東京大学数理情報学談話会

日 時： **2025年12月2日　16時00分 ～18時00分**

場所：東京大学工学部6号館3階 セミナー**AD**

タイトル：シャノン理論から情報スペクトル理論へ

講演者：韓 太舜 名誉教授（電気通信大学）

アブストラクト（資料）：

A. シャノン理論の歴史

情報理論は Claude E. Shannon が 1948 年に創始してから今年で 77 年になる．その誕生は間を置かず多方面に爆発的な衝撃を与え一大ブームを巻き起こしたが，その要因は，多義的で捉えどこのない「情報」を確率モデルを介して「情報量」という形で客観的に再定義したことにあった．そして，そのように定義された「情報と情報量」というものが，実は，「符号化・復号化（情報のデジタル化）」という工学的操作・工学的制御の対象であり，その操作・制御の下で達成し得る「情報」の理論的可能性と理論的限界を規定しているということを明らかにしたのである．天才 Shannon の天才たる所以である．

かくして，（定常無記憶性という制約があったものの），「情報理論」は「エントロピー」と「通信路容量」という新概念を引っ提げて，一挙に「科学的理論」への仲間入りを果たしたのである．続く 1950—1960 年代には，Shannon の「情報理論」に対する数理的基礎付けと共に様々で斬新な「符号化法」が次々と発表され，活発な理論研究活動が展開された（Shannon, Fano, Feinstein, Elias, Wolfowitz など）．有名な Fano の不等式もこの時代に作られた．例外的ではあるが，有限記憶通信路や有限状態通信路などMarkov記憶型情報システムも考えられ研究された．その後は，紆余曲折を経つつも，「情報理論」は，広範な工学的諸問題に応用され，情報圧縮や情報伝送などの具体的通信問題を技術的に解決するためのほぼ「唯一無二」の guiding principle としての成長発展を遂げることになる．

「情報理論」がこのような工学的成功を収めつつあるのに並行して，1950 年代初頭から，「情報理論」の理論体系としての確率論的・数学的構造に関する研究も進められた．この方面には，主として，東欧，ソ連，米国 などの 確率論研究者らが参加したが，彼らの主な関心は， Shannon の「情報理論」が大前提とした情報源や通信路の「定常性」と「無記憶性」の仮定を取り払って，「情報理論」の最も一般的なモデルを，「（整合性条件を満たし記憶を持つ）確率過程間の変換」として定式化することにあった．そのような枠組みの中で，「無限入力系列から無限出力系列への定常的変換」としての様々な通信

路問題が研究された（Birkoff, Adler, Nedoma,Breiman, Feinstein, Parthasarathy, Winkelbauer, Dobrushin, Pinsker, Kolmogorov など）．ここでは， Shannon による「情報理論」の数学的精緻化，エルゴード情報源の漸近等分割性（Shannon-McMillan-Breiman の定理），定常情報源や定常通信路のエルゴード分解定理，個別エルゴード定理，確率過程の同型定理，などの確率論的に重要な成果が輩出したが，工学的通信路容量の立場から見れば，通信路容量の定義が異なったり，通信路容量が相互情報量レートの最大値としてしか計算できないような通信路（確率過程）のクラスのみに研究が限定され，最後までその制約から脱却することは出来なかったと言えよう．彼らは，一貫して 「情報理論」を確率論の一分野とみなして，議論の確率論的精緻性を重視し，Shannon の「情報理論」が本来持っていた「工学的操作」という側面にはそれほど関心がなかったようにも見える．そのため，大抵の場合(漸近等分割性定理，個別エルゴード定理，などを除いて），彼らの理論的結果から「具体的な工学的知見」を引き出すことは難しかった．やはり，ここでも，「整合性を満たす定常（エルゴード）確率過程」という呪縛からは逃れられなかったのである．

