için sezgisel olarak standart sapmanın yani belirsizliğin azalması beklenir ancak artmaktadır.

Sıradaki iki örnekte, kutu içindeki parçacık yaklaşımında standart sapmanın yine sezgi karşısı davranışlarda bulunduğunu göstermek kolaydır. Beklenen ve ortaya çıkan sonuçlar bu konudaki tartışmaların nedenlerini de ortaya koymaktadır.

¹Sadelik açısından bütün hesaplarda $\hbar = 1$ kabul edilecektir.

Örnek 2.2 Sırasıyla Şekil.(2.1) ve (2.2)'de görülen A ve B sistemleri, her biri $L/4$ uzunluğunda olan dört kutucuktan oluşmaktadır. A sisteminde bir parçacığın bulunma olasılığı;

$$p_A(q) = \begin{cases} \frac{1}{L}, & q \in [0, L] \\ 0, & \text{diğer yerlerde.} \end{cases} \quad (2.6)$$



Şekil 2.1. A sistemi

ile verilmektedir. Konum için beklenen değer $\langle \hat{q} \rangle = L/2$ çıkar ve konumun belirsizliği hesaplanırsa,

$$\sigma(\hat{q}) = \left[\int_0^L (\hat{q} - \langle \hat{q} \rangle)^2 p(q) dq \right]^{1/2} = \left[\int_0^L (\hat{q} - \langle \hat{q} \rangle)^2 \frac{1}{L} dq \right]^{1/2} = \frac{L}{\sqrt{12}}, \quad (2.7)$$

elde edilir. Burada dq konum işlemcisi için integral değişkenidir.



Şekil 2.2. B sistemi.

B sistemi için, sistemde bulunma olasılığı:

$$p_B(q) = \begin{cases} \frac{2}{L}, & q \in [0, \frac{L}{4}] \cup [\frac{3L}{4}, L] \\ 0, & \text{diğer yerlerde.} \end{cases} \quad (2.8)$$

olarak verilmiştir ve konumun beklenen değeri yine $L/2$ ve belirsizlik,

$$\begin{aligned} \sigma(\hat{q}) &= \left[\int_0^{L/4} (\hat{q} - \langle \hat{q} \rangle)^2 \frac{2}{L} dq + \int_{3L/4}^L (\hat{q} - \langle \hat{q} \rangle)^2 \frac{2}{L} dq \right]^{1/2} \\ &= \sqrt{\frac{7}{4}} \frac{L}{\sqrt{12}}, \end{aligned} \quad (2.9)$$

çıkar. Parçacık daha dar bir alana hapsedildiğinde konumundaki belirsizliğin azalması beklenirken, hesaplarda A 'daki gibi daha geniş bir alana yayılmış parçacığın konumundaki belirsizlik daha küçük çıkmaktadır.

Giriş kısmında Heisenberg belirsizlik bağıntılarının güçlü ve sıkı alt sınırlar vermediğine değinilmişti. Aşağıdaki örnekle bu konudaki soru işaretleri daha iyi anlaşılacaktır.

Örnek 2.3 Spin-1/2 parçacıklar için Robertson bağıntısı ((1.3)) ele alınsın. Pauli işlemcileri $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ ve $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, Bloch küresi üzerinde x ve z eksenlerine karşılık gelen gözlenebilirlerdir. σ_x ve σ_z 'nin komütasyon bağıntısı incelenirse,

$$\begin{aligned} [\sigma_x, \sigma_z] &= \sigma_x \sigma_z - \sigma_z \sigma_x \\ &= -2(|0\rangle\langle 1| - |1\rangle\langle 0|) \\ &= -2i\sigma_y. \end{aligned} \tag{2.10}$$

olur. (1.3) göz önüne alınırsa,

$$\sigma(\sigma_x)\sigma(\sigma_z) \geq i \langle \psi | \sigma_y | \psi \rangle \tag{2.11}$$

olur ve bu alt sınır sadece σ_x ve σ_z için geçerlidir. Her farklı sıra değişmeyen işlemciler için farklı alt sınırlar elde edilir. Ancak EBB'nin amacı, kullanılan işlemcilere göre değişmeyen bir alt sınır elde etmektir ve Robertson bağıntısı bunu sağlamaz.

2.2 Ölçüm

Bir kuantum sisteminin durumları, yoğunluk işlemcileri (matrisleri) ile betimlenir.

Bir yoğunluk işlemcisi,

$$i) \quad \rho^\dagger = \rho \text{ (Hermite - sel)}$$

$$ii) \quad \rho \geq 0 \text{ (Pozitif)}$$

$$iii) \quad \text{Tr} \rho = 1 \text{ (Birim izli)}.$$

özelliklerine sahip kare matrislerdir². Bu işlemciler, sistem hakkındaki bütün bilgiyi taşır ve olasılıkların elde edilmesinde kullanılır.

²Her pozitif işlemci Hermite-sel'dir ancak her Hermite-sel işlemci pozitif olmak zorunda değildir.

Laboratuvarda ölçülebilen her fiziksel nicelik (konum, momentum, enerji v.b.) Hilbert uzayı $\mathcal{H}^d$ 'de tanımlı çizgisel dönüşümlerin $B(\mathcal{H}^d)$ uzayında tanımlı bir Hermite-sel (*self-adjoint*) işlemciye (matrise) karşılık gelir. Ölçüm işlemcileri, $\{M_i\}$ işlemcilerinin bir kümesi tarafından, $X_i = M_i^\dagger M_i$ olacak şekilde tanımlanır. i ile etiketlenmiş ölçüm sonucuna ait olasılıklar bir saf $\rho = |\psi\rangle\langle\psi|$ durumunda şöyle bulunur;

$$\begin{aligned} p(X_i) &= \langle\psi| M_i^\dagger M_i |\psi\rangle \\ &= \text{Tr}(M_i |\psi\rangle\langle\psi| M_i^\dagger) \\ &= \text{Tr}(M_i \rho M_i^\dagger) = \text{Tr}(\rho X_i). \end{aligned} \quad (2.12)$$

Son satırda yer alan yazıma *Born kuralı* denir. Saf olmayan durumlar, saf durumların bir konveks kombinasyonu olduğundan, bu yazım saf olmayan durumlarda da geçerlidir. Sistemin i . ölçüm olasılığı ile birlikte ölçüm sonrası durum (*post-measurement state*) şu şekilde ifade edilir,

$$|\psi'\rangle = \frac{M_i |\psi\rangle}{\sqrt{\langle\psi| M_i^\dagger M_i |\psi\rangle}}. \quad (2.13)$$

Bütün olasılıkların toplamının $\sum_i p(M_i) = 1$ olması gerektiğinden, ölçüm işlemcilerinin kümesi tamlık bağıntısını sağlamalıdır,

$$\sum_i X_i = \sum_i M_i^\dagger M_i = \mathbb{1}. \quad (2.14)$$

Bu çalışmada izdüşüm (*projection*) işlemcileri ve pozitif-operatör değerli ölçüler (*positive-operator valued measure, POVM*) ele alınacaktır.

2.2.1 İzdüşüm işlemcileri

Verilen herhangi bir gözlenebilir X (Hermite-sel işlemci),

$$X = \sum_i \mu_i P_i = \sum_i \mu_i |x_i\rangle\langle x_i| \quad (2.15)$$

şeklinde spektral ayrışma sahiptir. Buradaki $P_i = |x_i\rangle\langle x_i|$ işlemcilerine X 'in öz uzayı üzerine iz düşüren öz-izdüşüm işlemcileri (von Neumann ölçümleri) denir ve μ_i , i . ölçüm sonucunun olasılığıdır. İzdüşüm işlemcileri aşağıdaki şartları sağlamalıdır,

$$i) \quad P_i^\dagger = P_i \text{ (Hermite - sel)}$$

ii) $P_i^2 = P_i$ (*Karesi kendisine eşit - idempotent*)

iii) $P_i P_j = \delta_{ij} P_j$; $\forall i, j \in [1, d]$ için (*Diklik bağıntısı*) .

Burada d , Hilbert uzayının boyutudur. İzdüşüm işlemcileri tamlık bağıntısını da sağlar, $\sum_i P_i^\dagger P_i = \sum_i P_i^2 = \sum_i P_i = \mathbb{1}$. Bu işlemciler, uygulandığı yoğunluk işlemcisini kendi alt uzayına iz düşürür. Örneğin, $P = |0\rangle\langle 0|$, saf $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ durumuna uygulanırsa,

$$\begin{aligned} \langle\psi| P_i^\dagger P_i |\psi\rangle &= \langle\psi|0\rangle \langle 0|0\rangle \langle 0|\psi\rangle \\ &= \langle\psi|0\rangle \langle 0|\psi\rangle \\ &= (\alpha^* \langle 0| + \beta^* \langle 1|)(|0\rangle\langle 0|)(\alpha|0\rangle + \beta|1\rangle) \\ &= |\alpha|^2, \end{aligned} \tag{2.16}$$

olur ve “sistem, $|0\rangle$ durumda $|\alpha|^2$ olasılığı ile bulunabilir” denir. Ölçüm sonrası durumlar aşağıdaki gibi temsil edilir,

$$\text{Saf durumlar için; } |\psi'\rangle = \frac{P_i |\psi\rangle}{\sqrt{\langle\psi| P_i |\psi\rangle}}, \tag{2.17}$$

$$\text{Saf olmayan durumlar için; } \rho' = \frac{P_i \rho P_i}{\text{Tr}(P_i \rho)}. \tag{2.18}$$

En basit (ilkel) izdüşüm işlemcileri rank-1 işlemcilerdir (birim izli), ancak bütün izdüşüm işlemcilerinin rank-1 olmasına gerek yoktur.

2.2.2 Pozitif-operatör değerli ölçü (POVM)

$B(\mathcal{H}^d)$ 'de tanımlı herhangi bir $\{M_i\}$ işlemciler kümesi düşünölsün. Bu kümenin elemanları kullanılarak,

$$E_i = M_i^\dagger M_i \tag{2.19}$$

olacak şekilde pozitif işlemciler tanımlanabilir. Böylece i ile etiketlenmiş bir $\{E_i\}$ kümesi elde edilebilir. Eğer bu kümenin elemanları,

i) $E_i \geq 0$ (*Pozitif*)

ii) $\sum_i E_i = \mathbb{1}$ (*Tamlık bağıntısı*)

özelliklerini sağlıyorsa, bu şekilde tanımlanmış $\{E_i\}$ tam kümesine bir POVM (*positive operator-valued measure*) ve her bir E_i işlemcisine bir POVM elemanı denir. i . ölçüm sonucunun gelme olasılığı $p(E_i) = \text{Tr}(\rho E_i)$ şeklinde elde edilir ve ikinci özellik olasılıkların toplamlarının 1 olması, $\sum_i p(E_i) = 1$, şartından gelmektedir.

POVM elemanları diklik bağıntısını sağlamak zorunda değildir ve izdüşüm işlemcilerini kapsar.

2.3 Entropi

Entropi, termodinamiğin ikinci yasasına göre düzensizliğin bir ölçüsü olarak tanımlanır. Ancak bu çalışmada “bilimsel entropi” kavramı ele alınacaktır. Aşağıda bu çalışma kullanılacak entropi türlerine yer verilmiştir.

2.3.1 Klasik bilişimde entropi: Shannon entropisi

Cloud Shannon (1948) tarafından klasik bilişim kuramının temel kavramı olarak ele alınan bilimsel entropi, bilişim faaliyetleri ve karşılıklı iletişimde anahtar rol üstlenmektedir. Bir rasgele X değişkeni ele alınırsa, bu değişken ile ilgili bilişim faaliyetlerinde (kodlama, işleme, iletilme, okunma, depolanma v.b) bu değişkenin çıktıları değil, çıktıların olasılıkları önemlidir. X değişkenin çıktılarının olasılıkları üzerinden bilişim faaliyetlerinin yürütülebilmesi *Shannon entropisi* ile nicelendirilir. Tanım olarak, bir rasgele X değişkenin Shannon entropisi, X 'in değerini öğrendikten sonra ne kadar bilişim kazancı olacağını veya X 'in değerini öğrenmeden önceki belirsizlik miktarını nicelendirir (Nielsen ve Chuang 2011 Syf. 500). X değişkenine ait bir $p_X(x)$ ayrık olasılık dağılımının Shannon entropisi ($p_X(x) \geq 0$, $\sum_x p_X(x) = 1$, $H(X)$), şu şekilde tanımlanır;

$$H(X) := - \sum_x p_X(x) \log p_X(x). \quad (2.20)$$

Elde edilen sayısal değerlerin birimi mesaj başına *bit* (*bit per message*) olarak tanımlanır (2 tabanında logaritma kullanıldığı için bu birim kullanılmaktadır ve bu çalışmada her zaman $\log = \log_2$ kabul edilecektir.). Dikkat edilirse, $\log 0$ tanımsızdır.

Ancak $\lim_{x \rightarrow 0} x \log x = 0$ olduğundan bundan sonraki bütün hesaplarda $0 \log 0 = 0$ alınacaktır.

Eğer bir değişkenin olasılık dağılımı $\{1, 0, 0, \dots\}$ gibi, yani bir çıktının meydana gelme olasılığı kesin ve diğerleri imkansız ise, bu değişkenin Shannon entropisi $H(X) = 1 \log 1 = 0$ olur ve herhangi bir belirsizlik yoktur. Eğer, n elemanlı bir kümede olasılık dağılımı $\{\frac{1}{n}, \frac{1}{n}, \frac{1}{n}, \dots\}$ gibi tekdüze (bütün çıktılar için sabit ve aynı büyüklükte, *uniform*) bir dağılım gösteriyorsa, bu dağılımın Shannon entropisi $H(X) = -\sum_n (1/n) \log(1/n) = \log n$ yani maksimum olur. Burada çıkarılabilecek sonuç Shannon entropisi her zaman $0 \leq H(X) \leq \log n$ arasında değerler alır.

Çıktıları x olan bir X değişkeni ve çıktıları y olan bir Y değişkeninden oluşan ve birbirleriyle ilintili (korelasyon halinde) iki parçalı bileşik sistemin Shannon bileşik entropisi,

$$H(XY) := - \sum_{x,y} p(x,y) \log p(x,y), \quad (2.21)$$

şeklinde tanımlanır. Burada $p(x,y)$ *bileşik olasılık* olarak adlandırılır. Sistemin indirgenmiş (marjinal) olasılık dağılımları, $\sum_x p(x,y) = p(y)$ ve $\sum_y p(x,y) = p(x)$ şeklinde hesaplanır. Eğer X ve Y birbirinden bağımsızsa (istatistiksel olarak bağımsız) her x ve her y çıktılarının bileşik olasılığı için $p(x,y) = p(x)p(y)$ yazılabilir ve bileşik sistemin entropisi;

$$\begin{aligned} H(XY) &= - \sum_{x,y} p(x,y) \log p(x,y) \\ &= - \sum_x p(x) \log p(x) - \sum_y p(y) \log p(y) = H(X) + H(Y), \end{aligned} \quad (2.22)$$

şeklinde yazılabilir.

İki parçalı bir sistemde, bir Y değişkeninin bir y çıktısının verilmesi koşulunda X 'in entropisi aşağıdaki gibi tanımlanır;

$$H(X|y) := - \sum_x p(x|y) \log p(x|y). \quad (2.23)$$

Burada $p(x|y)$, *koşullu olasılık* olarak adlandırılır ($\sum_x p(x|y) = 1$) ve y verilmesi durumunda x gelme olasılığını nicelendirir. Bileşik olasılık ile koşullu olasılık arasındaki

ilişki *Bayes kuramı* ile verilir;

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)} = \frac{p(x,y)}{p(y)}. \quad (2.24)$$

Koşullu olasılıklar da $\sum_x p(x|y) = 1$ şartını sağlar. Böylece (2.23)'de her zaman pozitifdir ve bir Shannon entropisidir.

Koşullu Shannon entropisi, Y değişkenin bütün çıktıları üzerinden ağırlıklı ortalama alınarak elde edilir;

$$H(X|Y) := - \sum_{x,y} p(y)p(x|y) \log p(x|y) = \sum_y p(y)H(X|y). \quad (2.25)$$

Bu ifade $H(X|y)$ entropilerinin ortalaması olduğundan (kuantum koşullu entropinin tersine) her zaman pozitifdir. Koşullu entropi, Y 'nin verilmesi durumunda X üzerinde ne kadar belirsizlik kaldığı veya X hakkında ne kadar bilişime sahip olunabileceğinin bir ölçüsüdür. Bayes' kuramı kullanılarak, (2.16)'dan aşağıdaki özdeşlik türetilebilir,

$$\begin{aligned} H(X|Y) &= - \sum_{x,y} p(y)p(x|y) \log p(x|y) \\ &= - \sum_{x,y} p(x,y) \log \left(\frac{p(x,y)}{p(y)} \right) \\ &= - \sum_{x,y} p(x,y) \log p(x,y) + \sum_y p(y) \log p(y) = H(XY) - H(Y). \end{aligned} \quad (2.26)$$

Rasgele bir X değişkeni için iki olasılık dağılımı $p(x)$ ve $q(x)$ arasındaki *bağıl entropi* şu şekilde tanımlanır,

$$\begin{aligned} D(p(x)||q(x)) &:= \sum_x p(x) \log \frac{p(x)}{q(x)} \\ &= \sum_x p(x) \log p(x) - \sum_x p(x) \log q(x). \end{aligned} \quad (2.27)$$

Bağıl entropinin her zaman pozitifdir, $D(p(x)||q(x)) \geq 0$, ve eşitlik için gerek ve yeter koşul $p(x) = q(x)$ olmasıdır. İki olasılık dağılımı arasındaki simetrik olmayan bir uzaklık ölçüsü olarak ele alınır. Bağıl entropinin pozitifliği EK 1'de incelenmiştir.

Klasik karşılıklı bilişim $I(X;Y)$, X ve Y değişkenlerinin karşılıklı veya ortak bilişim

miktarını karakterize eder. X ve Y 'nin karşılıklı bilişim miktarı,

$$\begin{aligned}
I(X; Y) &:= \sum_{x,y} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} \\
&= \sum_{x,y} p(x, y) \log p(x, y) - \sum_x p(x) \log p(x) - \sum_y p(y) \log p(y) \\
&= H(X) + H(Y) - H(XY) \\
&= H(X) - H(X|Y) = H(Y) - H(Y|X),
\end{aligned} \tag{2.28}$$

olarak tanımlanır. İlk satıra dikkat edilirse, $I(X; Y) = D(p(x, y) || p(x)p(y)) \geq 0$ olduğu görülür ve eşitlik için gerek ve yeter koşul X ve Y değişkenleri istatistiksel olarak bağımsız olmasıdır. Böylece klasik karşılıklı bilişim de her zaman pozitifdir. Sistemler arasındaki tüm klasik korelasyonların bir ölçüsü olarak ele alınır.

2.3.2 Kuantum bilişimde entropi: von Neumann entropisi

Bir ρ yoğunluk işlemcisinin von Neumann entropisi şöyle tanımlanır;

$$S(\rho) := -\text{Tr}(\rho \log \rho). \tag{2.29}$$

Her yoğunluk işlemcisi $\rho = \sum_i \lambda_i |i\rangle\langle i|$ olacak şekilde *spektral ayrışım* kabul eder. Burada λ_i , ρ işlemcisinin özdeğerleridir. λ_i özdeğerleri kullanılarak von Neumann entropisi (dejenerelik varsa hesaba katılarak) şöyle yazılabilir,

$$S(\rho) = - \sum_i \lambda_i \log \lambda_i. \tag{2.30}$$

Eğer $\rho = |\psi\rangle\langle\psi|$ yazılabiliyorsa bu durumlara saf durumlar (*pure states*) denir ve özdeğerlerinden birisi $\lambda_i = 1$ ve diğer özdeğerleri çakışık olup sıfıra eşittir. Saf durumların von Neumann entropisi, $S(\rho) = 0$ çıkar. $\rho = \sum_i \mu_i |\phi\rangle\langle\phi_i|$ şeklinde (en az iki $|\phi_i\rangle$ çizgisel bağımsızsa) yazılabiliyorsa bu durumlara saf olmayan durumlar (*mixed states*) denir. Bütün özdeğerler $\lambda_i = 1/d$ şeklinde tek düze (*uniform*) ise bu duruma en saf olmayan durum (*maximally mixed state*) denir ve bu durumda $S(\rho) = \log d$ maksimum olur. Burada d , Hilbert uzayı boyutudur. von Neumann entropisinin değerleri de $0 \leq S(\rho) \leq \log d$ arasında yer almaktadır.

İki parçalı bir bileşik sisteme ait ρ_{AB} yoğunluk işlemcisinin von Neumann entropisi,

$$\begin{aligned} S(\rho_{AB}) &:= -\text{Tr}(\rho_{AB} \log \rho_{AB}) \\ &= -\sum_j \eta_j \log \eta_j \end{aligned} \quad (2.31)$$

şeklinde tanımlanır. Burada η_j 'ler ρ_{AB} 'nin özdeğerleridir. Bileşik sistemin indirgenmiş (*marginal*) yoğunluk işlemcileri $\text{Tr}_B(\rho_{AB}) = \rho_A$ ve $\text{Tr}_A(\rho_{AB}) = \rho_B$ şeklinde parçalı izleri alınarak (Tr_A ve Tr_B) bulunur.

Kuantum koşullu entropi;

$$S(A|B) := S(\rho_{AB}) - S(\rho_B) \quad (2.32)$$

şeklinde tanımlanır. Shannon entropisinde bileşik sistemin entropisi parçaların entropilerinden her zaman büyük veya eşitken ($H(XY) \geq \{H(X), H(Y)\}$), bu durum von Neumann entropisi için geçerli değildir. Örneğin, sistem $\rho_{AB} = |\phi^+\rangle\langle\phi^+|$ gibi saf en dolanık bir Bell durumunda bulunuyorsa, indirgenmiş durumlar en saf olmayan $\rho_A = \rho_B = \mathbb{1}/d$ durumundadır. Bu durumda $S(\rho_{AB}) = 0$ iken, alt sistemlerinin entropileri maksimum ve $\log d$ olur. Ayrıca $S(A|B) = S(\rho_{AB}) - S(\rho_B) = -\log d$ olur. Bu sonuç kuantum koşullu entropiye özgü bir durumdur.

ρ ve σ gibi iki yoğunluk işlemcisi arasındaki *kuantum bağıl entropi* şöyle tanımlanır,

$$D(\rho||\sigma) := \text{Tr}(\rho \log \rho) - \text{Tr}(\rho \log \sigma) \quad (2.33)$$

Klasik bağıl entropi ile benzer olarak kuantum bağıl entropi de her zaman pozitifdir ve eşitlik için gerek ve yeter koşul $\rho = \sigma$ olmasıdır. İki yoğunluk işlemcisi arasında simetrik olmayan bir uzaklık ölçüsü olarak düşünülür.

İlerleyen bölümlerde kullanılacağından bağıl entropinin kuantum kanallar altında monotonluğundan bahsedilmelidir. Kanal kavramı, klasik iletişim teorisi çekilmiştir ve bir göndericinin, bir ρ durumunu bir iletişim bağlantısıyla beraber, kanal uygulanmış $\mathcal{E}(\rho)$ durumunu alan diğer partiye iletmesi olarak hayal edilebilir

³. Bir kuantum kanal $\mathcal{E}(\cdot)$,

³Preskill J., Lecture Notes for Ph219/CS219:var Quantum Information Chapter 3 Syf: 12

- i) $\mathcal{E}(\alpha\rho_1 + \beta\rho_2) = \alpha\mathcal{E}(\rho_1) + \beta\mathcal{E}(\rho_2)$ (*Çizgisel*)
- ii) $\rho = \rho^\dagger \Rightarrow \mathcal{E}(\rho) = \mathcal{E}(\rho)^\dagger$ (*Hermite-selliğin koruyan*)
- iii) $\rho \geq 0 \Rightarrow \mathcal{E}(\rho) \geq 0$ (*Pozitifliği koruyan*)
- iv) $\text{Tr}[\mathcal{E}(\rho)] = \text{Tr}\rho$ (*İzi koruyan*) .

özelliklerini taşıyan tamamen pozitif iz-koruyan gönderimler (*completely positive trace-preserving map, CPTP*) olarak adlandırılır ve Kraus temsili ile gösterilir;

$$\mathcal{E}(\rho) = \sum_i K_i \rho K_i^\dagger.$$

Bu gösterime kanalın operatör-toplam gösterimi de denir ve her K_i elemanına kanalın işlemcileri veya *Kraus işlemcileri* denir. Bu işlemciler, $\sum_i K_i^\dagger K_i = \mathbb{1}$ olacak şekilde tamlık bağıntısını sağlamalıdır.

Bağıl entropi kuantum kanallar altında her zaman monoton azalır ve bu özelliğe *veri-işleme eşitsizliği* denir (Lieb ve Ruskai 1973).

$$D(\rho||\sigma) \geq D(\mathcal{E}(\rho)||\mathcal{E}(\sigma)) \quad (2.34)$$

Kuantum karşılıklı bilişim,

$$\begin{aligned} I(A; B) &:= S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \\ &= S(\rho_A) - S(A|B) \\ &= S(\rho_B) - S(B|A), \end{aligned} \quad (2.35)$$

şeklinde tanımlanır. Yine ilk satırdan kuantum karşılıklı bilişim, $I(A; B) = D(\rho_{AB}||\rho_A \otimes \rho_B)$ şeklinde yazılabilir. $I(A; B) \geq 0$ ifadesi her zaman doğrudur ve bileşik sistemin, alt sistemlerin çarpım durumundan ne kadar uzak olduğunun bir ölçüsüdür. Böylece parçalar arasında varolan bütün korelasyonları (klasik ve kuantum) nicelendirmekte kullanılır.

2.3.3 Rényi entropisi

Rényi entropisi, Shannon ve von Neumann entropilerinin bir genellemesi olarak ele alınmakta ve özellikle kuantum kriptoloji alanında sık kullanılmaktadır. Bir rasgele

X deęişkeninin çıktılarına ait bir ayrık olasılık daęılımının Rényi entropisi şöyledir,

$$H_\alpha(X) := \frac{1}{1-\alpha} \log \sum_x [p_X(x)]^\alpha. \quad (2.36)$$

Burada $\alpha \in (0, 1) \cup (1, \infty)$, $p_X(x) \geq 0$ ve $\sum_x p_X(x) = 1$ olarak tanımlanır ve olasılık daęılımı $p_X(x) = \{p_X(1), p_X(2), \dots\}$ ile birlikte alfa kuvvetinin bilişiminin bir ölçüsüdür. Nihayetinde belirsizlik kayıp bilişim olduğundan, Rényi entropisi bir belirsizlik ölçüsü olarak görülebilir.

Rényi entropisi α parametresine göre monoton azalan bir fonsiyondur; yani α deęerleri büyüdükçe Rényi entropisinin deęeri küçülür. $\alpha \rightarrow 1$ limitinde, $\lim_{\alpha \rightarrow 1} H_\alpha(X) = H(X)$, Shannon entropisi elde edilir. Monotonluk ve limit durumları EK-2’de incelenmiştir.

