■1 群（信号・システム）- 2 編（符号理論）

2 章 代数的符号

（執筆者：藤原　融）［2012 年 3 月 受領］

■概要■

1 章では，符号理論の基礎的事項について述べた．誤り訂正符号を利用するに当たっては，誤り訂正能力とともに，符号化や復号の計算複雑度が重要になる．一般に復号の計算量は，符号化のそれより大きくなるので，復号の計算量が特に重要である．もちろん，復号の計算量を重視し過ぎてもいけない．誤り訂正能力と復号計算量のバランスが重要である．

このような意味で適切な符号を設計するためには，符号に何らかの構造の導入が必要となる．本編 1-4 節で述べた線形符号も線形代数における線形空間という構造を導入しているが，更に，制約を加えることで，より簡単に設計できる．本章では，代数的構造にもとづく，代表的な符号のクラスとその復号法について述べる．

まず，巡回符号について述べる．これは，符号語が巡回置換について閉じているという制約であるが，多項式の剰余類環やそのイデアルと関係している．実際使われている線形符号のほとんどは巡回符号である．

次に，巡回符号のなかでも，特に重要な BCH 符号，非 2 元 BCH 符号の代表的な部分クラスであるリード-ソロモン符号について述べる．更に，代数的幾何符号についても説明する．これは，代数幾何学における数学的構造を符号に導入したものである．

復号法については，符号の構成に用いた代数的構造を利用した復号法，特に，リード-ソロモン符号の復号法について紹介する．次に，通信路の出力情報を活用する軟判定復号法をいくつか紹介する．また，代数幾何符号の復号法についても述べる．一般に復号においては，復号結果となる符号語を一つだけ出力するものが多いが，復号結果の候補を複数出力するものも考えられる．リスト復号法はそのような復号法であり，これを最後に紹介する．

【本章の構成】

本章は，巡回符号（2-1 節），BCH 符号（2-2 節），リード-ソロモン符号（2-3 節），代数幾何符号（2-4 節），代数的復号法（2-5 節），軟判定復号法（2-6 節），代数幾何符号の復号法（2-7 節），リスト復号（2-8 節）からなる．

■1 群 - 2 編 - 2 章

2-1 巡回符号

（執筆者：常盤欣一朗）[2012 年 3 月 受領]

線形符号において，任意の符号語を巡回置換した語もまた符号語であるとき，その線形符号を巡回符号（cyclic code）と呼ぶ．すなわち，GF(q) 上の符号長 n の線形符号 C において，$\boldsymbol{c} = (c_1, c_2, \ldots, c_n) \in C$ のとき常に $\boldsymbol{c}' = (c_n, c_1, \ldots, c_{n-1}) \in C$ であるならば，符号 C を巡回符号あるいは q 元巡回符号と呼ぶ[1)]．巡回符号は，符号化や復号が比較的容易に行える優れた符号を含んでおり，線形符号の最も重要な部分クラスである．

一般に，巡回符号を取り扱う場合には多項式表現を利用する．通常，q 元巡回符号 C の符号語 $\boldsymbol{c} = (c_1, c_2, \ldots, c_n)$ を GF(q) 上の多項式を用いて

$$c(X) = c_1 + c_2 X + \cdots + c_n X^{n-1} \tag{2･1}$$

のように表現する．この多項式 $c(X)$ を符号多項式（code polynomial）と呼ぶ．このとき，符号語 $\boldsymbol{c}$ を巡回置換して得られる符号語 $\boldsymbol{c}' = (c_n, c_1, \ldots, c_{n-1})$ に対応する多項式は

$$c'(X) = c_n + c_1 X + \cdots + c_{n-1} X^{n-1} \equiv X c(X) \pmod{X^n - 1} \tag{2･2}$$

と書ける．

ここで，GF(q) 上の多項式の剰余類環（residue class ring）GF(q)[X]/($X^n - 1$) を考えると，この剰余類環の元である各剰余類は GF(q) 上の $n - 1$ 次以下の多項式で表される．したがって，q 元巡回符号 C の各符号多項式 $c(X)$ をこの剰余類環の元に対応させることができる．また，明らかに，次の (1)，(2) が成り立つ．

(1) 符号 C は剰余類環 GF(q)[X]/($X^n - 1$) の加法に関する部分群である．

(2) 任意の $c(X) \in C$ 及び任意の $a(X) \in$ GF(q)[X]/($X^n - 1$) に対して，$a(X)c(X) \in C$ かつ $c(X)a(X) \in C$ である．

したがって，巡回符号 C は剰余類環 GF(q)[X]/($X^n - 1$) のイデアル（ideal）である．

巡回符号 C に属する非零の符号多項式の中で，最小次数のモニック多項式（monic polynomial）を一意に決定することができる．このような多項式を巡回符号 C の生成多項式（generator polynomial）という．ここで，モニック多項式とは最高次の係数が 1 であるような多項式のことである．

多項式 $g(X)$ が符号長 n の巡回符号 C の生成多項式であるための必要十分条件は，$g(X) \mid X^n - 1$ が成り立つことである．また，生成多項式 $g(X)$ の周期を e とすると，すなわち，$g(X) \mid X^e - 1$ となる最小の正整数を e とすると，明らかに，$e \mid n$ なる関係が成り立ち，符号長 n は生成多項式の周期 e の倍数である．ところが，符号長 n を e よりも大きくしたときの巡回符号は $X^e - 1$ を符号多項式としてもつ．そのために，符号の最小距離が 2 となり，そのような巡回符号ではランダム誤りの訂正が行えないことになる．そこで，ランダム誤りを訂正するための巡回符号を考えるときには，符号長 n を生成多項式 $g(X)$ の周期 e と等しくする．

GF(q) 上の $n-1$ 次以下の多項式が符号長 n の q 元巡回符号 C の符号多項式となるための必要十分条件は，その多項式が C の生成多項式 $g(X)$ で割り切れることである．したがって，符号 C の任意の符号多項式 $c(X)$ は，適当な多項式 $u(X)$ を用いて，

$$c(X) = u(X)g(X) \tag{2･3}$$

と書ける．符号多項式 $c(X)$ の次数は $n-1$ 以下であるので，多項式 $u(X)$ の次数はたかだか $n - \deg g(X) - 1$ となり，$u(X)$ として $q^{n-\deg g(X)}$ 通り考えることができる．異なる $u(X)$ に対しては $c(X)$ も異なることから，明らかに，巡回符号 C の符号多項式も $q^{n-\deg g(X)}$ 個存在する．したがって，巡回符号 C の情報記号数を k とすると，$k = n - \deg g(X)$ となる．すなわち，q 元 (n,k) 巡回符号において，生成多項式 $g(X)$ の次数は検査記号数 $r = n - k$ に等しいことになる．

GF(q) 上の (n,k) 巡回符号 C の生成多項式を $g(X)$ とするとき，

$$h(X) = \frac{X^n - 1}{g(X)} \tag{2･4}$$

で与えられる多項式 $h(X)$ を巡回符号 C の検査多項式（check polynomial）またはパリティ検査多項式（parity check polynomial）と呼ぶ．明らかに，$h(X)$ は k 次のモニック多項式である．また，任意の符号多項式 $c(X)$ は式 (2･3) のように書けるので，

$$c(X)h(X) = u(X)g(X)h(X) \equiv 0 \pmod{X^n - 1} \tag{2･5}$$

なる関係が成り立つ．逆に，$c(X)$ が符号多項式でなければ，式 (2･5) は成り立たないことに注意されたい．更に，巡回符号 C の双対符号（dual code）$C^\perp$ は $(n, n-k)$ 巡回符号であり，その生成多項式 $g^\perp(X)$ は

$$g^\perp(X) = \frac{X^k\, h(X^{-1})}{h(0)} \tag{2･6}$$

で与えられる．ここで，$h(X)$ を生成多項式とする $(n, n-k)$ 巡回符号は，$C^\perp$ のすべての符号語の成分の順序を逆転して得られる符号（$C^\perp$ の相反符号（reciprocal code））であり，もとの巡回符号 C の双対符号にはならないことに注意されたい．

巡回符号 C の符号化は，式 (2･3) に示したように，情報記号を係数とする多項式（情報記号多項式）$u(X)$ と生成多項式 $g(X)$ を単にかけ合わせることによって実行することができる．しかしながら，このような符号化では情報記号が符号語の特定の位置にそのまま現れないので，非組織符号（nonsystematic code）になってしまう．これに対して，次のようにすれば，巡回符号を組織符号（systematic code）として符号化することができる．

step 1 : 情報記号多項式 $u(X)$ を X^{n-k} 倍し，それを生成多項式 $g(X)$ で割った剰余多項式 $r(X)$ を求める．すなわち，

$$r(X) \equiv u(X)X^{n-k} \pmod{g(X)} \tag{2･7}$$

なる関係を満たすような $n-k-1$ 次以下の多項式 $r(X)$ を求める．

step 2 : 符号多項式 $c(X)$ を

$$c(X) = u(X)X^{n-k} - r(X) \tag{2·8}$$

とする．

このようにすれば，符号多項式 $c(X)$ において，情報記号は $X^{n-k}, X^{n-k+1}, \ldots, X^{n-1}$ の係数にそのまま現れ，検査記号は $X^0, X^1 \ldots, X^{n-k-1}$ の係数に現れる．

前述したように，巡回符号の符号多項式 $c(X)$ は生成多項式 $g(X)$ で常に割り切れる．したがって，受信多項式 $r(X)$ を生成多項式 $g(X)$ で割り算した結果，

- 割り切れたならば，受信多項式 $r(X)$ には誤りが含まれていない
- 割り切れなかったならば，受信多項式 $r(X)$ には誤りが含まれている

と判断できる．巡回符号を用いたこのような誤り検出の方法を CRC（cyclic redundancy check）と呼ぶ．通常，CRC には 2 元巡回符号が用いられる．CRC に用いられる 2 元巡回符号の代表的な生成多項式を表 2·1 に示す[2, 3]．

一般に，2 元 (n, k) 巡回符号 C の誤り検出能力について次のことが成り立つ[2, 3, 4]．

▶ ランダム誤りに対して

符号 C の最小距離が $d_{\min}$ であるとき，符号 C は $d_{\min}-1$ 個以下のランダム誤りをすべて検出できる．また，符号 C の生成多項式 $g(X)$ が $X+1$ を因数に含むならば，符号 C は奇数個の誤りをすべて検出できる．

▶ バースト誤りに対して

符号 C は長さ $n-k$ 以下のバースト誤りをすべて検出できる．そして，符号 C は長さ $n-k+1$ のすべてのバースト誤りのうち $1-2^{-(n-k-1)}$ の割合の誤りを検出できる．更に，符号 C は長さ $\ell\ (\geq n-k+2)$ のすべてのバースト誤りのうち $1-2^{-(n-k)}$ の割合の誤りを検出できる．

表 2·1　CRC に用いられる 2 元巡回符号の代表的な生成多項式

呼称	生成多項式 $g(X)$
CRC-12	$1+X+X^2+X^3+X^{11}+X^{12}$
CRC-ANSI	$1+X^2+X^{15}+X^{16}$
CRC-CCITT	$1+X^5+X^{12}+X^{16}$
CRC-SDLC	$1+X+X^2+X^4+X^7+X^{13}+X^{15}+X^{16}$
CRC-24	$1+X^8+X^{12}+X^{14}+X^{23}+X^{24}$
CRC-32a	$X+X^5+X^6+X^7+X^{11}+X^{12}+X^{15}+X^{22}+X^{30}+X^{32}$
CRC-32b	$1+X+X^2+X^4+X^5+X^7+X^8+X^{10}+X^{11}+X^{12}+X^{16}+X^{22}+X^{23}+X^{26}+X^{32}$

巡回符号に密接に関係した符号のクラスとして準巡回符号（quasi-cyclic code）がある[5]．符号長 n の線形符号 C に対して，任意の符号多項式 $c(X)$ を s 記号だけ巡回置換して得られる $X^s c(X) \pmod{X^n-1}$ が常に C の符号多項式であるような整数 s が存在するとき，この符号 C を準巡回符号と呼ぶ．明らかに，$s=1$ の準巡回符号は通常の巡回符号である．

