コンパクトディスクから流れる数学のメロディー

——デジタルと符号理論

桂　利行

0　序

本稿は, 2000年12月24日に湘南国際村センターで行った「現代数学入門市民講座」の予稿に基づいている. 湘南国際村センターは, JRの逗子駅からバスで約３０分の小高い丘の上にあり, 見晴しのよい, 設備のよく整った会議場である. この講座は, 日本数学会, 湘南国際村協会, かながわ学術研究交流財団の主催で毎年行われており, 神奈川県教育委員会と湘南国際村倶楽部が後援している. 今回の参加者は約100名. 10代から60才以上の方まで幅広い年令層にわたっていた. クリスマスイブの午後であったにもかかわらず, 熱心な聴衆に恵まれ, とても気分よく話をすることができた. 講演後のアンケートに75名の方が回答をよせられたが, 「いい勉強でなつかしかった.」などという感想を述べられた方もおられ, このような公開講座の必要性を肌で感じる良い機会となった. 講演にはOHPを用いたが, この誌上でそれを再現することはできないので, 配付した予稿を修正し, 参考文献を大幅に拡充したものをここに掲載させていただくことにした. 参考文献のリストは, 数学の立場から符号理論を学ぶのに有用と思われる文献を, 私見によって選んだものであり, 符号理論に関する主要な文献を網羅したものではないことをお断りしておく.

1　デジタルの数学

コンピュータの発達とともにデジタルがアナログをおさえて急速に普及してきた. CD, CD-ROM, カメラ, ビデオを始め最近では電話, ビデオカセットデッキ, テレビに至るまでデジタル化の波は押し寄せている. そのようなデジタル機器に欠かせない数学が符号理論である. デジタル信号に起こりがちな小さな誤りを訂正するこの理論によって, デジタル機器の安定した作動が保証される.

CDの場合には, 凹凸のある螺旋状の軌道が作られており, レーザー光線をあて, 反射光によって凹凸をチェックする仕組みになっている. 平坦な部分が0, 高さの変化する位置を1としてデジタル化してある. CDには小さな傷はつきものであるから, これによって生じるデジタルの誤りを修正する必要があり, その修正のために**誤り訂正符号**が組み込まれている.

誤り訂正符号の原理をわかりやすく説明するために, ロケットを飛ばして木星の写真をとり, その映像を地球に送る場合を考えよう. 写真はデジタル信号で地球に送られる. その信号が通信経路の途中で何の障害もなく地球にとどけば, 正確な写真が再現されるであろう. しかし, 途中で妨害を受け地球で受信された信号がもとのものとは違っている可能性も少ない確率ではあるが存在する. そこで誤り訂正符号を組み込んで, 受信された信号から正しい情報をよみとり, 正確な写真を再現するのである.

簡単な例をあげよう. 信号は, 数字0と1からなるとする. 送信したい1つの信号が$(0,1,0)$であるとき, 同じ数字を3個ずつ重ねて送ることにする. つまり, この例ではこの信号を

$$(0,0,0,1,1,1,0,0,0)$$

として送信する. このように無駄な情報を追加しておけば, どこか1箇所でエラーが生じても, 多数決でもとの信号が再現できるわけである. たとえば

$$(0,1,0,1,1,1,0,0,0)$$

なる信号を受信した場合もとの信号は

$$(0,0,0,1,1,1,0,0,0)$$

であったことが高い確率で推定されるであろう.

このように, 余分な情報を付け加えることによって誤りをチェックするという考え方は身近なところでも用いられている. たとえば受験番号で2000A, 2001B, 2002Cというような番号付けがしばしば用いられるが、これらの番号付けにおいてA, B, Cなどは余分な情報である. しかし, たとえば2002Cを過って2000Cとコンピュータに入力したとすれば, そのような番号は存在しないから, 数字の入力を過ったことがチェックできる. このように誤りをチェックするシステムを**誤り検出符号**という.

CDや写真を送る場合には, 誤りを検出するだけではなく, 誤りを訂正するシステムが必要になる. このような誤り訂正符号の理論の基礎になるのは有限体という代数系に基づく数学である. この講座では有限体とはどのような代数系であるかという話から始める. それに基づいて符号理論がどのように構成され, 誤り訂正がどのような原理で行われるかについて, その数学的側面をお話をしたい.

