修正箇所あり

The 31st Symposium on Information Theory and its Applications (SITA2008)
Kinugawa, Tochigi, Japan, Oct. 7–10, 2008

ネットワークコーディングにおける誤り訂正符号の復号法についての一検討

On decoding error correcting codes for linear network coding

栗原正純*
Masazumi KURIHARA

Abstract— In this paper several decoding methods for error correcting codes(ECC) for linear network coding are presented. We introduce a concept of a parity check matrix and syndromes into the decoding the ECC. We treat three types of 1) errors, 2) erasures, and 3) errors and erasures as noise in a network. For each noise, a decoding method by using the parity check matrix and syndromes is given and its time complexity is estimated.

Keywords— Network coding, error correcting codes(ECC), decoding, network error correcting codes(NECC)

1 まえがき

本稿では, 線型なネットワークコーディングを扱う. ネットワークコーディングにおける誤り訂正符号のことをネットワーク誤り訂正符号 (Network Error Correcting Code(NECC)) という.

Cai and Yeung によって最初に NECC についての研究が行なわれた [1, 2, 3]. その後, Zhang[4], Yang ら [6, 7], Matsumoto[8] により NECC の構成法や復号法に関する研究が行なわれた. Zhang[4, 5] や Yang ら [7] は, それぞれ符号空間にある種の距離の概念を導入し, それらを利用した探索的な復号法を示している. また, Matsumoto[8] も exhaustive search による復号法を示している.

一方, 復号法に関し, Bahramgiri ら [9] は, 線型性を利用し, 従来の符号理論で扱う検査行列およびシンドロームのアイデアを NECC に導入し, シンドロームを利用した復号法を示している. 本稿でも, NECC に対し検査行列およびシンドロームのアイデアを導入した復号法について提案をするが, Bahramgiri ら [9] とは独立に行なわれた研究である. 本稿で提案する幾つかの復号法や Bahramgiri ら [9] の提案する復号法のいずれも探索的な方法による復号法ではあるが, 検査行列を用いることで復号に要する計算量の評価において, q^k という因子が現れない点に特徴がある. ここで, q と k は, 有限体 $\mathbb{F}_q$ 上の線型な NECC の次元が k であることに対応する.

本稿では, Matsumoto[8] により提案された NECC の構成法で得られるネットワーク α-誤り訂正符号 (Network α-Error-Correcting Code(Nα-ECC)) に対する復号について議論する. 本稿の構成は以下の通り. 2 節では, 準備として, [8] にしたがった Nα-ECC の定義を主に行なう. 2 節では, Nα-ECC に対応する検査行列やシンドロームの定義を与える. ネットワーク上で発生する雑音を 1) 誤り, 2) 消失, 3) 誤り + 消失の 3 種類に分類し, 以下の幾つかの復号法を提案する: 単一誤り訂正 (4 節), 多重誤り訂正 (5 節), 消失訂正 (6 節), 誤り + 消失訂正 (7, 8 節). 最後に, 9 節は結論である.

2 準備

本節では, 準備として, Matsumoto[8] により示された Nα-ECC や記号等について説明を行なう.

記号 $\mathbb{F}_q$ は q 個の元からなる有限体を表す. ただし, 有限体のサイズは, Nα-ECC を構成可能なサイズであるとする. サイクルのない, 有向な多重グラフを $G = (V, E)$ と表す. 各リンクの通信容量は, $\mathbb{F}_q$ の 1 個の元のみを伝送可能な単位容量とする. 記号 $s(\in V)$ と $T(\subset V)$ をそれぞれソースとシンクの集合とする. ソースから各シンクへの最大流の最小値を n と表す. ノード $v \in V$ に対し, $\Gamma^-(v)$ ($\Gamma^+(v)$) は, v へ入力する (v から出力する) リンクの集合を表す. 有向リンク $e \in E$ に対し, start(e) (end(e)) は, e の始点 (終点) を表す.

ネットワーク G を用いてマルチキャストを行ない, 情報 $\vec{i} \in \mathbb{F}_q^k$ をソースから全てのシンクに伝送することを考える.

NECC では, 誤りを以下のように定義する. リンク $e \in E$ に対し, start(e) からの送信シンボルと end(e) での受信シンボルが異なるとき, リンク e で誤りが発生したという. そして, 誤り値は, 受信シンボルから送信シンボルを引いた値である. ネットワーク G 上で発生した誤りを $\vec{e} \in \mathbb{F}_q^{|E|}$ と表す. ベクトル $\vec{x}$ のハミング重みを $w(\vec{x})$ と表す.

Nα-ECC とは, 発生した誤り $\vec{e} \in \mathbb{F}_q^{|E|}$ が $w(\vec{e}) \le \alpha$ を満たすならば, 各シンクが受信シンボル列から送信情報 $\vec{i} \in \mathbb{F}_q^k$ を正しく復号できるネットワークコーディングのことである. ただし, n, k, α の関係は $n - k \ge 2\alpha$ を満たす.

記号 F をリンク E の部分集合で, $|F| = 2\alpha$ を満たすものとする. このとき, F をエラーパターンといい, F のリンクだけで誤りの発生が許されるものとする.

情報 $\vec{i} \in \mathbb{F}_q^k$ と誤り $\vec{e} \in \mathbb{F}_q^{|E|}$ に対し, シンク $t \in T$ がその入力リンクから受信する受信ベクトルを $\phi_t(\vec{i}, \vec{e}) \in \mathbb{F}_q^{|\Gamma^-(t)|}$ と表す (Definition 3 in [8]).

Matsumoto[8] の構成法により, $\mathbb{F}_q$ 上の線形な Nα-ECC を構成することができる. 具体的には, ネットワークの各リンクに対応する local coding vector が決定される. そして, 以下の線形空間が得られる (Section 3 in [8] を参照).

$$V_1 = \{\phi_t(\vec{i}, \vec{e}) \mid \vec{i} \in \mathbb{F}_q^k, \vec{e} \in \mathbb{F}_q^{|E|}\}, \tag{1}$$
$$V_2 = \{\phi_t(\vec{i}, \vec{0}) \mid \vec{i} \in \mathbb{F}_q^k\}, \tag{2}$$
$$V_3 = \{\phi_t(\vec{0}, \vec{e}) \mid \vec{e} \in \mathbb{F}_q^{|E|}\}. \tag{3}$$

ただし, 上式中の $\vec{e}$ について, $E \setminus F$ に対応する $\vec{e}$ の成分は零である. このとき, 以下の性質が成り立つ ([8] の式 (3,6,7) を参照).

