**ANKARA ÜNİVERSİTESİ**
**FEN BİLİMLERİ ENSTİTÜSÜ**

**YÜKSEK LİSANS TEZİ**

# KUANTUM ENTROPİLERİ VE MARKOV DURUMLARI

**Özgür KALE**

**FİZİK ANABİLİM DALI**

**ANKARA**
**2021**

**Her hakkı saklıdır**

# ÖZET

Yüksek Lisans Tezi

KUANTUM ENTROPİLERİ VE MARKOV DURUMLARI

Özgür KALE

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Fizik Anabilim Dalı

Danışman: Prof. Dr. Abdullah VERÇİN

Üç parçalı bileşik sistemlerin entropileri ile ilgili bir eşitsizlik olan güçlü alt-toplanabilirlik (GaT) bağıntısı, pek çok entropik bağıntıyı da genellediğinden temel fizik alanında geniş uygulama alanlarına sahiptir. Öte yandan, bu bağıntıyı eşitlik haliyle sağlayan Markov durumları klasik ve kuantum bilişim kuramlarının en çarpıcı olgularından birisidir. Bilişim kuramlarının temelini oluşturan matematiksel ve fiziksel kavramların birleştirilmesi ve derlenmesi amacıyla yazılan bu tezin ilk aşamasında, klasik ve kuantum entropileri derinlemesine incelenmiştir. Ardından GaT bağıntısı farklı bakışları göz önünde bulundurularak dört ayrı yoldan ispatlanmış, bu bağıntının özel bir hali olan Markov durumları detaylıca araştırılmıştır. Son aşamada ise GaT bağıntısının kuantum bilişim kuramındaki uygulamaları ele alınmıştır.

**Şubat 2021, 75 Sayfa**

**Anahtar Kelimeler:** Klasik Entropi, Kuantum Entropi, Koşullu Entropi, Bileşik Entropi, Karşılıklı Bilişim, Bağıl Entropi, Güçlü Alt-Toplanabilirlik (GaT), Markov Durumları, İz Bağıntısı, Ayrışım.

## ABSTRACT

Master Thesis

QUANTUM ENTROPIES AND MARKOV STATES

Özgür KALE

Ankara University
Graduate School of Natural and Applied Sciences
Physics Department

Supervisor: Prof. Dr. Abdullah VERÇİN

The strong subadditivity (SSa) relation, which is an inequality related to the entropy of composite systems that include three parts, has wide application areas in the field of fundamental physics as it also generalizes many entropic relations. On the other hand, Markov states that satisfy this equation as an equality are one of the most striking phenomena of classical and quantum information theories. In the first stage of this study written to combine and compile the mathematical and physical concepts that form the basis of information theories, classical and quantum entropies were examined in depth. Afterward, the SSa relation has been proved in four particular ways by taking into account different points of wiev and the Markov case, which is a special form of this relation, has been investigated in detail. In the last part, the applications of SSa relation in quantum are considered.



**February 2021, 75 Pages**

**Key Words:** Classical Entropy, Quantum Entropy, Conditional Entropy, Joint Entropy, Mutual Information, Relative Entropy, Strong Subadditivity (SSa), Markov States, Trace, Decomposition.

## ÖNSÖZ ve TEŞEKKÜR

Çalışmalarım süresince büyük ilgi ve yardımlarını görmüş olduğum tez hocam Sayın Prof. Dr. Abdullah Verçin'e (Ankara Üniversitesi) en içten duygularımla teşekkür eder, kendisi ile çalışmış olmanın verdiği haklı gururu bana yaşattığını belirtmek isterim. Bu sürece başlamamdaki en önemli kişi olan hocam Sayın Prof. Dr. Ali Ulvi Yılmazer'e (Ankara Üniversitesi); her sorunumu kendi sorunu belleyen en yakın dostum Dr. Hasan Özgür Çıldıroğlu'na; dersini dinlemiş olmaktan gurur duyduğum, örnek aldığım insanlardan biri olan Sayın Prof. Dr. Namık Kemal Pak'a (Orta Doğu Teknik Üniversitesi) şükranlarımı sunarım.

Beni her daim destekleyen, paylaştıkça çoğalan niceliğin sevgi olduğunu ve beni bu doğrultuda yetiştiren sevgili annem ve babam Nezaket ve Abdullah Kale'ye; çalışma arkadaşlarıma, bugüne kadar derslerini dinlemekten onur duyduğum saygıdeğer hocalarıma teşekkür ederim.

Özgür KALE

Ankara, Şubat 2021

# İÇİNDEKİLER

**TEZ ONAYI**
**ETİK** ..... **i**
**ÖZET** ..... **ii**
**ABSTRACT** ..... **iii**
**ÖNSÖZ ve TEŞEKKÜR** ..... **iv**
**ŞEKİLLER DİZİNİ** ..... **ivi**
**1. GİRİŞ** ..... **1**
**2. SHANONN VE VON NEUMANN ENTROPİLERİ** ..... **3**
**2.1 Klasik Bilişim Kuramında Entropi** ..... **3**
**2.1.1 Bileşik ve koşullu entropi** ..... **5**
**2.1.2 Klasik güçlü alt-toplanabilirlik (GaT) bağıntısı** ..... **8**
**2.1.3 Konvekslik ve konkavlık** ..... **9**
**2.2 Kuantum Bilişimde Entropi** ..... **12**
**3. GÜÇLÜ ALT-TOPLANABİLİRLİK BAĞINTISI** ..... **21**
**3.1 E.H.Lieb ve M.B. Ruskai İspatı** ..... **21**
**3.2 Nielsen-Petz İspatı** ..... **26**
**3.3 Hayden-Jozsa-Petz-Winter İspatı** ..... **31**
**3.4 Petz İspatı** ..... **33**
**4. MARKOV DURUMLARI** ..... **35**
**5. UYGULAMALAR** ..... **42**
**5.1 Holevo Niceliği** ..... **42**
**5.2 Üç Derin Gerçek** ..... **44**
**6. TARTIŞMA VE SONUÇ** ..... **46**
**KAYNAKÇA** ..... **47**
**EKLER** ..... **50**
**EK 1 İz ve Parçalı İz bağıntısı** ..... **50**
**EK 2 Öze Uygunluk** ..... **55**
**EK 3 Ayrışım Çeşitleri** ..... **66**
**EK 4 UYGULAMALAR** ..... **70**
**ÖZGEÇMİŞ** ..... **75**

# SİMGELER DİZİNİ

## Simgeler

| | |
|---|---|
| X, Y, Z | Klasik Rasgele Değişkenler |
| H(X) | Shannon Entropi |
| H(XY) | Bileşik Entropi |
| H(X\|Y) | Klasik Koşullu Entropi |
| D(p \|\|q) | Klasik Bağıl Entropi |
| I(X:Y) | Klasik Karşılıklı Bilişim |
| ρ, σ | Yoğunluk İşlemcileri |
| S(ρ) | von Neumann Entropi |
| $M_{nk}$ | İkili-Stokastik Matris |
| Tr | İz Bağıntısı |
| D(ρ,σ) | İz Uzaklığı |
| F(ρ,σ) | Öze-uygunluk |

| | |
|---|---|
| $\rho = \sum_k \lambda_k \left\|k\right\rangle \left\langle k\right\|$ | Bir yoğunluk matrisinin (işlemcisinin) spektral ayrışımı |
| $\left\|\Psi^{RQ}\right\rangle = \sum_k \sqrt{\lambda_k} \left\|k^R, k^Q\right\rangle$ | İki parçalı bir $\left\|\Psi^{RQ}\right\rangle$ saf durumunun Hilbert-Schmidt ayrışımı |

## Kısaltmalar

| | |
|---|---|
| GaT | Güçlü Alt-Toplanabilirlik Bağıntısı |

# 1. GİRİŞ

Klasik bilginin aktarılması ve işlenmesi açısından matematiksel bir iletişim modeli olarak düşünülebilecek klasik bilişim kuramı (CIT), Claude Shannon tarafından (Shannon 1948) sinyal iletiminin ve haberleşme işleminin kapasitesinin belirlenmesi amacıyla ortaya konulmuştur. Bu bağlamda, klasik bilişim kuramını temellendiren modelin ilk bileşeni, iletilecek mesajı oluşturan mesaj kaynağıdır. Mesajın gerçek sinyallere bağlanması amacıyla ortaya konulan kodlayıcı, mesajın taşındığı ortam olan kanallar, sinyalin iletimini engelleyen gürültü, sinyali aldığı şekliyle alıcının anlayabileceği şekle dönüştüren kod çözücü ve mesaj alıcısı modelin diğer bileşenleridir. Bununla birlikte, model soyut olarak geliştirildiğinden pek çok durumda geçerlidir ve optikten fizyolojiye kadar geniş uygulama alanlarına sahiptir.

Klasik ve kuantum bilginin kuantum iletişim kanalları üzerinden iletilmesini temel alan kuantum bilişim kuramı (QIT), fiziğin ve doğanın temel özelliklerinin daha derin bir şekilde anlaşılabilmesi açısından yeni bir araçtır. Kuantum bilişim kuramı kapsamında, sistemlerin taşıyabilecekleri en uygun bilgilerin kodlanması, işlenmesi (Horodecki vd. 1996), iletilmesi, algılanması ve depolanması gibi temel problemler ele alınmaktadır.

Bilişim kuramlarının en önemli araştırma alanlarından birisi de sistemin düzensizliği ve belirsizliği ile ilişkilendirilebilen, ölçülebilir fiziksel bir nicelik olan entropidir. İlk olarak Clausius tarafından 19. yüzyılın sonlarında ortaya atılan entropi, Max Planck'ın (Planck 1900) önemli çalışması ile detaylandırılmış, John von Neumann'ın (von Neumann 1932) yaptığı matematiksel analizlerle de bugünkü tanımına kısmen ulaşmıştır.

Günümüz fiziğinde pek çok alanda kullanılan entropi, klasik bilişim kuramında rasgele bir değişkenin değerine veya rasgele bir sürecin sonucuna dahil olan belirsizlik miktarını tanımlamaktadır. Bu kapsamda, temel bir ölçüm niceliği olarak, düzensizliğin, bilgisizliğin ya da belirsizliğin bilgisi olarak da düşünülebilir. Klasik ve kuantum bilişim kuramları, durumlara farklı açılardan yaklaşırlar. Klasik bilişim kuramında, en basit şekliyle, n harften oluşan bir mesajda her harf bir topluluktan bağımsız biçimde seçilerek incelenir. Bu durumda topluluğun bilgi miktarı Shannon entropisine eşit olacaktır (Shannon 1948). Kuantum bilişim kuramında ise n harften oluşan bir mesaj, üst üste gelme ilkesinden hareketle, kuantum durumları topluluğundan alınır ve incelenir. Genel olarak yoğunluk işlemcileri ile betimlenen kuantum durumlarına hem klasik bilgiler hem de kuantum bilgiler kodlanabileceğinden, mesajlar yoğunluk işlemcileri üzerine yüklenirler. Bunun yanı sıra, bilgi taşıyıcı sistemin içinde bulunduğu kuantum durumu ile taşıdığı bilgi-bilişim içeriği

kuantum von Neumann entropisi ile nicelendirilir ve nitelendirilir (von Neumann 1932). Veri işleme, veri sıkıştırma ve hata düzeltme gibi bilişim yöntem ve süreçleri yanında, çok parçalı sistemlerin bileşenleri ve içinde bulundukları çevreyle kuantum ve klasik korelasyonların nicelendirilmesinde ve nitelendirilmesinde de von Neumann entropisinin temel alındığı, bağıl entropi, koşullu entropi ve karşılıklı bilişim gibi nicelikler kullanılır. Bu farklılıklar, Kuantum bilişim kuramını klasik bilişim kuramına göre daha güvenilir kılmaktadır.

Klasik ve kuantum entropiler için sağlanan güçlü alt-toplanabilirlik (GaT) bağıntısı, üç parçalı bileşik sistemlerin entropileri ile ilişkili bir eşitsizliktir (Robinson ve Ruelle 1966, Lanford III ve Robinson 1968, Lieb ve Ruskai 1973). GaT bağıntısı pek çok entropik bağıntıyı da genellediğinden, özellikle günümüzde yoğun bir araştırma alanı olan kuantum bilişim kuramı için büyük bir öneme sahiptir. Öte yandan, bu bağıntıyı eşitlik haliyle sağlayan yoğunluk işlemcilerine de Markov durumları denir (Petz 2002). Bilgi taşıyıcı sistemlerin ve çevrelerinin giriş durumları bir Markov durumunun indirgenmiş (marjinal) durumu olması halinde, kuantum veri işleme eşitsizliğinin sağlanması (Nielsen ve Chuang 2000, Schumacher ve Westmoreland 2010, Holevo 2012) ve kuantum hata düzeltiminin tam olarak yapılabilmesi (Schumacher ve Westmoreland 2010) gibi çeşitli bilişim yükümlülükleri başarıyla gerçekleştirilebilmektedir. Ayrıca, bilgi taşıyıcı sistem ve çevresine ek olarak, etkileşmelere katılmayacak fakat sistemin korelasyon halinde bulunabileceği bir referans sistemi tarafından oluşturulan üç parçalı bir çalışma çerçevesi bilişim süreçlerinin analizinde önem kazanacağından, böyle bir çerçevede GaT bağıntısı ve Markov durumlarını temel alan analiz yöntemleri ön plana çıkmaktadır

Bu bilgiler ışığında, tezin ilk bölümünde, klasik ve kuantum entropileri, çeşitleri ve ilgili eşitsizlik bağıntıları özetlenerek GaT bağıntısı elde edilmiştir. İkinci bölümde ise GaT bağıntısının kronolojik olarak sıralanmış ispatları farklı bakış açıları çerçevesinde gösterilmiştir. Üçüncü bölümde, GaT bağıntısının eşitlik durumunu sağlayan Markov durumları incelenerek uygulama alanları hakkında araştırmalar yapılmıştır. Bu tezin son bölümünde GaT bağıntısının günümüz teknolojilerinde kullanıldığı farklı alanlar bulunmaktadır. Bu uygulamalar içerisinde en çok öne çıkan ve uygulanabilirliği en yüksek olan konu, Holevo niceliğidir (Holevo 1973, Nielsen ve Chuang 2000, Wilde 2011). Bir kuantum kanalının, taşıyabileceği klasik bilginin limitini belirleyen bu nicelik, kuantum entropisi için bir üst sınır oluşturmaktadır. Holevo niceliği sayesinde bir kuantum kanalın kapasitesi belirlenir.

# 2. SHANNON VE VON NEUMANN ENTROPİLERİ

Klasik ve kuantum olmak üzere iki çeşit bilişim (*information*) kuramı vardır. Bu bölümde entropi nedir sorusundan başlanılarak, bilişim kuramlarındaki entropilerin özellikleri ile sağladıkları önemli bağıntılar ve eşitsizlikler ele alınacaktır. Entropi, termodinamiğin temelini oluşturan bir niceliktir ve tanım olarak bir sistemin düzensizliğini temsil eder. Fakat bilişim kuramlarındaki entropiler farklı anlamlar içerebilir ki bu durum entropi kavramının bilişim kuramlarının gelişiminde önemli rol edinmiştir.

## 2.1 Klasik Bilişim Kuramında Entropi

Bilişim kuramında entropi; düzensizliğin, belirsizliğin veya bilgisizliğin ölçüsü olarak tanımlanabilir. Aynı zamanda bir mesajdaki bilgi miktarı olarak da tanımlanabilir. Klasik bilişim kuramında entropi Shannon entropisi olarak bilinir ve $H$ ile gösterilir. Eğer bir kaynağın M tane eş-olasılıklı mesaj ürettiği varsayılırsa entropi;

$$H = logM \tag{2.1}$$

ifadesi ile tanımlanır. Bu durum mesajı güvenle iletmek için mesaj başına gerekli olan minimum bit sayısını gösterir. (Aksi belirtilmediği sürece $log \equiv log_2$ olarak alınacaktır.) Eğer kaynak bu M mesajı eş-olasılıklı olarak üretiyorsa, entropiyi hesaplamak kolay bir işleme dönüşür. Fakat bu noktada sorulacak en doğru soru ise; kaynağın M tane eş-olasılıklı mesaj üretememe durumunda ne olacağıdır. Örnek olarak; eğer Türkçe karakterlerden oluşan bir mesaj kümesi eş dağılımlı harfler barındırıyor olsaydı, noktalama işaretlerini ve boşluk karakterinin sayılmadığı ve her harfin eş-olasılıklı olduğu düşünülürek her harf için en az $H = log29 = 4,86$ kadarlık bite ihtiyaç olacaktır. Fakat Türkçe harfler eş-olasılık ile bulunmazlar. Dolayısıyla (2.1) ifadesi kullanılamaz duruma gelir. Bu tip durumların entropisini hesaplamak için olasılık teorisinde kullanılan rasgele değişken (*random variable*) niceliği kullanılır.

İletilen mesajlar bir rasgele değişken olan $X$'in olası değerleri olarak alınırsa herhangi bir $x$ değeri için $p(x)$ olasılığında bulunması beklenir. Eğer mesajlar bir rasgele değişken üzerinden yüklenirse; $n_x$ eş-olasılıklı çıktılara karşılık gelmek üzere, her bir $x$ değeri için $x$'in olma olasılığı

$$p(x) = \frac{n_x}{N} \tag{2.2}$$

şeklinde tanımlanır. Hem $N$ eş-olasılığa sahip hem de daha büyük bir mesaj olan bir $Z$ mesajı alınarak $Z$'nin değerleri altkümelere ayrılıp, $X$'in değerleri ile etiketlensin. $x$ altkümesinin toplam olasılığı $p(x)$ olmak üzere, aşağıdaki iki duruma sadık kalma koşulu ile $Z$'nin değerleri özelleştirilebilir:

- (1) rasgele değişken $X$'in $x$ değeri,
- (2) hangi $n_x$ çıktısının geleceği.

Tüm entropi $H(Z) = logN$ iken her $x$ değeri için altkümenin entropisi $logn_x$ olur. Bu bilgiler ışığında aşağıdaki ifade yazılabilir:

$$H(Z) = logN = H(X) + \sum_x p(x) logn_x \tag{2.3}$$

Bu bağıntı, (2.2) kullanılarak $H(X)$ için çözülürse;

$$H(X) = -\sum_x p(x) logp(x) \tag{2.4}$$

eşitliği elde edilir. Bu eşitlik Shannon entropisinin en genel halidir ve klasik bilişim teorisinin temelini oluşturur. Rasgele değişken $X$, eş-olasılıklı $M$ mesaj içeriyor olmak üzere (2.4) ifadesi (2.1) haline gelir. $H(X)$ bir rasgele değişken üzerinden tanımlanıyor olmasına rağmen, $X$'in olasılık dağılımına bağlı bir fonksiyon olduğu söylenebilir. Yani $H(X)$ teriminin bir sistem üzerindeki bilgimiz olduğu düşünülebilir. Rasgele değişken $X$'in değeri başka bir rasgele değişken $Y$'nin üzerinden kodlanabilir. Fakat $p(x) = p(y)$ olduğu açıkça görülür. Bu durum aynı bilginin farklı iki rasgele değişken üzerinden temsilidir. Yani $H(X) = H(Y)$ bağıntısı aşikardır. Yani, entropide çıktılara bakılmaz esas olan olasılıklardır.

### 2.1.1 Bileşik ve Koşullu Entropi

$X$ ve $Y$ bileşik $p(x,y)$ olasılık dağılımına sahip iki rasgele değişken olmak üzere $XY$ kümesinin kardinalitesi üstten sınırlıdır. Bu bileşik sistemin entropisi,

$$H(XY) = -\sum_{x,y} p(x,y) logp(x,y) \tag{2.5}$$

ifadesi ile tanımlanır. (2.4) bağıntısına benzer olarak bileşik entropi de negatif olamaz.

Bileşik dağılım üzerinden bir çok bağıntı elde edilebilir. $X$ ve $Y$ için marjinal dağılımları belirlemek, bileşik olasılıkların değişkenleri üzerinden toplama yolu ile bulunur:

$$p(x) = \sum_y p(x,y), \;\; p(y) = \sum_x p(x,y). \tag{2.6}$$

Bu bilgiler ışığında $H(X)$ ve $H(Y)$ entropileri elde edilebilir. Verilen bir $Y$ değişkeni için sabit tutulan bir $y$ değeri $p(y) > 0$ ile birlikte, $X$ üzerinde koşullu olasılık dağılımı $\sum_x p(x|y) = 1$ bilgisi kullanılarak

$$p(x|y) = \frac{p(x,y)}{p(y)} \tag{2.7}$$

şeklinde hesaplanır. Koşullu olasılık dağılımı elde edildiğine göre tek koşullu entropi;

$$H(X|y) = -\sum_x p(x|y) log p(x|y) \tag{2.8}$$

şeklinde yazılabilir. Bu durum belirli bir $y$ değeri için (2.8) denklemi halini alır. Bu, bir y değeri verildiğinde x'te kalan belirsizlik miktarını ölçer anlamını taşır. Koşullu entropi $H(X|Y)$, böyle $y$ değerleri üzerinden ortalama olarak tanımlanır: Öyleyse

$$H(X|Y) = \sum_y p(y) H(X|y) = -\sum_{x,y} p(x,y) log p(x|y) \tag{2.9}$$

sonucu elde edilir. (2.7) bağıntısı kullanılarak;

$$\begin{aligned} H(X|Y) &= -\sum_{x,y} p(x,y) log \left( log \frac{p(x,y)}{p(y)} \right) \\ &= -\sum_{x,y} p(x,y) log p(x,y) + \sum_{x,y} p(x,y) log p(y) \end{aligned} \tag{2.10}$$

eşitliği elde edilir. (2.10) denkleminin ikinci teriminde $x$ üzerinden toplam alınırsa

$$H(X|Y) = -\sum_{x,y} p(x,y) log p(x,y) + \sum_y p(y) log p(y) \tag{2.11}$$

ifadesi ortaya çıkar. Shannon entropisinin tanımı kullanılarak (2.11) ifadesinin sağ tarafındaki ilk terim $H(XY)$ iken ikinci terim $-H(Y)$ olduğu görülür. Böylelikle aşağıdaki

denklemler elde edilir:

$$\begin{aligned} H(X|Y) &= H(XY) - H(Y) \\ H(XY) &= H(Y) + H(X|Y) \\ &= H(X) + H(Y|X). \end{aligned} \tag{2.12}$$

(2.9) denklemi *klasik koşullu entropi* olarak bilinir. Bu bakış açısından hareketle; $X$ ve $Y$ bileşik sisteminin bilgi miktarı, $Y$'nin ve verilen $Y$ koşulunda $X$'in bilgi miktarının toplamına eşittir denir. (2.9) denklemindeki tanım üç parçalı bir sisteme uygulanırsa;

$$\begin{aligned} H(XYZ) &= H(YZ) + H(X|YZ) \\ &= H(Z) + H(XY|Z) \end{aligned}$$

bağıntıları yazılır. Birinci denklemden ikinci denklem çıkarılırsa;

$$0 = -H(Z) + H(YZ) + H(X|YZ) - H(XY|Z)$$

eşitliği elde edilir. (2.12) tanımı kullanılarak

$$\begin{aligned} 0 &= H(Y|Z) - H(XY|Z) + H(X|YZ) \\ \Longrightarrow H(XY|Z) &= H(X|YZ) - H(Y|Z) \end{aligned} \tag{2.13}$$

denklemine ulaşılır. Bu bağıntı koşullu entropi için *zincir kuralı* olarak bilinir.

Koşullu entropi, negatif olmayan terimlerin ortalaması olduğundan $H(X|Y) \geq 0$ olur. Dolayısıyla (2.12) ifadesi kullanılarak $H(XY) \geq H(Y)$ eşitsizliği elde edelir. Bu özellik *klasik entropinin monotonluğu* olarak tanımlanabilir. Bu demektir ki; değişkenlerden birini atmakla entropi artmaz, aksine azalır. Bu durum kuantum entropi için geçerli değildir. Dolanık durumlar söz konusu olduğunda monotonluk özelliği geçerliliğini kaybeder.

Entropi fonksiyonunun temel özelliklerinden biri Gibbs eşitsizliğidir. Rasgele bir $X$ de-

ğişkeni için $p(x)$ ve $q(x)$ dağılımlar olmak üzere;

$$-\sum_x p(x)logp(x) \leq -\sum_x p(x)logq(x) \tag{2.14}$$

bağıntısı *Gibbs eşitsizliği* olarak bilinir. Eşitlik koşulu ancak ve ancak bu iki dağılımın aynı olduğu durumlarda geçerlidir: $p(x) = q(x)$, her $x$ için. Gibbs eşitsizliğinden entropi fonksiyonunun bir çok özelliği elde edilebilir.

