様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年　6 月　8 日現在

機関番号：14401
研究種目：基盤研究（C）
研究期間：2009～2011
課題番号：21560400
研究課題名（和文）　ネットワーク符号化向け誤り訂正符号の復号法とその性能解析

研究課題名（英文）　Decoding methods and performance analysis of error correcting codes for network coding

研究代表者
藤原　融（FUJIWARA TORU）
大阪大学・大学院情報科学研究科・教授
研究者番号：70190098

研究成果の概要（和文）：ネットワーク符号化は、ネットワーク通信路の効率的利用に関わる理論として近年盛んに研究されている。ネットワーク符号化の高信頼化のためには、効率化のために符号化されたデータを誤り訂正符号によりさらに符号化して、通信で生じる誤りを訂正する。本研究では、そのような状況における誤り訂正符号の復号法の考案及び性能解析手法の確立を目的とする。いくつかの復号法を示すとともに、符号の結合重み分布が性能解析に重要な役割を担っていることを明らかにした。結合重み分布を従来に比べて極めて効率よく計算するために、一般のネットワーク構成に適用可能なマックウィリアムズの等式を導出した。

研究成果の概要（英文）：Network coding is studied for efficient communication in networks. For reliable communication, error correcting code is used to encode data of network coding. This study aims to derive decoding method of codes and its performance analysis. Several decoding methods are given. It is shown that joint weight distribution of codes is very important for performance analysis. MacWilliams identy for joint weight distribution is derived for general network structure.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,500,000	450,000	1,950,000
2010 年度	1,200,000	360,000	1,560,000
2011 年度	900,000	270,000	1,170,000
総　計	3,600,000	1,080,000	4,680,000

研究分野：情報理論、符号理論
科研費の分科・細目：電気電子工学　・　通信・ネットワーク工学
キーワード：ネットワーク符号化、誤り訂正符号、符号化、復号、限界距離復号、重み分布、結合重み分布、復号誤り確率

１．研究開始当初の背景

ネットワーク符号化は、通信路の効率的利用や接続状態が動的に変化するネットワーク（アドホックネットワーク等）における通信の効率に関わる理論として、近年研究が盛んになっている。本研究では、ネットワーク符号化に用いられる誤り訂正符号について、その復号法の考案及び性能解析手法の確立を目的とする。

誤り訂正符号の復号法や性能解析については、さまざまな研究が行われている。性能解析の基本となるのは符号の重み分布であるが、分割重み分布など、より詳細な重み構造が得られれば、より正確な性能解析を行うことができる。申請者もこれまで長年にわたり、符号の構造（重み構造やトレリス構造）

に関する研究を行っている。
　一方、ネットワーク符号化の研究も文献[1]以来、近年盛んに行われている。ネットワーク符号化技術は、中継ノードでデータの演算（複数のデータベクトルの和をとる等）を許すことにより、通信効率を上げようとするものである。また、ネットワークのトポロジー（接続）が動的に変化し不明の場合でもランダム符号化と呼ばれる方法を用いることにより、情報伝送できるという利点がある。以下では、まず、ネットワーク符号化について簡単な例を用いて説明する。
　図１のようなネットワークにおいて、送信ノード（ソースノード）s から２つの受信ノード（シンクノード）t1，t2 への伝送を考える。このネットワークはその形状からバタフライネットワークと呼ばれる。各エッジは単位時間当たり１ビット伝送できるとする。ビット a と b の２ビット伝送するとき、中間ノード３では、a と b の２ビット受信するが１ビットしか送出できない。図のように中間ノード３が受信データ a，b からその和（排他的論理和）a+b を求めて送れば、同ノードが a，b のどちらか一方だけを中継するよりも効率よく伝送できる。すなわち、受信ノード t1 では、a と a+b から a と b を得ることができる。また、受信ノード t2 においても a+b と b から a と b を得ることができる。