■1 群 - 2 編 - 2 章

2-2 BCH 符号

（執筆者：常盤欣一朗）［2012 年 3 月 受領］

BCH 符号（Bose-Chaudhuri-Hocquenghem code）は，巡回符号のなかでも特に重要なクラスの符号であり，次のように定義される．

n を q^m-1 の約数とし，α を GF(q^m) の位数 n の元とする．そして，適当な整数 $b\,(\geq 0)$ 及び $\delta\,(2 \leq \delta \leq n)$ に対して，$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ を根にもつ GF(q) 上の最小次数のモニック多項式を $g(X)$ とする．このとき，$g(X)$ を生成多項式とするような符号長 n の q 元巡回符号が q 元 BCH 符号である．特に，$b=1$ の場合を狭義 BCH 符号（narrow sence BCH code）と呼ぶ．また，$n=q^m-1$ の場合を原始 BCH 符号（primitive BCH code）と呼ぶ．

任意の整数 ℓ に対して，GF(q^m) の元 α^ℓ の GF(q) 上の最小多項式（minimal polynomial），すなわち，α^ℓ を根にもつ最小次数の GF(q) 上のモニック多項式を $M_\ell(X)$ と表す．このとき，上述した q 元 BCH 符号の生成多項式 $g(X)$ は次式のように $\delta-1$ 個の根に対する最小多項式 $M_b(X), M_{b+1}(X), \ldots, M_{b+\delta-2}(X)$ の最小公倍多項式として与えられる．

$$g(X) = \mathrm{LCM}\,[\, M_b(X), M_{b+1}(X), \ldots, M_{b+\delta-2}(X)\,] \tag{2･9}$$

これらの最小多項式はいずれも GF(q) 上で既約であるので，実際には，生成多項式 $g(X)$ は最小多項式 $M_b(X), M_{b+1}(X), \ldots, M_{b+\delta-2}(X)$ のなかで異なるものの積に等しくなる．また，これらの最小多項式の次数がたかだか m 次であることを考慮すると，生成多項式 $g(X)$ の次数は $m(\delta-1)$ 以下になる．したがって，q 元 BCH 符号の検査シンボル数 $n-k$ は

$$n-k \leq m(\delta-1) \tag{2･10}$$

となる．更に，後述する BCH 限界から，BCH 符号の最小距離 $d_{\min}$ は

$$d_{\min} \geq \delta \tag{2･11}$$

で与えられる．この式の右辺の値 δ を q 元 BCH 符号の設計距離（designed distance）と呼ぶ．ここで，設計距離 δ と実際の最小距離 $d_{\min}$ とは必ずしも一致しないことに注意されたい．しかしながら，BCH 符号の代数的な復号法であるピーターソン（Peterson）復号法，バーレカンプ-マッシィ（Berlekamp-Massey）復号法，ユークリッド（Euclid）復号法などでは，いずれも設計距離で保証される個数の誤りを対象としており，設計距離が実際の最小距離に代わって重要な役割を担っている．

ここで BCH 限界（BCH bound）について述べる．BCH 限界は，BCH 符号を含む巡回符号の最小距離を評価する際に重要な役割を果たすものであり，次に述べるように巡回符号の生成多項式の根から最小距離を評価するものである．

いま n を q^m-1 の約数とし，α を GF(q^m) の位数 n の元とする．このとき，符号長 n の q 元巡回符号 C の生成多項式 $g(X)$ が，指数部の値が連続するような $\delta-1$ 個の元 $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ を根にもつならば，符号 C の最小距離 $d_{\min}$ は少なくとも δ である．このように与えられる

最小距離の下限が BCH 限界である．

なお，BCH 限界を改善したものとして，ハートマン-ツェン（Hartmann-Tzeng）限界，ルース（Roos）限界，ファンリント-ウィルソン（van Lint-Wilson）限界などが知られている[6, 7]．

通常よく用いられる重要な BCH 符号は，$q = 2$，$n = 2^m - 1$，$b = 1$，$\delta = 2t + 1$ として得られる t 重誤り訂正 2 元原始 BCH 符号である．この符号のパラメータ（符号長 n，情報ビット数 k，最小距離 $d_{\min}$）及び生成多項式 $g(X)$ は次のように与えられる．

$$\text{符号長} \qquad n = 2^m - 1 \tag{2･12}$$

$$\text{情報ビット数} \qquad k \geq n - mt \tag{2･13}$$

$$\text{最小距離} \qquad d_{\min} \geq 2t + 1 \tag{2･14}$$

$$\text{生成多項式} \qquad g(X) = \mathrm{LCM}\,[\, M_1(X), M_3(X), \ldots, M_{2t-1}(X)\,] \tag{2･15}$$

ここで，2 元の場合，任意の ℓ に対して，$M_\ell(X) = M_{2\ell}(X)$ なる関係が成り立つ．したがって，生成多項式 $g(X)$ の表現においては偶数べきの根 $\alpha^2, \alpha^4, \ldots, \alpha^{2t}$ に対する最小多項式 $M_2(X), M_4(X), \ldots, M_{2t}(X)$ が除かれている．また，この影響で，情報ビット数は $k \geq n - 2mt$ ではなく $k \geq n - mt$ になることに注意されたい．なお，$t = 1, 2$ ($\delta = 3, 5$) の場合には，式 (2･13) 及び式 (2･14) の等号が成り立つ．

表 2･2 に，符号長が 255 以下の 2 元原始 BCH 符号の符号長 n，情報ビット数 k，設計距離 δ を示す．

表 2･2　2 元原始 BCH 符号のパラメータ

n	k	δ	n	k	δ	n	k	δ	n	k	δ
7	4	3		18	21		22	47		131	37
				16	23		15	55		123	39
15	11	3		10	27		8	63		115	43
	7	5		7	31					107	45
	5	7				255	247	3		99	47
			127	120	3		239	5		91	51
31	26	3		113	5		231	7		87	53
	21	5		106	7		223	9		79	55
	16	7		99	9		215	11		71	59
	11	11		92	11		207	13		63	61
	6	15		85	13		199	15		55	63
				78	15		191	17		47	85
63	57	3		71	19		187	19		45	87
	51	5		64	21		179	21		37	91
	45	7		57	23		171	23		29	95
	39	9		50	27		163	25		21	111
	36	11		43	29		155	27		13	119
	30	13		36	31		147	29		9	127
	24	15		29	43		139	31			

■1 群 - 2 編 - 2 章

2-3 リード-ソロモン符号

（執筆者：常盤欣一朗）[2012 年 3 月 受領]

リード-ソロモン符号（Reed-Solomon code）は，符号長 $n = q - 1$ を有する q 元原始 BCH 符号であり，q 元 BCH 符号のなかでも理論面だけではなく実用面でも最も重要な符号のクラスである[8]．通常，RS 符号と略記される．以下では，RS 符号を原始 BCH 符号の特別なクラスとして定義するが，これに対して，RS 符号の部分体部分符号（subfield subcode）として原始 BCH 符号を定義することもできる．

いま α を GF(q) の原始元とする．そして，適当な整数 b (≥ 0) 及び δ ($2 \leq \delta < q$) に対して，$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ を根にもつような GF(q) 上の最小次数のモニック多項式を $g(X)$ とする．このとき，$g(X)$ を生成多項式とするような符号長 $n = q - 1$ の q 元巡回符号（BCH 符号）が RS 符号である．

RS 符号の生成多項式 $g(X)$ は

$$g(X) = (X - \alpha^b)(X - \alpha^{b+1}) \cdots (X - \alpha^{b+\delta-2}) \tag{2･16}$$

で与えられる．したがって，RS 符号は生成多項式 $g(X)$ の根を定義する体と符号語の成分を表す体が一致する符号である．また，生成多項式 $g(X)$ の次数が $\delta - 1$ であるので，RS 符号の検査記号数 $n - k$ は

$$n - k = \delta - 1 \tag{2･17}$$

で与えられる．更に，最小距離 $d_{\min}$ は，BCH 限界から，$d_{\min} \geq \delta$ なる関係を満たす．一方，最小距離 $d_{\min}$ は，シングルトン限界 [3 章 3-1 節 参照] からは，$d_{\min} \leq n - k + 1$ なる関係を満たす．そこで，式 (2･17) を考慮すると，

$$d_{\min} = \delta = n - k + 1 \tag{2･18}$$

となることが分かる．すなわち，RS 符号は，シングルトン限界を等号で満たす最大距離分離符号（maximum distance separable code : MDS code）であり，同一の最小距離を有する符号のなかで最小の検査記号数をもつ優れた符号である．

一般に，符号の重み分布（weight distribution）を求めることは難しい問題であるが，MDS 符号に関しては陽に重み分布が与えられている．いま GF(q) 上の $(n, k, d_{\min})$MDS 符号 C において，ハミング重み w を有する符号語の数を A_w ($w = 0, 1, \ldots, n$) とする．このとき，符号 C の重み分布は

$$A_0 = 1 \tag{2･19}$$

$$A_w = 0 \qquad w = 1, 2, \ldots, d_{\min} - 1 \tag{2･20}$$

$$A_w = \binom{n}{w} \sum_{j=0}^{w-d_{\min}} (-1)^j \binom{w}{j} \left(q^{w-d_{\min}+1-j} - 1 \right) \qquad w = d_{\min}, d_{\min} + 1, \ldots, n \tag{2･21}$$

で与えられる．RS 符号は MDS 符号であるので，RS 符号の重み分布も式 (2･19)〜式 (2･21) で与えられることになる．なお，式 (2･21) は次式のように表現することもできる．

$$A_w = \binom{n}{w}(q-1)\sum_{j=0}^{w-d_{\min}}(-1)^j\binom{w-1}{j}q^{w-d_{\min}-j} \qquad w = d_{\min}, d_{\min}+1, \ldots, n \quad (2\cdot22)$$

RS 符号の構造をより詳細に知るために，GF(2^m) 上の RS 符号に対して，完全重み分布（complete weight distribution）や 2 元重み分布（binary weight distribution）などに関する検討もなされているが，いまだ未解決な部分が多く残されてる[5, 9, 10, 11, 12]．完全重み分布とは，符号語の成分として GF(2^m) の各元が現れる様子を詳細に示したものであり，符号の構造を知るうえで極めて重要なものである．また，2 元重み分布とは，GF(2^m) の各元を 2 元展開することによって RS 符号から得られる 2 元線形符号の重み分布である．

ここで，RS 符号の別の定義を与えておく．いま α を GF(q) の原始元とし，$n = q-1$ とする．また，GF(q) の任意の k 個の元 $u_1, u_2, \ldots, u_k$ を情報記号として，これらを係数にもつ多項式 $u(X) = u_1 + u_2X + \cdots + u_kX^{k-1}$ を考える．そして，情報記号多項式 $u(X)$ に対して

$$u(X) \;\mapsto\; \boldsymbol{c} = \big(\, u(1),\, u(\alpha),\, \ldots,\, u(\alpha^{n-1}) \,\big) \quad (2\cdot23)$$

のように GF(q) 上の n 次元ベクトル $\boldsymbol{c}$ を符号語として対応させることによって符号化を行う．このようにして得られるすべての符号語の集合が符号長 n，情報記号数 k，最小距離 $d_{\min} = n-k+1$ の RS 符号である．なお，この RS 符号の生成多項式 $g(X)$ は $\alpha, \alpha^2, \ldots, \alpha^{n-k}$ を根としてもつことに注意されたい．

より一般には，

$$u(X) \;\mapsto\; \boldsymbol{c} = \big(\, u(1),\, \alpha^{-(b-1)}u(\alpha),\, \ldots,\, \alpha^{-(b-1)(n-1)}u(\alpha^{n-1}) \,\big) \quad (2\cdot24)$$

とすることによって，生成多項式 $g(X)$ が $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+n-k-1}$ を根としてもつような符号長 n，情報記号数 k，最小距離 $d_{\min} = n-k+1$ の RS 符号が得られる．

更に，RS 符号の考え方を次のように一般化することもできる．いま，$\alpha_1, \alpha_2, \ldots, \alpha_n$ を GF(q^m) の異なる n 個の元とし，$v_1, v_2, \ldots, v_n$ を GF(q^m) の n 個の非零元（必ずしも異なる必要はない）とする．このとき，GF(q^m) 上の任意の情報記号多項式 $u(X) = u_1 + u_2X + \cdots + u_kX^{k-1}$ に対して

$$u(X) \;\mapsto\; \boldsymbol{c} = (\, v_1u(\alpha_1),\, v_2u(\alpha_2),\, \ldots,\, v_nu(\alpha_n) \,) \quad (2\cdot25)$$

のように GF(q^m) 上の n 次元ベクトル $\boldsymbol{c}$ を符号語として対応させる．このようにして得られる符号長 n，情報記号数 k，最小距離 $d_{\min} = n-k+1$ の符号を一般化リード-ソロモン符号（generalized Reed-Solomon code）と呼び，通常，GRS 符号と略記する．GRS 符号は MDS 符号であるので，その重み分布は式 (2･19)〜式 (2･21) で与えられる．

