チュートリアル

量子力学と情報処理(II)

丸山 耕司

前回，ある情報源の生み出す情報の量は，情報を受け取ったときの'意外さ'，'驚き'の大きさで評価し，定量的には確率分布をもとにShannonエントロピー $H(p_i)=-\sum_i p_i \log_2 p_i$ で表されることをみた．さらに量子状態ρのもつエントロピーは，von Neumannエントロピー $S(\rho)=-\mathrm{Tr}(\rho \log_2 \rho)$ で与えられるのであった．von Neumannエントロピーの起源は熱力学にあることはすでに述べたが，Shannonエントロピーとの形式上の類似性から次のように解釈することもできる．状態 ρ を正規直交基底のセット $\{|e_i\rangle\}$ で射影測定したとき，結果 j が得られる確率は $p_j=\langle e_j|\rho|e_j\rangle$ であるが，von Neumannエントロピー $S(\rho)$ は確率分布 $\{p_j\}$ によるShannonエントロピー $H(p_j)$ の最小値を与える†1．$S(\rho)=H(p_j)$ となるのは，$\{|e_i\rangle\}$ が ρ の固有状態の組 $\{|\tilde{e}_i\rangle\}$ であるときだけである．つまり，ρ は確率 p_i で状態 $|\tilde{e}_i\rangle$ を生む'古典的'情報源であるとみなせる．ただ，量子情報で扱う多くの問題では，情報が直交基底 $\{|e_i\rangle\}$ のそれぞれを用いてエンコードされていなかったり，たとえ $\{|e_i\rangle\}$ に情報がエンコードされても，受け手には $\{|e_i\rangle\}$ が不明であったり，ノイズなどの影響で受け取る状態がもはや $\{|e_i\rangle\}$ では記述できなかったりで，一筋縄ではいかない．それでも，こうした直感的解釈は役に立つことが多く，実際，量子データ圧縮などはそれでかなりストレートに理解できる．

そこで今回は，情報を量子系に持たせるという考え方の紹介も兼ねて，量子データ圧縮と，Holevo限界とよばれる量子系にエンコードできる情報量，さらに量子誤り訂正について説明する．対応する初等的(古典)情報理論での扱いを少し詳しく述べるが，すでに詳細をご存知の方は斜め読みしていただいてかまわない．LandauerとBennettによって明確にされたエントロピーの二面性——熱力学的，および情報理論的な側面——が，こうしたトピックにおいても明快な物理的説明を与えてくれることもみる．

1 古典データ圧縮

量子データ圧縮は，基本的には通常の(古典)データ圧縮と同じ理屈で実行される．データ圧縮とは，当然のことながら，長い文字列("00101101..."など)を，情報を失わないようにしながら(復元可能なように)短い文字列に変換して，単位時間あたりの通信量やメモリーの単位サイズあたりの記憶量を可能な限り大きくする作業である†2．情報理論では符号化ともよばれる．古典といえども基礎となるアイデアは知っておいて損はないので，少し詳しくデータ圧縮の仕組みをみてみよう．圧

†1 証明は，たとえば，Nielsen, M. A. and Chuang, I. L., Quantum Computation and Quantum Information, Cambridge University Press, 2000, 中の Theorem 11.9 を参照．

まるやま こうじ．(独)理化学研究所基幹研究所．

†2 完全に復元可能でない(可逆でない)圧縮方法も存在する．ポピュラーな例として，画像データ圧縮のjpegや音声データ圧縮のmp3などがある．

縮の方法とともに，もとの文字列の長さを n ビット，圧縮された文字列の長さを m ビットとしたときの，圧縮率 $R=m/n$ をどれだけ小さくできるかを知りたい．ここでは通信や記憶の過程でノイズによって失われる情報量がゼロと仮定する．ノイズがある場合については後述する．