$$V_1 = V_2 + V_3, \tag{4}$$
$$\dim V_2 = k, \tag{5}$$
$$\dim V_2 \cap V_3 = 0. \tag{6}$$

符号化が構築され, ネットワーク内のすべてのリンクに対応する local coding vector が定まることは, すなわち, ϕ_t が定まることである. 具体的には, 線形な符号化が構築されることで, ϕ_t は $\mathbb{F}_q$ の元を成分としてもつ行列を用いて表現できる. このことより, 任意の $\vec{i}_1, \vec{i}_2 \in \mathbb{F}_q^k$, $\vec{e}_1, \vec{e}_2 \in \mathbb{F}_q^{|E|}$ と任意の $a_1, a_2, b_1, b_2 \in \mathbb{F}_q$ に対し, 次の関係が成立する:

$$\begin{aligned}\phi_t(a_1\vec{i}_1 + a_2\vec{i}_2, b_1\vec{e}_1 + b_2\vec{e}_2) &= a_1\phi_t(\vec{i}_1, \vec{0}) \\ &+ a_2\phi_t(\vec{i}_2, \vec{0}) + b_1\phi_t(\vec{0}, \vec{e}_1) + b_2\phi_t(\vec{0}, \vec{e}_2)\end{aligned} \tag{7}$$

特に, 式 (6) より, 任意の $\vec{i} \in \mathbb{F}_q^k$ と $\vec{e} \in \mathbb{F}_q^{|E|}$ に対し, $w(\vec{e}) \le \alpha$ ならば, $\phi_t(\vec{i}, \vec{e})$ を $\phi_t(\vec{i}, \vec{e}) = \phi_t(\vec{i}, \vec{0}) + \phi_t(\vec{0}, \vec{e})$ に一意に分解することができる.

さらに, 式 (5) より, 任意の $z \in V_2$ に対し, $\phi_t(\vec{i}, \vec{0}) = z$ を満たす $\vec{i} \in \mathbb{F}_q^k$ が一意に定まる. ϕ_t が行列を用いて表されることより, 代数的な演算のみで z から $\vec{i}$ を求めることが可能である. そこで, 便宜上, ϕ_t の逆写像のような表現を用いて, $z \in V_2$ に対応する $\vec{i} \in \mathbb{F}_q^k$ を

$$\phi_t^{-1}(z) = \vec{i} \tag{8}$$

と表すことにする.

* 電気通信大学 (UEC Tokyo) 情報通信工学科 Dept. of Infor. and Comm. Eng.(ICE), Univ. of Electro-Communications(UEC), 1-5-1, Chofugaoka Chofu-shi, Tokyo 182-8585 Japan. E-mail: kuri@ice.uec.ac.jp

3　検査行列とシンドローム

ベクトル間の内積を考え, 次元 k の線形空間 V_2 の直交補空間を $V_2^{\perp} = \{w \in \mathbb{F}_q^{|\Gamma^-(t)|} \mid wv^T = 0 \text{ for all } v \in V_2\}$ と表す. ただし, v^T はベクトル v の転置を表す. 線形空間の基礎知識より, $V_2^{\perp}$ は線形空間であり, $\dim V_2^{\perp} = |\Gamma^-(t)| - k$ が成り立つ. さらに, $(V_2^{\perp})^{\perp} = V_2$ が成り立つ.

空間 $V_2^{\perp}$ を張る $|\Gamma^-(t)| - k$ 個の基底を選び, それらを並べた $\mathbb{F}_q$ 上の $(|\Gamma^-(t)| - k) \times |\Gamma^-(t)|$ 行列を H_t と表す. このとき, 以下が成り立つ.

$$H_t z^T = 0^T \qquad \text{for all } z \in V_2, \tag{9}$$

$$H_t z^T \neq 0^T \qquad \text{for all } z \in \mathbb{F}_q^{|\Gamma^-(t)|} \setminus V_2. \tag{10}$$

ここで, 0 は零ベクトル $0 = (0, \ldots, 0) \in \mathbb{F}_q^{|\Gamma^-(t)|-k}$ を表す. 行列 H_t を V_2 の検査行列ということにする.

式 (9, 10) より, 任意の $\vec{i} \in \mathbb{F}_q^k$ と $\vec{e} \in \mathbb{F}_q^{|E|}$ に対し,

$$H_t\phi_t(\vec{i}, \vec{e})^T = H_t\phi_t(\vec{i}, \vec{0})^T + H_t\phi_t(\vec{0}, \vec{e})^T = H_t\phi_t(\vec{0}, \vec{e})^T$$

が成り立つ. 任意の $z \in \mathbb{F}_q^{|\Gamma^-(t)|}$ に対し, シンドローム $\sigma(z) = (\sigma_1(z), \ldots, \sigma_{|\Gamma^-(t)|-k}(z)) \in \mathbb{F}_q^{|\Gamma^-(t)|-k}$ を

$$\sigma(z)^T = H_t z^T \tag{11}$$

と定義する. 後に示す復号法で用いる準備として, $\sigma(z)$ に対する次数 $\deg \sigma(z)$ を

$$\deg \sigma(z) = \min\{i \mid \sigma_i(z) \neq 0,\ 1 \leq i \leq |\Gamma^-(t)| - k\} \tag{12}$$

と定義する.

シンク $t \in T$ に対し, V_3 の部分集合として次のものを考える. 誤り個数 (ハミング重み) が 1 で, かつ, 誤り値が 1 である誤り $\vec{e}$ による非零ベクトルになる $\phi_t(\vec{0}, \vec{e})$ の集合を

$$U_t = \{\phi_t(\vec{0}, \vec{e}) \mid \vec{e} \in \mathbb{F}_2^{|E|},\ w(\vec{e}) = 1\} \setminus \{(0, \ldots, 0)\} \tag{13}$$

