■1 群（信号・システム）- 2 編（符号理論）

7 章 符号理論の応用

（執筆者：鎌部　浩）[2013 年 10 月 受領]

■概要■

符号理論では，性能の良い符号を構成することを目的として様々な符号が提案されてきたが，それらを実際のシステムに応用するときには，どのような符号を選択するのかが大きな問題となる．選択の基準としては単に誤り訂正能力の高さだけではなく，対象とするシステムとの適合性や，応用対象が必要とする性質をもつように符号を設計できるかどうかが問題となってくる．本章では，応用においてどのような符号がどのように使用されているのか，どのような組合せが考えられているのか，符号に対してどのような性質が要求されているのかなどに重点を置いて，符号理論の応用について述べる．

衛星通信や携帯電話などのように高い信頼性が必要とされ，なおかつ，受信者側から送信者側への通信手段がある場合には，誤りを検出した場合に再送要求を送信することで信頼性を高めることができる．こうした通信路の誤り制御方式とその応用例について述べる．

符号理論の初期の応用例は計算機システムである．ハミング符号は真空管方式の計算機の信頼性を向上させるために発明されたが，現在でもこの符号を拡張した符号が使用されている．また，磁気ディスク装置などの外部記憶装置では，誤り訂正の機構なしには装置の存在意義がなくなってしまうほど，誤り訂正技術は重要な構成要素となっている．これらの装置は記憶のある通信路の典型例でもある．

符号理論の成果の最も重要な応用は通信である．近年では移動体通信，無線データ通信などの応用が重要になってきている．また，通信へ符号理論を応用するときには，変調との組合せを考慮することが非常に重要であり，これらについて概説する．

近い将来非常に重要になってくる応用の一つが量子通信である．この方式では本質的に誤りを含んでいるので，誤り訂正の機構は基本的な構成要素の一つである．

系列に関する理論は誤り訂正の理論とは異るが，スペクトル拡散，電子すかし，疑似乱数系列，ストリーム暗号などに広く応用されるようになっており，これらの基礎について解説する．

符号理論は，ネットワーク，分散ストレージ，暗号など非常に幅広い分野に応用されるようになってきている．そうした応用例の一つとして暗号への応用について最後に述べる．

【本章の構成】

本章は，誤り検出と再送（7-1 節），計算機のための符号（7-2 節），記憶装置のための符号（7-3 節），移動通信のための符号（7-4 節），符号化変調（7-5 節），時空間符号（7-6 節），量子誤り訂正符号（7-7 節），系列（7-8 節），符号理論の他分野への応用（7-9 節）からなる．

■1 群 - 2 編 - 7 章

7-1 誤り検出と再送

（執筆者：新家稔央）[2013 年 10 月 受領]

7-1-1 誤り検出

誤り検出（error detection）とは，受信系列に 1 ビットでも誤りがあると判断できる場合，誤りの訂正を行わずに誤りがあることを宣言して復号を終了することである．誤り検出では，符号の最小ハミング距離 $d_{\min}$ に対し，$d_{\min}-1$ 個までの誤りが生じても，シンドロームの計算によってこれを検出できる．

いま，正しく復号ができる確率を P_c，誤りが検出される確率を P_d，復号誤り確率（または，見逃し誤り確率）を P_e とする．すると，誤り検出では，誤り訂正をする場合よりも P_c が小さくなることを許す一方，P_e を非常に小さくすることが可能である．ここで，$P_c+P_d+P_e=1$ である．誤り検出では，誤りが検出されたあとの対処法がいくつかあるが，このなかで最も代表的な方法が後述する自動再送要求方式である．

(1) CRC：誤り検出をする符号の例

CRC（Cycric Redundancy Check）とは，巡回符号を用いた誤り検出の方式である．よく用いられる巡回符号の生成多項式 $g(x)$ は，$g(x)=1+X^5+X^{12}+X^{16}$ である．この生成多項式により，冗長シンボル数 $m=16$ ビットが送信する情報シンボル数 k に付加される．この $G(x)$ の周期 p は $p=32767$ であるので，符号長 $n=k+m\le p$ のときに $d_{\min}=4$ となる．したがって，3 個以下のランダム誤り，及び 16 ビット以下の任意のバースト誤りを検出できる．

7-1-2 自動再送要求方式

受信側から送信側への通信路を帰還通信路と呼ぶ．帰還通信路が利用できる場合，帰還通信路を用いて送信側に再送を要求することで，信頼度を高める方式が研究されてきた．この方式を自動再送要求（Automatic Repeat reQuest）（ARQ）方式と呼ぶ．

(1) 確認信号と符号語送信のタイミングによる ARQ 方式の分類

送信側では，伝送するメッセージを符号の情報シンボル数 k ごとのフレームに分割して符号化を行う．ARQ 方式では誤りが検出された場合に再送要求を求めるため，受信側より送信側へフレームごとに確認信号を送る必要がある．受け取った受信系列に誤りが含まれないと判断した場合に送信側へ送られる確認信号を ACK（positive acknowledgement），誤りが検出されて受信系列を棄却する場合に送られる確認信号を NAK（negative acknowledegment）と呼ぶ．なお，送信側では，一定時間の間に ACK が返ってこない場合に，これを NAK とみなす場合もある．送信側では確認信号を受け取り，その後に送信するフレームを符号化して送信を行うが，そのタイミングによって ARQ 方式は以下の 3 種類に大別される．

(a) Stop and wait 方式

最も基本的な方式であり，送信側は確認信号を受信するまで次の送信を待つ．ACK が受信された場合には次のフレームを送信し，NAK の場合には同じフレームの再送をする．

(b) Go Back N 方式

送信側では，確認信号を受け取ったか否かによらず，順番に次々とフレームを符号化して送信する．ただし，受信側からの NAK を受け取った場合には，NAK に対応する時点から順

番にすべてのフレームを再送し直す（図 7･1）.

（c）Selective repeat 方式

Go Back N 方式と同様，送信側が次々と順番にフレームを送信するが，受信側に十分に大きなバッファがあることを仮定する．送信側では NAK が返ってきた情報のみを再送し，受信側では，ACK と判断されたフレームをバッファから取り出して順番に並べ替える．したがって，三つの方式のなかでスループットは最大となるが，再送が頻繁に起きる状況では大きなバッファが必要となる[1].

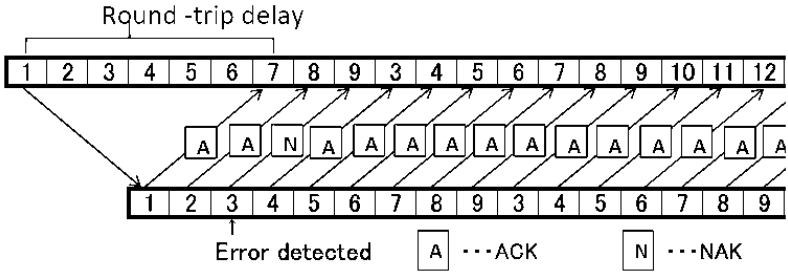

図 7･1 Go Back N **方式**

(2) ハイブリッド ARQ 方式

誤りが検出された場合に，必ず受信系列の再送を行うのではなく，ある程度の誤り訂正を併用する方式をハイブリッド ARQ 方式と呼ぶ．誤り訂正を併用しない ARQ 方式では，再送要求が頻発する状況下におけるスループットの低下が著しくなる．これに対しハイブリッド ARQ 方式では，このような状況下におけるスループットの低下を食い止めることができる．なお，ハイブリッド ARQ 方式には，再送要求が出されたときに 1 度目に送った符号系列と同じ系列を送信するタイプ 1 の方式と，異なる系列を送信するタイプ 2 の方式に大別ができる．

（a）タイプ 1 ハイブリッド ARQ 方式

タイプ 1 の方式では，一部の誤りの訂正を行い，それ以外の誤りの検出をしたときは再送の要求をする．このため，あらかじめ訂正能力の高い符号を用いることが必要であり，その符号の冗長シンボル数は大きくなる．この結果，再送要求がほとんど起きない状況下でのスループットが低いという特徴をもつ[2].