圧縮の対象となる文字列は，文字 $x_i(i\in\{1, 2, ..., N\})$ のそれぞれを確率 p_i で生成する情報源 X から得られるとする．また，この確率分布は文字列中の位置によらず常に一定で，他の位置に現れる文字との相関もないとする．このような情報源は独立同分布(independent and identically distributed，しばしば i. i. d. と略される)であるという．さて，確率分布 $\{p_i\}$ という制限のおかげで，実は多くの文字列はほとんど絶対に現れないことが言える．より正確には，文字列の長さ n を長くしていくと，列の中の x_j の数は np_j に近くなり，x_j の数が np_j から大きくはずれるような列はまず現れなくなる．もっと正確に言うために，typical set を定義しよう．文字列 $x_1, x_2, ..., x_n$ が現れる確率 $p(x_1, ..., x_n)$ が，ある $\varepsilon>0$ に対して，

$$2^{-n(H(X)+\varepsilon)} \le p(x_1, ..., x_n) \le 2^{-n(H(X)-\varepsilon)} \quad (1)$$

を満たすとき，この文字列は ε-typical であると言い，そうした文字列の集合を typical set とよぶ．式(1)の対数をとれば分かるように，これは typical sequence $x_1, x_2, ..., x_n$ のもつ一文字当たりのエントロピーが情報源のエントロピー $H(X)$ とほぼ一致することを意味している：

$$\left|-\frac{1}{n}\log_2 p(x_1, ..., x_n)-H(X)\right| \le \varepsilon. \quad (2)$$

さらに，各 typical sequence の出る確率が(n が大きい極限で)等しいことも分かる．上で述べたことは，文字列の長さ n が長くなると typical set に属さない文字列が出てくる可能性は事実上ゼロになる，と言い換えることができる．このことは定理として次のように言える：

(i) $\varepsilon>0$ を適当に選んで固定する．すると，任意の $\delta>0$ に対して，情報源から得られる文字列の長さ n を十分大きくとると，ε-typical である確率が $1-\delta$ より大きくなる．

(ii) ε-typical である長さ n の文字列全体の集合を $T(n, \varepsilon)$ と書こう．任意の $\varepsilon, \delta>0$ に対して，n を十分大きくとると，ε-typical である文字列の数，$|T(n, \varepsilon)|$，が次の関係を満たす：

$$(1-\delta)2^{n(H(X)-\varepsilon)} \le |T(n, \varepsilon)| \le 2^{n(H(X)+\varepsilon)}. \quad (3)$$

証明は省略するが，大数の法則と ε-typicality の簡単な応用である．

ここまで来れば，圧縮率に関する，Shannon の雑音のないときの符号化定理は簡単に理解できる．この定理は，以下の主張をする：確率変数 X を生成する i. i. d. 情報源のエントロピーが $H(X)$ であるとする．圧縮率 $R=m/n$ が $R>H(X)$ を満たすときは，復元可能なデータ圧縮が可能である．

証明の流れを簡単に追ってみよう．$R>H(X)$ であれば，$H(X)+\varepsilon<R$ となるような $\varepsilon>0$ を選ぶことができる．上の typical set に関する定理により，任意の $\delta>0$ に対して，十分大きな n をとれば，ε-typical な文字列 $T(n, \varepsilon)$ の数は高々 $2^{n(H(X)+\varepsilon)}<2^{nR}$ であり，生成される文字列が ε-typical である確率は $1-\delta$ 以上にできる．そこで，まず圧縮対象となる長さ n の文字列が，ε-typical かどうかを調べ，もしそうであれば，$|T(n, \varepsilon)|$ だけある可能性のうちのどれかを特定し，nR ビットで表せばよい．ε-typical でなければ(これは確率 δ 以下で起こる)，余っている $2^{nR}-2^{n(H(X)+\varepsilon)}$ のうちの文字列を使い，ε-typical でない旨の信号を入れる．その直後で，ε-typical でない文字列を長さ n のまま送る．

長さ n の文字列を圧縮するのに必要となる長さは，平均で1文字あたり $[(1-\delta)nR+\delta(nR+n)]/n=R+\delta$ となり，n を大きくすることで δ はいくらでも小さくできるから，$R>H(X)$ であれば，復元可能な圧縮が可能となる．