と表す. つまり, 式 (13) の $\vec{e}$ は単位ベクトルである. 式 (7) より, 任意の $\vec{e} \in \mathbb{F}_q^{|E|}$ に対し, シンク t での受信ベクトル $\phi_t(\vec{0}, \vec{e})$ は, U_t の適当な元の線形結合で表すことができる. 要素数が 1 個である U_t の部分集合の全体からなる集合を

$$\wp_1(U_t) = \{\{u\} \mid \{u\} \subseteq U_t\} \tag{14}$$

とする. すなわち, $|\wp_1(U_t)| = \binom{|U_t|}{1} = |U_t|$ である. そして, 集合 $\wp_1(U_t)$ の各要素 $\{u\}$ に対し, u を用いて張ることができる $\mathbb{F}_q$ 上の線型空間を対応させる. この線型空間を $\mathrm{spn}(\{u\})$ と表すことにする. このとき, 集合 $\wp_1(U_t)$ 上に線型部分空間の性質を用いた (半) 順序関係 $\preceq$ を導入することができる. つまり, $\wp_1(U_t)$ の二つの要素 $\{u\}$ と $\{u'\}$ に対応するそれぞれの線型空間 $\mathrm{spn}(\{u\})$ と $\mathrm{spn}(\{u'\})$ の間に, 部分空間の関係 $\mathrm{spn}(\{u\}) \subseteq \mathrm{spn}(\{u'\})$ が成り立つならば, $\{u\} \preceq \{u'\}$ と定義する. また, $\mathrm{spn}(\{u\}) \subseteq \mathrm{spn}(\{u'\})$ かつ $\mathrm{spn}(\{u\}) \supseteq \mathrm{spn}(\{u'\})$ のとき, 関係 $\preceq$ 上 $\{u\}$ と $\{u'\}$ を同一視する. ここで, 順序集合 $(\wp_\alpha(U_t), \preceq)$ の極大元のみからなる集合を以下のように表す.

$$\mathrm{maximal}(\wp_1(U_t)) \tag{15}$$

以上の準備より, 次節において単一誤り訂正の復号法について説明をする.

4　単一誤り訂正/α-誤り検出

4.1　アルゴリズム

最初に, 前節までに準備したものを用いて, Nα-ECC に対する単一誤り訂正/α-誤り検出可能なアルゴリズムを示す.

Initialize $M = \mathrm{maximal}(\wp_1(U_t))$.

1. Input the received vector z.
2. Compute $\sigma(z)^T = H_t z^T$.
3. If $\sigma(z) = 0$ then output the information vector $\phi_t^{-1}(z)$ and halt else goto 4. (See the eq. (8) for $\phi_t^{-1}(z)$.)
4. Choose an $\{u\} \in M$ and compute $\sigma(u)^T = H_t u^T$.
5. If $\deg \sigma(z) = \deg \sigma(u)$ then set $m = \deg \sigma(z)$ and goto 6 else goto 7. (See the eq. (12) for $\deg \sigma(z)$.)
6. If $\sigma(z) = \frac{\sigma_m(z)}{\sigma_m(u)}\sigma(u)$ then output the information vector $\phi_t^{-1}(z - \frac{\sigma_m(z)}{\sigma_m(u)}u)$ and halt else goto 7.
7. Update $M = M \setminus \{u\}$. If $M = \emptyset$ then output "Error is detected" and halt else goto 4.

次に, アルゴリズムが正しいことを示そう. 具体的には, 以下の 2 つの命題を示せばよい.

A. $^{\exists}u \in U$ such that $\sigma(z) = \frac{\sigma_m(z)}{\sigma_m(u)}\sigma(u)$ if $w(\vec{e}) = 1$.

B. $z - \frac{\sigma_m(z)}{\sigma_m(u)}u \in V_2$ if $\sigma(z) = \frac{\sigma_m(z)}{\sigma_m(u)}\sigma(u)$.

まず, A が成り立つことを示そう. 実際に発生した単一誤りを $\vec{e}_v$ と表す. すなわち, $w(\vec{e}_v) = 1$. その誤り値を $v \in \mathbb{F}_q$ と表す. 一方, 記号 $\vec{e}_1 \in \mathbb{F}_2^{|E|}$ を $\vec{e}_v = v\vec{e}_1$ を満たす単位ベクトルとする. このとき, $\phi_t(\vec{0}, \vec{e}_v) = v\phi_t(\vec{0}, \vec{e}_1)$ が成り立つ. したがって, 情報 $\vec{i}$ と誤り $\vec{e}_v$ に対する受信ベクトルは $z = \phi_t(\vec{i}, \vec{e}_v) = \phi_t(\vec{i}, \vec{0}) + v\phi_t(\vec{0}, \vec{e}_1)$ と表せる. また, U_t の定義より, $\phi_t(\vec{0}, \vec{e}_1) \in U_t$ である. そこで, $u = \phi_t(\vec{0}, \vec{e}_1)$ とすれば, 以下が成り立つ. $\sigma(z)^T = H_t\phi_t(\vec{i}, \vec{e}_v)^T = vH_t\phi_t(\vec{0}, \vec{e}_1)^T = v\sigma(u)^T$. これより, $m = \deg \sigma(z)$ とすれば, $\sigma_m(z) = v\sigma_m(u)$ を得る. ゆえに, $\sigma(z) = v\sigma(u) = \frac{\sigma_m(z)}{\sigma_m(u)}\sigma(u)$ を満たす $u \in U_t$ が存在することがいえた.

次に, B が成り立つことを示すには, $H_t(z - \frac{\sigma_m(z)}{\sigma_m(u)}u)^T = 0$ が成り立つことを示せばよい. $H_t(z - \frac{\sigma_m(z)}{\sigma_m(u)}u)^T = H_t z^T - \frac{\sigma_m(z)}{\sigma_m(u)}H_t u^T = \sigma(z)^T - \frac{\sigma_m(z)}{\sigma_m(u)}\sigma(u)^T = 0^T$. 以上より, B が成り立つことがいえた.

4.2　符号化と復号の例

図 1 のネットワーク G に対し, 有限体 $\mathbb{F}_5 = \mathbb{Z}/(5)$ 上の Nα-ECC を構成する. ここで, $\mathbb{Z}$ は整数の全体の集合を表す. ソースから各シンクへの最大流の最小値は $n = 3$ となる. そこで, $k = 1, \alpha = 1$ として, 以下のような Nα-ECC を構成する. $k = 1$ より, 図 1 にて, 仮想ソース s' からソース s への仮想リンクの本数が 1 本となる.

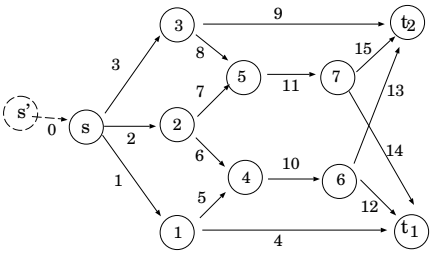

図 1: Example of a network $G = (V, E)$ with the imaginary source node s' and the imaginary edge e_0, where $V = \{s, v_1, \ldots, v_7, t_1, t_2\}$ and $E = \{e_1, \ldots, e_{15}\}$. Node s is the souce node and nodes t_1 and t_2 are the sink nodes.

