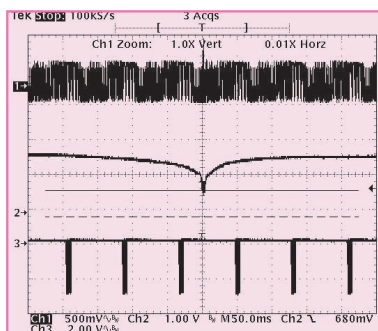




特定小電力無線モデムで使われる
誤り訂正のしくみと効能の実際

8ビット・マイコンによる 誤り訂正の処理速度

山辺 常広

Tsunehiro Yamabe

はじめに

組み込み用の小型モジュールでは、データ通信に伴う誤り訂正を行うハードウェアとして、一般的にはASICやFPGAを使うことが多いと思います。しかし、特定小電力無線モデムのように、伝送速度が1200～9600 bpsと比較的低速度の場合は、ソフトウェアによる処理でも賄える可能性があります。

本稿では一般的によく使用される8ビット・マイコン(NECの78K0/KE2シリーズ)を使用し、実際にソフトウェアを試作し、その処理速度がどの程度になるのか調べた結果をご紹介します。

ソフトウェアによる誤り訂正

現在よく使用されている代表的な誤り訂正符号には、バースト誤り訂正符号とランダム誤り訂正符号があります。前者としてはブロック符号である「リード・ソロモン符号」、後者としては畳み込み符号である「畳み込み符号」や「ビタビ復号」がよく使われています。

リード・ソロモン符号はCDやDVD、QRコードなどに、畳み込み符号/ビタビ復号はCDMAやGSMの携帯電話等に使われています。また、地上デジタル放送では外符号としてリード・ソロモン符号、内符号として畳み込み符号/ビタビ復号が使われています。

訂正符号の種類の詳細は、ここでは述べません。本誌No.2の「第5章 誤り訂正と信号処理」などをご参照ください。ここではリード・ソロモン符号と畳み込み符号/ビタビ復号のソフトウェア処理を試み、最後にその処理速度の比較を行います。

リード・ソロモン符号

リード・ソロモン符号(Reed-Solomon coding)は1960年にアービング・S・リード(Irving S. Reed)とギュスタブ・ソロモン(Gustave Solomon)によって開発された、符号語がガロア体(有限体)で構成された

BCH符号の一種です。開発当初は1誤りの復号のみでしたが、後にバーレカンブ復号法、ユークリッド復号法等の複数誤り訂正が可能な復号方法が開発されました。

ガロア体とは

これは19世紀にエバリスト・ガロアによって考案されました。リード・ソロモン符号の演算は、ガロア体(有限体)上で行われます。一般の整数が無数の集合からできているのに対し、ガロア体は整数を素数で割った余りの集合からできています。

リード・ソロモン符号では、符号語のシンボルがガロア体の元に対応します。8ビットが1シンボルのとき、ガロア体の元に対するシンボル・パターンは256個あることになります。2ⁿ個のシンボルを持つ体は、2ⁿのガロア拡大体と呼び、GF(2ⁿ)で表します。一般的にはGF(2⁸)が使用されます。表1に2進法での加算と乗算の例を示します。

リード・ソロモン符号ではGF(2)上の原始多項式(多項式の世界で素数に当たるもの)を使用して、演算を進めていきます。

送信側リード・ソロモン符号器の構成

● 生成多項式を求める

リード・ソロモン符号器を構成するために、まず生成多項式を求めます。

生成多項式 $g_j(x)$ は、

$$\begin{aligned} g_1(x) &= (x+1)(x+a) \\ &= x^2 + (a+1)x + a \\ &= x^2 + a^{25} + a \end{aligned}$$

です。これから1誤り訂正は、

$$g_2(x) = (x+1)(x+a)(x+a^2)$$

〈表1〉2進法での加算と乗算の例 [GF(2)]

	0	1
0	0	1
1	1	0

(a) 2進法での加算の例

	0	1
0	0	0
1	0	1

(b) 2進法での乗算の例

	データ部 (32バイト)	パリティ (余り) 部
1誤り訂正 (RS35, 32)	$D_0, D_1, D_2, \dots, D_{31}$	R_2, R_1, R_0
4誤り訂正 (RS40, 32)	$D_0, D_1, D_2, \dots, D_{31}$	$R_7, R_6, R_5, \dots, R_0$
8誤り訂正 (RS48, 32)	$D_0, D_1, D_2, \dots, D_{31}$	$R_{15}, R_{14}, R_{13}, \dots, R_0$

〈図1〉送信データの構成 (短縮リード・ソロモン符号)

$$\begin{aligned}
 &= g_1(x)(x+a^2) \\
 &= (x^2+a^{25}x+a)(x+a^2) \\
 &= x^3+(a^{25}+a^2)x^2+(a^{27}+a)x+a^3 \\
 &= x^3+a^{198}x^2+a^{199}x+a^3
 \end{aligned}$$