Bu noktadan yola çıkarak; $q(x)$, $p(x)$ aynı rasgele değişkenin birer olasılık dağılımı olarak alınarak iki dağılım arasındaki *bağıl entropi* tanımlanabilir:

$$\begin{aligned} D(p\|q) &= \sum_x p(x)\, log\frac{p(x)}{q(x)} \\ &= \sum_x p(x)logp(x) - \sum_x p(x)logq(x). \end{aligned} \tag{2.15}$$

Gibbs eşitsizliğinden görülebileceği gibi (2.15) denkleminin sağ tarafındaki ilk terim ikinci terimden büyük ya da eşittir. Bu bilgiye dayanarak $D(p \parallel q) \geq 0$ bağıntısı kolaylıkla görülebilir. Eşitlik durumu ise ancak ve ancak her $x$ için $p(x) = q(x)$ durumunda sağlanır. Bağıl entropi bir nevi uzaklık fonksiyonu olarak tanımlanabilir. Fakat bu uzaklık fonksiyonu olarak tanımlanan bağıl entropi fonksiyonu, simetriyi ve üçgen eşitsizliğini sağlamaz. Dolayısıyla tam anlamıyla bir uzaklık fonksiyonu belirtmez.

$X$ ve $Y$ rasgele değişkenleri için *klasik karşılıklı bilişim* $I(X:Y)$

$$\begin{aligned} I(X:Y) &= \sum_{x,y} p(x,y)log\frac{p(x,y)}{p(x)q(y)} \\ &= H(X)+H(Y)-H(XY) \end{aligned} \tag{2.16}$$

olarak tanımlanır. Klasik karşılıklı bilişim (2.15) niceliği kullanılarak bağıl entropi cinsinden yazılabilir. $-H(X|Y) = H(Y) - H(XY)$ eşitliği kullanılarak (2.16) ifadesi

$$\begin{aligned} I(X:Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \end{aligned} \tag{2.17}$$

haline getirilebilir. Bağıl entropi pozitif olduğundan $I(X:Y) \geq 0$ olur. Eşitlik durumu ise

ancak ve ancak $X$ ve $Y$ rasgele değişkenlerinin istatistiksel olarak bağımsız olduklarında gerçekleşir. Bu bilgiler ışığında klasik karşılıklı bilişimin aynı zamanda $X$ ve $Y$ arasındaki tüm klasik korelasyonların ölçüsü olduğu görülür. Bu noktadan yola çıkarak;

$$\begin{aligned} H(X) &\geq H(XY) - H(Y) = H(X|Y) \\ H(X) + H(Y) &\geq H(XY) \end{aligned} \tag{2.18}$$

elde edilir. (2.18) eşitsizliğine Shannon entropisi için *alt-toplanabilirlik bağıntısı* denir. Bir başka deyiş ile $Y$ değişkeninin değerinin belirlenmesi asla ve asla $X$ değişkeninin entropisini arttırmaz.

### 2.1.2 Klasik Güçlü Alt-Toplanabilirlik (GaT) bağıntısı

Koşullu karşılıklı bilişim $I(A:C|B=b)$, $B=b$, koşulunda $A$ ve $C$ değişkenleri arasındaki karşılıklı bilişim olmak üzere,

$$I(A:C|B) = \sum_b p(b)\, I(A:C|B=b) \tag{2.19}$$

şeklinde tanımlanır. $I(A|_{B=b} : C|_{B=b})$ ile

$$\begin{aligned} p\{A|_{B=b} = a : C|_{B=b} = c\} &= \frac{p(a,b,c)}{p(b)} \\ &:= p(a,c|b) \end{aligned} \tag{2.20}$$

olduğu görülür. Bu tanımlar kullanılarak;

$$\begin{aligned} I(A:BC) &= H(A) + H(BC) - H(ABC) \\ &= I(A:B) + I(A:C|B) \end{aligned} \tag{2.21}$$

ve

$$I(A:C|B) = H(A|B) + H(C|B) - H(AC|B) \tag{2.22}$$

sonucu elde edilir. (2.22) ifadesinin denklemin sol tarafı karşılıklı bilişimin konveks kombinasyon tanımından dolayı negatif değildir. Dolayısıyla klasik dağılımlar için GaT ba-

ğıntısı $I(A:C|B) \geq 0$ özelliğinin sonucu olarak elde edilmiş olur:

$$H(AB) + H(BC) \geq H(ABC) + H(B). \tag{2.23}$$

**Teorem 2.1:** Verilen bir $B$ için $A$ ve $C$'nin koşullu bağımsız olmaları durumunda $I(A:C|B) = 0$ olur. Her b değeri için bir $p(b) \neq 0$ olasılığı vardır öyle ki A ve C terimlerinin bağımsız olduğu söylenebilir. Böyle bir durumda

$$\begin{aligned} p(a,b,c) &= p(b)\,p(a|b)\,p(c|b) \\ &= p(a)\,p(b|a)\,p(c|b) \end{aligned} \tag{2.24}$$

$A - B - C$ bu sıra ile bir Markov zinciri olur.

**İspat:** Koşulların sağlandığı aşikardır. Tersine olarak varsayılsın ki $I(A:C|B) = 0$. Son niceliğin tanımında dolayı $p(b) \neq 0$ koşulunu sağlayan her $b$ için $I(A:C|B=b) = 0$ olur. Fakat bu $A|_{B=b}$ ve $C|_{B=b}$'nin bağımsız olduklarını söyler. Böylece

$$\begin{aligned} p(a,b,c) &= p(b)\,p(a,c|b) \\ &= p(b)\,p(a|b)\,p(c|b) \\ &= p(a)\,p(b|a)\,p(c|b) \end{aligned} \tag{2.25}$$

(2.24) sonucu elde edilir.

### 2.1.3 Konvekslik ve Konkavlık

Tek değişkenli bir fonksiyonun konveks olması üç farklı şekilde açıklanabilir:

(i) $f$ bir fonksiyon olmak üzere iki farklı $x$ ve $y$ girdileri ve $0 \leq \lambda \leq 1$ eşitsizliğini sağlayan her $\lambda$ parametresi için

$$f(\lambda x + (1-\lambda)y) \leq \lambda f(x) + (1-\lambda) f(y) \tag{2.26}$$

eşitsizliğini sağlayan fonksiyona konveks denir. Yani ortalamadaki değer, değerlerin orta-

lamasından küçük ise fonksiyon konvekstir denir.

(ii) Bir fonksiyonun konveksliği fonksiyonun grafiği üzerinden de tanımlanabilir. Grafik üzerinden rasgele seçilen iki nokta ile oluşturulan doğru parçası grafiğin üzerinde kalıyor ise bu fonksiyon konvekstir denir.

(iii) $f$ fonksiyonunun konveks olması için gerekli koşul, her $x$ değeri için $f''(x) \geq 0$ olmasıdır. Aynı zamanda fonksiyon $f''(x) > 0$ ise kesin konvekstir (*strictly convex*) denir. Eğer $f$ fonksiyonu iki kere türevlenebiliyor ise, yukarıdaki koşullar gerek ve yeterlidir.

Bazı eşitsizliklerin ispatı için konveks fonksiyonun ilk tanımı kullanılır. (2.26) eşitsizliği genelleştirilebilir. $f$ fonksiyonunun girdileri $x_1, x_2, \cdots, x_n$ ve $\sum_k \lambda_k = 1$ eşitliğini sağlayan $\lambda_1, \lambda_2, \cdots, \lambda_n$ negatif olmayan sayılar olmak üzere $f$ fonksiyonunun konveksliği tanımdan faydalanılarak

$$f\left(\sum_k \lambda_k x_k\right) \leq \sum_k \lambda_k f(x_k) \tag{2.27}$$

eşitsizliği ile ifade edilebilir. $x_k$ sayıları rasgele değişken $X$'in değerleri olarak düşünülebilir. Öyle ki $\lambda_k$'lar her $x_k$'nın olasılığına denk gelir. Öyleyse bu eşitsizlik beklenen değer üzerinden yazılabilir:

$$f(\langle X \rangle) \leq \langle f(X) \rangle . \tag{2.28}$$

(2.28) bağıntısı *Jensen eşitsizliği* olarak bilinir. Konveks fonksiyonların bazı özellikleri ilerleyen aşamalar için faydalı olacaktır.

**Lemma 2.2:** İki farklı konveks fonksiyonun toplamı yine bir konveks fonksiyonunu verir.

**İspat:** $f(x)$ ve $g(x)$ bir $S$ konveks kümesi üzerinde tanımlı iki konveks fonksiyon olmak üzere, $S$ kümesinden rasgele $x_1$ ve $x_2$ elemanları alınsın. Öyleyse bu iki konveks fonksiyonun toplamı başka bir fonksiyona eşit olmak üzere; $h(x) = f(x) + g(x)$ için

$$f(\lambda x_1 + (1-\lambda)x_2) + g(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda) f(x_2) + \lambda g(x_1) + (1-\lambda) g(x_2) \tag{2.29}$$

eşitsizliğinin gösterilmesi yeterli olacaktır. Konveks fonksiyonun tanımı kullanılarak

$$f(\lambda x_1 + (1-\lambda)x_2) \leq \lambda f(x_1) + (1-\lambda) f(x_2)$$

$$g(\lambda x_1 + (1-\lambda)x_2) \leq \lambda g(x_1) + (1-\lambda)g(x_2) \tag{2.30}$$

eşitsizlikleri yazılabilir. Bu iki eşitsizlik taraf tarafa toplanarak (2.29) gösterilmiş olur.

Eğer bir $-f(x)$ fonksiyonu konveks ise $f(x)$ fonksiyonuna konkav denir. Daha basit bir söylem ile (2.26) eşitsizliğinin işaretinin ters olması $f(x)$ fonksiyonunun konkav olduğunu söyler ki bu durum (2.27) ve (2.28) denklemleri için de geçerli olur. Dolayısıyla lemma 2.2 konkav fonksiyonlar için de gösterilebilir.

$X$, $p(x)$ olasılık dağılımına sahip bir rasgele değişken olarak alınarak $p(x)$ sayıları $P_X$ ile gösterilen sayısal rasgele değişkenin değerleri olarak düşünülebilir. Bu yeni değişken aşağıdaki ortalamaya sahiptir:

$$\langle P_X \rangle = \sum_x p(x)^2. \tag{2.31}$$

$f(y) = -logy$ fonksiyonu her $y > 0$ değeri için konveks olduğundan Jensen eşitsizliği kullanılarak entropi için bir eşitsizlik türetilebilir:

$$\begin{aligned} H(X) &= -\sum_x p(x) log p(x) \\ &= \langle -log P_X \rangle \\ &\geq -log \langle P_X \rangle = -log \left( \sum_x p(x)^2 \right). \end{aligned} \tag{2.32}$$

$g(y) = -ylogy$ fonksiyonu ise $0 \leq y \leq 1$ aralığındaki her y değeri için konkavdır. Bu terimlerin toplamları entropi fonksiyonunu verdiğinden, olasılık dağılımı fonksiyonu da konkav olur. Bu bilgilere dayanarak, $p_1(x)$ ve $p_2(x)$ aynı küme üzerinde tanımlı iki olasılık dağılımı ve $0 \leq \lambda \leq 1$ olsun. Öyleyse ortalama olasılık dağılımı yazılabilir:

$$p(x) = \lambda p_1(x) + (1-\lambda) p_2(x). \tag{2.33}$$

Entropi fonksiyonunun konkavlığı, bu dağılımların entropilerinin

$$H = -\sum_x p(x) log p(x) \geq \lambda H_1 + (1-\lambda) H_2 \tag{2.34}$$

denklemini sağlaması ile tanımlanır. Öyle ki $H_i$ terimleri $p_i(x)$ dağılımlarının entropisidir. Ortalama dağılımın entropisi, her zaman en az bu iki dağılımın entropilerinin ortalaması

kadardır.

## 2.2 Kuantum Bilişimde Entropi

Saf veya saf olmayan bir durumda olan bir kuantum sistemi yoğunluk matrisleri ile tanımlanır. Yoğunluk matrisi, kuantum mekaniksel bir sistemin olasılıksal durumunu tanımlayan bir matristir. Sadece saf durumlar için bir projeksiyon işlemcisi olan $\rho$, yoğunluk işlemcisinin[1] matris gösterimidir. Sistemin hazırlanışı bilinmediğinden saf olmayan durum önem kazanır. Örneğin; sistem başka sistemler ile dolanık halde ise bu durum entropiyi etkiler. Burada $\rho$ Hilbert uzayında $d$ boyutlu bir alt-uzayda tanımlı tekdüze (*uniform*) bir yoğunluk matrisi ve $\rho = I/d$ olmak üzere, sistemin kuantum entropisi;

$$S = logd \tag{2.35}$$

olarak tanımlanır. Bu kuantum entropi, tekdüze dağılım için tanımlanan klasik entropi ile paralel bir tanıma sahiptir. Klasik entropide olduğu gibi kuantum entropi için de daha genel dağılımlar yazılabilir. Kuantum entropi $(S)$ daha genel yoğunluk işlemcilerine genellenebilir.

İlk olarak Shannon entropisi ile kuantum entropisinin bazı farklı özelliklere sahip oldukları gösterilmelidir. Örneğin; $X$ ve $Y$ iki rasgele değişken olmak üzere, bileşik sistemin Shannon entropisi en az bir çarpanının Shannon entropisi kadardır. Yani $H(XY) \geq H(Y)$ olur. Fakat bir ebit[2], maksimum dolanık (*maximally entangled*[3]) durumda olan bir A ve B kübit[4] çifti düşünülürse, alt-sistem durumu bütün Hilbert uzayında tanımlı tekdüze bir yoğunluk işlemcisi olur. Dolayısıyla $S(A) = S(B) = 1$ eşitliği görülür. Fakat bileşik bir AB sistemi saf bir durum ise sistemin entropisi sıfıra eşit olur: $S(AB) = 0$. Dolanıklıktan ötürü tüm sistemin kuantum entropisi, bir çarpanının kuantum entropisinden küçük olabilir.

Kuantum entropinin genel tanımı von Neumann tarafından yapılmıştır (von Neumann 1932). Bu sebeple kuantum entropisine von Neumann entropisi de denir. Bir $\rho$ yoğunluk

[1] $|\psi>$ bir saf durumu betimleyen yoğunluk matrisi projeksiyon olduğundan $\rho = |\psi><\psi|$ şeklinde gösterilir.

[2] Ebit ismi ingilizcesi olan *entanglement bit* kavramının kısaltılması ile elde edilir.

[3] $\rho$ saf durumu iki parçalı bir $H_A \otimes H_B$ uzayında tanımlı olmak üzere, eğer $\rho$'nun indirgenmişi diagonal(köşegen) bir matris ise $\rho$'ya maksimum dolanık durum denir.

[4] Kübit ismi kuantum bit kavramının kısaltılması ile ortaya çıkarılmıştır.

işlemcisi ile tanımlanan $Q$ sistemi için, von Neumann entropi

$$S(Q) = -Tr\rho log\rho \tag{2.36}$$

olarak tanımlanır. $\rho$ bir işlemci olmasına karşın entropiyi hesaplamanın en kolay yolu; $\rho$ yoğunluk matrisini köşegenleştiren baz seçilerek yapılır. $\rho_k$'lar $\rho$ yoğunluk matrisinin özdeğerleri olmak üzere;

$$S(Q) = -\sum_k \rho_k log\rho_k \tag{2.37}$$

şeklinde tanımlanabilir. Klasik entropi rasgele değişkenler üzerinden tanımlanırken, kuantum entropi yoğunluk işlemcileri üzerinden tanımlanır. Bir başka deyiş ile; von Neumann entropi, $\rho$ yoğunluk işlemcisinin özdeğerlerinin Shannon entropisidir.

**Tanım 2.3:** Bir yoğunluk matrisinin köşegen elemanlarına nüfuslanmalar (*populations*) denir.

**Teorem 2.4:** $\rho$ yoğunluk işlemcisinin popülasyonlarının Shannon entropisi, $\rho$ yoğunluk matrisinin von Neumann entropisinden küçük olamaz.

**İspat:** Bir $|a_n\rangle$ bazı üzerinde tanımlı bir $Q$ sisteminde yapılan ölçüm sonucunda $a_n$ çıktısının gelme olasılığı, $\rho$'nun özdeğerleri $\rho_k$ ve özvektörleri $|k\rangle$ olmak üzere $p(a_n) = \langle a_n| \rho |a_n\rangle$ bağıntısından

$$p(a_n) = \sum_k |\langle a_k \mid k\rangle|^2 \rho_k \tag{2.38}$$

ile hesaplanır. (2.38) denklemi rasgele değişken $A$ üzerinde tanımlı olasılık dağılımı olarak düşünülebilir. Öyle bir matris alınsın ki elemanları $M_{nk} = |\langle a_k \mid k\rangle|^2 \geq 0$ ile tanımlansın[5]. Normalizasyon bağıntısı kullanılarak

$$\sum_n M_{nk} = 1 = \sum_k M_{nk}$$

eşitliği elde edilir. Bir başka deyiş ile $M$ matrisinin satırları ve sütunları olasılık dağılımları olarak düşünülebilir. Yani $M$ matrisinin her satır ve sutün elemanları toplamı 1 olur. Bu özelliğe sahip bir matrise *ikili-stokastik (double-stochastic)* denir. Bu matrislerin her biri klasik kanaldır. Dolayısıyla bu özelliği taşıyan herhangi bir yoğunluk matrisi

[5]CBS eşitsizliği : $|\langle\psi|\ \phi\rangle|^2 \leq \langle\psi|\ \psi\rangle\langle\phi|\ \phi\rangle$

$\rho = \sum_k M_{nk}\rho_k$ formunda alınabilir.

Shannon entropi $H(A)$, ikili-stokastik matris cinsinden tanımlanabilir:

$$H(A) = -\sum_n \left( \sum_k M_{nk}\rho_k \right) log \left( \sum_l M_{nl}\rho_l \right). \tag{2.39}$$

Dolayısıyla $R$, $\rho_k$ değerleri ve $M_{nk}$ olasılıkları ile tanımlanmış rasgele bir değişken olmak üzere, $n$ toplamındaki her bir terimin $f(\langle R \rangle)$ formuna sahip olduğu kolaylıkla görülebilir. Örneğin $f(x) = xlogx$ fonksiyonu konvekstir. Öyleyse, (2.28) denkleminde tanımlanan Jensen eşitsizliği kullanılarak

$$H(A) \geq -\sum_n \left( \sum_k M_{nk}\rho_k log\rho_k \right) \tag{2.40}$$

eşitsizliği elde edilir. Bu eşitsizliğin sağ tarafındaki iki toplamın yerleri değişebileceğinden

$$H(A) \geq -\sum_k \left( \sum_n M_{nk}\rho_k log\rho_k \right) \tag{2.41}$$

şeklinde yazılır. $\sum_n M_{nk} = 1$ özelliği kullanılarak

$$H(A) \geq -\sum_k \rho_k log\rho_k \tag{2.42}$$

haline getirilir. Eşitsizliğin sağ tarafı Shannon entropinin tanımı olur. Dolayısıyla

$$H(A) \geq S(Q) \tag{2.43}$$

eşitsizliği elde edilir. Eşitlik durumu ise $H$ ve $Q$ işlemcilerinin sıra değiştirmeleri ile gerçekleşir.

**Lemma 2.5:** $\rho$ ve $\sigma$, $Q$ sistemi için iki yoğunluk işlemcisi olsun. Öyle ki bu iki yoğunluk işlemcisi

$$\rho = \sum_k \rho_k |r_k\rangle \langle r_k| \tag{2.44}$$

$$\sigma = \sum_n \sigma_n |s_n\rangle \langle s_n| \tag{2.45}$$

olarak alınabilir. $-Tr\rho log\sigma$ bağıntısından yola çıkarak, $\rho$ ve $\sigma$ değerleri yerine yazılırsa

$$-Tr\rho log\sigma = -Tr\left[\sum_k \rho_k |r_k\rangle \langle r_k| log\sigma\right]$$

bağıntısı bulunur. Denklemin sağ tarafındaki iz bağıntısı kullanılarak;

$$-Tr\rho log\sigma = -\sum_k \rho_k \langle r_k| log\sigma |r_k\rangle$$

haline gelir. $\sigma$ yoğunluk işlemcisi yerine yazılırsa;

$$\begin{aligned} -Tr\rho log\sigma &= -\sum_k \rho_k \langle r_k| \left(\sum_n log\sigma_n |s_n\rangle \langle s_n|\right) |r_k\rangle \\ &= -\sum_k \rho_k \left(\sum_n log\sigma_n |\langle s_n \mid r_k\rangle|^2\right) \end{aligned}$$

haline dönüşür. $|\langle s_n \mid r_k\rangle|^2$ terimi $M_{nk}$, yani ikili-stokastik bir matris özelliği taşıdığından;

$$-Tr\rho log\sigma = -\sum_k \rho_k \left(\sum_n M_{nk} log\sigma_n\right)$$

şeklinde yazılabilir. Denklemin sağ tarafına Jensen eşitsizliği uygulanırsa;

$$-Tr\rho log\sigma \geq -\sum_k \rho_k log\left(\sum_n M_{nk}\sigma_n\right)$$

eşitsizliği elde edilir. $\tau_k = \sum_n M_{nk}\sigma_k$ olmak üzere

$$-Tr\rho log\sigma \geq -\sum_k \rho_k log\tau_k$$

halini alır. Gibbs eşitsizliği uygulanarak

$$-\sum_k \rho_k log\tau_k \geq -\sum_k \rho_k log\rho_k$$

sonucu elde edilir. Bu denklem de

$$-Tr\rho log\sigma \geq -Tr\rho log\rho \tag{2.46}$$

eşitsizliğini ortaya çıkarır. (2.46) eşitsizliği *Klein eşitsizliği* olarak bilinir. Klein eşitsizliği kuantum durumlarda kullanılır. Aslında klasik durumlar için kullanılan Gibbs eşitsizliğine paralel bir yapıya sahiptir. (2.46) ifadesinin eşitlik durumu ise ancak ve ancak $\rho = \sigma$ durumunda sağlanır. Böylece ispat tamamlanmış olur.

(2.46) bağıntısı kuantum bağıl $D(\rho||\sigma)$ entropinin tanımlanmasına yardımcı olur:

$$D(\rho||\sigma) = Tr\rho log\rho - Tr\rho log\sigma. \tag{2.47}$$

Klein eşitsizliğinden $D(\rho||\sigma) \geq 0$ olduğu açıkça görülebilir. Eşitlik durumu ise yine $\rho = \sigma$ durumunda geçerli olur.

Klasik bağıl entropi gibi kuantum bağıl entropi de asimetrik olmayan bir uzaklık fonksiyonu olarak düşünülebilir[6].

Shannon entropisinde olduğu gibi von Neumann entropisinin de belli başlı özelliklerinden bahsetmek gereklidir. Öyle ki klasik entropi için gösterilen çoğu özellik kuantum entropi için de benzer tanımlara sahiptir. Örneğin; bir AB bileşik sisteminin entropisi $S(AB)$ ve alt-sistemlerin entropileri ise $S(A)$ ve $S(B)$ şeklinde gösterildiğinden, *kuantum karşılıklı bilişim* $I(A:B)$;

$$D\left(\rho^{AB}\middle\|\rho^{A}\otimes\rho^{B}\right) = I(A:B) = S(A)+S(B)-S(AB) \tag{2.48}$$

olarak tanımlanır. İki kuantum durumunun çarpım şeklinde yazılabilmesi, $\rho^A \otimes \rho^B$, korele olmadıklarını belirtir. (2.48) ifadesinin sıfıra eşit olabilmesi için gerek ve yeterli koşul $\rho^{AB} = \rho^A \otimes \rho^B$ eşitliğinin sağlanmasıdır. Dolayısıyla, tüm klasik ve kuantum korelasyonları nitelemek ve nicelendirmek için en önemli araç karşılıklı kuantum bilişimdir denir.

Kuantum karşılıklı bilişim bağıl entropi cinsinden (2.48) denkleminde elde edilmiştir. Bununla beraber bilinmesi gereken birkaç önemli detay daha vardır.

[6]Bağıl entropi $D(\rho||\sigma)$, simetriyi ve üçgen eşitsizliğini sağlamaz.

**Lemma 2.6:**

**(1)** $E^A$ ve $F^B$ pozitif işlemcileri için aşağıdaki bağıntı daima sağlanır:

$$log\left(E^A \otimes F^B\right) = \left(logE^A\right) \otimes I^B + I^A \otimes \left(logF^B\right). \tag{2.49}$$

**(2)** Aşağıdaki parçalı (kısmi) iz bağıntıları daima sağlanır:

$$\begin{aligned} Tr_B\left[\rho^{AB}\left(A \otimes I\right)\right] &= \rho^A A,\ \rho^A = Tr_B \rho^{AB} \\ Tr_A\left[\rho^{AB}\left(I \otimes B\right)\right] &= \rho^B B,\ \rho^B = Tr_A \rho^{AB} \end{aligned} \tag{2.50}$$

**İspat: (1)** Pozitif işlemcilerin spektral ayrışımları $E^A = \sum_i \lambda_i \left|e_i\right\rangle \left\langle e_i\right|$ ve $F^B = \sum_j \eta \left|f_j\right\rangle \left\langle f_j\right|$ olsun. Bu iki pozitif işlemcinin tensör çarpımı alınırsa;

$$E^A \otimes F^B = \sum_{i,j} \lambda_i \eta_j \left|e_i\right\rangle \left\langle e_i\right| \otimes \left|f_j\right\rangle \left\langle f_j\right| \tag{2.51}$$

eşitliği ortaya çıkar. İki tarafın da logaritması alınarak;

$$\begin{aligned} log\left(E^A \otimes F^B\right) &= \sum_{i,j} log\left(\lambda_i \eta_j\right) \left|e_i f_j\right\rangle \left\langle e_i f_j\right| \\ &= \sum_{i,j} log\lambda_i \left|e_i f_j\right\rangle \left\langle e_i f_j\right| + \sum_{i,j} log\eta_j \left|e_i f_j\right\rangle \left\langle e_i f_j\right| \\ &= \sum_i log\lambda_i \left|e_i\right\rangle \left\langle e_i\right| \otimes I^B + I^A \otimes \sum_{i,j} log\eta_j \left|f_j\right\rangle \left\langle f_j\right| \\ &= logE^A \otimes I^B + I^A \otimes logF^B \end{aligned} \tag{2.52}$$

bağıntısı bulunur.