（b）タイプ 2 ハイブリッド ARQ 方式

文献 3) などに代表されるタイプ 2 の方式には，様々な提案がある．しかし，端的に表現すれば，「再送要求をすべき誤りが受信系列から検出されたとき，この系列を捨てず，送信側に更なる冗長シンボルの送信を要求する．そして，新たに受信した冗長シンボルと一緒に誤り訂正を試みることで信頼度を確保する方式」である．したがって，タイプ 1 よりもスループットは向上する．

■1 群 - 2 編 - 7 章

7-2 計算機のための符号

（執筆者：藤原英二）[2013 年 10 月 受領]

7-2-1 半導体メモリ用符号[4)]

半導体メモリ用符号の機能は RAM 素子の構造に依存している．すなわち，素子の入出力（I/O）データ幅が，1 ビットから 4 ビットへ，更に最近では 8 ビット，16 ビット，32 ビットへ変遷しており，それに伴い 1 ビット誤り，その後 4 ビットなどの複数ビットの誤り，すなわちバイト誤りに対する訂正・検出機能を有する符号へと変遷している．

（1）ビット誤り制御符号：

1 ビット I/O データ幅を有する RAM 素子を使用したメモリシステムでは，素子のいかなる誤りも 1 ビット誤りとなることから，1 素子の誤りはすべて訂正し 2 素子の同時誤りはすべて検出する 1 ビット誤り訂正・2 ビット誤り検出ハミング符号（SEC-DED Hamming code）が使用されている．特に高速な符号化・復号とその回路量の最適化を図った修正ハミング符号として，奇数重み列符号（odd-weight-column code）が多用されている．

（2）バイト誤り制御符号：

複数ビット（b ビット，b は 2 以上の整数）の塊りをバイトと称し，主として $b = 4$ ビットのバイト誤りを対象に GF(2^b) 上のリード - ソロモン符号（Reed-Solomon code）を拡張した 1 バイト誤り訂正・2 バイト誤り検出符号（SbEC-DbED code）が適用されている．

（3）スポッティバイト誤り制御符号：

近年主流の $b = 8$ ビット以上のバイト入出力 RAM 素子では，バイト中のせいぜい 2 または 3 ビットまでの誤りが主体である．これから，一般に，b ビットバイト内 t ビット（$1 < t < b$, t は整数）までの誤りをスポッティバイト誤りと称し，任意の b，t 値に対し，各種スポッティバイト誤り制御符号（spotty-byte error control code）が研究開発されている．

（4）ビット/バイト/スポッティバイト複合誤り制御符号：

以上の誤り制御機能を組み合わせた各種複合誤り制御符号（complex error control code）が多く提案されている．その内，特に，1 ビット誤り訂正・2 ビット誤り検出・1 バイト誤り検出符号（SEC-DED-SbED code）は，SEC-DED 符号と比較して検査ビット数の増加が少なく回路量の増加も極めて少ないことから，特に $b = 4$ ビットのバイト入出力を有する RAM 素子を使用したメモリシステムに適用されている．

7-2-2 プロセッサ用符号

一般にプロセッサ内の論理回路への符号の応用は限定的である．乗算器，除算器を対象に剰余-3 検査符号（residue-3 code），及び加算器などにパリティ予知検査（parity prediction check），またデータパス回路部へはパリティ検査符号（parity check code）が多用されている．また，バイトまたはシンボル単位の誤り検査を可能とするチェックサム符号（checksum code）が加算器における検査シンボル予知検査（check symbol prediction check）として使用されている．

一方，最近のマイクロプロセッサにおいては，チップの高集積化，素子の微細化に伴い，電源電圧レベルの低下，ノイズ，外部粒子，信号カップリング，等の影響，及び内在するキャッ

シュメモリ容量の増大に伴うソフトエラー（soft error）の増加に対して，パリティ検査符号，SEC-DED 符号，及び SEC-DED-S*b*ED 符号が適用されている[5]．

■1 群 - 2 編 - 7 章

7-3 記憶装置のための符号

（執筆者：井上 徹）[2013 年 10 月 受領]

記録媒体が磁気系メディア主体の時代にはあまり訂正時間に時間をかけず，軽く誤り訂正を実行してみて訂正できないと判断された誤りをデータの再読み込み（リトライ）などシステム側で救済する手段がとられていた．ところが記録機器に光ディスクが多用され，記録容量も大容量化しかつ入出力に要する時間も高速化されるようになるとデータ読み込み実行時間中（on-the-fly）に訂正できるよう，より強力な方式が要求されるようになってきている．誤りパターンを訂正する符号は圧倒的に GF(2^8) 上のリード-ソロモン（Reed-Solomon）符号が多く使われている．記録系の誤り訂正を考える場合，媒体の欠陥や埃，汚れによるドロップアウトなどを測定し，インタリーブ段数や欠落したデータの補間まで含む誤り訂正能力の必要な値を決定し，符号語フォーマットを決定することになる．

実際の伝送路は記録系ではドロップアウトによるバースト誤りが主として発生する．このような記憶のある通信路を模擬する数学モデルとしてギルバート（Gilbert）モデルが用いられる．E.N. Gilbert は誤りのない状態 G（good state）と誤りが発生する状態 B（bad state）及びこれらの状態が持続する確率 Q, q と互いに二つの状態 G と B を遷移する確率 P, p を定義し，更に B の状態でデータが正しい確率 h を定義した．h はバースト誤り状態において誤らないビットの生起確率で “0” と “1” が等しい確率で生起するとすると $h = 0.5$ である．$Q = 1 - P$，$q = 1 - p$ であるから三つのパラメータ P, p, h で通信路を表現したことになる．ギルバートモデルは $P + p = 1$ のときランダム誤り状態を表現する．しかし 2 状態のギルバートモデルで実際の記録系の誤り状態を表現するのは難しく，実際には二つの bad state と一つの good state をもつ 3 状態ギルバートモデルが使われる．ギルバートモデルは幾何分布に従うが，実際には指数分布で近似したモデルが使われる．この近似の誤差はわずかであり，実用上は差し支えない[6]．

CD プレーヤの誤り訂正符号として用いられている CIRC 符号は $(32, 28, 5)$ と $(28, 24, 5)$ のリード・ソロモン符号による 2 重符号化方式が使われている．DVD は CD より 10 余年後に世に出たためその間の技術成果を取り入れ，記憶容量 4.7GB をもち 1 本の映画を 1 枚のディスクに収容できる．$(182, 172, 11)$ と $(208, 192, 17)$ リード-ソロモン積符号が使われている．磁気記録系では固定ヘッド方式のマルチトラック PCM 録音機にリード-ソロモン符号と CRC による一般化積符号が，また DAT では $(32, 28, 5)$ と $(32, 26, 7)$ リード-ソロモン積符号が用いられている．業務用ディジタル VTR はコンポーネント信号記録の D1 方式に 3×5 のリード-ソロモン積符号，とコンポジット信号記録の D2 方式に 5×9 のリード-ソロモン積符号が採用されている．ブルーレイ（blu-ray）ディスクには $(248, 216, 33)$ と $(62, 30, 33)$ リード-ソロモン符号符号が組み合わされて使われている．

■1 群 - 2 編 - 7 章

7-4 移動通信のための符号

（執筆者：須田博人）[2013 年 10 月 受領]

本節では移動通信のなかでも特に広く利用されている携帯電話を取り上げ，そこに応用されている誤り訂正符号の事例を解説する．2009 年 3 月現在の携帯電話は，日本では 1 億件を越す利用契約があり，世界での利用は 40 億件を越え，日本はもちろん世界でも 1 人 1 台の時代に入ってきている．移動しながら無線通信を行う携帯電話においては，干渉やフェージング（電波の受信レベル減衰）などが常時発生し，伝送路の品質は劣悪でかつ変動も激しい．そのような伝送路環境でも安定した品質で情報を送受信するため，誤り訂正符号は携帯電話における必須技術となっている．

携帯電話は，元々は自動車電話システム（セルラーシステムとも呼ばれる）から発展してきたもので，現在は第 3 世代まで進化しその普及が広がっている．現在も利用されている第 2 世代は初のディジタル伝送方式（第 1 世代はアナログ伝送方式）であり，誤り訂正符号が本格的に利用されるようになった世代でもある．そこではディジタル化された電話音声の伝送品質向上を目的に，畳込み符号が利用されている．

第 3 世代方式は，世界で共通に使える携帯電話の実現を狙いとして開発され，IMT-2000（International Mobile Telephone 2000）とも呼ばれる．音声だけでなくインターネットの情報などデータや画像の伝送も行われ，ターボ符号が用いられている．ターボ符号の応用としては，携帯電話が最大規模の分野の一つといえよう．以下では，第 2 世代及び第 3 世代の携帯電話における符号の応用を述べる．

7-4-1 第 2 世代携帯電話の符号

第 2 世代方式の開発では，アナログ方式の第 1 世代からディジタル方式への変更が大きな技術的課題であった．ディジタル化によるコスト削減はもちろんのこと，アナログ方式との比較において伝送品質の向上と周波数利用効率の向上の両方の実現が必須となっていた．帯域圧縮（符号化率を上げること，または周波数利用率向上）と伝送品質向上とはトレードオフの関係にあり，アナログ方式と同等以上に両者をバランスさせることは難しい課題である．以下ではそのための音声伝送用の誤り訂正符号の技術として，PDC Half-rate[7]（PSI-CELP: Pitch Synchronous Innovation CELP）で用いられている，Unequal Error Protection（UEP），CRC を用いた補間，誤り訂正符号とベクトル量子化の組合せのマッピングの 3 点について説明する．