一方，1970 年代初頭に入り，人工衛星間通信や無線通信など様々なネットワーク通信の全盛時代に突入し始めると，情報源や通信路のモデルとして，Shannon の単一ユーザー・モデルに代わって，多数のユーザーが共通の通信媒体を介して情報を「同時に」やり取りする「多ユーザー情報理論（multi-user information theory)」を考える工学的必要に迫られて来た．そこで，数学と工学の両方のセンスを持った研究者が参入し始め，彼らが生み出したのが，multiple-access channel (多入力，単一出力），broadcast channel（単一入力，多出力），interference channel（多入力，多出力），relay channel (中継局を介した通信路）などの多彩な通信路モデルである．これらの新モデルでは，多ユーザーが同時に通信できる伝送レートには trade-off があり，「通信路容量」という単一の実数に代わって，多次元の「通信路容量域」というベクトル領域をどう決定するかが問題になった．問題は格段に難しくなるが，本質を探るために， Shannon のように再び「定常性」と「無記憶性」という仮定を置くことによって，多くの輝かしい理論的成果（各種の美しい容量域定理）を生み出すことに成功した（Ahlswede, Cover, Berger, Massey, Wyner, Ziv, Csiszar, Slepian, Wolf, など）．このような高揚した雰囲気の中で，情報理論全般に対する知見も大いに深まり，例えば，Shannon が補助量として便宜的に定義した「条件付きエントロピー」や「条件付き相互情報量」の操作的意味も，具体的な多ユーザー通信システムを考える中で初めて明らかにされた．さらに，ユニバーサル情報源符号化やユニバーサル通信路符号化などの画期的な符号化法が発表され，「情報理論」の研究に新風を吹き込んだ．その意味で，Shannonによる「情報理論」創始に続く1950年代を第一の黄金時代とすれば，この1970 年代は第二の黄金時代であるとも言えよう．ここに至って，Wyner (1974) は，Shannon以来発展して来た情報理論の理論的体系（可能性と限界，最適性を研究の主題とする）をまとめて「Shannon Theory」と命名した．Newton 以来の力学が「Newton Dynamics」と称されていたことを意識していたのかもしれない．また，時代の工学的要請にも応えて，これらの理論的限界を達成するための各種アルゴリズムも考案され，今日の高度情報社会（インターネット，スマホ，ATM, 各種決済システム，

GPS (全地球測位システム)，人工衛星間通信，深宇宙通信，など）の技術的基盤に至る理論的基礎を築いた．要するに，我々が現在住んでいる世界は，「情報理論に基づく工学的技術」なしには全く成り立たないのである．

B. 情報スペクトル理論の誕生

以上のような情報理論・情報技術の目覚ましい成功にも拘わらず，「記憶を有する最も一般的な情報源」というものはどう定義すべきで「記憶を有する最も一般的な通信路」というものもどう定義すべきか，そして，それらに対する「符号化と復号化」というものはどう定義すべきか，また，それらの通信路容量に対する一般公式を統一的に記述することは果たして可能なのか，という根本的な理論問題が未解決のまま残されていた．このことが伝統的な相互情報量レートのみを用いては解決不可能であることは早くから認識されてはいたものの，どうすれば良いか，手付かずのままでいたのである．

転期は，1980 年代末になって，Ahlswede と Dueck に依る「同定符号（identification code)」という新符号概念の発表によってもたらされた．この符号は，それまでの Shannon 流の伝送符号（伝送できるメッセージの個数がブロック長の指数関数）と全く異なるもので，多数の仮説検定問題を一つの通信路上に乗せて実現しようとするものであり，その結果，通信路を通して伝送できるメッセージの個数がブロック長の２重指数関数になるというそれまでの常識を大きく破る驚くべき符号であった．ここで，研究者達は，Shannon 伝送符号と Ahlswede-Dueck 同定符号を一つの枠組みの中でどう折り合いをつけ統一的に定式化すれば良いのかという新たな問題を突きつけられることになった．結論を言えば，この難問を克服しようとする努力の中で生まれたのが，1990 年代前半に Han と Verdu によって発表された「情報スペクトル理論 (Information Spectrum Theory)」であった．そこで考えられた情報源や通信路は，それぞれ，「一般情報源」と「一般通信路」と呼ばれ，次のように特徴づけられる：

1) 情報源も通信路もブロック系列（各ブロックの長さは任意で違って良い）の確率過程とするが，ブロック間の「確率的整合性条件」は満たす必要はない．
2) 各ブロック内では任意の記憶構造が許される（非定常でも非エルゴードでも良い）．
3) その結果，確率的上下極限という二つの極限操作が常に定義できる（下記参照）
4) 情報源アルファベットや通信路アルファベットも有限である必要はなく任意で良い．

これらの特徴のうち， Shannon theory の根幹をなす前提と決定的に異なるのは，1) の「整合性条件を仮定しない」というものである．と言うのは，Shannon theory は，その全歴史を通じて，確率論的な意味での（整合性条件を満たす）確率過程という枠組み（束縛）を超えることは無かったからである．しかし，1）の特徴によって，2) の特質も可