α ’nın deęerlerine göre, Rényi entropisi bazı isimler ile anılır. Örneęin, çarpışma entropisi $H_{\text{çarp}} = H_2$ şöyle tanımlanır;

$$H_{\text{çarp}}(X) := -\log p_{\text{çarp}}(X). \quad (2.37)$$

Buradaki çarpışma olasılıkları $p_{\text{çarp}}(X) := \sum_x p_x(X)^2$ ile tanımlanır; yani X deęişkeninin iki bağımsız olayının olasılıkları eşittir. Min-entropi $H_{\min} = H_\infty$, kuantum kriptolojide sık kullanılan bir niceliktir. Doğru tahmin için en iyi olasılığın karakterizasyonunda kullanılır ve minimum süpriz içerir,

$$H_{\min}(X) := -\log p_{\text{tahm}}(X). \quad (2.38)$$

Burada $p_{\text{tahm}}(X) := \max_x p_X(x)$ olarak tanımlanır. Min-entropi bir rasgele X deęişkeninin sürpriz sonuçlarının minimuma indirgenmişi olarak ele alınır, en büyük olasılığa bahis oynamak gibi düşünülebilir. Rényi entropisi kullanılırken, $\alpha < 1$ deęerleri için, minimum sürprizli olaylar daha ağırlıklı olur. Max-entropi ise $H_{\max} := H_{1/2}$ olarak tanımlanır.

3. BİR HAFIZA SİSTEMİ OLMADAN EBB

Bu bölümde herhangi bir yardımcı sisteme veya hafızaya sahip olmayan, tek parçalı sistemler için EBB incelenecektir. Shannon ve Rényi entropileri için bağıntıların tarihsel gelişimleri ve konu başlıkları altında ilgili olması durumunda daha güncel çalışmalara da yer verilecektir. Daha sonra bir düşünce deneyi olan *tahmin oyunu* ile bağıntıların kullanışlılığı değerlendirilecektir.

3.1 Shannon Entropisi ile EBB

Tek parçalı bir sistemde, EBB'nin iki avantajı dikkat çekmektedir. Bunlar, eşitsizliğin alt sınırının;

- i) Başlangıç durumundan bağımsız olması,
- ii) İşlemcilerle göre alt sınırın değişmemesidir.

Deutsch (1983): Deutsch'un (1983) çalışmasına göre, bir boylandırılmış $|\psi\rangle$ durum vektörü üzerine sıra değişmeyen ve bazları sırasıyla $\{|x\rangle\}$ ve $\{|z\rangle\}$ ile tanımlanan X ve Z izdüşüm ölçümleri uygunlansın ve olasılıklar $|\langle\psi|x\rangle|^2$ ve $|\langle\psi|z\rangle|^2$ olacak şekilde ayrık olsun ($\sum_x |\langle\psi|x\rangle|^2 = 1 = \sum_z |\langle\psi|z\rangle|^2$). Ölçümlerin Shannon entropileri,

$$H(X) = - \sum_x |\langle\psi|x\rangle|^2 \log |\langle\psi|x\rangle|^2, \quad (3.1)$$

$$H(Z) = - \sum_z |\langle\psi|z\rangle|^2 \log |\langle\psi|z\rangle|^2, \quad (3.2)$$

şeklindedir. Deutsch'e göre, X ve Z ölçüm sonuçlarının belirsizlikleri her zaman indirgenemez bir alt sınıra sahiptir ($H(X) + H(Z) \geq \text{indirgenemez alt sınır}$). Daha açık şu biçimde yazılabilir:

$$\begin{aligned} H(X) + H(Z) &= - \sum_x |\langle\psi|x\rangle|^2 \log |\langle\psi|x\rangle|^2 - \sum_z |\langle\psi|z\rangle|^2 \log |\langle\psi|z\rangle|^2 \\ &= - \sum_{x,z} |\langle\psi|x\rangle|^2 |\langle\psi|z\rangle|^2 [\log(|\langle\psi|x\rangle|^2 |\langle\psi|z\rangle|^2)]. \end{aligned} \quad (3.3)$$

Parantez içindeki terim her zaman pozitif-olmayan (0 veya negatif) tanımlıdır ve aşağıdaki özdeşlikten en büyük değeri elde edilebilir,

$$\max_{|\psi\rangle} [|\langle\psi|x\rangle|^2 |\langle\psi|z\rangle|^2] = \frac{1}{4} (1 + \max_{x,z} |\langle x|z\rangle|)^2. \quad (3.4)$$

Bu özdeşliğin ispatı EK-4'te incelenmiştir. Böylece,

$$\begin{aligned} H(X) + H(Z) &\geq - \sum_{x,z} |\langle \psi|x \rangle|^2 |\langle \psi|z \rangle|^2 \log \left(\frac{1 + \max_{x,z} |\langle x|z \rangle|}{2} \right)^2 \\ &= -2 \log \left(\frac{1 + \max_{x,z} |\langle x|z \rangle|}{2} \right) = q_D, \end{aligned} \quad (3.5)$$

elde edilir.

Kraus (1985): Kraus (1985), bu sonucun optimal bir sonuç olmadığını iddaa etmiştir. Baz vektörlerinin iç çarpımının, her $|x\rangle$ ve $|z\rangle$ için, $|\langle x|z \rangle| = 1/\sqrt{d}$ olan gözlenebilirler tamamlayıcı gözlenebilirler (*complementary observables*) tanımını yapmıştır. Burada d , çalışılan Hilbert uzayının boyutudur. Tamamlayıcı gözlenebilirler ve $d = 2, 3, 4$ için yapılan hesaplamalarda, aşağıdaki bağıntının Deutsch'un bağıntısından daha güçlü ve optimal olduğu sanıtında (*conjecture*) bulunmuştur,

$$H(X) + H(Z) \geq \log d. \quad (3.6)$$

Bu çalışmada, her $|x\rangle$ ve $|z\rangle$ için, $|\langle x|z \rangle| = 1/\sqrt{d}$ koşulunu sağlayan bazlara *karşılıklı yansız bazlar* denilecektir.

Maasen-Uffink (1988): Yukarıdaki sınırın bütün sıra değişmeyen gözlenebilirler genellenebileceği Maasen ve Uffink (1988) tarafından gösterilmiştir:

$$H(X) + H(Z) \geq \log \frac{1}{c} =: q_{MU}. \quad (3.7)$$

Burada $c = \max_{x,z} |\langle x|z \rangle|^2$ olarak tanımlanmaktadır. Dikkat edilirse, yukarıdaki sınırlar başlangıç durumu $|\psi\rangle$ 'den bağımsızdır. Bu da alışılmış (geleneksel) belirsizlik bağıntılarında pek karşılaşılmayan bir olgudur.

EK-3'te MU bağıntısı saf durumlar için ispatlanmıştır. Ancak saf olmayan durumlara da şöyle genellenebilir:

Spektral ayrışım ile bir yoğunluk işlemcisi $\rho = \sum_k \mu_k \rho_k = \sum_k \mu_k |\psi_k\rangle \langle \psi_k|$ şeklinde yazılabilir, burada özdeğerler $\mu_k \geq 0$ ve $\sum_k \mu_k = 1$ bağıntılarını sağlar. $\rho_k = |\psi_k\rangle \langle \psi_k|$ ifadesi saf durumları temsil etmektedir ve $|\psi_k\rangle$, ρ işlemcisinin tanımlı olduğu Hilbert uzayının alt uzaylarını geren bazlardır. X ve Z ölçümleri ρ durumuna

uygulandığında olasılıklar,

$$p_x(\rho) = \langle x|\rho|x\rangle = \sum_k \mu_k \langle x|\rho_k|x\rangle = \sum_k \mu_k |\langle \psi_k|x\rangle|^2,$$

$$p_z(\rho) = \langle z|\rho|z\rangle = \sum_k \mu_k \langle z|\rho_k|z\rangle = \sum_k \mu_k |\langle \psi_k|z\rangle|^2,$$

olur ($\sum_x p_x(\rho) = 1 = \sum_z p_z(\rho)$) ve Shannon entropileri,

$$H_\rho(X) = - \sum_x \left(\sum_k \mu_k |\langle \psi_k|x\rangle|^2 \right) \log \left(\sum_k \mu_k |\langle \psi_k|x\rangle|^2 \right), \quad (3.8)$$

$$H_\rho(Z) = - \sum_z \left(\sum_k \mu_k |\langle \psi_k|z\rangle|^2 \right) \log \left(\sum_k \mu_k |\langle \psi_k|z\rangle|^2 \right), \quad (3.9)$$

şeklinde elde edilir. Shannon entropisi konkav bir fonksiyondur ve

$$H_\rho(X) \geq \sum_k \mu_k H_{\rho_k}(X), \quad H(\rho_k) = \sum_x |\langle \psi_k|x\rangle|^2 \log |\langle \psi_k|x\rangle|^2, \quad (3.10)$$

bağıntısı her zaman doğrudur (Z ölçümü için de yazılabilir). Eşitsizliğin sağ tarafında yer alan $H_{\rho_k}(X)$, ρ_k ile tanımlanan saf durumlara uygulanan X ölçümünün Shannon entropisidir. Yani, saf olmayan durumlarda yapılan ölçümün $H_\rho(X)$ belirsizliği, k ile etiketlenmiş saf ρ_k durumlarında yapılan ölçümün $H_{\rho_k}(X)$ belirsizliklerinin ağırlıklı ortalamasından her zaman büyük veya eşittir. Bu özellik kullanılırsa,

$$H_\rho(X) + H_\rho(Z) \geq \sum_k \mu_k [H_{\rho_k}(X) + H_{\rho_k}(Z)] \geq q_{MU}. \quad (3.11)$$

elde edilir. Yani, MU bağıntısı saf olmayan durumlar için de geçerlidir.

(3.7)'in sağ tarafına bakıldığında q_{MU} değerinin alabileceği en küçük değer 0'dır ve bunun olması için gerek ve yeter koşul X ve Z işlemcilerinin en az bir ortak özvektöre sahip olmasıdır. Bu durumda, $|\langle x|z\rangle|^2 = 1$, $\log 1 = 0$ olur ve bağıntı aşık bir eşitsizliğe dönüşür. En büyük değerini ise gözlenebilir bazlarının karşılıklı yansız bazlar olduğu zaman, yani (her $\{|x\rangle, |z\rangle\}$ için) $|\langle x|z\rangle| = 1/\sqrt{d}$ olduğunda alır. Böylece MU sınırı şu değerler arasında yer alır,

$$\frac{1}{d} \leq c \leq 1 \quad veya \quad 0 \leq q_{MU} \leq \log d. \quad (3.12)$$

X ve Z işlemcilerinin çakışma matrisi, tanımlı oldukları Hilbert uzayının boyutu d olmak üzere, $|\langle x|z\rangle|$ elemanlarından oluşan $d \times d$ bir kare matris oluştururlar ve alt

sınır matrisin en büyük değeri 1'dir. Bu ikili-stokastik bir matristir; yani her bir satır ve sütun elemanlarının toplamı 1'dir. Böylece herhangi bir satır (veya sütundaki) en büyük matris elemanı $1/d$ olursa bütün diğer matris elemanları da $1/d$ olmak zorundadır.

3.2 Rényi Entropisi ile EBB

Maassen ve Uffink'in (1988) çalışmasında, EBB'nin aynı zamanda Rényi entropisi için de sağlandığını gösterilmiştir. $\alpha, \beta \geq 1/2$ ve $1/\alpha + 1/\beta = 2$ için,

$$H_\alpha(X) + H_\beta(Z) \geq q_{MU}, \quad (3.13)$$

bağıntısı doğrudur. (3.13) $\alpha, \beta \rightarrow 1$ limitinde (3.7) elde edilebilir. Diğer önemli bir sonuç, $\alpha \rightarrow \infty$ ve $\beta \rightarrow 1/2$ limit değerleridir,

$$H_{\min}(X) + H_{\max}(Z) \geq q_{MU}. \quad (3.14)$$

3.3 Daha Sıkı Bir Sınır: Kübitler

Klasik bilişimde, bilişim faaliyetlerinin maliyeti mesaj başına bit (*bit per message*) ile ölçülür. Kuantum bilişimde ise bitin karşılığına kuantum-bit, kısaca kübit denir ve kuantum bilişim faaliyetlerinin maliyetleri kübitlerle hesaplanır. Klasik bilişimde bir bitin hangi durumda olabileceği kesin iken (1 veya 0), bir kübit ise sonsuz farklı süperpozisyonlar halinde bulunabilir. Kübit sistemleri, Hilbert uzayı $\mathbb{C}^2$ 'de tanımlanır.

σ ile temsil edilen bir kuantum durumunun saflığı $\Pi_\sigma := \text{Tr}(\sigma^2)$ şeklinde tanımlanır. $\text{Tr}(\sigma^2) = 1$ saf durumları temsil eder ve bunun için gerek ve yeter koşul $\sigma^2 = \sigma$; yani σ 'nın saf olmasıdır; $\text{Tr}(\sigma^2) = 1/d$ ise en saf olmayan duruma karşılık gelir ve $1/d \leq \Pi_\sigma \leq 1$ aralığında yer alır. d , Hilbert uzayının boyutudur.

$\{|x\rangle\}_{i=1}^2$ ve $\{|z\rangle\}_{j=1}^2$ sırasıyla X ve Z 'nin bazları olsun. Kübit sisteminin bir ρ durumu için, X ve Z ölçümlerinin olasılıkları sırasıyla $p_i(X) = \langle x_i | \rho | x_i \rangle$ ve $p_j(Z) = \langle z_j | \rho | z_j \rangle$ şeklinde elde edilsin. X , Z ve ρ için saflıklar yazılırsa,

$$\pi_X = \sum_{i=1}^2 (p_i(X))^2, \quad \pi_Z = \sum_{j=1}^2 (p_j(Z))^2 \quad \text{ve} \quad \Pi = \text{Tr}(\rho^2) \quad (3.15)$$

İndirgenmiş saflıklar ise,

$$\bar{\pi}_X = \pi_X - \frac{1}{d}, \quad \bar{\pi}_Z = \pi_Z - \frac{1}{d} \quad \text{ve} \quad \bar{\Pi} = \Pi - \frac{1}{d} \quad (3.16)$$

şeklinde tanımlanır ve $0 \leq \bar{\pi}_X, \bar{\pi}_Z, \bar{\Pi} \leq 1 - 1/d$ aralığında yer alır.

Bir kübit sisteminde, $\{p, 1 - p\}$ gibi bir olasılık dağılımı indirgenmiş saflıklar cinsinden ifade edilebilir (Sanchez-Ruiz 1998),

$$\bar{\pi} = p^2 + (1 - p)^2 - \frac{1}{2} = 2p^2 - 2p + \frac{1}{2}. \quad (3.17)$$

Bu denklemin kökleri $(1 \pm \sqrt{2\bar{\pi}})/2$ çıkar ve entropi şu şekilde yazılabilir,

$$H = -\frac{1 + \sqrt{2\bar{\pi}}}{2} \log \left[\frac{1 + \sqrt{2\bar{\pi}}}{2} \right] - \frac{1 - \sqrt{2\bar{\pi}}}{2} \log \left[\frac{1 - \sqrt{2\bar{\pi}}}{2} \right] = f(\bar{\pi}). \quad (3.18)$$

$f(\bar{\pi})$ monoton azalan ($f'(\bar{\pi}) \leq 0$) ve konkav ($f''(\bar{\pi}) \leq 0$) bir fonksiyondur.

$H(X) + H(Z) = f(\bar{\pi}_X) + f(\bar{\pi}_Z)$ yazılabilir ve daha sıkı bir alt sınır için sağ tarafın minimumu incelenebilir.

$\bar{\pi}_X$ ve $\bar{\pi}_Z$, sabit bir $\bar{\Pi}$ ve $\cos \phi_m = 2c - 1$ olacak şekilde ($c = |\langle x|z \rangle|^2$), ϕ_m ve herhangi bir ϕ açılarının birer fonksiyonu olarak yazılabilir (Larsen 1990);

$$\bar{\pi}_X = \frac{1}{2} \bar{\Pi} [1 + \cos(\phi + \phi_m)] \quad , \quad \bar{\pi}_Z = \frac{1}{2} \bar{\Pi} [1 + \cos(\phi - \phi_m)], \quad (3.19)$$

Böylece,

$$\bar{\pi}_X + \bar{\pi}_Z = \bar{\Pi} \left(1 + \frac{\cos(\phi + \phi_m) + \cos(\phi - \phi_m)}{2} \right) = \bar{\Pi} (1 + \cos \phi \cos \phi_m) \quad (3.20)$$

yazılabilir ve $0 \leq \cos \phi \leq 1$ olduğundan $\bar{\pi}_X + \bar{\pi}_Z \leq \bar{\Pi} (1 + \cos \phi_m)$ sağlanır. $\cos \phi_m$ yerine konulursa,

$$\bar{\pi}_X + \bar{\pi}_Z \leq 2\bar{\Pi}c, \quad (3.21)$$

olur. $f(\bar{\pi})$ 'nin monotonluk özelliği eşitlik durumunda da sağlanmalıdır; yani $\bar{\pi}_X + \bar{\pi}_Z = 2\bar{\Pi}c$ olmalıdır. O zaman entropiler,

$$H(X) + H(Z) = f(\bar{\pi}_X) + f(2\bar{\Pi}c - \bar{\pi}_X) \quad (3.22)$$

şeklinde yazılabilir. $d = 2$ için, $0 \leq \bar{\pi}_X, \bar{\pi}_Z \leq 1/2$ aralığı keskinleştirilirse,

$$\begin{aligned} 0 \leq \bar{\pi}_X, \bar{\pi}_Z \leq 2\bar{\Pi}c \quad , \quad 0 \leq 2\bar{\Pi}c \leq \frac{1}{2} \quad \text{için} \\ 2\bar{\Pi}c \leq \bar{\pi}_X, \bar{\pi}_Z \leq \frac{1}{2} \quad , \quad \frac{1}{2} \leq 2\bar{\Pi}c \leq 1 \quad \text{için} \end{aligned} \quad (3.23)$$

olur. Minimum, $f(\bar{\pi})$ 'nin konkavlığından bulunabilir. Eğer $f(x)$ konkav bir fonksiyonsa ve $a \leq x \leq k - a$ aralığı için

$$f(a) + f(k - a) \leq f(x) + f(k - x) \leq 2f\left(\frac{k}{2}\right) \quad (3.24)$$

ifadesi doğrudur. Burada, $\phi(x) = f(x) + f(k - x)$ olacak şekilde, $\phi'(x) = 0$ olursa $f'(x) = f'(k - x)$ yani $x = k - x$ ve $x = k/2$ olur.

(3.22), (3.24), $x = \bar{\pi}_X$ ve k ve a değerleri (3.23)'deki gibi ele alınırsa,

$$H(X) + H(Z) \geq \begin{cases} \log 2 + f(2\bar{\Pi}c), & 0 \leq 2\bar{\Pi}c \leq \frac{1}{2} \text{ için} \\ f(2\bar{\Pi}c - \frac{1}{2}), & \frac{1}{2} \leq 2\bar{\Pi}c \leq 1 \text{ için} \end{cases} \quad (3.25)$$

elde edilir (Sanchez-Ruiz 1998). Sınır noktaları $f(0) = \log 2$ ve $f(1/2) = 0$ olur. Saf durumların özel durumu için; yani $\bar{\Pi} = 1/2$ olursa, $1/2 \leq 2\bar{\Pi}c \leq 1$ ifadesinden $1/2 \leq c \leq 1$ olur ve (3.25)'in ikinci satırından durum bağımsız bir sonuç elde edilebilir,

$$\begin{aligned} H(X) + H(Z) &\geq f\left(c - \frac{1}{2}\right) \\ &= -\frac{1 + \sqrt{2c - 1}}{2} \log\left(\frac{1 + \sqrt{2c - 1}}{2}\right) \\ &\quad - \frac{1 - \sqrt{2c - 1}}{2} \log\left(\frac{1 - \sqrt{2c - 1}}{2}\right) \\ &= h_{bin}\left(\frac{1 + \sqrt{2c - 1}}{2}\right) := q_{SR}. \end{aligned} \quad (3.26)$$

Aslında bu sonuç bütün aralıkları kapsamadığı için optimal bir sonuç olarak ele alınmamaktadır. Ancak kendi aralığında MU bağıntısının güçlendirilmiş hali olarak ele alınabilir.

3.4 Daha Sıkı Bir Sınır: Saf Olmayan Durumlar

Berta v.d (2010) bir hafıza sistemi olduğunda, eğer sistemler arasında dolanıklık mevcutsa, EBB için alt sınırın indirgenebileceğini göstermiştir. Bu sonuca (1.10)'da yer verilmişti,

$$H(X|B) + H(Z|B) \geq \log \frac{1}{c} + S(A|B). \quad (3.27)$$

Çok parçalı bir sistemde, alt sistemlerden birinin dışarlanması entropiyi azaltmaz (Lieb ve Ruskai 1973); yani $H(X) \geq H(X|B)$, $H(Z) \geq H(Z|B)$, $S(\rho_A) \geq S(A|B)$ olur ve aşağıdaki bağıntıya ulaşılır,

$$H(X) + H(Z) \geq \log \frac{1}{c} + S(\rho_A), \quad (3.28)$$

Bu bağıntı aynı zamanda bağıl entropinin kuantum kanallar altında monotonluğundan türetilir:

Yapılacak olan tam ölçümler $\mathcal{X}(\cdot) = \sum_x |x\rangle\langle x|(\cdot)|x\rangle\langle x|$ ve $\mathcal{Z}(\cdot) = \sum_z |z\rangle\langle z|(\cdot)|z\rangle\langle z|$ şeklinde kuantum kanaldır. Seçici olmayan ölçümler olarak da adlandırılan tam ölçümlerde, tek tek ölçüm sonuçlarına değil, tüm ölçümlerin bütüncül etkisine bakılır. Başlangıç durumu ρ_A ise, tam ölçüm sonucunda sistemin durumu $\mathcal{X}(\rho_A) = \sum_x |x\rangle\langle x|\rho_A|x\rangle\langle x| = \rho_X$ olacaktır. Bu köşegen elemanları $p_X(x) = \langle x|\rho_A|x\rangle$ olan bir köşegen matristir; yani ölçüm sonrası durum spektral ayrışımıyla ortaya çıkar ve $\log(\mathcal{X}(\rho_A)) = \sum_x \log p_X(x)|x\rangle\langle x|$ yazılabilir. Bu durumda çıkışın von Neumann entropisi, $p_X(x)$ olasılıklarının $H(X)$ Shannon entropisine eşittir: $H(X) = S(\mathcal{X}(\rho_A))$,

$$\begin{aligned} S(\mathcal{X}(\rho_A)) &= -\text{Tr}(\mathcal{X}(\rho_A) \log \mathcal{X}(\rho_A)) = \text{Tr}(\rho_X \log \rho_X) \\ &= -\sum_{x,x'} \text{Tr}(|x\rangle\langle x|\rho_A|x\rangle\langle x|x'\rangle\langle x'|\log p_X(x)|x'\rangle\langle x'|). \end{aligned}$$

İzdeşim ölçüm elemanları dik; yani $\langle x|x'\rangle = \delta_{x,x'}$ ve $|x\rangle\langle x|x\rangle\langle x| = |x\rangle\langle x|$ (*idempotent*) olduğundan yukarıdaki bağıntı şu hali alır:

$$\begin{aligned} S(\mathcal{X}(\rho_A)) &= -\sum_x \text{Tr}(\rho_A|x\rangle\langle x|\log p_X(x)|x\rangle\langle x|) \\ &= -\text{Tr}(\rho_A \log \mathcal{X}(\rho_A)) \end{aligned}$$

Böylece, ekleme çıkarma yapılarak;

$$\begin{aligned} S(\mathcal{X}(\rho_A)) &= -\text{Tr}(\rho_A \log \mathcal{X}(\rho_A)) - \text{Tr}(\rho_A \log \rho_A) + \text{Tr}(\rho_A \log \rho_A) \\ &= D(\rho_A \| \mathcal{X}(\rho_A)) + S(\rho_A), \end{aligned}$$

yazılabilir ve buradan çıkış ve giriş durumlarının entropileri arasındaki fark bağıl entropi cinsinden aşağıdaki gibi bulunur,

$$D(\rho_A \| \mathcal{X}(\rho_A)) = S(\mathcal{X}(\rho_A)) - S(\rho_A). \quad (3.29)$$

Bağıl entropi daima pozitif olduğundan, çıkış yani tam ölçüm sonrası durumun entropisi girişin entropisinden daima büyüktür. Bunun nedeni tam ölçümlerin ünital kanal (birimi koruyan: $\mathcal{X}(\mathbb{1}) = \mathbb{1}$) olmasındandır. Genel olarak kanal etkisinden sonra entropi artabilir de azabilir de. Fakat ünital kanallar daima entropiyi arttırır (Nielsen ve Chuang 2010).

$\mathcal{X}$ kanalı uygulandıktan sonra $\mathcal{Z}$ de uygulanırsa monotonluk özelliğinden:

$$\begin{aligned} D(\rho_A \| \mathcal{X}(\rho_A)) &\geq D(\mathcal{Z}(\rho_A) \| \mathcal{Z} \circ \mathcal{X}(\rho_A)) \\ &= D(\rho_Z \| \mathcal{Z} \circ \mathcal{X}(\rho_A)) \end{aligned} \quad (3.30)$$

elde edilir. Burada $\mathcal{Z} \circ \mathcal{X}(\rho_A) = \sum_z \left(\sum_x |\langle x|z\rangle|^2 \langle x|\rho_A|x\rangle \right) |z\rangle\langle z|$ olup bunun logaritması şöyledir: $\log [\mathcal{Z} \circ \mathcal{X}(\rho_A)] = \sum_z [\log (\sum_x |\langle x|z\rangle|^2 \langle x|\rho_A|x\rangle)] |z\rangle\langle z|$.

Buna göre (3.30) bağıntısının sağ tarafından,

$$\begin{aligned} D(\rho_Z \| \mathcal{Z} \circ \mathcal{X}(\rho_A)) &= \text{Tr}(\rho_Z \log \rho_Z) - \text{Tr}(\rho_Z \log \mathcal{Z} \circ \mathcal{X}(\rho_A)) \\ &= -H(Z) - \sum_z \langle z|\rho_A|z\rangle \log \left[\sum_x |\langle x|z\rangle|^2 \langle x|\rho_A|x\rangle \right] \\ &\geq -H(Z) - \sum_z \langle z|\rho_A|z\rangle \log \left[c \sum_x \langle x|\rho_A|x\rangle \right] \end{aligned} \quad (3.31)$$

elde edilir ve eşitsizlik log fonksiyonunun monotonluk özelliğinden gelmektedir.

Burada $c = \max_{x,z} |\langle x|z\rangle|^2$ olarak tanımlanır. Son satırdaki ifade Denk.(3.29) ile birleştirilirse şu sonuca ulaşılır (Coles v.d 2017, Appendix-B),

$$H(X) + H(Z) \geq q_{MU} + S(\rho_A). \quad (3.32)$$

Bu, EBB'nin durum bağımlığını da vurgulayan daha genel ifadesidir. ρ_A bir saf durum değilse, $S(\rho_A) > 0$ olur. Örneğin, $\rho_A = \mathbb{1}/d$ en saf olmayan durumda ise, $S(\rho_A) = \log d$ en büyük değerini alır. Böylece, (3.32)'nin sağ tarafı q_{MU} sınırından daha güçlü bir sınır olur. Ancak Bölüm (3.1)'de öne sürülen EBB'nin alt sınırının başlangıç durumundan bağımsız olduğu savı kaybedilmiş olur. Eğer A saf durumda ise, $S(\rho_A) = 0$ olur ve sağ taraf MU sınırına indirgenir.

3.5 Daha Sıkı Bir Sınır: Keyfi boyutlar

Keyfi boyutlarda, $d > 2$, alt sınırın geliştirilmesi, kübitlerden daha karmaşıktır çünkü d büyüdükçe çakışma matrisi daha çok parametreye bağlı olmaktadır. Coles

ve Piani (2014) yüksek boyutlarda çakışma matrisinin ikinci büyük elemanın, c_2 , alt sınır içerisinde yer aldığını göstermiştir,

$$q_{CP} := q_{MU} + \frac{1}{2}(1 - \sqrt{c}) \log \frac{c}{c_2}. \quad (3.33)$$

$d = 2$ ve $c = 1/2$ değerinde $q_{CP} = q_{MU}$ olur. $d > 2$, örneğin $d = 3$ için incelenirse, $q_{CP} > q_{MU}$ olduğu görülebilir. Bu bağıntı EK-6'da ayrıntılı olarak incelenmiştir.