（1）UEP（不均一誤り保護）：

高い周波数利用効率が求められる携帯電話では，高能率音声符号化が適用され，通常の PCM 符号化では 64Kbps となる音声情報を，10kps 程度以下（PSI-CELP では 3.45kbps）で符号化している．高能率音声符号化では，音声波形を AR（Auto Regressive）モデルで近似し，その AR 係数と残差波形を送信することで情報源圧縮（符号化）を行うことがベースとなる．伝送路で誤りが発生すると，その誤りが残差波形に重畳しても復号音声に生じる歪は小さいが，一方で AR 係数に重畳すると大きな歪が発生する．実際に，PSI-CELP で符号化されたビットの誤り感度を測定してみると，10dB 以上の違いがある．第 2 世代では，この誤り感度の

高いビットだけを選択して，そこだけに FEC を適用する UEP を採用している．PSI-CELP の 138 ビット（1 フレームの符号化ビット）中，感度の高い 66 ビットを選別し，そこに符号化率 1/2，拘束長 8 の畳込み符号（軟判定復号）を適用している．

(2) 補　間：

携帯電話の伝送路は劣悪なため，符号化率 1/2 の畳込みであっても訂正しきれない場合がある．残留誤りが存在するままで音声の復号化を行うと，大きな歪（バリッというような耳に痛い雑音）が発生する．これを避けるため，送信側ではまず CRC を適用しその後に畳込み符号化し，復号側では CRC チェックを行い，残留誤りが検出された場合には，そのフレームの受信ビットは捨て，前のフレームの音声波形を繰り返し用いるなどの復号波形の補間処理を行う．CRC を適用するビットの範囲を広くし過ぎると補間頻度が増えて音声品質が劣化するので，PSI-CELP では UEP の 66 ビット中更に誤り感度の高い 54 ビットだけに CRC を適用している．

(3) マッピング：

ベクトル量子化されたビットの誤り感度について，量子化のマッピングテーブルの工夫により（量子化歪を増加させることなく），強弱を付けることが可能である．PSI-CELP では，7 ビットのベクトル量子化のマッピングテーブルに工夫をして，7 ビット中の 4 ビットはできるだけ誤り感度を低く，残りの 3 ビットは誤り感度が高くてもよい（メリハリを付ける）調整をしている．そして，誤り感度の高い 3 ビットは UEP で保護し，感度の低い 4 ビットは保護なしで送信するフレーム構成としている．以上まとめると，PSI-CELP では 3.45kbps の音声符号化に 2.15kbps（CRC と畳込み符号）を組み合わせ，合計 5.6kbps で携帯電話の音声伝送を実現し，アナログ音声伝送と同程度以上の品質を，約 2 倍の周波数利用効率で実現している．

7-4-2 第 3 世代携帯電話の符号

(1) ターボ符号

第 2 世代では電話（がいわゆるキラーアプリであり）音声を効率的に伝送することが最重要な課題であったが，第 3 世代ではマルチメディア情報の効率的伝送の実現が技術課題となった．誤り訂正符号の設計の視点では，多様な長さのパケット（情報ビット 50 ビット程度から 5 千ビット程度まで）を，ビット誤り率 10 の –6 乗程度の品質で，効率よく伝送できる移動無線伝送路用の FEC の選択・設計が課題であり，基本的にターボ符号が選ばれている．

図 7･2 に，第 3 世代の標準方式として広く普及している W-CDMA 方式に適用されているターボ符号（図 7･2 では turbo と表記：recursive systematic convolutional codes の状態数 8）の特性を示す．横軸に最大ドップラー周波数をとり，符号長（情報ビット長）をパラメータとして 10 の –6 乗の BER を得るために所要受信電力を示している．また比較のため畳込み符号と Reed-Solomon 符号の連節符号（図 7･2 では CC-RS 表記）の特性も示す．ターボ符号の性能は連節符号より高く，符号長（L_{turbo}）が長い場合には特に優れている．

ただし，新たに解決すべき課題として，符号長を自在に変えられる（符号長を変えても高い利得を確保する）ことが，ターボ符号（第 3 世代の符号）に要求された．マルチメディアに対応するためには当然必要な条件であるが，ターボ符号にとっては任意の符号長における良好な内部インタリーバの構成という技術課題は，簡単ではなかった．多くの提案が行われ，W-CDMA

方式では素体を利用したランダム化の特徴をもつインタリーバ[8]（prime interleaver）が採用された．第 3 世代のターボ符号では，符号長を 100 ビット程度から 1 万ビット程度まで可変にできる内部インタリーバ技術が用いられている．

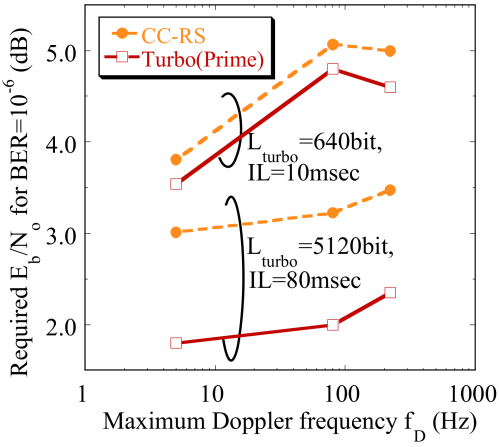

図 7･2　ターボ符号と連接符号の特性比較

（2）その他の符号

第 3 世代では，マルチキャスト技術（MBMS: Multimedia Broadcast Multicast Service）[9]が標準化されており，そこでは Raptor 符号[10] が適用されている．Raptor 符号は Fountain 符号の一つであり，符号の冗長ビットを On-the-fly で必要なだけ（泉から水が涌くように）生成できる特徴がある．移動通信のマルチキャストにも好都合である．また，Raptor 符号は universal 性（送信したい情報のビット数よりもわずかでも多くの正しいビット数が受信さえできれば，その受信ビットの位置にかかわらず，目的の送信情報を復号できる性質）をもつため，効率もよい．

ベストエフォートサービスを提供している第 3 世代では，ハイブリッド ARQ[11]と AMC（Adaptive Modulation and Coding scheme）にパケットスケジューリングを組み合わせて，効率のよい携帯電話のマルチアクセスを実現している[11]．ハイブリッド ARQ は，ターボ符号と再送制御の組合せで構成され，再送制御は不達のパケットが発生すると，それまではパンクチャ処理により送られていなかったターボ符号の冗長ビットを送信する方法（IR: Incremental Redundancy 法）を基本として用いている．

■1 群 - 2 編 - 7 章

7-5 符号化変調

（執筆者：小西たつ美）[2013 年 10 月 受領]

伝送速度が重要視されるデータ通信では，誤り訂正符号の付加で伝送速度や帯域が犠牲にならない技術が求められてきた．1970 年代後半から 80 年代にかけて，今井-平川[12]，ウンガーベック（Ungerboeck）[13]らが提案した符号系列とディジタル変調信号を効果的に対応付ける手法は，それらを犠牲にせず誤り訂正符号を付加する方式として発展した．この符号化と変調を統合し設計する手法は，符号化変調（coded modulation）と呼ばれる．以下本節では，符号化変調の仕組みと概念について述べる．

1982 年にウンガーベックは，振幅変調（AM），位相変調（PSK），直交振幅変調（QAM）に対し，トレリス符号化変調（Trellis coded modulation）（TCM）方式を提案した[13]．図 7･3 に 8PSK-TCM 方式の例を示す．

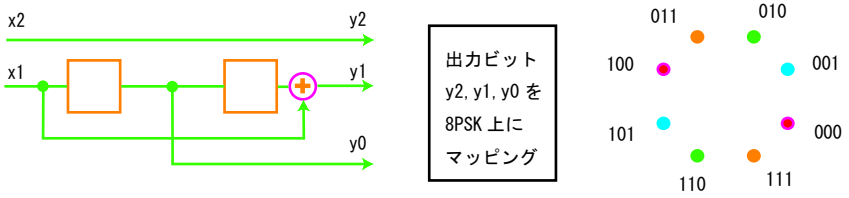

図 7･3　ウンガーベックの 8PSK トレリス符号化変調方式

符号器の 2 入力ビット $x1$ と $x2$ のうち，$x2$ は無符号化のまま出力ビット $y2$ となり，$x1$ は拘束長 3 の畳込み符号で符号化され，出力ビット $y1$，$y0$ になる．これら 3 出力ビット $y2, y1, y0$ は，8PSK 変調器の各信号点に割り当てられるが，この割当て（マッピング）をウンガーベックは，集合分割（set partitioning）という手法で行った．

