数理解析研究所講究録
第1956巻 2015年 75-93

モダン代数的符号と呼ばれる ネットワーク誤り訂正符号

萩原学*

1 はじめに

本稿は，愛知県立大学の平尾将剛氏から声掛け頂き，RIMS共同研究「デザイン，符号，グラフおよびその周辺」にて講演した内容を文書にまとめたものである．講演でも述べたが，内容は著者の新しい結果ではなく，ネットワーク誤り訂正符号のごくごく基礎的な事項を美味しいところだけ抜き出したものである．ネットワーク符号と呼ばれる，わりと最近生まれたばかりの人気分野に，1980年代に作られたランク距離誤り訂正符号が有用な道具として再発見されていく様は非常に興味深い．本稿を，この分野の入り口として楽しんで頂ければ幸いである．

2 背景

RichardsonとUrbankeの名著「Modern Coding Theory [1]」は，主としてLDPC符号と確率伝搬アルゴリズムを軸とし，密度発展法による符号設計，グラフ上の情報力学，疎の意義などが論じられている．本論文では，それらの議論による符号理論をモダン符号理論と呼ぶことにする．モダン符号理論の目指すところは，LDPC符号による通信路容量，もしくは，シャノン限界の達成と言える．つまり，符号理論のゴールをLDPC符号の枠組みで達成することにある．

*千葉大学大学院理学研究科 数学・情報数理学コース，Course of Mathematics and Informatics, Graduate Schoole of Science, Chiba University. E-mail: hagiwara@math.s.chiba-u.ac.jp

符号理論は，シャノンの論文「Mathematical Theory of Communication [2]」に端を発する．この論文にて，雑音のある通信路上で通信を行った場合，信頼性と通信効率にはトレードオフではなく，閾値が存在することを明らかにした．この閾値を，通信効率の視点で述べたものが通信路容量であり，雑音の大きさの視点で述べたものがシャノン限界である．それを受けて，高い信頼性を持ちつつ，それら閾値に非常に近い通信を実現する符号化法と復号法の二つを具体的に構成するという目的が，符号理論の原点である．

上記の書籍 [1] の発行以降，モダン符号理論は，日進月歩の発展を遂げた．ブレークスルーとなったのは，空間結合の概念 [3] が発見である．空間結合されたLDPC符号を用いれば，二元消失通信路において，モダン符号によるシャノン限界が達成できることが明らかとなった．その後，様々な通信路でも，空間結合LDPC符号が符号理論のゴールへたどり着けることがわかった．

モダン符号理論は輝かしい成功を収めた．それでは，符号理論にはどのような未来があるか，符号理論の研究者としては気になるところである．

符号理論を扱う研究集会は，国内外に数多くある．中でも，誤り訂正符号のワークショップは，最新の符号理論の入門講義を幅広く扱い，学生にも最先端の研究者にも有用な知見を提供している掲研究集会である [4]．２０１２年に開催された誤り訂正符号のワークショップでは，大学生・大学院生を対象とした誤り訂正符号入門講義が多数開講された．その講義の１つ，代数的符号理論を上智大学の渋谷氏が担当した．講義において，渋谷氏は次の提言をしている．

「モダン代数的符号理論とは何か」

符号理論において代数的なアプローチは１９４０年代から継続して行われてきた．一方，１９９０年台後半からのモダン符号理論においては，確率論，情報力学，解析学，グラフ理論などからのアプローチが主流と言える．モダン符号理論のゴールが現実的となった現在，符号理論に次の研究潮流が登場すると予想される．そこで，改めて代数的アプローチを主とする符号理論の姿を見据えようと言うのが，渋谷氏の提言の背景だろう．

渋谷氏の講義では，モダン代数的符号理論の一つの姿として，本質的には，ランク距離誤り訂正符号を取り上げた．この符号が代数的であるという主張は，線形化多項式の視点からみたリード・ソロモン符号の類似としてインスタンスが実現できること，および，Welch-Berlekamp ア

ルゴリズムの類似による復号の実現ができることを挙げている．[1] 雑音の発生源である通信路としては，消失オペレータ通信路を例示した．

ランク距離誤り訂正符号へは，ネットワーク符号と組み合わせることでより興味深い対象となる．これは，**ネットワーク誤り訂正符号**と呼ばれる．本稿では，まず，ネットワーク符号に関する基礎事項を解説する．その上で，ネットワーク符号とランク距離誤り訂正符号を結びつける．最後に，ランク距離誤り訂正符号の具体例として，ガビドゥーリン符号（Gabidulin 符号）を解説する．

3 ネットワーク符号 –ノイズレス–

3.1 段ボール箱の配送

符号理論の目的が，高い信頼性を持ちつつ，それら閾値に非常に近い通信を実現する符号化法と復号法の二つを具体的に構成することであるように，ネットワーク符号も同様の目的を持つ [5].（ネットワーク符号でない）符号理論において，通信路で雑音が発生しなければ，信頼性は保障され，同時に，通信効率の高さも保障される．以下で述べるように，ネットワーク符号では，通信路で雑音が発生しない場合であるとき，信頼性は保障されても，通信効率に議論の余地がでる．これがネットワーク符号の面白さである．

ネットワーク符号の理解を深める例として最も著名なものが**バタフライネットワーク**である．本稿でも，バタフライネットワークを通じてネットワーク符号の解説をしていく．