記号 $y(e) \in \mathbb{F}_q$ はリンク e を流れるシンボルを表す. リンク e に対応する local coding vector とは, 線形結合 $y(e) = \sum_{e' \in \Gamma^-(\mathrm{start}(e))} m_e(e')y(e')$ の係数ベクトル $(m_e(e'))_{e' \in \Gamma^-(\mathrm{start}(e))} \in \mathbb{F}_q^{|\Gamma^-(\mathrm{start}(e))|}$ のことである.

リンク e_{10} と e_{11} に対する local coding vector をそれぞれ $m_{e_{10}} = (m_{e_{10}}(e_5), m_{e_{10}}(e_6)) = (1, 1) \in \mathbb{F}_5^2$, $m_{e_{11}} = (m_{e_{11}}(e_7), m_{e_{11}}(e_8)) = (1, 2) \in \mathbb{F}_5^2$ と設定する. すなわち, $y(e_{10}) = 1 \cdot y(e_5) + 1 \cdot y(e_6)$, $y(e_{11}) = 1 \cdot y(e_7) + 2 \cdot y(e_8)$ である. そして, その他のリンクに対する local coding vector は 1 次元ベクトルとなるが, それらの成分の値はすべて 1 と設定する. このような local coding vector の設定により, 性質 (式 (4, 5, 6)) を満たす Nα-ECC が得られる.

このとき, シンク t_2 で受信する受信ベクトル $z \in \mathbb{F}_5^3$ を $z = \phi_{t_2} = (y(e_{13}), y(e_{15}), y(e_9))$ と設定する. すると, シンク t_2 での V_2 および U_{t_2} はそれぞれ $V_2 = \{a(2,3,1) \mid a \in \mathbb{F}_5\}$, $U_{t_2} = \{(1,0,0), (0,1,0), (0,2,0), (0,0,1), (1,1,0), (0,2,1)\}$ となる. さらに、maximal$(\wp_1(U_{t_2})) = \{(1,0,0), (0,1,0), (0,0,1), (1,1,0), (0,2,1)\}$ となる.

線形空間 V_2 の直交補空間 $V_2^{\perp}$ を張る 2 個の基底ベクトル $(1,1,0), (1,0,3)$ を選び, $H_{t_2} = \begin{bmatrix} 110 \\ 103 \end{bmatrix}$ とする.

ソースから情報 $\vec{i} = (3) \in \mathbb{F}_5^1$ を送信し, 誤り $\vec{e} = (0,0,2,0,\ldots,0) \in \mathbb{F}_5^{15}$ が発生したものとする. ただし, $\vec{e}$ はリンク e_3 において誤り値 2 の誤りが発生した誤りを表す. すると, シンク t_2 では受信ベクトル $z = \phi_t(\vec{i}, \vec{e}) = \phi_t(\vec{i}, \vec{0}) + \phi_t(\vec{0}, \vec{e}) = (1,4,3) + (0,4,2) = (1,3,0)$ を受信することになる.

4.1 節のアルゴリズムでは, 受信ベクトル $z = (1,3,0)$ を入力し (Step 1), z に対するシンドローム $\sigma(z) = (4,1)$ を計算する (Step 2). $\sigma(z) \neq (0,0)$ より (Step 3), $u \in U$ を選び, $\sigma(u)$ を計算で求める (Step 4). このとき, $u = (0,2,1) \in U$ が選ばれたとして, $\sigma(u) = (2,3)$ を計算で求める (Step 4). $\deg \sigma(z) = \deg \sigma(u) = 1$ より, $m = 1$ とする (Step 5). $\sigma_1(z) = 4, \sigma_1(u) = 2$ より, $\sigma(z) = (4,1) = \frac{4}{2}(2,3) = \frac{\sigma_1(z)}{\sigma_1(u)}\sigma(u)$ が成り立つことが分かる. そして, $z - \frac{\sigma_1(z)}{\sigma_1(u)}u = (1,3,0) - \frac{4}{2}(0,2,1) = (1,-1,-2) = (1,4,3)$ より, 推定送信情報として $\phi_{t_2}^{-1}((1,4,3)) = (3)$ を得ることができる (Step 6).

4.3 関数 ϕ_t の例

本節では, 前節までに設定した符号化により定まる ϕ_t を具体的に記述する. ϕ_t の表し方は幾通りか考えられる. 本例では, Koetter ら [10] の Section III.A. Transfer Matrices において定義されたリンク間の隣接状況を表す $|E| \times |E|$ 隣接行列 (adjacency matrix)F を修正した $(k+|E|) \times (k+|E|)$ 行列 F' を用いることにする. ここで, F は前節までに用いたエラーパターンではないことに注意する.

符号化のために与えられたネットワーク G に仮想ソースと仮想リンクを追加したネットワークに対する隣接行列を F' と表すと, その行列は $(k+|E|) \times (k+|E|)$ 行列となり, 本例では, 以下のように書き表される. ただし, 行 (列) に関して, 上から下 (左から右) 方向に対し, リンク $e_0, e_1, \ldots, e_{15}$ を順に対応させている.

$$F' = \begin{bmatrix}
0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

この F' から Transfer Matrix(Theorem 3 in [10]) の要素行列 $(I-F)^{-1}$ に対応する $(k+|E|) \times (k+|E|)$ 行列 $(I-F')^{-1} = I + F' + F'^2 + \cdots$ を計算する. ここで, I は単位行列を表す. 本例では, $(I-F')^{-1} = I + F' + F'^2 + F'^3 + F'^4$ が成り立つ.

各シンク $t \in T$ に対し, t への各入力リンクに対応する行列 $(I-F')^{-1}$ の列ベクトルを取り出して並べた $(k+|E|) \times |\Gamma^-(t)|$ 伝送行列を B_t と表す. 以上の準備より, 情報 $\vec{i}$ と誤り $\vec{e}$ を入力とする ϕ_t は,

$$\phi_t(\vec{i}, \vec{e}) = ([\vec{i}, \vec{0}_{|E|}] + [\vec{0}_k, \vec{e}])B_t \tag{16}$$

と表すことができる. ここで, $\vec{0}_{|E|}$, $\vec{0}_k$ はそれぞれ長さ $|E|$, k の零ベクトルを表す. $[\vec{i}, \vec{0}_{|E|}]$ は $\vec{i}$ と $\vec{0}_{|E|}$ を連接したベクトルを表す. $[\vec{0}_k, \vec{e}]$ も同様である.