8PSK の集合分割を図 7･4 に示す．図の一段目では，信号点間の最小ユークリッド距離は $d1$ であるが，$y0$ が 0 か 1 かで分割を行った二段目の信号点の部分集合では，信号点間の距離が $d2$ に増加する．このとき，この部分集合内の信号点の $y0$ の値は同じで，$y1$ または $y2$ の値は異なっている．続いて $y1$ の値で分割した三段目の部分集合では，$y1$ の値は同じで，$y2$ の値だけが異なり，その信号点間の最小ユークリッド距離は $d3$ になっている．よってこの分割の仕方では，$y0$ が等しければ，信号点間の距離は $d2$ 以上，$y1$ が等しければ信号点間の距離は $d3$ となることが保証される．

図 7･3 の TCM 方式のトレリス遷移の各状態間には，無符号化ビットによって，2 本のパラレルパスが存在するが，この無符号化パラレルパスは，図 7･4 の集合分割の三段目の部分集合に対応し，割り付けられた信号点間のユークリッド距離は，8PSK の信号点間距離として最大の $d3$ にできるため，無符号化パラレルパスに対応する信号点間の最小ユークリッド距離の 2 乗は $(d3)^2 = 4$ となる．

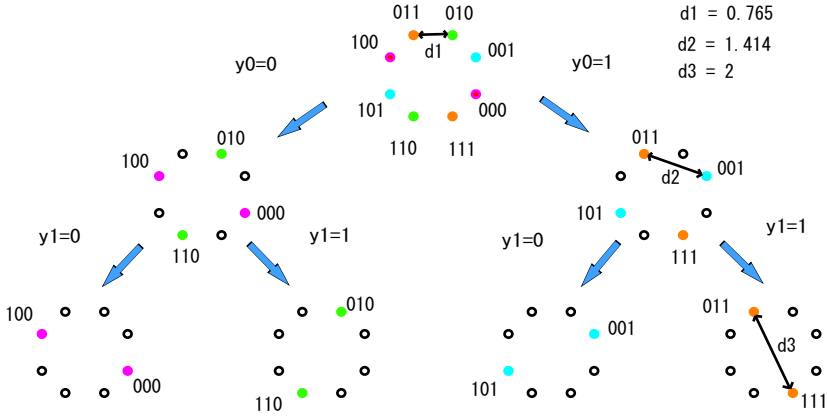

図 7･4　8PSK の集合分割

一方，図 7･3 の符号のトレリスパスの最小自由ユークリッド距離は，

$$(d2)^2 + (d1)^2 + (d2)^2 = 4.585$$

である．4 と 4.585 を比較した結果，この 8PSK-TCM 方式の最小自由ユークリッド距離は 4 になる．

この TCM 方式では，1 信号当たりの情報ビット数は 2 ビットで，無符号化 QPSK と同じであるので，無符号化 QPSK の最小ユークリッド距離の 2 乗が 2 であるのに対し，ウンガーベックの TCM 方式は，伝送速度や帯域の犠牲なしで，約 3dB の漸近的符号化利得が得られる．

このように集合分割により，信号点集合を最小ユークリッド距離が増加する部分集合に段階的に分割し，符号語と分割後の部分集合を対応づけることで，符号と変調信号の最小自由ユークリッド距離を直接結びつけることが可能になった．ただし，求められた最小自由ユークリッド距離は下界であり，常に真の値になるとは限らない．またその結果，符号化変調で用いる符号を，ユークリッド重み（の下界）を用いた線形符号として扱えるようになり，最良符号の探索が効率良く行えるようになった．

1 信号当たりの情報ビット数を 3 ビット以上にする場合は，2 次元または多次元の QAM 信号集合を用いる．多次元信号集合を用いた符号化変調では，一回の符号化で出力される符号化ビットを，複数個の 2 次元信号点に割り当てして送信する．この 2 次元または多次元信号点 QAM を用いた TCM は，主に音声帯域モデムを用いた高速データ通信や，固定無線中継方式などに利用されている．

例えば，国際電気通信連合（ITU-T）の音声帯域モデム国際標準規格で標準化されている V.32 では，二つの無符号化ビットと 32 個の信号点からなる十字型信号点配置を使い，1 シン

ボル当たり 4.0 ビットの帯域効果で，9,600bps のデータレートを実現し，無符号化 V.29 標準と比較して約 3.5dB の符号化利得を得ている．同じく V.33 では，符号器への入力ビットを 1 ビットとし，4 ビット無符号化で，128 信号点十字型配置 1 信号当たり 6.0 ビットを，V.34 では，多次元マッピングを用いることで，最高 1 信号当たり 10 ビット 33,600bps の伝送速度を達成している[15]．また，国際電気通信衛星機構（インテルサット）の公衆網でのディジタル衛星通信を提供する IDR（Intermedeate Data Rate）システムにおいて，8PSK 符号化変調方式が標準で採用されている．更に，トレリス符号化変調と時空間符号を組み合わせるシステムの研究も盛んに行われている[16]．

最後に，集合分割の数学表現について述べておく[17]．今，信号集合 S を生成する群を $U(S)$ とし，$U(S)$ の正規部分群を $U'(S)$，$U'(S)$ のコセットが対応する商群を $U(S)/U'(S)$ とする．信号集合 S が $U(S)$ の下での信号点 s_0 の軌跡で表せるとき，$U'(S)$ の複数のコセット下での s_0 の軌跡 S' は，互いに共通の元をもたない S の部分集合となり，正規部分群 $U'(S)$ によって引き起こされる S の分割 S/S' が得られる．これが集合分割の原理である．

ウンガーベックの符号のように，2 のべき乗個の信号点に 2 進系列の符号を割り当てる場合は，$U(S)/U(S')/U(S'')/\cdots$ と商群が多段階の 2 分割 $S/S'/S''/\cdots$ を引き起こす集合分割が利用される．

一般に集合分割は，信号集合を幾何学的に均一（geometrically uniform: GU）に分割する．GU とは信号集合 S 内の任意の s から s' への等長変換 $u_{s,s'}$ が，S を不変に保つ性質を指し，このような信号集合は任意の信号点に対するボロノイ領域が合同となるため，誤り率に代表される通信の重要な値が，信号点に依存しないという優れた性質をもつ．ただし QAM などで最も外側に位置する信号点には，別途考慮が必要である．

■1 群 - 2 編 - 7 章

7-6 時空間符号

（執筆者：大槻知明）[2013 年 10 月 受領]

時空間符号（STC: Space-Time Code）は，時空間領域で信号を事前処理（正負の反転，並び替え，複素共役など）して送信することにより，受信機において簡単な演算で空間あるいは時空間ダイバーシチを得る技術である．STC には，ダイバーシチ利得を目的とする時空間ブロック符号（STBC: Space-Time Block Code）と，ダイバーシチ利得と符号化利得の両方を目的とする時空間トレリス符号（STTC: Space-Time Trellis Code）の 2 種類がある．

7-6-1 時空間ブロック符号（STBC）

時空間ブロック符号（STBC）は，最大のダイバーシチ利得（フルダイバーシチ）とできるだけ高いスループットを，低複雑度の復号法で得ることを目的としている．符号という名前が付くものの，一般には符号化利得を目的としたものではなく，多送信アンテナに対する変調と見ることができる．送信アンテナが $N = 2$ 本の場合にフルダイバーシチを達成する手法として，アラモウチは STBC[18]を提案した．アラモウチの STBC では，2 シンボルを 2 本のアンテナから，2 シンボル時間にわたって送信する．2 シンボル $\mathcal{X}_1$，$\mathcal{X}_2$ を送信する場合，まずアンテナ 1, 2 から $\mathcal{X}_1, \mathcal{X}_2$ を，1 番目のシンボル時間にそれぞれ送信する．続くシンボル時間では，アンテナ 1 から $-\mathcal{X}_2^*$ を，アンテナ 2 から $\mathcal{X}_1^*$ をそれぞれ送信する．アラモウチの STBC は，1 シンボル時間当たり 1 シンボルを送信する．これは，フルダイバーシチを達成する符号の最大送信可能シンボル数であり，フルレートと呼ばれる．アラモウチの STBC は，受信アンテナ数が M であるとき，ダイバーシチ次数 $2M$ を与える．

次に，受信アンテナ数 $M = 1$ 本の場合の受信機での処理を考える．送信アンテナ 1, 2 から受信アンテナまでの通信路応答を，それぞれ $\mathcal{H}_1, \mathcal{H}_2$ とし，STBC のブロックサイズ 2 シンボル時間にわたって，それぞれ一定であるとする．2 シンボル時間での受信信号を $\mathcal{Y}_1, \mathcal{Y}_2$ とする．アラモウチの STBC は，受信信号に対して以下の簡単な線形演算を行うことにより，各送信アンテナからの信号を分離し，最ゆう検出する．

$$\tilde{\mathcal{X}}_1 = \mathcal{H}_1^* \mathcal{Y}_1 + \mathcal{H}_2 \mathcal{Y}_2^* \quad (7\cdot1)$$

$$\tilde{\mathcal{X}}_2 = \mathcal{H}_2^* \mathcal{Y}_1 - \mathcal{H}_1 \mathcal{Y}_2^*. \quad (7\cdot2)$$