図 1 が，バタフライネットワークと呼ばれる有効グラフを図示したものである．このグラフは 6 つの頂点と 7 つの辺からなる．上部には s_1, s_2 とラベルの貼られた頂点がそれぞれ 1 つずつ，下部には t_1, t_2 とラベルの貼られた頂点がそれぞれ 1 つずつある．前者は**始点**（Start Point）と，後者は**終点**（Terminal）とそれぞれ呼ばれる．

バタフライネットワーク上で，物流の効率を考察してみよう．各始点から同じ荷物を，二つの終点に届けたい．少し具体的に，始点 s_1 は荷物 b_1 を終点 t_1, t_2 へ，始点 s_2 は荷物 b_2 を終点 t_1, t_2 へ，それぞれ届けることとする．つまり，荷物は b_1, b_2 の計二種類ある．終点 t_1 はその二つの荷物

[1] 線形化多項式に関する教科書は [6] を，リード・ソロモン符号に関する教科書は [7] を，Welch-Berlekamp アルゴリズムに関する教科書は [8] をそれぞれ参照されたい．

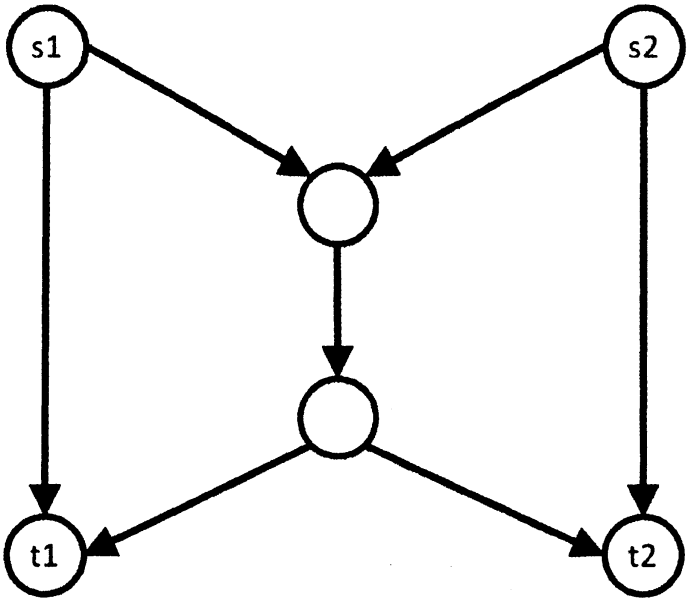

図 1: バタフライネットワーク

b_1, b_2 の両方を，終点 t_2 もその二つの荷物 b_1, b_2 の両方を受け取るようにする．

各辺は，配送経路を表す．始点にある荷物は，辺で繋がれた頂点のどれかへ移動．同様に，荷物はその頂点から，辺で繋がれた頂点のどれかへ移動する．これを繰り返して，下で述べる**配送料の限界の範囲**で，終点まで荷物を届けていく．ここまでを，配送にかかった時間を 1 時点とみなす．

辺には，配送量の限界がある．バタフライネットワークでは，各辺には，1 時点において，最大 1 つの荷物しか配送されない．[2] ある頂点に届いた荷物の合計の数が，そこから繋がれた辺の数を超えている場合は，配送できなかった荷物を次の時点まで保管する．

配送量の限界によってどの荷物も移動できない場合，もしくは，全ての荷物が終点まで届いた場合に，配送の時点が 1 つ経過したと考える．そして，全ての荷物が終点に届くまでは，始点は新たな荷物を届け始めないこととする．

一派的な荷物（段ボール箱など）を想定したとき，バタフライネットワークでは，両方の始点 s_1, s_2 のどちらも荷物を 1 つずつ送った場合，全ての荷物が終点に届くまでに 2 時点以上必要となる．これは，ネットワー

[2]現実のイメージ例として，配送するトラックの荷台には大きさの限界があると考えれば良い．

ク上の中心上部の頂点から中心下部への頂点への辺が1本しかない為である．図2に，最初の時点において，各辺を通る荷物を辺に書き入れた例を挙げている．この配送方法では，荷物b_2が終点t_1に届いていない．ネットワークの中心上部にある頂点で，荷物b_2は保管される為である．次の時点において，荷物b_2が終点t_1に届く．

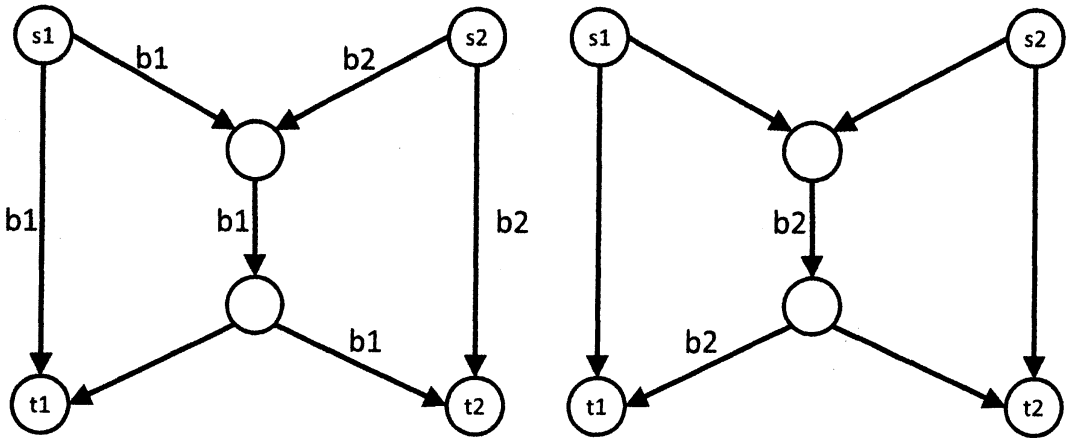

図 2: バタフライネットワーク上の段ボール箱配送

本稿では，ネットワーク符号の主な興味として.「1時点で全ての荷物を届けられる範囲で，始点から出される荷物の総数を最大にせよ」に注目していくことにする．この例では，荷物はb_1だけ，もしくは，b_2だけであれば，1時点で配送できる．ここまでの考察も踏まえると，最大の荷物の数は1となる．