■1 群 - 2 編 - 2 章

2-4 代数幾何符号

（執筆者：阪田省二郎）[2012 年 3 月 受領]

代数幾何符号（algebraic geometry code）は，現在もよく用いられている BCH 符号（本章 2-2 参照）やリード-ソロモン符号（本章 2-3 参照）の自然な一般化であり，代数幾何学の研究対象である多項式や有理式（分数式）で定義される代数曲線・曲面の性質を用いて構成され，優れた性能を有している線形ブロック符号（本章 1-4 参照）の 1 クラスである[13]．従来の実用的な符号がガロア体（本章 1-3 参照）上の 1 変数多項式を用いて定義されるのに対し，狭義の代数幾何符号はガロア体上の多変数多項式・有理式を用いて定義される．代数幾何学で最もよく扱われるのは，図 2･1 に示す実数体上の楕円曲線のように複素数体や実数体上の（連続性・無限性を備えた）概念であるが，符号に用いられるのは，ガロア体（有限体）上で定義され，元来，図 2･2 （この図の説明は後述）のような離散性*・有限性を備えた概念である．しかし，しばしば，同じ標数 p をもつガロア体の無限系列 $\mathrm{GF}(p^i), i \geq 1$ の和集合である閉体 $\bar{\mathcal{K}} \triangleq \cup_{i\geq 1}\mathrm{GF}(p^i)$ のなかで考えたり，それなりのトポロジー（連続性の一種）を想定する．

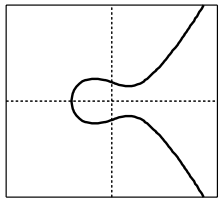

図 2･1 $y^2 = x^3 - x + 1$

$i\backslash j$	0	1	2	3
0	0	5	10	15
1	4	9	14	19
2	8	13	18	23
.	.	.	.	.
.	.	.	.	.
14	56	61	66	71
15	60	65	70	75

図 2･2　各基底関数 x^iy^j の極位数 $o(x^iy^j)$

ゴッパ（Goppa）によって，1977 年に初めて代数幾何符号が提唱され[14]，1981 年にその明確な定義と基本的な性質が明らかにされた[15]．これは，広義にはすべての線形符号を含むと見なすこともできる一方，狭義には新しく見いだされた符号クラスであって，ツファスマン（Tsfasman），ヴラジュ （Vlăduţ），ジンク（Zink）によって，ギルバート-バルシャモフ限界（本章 3-1 参照）に初めて達する（ある符号化率の範囲ではそれを超える）ものが存在することが構成的に示されている[16]という意味で画期的なものである．

代数幾何符号は，情報を担う記号の集合（アルファベット）であるガロア体 $\mathcal{K} = \mathrm{GF}(q)$（素数べき q はその濃度 $|\mathcal{K}|$）と同じか，その拡大体であるガロア体 $\tilde{\mathcal{K}}$ 上の代数的多様体（代数曲線・代数曲面）$\mathcal{X}$ におけるすべての点（$\tilde{\mathcal{K}}$ 有理点という）の集合 $\mathcal{X}(\tilde{\mathcal{K}})$ の部分集合 $\mathcal{P} = \{P_1, \cdots, P_n\}$，及び，代数的多様体 $\mathcal{X}$ 上で定義された関数 $f : \mathcal{X}(\tilde{\mathcal{K}}) \to \tilde{\mathcal{K}}$ のなす代数関数体 $\mathcal{F}$ の線形部分空間 $\mathcal{L}$（関数空間）から構成される[17]．点集合 $\mathcal{P}$ の濃度 $|\mathcal{P}|$ は この符号

* 実数体上の曲線は，人間の視覚がとらえたテレビ画像のような連続的なイメージに対応するが，有限体上の曲線は，その空間的サンプリングである 2 次元ドットパターン（2 次元配列）のような離散的な点の集合にすぎない．

の符号長（ブロック長）n である．一般の線形符号と同じく，代数幾何符号には，主符号（幾何的リード-ソロモン符号や $\mathcal{L}$ 符号と呼ばれる）と 双対符号（幾何的ゴッパ符号や Ω 符号と呼ばれる）の対

$$C = \{\boldsymbol{c} = \mathrm{eval}(f) \in \tilde{\mathcal{K}}^n \mid f \in \mathcal{L}\}, \quad C^{\perp} = \{\boldsymbol{c} \in \tilde{\mathcal{K}}^n \mid \boldsymbol{c} \cdot \mathrm{eval}(f) = 0,\ f \in \mathcal{L}\}$$

がある．ここで，$\mathrm{eval}(f) \triangleq (f(P_j))_{1\le j\le n} \in \tilde{\mathcal{K}}^n$, $\boldsymbol{a}\cdot\boldsymbol{b} \triangleq \sum_{1\le j\le n} a_j b_j \in \tilde{\mathcal{K}}$ である．主符号では，通常，$\tilde{\mathcal{K}} = \mathcal{K}$ とするが，双対符号では しばしば，$\mathcal{K}$ の真の拡大体を用いる場合があり，それは，BCH 符号等の巡回符号（本章 2-1 参照）の一般化であって，部分体部分符号と呼ばれるものになる．

最も基本的な代数幾何符号は，代数的多様体 $\mathcal{X}$ として特異点をもたない代数曲線をとり，曲線 $\mathcal{X}$ 上でできる限り多数個の $\tilde{\mathcal{K}}$ 有理点からなる集合 $\mathcal{P}$, 及び，関数空間 $\mathcal{L}$ として代数曲線 $\mathcal{X}$ 上のいくつかの特定の点を零点, あるいは, 極としてもつ代数関数の集合をとることによって定義される代数曲線符号である．一般的には, まず, 代数曲線 $\mathcal{X}$ を閉体 $\bar{\mathcal{K}}$ 上の m 次元アフィン空間 $\bar{\mathcal{K}}^m$ 内で考え，代数曲線 $\mathcal{X}$ のすべての点で 0 となる多項式 $f \in \bar{\mathcal{K}}[\boldsymbol{x}]$ の全体 $\bar{\mathcal{I}}(\mathcal{X})$ が m 変数多項式環 $\bar{\mathcal{K}}[\boldsymbol{x}] \triangleq \bar{\mathcal{K}}[x_1, \cdots, x_m]$ のイデアルとなることから，その剰余類環 $\bar{\Gamma}(\mathcal{X}) \triangleq \bar{\mathcal{K}}[\boldsymbol{x}]/\bar{\mathcal{I}}(\mathcal{X})$ の商体（1 変数代数関数体と呼ばれる）$\bar{\mathcal{K}}(\mathcal{X}) \triangleq \{\frac{g}{f} | f, g \in \bar{\Gamma}(\mathcal{X}),\ f \neq 0\}$ の元として代数関数を導入する．イデアル $\bar{\mathcal{I}}(\mathcal{X})$ を法とする剰余類環によるこの定義は，$fg' - f'g \in \bar{\mathcal{I}}(\mathcal{X})$ のとき，$\frac{g}{f}$ と $\frac{g'}{f'}$ が曲線上で値が一致し，見かけは異なっても本質的に同一の関数であるという事実に基づいている．

アフィン空間を射影空間に拡張し，無限遠点も含めた曲線上の任意の点 Q において，一種の加法性: $v(hh') = v(h) + v(h')$, $h, h' \in \bar{\mathcal{K}}(\mathcal{X})$ をもつ付値と呼ばれる整数 $v(h)$ が重要な働きをする．関数 $h \in \bar{\mathcal{K}}(\mathcal{X})$ の点 Q における付値 $v_Q(h)$ が正数のとき，h は，Q において位数（order）$o(h) \triangleq v_Q(h)$ の零点（zero）をもち，付値 $v_Q(h)$ が負数のとき，Q において位数（order）$o(h) \triangleq |v_Q(h)|$ の極（pole）をもつといわれる．任意の関数 $h \in \bar{\mathcal{K}}(\mathcal{X})$ は，有限個の極 $Q_i \in \boldsymbol{Q}_1$ と零点 $Q'_j \in \boldsymbol{Q}_2$ をもち（$\boldsymbol{Q}_1 \cap \boldsymbol{Q}_2 = \emptyset$），それぞれの位数の和は等しく，$\sum_{Q_i\in\boldsymbol{Q}_1} v_{Q_i}(h) + \sum_{Q'_j\in\boldsymbol{Q}_2} v_{Q'_j}(h) = 0$ が成り立つ．一般に，曲線 $\mathcal{X}$ 上の代数関数体は，有理関数体（1 変数有理式の全体）$\bar{\mathcal{K}}(x)$ の有限次代数的拡大体 $\bar{\mathcal{K}}(x, y)$ である．一つの 2 変数多項式 $f(x, y) \in \tilde{\mathcal{K}}[x, y]$ に対し，方程式 $f(x, y) = 0$ によって定義される平面曲線 $\mathcal{X}$ の場合，このことは二つの元 x, y の内，一方を超越元（独立変数）と見れば，他方はそれに対して，代数的に独立でないことを意味する．

以上のように，代数関数の零点と極の位数の概念は，1 変数有理式 $\frac{g(x)}{f(x)} \in \bar{\mathcal{K}}(x)$ の零点（根）と極の位数（重複度）の概念の拡張であるが，一般に複雑な計算を必要とする．ガロア体 $\tilde{\mathcal{K}}$ 上の代数曲線 $\mathcal{X}$ に基づいて符号を定義するとき，表記の簡略化のため，$\tilde{\mathcal{K}}$ 有理点集合 $\mathcal{X}(\tilde{\mathcal{K}})$ において，部分集合 $\boldsymbol{Q}_1, \boldsymbol{Q}_2 \subset \mathcal{X}(\tilde{\mathcal{K}}) \setminus \mathcal{P}$ に対し，正整数係数 $m_{Q_i}, n_{Q'_j}$ $(Q_i \in \boldsymbol{Q}_1, Q'_j \in \boldsymbol{Q}_2)$ をもつ形式的な和（因子と呼ばれる）$D \triangleq \sum_{Q_i\in\boldsymbol{Q}_1} m_{Q_i} Q_i - \sum_{Q'_j\in\boldsymbol{Q}_2} n_{Q'_j} Q'_j$ を導入し，ガロア体 $\tilde{\mathcal{K}}$ 上の関数空間 $\mathcal{L}$ として，各点 $Q_i \in \boldsymbol{Q}_1$ において位数 m_{Q_i} 以下の極をもち，かつ，各点 $Q'_j \in \boldsymbol{Q}_2$ において位数 $n_{Q'_j}$ 以上の零点をもつすべての $\tilde{\mathcal{K}}$ 上の代数関数のなす線形空間 $\mathcal{L}(D)$ をとる．元来，双対符号は，関数空間 $\mathcal{L}(D)$ でなく，曲線上の微分形式のなす線形空間 $\Omega(D)$ から直接定義された．しかし，符号理論の立場からは上記の定義でほとんど十分であり，数学的により複雑な議論を必要とする微分形式には触れない代数幾何学なしの代数幾何符号（algebraic

geometry code without Algebraic Geometry）という考え方が強調されることがある．

関数空間 $\mathcal{L}(D)$ の次元 $l(D)$ は，因子 D の次数と呼ばれる整数 $\deg(D) \triangleq \sum_{Q_i \in \mathcal{Q}_1} m_{Q_i} - \sum_{Q'_j \in \mathcal{Q}_2} n_{Q'_j}$ に対し，リーマン-ロッホ（Riemann-Roch）定理として知られる関係: $l(D) \geq \deg(D) - g + 1$ を満たす．ここで，整数 g は，曲線 $\mathcal{X}$ の種数（genus）と呼ばれる特性数である．また，$\deg(D) \geq 2g-1$ のとき $l(D) = \deg(D) - g + 1$ となることから，$\mu \triangleq \deg(D)$ が $2g-1 \leq \mu < n$ である場合，主符号 C，双対符号 $C^{\perp}$ のそれぞれの次元が $k = \mu - g + 1$, $k^{\perp} = n - \mu + g - 1$ となり，最小距離が $d \geq d_G \triangleq n - \mu$, $d^{\perp} \geq d_G^{\perp} \triangleq \mu - 2g + 2$ となる．これら最小距離の下界 $d_G, d_G^{\perp}$ は，ゴッパ限界，あるいは，ゴッパ設計距離（Goppa designed distance）と呼ばれる．