**(2)** $C = Tr_B\left[\rho^{AB}\left(A \otimes I\right)\right] \in B\left(\mathscr{H}_A\right)$ olmak üzere

$$\left\langle a_i\right| C \left|a_j\right\rangle = \sum_l \left\langle a_i b_l\right| \rho^{AB}\left(A \otimes I\right) \left|a_j b_l\right\rangle \tag{2.53}$$

olur. Burada $\rho^{AB}$ teriminin sağ tarafına $AB$ sistemine ait tamlık bağıntısı olan $I^{AB} =$

$\sum_{k,m} \left|a_k' b_m'\right\rangle \left\langle a_k' b_m'\right|$ yerleştirilir. Öyle ki buradaki bazlar ortonormaldir. Böylece (2.53) denklemi;

$$\begin{aligned}
\langle a_i|C\left|a_j\right\rangle &= \sum_{l,k,m} \langle a_i b_l|\rho^{AB}\left|a_k' b_m'\right\rangle \left\langle a_k' b_m'\right|A\otimes I\left|a_j b_l\right\rangle \\
&= \sum_{l,k} \langle a_i b_l|\rho^{AB}\left|a_k' b_l\right\rangle \left\langle a_k'\right|A\left|a_j\right\rangle \\
&= \sum_{k} \langle a_i|Tr_B\rho^{AB}\left|a_k'\right\rangle \left\langle a_k'\right|A\left|a_j\right\rangle \\
&= \sum_{k} \langle a_i|\rho^{A}\left|a_k'\right\rangle \left\langle a_k'\right|A\left|a_J\right\rangle \\
&= \langle a_i|\rho^{A}A\left|a_j\right\rangle
\end{aligned} \tag{2.54}$$

haline dönüşür. Bu eşitlik her $i, j$ değerleri için sağlanır. Dolayısıyla istenilen sonuç elde edilmiş olur.

Lemma 2.6 kullanılarak

$$\begin{aligned}
D\left(\rho^{AB}\left\|\rho^A\otimes\rho^B\right.\right) &= Tr\left(\rho^{AB}log\rho^{AB}\right) - Tr\left(\rho^{AB}log\rho^A\otimes\rho^B\right) \\
&= -S(AB) - Tr_{AB}\left[\rho^{AB}\left(log\rho^A\otimes I + I\otimes log\rho^B\right)\right] \\
&= -S(AB) - Tr_A\left[\rho^A log\rho^A\right] - Tr_B\left[\rho^B log\rho^B\right] \\
&= -S(AB) + S(A) + S(B)
\end{aligned} \tag{2.55}$$

sonucu elde edilir. Bu bilgiler ışığında

$$I(A:B) = D\left(\rho^{AB}||\rho^A\otimes\rho^B\right) \geq 0 \tag{2.56}$$

olduğu gösterilmiş olur. Kuantum karşılıklı bilişim, $\rho^{AB}$ ile altsistemlerinin tensör çarpımlarının $\rho^A\otimes\rho^B$ birbirlerine ne kadar uzaklıkta olduğunun ölçüsüdür. Bir başka deyiş ile A ve B sistemlerinin aralarındaki tüm klasik ve kuantum korelasyonlarının bir ölçüsüdür. Böylelikle (2.48) bağıntısının pozitif olma özelliği kullanılarak

$$S(AB) \leq S(A) + S(B) \tag{2.57}$$

eşitsizliği kolaylıkla elde edilebilir. (2.57) ifadesi von Neumann entropisi için *alt-toplanabilirlik* bağıntısı olarak bilinir.

Klasik koşullu entropi (2.12) denkleminde tanımlanmış olup, tanım gereği olası tüm değerlerin ortalaması olarak alındığından her zaman pozitif olacağı daha önceden gösterilmişti. Buradan yola çıkarak *kuantum koşullu entropi* ise yine benzer bir şekilde

$$S(A|B) = S(AB) - S(B) \tag{2.58}$$

olarak tanımlanır. Fakat $S(A|B)$ daima pozitif olmak zorunda değildir. Çünkü kuantum koşullu entropi diğer entropilerin ortalaması cinsinden yazılamaz. Bir başka deyiş ile bileşik sistemin von Neumann entropi $(S(AB))$, alt-sistemlerinden herhangi birinin von Neumann entropisinden $(S(A)$ ya da $S(B))$ büyük olmayabilir. Örneğin; A ve B durumları dolanık olarak seçilmiş ise bu durum gerçekleşebilir. Dolayısıyla koşullu kuantum entropi negatif olabilir. Ayrıca kuantum durumlarda koşullu olasılıklar çoğu durumda iyi-tanımlı değildir.

A ve B sistemleri saf bir $\left|\psi^{AB}\right\rangle$ durumunda ise, $\rho^A$ ve $\rho^B$ yoğunluk işlemcileri sıfırdan farklı aynı özdeğerlere sahiptirler[7]. Dolayısıyla bu iki sistemin entropileri aynı olur:

$$S(A) = S(B). \tag{2.59}$$

Bu entropi A ve B sistemlerinin dolanıklığının ölçüsüdür. (2.59) denklemi entropinin daha birçok özelliğinin gösterilmesi için faydalı bir niceliktir. Örneğin; saf olmayan bir $\rho^{AB}$ durumunda olan bileşik AB sistemi ele alınıp bu AB bileşik sistemini saflaştıran bir C sistemi düşünülsün. Alt-toplanabilirlik bağıntısı kullanılarak AC sistemi için $S(A)+S(C) \geq S(AC)$ bağıntısı elde edilebilir. Oluşturulan ABC sistemi artık saf olduğundan, birbirlerini tümleyen sistemlerin entropileri birbirlerine eşit olur: $S(A) = S(BC)$, $S(AB) = S(C)$. Dolayısıyla

$$S(A) + S(AB) \geq S(B) \tag{2.60}$$

olduğu görülür. Bu eşitsizlik

$$S(AB) \geq S(B) - S(A) \tag{2.61}$$

[7]Ek C'de tartışılan Schmidt ayrışımna bakınız.

şeklinde de yazılabilir.

**Lemma 2.7:**
*Araki-Lieb* bağıntısı

$$|S(A)-S(B)| \leq S(AB) \tag{2.62}$$

şeklinde gösterilir.

**İspat:**
(2.62) ifadesi aynı zamanda von Neumann entropisi için *üçgen eşitsizliği* olarak da bilinir. $C$ sistemi $\rho^{AB} = \sum_i \lambda_i \left|u_i^{AB}\right\rangle \left\langle u_i^{AB}\right|$ yoğunluk işlemcisinin bir saflaştırıcısı[8] olmak üzere,

$$\left|\Psi^{ABC}\right\rangle = \sum_i^r \sqrt{\lambda_i} \left|u_i^{AB}\right\rangle \otimes |c_i\rangle \tag{2.63}$$

olarak yazılabilir. (2.63) ifadesinin $C$ bileşenine göre iz bağıntısı alınarak $\rho^{AB}$ bulunabilir:

$$\rho^{AB} = Tr_C \left( \left|\Psi^{ABC}\right\rangle \left\langle \Psi^{ABC}\right| \right). \tag{2.64}$$

Bu denklemde ikili alt sistemler düşünülerek: $S(AC) \leq S(A)+S(C)$ ve $S(B) \leq S(A)+S(AB)$ eşitsizlikleri elde edilebilir. Bu iki eşitsizlik kullanılarak da

$$S(AB) \geq S(B)-S(A) \tag{2.65}$$

ve dolayısıyla

$$S(AB) \geq S(A)-S(B) \tag{2.66}$$

eşitsizlikleri elde edilir. (2.65) ve (2.66) bağıntıları birleştirilerek;

$$|S(A)-S(B)| \leq S(AB) \tag{2.67}$$

eşitsizliği gösterilmiş olur.

[8]Saflaştırıcı kullanıyor olmak bir üst uzaya çıkmak anlamına gelir. Yani bir yoğunluk işlemcisinin bir üst uzaydaki genişletilmişi saftır.

# 3. GÜÇLÜ ALT-TOPLANABİLİRLİK BAĞINTISI

Güçlü alt-toplanabilirlik (GaT) bağıntısı klasik bilişim kuramında üç parçalı bir sistemin, çeşitli altsistemlerinin entropileri arasındaki ilişkiyi açıklayan, uzun zamandır bilinen en önemli bağıntılardan birisidir. Kuantum bilişim kuramı kapsamında ise ilk olarak Robinson ve Ruelle ile Lanford III ve Robinson'nın çalışmaları ile bulunan GaT bağıntısı, takip eden süreçte ispatlanmaya çalışılmış ve bunu ilk başaran bilim insanları Lieb ve Ruskai (E.H.Lieb ve M.B.Ruskai 1973) olmuştur. Bu bağıntı kuantum bilişim kuramı için temel bir teorem olmanın yanı sıra, bağıl entropinin monotonluğu gibi birçok özelliğin de ortaya çıkartılmasına ışık tutmuştur.

Klasik bilişim kuramı çerçevesinde üç derin gerçek kısmında ispatlanan GaT bağıntısının, bir kuantum sisteminin altsistemlerini açıklayan indirgenmiş yoğunluk matrislerinin sıra-değişmemesinden ötürü bu bağıntının kuantum karşılığının ispatı oldukça karmaşık ve anlaşılması güçtür. Bu bölümde Lieb ve Ruskai, Nielsen ve Petz, Hayden, Jozsa, Petz ve Winter ile Petz ispatları ele alınarak GaT bağıntısı kuantum bilişim kuramında incelenecektir.

## 3.1 E.H.Lieb ve M.B. Ruskai İspatı

Lieb ve Ruskai 1973 yılında yaptıkları çalışma ile kuantum bilişim kuramı kapsamında GaT bağıntısı başta olmak üzere çok sayıda teoremin ispatını gerçekleştirmişlerdir (E.H. Lieb ve M.B.Ruskai 1973).

Bu bağlamda $\mathscr{H}$ ayrılabilir (*separable*) bir Hilbert uzayı ve $\rho$, $\mathscr{H}$ üzerinde pozitif ($\rho \geq 0$) ve iz-sınıflı bir işlemci ve $\lambda_i$'ler $\rho$'nun özdeğerleri olmak üzere ($\rho \geq 0$ demek her $|\psi\rangle$ için $\langle\psi|\rho\,|\psi\rangle \geq 0$ anlamında kullanılır.), $\rho$'nun entropisi

$$S(\rho) \equiv -Tr\rho log\rho = -\sum_{i=1} \lambda_i log\lambda_i \tag{3.1}$$

ifadesi ile tanımlanır.

$\mathscr{H}_{12} = \mathscr{H}_1 \otimes \mathscr{H}_2$, iki Hilbert uzayının tensörel çarpımı olarak alınırsa $\rho_{12}$, $\mathscr{H}_{12}$ üzerinde pozitif, iz-sınıflı işlemci olarak tanımlanır. Öyle ki $\mathscr{H}_1$ uzayında $\rho_1$ pozitif, iz-sınıflı bir işlemci elde etmek için (EK 1.12)'teki gibi kısmi iz bağıntısı kullanılır.

Burada, $\varphi \in \mathscr{H}_1$ ve $\{e_i\}_{i=1}^{\infty}$, $H_2$ üzerinde tanımlı herhangi bir ortonormal baz olmak üzere,

$$\langle \varphi | \rho_1 | \varphi \rangle = \sum_{i=1} \langle \varphi \otimes e_i | \rho_{12} | \varphi \otimes e_i \rangle \tag{3.2}$$

biçiminde yazılır[9].

**Teorem 3.1:** $\mathscr{H}_{12} = \mathscr{H}_1 \otimes \mathscr{H}_2$ olmak üzere, $\rho_{12} \mapsto S(\rho_1) - S(\rho_{12})$ gönderimi, $\mathscr{H}_{12}$ üzerinde tanımlı pozitif, iz-sınıflı işlemciler[10] için konveks olur.

**İspat:** $\rho_{12}$ gönderimi için, $0 \leq \alpha \leq 1$ ve $\rho_{12}^{'}$ ile $\rho_{12}^{''}$, $\mathscr{H}_{12}$ üzerinde tanımlı kesin pozitif varsayılan, iz-sınıflı işlemciler için $\rho_{12} = \alpha\rho_{12}^{'} + (1-\alpha)\rho_{12}^{''}$ konveks kombinasyon yazılır ve uygulanırsa,

$$(S(\rho_1) - S(\rho_{12}))(\rho_{12}) \leq \alpha (S(\rho_1) - S(\rho_{12})) \left(\rho_{12}^{'}\right) + (1-\alpha)(S(\rho_1) - S(\rho_{12})) \left(\rho_{12}^{''}\right) \tag{3.3}$$

elde edilir. Bu noktadan hareketle, önce

$$\Delta = \alpha Tr_{12}\rho_{12}^{'} \left(-log\rho_{12}^{'} + log\rho_1^{'} + log\rho_{12} - log\rho_1\right) \tag{3.4}$$

ve

$$\Gamma = (1-\alpha) Tr_{12}\rho_{12}^{''} \left(-log\rho_{12}^{''} + log\rho_1^{''} + log\rho_{12} - log\rho_1\right) \tag{3.5}$$

yazılırsa, (3.4) ve (3.5) denklemlerinin yardımı ile (3.3) eşitsizliğinin $\Delta + \Gamma \leq 0$ olduğu kolaylıkla görülebilir. (2.46) bağıntısında belirtilen Klein eşitsizliği

$$Tr(-AlogA + AlogB) \leq Tr(B - A) \tag{3.6}$$

ile verildiğinden, $A = \rho_{12}^{'}$ ve $B = exp\left(log\rho_1^{'} + log\rho_{12} - log\rho_1\right)$ biçiminde seçilerek, (3.6)

[9]Eğer $\rho_1$, $\mathscr{H}_{12}$ üzerinde tanımlanıyor ise $\rho_1 \otimes I_2$ tensör çarpımı anlamına gelmektedir.
[10]İz-sınıflı işlemci, iz tanımlanabilir bir işlemcidir.

ifadesi $\Delta$'ya ve ardından da $\Gamma$'ya uygulanırsa;

$$\begin{aligned}\Delta+\Gamma &\leq \alpha Tr_{12}\left[exp\left(log\rho_1^{'}+log\rho_{12}-log\rho_1\right)-\rho_{12}^{'}\right] \\ &\quad +(1-\alpha)\,Tr_{12}\left[exp\left(log\rho_1^{''}+log\rho_{12}-log\rho_1\right)-\rho_{12}^{''}\right] \\ &\leq Tr_{12}\left[exp\left(log\rho_1+log\rho_{12}-log\rho_1\right)-\rho_{12}\right]=0 \qquad (3.7)\end{aligned}$$

eşitsizliği bulunur. (3.7) bağıntısı $\Delta$'ya; pozitif bir $C$'nin, $K=log\rho_{12}-log\rho_1$ ile $\rho_1=\alpha\rho_1^{'}+(1-\alpha)\rho_1^{''}$ denklemine $C\mapsto Tr\left[exp\left(K+logC\right)\right]$ şeklinde etki etmesi ile ikinci eşitsizlik ortaya çıkartılır.

**Teorem 3.2: [Güçlü Alt-toplanabilirlik]:** $\mathscr{H}_{123}=\mathscr{H}_1\otimes\mathscr{H}_2\otimes\mathscr{H}_3$ olmak üzere $\rho_{123}$, $\mathscr{H}_{123}$ üzerinde tanımlı bir yoğunluk işlemcisi

$$S(\rho_{123})+S(\rho_2)-S(\rho_{12})-S(\rho_{23})\leq 0 \qquad (3.8)$$

ve

$$S(\rho_1)+S(\rho_3)-S(\rho_{12})-S(\rho_{23})\leq 0 \qquad (3.9)$$

özelliklerine sahiptir.
Gelinen aşamada ilk olarak (3.8) ve (3.9) denklemlerinin birbirlerine denk olduğu gösterilecektir. Bu bağlamda verilen her iki denklemin de ayrı ayrı ispatlanmasında fayda vardır.
**İspat:(Teorem 3.2):**

**(i):[(3.8) Denklemi]:** $A=\rho_{123}$ ve $B=exp\left(-log\rho_2+log\rho_{12}+log\rho_{23}\right)$ seçimiyle Klein eşitsizliği kullanıldığında,

$$\begin{aligned}F\left(\rho_{123}\right) &\equiv S(\rho_{123})+S(\rho_2)-S(\rho_{12})-S(\rho_{23}) \\ &\leq Tr_{123}\left[exp\left(log\rho_{12}-log\rho_2+log\rho_{23}\right)-\rho_{123}\right]. \qquad (3.10)\end{aligned}$$

bağıntısı elde edilir. Golden-Thompson eşitsizliğinin[11] (C.J.Thompson 1965, S.Golden

[11]Hermite-sel olan A ve B için $Tre^{A+B}\leq Tre^{A}e^{B}$ olarak yazılır.

1965) genelleştirilmiş hali

$$Tr\left[exp\left(logB-logC+logD\right)\leq Tr\int_{0}^{\infty}B\left(C+xI\right)^{-1}D\left(C+xI\right)^{-1}dx\right] \tag{3.11}$$

(3.10) eşitsizliğine uygulanırsa,

$$\begin{aligned} F\left(\rho_{123}\right) &\leq Tr_{123}\left[\int_{0}^{\infty}\rho_{12}\left(\rho_{2}+xI\right)^{-1}\times\rho_{23}\left(\rho_{2}+xI\right)^{-1}dx-\rho_{123}\right] \\ &= Tr_{2}\int_{0}^{\infty}\rho_{2}\left(\rho_{2}+xI\right)^{-1}\rho_{2}\left(\rho_{2}+xI\right)^{-1}dx-Tr_{123}\rho_{123} \\ &= Tr_{2}\rho_{2}-Tr_{123}\rho_{123}=0 \end{aligned} \tag{3.12}$$

sonucu ortaya çıkar.

**(ii):[(3.9) Denklem]:** (3.9) denkleminin sol tarafı $G(\rho_{123})$'dir. $\rho_{12}$ ve $S(\rho_1)-S(\rho_{12})$, $\rho_{123}$ üzerinde çizgisel olduğundan Teorem 3.1 kullanılarak, $S(\rho_1)-S(\rho_{12})$ bağıntısının $\rho_{123}$ üzerinde konveks olduğu söylenir. Böylece $G\left(\rho_{123}\right)$, $\rho_{123}$ üzerinde konvekstir denir.

Pozitif matrislerin konveks konisinde, uçlardaki ışınlar, $\alpha\geq 0$ ve $P$ tek-boyutlu bir projeksiyon olmak üzere, $\rho=\alpha P$ formundaki matrislerden meydana gelir. Eğer $\rho_{123}$ bu koninin uç kısmında ise, $S(\rho_1)=S(\rho_{23})$ ve $S(\rho_3)=S(\rho_{12})$ ve dolayısıyla $G\left(\rho_{123}\right)=0$ elde edilir. Her pozitif matris $\rho_{123}$, uç matrislerin konveks kombinasyonu şeklinde yazılarak $G$'nin konveksliğinden dolayı $G\left(\rho_{123}\right)\leq 0$ bulunur.

Teorem 3.1'in, Teorem 3.2'yi beraberinde getirdiği, (3.9) ifadesinin ispatında gösterilmiştir. Bunun tersinin de doğru olduğu aşikardır. Gelinen aşamada Teorem 3.1 ve 3.2 için alternatif ispatlar yapılarak, $F\left(\rho_{123}\right)$'ün konveks olmadığı ve ayrıca Teorem 3.1 için bir sonuç gösterilecektir.

Teorem 3.1 kullanılarak Teorem 3.2'nin çıkarılabileceğini göstermek için (3.8)'in (3.9) eşitsizliğine denk olduğu bilgisi kullanılacaktır. $\rho_{123}=\alpha\rho_{12}^{'}\otimes E_3+(1-\alpha)\rho_{12}^{''}\otimes F_3$ özel seçiminde $\mathscr{H}_3$ iki boyutlu, $E_3$ ile $F_3$ ortogonal ve $\mathscr{H}_3$ üzerinde tanımlı tek-boyutlu projeksiyonlar olarak alınarak bu denklik sağlanır.

Uhlmann (A.Uhlmann 1977) (3.8) eşitsizliğinin $C \mapsto Trexp(K + logC)$ konkavlığı ile elde edileceğini göstermiş, bunun doğruluğu ilk olarak Lieb (E.H.Lieb 1973) tarafından, alternatif bir ispatı ise Epstein (H. Epstein 1973) tarafından ortaya konulmuştur.

(3.9) bağıntısının ispatı, Teorem 3.1'in Teorem 3.2'yi ortaya çıkardığını gösterir. Fakat (3.3), (3.9) eşitsizliğine, başka kavramlar içerisinde denk değildir ve (3.9) klasik sürekli durumlarda yanlış olur. Yani, Teorem 3.1'in, (3.9) eşitsizliğini kullanmaksızın, direkt olarak (3.8) bağıntısından çıkarılabildiği anlaşılır. Bu aşamada Baumann ve Jost (Baumann ve Jost 1969) (3.3)'da $\rho_{12}^{'}$ ve $\rho_{12}^{''}$ için özel $A$ ile $C$ matris ve $C > 0$ seçimiyle, $(A,C)$ içerisinde $Tr\int_0^\infty A^*(C+xI)^{-1}A(C+xI)^{-1}dx$ bileşik konveks olduğunu göstermiştir. Takip eden aşamada Lieb ise durum $C \mapsto Trexp(K + logC)$'nin $C$ içerisinde konkav olduğu sonucuna ulaşmıştır. Bu son durum (3.8)'in ortaya çıkmasını sağlayan (3.11) eşitsizliğinin ispatında kullanılır. Alternatif olarak, üstte belirtildiği gibi $C \mapsto Trexp(K + logC)$'nin konkavlığı (3.8) bağıntısını ortaya çıkarır.

Böylece (3.9) eşitsizliğin sol tarafının, $G(\rho_{123})$, konveks olduğu gösterilmiştir. Buna benzer şekilde; (3.8) eşitsizliğin sol tarafının da konveks olup olmadığı kontrol edilerek, konveks olmadığı ispatlanabilir. Eğer konveks olsaydı, $\mathscr{H}_2$ tek-boyutlu seçildiği durumda

$$F(\rho_{123}) = S(\rho_{13}) - S(\rho_1) - S(\rho_3) \equiv E(\rho_{13}) \tag{3.13}$$

denklemi $\rho_{13}$'ün bir konveks fonksiyonu olarak yazılabilirdi. $\mathscr{H}_1$ ve $\mathscr{H}_3$ iki boyutlu ve $\rho_{13}^{'}$ ile $\rho_{13}^{''}$ tek-boyutlu, ortogonal projeksiyonlar ve $i_1$, $i_3$, $j_1$ ve $j_3$; $\rho_{13}^{'}$ ile $\rho_{13}^{''}$'e ait bazlar olmak üzere

$$\rho_{13}^{'}(i_1,i_3;j_1,j_3) = \frac{1}{2}\delta(i_1,i_3)\,\delta(j_1,j_3) \tag{3.14}$$

ve

$$\rho_{13}^{''}(i_1,i_3;j_1,j_3) = \frac{1}{2}[1-\delta(i_1,i_2)][1-\delta(j_1,j_3)] \tag{3.15}$$

şeklinde alınarak

$$\rho_1^{'} = \rho_1^{''} = \frac{1}{2}I_1 \; ve \; \rho_3^{'} = \rho_3^{''} = \frac{1}{2}I_3 \tag{3.16}$$

bulunur. Dolayısıyla

$$E\left(\rho_{13}^{'}\right)+E\left(\rho_{13}^{''}\right)-2E\left(\frac{1}{2}\rho_{13}^{'}+\frac{1}{2}\rho_{13}^{''}\right)=-2log2<0 \tag{3.17}$$

biçimindedir. Bu durumun ise bir çelişki ortaya çıkardığı aşikardır.

