数理解析研究所講究録
第211巻 1974年 25-39

Goppaの符号に関する考察

三菱電機通信機製作所　杉山　康夫
大阪大学　工学部　　笠原　正雄
三菱電機通信機製作所　平沢　茨一
大阪大学　工学部　　滑川　敏彦

§1.　まえがき

V. D. Goppaによって発見されたGoppa符号[(1),(2),(3)]はBCH符号およびSrivastava符号をサブクラスとして含む広い範囲の線形誤り訂正符号である。Goppa符号の能力は、少くともBCH符号の能力の下界式を満足している。さらにGoppa符号の顕著な性質として、符号長が十分長いとき既約多項式をGoppa多項式としてもつGoppa符号のほとんどすべてがVarsharmov-Gilbert下界式を満足することが挙げられる。Goppa符号の代数的復号化の方法は、BCH符号の復号化と同様に考えることができる。しかしながら、シンドローム多項式を与えて誤り位置多項式（Error Locator Polynomial）および誤り数値多項式（Error Evaluator Polynomial）を求めるときに、BCH符号の場合よりもより一般的な解法が要求される。（E.R. Berlekampはこれらの多項式の間に

なりたつ式をKey Equationと呼んでいる[4]。)したがって、この解法としてBCH符号の復号化のためのBerlekamp[5]-Massey[6]のアルゴリズムをそのまゝ適用することは、かなり困難と思われる。Goppaはその解法としてPetersonのアルゴリズムを使っているが、このアルゴリズムは計算時間が長くなる欠点をもっている。筆者らは、Euclidの互除法を利用することによってGoppa符号のKey Equationを解くアルゴリズムを見い出した[7]。このアルゴリズムはGoppa符号の特殊な場合であるBCH符号の復号化に限定したときですらBerlekamp-Masseyのアルゴリズムの数倍の計算時間であり、一般性に富むだけ優れたものと思われる。

本論文においては、Goppa符号の解説を兼ねてGoppa符号を特徴づけるGoppa多項式の根の性質によって符号の分類をおこない、Goppa符号とBCH符号、Srivastava符号との関連を明らかにする。次に、GF(q)上のSrivastava符号がGoppa多項式の次数だけLengthenできることを示す。さらに、GF(2)上のGoppa符号の場合に、代数的復号化のためのKey Equationを解くためのEuclidの互除法を使ったアルゴリズムを修正して、より計算時間を短縮したアルゴリズムを述べる。

§2. Goppa符号

2.1 Goppa符号の定義

Goppa符号を定義しよう。qを素数のべき、mを正の整数、$g(z)$を$GF(q^m)$上の係数をもつ次数t_0の多項式、Lを$GF(q^m)$から$g(z)$の根を除いた集合の部分集合、nをLの元の個数、α_k $(k=1,2,\cdots\cdots,n)$をLの中の相異なる元、β_kを$GF(q^m)$の非零の元、a_kを$GF(q)$の元とする。ベクトル$a=(a_1,a_2,\cdots\cdots,a_n)$に対して

$$(a_1,a_2,\cdots\cdots,a_n)\longrightarrow\sum_{k=1}^{n}\frac{a_k\beta_k}{z-\alpha_k}$$

なる写像をおこない、$GF(q^m)$上の有理式へ写す。この写像は$GF(q)$上の次元nのベクトル空間の$GF(q^m)$上の有理式の加法群への準同型対応である。このとき

$$(1)\quad \sum_{k=1}^{n}\frac{a_k\beta_k}{z-\alpha_k}\equiv 0 \qquad \mathrm{mod}\ g(z)$$

を満足する符号ベクトルaの集合AをGoppa符号と定義する。

こゝで、$a_k \neq 0$であるkの集合をKとする。そのとき

$$(2)\quad \eta_a(z)=\sum_{k\in K}a_k\beta_k\prod_{k'\in K,\,k'\neq k}(z-\alpha_{k'}),\quad \sigma_a(z)=\prod_{k\in K}(z-\alpha_k)$$

