1999（第15回）日本国際賞受賞者
1999 (15th) Japan Prize Laureate

ウェスリィ・ピーターソン博士（アメリカ合衆国）
ハワイ大学マノア校情報科学部教授
1924年生まれ

Dr. W. Wesley Peterson (United States of America)
Professor of Information and Computer Sciences, University of Hawaii at Manoa, Nationality United States of America
Born in 1924.

誤り検出・訂正における数学

ウェスリィ・ピーターソン

本講演では、誤り検出・訂正における問題解決に数学がどのように使われるかをお話したい。

誤り検出の実用に際し用いられた最初の着想はパリティチェックであった。データはすべて2進表現され、1と0で表されているとする。7ビットで構成されるメッセージ M を $M=(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ と表す。ただし、各成分 a_i は1か0である。ここで、M に含まれる1の数が偶数であるとき、M のパリティは偶数である（または M は偶数パリティである）と言い、1の数が奇数であるときは、M のパリティは奇数である（または M は奇数パリティである）という。送信側で偶数パリティのメッセージだけを送信し、受信側では、受信メッセージのパリティを検査することにすれば、メッセージの中に単一の誤りが発生した場合、パリティが奇数になるため、この誤りを検出することができる。

以下の説明では、算術演算において法を2とする演算を仮定する。すなわち、2は0に等しいと考えるのである。代数の通常の規則が、法を2とする代数でも成立し、代数で学んだ多くの考え方が適用できる。さて、$M=(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ とすると、$a_6+a_5+a_4+a_3+a_2+a_1+a_0$ の値は、M が偶数パリティのときに0となり、奇数パリティのとき1となる。

ここで、再び $M=(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ と仮定し、a_6, a_5, a_4, a_3 を情報とし、a_2, a_1, a_0 は、それぞれ、次の式 (2) (1) (0) に現れる記号の部分集合に関するパリティチェックとする。

(2) $a_2 = a_6 + a_5 + a_4$, すなわち $a_6 + a_5 + a_4 + a_2 = 0$
(1) $a_1 = a_5 + a_4 + a_3$, すなわち $a_5 + a_4 + a_3 + a_1 = 0$
(0) $a_0 = a_6 + a_5 + a_3$, すなわち $a_6 + a_5 + a_3 + a_0 = 0$

このような a_2, a_1, a_0 をチェックビットと呼ぶ。

ここで、見方を変えてみよう。これらの式において変数 a_i が式 j に含まれているとき、列(i)、行(j)の成分が1となる次のような行列を考える。

行\列	(6)	(5)	(4)	(3)	(2)	(1)	(0)
(2)	1	1	1	0	1	0	0
(1)	0	1	1	1	0	1	0
(0)	1	1	0	1	0	0	1

ここで、M=(1010011) とする。このとき、パリティチェック(2)は次式のように計算できる。

(M)	1	0	1	0	0	1	1
(2)	×1	×1	×1	×0	×1	×0	×0
	1	+0	+1	+0	+0	+0	+0 =0

この M は、(2) (1) (0) の三つの式すべてについてパリティチェックが0になる。このようなメ

ッセージが送信すべきメッセージである。いま、このメッセージが送信され、誤りが一つ発生して次式の M が受信されたとする。

M=(1000011)

この M について三つのパリティチェックを計算したとすると、次の結果が得られる。

パリティチェック（2） 1
パリティチェック（1） 1
パリティチェック（0） 0

単一誤りが生じたと仮定すると、誤りのある記号は式（2）および式（1）には含まれ、式（0）には含まれない。上の行列をみると、このパリティチェックは列(4)と一致することがわかる。変数 a_4 は式（2）と式（1）に含まれるが、式（0）には含まれない。これにより、誤りは変数 a_4 に生じたということになる。

上に示した行列のすべての列は異なっているので、それぞれの単一誤りに対し、パリティチェックを計算した結果は異なったパターンとなる。従って、この符号によって（チェックビットの誤りも含め）すべての単一誤りを訂正できる。この符号は、リチャード・ハミングにより見出されたものを少し変形したものである。

上に示した1、0を要素とする3行7列の行列を用いてメッセージ M のパリティチェックを計算する方法は、数学でよく知られている行列の乗算に他ならない。このことから、行列に関する膨大な数学理論が、符号の研究に応用でき、その理論的な枠組みとして有用となるのである。

メッセージ $M=(a_6, a_5, a_4, a_3, a_2, a_1, a_0)$ に対応して、次のような多項式を考えよう。

$$A(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$$

ある種の符号では、A(x)が特定の多項式 P(x)で割り切れるという条件と、パリティチェックが満たされる（パリティチェックがすべて0になる）という条件とが同等となるように記号を配列することができる。上の符号の例では、A(x)が $P(x)=x^3+x+1$ で割り切れるとき、またそのときに限って、パリティチェックが満たされるように記号を配列してある。このため、受信メッセージを $P(x)$ で割った剰余多項式の係数が、前述のようにして計算したパリティチェックと正確に一致する。

このようにして、誤り検出と訂正の理論に、多項式が導入され、それに伴って、多項式の因子分解、多項式の根の計算手法なども利用されるようになった。これらの概念は、誤り検出と訂正の理論に大きな進歩をもたらしたのである。

このような符号を用いると、誤り検出は非常に簡単になる。まず、多項式 $P(x)$ を選ぶ。送信側では、多項式で表したとき $P(x)$ で割り切れるようなメッセージを送る。受信側では、受信メッセージを $P(x)$ で割った剰余が0でないなら、誤りが生じたと判定する。P(x)による割り算と剰余の計算は極めて簡単である。これに要する回路は簡単なフィードバック・シフトレジスタである。これが、CRC（巡回冗長検査）として知られている誤り検出方式の基礎であり、その簡単さと強力な誤り検出能力とから、現在でも極めて広範に利用されている。特に、イーサネットやディスケットにはすべてこの方法が用いられている。

以上により、誤り検出や訂正に対する数学の利用の仕方について何かを理解して頂けたのではないかと思う。私は、現在でも代数学を学んでおり、数学がこれまでに果たしてきた幾多の事績に改めて深い感銘を受けている次第である。