量子情報理論

佐々木　雅英 < 独立行政法人 通信総合研究所 184-8795 小金井市貫井北町 4-2-1 e-mail:psasaki@crl.go.jp>
番　雅司 < 日立製作所 基礎研究所 350-0395 埼玉県比企郡鳩山町赤沼 2520 番地 e-mail: m-ban@harl.hitachi.co.jp>

2001 年 8 月 13 日

現在の情報理論は古典物理学の法則に従う媒体に載せられた情報の流れを数理モデルとして抽象化することで成り立っている。しかし、この抽象化は完全ではなく、情報理論はより基本的な法則である量子力学の下で再構築されなければならない。このいわゆる量子情報理論は、60 年代にすでに研究が始まり 90 年代に入って急速に進展し始めた。これは従来の情報理論を自然な形で包含し、さらに量子力学的効果を使う新しい情報操作とその性能限界、最適なシステム設計の方法を与えるための理論である。本稿では、その概要について、従来の通信理論の量子力学的一般化、量子状態そのものが伝送対象となる場合の通信性能の定式化、そして非局所的量子相関を新たな通信資源とする情報操作の定式化という 3 つの視点から解説する。

1　はじめに

現在の情報技術は、0 と 1 という 2 つの数字による抽象化の上に成り立っている。情報は 0 と 1 からなる系列によって表現され、系列間の遷移によって情報の伝送や処理が行われる。この操作を乱す雑音は、0-1 間の確率的遷移としてモデル化される。情報理論は、確率事象に伴う曖昧さとして情報量を定義することによって、外乱の下での最適な情報伝送と信号処理を設計する強力な手段を与えてきた。

しかし、情報技術は今や原子一個、電子一個、あるいは光子一個といった量子力学的対象を直接操作する領域に入りつつある。また、量子光学の進歩は、原子スケールに特徴的だった量子相関を数 10km にわたって展開することを可能にし、さらには、それが従来に類似のない転送技術や暗号技術、信号処理技術へ応用できることを明らかにしつつある [7]。こうした中で、従来の情報理論における情報操作のモデル化や情報量の定義は、実はほんの一つの可能性にしか過ぎず、もっと広い情報の定義、新しい伝送・処理の方式が可能であることがわかってきた。これまでの情報技術の指導原理であった情報理論は、量子力学と合流し量子情報理論として統一される時を迎えている。

あらゆる情報技術は $\{0,1\}$ の識別性の上に成り立っている。$\{0,1\}$ を担うのは多くの電子、あるいは光子の集合体であり、その物理的状態は雑音が小さい極限では完全に識別できるという仮定がなされる。また、そのような状態は複製や増幅も可能である。（このような仮定のもとで扱われる従来の情報記号のことを「古典情報」と呼ぶことにする。）しかし、$\{0,1\}$ を担う媒体の量子力学的性質が顕在化する領域では、状態を変えることなく複製や増幅を行うことは不可能であり [14,15]、状態間の完全な識別も（直交状態でない限り）一般に不可能となる [2,12]。このことは、情報技術に新たな原理的な性能限界を課す一方で、量子暗号という頑健な情報セキュリティーの原理を提供することにもなる。また $\{0,1\}$ の系列間の遷移によって行われる情報の伝送や処理には、必然的に確率振幅レベルでの量子力学的干渉効果が内在し、それを最適に制御することで、従来理論から外挿される限界を凌駕する性能が予言されてくる。情報理論はこのような極限まで含めて、量子力学の言葉で抽象化されなければならない。

また、量子計算のように古典的対応を持たない情報機能に対しては、その効率や限界の定式化のための新しい概念や測度が必要となる。量子計算では 2 準位系の直交状態 $\{|0\rangle, |1\rangle\}$ を導入して $\{0,1\}$ に対応させ、N ビットのテンソル積 $\{|0\rangle, |1\rangle\}^{\otimes n}$ の張る空間での unitary 変換を演算と考える。その過程で現れる N ビットの重ね合わせ状態、一般には各ビットの量子状態の積に因数分解できない形の “量子もつれ状態 (entangled state)”が従来にはない機能を提供する。量子コンピュータのメモリには、計算過程で現れる種々の量子もつれ状態が保存される。それは最終的解に至るまでのいろいろな可能性の重ね合わせであり、一般に我々には未知の状態である。量子コンピュータを結ぶインターネットが実現すれば、このような未知の量子状態自身を新たに伝送の対象としなければならない。また、CPU からメモリへの格納と読み出しも広い意味での量子状態の伝送である。伝送の対象となるのは古典的情報記号ではなく、重ね合わせ、あるいは量子もつれの「様相」である。

送りたい量子状態の素性が分かれば、それを古典情報に

符号化して送れるが、未知の量子状態を有限個のサンプルから正確に知ることは量子力学の原理として不可能であり、また複製を作ることも禁止されているためこの方法は使えない [14, 15]。しかし、量子力学は未知の量子状態の転送手段を用意している。量子テレポーテーションである [16–21] 。これは、量子もつれ状態にある光子対あるいは光ビーム対の片方ずつを遠く離れた 2 者間で共有し、送信者側で送りたい量子状態と対の片方を一括して測定し、その結果を伝えてもらった受信者が対のもう片方に適切な unitary 変換を施せば、未知の量子状態が未知のまま受信者に再生されるというものである。量子もつれ状態はこれまで原子スケールに特有の現象であったが、この量子相関効果を数 10km 以上離れた通信スケールまで展開する訳である。古典的対応を持たない通信資源がここで新たに加わることになる。

量子情報理論は、こう言った量子力学的媒体による情報通信や信号処理の効率と限界を明らかにし、実現化への指針を与えるための理論体系である。と同時に、従来の量子力学における諸概念を情報通信や信号処理といった機能的視点から眺め、量子力学に新しい解釈を与え、さらに深い構造を明らかにして行くと言う意味も持っている。

量子計算や量子暗号については、すでに本誌でも何度か解説記事が書かれているので [8]、本稿では、量子情報理論の中でもテーマを絞って、情報通信に関わる基礎理論を取り上げる。それを

・古典情報の伝送

・量子状態そのものの伝送

・通信スケールにおける量子もつれの制御

という 3 つの主題をに分けて解説する。まず、従来の情報理論が「情報」と言うものをどう定量化して捕らえるのか、その要点から説明する必要がある。

2 情報理論の基礎

2.1 情報とは

今、ある一冊の本の内容を伝送したいとしよう。本はアルファベット $\{a, b, ..., z\}$ で書かれている。本に現れるそれぞれのアルファベットの出現頻度から、生起確率 $\{P(a), P(b), ..., P(z)\}$ を定義できる。この確率事象系を情報源 $A = \{a_1, ..., a_M; P(a_1), ..., P(a_M)\}$ と呼ぶ。実際にアルファベットを運ぶのは電気や光のパルスである。パルスの種類が N 個あるとして、これらを文字記号 $\{x_1, x_2, ..., x_N\}$ で名前付けする。$\{0, 1\}$ が最も簡単な例である。アルファベットは文字 $\{x_i\}$ の系列で表現され、電気や光のパルス列となって通信路を伝わる。このような情報伝送の流れは情報源符号化と通信路符号化を二つの基本要素として図 1 の様に図式化される。情報源符号器はアルファベットを文字 $\{x_i\}$ の系列、符号語に変換する。伝送速度を向上させるためには符号語はできるだけ短いことが望ましい。次に、情報源符号器の出力は、通信路符号器によって通信路の物理的特性に適合した媒体に再度符号化される。通信路は、光ファイバや電話線であったりコンピュータ内部の半導体メモリであったりするわけだが、こう言った媒体には常に雑音が存在し情報に歪みや誤りを生じさせる。こういった雑音の効果を予想して、そこで起こりうる誤りを後で訂正できるよう符号語にさらに冗長な $\{x_i\}$ の文字系列を付加するわけである。そして、最終的に電気パルスや光パルスに変換してから通信路へ送りだす。通信路からの出力系列は、通信路復号器によって誤り訂正を行った後で情報源符号語に対応させられる。その後、情報源復号器で情報源符号器の逆変換を行ってアルファベットが復元される。

こう言った一連の操作の効率と限界を定量化し、情報理論の基本的骨格を作り上げたのが C. E. Shannon である [9]。この論文の中で Shannon は情報源 A の確率分布に対して定義される量

$$H(A) = -\sum_{i=1}^{M} P(a_i) \log P(a_i) \tag{1}$$

を情報源 A のエントロピーと呼び、A に関する情報量として定義した。対数の底を 2 にとった時の $H(A)$ の単位がビット（binary digit）である。

2.2 情報源符号化

Shannon によって最初に示された情報源符号化定理では、情報源からの出力を十分長い系列毎に観測した時に現れる確率統計的性質を証明の基礎としている。この考え方は、情報量に対する解釈や量子版への拡張という点で深い洞察を与えてくれる。

簡単な例として、統計的に独立な 2 元アルファベットの情報源 $A = \{a, b; p, 1-p\}$ を考える。この情報源から発生するアルファベット系列を観測した時、系列長 n を十分大きくとると、その中には a がほぼ np 個、b がほぼ $n(1-p)$ 個含まれていると予想される。もちろん、極端な場合には n 個全てが a となることもあり得るが、これは極めて稀な事象である。このような傾向は生起確率に片寄りがある場合にいっそう顕著である。例えば、$p = 0.1$ の場合、$abbbbbbbbb$ という系列が観測される確率は 0.039 であるが、$aaaaaaaaaa$ という系列が観測される確率は 10^{-10} とほとんど無視でき