簡単な例を示そう．4種類の文字A, B, C, Dをそれぞれ確率 $p_A=1/2$, $p_B=1/4$, $p_C=p_D=1/8$ で生成する情報源を考える．この情報源のエントロピーは7/4ビットである．では，上の各々の確率に従って生成された長さ8の文字列'ABACBDAA'を圧縮しよう．4種類の文字を表すには2ビット必要だから，2進符号でそのまま符号化すると16桁必要で，1桁あたりの情報量は $H(p_i)=7/8$ ビットとなる．この16桁の文字列を $16\times 7/8=14$ ビットの列(7文字の4進符号)に圧縮できるだろうか．

そこで，次のような符号化を考える．A→0, B→10, C→110, D→111, である．すると，先ほどの8文字の列は'01001101011100'となり，すでに14ビットに収まっている．これを2桁ずつ区切って，00→a, 01→b, 10→c, 11→dのように変換すれば，7文字の列'badbbda'に圧縮されたことになる．この過程はすべて逆をたどることができるので，元の文字列も一意に復元できる．これはまさに，$2^{16H(p_i)}=2^{14}$ 個のtypical sequences(のひとつ)を14ビットの2進符号(7文字の4進符号)で表したことに相当している．

2 量子データ圧縮

上でも述べたように，量子データ圧縮(量子符号化定理)はShannonの符号化定理の量子版への素直な拡張である．2^n 次元Hilbert空間 $H^{\otimes n}$ に作用する(密度)演算子で表される n 量子ビット(qubit)状態 $\rho^{\otimes n}$ を，2^{nR} 次元 $(0<R\leq 1)$ のHibert空間上の密度演算子へ，復元可能なように写像することが量子符号化である．2^{nR} 次元の空間は，実質的に nR qubitsの状態空間と同じであるから，n qubit状態を nR qubit状態に圧縮することになる．

状態 ρ を情報源から生成される状態として，その固有ベクトル $\{|\lambda_i\rangle\}$ による分解を $\rho=\sum_i p_i|\lambda_i\rangle\langle\lambda_i|$ とすると，当然 $H(p_i)=S(\rho)$ である．よって，式(2)中の $H(X)$ を $S(\rho)$ で置き換えれば，状態 $|x_1\rangle|x_2\rangle\cdots|x_n\rangle$ $(|x_i\rangle\in\{|\lambda_1\rangle, ..., |\lambda_n\rangle\})$ の ε-typicalityを，データ列 $x_1, x_2, ..., x_n$ の ε-typicalityとして定義できる．

すべての ε-typicalな $|x_1\rangle|x_2\rangle\cdots|x_n\rangle$ で張られる部分空間を，再び $T(n,\varepsilon)$ と書き，この部分空間への射影演算子を $P(n,\varepsilon)$ としよう．すると，古典情報の場合の定理が次のように'翻訳'される：

(i) $\varepsilon>0$ を適当に選んで固定する．すると，任意の $\delta>0$ に対して，量子情報源から得られるqubit列 $\rho^{\otimes n}$ の長さ n を十分大きくとると，$\rho^{\otimes n}$ が ε-typicalである確率が $1-\delta$ より大きくなる．すなわち，$\mathrm{Tr}(P(n,\varepsilon)\rho^{\otimes n})\geq 1-\delta$.

(ii) 任意の $\varepsilon, \delta>0$ に対して，n を十分大きくとると，ε-typicalな部分空間の次元 $|T(n,\varepsilon)|$ が次の関係を満たす：

$$(1-\delta)2^{n(S(\rho)-\varepsilon)}\leq |T(n,\varepsilon)| \leq 2^{n(S(\rho)+\varepsilon)}. \quad (4)$$

Schumacherによって示された(無雑音)量子符号化定理は，次のように表される[1]：

Hilbert空間 H 上の量子状態 ρ を生成するi. i. d. 量子情報源があるとする．圧縮率 R が $R>S(\rho)$ を満たすときは，復元可能な量子データ圧縮が可能である．