また, 式 (16) のように ϕ_t を定義した場合, $z \in V_2$ に対する ϕ_t^{-1} は

$$\phi_t^{-1}(z) = zB_t^{-1} \tag{17}$$

と表される. ここで, B_t^{-1} は $|\Gamma^{-1}(t)| \times k$ 行列で, $(k+|E|) \times k$ 行列 $B_t B_t^{-1}$ の上部部分の $k \times k$ 行列を単位行列にする行列である.

シンク t_2 では, $\phi_{t_2} = (y(e_{13}), y(e_{15}), y(e_9))$ と設定したので, $(1+15) \times 3$ 行列 B_{t_2} は $B_{t_2} = [\vec{f}'_{13}, \vec{f}'_{15}, \vec{f}'_9]$ となる. ただし, 記号 $\vec{f}'_j$, $1 \leq j \leq 16$, は行列 $(I-F')^{-1}$ の左から j 列目の列ベクトルを表す. ちなみに, B_{t_2} の 1 行目の行ベクトルは $[2,3,1]$ である. また, $B_{t_2}^{-1} = [1,1,1]^T$ となる.

4.4 計算量

4.1 節のアルゴリズムの時間計算量の主要な因子は, step $4 \to 5 \to 7 \to 4$ または step $4 \to 5 \to 7 \to 4$ というループの実行回数の上限である. このループ回数は, たかだか $|U_t|$ である. そして, $|U_t| \leq \binom{|E|}{1} = |E|$ が成り立つ. 最後に, この方法の特徴は, 情報 $\vec{i}$ の総数を表す q^k が計算量の因子に現れないことである.

5 多重誤り訂正

本節では, Nα-ECC に対し, α 個以下の多重誤りを訂正する復号法として, 探索的な手法について説明をする.

ソースから情報 $\vec{i} \in \mathbb{F}_q^k$ を送信したとき, $w(\vec{e}) \leq \alpha$ を満たす誤り $\vec{e} = (e_1, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$ が発生したとする. そして, シンク t では, 受信ベクトル $z = \phi_t(\vec{i}, \vec{e})$ を受信するとする.

式 (13) にて定義した集合 U_t の中から α 個の元 $u_1, \ldots, u_\alpha$ を選ぶ. この選び方の総数は $\binom{|U_t|}{\alpha}$ 通りある. 選び出した $u_1, \ldots, u_\alpha \in U_t$ に対し, 次の連立一次方程式 (18) を満たす解 $v_1, ..., v_\alpha \in \mathbb{F}_q$ が求まるかを調べる.

$$H_t \begin{bmatrix} u_1 \\ | \\ u_\alpha \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_\alpha \end{bmatrix} = \sigma(z)^T \tag{18}$$

$v_1, ..., v_\alpha$ が式 (18) を満たす解ならば, 以下の手続きにより, 受信ベクトル z から送信情報 $\vec{i}$ を求めることができる.

まず, $u_1, \ldots, u_\alpha$ と $v_1, ..., v_\alpha$ の組合せより, 線型結合 $\sum_{i=1}^{\alpha} v_i u_i$ を構成する. このとき, 受信ベクトル z と $\sum_{i=1}^{\alpha} v_i u_i$ の差 $z - \sum_{i=1}^{\alpha} v_i u_i$ は, $H_t(z - \sum_{i=1}^{\alpha} v_i u_i)^T = 0^T$ を満たす. したがって, $(z - \sum_{i=1}^{\alpha} v_i u_i) \in V_2$ が成り立つ. ゆえに, $\phi^{-1}(z - \sum_{i=1}^{\alpha} v_i u_i)$ を送信情報と推定することができる.

次に, 発生した誤りの個数が α 個以下ならば, 式 (18) を満たす $u_1, \ldots, u_\alpha$ と $v_1, ..., v_\alpha$ の組合せによる線型結合 $\sum_{i=1}^{\alpha} v_i u_i$ が一意に定まることを示す.

それには, 式 (18) を満たす組合せとして, $u_1, \ldots, u_\alpha$ と $v_1, ..., v_\alpha$ の組合せ以外に, $u'_1, \ldots, u'_\alpha \in U_t$ と $v'_1, ..., v'_\alpha \in \mathbb{F}_q$ の組合せが存在すると仮定すると, $\sum_{i=1}^{\alpha} v_i u_i = \sum_{i=1}^{\alpha} v'_i u'_i$ となることを示せばよい.

このことを $\sum_{i=1}^{\alpha} v_i u_i \neq \sum_{i=1}^{\alpha} v'_i u'_i$ と仮定し, 背理法を用いて証明しよう. まず, 背理法の仮定より, $\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i \neq 0$ である. さらに, $u_1, \ldots, u_\alpha$ と $v_1, ..., v_\alpha$ の組合せ, および $u'_1, \ldots, u'_\alpha$ と $v'_1, ..., v'_\alpha$ の組合せは, 式 (18) を満たすことより, $H_t(\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i)^T = 0^T$ が成り立つ. ゆえに, $0 \neq (\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i) \in V_2$ が成り立つ. 一方, ベクトル $\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i$ は, たかだか 2α 個の $u_1, \ldots, u_\alpha, u'_1, \ldots, u'_\alpha$ の線型結合で表されるベクトルであるから, $w(\vec{e'}) \leq 2\alpha$ かつ $\phi(\vec{0}, \vec{e'}) = \sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i$ を満たす誤り $\vec{e'} \in \mathbb{F}_q^{|E|}$ が存在する. したがって, V_3 の定義より, $0 \neq (\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i) \in V_3$ が成り立つ. 以上より, $0 \neq (\sum_{i=1}^{\alpha} v_i u_i - \sum_{i=1}^{\alpha} v'_i u'_i) \in V_2 \cap V_3$ が成り立つことがいえる. しかし, この結果は, Nα-ECC の構成における条件式 (6) に矛盾する. ゆえに, $\sum_{i=1}^{\alpha} v_i u_i = \sum_{i=1}^{\alpha} v'_i u'_i$ が成り立つことが示せた.

集合 U_t の中から α 個の元 $u_1, \ldots, u_\alpha$ を選び出す方法について説明する. 発生した誤りの個数が α 個以下ならば, $\binom{|U_t|}{\alpha}$ 通りある選び方の全てを試せば, 式 (18) を満たす $u_1, \ldots, u_\alpha$ と $v_1, ..., v_\alpha$ の組合せを見つけることはできる. しかし, 必ずしも $\binom{|U_t|}{\alpha}$ 通りの全てを対象にする必要はないことを以下に説明する.