3.2 情報の配送，ネットワーク符号化

ここからは始点から送られる荷物を，段ボール箱ではなくて，情報として考察していく．その意味で，問題である「1時点で全ての荷物を届けられる範囲で，始点から出される荷物の総数を最大にせよ」は，通信効率の最大化であるとみなせる．

ここでいう情報は，数値を表すと考えて頂いて良い．代表的な例としては，情報（数値）として，0もしくは1だけを届けることを想定する．

段ボール箱と情報には，本質的な違いがいくつもある．まず，違いとして，配送量の限界について述べたい．一度に運べる情報の量に，現実的に意味のある考え方を適用したい．通信速度という言葉ある．単位として，bps（ビットパーセカンド），Mbps（メガビットパーセカンド），

そして，Gbps（ギガビットパーセカンド）などが用いられるそれである．バタフライネットワークでは，各辺には，1時点において，最大1つの情報しか配送されない．[3]

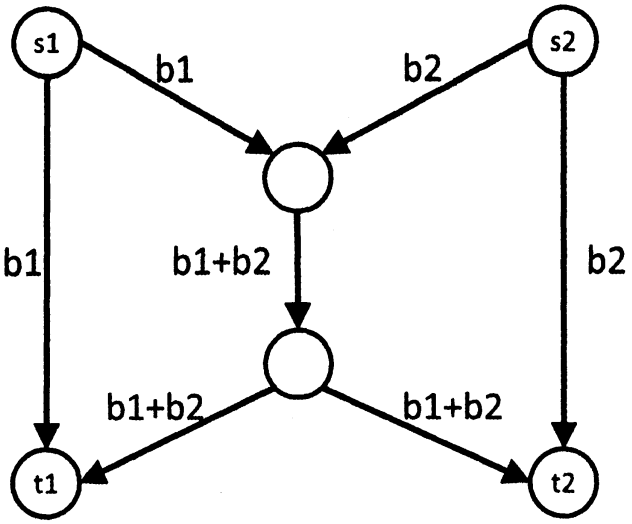

図 3: バタフライネットワークにおける符号化

図3をご覧頂きたい．この図では，終点 t_1 には情報 $b_1, b_1 + b_2$ の二つの情報が，終点 t_2 には情報 $b_1 + b_2, b_2$ の二つの情報がそれぞれ届いている．これは，中央上部のノードが受け取った2つの情報 b_1, b_2 のどちらかを通信路に送るのではなく，その和 $b_1 + b_2$ を送っていることで実現できている．

ネットワーク符号では，各頂点が受け取った情報に対して何らかの計算を行うことが許される．これが段ボール箱と情報における，本質的な違いの1つである．

終点 t_1 は，受け取った情報 $b_1, b_1 + b_2$ を利用して，元来の情報 b_1, b_2 の両方を復号できる．前者 b_1 はそのままで良い．後者 b_2 は計算 $(b_1 + b_2) - b_1$ によって得られる．同様に終点 t_2 は，受け取った情報 $b_2, b_1 + b_2$ を利用し，前者 b_2 はそのままで良い．後者 b_1 は計算 $(b_1 + b_2) - b_2$ によって得られる．

このようにすれば，t_1, t_2 ともに二つの情報を受け取ることができる．実は，三つ以上の情報は受け取れないことがわかるが，ここでは詳細は割愛する[4]．つまり，頂点上での計算を導入したことで，通信効率が最大化

[3]bps の意味をご存知の方は，次のように考えられる．もしも，0か1しか送らない場合，1時点を1秒と考えれば，単位は1bps であると言える．

[4]最大流最小カット定理という定理から得られる．

されたと言える．

届ける対象を段ボール箱のような物質から，情報へ変えることにより，通信効率を改善することが可能となる．それには，各頂点による計算，さらに終点による計算，という２つの計算が重要となる．前者（各頂点による計算）をネットワーク符号化，後者（終点による計算）をネットワーク復号とそれぞれ呼ぶ．ネットワーク符号の理論は，ネットワーク（グラフ）に対し，その符号化と復号をうまく考慮することで，通信効率を最大化することを研究していく．[5]