Yukarıda verildiği gibi eğer $f(A)$, $\mathbb{R}$ üzerinde tanımlı pozitif matrisler kümesinden konveks ve homojen[12] bir fonksiyon ise;

$$\frac{d}{dx}f(A+xB)\,|_{x=0}\equiv lim_{x\to 0}x^{-1}\left[f(A+xB)-f(A)\right]\leq f(B) \tag{3.18}$$

ilişkisi elde edilir. Burada $A$ ve $B$'nin pozitif matrisler ve $f(A+xB)$'nin verilen noktada limitinin var olduğu kabul edilmiştir. $(S(\rho_1)-S(\rho_{12}))(\rho_{12})$ fonksiyonu da bu özelliklere sahiptir. (3.18) bağıntısı $(S(\rho_1)-S(\rho_{12}))(\rho_{12})$ fonksiyonuna uygulanırsa;

$$\begin{aligned}\frac{d}{dx}S(\rho+x\gamma) &= -\frac{d}{dx}Tr\left[(\rho+x\gamma)log(\rho+x\gamma)\right]\\ &= -Tr\gamma log(\rho+x\gamma)-Tr\gamma\end{aligned} \tag{3.19}$$

ifadesine ulaşılır. Bu bilgiler ışığında şu sonuç elde edilmiştir:

**Lemma 3.3:** $\gamma_{12}$ ve $\rho_{12}$, $\mathscr{H}_{12}$ üzerinde tanımlı pozitif, iz-sınıflı matrisler olmak üzere, sabitlenmiş her $\gamma_{12}$ için

$$Tr_{12}\gamma_{12}log\rho_{12}-Tr_1\gamma_1log\rho_1\leq Tr_{12}\gamma_{12}log\gamma_{12}-Tr_1\gamma_1log\gamma_1 \tag{3.20}$$

olur. (3.20) eşitsizliğin sol tarafı maksimum değerine $\rho_{12}=\gamma_{12}$ durumunda ulaşır. Verilen ispat sonlu boyutlu uzaylar için yapılmıştır.

### 3.2 Nielsen-Petz İspatı

Klasik olarak, von Neumann entropisi Shannon entropi fonksiyonu ile yer değiştirdiğinde; koşullu entropi, bilinen B durumunda A durumu hakkındaki ortalama belirsizlik olarak yorumlanır. Bu yorum kuantum bilişim kuramında daha sorunlu olsa da - kuantum

[12][Her $\lambda>0$ için $f(\lambda A)=\lambda f(A)$].

koşullu entropi negatif olabileceğinden - yeni yorumlar ve sonuçlar ortaya çıkarmak için faydalıdır. Özellikle, GaT bağıntısının

$$S(A|BC) \leq S(A|B) \tag{3.21}$$

şeklinde yeniden yazılabileceğinden hareketle; $B$ ve $C$ bilindiğinde $A$ hakkındaki belirsizliğin sadece $B$ bilindiğindeki durumdan daha fazla olmayacağı anlaşılmaktadır. Bu yorum GaT bağıntısının inceliklerinin daha iyi görünmesini sağlar.

Çalışmanın bu aşamasında bağıl entropinin monotonluğunun GaT bağıntısını ortaya çıkardığı gösterilecektir. $D(\rho\|\sigma)$ entropisi simetrik değildir ve eğer $\rho$'nun desteği (*support*), $\sigma$'nın desteğini içermiyorsa $D(\rho\|\sigma)$ ıraksak olur. Bağıl entropinin monotonluğu, bir $AB$ bileşik sisteminin bir kısmı atıldığında, $\rho_{AB}$ ve $\sigma_{AB}$ yoğunluk matrisleri arasındaki bağıl entropi artış göstermez ve bu durum

$$D(\rho_A\|\sigma_A) \leq D(\rho_{AB}\|\sigma_{AB}) \tag{3.22}$$

bağıntısı ile temsil edilir. GaT bağıntısını bağıl entropi cinsinden yazıp,

$$S(B|A) = logd_B - D\left(\rho_{AB}\middle\|\rho_A \otimes \frac{I_B}{d_b}\right) \tag{3.23}$$

eşitliği kullanılarak GaT bağıntısı koşullu entropi formunda yazılabilir ve bu durum (3.21) eşitsizliği ile denk bir yapıya sahip olur:

$$D\left(\rho_{AB}\middle\|\frac{I_A}{d_A}\otimes\rho_B\right) \leq D\left(\rho_{ABC}\middle\|\frac{I_A}{d_A}\otimes\rho_{BC}\right). \tag{3.24}$$

Varsayılsın ki $I$ gerçel bir aralık, $I \subseteq \mathbb{R}$, ve $f : I \to \mathbb{R}$, $I$ üzerinde tanımlı gerçel değerli bir fonksiyon olsun. Buna karşılık gelen $f : M_n \to M_n$ gönderimi tanımlanabilir. Burada $M_n$; $n \times n$ spektrumları $I$'da olan Hermite-sel matrislerin uzayını temsil eder. Böyle bir gönderim tanımlamak için; $d_1, d_2, ..., d_n \in I$ gerçel köşegen elemanlarına sahip $n \times n$ bir $D$ matrisi ele alınsın. Böylece köşegen elemanları $f(d_1), f(d_2), ..., f(d_n)$ olan $n \times n$ köşegen matris $f(D)$ tanımlanabilir. Bu tanımın genelleştirilmesi açısından; eğer $X$, $M_n$'nin herhangi bir elemanı ise, üniter bir $U$ ve köşegen matris $D$ için $X = UDU^\dagger$ yazılabilir. İndirgenmiş gönderim ise $f\left(UDU^\dagger\right) \equiv Uf(D)U^\dagger$ kullanılarak $f : M_n \to M_n$ şeklinde tanımlanır. Başka bir deyiş ile, $X$'in köşegen olduğu bir baz üzerinde işlem yapılır ve $f$ her

köşegen girdiye uygulanır. $X$'in, $X = UDU^{\dagger}$ olarak farklı şekillerde çarpanlarına ayrıldığı durumlarda, $f(X)$ seçilen ayrışımdan bağımsızdır.

Operatör konveksliği tanımlamak için, Hermite-sel matrisler üzerinde kısmi sıralamayı (*partial ordering*) bilmek gereklidir. Verilen $X, Y \in M_n$ Hermite-sel matrisler ile, eğer $Y - X$ pozitif bir matris ise $X \leq Y$ olarak tanımlanır. Eğer her $n$, her $X, Y \in M_n$ ve her $p \in [0,1]$ için $f : I \to \mathbb{R}$ fonksiyonu

$$f(pX + (1-p)Y) \leq pf(X) + (1-p)f(Y) \tag{3.25}$$

eşitsizliğini sağlıyor ise $f$ operatör konvekstir denir.

İspat sırasında kullanılacak olan operatör konvekslik ile ilgili bilgiler şu şekildedir:

**Lemma 3.4:** $f(x) = -logx$ fonksiyonu operatör konvekstir.

**Lemma 3.5:** $f$ operatör konveks ve $U : V \to W$ bir izometri[13] ($dim(V) \leq dim(W)$) olmak üzere, her $X$ için $f\left(U^{\dagger}XU\right) \leq U^{\dagger}f(X)U$ olur.

Monotonluğun ispatında kullanılan fikirlerin öneminin daha iyi anlaşılabilmesi açısından bunların klasik sonuçlarına bakılması gerekir. Bu bağlamda, iki değişkenli $r_{jk}$ ve $s_{jk}$ olasılık dağılımları için $r_j \equiv \sum_k r_{jk}$ ve $s_j \equiv \sum_k s_{jk}$ terimleri marjinal olasılık dağılımları olmak üzere,

$$\sum_j r_j \left(logr_j - logs_j\right) \leq \sum_{jk} r_{jk} \left(logr_{jk} - logs_{jk}\right) \tag{3.26}$$

şeklinde bulunur. (3.26) eşitsizliğinin

$$\sum_{jk} r_{jk} log \frac{r_j s_{jk}}{r_{jk} s_j} \leq 0 \tag{3.27}$$

ifadesine denk olduğu anlaşılmaktadır.

Kuantum bilişim kuramındaki zorluk ise yoğunluk matrislerinin dahil olduğu durumların sıra-değişmemesinden kaynaklanır ve bu onları aynı logaritma altında tutar. Bu zorluğun üstesinden gelmek için *bağıl modüler operatör* olarak bilinen matrisler üzerinde tanımlı

[13] Norm koruyan dönüşüm.

çizgisel gönderim kullanılarak bağıl entropi $S(\rho \,\|\sigma\,)$ yeniden tanımlanmalıdır[14]. Sonuç olarak bağıl entropinin monotonluğu ve GaT bağıntısının ispatı sadece tersinir yoğunluk matrisleri için uygulanabilirdir. Genel sonuç süreklilik bağıntısının basit bir sonucundan ortaya çıkar.

Bağıl modüler operatörü tanımlamak için, $\rho$ ve $\sigma$ sabitlenerek $\mathscr{L}(X) \equiv \sigma X$ ve $\mathscr{R}(X) \equiv X\rho^{-1}$ ile matrisler üzerinde $\mathscr{L}$ ve $\mathscr{R}$ çizgisel gönderimleri tanımlanır. Bağıl modüler operatör, $\Delta \equiv \mathscr{L}\mathscr{R}$ birleşimi altında bu çizgisel gönderimlerin çarpımı olarak alınır. Burada $\mathscr{L}$ ve $\mathscr{R}$ daima sıra-değişir. Böylelikle $\Delta = \mathscr{R}\mathscr{L}$ yazılabilir.

Bir sonraki adımda matrisler üzerinde tanımlanan çizgisel gönderimlerdeki $log$ fonksiyonu kullanılacaktır. Hilbert-Schmidt iç çarpımına göre $\left[\langle X,Y\rangle \equiv Tr\left(X^{\dagger}Y\right)\right]$ kesin pozitif olan matrisler üzerinde bir $\mathscr{E}$ çizgisel gönderim ile $log\,(\mathscr{E})$ verilebilir. Operatör konveks fonksiyonlarda bahsedildiği şekilde bir yaklaşım sergileyerek, bir köşegen baz üzerinde $\mathscr{E}$, $\mathscr{E} = \sum_j \lambda_j \mathscr{E}_j$ olarak genişletilir ve $log\,(\mathscr{E}) \equiv \sum_j log\left(\lambda_j\right)\mathscr{E}_j$ biçiminde tanımlanır.

Bununla birlikte $log\,(\mathscr{L})$, $log\,(\mathscr{R})$ ve $log\,(\Delta)$ ifadeleri elde edilebilir. Dolayısıyla $\mathscr{L}$, $\mathscr{R}$ ve $\Delta$ Hilbert-Schmidt iç çarpımına[15] göre kesin pozitif olurlar. $\mathscr{L}$'nin kesin pozitif olduğunu görmek amacıyla, sıfır olmayan her $X$ değeri için $\langle X, \mathscr{L}(X)\rangle = Tr\left(X^{\dagger}\sigma X\right) > 0$ ilişkisini göstermek yeterlidir. $\mathscr{R}$'nin kesin pozitifliği benzer işlem adımları takip edilerek gösterilir. Son olarak; $\Delta$ matrisler üzerinde tanımlanan kesin pozitif ve sıra-değişen çizgisel gönderimlerin bir çarpımı olduğundan kesin pozitiftir.

Burada $log\,(\mathscr{L})\,(X) = log\,(\sigma)\,X$ ve $log\,(\mathscr{R})\,(X) = -X log\,(\rho)$ olacağı görülmektedir. Ayrıca $\mathscr{L}$ ve $\mathscr{R}$ sıra değiştiğinden, $log\,(\Delta) = log\,(\mathscr{L}) + log\,(\mathscr{R})$ eşitliğini veren bağıntı elde edilir. Bunların bir sonucu olarak,

$$D\,(\rho \,\|\sigma\,) = \left\langle \rho^{1/2}, -log\,(\Delta)\left(\rho^{1/2}\right)\right\rangle \tag{3.28}$$

eşitliğine ulaşılır.

Bağıl modüler operatör sayesinde; bağıl entropinin tanımında kullanılan logaritmalar, tek bir logaritma altında toplanarak analizin kolaylaştırılmasını sağlar. (3.28) denklemi kullanılarak, bağıl entropinin monotonluğu

[14] Bu işlemde $\rho$ ve $\sigma$'nın tersinir olduğu kabul edilir.

[15] Hilbert-Schmidt iç çarpımı için EK 3 kısmı incelenebilir.

$$\left\langle \rho_A^{1/2}, -log\left(\Delta_A\right)\left(\rho_A^{1/2}\right)\right\rangle \leq \left\langle \rho_{AB}^{1/2}, -log\left(\Delta_{AB}\right)\left(\rho_{AB}^{1/2}\right)\right\rangle \tag{3.29}$$

şeklinde yeniden yazılabilir. (3.29)'un sol tarafındaki iç çarpım $A$'ya etki eden $M(A)$ uzayında, sağ tarafındaki iç çarpım ise $AB$'ye etki eden $M(AB)$ uzayında tanımlıdır. $\Delta_A(X) \equiv \sigma_A X \rho_A^{-1}$ ile $\Delta_{AB} \equiv \sigma_{AB} X \rho_{AB}^{-1}$ doğal bağıl modüler operatörleri sırasıyla $A$ ve $AB$ sistemleri üzerindedir.

İspatın son adımında; $\mathscr{U} : M(A) \to M(AB)$ matrisleri üzerinde tanımlı bir çizgisel gönderim bulunarak aşağıdaki üç adımın gösterilmesi yeterlidir:

(1) $\mathscr{U}^\dagger \Delta_{AB} \mathscr{U} = \Delta_A$,
(2) $\mathscr{U}\left(\rho_A^{1/2}\right) = \rho_{AB}^{1/2}$,
(3) $\mathscr{U}$, $M(A)$'dan $M(AB)$'ye bir izometridir.

Böyle bir $\mathscr{U}$'nun varlığı yeterince açık değildir. $\mathscr{U}$'nun açık bir şekilde ortaya konulabilmesi açısından ilk aşamada $\mathscr{U}$'nun varlığı kabul edilerek ve sonuçları gözlemlenecektir. (3.29) ifadesi kullanılarak bağıl entropinin monotonluğu

$$\left\langle \rho_A^{1/2}, -log\left(\mathscr{U}^\dagger \Delta_{AB} \mathscr{U}\right)\left(\rho_A^{1/2}\right)\right\rangle \leq \left\langle \rho_{AB}^{1/2}, -log\left(\Delta_{AB}\right)\left(\rho_{AB}^{1/2}\right)\right\rangle \tag{3.30}$$

şeklinde yeniden yazılabilir. Lemma 3.4 ve 3.5'ten faydalanılarak $-log\left(\mathscr{U}^\dagger \Delta_{AB} \mathscr{U}\right) \leq -\mathscr{U}^\dagger log\left(\Delta_{AB}\right) \mathscr{U}$ yazılır. Böylelikle monotonluğun ispatı tamamlanmış olur:

$$\begin{aligned}
\left\langle \rho_A^{1/2}, -log\left(\mathscr{U}^\dagger \Delta_{AB} \mathscr{U}\right)\left(\rho_A^{1/2}\right)\right\rangle &\leq \left\langle \rho_A^{1/2}, -\mathscr{U}^\dagger log\left(\Delta_{AB}\right) \mathscr{U}\left(\rho_A^{1/2}\right)\right\rangle \\
&= \left\langle \mathscr{U}\left(\rho_A^{1/2}\right), -log\left(\Delta_{AB}\right) \mathscr{U}\left(\rho_{AB}^{1/2}\right)\right\rangle \\
&= \left\langle \rho_{AB}^{1/2}, -log\left(\Delta_{AB}\right) \rho_{AB}^{1/2}\right\rangle .
\end{aligned} \tag{3.31}$$

Gelinen aşamada yukarıda verilen üç adımı sağlayan bir $\mathscr{U}$ bulunabilir. (EK 1.12) öncülüne dayanarak

$$\mathscr{U}(X) \equiv \left(X \rho_A^{-1/2} \otimes I_B\right) \rho_{AB}^{1/2} \tag{3.32}$$

eşitliği yazılır. Bu tanım ile birlikte, $\mathscr{U}$'nun Hermite-sel eşleniğine göre $\left\langle \mathscr{U}^{\dagger}(Y), X \right\rangle = \langle Y, \mathscr{U}(X) \rangle$ eşitliğinin ve her $X \in M(A)$ ile $Y \in M(AB)$ için $\left\langle \mathscr{U}^{\dagger}(Y), X \right\rangle = \langle Y, \mathscr{U}(X) \rangle$ denkleminin sağladığı gösterilir. Sonuç olarak $\mathscr{U}^{\dagger}\Delta_{AB}\mathscr{U} = \Delta_A$ ve $\mathscr{U}^{\dagger}\mathscr{U} = \mathscr{I}_{\mathscr{A}}$ eşitlikleri elde edilerek yukarıda belirtilen öncüllerin ve monotonluğun ispatı tamamlanmıştır.

Monotonluğun bu ispatı $f(x) = -logx$ fonksiyonunun operatör konveksliğinin rolünü ortaya çıkarır. Eğer $f$ herhangi bir operatör konveks fonksiyon ve

$$D_f(\rho \| \sigma) \equiv \left\langle \rho^{1/2}, f(\Delta)\left(\rho^{1/2}\right) \right\rangle \tag{3.33}$$

tarafından tanımlanan bir $f$-bağıl entropi ise, bunlara paralel bir monotonluk özelliği çıkarılabilir.

### 3.3 Hayden-Jozsa-Petz-Winter İspatı

Eğer $\mathscr{X}$ kümesi $\mathscr{H}_{\mathscr{X}}$'nin bir ortonormal bazını $\{|x\rangle : x \in \mathscr{X}\}$ etiketliyor ise $\rho_P$ durumu $P$ olasılık dağılımına göre

$$\rho_P = \sum_x P(x) |x\rangle \langle x| \tag{3.34}$$

şeklinde tanımlanır. Bu dağılımdan durumlara bir küçük (*affine*) gönderim tanımlanarak $S(\rho_P) = H(P)$ bağıntısı çıkarılır. Böylelikle, tek-parçalı bir sistemin von Neumann entropisinin bütün özellikleri, tek-dağılım için tanımlanan Shannon entropisi için de geçerli olur.

Benzer şekilde, $\mathscr{X} \times \mathscr{Y}$ kartezyen çarpımındaki bir $P$ bileşik olasılık dağılımı için, bazların tensör çarpımları

$$\{|xy\rangle = |x\rangle \otimes |y\rangle : x \in \mathscr{X}, y \in \mathscr{Y}\} \tag{3.35}$$

kullanılarak $\mathscr{H}_{\mathscr{X}} \otimes \mathscr{H}_{\mathscr{Y}}$ üzerinde $\rho_P$ tanımlanabilir. Marjinalleri alınmış haline denk gelen indirgenmiş durumlar

$$Tr_Y(\rho_P) = \rho_{P|x}\ ,\ Tr_X(\rho_P) = \rho_{P|y} \tag{3.36}$$

biçiminde yazılabilir. İki-parçalı durumlar için sağlanan bütün entropi ilişkileri, aynı zamanda iki-parçalı dağılımlar için de geçerlidir. $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ sistemi üzerinde tanımlanan üç-parçalı $\rho_{ABC}$ durumu için (3.8) eşitsizliğinin ispatı Bölüm 3.1'de yapılmıştır. Bu

bağlamda $B : \mathscr{H}_B = \mathbb{C}$ sistemi için ortaya çıkarılmış önceki alt-toplanabilirlik bağıntısını geneller.

Gelinen aşamada GaT bağıntısının eşitlik koşulunu sağlayan durumlar incelenecektir. Bu kapsamda; bir kuantum sisteminin alt-sistemlerinden birinin atılması durumunda geri kalan sistemin entropi ilişkisini bağıl entropi cinsinden yazılacak GaT bağıntısı açıklar. Öyle ki bu durum sistemin sadece çevre ile olan korelasyonu bozar.

(2.15) denkleminden yola çıkarak, iki-parçalı bir sistem olan $\rho_{AB}$ için (2.47) ve (2.48) denklemlerinin farkları alınıp, (2.18) zincir kuralı da kullanıldığında $I(A:C|B)$ kuantum koşullu karşılıklı bilişim:

$$D(\rho_{ABC}\|\rho_A\otimes\rho_{BC}) - D(\rho_{AB}\|\rho_A\otimes\rho_B) = S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_B) \quad (3.37)$$

şeklinde elde edilir. (3.37) bağıntısının denklemin sağ tarafı GaT bağıntısından kaynaklı olarak negatif olamaz. Sol taraf ise $\rho = \rho_{ABC}$ ve $\sigma = \rho_A \otimes \rho_{BC}$, $\mathscr{T} = Tr_C\ \mathscr{H}_C$ üzerinde tanımlı bir kuantum kanal olmak üzere, $D(\rho\,\|\sigma) - D(\mathscr{T}\rho\,\|\mathscr{T}\sigma)$ biçiminde yazılır. Burada $\mathscr{T} = id_{AB}\otimes Tr$ bir çizgisel gönderimdir. Uhlmann teoremi[16] kullanılarak $\mathscr{H}$ uzayı üzerinde tanımlanan $\rho$ ve $\sigma$ durumları ve $\mathscr{T} : \mathscr{B}(\mathscr{H}) \to \mathscr{B}(\mathscr{K})$ kuantum işlemleri için

$$D(\rho\,\|\sigma) \geq D(\mathscr{T}\rho\,\|\mathscr{T}\sigma) \quad (3.38)$$

eşitsizliği elde edilir. Böylelikle, Uhlmann teoreminin GaT bağıntısını elde etmek için uygun bir yol olduğu görülür.

Üst kısımda detaylandırılan GaT bağıntısının kısmi-iz tanımı kullanılarak bağıl entropi cinsinden yazımında eşitlik durumundan bahsedilecektir. (3.38) eşitsizlikteki gibi bir kuantum kanal olan $\hat{T}$; $(\mathscr{T}\rho)$'dan $\rho$ ve $(\mathscr{T}\sigma)$'yı $\sigma$'ya götüren bir gönderim olsun.

**Teorem 3.7:** $\rho$ ve $\sigma$ durumları için, ancak ve ancak

$$\hat{T}T\rho = \rho\ ,\ \hat{T}T\sigma = \sigma \quad (3.39)$$

eşitliklerini sağlayan bir $\hat{T}$ kuantum kanal var ise,

[16](2.22 bağıntısı)

$$D(\rho\,\|\sigma) = D(T\rho\,\|T\sigma) \tag{3.40}$$

eşitliği sağlanır. Burada, $(T\sigma)$'nın desteği üzerinde, $\hat{T}$ kanalı,

$$\hat{T}\alpha = \alpha^{1/2}T^*\left((T\sigma)^{-1/2}\alpha\,(T\sigma)^{-1/2}\right)\sigma^{1/2} \tag{3.41}$$

formülü ile açıklanır. $T^*$, $T$'nin Hermite-sel eşleniği olmak üzere eğer $T(\alpha) = \sum_i A_i \alpha A_i^*$ ise

$$T^*(X) = \sum_i A_i^* X A_i \tag{3.42}$$

şeklindedir. (3.41) denkleminde tanımlanan $\hat{T}$, $\sigma$'ya bağlıdır. Dolayısıyla direkt olarak $\hat{T}T\sigma = \sigma$ eşitliği sağlanmış olur.

### 3.4 Petz İspatı[17]

Kuantum bilişim kuramı kapsamında GaT bağıntısının bir diğer ispatı Petz tarafından ortaya koyulmuştur. Bu bağlamda ilk olarak $exp(log\rho_{AB} - log\rho_B + log\rho_{BC})$ pozitif işlemcisi $\omega$ yoğunluk matrisi cinsinden $\lambda\omega$ şeklinde yazılarak;

$$\begin{aligned} S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_B) &= Tr\rho_{ABC}\,(log\rho_{ABC} - (log\rho_{AB} - log\rho_B + log\rho_{BC})) \\ &= S(\rho_{ABC}\,\|\lambda\omega) = S(\rho_{ABC}\,\|\omega) - log\lambda \end{aligned} \tag{3.43}$$

eşitlikleri elde edilir. Denklemin sol tarafının pozitifliği açısından $\lambda \leq 1$ koşulu yeterlidir. Golden-Thompson eşitsizliği göz önüne alınarak[18]

$$Tr\left[exp\,(log\rho_{AB} - log\rho_B + log\rho_{BC})\right] \leq \int_0^\infty Tr\rho_{AB}\,(tI+\rho_B)^{-1}\,\rho_{BC}\,(tI+\rho_B)^{-1}\,dt \tag{3.44}$$

bağıntısına ulaşılır. (3.44) ifadesine kısmi-iz bağıntısı uygulanırsa

$$Tr\rho_{AB}\,(tI+\rho_B)^{-1}\,\rho_{BC}\,(tI+\rho_B)^{-1} = Tr\rho_B\,(tI+\rho_B)^{-1}\,\rho_B\,(tI+\rho_B)^{-1} \tag{3.45}$$

[17] D. Petz, Quantum Information Theory and Quantum Statistics kitabından faydalanılmıştır.
[18] D. Petz, Quantum Information Theory and Quantum Statistics sayfa 199

eşitliği bulunarak iki tarafın da integrali alınırsa şu bağıntı elde edilir:

$$\int_0^\infty Tr\rho_{AB}\left(tI+\rho_B\right)^{-1}\rho_{BC}\left(tI+\rho_B\right)^{-1}dt = Tr\rho_B = 1 \tag{3.46}$$

Böylece 3.44 eşitsizliğinden $\lambda \leq 1$ bulunur ve GaT bağıntısı ispatlanmış olur. GaT bağıntısının eşitliği durumunda, gerek ve yeter koşul olarak
$S(B|A) = exp\left(log\rho_{AB} - log\rho_B + log\rho_{BC}\right)$ alınması durumunda

$$S\left(\rho_{ABC}\,\|exp\left(log\rho_{AB} - log\rho_B + log\rho_{BC}\right)\right) = 0 \tag{3.47}$$

ve bu

$$log\rho_{ABC} = log\rho_{AB} - log\rho_B + log\rho_{BC} \tag{3.48}$$

eşitliğini ortaya çıkarır.