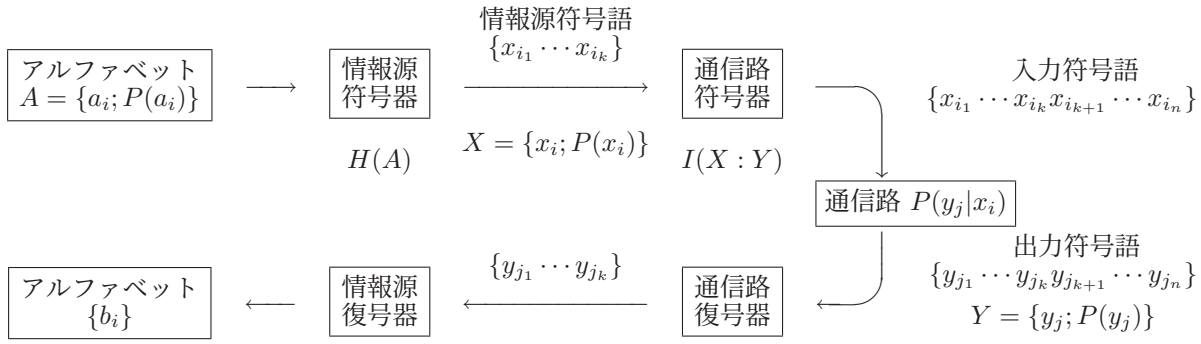

図 1: 情報伝送の基本模型。

る程度になる。このように、高い頻度で生起するアルファベット系列は、生起確率で決まるごく限られたパターンに集中していると予想できるわけである。こういった実際に我々が目にする頻度の高い系列のことを典型的系列と呼ぶ。一般に、情報源 $A = \{a_1, ..., a_M; P(a_1), ..., P(a_M)\}$ から生ずる長さ n の十分長い系列では、a_i はほぼ $nP(a_i)$ 個含まれていると予想してよい。このような系列の総数は、「場合の数」

$$\frac{n!}{[nP(a_1)]! \cdots [nP(a_M)]!} \sim 2^{nH(A)} \tag{2}$$

だけ存在し、ここに Shannon エントロピー $H(A)$ が出てくる。また、各典型的系列はどれも $2^{-nH(A)}$ という等確率で生起する。したがって、高々長さ $nH(A)$ の符号を用意して、それぞれの典型的系列に割り当てることにすれば、全ての典型的系列を符号化することができ、しかも非典型的系列の出現確率は n を大きく取ることでいくらでも小さくできるため、長さ $nH(A)$ のブロック符号で情報源を十分正確に符号化できるわけである。2 元情報源 $A = \{0, 1; p, 1-p\}$ の $p = 0.1$ という例では、$H(A) = 0.469$ であり、$n = 100$ の場合 2^{100} 個の系列を 2^{47} 個の系列という指数関数的に小さな数まで圧縮できるわけである。もちろん、非典型的系列の出現確率も完全にはゼロではないので、情報を圧縮して表現した際にはどうしても何らかの誤りを伴う。しかし、十分長い系列をブロック系列ごとに符号化すれば、符号長 n を増やすことでいくらでもその誤りを小さくできるわけである。このように式 (1) の Shannon エントロピーは漸近的極限における情報源符号化の限界という明確に機能的な意味を持つ。実際、情報量を多く含む情報源ほど、その表現に用する符号長は長くなるはずで式 (1) はそのような直観と一致している。より精密な定式化については、文献 [10,11] を参照されたい。

2.3 通信路符号化

情報源符号化器からの出力は $\{x_i\}$ からなる文字系列（情報源符号語）である。その中での各文字の生起確率を $P(x_i)$ とし、もう一つの情報源 $X = \{x_1, \ldots, x_M; P(x_1), \ldots, , P(x_M)\}$ を定義する（以後 M は文字総数)。通信路の特性は、通信路から出現しうる出力文字 $\{y_1, \ldots, y_N\}$ と、x_i が入力された時に y_j が出力される条件付き確率 $P(y_j|x_i)$ によって表現され、情報の操作はこれらの量のみを用いて抽象的に扱われる。出力文字の生起確率は $P(y_j) \equiv \sum_{x_i} P(y_j|x_i)P(x_i)$ から計算され、出力情報源 $Y = \{y_1, \ldots, y_N; P(y_1), \ldots, P(y_N)\}$ が定義される。

わかりやすく、X も Y も 2 元の文字 $\{0, 1\}$ からなるとし、$p = 10^{-4}$ の確率で 0 が 1 に、1 が 0 に誤るような通信路を考えよう (図 2)。今、復号誤り確率が 10^{-7} を切った

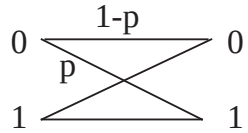

図 2: 2 元対称通信路。

らエラーフリーといってよいものとする。そのまま $\{0, 1\}$ を送ったらだめである。そこで、0 を 000、1 を 111 と 3 回くり返す通信路符号化を考える。出力側では計 8 つのパターンが出現しうるが、多数決で 0 か 1 かを判断することにすれば、復号誤り確率は 3.0×10^{-8} まで減少し、伝送の信頼性を高めることができる（図 3)。しかし、それは伝送速度を 1/3 まで劣化させると言うコストを費やしての話である。0 を $00\cdots0$、1 を $11\cdots1$ と繰り返す回数をどんどん増せば、復号誤り確率は当然ゼロに近付いて行くが、一方で伝送速度もゼロに近付いて行き、伝送に無限の時間を費やすはめとなって、伝送自体が意味をなさなくなってしまう。

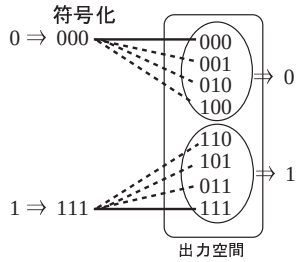

図 3: 3 ビット符号化による通信路。

これに対して、Shannon は符号語の長さを十分大きくとり、うまく符号語を選んで情報源符号語を再度符号化してやれば、伝送速度を有限に保ったまま復号誤り確率をいくらでもゼロに近付けることができるということを示した。長さ n の $\{0,1\}$ の文字系列からなる符号語を使って、$k\ (<n)$ ビット分のメッセージを伝送する場合、伝送速度は $R=k/n$ で定義される。符号語に含まれる冗長性は $n-k$ ビットである。できるだけ少ない冗長性でもって、できるだけ信頼性の高い伝送を行いたいわけである。Shannon の通信路符号化定理は、伝送速度 R をある値以下に保てば、符号長を十分大きく取ることによって、メッセージの復号誤り確率をいくらでも小さくできる符号化法が存在することを保証している。この伝送速度の上限値のことを通信路容量 C と呼ぶ。

通信路容量 C の定式化の概要を説明しよう。入力、出力情報源の文字は $x,\ y$ で区別する。長さ n の十分長い入力系列では、0 が $nP(x_0)$ 個程度、1 が $nP(x_1)$ 個程度含まれていると予想してよい。こういった入力系列のうちの一つを通信路に送り込むと、$nP(x_0)$ 個の 0 のうちおよそ $nP(x_0)P(y_1|x_0)$ 個が 1 へ、$nP(x_1)$ 個の 1 のうちおよそ $nP(x_1)P(y_0|x_1)$ 個が 0 へ、変化してしまうと予想される。したがって、ある一つの入力系列から生じ得る出力系列の総数は

$$\begin{aligned} N_{Y|X} &= \frac{[nP(x_0)]!}{[nP(x_0)P(y_1|x_0)]![nP(x_0)P(y_0|x_0)]!} \\ &\times \frac{[nP(x_1)]!}{[nP(x_1)P(y_0|x_1)]![nP(x_1)P(y_1|x_1)]!} \\ &\sim 2^{nH(Y|X)} \end{aligned} \tag{3}$$

程度存在する。ここで

$$H(Y|X) = -\sum_x P(x)\sum_y P(y|x)\log P(y|x) \tag{4}$$

は条件付きエントロピーである。つまり、情報源 X の各典型的系列からは、出力側で $2^{nH(Y|X)}$ 個程度の系列の “勢力圏”が形成される。各系列の勢力圏が重ならないようにすれば、出力系列から一意に誤りなく入力系列を復号できるはずである。一方、出力側で生じ得る典型的系列の総数は $N_Y \sim 2^{nH(Y)}$ 程度と見積もられ、これを各勢力圏の系列数で割った $N_Y/N_{Y|X} \sim 2^{n[H(Y)-H(Y|X)]}$ が、勢力圏が重ならないようにしながら取り得る入力系列の総数となる。さて、図 4 で見るように、もともと $2^{nH(Y)}$ 個程度ある出力系列は、送った入力系列が指定されると $2^{nH(Y|X)}$ 程度の可能性に絞られる。つまり、送った入力系列を知ることによって Y の曖昧さは $H(Y)$ から $H(Y|X)$ まで減少する。その差

$$I(X:Y) = H(Y) - H(Y|X) \tag{5}$$

は X を知ることによってもたらされた Y に関する情報量と解釈される。Shannon はこれを X と Y の間の相互情報量と定義し、これを用いて通信路符号化を定式化した。式 (5) は入力の生起確率と通信路行列を使って

$$I(X:Y) = \sum_x P(x)\sum_y P(y|x)\log\frac{P(y|x)}{\sum_{x'}P(x')P(y|x')} \tag{6}$$

と書かれる。よって $2^{nI(X:Y)}$ 個程度の符号語のみを選んで送ることにすれば、どうにか出力側での勢力圏が重ならないようにできそうである (図 4)。ではいったいどのよう

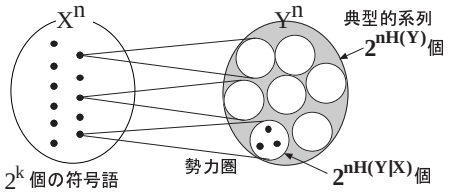

図 4: 典型的入力系列の勢力圏とその充填。

にして送信すべき符号語を選べば良いのであろうか。実はこれは簡単な問題ではない。Shannon はいっそのこと、$2^k\ (=2^{nR})$ 個の系列を全くランダムに選んで、出てきた情報源符号語にこれまたランダムに割り得て通信路に送り込むという符号化を考えた。そして、そのような全ての可能な符号化に対して平均をとった時の復号誤り確率が

$$\langle P_{\rm e}\rangle < 2^{n[R-I(X:Y)]} \tag{7}$$

と書かれることを示した。したがって、$R<I(X:Y)$ と取ればどこまでも誤りを小さくして行けることがわかる。全ての可能な符号化の平均としてこのような性質があれば、必ずそのような符号は存在するはずである。このようにして、雑音のある通信路でも原理的に誤りゼロの伝送を実現でき、伝送速度は $I(X:Y)$ まで上げられることが示され

るのである。さて、$I(X:Y)$ は通信路行列 $P(y|x)$ の他に x の生起確率 $P(x)$ を含むが、これは入力側で制御可能な変数である。したがって、与えられた通信路行列 $P(y|x)$ に対して $I(X:Y)$ ができるだけ大きくなるように $P(x)$ を選ぶのがよい。式 (7) は、どのように選んだ $P(x)$ に対しても成り立つのであるから、結局、伝送速度は

$$R < C \equiv \max_{p(x)} I(X:Y) \tag{8}$$

まで上げることができるのである。この C が通信路容量である。厳密な証明は文献 [10,11] 等を参照されたい。

3 古典情報の伝送

このように Shannon に始まる情報理論は、$\{0,1\}$ のような情報記号の生起確率と遷移確率のみから情報操作の効率と限界を導く。そこで扱われる情報記号は複製や増幅が可能であり、雑音が小さい極限では完全に識別できる。しかし、今や情報記号の背後にあるのは量子力学的媒体であり、これまでの仮定は一般には成り立たなくなる。量子力学の法則のもとで理論を再構築しなければならない。情報の流れは図 5 のようにモデル化される。I の過程は情報記号を量子状態へ載せる変調過程である。この過程では、まず情報源符号化を行い、圧縮した後の情報記号を量子状態へ載せる。圧縮を可能にしている原理は、情報記号の出現確率の偏りであった。この他に「0 が出た後は、しばらく 0 が続く確率が高い」というような記憶効果があってもそこには冗長度が潜み、情報の圧縮が可能である。実はもう一つ、古典的対応を持たない冗長性が存在する。量子状態間の非直交性（一般には非可換性）である。例えば、もし $\{\hat{\rho}_i^{\rm in}\}$ が、ある中継点で受け取る量子状態で非直交状態で受け取るしかないとしよう。そのような場合、次段の通信路へ入力する前の II の過程でさらに圧縮が可能となる。これを含めた一般化が 3.1 節で述べる量子情報源符号化である。