ここまで述べてきたネットワーク符号では，通信路に雑音がないことを仮定してきた．信頼度は常に高いが，通信効率を高くするには符号化と復号をうまく考える必要があった．

次節では，通信路に雑音がある場合のネットワーク符号について述べる．

4　ネットワーク符号 –ノイジー–

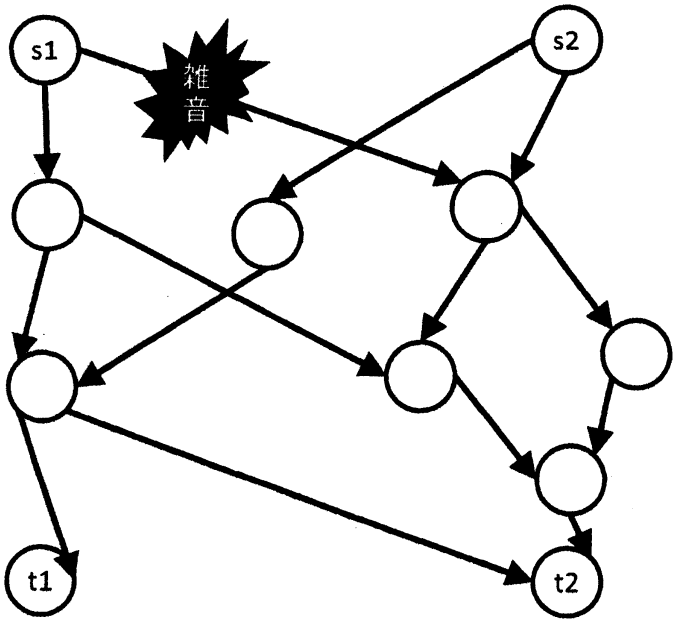

図 4: 雑音のある通信路をもつネットワーク

図 4 は，始点として s_1, s_2，終点として t_1, t_2 を持つネットワークである．図中には，ギザギザの雲のような記号を書いている．もし，ギザギ

[5]形式的には，(グラフ，符号化，復号）といった組をネットワーク符号と呼ぶ．

ザの乗った通信路で雑音が生じたらどうなるか想像して頂きたい．雑音とは，符号理論の専門用語である．通信路を通る前の情報と，通った後の情報が異なるときに，通信路で雑音が生じたと表現する．例えば，情報0が情報1に変わる，といったことが考えられる．

一旦，雑音が発生してしまうと，その後の通信路，頂点，特に，終点に対して，元来の情報とは異なる情報が届けられる．

特に，ネットワーク符号では，雑音は厄介な問題となる．先の図3の，始点s_1から右下へ伸びている通信路で雑音が発生したと想定してみよう．本来のb_1ではなく，別の情報b_1'へ変わってしまったとする．すると，中心の上部の頂点で符号化されて，中心上部から下部への通信路を通るのは情報$b_1' + b_2$である．そして，中心下部の頂点で情報が複製される．終点t_1に届く情報はb_1と$b_1' + b_2$である．ナイーブに復号すれば，t_1はb_1と$b_1' + b_2 - b_1$を受け取ることになる．これはb_1, b_2とは異なる情報である．同様に，終点t_2に届く情報はb_2と$b_1' + b_2$であり，復号結果はb_1'とb_2となる．つまり，どちらの終点も元来の情報b_1, b_2を正しく受け取れなかったことなる．

このように，ネットワーク符号では，一旦発生した雑音が次々に伝搬してしまう．非常に厄介な問題である．

4.1 線形ネットワーク

ネットワーク符号の通信路上の雑音を，数学的に記述しやすいようモデル化したものの1つが**線形ネットワーク（符号）**である．

線形ネットワークでは，元来の情報として，体上のベクトルを用いるとする．本稿では，元来の情報の所属するベクトル空間を$\mathbb{K}^n$としよう．

一方，頂点での符号化は，体$\mathbb{K}$上の一次結合であるとする．ある頂点に届けられた情報全体を$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M \in \mathbb{K}^n$とし，その頂点からある（1つの）通信路へ出される情報を$\mathbf{y} \in \mathbb{K}^n$としたとき（図5参照），

$$\mathbf{y} = \sum a_i \mathbf{x}_i \quad (a_i \in \mathbb{K}) \tag{1}$$

と表せる．

最後に，雑音が発生したとき，通信路を通った後の情報は$\mathbb{K}^n$の元であると設定する．つまり，他の集合の元にはならないとする[6]．

[6]現実的には，体$\mathbb{K}$の元でなくなるとしても不思議ではない．例として，情報が消失してしまった場合が挙げられる．消失誤りに対する符号を考えるのは面白いが，本稿では扱わない．

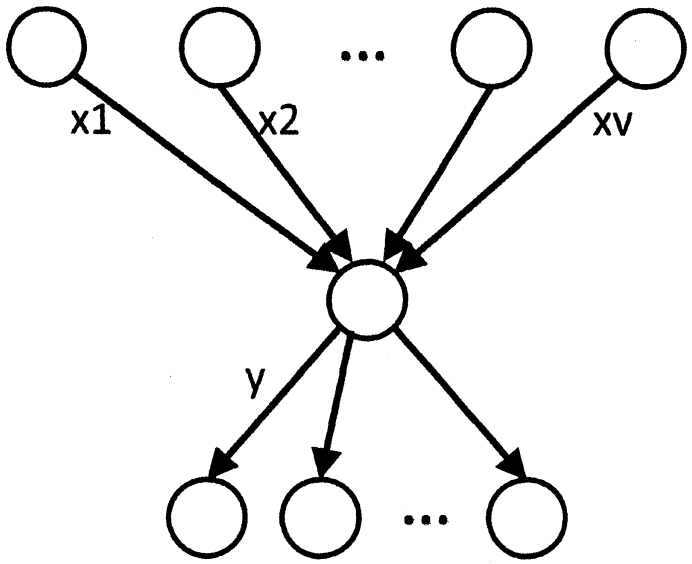

図 5: 線形ネットワークでの符号化

式 (1) は，ベクトル $\mathbf{a} := (a_1, a_2, \ldots, a_M)$ を用いて，次のように表わすことができる．

$$\mathbf{y} = \mathbf{a} \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_M \end{pmatrix}. \tag{2}$$