要素数が α 個となる U_t の部分集合の全体からなる集合を

$$\wp_\alpha(U_t) = \{\{u_1, \ldots, u_\alpha\} \mid \{u_1, \ldots, u_\alpha\} \subseteq U_t\} \tag{19}$$

とする．すなわち，$|\wp_\alpha(U_t)| = \binom{|U_t|}{\alpha}$ である．そして，集合 $\wp_\alpha(U_t)$ の各要素 $\{u_1, \ldots, u_\alpha\}$ に対し，$u_1, \ldots, u_\alpha$ を用いて張ることができる $\mathbb{F}_q$ 上の線型空間を対応させる．この線型空間を $\mathrm{spn}(\{u_1, \ldots, u_\alpha\})$ と表すことにする．このとき，集合 $\wp_\alpha(U_t)$ 上に線型部分空間の性質を用いた (半) 順序関係 $\preceq$ を導入することができる．つまり，$\wp_\alpha(U_t)$ の二つの要素 $\{u_1, \ldots, u_\alpha\}$ と $\{u'_1, \ldots, u'_\alpha\}$ に対応するそれぞれの線型空間 $\mathrm{spn}(\{u_1, \ldots, u_\alpha\})$ と $\mathrm{spn}(\{u'_1, \ldots, u'_\alpha\})$ の間に，部分空間の関係 $\mathrm{spn}(\{u_1, \ldots, u_\alpha\}) \subseteq \mathrm{spn}(\{u'_1, \ldots, u'_\alpha\})$ が成り立つならば，$\{u_1, \ldots, u_\alpha\} \preceq \{u'_1, \ldots, u'_\alpha\}$ と定義する．また，$\mathrm{spn}(\{u_1, \ldots, u_\alpha\}) \subseteq \mathrm{spn}(\{u'_1, \ldots, u'_\alpha\})$ かつ $\mathrm{spn}(\{u_1, \ldots, u_\alpha\}) \supseteq \mathrm{spn}(\{u'_1, \ldots, u'_\alpha\})$ のとき，関係 $\preceq$ 上 $\{u_1, \ldots, u_\alpha\}$ と $\{u'_1, \ldots, u'_\alpha\}$ を同一視する．

順序集合 $(\wp_\alpha(U_t), \preceq)$ において，いま，$\wp_\alpha(U_t)$ の二つの要素 $\{u_1, \ldots, u_\alpha\}$ と $\{u'_1, \ldots, u'_\alpha\}$ の間に，$\{u_1, \ldots, u_\alpha\} \preceq \{u'_1, \ldots, u'_\alpha\}$ が成り立つと仮定する．このとき，$\{u_1, \ldots, u_\alpha\}$ に対し，式 (18) を満たす解 $v_1, ..., v_\alpha$ が存在すれば，順序関係 $\preceq$ の定義より，$\{u'_1, \ldots, u'_\alpha\}$ に対しても式 (18) を満たす解 $v'_1, ..., v'_\alpha$ が必ず存在する．すなわち，式 (18) を満たす解を求める手続きにおいて，$\wp_\alpha(U_t)$ の全ての要素を対象にする必要はなく，順序集合 $(\wp_\alpha(U_t), \preceq)$ の極大元のみを対象にすれば十分であることが分かる．ここで，$(\wp_\alpha(U_t), \preceq)$ の極大元のみからなる集合を以下のように表す．

$$\mathrm{maximal}(\wp_\alpha(U_t)) \tag{20}$$

以上より，Nα-ECC に対する α 個以下の多重誤りを訂正する復号法として以下のアルゴリズムを示すことができる．

Initialize $M = \mathrm{maximal}(\wp_\alpha(U_t))$.

1. Input the received vector z.
2. Compute $\sigma(z)^T = H_t z^T$.
3. If $\sigma(z) = 0$ then output the information vector $\phi_t^{-1}(z)$ and halt else goto 4.
4. Choose an $\{u_1, \ldots, u_\alpha\} \in M$.
5. If the solution $v_1, \ldots, v_\alpha$ of the linear system(18) for $u_1, \ldots, u_\alpha$ can be found then goto 6 else goto 7.
6. Output the information vector $\phi_t^{-1}(z - \sum_{i=1}^{\alpha} v_i u_i)$ and halt.
7. Update $M = M \setminus \{\{u_1, \ldots, u_\alpha\}\}$. If $M = \emptyset$ then output “Error is detected” and halt else goto 4.

このアルゴリズムの時間計算量の主要な因子は，step 4 → 5 → 7 → 4 というループの実行回数の上限である．このループ回数は，たかだか $|\mathrm{maximal}(\wp_\alpha(U_t))|$ である．そして，$|\mathrm{maximal}(\wp_\alpha(U_t))| \leq |\wp_\alpha(U_t)| = \binom{|U_t|}{\alpha}$ が成り立つ．

6 消失訂正

6.1 消失の定義

本稿では，NECC での，消失を次のように定義する．

消失とは，ネットワーク中のリンクで発生した誤りに対し，受信側がそれら誤りの個々の誤り値を知ることはできないが，どこのリンクで誤りが発生したのかの位置情報を知ることができる誤りのことであると定義する．

したがって，送信側から情報 $\vec{i} \in \mathbb{F}_q^k$ を送信し，消失 $\vec{e'} = (e'_1, \ldots, e'_{|E|}) \in \mathbb{F}_q^{|E|}$ が発生したとする．そして，受信側は，受信ベクトル $z = \phi(\vec{i}, \vec{e'})$ と消失 $\vec{e'}$ の位置情報

$$F(\vec{e'}) = \{i \mid e'_i \neq 0,\ 1 \leq i \leq |E|\} \tag{21}$$

を得ることができると設定する．以下では，$w(\vec{e'}) \leq 2\alpha$ が成り立つと仮定する．

各 i, $1 \leq i \leq |E|$ に対し，ベクトル $\vec{e}_i \in \mathbb{F}_2^{|E|}$ を i 番目の成分のみが 1 で，それ以外はすべて 0 である単位ベクトルとする．これらの単位ベクトルを用いると，消失 $\vec{e'}$ は，$\vec{e'} = \sum_{i=1}^{|E|} e'_i \vec{e}_i = \sum_{i \in F(\vec{e'})} e'_i \vec{e}_i$ と表すことができる．

消失 $\vec{e'}$ の位置情報 $F(\vec{e'})$ から得られるベクトルの集合

$$U_t(\vec{e'}) = \{\phi(\vec{0}, \vec{e}_i) \mid \vec{e}_i \in \mathbb{F}_2^{|E|}, w(\vec{e}_i) = 1 \text{ for } i \in F(\vec{e'})\} \tag{22}$$