なる多項式を定義する。$\eta_a(z)$と$\sigma_a(z)$は互いに素である。これらの多項式を式(1)に代入すれば、

$$\frac{\eta_a(z)}{\sigma_a(z)}\equiv 0 \qquad \mathrm{mod}\ g(z)$$

を得る。すなわち、$g(z)$が$\eta_a(z)$を割り切るとき、ベクト

ルaはGoppa符号の符号語である。さらに、

$$(3)\quad \sum_{k=1}^{n} -a_k\beta_k \frac{g(z)-g(\alpha_k)}{z-\alpha_k} g^{-1}(\alpha_k) = 0$$

を満足するベクトルaの集合として、Goppa符号を定義することができる。この式(3)より検査行列を求めることができ、その検査行列はH.J.Helgert[(8)]が定義した一般化されたBCH符号の検査行列の特殊な場合と考えることができる。

[定理1(Goppa)]　Goppa符号の検査記号数はたかだかmt_0であり、最小符号間距離は少くともt_0+1ある。

2.2　Goppa多項式による符号の分類

Goppa符号の特長の一つは、$g(z)$が$GF(q^m)$上の次数t_0の任意の多項式であることである。この多項式$g(z)$を、Goppa多項式と呼ぶ。Goppa多項式$g(z)$の根z_j($j=1, 2, \cdots, t_0$)の性質に着目するとき、表1に示されたように符号を分類することができる。この表から、BCH符号およびSrivastava符号がどのように位置づけされるかが明らかとなる。符号長が十分長いときにほとんどすべてのGoppa符号がVarsharmov-Gilbert下界式を満足するという性質は、Goppa多項式$g(z)$が既約多項式である場合において導かれている。すべての根が同一である場合において、$g(z)=(z-z_0)^{t_0}$, ($z_0 \neq 0$), であるとき$(z-z_0)$をzにおきかえる

表1　Goppa多項式 $g(z)$ の根の性質による符号の分類

	根がすべて相異なる	根がすべて同一	相異なる根と同一根が混在
既約多項式	(符号長が長い時特に良い)		
すべての根が $GF(q^m)$ の元	Srivastava符号	BCH符号	
上記の二つの場合以外			

ことによって、$g(z)=z^{t_0}$ すなわちBCH符号がこの場合を代表していると考えることができる。さらにこの場合に、$\beta_k=\alpha_k^{-m_0}$, $(m_0 \neq 0)$, と選ぶとき、Goppa符号はAlternate BCH符号[5]であるといえる。

2．3　二元Goppa符号

GF(2)上のGoppa符号を考えよう。$\beta_k=1$ とする。そのとき、式(2)の $\eta_a(z)$ は $\sigma_a(z)$ に形式的微分をほどこした多項式となる。$GF(2^m)$ の元を係数とする任意の多項式に形式的微分をほどこしたとき、微分された多項式は偶数次のみから構成される。すなわち、$\eta_a(z)$ の根の重複度は偶数回である。Goppa多項式 $g(z)$ を、すべての根が同一である場合を除いて、

$$g(z)=\prod_{j=1}^{t_2}(z-z_j)^{m_j}\quad,\quad\sum_{j=1}^{t_2}m_j=t_0$$

とする。ただし、z_j ($j=1,2,\cdots,t_2$) は相異なる根、m_j は z_j の重複度を示す。さらに、$j\le t_1$ なら m_j は奇数であるとする。このとき、$g(z)$ が偶数次のみからなる多項式 $\sigma_a'(z)$ を割り切るならば、$\sigma_a'(z)$ は $g(z)\cdot\prod_{j=1}^{t_1}(z-z_j)$ によって割り切れねばならない。したがって、次の定理がなりたつ。

[定理2]　すべての根が同一である多項式を除いた t_0 次の Goppa多項式 $g(z)$ において根の重複度が奇数であるような相異なる根の数を t_1 とする。このとき、GF(2) 上の Goppa符号の検査記号数はたかだか mt_0 であり、最小符号間距離は少くとも t_0+t_1+1 ある。

