01 In Laboratory Now

研究室訪問 4

情報を守る理論の開拓

藤原研究室～計算工学専攻

藤原 英二　教授

最初のコンピュータが作られてからおよそ50年。その間常に進化し続け、今では我々の生活の至る所に洗練された技術の結晶を見ることができる。現在のコンピュータ技術の根底は高度な数学的理論で成り立っている。コンピュータだけではなく、情報の通信や記録の分野もその根元をたどれば数学的理論に行き着く。そのような数学的理論の一つが符号理論である。情報技術の基盤とも言える符号理論とは一体どういうものなのか。そしてそれを追い続ける藤原研究室はどのような取り組みをしているのだろうか。

01 情報の信頼性を守る符号理論

現代社会には様々な情報があふれている。パソコンや携帯電話などを利用することにより我々も気軽に情報のやりとりをすることができる。電子機器の内部では回路上を電気信号という形で情報がやりとりされている。我々の周囲では常に電気回路で、電話回線で、そして空気中を電波に乗って、情報が流れているのだ。

情報の流れが発達している背景には、情報の信頼性が高い水準に保たれているという事実がある。信頼性が高いと言ってもそれは情報の内容のことではない。情報をやり取りする過程において情報が誤った形に変わってしまうことが少ないということである。信頼性が高いと電子機器は誤動作を起こすことはなく、通信においては少ない雑音で情報をやり取りすることができる。

今から約50年前、草創期のコンピュータは簡単な方程式が解けるくらいの機能しかなかった。しかも、当時のコンピュータは信頼性が低く、故障で停止したり、簡単な方程式ですら誤った解を出してしまうことがよくあった。当時の技術は未熟であったため外部からの物理的影響を受けやすく、回路の内部素子自体が誤動作をすることがあったのだ。また、無線などの通信に関しても、雑音が入るなどして情報が正しく伝えられないことがあった。情報の信頼性の向上が次第に強く求められるようになっていった。

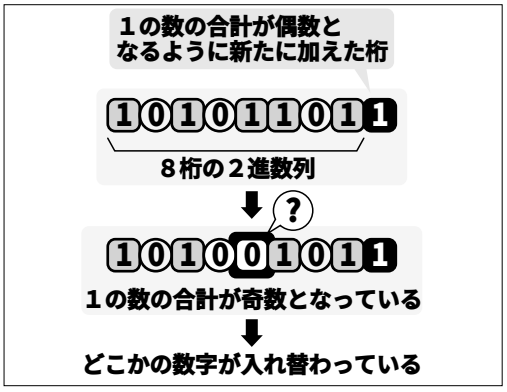

図１　単一パリティ検査符号

そこで開発されたのが藤原研究室で研究されている符号理論である。情報を扱うとき、その中に誤りが生じても修正できるように情報をある一定のルールに基づいて変換する。この変換により符号が生成できる。例えば、２進数列で表されてい

る情報に、一定のルールを与える行列や多項式を作用させることにより、情報を変換することができる。このときの行列や多項式が符号を定義している。符号を用いることによって情報の誤り、すなわちエラーを検出･訂正することが可能となる。符号理論の発展にともなって情報の信頼性は格段に向上した。今では、情報を扱うときになくてはならないものとなっているのだ。

具体的なエラー検出･訂正の例を示そう。コンピュータ内部ではデータは２進数で扱われる。ここに８桁の２進数列の情報が一つあったとしよう。これにある行列をかけるとこの数列は１桁増えて９桁となる。この９桁目の数字は２進数列中の１の数が偶数になるように設定してある（**図1**）。これだけでエラーが検出できるのだ。この情報の中の数字の一つが１から０に変わったとしよう。すると、それまで１の数の合計が偶数だったのが奇数になってしまう。当初は１の数は必ず偶数になるよう定めているため、奇数ならばエラーは確実に発生していることになるのだ。この数列の変換行列である符号は単一パリティ検査符号と言い、符号理論で最も基本的なものであるが、奇数個のエラーを100％検出できる効果は大きい。

だが、単一パリティ検査符号ではエラーの検出は可能であっても訂正はできない。どの数字が入れ替わったかわからないからだ。訂正をするためにはもう少し複雑な符号が必要となる。その中で最も簡単なのが、情報を数列から四角形の並びに置き換え、各行各列を単一パリティ検査符号とするため１行１列増やすものだ（**図2**）。こうすれば、一つの数字が入れ替わった場合、１の数の合計が奇数となった行と列の交点から誤りの位置が特定でき、訂正することが可能となる。

ハードウェア技術の向上により、故障によるエラーの発生は格段に減った。しかし、符号理論の必要性はむしろ現在においてこそ高まっている。その理由の一つとして電子機器の高集積化があげられる。携帯電話やノートパソコンをはじめとして、近年の電子機器の小型化･高性能化は著しいものがある。それは内部の電子回路の高集積化によるところが大きい。しかし、皮肉にもそれがエラーの発生を促す原因となってしまっている。回路内部の素子や配線が近接しすぎて互いに干渉してしまうということもあるが、それとともに問題