2 有限体

有理数全体の集合 $\mathbf{Q}$ を考える. その和と積については小学校以来慣れ親しんできた. 和と積の性質を抽出すれば次のようになるであろう.

$a, b, c \in \mathbf{Q}$ とする.

(I) (和 $+$ に関して)

(i) $(a+b)+c = a+(b+c)$

(ii) (0 元の存在) 任意の $a \in \mathbf{Q}$ に対し $0+a = a+0 = a$ となる元 0 が存在する.

(iii) (和に関する逆元の存在) $a \in \mathbf{Q}$ に対し $a+a' = a'+a = 0$ となる元 $a' \in \mathbf{Q}$ が存在する.

(iv) $a+b = b+a$

(II) (積 $\cdot$ に関して)

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(ii) (単位元の存在) 任意の $a \in \mathbf{Q}$ に対し $1 \cdot a = a \cdot 1 = a$ となる元 1 が存在する.

(iii) (積に関する逆元の存在) $b \in \mathbf{Q}$, $b \neq 0$ に対し $b \cdot b' = b' \cdot b = 1$ となる元 $b' \in \mathbf{Q}$ が存在する.

(iv) $a \cdot b = b \cdot a$

(III) (分配法則)

(i) $(a+b) \cdot c = a \cdot c + b \cdot c$

(ii) $a \cdot (b+c) = a \cdot b + a \cdot c$

(積を表す記号 $\times$ や $\cdot$ はしばしば省略される.)

有理数を扱う場合には, これらの性質は, 当然のこととして用いられ計算がなされるから, 特別に意識されることは少ないが, 計算の基礎となる大切なものである. そこで, これらの性質をもちいて次のように体の概念を定義する.

定義 2.1 集合 K に和 $+$ と積 $\cdot$ が定義されていて, これらの性質 (I)(II)(III) を充たす時, K を**体**という.

有理数全体の集合 $\mathbf{Q}$, 実数全体の集合 $\mathbf{R}$, 複素数全体の集合 $\mathbf{C}$ は, その和, 積によって体になる. 整数全体の集合 $\mathbf{Z}$ は, 性質 (II)(iii) を充たさないので体にはならない.

$\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ などの体の例では, それぞれ無限個の元を含んでいる. それでは, 有限個の元しか含まない体（有限体）は存在するのであろうか. 1830 年, フランスの若き数学者ガロワ (E. Galois: 1811-1832) は有限体に関する論文「数の理論について (Sur la théorie des nombres)」を発表した. 有限体は, 発見者にちなんでガロワ体ともよばれている.

まず, 簡単な場合を考えてみよう. 2 元からなる集合 $F = \{\bar{0}, \bar{1}\}$ をとり, 和を

$$\bar{0} + \bar{0} = \bar{0}, \quad \bar{0} + \bar{1} = \bar{1},$$
$$\bar{1} + \bar{0} = \bar{1}, \quad \bar{1} + \bar{1} = \bar{0}.$$

積を

$$\bar{0} \cdot \bar{0} = \bar{0}, \quad \bar{0} \cdot \bar{1} = \bar{0},$$
$$\bar{1} \cdot \bar{0} = \bar{0}, \quad \bar{1} \cdot \bar{1} = \bar{1}.$$

と定義する. これによって F は体になる. このようにして 2 元からなる体が構成できる.

以上の構成を一般化しよう. p をある素数とする:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \cdots.$$

整数を p で割った余りでグループに分ける. つまり, 割った余りが等しければ同じ類に入れる. このようにすれば, 余りの可能性は $0, 1, \cdots, p-1$ で, p 個の類ができる. その類の集合を $\mathbf{Z}/p\mathbf{Z}$ と書く. 整数 n を含む類を $\bar{n}$ と書くと,

$$\mathbf{Z}/p\mathbf{Z} = \{\bar{0}, \bar{1}, \cdots, \overline{p-1}\}$$

となる. この集合に和と積を

$$\bar{a} + \bar{b} = \overline{a+b}, \ \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

によって定義すれば, $\mathbf{Z}/p\mathbf{Z}$ は体になる. このようにして得られる体を $\mathbf{F}_p$ と書く. これは, p 個の元を持つ有限体になる.