なお，アラモウチの STBC では，送信機では通信路情報を用いないため，送信電力は送信アンテナ間で等分される．そのため，総送信電力が一定の場合，送信アンテナ数 $N = 1$，受信アンテナ数 $M = 2$ のシステムで MRC を用いる場合と比較すると，3dB 劣化する．

7-6-2 時空間トレリス符号（STTC）

時空間トレリス符号（STTC）は，複数のアンテナから送信される信号間に時間的空間的相関を付加し，ダイバーシチ利得と符号化利得の両方を得ることを目的としている．送信アンテナ数 N，受信アンテナ数 M の STTC システムを考える．QPSK，4 状態 STTC の場合，時刻 t で，情報ビット $\mathcal{U}_t = (\mathcal{U}_{t,1}, \mathcal{U}_{t,2})$ が時空間トレリス符号器に入力され，生成行列 G の各

行成分との積の和に modulo 4 をとったシンボル $(X_{t,1}, \cdots, X_{t,N})$ が符号器出力となる．N 個の出力符号語は，QPSK 変調後，各送信アンテナから同時に送信される．

図 7･5 に QPSK の信号配置及び[19]で報告されている QPSK，4 状態 STTC のトレリス遷移図をそれぞれ示す．ここで QPSK, 4 状態 STTC[19]の生成行列 G は，次式で与えられる．

$$G = \begin{pmatrix} 0 & 2 \\ 0 & 1 \\ 2 & 0 \\ 1 & 0 \end{pmatrix} \tag{7･3}$$

トレリス状態遷移図において，右側の送信シンボルは，状態 S_k からそれぞれ入力 0, 1, 2, 3 に対応する出力を表す．ここで，出力 2 シンボルのうち，左側のシンボルを第 1 送信アンテナから，右側のシンボルを第 2 送信アンテナから，それぞれ送信する．受信機では，このトレリス状態遷移図に基づき復号する．

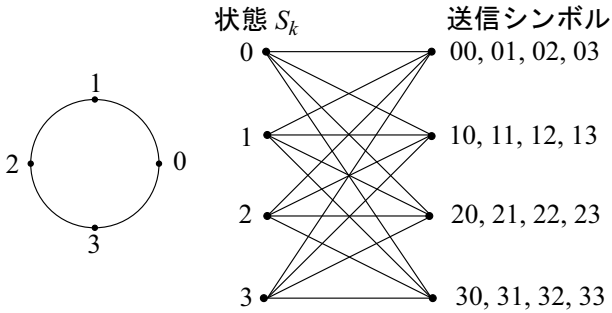

図 7･5　QPSK, 4 **状態** STTC[19]**状態遷移図**

■1 群 - 2 編 - 7 章

7-7 量子誤り訂正符号

（執筆者：浜田　充）[2013 年 10 月 受領]

量子計算機や通信において，情報を量子力学的なノイズから保護するための技術として量子誤り訂正符号が提案されている．本節では古典の線形誤り訂正符号に類似したシンプレクティック符号（symplectic codes）（ステイビライザ符号）について概説する．同符号のより詳しい解説は 文献 20) にある．

有限次元ヒルベルト空間 H に対し H 上の線形作用素全体の集合を L(H) で表す．以下では，H を 2 次元ヒルベルト空間とする．空間 H の正規直交基底を任意に固定し，$A \in \mathsf{L}(\mathsf{H})$ をこの基底に関する A の行列と同一視する．量子誤り訂正符号（quantum error-correcting codes）（量子符号）とは n 個の H のテンソル積 $\mathsf{H}^{\otimes n}$ の部分空間 C と復号を表す写像 $\mathcal{R} : \mathsf{L}(\mathsf{H}^{\otimes n}) \to \mathsf{L}(\mathsf{H}^{\otimes n})$ の組 $(C, \mathcal{R})$ であると定義する（通常 $\mathcal{R}$ には物理に起因する制約を課す）．古典の場合と同様に，復号を外し部分空間 C のみを符号と呼ぶことの方が多いので，本節でもこの慣習に従う．作用素

$$N_{(0,0)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad N_{(1,0)} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad N_{(1,1)} = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}, \quad N_{(0,1)} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

を用いてシンプレクティック符号は定められる（i は虚数単位）．ここで，添え字に使われた $\{0,1\}$ を有限体（ガロア体）$\mathsf{F} = \mathrm{GF}(2) = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ とみなし，$x = (u_1, v_1, \ldots, u_n, v_n) \in \mathsf{F}^{2n}$ に対して $N_x = N_{(u_1,v_1)} \otimes \cdots \otimes N_{(u_n,v_n)}$ と定義する．更に，$J \subseteq \mathsf{F}^{2n}$ に対して N_J を $N_J = \{N_x \mid x \in J\}$ で定義する．また，二つのベクトル $x = (u_1, v_1, \ldots, u_n, v_n)$ と $y = (u'_1, v'_1, \ldots, u'_n, v'_n) \in \mathsf{F}^{2n}$ との間にシンプレクティックな双線形形式 $\mathsf{f}_{\mathrm{sp}}(x,y) = \sum_{i=1}^{n} u_i v'_i - v_i u'_i$ を定め，部分空間 $S \subseteq \mathsf{F}^{2n}$ の f_{sp} に関する双対を $S^{\perp_{\mathrm{sp}}} = \{y \in \mathsf{F}^{2n} \mid \forall x \in S, \mathsf{f}_{\mathrm{sp}}(x,y) = 0\}$ で定義する．

補題 1 [21, 22] 線形符号 $L \subseteq \mathsf{F}^{2n}$ と集合 $J_0 \subseteq \mathsf{F}^{2n}$ が $L^{\perp_{\mathrm{sp}}} \subseteq L$, $\dim L = n+k$ 及び $\forall x, y \in J_0$, [$x \neq y \Rightarrow y - x \notin L$] を満たしているものとする．このとき $\{\psi \in \mathsf{H}^{\otimes n} \mid \forall M \in N_{L^{\perp_{\mathrm{sp}}}}, M\psi = \tau(M)\psi\}$ というかたちの互いに直交した $\mathsf{H}^{\otimes n}$ の 2^k 次元部分空間を 2^{n-k} 個取ることができるが，これらはいずれも N_J 訂正符号である．ここに $J = \{z + w \mid z \in J_0, w \in L^{\perp_{\mathrm{sp}}}\}$ である．また $\tau(M)$ はスカラー量であり，したがって $M \in N_{L^{\perp_{\mathrm{sp}}}}$ の固有値である．　◇

この補題のなかで定められた「N_J 訂正符号」をシンプレクティック符号と呼ぶ．実質的に同じ符号クラスが [23] でも見いだされた．ここで N_J 訂正符号という用語の意味は古典の符号理論から類推しても大きな間違いはないが，正確な意味は文献 24) などを参照して戴きたい．上記補題の量子符号の性能は，$\{0,1\}^2 \simeq \mathrm{GF}(4)$ 上の古典符号とみなした L の性能に近い．ここで L は $\mathsf{F} = \mathrm{GF}(2)$ 上線形であるが， GF(4) 上は線形でもそうでなくてもよい．

■1 群 - 2 編 - 7 章

7-8 系　列

（執筆者：松藤信哉，棚田嘉博）[2013 年 10 月 受領]

系列（sequence）は，拡散系列（spreading sequence）や擬似乱数系列（pseudo-random sequence）として，スペクトル拡散通信，レーダ，電子透かし，暗号，スクランブルなどの通信，計測，情報セキュリティなどの幅広い分野に適用されている．本節では，系列の基本的事項及び代表的な系列について述べる．詳細は文献 33, 34, 35, 36) を参照いただきたい．

7-8-1 系列の分類

数値の並び $\cdots, a_{-2}, a_{-1}, a_0, a_1, a_2, \cdots$ を系列と呼び，$a = \{a_i\}$ と表す．また，各異なる系列の集合を系列セット，または，符号（code）と呼び，$S = \{a, b, \cdots, c\}$ と書く．また，$M = \|S\|$ は系列数を表す．

系列は，あるシステムへの適用を考慮して，有限長系列（finite length sequence）と周期系列（periodic sequence）に分けて議論される．系列長 N の有限長系列は，$i < 0, i > N$ において $a_i = 0$ として系列の両側は零と仮定し，周期 N の周期系列は，$a_i = a_{i+N}$ として同じ系列が繰り返し現れるものと仮定する．