この段階では、良質の状態を作る努力がなされるから、構成要素としては直交状態に近い純粋状態が想定される。しかし、量子通信路を通った後の出力量子状態 $\{\hat{\mathcal{L}}(\hat{\rho}_i^{\rm in})\}$ は一般に非可換性な混合状態となり識別性が劣化しているのが普通である。そこから適切な測定を行って情報記号を取り出さなければならない。できるだけ正確に復元できる様、量子通信路についての先験的知識（それは量子状態から量子状態への完全正写像 $\hat{\mathcal{L}}$ として表される。4.1 節で詳述する。）をもとに II の過程で量子通信路符号化を行う。III の過程には復号のための演算と情報を取り出す量子信号検出過程が入る。3.2 節では、量子信号検出の問題を概説し、その基礎の上に立って 3.3 節で量子通信路符号化を説明する。

3.1 量子情報源符号化定理

2 元の量子情報源 $X = \{|\psi_0\rangle, |\psi_1\rangle; p_0 = p_1 = \frac{1}{2}\}$ を例にとる。$\langle\psi_0|\psi_1\rangle = \kappa \neq 0$ である。この量子状態を単に $\{0,1\}$ の記号として扱ってしまえば、$p_0 = p_1 = \frac{1}{2}$ であるため、Shannon エントロピーは $H(X) = 1$ となり情報源の圧縮は不可能である。

一方、このような量子系の統計的性質は、密度行列 $\hat{\rho} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ によって記述される。この密度行列は

$$\hat{\rho} = \frac{1+\kappa}{2}|0\rangle\langle 0| + \frac{1-\kappa}{2}|1\rangle\langle 1| \tag{9}$$

とも表すことができる。ここで $\{|0\rangle, |1\rangle\}$ は、$\hat{\rho}$ の固有状態である。$\{|0\rangle, |1\rangle\}$ は直交状態であるため、従来の $\{0,1\}$ の記号として扱って良い。つまり、量子情報源 X は、直交基底 $\{|0\rangle, |1\rangle\}$ を確率 $\{\frac{1+\kappa}{2}, \frac{1-\kappa}{2}\}$ で生起させる古典情報源と見なせる。したがって、$p = \frac{1+\kappa}{2}$ と置いて 2.2 節の情報源符号化定理の議論を適用すると

$$H(X) = -\frac{1+\kappa}{2}\log\frac{1+\kappa}{2} - \frac{1-\kappa}{2}\log\frac{1-\kappa}{2} \tag{10}$$

という量を用いて、量子情報源 X を長さ $nH(X)$ のブロック符号で十分正確に符号化できそうである。式 (10) は $\hat{\rho}$ の von Neumann エントロピーで通常 $S(\hat{\rho})$ と記す。Schmacher と Jozsa は、直交基底 $\{|0\rangle, |1\rangle\}$ の生起確率の偏りから決まる典型的基底系列が張る「典型的部分空間」という概念を導入し、これを厳密に証明した [22,23]。量子情報源符号化定理である。符号化はまず、長さ n の系列に、典型的成分と非典型的成分を分ける unitary 変換を施し、非典型的成分は捨てて典型的成分のみを残すことで圧縮が完了する。復元は、適当な状態（何でも良い）を加え、もともとの空間上で unitary 変換を行い完了する。この時、十分長い符号長のブロックで符号化すれば、復元後の状態を入力系列の状態にいくらでも近くなるよう圧縮できるのである。

以上は最も簡単な場合であるが、他の幾つかのシナリオへの拡張がなされている。例えば、圧縮対象の信号状態の素性が未知で von Neumann エントロピーだけが知られている場合でも同様の情報源符号化が可能である [24]。また、圧縮対象が一般の混合状態の場合では、幾つかの圧縮シナリオでの圧縮限界の不等式評価 [25] や信号状態間の非可換性を決めている最小の成分を引き出し、その表現を使って圧縮限界を記述する方法の提案 [26] などがなされている。また、実際の量子情報処理へ適用して行く上で、構成的符号化法の研究は極めて重要であり、この方向への研究では [27] が興味深い。

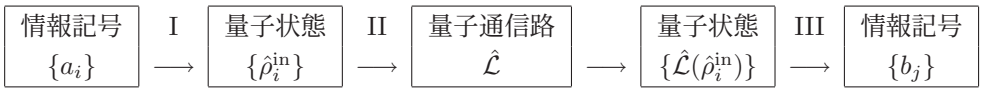

図 5: 量子効果まで含めた情報の流れのモデル。

3.2 量子信号検出

量子力学的媒体の識別とその限界はどうなるのか、この問題の研究は、レーザーの発明によって光通信の可能性が検討され始めた 1960 年代初頭まで遡り、1967 年に C. W. Helstrom によって量子信号検出の問題として定式化された [1]。これがその後の量子通信理論の方向を決定付けるものとなった。量子情報科学の源流である。(文献 [2] を参照。今では入手しにくい量子通信理論の先駆的論文の内容も詳しく紹介されている。)

ここでは Helstrom が最初に取り上げた 2 つの量子状態の識別について考える。例えば、現在の光通信で使われるオン-オフ強度変調方式では、単一モードのレーザ光をあるビット区間 T 秒毎にオン-オフさせ “1” と “0” の信号を生成するが、これに対応する量子状態はそれぞれコヒーレント状態 $|\alpha\rangle$ と真空状態 $|0\rangle$ である。このようなオン-オフ信号は、通常、光子計数を行って識別するが、実は、もっと優れた検出方法が数学的には存在する。信号検出過程は、現在では、確率作用素測度 (Probability Operator Measure, POM) と言う概念を用いて記述するのが一般的である [2,12]。これは、次の条件を満たす Hermite 作用素のセットである。

$$\hat{\Pi}_j = \hat{\Pi}_j^\dagger \geq 0, \qquad \sum_j \hat{\Pi}_j = \hat{I}. \tag{11}$$

はじめの条件は、確率の非負性を保証し、次の条件は検出過程における確率の保存則に対応する。光子計数器の例では、$\hat{\Pi}_{\rm on} = \sum_{n=1}^{\infty} |n\rangle\langle n|$、$\hat{\Pi}_{\rm off} = |0\rangle\langle 0|$ となり、識別の誤り確率（ビットエラーレート）は $P_e = \frac{1}{2}{\rm e}^{-|\alpha|^2}$ になる ($\{|0\rangle, |\alpha\rangle\}$ は等確率で生起するとする)。一方、最適検出器は誤り確率

$$P_e = \frac{1}{2}\langle\alpha|\hat{\Pi}_{\rm off}^{\rm min}|\alpha\rangle + \frac{1}{2}\langle 0|\hat{\Pi}_{\rm on}^{\rm min}|0\rangle, \tag{12}$$

を最小化する解 $\{\hat{\Pi}_{\rm off}^{\rm min}, \hat{\Pi}_{\rm on}^{\rm min}\}$ として求められ

$$|\omega_0\rangle = \sqrt{\frac{1-P_e^{\rm min}}{(1-\kappa^2)}}\,|0\rangle - \sqrt{\frac{P_e^{\rm min}}{(1-\kappa^2)}}\,|\alpha\rangle\,, \tag{13}$$

$$|\omega_1\rangle = \sqrt{\frac{P_e^{\rm min}}{(1-\kappa^2)}}\,|0\rangle + \sqrt{\frac{1-P_e^{\rm min}}{(1-\kappa^2)}}\,|\alpha\rangle\,, \tag{14}$$

なる正規直交基底 $\{|\omega_0\rangle, |\omega_1\rangle\}$ から

$$\hat{\Pi}_{\rm off}^{\rm min} = |\omega_0\rangle\langle\omega_0|, \quad \hat{\Pi}_{\rm on}^{\rm min} = |\omega_1\rangle\langle\omega_1|, \tag{15}$$

のように構成される [13]。ここで $P_e^{\rm min}$ が最小誤り確率で

$$P_e^{\rm min} = \frac{1}{2}\left(1 - \sqrt{1 - |\langle 0|\alpha\rangle|^2}\right), \tag{16}$$

で与えられる。

光のパワー（ビット当たりの平均光子数 $|\alpha|^2$）が十分大きければ信号間の内積 $\langle 0|\alpha\rangle = {\rm e}^{-|\alpha|^2/2}$ は極めて小さく直交状態と見なしてよい。このような状態は、従来の $\{0,1\}$ と全く等価である。しかし、信号パワーが小さくなるにつれ、どんな理想的なシステムでも必ず式 (16) に従って識別誤り確率が増加して行くわけである。

実際、衛星間や惑星間を光でリンクする深宇宙での光通信や膨大なユーザ間で信号を分配する次世代光ネットワークでは、受信端に最終的に届く光信号は非常に微弱で信号の識別性が著しく劣化しているのが普通であり、上述の識別限界に直面することになる。このような次世代光通信では、現在のオンオフ変調に替わり、光波の位相まで変調する方式が検討されている。波本来の性質を積極的に使うことで受信感度を飛躍的に改善できるからである。最も簡単なモデルは、2 値位相変調信号 $\{|\alpha\rangle, |-\alpha\rangle\}$ （マイナス符号は位相が π ずれていることを示す）である。$|\alpha|^2 < 10$ 程度になってしまうと、量子最適受信器でもビットエラー率 10^{-9} を切れなくなり高性能の符号化が必要となる。これを図式化した図 6 が、最も簡単な量子通信路のモデルとなる。この測定に基づく通信路のことを特に「量子-古典通信路」と呼ぶことにする。

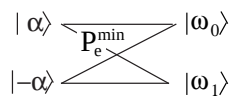

図 6: 2 元対称量子通信路。

3.3 量子-古典通信路符号化定理

このモデルを例として、情報伝送の究極の性能限界を決める通信路符号化の話に移ろう。4.5 節の量子状態そのものの伝送に関わる量子通信路符号化と区別して、これを「量子-古典通信路符号化」と呼ぶことにする。