証明はShannonの符号化定理を注意深く'量子化'すればよい．

さて，以上のような符号化定理を，Landauerの消去原理の視点から見るとどうなるだろうか．古典系でも量子系でも同じ議論が適用できるので，量子系で話を進めよう．状態 $|\psi_i\rangle$ を確率 p_i で生成する情報源を考える．'平均'の状態は密度演算子 $\rho=\sum_i p_i|\psi_i\rangle\langle\psi_i|$ で表されるから，前回述べたように，この状態に記録された情報を消去するのに必要なエントロピー増加は $k\ln 2S(\rho)$ である．そこで，量子状態 $\rho^{\otimes n}$ にエンコードされた情報を圧縮して，$n(S(\rho)-\varepsilon)$ qubits $(\varepsilon>0)$ に変換できたとしよう．圧縮(符号化)の結果できる文字列(qubit列)はどれも等しい確率で現れるはずだから(でなければ，さらなる圧縮が可能である)，ρ

を変換した結果の各 qubit は $|0\rangle$ と $|1\rangle$ が等しい確率 1/2 で現れる混合状態 $\omega=1/2(|0\rangle\langle 0|+|1\rangle\langle 1|)$ になっている．ここで $|0\rangle$ と $|1\rangle$ は2次元 Hibert 空間を張る，互いに直交する二つの基底である．

状態 ω にある $n(S(\rho)-\varepsilon)$ qubits が保持する情報を消去するのに必要なエントロピー増加は，$nk\ln 2(S(\rho)-\varepsilon)S(\omega)=nk\ln 2(S(\rho)-\varepsilon)$ となり，$nk\ln 2S(\rho)$ より小さい．ところが，Landauer の消去原理により，状態 $\rho^{\otimes n}$ 中の情報を消去するには少なくとも $k\ln 2S(\rho)$ だけのエントロピー増加が必要なはずである．我々は可逆な圧縮を考えており，圧縮の前後で系が保持する情報量に変化はないから，これは矛盾だ．したがって，量子データ圧縮がもっとも効率よく実現できるときの圧縮率は von Neumann エントロピーで与えられることが，消去原理から分かる．

3 Holevo 限界

純粋状態 $|\phi_i\rangle$ が確率 p_i で現れる系，$\{p_i,|\phi_i\rangle\}$，が保持する情報を消去するのに最低限必要なエントロピー増加は，前回述べたように，$S(\rho)$ である．ここで $\rho=\sum_i p_i|\phi_i\rangle\langle\phi_i|$ である．無駄なく実行すれば $S(\rho)$ のエントロピー増加で情報を消去できるということは，逆に見れば状態 ρ は $S(\rho)$ 分の情報を保持でき，それだけの情報量を受信者(観測者)に伝えることができる，とも解釈できる．また，$S(\rho)$ より大きい情報量は保持できないとも言える．これは，Holevo によって証明された，量子系を観測することで得られる情報量に関する不等式の特殊な場合に相当している．ここで，取り出せる情報量の上限を Holevo 限界という．

当然，より一般的には上の純粋状態 $|\phi_i\rangle$ を混合状態 ρ_i にまで拡張した形で議論され，観測としては射影測定だけでなく，一般化された正定値演算子による観測も考える†3．つまり，確率 p_i で現れる文字 i を ρ_i にエンコードした状態 $\rho=\sum_i p_i\rho_i$ に対して，任意の観測 $\{E_m\}$ を施して得られる情報の上限 $I(\rho,E)$ が，Helevo 限界として与えられ，

$$I(\rho,E)\le S(\rho)-\sum_i p_i S(\rho_i) \qquad (5)$$

と表される．右辺はしばしば $\chi(\rho)$ と表され，Holevo quantity とか Holevo's χ などとよばれる．

式(5)の右辺を Landauer の消去原理から導けるだろうか．上の純粋状態の場合のロジックでいけば，混合状態を用いてエンコードされた情報を消去するのに，どれだけのエントロピー増加が必要かが分かればよい．

