3H-04

Reed-Solomon符号を用いた修正積符号による不均一誤り訂正符号の構成

高橋　悠† 西島利尚†

法政大学情報科学部†

1. はじめに

通信路上に生じる様々な雑音からディジタル情報を保護する技術に誤り訂正・検出技術がある．特に音声データは，通信路で生じる雑音に影響を受けやすい情報とそうでない情報が混在している[4]．このようなデータに対して，符号語の位置によって誤り訂正可能な個数が異なる不均一誤り訂正技術を適用する．本論文では，音声符号化方式に組み込むことを視野に入れ，3 レベルの不均一誤り訂正符号を提案する．提案手法と積符号の違いを訂正能力の比較により示し，例を挙げて実際の符号化の流れや仕組みを示す．

2. Reed-Solomon(RS)符号

(n,k,d)Reed-Solomon(RS)符号cを以下に示す生成多項式と生成行列により定義する．

2.1. 生成多項式

定義 1:$GF(2^m)$上の(n,k,d)RS 符号cの生成多項式$g(x)$は

$$g(x)=(x-\alpha^l)(x-\alpha^{l+1})\dots(x-\alpha^{l+d-2})$$
$$=g_{n-k-1}x^{n-k-1}+g_{n-k-2}x^{n-k-2}+\cdots+g_0 \quad (1)$$

で与えられる．ここで，αは$GF(2^m)$上の原始元とし，$m\geq 3$の整数，$l\geq 0$の整数，$d=n-k+1$, $n=2^m-1$, $g_i\in GF(2^m)(i=0,1,\dots,n-k-1)$とする[1][2]．

2.2. 生成行列

定義 2: Gを RS 符号cの生成行列とする．そのとき$g(x)$の各係数を用いて，

$$G=\begin{bmatrix} g_{r-1} & g_{r-2} & \cdots & g_0 & 0 & 0 & \cdots & 0 \\ 0 & g_{r-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 0 & g_{r-1} & g_{r-2} & \cdots & g_0 \end{bmatrix} \quad (2)$$

と表すことができる．ここで，$r=n-k$とする．

2.3. 積符号

式(2)の生成行列で生成される$GF(2^m)$上の 2 つの RS 符号によって構成される積符号c_Pを以下に定義する．

定義 3: 第 1 段の符号を$GF(2^m)$上の(n_1,k_1,d_1)RS 符号c_1，第 2 段の符号を$GF(2^m)$上の (n_2,k_2,d_2)RS 符号c_2とする．そのとき，(n_P,k_P,d_P)積符号c_Pは

$$c_P=c_1\otimes c_2 \quad (3)$$

と定義される．ここで⊗はテンソル積を表す[2]．

2.4. 修正積符号

kとdが変化する$GF(2^m)$上の 2 つの RS 符号によって構成される修正積符号c_Mを定義する．ただし，ここでnは符号長，kは情報記号数，dは最小距離を表す．

定義 4: 第 1 段の(n_1,k_1,d_1)符号c_1が，k_1個の部分符号$c_1=c_1^{(1)}\supseteq c_1^{(2)}\supseteq\cdots\supseteq c_1^{(i)}\supseteq\cdots\supseteq c_1^{(k_1)}$をもつ非組織符号で与えられ，第 2 段の符号が，$k_1$個の$(n_2,k_2^{(i)},d_2^{(i)})$符号$c_2^{(i)}$，$k_2^{(1)}\leq k_2^{(2)}\leq\cdots\leq k_2^{(k_1)}$，$i=1,2,\dots,k_1$，で与えられる (n_M,k_M,d_M)積符号c_Mである[5]．

3. 提案手法

J個のレベルの訂正能力を有する$GF(2^m)$上の RS 符号を用いた修正積符号による$(n_U,k_U^{(j)},d_U^{(j)})$不均一誤り訂正符号を提案する．