Örnek 3.1 $d = 3$ için X ve Z arasındaki dönüşüm matrisi şöyle olsun,

$$U = \begin{pmatrix} 1/\sqrt{3} & 1/\sqrt{3} & 1/\sqrt{3} \\ 1/\sqrt{2} & 0 & -1/\sqrt{2} \\ 1/\sqrt{6} & -\sqrt{2/3} & 1/\sqrt{6} \end{pmatrix} \quad (3.34)$$

$q_{MU} = \log(3/2) \approx 0.58$ iken $q_{CP} = \log(3/2) + 1/2(1 - \sqrt{2/3}) \log[(2/3)/(1/2)] \approx 0.64$ olur, böylece $q_{CP} > q_{MU}$ olduğu görülebilir.

3.6 POVM ile Keyfi Ölçümler

EK-3'te, MU sınırının ispatı yapılmış ve izdüşüm işlemcileri kullanılmıştır. Bu seçim keyfi olup, POVM için de geçerli olduğu gösterilmelidir.

Bir $|\psi\rangle$ durumuna uygulanan X ve Z izdüşüm ölçümlerinden sonraki boylandırılmış $|x_i\rangle$ ve $|z_j\rangle$ durumları aşağıdaki gibidir,

$$|x_i\rangle = \frac{X_i |\psi\rangle}{\|X_i \psi\|} \quad \text{ve} \quad |z_j\rangle = \frac{Z_j |\psi\rangle}{\|Z_j \psi\|}. \quad (3.35)$$

Burada $\|\cdot\|$ norm olarak adlandırılır ve herhangi bir $\mathbf{x} = (x_1, \dots, x_d)$ vektörü için, $\mathbb{C}^d$ uzayında p-norm,

$$\|\mathbf{x}\|_p = \begin{cases} \left(\sum_{i=1}^d |x_i|^p \right)^{1/p} & \text{eğer } 1 \leq p < \infty \\ \max_{1 \leq i \leq d} |x_i| & \text{eğer } p = \infty. \end{cases} \quad (3.36)$$

olarak tanımlanır. (3.35)'teki norm ifadesi 2-norm olarak ele alınmalıdır, çünkü $\|X_i \psi\| = \sqrt{\langle \psi | X_i | \psi \rangle}$ olmaktadır (Bknz. (2.13)).

Böylece (3.35) ve MU bağıntısından ($c = \max_{i,j} |\langle x_i | z_j \rangle|^2$),

$$H(X) + H(Z) \geq -2 \log \max_{i,j} \frac{|\langle \psi | X_i Z_j | \psi \rangle|}{\|X_i \psi\| \|Z_j \psi\|}, \quad (3.37)$$

yazılabilir.

Bu sefer X ve Z birer POVM olarak seçilsin: $X = \{X_i \geq 0 : \sum_i X_i = \mathbb{1}_{\mathcal{H}}\}$. Naimark teoremi'nden, sonlu Hilbert uzayları için $\mathcal{H} \oplus \mathcal{K}$ formunda genişletilmiş bir Hilbert uzayı $\tilde{\mathcal{H}}$ her zaman vardır ve $\mathcal{H}$ 'de tanımlı bir POVM, $\tilde{\mathcal{H}}$ 'da bir izdüşüm işlemcisi olarak düşünülebilir (Parthasarathy 1999). Burada $\oplus$ vektör uzaylarının dik direk toplamını (*orthogonal direct sum*) göstermektedir. Bu genişletme X ve Z POVM'ları için yapılacak olunursa, X POVM'u için şu yazılabilir:

$$\tilde{X}_1 = \begin{pmatrix} X_1 & 0 \\ 0 & \mathbb{1}_{\mathcal{K}} \end{pmatrix} \quad \text{ve} \quad \tilde{X}_i = \begin{pmatrix} X_i & 0 \\ 0 & 0 \end{pmatrix}, \quad 2 \leq i \leq m \text{ için.} \quad (3.38)$$

Burada $\mathbb{1}_{\mathcal{K}}$, $\mathcal{K}$ 'nin birim operatörüdür. $\sum_{i=1}^m \tilde{X}_i = \mathbb{1}_{\mathcal{H} \oplus \mathcal{K}}$ tamlik bağıntısını sağlar ve aynı ifade bir Z POVM'u için de yazılabilir. Genişletilmiş uzaydaki bir ρ işlemcisi şöyle ifade edilir:

$$\tilde{\rho} = \begin{pmatrix} \rho & 0 \\ 0 & 0 \end{pmatrix} \quad \text{veya} \quad \tilde{\psi} = \begin{pmatrix} \psi \\ 0 \end{pmatrix}. \quad (3.39)$$

$Tr(\tilde{\rho}\tilde{X}) = Tr(\rho X)$ ifadesi doğru olur ve $\tilde{Z}$ için de geçerlidir. O zaman (3.37) bağıntısı yeniden yazılabilir,

$$H(X) + H(Z) \geq -2 \log \max_{i,j} \frac{|\langle \psi | X_i Z_j | \psi \rangle|}{\left\| X_i^{\frac{1}{2}} \psi \right\| \left\| Z_j^{\frac{1}{2}} \psi \right\|}. \quad (3.40)$$

Aşağıdaki iç çarpımdan,

$$\begin{aligned} |\langle \psi | X_i Z_j | \psi \rangle| &= |\langle X_i^{\frac{1}{2}} \psi | X_i^{\frac{1}{2}} Z_j^{\frac{1}{2}} | Z_j^{\frac{1}{2}} \psi \rangle| \\ &\leq \left\| \langle X_i^{\frac{1}{2}} \psi | X_i^{\frac{1}{2}} Z_j^{\frac{1}{2}} \right\| \left\| Z_j^{\frac{1}{2}} | \psi \rangle \right\| \\ &\leq \left\| X_i^{\frac{1}{2}} Z_j^{\frac{1}{2}} \right\| \left\| X_i^{\frac{1}{2}} | \psi \rangle \right\| \left\| Z_j^{\frac{1}{2}} | \psi \rangle \right\|, \end{aligned} \quad (3.41)$$

eşitsizliği elde edilebilir. Burada ikinci satır CBS eşitsizliğinden, üçüncü satır ise bir matris ve bir vektörün $\|X | \psi \rangle\| \leq \|X\| \| | \psi \rangle \|$ alt çarpım özelliğinden gelmektedir.

Böylece (3.41)'den POVM için belirsizlik bağıntısı şu şekilde elde edilir:

$$H(X) + H(Z) \geq -2 \log \max_{i,j} \left\| X_i^{\frac{1}{2}} Z_j^{\frac{1}{2}} \right\|. \quad (3.42)$$

$c = \max_{i,j} c_{ij}$, $c_{ij} = \left\| X_i^{\frac{1}{2}} Z_j^{\frac{1}{2}} \right\|$, sonucu hala MU sınırmı korur. Burada önemli bir sonuç tek POVM için belirsizliğin olabileceğidir. Eğer $X = Z$ kabul edilirse, (3.42) şu forma dönüşür,

$$H(X) \geq -\log \left\{ \max_{i,j} \left\| X_i^{\frac{1}{2}} X_j^{\frac{1}{2}} \right\| \right\}. \quad (3.43)$$

Bu ifade sağ tarafın sıfır olmadığında, POVM elemanları arasında belirsizlik olacağını göstermektedir.

3.7 Çoğullama Yaklaşımı ve EBB

Konveks analiz, olasılık kuramı v.b. alanlarda sıklıkla kullanılan çoğullama (*majorization*) bağıntısının tanımı şöyledir.

Tanım 3.1 (Çoğullama) $\mathbf{x} = \{x_i\}_{i=1}^d$, $\mathbf{y} = \{y_i\}_{i=1}^d \in \mathbb{R}^d$ de tanımlı bileşenleri gerçel sayılardan oluşan birer vektör olsun. $\mathbf{x}$, $\mathbf{y}$ tarafından çoğullanır denir, eğer

$$\sum_{i=1}^k x_i^\downarrow \leq \sum_{i=1}^k y_i^\downarrow \quad (1 \leq k \leq d-1 \text{ için}) \quad \text{ve} \quad \sum_{i=1}^d x_i^\downarrow = \sum_{i=1}^d y_i^\downarrow \quad (3.44)$$

koşulları sağlanıyorsa.

Burada aşağı yönlü ok, bileşenlerin $x_1 \geq x_2 \geq \dots \geq x_{d-1}$ olacak şekilde büyükten küçüğe sıralandığını göstermektedir. Eğer $\mathbf{x}$, $\mathbf{y}$ tarafından çoğullanıyorsa $\mathbf{x} \prec \mathbf{y}$ şeklinde gösterilir. Bu tanım $\mathbf{x}$ ve $\mathbf{y}$ birer olasılık vektörü olduğunda da geçerlidir. Bileşenleri pozitif ve toplamaları 1 olan vektörler olasılık vektörleridir.

Olasılıkların yerlerini değiştirmek Shannon entropisinin değerini değiştirmez ve belirsizliği azaltmaz. Buna rasgele yeniden etiketleme altında monotonluk (*monotonicity under random relabeling*) denir. Bu özelliği taşıyan herhangi bir belirsizlik ölçüsü kullanılarak, çoğullama ile indirgenmiş parçalı kısımlarda belirsizlik bağıntıları elde edilebilir. Bu koşulu sağlayan fonksiyonlar, *Schur-konkav fonksiyonların* bir sınıfıdır (Shannon, Rényi entropisi v.b.) (Friedland v.d 2013).

Şimdi, ρ bir yoğunluk işlemcisi olsun ve aynı uzayda $K = \{|k_m\rangle \langle k_m|\}_{m=1}^d$ ve $L = \{|l_n\rangle \langle l_n|\}_{n=1}^d$ izdüşüm operatörleri tanımlansın. Olasılıklar $p_m(\rho) = \text{Tr}[\rho |k_m\rangle \langle k_m|]$ ve $q_n(\rho) = \text{Tr}[\rho |l_n\rangle \langle l_n|]$ olsun ve karşılık gelen olasılık vektörleri de $\mathbf{p} = \{p_m(\rho)\}_{m=1}^d$ ve $\mathbf{q} = \{q_n(\rho)\}_{n=1}^d$ şeklinde yazılsın.

Amaç, $\mathbf{p}$ ve $\mathbf{q}$ için ortak bir belirsizlik alt sınırı bulmaktır. Bileşik olasılık vektörü $\mathbf{p} \otimes \mathbf{q} \in \mathbb{R}^{d^2}$ şeklinde yazılabilir ve bileşik olasılık dağılımını temsil eder. Varsayalım ki, $\boldsymbol{\omega} \in \mathbb{R}^{d^2}$ 'de tanımlı, ρ 'dan bağımsız herhangi bir olasılık vektörü olsun ve $\mathbf{p} \otimes \mathbf{q}$ çarpımını çoğulladığı varsayalım,

$$\mathbf{p} \otimes \mathbf{q} \prec \boldsymbol{\omega}. \quad (3.45)$$

Her $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ için, $\Lambda(\mathbf{x}) \geq \Lambda(\mathbf{y}) \leftrightarrow \mathbf{x} \prec \mathbf{y}$, olacak şekilde bir $\Lambda : \mathbb{R}^d \rightarrow \mathbb{R}$ belirsizlik ölçüsü tanımlansın ve (3.45) üzerine uygulansın,

$$\Lambda(\mathbf{p} \otimes \mathbf{q}) \geq \Lambda(\boldsymbol{\omega}) \quad (3.46)$$

Belirsizlik ölçüsü tensör çarpımı altında toplamsal özelliğe sahip ise (Rényi veya Shannon entropisi gibi), ifade yeniden düzenlenebilir.

$$\Lambda(\mathbf{p}) + \Lambda(\mathbf{q}) \geq \Lambda(\boldsymbol{\omega}). \quad (3.47)$$

Rényi entropisi için düzenlenirse;

$$H_\alpha(\mathbf{p}) + H_\alpha(\mathbf{q}) \geq H_\alpha(\boldsymbol{\omega}) \quad (3.48)$$

olur. (3.4) özdeşliğinden, min entropi için şu sonuca ulaşılır (Friedland v.d 2013),

$$p_{\text{tahm}}(X) \cdot p_{\text{tahm}}(Z) \leq \left(\frac{1+c}{2}\right)^2 \quad \text{veya} \quad H_{\min}(X) + H_{\min}(Z) \geq -2 \log \left(\frac{1+c}{2}\right). \quad (3.49)$$

Bu yaklaşımın ele alınmasının nedeni, yukarıdaki koşulları sağlayan bütün belirsizlik ölçülerine genellebilmesi ve EBB'yi de içermesidir.

3.8 Tahmin Oyunu

Bob, ρ_A durumunda hazırladığı bir A sistemini Alice'e gönderir. Alice, elinde bulunan X ve Z ölçümlerinden birini rasgele seçerek ρ_A durumu üzerine uygular. Elde ettiği sonuç K 'yi kaydeder ve $\Theta \in \{\theta_X, \theta_Z\}$ ile temsil edilen baz seçimini Bob'a yollayarak K sonucunu tahmin etmesini ister.

MU sınırı, Bob'un tahmin yeteneği üzerine bir kısıtlama getirir. A sistemi üzerinde $\{|k\rangle\}_{k=1}^d$ olacak şekilde bir standart baz olsun ve seçilen ölçüm kümesi U_X ve U_Z

üniter dönüşümleri ile bu baz kümesinden türetilirsin,

$$|X^k\rangle = U_X |k\rangle \quad ve \quad |Z^k\rangle = U_Z |k\rangle. \quad (3.50)$$

Bob'un θ_X bazını seçmesi koşulunda, koşullu olasılık dağılımı,

$$p_{K|\Theta=\theta_X}(k) = \langle k|U_X^\dagger \rho_A U_X |k\rangle \quad k \in \{1, \dots, d\} \text{ için}, \quad (3.51)$$

şeklinde elde edilir ve benzer bir yazım θ_Z için de yazılabilir. En genel hali ile olasılıklar,

$$p_{K|\Theta=\theta_j}(k) = \frac{1}{2} \langle k|U_j^\dagger \rho_A U_j |k\rangle \quad , \quad j = 1, 2 \text{ ile}, \quad (3.52)$$

şeklinde yazılabilir. Burada $1/2$ değeri, iki elemanlı bir baz kümesinin elemanlarından herhangi birinin rasgele seçilme olasılığıdır. $\Theta \in \{\theta_X, \theta_Z\}$ seçilmesi durumunda K sonucunu bulma belirsizliği, koşullu Shannon entropisi, yazılırsa,

$$\begin{aligned} H(K|\Theta) &= H(K\Theta) - H(\Theta) \\ &= \frac{1}{2} [H(K|\Theta = \theta_X) + H(K|\Theta = \theta_Z)], \end{aligned} \quad (3.53)$$

olur ve MU bağıntısı,

$$\frac{1}{2} [H(K|\Theta = \theta_X) + H(K|\Theta = \theta_Z)] \geq \frac{1}{2} q_{MU}, \quad (3.54)$$

şeklinde elde edilir. Böylece,

$$H(K|\Theta) \geq \frac{1}{2} q_{MU}, \quad (3.55)$$

yazılabilir. Alice, sıra değişmeyen gözlenebilirleri seçmişse yani $q_{MU} > 0$ ise Bob, K sonucunu hiçbir zaman kesin olarak bilemez ve MU sınırının getirdiği kısıtlama gösterilmiş olur.

3.9 Çoklu Ölçüm Kümeleri

Bir önceki bölüme benzer bir notasyon kullanarak, bir $\Theta = \{\theta_j\}_{j=1}^d$ ölçüm kümesi için (3.55)'e benzer bir alt sınır elde edilmelidir,

$$H(K|\Theta) \geq f(\Theta, \rho) > 0 \quad , \quad \Theta = \{\theta_1, \dots, \theta_m\} \text{ için}, \quad (3.56)$$

ve olasılık dağılımı da Denk.(3.52)'ye benzer şekilde;

$$p_{K|\Theta}(k, \theta_j) = \frac{1}{L} \langle k | U_j^\dagger \rho U_j | k \rangle \quad , \quad k \in \{1, \dots, L\} \text{ ve } j \in \{1, \dots, d\} \text{ için} \quad (3.57)$$

elde edilir. Koşullu entropi tekrar yazılırsa

$$H(K|\Theta) = \frac{1}{L} \sum_{j=1}^L H(K|\Theta = \theta_j). \quad (3.58)$$

şeklinde ifade edilebilir. Başlangıç olarak bir ölçüm kümesinin ikili elemanları ele alınabilir,

Örnek 3.2 $\{\sigma_x, \sigma_y, \sigma_z\}$ ölçüm kümesinin ikili kombinasyonları $\{\sigma_x, \sigma_y\}, \{\sigma_x, \sigma_z\}, \{\sigma_y, \sigma_z\}$ için tahmin oyununa benzer bir kurulum ve (3.28) ele alınırsa;

$$H(K|\Theta) \geq \frac{1}{2} + \frac{1}{2}H(\rho_a) \quad , \quad \Theta = \{\sigma_x, \sigma_y, \sigma_z\} \text{ için} \quad (3.59)$$

elde edilir ve bütün ikili kombinasyonlar için geçerlidir.

Daha genel bir ifade için KYB kullanılabilir. d boyutlu bir Hilbert uzayında, $d + 1$ tane KYB'nin bir tam kümesi bulunur. d bir asal kuvvet ve ölçüm kümesi $d + 1$ tane KYB'nin bir tam kümesi için aşağıdaki sonuç çıkmaktadır (Sanchez-Ruiz 1993).

$$H(K|\Theta) \geq \log(d + 1) - 1 \quad (d \text{ tek ise}) \quad (3.60)$$

Bu bağıntı $H_{\text{carp}}(K|\Theta)$ 'dan türetilir ve çarpışma entropisi için şu ifade yazılabilir (Ballester v.d. 2008):

$$H_{\text{carp}}(K|\Theta) = \log(d + 1) - \log(2^{-H_{\text{carp}}(K|\Theta=\theta_j)} + 1) \quad , \quad \Theta = \{\theta_1, \dots, \theta_{d+1}\} \text{ için.} \quad (3.61)$$

Rényi entropisi α -monotondur ve $H(M|\Theta) \geq H_{\text{carp}}(M|\Theta)$ yazılabilir.

Daha geniş bir genelleme için $d + 1$ tane KYB yerine, $L < d + 1$ tane KYB'nin genelleştirilmiş kümeleri ele alınabilir. Örneğin, Hilbert uzayının boyutu $d = p^{2l}$ bir asal kuvvet ise, $l \in \mathbb{N}$ için, $L = p^l + 1$ olacak şekilde KYB'nin bir kümesi vardır (Ballester and Wehner 2007). $d \geq 2$ için $\mathcal{B} = \{B_1, \dots, B_d\}$, KYB'nin bir kümesi olsun ve U_t , $\{|k\rangle\}_{k=1}^d$ ve $\{|l\rangle\}_{l=1}^d$ bazları ile $\mathcal{B}$ 'nin elemanlarını oluşturabilsin. O zaman,

$$\Theta = \{U_t |k\rangle \otimes U_t^* |l\rangle \mid k, l \in [d]\} \quad (3.62)$$

gibi bir ölçüm kümesi tanımlanabilir ve bu küme $\mathcal{H}^d \otimes \mathcal{H}^d$ 'de tanımlı KYB'nin bir kümesi olur. En dolanık durum $|\psi\rangle = 1/\sqrt{d} \sum_{k,l=1}^d |k\rangle \otimes |l\rangle$ ve $U \otimes U^* |\psi\rangle = |\psi\rangle$ için,

$$\begin{aligned}
\langle \psi | U \otimes U^* | \psi \rangle &= \frac{1}{d} \sum_{k,l=1}^d \langle k | U | l \rangle \langle k | U^* | l \rangle \\
&= \frac{1}{d} \sum_{k,l=1}^d \langle k | U | l \rangle \langle l | U^\dagger | k \rangle \\
&= \frac{1}{d} \text{Tr} U U^\dagger = 1,
\end{aligned} \tag{3.63}$$

olur. Herhangi bir U_t için,

$$\begin{aligned}
H(K|\Theta) &= - \sum_{kl} |\langle kl | U_t \otimes U_t^* | \psi \rangle|^2 \log |\langle kl | U_t \otimes U_t^* | \psi \rangle|^2 \\
&= - \sum_{kl} |\langle kl | \psi \rangle|^2 \log |\langle kl | \psi \rangle|^2 \\
&= \log \sqrt{d} = \frac{\log d}{2}
\end{aligned} \tag{3.64}$$

olur ve daha fazla belirsizlik gözlenmez. Yani karşılıklı yansızlığın miktarı en üst sınır için gerekli ancak yetersiz bir koşuldur. $L < d + 1$ 'in küçük kümeleri için ise MU bağıntısı kullanılarak şu sonuca ulaşılabilir,

$$H(K|\Theta) \geq \frac{\log d}{2}. \tag{3.65}$$

4. BİR HAFIZA SİSTEMİ VARLIĞINDA EBB

Bir hafıza sistemi, ölçüm yapılan sistemle korelasyon (*correlation*) halinde olan yardımcı (*ancilla, auxiliary*) sistemler olarak ele alınabilir. Bu sistemler kuantum yan bilişim (*quantum side information*) olarak da adlandırılır.

Öncelikle klasik ve kuantum hafıza arasındaki farklar incelenecek ve hafıza sistemi varlığında koşullu entropiler incelenecek, sonra da hafızanın belirsizliği nasıl etkilediği tartışılacaktır.

4.1 Klasik ve Kuantum Hafıza

Bir kuantum sisteminin klasik veya kuantum hafıza ile korelasyon halinde olmasının farkı aşağıdaki örneklerle açıklanabilir.



Şekil 4.1. Klasik hafıza; bir madeni para ile bir spin-1/2 parçacığı arasında klasik korelasyonlar olarak gibi tasvir edilebilir. (Coles v.d 2017)

Örnek 4.1 A sistemi, $Z = \{|0\rangle, |1\rangle\}$ olmak üzere bir spin-1/2 parçacık ve B sistemi bir madeni para olsun. Parçacığın durumu, yazı gelme durumunda $|0\rangle$, tura gelme durumunda ise $|1\rangle$ olacak şekilde hazırlanmışsa ölçümden önce AB sisteminin durumu şöyle betimlenebilir:

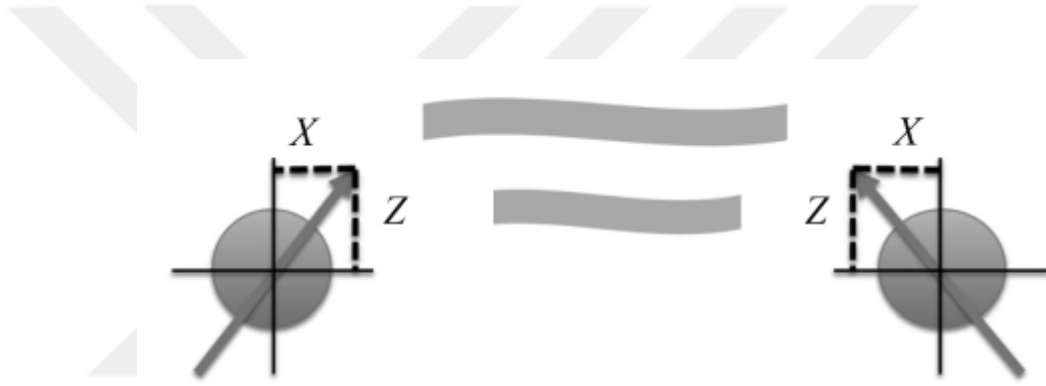
$$\rho_{AB} = \frac{1}{2} (|0\rangle\langle 0|_A \otimes \rho_B^0 + |1\rangle\langle 1|_A \otimes \rho_B^1). \quad (4.1)$$

Bu bir klasik-kuantum yoğunluk işlemcisidir ve $Tr[\rho_B^0 \rho_B^1] = 0$ olup birbirlerini dışlamaktadırlar. Burada, B 'yi elinde tutan bir gözlemci, A 'nın durumunu

kesin olarak bilebilir, çünkü B 'nin durumu, A 'yı belirlemektedir. B gözlemciden saklanırsa, A 'nın durumunu tahmin etmeye çalışan gözlemci için doğru tahmin olasılığı $1/2$ olacaktır.

Burada B ile sadece Z ölçümü ilişkilendirilmiştir. Yani Z ile sıra değişmeyen bir ölçüm yapılırsa, gözlemci B 'ye sahip olsa bile A üzerindeki belirsizlik azalmaz. Klasik hafıza, uyumsuz ölçümlerle alakalı alt sınırı etkilemez.

Şimdi başka bir C sistemi ile A iki özdeş parçacık olsun ve aralarında bütün korelasyonlar (klasik ve kuantum) var olsun. Böyle bir durumda C kuantum yan bilişim olur ve bazı durumlarda klasik hafızayı da barındırır.



Şekil 4.2. Kuantum hafıza; bir elektronun spininin X ve Z bileşenlerinin başka bir elektronun spininin X ve Z bileşenleri ile korelasyon halinde olması gibi tasvir edilebilir. Böylece sağdaki elektron bir kuantum hafıza, kuantum yan bilişim olur.

Örnek 4.2 İki spin-1/2 parçacıktan oluşan iki-kübit sistemi (A ve C) aşağıdaki Bell durumu ile temsil edilsin:

$$|\phi_{AC}^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle_{AC} + |11\rangle_{AC}). \quad (4.2)$$

C 'deki parçacığın $|0\rangle$ veya $|1\rangle$ durumu için A 'daki parçacık sırasıyla $|0\rangle$ veya $|1\rangle$ durumunda olacaktır. Klasik hafızaya benzer olarak, C 'yi elinde tutan gözlemci A 'daki parçacığın durumu ile ilgili kesin tahminde bulunabilir. Ancak, klasik hafızanın tersine, gözlemci C 'yi sadece $Z = \{|0\rangle, |1\rangle\}$ ile değil, $X = \{|+\rangle, |-\rangle\}$ ile

de ölçebilir, çünkü (4.2),

$$\begin{aligned}
|\phi_{AC}^+\rangle &= \frac{1}{\sqrt{2}} (|00\rangle_{AC} + |11\rangle_{AC}) \\
&= \frac{1}{2\sqrt{2}} [(|+\rangle + |-\rangle)_A \otimes (|+\rangle + |-\rangle)_C] + [(|+\rangle - |-\rangle)_A \otimes (|+\rangle - |-\rangle)_C] \\
&= \frac{1}{\sqrt{2}} (|++\rangle_{AC} + |--\rangle_{AC}).
\end{aligned} \tag{4.3}$$

şeklde de yazılabilir. Burada $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ olarak tanımlanan σ_X 'in öz durumlarıdır. Yani gözlemci C 'yi elinde tuttuğu müddetçe, A hakkında X ölçümü yaparak da bilgi edinebilir. Aslında bu gözlem X dışındaki herhangi bir ölçüm için de geçerlidir.

Bu noktada doğal olarak şu soru sorulabilir: Bir kuantum hafıza varlığında, sıra değişmeyen gözlenebilirler yüksek kesinlikle ölçülebilir mi?