Lubkin の流儀[2]にしたがってこれを計算してみよう．量子'気体'を操る代わりに，温度 T の熱浴と情報を保持したメモリー系を相互作用させ，メモリーの状態を熱浴の状態と同じにしてしまうことで情報を消去する(**図1**)．情報は熱浴へ逃げていってしまうが，熱浴はその程度の影響では状態が変わらないほど十分に大きいとする．熱浴とメモリーの各構成粒子を記述するハミルトニアンを H とし，熱浴中の粒子の状態は Gibbs 分布 $\omega=e^{-H/kT}/Z$ にあるとする．Z は分配関数で $Z=\mathrm{Tr}(e^{-H/kT})$ である．ところで，このままでは最終的なメモリー状態が混合状態 ω となり，Landauer 流に消去を定義したときのような，きれい

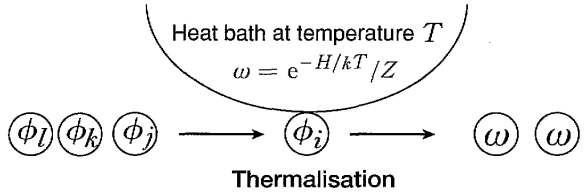

図1 熱浴との相互作用による情報の消去

†3 観測結果 m を与える(観測)演算子を M_m とすると，状態 ρ で結果 m が得られる確率は $p_m=\mathrm{Tr}(M_m^\dagger M_m\rho)$，$m$ が得られた後の状態は $\rho'=M_m\rho M_m^\dagger/p_m$ となる．全確率は常に1だから，$\sum_m M_m^\dagger M_m=I$ であり，M_m が射影演算子 P_m の場合は $P_jP_k=\delta_{jk}P_j$ を満たす．一般化された観測とは，最後の射影演算子に対する条件を取り払い，$\sum_m E_m=I$ を満たす任意の正定値演算子の組 $\{E_m\}$ で記述される観測のことである．このとき，状態 ρ において結果 m が得られる確率は $p_m=\mathrm{Tr}(E_m\rho)$，その観測後の状態は $M_m:=\sqrt{E_m}$ として $\rho'=M_m\rho M_m^\dagger/p_m$ となる．$\{E_m\}$ は，Positive Operator Valued Measure(POVM)とよばれる．

にリセットされた(純粋)状態にならない．しかし，温度 T を十分に低くすれば，$\omega=e^{-E_0/kT}|0\rangle\langle 0|+e^{-E_1/kT}|1\rangle\langle 1|+\ldots$ のうちのもっともエネルギーの低い基底状態 $|0\rangle\langle 0|$ の項が他と比べて圧倒的に大きくなり，純粋状態とみなせる．

全系のエントロピー変化は，メモリーと熱浴のエントロピー変化の和 $\Delta S_{\text{total}}=\Delta S_{\text{memory}}+\Delta S_{\text{bath}}$ である．メモリーのエントロピーは，初めの状態が ρ_i とすれば，

$$\Delta S^{(i)}_{\text{memory}} = k\ln 2(S(\omega)-S(\rho_i)) \qquad (6)$$

だけ変化する．熱浴のエントロピー変化は，熱浴とメモリーとの間でやりとりするエネルギーを温度で割ればよい：

$$\begin{aligned}\Delta S_{\text{bath}} &= \frac{\Delta Q_{\text{bath}}}{T}=\frac{\Delta Q_{\text{memory}}}{T}\\ &= -\frac{\text{Tr}\,(\omega H)-\text{Tr}\,(\rho H)}{T}\\ &= k\,\text{Tr}\,[(\omega-\rho)\ln(Z\omega)]\\ &= -k\ln 2[S(\omega)+\text{Tr}\,(\rho\log_2\omega)].\end{aligned} \qquad (7)$$

2行目から3行目への変形では，$H=-kT\ln(Z\omega)$ を使った．式(6)と式(7)より，(von Neumann エントロピーと熱力学的エントロピーの間の変換係数 $k\ln 2$ は1として)

$$\begin{aligned}\Delta S_{\text{total}} &= \sum_i p_i\Delta S^{(i)}_{\text{memory}}+\Delta S_{\text{bath}}\\ &= -\sum_i p_i S(\rho_i)-\text{Tr}\,[\rho\log_2\omega]\\ &\geq S(\rho)-\sum_i p_i S(\rho_i)\end{aligned} \qquad (8)$$