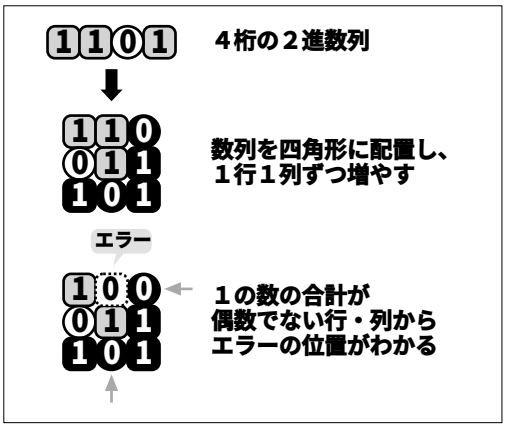

図２　水平垂直パリティ検査符号

となるのが電子回路に関するある一つの特性である。それは回路を高集積化していくと回路にかける電圧が低くなっていく、というものである。電圧が低くなることはそれだけ電力を節約できるので悪いことではない。しかし、回路の電気信号は電圧が低いと周囲の電磁波や微量な放射線などの影響を受けやすく、エラーの発生を促してしまうのだ。

現代の環境もエラー発生の原因となっている。携帯電話やパソコンなどの電子機器から発せられる電磁波は電子機器に少なからず悪影響を及ぼす。しかも電磁波の発生源は至る所にある。電子機器にとって、電磁波の充満した現代の環境は理想的とは到底言い難い。

これらの悪影響はハードウェアに直接の原因があるのではない。ハードウェアに原因があれば故障を修復するまでエラーが発生するが、高集積化や電磁波などの影響は一般に回路を破壊してしまう程強いものではないため発生するエラーは一時的なものである。その時点を過ぎれば回路は正常な動作に復帰している。ところが、このことがかえってエラーの発生時点と場所の特定を困難にしてしまい、厄介な問題となるのだ。

こういった原因により、現在の状況でエラーの発生を完全に食い止めることは不可能なのである。エラーが発生したときにいかにして被害を食い止めるか、一時的なエラーを瞬時に検出して訂正するか、符号理論はその課題を解決するために極めて有用なはたらきをする。

01 メモリで役立つ符号

コンピュータ関連で符号理論が特に活用されているのが半導体メモリや光、及び磁気ディスクなどの記憶媒体である。半導体メモリを使用した大容量のメインメモリはCPUと接続されており、プログラム実行の際には情報を一時的に保管しておく役割がある。メインメモリの記憶内容に誤りがあるとプログラムの実行に支障を来すことがあるため、信頼性は重要な要素である。しかし、小型化･高性能化･大容量化を目指していくと先に述べたように回路の高集積化でエラーの発生を促してしまい、高信頼性を得ることとは相反してしまう。この相反する二つの事柄を解決する鍵が符号理論に基づく符号化技術なのだ。

メモリ用の代表的な符号としてハミング符号があげられる。これは一つのエラーを訂正することができる。４桁の２進情報についてハミング符号を生成してみよう。まず４桁の２進情報のそれぞれの桁をx_1～x_4とおく。さらにc_1～c_3を

$$
\begin{aligned}
c_1 &= x_1 + x_2 + x_3 \\
c_2 &= \quad x_2 + x_3 + x_4 \\
c_3 &= x_1 + x_2 \quad + x_4
\end{aligned}
$$

とする。ただしこの場合の加算は１＋１＝０となる特殊なものである。このx_1～x_4とc_1～c_3の７桁が符号化された情報である。上式より通常は、

$$
\begin{aligned}
s_1 &= x_1 + x_2 + x_3 \quad + c_1 \quad = 0 \\
s_2 &= \quad x_2 + x_3 + x_4 \quad + c_2 \quad = 0 \\
s_3 &= x_1 + x_2 \quad + x_4 \quad + c_3 = 0
\end{aligned}
$$

のようになっている。しかし、エラーが発生するとs_1～s_3のうち最低でも一つは１となっている。この符号の最大のポイントは、s_1～s_3のどれが１になっているかの組み合わせによってどの桁にエラーが発生しているかが分かることである。**表１**のように、エラーが起こった箇所（表中では１となっている部分）によってs_1～s_3のパターンが異なる。s_1～s_3を見ればどの部分でエラーが発生したか瞬時に判明する。あとはその箇所の数字を入れ替えれば修正できる。

誤りパターン（１となっているところが誤り）							sのパターン		
X_1	X_2	X_3	X_4	C_1	C_2	C_3	S_1	S_2	S_3
1	0	0	0	0	0	0	1	0	1
0	1	0	0	0	0	0	1	1	1
0	0	1	0	0	0	0	1	1	0
0	0	0	1	0	0	0	0	1	1
0	0	0	0	1	0	0	1	0	0
0	0	0	0	0	1	0	0	1	0
0	0	0	0	0	0	1	0	0	1
0	0	0	0	0	0	0	0	0	0