一般に符号長を大きくとることによって，より性能のよい符号を構成できる可能性が増大するが，リード-ソロモン符号では，符号長がその定義ガロア体 $\mathcal{K}$ に依存し，$\mathcal{K}$ を固定したまま符号長 n を大きくすることはできない．しかし，定義ガロア体 $\mathcal{K} = \mathbf{F}_q$ を固定，かつ，$\tilde{\mathcal{K}} = \mathcal{K}$ としたまま，曲線を変化させることによって，$\mathcal{K}$ 有理点の個数，そして，符号長 n を，代数曲線 $\mathcal{X}$ 上の $\mathcal{K}$ 有理点の個数 $N_q(\mathcal{X})$ に対するハッセ-ヴェイユ-セール（Hasse-Weil-Serre）限界 $|N_q(\mathcal{X}) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor$ の許す範囲内で，漸近的に大きくすることができる．このことに関連して，エルミート曲線などの簡単な平面曲線を高次元空間の中へ次々に拡張して得られる関数空間の列（関数空間の塔（tower）と呼ばれる）を用いて，より簡単に構成できて，漸近的に優れた性能をもつ符号系列が与えられている[18]．

古典的ゴッパ符号は，リード-ソロモン符号と同様に，ガロア体上の直線，あるいは，ガロア体の元 α_j からなる $\mathcal{P}$ から定義される代数幾何符号である．それは，拡大体 $\tilde{\mathcal{K}}$ の部分集合 $\mathcal{P} = \{P_j (= \alpha_j) \mid 1 \leq j \leq n\}$，及び，差集合 $\tilde{\mathcal{K}} \setminus \mathcal{P}$ のなかに零点（根）をもつ多項式（ゴッパ多項式と呼ばれる）$g(x) \in \mathcal{K}[x]$ とその零点の全体 $\mathcal{R}$ をとって，$\tilde{\mathcal{K}}$ 上の関数空間 $\mathcal{L}(\sum_{Q_i \in \mathcal{R}} Q_i - \sum_{P_j \in \mathcal{P}} P_j)$ によって定義される双対符号の部分体部分符号である．

1 点代数曲線符号（one-point code from algebraic curve）は，非負整数 μ と曲線 $\mathcal{X}$ 上の 1 点 Q に対し，点集合 $\mathcal{P} = \mathcal{K}(\mathcal{X}) \setminus \{Q\}$，及び，関数空間 $\mathcal{L} = \mathcal{L}(\mu Q)$ によって定義される．通常，Q として，無限遠点 P_∞ が選ばれる．平面曲線 $f(x,y) = 0$ から定義される 1 点符号の場合，関数空間 $\mathcal{L}$ は，剰余類環 $\mathcal{K}[x,y]/(f(x,y))$ の部分集合である．近い将来実用化される可能性の最も高い代数幾何符号は，素数べき ρ に対し，濃度 $q = \rho^2$ をもつガロア体 $\mathcal{K} = \mathrm{GF}(q)$ 上のエルミート曲線（Hermitian curve）$\mathcal{X}: x^{\rho+1} - y^{\rho} - y = 0$ から定義されるエルミート曲線符号（Hermitian code）である．エルミート曲線は（ハッセ-ヴェイユ-セール限界を等式で満たすという意味で）最大曲線であり，その $\mathcal{K}$ 有理点は無限遠点 P_∞ 以外に $n = \rho^3$ 個あるが，そのすべてをとって $\mathcal{P} \triangleq \mathcal{K}(\mathcal{X}) \setminus \{P_\infty\}$ とする．関数空間 $\mathcal{L}(\mu P_\infty)$ は，$0 \leq \mu < n$ ならば，$\{x^i y^j \mid i \geq 0, \rho > j \geq 0, \rho i + (\rho+1) j \leq \mu\}$ を基底としてもつ．$\mathcal{K}$ を含む閉体 $\bar{\mathcal{K}} = \cup_{i \geq 1} \mathrm{GF}(q^i)$ 上の関数空間 $\mathcal{L}(\infty P_\infty) = \cup_{i \geq 0} \mathcal{L}(iP_\infty)$ に対し，その基底をなす関数をそれらの極位数の順に並べたものの集合 $\mathcal{B} = \{b^{(j)} \mid j \geq 1\}$，及び，それらの極位数の集合 $\mathcal{O} = \{o^{(j)} = o(b^{(j)}) \mid j \geq 1\}$，あるいは，ガロア体 $\mathcal{K}$ 上に限定した有限部分集合 $\mathcal{B}_q = \{b^{(j)} \mid 1 \leq j \leq n\}, \mathcal{O}_q = \{o^{(j)} \mid 1 \leq j \leq n\}$ に対し，関数空間の増大列 $\mathcal{L}_i \triangleq \langle b^{(j)} \mid 1 \leq j \leq i \rangle_{\mathcal{K}}$, $1 \leq i \leq n$，及び，それらによって定義される主符号の増大列 $C_i \triangleq \{c = \mathrm{eval}(f) \in \mathcal{K}^n \mid f \in \mathcal{L}_i\}$, $1 \leq i \leq n$ と双対符号の減小列 $C_i^{\perp} \triangleq \{c \in \mathcal{K}^n \mid c \cdot \mathrm{eval}(f) = 0, f \in \mathcal{L}_i\}$, $1 \leq i \leq n$ をつくることができる．例えば，$\rho = 2^2$ $(q = 16)$ の場合，冒頭に示した図 2･2 は基底関数 $x^i y^j$ の極位数のなす配列である．この極位数と基底関数の配列は，これらの符号の復号法（本章 2-7 節 参照）の基本となる．

■1 群 - 2 編 - 2 章

2-5 代数的復号法

（執筆者：神谷典史）[2012 年 3 月 受領]

誤り訂正符号化された送信符号語を $\boldsymbol{c}$ とし，通信路の出力である受信語を $\boldsymbol{r} \triangleq \boldsymbol{c} + \boldsymbol{e}$ とする．ここで，$\boldsymbol{e}$ は誤りベクトルである．受信語 $\boldsymbol{r}$ から未知の $\boldsymbol{c}$ を導く処理を復号という．誤り訂正符号の種類によっては，復号をある種の代数方程式に帰着させて行うことができ，このような復号方法は一般に代数的復号法と呼ばれている．本節では，実用と理論の両面において最も重要な符号の一つであるリード-ソロモン符号の代表的な代数的復号方法について説明する．その復号方法は主に次の四つのステップからなる．

1. 受信語 $\boldsymbol{r}$ に誤りが含まれているか否かを検査する（シンドロームの算出）．
2. 受信語中に含まれる誤り数を推定する．
3. 受信語中に含まれる誤り位置を推定する．
4. 推定した誤り位置における誤り値を算出し，訂正を行う．

$(n, k, d_{\min})$ リード-ソロモン符号の生成多項式の根を $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+d_{\min}-2}$ とするとき，次の $s_b, s_{b+1}, \cdots, s_{b+d_{\min}-2}$ を受信語 $\boldsymbol{r} = (r_0, r_1, \cdots, r_{n-1})$ に対するシンドロームと呼ぶ．

$$s_{b+j} \triangleq \sum_{i=0}^{n-1} r_i (\alpha^{b+j})^i, \ j = 0, 1, \cdots, d_{\min} - 2 \tag{2・26}$$

復号処理のステップ 1. において，$d_{\min} - 1$ 個のシンドローム成分がすべて零であった場合，誤りなしと判定する．シンドロームに零でない成分がある場合，ステップ 2. の誤り数の推定を行う．これは次に示すシンドローム行列 $\boldsymbol{S}_l$ の階数を調べることで行える．

$$\boldsymbol{S}_l \triangleq \begin{pmatrix} s_b & s_{b+1} & \cdots & s_{b+l} \\ s_{b+1} & s_{b+2} & \cdots & s_{b+l+1} \\ \vdots & \vdots & & \vdots \\ s_{b+d_{\min}-2-l} & s_{b+d_{\min}-1-l} & \cdots & s_{b+d_{\min}-2} \end{pmatrix} \tag{2・27}$$

$l = 0$ の場合から順次 $\boldsymbol{S}_l$ の階数 $\mathrm{rank}(\boldsymbol{S}_l)$ を算出し，$\mathrm{rank}(\boldsymbol{S}_l) < l + 1$ を満たす最小の自然数 t を求める．この t が受信語中に含まれる誤り数の推定値となる．ステップ 3. は，線形方程式 $\boldsymbol{S}_t \cdot \boldsymbol{\sigma}^T = \boldsymbol{0}$ の解 $\boldsymbol{\sigma} = (\sigma_t, \cdots, \sigma_1, 1)$ を係数とする多項式 $\sigma(X) \triangleq 1 + \sigma_1 X + \cdots + \sigma_t X^t$ の根を求めることによって行える．実際，誤りベクトル $\boldsymbol{e} = (e_0, e_1, \cdots, e_{n-1})$ のハミング重みが $d_{\min}/2$ よりも小さい場合には $\boldsymbol{e}$ の非零成分数はステップ 2. で算出した t に一致し，$e_{i_j} \neq 0$, $j = 0, 1, \cdots, t-1$ とすると $\sigma(X) = \prod_{j=0}^{t-1}(1 - \alpha^{i_j} X)$ となる．したがって，誤り数が訂正可能な範囲内ならば，多項式 $\sigma(X)$ の根を導くことにより，その位置を特定することができる．この $\sigma(X)$ は誤り位置多項式と呼ばれる．$\sigma(X)$ の根の算出は通常 $\alpha^0, \alpha^{-1}, \cdots, \alpha^{-(n-1)}$ を順次 $\sigma(X)$ に代入してその値が零か否かを検査するという方法がとられる（チェン（Chien）サー

チ）．ステップ 4. の誤り値は，検査行列の列ベクトルのうち，ステップ 3. で導かれた推定誤り位置に対応するものだけからなる行列を係数行列とする線形方程式を解くことによって算出できる．以上の復号方法は発明者の名前にちなんでピーターソン復号法（Peterson Decoding Algorithm）と呼ばれている[1)]．

ピーターソン復号法は訂正可能な誤り数が 2 ~ 3 シンボルと小さいときには非常に有効であるが，誤り数 t が大きい場合には，誤り数の推定，誤り位置多項式の算出などに多くの計算量が必要となり，より効率的な復号方法が求められる．このような復号方法として代表的なものにバーレカンプ-マッシィ復号法がある．ピーターソン復号法におけるシンドローム行列 (2･27) に相当するものとして，シンドロームを係数とする多項式 $S(X) \triangleq \sum_{i=0}^{d_{\min}-2} s_{b+i}X^i$ を用いる．与えられた $S(X)$ に関して，次式を満たす多項式の組 $\{\sigma(X), \omega(X)\}$ を考える．

$$\sigma(X)S(X) \equiv \omega(X) \bmod X^{d_{\min}-1}, \quad \sigma(0) = 1 \tag{2･28}$$

式 (2･28) を満たすすべての $\{\sigma(X), \omega(X)\}$ のなかで，$L \triangleq \max\{\deg(\sigma),\ 1 + \deg(\omega)\}$ の値が最小となる，ある一組の多項式を導くのが図 2･3 のバーレカンプ-マッシィアルゴリズム（Berlekamp-Massey Algorithm）である[19)]．

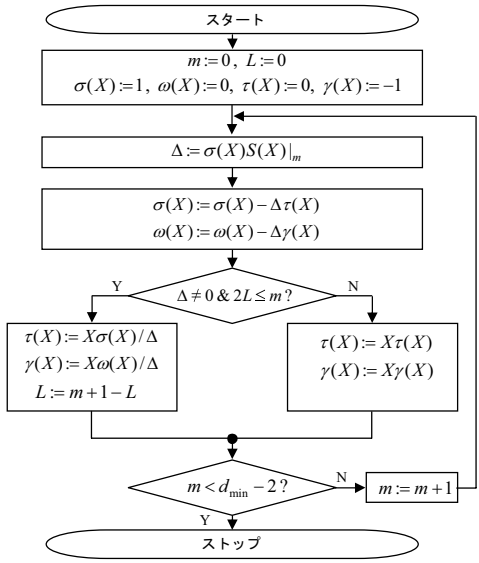

図 2･3　バーレカンプ-マッシィアルゴリズム

ここで，図 2･3 中の $\sigma(X)S(X)|_m$ は $\sigma(X)$ と $S(X)$ の積における m 次の項の係数を表す．

誤りベクトル $\boldsymbol{e}$ の非零成分が $e_{i_j},\ j = 0, 1, \cdots, t-1$ であり，誤り数 t が $d_{\min}/2$ よりも小さいとき，図 2･3 のアルゴリズムの計算結果 $\{\sigma(X), \omega(X)\}$ は前記の条件を満たすただ一つのものとなり，$\sigma(X) = \prod_{j=0}^{t-1}(1 - \alpha^{i_j}X)$，$\omega(X) = \sum_{j=0}^{t-1} e_{i_j}\alpha^{bi_j} \prod_{l=0, l\neq j}^{t-1}(1 - \alpha^{i_l}X)$ となる．したがってこのとき，ピーターソン復号法と同様に $\sigma(X)$ の根から誤り位置を推定することができる．