ここで，右辺の最右の項をサイズ $M \times n$ の行列とみなしている．

もしも全ての通信路で雑音が一度も発生しなければ，ある通信路 e を流れる情報 $\mathbf{y}_e$ はあるベクトル $\mathbf{a}_e \in \mathbb{F}^s$ を用いて，次のように表せることに注意したい．

$$\mathbf{y}_e = \mathbf{a}_e \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_s \end{pmatrix}, \tag{3}$$

ここで，$\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_s$ は “始点が送った情報” 全体を表す．つまり，符号化する頂点が受け取った情報ではなく，始点が送った情報であることが

重要である．さらに，

$$B := \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_s \end{pmatrix}$$

とおけば，

$$\mathbf{y}_e = \mathbf{a}_e B \tag{4}$$

と表せる．ここで，B をサイズ $M \times n$ の $\mathbb{K}$ 上の行列とみなしている．

この事実は帰納的に示せる．

まず，始点に繋がっている通信路 e に流れる情報を，式 (3) のように表せるのは，明らかである．特に，$\mathbf{a}_e$ として，その成分が 0 もしくは 1 であるベクトルを考えればよい．0 はその始点から出ていない情報の位置に，1 はその始点から出ている情報の位置におけば良い．

また，ある頂点の受け取った情報全体 $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M \in \mathbb{F}^n$ が，それぞれあるベクトル $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_M \in \mathbb{F}^s$ によって $\mathbf{x}_i = \mathbf{a}_i B$ と表せたとする，

いま，$\mathbb{K}$ 上のサイズ $M \times s$ の行列 A を，第 i 行がベクトル $\mathbf{a}_i$ と一致するよう定める．すると，

$$\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_M \end{pmatrix} = AB \tag{5}$$

が従う．線形ネットワークでの符号化は式 (2) で記述されることを思い出せば，符号化後の情報 $\mathbf{y}$ は

$$\begin{aligned} \mathbf{y} &= (a_1, a_2, \ldots, a_M) \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_M \end{pmatrix} && (6) \\ &= (a_1, a_2, \ldots, a_M)AB && (7) \\ &= (a'_1, a'_2, \ldots, a'_s)B && (8) \end{aligned}$$

と表せる．ここで，$(a'_1, a'_2, \ldots, a'_M) := (a_1, a_2, \ldots, a_M)A$ とおいた．

以上から，各終点で受け取る情報全体，もしくは，各頂点が符号化した情報全体 $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_M \in \mathbb{K}^n$ は，$\mathbb{K}$ 上のサイズ $M \times s$ の，ある行列 A_i

を用いて

$$\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_M \end{pmatrix} = A_i B \tag{9}$$

と表せる．

続いて，通信路に雑音がある場合，終点の受信情報全体が式(9)とどれだけ異なるか考察しよう．話の見通しを良くする為，ある1つの通信路eで雑音が発生し，他の通信路では雑音が発生しなかったと仮定しよう．式(4)の右辺の記号を用いて，雑音が無かった時の情報を$\mathbf{a}_e B$と書くことにする．また，雑音が発生した後の情報を$\mathbf{y}_e$とする．そして，これらの差分を$\mathbf{e}_e := \mathbf{y}_e - \mathbf{a}_e B \in \mathbb{K}^n$と書くことにする．[7]

このとき，通信路eに繋がれた頂点に届く情報全体$\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_M$を式(5)のように表そう．簡単の為，$\mathbf{x}_1 := \mathbf{y}_e$とおくことにする．すると，

$$\begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_M \end{pmatrix} = AB + E_e \tag{10}$$

となる．ただし，行列E_eは，第1行目が$\mathbf{e}_e$であり，他は0である$\mathbb{K}$上のサイズ$M \times n$の行列とする．

そして，式(8)と同様に，符号化後の情報$\mathbf{y}$は

$$\begin{aligned} \mathbf{y} &= (a_1, a_2, \ldots, a_M) \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_M \end{pmatrix} && (11) \\ &= (a_1, a_2, \ldots, a_M)AB + (a_1, a_2, \ldots, a_M)E_e && (12) \\ &= (a'_1, a'_2, \ldots, a'_s)B + (a_1, a_2, \ldots, a_M)E_e && (13) \end{aligned}$$

と表せる．行列Bと行列Eでは，左から掛けているベクトルが異なるかもしれないことを注意しておく．ちなみに，雑音が発生していない時は，行列E_eに掛けているベクトルがゼロベクトルであると考えることができる．

[7]式(4)では，$\mathbf{e}_e = \mathbf{0}$であったとみなせる．

以上を踏まえると，式(9)と同様に各終点で受け取る情報全体，もしくは，各頂点が符号化した情報全体 $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_M \in \mathbb{K}^n$ は，$\mathbb{K}$ 上のサイズ $M \times s$ の，ある行列 A_i, A_i' を用いて

$$\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_M \end{pmatrix} = A_i B + A_i' E_e \tag{14}$$

と表せる．

ここまでは，雑音の発生した通信路が1つだけとした場合の考察であった．もし，2つであれば，式(14)の代わりに

$$\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_M \end{pmatrix} = A_i B + A_i^{(1)} E_{e1} + A_i^{(2)} E_{e2} \tag{15}$$

となるのは，想像できるであろう．もっと一般に，p 個の通信路で雑音が発生すれば，

$$\begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_M \end{pmatrix} = A_i B + \sum_{j=1}^{p} A_i^{(j)} E_{ej} \tag{16}$$

と書ける．ただし，E_{ej} は，ある1つの行を除くと，その成分が全て0である行列を表す．誤りを表す行列は，

$$\sum_{j=1}^{p} A_i^{(j)} E_{ej}$$

と表現できることになった．

行列 E_{ej} のランクに注目すれば，その構造からランクは高々1である．ゆえに，行列 $A_i^{(j)} E_{ej}$ のランクも高々1である．よって，誤りを表す行列 $\sum_{j=1}^{p} A_i^{(j)} E_{ej}$ のランクは高々 p である．