4.2 Koşullu Entropiler

Kuantum hafıza B 'ye sahip bir gözlemci olsun ve ilk olarak (4.1)'dekine benzer klasik-kuantum durum ele alınsın. B ile korelasyon halinde bulunan bir klasik kayıt (*register*) K sisteminin ortak durumu aşağıdaki gibi ifade edilebilir:

$$\rho_{KB} = \sum_k p_K(k) |k\rangle \langle k|_K \otimes \rho_B^k. \tag{4.4}$$

Burada ρ_B^k , $K = k$ koşulunda B 'nin durumunu göstermektedir. Eğer gözlemci B 'ye sahip ise üzerinde ölçümler yaparak tahminini kesinleştirebilir. Bunun için en yüksek tahmin olasılığı p_{tahm} ele alınır ve B üzerine bir $\{X_B^k\}_{k=1}^d$ POVM uygulanırsa:

$$p_{tahm}(K|B) := \max_{X_B} \sum_k p_K(k) Tr[X_B^k \rho_B^k], \tag{4.5}$$

olur ve koşullu min-entropi yazılabilir (Renner 2005, König v.d. 2009):

$$H_{min}(K|B) = -\log p_{tahm}(K|B). \tag{4.6}$$

(4.5) ifadesindeki $Tr[X_B^k \rho_B^k]$, ρ_B^k durumunun X_B^k ölçümü koşulunda k çıkma olasılığıdır. Bu ifade gözlemci için K 'nın belirsizliğini nicelendirir. Küçük tahmin olasılıklarında yani yüksek koşullu min-entropi durumunda K 'nın değerini tahmin etmek daha zordur.

Kuantum koşullu entropi, (2.4)'te daha önce tanımlanmıştı:

$$S(K|B) := S(\rho_{KB}) - S(\rho_B) \quad (4.7)$$

(4.4)'ten ρ_B indirgenmiş durumu şöyle elde edilir:

$$\rho_B = \text{Tr}_K[\rho_{KB}] = \sum_k p_K(k) \rho_B^k.$$

von Neumann entropisinin, tahmin olasılığı gibi direk bir yorumu yoktur. Ancak, örneğin Alice elinde bulunan sistemin olasılık dağılımı ile ilgili bir parçayı Bob'a yollarsa $S(K|B)$ niceliği, K 'nın değerinin bulunabilmesi için Alice'in Bob'a göndermesi gereken minimum bilgi miktarı olarak tanımlanır.

Klasik-kuantum koşullu entropi, kuantum koşullu entropinin özel bir durumudur ve operasyonel açıdan Rényi entropileri incelenecek olunursa, tamamen kuantum min entropi dolanıklıkla ilişkilidir ve aşağıdaki gibi tanımlanır (Coles v.d 2017),

$$H_{min}(A|B) := -\log[d_A \cdot F(A|B)]. \quad (4.8)$$

Burada,

$$F(A|B) := \max_{\mathcal{E}:B \rightarrow A'} F((\mathbb{1} \otimes \mathcal{E})(\rho_{AB}), |\phi_{AA'}\rangle \langle \phi_{AA'}|) \quad (4.9)$$

olarak tanımlanır. Burada $|\phi_{AA'}\rangle$ kardinalitesi $|A|$ olan bir A sisteminin durum vektörüdür ve $\mathcal{E}:B \rightarrow A'$ olacak şekilde bir kuantum kanaldır. $F(A|B)$, öz uygunluk (*fidelity*) olarak adlandırılır ve şöyle tanımlanır,

$$F(\rho, \sigma) := \left(\text{Tr} \left[\sqrt{\sqrt{\rho} \sigma \sqrt{\rho}} \right] \right)^2. \quad (4.10)$$

Aslında $F(A|B)$ düzeltilebilir-tekrar kazanılabilir dolanıklık öz uygunluğu (*recoverable entanglement fidelity*) olarak da düşünülebilir çünkü $-H_{min}(A|B)$ en dolanık duruma ne kadar yakın olunabileceğini nicelendiren bir ölçü olmaktadır.

Kuantum korelasyonlar yoksa, K için koşullu entropiler her zaman pozitiftir (Bknz. (2.12)). Ayrıca $\rho_{AB} = \rho_A \otimes \rho_B$ gibi bir çarpım durumunda ise, koşullu entropi $H(A|B) = H(A)$ olacak şekilde indirgenebilir.

(2.34)'te bahsedilen veri-işleme eşitsizliği koşullu entropiler için de yorumlanabilir. $\mathcal{E}:B \rightarrow B'$ olacak şekilde bir kuantum kanal sisteme uygulanırsa sistemin koşullu

entropisi azalmaz (Lieb ve Ruskai 1973).

$$H(A|B) \leq H(A|B'). \quad (4.11)$$

$B = B_1 B_2 \dots$ olacak şekilde çok parçalı bir sistemse, alt sistemlerden birinin dışarlanması sistemin koşullu entropisini azaltmaz; $H(A|B_1 B_2 \dots) \leq H(A|B_2 \dots)$. Bu bağıntı, daha fazla bilişime erişilebildiği zaman belirsizliğin asla artmayacağını söylemektedir.

4.3 Klasik Hafıza Varlığında EBB

Koşullu Shannon entropisi,

$$H(X|Y) := \sum_y p_Y(y) H(X|Y = y). \quad (4.12)$$

şeklinde tanımlanmıştı (Bknz (2.25)). Bu ifade $Y = y$ koşulunda X 'in belirsizliğinin, Y 'nin bütün çıktıları üzerinden ortalamasıdır. (3.58)'e benzer olarak, bir ρ_A durumuna uygulanan ve olasılıkları $p_{X^n} = \langle X^n | \rho_A | X^n \rangle$ şeklinde elde edilen bir $X = \{X_i\}_{i=1}^d$ ölçüm kümesi üzerinden,

$$\sum_i H(X_i) \geq q \quad (4.13)$$

şeklinde yazılabilir. Burada $q > 0$ ve durum bağımsızdır. Şimdi, AY sistemi için kuantum-klasik yoğunluk işlemcisi aşağıdaki gibi verilsin,

$$\rho_{AY} = \sum_y p_y(y) \rho_A^y \otimes |y\rangle \langle y|. \quad (4.14)$$

Y sistemi klasik hafızadır ve olasılıklar $p_{X_i Y} = p_y(y) \langle X_i | \rho_A^y | X_i \rangle$ şeklinde elde edilir. (4.13)'ün bütün kuantum durumlar için doğru olduğu varsayılırsa, her ρ_A^y için bütün y durumları üzerinden ortalaması alınabilir,

$$\sum_y p_Y(y) \sum_n H(X_i|Y = y) \geq \sum_y p_Y(y) q, \quad (4.15)$$

ve aşağıdaki sonuca ulaşılır,

$$\sum_i H(X_i) \geq q \Rightarrow \sum_i H(X_i|Y = y) \geq q. \quad (4.16)$$

Bu eşitsizlik, veri-işleme eşitsiliğinden daha sıkı bir alt sınırdır.

Örnek 4.3 İki-parçalı bir ρ_{AB} durumu düşünölsün ve Alice elinde bulunan A sistemi üzerinde $\{X^x\}$ ve $\{Z^z\}$ ölçömlerinden birini uygulasin. Bob ise aynı anda elindeki B sistemi üzerinde $\{Y^y\}$ ölçümünü uygulasin. Olasılıklar,

$$\begin{aligned} p_{XY}(x, y) &= \langle X^x \otimes Y^y | \rho_{AB} | X^x \otimes Y^y \rangle, \\ p_{ZY}(z, y) &= \langle Z^z \otimes Y^y | \rho_{AB} | Z^z \otimes Y^y \rangle, \end{aligned} \quad (4.17)$$

şeklilde elde edilir ve aşğıdaki bağıntı her zaman doğrudur (Coles v.d. 2017).

$$H(X|Y) + H(Z|Y) \geq q_{MU}. \quad (4.18)$$

Bu sefer, ρ_{ABC} ile temsil edilen üç-parçalı sistem ele alınsın ve sistemler arasında sadece klasik korelasyonların olduğı varsayılınsın.

Örnek 4.4 Üç-parçalı ρ_{ABC} durumu, burada Alice, elinde bulunan A sistemi üzerinde X veya Z ölçömlerinden birini, Bob elinde bulunan B sistemine Y_B ölçümünü, Charlie ise elinde bulunan C sistemine Y_C ölçümünü uyguladığı varsayılınsın. Elde edilen olasılıklar:

$$\begin{aligned} p_{XY_B}(x, y) &= \langle X^x \otimes Y_B^y \otimes \mathbb{1} | \rho_{ABC} | X^x \otimes Y_B^y \otimes \mathbb{1} \rangle, \\ p_{ZY_C}(z, y) &= \langle Z^z \otimes \mathbb{1} \otimes Y_C^y | \rho_{ABC} | Z^z \otimes \mathbb{1} \otimes Y_C^y \rangle, \end{aligned} \quad (4.19)$$

olacak şekilde, MU-bağıntısı şunu söylemektedir,

$$H(X|Y_B) + H(Z|Y_C) \geq q_{MU}. \quad (4.20)$$

$H(X|Y_B)$ ne kadar sıfıra yakınsa, $H(Z|Y_C)$ o kadar büyük olacaktır. Bob X hakkında ne kadar fazla bilişim elde ederse, Charlie Z hakkında o kadar az bilişim elde edecektir. Ancak bu bağıntı yüksek güvenliğı garantilemez. Çünkü bir kulak misafiri, ölçömlerden biri hakkında oldukça az bilişim elde ederken, diğeri hakkında yüksek bilişim elde edebilir. Bu istenmeyen bir durumdur.

4.4 Kuantum Hafıza Varlığında EBB

Belirsizlik bağıntılarının alt sınırının, klasik korelasyonların varlığında değişmez kaldığı bir önceki bölümde ele alındı. Bu bölümde ise kuantum korelasyonların varlığında EBB incelenecektir.

4.4.1 İki-parçalı sistemler

İki parçalı bir AB sistemi bir ρ_{AB} durumu ile temsil edilsin. B , kuantum yan bilişim olsun. Renes ve Boileau (2009), genelleştirilmiş Pauli ölçümleri $Z = \sum_k \omega^k |k\rangle \langle k|$ ve $X = \sum_k |k+1\rangle \langle k|$ için saflaştırıcı bir E sistemi ile birlikte ρ^{ABE} saf durumu için güçlü alt toplanabilirlik bağıntısını, $S(A|BE) \leq S(A|B)$, kullanarak bu özel durum için aşağıdaki bağıntının doğru olduğu sanıtında bulunmuşlardır.

$$S(X^A|B)_\rho + S(Z^A|B)_\rho \geq \log d + S(A|B)_\rho \quad (4.21)$$

Daha önce de söylendiği gibi bu bağıntı sadece koşullu von Neumann entropileri için geçerlidir. Shannon ve Rényi entropisine genelleştirilmesi ise Berta v.d (2010) tarafından yapılmıştır,

$$H(X|B) + H(Z|B) \geq q_{MU} + S(A|B). \quad (4.22)$$

Bağıntının sol tarafında bulunan koşullu entropiler aşağıdaki gibi A sisteminin ölçüm sonrası klasik-kuantum durumlardan elde edilebilir,

$$\rho_{XB} = \sum_x |x\rangle \langle x|_X \otimes (X \otimes \mathbb{1}_B) \rho_{AB} (X \otimes \mathbb{1}_B). \quad (4.23)$$

Denk.(4.22), dolanıklık-destekli belirsizlik bağıntıları (*entanglement-assisted uncertainty relations*) olarak adlandırılır. Bu bağıntının sonuçları şöyledir:

- 1) A üzerinde ölçüm yapılsın ve B kuantum hafıza olsun. Eğer A ve B , en dolanık saf durumda bulunuyorsa, o zaman $S(A|B) = -\log d$ olur. Burada d , üzerinde ölçüm yapılan sistemin boyutudur. Denk.(3.26)'dan, $\log 1/c$ asla $\log d$ 'den büyük olamaz ve böylece (4.3)'un alt sınırı önemsiz olur. O zaman, A hakkında bilgi edinmek isteyen kulak misafiri, X ve Z ölçümelerini mükemmel şekilde tahmin edecek bir strateji geliştirebilir.
- 2) Eğer A ve B dolanık değilse, yani bileşik sistemin yoğunluk işlemcisi alt sistemlerin çarpım durumunun bir konveks kombinasyonu halinde bulunuyorsa, o zaman $S(A|B) \geq 0$ olur. Böylece, $H(X|B) + H(Z|B) \geq q_{MU}$ bağıntısı korunur ve MU bağıntısı elde edilir.

- 3) Eğer B sistemi dışarlarsa, (4.31), $H(X) + H(Z) \geq q_{MU} + S(A)$ bağıntının indirgenir. Böylece EBB'nin durum-bağımsız savı artık geçerli olmaz ve A sisteminin başlangıçtaki von Neumann entropisi alt sınırı etkiler. A sistemi bir saf durum ile temsil edilebiliyorsa, o zaman $S(A) = 0$ olur ve MU bağıntısı sağlanır. Ancak, A sistemi saf olmayan bir durumdaysa, $S(A) > 0$ olur ve bağıntının sağ tarafı MU sınırından daha güçlü bir sınır olmuş olur.

Denk.(4.22), şöyle de yorumlanabilir; en dolanık durumda bulunan iki-parçalı bir sistemin birden çok kopyası elde edilirse, bu kopyalar üzerinde farklı ölçümler yapılarak ölçümler arasındaki belirsizlik tamamen ortadan kaldırılabilir. Bu cümlelerin belirsizlik ilkesini ihlal ettiği düşünülebilir ancak bu doğru değildir. Sadece kuantum korelasyonların varlığında belirsizliğin sıfıra indirgenebileceği söylenebilir. Ayrıca tek parçalı sistemlerde hem Heisenberg belirsizlik bağıntısı hem de EBB geçerliğini korumaktadır.

Denk.(4.22) üzerine veri-işleme eşitsizliği uygulanırsa alt sınırın korunur,

$$H(X|Y_B) + H(Z|W_B) \geq q_{MU} + S(A|B). \quad (4.24)$$

(4.22)'nin alt sınırının geliştirilmesi ise Coles ve Piani (2014) tarafından yapılmıştır;

$$H(X|B) + H(Z|B) \geq q_{CP} + S(A|B). \quad (4.25)$$

Daha önceden belirtildiği gibi bu sınırın incelenmesi EK 6'da incelenmiştir.

Berta v.d (2010) tarafından ortaya konulan (4.22), sadece dolanıklıkla ilgili bir çalışmadır ve diğer kuantum korelasyonları kapsamamaktadır. Ancak kuantum diskord bu bağıntıya eklenebilir (Pati v.d 2010). Kuantum diskord, kuantum ve klasik korelasyonların toplam miktarından (kuantum karşılıklı bilişim) klasik korelasyonların miktarının (klasik karşılıklı bilişim) çıkarılması ile elde edilir ve sadece kuantum korelasyonların miktarını nicelendirir (Ollivier ve Zurek 2001).

Bir ρ_{AB} işlemcisi için, sistemler arasında bulunan klasik korelasyonların miktarı en büyük klasik karşılıklı bilişim $\max_X I(X; B) := J_A(\rho_{AB})$ ile tanımlanır (Burada X bir ölçümdür ve A sistemi üzerine uygulanmaktadır.) ve kuantum karşılıklı bilişim (bkz. Denk.(2.11)) ile birlikte kuantum diskord aşağıdaki gibi tanımlanır,

$$D_A(\rho_{AB}) := I(A; B) - J_A(\rho_{AB}). \quad (4.26)$$

Aşağıdaki yer alan hesaplama, kuantum diskordun Denk.(4.22)'ye eklenebileceği gösterilebilir (Pati v.d 2012),

$$\begin{aligned}
H(X|B) + H(Z|B) &= H(X) - I(X; B) + H(Z) - I(Z; B) \\
&\geq H(X) + H(Z) - 2J_A(\rho_{AB}) \\
&\geq q_{MU} + S(A) - 2J_A(\rho_{AB}) \\
&= q_{MU} + S(A|B) + D_A(\rho_{AB}) - J_A(\rho_{AB}). \tag{4.27}
\end{aligned}$$

Kuantum diskord, klasik karşılıklı bilişimden büyük olduğu zaman (4.27), (4.22)'in güçlendirilmiş halidir. Ancak klasik ve kuantum karşılıklı bilişim nicelikleri her zaman pozitif ve sistemler arasında kuantum korelasyonlar bulunmayabilir. O zaman kuantum diskord sıfıra eşit olur. Ayrıca kuantum diskordun büyüklüğü bazı durumlar için klasik korelasyonların miktarından küçük olabileceği için son eklenen terim belirsizliğin alt sınırını etkilemiş olur. Bu yüzden bağıntının sağ tarafı aşağıdaki gibi yeniden düzenlenmelidir,

$$H(X|B) + H(Z|B) \geq q_{MU} + S(A|B) + \max\{0, D_A(\rho_{AB}) - J_A(\rho_{AB})\}. \tag{4.28}$$

Daha açık anlatılmak istenirse, bileşik sistemin koşullu von Neumann entropisi $S(A|B) = 0$ olduğu varsayılın ve sistemler arasındaki klasik korelasyonların miktarı pozitif yani $I(X; B) > 0$ olsun. Klasik karşılık bilişim, alt toplanabilirlik bağıntısından her zaman pozitif olacağından ve parantez içindeki terim negatif çıkacağından bağıntının sağ tarafı önemsiz bir alt sınıra indirgenebilir. Yani klasik korelasyonlar belirsizliğin alt sınırını azaltmış olur. Ancak bu mantıklı değildir.

4.4.2 Üç parçalı sistemler

İki parçalı bir ρ_{AR} durumu ve R 'ye uygulanan bir Γ^R POVM'u düşünölsün ($\Gamma_j^R \geq 0$, $\sum_j \Gamma_j^R = \mathbb{1}^R$). A 'nın e_{kl} matris bazında $\rho_{AR} = \sum_{kl} e_{kl} \otimes T_{kl}$ blok yazımı göz önüne alınırsa, ölçüm öncesi indirgenmiş durumlar

$$\rho_A = \sum_{kl} e_{kl} \text{Tr}_R(T_{kl}) \quad , \quad \rho_R = \sum_k T_{kk}$$

olmaktadır. R 'de yapılan yerel ölçümden hemen sonraki durum,

$$\begin{aligned}\sigma_{AR} &= (id_A \otimes \Gamma^R)(\rho_{AR}) = \sum_{kl} e_{kl} \otimes \Gamma^R(T_{kl}) \\ &= \sum_{klj} e_{kl} \otimes \sqrt{\Gamma_j^R(T_{kl})} \sqrt{\Gamma_j^R}\end{aligned}$$

olup indirgenmiş durumlar

$$\sigma_A = Tr_R \left[\sum_{kl} e_{kl} \otimes \Gamma^R(T_{kl}) \right] = \sum_{klj} e_{kl} Tr_R(\Gamma_j^R T_{kl})$$

$$\begin{aligned}\sigma_R &= Tr_A \left[\sum_{klj} e_{kl} \otimes \sqrt{\Gamma_j^R(T_{kl})} \sqrt{\Gamma_j^R} \right] = \sum_{kj} \sqrt{\Gamma_j^R(T_{kk})} \sqrt{\Gamma_j^R} \\ &= \sum_j \sqrt{\Gamma_j^R(\rho_R)} \sqrt{\Gamma_j^R} = \sum_j p_j \sigma_j^R.\end{aligned}$$

j . tek ölçüm için sıfırdan farklı her

$$p_j = Tr_{AR}[(id_A \otimes \Gamma_j^R)\rho_{AR}] = Tr_R(\Gamma_j^R \rho_R) \quad (4.29)$$

olasılığı için R sistemi $\sigma_j^R = [\sqrt{\Gamma_j^R(\rho_R)} \sqrt{\Gamma_j^R}] / p_j$ ara indirgenmiş durumlarında bulunacaktır. A sisteminin de tek ölçüm sonrası indirgenmiş durumları $\sigma_j^A = Tr_R[\rho_{AR} \Gamma_j^R] / p_j$ şeklinde yazılabilir. Bu bağıntıdan açıkça görüldüğü gibi $\sum_j p_j \sigma_j^A = Tr_R[\rho_{AR} \sum_j \Gamma_j^R] = Tr_R \rho_{AR} = \rho_A$ olur; yani ölçümler R üzerinde yapıldığı için A 'nın durumu değişmemekte fakat ara indirgenmiş σ_j^A durumların bir konveks kombinasyonuna ayrıışmaktadır. Burada σ_j^A durumlarına (R 'nin σ_j^R olması koşulu altında) A 'nın koşullu durumları denir.

A 'nın koşullu σ_j^A durumunda, sıra değişmeyen X ve Z gözlenebilirleri için (3.7)'deki gibi MU bağıntısı yazılabilir,

$$H(X)_{\sigma_j^A} + H(Z)_{\sigma_j^A} \geq q_{MU}. \quad (4.30)$$

Bunun iki tarafını (4.29)'daki p_j olasılıkları ile çarpıp toplarsak sağ taraf değişmez ve $H(X|\Gamma^R)_\rho$, $H(Z|\Gamma^R)_\rho$ koşullu Shannon entropileri cinsinden;

$$H(X|\Gamma^R)_\rho + H(Z|\Gamma^R)_\rho \geq q_{MU}, \quad (4.31)$$

sonuca ulaşılır.

Şimdi R sistemi, B ve E gibi iki alt sistemden oluşsun ve $\Gamma_{jk}^R = \Lambda_j^B \otimes \Lambda_k^E$ bileşik (iki taraflı) ölçümü yapılsın. Koşullandırma entropiyi azalttığından, ayırık yardımcı sistemler B ve E 'ye aynı anda depolanan X ve Z bilişim miktarları arasında bir ödünleşme (mahsuplaşma, *tradeoff*) elde edilebilir;

$$H(X|\Lambda_j^B)_\rho + H(Z|\Lambda_k^E)_\rho \geq q_{MU} \quad (4.32)$$

Böylece herhangi bir parçayı elinde tutan gözlemci, diğer parçayı elinde tutan gözlemcinin tamamlayıcı gözlenebilirliği üzerine bir limit getirir. Bu ifadeye zayıf tamamlayıcı bilişim ödünleşmesi adı verilmektedir (Renes ve Boileau 2009).

Benzer bir bağıntı von Neumann entropisi için de türetilir. E bir saflaştırıcı olmak üzere, Saf bir ρ_{ABE} durumu için $|\psi_{ABE}\rangle = \sum_k \sqrt{p_k} |k\rangle_A \otimes |\phi_k\rangle_{BE}$ yazılabilir (Nielsen ve Chuang 2011 - Denk(2.207)) . von Neumann entropisinin özelliğinden (Nielsen ve Chuang 2011 - Teorem 11.8)

$$S(\rho_{Z^A}^{AB}) = H(p_k) + \sum_k p_k S(\phi_k^B) = H(p_k) + \sum_k p_k S(\phi_k^E) = S(\rho_{Z^A}^{AE})$$

yazılabilir. Burada $\phi_k^B := \text{Tr}_E(|\phi_k\rangle\langle\phi_k|_{BE})$ ve $\phi_k^E := \text{Tr}_B(|\phi_k\rangle\langle\phi_k|_{BE})$ tanımı yapılmıştır. Koşullu von Neumann entropileri incelenirse;

$$S(Z^A|B) = S(\rho_{Z^A}^{AB}) - S(\rho_B) = H(p_k) + \sum_k p_k S(\phi_k^B) - S(\rho^B) \quad (4.33)$$

$$S(Z^A|E) = S(\rho_{Z^A}^{AE}) - S(\rho_E) = H(p_k) + \sum_k p_k S(\phi_k^E) - S(\rho^E) \quad (4.34)$$

$$S(A|B) = S(\rho^{AB}) - S(\rho^B) \quad (4.35)$$

elde edilir. $|\psi_{ABE}\rangle$ 'nin başlangıçta tanımlanan durumundan $S(\rho^{AB}) = S(\rho^E)$ çıkar ve $S(Z^A|B) - S(Z^A|E) = S(A|B)$ olur. (4.26)'da yerine konulursa

$$S(X^A|B) + S(Z^A|E) \geq q_{MU} \quad (4.36)$$

sonucu çıkar. Bu ifade kuantum hafızalı durumlarda kullanılabildiğinden güçlü tamamlayıcı bilişim ödünleşmesi adını almaktadır.

Hafızalı durumda üç parçalı sistemler için EBB'nin genel türetimi EK-5'te incelenmiştir.

4.4.3 Hafıza varlığında çoklu ölçüm kümeleri

Bölüm 3.9 ile benzer bir notasyon kullanılarak, kuantum hafıza varlığında çoklu ölçüm kümeleri için alt sınır incelenebilir.

İlk olarak, A bir kübit sistemi olsun ve bu sistem üzerinde $\Theta \in \{\sigma_X, \sigma_Y, \sigma_Z\}$ Pauli ölçümlerinin, $\{\sigma_X, \sigma_Y\}$, $\{\sigma_X, \sigma_Z\}$ ve $\{\sigma_Y, \sigma_Z\}$ ikili kombinasyonlarının uygulansın. Denk.(3.49)'a benzer bir sonuç bu ölçüm çiftleri için yazılabilir,

$$H(M|B\Theta) \geq \frac{1}{2} + \frac{1}{2}S(A|B). \quad (4.37)$$

Burada, Bölüm 3.9'daki notasyon genişletilecek olunursa,

$$\rho_{M\Theta B} = \frac{1}{3} \sum_{k=1,2} \sum_{j=X,Y,Z} |m\rangle \langle m|_M \otimes |j\rangle \langle j|_\Theta \otimes (\langle m| U_j^\dagger \otimes \mathbb{1}_B) \rho_{AB} (U_j |m\rangle \otimes \mathbb{1}_B), \quad (4.38)$$

yazılabilir. Dikkat edilirse, Denk.(4.42)'nin sol tarafı alternatif olarak şu şekilde yazılabilir:

$$H(M|B\Theta) = \frac{1}{3} [H(M|B\Theta = \sigma_X) + H(M|B\Theta = \sigma_Y) + H(M|B\Theta = \sigma_Z)]. \quad (4.39)$$

Burada sistemin ölçüm sonrası durumu şu şekilde ifade edilir:

$$\rho_{MB|\Theta=\sigma_X} = \sum_{k1,2} |m\rangle \langle m|_M \otimes (\langle m| U_X^\dagger \otimes \mathbb{1}_B) \rho_{AB} (U_X |m\rangle \otimes \mathbb{1}_B). \quad (4.40)$$

σ_Y, σ_Z ölçümleri içinde benzer şekilde yazılabilir.

4.5 Bilişim Dışarlama Prensibi

Bir AY kuantum-klasik sisteminde, X ve Z ölçümleri, A sistemine uygulanan tam ölçümler olsun ve klasik kayıt Y 'nin A ile klasik korelasyonlar barındırdığı varsayalım. Klasik hafıza varlığından EBB, (4.18), göz önüne alınırsa;

$$\begin{aligned} H(X|Y) + H(Z|Y) &\geq q_{MU} \\ H(X) - I(X; Y) + H(Z) - I(Z; Y) &\geq q_{MU} \\ -I(X; Y) - I(Z; Y) &\geq q_{MU} - [H(X) + H(Z)], \end{aligned} \quad (4.41)$$

yazılabilir. Burada klasik karşılıklı bilişim (2.20)'de tanımlandığı gibidir. EK-1'de gösterildiği üzere $\{H(X), H(Z)\} \leq \log d$ olmaktadır ve (4.46)'nın sağ tarafının

minimum değeri $H(X) = \log d = H(Z)$ olduğunda elde edilir. Bu bilgiler yerine konulur ve son bağıntı -1 ile çarpılırsa *bilişim dışarlama prensibi* elde edilmiş olur (Hall 1995),

$$I(X; Y) + I(Z; Y) \leq \log(d^2 c) := r_H. \quad (4.42)$$

Burada c , MU bağıntısından gelmektedir. Bağıntının sağ tarafı incelenirse, minimum $c = 1/d$ iken ve maksimum ise $c = 1$ olduğunda elde edilir; yani $\log d \leq \log(d^2 c) \leq 2 \log d$ olur. Bu bağıntı şöyle yorumlanabilir; X uygulandığında, klasik hafıza Y ile ne kadar çok karşılıklı bilişim oluşuyorsa, Z uygulandığında oluşan karşılıklı bilişim o kadar az olur; yani X ve Y arasında ne kadar çok klasik korelasyon varsa, Z ve Y arasında o kadar az klasik korelasyon vardır.