2.3 節の冒頭で、信号を 3 回繰り返して送ることで誤り確率を減らすという例に触れたが、同じ考え方を量子通信

路に当てはめてみよう。0, 1 という記号をそれぞれ 3 つのパルス系列

$$|\Psi_0\rangle \equiv |\alpha\rangle \otimes |\alpha\rangle \otimes |\alpha\rangle\,, \tag{17}$$

$$|\Psi_1\rangle \equiv |-\alpha\rangle \otimes |-\alpha\rangle \otimes |-\alpha\rangle\,, \tag{18}$$

で符号化する。$\{|\alpha\rangle, |-\alpha\rangle\}$ を文字状態、$\{|\Psi_0\rangle, |\Psi_1\rangle\}$ を符号語状態と呼ぶ。2.3 節の冒頭の例に従えば、個々のパルスを $\{|\omega_0\rangle, |\omega_1\rangle\}$ で表される量子測定によって個別に測定し、その結果生じる合計 8 通りの出力パターンを 2 つのグループに分割して $\{|\Psi_0\rangle, |\Psi_1\rangle\}$ の識別を行うことになる。しかし、一方で $\{|\Psi_0\rangle, |\Psi_1\rangle\}$ という符号語状態を**??**章で述べた 2 元信号 $\{|0\rangle, |\alpha\rangle\}$ と同様に見なし、式 (13) 及び (14) に相当する 2 出力の量子測定

$$|\Omega_0\rangle = \sqrt{\frac{1-P_e^{(3)}}{(1-\kappa^6)}}\,|\Psi_0\rangle - \sqrt{\frac{P_e^{(3)}}{(1-\kappa^6)}}\,|\Psi_1\rangle\,, \tag{19}$$

$$|\Omega_1\rangle = \sqrt{\frac{P_e^{(3)}}{(1-\kappa^6)}}\,|\Psi_0\rangle + \sqrt{\frac{1-P_e^{(3)}}{(1-\kappa^6)}}\,|\Psi_1\rangle\,, \tag{20}$$

と言うものを考えることができる。ここで、$\kappa = \langle\alpha|-\alpha\rangle = \mathrm{e}^{-2|\alpha|^2}$、

$$P_e^{(3)} = \frac{1}{2}(1-\sqrt{1-\kappa^6}), \tag{21}$$

は最小誤り確率、また 2 つの符号語は等確率で生起するとした。式 (19)、(20) は、テンソル積にある符号語状態をひとまとめの量子状態と見なして、それらの重ね合わせ状態へ射影するという測定過程に対応し、量子一括測定と呼ばれる。例えば、もし文字状態の識別限界が

$$P_e^{(1)} = \frac{1}{2}(1-\sqrt{1-\kappa^2}) = 10^{-4}, \tag{22}$$

だったとしよう。個別測定に基づく復号では、個々の測定は独立事象であり、例えば、符号語 000 が入力され 111 と検出される確率は、$P(111|000) = P(1|0)^3$（但し $P(1|0) = |\langle\omega_1|\alpha\rangle|^2$）のように与えられ、結局、誤り率は 3×10^{-8} となる。一方、量子一括測定では式 (21) から計算されるように誤り率は一気に 1.6×10^{-11} まで減少する。その際の出力確率は、$|\langle\Omega_j|\Psi_i\rangle|^2$ で与えられるため、$\langle\Omega_j|\Psi_i\rangle$ という確率振幅の干渉をうまく使って $P(111|000)$ を $P(1|0)^3$ より小さくできるのである。これは符号語状態間の干渉効果で自動的に誤り訂正を行っていることに相当し、従来の符号理論にはない新しい量子効果である。従来の符号化理論では、文字状態の検出特性を規定する通信路モデル（図 6）のみを使って復号戦略を組み立てていたが、量子通信路の符号化では、個々の文字状態の検出特性に縛られることなく、符号語状態に対して新たに量子力学が許す最適な復号戦略を探して行く。したがって、通信路容量は与えられた文字状態の集合のみに依存した量となる。

この例を n 次拡大通信路へ一般化する。即ち、M 個のアルファベット $\{A_1, A_2, ..., A_M\}$ を文字 $\{x_i = 0, 1\}$ を使って長さ n の符号語 $\{\mathbf{x}_i = x_{i_1}x_{i_2}\cdots x_{i_n} | i = 1, \ldots, M\}$ で表現し伝送する。各文字 x_i に対応する通信路出力は $|\psi_i\rangle$ $(= |\alpha\rangle, |-\alpha\rangle)$ である。符号語状態は n 個の文字状態からなるテンソル積状態であり、それらを $\{|\Psi_i\rangle = |\psi_{i_1}\rangle \otimes \cdots |\psi_{i_n}\rangle\,|i = 1, ..., M, \}$ とする。当然、$M < 2^n$ である。合計 2^n 個のブロック系列からうまい組み合わせの符号語を選んでアルファベットを符号化するが、$\{|\Psi_i\rangle\}$ はまだ一般に互いに非直交状態にあり、これがエラーの原因になる。$\{|\Psi_i\rangle\}$ を識別する最適復号過程は**??**章での議論を M 元信号へ一般化した理論で与えられ、n 次拡大空間上の適当な確率作用素測度 $\{\hat{\Pi}_1, \hat{\Pi}_2, \ldots, \hat{\Pi}_N\}$ で表現される。これらはそれぞれ出力記号 $\{\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N\}$ に対応している。出力数 N もこれ自身最適化すべき変数となる。n 次拡大通信路の通信路行列は $P(\mathbf{y}_j|\mathbf{x}_i) = \langle\Psi_i|\hat{\Pi}_j|\Psi_i\rangle$ で与えられ、これを使って n 次の相互情報量が

$$I(X^n : Y^n) = \sum_{\mathbf{x}_i} P(\mathbf{x}_i) \sum_{\mathbf{y}_j} P(\mathbf{y}_j|\mathbf{x}_i) \log \frac{P(\mathbf{y}_j|\mathbf{x}_i)}{\sum_{\mathbf{x}'_i} P(\mathbf{x}'_i)P(\mathbf{y}_j|\mathbf{x}'_i)} \tag{23}$$

と定義される。これを符号語の選択 $\mathcal{E} = \{\mathbf{x}_i; P(\mathbf{x}_i)\}$ と復号戦略 $\mathcal{D} = \{\hat{\Pi}_j\}$ に関して最大化したした量を

$$C_n = \max_{\mathcal{E},\mathcal{D}} I(X^n : Y^n), \tag{24}$$

と定義する。

さて、もし復号戦略 $\mathcal{D}$ として個別測定に基づく方法をとったとすると、符号間の入出力の遷移確率は

$$P(\mathbf{y}_j|\mathbf{x}_i) = P(y_{j_1}|x_{i_1})P(y_{j_2}|x_{i_2})\cdots P(y_{j_n}|x_{i_n}), \tag{25}$$

であり、その結果、$I(X^n : Y^n) = nI(X : Y)$ となる。このような通信路を記憶のない通信路と呼ぶ。よって $C_n = nC_1$ であり、通信路容量は $C = C_n/n = C_1$ で定義され、もともとの拡大前の通信路モデルの特性で一意に決まることになる。ところが、量子-古典通信路の n 次拡大では、量子一括測定における符号語状態間の干渉効果のため、一般に式 (25) の仮定は成り立たない。つまり、一種の記憶のある通信路になっており、一般には $C_n \geq nC_1$ となる。このような場合の最終的な通信路容量は $C \equiv \lim_{n\to\infty} C_n/n$ で定義される。

通信路容量 C を決めている最も基本的な要素は量子一括測定であるが、その解析的表現とそれに基づく C_n を求めるのは、一般に極めて難しい問題で、実際 2 元の純粋状態の C_1 しか求まっていない [28–30]。よって、この方向から極限値を求めるのは現実的でない。歴史的には、まず

C の定義のもとになる相互情報量 $I(X:Y)$ に対して

$$\max_{\mathcal{D}} I(X:Y) \leq S\left(\sum_i p_i\hat{\rho}_i\right) - \sum_i p_i S(\hat{\rho}_i), \qquad (26)$$

という上界が Holevo によって与えられた [31] 。ここで $\{\hat{\rho}_i\}$ $(=\{\hat{\mathcal{L}}(\hat{\rho}_i^{\rm in})\})$ は量子-古典通信路の入力で一般的な混合状態としている (図 5)。次に

$$\bar{C} \equiv \max_{\{p_i\}}\left(S\left(\sum_i p_i\hat{\rho}_i\right) - \sum_i p_i S(\hat{\rho}_i)\right), \qquad (27)$$

という量を定義するとこれが C に対する一つの上界となる。しかし、通信路容量 C そのものに迫るためには量子一括測定を真剣に考慮しなければならない。これを最初にあらわな形で考慮し Shannon のとった証明法に沿って符号化定理を考えたのは Stratonovich と Vantsyan である [32] 。彼等は量子一括測定として現在では「平方根測定」と呼ばれるようになった方法 [33,34] を使って、純粋状態の場合に符号語状態の復号誤り確率を評価した。符号語状態とその生起確率の集合 $\{|\Psi_i\rangle\,;P_i\}$ に対して、平方根測定 $\{\hat{\Pi}_i = |\mu_i\rangle\langle\mu_i|\}$ は以下のように定義される。

$$|\mu_i\rangle \equiv \hat{\Psi}^{-\frac{1}{2}}\sqrt{P_i}|\Psi_i\rangle, \quad \hat{\Psi} \equiv \sum_{i=1}^{M} P_i|\Psi_i\rangle\langle\Psi_i|. \qquad (28)$$

この方法では出力数は入力符号語の数と同じになる。Stratonovich らは、のちに量子カットオフレートと呼ばれることになる

$$R_{\rm C} = -\log_2 \min_{\{p_i\}}\left(\sum_{i,j=1}^{L} p_i|\langle\psi_i|\psi_i\rangle|^2 p_j\right) \qquad (29)$$

という量を導入して、Shannon がとったランダム符号化による平均操作のもと $P_{\rm e}$ の特性を評価したが、最終的には Holevo によって計算が整備され、$R_{\rm C}$ が通信路容量 C に対する下界となること、さらに、$\bar{C} \geq C \geq R_{\rm C} > C_1$ となる例が存在することが示された [35]。