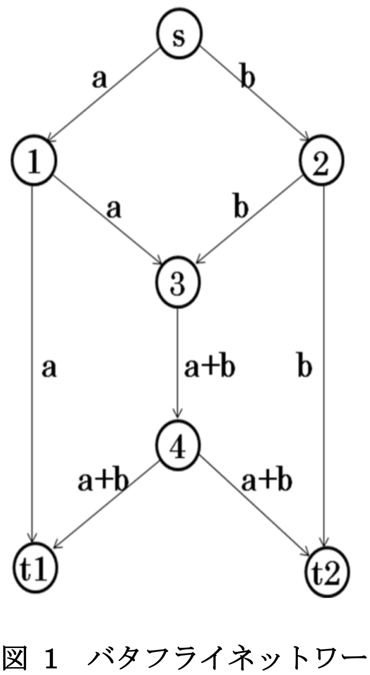

図 1　バタフライネットワーク

　この例では、エッジ（辺）は１ビット伝送できるとしているが、ベクトル（ビット列）を伝送すると考えることができる。また、受信ノード t1，t2 で受信されるデータが異なることに注意すれば、受信ノードへベクトルを伝送するのではなく、線形ベクトル空間（の基底ベクトル）を伝送すると解釈することもできる。右図の例では、{a，b，a+b，0} という線形ベクトル空間を考え、送信ノード s から、受信ノード t1，t2 へこの空間を伝送するとみなすのである。
　ネットワーク符号化が行われる通信路においても誤りは発生するため、誤り訂正符号に関する研究がなされている。もちろん、ノード間の通信それぞれで誤り訂正符号化を行う問題は従来と同じである。しかし、より上位の層での通信では異なる。送信ノードで符号化し、受信ノードで復号する場合の問題は、次のような点で従来の問題と異なる。第１の相違点は、ベクトルの通信においては、演算が行われるため、受信ベクトルの独立性がないことである。第２の相違点は、線形ベクトル空間の伝送と捉えたとき、線形ベクトル空間を符号語とみなして、そのレベルで復号を考えることができることである。

２．研究の目的

　本研究では、ネットワーク符号化における誤り訂正符号の復号法を考案し、その性能解析を行い、既知の符号等の性能を明らかにする。具体的には、以下の(1)～(4)を行う。
(1) ベクトル伝送に用いる誤り訂正符号の復号法：送信するベクトルはその伝送経路が同じでないため、受信ベクトルにより、含まれる誤りに差がある。また、演算がなされるため、誤りが独立ではない。そこで、いくつかの基本的なネットワーク構造について、最適（最尤）復号や準最適復号法を考案する。
(2) 考案した復号法の性能評価：復号法の性能評価を、解析的およびシミュレーションにより行う。また、いくつかの基本的なネットワーク構造のもとで、復号法の性能評価を行い、ベクトル毎に独立な復号法に対する優位性を評価する。
(3) 線形ベクトル空間を符号語とする符号の重み構造の解析：線形ベクトル空間を符号語とする符号に対して、符号の重み構造の計算アルゴリズムを考案する。
(4) 符号の性能評価：上で求めた計算アルゴリズムに基づき、これまでに知られている符号の性能評価を行う。
　具体的な目的(1)と(2)は前述の第１の相違点に関するものであり、(3)と(4)は第２の相違点に関わるものである。

３．研究の方法

研究の目的に記した具体的な目的(1)～(4)について、以下の方法で研究を実施した。
(1) ベクトル伝送に用いる誤り訂正符号の復号法：図１に示す基本ネットワークをはじめ、いくつかの具体的な基本ネットワークに

ついて、最適復号の条件について考察する。その際、各エッジは、２元や多元の対称通信路、あるいは加法的白色ガウス雑音のような代表的な通信路と考える。そして、最適や準最適な復号アルゴリズムを考案する。
(2) 考案した復号法の性能評価：考案した復号アルゴリズムについて、解析的手法で性能解析を行う。また、復号アルゴリズムを実現するプログラムを作成し、シミュレーションにより性能評価を行う。さらに、ベクトル毎に独立な復号法についても性能評価を行い、提案アルゴリズムの優位性を評価する。なお、誤り訂正符号の復号法や性能評価に関しては、これまでに各種のプログラム群をＣ言語で記述しており、それを拡充する形でこれらのプログラムを整備する。
(3)の線形ベクトル空間を符号語とする符号の重み構造の解析に関しては以下のように実施する。２つの符号語間距離は、dim(A∩B)で定義される。線形性をもつ符号については、従来の符号と同様、距離分布の代わりに重み分布を考えることができる。一般の符号の重み分布の計算には、全ての符号語それぞれについてその重みを計算する必要があるが、符号の構造を利用して、重みを計算する必要のある符号語数を減らすことを考える。すなわち、同じ重みをもつ符号語については代表符号語の重みだけを求めればよいので、重み分布計算の計算量を減らすことができる。
(4)の符号の性能評価については、上で考案した計算アルゴリズムに基づき、これまでに知られているいくつかの符号について、性能評価を行う。

４．研究成果

ここでは、学会発表①、②での発表内容を中心に述べる。

図１のようなネットワークを一般化して送信ノードから出るエッジがm本、受信ノード毎にそのノードへ入るエッジもm本とする。中継ノードでは、入力されたすべての情報の和をとり、すべての出力エッジへ同じデータを送る。もちろん、受信ノードそれぞれで受信したデータから送信データを復元できるようなネットワークトポロジーであることが必要である。