また，誤り値については $\omega(X)$ と $\sigma(X)$ の形式的微分 $\sigma'(X)$ を用いて次のように求めることができる．

$$e_{i_j} = -\frac{\omega(\alpha^{-l_j})}{\alpha^{(b-1)i_j}\sigma'(\alpha^{-i_j})}, \quad j = 0, 1, \cdots, t-1 \tag{2･29}$$

$\omega(X)$ は特に誤り数値多項式と呼ばれている．図 2･3 はバーレカンプ-マッシィアルゴリズムの基本形の一つであるが，この形以外にも主にハードウェア実装性を考慮した様々な変形版が考えられている．

バーレカンプ-マッシィ復号法と同様に効率的な復号法として，ユークリッド復号法（Euclid Decoding Algorithm）がよく知られている．ユークリッド復号法においてもシンドロームを係数とする多項式 $S^*(X) \triangleq \sum_{i=0}^{d_{\min}-2} s_{b+i}X^{d_{\min}-2-i}$ を用いる．与えられた $S^*(X)$ に対して，$U(X)S^*(X) \equiv R(X) \bmod X^{d_{\min}-1}$, $\deg(U) \le \lfloor (d_{\min}-1)/2 \rfloor$, $\deg(R) < \lceil (d_{\min}-1)/2 \rceil$, $\gcd(U, V) = 1$ の条件を満たす多項式組 $\{U(X), R(X)\}$ は定数倍を除いてただ一つに定まり（ただし $V(X) \triangleq (U(X)S^*(X) - R(X))/X^{d_{\min}-1}$），次のユークリッドアルゴリズムによって導くことができる．

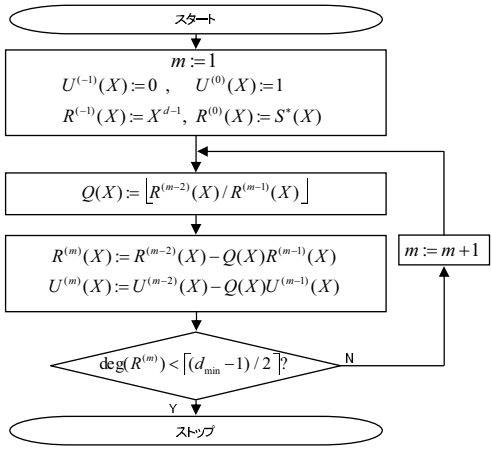

図 2･4　ユークリッドアルゴリズム

図中において $Q(X)$ は $R^{(m-2)}(X)$ と $R^{(m-1)}(X)$ の商多項式を表し，$R^{(m)}(X)$ は剰余多項式となる．

バーレカンプ-マッシィ復号法の場合と同様に，誤り数 t が $d_{\min}/2$ よりも小さいとき，図 2･4 のアルゴリズムの出力は $U(X) = \prod_{j=0}^{t-1}(X - \alpha^{i_j})$, $R(X) = -\sum_{j=0}^{t-1} e_{i_j}\alpha^{(b+d_{\min}-1)i_j} \prod_{l=0, l\neq j}^{t-1}(X - \alpha^{i_l})$ となる．$U(X)$ の根は誤り位置に相当し，誤り値は $R(X)$ と $U(X)$ の形式的微分から，式 (2･29) と同様の手順で導くことができる．ユークリッド復号法においても図 2･4 の基本形をベースに，ハードウェア実装性を考慮した変形版が考えられている．

このほかにもウェルチ-バーレカンプアルゴリズム（Welch-Berlekamp Algorithm）がよく知られている．この復号方法も誤り位置・数値多項式を算出して訂正を行うという点において前記の復号方法と同様の考え方に基づいているが，後にスダーン・グルスワミ復号法として知られるリスト復号法の基礎となる斬新な考え方を提供している．

■1 群 - 2 編 - 2 章

2-6 軟判定復号法

（執筆者：日下卓也）[2012 年 3 月 受領]

一般に，通信路へ送信される記号の集合（符号語を構成する記号の集合）と受信される記号の集合が一致する（あるいは消失も許す）復号法は硬判定復号法と呼ばれ，通信路符号の記号に関する演算に閉じた処理となるため，実装が容易で高速な処理が可能な場合が多く，広く利用されている．軟判定復号法の代表例として，限界距離復号法（本編 1-5 節参照）が挙げられる．一方，通信路から得られる受信語が通信路符号の記号の信頼度（reliability）に関する情報の軟値，つまりアナログ値またはディジタル値（例えば，2 元符号において 8 階調）の列であるという前提のもとで受信語と符号語のユークリッド距離（Euclidean distance）を利用することにより，硬判定復号法よりも優れた誤り制御性能を発揮しうる手法が軟判定復号法（soft-decisiondecoding）である．軟判定復号法の復号では通信路符号の記号ではなく，軟値の演算が必要となり，硬判定復号法に比べて実装は複雑になり，処理時間は長くなることが多いが，それに見合うだけの誤り率の改善が見込める場合が多い．本節においては軟判定復号法として，最ゆう復号法を別として最も基本的な手法としてよく知られている三つの復号法を紹介する．

その前に，これらの復号法に共通のいくつかの前提を明確にし，必要な記号の定義をしておく．まず，対象とする符号は，符号長 n，情報ビット数 k，最小（ハミング）距離 $d_{\min}$ の 2 元 $(n, k, d_{\min})$ 線形ブロック符号 C とする．加法的白色ガウス雑音通信路（AWGN）にて BPSK を用いるものとする．受信系列として n 次元の軟値ベクトル $\boldsymbol{r} = (r_1, r_2, \cdots, r_n)$ が与えられる．受信系列 $\boldsymbol{r}$ に対し，各成分をその絶対値の昇順に並べ替えた軟値系列 $\boldsymbol{r}' = (r'_1, r'_2, \cdots, r'_n)$ を考える．つまり，$0 \le i < j \le n$ なる i, j に関し，$|r'_i| \le |r'_j|$ とする．また，このベクトル $\boldsymbol{r}'$ を硬判定した 2 元ベクトルを $\boldsymbol{z}' = (z'_1, z'_2, \cdots, z'_n)$ とする．

軟判定復号法の目的は $\boldsymbol{r}$ とのユークリッド距離が最小の語（最ゆう語）あるいはそれに近い符号語を少ない計算量で求めることであり，復号法ごとにその手法に特徴がある．

2-6-1 一般化最小距離復号法（GMD: generalized minimum distance decodieng）

一般化最小距離（GMD: generalized minimum distance）復号法[20]の誤り制御特性はここで紹介するほかの軟判定復号法に比べて良くないが，軟値演算に関しては $O(d_{\min} n)$ の多項式オーダの加算または比較によって実現が可能なことが特長である．またこの復号法は対象とする符号に対する硬判定された受信語（消失を許す）に対する復号法である消失訂正復号（erasure decoding）を繰り返し用いるため，その分の論理演算も必要とする．消失訂正復号は非負整数 s, t（ただし，$d_{\min} > 2t + s$）に対して，t 個の誤りと s 個の消失を訂正可能である．その計算量は限界距離復号と同じオーダの論理演算数であるので上述の軟値演算に比べて十分に小さいコストと考えることが多い．

続いて，一般化最小距離復号法の具体的な処理手順を説明する．この復号法では，$\boldsymbol{z}'$ において，最も信頼度の低い $d_{\min} - 1$ 個のビット $z'_1, z'_2, \ldots, z_{d_{\min}}$ に着目する．次に $m \triangleq \lfloor (d_{\min} + 1)/2 \rfloor$ なる整数 m を考える．m は一般化最小距離復号法における消失訂正復号の最大繰り返し回数である．$*$ が消失ビットを表すものとし，$\boldsymbol{z}'$ に対して $d_{\min}$ が奇数の場合には

$$
\begin{aligned}
\boldsymbol{g}_1 &\triangleq (z'_1, z'_2, z'_3, z'_4, z'_5, \cdots, z'_n)\\
\boldsymbol{g}_2 &\triangleq (*, *, z'_3, z'_4, z'_5, \cdots, z'_n)\\
\boldsymbol{g}_3 &\triangleq (*, *, *, *, z'_5, \cdots, z'_n)\\
&\vdots\\
\boldsymbol{g}_m &\triangleq (*, *, \cdots, *, z'_{d_{\min}}, \cdots, z'_n)
\end{aligned}
$$

なる，また $d_{\min}$ が偶数の場合には

$$
\begin{aligned}
\boldsymbol{g}_1 &\triangleq (*, z'_2, z'_3, z'_4, z'_5, z'_6, \cdots, z'_n)\\
\boldsymbol{g}_2 &\triangleq (*, *, *, z'_4, z'_5, z'_6, \cdots, z'_n)\\
\boldsymbol{g}_3 &\triangleq (*, *, *, *, *, z'_6, \cdots, z'_n)\\
&\vdots\\
\boldsymbol{g}_m &\triangleq (*, *, \cdots, *, z'_{d_{\min}}, \cdots, z'_n)
\end{aligned}
$$

なる m 個のベクトル集合を考える．$\boldsymbol{g}_1, \boldsymbol{g}_2, \ldots, \boldsymbol{g}_m$ の順に消失訂正復号し，符号語が生成された場合に停止条件が満たされればその符号語を復号語として停止し，最後まで停止条件を満たす符号語が生成されなければ復号語は生成されず，復号失敗とする．

以上のように，消失訂正復号の繰り返し回数は最小距離の定数倍であり，論理演算と軟値演算は最小距離と符号長に関して多項式オーダの計算量となるが，誤り制御性能は軟判定復号法のなかでも低い部類となる．例えば符号長 64 程度の拡大原始 BCH 符号でも達成される誤り率は限界距離復号に近いものとなることが知られている．

2-6-2 チェイス復号法（Chase decoding）

次に紹介するチェイス復号法[21]も硬判定復号法を複数回用いる．チェイス復号法にはタイプ 1, 2, 3 の 3 種類があるが，タイプ 1 は参照されることが少ないため，本節ではタイプ 2 に関して解説する．タイプ 3 は基本構造をタイプ 2 と同一とし，用いる硬判定復号法の回数を減らしたもので，上述の一般化最小距離復号法に近い手法である．

タイプ 2 復号法は硬判定の限界距離復号法を多数回繰り返し用いることが特徴であり，上述の一般化最小距離復号法[20]と比べて計算量のオーダに根本的な差があり，達成される誤り率も符号によっては大きく改善されることが知られている．

タイプ 2 復号法でも軟値系列 $\boldsymbol{r}'$ とその硬判定 2 元ベクトル $\boldsymbol{z}'$ を用いる．また，$\tau = \lfloor d_{\min}/2 \rfloor$ なる整数 τ を求め，最も信頼度が低い τ 個のビット $z'_1, z'_2, \ldots, z_\tau$ に着目する．一般化最小距離復号法に比べて着目するビット数は半減させてある．これらのビットの復元に際し，消失訂正復号を用いるのではなく，長さ τ の 2 元ベクトルをすべて生成し，信頼度の低い τ 個の記号位置に配することにより，

$$
\begin{aligned}
\boldsymbol{c}_0 &\triangleq (0, 0, 0, 0, \cdots, 0, z'_{\tau+1}, \cdots, z'_n)\\
\boldsymbol{c}_1 &\triangleq (1, 0, 0, 0, \cdots, 0, z'_{\tau+1}, \cdots, z'_n)\\
\boldsymbol{c}_2 &\triangleq (0, 1, 0, 0, \cdots, 0, z'_{\tau+1}, \cdots, z'_n)
\end{aligned}
$$

$$\boldsymbol{c}_3 \triangleq (1,1,0,0,\cdots,0,z'_{\tau+1},\cdots,z'_n)$$
$$\vdots$$
$$\boldsymbol{c}_{2^\tau} \triangleq (1,1,1,1,\cdots,1,z'_{\tau+1},\cdots,z'_n)$$