能になったのである，しかし，このように一般的な情報源や通信路を扱うための数学的道具として，確率論の標準的な収束概念である「確率収束」や「概収束」がもはや無用であることは明らかであった．それらに代わって，情報スペクトル理論で新しく導入されたのが，上記「確率的上極限 (limit superior in probability)」と「確率的下極限 (limit inferior in probability)」という二つの確率的極限操作であった．これは，どのような確率変数列（整合性条件を満たす必要はない）に対しても（無条件に常に！）定義されるもので，確率論での確率収束や概収束が適切な条件を満たす確率過程にしか定義できないのと対極にある．要するに，この「確率的上極限」と「確率的下極限」という操作は，確率論の立場からは全く無縁であるが，情報理論の立場からは，情報の符号化・復号化の本質を追求し続けた結果必然的に到達した必須の数学的操作なのである．（ここで，「確率的上極限」と「確率的下極限」という操作を非確率的な実数列に対して適用したものは，解析学で登場する上極限と下極限に他ならない．特に，実数列の極限は常に存在するとは限らないが，上極限と下極限は常に存在することに対応している）．こうして新たに導入された「確率的上下極限」という操作は，全ての一般情報源と一般通信路に対しても数学的に定義できるので，これを用いて，一般情報源の最適符号化レートや一般通信路の通信路容量を（例外なく常に！）統一的に記述する一般公式を与えることが可能になったのである．さらに，この手法は，乱数生成，仮説検定，レート・歪理論，多ユーザー情報理論，など情報理論の他の主要分野にも（無条件に常に！）適用され重要な結果を生み出すことも明らかにされ，これらはまとまって，Information Spectrum Methods という一分野を形成している．

ここで，特に強調しておきたい情報スペクトル理論の重要な副産物は次の3つである．
一つ目は，一般通信路の通信路容量に対する一般公式は「確率的下極限」で記述されることは分かったが，それでは，もう一つの「確率的上極限」で記述される「情報理論的実体」は果たして何なのか，そしてそれはそもそも存在するのか，という情報スペクトル的問題が提起されたが，結論を言えば，それは実際に存在し，「通信路分解能（channel resolvability）」という通信路理論の（全く新しい!）「操作的基本概念」を統一的に記述するものに他ならないことが判明したのである．この新概念は，上記「同定符号」の 強逆性（未解決問題）を証明するために決定的な役割を果たしただけでなく，その後も，通信路を介した各種の秘密通信問題を解析するための理論的武器として重用されている．
二つ目は，Shannon 以来，情報理論の体系全体を貫いて，陰に陽に様々な形で議論や論争が繰り返されて未解決だった「強逆性問題」を，そのための統一的な「必要十分条件」を与えることによって最終的に解決したことである（これも情報スペクトル的「確率的上下極限」を用いて記述される）．三つ目は，従来の Shannon theory 中ではその位置付けが曖昧だった「仮説検定問題」が実は，情報源符号化問題（や通信路符号化問題）

をその一部として含む情報理論の中の「中核的理論」の一つであるという情報スペクトル的構造を明らかにしたことである.

以上をまとめれば, Information spectrum theory は, Shannon theory の長い歴史を通じて到達した一つの「結節点」であると言って良いであろう. これによって, 「情報理論」は最終的に「確率論の呪縛」から解放され, 独自の方法論と独自の論理展開を持つ独自の理論体系に成長するまでに至ったのである.

C. 情報スペクトル理論から量子情報スペクトル理論へ

振り返ってみれば, 今まで 50 年もの間ひたすら, Shannon theory の研究だけに没頭して来た門外漢からすると, 長い歴史を持つ重厚な量子力学研究の陰で "細々としかし着実に" 進められて来たと思っていた「量子情報理論」の研究が, 2000 年代初頭に入って突如として一斉に開花し始めたかに見える. この頃, 盛んに, non-i.i.d. とか beyond i.i.d. というような言葉を聞くようになり, 小生も関連するワークショプや研究会に参加したことがあったが, それは, Shannon theory の大前提だった「定常無記憶性」から離れていよいよ本格的に non-i.i.d. の世界に参入する時代になり, information spectrum theory の出番が来たことを意味するものと無邪気に喜んでいた.