Bu bölümde gösterilen dört farklı çalışma sonucunda ispatlanan GaT bağıntısı yeni soruların ve gelişmelerin önünü açmıştır. Sonuçta ortaya çıkan en önemli ve cevabı bir sonraki bölümde verilecek olan soru GaT bağıntısının eşitlik durumunu sağlayan yoğunluk işlemcilerinin açık yapısıdır. 3.48 ile ifade edilen bu durumlar Markov durumları olarak bilinirler.

# 4. MARKOV DURUMLARI

Bir önceki bölümde dört farklı yöntem ile GaT bağıntısının ispatı yapılmıştır. Bu bölümde ise GaT bağıntısının eşitlik koşulu olarak bilinen *Markov durumları* incelenecektir.

$\rho_{ABC}$, $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ üzerinde tanımlı bir durum olsun. Uhlmann teoreminin özelleştirdiği $\rho_{ABC}$ ile $\sigma_{ABC} = \rho_A \otimes \rho_{BC}$ durumları ve $T = Tr_C$ gönderiminin (2.47) ile verilen kuantum bağıl entropi ifadesinde kullanılması sonucunda

$$D(\rho_{ABC} \| \rho_A \otimes \rho_{BC}) \geq D(\rho_{AB} \| \rho_A \otimes \rho_B) \tag{4.1}$$

eşitsizliğine ulaşılır. Teorem 3.7 sayesinde $\hat{T}T\rho = \rho$ eşitlik koşulu sağlanır. $R_{BC} = id_B \otimes Tr_C$ sınırlandırılmış bir gönderim (*restriction map*), $T = id_A \otimes R_{BC}$ ve $\sigma$ bir tensör çarpım olmak üzere

$$\hat{T} = id_A \otimes \hat{R} \tag{4.2}$$

ifadesine ulaşılır[19]. Yukarıdaki monotonluk ve GaT bağıntısı göz önüne alındığında ancak ve ancak

$$\rho_{ABC} = \left(id \otimes \hat{R}\right) \rho_{AB} \tag{4.3}$$

durumunda eşitlik koşulunun sağlandığı görülür.

**Teorem 4.1:** $\rho_{ABC}$, $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ üzerinde tanımlı ve (3.35) GaT bağıntısını sağlasın. Eşitlik koşulu ise ancak ve ancak $B$ sisteminin ayrışımının direkt toplamlar cinsinden

$$\mathscr{H}_B = \bigoplus_j \mathscr{H}_{b_j^L} \otimes \mathscr{H}_{b_j^R} \tag{4.4}$$

şeklinde yazılması ile elde edilir. Öyle ki $\rho_{Ab_j^L}$, $\mathscr{H}_A \otimes \mathscr{H}_{b_j^L}$ ve $\rho_{b_j^R C}$, $\mathscr{H}_{b_j^R} \otimes \mathscr{H}_C$ üzerinde tanımlanırken

$$\rho_{ABC} = \sum_j q_j \rho_{Ab_j^L} \otimes \rho_{b_j^R C} \tag{4.5}$$

[19] Burada $\hat{R} = \hat{R}_{\rho_{BC}}$ olarak alınır.

eşitliği yazılabilir. Burada $\{q_j\}$ bir olasılık dağılımıdır.

**İspat:** İspatın gerekliliği kuantum Markov zinciri koşulu ile elde edilecektir. Kuantum kanal olan $\varphi = Tr_C \circ \hat{R}$ tanımlanırsa, Markov koşulu sayesinde

$$(id \otimes \varphi)\rho_{AB} = \rho_{AB} \tag{4.6}$$

eşitliği yazılabilir. $\mathscr{H}_A$ üzerinde verilen ve $0 \leq M \leq I$ koşulunu sağlayan bir $M$ işlemcisi ele alınsın. $\mu$ durumu $p = Tr(\rho_{AB}(M \otimes I))$ olmak şartı ile

$$p\mu = Tr_A(\rho_{AB}(M \otimes I)) \tag{4.7}$$

şeklinde tanımlanır. Eğer $p \neq 1$ ise (4.6) denklemi $\varphi(\mu) = \mu$ eşitliğini verir. $M$ işlemcisini çeşitlendirerek, invaryant kalan bir $\varphi$ için $\mathscr{H}_A$ üzerinde tanımlanan durumların bir $M$ ailesi bulunur. Böylelikle,

$$\mathscr{H}_B = \sum_j \mathscr{H}_{b_j^L} \oplus \mathscr{H}_{b_j^R} \tag{4.8}$$

ayrışımı elde edilir. Öyleyse, her $\mu \in M$ için

$$\mu = \sum_j q_j(\mu)\rho_j(\mu) \otimes \omega_j \tag{4.9}$$

yazılır. Burada $\rho_j(\mu)$ durumu $\mathscr{H}_{b_j^L}$ ve $\omega_j$ durumu ise $\mathscr{H}_{b_j^R}$ üzerinde tanımlanır. Bu bilgiler ışığında $\rho_{AB}$,

$$\rho_{AB} = \sum_j q_j \rho_{AB_j^L} \otimes \omega_{B_j^R} \tag{4.10}$$

şeklinde yapılandırılır. Bunu görmek için $\mathscr{H}_B$ üzerinde tanımlı bir kuantum kanal olan

$$P_0(\xi) = \sum_j Tr_{b_j^R}\left(\prod_j \xi \prod_j\right) \otimes \omega_j \tag{4.11}$$

terimi kullanılacaktır. Burada $\prod_j$ terimi, (4.8) denklemindeki $\mathscr{H}_{b_j^L} \otimes \mathscr{H}_{b_j^R}$ alt-uzayında tanımlı bir ortogonal projeksiyondur. $P_0$'ın duali olan $P_0^*$ terimi ise alt-cebir projeksiyonudur. Dolayısıyla, 0 ile $I$ arasında sınırlandırılmış rasgele $M$ ve $N$ işlemcileri için verilen

işlem adımları takip edilerek,

$$\begin{aligned} Tr\left(\rho_{AB}\left(M\otimes N\right)\right) &= pTr\left(\mu N\right) \\ &= pTr\left(P_0\left(\mu\right)N\right) \\ &= pTr\left(\mu P_0^*\left(N\right)\right) \\ &= Tr\left(\rho_{AB}\left(M\otimes P_0^*\left(N\right)\right)\right) \\ &= Tr\left(\left(\left(id\otimes P_0\right)\rho_{AB}\right)\left(M\otimes N\right)\right) \end{aligned} \tag{4.12}$$

ifadesine ulaşılmış olur. Gelinen aşamada çizgisellik göz önünde bulundurulduğunda bu eşitliğin $M\otimes N$ yerine alınacak her işlemci için sağlandığı söylenebilir. Sonuç olarak,

$$\left(id\otimes P_0\right)\xi = \sum_j Tr_{b_j^R}\left(\left(I\otimes\prod_j\right)\xi\left(I\otimes\prod_j^*\right)\right)\otimes\omega_j \tag{4.13}$$

ve

$$\rho_{AB} = \left(id\otimes P_0\right)\rho_{AB} \tag{4.14}$$

denklemleri gereğince (4.10) ortaya çıkar.

$\varphi$ kanalı ile ilişkili $\mathscr{E}$ durumunda olan bir çevre $\mathscr{H}_E$ ile temsil edilsin. $C$ sistemi üzerinden alınacak bir iz bağıntısı $\varphi$ terimini vereceğinden $\mathscr{H}_B\otimes\mathscr{H}_C\otimes\mathscr{H}_E$ üzerinde tanımlanan üniter bir $U$ için $\mathscr{H}_C$'de bulunan $|0\rangle$ vektörünü de içeren standart bazı kullanılarak

$$\hat{R}\left(\alpha\right) = Tr_E\left(U\left(\alpha\otimes|0\rangle\langle 0|\otimes\mathscr{E}\right)U^*\right) \tag{4.15}$$

eşitliği yazılır. $\mathscr{E} = \mathscr{H}_C\otimes\mathscr{H}_E$ olmak üzere $U$'nun bir formu,

$$U = \sum_j I_{H_{b_j^L}}\otimes U_j \tag{4.16}$$

şeklinde bulunabilir. Burada $U_j$, $H_{b_j^L}\otimes\mathscr{E}$ üzerinde tanımlı bir üniter dönüşümdür. (4.10) ve (4.16) ifadeleri kullanılarak

$$\begin{aligned}\rho_{ABC} &= \left(id_A \otimes \hat{R}\right)\rho_{AB} \\ &= Tr_E\left((I_A \otimes U)\,\rho_{AB}\,(I_A \otimes U^*)\right) \\ &= \sum_j q_j \rho_{AB_j^L} \otimes Tr_E\left(U\left(\omega_{b_j^R} \otimes |0\rangle\langle 0|\, U^*\right)\right) \\ &= \sum_j q_j \rho_{AB_j^L} \otimes \rho_{b_j^R C} \end{aligned} \tag{4.17}$$

eşitlikleri elde edilerek ispat tamamlanmış olur.

Sonuç olarak, GaT bağıntısının eşitlik koşulunu sağlayan bir $\rho_{ABC}$ sistemi için

$$I(A:C|B) = S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_{ABC}) - S(\rho_B) = 0 \tag{4.18}$$

denklemi yazılabilir. Burada $\rho_{AC}$ marjinal durumu ayrılabilirdir (*separable*). Tersine olarak, ayrılabilir her $\rho_{AC}$ durumu için $\rho_{ABC}$ gibi $I(A:C|B) = 0$ koşulunu sağlayan bir genişletilmişi vardır.

**Teorem 4.2 (D.Petz 2008):** Aşağıda verilen öncüller birbirlerine denktir.

***(i)*** von Neumann entropisinin GaT bağıntısının eşitlik koşulu sağlanır:

$$S(\rho_{ABC}) + S(\rho_B) = S(\rho_{AB}) + S(\rho_{BC}) \tag{4.19}$$

***(ii)*** $\tau_A$, $B(H_A)$[20] uzayında tanımlı bir durum olmak üzere,

$$S(\rho_{ABC}\,\|\,\tau_A \otimes \rho_{BC}) = S(\rho_{AB}\,\|\,\tau_A \otimes \rho_B) \tag{4.20}$$

eşitliği sağlanır.

***(iii)*** $\mathscr{A}$ bir alt-cebir ve $B(\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C)$ uzayından seçilen bir koşullu beklenti (*conditional expectation*) $\mathscr{A}$ üzerinde olma durumunda; $\mathbb{C}I_B$ ve $\mathbb{C}I_C$, sırasıyla $B$ ve $C$ sistemlerinin Hilbert uzaylarında tanımlı $n \times n$ hermite-sel matrisleri olmak üzere,

[20] $B(H_A)$ sonlu boyutlu Hilbert uzayıdır.

$$B(\mathscr{H}_A)\otimes\mathbb{C}I_B\otimes\mathbb{C}I_C\subset\mathscr{A}\subset B(\mathscr{H}_A)\otimes B(\mathscr{H}_B)\otimes\mathbb{C}I_C \tag{4.21}$$

şeklinde yazılabilir ve $E$, $\rho_{ABC}$ durumunu invaryant bırakır.

***(iv)*** Genellenmiş koşullu beklenti

$$E_\rho : B(\mathscr{H}_A\otimes\mathscr{H}_B\otimes\mathscr{H}_C)\to B(\mathscr{H}_A)\otimes B(\mathscr{H}_B)\otimes\mathbb{C}I_C$$

$B(\mathscr{H}_A)\otimes\mathbb{C}I_B\otimes\mathbb{C}I_C$ üzerinde işlemcileri sabit bırakır.

**(v)** $\mathscr{E} : B(\mathscr{H}_B)\to B(\mathscr{H}_B\otimes\mathscr{H}_C)$, $(id_A\otimes\mathscr{E})(\rho_{AB})=\rho_{ABC}$ eşitliğini sağlayan bir durum dönüşümüdür.

**İspat:** $(i)\Leftrightarrow(ii)$ eşitliği, güçlü alt-toplanabilirlik bağıntısının ispatından açıkça görülebilir.

$(iii)\Rightarrow(ii)$: E'nin aynı zamanda $\tau\otimes\rho_{BC}$ durumunu invaryant bıraktığının gösterilmesi için $E(I_A\otimes X_B\otimes X_C)$ teriminin her $X_A\otimes I_B\otimes I_C$ durumu ile sıra-değiştirdiğinin gösterilmesi gerekir. Yani $E(I_A\otimes X_B\otimes X_C)\in\mathbb{C}I_A\otimes B(\mathscr{H}_B)\otimes\mathbb{C}I_C$ olur. Öyleyse

$$\begin{aligned}(\tau\otimes\rho_{BC})E(X_A\otimes X_B\otimes X_C) &= (\tau\otimes\rho_{BC})(X_A\otimes I_B\otimes I_C)E(I_A\otimes X_B\otimes X_C)\\ &= \tau_A(X_A)\,Tr\rho_{BC}E(X_A\otimes X_B\otimes X_C)\\ &= (\tau\otimes\rho_{BC})(X_A\otimes X_B\otimes X_C)\end{aligned} \tag{4.22}$$

eşitliği elde edilerek,

$$S(\rho_{ABC}\|\tau_A\otimes\rho_{BC})=S(\rho_{ABC}|\mathscr{A}\|\tau_A\otimes\rho_{BC}|\mathscr{A}) \tag{4.23}$$

sonucuna ulaşılır.

$(iv)\Rightarrow(iii)$ : $E_\rho$, $\rho_{ABC}$'yi ve kuvvetlerini korur. $E$ sabit sayılar cebri üzerinde tanımlı bir koşullu beklenti olmak üzere

$$\frac{1}{n}\left(id + E_\rho + \cdots + E_\rho^{n-1}\right) \to E \tag{4.24}$$

şeklinde yazılabilir.

$(ii) \Rightarrow (iv)$ ve $(v)$ : Genelleştirilmiş koşullu beklenti olan $E\rho$, $F$ normalize izi koruyan bir koşullu beklenti olmak üzere

$$E_\rho(X) = (\tau_A \otimes \rho_B)^{-1/2} F\left((\tau_A \otimes \rho_{BC})^{1/2} X (\tau_A \otimes \rho_{BC})^{1/2}\right)(\tau_A \otimes \rho_B)^{-1/2} \tag{4.25}$$

biçiminde yazılır. $\mathscr{A}$, $E\rho$'nun sabit sayılar cebri olmak üzere, $E_\rho(X_A \otimes I_B \otimes I_C) = X_A \otimes I_B \otimes I_C$ eşitliği görülür. Dolayısıyla,

$$B(\mathscr{H}_A) \otimes \mathbb{C}I_B \otimes \mathbb{C}I_C \subset \mathscr{A} \subset B(\mathscr{H}_A) \otimes B(\mathscr{H}_B) \otimes \mathbb{C}I_C \tag{4.26}$$

bulunarak $(iv)$ bağıntısı çıkarılır. (4.26) ifadesi, $\mathscr{A}$ alt-cebri $B(\mathscr{H}_B)$ üzerindeki bir $\mathscr{A}_B$ alt-cebri ile tanımlanan $B(\mathscr{H}_A) \otimes \mathscr{A}_B \otimes \mathbb{C}I_C$ formundadır. Bu durumda $E\rho$'nun duali ise $id_A \otimes \mathscr{E}$ formunda olacağından $(v)$ öncülüne ulaşılır.

$(v)$ kullanılarak $\mathscr{E}(\tau_A \otimes \rho_B) = \rho_{ABC}$ sonucu ortaya çıkarılır ve $(ii)$ öncülünün doğruluğu ispatlanmış olur.

Eğer bir yoğunluk matrisi $\rho_{ABC}$, $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ Hilbert uzayına etki ettiğinde Teorem 4.1'in koşulları sağlanıyorsa, $\rho_{ABC}$ bir Markov durumu olarak tanımlanır.

Eğer notasyon

$$I(A:C|B)_\rho := S(\rho_{AB}) + S(\rho_{BC}) - S(\rho_B) - S(\rho_{ABC})$$

şeklinde kullanılıyorsa, $\rho$ yoğunluk matrisinin Markoviyanlık koşulu $I(A:C|B)_\rho = 0$ şeklinde tanımlanır.

**Teorem 4.3:** $\rho_{ABC}$, $\mathscr{H}_A \otimes \mathscr{H}_B \otimes \mathscr{H}_C$ sonlu boyutlu Hilbert uzayında tanımlı bir Markov durumu olmak üzere, $\mathscr{H}_B$ uzayı,

$$\mathscr{H}_B = \sum_k \mathscr{H}_k^L \oplus \mathscr{H}_k^R$$

halinde yazılabilen bir ortogonal ayrışıma sahiptir ve her $k$ için $\rho_{AL}^k \in B\left(\mathscr{H}_A \otimes \mathscr{H}_k^L\right)$ ve $\rho_{RC}^k \in B\left(\mathscr{H}_k^R \otimes \mathscr{H}_C\right)$ biçiminde yazılabilen yoğunluk matrisleri vardır. Buradan hareketle $\rho_{ABC}$ konveks kombinasyonu

$$\rho_{ABC} = \sum_k p_k \rho_{AL}^k \oplus \rho_{RC}^k$$

bulunur.

**İspat:** $\omega \coloneqq \tau_A \otimes \rho_{BC}$ ve $\rho \coloneqq \rho_{ABC}$ olmak üzere Teorem 4.1'den çıkarılan sonuç kullanılarak, Markoviyanlık genelleştirilmiş koşullu beklentiyi ortaya çıkarır. Yani,

$$E_\omega : B(\mathscr{H}_A) \otimes B(\mathscr{H}_B) \otimes B(\mathscr{H}_C) \to B(\mathscr{H}_A) \otimes B(\mathscr{H}_B) \otimes \mathbb{C}I_C.$$

$\omega$ durumuna göre $E_\rho$ ve sabit sayılar cebri $\mathscr{A}$ aynı özelliğe sahiptirler:

$$B(\mathscr{H}_A) \otimes \mathbb{C}I_B \otimes \mathbb{C}I_C \subset \mathscr{A} \subset B(\mathscr{H}_A) \otimes B(\mathscr{H}_B) \otimes \mathbb{C}I_C.$$

Bu bakış açısından hareketle $\mathscr{A}$, $B(\mathscr{H}_B)$ üzerinde tanımlı $\mathscr{A}_B$ alt-cebri ile $B(\mathscr{H}_A) \otimes \mathscr{A}_B \otimes \mathbb{C}I_C$ formunda olmalıdır. $\mathscr{A}_B$ alt-cebrinin elementleri ise $A_k^L \in B\left(\mathscr{H}_k^L\right)$ ve $I_k^R$, $\mathscr{H}_k^R$ üzerinde tanımlı birim olmak üzere

$$\sum_{k=1}^K A_k^L \otimes I_k^R$$

ve

$$\mathscr{H}_B = \sum_{k=1}^K \mathscr{H}_k^L \otimes \mathscr{H}_k^R$$

şeklinde tanımlanır. Bu kapsamda $\mathscr{A}$,

$$\sum_{k=1}^K B\left(\mathscr{H}_A \otimes \mathscr{H}_k^L\right) \otimes \mathbb{C}I_k^R \otimes \mathbb{C}I_C$$

terimine izomorfik olur.

## 5. UYGULAMALAR

GaT bağıntısı klasik ve kuantum bilişim kuramlarında çok önemli uygulamalara sahiptir. Bunlardan en önemlisi bir kuantum kanalından ne kadar klasik bilgi aktarılabileceğini açıklayan Holevo niceliğidir (D.Petz 2008, B.Schumacher ve
M.D.Westmoreland 2010 ). Bu nicelik pek çok alanlarda kullanılmaktadır[21]. Ayrıca, GaT bağıntısı, bağıl entropinin monotonluğu ve kuantum karşılıklı bilişimin monotonluğu ile birlikte üç derin gerçekten birisidir. Bu kavramlardan teki kabul edilip diğerleri çıkarılabiliyorken herhangi birinin tek başına elde edilmesi oldukça zordur. Dolayısıyla, tezin önceki aşamalarında farklı yöntemler ile ispatlanan GaT bağıntısının varlığı kabul edilerek, diğer derin gerçeklerin çıkarılması mümkün kılınabilir. Bu bölümde, GaT bağıntısının uygulamaları olarak ilk aşamada Holevo niceliğinin detaylıca incelenmesinin ardından üç derin gerçek ele alınacaktır.

### 5.1 Holevo Niceliği

Holevo niceliği kuantum bilişim kuramında birçok sonucun çıkarılmasında önemli bir rol oynar.

$\mathscr{E} : B(\mathscr{H}) \to B(\mathscr{K})$ bir durum dönüşümü (*state transformation*)[22] olmak üzere, *Holevo niceliği*

$$I(\{p_x\}, \{\rho_x\}, \mathscr{E}) := S(\mathscr{E}(\rho)) - \sum_i p_x S(\mathscr{E}(\rho_x)) \tag{5.1}$$

şeklinde tanımlanır. Burada $\rho = \sum_x p_x \rho_x$, $p(x)$ olasılık dağılımı ve $\rho_x$ yoğunluk işlemcileri olmak üzere (5.1) denklemi bağıl entropi kullanılarak

$$I(\{p_x\}, \{\rho_x\}, \mathscr{E}) = \sum_x p(x) D(\mathscr{E}(\rho_x) \| \mathscr{E}(\rho)) \tag{5.2}$$

ifadesine denk olacak şekilde dönüştürülebilir. (5.2) denkleminde bağıl entropi ile karşılaşıldığından bazı özelliklerin çıkarılması daha kolay olacaktır. Örneğin;

$$I(\{p_x\}, \{\rho_x\}, \mathscr{E}) \geq I((p_x), (\rho_x), \mathscr{E}' \circ \mathscr{E}) \tag{5.3}$$

[21] Holevo niceliğinin kullanıldığı örnekler için Bkz. Nielsen ve Chuang 2000.
[22] Bkz. Ek 4

eşitsizliği bağıl entropinin monotonluk özelliği kullanılarak elde edilebilir. Burada $\mathscr{E}'$ bir başka durum dönüşümünü (yani kuantum kanalı) göstermektedir.

Holevo niceliği, klasik bilginin (yoğunluk işlemcilerine alt indis olarak kodlanmış $\{x\}$ kümesi) ne kadarının bir kuantum kanaldan $(\mathscr{E})$ geçtiği ile alakalıdır. Holevo niceliği von Neumann entropisi için bir üst sınır oluşturur. Öyle ki von Neumann entropi bu üst sınırı geçemez. Ancak, ulaşabildiği yani eşit olduğu durumlar olabilir. Bu durumlarda ise gönderilen tüm bilginin kanaldan sorunsuz geçtiği anlaşılır. Kanalların başka bir özelliği olan öze-uygunluk kavramı da kanalların daha iyi anlaşılması için faydalıdır.[23]

$\mathscr{X}$ giriş alfabesi $\mathscr{Y}$ ise çıkış alfabesi olmak üzere bir kuantum kanal ele alınsın: $\mathscr{E}$ : $B(\mathscr{H}) \to B(\mathscr{K})$ ve bu kuantum kanaldan klasik bilgi aktarılıyor olsun. $X$ kümesi üzerinde bir girdi dağılımı $p(x)$ alınabilir ve seçilen her $x \in \mathscr{X}$ için karşılık gelen bir yoğunluk işlemcisi $\rho_x \in B(\mathscr{H})$ olur ve alıcı $\mathscr{K}$ sistemi üzerinde ölçüm yapar. Yani, her $y \in \mathscr{Y}$ için bir pozitif işlemci $F_y \in B(\mathscr{K})$ ele alınarak $\sum_y F_y = I_{\mathscr{K}}$ sağlanır. Kodlama ve ölçüm $\mathscr{E}$'dan klasik bir kanal oluşturur. Öyle ki $x \in \mathscr{X}$ gönderildiğinde $y \in \mathscr{Y}$'nin gözlenme olasılığı

$$T_{yx} = Tr\rho_x F_y \tag{5.4}$$

ile tanımlanır. Kanaldan geçen klasik bilgi miktarı Holevo niceliği ile sınırlandırılmıştır:

$$I(X:Y) \leq I((p_x),(\rho_x),\mathscr{E}). \tag{5.5}$$

Holevo, bu niceliği ortaya attığında kuantum bağıl entropi tam olarak yerleşmiş bir kavram değildi. Ancak, şu an (5.5) denklemi kuantum bağıl entropi cinsinden yazabilir: Her $x \in \mathscr{X}$ için

$$\sum_x p(x) D\left(Tr\mathscr{E}(\rho_x)F_y \parallel Tr\mathscr{E}(\rho)F_y\right) \leq \sum_x p(x) S\left(\mathscr{E}(\rho_x) \parallel \mathscr{E}(\rho)\right) \tag{5.6}$$

olur. Bu bağıntının doğruluğu

$$D\left(Tr\mathscr{E}(\rho_x)F_y \parallel Tr\mathscr{E}(\rho)F_y\right) \leq S\left(\mathscr{E}(\rho_x) \parallel \mathscr{E}(\rho)\right) \tag{5.7}$$

eşitsizliği kullanılarak görülür. Dolayısıyla, (5.5) ifadesi kanaldan aktarılan bilgiyi sınırlandıran nicelik olur.

[23] Öze-uygunluk kavramı için EK-2 kısmına bakılabilir.