最後の不等号は(量子)相対エントロピーの非負性 $S(\rho\|\omega)=-S(\rho)-\text{Tr}\,[\rho\log_2\omega]\geq 0$ による[†4]．

式(8)の最右辺はまさしく式(5)の右辺と同じ形であり，データ圧縮の節で使ったような論理でみれば，これが状態 ρ から取り出せる情報量の上限ということになる．消去原理から Holevo 限界がきっちり出てくるのは驚きだが，これはあくまで式(5)の簡易な正当化であり，厳密な意味での導出ではない．式(6)-(8)の計算の中には，本来の証明[†5]の中で現れるべき一般化された(POVM)観測等がまったく考慮されていない．とは言え，こうも単純な論理できれいに出てくるのは興味深くはないだろうか．

4 古典および量子誤り訂正

誤りのない場合の符号化について触れた勢いで，誤り(エラー)の起こる場合についても簡単にその概念を紹介しておこう．例によって，まずは古典的な誤り訂正を考える．簡単のため，**図2**のような，確率 p でビットを反転させてしまうような通信路で説明する．このとき，どれだけの情報量が受信者に届くだろうか．送信側の情報源がもつエントロピーを $H(X)$ とし，受信者が信号を受け取った後の送信信号についての条件付きエントロピーを $H(X|Y)$ としよう．受信によって減った不確定さが得られた情報量だから，受信者は，

$$R = H(X)-H(X|Y) \qquad (9)$$

だけの情報を受け取ったことになる．これは相互情報量 $I(X:Y)$ とよばれる量で，$I(X:Y)=H(X)+H(Y)-H(X,Y)=H(Y)-H(Y|X)$ とも表される．

図2のモデルにおいて，送信側で0,1の発生する確率をそれぞれ p_0, p_1，受信側で0,1を受け取る確率を q_0, q_1 として，R を計算すると，$R=H(q_0)-H(p)$ となる．伝わる情報量 R を最大にするのは $q_0=q_1=1/2$ のときで，$R_{\max}=1-H(p)$ となる(これはまた $p_0=p_1=1/2$ のときでもある)．

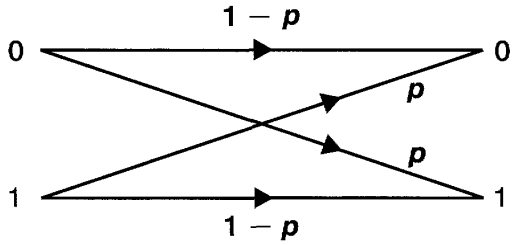

図2 バイナリ信号を送る通信路で，確率 p でビットが反転するもの

†4 脚注†1の文献中，Theorem 11.7 に証明がある．

†5 量子相対エントロピーの強加法性 strong additivity を用いたスマートな証明が，脚注†1の文献中の Theorem 12.1 に解説されている．元の文献は，Yuen, H. P. and Ozawa, M., Phys. Rev. Lett., 70, 363(1993)である．

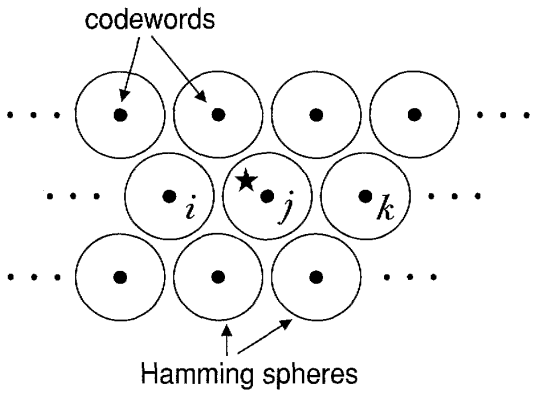

図3 誤り訂正符号の概念図

黒丸は符号，そのまわりの円は典型的なエラーがその符号に起こったときの受信信号の範囲を表す．受信信号(星印)がどの符号にもっとも近いかで送信符号(この場合は j)を推定，復元する．