Holevo は $\bar{C} = C$ という可能性を強く示唆しながらも、当時はまだ最終的な証明に至らなかった。これを最初に証明したのは Hausladen らである [36]。彼等は文字状態が純粋状態である場合に限定して、Stratonovich らや Holevo が使った平方根測定とランダム符号化による平均操作の他に、新たに典型的部分空間という概念を加えて、Holevo の上界、式 (27) が実際に達成可能な伝送速度であること、つまり

$$C = \bar{C} = \max_{\{p_i\}} S(\hat{\rho}), \qquad (30)$$

となることを証明した。

2 元量子情報源 $\{|\psi_0\rangle, |\psi_1\rangle\,; p_0, p_1\}$ の例では、式 (30) の最大化は $p_0 = p_1 = \frac{1}{2}$ で達成され [37]、通信路容量は $\hat{\rho} = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|$ の 2 つの固有値 $\{\frac{1+\kappa}{2}, \frac{1-\kappa}{2}\}$ $(\kappa = \langle\psi_0|\psi_1\rangle)$ を使って

$$C = -\frac{1+\kappa}{2}\log\frac{1+\kappa}{2} - \frac{1-\kappa}{2}\log\frac{1-\kappa}{2} \qquad (31)$$

と書かれる。生起確率が等しい場合、$\{|\psi_0\rangle, |\psi_1\rangle\}$ からなる十分長い系列にはどちらの文字状態も平均 $n/2$ 個含まれ、そのような系列の数は 2^n と同程度の個数存在し、結局、どの系列も同じくらい目にする確率がある。式 (30) は、こういった状況でも 2^{nC} 個までなら（量子情報源符号化で登場した典型的部分空間の次元である）、それらが互いに「ほとんど直交」するように「うまく」刈り込む方法が存在することを意味している。これは、生起確率を単に密度行列の固有値で置き換えることで得られた量子情報源符号化ほどは自明なことではないだろう。Hausladen らが証明に使った平方根測定では M 個の符号語 $\{|\Psi_i\rangle\}$ は M 個の正規直交基底 $\{|\mu_i\rangle\}$ への射影という形で復号されるが、その状況では一つの入力系列には一つの出力系列が対応している。一方、もし個別測定で復号してしまえば一つの入力系列からは $2^{nH(Y|X)}$ 個程度の出力系列が出現しうる。この場合、2^{nC_1} 個を超えない程度まで「うまく」刈り込まなければ勢力圏の重なりを消して行くことはできない。このように通信路容量が C_1 から $C = \max_{p_i} S(\hat{\rho})$ まで上がる原因は量子一括測定による完全に非古典的効果である。Hausladen らによる厳密な証明では、上述の「ほとんど直交」「うまく」等の表現を、十分長い符号長領域で現れる典型的部分空間の性質を用いて精密に表現し、ロシアの数学者らが平方根測定とランダム符号化を用いて後一歩まで迫っていた定理の証明を完成させたものであった。

これはその後すぐに混合状態の場合へ Holevo 及び Schumacher と Westmoreland によって拡張され、

$$C = \bar{C} = \max_{p_i}\left(S\left(\sum_i p_i\hat{\rho}_i\right) - \sum_i p_i S(\hat{\rho}_i)\right), \qquad (32)$$

となることが証明された [38,39] 。混合状態の場合、一つの入力系列から生ずる出力系列は古典雑音のため有限個となり、一つの入力系列に附随する勢力圏のパッキングの問題が再び現れる。これによる通信路容量の減少分が式 (32) の第 2 項に相当する。これによって、Shannon の通信路符号化定理を一つの極限として含む一般的な通信路符号化定理が確立されるに至ったわけである。

この定理は、十分長い符号長領域で現れる典型的部分空間の性質を証明の一つの基礎として符号系の存在のみを保証するもので、具体的符号構成についてはいっさい述べていない。また、実用的符号長領域における通信性能も

このままでは具体的に評価できない。従来の情報理論では、Shannon (1948) の最初の証明の後、Feinstein (1955)、Fano (1961)、Gallager (1965) らによって誤り率限界を $P_{\rm e} < \exp[-nE(R)]$ の形で定式化する信頼性関数の理論が完成され [10] （R は伝送速度で $E(R)$ が信頼性関数)、これによって通信路符号化定理は、より精密に定量化され実用に向かって大きく前進した。

量子論的拡張は純粋状態の場合に対して Burnashev と Holevo によってなされている [40] (混合状態の場合についての信頼性関数はまだ未解決のままである)。彼等は、典型的部分空間という概念は使わずに、平方根測定とランダム符号化による平均操作のみに基づいて、

$$E(R) = \max_{p_i} \max_{0\le s\le 1} \left[-\ln(\mathrm{Tr}\hat{\rho}^{1+s}) - sR\right], \qquad (33)$$

という表式を導いている。信頼性関数 $E(R)$ は、与えられた文字状態集合のみに依存した関数となる。これを具体的な形で求めることは実はかなり難しい問題である。これは、古典論でも同様であり、カットオフレートと呼ばれる、より計算のしやすい量で通信性能を評価することが行われる。それは式 (33) の右辺で $s = 1$ ととったときの第 1 項に相当する [41, 42]。純粋状態の場合は式 (29) となる。

このように通信路符号化による誤り率特性の評価理論ができつつあるが、これらは具体的符号構成を直接示唆するものではない。式 (32) の容量限界 (Holevo 限界) を実現するための構成的符号理論は、量子情報理論を通信システムへ具現化して行く上で極めて重要な課題である。現在のところ、平方根測定を用いた時に、どのような符号語を選択すれば、Shannon 理論にはない超加法的な通信路が効果的に構成できるかという研究に止まっている [43–45]。

ここで述べた通信路符号化定理は離散的文字集合に対するものであるが、これを連続無限個の文字集合へ一般化する問題についてはここで詳しく触れる余裕はない。歴史的経過も含め最近の成果に興味ある読者は文献 [46–48] を参照されたい。

4 量子状態の伝送：符号化定理に向けて

ここまでの話は従来の情報伝送が、量子効果が顕在化する極限においてどう扱われるかという話であった。ここからは量子状態そのもの、つまり重ね合わせや量子もつれの「様相」といった、いわば「量子情報」が伝送の対象となる。

4.1 量子通信路

与えられた量子通信路を通じて、一般には未知の量子状態 $\hat{\rho}_{\rm in}^{Q}$ をできるだけ正確に伝送あるいは記憶したい。量子通信路は一般的に図 7 のようにモデル化される。入力された量子状態 $\hat{\rho}_{\rm in}^{Q}$ は、自らの系 Q のダイナミクスや外部環境 E との様々な相互作用によって変化する。外部環境の影響を含めた系全体 QE の量子状態の変化は適当な unitary 作用素 $\hat{U}^{QE}$ によって記述することができる。我々の興味は

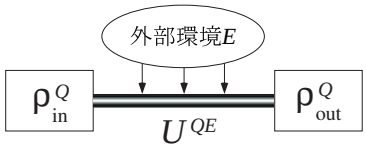

図 7: 量子通信路の一般的なモデル。

入力された量子状態 $\hat{\rho}_{\rm in}^{Q}$ が如何に変化したかである。量子通信路からの出力 $\hat{\rho}_{\rm out}^{Q}$ は外部環境の情報を消去することによって次のように表わすことができる [49, 50]。

$$\hat{\rho}_{\rm out}^{Q} = \mathrm{Tr}_E\left[\hat{U}^{QE}\left(\hat{\rho}_{\rm in}^{Q}\otimes\hat{\rho}_{\rm in}^{E}\right)\hat{U}^{QE\,\dagger}\right] \equiv \hat{\mathcal{L}}^{Q}\hat{\rho}_{\rm in}^{Q} \qquad (34)$$

ここで、$\hat{\rho}_{\rm in}^{E}$ は外部環境の初期状態であり、Tr_E は外部環境に関する部分トレースを表わす。この式で定義される写像 $\hat{\mathcal{L}}^{Q} : \hat{\rho}_{\rm in}^{Q} \to \hat{\rho}_{\rm out}^{Q}$ が量子通信路を表わす。

次に外部環境 E の初期状態 $\hat{\rho}_{\rm in}^{E}$ のスペクトル分解 $\hat{\rho}_{\rm in}^{E} = \sum_k p_k|\phi_k^E\rangle\langle\phi_k^E|$ $(p_k \ge 0, \sum_k p_k = 1)$ を考えれば、式 (34) はまた次のようにも表わすことができる [49, 50]。

$$\hat{\rho}_{\rm out}^{Q} = \hat{\mathcal{L}}^{Q}\hat{\rho}_{\rm in}^{Q} = \sum_{\mu}\hat{A}_{\mu}^{Q}\hat{\rho}_{\rm in}^{Q}\hat{A}_{\mu}^{Q\,\dagger}, \qquad (35)$$

ここで、$\hat{A}_{\mu}^{Q} = \sqrt{p_l}\langle\phi_k^E|\hat{U}^{QE}|\phi_l^E\rangle$、$\mu = (k,l)$ であり、$\hat{A}_{\mu}^{Q}$ は規格化条件 $\sum_{\mu}\hat{A}_{\mu}^{Q\,\dagger}\hat{A}_{\mu}^{Q} = \hat{1}^{Q}$ を満す。この規格化条件は量子通信路が $\hat{\rho}_{\rm in}^{Q}$ のトレースを保存することを保証する。量子通信路 $\hat{\mathcal{L}}^{Q}$ が式 (35) として与えられた場合、逆に、適当な unitary 作用素 $\hat{U}^{QE}$ と量子状態 $\hat{\rho}_{\rm in}^{E}$ が存在して、式 (34) の表現を導くことができる。即ち、式 (34) と式 (35) は同じ量子通信路 $\hat{\mathcal{L}}^{Q}$ の異なる表現に他ならない [49,51]。前者を unitary 表現、後者を Kraus 表現 (或いは operator-sum 表現) と呼ぶ [51]。

Hilbert 空間 $\mathcal{H}^{Q}\otimes\mathcal{H}^{R}$ 上で表される合成系の部分系 Q に対する量子操作や量子測定が量子通信路として記述される為には、任意の量子状態 $\hat{\rho}^{QR}$ と恒等写像 $\hat{\mathcal{I}}^{R}$ に対して、$(\hat{\mathcal{L}}^{Q}\otimes\hat{\mathcal{I}}^{R})\hat{\rho}^{QR} > 0$、すなわち $\mathcal{L}^{Q}$ が完全正写像でなければならない。

4.2 量子もつれ忠実度

$\hat{\mathcal{L}}^Q$ による伝送の正確さの測度として量子もつれ忠実度 (entanglement fidelity) [51] を導入する。まず、入力状態のスペクトル分解 $\hat{\rho}_{\rm in}^Q = \sum_j p_j |\psi_j^Q\rangle\langle\psi_j^Q|$ $(p_j \geq 0, \sum_j p_j = 1)$ に対し参照系 R を用意して $\mathcal{H}^Q \otimes \mathcal{H}^R$ 上の純粋化

$$|\Psi^{QR}\rangle = \sum_j \sqrt{p_j}|\psi_j^Q\rangle \otimes |\psi_j^R\rangle \tag{36}$$