この定理より、すべての根が相異なる場合、最小符号間距離は少くとも $2t_0+1$ あることが明らかであろう。この場合が保証されている最小符号間距離としては最大となる。

　すべての根が同一である場合、Goppa符号はBCH符号となることから次の定理が得られる。

[定理3 (Goppa)]　すべての根が同一である次数 t_0 の Goppa多項式 $g(z)$ をもつ GF(2) 上の Goppa符号の検査記号数はたかだか $m[(t_0+1)/2]$ であり、最小符号間距離は少くとも t_0+1 ある。ただし、$[x]$ は x を超えない最大の整数を示す。

これら二種類の定理（定理2と定理3）と定理1との相違を明確にしておこう。次数 $t_0 = 2t$ の Goppa多項式 $g(z)$ により定義されたGF(2)上のGoppa符号において、Goppa多項式の根がすべて相異なるとき、定理1のパラメータよりも最小符号間距離が約2倍に増加しており、Goppa多項式の根がすべて同一のとき、定理1のパラメータよりも検査記号数が1/2に減少している。

2.4 "Lengthened" Srivastava 符号

GF(q)上のSrivastava符号は、先に述べたように、Goppa多項式 $g(z)$ の根がすべて相異なるGF(q^m)の元からなるGoppa符号である。$g(z)$ の次数が t_0 であるとき、Srivastava符号のパラメータは、符号長 $n \leq q^m - t_0$，検査記号数 $\leq m t_0$，最小符号間距離 $\geq t_0 + 1$ である。こゝではSrivastava符号が t_0 Lengthenできることを示す。符号長 n のSrivastava符号を t_0 Lengthenした符号は

$$(4)\quad \sum_{k=1}^{n} \frac{a_k \beta_k}{z - \alpha_k} + \sum_{k=n+1}^{n+t_0} a_k \beta_k \prod_{\substack{k'=1 \\ k' \neq n-k}}^{t_0} (z - z_{k'}) \equiv 0 \mod g(z)$$

を満足する符号ベクトル a の集合として定義される。こゝで $g(z) = \prod_{j=1}^{t_0} (z - z_j)$ であり、z_j, α_k, β_k はGF(q^m)の元である。さらに、$z_{j_1} \neq z_{j_2}$ ($j_1 \neq j_2$)，$\alpha_{k_1} \neq \alpha_{k_2}$ ($k_1 \neq k_2$)，$z_j \neq \alpha_k$，$\beta_k \neq 0$ である。式(4)の左辺の第1項

はLengthenされる前のSrivastava符号を示している。第2項がLengthenされた部分に相当している。このLengthenされた部分をみることによって、LengthenされたSrivastava符号の検査記号数はやはりたかだか mt_0 であることがわかる。次に最小符号間距離について考えよう。以下の三つの場合にわけて述べる。

(i) $a_k = 0$ $(k = 1, 2, \cdots, n)$

式(4)の左辺第1項は0であり、右辺の次数はたかだか t_0-1 であるから、この場合は符号語となりえない。

(ii) $a_k = 0$ $(k = n+1, n+2, \cdots, n+t_0)$

式(4)の左辺第2項が0となり、元のSrivastava符号に帰するので、最小符号間距離は少くとも t_0+1 ある。

(iii) 上記二つの場合以外

$k = 1, 2, \cdots, n$ の範囲で $a_k \neq 0$ となる k の集合を K_1 とし、その集合 K_1 の元の個数を d_1 とする。$k = n+1, n+2, \cdots, n+t_0$ の範囲で $a_k \neq 0$ となる k の集合 K_2 とし、その集合 K_2 の元の個数を d_2 とする。さらに、$k = n+1, n+2, \cdots, n+t_0$ なる k の集合を K_0 とする。そのとき、式(4)は

$$\frac{\sum_{k\in K_1} a_k\beta_k \prod_{\substack{k'\in K_1\\ k'\neq k}}(z-\alpha_{k'})}{\prod_{k\in K_1}(z-\alpha_k)} + \prod_{k\in K_0-K_2}(z-z_{k-n})\left\{\sum_{k\in K_2} a_k\beta_k \prod_{\substack{k'\in K_2\\ k'\neq k-n}}(z-z_{k'})\right\}$$