Eğer klasik kayıt Y sistemi ile bir kuantum hafıza B sistemi ile yer değiştirirse, klasik hafızadaki yönteme benzer şekilde, bir ρ_{AB} durumu için (4.22)'den bir bağıntı türetilir (Coles ve Piani 2014),

$$I(X; B) + I(Z; B) \leq r_{CP} - S(A|B). \quad (4.43)$$

Sağ tarafta yer alan r_{CP} sınırı;

$$r_{CP} := \min \left\{ \log \left(d \sum_x \max_z c_{xz} \right), \log \left(d \sum_z \max_x c_{xz} \right) \right\} \quad (4.44)$$

olarak tanımlanır ve $r_{CP} \leq r_H$ olur. Bu sınırın ispatı EK-6'da yer almaktadır. Klasik hafıza varlığında ($S(A|Y) \geq 0$) ve $d = 2$ için bu bağıntı yine (4.46)'ya indirgenir. Diğer bir örnek olarak, en saf dolanık halde bulunan bir ρ_{AB} için ele alınırsa; $I(X; B) = \log d = I(Z; B)$ olacaktır. Böylece üst sınır r_{CP} , $-S(A|B)$ terimi yüzünden zayıflayabilir ve önemsiz bir sınır olabilir.

4.6 Kuantum Kanal Yaklaşımı

Uyuşumsuz iki klasik bilişimin bir kuantum kanal üzerinden iletmeye çalışılması EBB ile ilişkilidir. Alice, $X = \{|x_i\rangle \langle x_i|\}_{i=1}^d$ ile etiketlenmiş, $1/d$ olasılığındaki d tane ortonormal durumdan birini seçsin ve $\mathcal{E}$ aracılığıyla Bob'a yollasın. Bob, hangi durumun yollandığını ayırt etmeye çalışsın. Benzer şekilde aynı senaryo $Z = \{|z_i\rangle \langle z_i|\}_{i=1}^d$ içinde gerçekleşsin. Böyle bir durumda Bob'un X durumunu ayırt

edebilme yeteneği, Holevo niceliği ile nicelendirilir (Holevo 1973),

$$\chi(\mathcal{E}, X) = H\left(\sum_x \frac{1}{d} \mathcal{E}(|x\rangle\langle x|)\right) - \sum_x \frac{1}{d} H(\mathcal{E}(|x\rangle\langle x|)) \quad (4.45)$$

ve $\chi(\mathcal{E}, Z)$ niceliğinde benzer şekilde tanımlanır. Bu iki Holevo niceliği arasında ,

$$\chi(\mathcal{E}, X) + \chi(\mathcal{E}, Z) \leq \log d + I_{coh}\left(\frac{1}{d}, \mathcal{E}\right), \quad (4.46)$$

bağıntısı vardır (Christandl ve Winter 2005). Burada $I_{coh}(\rho, \mathcal{E})$, koherent bilişim (*coherent information*) olarak tanımlanır ve kuantum kanal $\mathcal{E}$ 'un kalitesinin bir ölçüsüdür. Örneğin en saf olmayan durum $\mathbb{1}/d$ için koherent bilişim:

$$I_{coh}\left(\frac{1}{d}, \mathcal{E}\right) := H(\mathcal{E}(\mathbb{1}/d)) - H[(\mathcal{I} \otimes \mathcal{E})(|\Phi\rangle\langle\Phi|)] \quad (4.47)$$

olarak tanımlanır. Burada $|\Phi\rangle = \sum_j (1/d) |j\rangle |j\rangle$ en dolanık saf durumu temsil etmektedir.

(4.47) herhangi KYB için doğrudur ancak herhangi iki keyfi X ve Z ortonormal kümesi için bağıntının sağ tarafı geliştirilebilir (Coles v.d 2011),

$$\chi(\mathcal{E}, X) + \chi(\mathcal{E}, Z) \leq \log(d^2 c) + I_{coh}\left(\frac{1}{d}, \mathcal{E}\right). \quad (4.48)$$

Daha sonra Coles ve Piani (2014) bağıntının sağ tarafının geliştirebileceğini göstermişlerdir,

$$\chi(\mathcal{E}, X) + \chi(\mathcal{E}, Z) \leq r_{CP} + I_{coh}\left(\frac{1}{d}, \mathcal{E}\right). \quad (4.49)$$

Kısaca, eğer Alice, Bob'a X ve Z durumlarının ikisini birden çok iyi şekilde iletebiliyorsa, $\mathcal{E}$ gürültüsüz bir kanaldır, yani koherent bilişim ile nicelendirilebilen mükemmel bir kanala yakındır.

4.7 Kuantum Hafıza Varlığında Tahmin Oyunu

İki-parçalı sistemler:

Kuantum hafıza varlığında bir tahmin oyunu şu şekilde tasarlanabilir:

- 1) Bob, ρ_{AB} dolanık bir kübit durumunu hazırlasın ve parçalardan birini Alice'e yollarken, kuantum hafıza B 'yi elinde tutsun,

- 2) Alice, kendi sistemi üzerinde X veya Z ölçümlerinden birini uygulasin ve sonucu klasik kayıt K 'ye kaydetsin.
- 3) Sonra, elinde bulunan ölçüm kümesini Bob'a yollasin ve K 'yı tahmin etmesini istesin.

Bölüm 3.8'deki notasyondan devam edilirse, X için ölçüm sonrası durum;

$$\rho_{KXB} = \sum_k |k\rangle\langle k| \otimes [(X^k \otimes \mathbb{1}_B)\rho_{AB}(X^k \otimes \mathbb{1}_B)], \quad (4.50)$$

olur ve Z için de aynısı yazılabilir. (3.52)'den genel olarak koşullu olasılıklar,

$$p_{K|B\Theta=\theta_j} = \frac{1}{2} \text{Tr}(\rho_{AB}\theta_j), \quad \theta_j = \{X, Z\} \quad (4.51)$$

olarak elde edilir. Koşullu Shannon entropisi,

$$\begin{aligned} H(K|B\Theta) &= H(KB\Theta) - H(B\Theta) \\ &= \frac{1}{2}[H(K|B\Theta = \theta_X) + H(K|B\Theta = \theta_Z)], \end{aligned} \quad (4.52)$$

yazılabilir. (4.22) göz önüne alınır;

$$H(K|B\Theta) \geq \frac{1}{2}[q_{MU} + S(A|B)] \quad (4.53)$$

elde edilir. Alice, ölçüm kümesi elemanlarından hangisi ile ölçüm yaparsa yapsın, Bob doğru bir tahminde bulunabilir. Örneğin Bob'un hazırladığı durum saf en dolanık bir durum ise $S(A|B) = -\log d$ olacağından ($d = \dim(A) = \dim(B)$) (4.53)'in sağ tarafı önemsiz bir alt sınıra indirgenir ve Bob kesin sonuca ulaşabilir. Bu örnek kuantum hafızanın gücünü göstermektedir

Üç-parçalı sistemler:

Bu sefer, ρ_{ABC} durumu ele alınsın ve A sisteminin B veya C 'nin hangisiyle korelasyon halinde olduğu bilinmesin. A , B ve C sistemleri sırasıyla Alice'e, Bob'a ve Charlie'ye yollansın. A üzerinde X veya Z ölçümlerinden birini uygulasin. Oyun şöyle tasarlanmıştır; eğer Alice, elindeki sisteme X ölçümünü uygularsa, Bob'un amacı X hakkındaki belirsizliği en aza indirmek (en fazla bilişimi elde etmek), eğer Z ölçümünü uygularsa, bu sefer Charlie'nin amacı Z hakkındaki belirsizliği en aza

indirmek olacaktır. Bu durum X ve Z ölçümleri arasında bir kısıtlama konularak gerçekleştirilebilir (Renes ve Boileau 2009). (4.74)'ten, bu işlemcileri birbirlerine bir Fourier dönüşümü F ile bağlı ise;

$$|X^j\rangle = F |Z^j\rangle \quad \text{ve} \quad F = \sum_{j,j'} \frac{\omega^{jj'}}{\sqrt{d}} |Z^j\rangle \langle Z^{j'}|, \quad (4.54)$$

EBB kullanılarak bir eşitsizlik yazılabilir (Bknz. Bölüm 4.4.2). Burada $\omega := e^{2\pi i/d}$ olarak tanımlanır. Dönüşümden, X ve Z 'nin KYB olduğu görülebilir, ancak bütün KYB'lerin birbirlerine bir Fourier dönüşümü ile bağlı olmaları gerekmez. Bob'un ve Charlie'nin belirsizlikleri sırasıyla $S(X|B)$ ve $S(Z|C)$ koşullu entropileri ile nicelendirildiğinden, (4.36)'dan;

$$S(X|B) + S(Z|C) \geq \log d. \quad (4.55)$$

yazılabilir ve yine aynı bölümden benzer bir bağıntı koşullu Shannon entropileri cinsinden ifade edilebilir.

$$H(X|B) + H(Z|C) \geq q_{MU} \quad (4.56)$$

(4.55) ve (4.56) şöyle yorumlanabilir; Bob X hakkında ne kadar bilişime sahip ise, Charlie Z hakkında o kadar az bilişime sahiptir veya tam tersi. Bu bağıntılar dolanıklığın tek eşliliğinin (*monogamy of entanglement*) ödünleşmesinin bir işareti olarak görülebilir. Kabaca söylenirse; A 'nın B ile arasında ne kadar çok dolanıklık varsa, C ile o kadar az dolanıklık vardır.

Denk.(4.55), hem MU bağıntısını hem de (4.20)'yi ima eder. Veri işleme eşitsizliğine göre, B sistemi üzerine uygulanan herhangi bir Y ölçümü için ,

$$H(X|B) \leq H(X|Y) \leq H(X), \quad (4.57)$$

eşitsizlikleri doğrudur (Nielsen ve Chuang 2011- Teorem 11.3) . Buna göre (4.55), (4.20)'den daha güçlü bir sınır olmaktadır.

Üç-parçalı sistemlerde tahmin oyunu, min-entropiyle de nicelendirilebilir. (3.49)'dan, Bob'un $p_{tahm}(M|B\Theta)$ ile Charlie'nin $p_{tahm}(M|C\Theta)$ tahmin olasılıkları arasında ödünleşme vardır (Tomamichel v.d 2013),

$$p_{tahm}(M|B\Theta) + p_{tahm}(M|C\Theta) \leq 2b. \quad (4.58)$$

Burada b , (3.49)'da verildiği gibidir. Bu bağıntı min-entropi cinsinden yazılır ve log fonksiyonunun konkavlık özelliğinden yararlanılırsa,

$$H_{\min}(M|B\Theta) + H_{\min}(M|C\Theta) \geq 2 \log \frac{1}{b} \quad (4.59)$$

bağıntısına ulaşılabilir. Bu bağıntı, Bob ile Charlie'nin kazanma olasılıklarının arasında bir ödünleşme olduğunu gösterir.



5. UYGULAMALAR

5.1 Kuantum Anahtar Dağıtımı

Kuantum anahtar dağıtımı (*quantum key distribution, QKD*), iki karşılıklı dürüst tarafın gizli bir anahtarı halka açık bir kanal üzerinden paylaşması senaryosudur (Bennett ve Brassard 1984). Eğer taraflar, ellerindeki ölçüm kümelerini, X ve Z , anahtar üzerine uyguladıklarında çoğu seferde anlaşılabiliyorlarsa, hata düzeltimi yapılarak anahtar çıkarılır. Ancak bir kulak misafiri, Eve, anahtar hakkında bilişim elde etmeye çalışabilir ve eğer kanalla etkileşirse gürültü oluşur. Bu yüzden Alice ve Bob ölçüm sonuçlarının çoğunda anlaşılamazlar ve Eve'in kanalla etkileştiğini anlayarak protokolü iptal ederler.

QKD'nin güvenliğini göstermek için aşağıdaki iki kriter karşılıklı dışlayıcı olmalıdır,

- a) Alice ve Bob, ölçüm sonuçlarının çoğunda anlaşmalıdır,
- b) Eve, Alice ve Bob'un ölçüm sonuçları hakkında oldukça fazla bilişime sahip olmalıdır.

QKD'nin güvenlik kriterinin EBB ile ilişkisini anlatabilmek için E91 protokolü (Ekert 1991) kullanılabilir. Protokol şöyledir:

- i) Alice ve Bob, en dolanık bir iki-kübit durumunu bir halka açık kanal üzerinden paylaşmaktadır ve Eve kullanılan kanalla eş fazlı halde etkileşim halindedir.
- ii) $X = \{|+\rangle\langle +|, |-\rangle\langle -|\}$ veya $Z = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ ölçüm kümelerinden biri rasgele kabul edilir, her taraf kendi kübitlerini ölçer ve bu prosedür defalarca tekrarlanır.
- iii) Alice kendi ölçüm sonuçlarının bir alt kümesini Bob'a duyurur. Eğer ölçüm sonuçlarının çoğu seferinde anlaşıyorlarsa, hata düzeltimi yapılarak anahtar çıkarılır. Değilse protokol iptal edilir.

Şimdi hem tek sefer hem de çoklu seferlerde inceleme yapılırsa:

Tek sefer: Alice ve Bob'un en dolanık durum paylaştığı bilinmesin, ancak genelliği kaybetmemek adına Alice (A), Bob (B) ve Eve'in (E) bir ρ_{ABE} durumunu paylaştığı varsayılın. Burada A ve B bir kübit sistemi ve E , Eve'in elinde tuttuğu kuantum sistemidir. $\Theta = \{X, Z\}$ ölçüm kümesi olsun ve Y kayıt sistemi, Alice'in ölçüm sonuçlarının çıktılarını temsil etsin. (4.52)'den,

$$H(Y|B\Theta) = \frac{1}{2}[H(X|B) + H(Z|B)], \quad (5.1)$$

$$H(Y|E\Theta) = \frac{1}{2}[H(X|E) + H(Z|E)] \quad (5.2)$$

yazılabilir. Böylece aşağıdaki ifade elde edilebilir,

$$H(Y|E\Theta) + H(Y|B\Theta) \geq q_{MU} = 1. \quad (5.3)$$

Burada entropiler, Alice'in kübiti üzerinde ölçüm yapıldıktan sonra elde edilen ölçüm sonrası durum $\rho_{Y\Theta BE}$ için türetilmiştir. Sonra Bob, aynı ölçüm kümesini kullansın ve kayıt sistemi $\hat{Y}$ ile temsil edilsin. Veri-işleme eşitsizliğinden $H(Y|B\Theta) \leq H(Y|\hat{Y})$ olur ve (5.3)'ten $H(Y|E\Theta) \geq 1 - H(Y|\hat{Y})$ sonucu elde edilir. Bu ifade Alice'in ölçüm sonucunun Eve belirsizliği (von Neumann entropisi), $H(Y|\hat{Y})$ ifadesinin küçük olduğu zamanlarda $H(Y|E\Theta)$ ifadesinin büyük olduğunu garantiler. Böylece güvenlik kriteri nicelendirilmiş olur.

Örnek 5.1 Alice ve Bob ölçüm sonuçlarını yüksek olasılıkla kabul etsin ve olasılık $1 - \delta$ olsun, o zaman $H(Y|\hat{Y})$, $h_{bin}(\delta) = \delta \log(1/\delta) + (1 - \delta) \log[1/(1 - \delta)]$ olarak değerlendirilebilir. Böylece,

$$H(Y|E\Theta) \geq 1 - h_{bin}(\delta) \quad (5.4)$$

bulunur ki $\delta \leq 1/2$ ise sonuç kesinlikle pozitif çıkar.

Çoklu sefer: Tek seferde elde edilen entropilerin toplanması yoluyla EBB elde edilebilir ancak çoklu seferleri direk olarak tanımlayan bir EBB bulmak daha mümkündür.

Alice ve Bob'un elinde olan n tane kübitin ölçüm yapılmadan aralarında değiş-yokuş edildiği varsayılın. Aslında taraflar her zaman kendi kübitlerini ölçüyor

iken bu varsayımsal bir durumdur. Ancak, Eve'in stratejisi ölçüm zamanı ile bağımlı olmayacağından, Alice ve Bob'un kendi ölçümlerini geciktirdiği hayal edilebilir. Değiş-tokuştan sonra, Alice'in sistemi $A^n = A_1 \dots A_n$ ve Bob'un sistemi $B^n = B_1 \dots B_n$ sistemleri içinde n tane kübit tutulur. Bu durum Eve'in elinde tuttuğu keyfi bir $\rho_{A^n B^n E}$ durumu ile temsil edilsin. Ölçüm kümesi $\Theta^n = \{\Theta_1, \dots, \Theta_n\}$ olacak şekilde seçilsin, burada Θ_i , i ile işaretlenmiş ölçüm elemanıdır. Benzer olarak Alice'in ölçüm sonuçları $Y^n = (Y_1, \dots, Y_n)$ ve Bob'un ölçüm sonuçları, kayıt sistemi $\hat{Y}^n = (\hat{Y}_1, \dots, \hat{Y}_n)$ üzerine kaydedilsin.

Önemli bir gözlem (5.3)ün ima ettiğidir,

$$H(X_1 X_2 Z_3 X_4 \dots X_{n-1} Z_n | E) + H(Z_1 Z_2 X_3 Z_4 \dots Z_{n-1} X_n | B) \geq n. \quad (5.5)$$

Burada n tane sistemin karşılıklı uyumsuz şekilde ölçüldüğüne emin olunmuştur. Kübit sistemin için $c = 1/2$ olduğundan $\log(1/c^n) = n$ elde edilmiştir.

Benzer bir argüman, data-işleme eşitsizliğinden ve tek sefer durumuna benzer şekilde elde edilebilir,

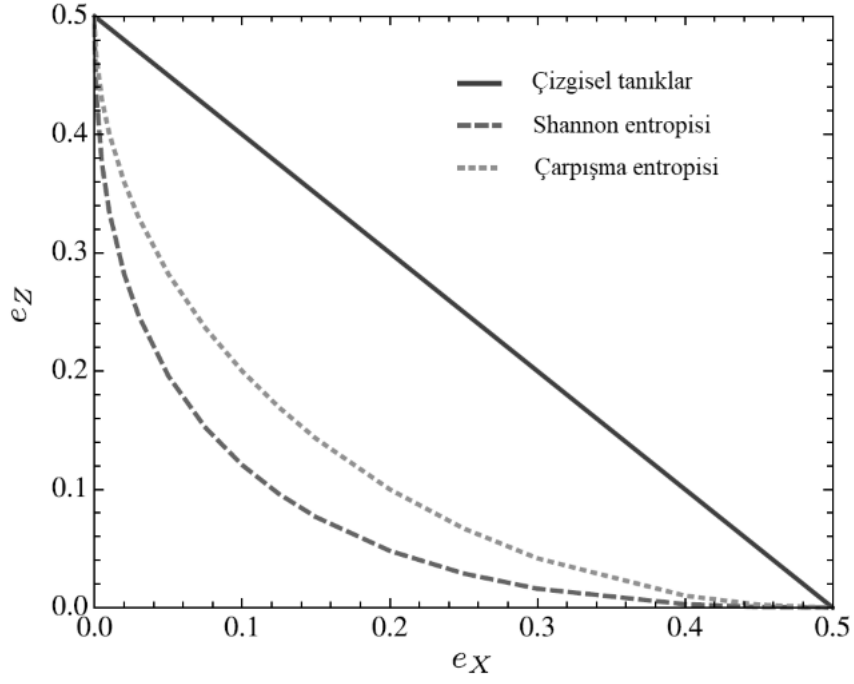
$$H(Y^n | E \Theta^n) + H(Y^n | \hat{Y}^n) \geq H(Y^n | E \Theta^n) + H(Y^n | B \Theta^n) \geq n. \quad (5.6)$$

Böylece Y^n ölçüm sonucunda Eve'in belirsizliği (von Neumann terimleri ile) her sefer sayısı için artmaktadır. Saldırı hakkında herhangi bir kabul yapılmaksızın bu ifade doğrudur. Özellikle, ölçüm öncesi $\rho_{A^n B^n E}$ durumu herhangi bir özel yapıya ihtiyaç duymaz ve keyfi kabul edilir.

5.2 Dolanıklık Tanıkları

$\rho_{AB} = \sum_{ab} p(a, b) \rho_A^a \otimes \rho_B^b$ şeklinde yazılabilen saf olmayan durumlara ayrılabilir (*separable*) durumlar denir. Böyle yazılamayan durumlara ise dolanık saf olmayan durumlar denir. Dolanıklık tanıkları ise dolanık üretilmiş parçaçıkların oluşturduğu bir kaynağın doğrulanma sürecine karşılık gelir. Bunun için ayrılabilir (dolanık olmayan) durumlar tarafından sağlanan bir özdeşlik ispatlanır, eğer kaynak bu özdeşliği ihlal ederse dolanık olduğu söylenir.

İki-parçalı bir sistemin dolanıklığı ele alınsın. Dolanıklık tanıkları entropik olmayan bir kavram olsa da, tamamlayıcı gözlenebilirliklere dayanır ve direk olarak entropik



Şekil 5.1. Belirtilmiş çizgilerin altın kalan bölgeler dolanıklığın mevcut olduğu bölgeler olarak görülmektedir. (Coles v.d 2017)

tanıklarla karşılaştırılabilir. Aşağıdaki gibi bir işlemci ele alınsın,

$$E_{XZ} = E_X + E_Z. \quad (5.7)$$

Burada;

$$\begin{aligned} E_X &:= |+\rangle \langle +| \otimes |-\rangle \langle -| + |-\rangle \langle -| \otimes |+\rangle \langle +|, \\ E_Z &:= |0\rangle \langle 0| \otimes |1\rangle \langle 1| + |1\rangle \langle 1| \otimes |0\rangle \langle 0| \end{aligned} \quad (5.8)$$

olarak tanımlanır ve bunlara hata (gürültü) işlemcileri denir. Bir Bell durumu $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ için hata olasılığı sıfırdır. Diğer taraftan herhangi ayrılabilir bir durum için aşağıdaki ifade doğrudur (Namiki ve Tokunaga 2012),

$$\text{Tr}[\rho_{AB} E_{XZ}] \geq \frac{1}{2}. \quad (5.9)$$

Böylece eğer $\langle E_X \rangle + \langle E_Z \rangle < 1/2$ ise ρ_{AB} dolanıktır, burada $\langle O \rangle = \text{Tr}[\rho_{AB} O]$ olarak tanımlanır.

5.2.1 Shannon entropik tanıkları

Ayrılabilir durumlar için $S(A|B) \geq 0$ olur ve veri-işleme eşitsizliğinden $H(X_A|X_B) \geq H(X_A|B)$ ve $H(Z_A|Z_B) \geq H(Z_A|B)$ olacağından (4.18) bağıntısı aşağıdaki gibi

sağlanır,

$$H(X_A|X_B) + H(Z_A|Z_B) \geq q_{MU}. \quad (5.10)$$

Burada q_{MU} parametresi Alice'in sistemine bağlıdır, ancak Bob'un sistemi üzerinde X_B ve Z_B gözlenebilirleri keyfi seçilebilir.

ρ_{AB} 'nin çoklu kopyalarına sahip Alice ve Bob'un kendi sistemleri üzerinde X veya Z gözlenebilirlerini ölçtüğü bir protokol ile (5.10), dolanıklık tanıkları için kullanılabilir. $H(X_A|X_B)$ ve $H(Z_A|Z_B)$ koşullu entropileri, $Pr(X_A = x_A, X_B = x_B)$ ve $Pr(Z_A = z_A, Z_B = z_B)$ ortak olasılık dağılımlarından hesaplanabilir ve Denk.(5.10) ihlal edilirse ρ_{AB} dolanıktır denir. İşlevsellik açısından (5.9) daha çok dolanık durum saptar ancak, (5.10)'un saptadığı dolanıklığın kalitesi daha yüksektir (Coles v.d 2017).

Bu ifade dolanıklık tanıklarında, entropik yaklaşımın bir avantajı olarak açığa çıkmaktadır. Yani (5.9)'u verdiği *evet - hayır* cevabı yerine bir alt sınır verir. Diğer bir avantajı, Bob'un sistemi üzerinde herhangi bir yapı gerektirmez. (5.9), Alice ve Bob'un ölçümlerinde karşılıklı yansızlık gerektirirken, (5.10), Bob'un sistemi üzerinde keyfi ölçümlere izin verir.

5.2.2 Diğer entropik tanıklar

Benzer bir yaklaşım çarpışma entropisi için türetilir. İki-parçalı bir sistemde, Alice'in sistemi üzerinde n tane KYB'nin bir kümesinin kullanıldığı dolanık durumlar için ($d_A + 1$ tane KYB'nin n elemanlı bir alt kümesi, $d_A \geq n$), eğer Alice'in sistemi üzerinde n tane KYB'nin bir $\{X_j\}$ alt kümesi ve Bob'un sistemi üzerinde n tane POVM $\{Y_j\}$ kümesi düşünülürse, bütün ayrılabilir durumlar için aşağıdaki bağıntı sağlanmalıdır (Berta v.d 2016),

$$\sum_{j=1}^n 2^{-H_2(X_j|Y_j)} \leq 1 + \frac{n-1}{d_A}. \quad (5.11)$$

Bu ifade (5.10)'dan daha çok ancak (5.9)'dan daha az dolanık durum saptar.

5.3 Steering Eşitsizlikleri

Schrödinger (1935) tarafından vurgulanan steering, iki parçalı sistemler için, dolaşıklıkla ilişkili bir olaydır (tam olarak aynı olmamasına rağmen). İki parçalı AB sisteminde, bir taraftaki ölçüm seçiminin (A üzerinde) diğer tarafın durumunda (B üzerinde) farklı bir topluluğa yol açmasına karşılık gelir. Bu olay bütün kuantum durumlarında gözlenmez, örneğin: ayrılabilir durumlar. Diğer taraftan Bell eşitsizliğini ihlal eden bütün durumlar, steerable durumlar olarak ele alınır (Coles v.d 2017).

Yerel gizli değişken modelinde B sistemi, A üzerinde yapılan keyfi ölçümlerle klasik korelasyonlar barındıran bir yerel kuantum duruma sahiptir. Eğer B yerel gizli duruma sahipse, kendi ölçüm olasılıkları A üzerindeki ölçüm sonuçlarına koşullandırılmış olsa bile mutlaka tek parçalı belirsizlik bağıntısına ait olmalıdır.