送信ノードでは出るエッジそれぞれに同一符号長nの２元誤り訂正符号$C_1, C_2, \ldots, C_m$を割り当てる。これらの符号は同一でもよいし、異なっていてもよい。送信ノードから各エッジに情報を送る場合には、送る情報をそのエッジに割り当てられている符号で符号化を行う。中継ノードでは、受信した複数の符号語のビット毎の排他的論理和をとり、出力する。

以下では、まず。受信ノードで受信されたビットに発生している誤りの確率を考える。1 つの受信ノードに着目する。送信ノードから着目した受信ノードまでのすべてのパスを考え、いずれかのパスに含まれるエッジを考える。このようなエッジの総数をKとし、それらすべてのエッジに対して、番号$1, 2, \cdots, K$が割り当てられているとする。一般性を失うことなく、受信ノードへの入力エッジの番号は$1, 2, \cdots, m$ とする。番号kが割り当てられたエッジをエッジkと呼ぶ。また、整数iについて$V_i = \{0,1\}^i$とする。

各エッジで発生する誤りが受信ノードで受信されるどのデータに影響するかを調べるために、まず各エッジk（$1 \le k \le K$）に対してV_mのベクトルL_kを定める。L_kのiビット目が 1 のとき、そのときに限り、エッジkで発生した誤りが受信ノードへの入力エッジi（$1 \le i \le m$）で伝わるデータに影響するものとする。このL_kは、次のアルゴリムで求めることができる。まず、各エッジk（$1 \le k \le K$）についてV_Kのベクトルを求める。エッジk（$1 \le k \le K$）のベクトルにおいて、そのk'ビット目（$1 \le k' \le K$）が 0 であるとはエッジk'の誤りがエッジ k で伝送されるデータに影響することを意味し、0 であるとはエッジkで伝送されるデータには影響しないことを意味する。このようなベクトルを送信ノードに近いエッジから順次求め、それらを用いて、各エッジについてL_k（$1 \le i \le K$）を求める。

次に、このL_kの値に基づき、エッジを分類し、各分類のエッジの本数から各誤りパターンの生起確率を求めることができることを示した。例えば、各エッジがビット誤り率pの２元対称通信路であるときに、図１のネットワークの受信ノード t1 において、a と a+b が共に誤る確率をP_{00}、a だけが誤る確率をP_{01}、a+b だけが誤る確率をP_{10}、両方誤る確率をP_{11}とする。この成果を適用すると、

$$P_{00} = \frac{(1-2p)^6}{2} + \frac{(1-2p)^2}{4} + \frac{1}{4}$$

$$P_{01} = -\frac{(1-2p)^6}{2} + \frac{(1-2p)^2}{4} + \frac{1}{4}$$

$$P_{10} = p(1-p)$$

$$P_{11} = p(1-p)$$

であることが得られる。

受信ノードで復号する場合の復号法の 1 つとして、ネットワーク符号化を適用したマルチキャストネットワークにおいて、受信語の組に対する最尤復号を実現する方法を示した。ここで、復号法とは、受信語から送信符号語を復元することを言い、最尤復号とは正しく復号される確率が最大となる復号法

である。最尤復号法は上述の確率の解析結果を用いて導出している。

また、ネットワーク符号化を適用したバタフライネットワークにおいて、4 つの復号法についての考察と性能評価を行った。以下 4 つの復号法について、復号法 1，2，3，4 と呼ぶ。復号法 1 では２つの受信語を独立に最尤復号する。 復号法 2 では、受信語に対してネットワーク符号化で行われる排他的論理和演算を行ってから最尤復号する。復号法 3 では復号法 1，2 の復号結果のうち、尤度の高い方を選択する。復号法 4 では前述の受信語の組に対する最尤復号を行う。シミュレーションの結果、復号法 3 と復号法 4 では計算量は大きく異なるが復号誤り率に大きな差はなかった。

これらの復号法の性能には、符号の結合重み分布が重要な役割を果たしていることがわかった。また、最尤復号ではなく限界距離復号法を用いる場合に、結合重み分布は特に重要である。

以下では、まず結合重み分布の定義を述べる。符号$C_1, C_2, \dots, C_m$それぞれから符号語をひとつずつ選ぶ。符号C_iの符号語を

$$\bar{v}_i = (v_{i1}, v_{i2}, \dots, v_{in})$$

とする。これらの符号語の組$(\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m)$に対して、整数$w_j$ $(0 \leq \mathrm{j} < 2^m)$を

$$w_j = \left|\left\{h \mid j = \sum_{i=1}^{m} v_{ih} 2^{i-1}\right\}\right|$$

とする。そして、

$$\bar{w} = (w_0, w_1, \dots, w_{2^m-1})$$

を符号語の組$(\bar{v}_1, \bar{v}_2, \dots, \bar{v}_m)$の結合重みと呼ぶ。すべての符号語の組のうち結合重みが$\bar{w}$である符号語の組の数を$A_{\bar{w}}$と書く。すべての結合重み$\bar{w}$について$A_{\bar{w}}$を集めたものを符号$C_1, C_2, \dots, C_m$の結合重み分布と呼ぶ。