更に，これらは要素 a_i の値の取り方により分けられる．複素値の要素からなる系列を複素系列，複素単位円周上の絶対値 1 の要素からなる系列を多相系列，実数値の要素からなる系列を実数系列，整数値の要素からなる系列を多値系列と呼ぶ．複素系列は，すべての系列を含むので，一般的に議論する場合に便利に扱われる．一方，系列要素が 0 から $q-1$ の q 値を取る系列を q 元系列，$q = 2$ の場合を 2 元系列または 2 値系列，$q = 4$ の場合を 4 元系列と呼ぶ．そして，一般には，q 元系列 $\{a_i\}$ は，$e^{\frac{2\pi\sqrt{-1}}{q}a_i}$ のように q 相系列に変換して議論される．

7-8-2 系列の相関関数

誤り訂正符号では，符号語間の最小ハミング距離が誤り訂正能力を表す指標となるが，系列では，系列間の相関関数（correlation function）が系列の乱雑さやシステム性能を表す指標となる．本節では，スペクトル拡散方式の直接拡散方式と周波数ホッピング方式で用いられる代表的な二つの相関関数を述べる．また，系列を周期系列と有限長系列に区別することにより，同じ式により相関関数を説明する．

周期 N，あるいは，系列長 N の二つの系列を $a = \{a_i\}$，$b = \{b_i\}$ とする．前者では，各々の系列の位相シフト τ において，

$$R_{ab}(\tau) = \sum_{i=0}^{N-1} a_{i+\tau} b_i^*$$

と定義する．ただし，b_i^* は b_i の複素共役を示す．ここで，$a = b$ の場合を自己相関関数と呼び，$a \neq b$ の場合を相互相関関数と呼ぶ．また，周期系列の場合を周期相関関数と呼び，有限長系列の場合を非周期相関関数と呼ぶ．一般には，q 元系列は q 相系列に変換して相関関数を議論する．

同様に，後者では，系列を q 元系列として，

$$H_{ab}(\tau) = \sum_{i=0}^{N-1} a_{i+\tau} \odot b_i$$

と定義する．ただし，$a_{i+\tau} \odot b_i$ は同じ値の場合 1, 異なる場合 0 と置く．このように，$H_{ab}(\tau)$ は，位相シフト τ における系列値の一致数を表し，ハミング距離を用いて表せるので，前者の相関関数と区別するために，ハミング相関関数と呼ぶ．ところで，巡回符号は周期系列として取り扱えることに注意しよう．

7-8-3 有限長系列

Barker 系列は，非周期自己相関関数のサイドローブ（シフト零以外）が絶対値 1 以下となる有限長系列である．最大の系列長は，2 元系列では 13，4 元系列でも 15 と短い．しかし，理想に近いインパルス的相関特性を有するので同期用系列として適用可能であり，系列長 11 の 2 元 Barker 系列は無線 LAN 規格に採用されている．Huffman 系列は，非周期自己相関関数が零シフトと端点以外零となる実数値，複素値の有限長系列であって，任意の長さに対して，無限個構成できる．

相補系列は，二つの系列 $\{a_i\}$ と $\{b_i\}$ の対を意味し，各々の非周期自己相関関数の同じ位相シフトにおける総和が $R_{aa}(\tau) + R_{bb}(\tau) = 0(\tau \neq 0)$ と理想的なインパルス特性を有する．相補系列は，最小の長さ K の相補系列から順に 2 倍の系列長 $K2^m(m \geq 0)$ の相補系列を多数構成できる．ここで，2 元相補系列では $K = 2, 10, 26$，4 元相補系列では，$K = 2, 3, 5, 13$ において存在する．また，非周期自己相関関数のサイドローブが偶数シフトで零値を取る偶差直交系列（E 系列）は，相補系列に含まれており，無線 LAN 規格に採用されている系列長 8 の 4 元相補系列は，4 元 E 系列でもある．

7-8-4 周期系列

周期系列の代表的な系列として M 系列（Maximum length sequence）がある．M 系列は，$GF(q)$ 上の n 次原始多項式 $f(x)$ を特性多項式とする n 段線形帰還シフトレジスタ（LFSR）により発生される最大周期 $q^n - 1$ をもつ q 元系列である．その周期自己相関関数のサイドローブが $R_{aa}(\tau) = -1(\tau \neq 0)$ とインパルス的特性であり，ほかの要素より 0 元だけが 1 個のみ少なく現れるという意味で平衡性を有す．また，長さ l $(1 \leq l \leq n)$ の同じ元の連なりが 1 周期において $1/q^l$ の割合で存在するように連なり性が優れていることなどの特徴を有す．このように，乱数性の高い系列なので，擬似乱数（PN: Pseudorandom Noise）系列は M 系列を指すことが多く，例えば，携帯電話方式 cdma2000 では，2 元 M 系列の一部を用いて，拡散系列を構成している．

M 系列から，複数個前の乱数値とまったく独立であるとみなすことができるような高次均等分布する乱数（TLP 乱数）を与えることができる．また，2 元 M 系列 $\{a_{i+k}\}$ の初期値 k を変えることにより，2 元 Barker 系列の性質に近い非周期自己相関関数が鋭い特性を有する有限長系列を与えることもできる．M 系列と同じ周期自己相関特性を有する系列に，周期 $4n - 1$ の 2 元平方剰余系列や周期 $q^n - 1$ の q 元 GMW 系列などがある．これらは，乱数列としての解析しやすさを示す尺度，または，乱雑さを示す尺度として使用される線形複雑度が大きいことで知られている．また，実数系列では，周期自己相関関数がインパルス特性を

有す直交系列が無限個構成できる．

7-8-5 直接拡散符号

Gold 系列は，周期 $N = 2^n - 1$ で系列数 $N + 2$ からなり，二つの同じ周期の 2 元 M 系列 $a = \{a_i\}$ と $b = \{b_i\}(b_i = a_{ri})$ を用いて $S = \{a, b, c^k(0 \le k \le N-1)\}, c_i^k = a_{i+k} + b_i$ として表せる．ただし，n は 4 の倍数でなく，$r = 2^{[(n+2)/2]} + 1$（$[x]$ は，x の整数部）である．その周期相関関数は $R_{aa}(0)$ 以外，3 値の値 $R_{ab}(\tau) \in \{-1, -1 \pm 2^{[(n+2)/2]}\}$ を取る周期自己・相互相関関数の低い 2 元線形符号である．n が奇数の場合，周期と系列数が等しい（$N = M$）と仮定したときの $R_{aa}(0)$ 以外の最大相関値 R_{max} が Sidelnikov の下界 $R_{max} \approx \sqrt{2N}$ を満足する．そのため，測位システム GPS や携帯電話方式 W-CDMA などに適用されている．また，n が 4 の倍数の場合，$\{a_{ri}\}$ は M 系列とはならないが，これらの線形和で与えられる Gold-like 系列は，Gold 系列と同様の相関特性を有する．また，パラメータ r の選択によっては M 系列間の周期相互相関関数が上記相関値を満たす場合があり，これをプリファードペアと呼んでいる．

小セット Kasami 系列は周期自己相関のサイドローブと周期相互相関の絶対最大値 R_{max} が Welch の下界 $R_{max} \approx \sqrt{N}$ に到達する．これは，周期 $2^n - 1$ の 2 元 M 系列と周期 $2^{n/2} - 1$ の 2 元 M 系列の線形和として表され，系列数は $2^{n/2}$ であり，M 系列を除いてすべて非平衡系列である．Bent 系列は，周期，系列数，周期相関特性が小セット Kasami 系列と同じですべて平衡系列からなる非線形符号である．ただし，n は 4 の倍数である．周期 $N = p^n - 1$ の Kumar-Moreno 系列は，Welch の下界を満たし，系列数が $N + 1$ と多い 4 元符号である．

更に，周期 $2^n - 1$（n は偶数）の Gold 系列または Gold-like 系列と Kasami 系列の組合せで，Gold 系列と同じ最大相関値で系列数 $M = 2^{n/2}(N + 2)$（n が 4 の倍数の場合，系列数は $M - 1$）となる 2 元符号である大セット Kasami 系列を構成できる．

周期自己・相互相関関数が $R_{aa}(\tau) = 0\ (1 \le |\tau| \le Z)$, $R_{ab}(\tau) = 0\ (0 \le |\tau| \le Z)$ と零相関領域（zero correlation zone）を有する周期 N の系列を ZCZ 系列と呼ぶ．系列数を M とすると $M \le N/(Z + 1)$ の関係がある．また，低い相関領域（low correlation zone）を有する系列を LCZ 系列と呼ぶ[37]．これらは，他局間干渉を除去あるいは低減できる準同期 CDMA 方式を提供できる．