を考える。$\{|\psi_j^R\rangle\}$ は Hilbert 空間 $\mathcal{H}^R$ の適当な基底ベクトルである。量子状態 $|\Psi^{QR}\rangle$ は $\hat{\mathcal{L}}^Q$ によって

$$\hat{\rho}_{\rm out}^{QR} = \left(\hat{\mathcal{L}}^Q \otimes \hat{\mathcal{I}}^R\right)|\Psi^{QR}\rangle\langle\Psi^{QR}| \tag{37}$$

へと変換される。(当然 $\hat{\rho}_{\rm in(out)}^Q = {\rm Tr}_R \hat{\rho}_{\rm in(out)}^{QR}$ である。) このとき、量子通信路 $\hat{\mathcal{L}}^Q$ の量子もつれ忠実度 $F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)$ は次の式で定義される。

$$F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = \langle\Psi^{QR}|\hat{\rho}_{\rm out}^{QR}|\Psi^{QR}\rangle \tag{38}$$

これは $0 \leq F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) \leq 1$ を満たし、$\mathcal{H}^R$ に関する量には依存しない。実際、

$$\begin{aligned} F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) &= \sum_j \sum_k p_j p_k \langle\psi_j^Q|\hat{\mathcal{L}}^Q\left(|\psi_j^Q\rangle\langle\psi_k^Q|\right)|\psi_k^Q\rangle, \\ &= \sum_\mu \left({\rm Tr}_Q[\hat{A}_\mu^Q \hat{\rho}^Q]\right)\left({\rm Tr}_Q[\hat{A}_\mu^{Q\,\dagger}\hat{\rho}^Q\right) \end{aligned} \tag{39}$$

と表せる。さて、$F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = 1$ 即ち

$$\left(\hat{\mathcal{L}}^Q \otimes \hat{\mathcal{I}}^R\right)|\Psi^{QR}\rangle\langle\Psi^{QR}| = |\Psi^{QR}\rangle\langle\Psi^{QR}| \tag{40}$$

が成り立つということは、実は単に $\hat{\mathcal{L}}^Q\hat{\rho}_{\rm in}^Q = \hat{\rho}_{\rm in}^Q$ が成り立つということ以上に強い意味を持っている。上式の両辺の行列要素 $\langle\psi_j^R|\cdots|\psi_k^R\rangle$ を計算すれば次の式が得られる。

$$\hat{\mathcal{L}}^Q\left(|\psi_j^Q\rangle\langle\psi_k^Q|\right) = |\psi_j^Q\rangle\langle\psi_k^Q| \qquad (\forall j,k) \tag{41}$$

この結果は $\hat{\rho}_{\rm in}^Q$ の固有ベクトルで展開することができる“全て”の量子状態 $\hat{\sigma}^Q = \sum_j\sum_k a_{jk}|\psi_j^Q\rangle\langle\psi_k^Q|$ に対して等号 $\hat{\mathcal{L}}^Q\hat{\sigma}^Q = \hat{\sigma}^Q$ が成り立つことを意味する。この逆もまた真である。即ち、次の関係が成り立つ。

$$F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = 1 \longleftrightarrow \hat{\mathcal{L}}^Q\hat{\sigma}^Q = \hat{\sigma}^Q \tag{42}$$

4.3 コヒーレント情報量

Shannon は相互情報量 $I(X:Y) = H(Y) - H(Y|X)$ を用いて通信路符号化を定式化したが、そのアナロジーで量子状態の伝送の定式化が試みられている。ここでは、Schumacher によって導入されたコヒーレント情報量 (coherent information) [51,53] とその基本的性質を紹介する。まず、条件付きエントロピー $H(Y|X)$ に相当するエントロピー交換 (entropy exchange) と呼ばれる量

$$S_e(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = -{\rm Tr}_{QR}\left[\hat{\rho}_{\rm out}^{QR}\log\hat{\rho}_{\rm out}^{QR}\right] \tag{43}$$

を導入する [51,53]。Kraus 表現 (35) を用いれば、

$$S_e(\hat{\rho}^Q, \hat{\mathcal{L}}^Q) = -{\rm Sp}[W\log W], \quad W_{\mu\nu} = {\rm Tr}_Q[\hat{A}_\mu^Q\hat{\rho}^Q\hat{A}_\nu^{Q\,\dagger}] \tag{44}$$

と表わすことができる。Sp は行列のトレースで作用素のトレース Tr と区別する。この式から分かるように、エントロピー交換 $S_e(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)$ は Hilbert 空間 $\mathcal{H}^R$ に関する量には依存しない。また、D を $\mathcal{H}^Q$ の次元とすると

$$S_e(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) \leq H\left(F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)\right) + \left[1 - F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)\right]\log(D^2-1) \tag{45}$$

が成り立つ [51, 53]。ここで、$H(x) = -x\log x - (1-x)\log(1-x)$ である。この不等式は従来の情報理論において条件付きエントロピーと平均誤り確率の間に成り立つ Fano の不等式 [11] と類似の構造を持ち、量子 Fano の不等式と呼ばれる。$F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = 1$ ならエントロピー交換はゼロである。

量子通信路 $\hat{\mathcal{L}}^Q$ のコヒーレント情報量 $I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)$ は

$$I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = S(\hat{\rho}_{\rm out}^Q) - S_e(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) \tag{46}$$

で定義され [51, 53]、$H(Y) \leftrightarrow S(\hat{\rho}_{\rm out}^Q)$、$H(Y|X) \leftrightarrow S_e(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)$、$I(X:Y) \leftrightarrow I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q)$ という対応関係を付けることができる。また、縦続通信路 $\hat{\mathcal{L}}_2^Q\hat{\mathcal{L}}_1^Q$ に対しては、

$$I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}_1^Q) \geq I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}_2^Q\hat{\mathcal{L}}_1^Q) \tag{47}$$

という量子データ処理不等式が成り立ち [51,53]、ここでも古典縦続通信路 $X \to Y \to Z$ に対するデータ処理不等式 $I(X:Y) \geq I(Z:X)$ での相互情報量との類似が見られる。しかし、コヒーレント情報量は

$$-S(\hat{\rho}_{\rm in}^Q) \leq I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) \leq S(\hat{\rho}_{\rm in}^Q) \tag{48}$$

なる不等式を満足し、負の値もとってしまう。この点が Shannon の相互情報量と異なっている。

4.4 量子誤り訂正

Shannon の相互情報量 $I(X:Y) = H(Y) - H(Y|X)$ は実は $I(X:Y) = H(X) - H(X|Y)$ とも書かれる。今、X

と Y をそれぞれ n 次拡大した符号語集合 X_C^n とその出力集合 Y_D^n と見なせば、図 4 のような漸近的誤りゼロの伝送が実現している状況は $I(X_C^n : Y_D^n) \sim H(X_C^n)$ $(n \to \infty)$、即ち $H(X_C^n|Y_D^n) \sim 0$ という条件に一致する。つまり、何らかの誤り訂正によってエラーフリー伝送が実現される通信路の条件は $I(X:Y) = H(X)$ である。量子情報の伝送に対しては、コヒーレント情報量を使ってこれに類似の条件が導かれる。量子通信路 $\hat{\mathcal{L}}^Q$ が量子誤り訂正可能であるとは、適当なトレースを保存する完全正写像 $\hat{\mathcal{R}}^Q$ が存在して、合成量子通信路 $\hat{\mathcal{R}}^Q\hat{\mathcal{L}}^Q$ に対して

$$F(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{R}}^Q\hat{\mathcal{L}}^Q) = 1 \tag{49}$$

とできること、つまり出力状態 $\hat{\rho}_{\rm out}^Q$ から量子誤り訂正 $\hat{\mathcal{R}}^Q$ によって $\hat{\rho}_{\rm in}^Q$ が復元できるを意味する [53, 54]。そのための必要十分条件は、

$$I_C(\hat{\rho}_{\rm in}^Q, \hat{\mathcal{L}}^Q) = S(\hat{\rho}_{\rm in}^Q) \tag{50}$$

で与えられることが示されている [53]。解釈は古典通信路の場合と同様である。Kraus 表現 $\hat{\mathcal{L}}^Q\hat{X} = \sum_\mu \hat{A}_\mu^Q \hat{X} \hat{A}_\mu^{Q\dagger}$ を用いると式 (50) は

$$\langle\psi_k^Q|\hat{A}_\nu^{Q\dagger}\hat{A}_\mu^Q|\psi_j^Q\rangle = \delta_{jk}M_{\mu\nu} \tag{51}$$

という形にも書くことができる [54]。ここで $\hat{\rho}_{\rm in}^Q = \sum_j p_j|\psi_j^Q\rangle\langle\psi_j^Q|$ (スペクトル分解)、$M_{\mu\nu}$ はパラメータ j に依存しないエルミート行列である。条件 (51) は $\hat{\rho}_{\rm in}^Q$ の固有ベクトルにのみ依存し、固有値 p_j には依存しない。したがって、条件 (50) も実は $\hat{\rho}_{\rm in}^Q$ の固有値には依存しないのである。また式 (42) から分かる通り、式 (50) 或いは式 (51) が成り立てば、$\hat{\rho}^Q$ の固有ベクトルで展開できる $\mathcal{H}^Q$ 上の任意の量子状態 $\hat{\sigma}^Q$ に対して量子誤り訂正が可能である。即ち、量子状態 $\hat{\rho}_{\rm in}^Q$ の固有ベクトル $|\psi_j^Q\rangle$ で展開できる任意の量子状態 $\hat{\rho}_1^Q$ と $\hat{\rho}_2^Q$ があった時、$F(\hat{\rho}_1^Q, \hat{\mathcal{R}}_1^Q\hat{\mathcal{L}}^Q) = 1$ を満足する完全値写像 $\hat{\mathcal{R}}_1^Q$ が存在すれば、$F(\hat{\rho}_2^Q, \hat{\mathcal{R}}_2^Q\hat{\mathcal{L}}^Q) = 1$ を満足する完全値写像 $\hat{\mathcal{R}}_2^Q$ も存在するのである。