ところが, 時は大分経ち今年になって, 小川朋宏さんや林正人らが書いた「情報科学入門」という本に目に通す機会があり, 少し読んでみた所ですっかり虜になり夢中で読み進み, 読了後には深い感動に囚われてしまった. 量子概念の説明も定理の証明も完璧で, そこには, 今まで見たことのない夢のような「量子情報という名の別世界」が繰り広げられていたではないか. 浦島太郎のような心境であった. もう少し若かった時に出会えていれば良かったと悔みながらも, 一念発起して, 関連するいくつかの原著論文を読んでみることにした. まず易しそうな所から, Datta と Renner の論文 "Smooth entropies and quantum information spectrum" (2009) を読んで見て, 情報スペクトル理論を取り巻くおおよその状況を理解した. すなわち, non-i.i.d. というのは量子情報理論の側からの切実な要求であったこと, 「確率的上下極限」という基本操作は量子論においても必須なものであるとして, その量子版を簡潔に見事に定式化しており, 特に, ダイバージェンス・レートやエントロピー・レートに対する「確率的上下極限 」の量子版が量子情報理論において重要な役割を果たすこと, さらには, 量子論的乱数生成問題からの要請に応えるために独自に導入された smooth min- max- entropy という量 (one-shot)のレートに対する漸近的上下極限が実は対応する情報スペクトル的量の「確率的上下極限の量子版」に完全に一致すること, 従って, このような事実からしても, 「確率的上下極限 」という情報スペクトル的操作の導入は, (古典論においても量子論においても) fully justify されるということを理解した.

次に，Bowen と Datta の論文 "Quantum coding theorems for arbitrary sources, channels and entanglement resources" (2006) に取り掛かってみた（この論文は IEEE-IT に submit されたようだが，何故か未だに出版されていない）．ここでは，一般量子情報源に対する符号化定理，一般量子混合情報源に対する符号化定理，一般量子通信路に対する古典容量定理，一般量子情報源に対する超稠密符号化定理が，「確率的上下極限の量子版」だけを用いて統一的に極めて整然と導出されており，Shannon theory の「結節点」としての「情報スペクトル理論」に入れ込んだ者としては，量子論の初心者ながら，この辺りの論理展開が一番腑に落ちる．

以上の準備のもとに，重要だが最も手強そうに見えた Hayashi と Nagaoka による二つの論文に挑戦して見た：すなわち，論文1”General formulas for capacity of classical-quantum channels" (2003) と論文2”An information-spectrum approach to classical and quantum hypothesis testing for simple hypothesis” (2007)の二つである．このうち，論文1では，一般古典-量子通信路の通信路容量を与えることが主テーマであるが，ここでも，（古典）情報スペクトル理論で確立された理論構成に沿って，「確率的上下極限の量子版」を用いた議論を展開している．しかし，ここで特筆すべきは，符号化定理の direct part を導くための補題である “Feinstein’s lemma” の量子版および converse part を導くための補題 “Verdu-Han’s lemma”の量子版を確立したことである．まことに見事で感嘆するしかない．この二つの強力な lemmas から所期の通信路容量の公式を導くことは straightforward である．また，古典-量子通信路容量の一般公式から特別の場合として，定常無記憶通信路(Holevo 通信路）に対する容量公式を導く際に converse part を証明する論理は（古典）情報スペクトル理論におけるそれに倣っている．一方，この二つの補題を用いて（古典）情報 スペクトル理論における一般通信路容量の導出過程に倣えば，有限の誤り確率を許容した場合の一般古典-量子通信路の容量公式が直ちに従うのにもかかわらず，この論文ではそれには触れていない，惜しまれる．また，この論文では，Hilbert 空間の次元は任意（finite でも infinite でも良い）としているが，通常の行列演算操作しか身に付いていない「初学者」にとっては finite でなければ理解不能である．また，（古典）情報スペクトル理論では，有限とは限らない任意のアルファベット（ここでは通信路アルファベット）の下でも理論展開が統一的に行えることを「売り」にしているが，量子情報理論でもそれは可能なのかどうかそれが分からない．例えば，演算子が「連続スペクトル」を持つような場合には，どうすれば良いのであろうか．その場合でも，量子演算で中核をなすスペクトル展開などのような様々な操作が自在に行えるのであろうか．

