符号の基礎

渡辺研究室

符号の基礎

- 無線通信の基礎技術の1つである符号化
  - ノイズの影響を受けやすい電波を用いた通信には誤り訂正が重要
  - 再送よりも効率的な場合が存在
  - 通信距離にも影響

以降では符号化方式についての資料と概要を記述

リード・ソロモン符号 (1/2)

- リードソロモン符号[6]は符号の生成や復号が複雑だが、誤り訂正能力が高く実用化もされている巡回符号の一種
- ガロア体の概念と、原始多項式（3 + + 1 = 0）や生成多項式によって符号語を作り上げ、受信側では受信した符号と検査行列を用いて符号の誤り位置情報を取得
- （誤り位置情報を表す、シンドロームという行列が0）＝（誤りを含まない符号）
- シンドロームが0になるまで誤り訂正を繰り返す
- 誤りの位置が多い場合には復号できない

リード・ソロモン符号 (2/2)

- 利点
  - 線形符号に比べて効率のよい符号化ができる
  - リード・ソロモン符号は最大分離距離を達成する符号[1]
- 欠点
  - 巡回符号特有の処理の多さ
  - 符号化の時間や復号の時間が長くなる

最大距離分離符号

- 最小（ハミング）距離がn - k + 1であるような(n, k)線形符号の総称（リード・ソロモン符号も含まれる）
- 最大距離分離符号を語る上で、シングルトン限界(Singleton bound) という概念が出てくる。
- シングルトン限界の式は、$d_{min} \leqq n - k + 1$
  - nは符号語の長さ、k はシンボル数
  - 最小距離が冗長シンボル数+ 1以下にしかならない
- 最大距離分離符号は冗長シンボルから得られるハミング距離を限界まで利用（式を等式にする）

BCH符号

- 実践的に使用されている巡回ブロック符号はBCH符号の一種で、応用範囲が広い符号化方式[7]
- 2個以上の訂正能力を持つものをBCH符号
  - （ハミング符号も巡回ブロック符号ではあるが、一般的に複数の冗長ビットに対して訂正できる誤りは1つ）
- 利点
  - シンドローム復号という簡潔な代数学的手法で容易に復号できる仕組みをもつため、電子回路が非常に単純であり、低電力で小型の機器で復号可能
- （符号化の名前であるBCHは考案した3人の人間(Bose, Chaudhuri, Hocquenghem)のイニシャル）

Golay符号

- Golay符号は完全符号の1つ
- Golay符号の符号長は23ビットで、情報ビットが12ビット
- 符号長が24ビットになる拡張Golay符号も存在
- 利点
  - BCH符号に比べ、3ビットまでの誤り訂正を11ビットのパリティビットで訂正
  - 誤りを確実に訂正
  - 2値画像や濃淡画像に応用し、ハミング符号よりも高い性能を発揮[3]
- 下記のurlでは、実際に二元Golay符号が体験
  - http://math.shinshu-u.ac.jp/~hanaki/script/BinaryGolay.html

LDPC符号

- LDPC(Low-Density Parity Check)符号は、疎な検査行列により定義される線形符号の一つ
- サム・プロダクトアルゴリズムに基づく反復復号法と組み合わせることで、シャノン限界に迫る高い複合性能を達成
  - 疎な検査行列：成分のほとんどが0である行列
  - 線形符号：生成行列を使った符号化
  - サム・プロダクトアルゴリズム：グラフ上でメッセージをやり取りする分散アルゴリズムで、可観測変数の観測値に基づき、隠れ変数の事後確率分布を計算
  - 反復復号法：同じビットをいくつか重ねたものを複合
  - c=110 001 111のとき、数の多い符号語を選択してm=1 0 1と復号
- LDPC符号の作成
  - http://www.kumikomi.net/interface/sample/201210/if10_157.pdf

多元LDPC符号[17]

- Turbo復号アルゴリズムやLDPCで用いられるsum-productsアルゴリズムはBN (BayesianNetwork)の代表的推論アルゴリズムであるBP(Belief Propagation)と等価
- 文献[4]は復号アルゴリズムをグラフ上で表現して高効率かつ高性能な復号アルゴリズムを検討

ブロック符号・線形符号

- ブロック符号：k bits の情報ブロックにm bitsの検査記号を取り付けてn bits の符号語を作成
- 符号化率r = k/n
- 良い符号
  - 符号化率は小さく
  - 最小ハミング距離は大きく
- 線形符号は、kを大きくして検査ビットを選ぶ符号
- 線形符号の特徴
  - XORで符号語を足すと、足した値もまた符号語になること
- （巡回符号は符号語を巡回シフトさせると符号語になる）
  - CRCと呼ばれるもので誤り検出が簡単
  - http://sakaiyas.cocolog-nifty.com/nikki/2010/03/ldcp-staircase-.html
    - URLは参考ページの中でも簡単に説明してくれるページ