4.5 量子通信路符号化定理へ向けて

以上が量子状態の通信路符号化定理へ向けた道具立ての一例である。コヒーレント情報量の他にも、量子通信路の特性を記述する量として幾つかのエントロピックな量が考えられるが、どのように量子状態の通信路符号化定理を定式化し、量子状態そのものの伝送効率の限界を求めるかは今後の課題である。符号化は従来同様、入力情報源を拡大し冗長度を付加することによって行われる。それは n 次拡大量子情報源 $\hat{\rho}^{Q\otimes n}$ が張る空間での適当な完全正写像 $\hat{\mathcal{C}}_n^Q$ であり (一般には $\hat{\mathcal{C}}_n^Q \neq \hat{\mathcal{C}}_1^{Q\otimes n}$)、符号語状態は $\hat{\mathcal{C}}_n^Q\hat{\rho}^{Q\otimes n}$ である。通信路からの出力 $\hat{\mathcal{L}}^{Q\otimes n}\hat{\mathcal{C}}_n^Q\hat{\rho}^{Q\otimes n}$ は復号化 $\hat{\mathcal{D}}_n^Q$ によって $\hat{\rho}_n^Q = \hat{\mathcal{D}}_n^Q\hat{\mathcal{L}}^{Q\otimes n}\hat{\mathcal{C}}_n^Q\hat{\rho}^{Q\otimes n}$ に復元される。拡大情報源 $\hat{\rho}^{Q\otimes n}$ と合成量子通信路 $\hat{\mathcal{K}}_n^Q = \hat{\mathcal{D}}_n^Q\hat{\mathcal{L}}^{Q\otimes n}\hat{\mathcal{C}}_n^Q$ に対する量子もつれ忠実度が $\lim_{n\to\infty} F(\hat{\rho}^{Q\otimes n}, \hat{\mathcal{K}}_n^Q) = 1$ となれば漸近的エラーフリー伝送が実現できたことになる。問題はそのような符号化 $\hat{\mathcal{C}}_n^Q$ と復号化 $\hat{\mathcal{D}}_n^Q$ が存在するか否かである。現在はその必要条件が $S(\hat{\rho}^Q) \le Q \equiv \max_{\hat{\sigma}^Q} I_C(\hat{\sigma}^Q\,\hat{\mathcal{L}}^Q)$ である、ということが示されている段階である [55–57]。この不等式において等号が成り立つような符号化 $\hat{\mathcal{C}}_n^Q$ と復号化 $\hat{\mathcal{D}}_n^Q$ の存在を示すことができれば、コヒーレント情報量 $I_C(\hat{\rho}^Q\,\hat{\mathcal{L}}^Q)$ の最大値 Q が量子通信路の容量を与えることになるのだが、これは今後の研究課題である。

5 量子もつれの制御

最後に、古典的対応を持たない通信資源、量子もつれについて、漸近的極限における性能限界という観点から整理する。通信スケールに展開された量子もつれ状態 $\hat{\rho}^{AB}$ の操作は、多くの場合、各サイト A, B での局所的な量子操作とその結果を古典通信よってやり取りするという形 (Local Operation + Classical Communication, LOCC) で行わなければならない (図 8)。Hilbert 空間 $\mathcal{H}^A \otimes \mathcal{H}^B$ 上で定義

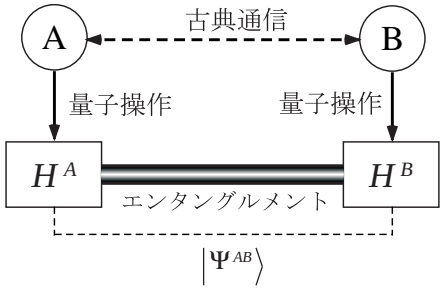

図 8: 局所的な量子操作と古典通信による量子状態の変換。

される量子状態 $\hat{\rho}^{AB}$ の量子もつれの基本性質を纏めると次のようになる [58]。

1. 量子状態 $\hat{\rho}^{AB}$ が可分 (separable) ならば、即ち、$\hat{\rho}^{AB} = \sum_k p_k\hat{\rho}_k^A \otimes \hat{\rho}_k^B$ $(p_k \ge 0, \sum_k p_k = 1)$ の形に表わすことができるとき、量子状態 $\hat{\rho}^{AB}$ の量子もつれはゼロである。

2. 局所的な unitary 変換 $\hat{U}^A \otimes \hat{U}^B$ の下で量子状態 $\hat{\rho}^{AB}$ の量子もつれの大きさは不変である。

3. 局所的量子作用と AB 間の古典通信を用いた量子状態 $\hat{\rho}^{AB}$ の変換によって、量子状態 $\hat{\rho}^{AB}$ の量子もつれ

の大きさは “平均として” 増加することはない。

第 1 番目の性質は自明である。第 2 番目の性質は局所的な unitary 変換が各系の量子状態の表現を変えるだけであり、AB 間の量子もつれには影響を及ぼさないことを意味している。第 3 番目の性質は、量子状態の No-cloning 定理と密接に関係している。また、第 3 番目の性質では、量子もつれが平均として増加しなければ、量子操作の個別の結果によっては (有限の確率で) 量子もつれが増加して良い。混合状態の量子もつれに関しては未解決の問題が多く残されているので、ここでは量子状態 $\hat{\rho}^{AB}$ が純粋状態である場合のみを考える。

Hilbert 空間 $\mathcal{H}^A \otimes \mathcal{H}^B$ の任意の状態ベクトル $|\Psi^{AB}\rangle = \sum_j \sum_k a_{jk} |\phi_j^A\rangle \otimes |\phi_k^B\rangle$ は適当な基底ベクトルの変換を行うことによって、総和が一つだけ現れる $|\Psi^{AB}\rangle = \sum_k a_k |\phi_k^A\rangle \otimes |\phi_k^B\rangle$ と言う形に表わすことができる (Schmidt 表現)。ここで $\{|\phi_k^{A(B)}\rangle\}$ は $\mathcal{H}^{A(B)}$ の適当な基底ベクトルである。縮約された量子状態 $\hat{\rho}^A = \mathrm{Tr}_B |\Psi^{AB}\rangle\langle\Psi^{AB}|$ は一般には混合状態であり、純粋状態になるのは $|\Psi^{AB}\rangle$ に量子もつれがある場合のみである。よって、量子もつれの度合いを $\hat{\rho}^A$ の混合度として

$$E(|\Psi^{AB}\rangle) = S(\hat{\rho}^A) = -\mathrm{Tr}_A[\hat{\rho}^A \log \hat{\rho}^A] \qquad (52)$$

定義するのは自然であろう。対数の底を 2 にとった時の単位を “ebit” (entanglement bit) と呼ぶ。また、明らかに $S(\hat{\rho}^A) = S(\hat{\rho}^B)$ である。$E(|\Psi^{AB}\rangle)$ は “entropy of entanglement” と呼ばれ、基本性質 1 − 3 を満足する。$\dim \mathcal{H}^A = \dim \mathcal{H}^B = N$ の場合、完全に縺れ合った量子状態 $|\Phi_N^{AB}\rangle = (1/\sqrt{N}) \sum_{k=1}^N |\phi_k^A\rangle \otimes |\phi_k^B\rangle$ の量子もつれの大きさは、$E(|\Phi_N^{AB}\rangle) = \log N$ である。$E(|\Psi^{AB}\rangle)$ は次のような漸近的極限における機能的意味を持つ [59]。

- **Distillation:** LOCC によって n 個の $|\Psi^{AB}\rangle$ から生成される完全な量子もつれ状態 $|\Phi^{AB}\rangle$ の個数を m とすれば、$E_D \equiv \lim_{n\to\infty}(m/n) = E(|\Psi^{AB}\rangle)/E(|\Phi^{AB}\rangle)$ が成り立つ。
- **Formation:** LOCC によってによって n 個の $|\Psi^{AB}\rangle$ を生成する為に必要な完全な量子もつれ状態 $|\Phi^{AB}\rangle$ の個数を m とすれば、$E_F \equiv \lim_{m\to\infty}(m/n) = E(|\Psi^{AB}\rangle)/E(|\Phi^{AB}\rangle)$ が成り立つ。

この結果は純粋状態の場合には量子状態の量子もつれの操作は可逆的であることを意味するが (図 9)、混合状態の場合には一般には不等式 $E_D \le E_F$ が成り立ち、このような性質は必ずしも成り立たない [58, 60]。

量子もつれの distillation や formation の実際の操作性を規定するための条件について、幾つかの結果を紹介して

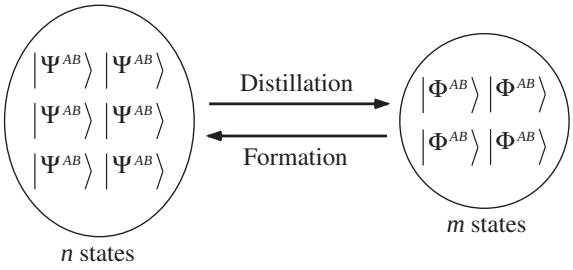

図 9: 量子状態の distillation と formation の概念図。

おく。まず、$\mathcal{H}^A \otimes \mathcal{H}^B$ 上 ($\dim \mathcal{H} = \dim \mathcal{H}^B = N$) の状態 $|\Psi^{AB}\rangle$ の順序付けられた Schmidt 表現

$$|\Psi^{AB}\rangle = \sum_{k=1}^N \sqrt{\lambda_j^\psi} |\phi_k^A\rangle \otimes |\phi_k^B\rangle, \quad \left(1 \ge \lambda_1^\psi \ge \cdots \ge \lambda_N^\psi \ge 0\right) \qquad (53)$$

と “entanglement monotone” と呼ばれる量 [61]

$$E_k(\psi) = \sum_{j=k}^N \lambda_j^\psi, \qquad (k = 1, 2, \ldots, N) \qquad (54)$$

を導入する。規格化条件から $E_N(\psi) = 1$ である。変換 $|\Psi^{AB}\rangle \to |\Phi^{AB}\rangle$ が LOCC によって確率 1 で実現できる為の必要十分条件は

$$E_k(\psi) \ge E_k(\phi), \quad (k = 1, 2, \ldots, N) \qquad (55)$$

で与えられる [61, 62]。さらに一般化して、変換 $|\Psi^{AB}\rangle \to |\Phi^{AB}\rangle$ が起り得る確率の最大値 $P\left(|\Psi^{AB}\rangle \to |\Phi^{AB}\rangle\right)$ が

$$P\left(|\Psi^{AB}\rangle \to |\Phi^{AB}\rangle\right) = \min_{1\le k\le N} \frac{E_k(\psi)}{E_k(\phi)} \qquad (56)$$

で与えられることも示されている [63, 64]。同様のことは “majorization” を用いることによっても可能である [50, 62]。また、変換 $|\Psi^{AB}\rangle \to |\Phi^{AB}\rangle$ を直接行うことは不可能であっても、別の量子状態 $|\Upsilon^{AB}\rangle$ を用いて、変換 $|\Psi^{AB}\rangle \otimes |\Upsilon^{AB}\rangle \to |\Phi^{AB}\rangle \otimes |\Upsilon^{AB}\rangle$ を行うことが可能になる場合が存在する [65, 66]。このとき、付加された量子状態 $|\Upsilon^{AB}\rangle$ は変換の前後で不変であり、ちょうど化学反応における触媒と同じ働きをする。この他にも多者間での量子もつれを利用した機能 [67] など多くの興味深い機能に関する研究が進められている。

