補助ノードを用いた安全な線形ネットワーク符号構成多項式時間アルゴリズム

久保友樹 48096214 指導教員 山本博資教授

2011 年 2 月 1 日

1 はじめに

ネットワーク符号化とは，情報を送信する情報源点と情報を受信する受信点の間に多くの情報を伝送することを考える分野である．1 点から複数の点へ同一の情報を伝送するマルチキャスト通信に対しては，伝送可能な情報量の上限が最大フローと関係した値で厳密に与えられる [1]．この上限を達成する符号が，線形符号を用いて構成できる [2]．盗聴者に対する安全性を高め，秘密情報を秘匿して伝送する方式も知られている [3]．さらに情報源点と受信点以外である点の補助ノードを利用することで，安全性を維持したまま，より多くの秘密情報を秘匿して伝送する方式も知られている [4]．しかしこの補助ノードを用いた方式はサイクルを含まないネットワークにのみ適用可能であった．

本稿では補助ノードを利用したネットワーク符号化のアルゴリズムをサイクルを含むネットワークにおいても適用出来るように拡張したアルゴリズムを提案する．さらにそのアルゴリズムにおいて乱数生成個数の決定問題がノード数の指数時間かかることを説明し，多項式時間アルゴリズムを提案する。

2 線形ネットワーク符号化

2.1 線形ネットワーク符号化

ネットワークを有向グラフ $G = (V, E)$ で示す．V, E はそれぞれ点および枝の集合を表す．任意の $e \in E$ に対して枝の容量は $\mathrm{cap}(e) = 1$ であるとする．

定理 2.1 ([1])**.** 有向グラフ $G = (V, E)$ において，情報源点 $s \in V$ から受信点集合 $T \subset V$ へ $X^n = (X_1, X_2, \cdots, X_n)$ を誤りなく伝送できる必要十分条件は，$n \leq h$ である．ただし h は次式で定義される．

$$h \equiv \min_{t \in T} \mathrm{maxflow}(s, t). \tag{1}$$

線形ネットワーク符号化では枝に符号化ベクトルを割り当てることで符号化を行う．符号化ベクトルは次に定義する枝の位相的順序に従いを割り当てる．

定義 2.1 (位相的順序)**.** アサイクリックな有向グラフ $G = (V, E)$ に対して，点 $u \in V$ から点 $v \in V$ へのパスが存在するなら $u \prec v$ という半順序 $\prec$ を構成できる．この半順序を満たす線形順序を位相的順序という．

2.2 k-secure ネットワーク符号化

盗聴者が G のいくつかの枝を盗聴できる時，情報源点 s から全ての受信点 $t \in T$ に秘密情報 $S^r = (S_1, S_2, \cdots, S_r)$ を安全に伝送することを考える．また，情報源点は S^r およびそれと独立な F_q 上の一様乱数 $R_1, R_2, \cdots, R_{h-r}$ を生成する．k-secure ネットワーク符号とはどの k 本以下の枝を盗聴したとしても，盗聴者に S^r の情報は漏洩しない符号のことである．strongly k-secure な線形ネットワーク符号とは，k-secure であり，$0 \leq j \leq r-1$ に対して盗聴者がどの $k+j$ 本の枝を盗聴したとしても，どの $(S_{i_1}, S_{i_2}, \cdots, S_{i_{r-j}})$ も陽に漏洩しない，k-secure な符号よりもより安全な符号のことである．

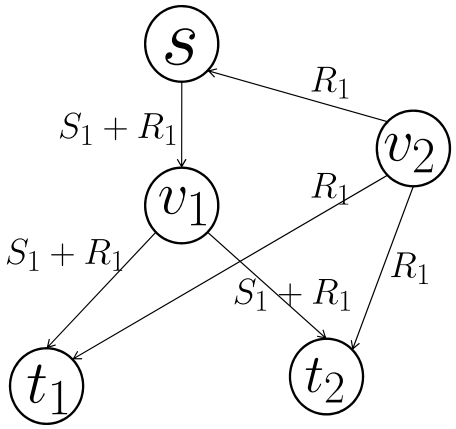

図 1 補助点を用いた符号化例

安全なネットワーク符号について次の定理が証明されている．

定理 2.2 ([2][3])**.** k-secure な線形ネットワーク符号及び strongly k-secure な線形ネットワーク符号が存在するための必要十分条件は，$r \leq h - k$ を満たすことである．