と表せます。同様に2誤り訂正は、

$$\begin{aligned}
 g_3(x) &= (x+1)(x+a)(x+a^2)(x+a^3) \\
 &= g_2(x)(x+a^3) \\
 &= (x^3+a^{198}x^2+a^{199}x+a^3)(x+a^3) \\
 &= x^4+(a^{198}+a^3)x^3+(a^{201}+a^{199})x^2 \\
 &\quad +(a^{202}+a^3)x+a^6 \\
 &= x^4+a^{75}x^3+a^{249}x^2+a^{78}x+a^6
 \end{aligned}$$

と表せます。上記と同様な計算で $g_4(x)$, $g_5(x)$, $g_6(x)$, …と順に求めていきます。以下に4誤り, 8誤り訂正の生成多項式の例を示します。

▶ 4誤り訂正

$$\begin{aligned}
 g_7(x) &= (x+1)(x+a)(x+a^2)(x+a^3)(x+a^4) \\
 &\quad (x+a^5)(x+a^6)(x+a^7) \\
 &= x^8+a^{175}x^7+a^{238}x^6+a^{208}x^5+a^{249}x^4 \\
 &\quad +a^{215}x^3+a^{252}x^2+a^{196}x+a^{28}
 \end{aligned}$$

▶ 8誤り訂正

$$\begin{aligned}
 g_{15}(x) &= (x+1)(x+a)(x+a^2)(x+a^3)(x+a^4) \\
 &\quad (x+a^5)(x+a^6)(x+a^7)(x+a^8)(x+a^9) \\
 &\quad (x+a^{10})(x+a^{11})(x+a^{12})(x+a^{13}) \\
 &\quad (x+a^{14})(x+a^{15}) \\
 &= x^{16}+a^{120}x^{15}+a^{104}x^{14}+a^{107}x^{13}+a^{109}x^{12} \\
 &\quad +a^{102}x^{11}+a^{161}x^{10}+a^{76}x^9+a^3x^8+a^{91}x^7 \\
 &\quad +a^{191}x^6+a^{147}x^5+a^{169}x^4+a^{182}x^3+a^{194}x^2 \\
 &\quad +a^{225}x+a^{120}
 \end{aligned}$$

● 送信データのパリティ (余り) を求める

生成多項式が求まったら、この式を使用して送信データのパリティ (余り) を求めます。前提となる送信データ構成図を図1に示します。ここで送るデータは1誤り, 4誤り, 8誤り共通で32バイトとします。これに続いて誤り訂正用のパリティ (余り) が1誤りで3バイト, 4誤りで8バイト, 8誤りで16バイト付加されます。実際の送信データ・フォーマットでは、これ以外に同期コード, 識別コード, CRCコードなどが付加されます。

ここでは1誤り訂正について説明します。図2は1誤り訂正のパリティ (余り) を求めるための概念図です。

これは送信データ $M(x)$ から1バイトごとに1誤り用多項式を使用してパリティ (余り) R_2, R_1, R_0 を計算する流れを示しています。計算順序は次の通りです。

① R_0, R_1, R_2 を0に初期化する。

② $\{M(x) + R_2\} a^{198} + R_1 \rightarrow R_2$

③ $\{M(x) + R_2\} a^{199} + R_0 \rightarrow R_1$

④ $\{M(x) + R_2\} a^3 \rightarrow R_0$

⑤ 送信データ $M(x)$ の代入値を D_0, D_1 と順に D_{31} まです32回にわたり、②, ③, ④の工程を繰り返す。これでパリティ (余り) 計算は終了し、 R_2, R_1, R_0 の値が確定します。以上はすべてガロア体上の計算になります。プログラム上では、演算を高速かつ容易にするためにあらかじめ0~255の数値に対する a^{198}, a^{199}, a^3 等の剰余計算結果をテーブルにしておき、演算はテーブルを引くことで行います。

■ 受信側リード・ソロモン復号器の構成

● シンドローム計算式

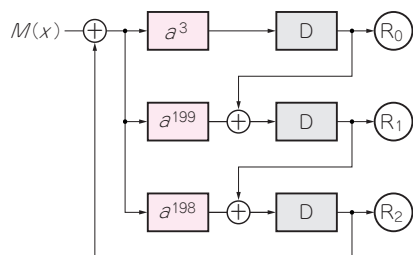
受信側のリード・ソロモン復号器を構成するために必要なシンドローム計算式 (コラム参照) は、送信側リード・ソロモン符号器に使用した展開する前の式を使用します。以下に1, 4, 8誤り訂正のシンドローム計算式を示します。

▶ 1誤り訂正

$$g_2(x) = (x+1)(x+a)(x+a^2)$$

▶ 4誤り訂正

$$\begin{aligned}
 g_7(x) &= (x+1)(x+a)(x+a^2)(x+a^3)(x+a^4) \\
 &\quad (x+a^5)(x+a^6)(x+a^7)
 \end{aligned}$$



〈図2〉送信側で1誤り訂正のパリティ (余り) を求めるための概念図