注意 2.2 先の体の例 F は, $p = 2$ の場合にあたっている.

例 2.3

$$\mathbf{F}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{8} = \bar{3}\}$$

$\bar{2} + \bar{4} = \bar{1}$, $\bar{3} \cdot \bar{4} = \bar{2}$ など.

注意 2.4 n を自然数として, $q = p^n$ とおけば, q 個の元をもつ有限体 $\mathbf{F}_q$ が存在することが知られている. また, 任意の有限体は, ある素数 p とある自然数 n に対して $\mathbf{F}_{p^n}$ の形になることも知られている.

3　有限体$\mathbf{F}_q$上の数ベクトル空間

nを自然数として

$$\mathbf{F}_q^n = \{x = (x_1, x_2, \cdots, x_n) \mid x_i \in \mathbf{F}_q \ (i = 1, 2, \cdots, n)\}$$

とおく. $\mathbf{F}_q^n$の2元

$$x = (x_1, x_2, \cdots, x_n),\ y = (y_1, y_2, \cdots, y_n)$$

に対し, 和を

$$x + y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$

$c \in \mathbf{F}_q$によるスカラー倍を

$$c \cdot x = (cx_1, cx_2, \cdots, cx_n)$$

と定義する. このような和とスカラー倍を持つ集合$\mathbf{F}_q^n$を有限体$\mathbf{F}_q$上のn**次元数ベクトル空間**という. このベクトル空間も$\mathbf{R}$上の数ベクトル空間$\mathbf{R}^n$と同様に扱うことができる.

$\mathbf{F}_q^n$の部分集合Vが, $\mathbf{F}_q^n$に与えられた和とスカラー倍によって閉じている時, Vを$\mathbf{F}_q^n$の**部分空間**という. Vの元$v_1, v_2, \cdots, v_m$が存在して, Vの任意の元xが

$$x = c_1v_1 + c_2v_2 + \cdots + c_mv_m \quad (c_i \in \mathbf{F}_q)$$

とただ一通りに表される時, $v_1, v_2, \cdots, v_m$をVの基底という. また, mをVの次元という.

例 3.1 $\mathbf{F}_q^n$はn次元:

$$\mathbf{F}_q^n = \mathbf{F}_q(1, 0, 0, \cdots, 0) + \mathbf{F}_q(0, 1, 0, \cdots, 0) + \cdots + \mathbf{F}_q(0, 0, 0, \cdots, 0, 1)$$

例 3.2 ${\mathbf{F}_2}^3$の部分空間

$$\begin{aligned} C &= \mathbf{F}_2(1, 1, 0) + \mathbf{F}_2(1, 0, 1) \\ &= \{(0, 0, 0), (1, 1, 0), (1, 0, 1), (0, 1, 1)\} \end{aligned}$$

の次元は2. たとえば, $(1, 1, 0)$, $(1, 0, 1)$が基底となる.

4　符号理論

情報源からの情報を符号化して送信し, 受信する手続きを図式化すると次のようになる.

第1節の例で見たように, 送信者は情報を符号器で誤り訂正のできる信号にかえ, それを送信する. 受信者は受信した信号を復号器にかけ, 正しい信号を再現し, 正確な情報を得るのである. $\mathbf{F}_q$ 上の n 次元横数ベクトル空間 ${\mathbf{F}_q}^n$ の元 $(x_1, x_2, \ldots, x_n)$ を**語** (alphabet) とよぶ. ${\mathbf{F}_q}^n$ の部分集合 C を**符号** (code) といい, n を C の**符号長**という. C の元を情報の alphabet として用い, 冗長部分 ${\mathbf{F}_q}^n \setminus C$ を誤り訂正に用いる. C が大きい方が多くの情報を伝えることができ、${\mathbf{F}_q}^n \setminus C$ が大きいほうが一般に誤り訂正能力が高い. 相反するこの両方の条件を充たすできるだけ効率のよい符号をつくることをめざすのである.

エラーを調べるために, ${\mathbf{F}_q}^n$ にエラーの大きさをはかる尺度を導入したい. その尺度として便利なのが数学でしばしば用いられる距離の概念である.

典型的な距離の例として, 3次元ユークリッド空間 $\mathbf{R}^3$ の2点 $P = (x_1, x_2, x_3)$, $Q = (y_1, y_2, y_3)$ の距離

$$d(P, Q) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2}$$

を考えよう. この距離は次の3つの性質をみたす.