以上から，線形ネットワークの枠組みでは，「p 個の通信路で発生した雑音とは，ランクが p 以下の行列を加えること」とみなせることがわかった．次節では，そのような雑音に耐性のある符号について議論していく．

5 ランク誤り訂正符号

体 $\mathbb{K}$ 上の同じサイズの行列 B_1, B_2 に対し，整数 $d_R(B_1, B_2)$ を

$$d_R(B_1, B_2) := \mathrm{rank}(B_1 - B_2)$$

と定義する．ただし，$\mathrm{rank}(X)$ は行列 X のランクを表す．

行列のサイズを固定し，その行列全体を $\mathcal{M}$ と書くことにする．$d_R(,)$ を行列の組 $\mathcal{M}^2$ から実数への写像とみなせば，距離の公理を満たすことが容易に示せる．この距離を**ランク距離**と呼ぶ．

p を正整数とし，行列の集合 $\mathcal{M}$ の部分集合 $\mathcal{C}$ を，勝手な $B_1, B_2 \in \mathcal{C}$ $(B_1 \neq B_2)$ に対して $d_R(B_1, B_2) \geq 2p+1$ を満たすように選ぶことができれば，集合 $\mathcal{C}$ を高々 p 個の通信路で発生した雑音に耐性のある符号とみなせる．これは，ハミング距離上の誤り訂正符号と同じ理屈である．

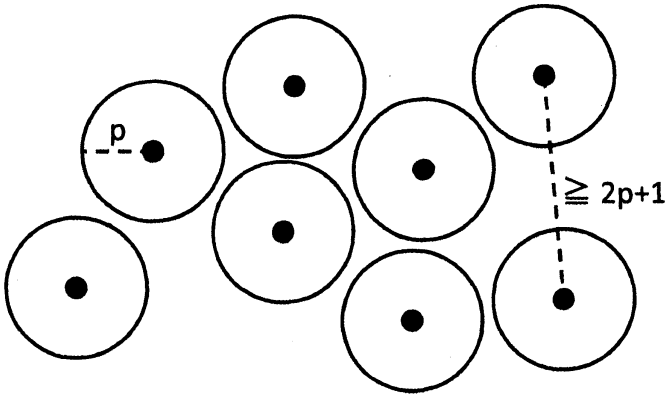

図 6: 符号語を中心としたランク距離に関する球

図 6 全体は $\mathbb{K}$ 上の同じサイズの行列全体 $\mathcal{K}$ を表し，黒丸が符号語 $\mathcal{C}$ の各元（一般に，符号語と呼ばれる対象）を表す．各黒丸を中心に円（球と呼ばれることもある）を描いており，この半径を p としている．符号語間の距離がどれも $2p+1$ 以上であれば，これらの円に重なりができない．この状況は，符号理論では次の様に応用される．符号語 C に雑音が発生し，別の行列 Y へ変わったとする．もしも，それらのランク距離 $d_R(C, Y)$ が p 以下であったとしよう．その場合，Y を表す点を図 6 に書くならば，C を表す黒点を中心とした円の内側の点として描写される．また，Y を表す点に一番近い黒点は，C を表す点であることもわかる．このことから，集合 $\mathcal{C}$ を高々 p 個の通信路で発生した雑音に耐性のある符号とみなせる．

ランク距離誤り訂正符号の概念は，数学者ガビドゥーリンによって１９８４年に提案された．時期だけ考えれば新しい符号とは言えない．さらに，当時は，ネットワーク符号の文脈ではなく，ハミング符号の一般化としての位置づけであったと文献 [9] から読み取れる．

ガビドゥーリンはランク誤り訂正符号の一般論から，MRD（最大ランク距離）符号という概念を提案した．そして，MRD 符号の構成例を具体的に与えた．その構成例が，現在，ガビドゥーリン符号と呼ばれるようになった．

以下，MRD 符号を導入しよう．そして，次節にて，ガビドゥーリン符号の解説を行っていく．

$\mathbb{K}_M$ を体 $\mathbb{K}$ の M 次拡大体とする．$\mathbb{K}_M$ と，体 $\mathbb{K}$ 上の M 次元列ベクトル全体を同一視する方法が知られている．そこで，(行) ベクトル空間 $\mathbb{K}_M^n$ の各成分を列ベクトルと対応させることで，$\mathbb{K}_M^n$ とサイズ $M \times n$ の行列全体 $\mathcal{M}$ を同一視する．この同一視により，行列の集合 $\mathcal{M}$ は体 $\mathcal{K}_M$ 上の n 次元ベクトル空間である．そこで，$\mathcal{C}$ を $\mathcal{M}$ の k 次元部分ベクトル空間とする．部分ベクトル空間 $\mathcal{C}$ に対し，

$$d_R(\mathcal{C}) := \min_{C \neq C' \in \mathcal{C}} d_R(C, C')$$

と定める．つまり，$\mathcal{C}$ の異なる二元間のランク距離の最小値として定義している．このとき，次の不等式が成立することがわかる [9]．

$$n - k \geq d_R(\mathcal{C}) - 1. \tag{17}$$

MRD 符号とは，上の不等式の等号が成り立つ $\mathcal{C}$ を意味する．解釈の１つとして，n, k を固定した時に，できるだけ大きな $d_R(\mathcal{C})$ を実現する符号 $\mathcal{C}$ に名前を付けたということである．この $d_R(\mathcal{C})$ は，本節の冒頭で述べた p に相当する値である．大きい方が，誤り訂正の性能が高いと考えられるから，大きい時に名前をつけたくなる．なぜ，名前が最大ランク距離符号と呼ぶのかも，納得いただけたと思う．