なる，2^τ 個の 2 元ベクトルを生成する．これらのベクトルに対して 2^τ 回の限界距離復号をし，符号語が一つも生成されなければ復号失敗とし，1 個以上の符号語が生成された場合にはそのなかで $\boldsymbol{r}$ とのユークリッド距離が最も近いものを復号語とする．

復号語が生成された場合には，それが最ゆう語となる確率も高く，一般化最小距離復号法と比べて達成される誤り制御特性は良好である．しかし，限界距離復号の回数が $d_{\min}$ に対して指数オーダとなることや，復号失敗が発生し得ることがこの方式の大きな欠点である．よって，無駄な限界距離復号の省略や，消失扱いするビット数 τ を増加させるなどといった改良手法が多く提案されている．

2-6-3 順序統計量復号法（OSD: ordered statistics decodeing）

順序統計量復号法[22]（OSD: Ordered Statistics Decodeing）も軟値受信系列の各記号位置の信頼度情報を活用する点は上述の一般化最小距離復号法とチェイス復号法に類似性はあるが，符号化に基づく復号法であることが最大の特徴である．また，復号語が必ず生成されることが当該手法の有用性を高めていると考えられる．また，フォッソリエ（Fossorier）の提案以来，提案者本人を含めてその発展型アルゴリズムの研究が非常に盛んに行われている興味深い手法であり，類似する手法として A* 復号法[23]もよく知られている．

順序統計量復号法では次数と呼ばれる 0 以上の整数値 l を決めておく．そして，$\boldsymbol{r}'$ を用いて，次に述べる手順で記号位置を入れ替えた軟値系列 $\boldsymbol{r}'' = (r''_1, r''_2, \cdots, r''_n)$ をつくる．$\boldsymbol{r}'$ に関して最も信頼度の高い r'_n から降順に各成分を調べていき，k 個の信頼度の高い一次独立な成分を求め，それらを順序を保存して $r''_{n-k+1}, \cdots, r''_n$ にコピーし，残りの $n-k$ 個の成分も順序を保存して $r''_1, \cdots, r''_{n-k}$ にコピーする．これと同様の記号位置の入れ替えをした生成行列は右標準形（行列の右側が単位行列）で表現できる．次に $\boldsymbol{r}''$ を硬判定したベクトル $\boldsymbol{z}''$ を考える．つまり，$z''_{n-k+1}, z''_{n-k+2}, \ldots, z''_n$ は信頼度が高く，一次独立な k ビットとなり，誤りが生じている確率が低いと考えられる．

ここで，$z''_{n-k+1}, z''_{n-k+2}, \ldots, z''_n$ を情報ビットと考えて，対応する右標準形の生成行列を用いて符号化を行って $z'''_1, z'''_2, \ldots, z'''_{n-k}$ を生成することを考える．すると，$(z'''_1, z'''_2, \ldots, z'''_{n-k}, z''_{n-k+1}, z''_{n-k+2}, \ldots, z''_n)$ が一つ目の候補符号語となる．$l > 0$ の場合には $z''_1, z''_2, \ldots, z''_k$ のビット中，l 個以下のビットを反転した総数 $\sum_{i=0}^{l} \binom{k}{i}$ のベクトルに対する符号化をした結果の候補符号語のなかで $\boldsymbol{r}$ とのユークリッド距離が最小のものを復号語とする．通常，k が大きな符号であれば l を大きくするのは計算量の点で簡単ではないことが多く，そうされることはほとんどない．また，$l = k$ とすれば最ゆう復号となることは明らかである．

■1 群 - 2 編 - 2 章

2-7 代数幾何符号の復号法

（執筆者：阪田省二郎）[2012 年 3 月 受領]

ガロア体 $\mathcal{K}$ 上の符号 $C \subset \mathcal{K}^n$ の復号（本章 1-1, 1-5, 2-5 節 参照）では，（受信者には未知の）送信語 $\boldsymbol{c} = (c_j)\,(\in C)$ と誤り語（ベクトル）$\boldsymbol{e} = (e_j)\,(\in \mathcal{K}^n)$ に対し，受信語 $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} = (r_j)\,(\in \mathcal{K}^n)$ を与えられて，$\boldsymbol{c}$（あるいは，$\boldsymbol{e}$）を求めなければならない．代数幾何符号[17]（本章 2-4 節 参照）*は，美しい代数的な構造をもつので，それをうまく利用することによって様々の効率的な復号法が与えられている．そのなかでも，双対符号 $C^\perp$ に対する復号法が最も基本的なものであり，実用化に近い復号法としてほぼ確立されたといえる†．本節では，エルミート曲線符号の双対符号 $C^\perp$（本章 2-4 節 参照）に絞って，その基本的な復号法[24]とその高速化[17]を述べる．一般の代数曲線符号についても，ほぼ同様な復号法が成立する．

一般に，双対符号 $C^\perp$ の復号法は，誤り位置の決定と誤り値の決定の 2 段階からなる．ここで，誤り語 $\boldsymbol{e} = (e_j)$ において，$e_j \neq 0, 1 \leq j \leq n$ である各 j を誤り位置（error location）と呼び，その j に対する $e_j\,(\in \mathcal{K})$ を誤り値（error value）と呼ぶ．1 点代数曲線符号 $C^\perp$（本章 2-4 節 参照）の場合は，定義に現れた曲線上の点集合 $\mathcal{P} = \{P_j \mid 1 \leq j \leq n\}$ の部分集合 $\mathcal{E} \triangleq \{P_j \in \mathcal{P} \mid e_j \neq 0\}$ を誤り位置集合とする．誤り位置集合 $\mathcal{E}$，あるいは，それを含む $\tilde{\mathcal{E}}$ で $\tilde{t} \triangleq |\tilde{\mathcal{E}}| \leq d^\perp - 1$ であるものが求められているとき，検査行列 H の $(n-k) \times \tilde{t}$ 部分行列 $\tilde{H}$ を係数行列とするガロア体上の連立 1 次方程式 $\tilde{H}\tilde{\boldsymbol{e}} = \boldsymbol{s}$ を解くことによって，誤り値を求めることができる．ここで，$\boldsymbol{s} \triangleq H\boldsymbol{r}\,(\in \mathcal{K}^{n-k})$ は，受信語 $\boldsymbol{r}$ から得られるシンドロームである．

ガロア体 $\mathcal{K} = \mathrm{GF}(q)$ 上の 1 点代数曲線符号の復号には，曲線上の代数関数体の構造，特に，極位数の系列 $\mathcal{O}_q = \{o^{(i)} \mid 1 \leq i \leq n\}$（例えば，本章 2-4 節 中の図 2･2 参照）とそれに対応する関数の系列 $\mathcal{B}_q = \{b^{(i)} \mid 1 \leq i \leq n\}$ が重要な鍵となる．これらの系列から，主符号，双対符号の系列 $C_1 \subset C_2 \subset \cdots \subset C_n$，$C_1^\perp \supset C_2^\perp \supset \cdots \supset C_n^\perp$ が導入される．特に，整数 m, $1 \leq m \leq n$ を一つ固定し，関数空間 $\mathcal{L}_m = \langle b^{(j)} \mid 1 \leq j \leq m \rangle_{\mathcal{K}}$ によって定義される双対符号 $C_m^\perp = \{c = (c_j) \in \mathcal{K}^n \mid \sum_{1 \leq j \leq n} c_j f(P_j) = 0,\ f \in \mathcal{L}_m\}$ の復号法を扱う．ただし，$m \geq g + 1$ とする．この符号のゴッパ設計距離 $d_G^\perp = m - g + 1$（本章 2-4 節 参照）に対し，基本復号アルゴリズム（basic decoding algorithm）では，$t = \lfloor \frac{d_G^\perp - 1 - g}{2} \rfloor\,(\geq 1)$ 個以下の誤り訂正が可能である．まず，シンドロームの変種であるシンドローム行列 $S = [s_{ij}]$ を $s_{ij} \triangleq \sum_{\kappa=1}^{n} r_\kappa b^{(i)}(P_\kappa) b^{(j)}(P_\kappa),\ 1 \leq i, j \leq n$ によって定義し，それから定められる関数空間 $K_{ij}(\boldsymbol{r}) \triangleq \{f = \sum_{\kappa=1}^{j} u_\kappa b^{(\kappa)} \in \mathcal{L}_j \mid \sum_{\kappa=1}^{j} s_{\kappa\lambda} u_\kappa = 0,\ 1 \leq \lambda \leq i\},\ 1 \leq i, j \leq n$ を導入する．$o^{(i)} + o^{(j)} \leq o^{(l)}$ ならば，$b^{(i)} b^{(j)} \in \mathcal{L}_l$ であり，したがって，$K_{ij}(\boldsymbol{r}) = K_{ij}(\boldsymbol{e})$ である．なお，$b^{(i)} b^{(j)} = b^{(l)}$ である場合は，$o^{(i)} + o^{(j)} = o^{(l)}$ であって，s_{ij} は，シンドロームの値 $s_l(\boldsymbol{r}) \triangleq \sum_{\kappa=1}^{n} r_\kappa b^{(l)}(P_\kappa)$ に等しい．しかし，$b^{(i)} b^{(j)} = b^{(l)}$ でなくとも，$o^{(i)} + o^{(j)} = o^{(l)}$ である場合は，定義曲線式に由来する関数の 1 次従属関係 $b^{(i)} b^{(j)} = b^{(l)} + \sum_{\kappa<l} c_\kappa b^{(\kappa)}$ に基づいて，s_{ij} の値は，$s_l(\boldsymbol{r})$ と $s_\kappa(\boldsymbol{r}), \kappa < l$ から定められる．このように，一定の l に対し，$o^{(i)} + o^{(j)} = o^{(l)}$ である (i, j) に対応するシンドローム成分 s_{ij} は互いに共役（conjugate）であるという．誤

* 本節の記述は，すべて 本章 2-4 節「代数幾何符号」の内容を前提とする．

† 主符号に対する復号法には，リスト復号（本章 2-8 節 参照）に基づくものがある．

り位置集合 $\mathcal{E}$ ($\subset \mathcal{P}$) を直接扱う代わりに，関数空間 $\mathcal{L}_j$ 内に限定した誤り位置関数空間 $\mathcal{L}_j(\mathcal{E}) \triangleq \{f \in \mathcal{L}_j \mid f(P_\kappa) = 0,\ P_\kappa \in \mathcal{E}\}$ を考える．$o^{(i)} + o^{(j)} \le o^{(l)}$ として，誤り個数，すなわち，重み $w_H(\boldsymbol{e})$ が符号 $C_i^\perp$ の最小距離 $d(C_i^\perp)$ より小さいならば，$\mathcal{L}_j(\mathcal{E}) = K_{ij}(\boldsymbol{r})$ が成り立つので，誤り個数 $w_H(\boldsymbol{e})$ が上記の t 以下であるとき，$j = t+1, i = \lfloor \frac{m}{2} \rfloor$ の場合の $K_{ij}(\boldsymbol{r})$ を，連立 1 次方程式を解くことによって求めることができる．それは，誤り位置関数空間 $\mathcal{L}_j(\mathcal{E})$ に等しいから，その元である複数の関数の共通零点を求めれば，誤り位置が得られる．

極位数の性質をうまく利用すると，一般にゴッパ設計距離 $d_G^\perp$ より強い最小距離の下界であるフェン-ラオ設計距離（Feng-Rao designed distance）$d_{FR}^\perp$ が以下のように定められ，$t_{FR} \triangleq \lfloor \frac{d_{FR}^\perp - 1}{2} \rfloor$ 個以下の誤りを訂正する方法が，基本復号アルゴリズムを拡張したかたちで与えられる[25]．$d_{FR}^\perp \ge d_G^\perp$ なので，この復号法により，$t_G \triangleq \lfloor \frac{d_G^\perp - 1}{2} \rfloor$ 個以下の誤り訂正が可能である．非負整数 $l, l \ge 0$ に対し，共役なシンドローム成分 s_{ij} に対応する整数対 (i, j) の集合 $N_l \triangleq \{(i, j) \mid o^{(i)} + o^{(j)} = o^{(l+1)}\}$ とその濃度 $\nu_l \triangleq |N_l|$ を考えると，符号 $C_l^\perp$ のフェン-ラオ設計距離は $d(l) \triangleq \min\{\nu_\lambda \mid \lambda \ge l\}$ で定義される．一般に，ベクトル $\boldsymbol{c} \in C_l^\perp \setminus C_{l+1}^\perp$ が，$w(\boldsymbol{c}) \ge \nu_l$ を満たすことから，$d(C_l^\perp) \ge d(l)$ が示される．$q = 16$（$\rho = 4$）のときの，各 $l, 1 \le l \le n$ に対するエルミート曲線符号 $C_l^\perp$ について，フェン-ラオ設計距離 $d(l)$ の値を表 2･3 に示す．