$\equiv 0 \quad \bmod g(z)$

とかきかえられる。$g(z)$と$\prod_{k\in K_0-K_2}(z-z_{k-n})$は共通因数として、$\prod_{k\in K_0-K_2}(z-z_{k-n})$をもつから、$\sum_{k\in K_1} a_k\beta_k \prod_{k'\in K_1,\, k'\neq k}(z-\alpha_{k'})$もまた$\prod_{k\in K_0-K_2}(z-z_{k-n})$によって割り切れねばならない。これらの多項式の次数を考えるとき、$d_1-1 \geq t_0-d_2$がなりたつ。d_1+d_2はa_k $(k=1,2,\cdots\cdots,n)$の非零のものの個数であるから、最小の重みはt_0+1ある。

以上より、Lengthenされた Srivastava 符号は、保証された最小符号間距離として、元の Srivastava 符号の保証された最小符号間距離と同一のt_0+1をもつことがわかる。

§3.　代数的復号化とGF(2)上の Key Equationの解法

3.1　代数的復号化

Goppa符号すなわち集合Aに属する符号ベクトル$\mathbf{a}$が送信され、通信路において誤りベクトル$\mathbf{e}=(e_1,e_2,\cdots\cdots,e_n)$, $(e_k\in GF(q))$,が加わるとき、受信ベクトル$\mathbf{r}$は$(r_1,r_2,\cdots\cdots,r_n)=(a_1+e_1,a_2+e_2,\cdots\cdots\cdots\cdots,a_n+e_n)$となる。このとき、シンドローム多項式$S(z)$は

(5)　$$S(z) = -\sum_{k=1}^{n} r_k\beta_k \frac{g(z)-g(\alpha_k)}{z-\alpha_k} g^{-1}(\alpha_k)$$

によって与えられる。$e_k\neq 0$であるようなkの集合をMとするとき、

$$\sigma(z)=\prod_{k\in M}(z-\alpha_k)$$

$$\eta(z)=\sum_{k\in M}e_k\prod_{k'\in M,\,k'\neq k}(z-\alpha_{k'})$$

なる多項式を定義し、$\sigma(z)$ を誤り位置多項式、$\eta(z)$ を誤り数値多項式と呼ぶ。このとき、シンドローム多項式 $S(z)$ と誤り位置多項式 $\sigma(z)$、誤り数値多項式 $\eta(z)$ との間に

$$S(z)\equiv\frac{\eta(z)}{\sigma(z)}\qquad \bmod g(z) \tag{6}$$

なる関係がなりたつ。したがって、Goppa符号の代数的復号化の方法は、BCH符号の代数的復号化と同様に、次の4ステップで構成される。

（i）受信ベクトル $\mathbf{r}$ から式(5)を使ってシンドローム多項式 $S(z)$ を求める。

（ii）シンドローム多項式 $S(z)$ から式(6)を使って誤り位置多項式 $\sigma(z)$ と誤り数値多項式 $\eta(z)$ を求める。

（iii）誤り位置多項式 $\sigma(z)$ の根を求めることによって、誤り位置 α_k（$k\in M$）を得る。

（iv）誤り位置多項式 $\sigma(z)$ の形式的微分多項式 $\sigma'(z)$ および誤り数値多項式 $\eta(z)$ に誤り位置 α_k を代入し、誤り数値 $e_k=\eta(\alpha_k)/\sigma'(\alpha_k)$ を得る。

これらのステップの中で、ステップ(ii)のシンドローム多項式を与えることによって誤り位置多項式および誤り数値多項

式を求めるための比較的簡単な手法は知られていなかった。Berlekampはこの問題をGoppa符号の復号化のためのKey Equationと呼んでいる[4]。BCH符号の復号化のためのKey Equationは $g(z)=z^{2t}$ の場合であり、この特殊な場合についてはBerlekamp[5]-Massey[6]のアルゴリズムがある。しかしながら、このアルゴリズムを一般の $g(z)$ に対して、そのまゝ適用することは困難と思われる。筆者らは、最近、このGoppa符号の復号化のためのKey Equationが、Goppa多項式とシンドローム多項式の最大公約数を求めるためのEuclidの互除法を適用することによって解けることを発見した[7]。こゝでは、GF(2)上のGoppa符号の場合についてそのアルゴリズムの若干の修正について述べる。