ちなみに，$\mathcal{C}$ が減法で閉じている時，

$$d_R(\mathcal{C}) = \min_{0 \neq C \in \mathcal{C}} d_R(0, C) = \min_{0 \neq C \in \mathcal{C}} \mathrm{rank} C$$

が従う．これは，一般的な古典の符号のハミング距離に対する線形符号の最少距離の議論と同様に示せる．

6 ガビドゥーリン符号の符号空間

ガビドゥーリン符号は文献 [9] で提案された符号である．この文献を読むには，一般的な線形代数，一般的な古典の符号理論の知識，加えて，有限体（特に，線形化多項式や正規基底の理論など），組合せ論（q-二項係数や q-整数など）の知識が必要である．有限体に関しては文献 [6] を，組合せ論に関しては文献 [10] をそれぞれお薦めする．[8]

本稿では，ガビドゥーリン符号（ここでは符号語全体のなす集合という意味）の定義とその MRD 性を解説するに留める．

有限体 $\mathbb{K}$ の M 次拡大体を 1 つ固定し，$\mathbb{K}_M$ で表す．有限体 $\mathbb{K}$ の濃度を q で表し，整数 t に対して整数 q^t を $[t]$ と表すことにする．そして，$\mathbb{K}_M$ 上の n 次元ベクトル空間 $\mathbb{K}_M^n$ の部分ベクトル空間 $\mathcal{C}$ を次で定義する．

$$\mathcal{C} := \{c \in \mathbb{K}_M^n \mid Hc^T = \mathbf{0}\},$$

ただし，H は次で定めるサイズ $(d-1) \times n$ の $\mathbb{K}_M$ 上の行列である．

$$H := \begin{pmatrix} h_1^{[0]} & h_2^{[0]} & \dots & h_n^{[0]} \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \vdots & \vdots & & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{pmatrix} \tag{18}$$

ここで，$h_1, h_2, \dots, h_n \in \mathbb{K}_M$ は $\mathbb{K}$ 上一次独立な元であるとする．このようにして構成した符号 $\mathcal{C}$ を**ガビドゥーリン符号**と呼ぶ．古典的な符号と同様に，H をパリティ検査行列と呼ぶ．

さて，次のことがわかる．

(G1) $\mathcal{C}$ は $\mathbb{K}_M$ 上 $n-d+1$ 次元ベクトル空間である．

(G2) $\mathbb{K}_M^n$ をサイズ $M \times n$ の $\mathbb{K}$ 上の行列全体 $\mathcal{M}$ と同一視すれば，$\mathcal{C}$ に対して等号 $d_R(\mathcal{C}) = d$ が成りたつ．

この二つの帰結として，「ガビドゥーリン符号 $\mathcal{C}$ は MRD 符号である」が得られる．以下，解説していく．

性質 (G1) を示すには，パリティ検査行列 H のランクが $d-1$ であることを示せばよい．実は，H を第 1 列から第 $d-1$ 列に制限して作ったサイ

[8] 特に，どんな知識が必要かは，著者が２０１４年９月に行われた誤り訂正符号のワークショップ [4] にて行ったガビドゥーリン符号の解説にて詳細を述べている．解説時のスライド等があるので，興味のある読者はそれを参照頂きたい．

ズ $d-1 \times d-1$ の（正方）行列が正則であることからわかる．正則であることは，「各 $h_1, h_2 \ldots, h_n$ が $\mathbb{K}$ 上一次独立であること」，「$\mathbb{K}$ の濃度が q であること」，そして，「次の構造

$$\begin{pmatrix} h_1^{[0]} & h_2^{[0]} & \ldots & h_j^{[0]} \\ h_1^{[1]} & h_2^{[1]} & \ldots & h_j^{[1]} \\ \vdots & \vdots & & \vdots \\ h_1^{[j-1]} & h_2^{[j-1]} & \ldots & h_j^{[j-1]} \end{pmatrix}$$

を持つ行列が正則であることの必要十分条件が，$h_1, h_2, \ldots, h_j$ が q 元体上一次独立であること」からわかる．

式 (17) から，ランク距離に基づく一般的な評価式として

$$n - (n - d + 1) \geq d_R(\mathcal{C}) - 1$$

が従う．特に左辺は $d-1$ だから，$d \geq d_R(\mathcal{C})$ を意味する．性質 (G2) とは，

$$d \leq d_R(\mathcal{C}) \tag{19}$$

の成立を意味している．

ところで，ガビドゥーリン符号の性質を論じるときは，次の性質が有用である．

- ベクトル $v \in \mathbb{K}_M^n$ に対し，「対応する行列のランクが r 以下である」ことと，「$\mathbb{K}_M$ 上の r 次元ベクトル $z \in \mathbb{K}_M^r$ と，サイズ $r \times n$ の $\mathbb{K}$ 上の行列 Z であってランクが r であるものが存在し，$v = zZ$ と表せる」ことは同値．