Şimdi steering gözlemlenmeyen bir AB sistemi düşünölsün. Yerel gizli durum modelinde, A sistemi üzerinde X_A ve B sistemi üzerinde X_B ayrık gözlenebilirleri için ortak olasılık dağılımı şöyle ifade edilebilir;

$$p(X_A, X_B) = \sum_{\lambda} p(\Lambda = \lambda) p(X_A | \Lambda = \lambda) p_Q(X_B | \Lambda = \lambda). \quad (5.12)$$

Burada Λ , Bob'un lokal durumundan belirlenen gizli değişken, λ ise bu değişkenin alabileceği özel bir olasılık ve Q alt indisi tek bir kuantum sisteminden kaynaklanan olasılık dağılımını vurgular. Güçlü alt toplanabilirlik bağıntısından;

$$\begin{aligned} H(X_B | X_A) &\geq H(X_B | X_A \Lambda) \\ &= \sum_{\lambda} p(\Lambda = \lambda) H(X_B | X_A \Lambda = \lambda) \\ &= \sum_{\lambda} p(\Lambda = \lambda) H(X_B | \Lambda = \lambda) \end{aligned} \quad (5.13)$$

yazılabilir. Burada $H(X_B | X_A \Lambda = \lambda)$, X_A üzerine ve $\Lambda = \lambda$ olayına koşullanmış X_B 'nin entropisidir. Üçüncü satır Bayes' kurallarından (Bknz (2.16)) ve (5.12)'den yararlanılarak elde edilebilir. Böylece B üzerinde X_B ve Z_B gibi iki gözlenebilir ve A üzerinde gözlenebilirler X_A ve Z_A için,

$$H(X_B | X_A) + H(Z_B | Z_A) \geq \sum_{\lambda} p(\Lambda = \lambda) [H(X_B | \Lambda = \lambda) + H(Z_B | \Lambda = \lambda)], \quad (5.14)$$

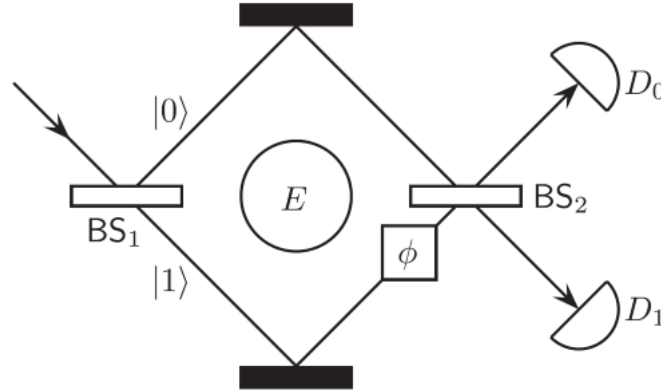
elde edilir. Bu ifade MU bağıntısı ile birleştirilirse steering eşitsizliği elde edilmiş olur (Schneeloch v.d 2013),

$$H(X_B|X_A) + H(Z_B|Z_A) \geq q_{MU}. \quad (5.15)$$

Burada q_{MU} niceliği Bob'un gözlenebilirlerine karşılık gelmektedir. Yerel gizli durum modelini kabul eden herhangi bir ρ_{AB} durumu, (5.15)'i mutlaka sağlamalıdır. Böylece bu bağıntının deneysel ihlali steering sergilenmesini oluşturacaktır.

5.4 Dalga-Parçacık İkiliği

Uzun yıllar önce ışığın hem dalga hem de parçacık gibi davrandığına dair deneyler yapılmış, her iki davranış biçimini de sergilediği gözlemlenmiş ve buna ışığın *dalga-parçacık ikiliği* denilmiştir. Işık, bir yarıktan kırınıma uğrarken dalga gibi, fotoelektrik olay gibi deneyler de ise parçacık gibi hareket eder. Ancak ışığın bu davranış biçimlerini hiçbir zaman aynı anda göstermediği bilinmektedir.



Şekil 5.2. Tek foton için Mach-Zehnder interferometresi. Fotonun aldığı yol Z 'nin bazları $\{|0\rangle, |1\rangle\}$ ile etiketlenmiştir. E ise fotonun çevresini temsil etmektedir. Bir faz ϕ alt kola uygulanmış ve fotonun alabileceği iki yol ikinci ışın ayırıcıya (*beam splitter*) gelmektedir. En son olarak gelen foton dedektörler D_0 veya D_1 'den birinde tespit edilir (Coles v.d 2017).

Dalga-parçacık ikiliği bağıntıları (*wave-particle duality relations*), EBB uygulamalarından önce ortaya atılmıştır (Wooters ve Zurek 1979, Jaeger v.d 1995). Bu bağıntıların çoğunda, tek bir foton için Mach-Zehnder interferometresi ele alınmıştır. Bu durumda fotonun parçacık özelliği interferometre içinde aldığı bilinen

yol, dalga özelliği ise iki kol arasındaki ϕ görelî faz farkından belirli bir çıktı modunda fotonu tespit etme olasılığındaki salınımları görmekle ilişkilidir. Varsayılın ki, $Z = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ hangi yoldan ilerlediğini betimleyen gözlenebilir olsun ve parçacık davranışı yol tahmin edilebilirliği $\mathcal{P} = p_{\max} - p_{\min} = 2p_{\text{tahm}}(Z) - 1$ olarak önerilsin (Wooters ve Zurek 1979); yani $\mathcal{P} = 1$ ise bir koldan gitme tahmin edilebilirliği kesindir. Dalga davranışı ise saçak görünebilirliği tarafından ,

$$\mathcal{V} = \frac{p_0^{\max} - p_0^{\min}}{p_0^{\max} + p_0^{\min}}; \quad p_0^{\max} := \max_{\phi} p_0 \quad \text{ve} \quad p_0^{\min} := \min_{\phi} p_0, \quad (5.16)$$

ile nicelendirilebilir. Burada p_0 , D_0 detektörü tarafından saptanan foton için olasılıktır. Aşağıdaki bağıntının doğruluğu Wooters ve Zurek (1979) tarafından gösterilmiştir,

$$\mathcal{P}^2 + \mathcal{V}^2 \leq 1. \quad (5.17)$$

$\mathcal{V} = 0$ iken $\mathcal{P} = 1$; yani tamamen parçacık davranışında hiç dalga davranışı gözlemlenmeyeceği veya tam tersini ima eder.

Daha genel olarak, interferometre içinde çevresi E ile etkileşim halinde olan bir foton düşünölsün. Eğer E ölçülebilirse, çevresi ile koşullandırılmış bir foton için yol ayırt edilebilirliği,

$$\mathcal{D} = 2p_{\text{tahm}}(Z|E) - 1. \quad (5.18)$$

olarak önerilebilir ve (5.17)'un güçlendirilmiş bir versiyonu elde edilebilir (Jaeger v.d 1995),

$$\mathcal{D}^2 + \mathcal{V}^2 \leq 1. \quad (5.19)$$

Yakın zamanda (5.17) ve (5.19)'un aslında EBB'nin kılık değıştirmiş halleri olduğı ispatlanmıştır (Coles v.d 2014). Dalga ve parçacık olasılıkları, min ve max entropiler cinsinden yazılabilir ve tamamlayıcı kübit gözlenebilirlerine uygulanabilir. Şöyle ki, (5.17) aslında aşağıdaki belirsizlik bağıntısına eşdeğerdur (Coles v.d 2014),

$$H_{\min}(Z) + \min_{W \in XY} H_{\max}(W) \geq 1. \quad (5.20)$$

Burada $\min_{W \in XY}$, Bloch küresi üzerinde x-y düzleminde yer alan bütün gözlenebilirler üzerinde alınan minimizasyona karşılık gelmektedir. Buna benzer bir şekilde

(5.19)'da aşağıdaki bağıntıya eşdeğerdir (Coles v.d 2014),

$$H_{min}(Z|E) + \min_{W \in XY} H_{max}(W) \geq 1. \quad (5.21)$$

Bu ifadeler dalga-parçaçık ikiliği bağıntısı ile EBB'yi birleştirmekte ve (5.17)'in, (5.19)'un özel bir durumu olduğunu göstermektedir.

Min ve max entropiler yerine diğer entropilerin kullanılması incelenmiş (Boysk v.d 2013), ancak dalga-parçaçık ikililiği ilişkisine tam bir karşılık elde edilememiştir. Ayrıca çok kollu interferometreler için dalga ve parçaçık davranışı arasındaki entropik ölçüler üzerine çalışmalar da vardır (Englert v.d 2008).

5.5 Koherenslik

Baumgratz v.d (2014), koherensliği nicelendirmek için bir çerçeve oluşturmuşlardır ki, bu koherent olmayan operasyonlar altında artmayan bir ölçüdür. Bir çok ölçü ele alınabilir, ancak bu kısımda operasyonel açıdan en koherent halde bulunan durumların damıtılmasının miktarı (Winter ve Yang 2016) terimleri cinsinden,

$$\Phi(Z, \rho) := D \left(\rho \parallel \sum_z |Z\rangle \langle Z| \rho |Z\rangle \langle Z| \right), \quad (5.22)$$

koherensliğin görelî entropisi terimleri ile incelenecektir. Koherenslik hem ortonormal bazlar $Z = \{|Z\rangle \langle Z|\}$ hem de ρ durumunun bir fonksiyonudur.

Bir ρ_A durumu ele alınsın ve Z bu durum üzerine uygulanan seçici olmayan bir tam izdüşüm işlemcisi olsun. Eğer ρ_A için bir saflaştırıcı E sistemi düşünülürse,

$$\Phi(Z, \rho_A) = H(Z|E), \quad (5.23)$$

ifadesi doğru olur (Coles v.d 2011, 2012). İzdüşüm işlemcisi için koherensliğin görelî entropisi olan bu durum, saflaştırma sistemi ile verilen ölçümün belirsizliğine eşdeğerdir. Diğer bir deyişle E 'ye erişime izin verilirse, (5.23)'ün sağ tarafı kuantum hafıza varlığında belirsizliği nicelendirir. Bu sayede (4.22) farklı ölçümler için koherensliğin bir alt limiti olarak ele alınabilir. Toplam belirsizlik klasik ve kuantum olarak ayrılırsa, rank-1 izdüşüm işlemcileri ve bir ρ kuantum durumu için $C(Z, \rho) :=$

$H(\rho)$ olacak şekilde bir klasik belirsizlik tanımlanabilir ve kuantum belirsizlik koherensliğin göreceli entropisi olur (Korzekwa v.d 2014, Luo 2015)

$$Q(Z, \rho) := D \left(\rho \parallel \sum_z |Z\rangle \langle Z| \rho |Z\rangle \langle Z| \right). \quad (5.24)$$

Bütün belirsizlik, klasik ve kuantum parçalar üzerinden direk olarak toplanarak gösterilir,

$$H(Z) = Q(Z, \rho) + C(Z, \rho). \quad (5.25)$$

Kuantum kısımlar için bazı belirsizlik bağıntıları Korzekwa v.d (2014) tarafından gösterilmiştir, ancak (5.23) ve (4.22) birlikte kullanılarak kuantum hafıza varlığında EBB yeniden yorumlanabilir.

5.6 Diskord

Diskord kavramı ilk defa Ollivier ve Zurek (2001) tarafından tüm kuantum korelasyonları nicelendirmek için şöyle tanımlanmıştır (Bknz (4.30)):

$$D(B|A) := I(A; B) - J_A(\rho_{AB}). \quad (5.26)$$

Burada, $I(A; B)$ karşılıklı bilişimi, iki parçalı bir AB sisteminin herhangi bir ρ_{AB} durumundaki bütün korelasyonları (kuantum ve klasik) nicelendirir. $J_A(\rho_{AB})$ ise A üzerindeki POVM ölçümleri ile belirlenen ve ölçümden bağımsızlığı sağlamak için maksimumu alınan aşağıdaki ifade ile tanımlanır;

$$J_A(\rho_{AB}) := \max_X I(X; B). \quad (5.27)$$

Burada optimizasyon A sistemine etki eden bütün X POVM ölçümleri üzerinden yapılmaktadır. Aşağıdaki bağıntı kuantum hafıza varlığında belirsizlik bağıntılarının diskord eklenerek güçlendirilmiş halidir (Bknz (4.27));

$$H(X|B) + H(Z|B) \geq q_{MU} + S(A|B) + [D(B|A) - J_A(\rho_{AB})]. \quad (5.28)$$

Bu ifade diskord için bir üst sınır elde etmede kullanılabilir (Hu ve Fan 2013),

$$\begin{aligned} H(X|B) + H(Z|B) - q_{MU} + S(A|B) &\geq [D(B|A) - J_A(\rho_{AB})] \\ H(X|B) + H(Z|B) - q_{MU} + S(A|B) &\geq [D(B|A) - I(A; B) + D(B|A)] \end{aligned} \quad (5.29)$$

$$\frac{1}{2} [I(A; B) - \delta_T] \geq D(B|A).$$

Burada $\delta_T := H(X|B) + H(Z|B) - q_{MU} - S(A|B)$ olarak tanımlanmaktadır. Böylece A ve B bileşenleri arasında bulunan kuantum korelasyonların miktarı için bir üst sınır elde edilmiş olunur.

5.7 Klasik Korelasyonların Kilitlenmesi

Bu bölümde klasik korelasyonların kilitlenmesi, Fawzi v.d. (2011) tarafından geliştirilen kriptografik bakış açısı ile ele alınarak kısaca özetlenecektir. Klasik korelasyonların kilitlenmesi kabaca bir klasik mesajın , mesajın boyutundan küçük bir klasik anahtar kullanarak bir kuantum durumuna şifrelenmesi protokolü olarak tanımlanır. Amaç, mesajın anahtar bilinmiyorken kuantum durumu içine kitleme-sidir, örneğin olası bir ölçümde mesaj hakkında göz ardı edilebilecek kadar bilişim açığa çıksın. Dahası, mesajın tekrar açığa çıkarılması ve tamamen kurtarılması anahtarın bilinmesi ile mümkün olsun. Bu olgunun EBB ile bağıntısı, n kübit BB84 ölçümleri için türetilen MU sınırı ile anlatılabilir,

$$H(M^n|\Theta^n) \geq n \cdot \frac{1}{2}. \quad (5.30)$$

Burada $\Theta^n \in \{\theta_1, \dots, \theta_n\}$ olarak tanımlanır. Tekdüze rasgele bir n -bit X dizisini şifrelemek için, BB84 bazlarından rasgele seçilen n kübit seçilir ve mesaj bu bazlara şifrelenir. (5.30)'den, herhangi bir ölçüm için, ölçüm sonucu ve orjinal X mesajı arasında en fazla $n/2$ kadar karşılıklı bilişim olabilir. Yani, bu duruma $n/2$ bit şifrelenebilir ve anahtar bilinmeden erişilemez. Bu önemli bir gelişmedir, çünkü n -bit mesajın herhangi önemsiz olmayan tamamen saf klasik şifrelemesi en az n boyutunda anahtar gerektirmektedir. Burada, anahtar boyutuyla kilitlenebilir bit sayısı arasında uygun bir takas olabileceği sorusu yöneltilebilir ve bu amaç için EBB kullanılabilir (Fawzi v.d. 2011).

$$H(M|\Theta) \geq n \cdot (1 - 2\epsilon) - h_{bin}(\epsilon) \quad , \quad \Theta = \{\theta_1, \dots, \theta_n\} \text{ ile.} \quad (5.31)$$

Burada $\epsilon \geq (1/2d) \sum_{i=1}^d |Tr[\rho\theta_i] - (1/d)|$ olarak tanımlanır. Bundan yola çıkılarak, $L = O[\log(n/\epsilon)]$ boyutunda bir anahtarın en fazla $\epsilon > 0$ 'dan daha küçük bir karşılıklı bilişim kadar n -bit dizisi kilitlenmesi için izin verdiği gösterilmiştir.

6. SONUÇ

Entropik belirsizlik bağıntıları ellili yılların sonunda ortaya atılmasına rağmen, kuantum bilişim kuramının son yıllarda katettiği yol ile birlikte kendine çok geniş bir kullanım alanı bulmuştur. Özellikle kuram içerisinde entropi ile açıklanmaya çalışılan konularda ve tamamlayıcı gözlenebilirler açısından bilişim elde etme amacıyla yapılan hesaplamalarda elde edilebilecek bilişim için bir alt sınır oluşturulmasına olanak sağlamıştır. Bağıntıların, bir hafıza sistemi olmadan ve bir hafıza sistemi varlığı üzerinden tartışılması, tek ve çok parçalı sistemlerde belirsizliğin nasıl nicelendirilebileceği üzerine bir bakış açısı geliştirmiştir.

İlk olarak, tek parçalı sistemlerde EBB için, Maasen ve Uffink'in kanıtladığı alt sınır haricinde, farklı durumlar için daha güçlü alt sınırların elde edilebileceği gösterilmiştir. Bu alt sınırın da durum bağımsız olması dikkat çeken ilk sonuçtur. Bölüm 3'te yer alan tahmin oyununda Bob'un, Alice'in ölçüm kümesini bilse de, asla kesin bir tahmin yapamayacağı görülmektedir. Ayrıca kuantum sistemlerde ölçüm, sistemin durumunu değiştirdiği için tek bir ölçüm şansı olan Bob'un, doğru tahmin yapamazsa tekrar ölçüm yapma şansı olmayacaktır. Yani Alice'in kullandığı sıra değişmeyen işlemciler arasında her zaman belirsizlik olacaktır ve bu Heisenberg'in elde ettiği sonuç ile tam olarak uyumaktadır.

Çok parçalı sistemlerde ise, özellikle sistemler arasındaki korelasyonların belirsizliği ne kadar etkilediği ile ilgili araştırmalar odak noktası olmuştur. Klasik korelasyonların belirsizliği etkilemediği açıkça söylenebilse de, kuantum korelasyonlar için aynı şey söylenememektedir. Dolanıklık, kuantum mekaniksel bir olgudur ve belirsizliği önemsiz bir alt sınıra indirgeyebilmesi dikkat çekici bir sonuçtur (Bknz (4.22)).

Aralarında dolanıklık gibi kuantum korelasyonların olduğu çok-parçalı sistemlerin kopyaları üzerinde farklı ölçümler yaparak, kesin bir sonuç elde etmenin mümkün olduğu gösterilmiştir. Dolanıklık-destekli belirsizlik bağıntısının diğer bir sonucu da, bu bağıntının tek parçalı sistemlere indirgenmesiyle elde edilen sonuçtur. İlk bölümlerde üzerinde sıkça sözü edilen durum-bağımsız alt sınırın, tek-parçalı sistemlerde saf olmayan durumlar için geçerli olmadığı ve üzerinde ölçüm yapılan durumun başlangıçtaki entropisinin aslında alt sınırı geliştirdiği gözlenmiştir (Bknz (3.28)).

Bağıntıların bilişim kuramı uygulamalarında, özellikle son 20 yıl içerisinde birçok konuda sadece belirsizlik için alt sınır elde etmek amacıyla kullanılmadığı görülmektedir. Özellikle dolanıklık tanıklıkları içerisinde, daha iyi damıtılmış ve daha kaliteli dolanıklıkları yakalamakta kullanılması, bağıntıların uygulamalarına iyi bir örnektir. Kuantum diskord için verilen üst sınır, bu bağıntıların farklı bir kullanım amacını da ortaya koymaktadır. Ayrıca kuantum anahtar dağıtımı gibi, çok-parçalı sistemlerde kulak misafirinin elde etmeye çalıştığı bilişim miktarı için verilen alt sınır, kuantum kriptolojide vaad edilen yüzde yüz güvenliğin mümkün olduğunu göstermektedir.

Sonuç olarak EBB, bilişim kuramı içerisinde, özellikle standart sapma kullanılan Heisenberg belirsizlik bağıntılarından daha geniş bir kullanıma sahiptir. Sadece belirsizliklerin alt sınırı için değil, aynı zamanda birçok bilişim faaliyetinde farklı amaçlar için araç olarak kullanılmış ve kullanılmaya devam etmekte olup, hala güncel olarak çalışılan bir konudur.

KAYNAKLAR

- Ballester, M. A. ve Wehner, S. Entropic uncertainty relations and locking: Tight bounds for mutually unbiased bases. *Phys. Rev. A* 75, 022319 (2007).
- Ballester, M. A., Wehner, S. ve Winter, A. State Discrimination With Post-Measurement Information. *IEEE Trans. Inf. Theory* 54, 4183–4198 (2008).
- Baumgratz, T., Cramer, M. ve Plenio, M. B. Quantifying Coherence. *Phys. Rev. Lett.* 113, 140401 (2014).
- Bennett, C. H. ve G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing 1984*, Vol. 1 (IEEE, Bangalore), pp. 175–179.
- Berta, M., Christandl, M., Colbeck, R., Renes, J. M. ve Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* 6, 659–662 (2010).
- Berta, M., Wehner, S. ve Wilde, M. M. Entropic uncertainty and measurement reversibility. *New J. Phys.* 18, 073004 (2016).
- Białyński-Birula, I ve Mycielski, J. Uncertainty relations for information entropy in wave mechanics. *Commun. Math. Phys.* 44, 129–132 (1975).
- Christandl, M. ve Winter, A. Uncertainty, Monogamy, and Locking of Quantum Correlations. *IEEE Trans. Inf. Theory* 51, 3159–3165 (2005).
- Coles, P. J., Yu, L., Gheorghiu, V. ve Griffiths, R. B. Information-theoretic treatment of tripartite systems and quantum channels. *Phys. Rev. A* 83, 062338 (2011).
- Coles, P. J. Unification of different views of decoherence and discord. *Phys. Rev. A* 85, 042103 (2012).
- Coles, P. J., Colbeck, R., Yu, L. ve Zolowak, M. Uncertainty Relations from Simple Entropic Properties. *Phys. Rev. Lett.* 108, 210405 (2012).
- Coles, P. J., Kaniewski, J. ve Wehner, S. Equivalence of wave–particle duality to entropic uncertainty. *Nat. Commun.* 5, 5814 (2014).
- Coles, P. J. ve Piani, M. Improved entropic uncertainty relations and information exclusion relations. *Phys. Rev. A* 89, 022112 (2014).
- Coles, P. J., Berta, M., Tomamichel, M. ve Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* 89, 015002 (2017).
- Deutsch, D., Uncertainty in Quantum Measurements. *Phys. Rev. Lett.* 50, 631–633 (1983).
- Ekert, A. K. Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* 67, 661–663 (1991).

- Englert, B.-G., Kaszlikowski, D., Kwek, C.L., Wei, H. C. Wave-particle duality in multi-path interferometers: general concepts and three-path interferometers, *International Journal of Quantum Information* Volume 6 Issue 01 Pages 129-157 (2008)
- Everett, H. ‘Relative State’ Formulation of Quantum Mechanics. *Rev. Mod. Phys.* 29, 454–462 (1957).
- Fawzi, O., Hayden, P. ve Sen, P. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. in *Proceedings of the 43rd annual ACM symposium on Theory of computing - STOC '11* 773 (ACM Press, 2011).
- Friedland, S., Gheorghiu, V. ve Gour, G. Universal Uncertainty Relations. *Phys. Rev. Lett.* 111, 230401 (2013).
- Hall, M. J. W. Information Exclusion Principle for Complementary Observables. *Phys. Rev. Lett.* 74, 3307–3311 (1995).
- Heisenberg, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Phys.* 43, 172–198 (1927).
- Hirschman, I. I. A Note on Entropy. *Am. J. Math.* 79, 152 (1957).
- Hu, M.-L. ve Fan, H. Upper bound and shareability of quantum discord based on entropic uncertainty relations. *Phys. Rev. A* 88, 014105 (2013).
- Jaeger, G., Shimony, A. ve Vaidman, L. Two interferometric complementarities. *Phys. Rev. A* 51, 54–67 (1995).
- Kennard, E. H. Zur Quantenmechanik einfacher Bewegungstypen. *Zeitschrift für Phys.* 44, 326–352 (1927).
- Kraus, K. Complementary observables and uncertainty relations. *Phys. Rev. D* (1987) doi:10.1103/PhysRevD.35.3070.
- Krishna, M., ve Parthasarathy, K. R., “An Entropic Uncertainty Principle for Quantum Measurements.” *Sankhyā: The Indian Journal of Statistics, Series A* (1961-2002), vol. 64, no. 3, 2002, pp. 842–851.
- [(Li v.d 2011)] Li2011 Li, C.-F., Xu, J.-S., Xu, X.-Y., Li, K. Guo, G.-C. Experimental investigation of the entanglement-assisted entropic uncertainty principle. *Nat. Phys.* 7, 752–756 (2011).
- Lieb E. H. ve Ruskai M. B., Proof of the strong subadditivity of quantum-mechanical entropy. *J. Math. Phys.* 14, 1938–1941 (1973).
- Maassen, H. ve Uffink, J. B. M. Generalized entropic uncertainty relations. *Phys. Rev. Lett.* 60, 1103–1106 (1988).
- Nielsen, M. A. ve Chuang, I. L. *Quantum Computation and Quantum Information*, 10th Anniversary Edition. (Cambridge University Press , 2011).

- Ollivier, H. ve Zurek, W. H. Quantum Discord: A Measure of the Quantumness of Correlations. *Phys. Rev. Lett.* 88, 017901 (2001).
- Pati, A. K., Wilde, M. M., Devi, A. R. U., Rajagopal, A. K. ve Sudha. Quantum discord and classical correlation can tighten the uncertainty principle in the presence of quantum memory. *Phys. Rev. A* 86, 042105 (2012).
- Renes, J. M. ve Boileau, J.-C. Conjectured Strong Complementary Information Tradeoff. *Phys. Rev. Lett.* 103, 020402 (2009).
- Robertson, H. P. The Uncertainty Principle. *Phys. Rev.* 34, 163–164 (1929).
- Sánchez-Ruiz, J. Entropic uncertainty and certainty relations for complementary observables. *Phys. Lett. A* 173, 233–239 (1993).
- Sánchez-Ruiz, J. Optimal entropic uncertainty relation in two-dimensional Hilbert space. *Phys. Lett. A* 244, 189–195 (1998).
- Wehner, S. ve Winter, A. Entropic uncertainty relations—a survey. *New J. Phys.* 12, 025009 (2010).
- Weyl, H. Quantenmechanik und Gruppentheorie. *Zeitschrift für Phys.* 46, 1–46 (1927).
- Winter, A. ve Yang, D. Operational Resource Theory of Coherence. *Phys. Rev. Lett.* 116, 120404 (2016).

SHANNON ENTROPİSİNİN EN BÜYÜK DEĞERİ VE BAĞIL ENTROPİNİN POZİTİFLİĞİ

Bölüm(2.2.1)'de Shannon entropisinin en büyük değerini, olasılık dağılımı tekdüze dağılım gösteriyorsa aldığı söylenmişti. Şimdi bunu göstermek gereklidir.

n elemanlı bir olasılık dağılımı kümesinde, örneğin $p_1 = 1 - \sum_{i=2}^n p_i$ şeklinde yazılabildiğinden sadece $n - 1$ tane bağımsız değişken vardır. Shannon entropisi de sadece $n - 1$ bağımsız olasılığa bağlıdır. Böylece¹,

$$H(X) = -p_1 \ln p_1 - \sum_{i=2}^n p_i \ln p_i, \quad (\text{EK1.1})$$

şeklinde yazılabilen Shannon entropisinin p_j elemanına göre türevi alınarak sıfıra eşitlenir ve ekstremum noktaları incelenirse, her $j \geq 2$ için,

$$\begin{aligned} \frac{\partial H(X)}{\partial p_j} &= -\frac{\partial p_1}{\partial p_j} \ln p_1 - p_1 \frac{\partial \ln p_1}{\partial p_j} - \sum_{i=2}^n \left(\frac{\partial p_i}{\partial p_j} \ln p_i + p_i \frac{\partial \ln p_i}{\partial p_j} \right) \\ &= \ln p_1 + p_1 \frac{1}{p_1} - \sum_{i=2}^n \left(\delta_{ij} \ln p_i + p_i \frac{\delta_{ij}}{p_i} \right) \\ &= \ln p_1 - \ln p_j = 0, \end{aligned} \quad (\text{EK1.2})$$

olmalıdır. Buradan, her $j \geq 2$ için, $\ln p_j = \ln p_1$ olduğu görülür ve böylece $p_j = p_1$ olur; yani bütün olasılık dağılımı aynı büyüklükte, $p_j = 1/n$ gibi tekdüze bir dağılım göstermelidir. Böylece istenen ispatlanmış olur.