Holevo niceliğinin GaT bağıntısı yardımı ile çıkarıldığı açık bir şekilde gösterilmiştir. Bir kanal aracılığı ile gönderilen bilgi miktarını sınırlandıran Holevo niceliği, dolanıklık barındıran üç-parçalı bir sistem için GaT bağıntı kullanılarak dolanıklığı ortadan kaldırmaya yardımcı olur.

Temel olarak, Holevo niceliği, verilen n kübit - kuantum süperpozisyon sayesinde - daha büyük miktarda klasik bilgi taşıyabilmelerine rağmen, geri alınabilen, yani erişilebilen klasik bilgi miktarının yalnızca klasik olarak kodlanmış n bit bilgiye bağlıdır. Bu durum iki nedenden ötürü önemlidir. (1) Kuantum kanal genellikle klasik kanaldan çok daha güçlüdür, bu nedenle sadece geleneksel tekniklerden daha iyi veya daha düşük olduğunu gösteren sonuçlar olağandışıdır. (2) sadece n biti temsil eden kübitleri kodlamak için $2^n$ tane karmaşık sayı alır.

## 5.2 Üç Derin Gerçek

Bu bölümde kuantum entropinin üç önemli özelliğinden bahsedilecektir. Bu üç özellik birbirleri ile bağıntılıdır. Öyle ki ilk özellik kullanılarak ikinci ve üçüncü özellik elde edilebilir. Fakat herhangi birinin diğer ikisi kullanılmadan elde edilmesi güç bir matematiksel işlem gerektirir.

Üç derin gerçekten ilki *bağıl entropinin monotonluğu* olarak bilinir ve bu bağıntı (3.22) ifadesi ile gösterilmiştir. Yani, iki kuantum durumu arasındaki bağıl entropi (uzaklık) alt-sistemlerinden birisi atılarak arttırılamaz. Bu durum açık kuantum sistemleri için önemli bir sonuç içermektedir. Bu bağlamda, $\rho$ ve $\sigma$, $Q$ sisteminin olası başlangıç iki durumu olsun. Bu sistem çevre[24] ile etkileşim içerisindedir. Bu çevre $Q$ sistemi için bir kuantum kanal olan bir gelişim gönderimi (*evolution map*) ($\mathscr{E}$) üretir:

$$\mathscr{E}(\rho) = Tr_E \left[ U \left( \rho \otimes |0\rangle \langle 0| \right) U^\dagger \right]. \tag{5.8}$$

Aynı üniter gelişim iki durumun bağıl entropisini değiştirmez. Bir başka deyişle,

$$\begin{aligned} D(\rho \parallel \sigma) &= D(\rho \otimes |0\rangle \langle 0| \parallel \sigma \otimes |0\rangle \langle 0|) \\ &= D\left( U \left( \rho \otimes |0\rangle \langle 0| \right) U^\dagger \parallel U \left( \sigma \otimes |0\rangle \langle 0| \right) U^\dagger \right) \end{aligned} \tag{5.9}$$

[24] Çevre başlangıç olarak $|0\rangle \langle 0|$ durumunda olarak alınır.

ifadesi sağlanır. Denklemin sağ tarafı için (3.22) eşitsizliği kullanılarak,

$$D(\rho \parallel \sigma) \geq D(\mathscr{E}(\rho) \parallel \mathscr{E}(\sigma)) \tag{5.10}$$

bağıntısı yazılır. Gelişim gönderimi sayesinde $\rho$ ve $\sigma$ durumları birbirlerine yaklaşır. Dolayısıyla, bağıl entropi azalır. (3.22) kullanılarak entropinin ikinci temel özelliği olan *kuantum karşılıklı bilişimin monotonluğu* elde edilir.
(2.49) denkleminde bağıl entropi cinsinden belirtilen kuantum karşılıklı bilişim kavramı kullanılarak $ABC$ bileşik bir kuantum sisteminin herhangi bir durumu için,

$$I(A:BC) \geq I(A:B) \tag{5.11}$$

eşitsizliği çıkarılabilir.

Bu durum açık sistemler için bir sonuç içerir. Bileşik bir sistem olan $RQ$ kuantum karşılıklı bilişim $(I(R:Q))$ başlangıç durumunda olmak üzere, $|0\rangle\langle 0|$ başlangıç durumunda olan bir çevre $(E)$ bu sisteme eklenirse, $I(R:QE) = I(R:Q)$ elde edilir. Eğer $QE$ sistemi üniter bir gelişim gösterirse, bu durum karşılıklı bilişimi etkilemeyecektir. Yani, $I(R:QE') = I(R:QE)$ olduğu söylenir. Son olarak, çevre üzerinden kısmi iz alınırsa, $Q$ sisteminin açık sistem gelişimi, onun $R$ ile karşılıklı kuantum bilişimini arttıramaz denir:

$$I(R:Q) \geq I\left(R:Q'\right). \tag{5.12}$$

Entropinin üçüncü temel özelliği ise (5.11) eşitsizliğinin iki tarafının da açık bir şekilde yazılması ile ortaya çıkar:

$$S(A)+S(BC)-S(ABC) \geq S(A)+S(B)-S(AB), \tag{5.13}$$

Dolayısıyla, (5.13) düzenlenerek kuantum entropinin *güçlü alt-toplanabilirlik* (GaT) bağıntısı elde edilir:

$$S(BC)+S(AB) \geq S(ABC)+S(B). \tag{5.14}$$

(5.14) bağıntısı, üç rasgele değişkeni içeren klasik eşitsizliğin kuantum karşılığıdır.

# 6. TARTIŞMA VE SONUÇ

Bu çalışmanın temel amaçlarından biri olarak belirlenen, klasik ve kuantum entropileri anlamak ve GaT bağıntısının çıkarılmasının kavramsal ve matematiksel olarak incelenmesi doğrultusunda, ilk aşamada temel bilgiler derinlemesine incelenmiştir. Bu bilgiler ışığında, üç parçalı bir sistemin çarpanlarının entropileri ile ilişkisini anlatan bir eşitsizlik olan GaT bağıntısının, klasik ve kuantum entropileri için geçerli olduğu gösterilmiştir.

Bu bölümde tanımlanan kavramların kullanılması sonucu ortaya çıkan güçlü alt-toplanabilirlik (GaT) bağıntısının farklı kişiler tarafında yapılmış olan ispatları ve başka eşitsizliklerle olan ilişkileri üçüncü bölümde kronolojik olarak verilmiştir. Bu farklı bakış açılarının incelenmesi ve matematiksel analizlerinin anlaşılması ile hem kuantum bilişim kuramının detaylıca anlaşılması hem de ilerleyen aşamalar için bir temel oluşturması amaçlanmıştır. Lieb ve Ruskai'nin (Lieb ve Ruskai, 1973) öncülüğünü yaptığı ispat daha sonraki ispatlar için ilham kaynağı oluşturarak bilişim kuramlarına yeni bakış açısı kazandırmıştır.

Dördüncü bölümde ise GaT bağıntısının eşitlik durumu olan Markov durumlarının ne olduğu açıklanmış ve uygulamalarından bahsedilerek GaT bağıntısı ile aralarındaki bağ gösterilmiştir. Markov durumları son yıllarda gelişen bir alan olmakta beraber gelecek vaat eden bir alandır. Bölüm 5'te anlatılan bazı uygulamalar bu durumu açıkça gözler önüne sermektedir.

Son bölümde ise GaT bağıntısının uygulamalarından bahsedilmiş olup önemleri üzerinde durulmuştur. Holevo niceliği ve kanaldan aktarılan klasik bilgi miktarının bu nicelik ile sınırlandırılıyor oluşundan, üç derin gerçekten bahsedilerek uygulamalar bölümü tamamlanmıştır. Bununla beraber Ek-4 kısmında farklı uygulamalar da yer almaktadır. Kuantum ve klasik kanalların haberleşme teknolojisindeki yeri ve durum dönüşümleri için GaT bağıntısının nasıl bir işleve sahip olduğu detaylandırılarak anlatılmıştır.

Ek kısmında tezin içeriğini tam olarak anlayabilmek adına gerekli terimleri ve onların matematiksel çıkarımları üzerine bilgiler yer almaktadır. Öze-uygunluk, İz-uzaklığı ve özellikle iz ile kısmi iz bağıntıları tez içerisinde fazlasıyla kullanılmış olduğundan gerekli noktalarda Ek kısımları incelenebilir.

## KAYNAKLAR


Barnum, H., Nielsen, M.A. and Schumacher, B. 1998. Information transmission through a noisy quantum channel, Physical Review A, 57, 4153.

Baumann, F. and Jost, R. 1969. In problems of Theoretical Physics; Essays Dedicated to N.N. Bogoliubov, 285. Moscow, Nauka.

Frank, R.L. and Lieb, E.H. 2013. Monotonicity of a relative Rényi entropy, Journal of Mathematical Physics, 54, 122201.

Hayden, P., Jozsa, R., Petz, D. and Winter, A. 2004. Structure of states which satisfy strong subadditivity of quantum entropy with equality, Communications Mathematical Physics, 246, 359-374.

Hiai F. and Petz D. 2014. Introduction to Matrix Analysis and Applications, Hindustan Book Agency, Springer.

Holevo, A.S. 1973, Problemy Peredachi Informatsii. 9, 3.

Holevo, A.S. 1997. Coding Theorems for Quantum Communication Channels. arXiv:quant-ph/9708046v1.

Holevo, A.S. 1998. The Capacity of Quantum Channel with General Signal States. IEEE Trans.Info.Theor. 44, 269-273.

Holevo, A.S. 2000. Reliability Function of General Classical-Quantum Channel, IEEE.

Holevo, A.S. 2011. Probabilistic and statistical aspects of quantum theory. Steklov Mathematical Institute Moscow.

Holevo, A.S. 2012. Quantum systems, channels, information: A mathematical introduction, de Gruyter, Berlin, Boston.

Horodecki, R., Horodecki, P. and Horodecki, M. 1996. Physics Letters A, 210, 377.

Lanford, O.E. and Robinson, D. 1968. Mean entropy of states in quantum-statistical mechanics, Mathematical Physics, 9(7):1120-1125.

Lieb, E.H. 1973. Convex trace functions and the Wigner-Yanase-Dyson conjecture. Advances in Mathematics. 11 (3): 267–288.

Lieb, E.H. and Ruskai, M.B. 1973. Proof of the strong subadditivity of quantum mechanical entropy. Jornal of Mathematical Physics, 14, 1938–1941.

Lieb, E.H. 1975. Some Convexity and Subadditivity Properties of Entropy. Bull. AMS. 81: 1–13.

Lindblad, G. 1974. Expectations and entropy inequalities for finite quantum systems, Communications in Mathematical Sciences, 39, 111-119.

Lindblad, G. 1975. Completely positive maps and entropy inequalities. Communications in Mathematical Physics. Springer Science and Business Media LLC. 40 (2): 147–151.

Markov, A.A. 1913. An example of statistical investigation of the text Eugene onegin concerning the connection of samples in chains, 19(4), 591–600

Nielsen, M.A. and Chuang, L.I. 2010. Quantum Computation and Quantum Information, Cambridge University Press, Cambridge.

Ohya, M. and Petz, D. 1993. Quantum Entropy and Its Use, Springer.

Ruskai, M.B. 1994. Beyond strong subadditivity? Improved bounds on the contraction of generalized relative entropy. Rev. Mathematical Physics. 6, 1147.

Ruskai, M.B. 2002. Inequalities for quantum entropy: A review with conditions for equality. Journal of Mathematical Physics. AIP Publishing. 43 (9): 4358–4375.

Ruskai, M.B. 2005. Lieb's simple proof of concavity of Tr A^p K^* B^(1-p) K and remarks on related inequalities, International Journal Quantum Information, 3, 570-590.

Petz, D. 1986. Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. Communications in Mathematical Physics. Springer Science and Business Media LLC. 105 (1): 123–131.

Petz, D. Sufficiency of Channels over von Neumann Algebras, Quarterly Journal of Mathematics, Oxford 35, 475–483 (1986).

Petz, D. 1994. A survey of trace inequalities, in functional analysis and operator theory, 287-298, Banach Center Publications.

Petz, D. 2003. Monotonicity of quantum relative entropy revisited. Rev. Mathematical Physics, 15, 79.

Petz, D. 2008. Quantum Information Theory and Quantum Statistics, Springer, Berlin Heidelberg.

Schumacher, B. and Nielsen M.A. 1996. Quantum data processing and error correction, Physical Reviews A, 54, 2629.

Schumacher B. and Westmoreland M. 2010. Quantum Processes Systems and Information, Cambridge.

Shanon, C.E., 1948. Bell System Tech. Mathematical Theory of Communication, Journal, 27, pp. 379-423.

Uhlmann, A. "Endlich Dimensionale Dichtematrizen, II", Wiss. Z. Karl-Marx Universitate, Liepzig, Math-Naturwiss. R., to appear.

Uhlmann, A. 1977. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory, Communications Mathematical Physics, 54, 21-32.

Verçin A. ve Dereli T. 2014. Kuantum Mekaniği: Temel Kavramlar ve Uygulamaları, TÜBA, Ankara.

von Neumann, J. 1932. Mathematische Grundlagen der Quantenmechanic, Springer, Berlin.

# EKLER

## EK 1 İz ve Parçalı İz bağıntısı

### İz (*Trace*) Bağıntısı

Şimdiye kadar matrisler üzerinden tanımlanan iz bağıntısını, bir işlemcinin izi şeklinde tanımlamak mümkündür. İz bağıntısı operatörler üzerinde çizgisel bir fonksiyoneldir.[1] İz bağıntısı

$$Tr\left|\alpha\right\rangle\left\langle\beta\right| = \left\langle\beta\right|\left.\alpha\right\rangle \tag{1}$$

olarak tanımlanır. Yani iz bağıntısı dış çarpımı, iç çarpıma çeviren bir işlem olarak düşünülebilir. Herhangi bir işlemci elemanlarının dış çarpımlarının toplamı şeklinde yazılabileceğinden, iz'in tanımı için matris gösterimi ile yapılabilecek

$$\begin{aligned} TrA &= Tr\left(\sum_{mn} A_{mn}\left|m\right\rangle\left\langle n\right|\right) \\ &= \sum_{mn} A_{mn}\left(Tr\left|m\right\rangle\left\langle n\right|\right) \\ &= \sum_{mn} A_{mn}\delta_{mn} \\ &= \sum_{n} A_{nn} \end{aligned} \tag{2}$$

işlemler ile açık bir şekilde görülebilir. Açıkça görüldüğü üzere; bir işlemcinin izi, o işlemcinin matris gösteriminin diagonal elemanlarının toplamına eşittir ve matrisin yazıldığı bazdan bağımsızdır. (2) bağıntısı farklı bir notasyon ile

$$TrA = \sum_{n}\left\langle n\right|A\left|n\right\rangle \tag{3}$$

şeklinde gösterilebilir. İz bağıntısını hesaplamak seçilen bazdan bağımsız olduğundan, hangi bazı kullandığımız çok da önem arz etmez. Öyle ki $\{|\alpha_n\rangle\}$ ve $\{|\beta_n\rangle\}$ ortonormal iki baz olmak üzere

[1] Fonksiyonel, bir vektör uzayı V'den onun skalerlerine tanımlanan bir çizgisel gönderimdir.

$$\begin{aligned}
\sum_n \langle \alpha_n | A | \alpha_n \rangle &= \sum_n \langle \alpha_n | A \left( \sum_m |\beta_m\rangle \langle \beta_m| \right) |a_n\rangle \\
&= \sum_{mn} \langle \alpha_n | A |\beta_m\rangle \langle \beta_m| \, \alpha_n\rangle \\
&= \sum_{mn} \langle \beta_m| \, \alpha_n\rangle \langle \alpha_n | A |\beta_m\rangle \\
&= \sum_m \langle \beta_m| \left( \sum_n |\alpha_n\rangle \langle \alpha_n| \right) A |\beta_m\rangle \\
&= \sum_m \langle \beta_m | A |\beta_m\rangle \qquad (4)
\end{aligned}$$

işlemleri ile bu durum açıkça gösterilebilir.

$A$ ve $B$ işlemcileri iz bağıntısı altında sıra değişirler:

$$TrAB = TrBA. \qquad (5)$$

Bunu en kolay yoldan görmek gerekirse, matris gösterimi kullanılarak

$$\sum_n (AB)_{nn} = \sum_{nm} A_{nm} B_{mn} = \sum_{nm} B_{mn} A_{nm} = \sum_m (BA)_{mm} \qquad (6)$$

eşitliği gösterilebilir. Bu durum iki çarpanlı sistem yerine çok çarpanlı sistemlere de uygulanabilir. Bu özelliğe ise çevrimsel (*cyclic*) denir:

$$Tr(A \cdots BC) = Tr(CA \cdots B). \qquad (7)$$

Burada dikkat edilmesi gerekilen en önemli nokta, işlemcilerin rasgele sıra değişmemesidir. Çevrimsel permütasyon; yani ardışıklık bozmamalıdır.

### Parçalı İz Bağıntısı

Bu kısımda ise bir önceki bölümde öğrenilen iz bağıntısının biraz daha özel bir durumu ile ilgilenilecektir. Öyle ki, bileşik bir sistem olan $RQ$ ele alınsın ve bu sistem $\left|\Psi^{RQ}\right\rangle$ ile dolanık[2] olsun. $R$ sistemi üzerinde bir ölçüm yapılması, $Q$ sistemi üzerinde bir koşullu saf

[2]Kuantum mekaniğinde bileşik sistemlerin durum uzayı tensörel yapıdadır. Bu da sistemin altssitemlerinin özellikleri ile basitçe ifade edilemeyen, bu nedenle klasik tezahürleri olmayan, ya da tümünden

olmayan duruma yönlendirir. $R$ sistemi için $\left|k^R\right\rangle$ bazı alınarak, kısmi iç çarpım yapılırsa;

$$\sqrt{p_k}\left|\psi_k^Q\right\rangle = \left\langle k^R\right| \Psi^{RQ}\Big\rangle \tag{8}$$

denklemi çıkarılır. Burada $p_k$ ölçüm sonunda k'nıncı değerin gelme olasılığıdır ve $\left|\psi_k^Q\right\rangle$ ket'i koşullu $Q$ sistemine karşılık gelir. $Q$ sistemine ait saf olmayan yoğunluk işlemcisi

$$\begin{aligned}\rho^Q &= \sum_k p_k \left|\psi_k^Q\right\rangle\left\langle\psi_k^Q\right| \\ &= \sum_k \left\langle k^R\right| \Psi^{RQ}\Big\rangle\Big\langle\Psi^{RQ}\Big| k^R\Big\rangle\end{aligned} \tag{9}$$

olarak yazılabilir. (9) bağıntısı, $\rho^{RQ} = \left|\Psi^{RQ}\right\rangle\left\langle\Psi^{RQ}\right|$ alınarak daha güzel bir şekilde yazılabilir;

$$\rho^Q = \sum_k \left\langle k^R\right| \rho^{RQ} \left|k^R\right\rangle. \tag{10}$$

(10) denkleminin sağ tarafı $\rho^{RQ}$ üzerinde $R$ üzerinden alınmış iz işlemini andırıyor ve (3) denklemi ile benzerlik göstermektedir. Fakat dikkat etmekte fayda vardır ki; burada kullanılan baz $\mathscr{H}^R$ Hilbert uzayına aittir.

Bu noktada $\mathscr{H}^{RQ}$ Hilbert uzayı üzerinde bir işlemci için *kısmi iz* tanımı yapılabilir. Varsayılsın ki dış çarpım şeklinde yazılabilen bir işlemci olsun: $G^{RQ} = \left|\alpha^R, \phi^Q\right\rangle\left\langle\beta^R, \psi^Q\right|$. Öyleyse

$$\begin{aligned}Tr_R G^{RQ} &= Tr_R\left(\left|\alpha^R, \phi^Q\right\rangle\left\langle\beta^R, \psi^Q\right|\right) \\ &= Tr_R\left(\left|\alpha^R\right\rangle\left\langle\beta^R\right| \otimes \left|\phi^Q\right\rangle\left\langle\psi^Q\right|\right) \\ &= \left\langle\beta^R\right| \alpha^R\Big\rangle\left|\phi^Q\right\rangle\left\langle\psi^Q\right|\end{aligned} \tag{11}$$

farklı olan bütünlükçü özelliklerinin olabileceğini göstermektedir. Bileşik sistemlerin klasik tezahürü olmayan en ayrıcalıklı özelliği, ilk olarak 1935 yılında Schrödinger tarafından farkedilen ve aynı yıl Einstein, Podolsky ve Rosen'ın önemli çalışmaları ile büyük bir araştırma konusu haline gelen kuantum dolanıklığıdır. Kuantum dolanıklığı, bileşik sistemin bileşenleri arasında kuantum korelasyonlarının varlığını vurgular. Matematiksel olarak bir sistemin bileşenlerine ait durum vektörlerinin tensör çarpımları olarak yazılamayan durum vektörleri ile temsil edilen durumlara dolanık (saf) durumlar denir (A. Verçin ve T.Dereli, 2014).

denklemleri yazılabilir. Kısmi iz bağıntısı $\mathscr{H}^R$ üzerinde tanımlanan bir dış çarpımı iç çarpım işlemine dönüştürür. $Tr_R$ bağıntısının çizgiselliğini koruma şartını uygulayarak bu tanımı rasgele işlemcilere genişletilebilir. Herhangi bir durumda $\mathscr{H}^{RQ}$ Hilbert uzayı üzerinde tanımlanan bir işlemcinin $R$ üzerinden kısmi izi $\mathscr{H}^Q$ uzayında yaşayan bir operatöre denk gelir.

Kısmi iz, $\mathscr{H}^R$ uzayına ait bir baz kullanılarak da hesaplanabilir. $G^{RQ}$ işlemcisi için

$$Tr_R G^{RQ} = \sum_k \left\langle k^R \right| G^{RQ} \left| k^R \right\rangle \tag{12}$$

eşitliği yazılabilir. $Tr_R$ tanımının $\mathscr{H}^R$ uzayında seçilen bazdan bağımsız olduğundan dolayı, bu sonuç çizgisellik vasıtasıyla, $\mathscr{H}^{AB}$ uzayında bulunan rasgele bir işlemciye genişletilebilir. Öyle ki bu durum için kısmi iz bazdan bağımsızdır denir.

(10) denkleminde seçilen $\rho^Q$ yoğunluk işlemcisi

$$\rho^Q = Tr_R \rho^{RQ} \tag{13}$$

şeklinde kısmi iz üzerinden yeniden yazılabilir. Burada aynı yoğunluk işlemcisi $\rho^{RQ}$ üzerinde $Q$ durumuna koşullu herhangi bir $R$ ölçümü yapılırsa, yine aynı yoğunluk işlemcisi $\rho^Q$ ortaya çıkacaktır. Yani $R$ ölçümünün seçimi $Q$ gözlenebilirlerinin ortalama değeri üzerinde herhangi bir etkiye sahip değildir.

$R$ ölçümünün yapılıp yapılmamasından bağımsız olarak, $Q$ alt-sisteminin durumunu açıklamak için (13) eşitliğindeki $\rho^Q$ yoğunluk işlemcisini kullanmak anlam ve hesap kolaylığı yaratacaktır. Öyle ki, $\left|\Psi^{RQ}\right\rangle$ bileşik durumunda bulunan iki parçalı bir sistem olan $RQ$ için, $Q$ sistemi üzerindeki $A^Q$ gözlenebilirinin beklenen değeri

$$\begin{aligned}
\left\langle A^Q \right\rangle &= \left\langle \Psi^{RQ} \right| I \otimes A^Q \left| \Psi^{RQ} \right\rangle \\
&= \sum_k \left\langle \Psi^{RQ} \right| \left( \left| k^R \right\rangle \left\langle k^R \right| \otimes A^Q \right) \left| \Psi^{RQ} \right\rangle \\
&= \sum_k \left\langle \Psi^{RQ} \left| k^R \right\rangle A^Q \left\langle k^R \right| \Psi^{RQ} \right\rangle \\
&= Tr_Q \left( \sum_k \left\langle k^R \right| \Psi^{RQ} \right\rangle \left\langle \Psi^{RQ} \left| k^R \right\rangle \right) A^Q
\end{aligned} \tag{14}$$

olarak bulunabilir. Yani,

$$\left\langle A^{Q}\right\rangle = Tr_{Q}\rho^{Q}A^{Q} \tag{15}$$

olarak yazılabilir. Yoğunluk işlemcisi $\rho^{Q} = Tr_{R}\left|\Psi^{RQ}\right\rangle\left\langle\Psi^{RQ}\right|$, $Q$ sistemi üzerindeki herhangi bir gözlenebilirin beklenen değerini verir. Eğer $RQ$ sistemi dolanık ise, $Q$ sisteminde saf bir durum tanımlanamaz. Fakat sadece $Q$'nun kendi içindeki gözlenebilir özellikleri düşünülürse, $Q$ sisteminde saf olmayan ve kısmi iz bağıntısı ile bulunabilen bir yoğunluk işlemcisi $\rho^{Q}$ tanımlanabilir.

İz bağıntısı kullanılarak entropi çeşitleri tanımlanabilir. Öyle ki

$$S(A) = -Tr_{A}\left(\rho^{A}log\rho^{A}\right) \tag{16}$$

von Neumann entropisinin iz bağıntısı cinsinden yazılımıdır.

