科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ２ 日現在

機関番号：１３３０１
研究種目：若手研究(B)
研究期間：2011～2013
課題番号：２３７０００１０

研究課題名（和文）誤り訂正符号に潜むランダムネスと構造の解明

研究課題名（英文）Randomness and Structure in Error-Correcting Codes

研究代表者
安永　憲司（Yasunaga, Kenji）

金沢大学・電子情報学系・助教

研究者番号：５０５１０００４

交付決定額（研究期間全体）：（直接経費）　　2,800,000円、（間接経費）　　840,000円

研究成果の概要（和文）：サンプル可能な加法的通信路という通信路モデルを導入し、この通信路における誤り訂正の可能性と限界を明らかにした。サンプル可能とは多項式時間で計算可能という意味であり、加法的というのは符号や符号語の知識を使わずに誤りが付加されることを意味する。サンプルされる分布が線形空間を成す場合、効率的に線形符号で訂正することができる。オラクルで相対化された状況では、エントロピーが小さいにもかかわらず効率的にシンドローム復号ができないサンプル可能な分布が存在することがわかった。サンプルされる分布が小バイアスの場合、バイアスの大きさと訂正可能なレートの限界に関係性があることがわかった。

研究成果の概要（英文）：We have introduced samplable additive-error channels, and studied the possibilities and limitations of error correction in the channels. "Samplable" means that the errors are efficiently computable, and "additive" means that the errors are added to input codewords without the knowledge of the code or the codewords. If samplable distributions form linear subspaces, we can correct the errors by linear codes. In the situations relativized by oracles, there are samplable errors with low entropy for which no efficient syndrome decoding exists. If samplable distributions are of small-bias, there is a relation between the magnitude of the bias and the information rate on which the errors are correctable.

研究分野：その他

科研費の分科・細目：その他

キーワード：誤り訂正符号　多項式時間計算　加法的通信路　誤り訂正能力

１．研究開始当初の背景

符号をランダムに構成すれば優れた誤り訂正能力をもつことが知られている。しかし、実際に符号として利用するには、ランダムな構成ではなく、明示的に構成しなければならない。そのため、符号は、ランダムに構成するのではなく、明示的に擬似ランダムに構成する必要がある。

誤り訂正能力が高い符号が存在したとき、その符号に対して効率的に実行できる復号法がなければ現実的には利用できない。また、暗号理論や計算量理論などへの理論的な応用を考えた場合も、効率的な復号法が必要である場合が多い。一般的に、効率的な復号法では、対象とする符号がある構造を有しており、その構造を利用することで効率的に復号を行う。このような点から、様々な符号に適用できる復号法の開発も重要である。

２．研究の目的

本研究は、ランダムネスをもつことで多くの誤り手を訂正でき、かつ構造をもつことで効率的な復号法を有する符号の設計及びその性能を解明することを目的とする。

符号が達成すべき訂正能力は、仮定する通信路モデルに依存して変わるため、様々な通信路モデルを検討し、そのモデルにおける符号の訂正可能性およびその限界についての考察も行う。

３．研究の方法

代表的な通信路モデルである確率的通信路と最悪ケース通信路の中間的な位置づけのモデルを検討する。具体的には、通信路における誤りの発生を多項式時間計算と考える計算能力制限通信路等をベースに考える。

４．研究成果

符号理論研究における２つの代表的な通信路は、確率的通信路と最悪ケース通信路である。確率的通信路の代表は 2 元対称通信路であり、各ビットを一定確率で反転させる通信路である。最悪ケース通信路とは、敵対的通信路とも呼ばれ、与えられた符号および符号語に対して、誤り数だけを制限した場合の最悪ケースの誤りを考える通信路である。

計算量的な観点から見ると、確率的通信路は低コスト計算、最悪ケース通信路は高コスト計算を行っているといえる。この点を踏まえ、Lipton(STACS‘94)は計算量制限通信路という通信路モデルを提案した。暗号理論等でよく使われるように、通信路は多項式時間計算に制限されていると仮定する通信路モデルである。