ビタビ復号

- 畳み込み符号の代表的な復号法の1つ
- 復号には状態の概念を利用
  - 1ビットの入力に対して、1つの状態遷移
  - 各状態において、メトリック（確からしさ）を計算
    - メトリックを参考にして、各状態を取捨選択
    - 硬判定復号 → ハミング距離
    - 軟判定復号 → 尤度
    - 軟判定復号は、復号方法が複雑な分、硬判定復号よりも復号成功率が高い
- 利点
  - ランダム誤りに強い
- 欠点
  - 復号に時間がかかる
- ビタビ復号法は、衛星通信システムなどの通信遅延が大きく、ランダムノイズの影響を受けやすい環境に応用[8]。

逐次復号

- 逐次復号は、木探索の手法によって近似的に最尤復号を実現しようとする復号法
  - ビタビ復号のようなトレリスを用いる復号が困難な拘束長の長い畳み込み符号に対抗
- 逐次復号の歴史は古く、1960年代に畳み込み符号が議論されていた時期から研究されている

Turbo符号

- Turbo符号[9]はLDPCと並んでシャノン限界に近い誤り訂正符号
- 利点
  - 送信機の出力を上げずにデータレートを高める点
  - 送信にかかる電力は小さい
- 欠点
  - 復号処理に時間がかかるため、遅延が非常に大きい
  - 復号自体にかかる電力は大きい
- Turbo復号器が持つ2つの畳込み復号器がそれぞれビットパターンの仮説を生成して、この仮説を両方の復号器が合意するまでチェックを繰り返す
- できるだけ伝送路の状態によらない最もありそうなデータ列を見つける手段が必要なため、広範囲の時系列にデータをばらまいてランダム化
- 符号語をまったく同じ伝送路に通しても伝送路で受ける誤りの影響は異なることを利用
- 最尤復号と比較して、最尤復号は間違った復号結果にたどり着くとき、辿り着いた復号結果は正しい符号語列から大きく逸脱している場合が多い[7]

ビットインターリーブ符号

- バースト誤りに対して強い符号化
- ビットインターリーブ符号は符号語をシャッフルして転送
- 利点
  - まとまった誤りをなくして推測をしやすくする
- 欠点
  - シャッフルしたブロック全部を受信できるまでデコードができない点
- 任意で高次の信号コンステレーションに最適なインデックスの割り当てを求める問題に取り組む[20]

空間-周波数符号化

- Spatio-temporal vector-coding (STVC) はMIMOチャネルを達成するための符号化[18]
- Discrete Matrix Multitoneから複雑性を減らすことが目標
- 適応格子トレリス符号化技術はDiscrete Matrix Multitone (DMMT)チャネルの空間と周波数の次元上で符号化する方法
- 文献[19]は高データレートの無線通信に適した新しいモデム技術の理論と周波数フラットレイリーフェージングチャネルを介した実践について示されている
- データは空間-時間チャネル符号化で符号化された後にN本のストリームに分割されて送信される

時空間符号 (1/3)

- 時空間符号は複数の送信アンテナを所有している送信機が用いる
- 空間ダイバーシティの取得のために複数のアンテナで独立したフェージングを利用するように符号化
  - （通常は、複数の送信アンテナを用いて単一のデータストリームを送信）
- 詳細な解説
  - http://news.mynavi.jp/articles/2009/06/01/idt_mimo/002.html
  - URLは時空間符号の基礎であるAlamouti符号についても解説

時空間符号 (2/3)

- 利点
  - 多重化ができるので複数のデータストリームを送信できる
- 欠点
  - 受信側での検出が複雑になる
    - （時空間符号を用いると簡易に検出できるが、データストリームが単一になる）
- 文献[21]では、時空間ブロック符号のパフォーマンスを示している
- 時空間ブロック符号はブロック符号と似た構造
- ダイバーシティゲインを向上させる（複数アンテナ使用の為）が、符号化ゲインは得られない

時空間符号 (3/3)

- 文献[22]では、分散時空間符号を中継通信に用いる例を示している。
- 複数アンテナから、複数の端末宛に送信するために、時空間符号を複数端末宛にも送信できるようにしたDistributed Space-Time Codingが文献[22]のメインポイント
- 文献内で示されている時空間符号の一種である線形分散符号(Linear Dispersion Code) は文献[23]に示されている