つまり，1ビットの情報を一度に送ろうとしても，エラーのせいでどうしても$1-H(p)$ビットしか伝わらない．$H(p)$ビット分の情報は，我々には手の届かないところへと逃げてしまうのだ．ちなみに，与えられたエラーモデルの中でRの最大値$C=\max\{R\}$は通信路容量とよばれる．

では，エラーのある状況下で，誤り確率を任意に小さくするような符号化方法は存在するのだろうか．そうすれば，送った分の情報はすべて間違いなく受信者に届く．こんなうまい話が可能であることを示したのが，Shannonの雑音のある通信路の定理だ：容量Cの通信路とエントロピー$H(X)$の情報源があるとき，一文字あたりのエントロピーを$R(<C)$にすることで，(送受信者間での)誤り確率を任意に小さくするような符号化が存在する．

この定理が誤り訂正符号の根幹をなしているのだが，そのカラクリは明快だ．**図3**にその概念図を示す．$2^{nH(X)}$個あるtypical sequencesのうち一部分だけを符号(codeword)として送信信号に用いる．すると，典型的にはnp個のエラーが起こるので，np個のビットが反転したビット列のどれかを受け取ることになる．反転したビットの数でふたつのビット列間の距離(Hamming distance)を測ることにすれば，受信信号は高い確率で符号を中心とした半径npの'球'(Hamming sphere)の中に入り，逆に受信信号がどの球に含まれているかをみれば，元の符号を復元できる．もっとも単純な例は，0, 1を送るのに000, 111とブロックにして送る方法である．ブロック内のどれかひとつが反転して001, 101などになっても，元の信号を'多数決'で推定できるというわけだ．

それでも，typical setの中でどう符号(の集合)を選ぶかという問題は残る．これに対しShannonは，ランダムに2^{nR}個の符号を選んでしまうという大技を使って，定理を証明してしまった．符号の選び方が決まれば，定理の証明のために示すべきことは，エラーが起きても受信信号を中心とした半径npの球の中にふたつ以上の符号が入る確率をいくらでも小さくできる，ということになる．詳細は[3]などの教科書を参照されたい．

さて，誤り訂正を量子系で実行する場合はどうなるのだろうか．基本的には上の古典の場合を量子力学の言葉に翻訳すればよい．qubitの場合には0, 1の二値ではなく複素ベクトルとして表されるので，エラーも連続的な値をとり得るが，実はビット反転$|0\rangle\leftrightarrow|1\rangle$と位相反転$|0\rangle+|1\rangle\leftrightarrow|0\rangle-|1\rangle$，さらにその組み合わせの三種類[†6]の作用だけを考えればよいことが示される．よって，**図3**のような機構をn qubit状態を記述するHilbert空間に持ち込めばいいという意味で，本質的な違いはない．ただ，決定的に違うのは，各qubitを個別に射影測定するわけにはいかない，という点である．元の量子状態に含まれる重ね合わせなどの情報が壊れてしまうからである．つまり，エラーの種類を判定する測定は，**図3**のHamming sphereに相当する(互いに直交する)部分空間への非破壊の射影でなければならず，受信状態がどの部分空間に属するかという情報以外，手をつけてはいけない．

一般に複数の部分からなる系に対し，各々の部

†6 順に，三つのPauli演算子 $\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, $\sigma_y=i\sigma_x\sigma_z=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$ の作用と同一視できる．

分系への射影測定の直積で表せないような測定を実際に行うのは非常に難しい．たったふたつのqubitに対してでさえ，たとえば観測演算子 $\sigma_z\otimes\sigma_z$ の固有値 ±1 の部分空間に射影することは困難を極める．固有値 $+1$ の空間とは，$|00\rangle$ と $|11\rangle$ で張られる空間であるから，$(|00\rangle+|11\rangle)/\sqrt{2}$ のような状態も，この部分空間に属する．この重ね合わせ状態を壊すことなく $\sigma_z\otimes\sigma_z$ を測定して，観測結果 $+1$ を得るにはどうすればよいだろうか．量子誤り訂正では，さらに多くのqubitに対してこのような射影が必要となるが，この点が未だ量子誤り訂正の‘技術’としての見通しが立たない大きな要因となっている．