結合重み分布は、すべての符号語の組を生成すれば求めることができる。しかし、すべてを列挙することは計算量の点で困難な場合が多い。そこで、その計算量を大幅に軽減するため、結合重み分布におけるマックウィリアムズの等式を導出した。この等式は$m = 2$の場合には既知であったが、mが 3 以上の場合は知られていなかった。

マックウィリアムズの等式では、次に定義する結合重み多項式を用いる。2^m個の変数をもつ多項式

$$\mathrm{J}(y_0, y_1, \dots, y_{2^m-1}) = \sum_{(w_0, w_1, \dots, w_{2^m-1})} A_{(w_0, w_1, \dots, w_{2^m-1})} \prod y_h^{w_h}$$

を符号$C_1, C_2, \dots, C_m$の結合重み分布多項式と呼ぶ。

符号$C_1, C_2, \dots, C_m$の代わりにそれらの双対符号を考えたとき、その結合重み分布多項式を$\mathrm{J}'(y_0, y_1, \dots, y_{2^m-1})$と書く。$m = 2$の場合は、

$$\mathrm{J}'(y_0, y_1, y_2, y_3) = \frac{1}{|C_1||C_2|} J(y_0 + y_1 + y_2 + y_3, y_0 - y_1 + y_2 - y_3, y_0 + y_1 - y_2 - y_3, y_0 - y_1 - y_2 + y_3)$$

がマックウィリアムズの等式として知られている。この式から双対符号について結合重み分布を求めることができれば、元の符号についての結合重み分布を求めることができる。この等式を一般のmの場合に拡張した式を示した。

例えば、$m = 3$の場合は、次式が得られている。

$$\begin{aligned}
&\mathrm{J}'(y_0, y_1, y_2, y_3, y_4, y_5, y_6, y_7) \\
&= \frac{1}{|C_1||C_2||C_3|} \\
&\mathrm{J}(y_0 + y_1 + y_2 + y_3 + y_4 + y_5 + y_6 + y_7, \\
&\quad y_0 - y_1 + y_2 - y_3 + y_4 - y_5 + y_6 - y_7, \\
&\quad y_0 + y_1 - y_2 - y_3 + y_4 + y_5 - y_6 - y_7, \\
&\quad y_0 - y_1 - y_2 + y_3 + y_4 - y_5 - y_6 + y_7, \\
&\quad y_0 + y_1 + y_2 + y_3 - y_4 - y_5 - y_6 - y_7, \\
&\quad y_0 - y_1 + y_2 - y_3 - y_4 + y_5 - y_6 + y_7, \\
&\quad y_0 + y_1 - y_2 - y_3 - y_4 - y_5 + y_6 + y_7, \\
&\quad y_0 - y_1 - y_2 + y_3 - y_4 + y_5 + y_6 - y_7)
\end{aligned}$$

$m = 3$の場合、すべての符号が (63，57) ハミング符号であれば、符号語の組の総数は 2^{171} 個あり、すべてを列挙することはできない。一方、すべての符号について、その双対符号を考えれば符号語の組の総数は 2^{18} 個なので、数え上げが容易であり、計算量は大幅に軽減できる。ただし、双対符号の符号語数があまり少なくない場合に計算するためには、マックウィリアムの等式の計算手順を工夫して、記憶量や計算時間を減らすことが必要である。これについては検討を続けている。

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）

〔学会発表〕（計 2 件）

① 貴戸 祥郎、藤原 融：“ネットワーク符号化における線形ブロック符号の復号誤り確率の評価のための結合重み分布に対するマックウィリアムズの等式”、第 34 回

情報理論とその応用シンポジウム、3.4.1 (CD-ROM) (2011-11)

② 太田 和伸、<u>藤原 融</u>:“ネットワーク符号化における 2 元線形符号の最尤復号とその性能評価”、第 33 回情報理論とその応用シンポジウム、41.2 (CD-ROM) (2010-12)

６．研究組織

(1)研究代表者

藤原　融 (FUJIWARA TORU)

大阪大学・大学院情報科学研究科・教授

研究者番号：70190098

(2)研究分担者

なし

(3)連携研究者

なし