本研究では、確率的通信路と最悪ケース通信路の中間に位置する通信路として、サンプル可能な加法的通信路を考えた。サンプル可能というのは、多項式時間で誤りベクトルを計算可能という意味であり、加法的というのは、誤りの生成が符号や符号語の情報とは独立に行われ、誤りが加法的に加わることを意味する。例えば、2 元対称通信路は、符号や符号語とは独立に誤りが生成され、加法的に加わっており、その生成は多項式時間で可能なため、サンプル可能な加法的通信路の１つである。また、本研究で考えたサンプル可能な加法的通信路では、発生する誤りの数を制限しないものを考えた。多くの通信路モデルにおいて発生する誤りの数（誤りベクトルのハミング重み）を制限しているのに対して、誤りの数を制限していない点は特徴的である。特に、計算量制限通信路においてこのような誤り数を制限しない通信路はこれまで考えられていなかった。

提案した通信路モデルでは、符号化方式の設計にあたって、サンプル可能な加法的通信路の知識を使ってよい状況を考えた。つまり、多項式時間でサンプルを行うアルゴリズム自体は、符号を設計する設計者は知識としてもっているが、実際にサンプルする際の乱数の情報は与えられないということである。

次に、サンプル可能な加法的通信路における誤り訂正の可能性と限界を明らかにすることを目指した。まず、誤り訂正可能かどうかを調べ、可能であるならばどの程度高いレートが達成可能かを調べた。

サンプル可能な加法的通信路では、誤りベクトルを生成する分布 Z によって誤りの訂正可能性が変わると考えられる。そこで、サンプルされる分布のシャノンエントロピー H(Z)を１つの基準として訂正可能性を調べた。符号長を n ビットとすると、H(Z)は 0 から n の間の実数値をとる。

まず、H(Z) = 0 の場合、つまり生成される誤りベクトルが一意に定まる場合、誤り訂正は簡単に行うことができる。復号時にその誤りベクトルを引けばよいからである。逆に、H(Z) = n の場合、これは完全にランダムな系列が誤りとして加わることを意味し、この場合、誤り訂正は不可能である。

次に、Z は 2 元対称通信路をシミュレート可能であるという事実から、Shannon の通信路符号化逆定理により、H(Z) = nh(p)を満たすある Z に対して、符号化レート R を 1 - H(Z)/n より大きくすることはできないことがわかる。ここで、p は 2 元対称通信路の反転確率であり、h(p)は 2 元エントロピー関数である。

効率的な符号化方式に関して、付加される誤りが（暗号学的な意味で）擬似ランダムである場合も、誤りの訂正が不可能であることが分かる。訂正可能であるとすると、それは擬似ランダムであることに矛盾するからで

ある。一方向性関数の存在を仮定すると、任意の正定数 $e < 1$ に対して $H(Z) = n^e$ の擬似ランダム分布が存在するため、そのようなエントロピーをもち、効率的な誤り訂正が不可能な分布が存在することが分かる。

次に、線形関数による符号化に限定した場合、あるオラクルで相対化された状況では、$H(Z)$が $\log(n)$よりも真に大きな関数の時に、効率的なシンドローム復号ができない分布が存在することが分かった。この結果は、オラクルで相対化された状況で線形圧縮できない分布の存在性と、線形圧縮と線形符号化の関係性より示すことができる。

Z を平坦分布に限定した場合を考える。このとき、Z が線型部分空間を成す場合、レート R が $1 - m/n$ 以下の効率的な符号化方式の存在性を示すことができる。ここで m は Z の次元である。また、一般の平坦分布 Z に対して、レート R が $1 - m/n - O(\log(1/e))/n$ 以下で誤り率 e の誤り訂正が可能な符号化方式の存在性も示すことができる。この結果は、線形符号アンサンブルと線形無損失濃縮器との関係から導かれる。逆に、任意の平坦分布 Z は、レート $R > 1 - m/n + \log(1/(1-e))/n$ で誤り率 e の誤り訂正はできないことも分かる。また、決定性の符号化方式では、あるエントロピーをもつすべての平坦分布を訂正できないことも分かる。より具体的には、任意の決定性符号化方式に対して、その符号化方式では訂正できない $H(Z)=1$ であるような分布 Z の存在を示すことができる。

最後に、Z が小バイアス分布である場合を考える。小バイアス分布とは、出力系列の任意の部分系列のパリティ値が一様ランダムに近い分布のことである。このとき、バイアス d の分布はレート $R > 1 - (2\log(1/d)+1)/n$ では訂正できないことが分かる。また、レート $R > 1 - m/n + (2\log(n)+O(1))/n$ では訂正できない $H(Z) = m$ を満たすサンプル可能な小バイアス分布 Z が存在することも分かる。これらの結果は、小バイアス分布が高エントロピー分布に対して使い捨て鍵暗号の役割を果たすという性質を利用することで導かれる。