を考える．さらに，$U_t(\vec{e'})$ の元によって張られる $\mathbb{F}_q$ 上の線型空間を

$$V_t(\vec{e'}) = \mathrm{spn}(U_t(\vec{e'})) \tag{23}$$

と簡略して表し，線型空間 $V_t(\vec{e'})$ の次元を

$$m'_t = \mathrm{dim} V_t(\vec{e'}) \tag{24}$$

と表す．そして，線型空間 $V_t(\vec{e'})$ の基底として，$U_t(\vec{e'})$ の中から線型独立な m'_t 個を選び，

$$u'_1, \ldots, u'_{m'_t} \in U_t(\vec{e'}) \tag{25}$$

と表す．したがって，$\phi(\vec{0}, \vec{e'}) = \phi(\vec{0}, \sum_{i \in F(\vec{e'})} e'_i \vec{e}_i)$
$= \sum_{i \in F(\vec{e'})} e'_i \phi(\vec{0}, \vec{e}_i) \in V(\vec{e'})$ より，消失 $\vec{e'}$ に対する $\phi(\vec{0}, \vec{e'})$ は，$V_t(\vec{e'})$ の基底 $u'_1, \ldots, u'_{m'_t}$ を用いて，それらの $\mathbb{F}_q$ 上の線型結合で一意に表すことができる．

$(v'_1, \ldots, v'_{m'_t}) \neq (0, \ldots, 0)$ を満たす m'_t 個の任意の $v'_1, \ldots, v'_{m'_t} \in \mathbb{F}_q$ に対し，$u'_1, \ldots, u'_{m'_t}$ は線型独立であるから，$\sum_{i=1}^{m'_t} v'_i u'_i \neq 0$ が成り立つ．$w(\vec{e'}) \leq 2\alpha$ より，$F(\vec{e'}) \subseteq F$ を満たす $|F| = 2\alpha$ である $F \subseteq E$ が存在する．したがって，$0 \neq \sum_{i=1}^{m'_t} v'_i u'_i \in V_t(\vec{e'}) \subseteq V_3$ と条件式 (6) より，$\sum_{i=1}^{m'_t} v'_i u'_i \notin V_2$ が成り立つ．これより，$(v'_1, \ldots, v'_{m'_t}) \neq (0, \ldots, 0)$ を満たす任意の $v'_1, \ldots, v'_{m'_t} \in \mathbb{F}_q$ に対し，以下が成り立つ．

$$0^T \neq H_t(\sum_{i=1}^{m'_t} v'_i u'_i)^T = \sum_{i=1}^{m'_t} v'_i H_t u_i'^T = \sum_{i=1}^{m'_t} v'_i \sigma_i^T$$

ただし，σ_i, $1 \leq i \leq m'_t$ は次のように定義される行ベクトル:

$$\sigma_i^T = H_t u_i'^T,\ 1 \leq i \leq m'_t$$

すなわち，$\sigma_1, \ldots, \sigma_{m'_t}$ が線型独立であることを示している．ゆえに，$(|\Gamma^-(t)| - k) \times m_{t'}$ 行列 $[\sigma_1^T, \ldots, \sigma_{m'_t}^T]$ のランクは，$\mathrm{rank}\ [\sigma_1^T, \ldots, \sigma_{m'_t}^T] = m'_t$ を満たす．

以上より，次のことが言える．$w(\vec{e'}) \leq 2\alpha$ を満たす消失 $\vec{e'} \in \mathbb{F}_q^{|E|}$ に対し，ベクトル $\phi(\vec{0}, \vec{e'})$ は，線型独立な m'_t 個の $u'_1, \ldots, u'_{m'_t}$ を用いて，$\phi(\vec{0}, \vec{e'}) = \sum_{i=1}^{m'_t} v'_i u'_i$ と表すことができ，そのような $v'_1, \ldots, v'_{m'_t} \in \mathbb{F}_q$ が一意に定まる．

したがって，

$$\begin{aligned} \sum_{i=1}^{m'_t} v'_i \sigma_i^T &= \sum_{i=1}^{m'_t} v'_i H_t u_i'^T = H_t(\sum_{i=1}^{m'_t} v'_i u'_i)^T = H_t \phi(\vec{0}, \vec{e'})^T \\ &= H_t \phi(\vec{i}, \vec{e'})^T = H_t z^T = \sigma(z)^T \end{aligned} \tag{26}$$

と $\mathrm{rank}\ [\sigma_1^T, \ldots, \sigma_{m'_t}^T] = m'_t$ より，受信ベクトル $z = \phi(\vec{i}, \vec{e'})$ と消失 $\vec{e'}$ の位置情報 $F(\vec{e'})$ から，式 (26) を満たす解 $v'_1, \ldots, v'_{m'_t}$ を一意に求めることができる．そして，求めた $v'_1, \ldots, v'_{m'_t}$ を用いて，

$$\begin{aligned} z - \sum_{i=1}^{m'_t} v'_i u'_i &= \phi(\vec{i}, \vec{e'}) - \sum_{i=1}^{m'_t} v'_i u'_i \\ &= \phi(\vec{i}, \vec{0}) + \phi(\vec{0}, \vec{e'}) - \sum_{i=1}^{m'_t} v'_i u'_i = \phi(\vec{i}, \vec{0}) \in V_2 \end{aligned}$$

という結果を得る．ゆえに，$\phi^{-1}(z - \sum_{i=1}^{m'_t} v'_i u'_i)$ を推定送信情報として求めることができる．

以上より，$w(\vec{e'}) \leq 2\alpha$ を満たす消失 $\vec{e'}$ に対する消失訂正アルゴリズムを，以下のように示すことができる．

6.2 アルゴリズム

1. Input the received vector z and the information $F(\vec{e'})$ of error locations for the erasure $\vec{e'}$. (See the eq. (21) for $F(\vec{e'})$.)
2. Compute $\sigma(z)^T = H_t z^T$.
3. If $F(\vec{e'}) = \emptyset$ then goto 4 else goto 5.
4. If $\sigma(z) = 0$ then output the information vector $\phi_t^{-1}(z)$ and halt else output "Error is detected" and halt.
5. Find $U_t(\vec{e'})$ from $F(\vec{e'})$. (See the eq. (22) for $U_t(\vec{e'})$.)
6. Find the dimension m'_t of the linear space $V_t(\vec{e'})$. (See the eq. (23) for $V_t(\vec{e'})$.)
7. Select a basis $u'_1, \ldots, u'_{m'_t} \in U_t(\vec{e'})$ of $V_t(\vec{e'})$.
8. Compute $\sigma_i^T = H_t u_i'^T$ for all i, $1 \leq i \leq m'_t$.
9. Find the solution $v'_1, \ldots, v'_{m'_t}$ of the linear system $\sum_{i=1}^{m'_t} v'_i \sigma_i^T = \sigma(z)^T$.
10. Compute $z - \sum_{i=1}^{m'_t} v'_i u'_i$ and output the information vector $\phi_t^{-1}(z - \sum_{i=1}^{m'_t} v'_i u'_i)$, and halt.