## EK 2 Öze-uygunluk

### İki Kuantum Durumunun Yakınlığı

İki farklı yoğunluk işlemcisi ile tanımlanan iki farklı kuantum durumunun birbirine olan uzaklıklarını bağıl entropi ile gösterilebildiği daha önceden belirtilmişti. Fakat burada bahsedilen bağıl entropi için kesin bir şekilde uzaklık fonksiyonu olduğu söylenemez. Çünkü bu entropi fonksiyonu simetriyi ve üçgen eşitsizliğini sağlamaz. Bu bağlamda iki kuantum durumunun birbirlerine olan uzaklıklarını iki farklı yol ile belirtmekte fayda vardır. Bunlar öze-uygunluk (*fidelity*) ve iz uzaklığı (*trace distance*) olarak tanımlanır.[3]

### İz-Uzaklığı (*Trace Distance*):

İki kuantum durumu arasındaki iz uzaklığı

$$D(\rho,\sigma) \equiv \frac{1}{2} Tr|\rho-\sigma| \tag{17}$$

olarak tanımlanır. Burada $|A| \equiv \sqrt{A^{\dagger}A}$ değerinin pozitif kökü olarak alınır. İz-uzaklığını kuantum ve klasik olarak ikiye ayırabilmek mümkündür. Fakat eğer $\rho$ ve $\sigma$ sıra değişiyorlarsa $\rho$ ve $\sigma$ arasındaki kuantum iz-uzaklığı, $\rho$ ve $\sigma$'nın özdeğerleri arasındaki klasik iz-uzaklığına eşit olur. Yani kuantum iz-uzaklığının, klasik iz-uzaklığını bu bağlamda genellediği söylenebilir. Bir başka deyiş ile, eğer $\rho$ ve $\sigma$ sıra değişiyorlarsa, ortonormal olan aynı baz üzerinde köşegendirler,

$$\rho = \sum_i r_i |i\rangle \langle i| \; ; \; \sigma = \sum_i s_i |i\rangle \langle i|. \tag{18}$$

Öyleyse, $\rho$ ve $\sigma$ değişkenleri (17) denkleminde yerine yazılırsa;

$$\begin{aligned} D(\rho,\sigma) &= \frac{1}{2} Tr \left| \sum_i (r_i - s_i) |i\rangle \langle i| \right| && (19) \\ &= \frac{1}{2} \sum_i |r_i - s_i| && (20) \\ &= D(r_i, s_i) && (21) \end{aligned}$$

[3] Ek 2.1 ve Ek 2.2 için Nielsen ve Chuang Bölüm 9'dan faydalanılmıştır.

eşitliği elde edilir.

İz-uzaklığını daha iyi anlamak için kübit durumunu düşünmek faydalı olacaktır. Öyle ki bu kübit durumunu Bloch küresi üzerinde düşünülsün. $\rho$ ve $\sigma$ Bloch küresi üzerinde sırasıyla $\overrightarrow{r}$ ve $\overrightarrow{s}$ vektörleri ile temsil edilmek üzere,

$$\rho = \frac{I + \overrightarrow{r} \cdot \overrightarrow{\sigma}}{2} \; ; \; \sigma = \frac{I + \overrightarrow{s} \cdot \overrightarrow{\sigma}}{2} \tag{22}$$

olarak tanımlanır. Burada $\overrightarrow{\sigma}$, bir durumu değil Pauli matrislerinin bir vektörünü temsil eder. $\rho$ ve $\sigma$ arasındaki iz-uzaklığı kolaylıkla hesaplanabilir:

$$\begin{aligned} D(\rho,\sigma) &= \frac{1}{2} Tr|\rho - \sigma| \\ &= \frac{1}{4} Tr\left|\left(\overrightarrow{r} - \overrightarrow{s}\right) \cdot \overrightarrow{\sigma}\right|. \end{aligned} \tag{23}$$

$\left(\overrightarrow{r} - \overrightarrow{s}\right) \cdot \overrightarrow{\sigma}$ terimi $\pm\left|\overrightarrow{r} - \overrightarrow{s}\right|$ özdeğerlerine sahiptir. Yani $\left|\left(\overrightarrow{r} - \overrightarrow{s}\right) \cdot \overrightarrow{\sigma}\right|$ teriminin iz-uzaklığı $2\left|\overrightarrow{r} - \overrightarrow{s}\right|$ olur. Dolayısıyla,

$$D(\rho,\sigma) = \frac{\left|\overrightarrow{r} - \overrightarrow{s}\right|}{2} \tag{24}$$

olur. Bu sonuçtan anlaşılabileceği gibi iki kübit durumunun aralarındaki uzaklık, bu iki durumun, Bloch yuvarı (*ball*) üzerinde, aralarındaki Öklidiyen uzaklığın yarısı olur.

İz-uzaklığının genel özelliklerini daha iyi anlamak için, işin geometrisine bakmak faydalı olabilir. Öyle ki Bloch küresi üzerinde yapılan dönmeler Öklidiyen uzaklığı invaryant bırakır. Bu durum şöyle bir sonuç doğurabilir: iz-uzaklığı üniter dönüşümler altında korunur. Yani

$$D\left(U\rho U^{\dagger}, U\sigma U^{\dagger}\right) = D(\rho,\sigma) \tag{25}$$

yazılabilir.

İki yoğunluk işlemcisi iz-uzaklığı anlamında birbirlerine yakın ise, herhangi bir ölçüm olasılık dağılımlarını arttırarak klasik bu iki durumu birbirine yakınlaştırır. İz-uzaklığı bir uzaklık olarak düşünülebilir fakat yoğunluk işlemcilerinin uzayında bir metrik belirtip

belirtmediği kontrol edilmelidir. Bunun için simetrik olup olmadığını ve üçgen eşitsizliğini sağlayıp sağlamadığını kontrol etmek gerekir. Bu durum geometrik yorum üzerinden kolaylıkla anlaşılabilir. Öyle ki tek bir kübit üzerinden düşünülürse doğru olduğu bariz bir şekilde görülebilir. Önemli olan bu durumun genellenip genellenemeyeceğidir. $D(\rho,\sigma)=0$ olur ancak ve ancak $\rho=\sigma$ ise ve ayrıca $D(\cdot,\cdot)$ fonksiyonu, girdilere göre simetriktir. Öyleyse geriye üçgen eşitsizliği kalır:

$$D(\rho,\tau)\leq D(\rho,\sigma)+D(\sigma,\tau)\,. \tag{26}$$

Bu eşitsizliğin doğruluğunu kontrol etmek için $P$ bir projeksiyon olmak üzere,

$$D(\rho,\tau)=Tr(P(\rho-\tau)) \tag{27}$$

denklemi kullanılabilir.[4] (27) eşitliği, (19) yardımı ile;

$$\begin{aligned} D(\rho,\tau) &= Tr(P(\rho-\sigma))+Tr(P(\sigma-\tau)) \\ &\leq D(\rho,\sigma)+D(\sigma,\tau) \end{aligned} \tag{28}$$

haline getirilerek üçgen eşitsizliğini sağladığı gösterilebilir. Öyleyse iz-uzaklığı bir metriktir denir.

Bu noktada gösterilebilecek birkaç sonuç vardır. Bunlardan en önemlisi: Herhangi fiziksel bir süreç asla ve asla iki kuantum durum arasındaki uzaklığı arttırmaz.

**Teorem 2.1:** $\mathscr{E}$ bir iz koruyan kuantum kanal, $\rho$ ve $\sigma$ birer yoğunluk işlemcileri olmak üzere;

$$D(\mathscr{E}(\rho),\mathscr{E}(\sigma))\leq D(\rho,\sigma) \tag{29}$$

olur.

**İspat:** Spektral ayrışım[5] kullanılarak, $Q$ ve $S$ ortogonal desteğe(support) sahip pozitif

[4] Nielsen-Chuang, sayfa 404

[5] Daha fazla bilgi için EK-3 incelenebilir.

matrisler olmak üzere; $\rho-\sigma=Q-S$ eşitliği yazılabilir. Ayrıca $P$ bir projeksiyon olmak üzere $D(\mathscr{E}(\rho),\mathscr{E}(\sigma))=Tr[P(\mathscr{E}(\rho)-\mathscr{E}(\sigma))]$ eşitliği de yazılabilir. $Tr(Q)-Tr(S)=Tr(\rho)-Tr(\sigma)=0$ olur ve dolayısıyla $Tr(Q)=Tr(S)$ ve $Tr[\mathscr{E}(Q)]=Tr[\mathscr{E}(S)]$ eşitliği elde edilir. Bu çıkarım kullanılarak,

$$\begin{aligned} D(\rho,\sigma) &= \frac{1}{2}Tr|\rho-\sigma|=\frac{1}{2}Tr|Q-S| \\ &= \frac{1}{2}Tr(Q)+\frac{1}{2}Tr(S)=\frac{1}{2}Tr(\mathscr{E}(Q))+\frac{1}{2}Tr(\mathscr{E}(S)) \\ &= Tr(\mathscr{E}(Q))\geq Tr(P\mathscr{E}(Q)) \\ &\geq Tr[P(\mathscr{E}(Q)-\mathscr{E}(S))]=Tr[P(\mathscr{E}(\rho)-\mathscr{E}(\sigma))] \\ &= D(\mathscr{E}(\rho),\mathscr{E}(\sigma)) \end{aligned} \tag{30}$$

terimine kadar ulaşılabilir. Ki bu durum ispatın tamamlanmasını sağlar.

**Teorem 2.2:** $\{p_i\}$ ve $\{q_i\}$ aynı küme üzerinde tanımlı olasılık dağılımları (konveks bileşim katsayıları), $\rho_i$ ve $\sigma_i$ yoğunluk işlemcileri olmak üzere;

$$D\left(\sum_i p_i\rho_i,\sum_i q_i\sigma_i\right)\leq D(p_i,q_i)+\sum_i p_iD(\rho_i,\sigma_i), \tag{31}$$

eşitsizliği yazılabilir. Burada $D(p_i,q_i)$, $\{p_i\}$ ve$\{q_i\}$ olasılık dağılımları arasındaki klasik iz-uzaklığı olarak tanımlanır.

**İspat:** (27) denklemi kullanılarak

$$\begin{aligned} D\left(\sum_i p_i\rho_i,\sum_i q_i\sigma_i\right) &= \sum_i p_iTr(P\rho_i)-\sum_i q_iTr(P\sigma_i) \\ &= \sum_i p_iTr(P(\rho_i-\sigma_i))+\sum_i (p_i-q_i)Tr(P\sigma_i) \\ &\leq \sum_i p_iD(\rho_i,\sigma_i)+D(p_i,q_i), \end{aligned} \tag{32}$$

eşitsizliği ile ispat tamamlanmış olur.

Bu teoremin özel bir sonucu olarak, iz-uzaklığının girdilerinde birlikte konveks olduğu görülebilir:

$$D\left(\sum_i p_i\rho_i, \sum_i p_i\sigma_i\right) \leq \sum_i p_i D\left(\rho_i, \sigma_i\right). \tag{33}$$

**Öze-uygunluk (*Fidelity*)**

İki kuantum durum arasındaki mesafeyi ölçmek için ikinci bir yol olarak öze-uygunluk kullanılır. Öze-uygunluk aslında tam olarak şu anlama gelir: Gönderici bir mesajı kodlayarak gönderir. Alıcı aldığı kodlar üzerinde ölçümler yaparak mesajları çözer. Alıcının ölçüm sonucu elde ettiği durumların, göndericinin gönderdiği durumlara izdüşümü öze-uygunluk olarak tanımlanabilir. Öze-uygunluk, yoğunluk işlemcilerinin uzayında bir metrik tanımlamaz ama yararlı bir metriğin oluşmasına sebep olur. $\rho$ ve $\sigma$ durumlarının öze-uygunluğu

$$F\left(\rho,\sigma\right) \equiv Tr\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}} \tag{34}$$

olarak tanımlanır. İlk bakışta öze-uygunluğun simetrik olması net bir şekilde görülemeyebilir.

Öze-uygunluğun iki özel durumu üzerinde durulacaktır. Bunlardan ilki; bağıl entropide olduğu gibi, eğer $\rho$ ve $\sigma$ sıra değişiyorlar ise aynı ortogonal baz $|i\rangle$ üzerinde diagonal olurlar:

$$\rho = \sum_i r_i \left|i\right\rangle \left\langle i\right|; \sigma = \sum_i s_i \left|i\right\rangle \left\langle i\right| \tag{35}$$

Bu terimler (34) bağıntısında yerine yazılırsa,

$$\begin{aligned} F\left(\rho,\sigma\right) &= Tr\sqrt{\sum_i r_i s_i \left|i\right\rangle \left\langle i\right|} \\ &= Tr\left(\sum_i \sqrt{r_i s_i}\left|i\right\rangle \left\langle i\right|\right) \\ &= \sum_i \sqrt{r_i s_i} \\ &= F\left(r_i, s_i\right) \end{aligned} \tag{36}$$

haline getirilebilir. $\rho$ ve $\sigma$ sıra değiştiğinde kuantum öze-uygunluk $F(\rho,\sigma)$ klasik öze-uygunluğa $F(r_i,s_i)$ indirgenebilir. Buradaki $r_i$ ve $s_i$ sırasıyla $\rho$ ve $\sigma$'nın özdeğerleri olarak alınır.

İkinci durum ise saf bir durum $|\psi\rangle\langle\psi|$ ile rasgele bir durum arasındaki $\rho$ öze-uygunluğu hesaplamaktır. (34) ifadesi kullanılarak,

$$\begin{aligned} F(|\psi\rangle,\rho) &= Tr\sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} \\ &= \sqrt{\langle\psi|\rho|\psi\rangle} \end{aligned} \tag{37}$$

halini alır. Buradaki öze-uygunluk $|\psi\rangle\langle\psi|$ ile $\rho$'nun kesişiminin karekökü eşit olur. Öyle ki bu sonuç bize matematiksel anlamda faydalı bir eşitlik sağlayacaktır.

Kübit durumu için iki durum arasındaki iz-uzaklığını, basit bir geometrik yorum ile Öklidiyen uzaklığın yarısı olduğu gösterilmiştir. Fakat, bir kübitin iki durumu arasındaki öze-uygunluk için basit bir geometrik yorum yapmak ne yazık ki o kadar kolay değildir. Yine de; öze-uygunluk, iz-uzaklığı ile benzer özelliklere sahiptir. Örneğin; üniter dönüşümler altında invaryant kalır:

$$F\left(U\rho U^{\dagger},U\sigma U^{\dagger}\right)=F(\rho,\sigma). \tag{38}$$

**Teorem 2.3:[*Uhlmann Teoremi*]** $\rho$ ve $\sigma$, $Q$ kuantum sisteminin iki durumu olmak üzere, $Q$'nun bir kopyası olan $R$ sistemi ele alınsın. Öyleyse burada $RQ$ sistemi içerisinde $|\psi\rangle$, $\rho$'ya $|\varphi\rangle$ ise $\sigma$'ya ait olduğu varsayılarak

$$F(\rho,\sigma)=max_{|\psi\rangle,|\phi\rangle}\,|\langle\psi|\,\varphi\rangle| \tag{39}$$

eşitliği elde edilebilir.

Uhlmann teoremini ispatlamadan önce faydalı olabilecek bir lemma vardır.

**Lemma 2.4:** $A$ rasgele bir işlemci ve $U$ üniter olmak üzere,

$$|Tr(AU)| \leq Tr|A| \tag{40}$$

eşitsizliği sağlanır. Eşitlik durumu ise $U = V^\dagger$ seçilerek elde edilir ki $A = |A|V$ eşitliği $A$'nın ayrışımıdır.

**İspat:** Eşitliği görmek açıktır. Öyle ki

$$|Tr(AU)| = |Tr(|A|VU)| = \left|Tr\left(|A|^{1/2}|A|^{1/2}VU\right).\right| \tag{41}$$

Hilbert-Schmidt iç çarpımı için Cauchy-Schwarz eşitsizliği yazılırsa

$$|Tr(AU)| \leq \sqrt{Tr|A|\,Tr(U^\dagger V^\dagger|A|VU)} = Tr|A| \tag{42}$$

eşitsizliği ortaya çıkar ve bu da ispatın tamamlanmasını sağlar.

**İspat:[*Uhlmann Teoremi*]** $R$ ve $Q$ sistemlerine ait $|i_R\rangle$ ve $|i_Q\rangle$ bazları sabitlensin(fix). Çünkü $R$ ve $Q$ sistemleri aynı boyutta olduklarından indis $i$ aynı değer kümesinde olur. $|m\rangle \equiv \sum_i |i_R\rangle|i_Q\rangle$ olarak tanımlansın. Ayrıca $\rho$'yu saflaştıran bir $|\psi\rangle$ alınsın. Böylelikle Schmidt ayrışımı kullanılarak, $R$ ve $Q$ sistemleri üzerinde tanımlı $U_R$ ve $U_Q$ üniterleri için

$$|\psi\rangle = (U_R \otimes \sqrt{\rho}U_Q)|m\rangle \tag{43}$$

eşitliği yazılabilir. Benzer bir şekilde $|\varphi\rangle$, $\sigma$'ya ait bir saflaştırma ise $V_R$ ve $V_Q$ üniterleri vardır. Böylece

$$|\varphi\rangle = \left(V_R \otimes \sqrt{\sigma}V_Q\right)|m\rangle \tag{44}$$

yazılabilir. (43) ve (44) denklemlerinin iç çarpımı alınırsa,

$$|\langle\psi|\,\varphi\rangle| = \left|\langle m|\left(U_R^\dagger V_R \otimes U_Q^\dagger\sqrt{\rho}\sqrt{\sigma}V_Q\right)|m\rangle\right| \tag{45}$$

elde edilir. Hilbert-Schmidt iç çarpımı kullanılarak

$$|\langle\psi|\,\varphi\rangle| = \left|Tr\left(V_R^\dagger U_R U_Q^\dagger\sqrt{\rho}\sqrt{\sigma}V_Q\right)\right| \tag{46}$$

olduğu görülür. Eğer $U \equiv V_Q V_R^\dagger U_R U_Q^\dagger$ olarak alınırsa,

$$|\langle\psi|\,\varphi\rangle| = \left|Tr\left(\sqrt{\rho}\sqrt{\sigma}U\right)\right| \tag{47}$$

olur. Lemma B.4 kullanılarak,

$$|\langle\psi|\,\varphi\rangle| \leq Tr\left|\sqrt{\rho}\sqrt{\sigma}\right| = Tr\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \tag{48}$$

haline getirilebilir. Eğer $U_Q = U_R = V_R = I$ ve $V_Q = V^\dagger$ olarak alınırsa eşitliğin sağlandığı kolaylıkla görülebilir.

Üç derin gerçek bölümünde bahsedilen monotonluk özelliği büyük bir önem arz ediyor. Bu sebeple monotonluk üzerinde fazlasıyla durulacaktır.

**Teorem 2.5:[*Öze-uygunluğun monotonluğu*]** $\mathscr{E}$ iz-koruyan bir kuantum işlem, $\rho$ ve $\sigma$ yoğunluk işlemcileri olmak üzere,

$$F\left(\mathscr{E}(\rho),\mathscr{E}(\sigma)\right) \geq F\left(\rho,\sigma\right) \tag{49}$$

olur.

**İspat:** $RQ$ bileşik sisteminde; $|\psi\rangle$ ve $|\varphi\rangle$, sırasıyla $\rho$ ve $\sigma$ sistemlerine ait birer saflaştırma olmak üzere, $F\left(\rho,\sigma\right) = |\langle\psi|\,\varphi\rangle|$ eşitliği yazılabilir. Kuantum işlemler için çevre (*Environment*) $E$ olmak üzere, $\mathscr{E}$ başlangıç olarak $|0\rangle\langle 0|$ saf durumunda ve bir $U$ üniter işlemcisi ile $Q$ sistemine bağlı olsun. Burada $\mathscr{E}(\rho)$'nun bir saflaştırıcısı $U|\psi\rangle|0\rangle$ ve benzer şekilde $\mathscr{E}(\sigma)$'nın bir saflaştırıcısı da $U|\varphi\rangle|0\rangle$ olur. Uhlmann teoremi kullanılarak

$$\begin{aligned} F\left(\mathscr{E}(\rho),\mathscr{E}(\sigma)\right) &\geq \left|\langle\psi|\langle 0|U^\dagger U|\varphi\rangle|0\rangle\right| \\ &= |\langle\psi|\,\varphi\rangle| \\ &= F\left(\rho,\sigma\right) \end{aligned} \tag{50}$$

işlemleri yapılabilir. Böylece istenilen sonuca ulaşılmış olur.

**Teorem 2.6: [*Öze-uygunluğun güçlü konkavlığı*]** $p_i$ ve $q_i$ aynı girdi kümesi üzerinde tanımlanan olasılık dağılımları, $\rho_i$ ve $\sigma_i$ de yine aynı küme üzerinde tanımlı yoğunluk işlemcileri olmak üzere,

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq \sum_i \sqrt{p_i q_i} F\left(\rho_i, \sigma_i\right) \tag{51}$$

eşitsizliği elde edilir.

**İspat:** $|\psi_i\rangle$ ve $|\varphi_i\rangle$, sırasıyla $\rho_i$ ve $\sigma_i$ sistemlerine ait birer saflaştırma olmak üzere, $F\left(\rho_i, \sigma_i\right) = \langle\psi_i|\,\varphi_i\rangle$ olarak seçilsin. İspatı kolaylaştıracak bir yardımcı sistem tanımlansın. Öyle ki bu sistem $|i\rangle$ ortonormal bazlarına sahip olan ve $i$ girdi kümesi üzerinde tanımlı bir olasılık dağılımı olmak üzere,

$$|\psi\rangle \equiv \sum_i \sqrt{p_i}\,|\psi_i\rangle\,|i\rangle\,; |\varphi\rangle \equiv \sum_i \sqrt{q_i}\,|\varphi_i\rangle\,|i\rangle \tag{52}$$

olarak tanımlansın. Dikkat edilmelidir ki $|\psi\rangle$; $\sum_i p_i\rho_i$ teriminin, $|\varphi\rangle$ise $\sum_i q_i\sigma_i$ teriminin saflaştırıcısıdır. Uhlmann teoremi kullanılarak,

$$F\left(\sum_i p_i\rho_i, \sum_i q_i\sigma_i\right) \geq |\langle\psi|\,\varphi\rangle| = \sum_i \sqrt{p_i q_i}\,\langle\psi_i|\,\varphi_i\rangle = \sum_i \sqrt{p_i q_i} F\left(\rho_i, \sigma_i\right) \tag{53}$$

sonucu elde edilebilir.

### Uzaklık Ölçütleri Arasındaki İlişki

İz-uzaklığı ve öze-uygunluk kavramları farklı formlarda olmalarına rağmen, birbiri ile yakın bir ilişki içerisindedirler. Nitelik olarak bu iki kavram birçok uygulama için, birer eş uzaklık ölçüsü olarak düşünülebilir. Bu kısımda bu iki kavram arasındaki ilişki irdelenecektir.

Saf durumlar söz konusu iken, iz-uzaklığu ve öze-uygunluk tamamen birbirlerine eş kavramlara dönüşürler. Bunu görmek için, $|a\rangle$ ve $|b\rangle$ saf durumları arasındaki iz-uzaklığı ele alınsın. Gram-Schmidt prosedürü kullanılarak, $|a\rangle = |0\rangle$ ve $|b\rangle = cos\theta\,|0\rangle + sin\theta\,|1\rangle$ eşitliklerini sağlayan ortonormal durumlar $|0\rangle$, $|1\rangle$ bulunabilir. Kolaylıkla görülebileceği gibi $F\left(|a\rangle, |b\rangle\right) = |cos\theta|$ olur. Dahası,

$$
\begin{aligned}
D(|a\rangle,|b\rangle) &= \frac{1}{2}Tr\left|\begin{bmatrix} 1-cos^2\theta & -cos\theta sin\theta \\ -cos\theta sin\theta & -sin^2\theta \end{bmatrix}\right| \\
&= |sin\theta| \\
&= \sqrt{1-F(|a\rangle,|b\rangle)^2} \qquad (54)
\end{aligned}
$$

eşitliği hesaplanabilir. Bu bilgiler ışığında; iki saf durum arasındaki iz-uzaklığı, onların öze-uygunluk fonksiyonu olur. Ya da tam tersi olarak anlaşılabilir. Saf durumlar üzerinden konuşulduğunda bu ilişki saf olmayan durumlar(mixed states) için yeni bir bağıntı ortaya çıkarır. $\rho$ ve $\sigma$ iki kuantum durumu, $|\psi\rangle$ ve $|\varphi\rangle$ saflaştırıcılar olmak üzere $F(\rho,\sigma) = |\langle\psi|\,\varphi\rangle| = F(|\psi\rangle,|\varphi\rangle)$ eşitlikleri sağlanır. Kısmi-iz operasyonu altında iz-uzaklığının artmayan olduğu bilindiğinden,

$$
\begin{aligned}
D(\rho,\sigma) &\leq D(|\psi\rangle,|\varphi\rangle) \\
&= \sqrt{1-F(\rho,\sigma)^2} \qquad (55)
\end{aligned}
$$

olarak yazılabilir. Buradan anlaşılabildiği gibi eğer iki durum arasındaki öze-uygunluk birine yakın ise, durumlar ayrıca iz-uzaklığı anlamında da birbirlerine yakındır. Bu bilginin tersi de doğrudur. Bunu görmek için, $\{E_m\}$ bir *POVM*[6] ve $p_m \equiv Tr(\rho E_m)$, $q_m \equiv Tr(\sigma E_m)$ olarak alınırsa

$$
F(\rho,\sigma) = \sum_m \sqrt{p_m q_m} \qquad (56)
$$

eşitliği yazılabilir. Burada $p_m$ ve $q_m$ terimleri sırası ile $\rho$ ve $\sigma$ durumları için m çıktısının belirlenme olasılığıdır. İlk olarak

$$
\begin{aligned}
\sum_m (\sqrt{p_m}-\sqrt{q_m})^2 &= \sum_m p_m - \sum_m q_m - 2F(\rho,\sigma) \qquad (57) \\
&= 2(1-F(\rho,\sigma)) \qquad (58)
\end{aligned}
$$

eşitliği elde edilir. Fakat ayrıca $\left|\sqrt{p_m}-\sqrt{q_m}\right| \leq \left|\sqrt{p_m}+\sqrt{q_m}\right|$ eşitsizliği de doğru oldu-

[6]Pozitif değerli işlemciler *(Positive operator-valued measure)*

ğundan

$$\begin{aligned}\sum_m (\sqrt{p_m}-\sqrt{q_m})^2 &\leq \sum_m |\sqrt{p_m}-\sqrt{q_m}|\,|\sqrt{p_m}+\sqrt{q_m}| \\ &= \sum_m |p_m - q_m| \\ &= 2D(p_m, q_m) \\ &\leq 2D(\rho,\sigma) \end{aligned} \tag{59}$$

şeklinde bir bağıntı da elde edilebilir. (57) ve (59) ifadeleri kıyaslandığında

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \tag{60}$$

eşitsizliği kolaylıkla görülebilir. Bir de bu duruma (55) bağıntısı eklendiğinde

$$1 - F(\rho,\sigma) \leq D(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)^2} \tag{61}$$

eşitsizliği bulunur. Sonuç olarak; iz-uzaklığı ve öze-uygunluk, iki kuantum durumunun birbirlerine olan yakınlığının ölçüsü olarak algılanırsa, nitelik olarak aynı anlama gelirler. Aslında birçok uygulama için iz-uzaklığının ya da öze-uygunluğun hangisinin hesaplanacağı fark etmez. Çünkü biri diğerinin sonucu olarak ortaya çıkar.