表１

従来、メインメモリには実用性の観点からハミング符号の応用形、変化形が使われている。このメモリの場合、エラーが大量かつ連鎖的に発生することはほとんどなく、ほとんどの場合ランダムに発生するためエラーはとびとびである。そのため、メモリに使われる符号は一、二個のエラーを検出･訂正できるものが多い。しかし、近年の半導体メモリにおけるハードウェアの進歩により生じるエラーのパターンも多様化しており、さらなる高効率性、高信頼性を実現できる新しい符号が求められている。藤原研究室ではそのような社会のニーズに答えられるような符号の設計に関する研究に取り組んでいるのだ。

01 符号が新技術を可能にする

現在注目されている新技術にホログラフィックメモリという記録媒体がある。藤原研究室ではそれに関する符号の研究も行っている。先に述べたメモリは半導体をベースとした回路で構成されているが、ホログラフィックメモリは光技術を基盤としている。読み出し専用のCDやDVDは細かい溝の刻まれたディスクにレーザーを当て、その反射によって二次元画像や音声などを再生するのだが、ホログラフィックメモリの記録媒体であるホログラムは元々三次元の立体画像を記録、再生するための媒体である。立体画像を再生可能にするために、レーザーを使って元の物体の放つ光の強度、位相といった莫大な情報を高密度にホログラムに記録している。この技術を三次元画像に留ま

らず汎用的な情報の記録に使えないか、との考えのもとでホログラフィックメモリの開発は進められている。情報の記録に使う場合、三次元画像ではなく２進数の情報を平面上に並べて大量に記録していく。その記録容量は、名刺大の大きさに約100GB、映画が約20本分記録できる程である。

ホログラフィックメモリに関しても種々のタイプのエラーが発生する。しかし、半導体メモリと比べるとそのエラーの発生の仕方はやや特殊である。通常、エラーはどんな場所でも等確率で発生するとされている。しかし、ホログラフィックメモリは記録に用いている光の特性上、二次元平面となっている記録面の端の部分に記録ひずみが生じてしまい、そこでエラーが発生することが多いのだ。だが記録面の中央付近はそれほどエラーは発生しない。そのため、端の部分のエラーを主に訂正できる符号だと非常に効率が良い。藤原研究室ではこのような条件に適合するホログラフィックメモリ用の符号の設計を進め、すでに開発している。現在一般に普及している音楽CDもそうだったのだが、符号技術が適用され信頼性が保証されて初めて製品として世の中に登場できる。大容量のホログラフィックメモリが我々の身近に登場する日もそう遠くないかもしれない。

もう一つ、現在研究中の面白い符号を紹介しよう。パソコンのキーボードを打っているとき、間違えて別のキーを打ってしまった経験は多くの人にあるのではないだろうか。間違えたキーによって入力されたデータ、これもエラーの一種だと考えることができる。このエラーも先に述べたホログラフィックメモリの場合と同様に、起こる確率に差異がある。Aを打とうとして隣接するSと間違えることはあっても位置の離れたPと打ち間違えることはまずないと考えて良いだろう。打ちたいキーが何かによって、そのとき発生するエラーの種類が異なるのだ。従って特殊な符号を考えなければならない。藤原研究室ではこのような符号に関しても研究を進めている。

01 理論家よりむしろエンジニアとして

符号理論研究者の多くは、符号理論の名の通り理論を主眼に置いて研究している。従って、理論を実際に電気回路で実現したり、経済性まで考慮したりすることは通常ない。符号としての理論限界を追求していく研究者が多いのだ。しかし藤原先生は、理論研究のみならず現実に応用できるための符号設計論に大いに力を注いでいる。先生は符号の設計および開発の研究に関して藤原研究室は世界一であると自負しており、実際先生の研究室から誕生した符号の多くは企業によって採用され、実用化されている。

このような研究成果は、先生の研究スタンスによるところが大きい。先生の研究の出発点は現実の要求に耳を傾けることである。そして現実の条件、誤りの特性、適用する対象を十分勘案して、それに最も適合し経済的にも最も優れた符号を設計・開発していく。元々企業で研究をしていたという先生の経験が活かされているのだろう。「ただ単に発明や発見だけが研究ではなくて、使える形を重視して設計開発する、あるいはすばらしい理論を使える形に変えてやることも立派な研究です」自らを純粋な理論家ではなくエンジニアと称する先生のポリシーがこの言葉に滲み出ている。

研究室では先生と学生が一丸となって社会からのニーズに応じた符号の開発に取り組んでいる。企業と共同研究をしたり、企業から依頼を受けることも多いという。学生が開発した符号でも、性能が良ければ企業はすぐに採用して使ってくれるため、学生にとって大変やりがいがあるそうである。先生にとっても学生の研究から学ぶことも多いそうだ。このような気風が藤原研究室の業績の一因となっているのだろう。今後の活躍に大いに期待できそうである。

現実に役に立つように。信念を持って研究に取り組む藤原先生はこれからも多くの業績を生み出していくだろう。最後になりましたが、たびたびの取材に快く応じて下さった藤原先生に心よりお礼申し上げます。ありがとうございました。

（伊藤　晃）