(i) $d(x, y) \geq 0$. また, $d(x, y) = 0 \Leftrightarrow x = y$.

(ii) $d(x, y) = d(y, x)$

(iii) [三角不等式] $d(x, y) + d(y, z) \geq d(x, z)$

距離にとって大事なのはこの3つの性質であり, この3つの性質をもつものは距離と呼ぶにふさわしいものである.

このことを念頭において, ${\mathbf{F}_q}^n \ni x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ の距離を次のように定義する.

定義 4.1 (ハミング距離)

$$d(x, y) = \sharp\{1 \leq i \leq n \mid x_i \neq y_i\}$$

ここに, 集合 S に対して $\sharp S$ は S の元の数を表す.

たとえば, $\mathbf{F}_2{}^6$ において, $x=(1,1,1,0,1,0)$ と $y=(1,1,0,0,0,0)$ では2つの成分が異なるから, $d(x,y)=2$ となる. 言い換えると, $x=(1,1,1,0,1,0)$ を送信し $y=(1,1,0,0,0,0)$ を受信したとすれば, ハミング距離 $d(x,y)=2$ だけの誤りが生じたことになる.

このように定義されたハミング距離が, 距離の3性質を満たすことは容易にたしかめられる.

$z\in\mathbf{F}_q^n$ と自然数 r に対して

$$B_r(z)=\{x\in\mathbf{F}_q^n \mid d(z,x)\le r\}$$

を z を中心とする半径 r の**球**と呼ぶ.

定義 4.2 $\mathbf{F}_q{}^n$ の部分集合 C に対し, その**最小距離** d を次のように定義

$$d=\min\{d(x,y)\mid x,y\in C, x\neq y\}$$

ここに, min は最小値を表す.

たとえば, $\mathbf{F}_2{}^2\supset C=\{(0,0),(1,1)\}$ において C の最小距離は $d=2$ である.

エラー訂正は, **最尤復号**と呼ばれる次のような方法によって行う. 状況をわかりやすくするため, C の最小距離 d が $d=2e+1$ (e は整数) のときを考える. C の元を中心とする半径 e の球を考えると, d の定義によって, それらの球には互いに共通部分がない. したがって, C のある元が情報として発信されたとき, 受信した符号がそれらの球のいずれかに入れば, 距離的に一番近い球の中心である C の元が送信された元である確率が最も高い. そこで, その球の中心が発信された元であるとして復号するのである. このときには, 確率的にいって, e 個までのエラーを訂正できることになる. また, d が偶数のときには $(d-2)/2$ 個のエラーが訂正できる.

C が $\mathbf{F}_q{}^n$ の部分空間である場合, C を**線形符号**という. $\mathbf{F}_q{}^n$ の元 x に対し

$$w(x)=d(x,0)$$

とおいて, これを x の**重さ**という.

定義 4.3 線形符号 C の**最小重み** w を次のように定義する.

$$w=\min\{d(x,0)\mid x\in C, x\neq 0\}$$

$d(x,y)=d(x-y,0)$ であるから, $x,y\in C$, $x\neq y$ なる条件の下におけるこの両辺の最小値を考えれば, 線形符号 C に対し $d=w$ が成り立つことがわかる. この結果から, 線形符号の場合には最小距離を計算するには最小重みを計算すればよく, 計算量が大幅に少なくてすむ.

定義 4.4 線形符号 $C \subset {\mathbf{F}_q}^n$ の次元が k でその最小距離が d のとき, C を $[n,k,d]$-**符号**という.

線形符号 C の重要な量は, 符号長 n, 次元 k, 最小距離 d の3つの量であり, それらが決まれば符号 C の性質はきまる. **伝送率** $R = k/n$ と**相対距離** $\delta = d/n$ が大きい程, 一般には能率のよい符号といえるが, n,k,d はまったく独立な値をとれるわけではなく, $[n,k,d]$-符号 C に対して次のような不等式が知られている.

(1) $d \leq n-k+1$ [**シングルトン限界式** (Singleton bound)]

(2) t を $(d-1)/2$ の整数部分とすれば,

$$k \leq n - \log_q(\sum_{i=0}^{t} \binom{n}{i}(q-1)^i)$$

が成り立つ [**ハミング限界式** (Hamming bound)]. ただし, $\binom{n}{i}$ は2項係数である.