3 補助ノードを用いた線形ネットワーク符号化

3.1 導入

乱数 R^l は容量が h のとき，$r + k \leq r + l \leq h$ を満たしていなければならない．よって $r > h - k$ であるような S^r に対して k-secure なネットワーク符号を構成することができないことが分かる．しかし，定理 2.2 において，暗に情報源点以外の点では乱数を生成できないことを仮定している．

例として図 1 のようなネットワークについて考えてみる．s は情報源点，t_1, t_2 は受信点である．このネットワークは $h = 1$ であるから，定理 2.2 より安全なネットワーク符号化を行うことは不可能である．しかし，点 v_2 が乱数 R_1 を生成できるとき，図 1 のように容易に 1-secure なネットワーク符号化を行うことができる．

このような補助点を用いた安全なネットワーク符号化が原田 [3] によって提案されている．

乱数を生成する補助ノードの集合 $W \subset V \setminus (\{s\} \cup T)$ が与えられている場合を考える．$v \in W$ を補助ノードとする．

ここで (s, T, W) に対して次のように k_0 を定義する．

$$k_0 \equiv m(W) = \sum_{v:v\in W} m(v). \tag{2}$$

ただし $m(v)$ はどの $U \subseteq W$ に対しても次の不等式を満たす整数とする．

$$m(U) = \sum_{v:v\in U} m(v) \le \min \Bigg[\min_{t\in\{s\}} \mathrm{maxflow}(U,t), \min_{t\in T} \mathrm{maxflow}(s\cup U, t) - h \Bigg] \tag{3}$$

このとき次の定理が成立する．

定理 3.1 ([4])**.** (s, T) が容量 $h = \mathrm{maxflow}(s, T)$ を持ち，ある $W \subset V \setminus (\{s\} \cup T)$ に対して式 (2) で定義される値が k_0 であるとする．このとき $S^h = (S_1, S_2, \cdots, S_h)$ を s から T へ，strongly k_0-secure なネットワーク符号により伝送できる．

グラフにサイクルがない場合に対して，原田が定理 3.1 を証明したが，3.2 節の方式を用いることにより，グラフにサイクルがある場合でも，式 (3) が達成可能なことを明らかにした

3.2 ネットワークがサイクルを含む場合

サイクルを含むネットワークでは位相的順序が定義できない．そこでサイクル内の枝を一度に符号化することによって符号化を行う．サイクルを含むネットワーク符号を取り扱っている文献 [5] の手法を用い，時刻という概念を導入する．時刻 a で生成される情報と乱数を $S(a), R(a)$ のように表す．さらに線形遅延演算子 D を導入する．D は次のように $\sigma(a)$ に作用する．

$$D(\sigma(a)) = D\sigma(a) = \sigma(a-1) \tag{4}$$

符号化ベクトルの要素は D の有理関数 $F(D)$ となる．

4 補助ノードを用いたネットワーク符号構成のための多項式時間アルゴリズム

本章では式 (2) の k_0 を最大化することについて考える．そのためには，式 (3) を満たす $m(v)$ を求める必要があるが，式 (3) は補助点集合 W の任意の部分集合を調べる必要があり，$\max k_0$ を求めようとすると W の全てのべき集合について調べなければならない．そのため W のサイズが大きい時，計算量が大きくなり，実用的に困難になる欠点がある．そこで本章では，計算量が W のサイズの多項式時間で $k_0 = \sum_v m(v)$ が求められるアルゴリズムを考える．