Klasik bağıl entropinin her zaman pozitif olduğunu gösterebilmek için *Gibbs eşitsizliği* ispatlanmalıdır. Bir rasgele X değişkeni için, $p(x)$ ve $q(x)$ gibi iki olasılık dağılımının Gibbs eşitsizliği şöyledir,

$$-\sum_x p(x) \ln p(x) \leq -\sum_x p(x) \ln q(x), \quad (\text{EK1.3})$$

ve eşitlik durumu ancak ve ancak $p(x) = q(x)$ olduğunda elde edilir. Şimdi, eşitsizlik aşağıdaki gibi düzenlenirse $-\ln x$ fonksiyonun konveksliğinden ($x \geq 0$ için),

$$-\sum_x p(x) \ln \frac{q(x)}{p(x)} \geq -\ln \left(\sum_x p(x) \frac{q(x)}{p(x)} \right) = 0, \quad (\text{EK1.4})$$

¹Ekler bölümünde işlem kolaylığı için, log fonksiyonu yerine $\ln$ fonksiyonu kullanılacak ve $\ln(x) = \log(x) \ln(2)$ özdeşliğinden gelen $\ln(2)$ terimi hesaplarda dikkate alınmayacaktır.

elde edilir ve böylece Gibbs eşitsizliği gösterilmiş olur. Klasik bağıl entropi tekrar yazılırsa,

$$\sum_x p(x) \ln p(x) - \sum_x p(x) \ln q(x) = D(p(x)||q(x)) \geq 0, \quad (\text{EK1.5})$$

çıkar ve bağıl entropinin her zaman pozitif olduğu ispatlanmış olur.

Gibbs eşitsizliği şu şekilde de ispatlanabilir. $\ln x \leq x - 1$, $x > 0$, özdeşliğinden yararlanarak, aşağıdaki ifadeler yazılabilir (eşitlik için $x = 1$ gerek ve yeter koşuldur.),

$$\begin{aligned} -\sum_x p(x) \ln \frac{q(x)}{p(x)} &\geq -\sum_x p(x) \left(\frac{q(x)}{p(x)} - 1 \right) \\ &= -\sum_x q(x) + \sum_x p(x) = -\sum_x q(x) + 1 \geq 0. \end{aligned} \quad (\text{EK1.6})$$

Son satırdaki ifade her zaman doğrudur çünkü $q(x)$ bir olasılık dağılımıdır ve $q(x) \geq 0$ ve $\sum_x q(x) = 1$ sağlanır. Böylece Gibbs eşitsizliği tekrar ispatlanmış olur.

Kuantum bağıl entropi için ise *Klein eşitsizliği* ispatlanmalıdır,

$$-Tr(\rho \ln \sigma) \geq -Tr(\rho \ln \rho). \quad (\text{EK1.7})$$

Burada $\rho = \sum_i \lambda_i |r_i\rangle \langle r_i|$ ve $\sigma = \sum_j \sigma_j |s_j\rangle \langle s_j|$ spektral ayrışmaları ile birlikte iki yoğunluk işlemcisidir, burada λ_i ve σ_j 'ler özdeğerlerdir. Sol taraf ele alınırsa,

$$\begin{aligned} -Tr(\rho \ln \sigma) &= -\sum_i \lambda_i \langle r_i | \ln \sigma | r_i \rangle \\ &= -\sum_i \lambda_i \langle r_i | \left(\sum_j \ln \sigma_j |s_j\rangle \langle s_j| \right) | r_i \rangle = -\sum_i \lambda_i \left(\sum_j \mu_{ji} \ln \sigma_j \right), \end{aligned} \quad (\text{EK1.8})$$

çıkar. Burada $\mu_{ji} = |\langle s_j | r_i \rangle|^2$, ikili stokastik bir matristir ($\sum_i \mu_{ij} = 1 = \sum_j \mu_{ij}$). Yine $-\ln x$ fonksiyonunun konveksliğinden,

$$-\sum_i \lambda_i \left(\sum_j \mu_{ji} \ln \sigma_j \right) \geq -\sum_i \lambda_i \ln \left(\sum_j \mu_{ji} \sigma_j \right) = -\sum_i \lambda_i \ln \eta_i, \quad (\text{EK1.9})$$

elde edilir ve burada $\eta_i = \sum_j \mu_{ji} \sigma_j$ olarak tanımlanır. Gibbs eşitsizliğinden,

$$-\sum_i \lambda_i \ln \eta_i \geq -\sum_i \lambda_i \ln \lambda_i = -Tr(\rho \ln \rho), \quad (\text{EK1.10})$$

yazılabilir ve böylece

$$-Tr(\rho \ln \sigma) \geq -Tr(\rho \ln \rho), \quad (\text{EK1.11})$$

gösterilmiş olur.



EK 2

RÉNYİ ENTROPİSİNİN MONOTONLUĞU VE LİMİTLERİ

Çıktıları x olan bir rasgele X değişkeninin çıktılarına ait bir ayırık olasılık dağılımının Rényi entropisi α -monoton azalan bir fonksiyondur; yani α 'nın değeri büyüdükçe Rényi entropisi azalır. Bunu göstermek için α 'ya göre türevinin pozitif olmadığını göstermek gereklidir,

$$\frac{d}{d\alpha} H_\alpha(X) \leq 0. \quad (\text{EK2.1})$$

$H_\alpha(X)$ 'in α 'ya göre türevi (bundan sonra $p_X(x) = p(x)$ kısaltması kullanılacaktır.),

$$\begin{aligned} \frac{d}{d\alpha} H_\alpha(X) &= \frac{d}{d\alpha} \left[\frac{1}{1-\alpha} \ln \left(\sum_x p^\alpha(x) \right) \right] \\ &= \frac{1}{(1-\alpha)^2} \ln \left(\sum_x p^\alpha(x) \right) + \frac{1}{1-\alpha} \frac{1}{\sum_x p^\alpha(x)} \frac{d}{d\alpha} \left(\sum_x p^\alpha(x) \right). \end{aligned} \quad (\text{EK2.2})$$

Türevin daha kolay alınabilmesi için form değiştirilirse,

$$\begin{aligned} \frac{d}{d\alpha} H_\alpha(X) &= \frac{1}{(1-\alpha)^2} \ln \left(\sum_x p^\alpha(x) \right) + \frac{1}{1-\alpha} \frac{1}{\sum_x p^\alpha(x)} \left(\sum_x \frac{d}{d\alpha} e^{\alpha \ln p(x)} \right) \\ &= \frac{1}{(1-\alpha)^2} \ln \left(\sum_x p^\alpha(x) \right) + \frac{1}{1-\alpha} \frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p(x) \\ &= \frac{1}{(1-\alpha)^2} \left[\ln \left(\sum_x p^\alpha(x) \right) + \frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p^{1-\alpha}(x) \right], \end{aligned} \quad (\text{EK2.3})$$

elde edilir. $1/(1-\alpha)^2$ terimi pozitifdir ve parantez içindeki ifadenin pozitif olmadığını göstermek yeterlidir:

$$\begin{aligned} &\ln \left(\sum_x p^\alpha(x) \right) + \frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p^{1-\alpha}(x) \leq 0 \\ \Rightarrow &\left(\sum_x p^\alpha(x) \right) \ln \left(\frac{1}{\sum_x p^\alpha(x)} \right) \geq \sum_x p^\alpha(x) \ln p^{1-\alpha}(x). \end{aligned} \quad (\text{EK2.4})$$

Bu eşitsizlik doğrulanırsa, Rényi entropisinin α -monoton azalan bir fonksiyon olduğu ispatlanmış olur. Bu doğrulama Jensen eşitsizliğinin bir uygulamasından elde edilebilir. Aşağıdaki bağıntı, Jensen eşitsizliğinden konveks fonksiyonlar için doğrudur,

$$\sum_x a_x f(b_x) \geq f \left(\sum_x a_x b_x \right). \quad (\text{EK2.5})$$

a_x ve b_x rasgele iki değişkendir. Şimdi değişkenler aşağıdaki gibi seçilsin,

$$a_x = \frac{p^\alpha(x)}{\sum_y p^\alpha(y)} \quad , \quad b_x = \frac{p(x)}{p^\alpha(x)} \quad \text{ve} \quad f(\cdot) = -\ln(\cdot). \quad (\text{EK2.6})$$

Burada $p(y)$, çıktıları y olan rasgele bir Y değişkeninin olasılıklarıdır. Bu değişkenler (EK2.5)'te yerine konulursa ($\sum_x p(x) = 1$),

$$\begin{aligned} -\sum_x \frac{p^\alpha(x)}{\sum_y p^\alpha(y)} \ln \left(\frac{p(x)}{p^\alpha(x)} \right) &\geq -\ln \left(\sum_x \frac{p^\alpha(x)}{\sum_y p^\alpha(y)} \frac{p(x)}{p^\alpha(x)} \right) \\ -\sum_x p^\alpha(x) \ln \left(\frac{p(x)}{p^\alpha(x)} \right) &\geq -\sum_y p^\alpha(y) \ln \left(\frac{\sum_x p(x)}{\sum_y p^\alpha(y)} \right), \end{aligned} \quad (\text{EK2.7})$$

elde edilir. Bu bağıntı için $X = Y$ kabulü yapılır ve -1 ile çarpılırsa (EK2.4)'ün doğru olduğu ispatlanmış olur.

Shannon entropisi, $\alpha \rightarrow 1$ limitinde elde edilir,

$$\lim_{\alpha \rightarrow 1} H_\alpha(X) = \lim_{\alpha \rightarrow 1} \frac{1}{1-\alpha} \ln \left(\sum_x p^\alpha(x) \right) = -\sum_x p(x) \ln p(x). \quad (\text{EK2.8})$$

Şimdi bu ifade ispatlanmaya çalışılsın. $0/0$ tanımsızlığından L'hospital kuralı kullanılmalıdır. Pay ve paydanın α 'ya göre türevleri,

$$\begin{aligned} \frac{\partial}{\partial \alpha} (1-\alpha) &= -1, \\ \frac{\partial}{\partial \alpha} \ln \left(\sum_x p^\alpha(x) \right) &= \frac{1}{\sum_x p^\alpha(x)} \frac{\partial}{\partial \alpha} \sum_x p^\alpha(x), \end{aligned} \quad (\text{EK2.9})$$

çıkar ve ikinci ifadenin sağ taraftaki türev incelenirse,

$$\begin{aligned} \frac{\partial}{\partial \alpha} p^\alpha(x) &= \frac{\partial}{\partial \alpha} e^{\ln p^\alpha(x)} = \frac{\partial}{\partial \alpha} e^{\alpha \ln p(x)} \\ &= \ln p(x) e^{\alpha \ln p(x)} = p^\alpha(x) \ln p(x), \end{aligned} \quad (\text{EK2.10})$$

olur. Yerine konulursa,

$$\frac{\partial}{\partial \alpha} \ln \left(\sum_x p^\alpha(x) \right) = \frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p(x), \quad (\text{EK2.11})$$

elde edilir. Böylece,

$$\begin{aligned} \lim_{\alpha \rightarrow 1} H_\alpha(X) &= \lim_{\alpha \rightarrow 1} -\frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p(x) \\ &= -\sum_x p(x) \ln p(x) = H(X). \end{aligned} \quad (\text{EK2.12})$$

sonucu elde edilir.

Min-entropi için $\alpha \rightarrow \infty$ limiti incelenmelidir. $-\infty/\infty$ tanımsızlığından dolayı yine L'Hospital kuralı kullanılırsa,

$$\lim_{\alpha \rightarrow \infty} \frac{\partial}{\partial \alpha} H_\alpha(X) = \lim_{\alpha \rightarrow \infty} \frac{\frac{\partial \ln(\sum_x p^\alpha(x))}{\partial \alpha}}{\frac{\partial(1-\alpha)}{\partial \alpha}}. \quad (\text{EK2.13})$$

Bir önceki ispattan bu ifadenin türevi yazılabilir,

$$\lim_{\alpha \rightarrow \infty} H_\alpha(X) = -\frac{1}{\sum_x p^\alpha(x)} \sum_x p^\alpha(x) \ln p(x). \quad (\text{EK2.14})$$

Pay ve paydadaki terimler $p_{\max}^\alpha$ ile genişletilirse,

$$\lim_{\alpha \rightarrow \infty} H_\alpha(X) = \lim_{\alpha \rightarrow \infty} -\frac{1}{\sum_x \left(\frac{p(x)}{p_{\max}}\right)^\alpha} \sum_x \left(\frac{p(x)}{p_{\max}}\right)^\alpha \ln p(x) \quad (\text{EK2.15})$$

elde edilir. Şimdi, $p(x)/p_{\max}$ incelenirse,

$$\left(\frac{p(x)}{p_{\max}}\right) \begin{cases} = 1, & p(x) = p_{\max} & \text{için} \\ < 1, & p(x) < p_{\max} & \text{için} \end{cases}. \quad (\text{EK2.16})$$

olur ve $\alpha \rightarrow \infty$ limiti,

$$\lim_{\alpha \rightarrow \infty} \left(\frac{p(x)}{p_{\max}}\right)^\alpha = \begin{cases} 1, & p(x) = p_{\max} & \text{için} \\ 0, & p(x) < p_{\max} & \text{için} \end{cases}, \quad (\text{EK2.17})$$

elde edilir ve sadece aşağıdaki terim kalır,

$$\lim_{\alpha \rightarrow \infty} H_\alpha(X) = -\frac{1}{\left(\frac{p_{\max}}{p_{\max}}\right)} \left(\frac{p_{\max}}{p_{\max}}\right) \ln p_{\max} = -\ln p_{\max}. \quad (\text{EK2.18})$$

EK 3

İKİ OLASILIĞIN ÇARPIMININ EN BÜYÜK DEĞERİ

(3.4) bağıntısı, Deutsch bağıntısında önemli bir yere sahip olup, doğruluğu gösterilmelidir (Friedland v.d 2013 - Appendix A - Lemma 1).

Bir saf yoğunluk işlemcisi $\rho = |\psi\rangle\langle\psi|$ ve $X = |x\rangle\langle x|$, $Z = |z\rangle\langle z|$ birer rank-1 izdüşüm işlemcisi olsun. X ve Z , ρ 'ya uygulanacak olursa olasılıkların çarpımından,

$$\langle x|\rho|x\rangle\langle z|\rho|z\rangle = \left(\sqrt{\langle x|\rho|x\rangle\langle z|\rho|z\rangle}\right)^2 \leq \frac{1}{4}\text{Tr}[\rho(|x\rangle\langle x| + |z\rangle\langle z|)]^2 \quad (\text{EK3.1})$$

$$\leq \frac{1}{4}\| |x\rangle\langle x| + |z\rangle\langle z| \|^2_\infty. \quad (\text{EK3.2})$$

bulunur. Burada, birinci eşitsizlik geometrik-aritmetik ortalama eşitsizliğinden ($\sqrt{ab} \leq (a+b)/2$), ikincisi ise normun tanımından gelmektedir (Bknz. (3.36)). Şimdi maksimum elde edebilmek için, ρ 'nın tanımlı olduğu Hilbert uzayını geren $\{|y\rangle, |z\rangle\}$ ortonormal baz kümesi düşünölsün ve $|x\rangle$ de bu bazlar tarafından gerilmiş uzayda yer alsın. $|\psi\rangle$ bu bazların bir süperpozisyonu olarak ifade edilebilir:

$$|\psi\rangle = e^{i\phi}r|z\rangle + e^{i\theta}\sqrt{1-r^2}|y\rangle. \quad (\text{EK3.3})$$

Burada $0 \leq r \leq 1$, θ ve ϕ gerçel sayılardır. Toplamın ikinci kısmında $\sqrt{1-r^2}$ değeri, normalizasyon koşulundan bu şekilde seçilmiştir. Eğer $e^{i\phi}\langle x|z\rangle = |\langle x|z\rangle| = c$ ve $e^{i\theta}\langle x|y\rangle = |\langle x|y\rangle| = \sqrt{1-c^2}$ olacak şekilde θ ve ϕ seçilirse,

$$\langle x|\rho|x\rangle\langle z|\rho|z\rangle = |\langle\psi|x\rangle|^2|\langle\psi|z\rangle|^2 = r^2(rc + \sqrt{1-r^2}\sqrt{1-c^2}), \quad (\text{EK3.4})$$

elde edilir. (EK3.4)'ü r üzerinden optimize edebilmek için, $r = \cos\alpha$ ve $c = \cos\beta$ tanımları yapılsın ($0 \leq \alpha, \beta \leq \pi/2$). Yerine konulacak olunursa,

$$\begin{aligned} \langle x|\rho|x\rangle\langle z|\rho|z\rangle &= \cos^2\alpha(\cos\alpha\cos\beta + \sin\alpha\sin\beta)^2 = \cos^2\alpha\cos^2(\alpha - \beta) \\ &= \frac{1}{4}[\cos(2\alpha - \beta) + \cos\beta]^2, \end{aligned} \quad (\text{EK3.5})$$

$\alpha = \beta/2$ seçimi yapılrsa, (3.4) ispatlanmış olur,

$$\langle x|\rho|x\rangle\langle z|\rho|z\rangle = \frac{1}{4}(1+c)^2. \quad (\text{EK3.6})$$

EK 4

RİEZS-THORİN İÇ-UZANIM (İNTERPOLASYON) TEOREMİ VE MU SINIRININ İSPATI

Riesz-Thorin iç-uzanım teoremi kısaca şöyle ifade edilebilir¹. $T = (t_{ij})$, $1 \leq i \leq m$ ve $1 \leq j \leq n$ olmak üzere $m \times n$ boyutunda bir matris olsun.

Burada $\mathbf{x} = (x_1, \dots, x_n)$ olmak üzere, $T : \mathbb{C}^n \rightarrow \mathbb{C}^m$ olacak şekilde bir çizgisel gönderimdir,

$$(T\mathbf{x})_i = \sum_{j=1}^n t_{ij}x_j, \quad (\text{EK4.1})$$

Böyle bir çizgisel gönderimin (p, q) normu (Bknz. (3.36)),

$$\|T\|_{p,q} = \max_{x: \|x\|_p=1} \|T\|_q, \quad \left(\frac{1}{p} + \frac{1}{q} = 1 \right) \quad (\text{EK4.2})$$

olarak tanımlanır. Sonra, $p_0, q_0, p_1, q_1 \in [1, \infty]$,

$$\frac{1}{p_0} + \frac{1}{q_0} = \frac{1}{p_1} + \frac{1}{q_1} = 1 \quad (\text{EK4.3})$$

ve $M_0, M_1 \in (0, \infty)$ için,

$$\|T\|_{p_0, q_0} \leq M_0 \text{ ve } \|T\|_{p_1, q_1} \leq M_1, \quad (\text{EK4.4})$$

olmak üzere her $0 < t < 1$ için p_t ve q_t ,

$$\frac{1}{p_t} = \frac{t}{p_1} + \frac{1-t}{p_0} \text{ ve } \frac{1}{q_t} = \frac{t}{q_1} + \frac{1-t}{q_0} \quad (\text{EK4.5})$$

olarak tanımlanırsa $1/p_0 + 1/q_0 = 1$ sağlanır. Daha sonra

$$\|T\|_{p_t, q_t} \leq M_t, \quad \text{burada } M_t = M_0^{1-t} M_1^t \quad (\text{EK4.6})$$

olur. Bu form, Riesz-Thorin iç-uzanım teoreminin oldukça sadeleştirilmiş bir halidir ve MU sınırını bulmakta yardımcı olacak şekilde ele alınmıştır.

Teorem 4 .1 $A = (A_1, \dots, A_m)$ ve $B = (B_1, \dots, B_n)$ iki izdüşüm işlemcileri kümesi ve $\rho = |\psi\rangle\langle\psi|$ bir saf durum olmak üzere

$$H_{|\psi\rangle}(A) + H_{|\psi\rangle}(B) \geq \log \frac{1}{c} = q_{MU} \quad (\text{EK4.7})$$

ifadesi doğrudur. Burada $c = \max_{i,j} |\langle a_i | b_j \rangle|^2$ olarak tanımlanır.

¹Bu kısımdaki ispatlar, Krishna, M., ve K. R. Parthasarathy. "An Entropic Uncertainty Principle for Quantum Measurements." makalesinden alınmıştır

İspat. (EK4.7) şu şekilde ifade edilebilir,

$$H(A) + H(B) \geq -2 \log \max_{i,j} \frac{|\langle \psi | A_i B_j | \psi \rangle|}{\|A_i \psi\| \|B_j \psi\|} \quad (\text{EK4.8})$$

$A_i |\psi\rangle \neq 0$ ve $B_j |\psi\rangle \neq 0$; $1 \leq i \leq m$ ve $1 \leq j \leq n$ olmak üzere, şu tanımlar yapılabilir,

$$|\phi_i\rangle = \frac{A_i |\psi\rangle}{\|A_i \psi\|} \text{ ve } |\psi_j\rangle = \frac{B_j |\psi\rangle}{\|B_j \psi\|}. \quad (\text{EK4.9})$$

Bu durumlar ölçüm sonrası durumlar olup, $\{|\phi_i\rangle\}$ ve $\{|\psi_j\rangle\}$ kümeleri ortonormal kümelerdir. $t_{ij} = \langle \phi_i | \psi_j \rangle$ kabülü altında, herhangi bir $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{C}^n$ için,

$$\sum_{i=1}^m \left| \sum_{j=1}^n t_{ij} x_j \right|^2 = \sum_{i=1}^m \left| \langle \phi_i | \sum_{j=1}^n x_j |\psi_j\rangle \right|^2 \quad (\text{EK4.10})$$

ve $\sum_{j=1}^n x_j |\psi_j\rangle = |\eta\rangle$ denilirse,

$$\begin{aligned} \sum_{i=1}^m \left| \langle \phi_i | \sum_{j=1}^n x_j |\psi_j\rangle \right|^2 &= \sum_{i=1}^m \left| \langle \phi_i | \eta \rangle \right|^2 \\ &= \sum_{i=1}^m \langle \eta | \phi_i \rangle \langle \phi_i | \eta \rangle \\ &= \langle \eta | \left(\sum_{i=1}^m |\phi_i\rangle \langle \phi_i| \right) | \eta \rangle \\ &\leq \langle \eta | \eta \rangle \\ &= \left\| \sum_{j=1}^n x_j |\psi_j\rangle \right\|^2 = \sum_{j=1}^n |x_j|^2 \end{aligned} \quad (\text{EK4.11})$$

olur ki , $T_{2,2} \leq 1$ eşitsizliği sağlanmış olur. Sonra,

$$\max_i \left| \sum_{j=1}^n t_{ij} x_j \right| = \max_i \sum_{j=1}^n |t_{ij}| |x_j| \leq \max_{i,j} |t_{ij}| \sum_{j=1}^n |x_j|, \quad (\text{EK4.12})$$

eşitsizliği ele alınır ve bu ifade $p = 1$ ve $q = \infty$ değerleri için düşünülürse

$\|T\|_{1,\infty} \leq \max_{i,j} |t_{ij}| = R$ olur. Şimdi $p_0 = q_0 = 2$, $p_1 = 1$, $q_1 = \infty$, $M_0 = 1$ ve $M_1 = \max_{i,j} |t_{ij}|$ değerleri (EK4.8) için uygulanırsa

$$\|T\|_{p_t, q_t} \leq R^t, \quad 0 < t < 1 \text{ için.} \quad (\text{EK4.13})$$

olur ve p_t ve q_t için (EK4.5) üzerinde açık hesaplamalar yapılsa $p_t = 2/(1+t)$ ve $q_t = 2/(1-t)$ olduğu rahatça görülebilir.

Şimdi, $\mathbf{a} = (a_1, \dots, a_n)$ ve $\mathbf{b} = (b_1, \dots, b_m)$ kompleks vektörleri şu şekilde tanımlansın.

$$a_j = \langle \psi_j | \psi \rangle, j = 1, \dots, m \quad \text{ve} \quad b_i = \langle \phi_i | \psi \rangle, i = 1, \dots, n \quad (\text{EK4.14})$$

Bu vektörler olasılık genlikleri olarak düşünülebilir ve aşağıda belirtileceği gibi kareleri gerçel sayılardır (olasılıklar). T gönderimi a_j 'yi b_i 'ye götürür,

$$\begin{aligned} (T\mathbf{a})_i &= \sum_{j=1}^n t_{ij} a_j = \sum_{j=1}^n \langle \phi_i | \psi_j \rangle \langle \psi_j | \psi \rangle \\ &= \sum_{j=1}^n \frac{\langle \phi_i | A_j \psi \rangle \langle A_j \psi | \psi \rangle}{\|A_j \psi\|^2} \\ &= \sum_{j=1}^n \langle \phi_i | A_j \psi \rangle = \langle \phi_i | \sum_{j=1}^n A_j | \psi \rangle = \langle \phi_i | \psi \rangle = b_i. \end{aligned} \quad (\text{EK4.15})$$

Şimdi (EK.4.11) ve (EK4.12)'ye tekrar dönerek elde edilen sonuçları bu ifadeler içinde yerine konulursa,

$$\left(\sum_{i=1}^m |\langle \phi_i | \psi \rangle|^{\frac{2}{1-t}} \right)^{\frac{1-t}{2}} \leq R^t \left(\sum_{j=1}^n |\langle \psi_j | \psi \rangle|^{\frac{2}{1+t}} \right)^{\frac{1+t}{2}} \quad (\text{EK4.16})$$

$0 < t < 1$ için Riesz-Thorin teoreminin uygulanmış halidir. $p_i = |\langle \phi_i | \psi \rangle|^2$ ve $q_j = |\langle \psi_j | \psi \rangle|^2$ olasılıkları cinsinden yazılır ve her iki tarafında kuvveti $2/t$ kadar alırttırılırsa;

$$\left(\sum_{i=1}^m p_i p_i^{\frac{t}{1-t}} \right)^{\frac{1-t}{t}} \left(\sum_{j=1}^n q_j q_j^{\frac{t}{1+t}} \right)^{-\frac{1+t}{t}} \leq R^2, \quad (\text{EK4.17})$$

olur. $t \rightarrow 0$ limitine bakılırsa $0/0$ belirsizliği çıkar ve L'Hospital kuralı uygulanırsa aşağıdaki ifade elde edilir.

$$\sum_{i=1}^m p_i \log p_i + \sum_{j=1}^n q_j \log q_j \leq 2 \log R \quad (\text{EK4.18})$$

olur. $R = \max_{i,j} t_{ij}$ olması gerektiği daha önce belirtilmişti. Böylece (EK4.18) ifadesinin MU bağıntısı olduğu açıktır. ■

EK 5

HAFIZALI DURUMDA ÜÇ PARÇALI SİSTEMLER İÇİN EBB

Bu kısımda kuantum hafızaya sahip üç parçalı sistemleri için EBB'nin bağıl entropi üzerinden ispatı incelenecektir. Bu ispatta başat olarak Coles v.d (2012) makalesinde yararlanılmıştır.

Bağıl entropi, S ve T birer pozitif operatör ve ρ bir yoğunluk işlemcisi olmak aşağıdaki özelliklere sahiptir:

- i)* Kuantum kanallar altında monotondur, $D(\mathcal{E}(S)\|\mathcal{E}(T)) \leq D(S\|T)$,
- ii)* Sıfır uzay eklemede, dik-direk toplamdan etkilenmez, $D(S\|T) = D(S \oplus 0\|T \oplus T')$,
- iii)* m bir pozitif sayı olmak üzere, $D(S\|mT) = D(S\|T) + \log \frac{1}{m}$ doğrudur,
- iv)* $D(\rho\|\rho) = 0$.

(*i*) özelliğinden (2.26)'da bahsedilmişti. (*ii*) özelliği $D(S\|T) = \text{Tr}[S(\log S - \log T)]$ tanımından, (*iii*) ve (*iv*) özellikleri ise bağıl entropinin tanımından gelmektedir.