- サイズ $r \times n$ の $\mathbb{K}$ 上の任意の行列 Z に対して，ある $g_1, g_2, \ldots, g_r \in \mathbb{K}_M$ により，

$$HZ^T = \begin{pmatrix} g_1^{[0]} & g_2^{[0]} & \ldots & g_r^{[0]} \\ g_1^{[1]} & g_2^{[1]} & \ldots & g_r^{[1]} \\ \vdots & \vdots & & \vdots \\ g_1^{[d-2]} & g_2^{[d-2]} & \ldots & g_r^{[d-2]} \end{pmatrix} \tag{20}$$

と表せる．とくに，Z のランクが r であれば $g_1, g_2, \ldots, g_r$ は $\mathbb{K}$ 上一次独立．

さて，性質 (G2) を示すために，その十分条件である，式 (19) を示そう．$\mathcal{C}$ が減法について閉じていることから，$\mathcal{C}$ のゼロベクトルでないどの元のランクも d 以上であることを示せばよい．つまり，$\mathcal{C}$ のゼロベクトルでない元のランクは $d-1$ 以下にはなり得ないことを示せばよい．つまり，「$\mathcal{C}$ のゼロベクトルでない任意の元 c は，$\mathbb{K}_M$ 上の $d-1$ 次元ベクトル $z \in \mathbb{K}_M^{d-1}$ とサイズ $(d-1)\times n$ の $\mathbb{K}$ 上の行列 Z でランクが $d-1$ であるものをどのように選んでも $c = zZ$ とは表せない」ことを示せばよい．

Z として，サイズ $(d-1)\times n$ の $\mathbb{K}$ 上の行列であり，そのランクを $d-1$ とする．パリティ検査行列 H と掛け合わせた HZ^T を考察する．式 (20) により，

$$HZ^T = \begin{pmatrix} g_1^{[0]} & g_2^{[0]} & \cdots & g_{d-1}^{[0]} \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_{d-1}^{[1]} \\ \vdots & \vdots & & \vdots \\ g_1^{[d-2]} & g_2^{[d-2]} & \cdots & g_{d-1}^{[d-2]} \end{pmatrix}$$

と表せる．特に，$g_1, g_2, \ldots, g_{d-1}$ は $\mathbb{K}$ 上一次独立である．この一次独立性と，HZ^T の正則性が同値であるから，

$$0 = HZ^T z^T = Hc^T$$

となる z はゼロベクトルに限られる．ちなみにこの式は c が符号 $\mathcal{C}$ の元であることの必要十分条件である．以上から，ランク $d-1$ 以下の符号語 $c(= zZ)$ はゼロベクトルに限られることがわかった．

よって，$d \le d_R(\mathcal{C})$ を満足し，$\mathcal{C}$ が MRD 符号であることがわかった．

余談になるが，パリティ検査行列 H を定めた $h_1, h_2, \ldots, h_n$ として，ある元 $a \in \mathbb{K}_M$ をうまく選ぶと $h_i := a^{[i-1]}$ とできることがわかる．つまり，$a^{[0]}, a^{[1]}, \ldots, a^{[n-1]}$ が $\mathbb{K}$ 上一次独立，つまり，基底にできる．このような基底は**正規基底**と呼ばれ，文献 [6] に存在性等が解説されている．正規基底を用いると，ガビドゥーリン符号のパリティ検査行列がリード・ソロモン符号のパリティ検査行列の類似にみえてくる．さらに，リード・ソロモン符号では符号語を多項式に対応させることができたように，ガビドゥーリン符号では符号語を線形化多項式に対応させることができる．線形化多項式は，合成に関して閉じていることから，合成を積として符号に非可換環の構造を与える．非可換環であっても，ユークリッド整域の性質を持つことがわかり，ユークリッド互除法を適用することができる．これは，次節でさらっと述べる，誤り訂正アルゴリズムに関連する事項である．

7　誤り訂正の為のアルゴリズムなど

文献 [9] では，ガビドゥーリン符号の復号アルゴリズム（誤り訂正アルゴリズム）も記述されている．リード・ソロモン符号の復号アルゴリズムの 1 つ「ユークリッド復号」の類似で計算できることが述べられいて大変興味深い．ただ，ここでは紙面の制限により割愛する．

他にも文献 [9] では，ガビドゥーリン符号のスペクトル（重み分布，母関数）が決定されている．こちらも非常に面白い．

Acknowledgment

本研究は JSPS 科研費 25289118，および，26289116 の助成を受けたものです．

参考文献

[1] Tom Richardson and Ruediger Urbanke, *Modern Coding Theory*, Cambridge University Press, 2008.

[2] Claude E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal 27 (3): 379-423. doi:10.1002/j.1538-7305.1948.tb01338.x.

[3] S. Kudekar, T. Richardson, and R. Urbanke, *Threshold saturation via spatial coupling: Why convolutional LDPC ensembles perform so well over the BEC*, IEEE Trans. Inf. Theory, vol.57, no.2, pp.803-834, Feb. 2011.

[4] 誤り訂正符号のワークショップ公式ホームページ, *http://manau.jp/WS/ECCWS/*

[5] *Information Theory and Network Coding (Information Technology: Transmission, Processing and Storage)*, Raymond W. Yeung, Springer; 2008 edition, ISBN-10: 0387792333, ISBN-13: 978-0387792330.

[6] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Press, 1997.

[7] 萩原学，符号理論～デジタルコミュニケーションにおける数学～, 日本評論社, 2012.

[8] 今井秀樹, 符号理論, 電子情報通信学会, 1990.

[9] E. M. Gabidulin, *Theory of Codes with Maximum Rank Distance*, Problems of Information Transmission, 21 (1): pp.1-12, 1985.

[10] R. Stanley, *Enumarative Combinatorics*, 2nd Edition, Cambridge University Press, 2011.