協調符号

- 通信における協調はダイバーシティゲインの向上に繋がる
- 複数存在するアンテナの割り当ての検討によって、無線ネットワーク全体のスループットが上がる
- 文献[24]は、協調を符号化に適用したデザインを提唱

レートレス符号

- レートレス符号は符号化率を固定しない符号化方式
- レートレス符号化では冗長な符号語を徐々に送信する仕組みのため、レートという概念がない
  - （従来の符号化はあらかじめ冗長に符号語を付加して送信＆復号に利用）

LT Codes[10]

- 最初に考案されたレートレス符号化
- LT Codesは冗長符号の一種
  - 符号語を限りなく作成し続けられる設計
- この符号化は誤り訂正ではないが、消失チャネルに強い符号
- 符号化の詳細については以下のとおり
  1. 次数分布から次数dをランダムに選択
  2. 符号語の隣の入力信号の違うものを均一に選択
  3. d個の符号語の値でExORを取る

Raptor Codes[11-13]

- Rapter Codes は2006年にLT Codesの拡張版として考案されたレートレス符号化
- LT Codesの弱点を克服するRaptor Codes
  - 入力信号と出力信号の数に差がない場合に一定のコストでエンコードすることができない
    - ランダムな次数でランダムな符号語を選択する仕組みのLT-Codesは少ない符号語でデコード可能な場合、所望の符号語をピンポイントで選択できないため
- Raptor CodesではPre-codingを用いる
  - LDPCの誤り訂正能力を組み合わせることや、Pre-codingを用いることによる冗長ビットの作成によって、最小限の送信で信号を送信可能
- http://www.merl.com/publications/docs/TR2004-037.pdfに示される、MITSUBISHI ELECTRIC RESERCH LABORATORIES のRateless Codes on Noisy Channelsという調査論文に示される図にLT-CodesとRaptor CodesのBERを比較している評価結果がある
  - 評価結果から、Raptor Codesはレートが高くなるに従ってBERも低下

Strider[14]

- Striderはオーバヘッドの影響を限りなく小さくした最適な適応変調をする符号化
- レートレス符号化と衝突耐性の両方を持つ
  - 送信側はレートレス符号部分の特性によって、チャネル情報を知らなくても最低なレートで送信可能
  - 衝突耐性を持った衝突した信号を両方とも受信可能
- 従来の符号化や変調方式では特定のSNRスレッショルドを持っているが、Striderはその従来の固定された符号化や変調方式をすべてのSNRで実現することができる点が新しい

Spinal Codes[15, 16]

- Spinal Codesはレートレス符号化の中でも特に高い伝送レートを達成する符号化
- Spinal Codesの符号化・復号化の中心は、畳み込み符号とビタビ復号
  - 畳み込み符号とビタビ復号を用いることで、ビット列の前後に相関を持たせて復号時の判定に利用
    - AWGNのチャネルノイズに対抗
- 特徴
  - 畳み込み符号の際にハッシュ（乱数生成器）を用いる
  - 従来の畳み込み符号では、生成多項式にしたがって符号化されていくが、Spinal Codesでは生成多項式そのものにハッシュ関数が関わる
  - 符号語が長ければ長いほど、トレリス図などでみる状態の数が無限大に発散するが、状態数を管理して、効果を高めた符号化を更にレートレス化
  - 通信路によるロスは少ないが、ビタビ復号の特性をもつためデコードに計算量・時間を多く消費

- ハミング符号
- ブロック符号
  - BCH 符号（ランダム誤り） [1]
  - Golay 符号（ランダム誤り） [2,3]
  - LDPC 符号（ランダム誤り） [4]
    - LDGM 符号 (派生？)
  - ファイヤ符号（バースト誤り） [5]
  - リードソロモン符号（バースト誤り） [6,7]
- 畳み込み符号
  - しきい値復号（ランダム誤り）
  - ビタビ復号（ランダム誤り） [8]
  - 逐次復号（ランダム誤り）
  - ターボ符号（ランダム誤り） [4,7,9]
    - SOVA 復号
    - MAP 復号
- 連接符号
  - BCH 符号＋リードソロモン符号
  - 畳み込み符号＋リードソロモン符号
- レートレス符号
  - LT 符号 [10]
  - Raptor 符号 [11–13]
  - strider 符号 [14]
  - spinal 符号 [15,16]

参考文献

[1] Yingquan Wu. New list decoding algorithms for reed-solomon and bch codes. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pp. 2806–2810, June 2007.

[2] Vera Pless. On the uniqueness of the golay codes. *Journal of Combinatorial theory*, Vol. 5, No. 3, pp. 215–228, 1968.

[3] 笠原祥一, 横尾英俊. ゴーレイ符号による情報ハイディングと画像データへの応用. 電子情報通信学会論文誌 A, Vol. 91, No. 6, pp. 685–694, 2008.