Diğer bir özellik, izometrilere ($V^\dagger V = \mathbb{1}$) altında değişmezliktir;

$$D(S\|T) = D(VSV^\dagger\|VTV^\dagger). \quad (\text{EK5.1})$$

$T' \geq T$ olmak üzere aşağıdaki özellik de tanımdan rahatça anlaşılmaktadır;

$$D(S\|T) \geq D(S\|T'). \quad (\text{EK5.2})$$

Son olarak, ρ_{AB} ve $\mathbb{1}_A \otimes \rho_B$ arasındaki bağıl entropi,

$$\begin{aligned} D(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B) &= \text{Tr} [\rho_{AB}(\log \rho_{AB} - \log(\mathbb{1}_A \otimes \rho_B))] \\ &= \text{Tr}(\rho_{AB} \log \rho_{AB}) - \text{Tr}[\rho_{AB}(\mathbb{1}_A \otimes \log \rho_B)] \\ &= -S(\rho_{AB}) + S(\rho_B) = -S(A|B), \end{aligned} \quad (\text{EK5.3})$$

koşullu entropi, $S(A|B)$, cinsinden yazılabilir.

⋮

Üç parçalı bir ρ_{ABC} saf durumu için, $Tr_C(\rho_{ABC}) = \rho_{AB}$ ve $Tr_{AC}(\rho_{ABC}) = \rho_B$ yazılabilir. $X = \{X_j\}$ ve $Z = \{Z_k\}$, $X_j, Z_k \geq 0$ ve $\sum_j X_j = \mathbb{1} = \sum_k Z_k$ olmak üzere, birer POVM olsun ve aşağıdaki izometrilere¹ tanımlansın;

$$V_X = \sum_j |j\rangle_X \otimes |j\rangle_{X'} \otimes \sqrt{X_j} \quad (\text{EK5.4})$$

$$V_Z = \sum_k |k\rangle_Z \otimes |k\rangle_{Z'} \otimes \sqrt{Z_k}. \quad (\text{EK5.5})$$

Burada $V_X : \mathcal{H}_A \mapsto \mathcal{H}_X \otimes \mathcal{H}_{X'} \otimes \mathcal{H}_A$ ve $V_Z : \mathcal{H}_A \mapsto \mathcal{H}_Z \otimes \mathcal{H}_{Z'} \otimes \mathcal{H}_A$ şeklinde izometrilere ve $\{|j\rangle\}$, $\mathcal{H}_X \cong \mathcal{H}_{X'}$ için ve $\{|k\rangle\}$, $\mathcal{H}_Z \cong \mathcal{H}_{Z'}$ için ortonormal bazlardır. İzometrilere

$M = V_Z V_Z^\dagger$ izdüşüm işlemcisi için $\mathcal{E} : \rho \mapsto M\rho M^\dagger \oplus (\mathbb{1} - M)\rho(\mathbb{1} - M)^\dagger$ bir kuantum kanal göz önüne alınsın. Başta seçilen saf ρ_{ABC} için, $\bar{\rho}_{ZZ'AB} = V_Z \rho_{ABC} V_Z^\dagger$ durumu da saftır ve Schmidt ayrışımından;

$$S(Z|C) = -S(Z|Z'AB), \quad (\text{EK5.6})$$

yazılabilir. Böylece (EK5.3)'ten yararlanarak,

$$\begin{aligned} -S(Z|Z'AB) &= D(\bar{\rho}_{ZZ'AB} \| \mathbb{1}_Z \otimes \rho_{Z'AB}) \\ &\geq D\left(\bar{\rho}_{ZZ'AB} \| V_Z V_Z^\dagger (\mathbb{1}_Z \otimes \rho_{Z'AB}) V_Z V_Z^\dagger\right) \\ &= D\left(\rho_{AB} \| V_Z^\dagger (\mathbb{1}_Z \otimes \rho_{Z'AB}) V_Z\right) \\ &= D\left(\tilde{\rho}_{XX'AB} \| V_X V_Z^\dagger (\mathbb{1}_Z \otimes \rho_{Z'AB}) V_Z V_X^\dagger\right), \end{aligned} \quad (\text{EK5.7})$$

yazılabilir. Burada ikinci satır (i) özelliğinden, ikinci ve üçüncü satırlar ise (EK5.1)'den gelmektedir. Son satırda sağ taraftaki $V_Z^\dagger (\mathbb{1}_Z \otimes \rho_{Z'AB}) V_Z$ ifadesi

¹Bir izometri $V \in B(\mathcal{H})$ olmak üzere, $V^\dagger V = \mathbb{1}$, $\langle V\psi | V\phi \rangle = \langle \psi | \phi \rangle$, $\|V\rho\| = \|\rho\|$ koşullarını sağlayan çizgisel gönderimleridir.

açıkça hesaplanırsa,

$$\begin{aligned}
& V_Z^\dagger (\mathbb{1}_Z \otimes \rho_{Z'AB}) V_Z \\
&= \sum_k \left(\langle k|_Z \otimes \langle k|_{Z'} \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right) (\mathbb{1}_Z \otimes \rho_{Z'AB}) \left(\sum_l |l\rangle_Z \otimes |l\rangle_{Z'} \otimes \sqrt{Z_l} \otimes \mathbb{1}_B \right) \\
&= \left(\sum_k \langle k|_{Z'} \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right) \rho_{Z'AB} \left(\sum_l |l\rangle_{Z'} \otimes \sqrt{Z_l} \otimes \mathbb{1}_B \right) \delta_{kl} \\
&= \sum_k \left(\langle k|_{Z'} \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right) \rho_{Z'AB} \left(|k\rangle_{Z'} \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right),
\end{aligned}$$

olur. (EK5.7)'nin sağ tarafı V_X izometrisinin (EK5.4)'teki tanımı kullanılarak incelenmeye devam edilirse şunlara ulaşılır,

$$\begin{aligned}
& D \left(\tilde{\rho}_{XX'AB} \parallel \sum_k V_X \left(\langle k|_{Z'} \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right) \rho_{Z'AB} \left(|k\rangle \otimes \sqrt{Z_k} \otimes \mathbb{1}_B \right) V_X^\dagger \right) \\
&\geq D \left(\tilde{\rho}_{XB} \parallel \sum_{j,k} |j\rangle\langle j|_X \otimes Tr_{Z'A} \left((|k\rangle\langle k|_{Z'} \otimes \sqrt{Z_k} X_j \sqrt{Z_k} \otimes \mathbb{1}_B) \rho_{Z'AB} \right) \right) \\
&\geq D(\tilde{\rho}_{XB} \parallel c(X, Z) \mathbb{1}_X \otimes Tr_{Z'A}(\rho_{Z'AB})) \\
&= \log \frac{1}{c(X, Z)} + D(\tilde{\rho}_{XB} \parallel \mathbb{1}_X \otimes \rho_B). \tag{EK5.8}
\end{aligned}$$

Burada üçüncü satırda, $c(X, Z) = \max_{j,k} \|\sqrt{X_j} \sqrt{Z_k}\|_\infty^2$ olmak üzere $\sqrt{Z_k} X_j \sqrt{Z_k} = c(X, Z) \mathbb{1}_A$, $\sum_j |j\rangle\langle j|_X = \mathbb{1}_X$ ve $\sum_k |k\rangle\langle k|_{Z'} = \mathbb{1}_{Z'}$ bağıntıları kullanılmıştır. Sonuç olarak (EK5.8) , (EK5.7)'da yerine konulursa,

$$D(\bar{\rho}_{ZZ'AB} \parallel \mathbb{1}_Z \otimes \rho_{Z'AB}) \geq \log \frac{1}{c(X, Z)} + D(\tilde{\rho}_{XB} \parallel \mathbb{1}_X \otimes \rho_B). \tag{EK5.9}$$

elde edilir. (EK5.3) bağıntısı kullanılarak bu ifade koşullu entropiler cinsinden;

$$-S(Z|Z'AB) \geq \log \frac{1}{c(X, Z)} - S(X|B) \tag{EK5.10}$$

halini alır ve (EK5.6)'dan yararlanılarak;

$$S(X|B) + S(Z|C) \geq \log \frac{1}{c(X, Z)}. \tag{EK5.11}$$

elde edilir ve ispat tamamlanmış olur.

EK 6

COLES - PİANİ SINIRI

Bölüm(3.5)'te , $d > 2$ için q_{CP} sınırı ile ilgili bilgi verilmişti. Şimdi (4.27)'den bu sınırın nasıl elde edilebileceği incelenebilir.

ρ_{AB} , AB sisteminin kuantum durumu olsun ve ortonormal bazlara sahip $\mathcal{X}(\cdot) = \sum_j |x_j\rangle \langle x_j| (\cdot) |x_j\rangle \langle x_j|$ ve $\mathcal{Z}(\cdot) = \sum_k |z_k\rangle \langle z_k| (\cdot) |z_k\rangle \langle z_k|$ birer kuantum kanal olacak şekilde A sistemine uygulansın;

$$\begin{aligned}\rho_{XB} &= \mathcal{X}(\rho_{AB}) = \sum_j |x_j\rangle \langle x_j| \rho_{AB} |x_j\rangle \langle x_j| = \sum_{jlm} |x_j\rangle \langle x_j| e_{lm} |x_j\rangle \langle x_j| \otimes T_{lm} \\ \rho_{ZB} &= \mathcal{Z}(\rho_{AB}) = \sum_k |z_k\rangle \langle z_k| \rho_{AB} |z_k\rangle \langle z_k| = \sum_{klm} |z_k\rangle \langle z_k| e_{lm} |z_k\rangle \langle z_k| \otimes T_{lm}\end{aligned}\tag{EK6.1}$$

En sağ taraftaki etkiler kısmi iç çarpımlarla sadece A üzerinedir. En sağdaki ifadeler yazılırken e_{lm} matris bazı cinsinden, $\rho_{AB} = \sum_{lm} e_{lm} \otimes T_{lm}$ blok yazımı yapılmıştır. Bu yazımdan $Tr e_{lm} = \delta_{lm}$ olduğundan $\rho_B = \sum_l T_{ll}$ bulunur. Aynı hesap (EK6.1)'in son satırından yapılırsa;

$$\begin{aligned}\rho_B &= Tr_A(\rho_{ZB}) = \sum_{klm} \langle z_k| e_{lm} |z_k\rangle T_{lm} \\ &= \sum_{lm} Tr(e_{lm}) T_{lm} = \sum_l T_{ll}\end{aligned}$$

aynı sonuç bulunur: Çünkü tam ölçüm A üzerinde yapılmaktadır, B 'nin durumu değişmez.

Şimdi, $H(Z|B)$ ve $S(A|B)$ koşullu entropiler göz önüne alınırsa,

$$\begin{aligned}H(Z|B) - S(A|B) &= H(\rho_{ZB}) - S(\rho_B) - S(\rho_{AB}) + S(\rho_B) \\ &= H(\rho_{ZB}) - S(\rho_{AB})\end{aligned}\tag{EK6.2}$$

A üzerindeki ölçümler B 'yi değiştirmez ve yukarıdaki sadeleşmeler gerçekleşir. Şimdi gösterileceği gibi yerel tam ölçümler yapıldıktan sonraki entropiler ile ölçümden önceki entropiler arasındaki fark bir bağıl entropi olarak yazılabilir.

$H(\rho_{ZB})$ yazılırsa;

$$\begin{aligned}
H(\rho_{ZB}) &= -Tr \left[\sum_{klm} |z_k\rangle \langle z_k| e_{lm} |z_k\rangle \langle z_k| \otimes T_{lm} \log \left(\sum_{klm} |z_k\rangle \langle z_k| e_{lm} |z_k\rangle \langle z_k| \otimes T_{lm} \right) \right] \\
&= -Tr(\rho_{AB} \log \rho_{ZB})
\end{aligned}$$

Bu bağıntı (EK6.2)'de yerine konulursa;

$$\begin{aligned}
H(\rho_{ZB}) - S(\rho_{AB}) &= -Tr(\rho_{AB} \log \rho_{ZB}) + Tr(\rho_{AB} \log \rho_{AB}) \\
&= D(\rho_{AB} || \rho_{ZB}).
\end{aligned} \tag{EK6.3}$$

elde edilir.

Kuantum bağıl entropi, kuantum kanallar altında monoton azalır (Bknz 2.26). Bu özellik göz önüne alınarak hem ρ_{AB} hem de ρ_{ZB} üzerine $\mathcal{X}$ yerel tam ölçüm kanalı uygulanırsa,

$$\begin{aligned}
D(\rho_{AB} || \rho_{ZB}) &\geq D(\mathcal{X}(\rho_{AB}) || \mathcal{X}(\rho_{ZB})) \\
&= D \left(\rho_{XB} || \sum_{jk} c_{jk} |x_j\rangle \langle x_j| \otimes Tr_A(|z_k\rangle \langle z_k| \rho_{AB}) \right)
\end{aligned}$$

ve $c_{jk} = |\langle x_j | z_k \rangle|^2$ olarak tanımlanmıştır. Bunun maksimum değeri alınırsa;

$$\begin{aligned}
D(\rho_{AB} || \rho_{ZB}) &\geq D(\rho_{XB} || \sum_j (\max_k c_{jk}) |x_j\rangle \langle x_j| \otimes \rho_B) \\
&= Tr(\rho_{XB} \log \rho_{XB}) - Tr \left(\rho_{XB} \log \sum_j (\max_k c_{jk}) |x_j\rangle \langle x_j| \otimes \rho_B \right) \\
&= -H(XB) - Tr \left[\rho_{XB} \left[\log \left(\sum_j (\max_k c_{jk}) |x_j\rangle \langle x_j| \right) \otimes \mathbb{1}_B \right] \right] \\
&\quad - Tr[\rho_{XB} (\mathbb{1}_X \otimes \log \rho_B)] \\
&= -H(X|B) - Tr_A \left(\rho_X \log \left(\sum_j \max_k c_{jk} |x_j\rangle \langle x_j| \right) \right) \\
&= -H(X|B) - \sum_j \langle x_j | \rho_X | x_j \rangle \log(\max_k c_{jk}) \\
&= -H(X|B) - q_{\rho_A, \mathcal{X}, \mathcal{Z}}.
\end{aligned} \tag{EK6.4}$$

elde edilir. Burada $q_{\rho_A, \mathcal{X}, \mathcal{Z}} = \sum_j \langle x_j | \rho_X | x_j \rangle \log(\max_k c_{jk})$ olarak tanımlanır. İlk satır, eğer $T' \geq T$ ise $D(S||T) \leq D(S||T')$ olmasından gelir. Simetriden $q_{\rho_A, \mathcal{Z}, \mathcal{X}}$ için de benzer bir çıkarım yapılabilir ve bu iki değerden en büyük olanı kullanılır. Böylece Denk.(EK6.2) ve (EK6.4) birleştirilirse,

$$H(X|B) + H(Z|B) \geq q' + S(A|B) \quad (\text{EK6.5})$$

elde edilir. Burada $q' = \max\{q_{\rho_A, \mathcal{X}, \mathcal{Z}}, q_{\rho_A, \mathcal{Z}, \mathcal{X}}\}$ olarak tanımlanır.

$\langle x_j | \rho_X | x_j \rangle = p_j^x$ ve $\langle z_k | \rho_Z | z_k \rangle = p_k^z$ yazılır ve q' incelenirse;

$$\begin{aligned} q' &= \max\left\{-\sum_j p_j^x \log(\max_k c_{jk}), -\sum_k p_k^z \log(\max_j c_{jk})\right\} \\ &\geq \frac{1}{2}\left[-\sum_j p_j^x \log(\max_k c_{jk}) - \sum_k p_k^z \log(\max_j c_{jk})\right] \\ &\geq \frac{1}{2}\left[-p_j^x \log c - (1 - p_j^x) \log c_2 - p_k^z \log c - (1 - p_k^z) \log c_2\right] \\ &= q + \frac{1}{2} \log\left(\frac{c}{c_2}\right) [2 - (p_j^x + p_k^z)]. \end{aligned} \quad (\text{EK6.6})$$

$\log(c/c_2) \geq 0$ kabulü altında, (EK6.6)'nın en büyük değerini en sağdaki olasılıkların toplamının en büyük değeri sağlar ;

$$\begin{aligned} \max_{\rho_A} (p_j^x + p_k^z) &= \max_{\rho_A} \text{Tr}[\rho_A(|x_j\rangle\langle x_j| + |z_k\rangle\langle z_k|)] \\ &= \| |x_j\rangle\langle x_j| + |z_k\rangle\langle z_k| \|_{\infty} \\ &= 1 + \max_{jk} |\langle x_j | z_k \rangle| \\ &= 1 + \sqrt{c}. \end{aligned}$$

Bu ifade, (EK6.6)'da yerine konulursa (3.33) ispat edilmiş olur.

Bilişim dışarlama prensibi için r_{CP} sınırı bulunmak istenirse, $H(X|B) = H(X) - I(X; Y)$ (veya benzeri $H(Z|B)$ için) yazılarak (EK6.5)'te yerine konulursa;

$$I(X; Y) + I(Z; Y) \leq \log d + H(X) + q_{\rho_A, \mathcal{X}, \mathcal{Z}} - S(A|B) \quad (\text{EK6.7})$$

yazılabilir. Üst sınır için bağıntının sağ tarafı ele alınırsa,

$$\begin{aligned}
H(X) + q_{\rho_A, \mathcal{X}, \mathcal{Z}} &= - \sum_j p_j^x \log p_j^x + \sum_j p_j^x \log \left(\max_k c_{jk} \right) \\
&= \sum_j \log \left(\max_k c_{jk} / p_j^x \right) \\
&\leq \log \left(d \sum_j \max_k c_{jk} \right). \tag{EK6.8}
\end{aligned}$$

elde edilir. Burada son satır log fonksiyonunun konkavlığından gelmektedir. Simetriden aynı ifade Z için de elde edilebilir. Böylece (4.50) ispatlanmış olur.



KARŞILIKLI YANSIZ BAZLAR

Karşılıklı yansız bazlar EBB’de önemli bir rol oynadığından, burada kısaca tanıtımı yararlı olacaktır¹.

Karşılıklı yansız bazlar: $B_1 = \{|b_1^1\rangle, \dots, |b_1^d\rangle\}, B_2 = \{|b_2^1\rangle, \dots, |b_2^d\rangle\} \in \mathbb{C}^d$ olacak şekilde iki ortonormal baz kümesi olsun. Eğer, $\forall k, l \in [d]$ için $|\langle b_k^1 | b_l^2 \rangle| = 1/\sqrt{d}$ ise, bu ortonormal kümeler karşılıklı yansız, bu bazların bir $\{B_1, \dots, B_m\}$ kümesine de, eğer her baz çifti karşılıklı yansız ise, karşılıklı yansız bazların bir kümesi denir. Burada d Hilbert uzayının boyutudur.

Örneğin hesaplamalı bazlar $\{|0\rangle, |1\rangle\}$ ve Hadamard bazları $\{|+\rangle, |-\rangle\}$ karşılıklı yansızdır.

d boyutta KYB’nin maksimum sayısı $N(d)$ ile temsil edilsin. Herhangi bir d boyutta $N(d) \leq d+1$ olacak şekildedir. Eğer $d = p^k$ bir asal kuvvet şeklindeyse, $N(d) = d+1$ olur ve bilinen yapılar açıktır. Eğer $d = s^2$ bir kare kuvvetse, $N(d) \geq KYLK(s)$ olur, burada $KYLK(s)$, karşılıklı yansız $s \times s$ Latin karelerini temsil etmektedir. Herhangi bir boyutta 3 KYB için açık bir yapı vardır. Ne yazık ki daha fazlası bilinmemektedir. Örneğin $d = 6$ boyutta (yani iki asal sayının çarpımı olan boyutlarda) 7 KYB’nin açık bir kümesi olup olmadığı açık bir problemdir.

Latin kareleri: İlk olarak, $s \in \mathbb{N}$ için, $d = s^2$ kare kuvvet boyutunda yapılandırılabilen Latin karelerine dayanadırılan KYB’ler ele alınsın. Bir $s \times s$ Latin karesi, $[s]$ kümesi sembolleri üzerinden $s \times s$ kare içinde $[s]$ kümesi elemanlarının bir düzenlemesidir. Burada her satır ve sütunda her eleman kesinlikle bir kez yer alır (Şekil 7.1). L_{ij} , i . satırda ve j . sütunda bulunan elemanı tanımlasın. İki Latin karesi L ve L' karşılıklı ortogonal denir ancak ve ancak $\{L_{ij}, L'_{ij} | i, j \in [s]\} = \{(u, v) | u, v \in [s]\}$ ise. Burada (u, v) terimi üst üste yerleştirilen karelerin oluşturduğu çiftleri temsil etmektedir. Sezgisel olarak bunun anlamı, eğer bir karenin üzerine diğer kare yerleştirilirse ve üst üste gelen durumlara bakılacak olunursa, bütün olası çiftler

¹Bu kısım Stephanie Wehner ve Andreas Winter’in “Entropic uncertainty relations—a survey” (2008) adlı çalışmasından alınmıştır.

gözlemlenir.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

Şekil 7 .1. 3×3 karşılıklı yansız Latin kareleri

$s \times s$ Latin karesinden $\mathbb{C}^s \times \mathbb{C}^s$ için bir baz elde edilebilir. İlk olarak Latin karelerinin girişlerinden baz vektörlerin s tanesi kurulsun,

$$|v_{1,l}\rangle = \frac{1}{\sqrt{s}} \sum_{i,j \in [s]} E_{i,j}^L(l) |i, j\rangle. \quad (\text{EK7.1})$$

Burada E^L bir doğrulamadır, örneğin $E_{i,j}^L(l) = 1$ olur ancak ve ancak $L_{i,j} = l$ ise. Dikkat edilirse her l için kesinlikle her i, j çiftinin s tanesine sahip olunur, mesela $E_{i,j}^L(l) = 1$, çünkü $[s]$ kümesinin her elemanı Latin karesi içinde kesinlikle s kere var olmaktadır. İkinci olarak $t \in [s]$ olmak üzere, böyle her vektörden $s \times s$ kompleks Hadamard matrisinin $H = (h_{ij})$ ardışık satırlarının katsayıları gibi eklenmesi ile kalan $|v_{t,j}\rangle$ için $s - 1$ tane ek vektör elde edilir, burada $i, j \in \{0, \dots, s - 1\}$ olmak üzere, $h_{ij} = \omega^{ij}$ ve $\omega = e^{2\pi i/s}$ olarak tanımlanmaktadır.

Örnek olarak, Şekil (3.1) ve aşağıda verilen 3×3 Hadamard matrisi düşünölsün,

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad (\text{EK7.2})$$

burada $\omega = e^{2\pi i/3}$ olarak tanımlanmaktadır. İlk olarak, Şekil.(7.1)'den aşağıdaki vektörler elde edilir,

$$|v_{1,1}\rangle = \frac{1}{\sqrt{3}}(|1, 1\rangle + |2, 3\rangle + |3, 2\rangle), \quad (\text{EK7.3})$$

$$|v_{1,2}\rangle = \frac{1}{\sqrt{3}}(|1, 2\rangle + |2, 1\rangle + |3, 3\rangle), \quad (\text{EK7.4})$$

$$|v_{1,3}\rangle = \frac{1}{\sqrt{3}}(|1,3\rangle + |2,2\rangle + |3,1\rangle). \quad (\text{EK7.5})$$

H matrisinin yardımı ile, bu vektörlerin bir tanesinde üç ek vektör elde edilebilir,

$$|v_{1,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + |2,3\rangle + |3,2\rangle), \quad (\text{EK7.6})$$

$$|v_{2,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + \omega |2,3\rangle + \omega |3,2\rangle), \quad (\text{EK7.7})$$

$$|v_{3,1}\rangle = \frac{1}{\sqrt{3}}(|1,1\rangle + \omega^2 |2,3\rangle + \omega |3,2\rangle). \quad (\text{EK7.8})$$

Bu, $s = 3$ için, $\mathcal{B} = \{|v_{t,l}\rangle | t, l \in [s]\}$ bazlarını verir. Diğer bir baz yapılandırması da karşılıklı ortogonal Latin karelerinden kesinlikle aynı yol izlenerek yapılandırılabilir. L ve L' iki Latin karesinin karşılıklı ortogonal olması gerçeği, bazların karşılıklı yansız olmasını garantiler. L' karesine ait olan başka bir $\mathcal{B} = \{|u_{t,l}\rangle | t, l \in [s]\}$ verildiği düşünölsün. Herhangi bir $l, l' \in [s]$ için, $|\langle u_{1,l} | v_{1,l'} \rangle|^2 = |(1/s) \sum_{i,j \in [s]} E_{i,j}^{L'}(l) E_{i,j}^L(l)|^2 = 1/s^2$ sahip olunur, tıpkı örneğin $E_{i,j}^{L'}(l) E_{i,j}^L(l) = 1$ olacak şekilde bir çift $l', l \in [s]$ varolması gibi. Açık bir biçimde, benzer argüman kompleks Hadamard matrisinden türetilen ek vektörler için de korunur.

Genelleştirilmiş Pauli bazları: İkinci yapı olarak, hesaplamasal bazların bir $C = \{|0\rangle, \dots, |d-1\rangle\}$ kümesine etki etmesi aşğıdaki gibi tanımlananan genelleştirilmiş Pauli X_d ve Z_d matrislerine dayanan bir yapı ele alınabilir,

$$\begin{aligned} X_d |k\rangle &= |k+1 \pmod{d}\rangle \\ Z_d |k\rangle &= \omega^k |k\rangle, \quad \forall |k\rangle \in C, \end{aligned} \quad (\text{EK7.9})$$

burada $\omega = e^{2\pi i/d}$ olarak tanımlanmaktadır. $k \in [N]$ ve $a_k, b_k \in \{0, \dots, d-1\}$ için, $(X_d)^{a_1} (Z_d)^{b_1} \otimes \dots \otimes (X_d)^{a_N} (Z_d)^{b_N}$ ifadesine Pauli matrislerinin bir dizisi denir. Dikkat edilirse, $d = 2$ için bilinen Pauli matrisleri olurlar. Eğer d asal ise, $(d+1)$ KYB yapılandırılabilir. Ayrıca $Z_d, X_d, X_d Z_d^2, \dots, X_d Z_d^{d-1}$ matrislerinin özvektörlerinden elde edilebilir (Bandyopadhyay v.d. 2002). Eğer $d = p^k$ bir asal kuvvet ise, birimi içeren, $C_1, \dots, C_{d+1}$ kümesi içerisinde grup olan örneğin $|C_i| = d-1$, $i \neq j$ için $C_i \cap C_j = \emptyset$ olan ve C_i ile komüte eden bütün $d^2 - 1$ olası Pauli matrislerinin dizisi düşünölsün. B_i ise C_i 'nin bütün elemanlarının ortak özbazı olsun. Sonra $B_1, \dots, B_{d+1}$

KYB olur. $d = 2^k$ için benzer bir sonuç ayrıca gösterilmiştir. Bu yapının özel bir durumu, $d = 2^k$ boyutta, hesaplamasal bazlara uygulanan üniter $\mathbb{1}^{\otimes k}$, $K^{\otimes k}$ ve $H^{\otimes k}$ ile verilen üç KYB'dir, burada H Hadamard dönüşümü, $K = (1 + i\sigma_x)/\sqrt{2}$ olarak tanımlanmaktadır. Bu yapının basit bir örneği X , Y ve Z Pauli matrislerinin bazıları tarafından verilen, $d = 2$ boyutunda karşılıklı yansız bazlardır. Bu tarz KYB'ler için ilginç bir bakış açısı, $B_1, \dots, B_{d+1}$ ve bütün bazlara $UB_j = B_{j+1}$ şeklinde çevrimsel olarak etki eden üniter bir U dönüşümünün varolmasıdır., burada $UB_{d+1} = B_1$ olarak tanımlanmaktadır.