7-8-6 光直交符号

光通信に適用される 2 元符号として光直交符号がある．これは，2 元系列間（2 相系列に変換しない）の周期自己相関関数のサイドローブと周期相互相関関数の最大値を R_{max} とすると，それらが，規定値以下となる符号である．系列数を M とすると，各系列の 1 の数が w，すなわち，$R_{aa}(0) = w$ の場合，$M \le \frac{(N-1)(N-2)\cdots(N-R_{max})}{(w-1)(w-2)\cdots(w-R_{max})}$ の関係がある．一般には，R_{max} は 1 あるいは 2 を仮定し，それを満足する多くの光直交系列が提案されている．

7-8-7 周波数ホッピング符号

周波数ホッピンング符号は，ハミング自己相関のサイドローブとハミング相互相関関数が低いこと以外に，帯域内で周波数が一様分布するために，系列の各要素が同確率で現れること，できるだけ大きくホッピングするように隣接の要素値の差が大きいことが望まれる．

代表的な符号として，OCC（One-Coincidence Code）符号がある．これは，ハミング自己・

相互相関関数が 1 となる q 元符号である．つまり，位相シフトした系列間の同じ要素が 1 回のみ一致するような巡回符号の特別な場合である．例えば，p を素数，m を正整数，$q = p^m$ としたとき，周期 $q-1$，系列数 q の OOC 符号が構成できる．また，系列長 $p-1$，系列数 $p-1$，ハミング非周期自己・相互相関関数が 1 以下となる OCC 符号もある．このときの周期自己・相互相関関数の最大値は 2 である．

■1 群 - 2 編 - 7 章

7-9 符号理論の他分野への応用

（執筆者：古原和邦）[2013 年 10 月 受領]

本節では，符号理論の他分野への応用例として，公開鍵暗号（public-key cryptosystems）と秘密分散（secret sharing）について解説する．なお，公開鍵暗号とは暗号化に使う鍵（暗号化鍵）を公開できる暗号方式のことであり，秘密分散とは秘密情報を複数に分割し，そのうちいくつか，もしくはすべてを集めることにより元の情報を復元する方式である．いずれも，重要情報を保護するうえで欠かせない要素技術となっている．

7-9-1 公開鍵暗号への応用

公開鍵暗号とは，暗号化に使う鍵（暗号化鍵あるいは公開鍵）を公開したとしても復号鍵を求めることが困難な暗号方式である．暗号化鍵を広く一般に公開できるため鍵の配布が容易になるという利点*と，すべての通信相手に同じ暗号化鍵を配布できるため，管理すべき復号鍵の数を一つにできるという利点がある．

公開鍵暗号は計算量的に困難な問題をもとに構成され，現在普及している多くの方式は素因数分解問題†あるいは離散対数問題‡をもとに構成されている．線形符号の復号問題をもとに公開鍵暗号を構成する試みは，1978 年にマクエリース（McEliece）により提案され，その方式はマクエリース暗号（McEliece cryptosystem）[25]として知られている．以下にそのアルゴリズムを示す．

McEliece 暗号

鍵生成アルゴリズム

入力: 乱数
出力: 秘密鍵 $(\boldsymbol{S}, \boldsymbol{P}, \Psi(\cdot))$，公開鍵 $(\boldsymbol{G}', t)$

Step 1: t 重誤り訂正可能な 2 元 (n, k) ゴッパ (Goppa) 符号の生成行列 $\boldsymbol{G}$ をランダムに生成する．また，それに対応する誤り訂正アルゴリズムを $\Psi(\cdot)$ とする．

Step 2: $k \times k$ の 2 元正則行列 $\boldsymbol{S}$ と，列の置換を表す 2 元 $n \times n$ 行列 $\boldsymbol{P}$ をランダムに生成．

Step 3: $(\boldsymbol{S}, \boldsymbol{P}, \Psi(\cdot))$ を秘密鍵として出力．

Step 4: $\boldsymbol{G}' = \boldsymbol{SGP}$ を計算し $(\boldsymbol{G}', t)$ を公開鍵として出力．

* ただし，改ざんや成りすましの可能な通信路経由で公開鍵を受け取った場合，その鍵が誰のものであるかを拇印（Fingerprint）やディジタル署名などを利用し確認しなければならない．これの確認を怠ると，攻撃者の鍵を別のエンティティの鍵として受け入れてしまい，そのエンティティ向けの暗号文を攻撃者に読まれる危険性がある．

† 与えられた合成数を素因数に分解する問題．

‡ 与えられた群の二つのもとの一方がもう一方にその群を構成する 2 項演算を何回適用することにより得られるかを求める問題．

暗号化アルゴリズム

入力: 2 元 k 次元行ベクトルとして表現された平文 $\boldsymbol{m}$，乱数
出力: 暗号文 $\boldsymbol{c}$

Step 1: 重み t の 2 元 n 次元行ベクトル $\boldsymbol{e}$ をランダムに生成.

Step 2: $\boldsymbol{c} := \boldsymbol{mG}' \oplus \boldsymbol{e}$ を計算し，$\boldsymbol{c}$ を出力．ここで，$\oplus$ は排他的論理和を表す.

復号アルゴリズム

入力: 暗号文 $\boldsymbol{c}$
出力: 平文 $\boldsymbol{m}$

Step 1: $\boldsymbol{c}$ に $\boldsymbol{P}$ の逆行列 $\boldsymbol{P}^{-1}$ を右からかける.

Step 2: $\boldsymbol{cP}^{-1}$ に誤り訂正アルゴリズム $\Psi(\cdot)$ を適用．$\boldsymbol{cP}^{-1} = (\boldsymbol{mS})\boldsymbol{G} \oplus \boldsymbol{eP}^{-1}$ なので $\boldsymbol{mS}$ が得られる.

Step 3: $\boldsymbol{mS}$ に $\boldsymbol{S}$ の逆行列 $\boldsymbol{S}^{-1}$ を右からかけ，得られた $\boldsymbol{m}$ を出力.

マクエリース暗号では，誤りの加わった符号語を暗号文とし生成行列を公開鍵とするが，パリティ検査行列と誤りパタン $\boldsymbol{e}$ をそれぞれ公開鍵と平文とし，それに対応するシンドロームを暗号文とすることも可能である．この方式はニーダライタ（Niederreiter）暗号[26]として知られている．マクエリース暗号もニーダライタ暗号も，残念ながら，そのままでは現実的な攻撃を受けるため安全ではないが，簡単な処理を追加することによりそれらの攻撃を回避し，公開鍵暗号に求められる最高の安全性である IND-CCA（適応的選択暗号文攻撃に対する識別困難性）を達成することが可能である[27].

7-9-2 秘密分散への応用

秘密分散（secret sharing）とは，図 7･6 に示すように秘密情報 s を複数に分割し，その内いくつか，もしくはすべてを集めることによりもとの情報を復元する方式である．分割された情報は分散情報と呼ばれ，秘密情報を復元できる集合の情報はアクセス構造と呼ばれている[29]．一般的には，1979 年にシャミア（Shamir）とブレイクリ（Blakley）が独立に提案した (k, n) しきい値法（threshold scheme）[30, 31]が有名である．(k, n) しきい値法では，秘密情報 s を n 個に分割し，その内任意の k 個以上を集めることにより s の復元を可能にする．更に，k 個未満の分散情報からでは s を情報量的に復元することが困難な方式は，完全秘密分散（perfect secret sharing）と呼ばれ，そうでない方式は，非完全秘密分散（non-perfect secret sharing）と呼ばれている．以下では，線形符号との関係を直観的に理解しやすいようにブレ

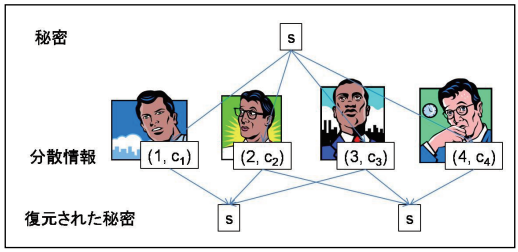

図 7·6　秘密分散

イクリの方式を行列で表現し，かつ，完全秘密分散に変換*した (k, n) しきい値法について説明する．

7-9-3 秘密の分散方法

GF(q) 上の最大距離分離符号（MDS code: maximum distance separable code）の $k \times n$ 生成行列を $\boldsymbol{G}$ とし，分散したい秘密情報を $s \in \mathrm{GF}(q)$ とする．n 個の分散情報 $\boldsymbol{c} = \{c_1, c_2, \cdots, c_n\}$ は以下の方法により計算される．

1. GF(q) 上の $k-1$ 次元ベクトル $\boldsymbol{r} = \{r_1, \cdots, r_{k-1}\}$ をランダムに生成し，それを s と連結した k 次元ベクトルを $\boldsymbol{u}$ とする．すなわち，$\boldsymbol{u} = \{s, r_1, \cdots, r_{k-1}\}$ である．