表 2･3　フェン-ラオ設計距離 $d(l)$

l	1	2	3	4	5	6	⋯	12	13	14	15	16	17	⋯
$d(l)$	2	2	3	3	3	4	⋯	8	8	9	10	12	12	⋯

包含関係 $\{i \in \mathbf{Z}_0 \mid i \ge c\} \subset O$ が成り立つ最小の正整数を c とおくと，$l > 2c - g - 2$ のとき，$d_{FR}^\perp (\triangleq d(l)) = d_G^\perp$ となることが証明される．表 2･3 の場合は，$c = 12$ であり，$l \ge 17$ において $d_{FR}^\perp = d_G^\perp$ となる．例えば，符号 $C_{18}^\perp$ は同一のゴッパ設計距離とフェン-ラオ設計距離 13 をもつ．誤り語 $\boldsymbol{e}$ に対応する $s_i(\boldsymbol{e}) \triangleq \sum_{\kappa=1}^n e_\kappa b^{(i)}(P_\kappa), i \le l$ の値は受信語 $\boldsymbol{r}$ から得られるシンドローム $s_i(\boldsymbol{r})$ の値に等しく，基本復号アルゴリズムでは，これらの値を用いることによって $\lfloor \frac{d_G^\perp - 1 - g}{2} \rfloor$ 個以下の誤り訂正が可能であった．今後は，誤り語から定義される $s_i \triangleq s_i(\boldsymbol{e}), 1 \le i \le n$，及び，$s_{ij} \triangleq \sum_{\kappa=1}^n e_\kappa b^{(i)}(P_\kappa) b^{(j)}(P_\kappa), 1 \le i, j \le n$ を，改めて，シンドロームと呼ぶことにし，s_i, $i \le m$ を既知シンドローム，$s_i, i > m$ を未知シンドローム（unknown syndrome）という．このような未知シンドロームの値が分かると，基本復号アルゴリズムに比べて $\lfloor \frac{g}{2} \rfloor$ だけ多くの個数の誤り訂正が可能となる．各 $(i, j) \in N_m$ に対し，$s_{i'j'}, i' \le i, j' \le j, (i', j') \ne (i, j)$ はすべて既知であるが，s_{ij} は未知である．行列 $S = [s_{\kappa\lambda}], 1 \le \kappa, \lambda \le n$ の部分行列 $S(i, j) \triangleq [s_{\kappa\lambda}]$, $\kappa \le i, \lambda \le j$ を考える．三つの部分行列 $S(i-1, j-1), S(i-1, j), S(i, j-1)$ の階数が等しいとき，未知シンドロームの候補値 $\tilde{s}_{ij}$ を，部分行列 $S(i, j)$ の階数が上記の三つの部分行列の階数と等しくなるように一意に定めることができる．この候補値 $\tilde{s}_{ij}$ は真のシンドローム値 s_{ij} に等しく**正しい**こともあれば，等しくなく**間違っている**こともあり得る．$w_H(\boldsymbol{e}) \le \frac{\nu_m - 1}{2}$ であるとき，候補値のなかで正しいものの個数が間違っているものの個数より大きくなるという事実を利用し，未知シンドロームの候補値 $\tilde{s}_{ij}$ の間で多数決をとることによって，正しいシンドロームの値 s_{ij} を求めることができる．これら共役なシンドロームの一組のなかに s_{m+1} が含まれている．この手続きを繰り返して，$s_{m+1}, \cdots, s_{m+g}$ を求めれば，t_{FR} 個の誤り訂正が

可能となる．

基本復号アルゴリズムの計算量は，その主要な手続きである連立 1 次方程式を解くためのガウス（Gauss）消去法の計算量 $O(n^3)$ に等しいのに対し，計算量 $O(n^{\frac{7}{3}})$ でフェン-ラオ設計距離までの復号を可能とする高速復号法[27]が知られている．基本復号アルゴリズムでは，入力データとして，シンドローム行列を用いているが，それは冗長なデータであり，関数空間の基底関数から得られる元のシンドローム $s_i, 1 \le i \le m$ を直接無駄なく使う方法がある．エルミート符号の場合，関数列 $\mathcal{B}_q$ が座標関数 x, y のべき関数（単項式）$\boldsymbol{x^i} \triangleq x^i y^j$（$\boldsymbol{i} = (i, j)$）からなり，かつ，それらが極位数の昇順で決まる全順序 $\le_T$（グレーブナ（Gröbner）基底の理論での単項式順序）に従って与えられ，その結果，$\Sigma \triangleq \{\boldsymbol{i} = (i, j) \in \mathbf{Z}_0^2 \mid j \le \rho - 1\}, \Sigma(\mu) \triangleq \{\boldsymbol{i} = (i, j) \in \Sigma \mid \rho i + (\rho + 1)j \le \mu\}$ とおくと，2 次元シンドローム配列（two-dimensional syndrome array）$s = (s_{\boldsymbol{i}}), \boldsymbol{i} = (i, j) \in \Sigma(\mu)$ が入力データとなる*．配列 $s = (s_{\boldsymbol{i}})$ は，より広く $\mathbf{Z}_0^2$ 全体，あるいは，倍の大きさの部分集合 $2\Sigma \triangleq \{\boldsymbol{i} + \boldsymbol{j} \in \mathbf{Z}_0^2 \mid \boldsymbol{i}, \boldsymbol{j} \in \Sigma\}, 2\Sigma(\mu) \triangleq \{\boldsymbol{i} = (i, j) \in 2\Sigma \mid \rho i + (\rho + 1)j \le \mu\}$ に拡張することができる．ここで，定義曲線方程式による 1 次従属関係が成立している．すなわち，$\boldsymbol{i}' \in 2\Sigma$ におけるシンドローム値 $s_{\boldsymbol{i}'}$ は，$o(\boldsymbol{x^i}) = o(\boldsymbol{x^{i'}})$ を満たす $\boldsymbol{i} \in \Sigma$ における値 $s_{\boldsymbol{i}}$ と有限個の値 $\{s_{\boldsymbol{j}} \mid \boldsymbol{j} \in \Sigma, o(\boldsymbol{x^j}) < o(\boldsymbol{x^i})\}$ によって定められる．$q = 16$（$\rho = 4$）のエルミート符号 $C_{18}^{\perp}$ は 6 個誤り訂正可能であるが，例えば，誤り位置と誤り値の組合せが $(\alpha^{14}, \alpha^{14})|\alpha^{12}$, $(\alpha^{13}, \alpha^{13})|\alpha^4$, $(\alpha^{11}, \alpha^{11})|\alpha^7$, $(\alpha^7, \alpha^7)|\alpha^8$, $(1, \alpha)|\alpha^9$, $(0, 0)|\alpha^9$ である 6 個誤りの場合，シンドローム配列は，図 2･5（本章 2-4 節 中の図 2･2 の 2Σ 上への拡張）に示した関数 $x^i y^j$ の極位数 $o(x^i y^j)$ の配列に対応して，図 2･6 のようになる．ここで，曲線の定義式 $x^5 = y + y^4$ に対応する関係 $s_{i+5,j} = s_{i,j+1} + s_{i,j+4}$ が成立している．

$i \backslash j$	0	1	2	3	4	5
0	0	5	10	15	20	·
1	4	9	14	19	(24)	
2	8	13	18	23*		
3	12	17	22			
4	16	21				
5	20	·				
6	(24)					

図 2･5　極位数の配列

$i \backslash j$	0	1	2	3	4	5
0	α	α^2	α^9	α^5	α^5	·
1	α^{14}	α^4	α^{10}	α^2	∘	
2	α^{11}	α^{11}	α^8	α^{10}		
3	α^4	α^6	α^5			
4	1	α^{12}				
5	α	·				
6	∘					

図 2･6　シンドローム配列の例

この 2 次元シンドローム配列 $s_{\boldsymbol{i}}, \boldsymbol{i} \in 2\Sigma$ に対して，多数決論理を併用した BMS アルゴリズム（BMS algorithm）[26, 27] を適用することによって，誤り位置関数空間（この場合，イデアル）のグレーブナ基底（Gröbner basis）を高速に求めることができる．

* $m \ge g + 1$ のとき，$\mu = m + g - 1$ である．

■1 群 - 2 編 - 2 章

2-8 リスト復号

（執筆者：松本隆太郎）[2012 年 3 月 受領]

本節では，リード-ソロモン符号（Reed-Solomon code）[本章 2-3 節 参照] 及びその部分体部分符号である BCH 符号（BCH code）[本章 2-2 節 参照]，リード-マラー符号（Reed-Muller code）[本章 1-7 節 参照] に対する代表的なリスト復号（list decoding）アルゴリズムであるグルスワミ-スーダン復号法（Guruswami-Sudan decoding）を説明する．リスト復号とは送信符号語の候補を複数算出する復号である．このリスト復号法を記述するために，以下のような標準的ではない方法で GF(q) 上の (n,k) リード-ソロモン符号を定義する必要がある．$\alpha_1,\ldots,\alpha_n$ を GF(q) の相異なる元とする．(n,k) リード-ソロモン符号を $C \triangleq \{(f(\alpha_1),\ldots,f(\alpha_n)) \mid f(X)$ は GF(q) に係数をもつ次数 k 未満の多項式 $\}$ によって定義する．このように定義した C は一般に巡回符号 [本章 2-1 節 参照] ではないが，ある $\beta \in \mathrm{GF}(q)$ が存在して $\beta^n = 1$ かつ $\alpha_i = \beta^i$ と表現できる場合は C は巡回符号となる．また $n = q$ と選び $\alpha_1,\ldots,\alpha_n$ として GF(q) のすべての元を選んだ場合に C は 1 次伸長リード-ソロモン符号 [本章 2-3 節 参照] になる．

通信路の入出力アルファベットは GF(q) であるとし，受信語を $\boldsymbol{r} \in \mathrm{GF}(q)^n$ とする．グルスワミ-スーダン復号法は受信語 $\boldsymbol{r}$ からハミング距離が t 以内にある複数の符号語 $\boldsymbol{c} \in C$ をすべて算出する．まずアルゴリズムの詳細を記述し，次に訂正できる誤りの数 t を評価する．これ以降特に断らない限り多項式の係数はすべて GF(q) に属するものとする．

2 変数多項式 $Q(X,Y)$ の根として符号語を求める．アルゴリズムのパラメータとして t のほかに ℓ と重複度 m が与えられているものとする．ℓ, m, t の選び方については後述する．$Q(X,Y)$ が点 $(x,y) \in \mathrm{GF}(q)^2$ において m 以上の重複度（multiplicity）をもつとは，$i+j<m$ ならば $Q(X+x,Y+y)$ のなかの X^iY^j の係数が 0 であることを指す．

受信語 $\boldsymbol{r} = (r_1,\ldots,r_n)$ が与えられたときに，まず以下の条件を満たす非零な $Q(X,Y) = Q_{\lfloor \ell/(k-1) \rfloor}(X)Y^{\lfloor \ell/(k-1) \rfloor} + Q_{\lfloor \ell/(k-1) \rfloor - 1}(X)Y^{\lfloor \ell/(k-1) \rfloor - 1} + \cdots + Q_1(X)Y + Q_0(X)$ を求める．

1. すべての $i = 1,\ldots,n$ について $Q(X,Y)$ の点 (α_i, r_i) における重複度は m 以上である．
2. $Q_i(X)$ の次数は $\ell - (k-1)i$ 以下．