[4] 松嶋敏泰. ターボ符号，ldpc 符号の復号アルゴリズム. ベイジアンネットチュートリアル, 2001.

[5] 博一岡野. マイクロコンピュータによる fire 符号の高速復号法. 情報処理学会論文誌, Vol. 21, No. 5, pp. 375–382, sep 1980.

[6] Omar Aitsab and Ramesh Pyndiah. Performance of reed-solomon block turbo code. In *Global Telecommunications Conference, 1996. GLOBECOM '96. 'Communications: The Key to Global Prosperity*, Vol. 1, pp. 121–125 vol.1, Nov 1996.

[7] 西村芳一（編）. 改訂新版 データの符号化技術と誤り訂正の基礎. CQ 出版社, 2011.

[8] 安田豊. ヴィタビ復号による誤り訂正方式の研究. PhD thesis, 京都大学, 1984.

[9] Claude. Berrou, Alain. Glavieux, and Punya. Thitimajshima. Near shannon limit error-correcting coding and decoding: Turbo-codes. 1. In *Communications, 1993. ICC '93 Geneva. Technical Program, Conference Record, IEEE International Conference on*, Vol. 2, pp. 1064–1070 vol.2, May 1993.

[10] M. Luby. Lt codes. In *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*, pp. 271–280, 2002.

[11] Amin. Shokrollahi. Raptor codes. *Information Theory, IEEE Transactions on*, Vol. 52, No. 6, pp. 2551–2567, June 2006.

[12] Omid Etesami and Amin Shokrollahi. Raptor codes on binary memoryless symmetric channels. *IEEE TRANSACTIONS ON INFORMATION THEORY*, Vol. 522006, No. 5, pp. 2033–2051, 2006.

[13] Auguste Venkiah, Charly Poulliat, and David Declercq. Jointly decoded raptor codes: Analysis and design for the BIAWGN channel. *EURASIP J. Wirel. Commun. Netw.*, Vol. 2009, pp. 16:1–16:11, 2009.

[14] Aditya Gudipati and Sachin Katti. Strider: Automatic rate adaptation and collision handling. In *Proceedings of the ACM SIGCOMM 2011 Conference*, SIGCOMM '11, pp. 158–169, New York, NY, USA, 2011. ACM.

[15] Jonathan Perry, Hari Balakrishnan, and Devavrat Shah. Rateless spinal codes. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks*, HotNets-X, pp. 6:1–6:6, New York, NY, USA, 2011. ACM.

[16] Jonathan Perry, Peter Iannucci, Kermin Elliott Fleming, Hari Balakrishnan, and Devavrat Shah. Spinal Codes. In *ACM SIGCOMM*, Helsinki, Finland, August 2012.

[17] 笠井健太. 多元 ldpc 符号とその応用. 電子情報通信学会技術研究報告, pp. 1–6, 宮城県, 9 月 2010.

[18] Gregory G. Raleigh and John M. Cioffi. Spatio-temporal coding for wireless communication. *Communications, IEEE Transactions on*, Vol. 46, No. 3, pp. 357–366, Mar 1998.

[19] Ayman.F. Naguib, Vahid Tarokh, Nambirajan. Seshadri, and A.Robert. Calderbank. A space-time coding modem for high-data-rate wireless communications. *Selected Areas in Communications, IEEE Journal on*, Vol. 16, No. 8, pp. 1459–1478, Oct 1998.

[20] F. Schreckenbach, N. Görtz, J. Hagenauer, and G. Bauch. Optimized symbol mappings for bit-interleaved coded modulation with iterative decoding. *IEEE Commun. Lett*, Vol. 7, pp. 593–595, 2003.

[21] Vahid Tarokh, Hamid Jafarkhani, and A.Robert. Calderbank. Space-time block coding for wireless communications: performance results. *Selected Areas in Communications, IEEE Journal on*, Vol. 17, No. 3, pp. 451–460, Mar 1999.

[22] Yindi Jing and Babak Hassibi. Distributed space-time coding in wireless relay networks. *Wireless Communications, IEEE Transactions on*, Vol. 5, No. 12, pp. 3524–3536, December 2006.

[23] Babak. Hassibi and Bertrand M. Hochwald. High-rate codes that are linear in space and time. *Information Theory, IEEE Transactions on*, Vol. 48, No. 7, pp. 1804–1824, Jul 2002.

[24] Andrej. Stefanov and Elza. Erkip. Cooperative coding for wireless networks. *Communications, IEEE Transactions on*, Vol. 52, No. 9, pp. 1470–1476, Sept 2004.