3．2　Goppa多項式が既約多項式のとき

Goppa多項式が次数tの既約多項式 $g(z)$ であるときGF(2)上のGoppa符号のシンドローム多項式 $S(z)$ は

$$S(z)=\sum_{k=1}^{n} r_k \frac{g^2(z)-g^2(\alpha_k)}{z-\alpha_k} g^{-2}(\alpha_k)$$

で与えられる。Key Equationは

$$(7)\qquad S(z)\equiv\frac{\sigma'(z)}{\sigma(z)}\qquad \mathrm{mod}\ g^2(z)$$

で与えられる。こゝで、$\sigma(z)$ は誤り位置多項式である。実

際に生起した誤りの個数eは$1 \leq e \leq t$であるとする。このとき、多項式を奇数次の多項式と偶数次の多項式に分解する。

$$S(z) = \tilde{S}(z) + \hat{S}(z)$$

$$\sigma(z) = \tilde{\sigma}(z) + \hat{\sigma}(z)$$

こゝで、~は奇数次、^は偶数次を意味する。なお、$\sigma'(z) = \tilde{\sigma}(z)/z$ と $g^2(z)$ は偶数次の多項式であることに注意しよう。これらの関係を式(7)に代入することによって、

$$\hat{S}(z)\ \hat{\sigma}(z) \equiv (1 + \tilde{S}(z)\ z)(\tilde{\sigma}(z)/z) \mod g^2(z)$$

$$\hat{S}(z)(\tilde{\sigma}(z)/z) \equiv (\tilde{S}(z)/z)\ \hat{\sigma}(z) \mod g^2(z)$$

なる関係を得ることができる。$g^2(z)$と$S(z)$は互いに素であるから、まず多項式$f_0(z)$

(8) $$f_0(z) \equiv 1/\hat{S}(z) \mod g^2(z)$$

を求め、次に多項式$f(z)$

(9) $$f(z) \equiv f_0(z)(\tilde{S}(z)/z) \mod g^2(z)$$

を求め、

(10) $$\hat{\sigma}(z) \equiv f(z)(\tilde{\sigma}(z)/z) \mod g^2(z)$$

に対して、Euclidの互除法を使ったアルゴリズム[7]を適用することによって、$\hat{\sigma}(z)$と$\tilde{\sigma}(z)/z$を求めれば、誤り位置多項式$\sigma(z)$を得ることができる。なお、$\hat{\sigma}(z)$と$\tilde{\sigma}(z)/z$が互いに素であること、$g^2(z)$と$f(z)$が互いに素であること、および$f(z)$の次数がt以上あることを注意してお

く。これらの式(8)，(9)，(10)の多項式はすべて偶数次の多項式であるから、z^2をzでおきかえることによって次数を半分に減らすことができる。これらの演算に要する$GF(2^m)$の元の掛算の回数は約$4t^2+2te-e^2/8$である。ちなみに、式(7)のKey Equationをそのまゝ Euclid の互除法を使ったアルゴリズムによって解けば$8te-e^2/2$である。したがって、$e \approx t$のとき若干の演算回数における改良がみられる。

3.3 Goppa多項式の根がすべて同一のとき

Goppa多項式の根がすべて同一のときすなわちBCH符号のとき、そのKey Equation

$$S(z) \equiv \frac{\sigma'(z)}{\sigma(z)} \qquad \mathrm{mod}\ z^{2t}$$

である。ただし、シンドローム多項式$S(z)$は

$$S(z) = \sum_{k=1}^{n} r_k \frac{z^{2t} - \alpha_k^{2t}}{z - \alpha_k} \ \alpha_k^{-2t}$$