誤り訂正符号を実行する過程を熱力学的視点から見ることはできるだろうか．残念ながら，筆者の知る限り，Shannonの雑音のある通信路の定理を直接熱力学的に正当化する方法はない．それでも，**図2**のようなモデルの場合には，次のような熱力学的描像を考えることはできる．

n ビット信号情報を，ブロックに分割した空間内の(気体分子の)位置情報として記憶させよう．この(メモリー)空間全体を受け取った受信者は，分子の位置を読み取って送信情報を推定する．誤り訂正とは，分子の位置情報が多少ボケても元のクリアな状態を復元する作業に相当する．ボケても元の位置を推定できるようにするために，($2^{nH(X)}$ 個あるうちの)信号ひとつに対応するメモリー状態のまわりに‘バッファー’となる空間を用意する．こうすると $2^{nH(X)}$ 個のすべての信号を使うことができなくなるから，メモリーが表現できる信号数が減るが，この数を 2^{nR} とする．ひとつの n ビット信号あたりに与えられた空間の体積は $2^{n(H(X)-R)}$ であり，エラーが起きていない(気体分子の位置情報に不確定さがない)状態と，元の信号を確実に推定できる最大の体積 $2^{n(H(X)-R)}$ を占める状態との自由エネルギーの差は $n(H(X)-R)$ となる．

エラーが確率 p で起きると，エラーが起きたか否かの不確定さ(情報量)に相当する $H(p)$ だけ分子の位置に不確定さが生じ，1ビットあたりの自由エネルギーは $H(X)-R-H(p)$ に減少する．誤り訂正とは，エラーによる不確定さを除去し減少した自由エネルギーを元に戻す作業とみなせる．これは，仕事を加えて等温圧縮する過程であり，外界(熱浴)に $H(p)$ だけのエントロピーを放出する．すでに明らかなように，エラーの有無についての $H(p)$ ビットの情報を消去することこそが，誤り訂正なのだ．今の例でいくと，位置情報のボケがひとつのバッファー体積より大きくなると，もはや一意に元の位置情報を復元できなくなる．これは自由エネルギーが正でなくなることに相当するから，$H(X)-R-H(p)\geq0$ でないと誤り訂正できない．したがって，$R\leq H(X)-H(p)$，つまりエンコードできる最大の情報量は $1-H(p)$ となり，上の議論の結果と一致する．

5 まとめ

ここまでは，情報と物理の基本的関わり，さらに情報を量子系で扱うとはどういうことか，という点の紹介に重点を置き，比較的素直に古典情報理論を量子系に転用できるものを扱ってきた．こうした基礎の上に，さらに量子系に特有のentanglement(量子もつれとか量子相関と訳される)などがからむ奥深い理論が構築されていくわけである．Entanglementの理論は非常におもしろいが，それだけで泥沼にはまりかねないほど膨大な説明を要するので，本チュートリアルでは思い切って割愛し，2, 3の参考となる文献を紹介しておく[4]．しかし，その深い世界へ足を踏み入れるにしても，ここに述べてきた直感的イメージは重要な武器・道具となる．次回はいよいよ量子情報処理へと進んで，量子コンピューターの沼の深みを垣間見ていこう．

参考文献

[1] Schumacher, B., Phys. Rev. A, 51(1995), 2738.
[2] Lubkin, E., Int. J. Theor. Phys., 26(1987), 523.
[3] Cover T. M. and Thomas, J. A., Elements of Information Theory, John Wiley & Sons, Inc., New

York, 1991.
[4] Bruss, D. and Leuchs, G.(Eds.), Lectures on Quantum Information, Wiley-VCH, Weinheim, 2007. Horodecki, R., Horodecki, P., Horodecki, M. and Horodecki, K., eprint arXiv : quant-ph/0702225, Rev. Mod. Phys.(in press). Brukner, C., Zukowski, M. and Zeilinger, A., eprint arXiv : quant-ph/0106119.