(3) $\lceil a \rceil$ を実数 a 以上の最小の整数とすれば,

$$n \geq \sum_{i=0}^{k-1} \lceil d/q^i \rceil$$

が成り立つ [**グリースマ限界式** (Griesmer bound)].

この他にも様々な限界式が知られている ([13] 参照).

最後に線形符号の簡単な例をあげておく.

例 4.5 ${\mathbf{F}_2}^2$ の部分空間

$$C_1 = \mathbf{F}_2(1,1) = \{(0,0),(1,1)\}$$

を考える. この部分空間の次元は1. 最小重みは元 $(1,1)$ が与えるから, 最小重みは2. したがって, C_1 は $[2,1,2]$ 線形符号である.

次に, ${\mathbf{F}_2}^3$ の部分空間

$$C_2 = \mathbf{F}_2(1,1,0) + \mathbf{F}_2(1,0,1) = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$$

を考える. この部分空間の次元は2で最小重みも2. したがって, C_2 は $[3,2,2]$ 線形符号である.

これらの例では, $(d-2)/2 = 0$ となるから, 符号 C_1, C_2 を用いても誤りをまったく訂正できない.

例 4.6 ([7,4,3]– ハミング符号) $\mathbf{F}_2$ 上の2次元射影平面 $\mathbf{P}^2(\mathbf{F}_2)$ において, $\mathbf{F}_2$ 有理点は

$$(1,0,0),(0,1,0),(1,1,0),(0,0,1),(1,0,1),(0,1,1),(1,1,1)$$

の7個である. これを縦ベクトルとして並べて $(3,7)$ 型の行列 H を作る.

$$H=\begin{pmatrix}1&0&1&0&1&0&1\\0&1&1&0&0&1&1\\0&0&0&1&1&1&1\end{pmatrix}$$

H には一次独立な3個の列ベクトルが存在するから, rank $H=3$ である.

$$C=\{x\in {\mathbf{F}_2}^7 \mid x\,{}^tH=0\}$$

とおく. H を C のパリティー検査行列という. 行列を用いないで表示すれば, C は3元連立1次方程式

$$\begin{aligned}x_1+x_3+x_5+x_7&=0\\x_2+x_3+x_6+x_7&=0\\x_4+x_5+x_6+x_7&=0\end{aligned}$$

の解空間である.

一次方程式の理論から $\dim_{\mathbf{F}_2} C=7-3=4$ となる. 任意の2つの列の和は0にならないから, C の元の最小距離は少なくとも3以上である.

$$x=(1,1,1,0,0,0,0)\in {\mathbf{F}_2}^7$$

を考えれば $w(x)=3$ で, $x\,{}^tH=0$ ゆえ x は C の元である. したがって, C の最小距離は3に等しく, C は $[7,4,3]$-線形符号となる. この符号を用いれば1個の誤りが訂正できる. この符号を $[7,4,3]$-ハミング符号という.

5 符号理論の歴史

ここでは, 線形符号の理論の歴史を簡単に紹介する. 符号理論は1948年のシャノン (C. E. Shannon) の論文に始まるといっても過言ではないであろう. 彼は, ある条件が充たされれば符号長を大きくするに従い, 誤り確率がいくらでも小さくなるような符号の列が存在することを示した. 1950年にはハミング符号が構成された. この符号はコンピュータの記憶装置の誤り訂正にしばしば利用される. 1957年には巡回符号が構成され, 1959年には BCH 符号が, 1960年には RS 符号が構成された. これらの符号は線形符号の理論の中で重要な位置をしめる符号であり, RS 符号