6 展望

従来の情報理論との対比から見た一つの切り口として、量子情報理論を（1）古典情報の伝送、（2）量子状態そ

のものの伝送、（３）通信スケールにおける量子もつれの制御、という３つの主題に分けて概観して来た。

（１）に関しては、Shannon 以来の体系に沿って比較的精密な理論ができつつあるが、混合状態の場合の圧縮限界や歪みが許される場合の圧縮問題、通信路符号化に関する信頼性関数の導出まどの未解決課題が残されている。さらに現代情報理論でのトピックであるネットワーク情報理論や符号複雑さ問題などもいずれ量子領域への拡張が検討されてしかるべきである。

また、何といっても情報源符号化、通信路符号化のための構成的符号理論の構築は、実用へ向けた最重要課題である。従来理論同様、これも代数的群論的基盤の上で進められて行くことになろう。Shannon の理論が発表されてからその容量限界へ達する構成的符号への足掛かりが得られるまで、40 年以上の歳月を要しているが、量子-古典通信路符号化も同様の年数を要するのだろうか。

以上の問題には多かれ少なかれ、量子状態から古典情報を取り出すための量子信号検出という問題が常に付いてまわる。誤り率最小化や相互情報量最大化に始まり、種々の性能限界を見極める問題は、適当なコスト関数を POM といういわば行列の集合を変数として最適化する問題である。この問題の数学的困難さが、おそらくは古典から量子領域への拡張を容易には行わせない主要因である。数学的道具立ての突破口が必要なように思われる。また、最適解として求まった POM が表す物理過程も一般には自明ではない。特に量子一括測定は量子もつれの制御そのものであり、一般には量子計算過程と何らかの測定過程により構成される。しかも、通信では、与えられた受信状態の一切の性質を無駄にすることなく処理しなければならない。確率的量子計算では意味がない。こういった条件下で、与えられた POM から系統的に物理モデルを導く量子回路構成論も必要である。

（２）は、Shannon 理論の一般化という枠を超えた新しい問題であり、特に、量子通信路を規定する測度の体系化と量子通信路符号化の定式化は量子情報理論の最重要課題の一つである。現在はまだ問題の要点を整理している段階と言えそうだ。多くの基本問題が眠っているように思われる。いずれ、精密な定量化が為されて行くと期待されるが、その過程でやはり Shannon の精神は大きな道しるべになるだろう。具体的符号構成としての量子誤り訂正理論は、その物理的実現性とは大きな隔たりがあるが、量子もつれ状態や完全正写像についての深い理解を得る意味でも、重要な理論的課題である。

（３）は、現在の量子情報理論の中でも一番ファッショナブルなテーマで、最近、とみに数学的色彩が強まって来たようだ。量子情報処理に登場する量子もつれ状態は、量子多体系の基底状態などとは違って、（今のところ）極めて簡単な構造をしている。しかし、それを信号処理や情報伝送へ積極的に使おうと思うと、その潜在的能力や機能的性質について我々がこれまで如何に多くを知らなかったかに愕然とするのである。今後は、２者間、３者間を超えてネットワーク上に張られる量子もつれの操作性や定量化が研究の対象になって行く気配であるが、そろそろ現代情報理論の成果も取り入れた本格的な量子ネットワーク研究が出て来ても良いように思う。

まだ始まったばかりの研究分野ということもあって、量子情報理論に対するとらえ方は千差万別で、ここで述べたものも一つの切り口に過ぎず、しかも随所に著者らのバイアスがかかっていると思われる。当然入れるべき多くの重要課題が触れられずに終わった。是非、また別の視点から解説が書かれることを期待する。

最後に、有益な助言と原稿作成に協力を頂いた水野潤氏、有益な議論をして頂いた広田修氏に感謝致します。

参考文献

[1] C. W. Helstrom, Inform. Contr. **10**, pp254-291, (1967).

[2] 広田修、光通信理論 (森北出版, 1985).

[3] R. Landauer, IBM J. Res. Dev. 5, 183 (1961); C. H. Bennett, *ibid* 17(6), pp525-32 (1973).

[4] D. Deutsch, Proc. R. Soc. Lond. A 400, 97 (1985).

[5] P. Shor, in Proc. of 35th Annual Symp. on the theory of Computer Science, p124 (1994).

[6] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. A **47**, 777 (1935).

[7] C. H. Bennett and P. Shor, IEEE Trans. Inform. Theory, IT-**44**, No. 6, pp2724-2742 (1998).

[8] 細谷曉夫, vol**52**, no. 10, 748 (1997); 竹内繁樹, vol**54**, no. 4, 263 (1999); 井元信之、小芦雅斗, vol**56**, no. 1, 17 (2001).

[9] “A Mathematical Theory of Communication,” Bell System Tech. J. vol. **27**, pp379-423 (Part I), pp623-656 (Part II) (1948).

[10] R. G. Gallager, *Information Theory and Reliable Communication*, J. Wiley (New York), (1968).

[11] T. Cover and J. Thomas : *Elements of Information Theory* (John Wiley and Sons, New York, 1991).

[12] C. W. Helstrom : *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[13] このような最適受信器の物理的対応は決して自明ではない。M. Sasaki and O. Hirota, Phys. Rev. A**54**, 2728, (1996); M. Sasaki, et al., Phys. Rev. A**58**, 159 (1998). 等で幾つかの物理的対応が解って来てはいるが、多くの場合その物理的対応はほとんど未解決のままである。

[14] W. K. Wootters and W.H. Zurek, Nature **299**, 802 (1982).

[15] H. P. Yuen, Phys. Lett. A, **113**, 405 (1986).

[16] C. H. Bennett, et al., *Phys. Rev. Lett.* **70**, 1895 (1993).

[17] L. Vaidman, Phys. Rev. Lett. A**49**, 1473 (1994).

[18] S. L. Braunstein and H. J. Kimble, Nature **394**, 840 (1998).

[19] D. Bouwmeester, et al., Nature **390**, 575 (1997).

[20] D. Boshi, et al., Phys. Rev. Lett. **80**, 1121 (1998).

[21] A. Furusawa, et al., Science **282**, 706 (1998).

[22] B. Schumacher, Phys. Rev. A**51**, 2738 (1995).

[23] R. Jozsa and B. Schumacher, J. Mod. Opt., **41**, 2343 (1994).

[24] R. Jozsa, et al, Phys. Rev. Lett**81**, 1714 (1998).

[25] M. Horodecki, Phys. Rev. A**57**, 3364 (1998).

[26] M. Koashi and N. Imoto, LANL e-print arXiv: quant-ph/0101144, quant-ph/0103128.

[27] B. Schumacher and M. D. Westmoreland, LANL e-print arXiv: quant-ph/0011014.

[28] E. B. Davies, IEEE Trans. Inf. Theory **IT-24**, 596 (1978).

[29] L. B. Levitin, *Quantum Communication, and Measurement*, pp401-409, (Ed. by V. P. Belavkin, O. Hirota, and R. L. Hudson, Prenum, New York, 1995).

[30] M. Osaki, et al., pp17-26, *Quantum Communication, Computing, and Measurement 2* (Ed. by P. Kumar, G. M. D'Ariano, and O. Hirota, Kluwer academic/Prenum publishers, New York, 2000).

[31] A. S. Holevo, Probl. Peredachi Inform. vol 9, no. 3, pp. 3-11 (1973). 最初の予想は J. P. Gordon, pp.156-181 in *Quantum Electronics and Coherent Light*, Proc. Int. School Phys. "Enrico Fermi", Course XXXI, (Ed. P. A. Miles, New York: Academic Press 1964) である。

[32] R. L. Stratonovich and A. G. Vantsyan, Probl. Upr. Teor. Inf., vol. 7, no. 3, 161-174 (1978).

[33] A. S. Holevo, Theory Prob. Appl., vol. 23, 411, June(1978).

[34] P. Hausladen and W. K. Wootters, J. Mod. Opt. **41**, 2385 (1994).

[35] A. S. Holevo, Probl. Peredachi Inform. vol 15, no. 4, 3-11 (1979).

[36] P. Hausladen, et al., Phys. Rev. A**54**, 1869 (1996).

[37] K. Kato, et al., Phys. Lett. A**251**, 157 (1999).

[38] A. S. Holevo, IEEE Trans. Inf. Theory **IT-44**, 269 (1998).

[39] B. Schumacher and M. Westmoreland, Phys. Rev. A**56**, 131 (1997).

[40] M. V. Burnashev and A. S. Holevo, Probl. Peredachi Inform., vol. 34, pp1-13, (1998); (LANL e-print arXiv:quant-ph/9703013).

[41] M. Ban, et al., J. Opt. B **1**, 206 (1999).

[42] A. S. Holevo, IEEE Trans. Inf. Theory, **IT-46**, 2256 (2000).

[43] M. Sasaki, et al., Phys. Rev. A**58**, 146 (1998).

[44] J. R. Buck, et al., Phys. Rev. A**61**, 032309 (2000).

[45] S. Usami, et al., *Quantum Communication, Computing, and Measurement 3* (Ed. by P. Tombesi and O. Hirota, Kluwer academic/Prenum publishers, New York, in press).

[46] A. S. Holevo, Tamagawa University Research Review **4**, 1 (1998); (extended version, LANL e-print arXiv:quant-ph/9809023).

[47] H. P. Yuen and M. Ozawa, Phys. Rev. Lett 70, 363 (1993).

[48] M. Shoma and O. Hitota, Phys. Rev. A**62**, 052312 (2000).

[49] K. Kraus, *States, Effects, and Operations* (Springer-Verlag, Berlin, 1983).

[50] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[51] B. Schumacher, Phys. Rev. A **54**, 2614 (1996).

[52] M. Horodecki, et al., Phys. Lett. A**223**, 1 (1996).

[53] B. Schumacher and M. A. Nielsen, Phys. Rev. A **54**, 2629 (1996).

[54] E. Knill and R. Laflamme, Phys. Rev. A **55**, 900 (1997).

[55] H. Barnum, et al., Phys. Rev. A **57**, 4153 (1998).

[56] H. Barnum, et al., Phys. Rev. A **58**, 3496 (1998).

[57] H. Barnum, et al., IEEE Trans. Inf. Theory **IT-46**, 1317 (2000).

[58] C. H. Bennett, et al., Phys. Rev. A **54**, 3824 (1996).

[59] C. H. Bennett, et al., Phys. Rev. A **53**, 2046 (1996).

[60] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).

[61] G. Vidal, **47**, 355 (2000).

[62] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).

[63] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).

[64] G. Vidal, et al., Phys. Rev. A **62**, 012304 (2000).

[65] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999).

[66] F. Morikoshi, Phys. Rev. Lett. **84**, 3189 (2000).

[67] M. Murao, et al., Phys. Rev. A **59**, 158 (1999).