リード-ソロモン符号の符号語 $\boldsymbol{c} = (c_1,\ldots,c_n)$ には必ず次数 $k-1$ 以下の多項式 $f(X)$ が対応し $c_i = f(\alpha_i)$ をすべての i について満たす．符号語 $\boldsymbol{c}$ の受信語 $\boldsymbol{r}$ とのハミング距離が t 以下であるならば，$n-t$ 個以上の添字 i において $r_i = f(\alpha_i)$ が成立する．もし $r_i = f(\alpha_i)$ ならば，$f(Z+\alpha_i) - r_i = Zg(Z)$ と書ける．$Q(X,Y)$ に対する条件 1 に $X = Z, Y = Zg(Z)$ を代入することにより，Z^m は $Q(Z+\alpha_i, Zg(Z)+r_i) = Q(Z+\alpha_i, f(Z+\alpha_i))$ を割り切り，$Z = X - \alpha_i$ を代入すると $(X-\alpha_i)^m$ が $Q(X, f(X))$ を割り切る．したがって $\prod_{r_i = f(\alpha_i)} (X-\alpha_i)^m$ は $Q(X, f(X))$ を割り切る．このことは $Q(X, f(X))$ の次数が $m(n-t)$ 以上であるか $Q(X, f(X)) = 0$ を意味する．$f(X)$ の次数はたかだか $k-1$ なので $Q(X, f(X))$ の次数はたかだか ℓ である．もし

$$\ell < m(n-t) \tag{2･30}$$

を満たすように $Q(X,Y)$ を選べば $Q(X, f(X)) = 0$ であるから，$Q(X,Y)$ を Y の 1 変数多項式

と見たときの 1 次の因子 $Y - f(X)$ をすべて求めることにより受信語からハミング距離が t 以内の符号語を求めることができる．1 次の因子を効率良く計算する手続きはこの節の末尾で述べる．

次にパラメータの組 ℓ, m, t を n, k から求める考え方を説明する．十分大きく選んだ重複度 m について以下のように誤りの数 t を定める．$Q(X, Y)$ に対する条件 1 は $n\binom{m+1}{2}$ 個の一次制約からなる．$Q(X, Y)$ の係数を一次方程式の未知変数とみたとき，ℓ を定めると未知変数の数が決まる．未知変数の数が一次制約の個数 $n\binom{m+1}{2}$ よりも大きくなるように ℓ を定める．ℓ を定めれば式 (2･30) より訂正できる誤りの数 t を計算できる．m を十分大きくとればこの考え方に従って $t = \lceil n - 1 - \sqrt{n(k-1)} \rceil$ 個の誤りを訂正できることが分かる．また一般に t 個の誤りを訂正するためには重複度 m を

$$1 + \left\lfloor \frac{(k-1)n + \sqrt{(k-1)^2 n^2 + 4((n-t)^2 - (k-1)n)}}{2((n-t)^2 - (k-1)n)} \right\rfloor \tag{2･31}$$

以上に取ればよい．計算の詳細は文献 28) にある．また式 (2･31) は必要な重複度の上界式であり，実際に必要な重複度は式 (2･31) よりも小さい．リスト復号と標準的復号で訂正できる誤りの数を図 2･7 に図示した．図 2･7 において，縦軸は訂正できる誤りの数であり横軸は符号の次元 k である．

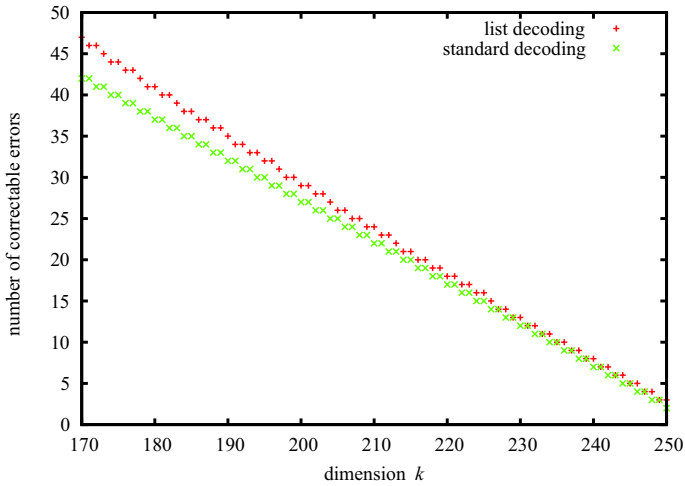

図 2･7　GF(256) 上の $(255, k)$ リード－ソロモン符号が訂正できる誤りの数．

次に Y に関する 1 変数多項式とみなした $Q(X, Y)$ から 1 次の因数 $Y - f(X)$ を求める手順を文献 29) にならって記述する．より高速な手順は文献 30) で提案されている．GF(q) を係数とする次数 k の既約多項式 $p(X)$ を一つ選ぶ．$p(X)$ は原始多項式である必要はない．本章 1-3 節で記述されているとおり，GF(q) を係数とする多項式 $f(X)$ を $p(X)$ で割った剰余 $\bar{f}$ は GF(q^k) の元とみなせる．同様に，$Q(X, Y)$ を $p(X)$ で割った剰余 $\bar{Q}(Y)$ は GF(q^k) を係数とす

る Y の 1 変数多項式とみなせる．更に，もし $Y - f(X)$ が $Q(X,Y)$ を割り切るならば，$Y - \bar{f}$ は $\bar{Q}(Y)$ を割り切る．$p(X)$ の次数が k であることから $\bar{f}$ から $f(X)$ を復元することができる．したがって符号語に対応する $f(X)$ は $\bar{Q}(Y)$ を因数分解することにより得られる．有限体を係数とする 1 変数多項式の因数分解アルゴリズムはよく知られていて，例えば文献 31) にある．

BCH 符号及びリード-マラー符号はリード-ソロモン符号の部分符号である[32]から，上記の手続きをそのままこれらの符号に適用することができる．しかしそのような単純な適用はこれらの符号が部分符号である事実を有効に活用していない．狭義 BCH 符号については，リード-ソロモン符号の部分体部分符号である事実を活用して，

$$\left\lfloor \frac{n - \sqrt{n(n-2\delta)}}{2} - 1 \right\rfloor$$

個までの誤りを訂正できるアルゴリズムが文献 33) で提案されている．ただし δ は BCH 符号の設計距離である．また，同一の文献において巡回リード-ソロモン符号のリスト復号の計算量を削減する手法も提案されている．なお，本節で定義したリード-ソロモン符号は巡回符号とは限らない．

また，本節で述べた復号法の入力は一つのベクトル $\boldsymbol{r}$ である．これは通常複素数の列として与えられる受信信号を硬判定して得られる．軟判定を行った方が復号誤り率が減少することがよく知られているが [本章 2-6 節 参照]，軟判定で得られる情報を用いてリスト復号を行う方法をケッター（Kötter）とバーディ（Vardy）が提案している[34]．軟判定を用れば受信信号が与えられたときの各々のベクトル $\boldsymbol{c} \in \mathrm{GF}(q)^m$ が送信された事後確率が得られる．これらのベクトル $\boldsymbol{c}$ とその事後確率の組から 2 変数多項式 $Q(X,Y)$ が根をもつべき点 (x_i, y_i) 及びその点における重複度 m_i を巧みに定めると，$(255, 144, 112)$ リード-ソロモン符号を 256QAM 信号点配置とともに AWGN 通信路で用いたときに，10^{-5} のブロック誤り確率を達成するために必要な SNR が一般化最小距離（GMD）復号法 [本章 2-6 節 参照] 及び硬判定を行うリスト復号を用いた場合に比べて約 1dB 削減されることが知られている[34]．

■参考文献

1) W.W. Peterson and E.J. Weldon, Jr., “Error-Correcting Codes,” Second Edition, MIT Press, 1972.
2) S.B. Wicker, “Error Control Systems for Digital Communication and Storage,” Prentice-Hall, 1995.
3) T.K. Moon, “Error Correction Coding : Mathematical Methods and Algorithms,” John Wiley & Sons, 2005.
4) S. Lin and D.J. Costello, Jr., “Error Control Coding,” Second Edition, Prentice-Hall, 2004.
5) F.J. MacWilliams and N.J.A. Sloane, “The Theory of Error-Correcting Codes,” North-Holland, 1977.
6) R.E. Blahut, “Algebraic Codes for Data Transmission,” Cambridge University Press, 2003.
7) W.C. Huffman and V. Pless, “Fundamentals of Error-Correcting Codes,” Cambridge University Press, 2003.
8) R.M. Roth, “Introduction to Coding Theory,” Cambridge University Press, 2006.
9) T. Kasami and S. Lin, “The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed-Solomon codes over GF(2^m) with generator polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$,” Linear Algebra and Its Applications, vol.98, pp.291–307, 1988.
10) I. Blake and K. Kith, “On the complete weight enumerator of Reed-Solomon codes,” SIAM Journal on Discrete Math., vol.4, pp.164–171, 1991.

11) 常盤欣一朗，田中初一，“リードソロモン符号の完全重み分布の導出に関する一考察,” 電子情報通信学会論文誌 A, vol.J75-A, no.11, pp.1746–1751, 1992.
12) 常盤欣一朗，田中初一，“リードソロモン符号の完全重み分布の導出法の改良,” 電子情報通信学会論文誌 A, vol.J77-A, no.9, pp.1276–1283, 1994.
13) M.A. Tsfasman and S.G. Vlăduţ, “Algebraic-Geometric Codes,” Kluwer Publ., Dordrecht, 1991.
14) V.D. Goppa, “Codes associated with divisors,” Problemy Peredachi Informatsii, vol.13, no.1, pp.33–39, 1977.
15) V.D. Goppa, “Codes on algebraic curves,” Dokl. Akad. Nauk SSSR, vol.24, pp.170–172, 1981.
16) M.A. Tsfasman, S.G. Vlăduţ, and T. Zink, “Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound”, Math. Nachr., vol.109, pp.21–28, 1982.
17) T. Høholdt, J.H. van Lint, and R. Pellikaan, “Algebraic geometry codes,” in Handbook on Coding Theory (Eds. V.S. Press, W.C. Huffman), Springer, §10, pp.871–961, 1998.
18) A. Garcia and H. Stichtenoth, “A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound,” Invent. Math., vol.121, pp.211–222, 1995.
19) E. R. Berlekamp “Algebraic Coding Theory,” revised 1984 ed., Aegean Park Press, 1984.
20) G.D. Forney, Jr., “Generalized Minimum Distance Decoding,” IEEE Trans. Inf. Theory, vol.IT-12, pp.125–131, Apr. 1966.
21) D. Chase, “A New Class for Decoding Block Codes with Channel Measurement Information,” IEEE Trans. Inf. Theory, vol.IT-18, pp.170–182, Jan. 1972.
22) M.P.C. Fossorier and S. Lin, “Soft-decision decoding of linear block codes based on ordered statistics,” IEEE Trans. Inf. Theory, vol.41, pp.1379–1396, Sep. 1995.
23) Y.H.S. Han, C.R.P. Hartman, and C.C. Chen, “Efficient priority first search maximum likelihood soft-decision decoding of linear block cods,” IEEE Trans. Inf. Theory, vol.39, pp.1514–1523, Sep. 1993.
24) A.N. Skorobogatov and S.G. Vlăduţ, “On the decoding of algebraic-geometric codes,” IEEE Trans. Inf. Theory, vol.36, pp.1051–1060, 1990.
25) G.L. Feng and T.R.N. Rao, “Decoding of algebraic-geometric codes up to the designed distance,” IEEE Trans. Inf. Theory, vol.39, pp.37–45, 1993.
26) S. Sakata, “Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array,” J. Symbol. Comp., vol.5, pp.321–337, 1988.
27) S. Sakata, H.E. Jensen, and T. Høholdt, “Generalized Berlekamp-Massey decoding of algebraic geometric codes up to half the Feng-Rao bound,” IEEE Trans. Inf. Theory, vol.41, pp.1762–1768, 1995.
28) V. Guruswami and M. Sudan, “Improved decoding of Reed-Solomon and algebraic-geometry codes,” IEEE Trans. Inf. Theory, vol.45, no.6, pp.1757–1767, Sept. 1999.
29) J. Justesen, T. Høholdt（著）, 阪田省二郎, 栗原正純, 松井 一, 藤沢匡哉（訳）, “誤り訂正符号入門,” 森北出版, 2005.
30) R.M. Roth and G. Ruckenstein, “Efficient decoding of Reed-Solomon codes beyond half the minimum distance,” IEEE Trans. Inf. Theory, vol.46, no.1, pp.246–257, Jan. 2000.
31) E. Kaltofen and V. Shoup, “Subquadratic-time factoring of polynomials over finite fields,” Mathematics of Computation, vol.67, no.223, pp.1179–1197, July 1998.
32) R. Pellikaan and X.-W. Wu, “List decoding of *q*-ary Reed-Muller codes,” IEEE Trans. Inf. Theory, vol.50, no.4, pp.2809–2825, Apr. 2004.
33) Y. Wu, “New list decoding algorithms for Reed-Solomon and BCH codes,” IEEE Trans. Inf. Theory, vol.54, no.8, pp.3611–3630, Aug. 2008.
34) R. Koetter and A. Vardy, “Algebraic soft-decision decoding of Reed-Solomon codes,” IEEE Trans. Inf. Theory, vol.49, no.11, pp.679–682, Nov. 2003.