はBCH符号の, BCH符号は巡回符号の特殊なものである. また, RS符号はCDやCD-ROMの誤り訂正符号として利用されている. 1968年にはバーレカンプ・マッシィ(Berlekamp-Massey)法というBCH符号の効率的な復号法が考案されている. 1971年にはゴッパ(Goppa)によりゴッパ符号が考案された. この符号は, 1981年にゴッパによって代数幾何符号として一般化された([6], [7], [10], [12], [14], [17], [18], [22], [23], [24] 参照). 1982年には代数幾何符号を用いてそれまでは最良と思われていたヴァルシャモフ・ギルバート(Varshamov-Gilbert)限界式を越える符号の列が構成され, 代数幾何符号の理論的な優秀性が示された([25] 参照). 1991年には任意の線形符号が弱い意味の代数幾何符号として実現されることが示され([19] 参照), 1993年にはフェン・ラオ(Feng-Rao)により代数幾何符号の効率的な復号法が考案されている([4], [21] 参照). また, 符号理論はデザインや格子理論とも関係があることが知られている([1], [2], [3], [5] 参照). 最近では, 線形符号の理論は, デジタルへの応用ばかりではなく, 数理物理における共形場の理論, 数論における保形形式の理論など, 数学のいろいろな領域でも用いられている.

参考文献

[1] P. J. Cameron and J. H. van Lint, Designs, Graphs, Codes and their Links, London Mathematical Society, Student Texts 22, 1991.

[2] J. H. Conway and N. J. A. Sloane, Sphere Packings, Lattices and Groups, 2nd ed., Grundlehren der mathematischen Wissenschaften 290, Springer-Verlag, 1993.

[3] W. Ebeling, Lattice and Codes, Vieweg, 1994.

[4] G.-L. Feng and T. R. N. Rao, Decoding algegraic-geometic codes up to the designed minimum distance, IEEE Trans. Inform. Theory, 39 (1993), 37-45.

[5] 藤原　良・神保　雅一, 符号と暗号の数理, 共立出版, 1993.

[6] V. D. Goppa, Codes on algebraic curves, Dokl. Akad. Nauk SSSR, 259 (1981), 1289-1290.

[7] V. D. Goppa, Geometry and Codes, Kluwer Academic Publishers, 1988.

[8] D. G. Hoffman and D. A. Leonard, C. C. Lindner, K. T. Phelps, C. A. Rodger and J. R. Wall, *Coding Theory: The Essentials,* Monographs and Textbooks in

Pure and Applied Mathematics 150, Marcel Dekker, Inc., New York-Basel-Hong Kong,1991.

[9] 今井　秀樹, 符号理論, 電子情報通信学会, 1990.

[10] 桂　利行, 代数幾何入門, 共立講座 21 世紀の数学, 共立出版, 1998.

[11] 桂　利行, デジタルの数学, 「数学のたのしみ」21 号, 2000 年 10 月, 54–65, 日本評論社.

[12] G. Lachaud, Les codes géométriques de Goppa, Séminaire Bourbaki 37ème année, 1984-85, no641, Astérisque 133-134 (1986), 189-207.

[13] J. H. van Lint, Introduction to Coding Theory, Graduate Texts in Mathematics 86, Springer-Verlag, 1991.

[14] J. H. van Lint and G. van der Geer, Introduction to Coding Theory and Algebraic Geometry, Birkhäuser Verlag, 1988.

[15] F. J. Macwilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, 1977.

[16] Yu. I. Manin, What is the maximal number of points on a curve over $\mathbf{F}_2$, J. Fac. Sci. Univ. Tokyo Sect. IA Math., 28 (1982), 715-720.

[17] J.-F. Michon, Codes de Goppa, Séminaire de Théorie des Nombres de Bordeaux, Année 1983-1984, exposé no7 (1983).

[18] C. J. Moreno, Algebraic Curves over Finite Fields, Cambridge University Press, 1993.

[19] R. Pellikaan, B.-Z. Shen, and G. J. van Wee, Which linear codes are algebraic-geometric? IEEE Trans. Information Theory, 37-3 (1991), 583-602.

[20] O. Pretzel, Error-Correcting Codes and Finite Fields, Clarendon Press, Oxford, 1992.

[21] 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. Inform. Theory, 41 (1995), 1762-1768.

[22] C. A. Stepanov, Codes on Algebraic Curves, Kluwer Academic/ Plenum Publishers, 1999.

[23] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, 1991.

[24] M. A. Tsfasman and S. G. Vlădut, Algebraic-Geometric Codes, Kluwer Academic Publishers, 1991.

[25] M. A. Tsfasman, S. G. Vlădut and Th. Zink, Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound, Math. Nachr. 109 (1982), 21-28.

(かつら　としゆき・東京大学大学院数理科学研究科)