以上の結果をまとめると、サンプル可能な加法的誤りの訂正可能性に関して、多くの場合、サンプルされる分布のシャノンエントロピーが m のとき、レート R を $1 - m/n$ より小さく取れば訂正可能であり、逆に、レートを $1 - m/n$ より大きく取ると訂正できないと言える。ただし、符号化方式を効率的なものに限定すると、劣線形エントロピーの分布でも訂正できないものが存在する。また、オラクルで相対化された状況では、対数関数エントロピーの分布でも、効率的なシンドローム復号は望めない。

本研究において、サンプル可能な加法的通信路の訂正能力はある程度解明されたが、未解決な問題も多い。例えば、効率的な符号化方式に限定した場合、シンドローム復号以外の方法を考えたときに対数関数エントロピーの分布は訂正できるか否かは未解決である。また、シンドローム復号の場合も含め、オラクルで相対化した状況を考えない場合に、同様の結果が得られるかも未解決である。その他にも、擬似ランダム分布が訂正できないことを理由に、劣線形エントロピーで訂正できない分布の存在を示したが、擬似ランダム分布の存在性は一方向性関数の存在性を必要とする。一方向性関数の存在性を仮定せずに同様の結論が示せるかも未解決である。逆に、一方向性関数が存在しない場合に、任意のサンプル可能な分布が訂正できるという可能性がまだ残っている。上で述べたように、効率的に訂正可能という範囲においては、誤り訂正可能性の特徴付けがまだ十分であるとはいえない。この点に関して今後研究が進むことが期待される。

また、サンプル可能な分布においてサンプルするアルゴリズムを定数段回路や対数領域計算などのより低コストな計算に限定した場合の訂正可能性を明らかにすることも、今後の課題として残っている。

その他に、具体的な符号化方式についても、非常に簡素な構成法を示した場合があるだけであるため、今後のさらなる研究が期待される。例えば、2 元対称通信路に関しては、Justesen 構成を用いることで、非効率な復号法を小部分として組み合わせることで全体として効率的な復号法を得ることが可能である。同様の結果を、2 元対称通信路以外に拡張すること、また拡張可能な通信路を特徴づけることも今後の研究として期待される。

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

① Kenji Yasunaga. Correction of samplable additive errors. In Proceedings of the 2014 IEEE International Symposium on Information Theory, to appear.（査読有）

② Hitoshi Namiki, Keisuke Tanaka, and Kenji Yasunaga. Randomness leakage in the KEM/DEM framework. IEICE Transactions on Fundamentals, volume E97-A, number 1, pages 191-199, January 2014.（査読有）
DOI: 10.1587/transfun.E97.A.191

③ Kenji Yasunaga. List decoding of Reed-Muller codes based on a generalized Plotkin construction. IEICE Transactions on Fundamentals, volume E96-A, number 7, pages 1662-1666, July 2013.（査読有）
DOI: 10.1587/transfun.E96.A.1100

④ Keisuke Tanaka, Akihiro Yamada, and Kenji Yasunaga. Weak oblivious transfer from strong one-way functions. In

Proceedings of the 5th International Conference on Provable Security (ProvSec 2011), Lecture Notes in Computer Science, Springer-Verlag, volume 6980, pages 34-51, October 2011. （査読有）
DOI: 10.1007/978-3-642-24316-5_5

〔学会発表〕（計 6 件）
① Kosuke Yuzawa, Kenji Yasunaga, Masahiro Mambo. A study on computational fuzzy extractors. 2014年暗号と情報セキュリティシンポジウム, 2014年1月21-24日, 鹿児島県鹿児島市.
② Haruna Higo, Keisuke Tanaka, and Kenji Yasunaga. Game-theoretic security for bit commitment. The 8th International Workshop on Security, November 18-20, 2013, Okinawa, Japan.
③ Kenji Yasunaga. Error correction in computationally bounded channels. 第六回計算量理論若手の会ワークショップ, 2013年9月11-13日, 山形県米沢市.
④ Kenji Yasunaga. Correctability of efficiently computable additive errors. 第35回情報理論とその応用シンポジウム, 2012年12月11-14日,大分県速見郡日出町.

６．研究組織
(1)研究代表者
安永 憲司（YASUNAGA, Kenji）
金沢大学・電子情報学系・助教

研究者番号：５０５１０００４