3.1. 不均一誤り訂正符号

不均一誤り訂正符号とは，情報源符号化から生成される各シンボルに対し，それぞれ異なる訂正能力を割り付ける符号である[6]．

3.2. 提案手法の構成

第 1 段の(n_1,k_1,d_1)符号c_1が，j個の部分符号$c_1=c_1^{(1)}\supseteq c_1^{(2)}\supseteq\cdots\supseteq c_1^{(j)}$をもつ非組織符号で与えられ，第 2 段の符号が，$j$個の$(n_2,k_2,d_2)$符号$c_2$の符号語を与える．部分符号$c_1^{(1)},c_1^{(2)},\dots,c_1^{(j)}$の生成多項式をそれぞれ

$$g_1^{(1)}(x)=g_{n_1-j}^{(1)}x^{n_1-j}+g_{n_1-j-1}^{(1)}x^{n_1-j-1}+\cdots+g_0 \quad (4)$$
$$g_1^{(2)}(x)=g_{n_1-j+1}^{(2)}x^{n_1-j+1}+g_{n_1-j}^{(2)}x^{n_1-j}+\cdots+g_0 \quad (5)$$
$$\vdots$$
$$g_1^{(j)}(x)=g_{n_1-1}^{(j)}x^{n_1-1}+g_{n_1-2}^{(j)}x^{n_1-2}+\cdots+g_0 \quad (6)$$

とし，$k_1\times n_1$行列の生成行列G_1を

$$G_1=\begin{bmatrix} g_{n_1-j}^{(1)} & g_{n_1-j-1}^{(1)} & \cdots & g_0^{(1)} & 0 & 0 \\ g_{n_1-j+1}^{(2)} & g_{n_1-j}^{(2)} & \cdots & g_1^{(2)} & g_0^{(2)} & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ g_{n_1-1}^{(j)} & g_{n_1-2}^{(j)} & \cdots & g_2^{(j)} & g_1^{(j)} & g_0^{(j)} \end{bmatrix} \quad (7)$$

とする．そのとき，$(n_U,k_U^{(j)},d_U^{(j)})$不均一誤り訂正符号は以下を満たす．

$$n_U=n_2\times n_1 \quad (8)$$
$$k_U^{(j)}=k_2\times(k_1-j+1) \quad (9)$$
$$d_U^{(j)}=d_2\times(d_1+j-1) \quad (10)$$

Construction of Unequal Error Protection Codes by Using Modified Product Codes Based on Reed-Solomon Codes

†Haruka Takahashi, Toshihisa Nisijima

†Faculty of Computer and Information Science, Hosei University Tokyo, Koganei-shi, 3-7-2 Kajino-chou

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.

3.3. 構成例

実用的には，例えば，音声符号化において 3 レベルの異なる訂正能力を持つ誤り訂正符号を各々に割り付ける[3][4]．以下本論文では， 3 レベルの不均一誤り訂正符号の構成例である$GF(2^3)$上の符号語例について述べる．

$GF(2^3)$の原始元αの最小多項式をx^3+x+1とする．第 1 段の符号c_1を(7,3,5)RS 符号とし，部分符号$c_1^{(1)},c_1^{(2)},c_1^{(3)}$をそれぞれ(7,3,5)RS 符号，(7,2,6)RS 符号，(7,1,7)RS 符号とする．部分符号$c_1^{(1)},c_1^{(2)},c_1^{(3)}$の生成多項式$g_1^{(1)}(x),g_1^{(2)}(x),g_1^{(3)}(x)$を以下のように定める．

$$\begin{aligned} g_1^{(1)}(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\ &= x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3 \end{aligned} \tag{11}$$

$$\begin{aligned} g_1^{(2)}(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3) \\ &\qquad (x-\alpha^4)(x-\alpha^5) \\ &= x^5+\alpha^2x^4+\alpha^3x^3+\alpha^6x^2+\alpha^4x+\alpha \end{aligned} \tag{12}$$

$$\begin{aligned} g_1^{(3)}(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\ &\qquad (x-\alpha^5)(x-\alpha^6) \\ &= x^6+x^5+x^4+x^3+x^2+x+1 \end{aligned} \tag{13}$$

これらを行列表現にした生成行列G_1を

$$G_1=\begin{bmatrix} 1 & \alpha^3 & 1 & \alpha & \alpha^3 & 0 & 0 \\ 1 & \alpha^2 & \alpha^3 & \alpha^6 & \alpha^4 & \alpha & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{14}$$

とする．第 2 段の符号c_2を(7,3,5)RS 符号とする．第 2 段の符号c_2の生成多項式$g_2(x)$は

$$\begin{aligned} g_2(x) &= (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) \\ &= x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3 \end{aligned} \tag{15}$$