で与えられる。こゝで、$S(z)$および$\sigma(z)$を奇数次と偶数次にわけることによって、

$$(11) \quad \begin{aligned} \hat{S}(z)\,\hat{\sigma}(z) &\equiv (1 + \tilde{S}(z)\,z)(\tilde{\sigma}(z)/z) && \mathrm{mod}\ z^{2t} \\ \hat{S}(z)(\tilde{\sigma}(z)/z) &\equiv (\tilde{S}(z)/z)\,\hat{\sigma}(z) && \mathrm{mod}\ z^{2t} \end{aligned}$$

なる関係を得る。このとき、$\tilde{S}(z)$と$\hat{S}(z)$の間に

(12) $$\{\hat{S}(z)\}^2 + \{\tilde{S}(z)\}^2 \equiv \tilde{S}(z)/z \qquad \mathrm{mod}\ z^{2t}$$

がなりたつ。

$$1/\{1+\tilde{S}(z)z\} \equiv \sum_{i=0}^{\infty}\{\tilde{S}(z)z\}^i \qquad \mathrm{mod}\ z^{2t}$$

であるから、式(11)および式(12)を使って、

(13) $$\left[\sum_{i=1}^{l_t-1}\{\hat{S}(z)\}^{2^i-1} z^{2^i-2}\right]\hat{\sigma}(z) \equiv \tilde{\sigma}(z)/z \qquad \mathrm{mod}\ z^{2t}$$

を得ることができる。ここで、l_t は $\log_2(t+1)$ より大きい最小の整数である。式(13)をEuclidの互除法を使ったアルゴリズムによって解けば、$\hat{\sigma}(z)$ および $\tilde{\sigma}(z)/z$ を得ることができる。これらの演算に要する $GF(2^m)$ の元の掛算の回数は約 $t^2/2+2te-e^2/8$ である。ここで、実際に生起した誤りの個数を e ($1\leq e\leq t$) とする。Burton[9]によって変形されたBCH符号の復号化のためのBerlekamp-Masseyアルゴリズムにおいては、その演算回数は約 $2te-(1/2)e^2$ である。$e\approx t$ のとき、ここで述べたアルゴリズムは、Berlekamp-Masseyアルゴリズムの約1.6倍の $GF(2^m)$ の元の掛算回数を必要とする。

§4. あとがき

Goppa符号は、未だ知られていない性質をもった興味ある符号であると思われる。本論文が今後のGoppa符号の研究に少しでも寄与すれば幸いである。

謝辞　Goppa符号の研究の必要性を示唆いただいたカリフォルニア大学のBerlekamp教授・大阪大学の嵩教授に感謝する。

参考文献

(1) V. D. Goppa : "A new class of linear error correcting codes", Probl. Peredach. Inform., Vol. 6, No. 3, p.24, Sept. '70.

(2) V. D. Goppa : "Rational representation of codes and (L, g) codes", Probl. Peredach. Inform., Vol. 7, No. 3, p.41, Sept. '71.

(3) V. D. Goppa : "Some codes constructed on the basis of (L, g) codes", Probl. Peredach. Inform., Vol. 8, No. 2, p.107, June '72.

(4) E.R. Berlekamp : "Goppa codes", IEEE Trans., Vol. IT-19, No. 5, p.590, Sept. '73.

(5) E.R. Berlekamp : "Algebraic Coding Theory", New York, McGraw-Hill, '68, p.176-240.

(6) J. L. Massey : "Shift register synthesis and BCH decoding", IEEE Trans., Vol. IT-15, No. 1, p.122, Jan. '69.

(7) 杉山・笠原・平沢・滑川 : "Goppa符号に関する二・三の考察", 電子通信学会・パターン認識と学習研究会資料 PRL73-77, Jan. '74.

(8) H. J. Helgert : "Noncyclic generalizations of BCH and Srivastava codes", Information and Control Vol. 21, p.280, '72.

(9) H. O. Burton : "Inversionless decoding of binary BCH codes", IEEE Trans., Vol. IT-17, No. 4, p.464, July '71.