2. $\boldsymbol{c} = \boldsymbol{u}\boldsymbol{G}$ により得られた符号 $\boldsymbol{c} = \{c_1, c_2, \cdots, c_n\}$ の各軸の値 c_i とその軸のインデックス情報 i を分散情報として対応するエンティティに配布する．

7-9-4 秘密の復元方法

1. 集められた k 個の分散情報を連ねたベクトルを $\boldsymbol{c}' = \{c_{i_1}, c_{i_2}, \cdots, c_{i_k}\}$，それに対応するインデックス情報を連ねたベクトルを $\boldsymbol{i} = \{i_1, i_2, \cdots, i_k\}$，$\boldsymbol{G}$ から $\boldsymbol{i}$ に対応する列を抜き出して連ねた行列を $\boldsymbol{G}' = \{\boldsymbol{G}[i_1], \boldsymbol{G}[i_2], \cdots, \boldsymbol{G}[i_k]\}$ とする．

2. $\boldsymbol{u} = \boldsymbol{c}'\boldsymbol{G}'^{-1}$ により $\boldsymbol{u} = \{s, r_1, \cdots, r_{k-1}\}$ が得られるため，そこから s を取り出す*．

ちなみに，$\boldsymbol{G}$ が最大距離分離行列でない場合は，しきい値法にはならない．なぜなら，その場合，k 個以上の分散情報を集めても秘密情報 s を復元できない場合が出てきたり，k 個未満でも s を復元できる場合が出てきたりするためである．また，$\boldsymbol{G}$ の (j, i) 成分を i^{j-1} と

---

* ブレイクリの提案した方式は，非完全秘密分散であった．

* 厳密には G' の逆行列 G'^{-1} を計算しなくとも，以下の方法で s を求めることができる．k 次元のベクトル $\boldsymbol{v}$ を $\{1, 0, \cdots, 0\}^T$ とする．$\boldsymbol{G}'$ と $\boldsymbol{v}$ を連結させた行列の $\boldsymbol{G}[i_1]$ を吐き出し法で $\boldsymbol{v}$ のかたちに変換した際に，連結された $\boldsymbol{v}$ が変換された行列を $\boldsymbol{v}'$ とすると，s は $\boldsymbol{c}'\boldsymbol{v}'$ により与えられる．

するとシャミアのしきい値法となり，情報系列の乱数 r_i の部分にも秘密情報を入れると非完全秘密分散になる．非完全秘密分散であっても，s を暗号文とし，その鍵を完全秘密分散で分散すると平文の復元を計算量的に困難にすることが可能である．この方式は計算量的秘密分散と呼ばれている[32]．

■参考文献

1) M.J. Miller and S. Lin, “The analysis of some selective-repeat ARQ schemes with finite receiver buffer,” IEEE Trans. Commun., vol.COM-29, pp.1307–1315, Sept. 1981.
2) S. Lin and D.J. Costello, Jr., “Error Control Coding,” Second Edition, Pearson Prentice Hall, 2004.
3) D.M. Mandelbaum, “Adaptive-feedback coding scheme using incremental redundancy,” IEEE Trans. Inf. Theory, vol.IT-20, no.3, pp.388–389, May 1974.
4) E. Fujiwara, “Code Design for Dependable Systems, Theory and Practical Applications,” Chapters 4 to 7, John Wiley & Sons. Inc. 2006.
5) S. Rusu, J. Stinson, S. Tam, J. Leung, H. Muljono, and B. Cherkauer, “A 1.5-GHz 130-nm Itanium 2 processor with 6-MB On-Die L3 cache,” IEEE J. Solid-State Circ., vol.38, no.11, pp.1887–1895, Nov. 2003.
6) 情報理論とその応用学会（編），“符号理論とその応用, 情報理論とその応用シリーズ 3,” 培風館, 2003.
7) “RCR 標準規格；デジタル方式自動車電話システム,” RCR STD-27B, 1992.
8) 須田博人, 渋谷彰, 今井秀樹, “素体を利用したターボ符号用インターリーバ, ” 信学論 (A), vol.J85-A, no.11, pp.1168–1181, Nov.2002.
9) “Technical Specification Group Services and System Aspects; Multimedia Broadcast/Multicast Services (MBMS); Protocols and Codes,” 3GPP, Tech. rep. TS 26.346, 2005.
10) A. Shokrollahi, “Raptor Codes,” IEEE Trans. Inf. Theory, vol.52, no.6, pp.2551–2567, Jun. 2006.
11) “Technical Specification Group Radio Access Network; High Speed Down Link Access (HSDPA); Overall Description,” 3GPP, Tech. rep. TS 25.308, 2007.
12) H. Imai and S. Hirakawa, “A new multilevel coding method using error-correcting codes,” IEEE Trans. Inf. Theory, vol.IT-23, pp.371–377, May 1977.
13) G. Ungerboeck, “Channel coding with multilevel/phase signals,” IEEE Trans. Inf. Theory, vol.IT-28, pp.55–67, Jan. 1982.
14) D.J. Costello, Jr., J. Hagenauer, H. Imai, and S.B. Wicker, “Applications of error-control coding,” IEEE Trans. Inf. Theory, vol.IT-44, pp.2531–2560, Oct. 1998.
15) L.F. Wei, “Rotationally invariant convolutional channel coding with expanded signal space. Part II: Nonlinear codes,” IEEE J. Select. Areas Commun., vol.SAC-2, pp.672–686, Sept. 1984.
16) S. Baro, G. Bauch, and A. Hansmann, “Improved codes for space-time trellis-coded modulation,” IEEE Commun. Lett., vol.4, pp.20–22, Jan. 2000.
17) G.D. Forney, Jr., “Geometrically uniform codes,” IEEE Trans. Inf. Theory, vol.IT-37, pp.1241–1260, Sept. 1991.
18) S. Alamouti, “A simple transmit diversity technique for wireless communications,” IEEE J. Select. Areas Commun., vol.16, pp.1451–1458, Oct. 1998.
19) V. Tarokh, N. Seshadri, and A.R. Calderbank, “Space-time codes for high data rate wireless communication: Performance criterion and code construction,” IEEE Trans. Inform. Theory, vol.44, pp.744–765, Mar. 1998.
20) 浜田 充, “量子誤り訂正,” 電子情報通信学会知識ベース 知識の森, S2 群 5-3-2 節, http://www.ieice-hbkb.org/portal/ , 2008.
21) A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, “Quantum error correction and orthogonal geometry,” Phys. Rev. Lett., vol.78, pp.405–408, Jan. 1997.

22) A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, “Quantum error correction via codes over GF(4),” IEEE Trans. Inf. Theory, vol.44, pp.1369–1387, July 1998.
23) D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound,” Phys. Rev. A, vol.54, pp.1862–1868, Sept. 1996.
24) E. Knill and R. Laflamme, “Theory of quantum error-correcting codes,” Phys. Rev. A, vol.55, pp.900–911, Feb. 1997.
25) R.J. McEliece: “A public-key cryptosystem based on algebraic coding theory,” Deep Space Network Progress Report, 1978.
26) H. Niederreiter, “Knapsack-type cryptosystem based on algebraic coding theory,” Problems of Control and Inf. Theory, vol.15, no.2, pp.157–166, 1986.
27) 古原和邦，今井秀樹，“線形符号の復号問題に基づいた強い意味で安全な公開鍵暗号方式，” 信学論 (A), vol.J87-A, no.7, pp.870–880, 2004.
28) N.T. Courtois, M. Finiasz, and N. Sendrier, “How to achieve a McEliece-based digital signature scheme,” Proc. of ASIACRYPT 2001, pp.157–174, Springer-Verlag, 2001.
29) M. Itoh, A. Saito, and T. Nishizeki, “Secret sharing scheme realizing general access structure,” Proc. of IEEE Globecom’87, pp.99–102, 1987.
30) A. Shamir, “How to share a secret,” Commun. ACM, vol.22, no.11, pp.612–613, 1979.
31) G.R. Blakley: “Safeguarding cryptographic keys,” AFIPS 1979 Nat. Computer Conf., vol.48, no.11, pp.313–317, 1979.
32) H. Krawczyk, “Secret sharing made short,” Proc. of CRYPTO’93, LNCS 773, pp.136–146, Springer-Verlag, 1994.
33) 横山光雄，“スペクトル拡散通信システム,” 科学技術出版，1988.
34) 今井秀樹，“符号理論,” (社) 電子情報通信学会, 1990.
35) M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, “Spread Spectrum Communications,” vol.1, charp. 5, Computer Science Press, 1985.
36) P. Fan and M. Darnell, “Sequence Design for Communications Applications,” Research Studies Press Ltd. 1996.
37) X.H. Tang, Pingzhi Fan, Shinya Matsufuji, “Lower Bounds on the Maximum Correlation of Sequence Sets with Low or Zero Correlation Zone,” Electronics Letters, 36-6, pp.551-552, March 2000.