である．

まず初めに，1001000001100011001111101011 という情報ビット系列が与えられたとする．これをシンボル系列で表すと$\alpha^2\alpha^20\alpha^41\alpha^2\alpha^5\alpha^6\alpha^3$となる．この情報シンボル系列を図 1 のように配置する．次に$g_2(x)$を用いて各列を組織符号化する(図 2)．

α^2	α^4	α^5
α^2	1	α^6
0	α^2	α^3

図 1　情報シンボル系列

α^2	α^4	α^5
α^2	1	α^6
0	α^2	α^3
α^3	1	α^3
0	α^3	1
α^5	α^2	α^6
α^3	α^4	1

図 2　符号化c_2

その次にG_1を用いて各行を符号化し，$(49,k_U^{(j)},d_U^{(j)})$RS 符号を得る(図 3)．

α^6	α^6	α	α^5	α	0	α^5
0	α^4	α	α^3	α^2	α^5	α^6
α^5	α^6	α^2	1	α^4	0	α^3
1	α	α^3	0	0	1	α^3
α	α^4	α^2	α^6	0	α^5	1
α^4	1	α^6	α	α	α^4	α^6
α^2	1	α^3	α^2	α^4	α^4	1

図 3　符号化c_1

このときの$k_U^{(j)}$と$d_U^{(j)}$は以下の通りである．

$$j=1\text{のとき}\begin{cases} k_U^{(1)}=3\times3=9 \\ d_U^{(1)}=5\times5=25 \end{cases} \tag{16}$$

$$j=2\text{のとき}\begin{cases} k_U^{(2)}=3\times2=6 \\ d_U^{(1)}=5\times6=30 \end{cases} \tag{17}$$

$$j=3\text{のとき}\begin{cases} k_U^{(3)}=3\times1=3 \\ d_U^{(3)}=5\times7=35 \end{cases} \tag{18}$$

4. 考察

(49,9,25)積符号と構成例に示した$(49,k_U^{(j)},d_U^{(j)})$符号を比較する．両符号で用いられる RS 符号は，MDS 符号ゆえ部分符号が組織的に作れる．積符号の最小距離は 25 と定まっているが，提案手法は 25，30，35 と最小距離が 3 レベルに変わる．レベルが増えるごとに誤り訂正能力が上がることがわかる．また実用的には，各符号を 2 元に展開したときの符号パラメータが重要である．積符号は(147,27,75)，提案手法はレベル$j=1$のとき(147,27,75)，$j=2$のとき(147,18,90)，$j=3$のとき(147,9,105)となる．よって，RS 符号パラメータn,k,d,lの値によって 2 元の符号パラメータは変化する[7]．したがって，最適なパラメータを選択する必要がある．

5. 課題

本論文では音声符号化方式への組み合わせを視野に入れ，3 レベルを有する最も簡単な$GF(2^3)$上の RS 符号を用いた符号例を示した．今後の課題として，より大きなガロア体上で符号を構成すれば，より実用的で強力な符号化が可能である．同時に復号にかかる計算量を考慮した実用化へ向けての研究も重要である．

文献

[1] 先名健一，例題で学ぶ符号理論入門，森北出版株式会社，東京，2011.

[2] 平澤茂一，西島利尚，符号理論入門，培風館，東京，1999.

[3] 森岳至，金子孝夫，岩上直樹，守谷健弘，池田和永，“IMT-2000 用 TwinVQ リアルタイム音楽 配信システムの構築”，電子情報通信学会論文誌，Vol. J83-D-II No. 11，pp. 2215-537，2000.

[4] 守谷健弘，音声符号化，電子情報通信学会，1998.

[5] S. Hirasawa, M. Kasahara, Y. Sugiyama, and T. Namekawa, “Modified Product Codes,” IEEE Transactions on Information Theory, VOL. IT-30, NO. 2, pp. 299-306, 1984.

[6] S. Hirasawa and M. Kasahara, “Coding and decoding schemes with unequal symbol Reliability,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, Vol. E73-E No. 7 pp. 1176-1180, 1990.

[7] 臼木夏織，$GF(2^4)$上の Reed-Solomon 符号の 2 元重み分布多項式，2016 年度法政大学情報科学部卒業論文，2017.

Copyright ©2017 Information Processing Society of Japan.
All Rights Reserved.