## EK 3 Ayrışım (*Decomposition*) Çeşitleri

Bazı teoremler ve onların ispatlarında kullanılan ayrışım metotları uygulanmaktadır. Bu ayrışım çeşitlerinin bazıları ile ilgilenilecektir.
Spektral Ayrışım

Herhangi *Hermite-sel* işlemci[7]

$$A = \sum_n A_n |n\rangle \langle n| \tag{62}$$

formunda yazılabilir. Bu açılıma $A$'nın *spektral ayrışımı* denir. $\{|n\rangle\}$ bazına göre, $A$ köşegen matris gösterimine sahiptir:

$$A = köşegen(A_1, \cdots, A_d). \tag{63}$$

Burada $A_n$ $(n = 1, 2, \ldots, d)$ şeklinde gösterilen elemanlar $A$ işlemcisinin özdeğerleridir.

### Hilbert-Schmidt Ayrışımı

$\rho$ yoğunluk işlemcisinin özdurumları, $\{|k\rangle\}$ bazlarından oluşuyor olsun. Bu baz düzeninde yoğunluk matris diagonaldir. Özdeğer spektrumu $\{\lambda_i\}$, negatif olmayan ve toplamları 1 olan$(\sum_i \lambda_i = 1)$ reel sayıların birleşiminde oluşur. Yani aslında bir olasılık dağılımıdır denir. Öyleyse $\rho$ için spektral ayrışım,

$$\rho = \sum_k \lambda_k |k\rangle \langle k| \tag{64}$$

şeklinde yazılabilir. (64) denklemi $|k\rangle$ bazı halinde bulunan durumların, $\lambda_k$ olasılıklarının karışımları ile görülmesi anlamındadır.

$R$ sistemine ait bir yoğunluk işlemcisi $\rho^R$ ele alınsın. Bu işlemci $RQ$ bileşik sistemine ait dolanık bir $\left|\Psi^{RQ}\right\rangle$ sisteminin dolanık ve saf olan bir durumundan elde edilebilir. Dolanık durumu genişletmek için $\rho^R$ işlemcisinin özbazları (*eigenbasis*) kullanılabilir:

$$\left|\Psi^{RQ}\right\rangle = \sum_k \left|k^R\right\rangle \otimes \left|\psi_k^Q\right\rangle. \tag{65}$$

[7]Eğer gerçel değerli gözlenebilirler her n değeri için $A_n^* = A_n$ özelliğini sağlıyorsa, her A işlemcisi $A^\dagger = A$ özelliğini sağlar. Bu özelliğe sahip işlemcilere Hermite-sel denir.

Bundan dolayı yoğunluk işlemcisi,

$$\rho^R = Tr_Q \left|\Psi^{RQ}\right\rangle \left\langle\Psi^{RQ}\right| = \sum_k \left\langle \psi_k^Q \right| \left. \psi_k^Q \right\rangle \left|k^R\right\rangle \left\langle k^R\right| \tag{66}$$

şeklinde yazılabilir. Eğer bu eşitlik ile $\rho^Q$'nun spektral ayrışımı karşılaştırılır ise,

$$\left\langle \psi_k^Q \right| \left. \psi_k^Q \right\rangle = \lambda_k \delta_{kk'} \tag{67}$$

sonucu çıkarılır. $\left|\psi_k^Q\right\rangle = \left\langle k^R\right| \left.\Psi^{RQ}\right\rangle$ vektörleri ortogonaldir. Öyleyse $\left|k^Q\right\rangle$ vektörlerinin bir ortonormal kümesi bulunabilir:

$$\left|\psi_k^Q\right\rangle = \sqrt{\lambda_k} \left|k^Q\right\rangle. \tag{68}$$

(68) ifadesi ihtiyaç dahilinde $\mathscr{H}^Q$ Hilbert uzayı için bir baz üzerinde genişletilebilir. Dolayısıyla, dolanık durum

$$\left|\Psi^{RQ}\right\rangle = \sum_k \sqrt{\lambda_k} \left|k^R, k^Q\right\rangle \tag{69}$$

şeklinde tanımlanabilir. (69) eşitliği, $\left|\Psi^{RQ}\right\rangle$ dolanık durumunun *Schmidt ayrışımı* olarak bilinir.

**Kutupsal ve Tekil Ayrışımı (*Polar and Singular Value Decomposition*)**

*Kutupsal* ve *tekil ayrışımı* çizgisel işlemcilerin daha basit çarpanlar halinde yazılmasında faydalıdır. Daha detaylı konuşmak gerekirse; bu ayrışımlar çizgisel işlemcileri, üniter ve pozitif işlemcilerin çarpımları şeklinde ayırmaya yardımcı olurlar.

**Teorem 3.1: [Kutupsal Ayrışım]** $A$, bir vektör uzayı olan $V$ üzerinde tanımlı, bir çizgisel işlemci olsun. Öyleyse üniter $U$ ve pozitif işlemciler $J$ ve $K$ için

$$A = UJ = KU \tag{70}$$

denklemi yazılabilir. Burada seçilen $J$ ve $K$ biricik(unique) pozitif işlemciler $J \equiv \sqrt{A^\dagger A}$ ve $K \equiv \sqrt{AA^\dagger}$ denklemlerini sağlarlar. Dahası, $A$ işlemcisi tersinir(invertible) ise $U$ tektir.

Ayrıca $A = UJ$ sol, $A = KU$ ise sağ kutupsal ayrışım olarak tanımlanabilir.

**İspat:** $J \equiv \sqrt{A^\dagger A}$ olarak yazıldığından pozitif bir işlemcidir. Öyleyse $J$'nin spektral ayrışımı yazılabilir. $J = \sum_i \lambda_i |i\rangle \langle i|$, $\lambda_i \geq 0$. $|\psi_i\rangle \equiv A|i\rangle$ olarak tanımlansın. Tanım kullanılarak $\langle \psi_i | \psi_i \rangle = \lambda_i^2$ olduğu görülebilir. Sıfır olmayan $\lambda_i$'lere karşılık gelen $i$'ler ele alınırsa; her $i$ için $|e_i\rangle \equiv |\psi_i\rangle / \lambda_i$ tanımlanıp $|e_i\rangle$'lerin normalize olduğu görülebilir. Dahası, $i \neq j$ için

$$\langle e_i | e_j \rangle = \frac{\langle i | A^\dagger A | j \rangle}{\lambda_i \lambda_j} = \frac{\langle i | J^2 | j \rangle}{\lambda_i \lambda_j} = 0 \tag{71}$$

olduğundan ortogonaldirler denir.

$\lambda_i \neq 0$ durumunu sağlayan $i$ terimleri ile ilgilendik. Şimdi ise Gram-Schmidt prosedürünü kullanılarak, $|e_i\rangle$ortonormal kümesinin oluşturduğu ortonormal bazlara geçiş yapılabilir. Öyle ki bu bazlar da $|e_i\rangle$ notasyonu ile gösterilsin. Bir üniter işlemci $U \equiv \sum_i |e_i\rangle \langle i|$alınsın. $\lambda_i \neq 0$ olduğundan $UJ|i\rangle = \lambda_i |e_i\rangle = |\psi_i\rangle = A|i\rangle$ eşitliği sağlanır. $\lambda_i = 0$ olduğunda ise $UJ|i\rangle = 0 = |\psi_i\rangle$ sonucu görülebilir. Dolayısıyla $A$ ve $UJ$'nin, $|i\rangle$ bazı üzerindeki aksiyomları tanımlanmış olur. Sonuç olarak; $A = UJ$ eşitliği bulunur.

$J$ pozitif bir işlemci olmanın yanı sıra aynı zamanda tektir. Öyle ki $A = UJ$ terimini soldan *hermite-sel eşleniği* (*adjoint*)[8] $A^\dagger = JU^\dagger$ ile çarpılırsa, $J^2 = A^\dagger A$ eşitliği elde edilir. Eğer $A$ tersinir ise, $J$ de tersinirdir. Öyleyse $U$ özgün bir şekilde $U = AJ^{-1}$ ile belirlenebilir. Dolayısıyla, sağ kutupsal ayrışımın ispatı: $K \equiv UJU^\dagger$ pozitif bir işlemci olarak alınırsa $A = UJ = UJU^\dagger U = KU$ eşitliğinden gösterilebilir. $AA^\dagger = KUU^\dagger K = K^2$ olduğundan $K = \sqrt{AA^\dagger}$ eşitliği istenildiği gibi elde edilir.

Kutupsal ayrışım ve spektral ayrışımın birleştirilmesi ile tekil ayrışımı elde edilir.

**Corollay 3.2: [Tekil Ayrışım]** $A$ bir kare matris olmak üzere, $U$ ve $V$ üniter matrisleri ve negatif olmayan girdilere sahip köşegen bir matris olan $D$ alınırsa,

$$A = UDV \tag{72}$$

eşitliği yazılabilir. $D$ diagonal matrisinin elemanları $A$'nın tekil değerleridir.

[8] $\mathscr{H}$'de tanımlı her $|\alpha\rangle$ ve $|\beta\rangle$, $\langle \alpha | A^\dagger | \beta \rangle = (\langle \beta | A | \alpha \rangle)^*$ eşitliğini sağlıyorsa A Hermite-sel eşleniktir denir.

**İspat:** Kutupsal ayrışım kullanılarak; $S$ bir üniter, $J$ ise bir pozitif olmak üzere $A = SJ$ yazılır. Spektral teoremden yola çıkarak; $T$ bir üniter ve $D$ pozitif elemanlı diagonal olarak alınırsa, $J = TDT^{\dagger}$ eşitliği yazılır. $U \equiv ST$ ve $V \equiv T^{\dagger}$ eşitliklerinden ispat tamamlanmış olur.

## UYGULAMALAR

### Kraus Gösterimi

Bir sistem olan $QE$, $E$ çevresi $|0\rangle$ saf durumunda , $G$ ise açık $Q$ sistemine ait bir işlemci (yoğunluk işlemcisi); $U$ ise kapalı (yalıtılmış) $QE$ bileşik sisteminin üniter gelişimini temsil etmek üzere, çevre üzerinden iz alınıp çevre aradan çıkarıldığında, $Q$'nun indirgenmiş gelişimini betimleyen $(\mathscr{E})$ kuantum kanal (kuantum gelişim, durum dönüşümü)

$$\mathscr{E}(G) = Tr_E U\left(G \otimes |0\rangle\langle 0|\right) U^{\dagger} \tag{73}$$

şeklinde tanımlanır. Burada $E$'nin Hilbert uzayı için özel bir baz olan $\{|e_k\rangle\}$ seçilsin. Her $k$ için bir işlemci olan $A_k$ ve $U \in \mathscr{H}^{QE}$, her $\phi \in \mathscr{H}^{Q}$ için,

$$A_k |\phi\rangle = \langle e_k | U | \phi, 0\rangle \tag{74}$$

şeklinde ifade edilir. Burada çevre $E$ ile $U$ etkileşimi kullanılır olmasına rağmen, $A_k$ işlemcileri sadece $\mathscr{H}^{Q}$ üzerinde işlem görürler. (13) bağıntısında gösterilen kısmi iz ifadesini uygulayabilmek için seçilen özel $\{|e_k\rangle\}$ bazı kullanılır. Eğer bir saf durum olan $|\phi\rangle$ üzerinde işlem yapılırsa;

$$\begin{aligned} \mathscr{E}\left(|\phi\rangle\langle\phi|\right) &= \sum_k \langle e_k| U\left(|\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|\right) U^{\dagger} |e_k\rangle \\ &= \sum_k A_k |\phi\rangle\langle\phi| A_k^{\dagger} \end{aligned} \tag{75}$$

sonucuna ulaşılır. $Q$ için tanımlı herhangi bir yoğunluk işlemcisi, saf yoğunluk işlemcilerinin bir çizgisel kombinasyonları şeklinde yazılabileceğinden

$$\mathscr{E}(\rho) = \sum_k A_k \rho A_k^{\dagger} \tag{76}$$

bağıntısı genellenebilir. Bu denklem bir gönderim olan $\mathscr{E}$ için Kraus gösterimi ve $A_k$ terimleri ise Kraus işlemcileri olarak tanımlanır. Bir Kraus işlemcisi normalizasyon koşulunu sağlar.

### Klasik ve Kuantum Kanallar

Günlük iletişimler klasik kanallar vasıtasıyla gerçekleşmektedir. Klasik bir kanal ayan

beyan olduğundan, klasik kanallar ile taşınan bir bilgi üçüncü bir kişi tarafından elde edilebilir. Klasik kriptografi üçüncü kişilerin klasik kanalları bölmesini ve bilgiyi elde etmesini her ne kadar engellemeye çalışsa da sadece geciktirme gerçekleştirebilir.

Bu duruma farklı bir açı ile yaklaşılırsa kuantum kanallar ile karşılaşılacaktır. Kuantum kanallar, klasik kanallardan farklı bir duruma sahiptir. Kuantum kanal ile iletişim sırasında üçüncü bir kişi iletişime dahil olmaya çalışırsa aktarılan bilgi bozulacak ve kanala sızılmaya çalışıldığı ortaya çıkacaktır. Kuantum kanallar tamamen pozitif ve iz koruyan çizgisel gönderimlerdir. Klasik kanallar ile sadece klasik bilgi gönderilebiliyor iken, kuantum kanallar ile hem klasik hem de kuantum bilgi aktarılabilir. Kuantum kanallarda kübitin herhangi bir durumu yoğunluk işlemcisidir. Kübir dönüşümleri kuantum kanallar ile ifade edilir. Başka bir örnek olarak CPTP[9] gönderimler kuantum kanal olarak tanımlanabilir.

$\mathscr{E} : B(\mathscr{H}_A) \to B(\mathscr{H}_B)$ tanımlı bir gönderim olmak üzere eğer $A \in B(\mathscr{H}_A)$ olan her $A \geq 0$ için $\mathscr{E}(A) \geq 0$ koşulunu sağlıyor ise $\mathscr{E}$ pozitiftir denir. $\mathscr{H}_A \to \mathscr{H}_C \otimes \mathscr{H}_A = \mathscr{H}_{CA}$ olarak alınır ve eğer $B(\mathscr{H}_{CA}) \to B(\mathscr{H}_{CB})$ olarak tanımlanan $(id_k \otimes \mathscr{E})$ gönderimi pozitif ise $\mathscr{E}$ k-pozitif olarak tanımlanır. Her $k \in \mathbb{Z}_+$ değeri için eğer $\mathscr{E}$ pozitif ise, $\mathscr{E}$ tamamen pozitiftir (CP) denir.

$\Phi : M_n \to M_m$ şeklinde tanımlanan bir gönderim olmak üzere eğer $Tr\Phi(A) = TrA$ eşitliği sağlanıyor ise $\Phi$ iz korur (*trace preserving* - TP) denir. Her $A \in M_n$ için

$$\begin{aligned} Tr\left(\sum_{j=1}^{r} F_j A F_j^\dagger\right) &= TrA \\ Tr\left(\sum_{j=1}^{r} A F_j^\dagger F_j\right) &= TrA \\ Tr\left[A\left(\sum_{j=1}^{r} F_j^\dagger F_j - I_n\right)\right] &= 0 \\ \sum_{j=1}^{r} F_j^\dagger F_j &= I_n \end{aligned} \tag{77}$$

adımları ile kuantum kanalların iz korunumu gösterilir.

[9] *Completely positive and trace-preserving (CPTP map)*

**Durum Dönüşümleri (*State Tranformations*)**

Başlangıçta $\rho$ durumuna sahip olan bir kuantum sisteminin Hilbert uzayı $\mathscr{H}$ olsun. Eğer bu kuantum sistem izole (yalıtılmış) değil ise başka bir sistem olan *çevre* ile etkileşime girer. Çevre, $\mathscr{H}_e$ Hilbert uzayına ve $\rho_e$ istatiksel operatöre sahip olmak üzere, etkileşmeden önce tüm sistem $\rho_e \otimes \rho$ yoğunluk işlemcisine sahipse, etkileşmeden kaynaklı dinamik değişim bir üniter işlemci ile tanımlanabilir. Öyle ki $Tr_E U(\rho_e \otimes \rho) U^\dagger$ yeni istatiksel işlemci olarak ortaya çıkar. Bu durumda $\tilde{\rho}$ ilgilenilen kuantum sisteminin yeni istatiksel işlemcisi olarak alınabilir. Buradaki küçük değişim (*affine change*) $\rho \to \tilde{\rho}$ kuantum mekaniği için özgündür ve buna *durum dönüşümü* (*state transformation*) denir. Bu şekilde tanımlanan $\rho \to \tilde{\rho}$ gönderimi yoğunluk matrisleri üzerinde tanımlanır ve çizgisellik özelliği kullanılarak tüm matrislere genişletilebilir. Dolayısıyla bu yol ile iz-korunumlu ve pozitifliği koruyan çizgisel dönüşümler elde edilebilir.

Bir çizgisel gönderim olan $\mathscr{E}$ için, eğer $id_n \otimes \mathscr{E}$[10], herhangi bir matris cebir üzerinde tanımlanan ve özdeşlik gönderimi olan $id_n : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ için pozitifliği koruyor ise $\mathscr{E}$ tamamen pozitif (completely positive) denir.

Yukarıda tanımlanan durum dönüşümü başka formlarda da gösterilebilir. Öyle ki bu formlar içerisinde çevre tamamen çıkarılmış da olabilir. Varsayılsın ki $\rho$, $n \times n$ olarak tanımlanan bir kare matris ve $(z_1, z_2, \ldots, z_m)$, m-boyutlu $\mathscr{H}_e$ uzayında tanımlı bir birim vektör olmak üzere $\rho_e$, $(z_k \bar{z}_l)_{kl}$ formunda tanımlansın. Burada $\rho_e$ saf bir durum olarak alınır. $\mathscr{H}_e \otimes \mathscr{H}$ üzerinde etki eden tüm işlemciler blok-matris formunda yazılabilir. Öyle ki $m \times m$ matrisler $n \times n$ girdiler ile tanımlanır. Aslında, $U = \left(U_{ij}\right)_{i,j=1}^{m}$ ve $U_{ij} \in M_n$ olarak görülebilir. Eğer $U$ üniter ise $U^\dagger U$ birim olur ve bu durum

$$\sum_i U_{ik}^\dagger U_{il} = \delta_{kl} I_n \tag{78}$$

sonucunu ortaya çıkarır. İndirgenmiş yoğunluk matrisleri için var olan kısmi-iz bağıntısı kullanılarak;

[10] id: özdeşlik dönüşümü

$$
\begin{aligned}
\tilde{\rho} &= Tr_E\left(U\left(\rho_e \otimes \rho\right)U^{\dagger}\right) \\
&= \sum_i \left(U\left(\rho_e \otimes \rho\right)U^{\dagger}\right)_{ii} \\
&= \sum_{i,k,l} U_{ik}\left(\rho_e \otimes \rho\right)_{kl}\left(U^{\dagger}\right)_{li} \\
&= \sum_{i,k,l} U_{ik}\left(z_k \bar{z}_l \rho\right)\left(U_{il}\right)^{\dagger} \\
&= \sum_i \left(\sum_k z_k U_{ik}\right)\rho\left(\sum_l z_l U_{il}\right)^{\dagger} \\
&= \sum_i A_i \rho A_i^{\dagger}
\end{aligned} \tag{79}
$$

bağıntısı elde edilir. Burada $A_i \coloneqq \sum_k z_k U_{ik}$ olarak tanımlanan işlemciler

$$\sum_p A_p^{\dagger} A_p = I \tag{80}$$

eşitliğini sağlar. (78) denklemi kullanılarak da $\sum_k |z_k|^2 = I$ bağıntısı elde edilir.

**Teorem 4.1:** $\rho \mapsto \mathscr{E}(\rho)$ herhangi bir kuantum kanal olmak üzere

$$\mathscr{E}(\rho) = \sum_p A_p \rho A_p^{\dagger} \tag{81}$$

formunda yazılabilir. Tersine, bu formdaki bütün çizgisel gönderimler durum dönüşümleridir.

**İspat:** Teoremin ilk kısmı yukarıda çıkartılmıştır. Tersine durumu ispatlamak için ise,

$$A_i \coloneqq \sum_k z_k U_{ik} \;\; (i = 1, 2, \ldots, m) \tag{82}$$

denkleminin çözülmesi gerekmektedir. Basit bir seçim ile $z_1 = 1$ ve $z_2 = z_3 = \ldots = z_m = 0$, denklemler $U_{p1} = A_p$ durumuna indirgenebilir. Bunun anlamı; $U$ blok-matrisinin ilk sütunu verilmiş olur ve $U$'nun üniter olma koşulu ile diğer sütunlar belirlenir. (80) bağıntısının eşitlik koşulu ile bu durum sağlanır. (80) denkleminin anlattığı durum ise blok-matrisin ilk sütunu bir izometri belirtir ki bu izometri bir ünitere genişletilebilir.

Operatör-toplam açılımında katsayılar olan $A_p$ terimlerine, durum dönüşümünün operatör elemenları denir. Durum dönüşümleri terimi yerine kuantum işlemi ya da kanal dönüşümü denilebilir. Durum dönüşümü, elemanları pozitif ve iz-koruyan çizgisel dönüşümler kümesinin bir konveks altkümesini oluşturur.

**Teorem 4.2:** $\mathscr{E} : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ bir çizgisel gönderim olmak üzere, ancak ve ancak

$$\mathscr{E}(A) = \sum_u V_u A V_u^\dagger \tag{83}$$

açılımı yazılabiliyorsa, $\mathscr{E}$ tamamen pozitif denir. Burada $V_u : \mathbb{C}^n \to \mathbb{C}^k$ olarak tanımlı çizgisel operatörlerdir.

Bu sonuç ilk olarak Kraus tarafından ispatlanmıştır. Bir durum dönüşümü tamamen pozitif ve operatör toplam açılımına ayrıca Kraus ayrışımı[11] denir. Bu gösterim biricik değildir.
$\mathscr{E} : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ bir çizgisel gönderim olsun. $\mathscr{E}$, blok matris olan $\left(X_{ij}\right)_{1\leq i,j\leq k}$ tarafından belirlenir. Öyle ki burada

$$X_{ij} = \mathscr{E}\left(E_{ij}\right) \tag{84}$$

eşitliği kullanılır. $E_{ij}$ ise matris birimlerini temsil eder. Bu denkleme $\mathscr{E}$'nin blok matris gösterimi denir.

**Teorem 4.3:** $\mathscr{E} : M_n(\mathbb{C}) \to M_k(\mathbb{C})$ bir çizgisel gönderim olsun. Ancak ve ancak açılım blok matrisi $\left(X_{ij}\right)_{1\leq i,j\leq k} \in M_k(\mathbb{C}) \otimes M_n(\mathbb{C})$ pozitif ise $\mathscr{E}$ tamamen pozitif olur.

Kraus ayrışımı ve blok matris gösterimi, bir durum dönüşümünü sonlu boyutlarda tanımlamak için en iyi yollardır.

[11] Ayrışım çeşitleri için ek kısmı incelenebilir.