次は，論文2についてである．量子情報源に対する仮説検定における誤り確率の一般公式を与えることが主テーマであるが，ここでも，（古典）情報スペクトル理論で確立された

理論構成に沿って，（ダイバージェンス・レートの）「確率的上下極限の量子版」を用いた議論を展開して「一般量子情報源」を扱うことに成功している．最初に，簡単であるが極めて重要な量子不等式 Tr(A{A>0})¥le 0 と Tr(A{A>0})¥le Tr{AT}を示した上で，これから直ちに，量子版の Neyman-Pearson Lemma を得ている（ T は 0¥le T¥le I なる任意の演算子）．この論文では，たったこれだけの二つの不等式から，（古典）情報スペクトル理論が確立した一般情報源仮説検定に関するほとんど全ての主要定理（一般 Stein's lemma，有限の誤り確率を許した場合の一般 Stein's lemma，一般 Hoeffding theorem，など）の量子版が続々と導出されるが，そもそも，こんなに「旨い」話がこの世で許されて良いのだろうか，と思える程である．これらの定理の証明にはある種の「量子的技巧」を要するが，論理展開は統一的で見通しが良く，（古典）情報スペクトル理論において，一般 Hoeffding theorem の証明であれほど苦闘したことがまるで嘘のようである（「雛形」というものが全く無かったので，無理もなかったかもしれないが）．ところで，この論文は， “present a unifying framework to treat the classical and quantum generalized hypothesis testing problem in the most general and simplest manner” ということやそれに類する趣旨のことを繰り返し強調しているが，実態に即して言えば，（古典）一般情報源仮説検定に関する情報スペクトル理論の主要定理をほぼそのまま量子的技巧を用いて「翻訳・変換」したと言うことではないだろうか．それを，”unifying framework” と言うのは，やや無理があるのではないだろうか．しかし，本論文の極めつきの「ハイライト」は，一般 Hoeffding 型の量子仮説検定に関する各種の誤り指数問題を整理し，それらに simple かつ beautiful な解決を与えたことであろう．その古典版はその結果として直ちに導かれ，すでに知られていた古典の定理に一致する（一部はその refinement になっている）．ここでは， Hilbert 空間の次元は finite であるとして議論を展開し，infinite でも同様との注記をしているが，にわか仕立ての「初学者」にとっては，やはり，ここに述べられている全ての定理と全ての証明は，次元が finite とした上でしか理解できないものであった．次元が infinite の場合については，手掛かりすら掴めず小生の守備範囲をはるかに超えていた．一般古典仮説検定では情報源アルファベットは finiteでもinfiniteでも論理展開は全く変わらないことを考えると，誠に残念であった．

また，（古典）情報スペクトル理論で一般情報源符号化問題に対して確立された諸公式は，ここでの一般量子仮説検定に対する定理のcorollary だとしてそれらを列挙しているが，このことは，古典論では情報源アルファベットは countably infinite であることと矛盾はしないのか．このままだと，「古典論」は「量子論の一部分」（あるいは，その特別の場合）だと言う (unifying framework) の主張に齟齬が出てしまうのではないか．これらの問題は，可分Hilbert 空間とか有界な自己共役作用素とかを考えてスペクトル分解定理などを使えば万事うまく行くのであろうか．この場合でも，作用素に半順序とトレースが定義出来るのであれば，任意の作用素列に対して常に確率的上下極限が定義できるので，これを基にすれば何とかなるのであろうか．この辺が量子系固有の難しさなのであろう．とても悩ましい．ご教示を願う次第である．

以上を要するに，1990年代前半に生まれた「情報スペクトル理論」は，2000年代に入って，量子という新天地で確実に芽を吹き着実に花を咲かせていると言えよう．情報スペク

ル理論の基本的枠組みを引き継ぎながら，その重要な基幹部分，すなわち，一般情報源符号化問題，一般通信路符号化定理，一般仮説検定定理はすでに量子情報理論の世界にしっかり「移植」され堅固な足場を固めており，そこで得られた新しい斬新な論法・発想は逆に古典論にも影響を与えている．情報スペクトル理論の量子化の問題としては，この他にも，一般乱数生成問題，一般レート・歪問題，一般Slepian-Wolf 問題，一般多重アクセス通信路問題，一般同定符号問題，一般 resolvability 問題，一般放送通信路問題，など，多くの重要問題が手付かずで残っていることを考慮すれば．このトレンドは今後もますます強まって行くものと思われる．かくして，「quantum information spectrum theory」という新分野の今後の成長が楽しみである．

最後に一言．今まで「情報スペクトル理論」の一般情報源や一般通信路について述べてきたが，それらの特別な場合，例えば，量子 _i.i.d. システム _などの性能を具体的に計算できるようにすることも大切である．このような場合には，古典論で確率収束や概収束を評価するための各種不等式に対応する量子版が必要になる．この点では，Ahlswede と Winter の論文 “Strong converse for identification via quantum channel”(2002)で述べられている「量子 Markov 不等式」，「量子 Chebyshev 不等式」．「量子Chernoff 不等式」などの量子版が新鮮で面白い．他に目を通した論文の中では，Ogawa や Nagaoka らが行った一連の仕事（定常無記憶システムに対する各種の誤り確率指数決定問題）にも感銘を受けた． これらは，古典論での対応する問題にも新しい示唆を与えている．