4.1 受信点が一つの場合

受信点が一つの場合について，式 (2)(3) を満たす $m(v)$ を求める問題を次の二つのポリマトロイドの交差問題に帰着できる．

$$\begin{aligned} &\text{Maximize } \ m(W) \\ &\text{subject to } \ m(X) \le \min\{f_1(X), f_2(X)\} \ \ \forall X \in W \end{aligned}$$

なお f_1, f_2 は次に定義する劣モジュラ関数である．

定義 4.1. E を空でない有限集合とし，D を E のべき集合とする．また，$X, Y \in D$ とする時，$X \cup Y, X \cap Y \in D$ である．任意の X, Y で次式を満たす関数 $f : D \to R$ を D 上の劣モジュラ関数とする．

$$\forall X, Y \in D : f(X) + f(Y) \ge f(X \cup Y) + f(X \cap Y) \tag{5}$$

この問題は文献 [6] の Fujishige のアルゴリズム (An Algorithm by Path Augmentation) を実行することで解けるが，その際に交換容量という値を計算する必要がある．文献 [6] のアルゴリズムは W の要素数 $|W|$ をとすると，$\mathrm{O}(|W|^3\eta)$ で計算できる．Ford-Fulkerson のアルゴリズム [7] を用いることにより，交換容量を v を始点とする有向枝の数 $\mathrm{Out}(v)$ を用いて $\mathrm{O}(|E| \cdot |\max_{v\in W}(\mathrm{Out}(v))|)$ 時間で計算することができる．したがって次の定理が成立する．

定理 4.1. 受信点一つの場合には $\mathrm{O}(|W| \cdot |E| \cdot |\max_{v\in W}(\mathrm{Out}(v))|)$ 時間で最適な k_0 と $m(v), v \in W$ を求めることができる．

4.2 受信点が二つ以上の場合

受信点が二つ以上の場合は三つ以上のポリマトロイドの交差問題に対応するため，整数範囲での最適解を求めるのは非常に困難である．そこで各補助点 v から情報源点 s と各受信点 t へ，それぞれ辺素パス $m(v)$ 本を求めるための「パス選定アルゴリズム」を，Greedy アルゴリズムとして提案する．$d_t, t \in T$ を受信点 t の入力枝の数とする．条件 $(k_0 = \min_t d_t - h)$ を満たして終了したときは，最適値を達成できる．しかし，そうでない場合は，一般には最適値を実現できるとは限らない．このアルゴリズムは計算量が W の要素数 $|W|$ の多項式時間で終了する．「パス選定アルゴリズム」によって最適値が求まらなかった場合に，求まっている k_0 を改善する「k_0 改善アルゴリズム」も提案する．しかし「k_0 改善アルゴリズム」を実行しても最適解が得られるとは限らない．

参考文献

[1] R. Ahlswede, N. Cai, S. Y. R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. on Inform. Theory, vol. 46, no. 4, pp. 1204–1216, July 2000.

[2] N. Cai and R. Y. Yeung, "Secure network coding," Proceedings of IEEE ISIT'02, p. 323, June 2002.

[3] K. Harada and H. Yamamoto, "Strongly Secure Linear Network Coding," IEICE Trans. on Fundamentals, vol. E91, no. 10, pp. 2720–2728, Oct. 2008.

[4] 久保友樹, 原田邦彦, 山本博資, "余剰リソースを利用する安全な線形ネットワーク符号化,"信学技報, IT2009-142, pp. 449–455, 2010.

[5] A. I. Barbero and Ø. Ytrehus, "An effcient centralized binary multicast network coding algorithm for any cyclic network," arXiv:0705.0085v1 [cs.IT] 1 May 2007, Feb. 5, 2008

[6] S. Fujishige, X. Zhang, New Algorithms for the Interesection Problem of Submodular Systems. Japan J. Indust. Appl. Math., vol. 9, Number 3, pp. 369–382

[7] A. Schrijver, "Combinatorial Optimization," Algorithms and Combinatorics, Springer Velag, 2003.