6.3 消失訂正の例

4.2 節の例と同じネットワークと Nα-ECC を用いる. そして, 消失が発生した場合のシンク t_2 での消失訂正の例について述べる.

まず, ソースから情報 $\vec{i} = (4) \in \mathbb{F}_5^1$ を送信し, 消失 $\vec{e'} = (0,3,2,0,\ldots,0) \in \mathbb{F}_5^{15}$ が発生したものとする. ただし, $\vec{e'}$ はリンク e_2 と e_3 においてそれぞれ誤り値 3 と 2 の誤りが発生したことを表す.

このとき, シンク t_2 では受信ベクトル $z = \phi(\vec{i}, \vec{e'}) = (1,4,1)$ を受信すると同時に, 補助情報として, 消失 $\vec{e'}$ の位置情報 $F(\vec{e'}) = \{2,3\}$ も得る.

6.2 節のアルゴリズムでは, 受信ベクトル $z = (1,4,1)$ と $F(\vec{e'}) = \{2,3\}$ を入力する (Step 1). z に対するシンドローム $\sigma(z) = (0,4)$ を計算する (Step 2). $F(\vec{e'}) \neq \emptyset$ より (Step 3), 次に, $F(\vec{e'})$ の情報から $U_t(\vec{e'}) = \{(1,1,0),(0,2,1)\}$ を求める (Step 5). $U_t(\vec{e'})$ の元で張るベクトル空間 $V_t(\vec{e'})$ の次元を求めると, $m'_t = 2$ である (Step 6). そこで, $V_t(\vec{e'})$ の基底を $(u'_1, u'_2) = ((1,1,0),(0,2,1))$ とする (Step 7). そして, u'_1, u'_2 に対するそれぞれのシンドローム $\sigma_1 = (2,1), \sigma_2 = (2,3)$ を計算する (Step 8). 2×2 行列 $[\sigma_1^T, \sigma_2^T] = \begin{bmatrix} 22 \\ 13 \end{bmatrix}$ より, $[\sigma_1^T, \sigma_2^T]^{-1} = \begin{bmatrix} 22 \\ 13 \end{bmatrix}$ を計算することで, $\sum_{i=1}^{2} v'_i \sigma_i^T = \sigma(z)^T$ を満たす $(v'_1, v'_2) = (3,2)$ が求まる (Step 9). 最後に, $z - (3u'_1 + 2u'_2) = (1,4,1) - (3,2,2) = (3,2,4)$ を計算し, 推定送信情報として $\phi_t^{-1}((3,2,4)) = (4)$ を出力する (Step 10).

7 誤り + 消失訂正 (その 1)

本節では, 誤り + 消失訂正に対する探索的な復号法について説明する.

ソースから情報 $\vec{i} \in \mathbb{F}_q^k$ を送信したとき, 誤り $\vec{e} = (e_1, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$ と消失 $\vec{e'} = (e'_1, \ldots, e'_{|E|}) \in \mathbb{F}_q^{|E|}$ が発生したとする. ただし, $2w(\vec{e}) + w(\vec{e'}) \leq 2\alpha$ を仮定する.

そして, シンク t では, 受信ベクトル $z = \phi_t(\vec{i}, \vec{e} + \vec{e'})$ と補助情報として, 消失 $\vec{e'}$ の位置情報 $F(\vec{e'})$ を得ることができると設定する. ($F(\vec{e'})$ については式 (21) を参照)

以下の記述を簡便にするために, 非負整数 γ と β を

$$\gamma = w(\vec{e'}), \tag{27}$$

$$\beta = \lfloor \frac{2\alpha - \gamma}{2} \rfloor \tag{28}$$

と定義する. このとき, $w(\vec{e}) \leq \beta$ であることに注意する.

シンク t では, 位置情報 $F(\vec{e'})$ から $U_t(\vec{e'})$ を構成することができる. ($U_t(\vec{e'})$ については式 (22) を参照) そこで, 式 (19) の $\wp_\alpha(U_t)$ に対応する集合として,

$$\wp_\beta = \{\{u_1, \ldots, u_\beta\} \cup U_t(\vec{e'}) \mid \{u_1, \ldots, u_\beta\} \subseteq U_t \setminus U_t(\vec{e'})\} \tag{29}$$

を定義する. 集合 $\wp_\beta$ の各要素は U_t の部分集合で, その部分集合の濃度は $\beta + \gamma$ である. そして, 集合 $\wp_\beta$ の濃度は $\binom{|U_t \setminus U_t(\vec{e'})|}{\beta}$ である.

集合 $\wp_\beta$ の各要素 $\{u_1, \ldots, u_{\beta+\gamma}\}$ に対し, 次の連立一次方程式 (30) を満たす解 $v_1, ..., v_{\beta+\gamma} \in \mathbb{F}_q$ が求まるかを調べる.

$$H_t \begin{bmatrix} u_1 \\ | \\ u_{\beta+\gamma} \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_{\beta+\gamma} \end{bmatrix} = \sigma(z)^T \tag{30}$$

集合 $\wp_\beta$ のある要素 $\{u_1, \ldots, u_{\beta+\gamma}\}$ に対し, $v_1, ..., v_{\beta+\gamma}$ が式 (30) を満たす解ならば, 5 節で議論, 提案した多重誤り訂正に対する手法およびアルゴリズムと同様の考え方で, 受信ベクトル z から送信情報 $\vec{i}$ を求めることができることが容易に理解できる.

8 誤り + 消失訂正 (その 2)

本節では, 前節と同様の誤り + 消失訂正について考える. ただし, 本節の目的は, シンク t にて受信した受信ベクトル $z = \phi_t(\vec{i}, \vec{e} + \vec{e'})$ と位置情報 $F(\vec{e'})$ を用いて, 誤り $\vec{e}$ と消失 $\vec{e'}$ の両方の影響を受けたシンドローム $\sigma(z)^T = H_t z^T$ から消失 $\vec{e'}$ の影響を取り除き, 誤り $\vec{e}$ のみの影響しか受けていない修正シンドロームを代数的手続きで求める方法を説明することにある. このアイデアは, [11] にて Forney が BCH 符号に対して示したアイデアの一般化になっている.

前節と同様に, 誤り $\vec{e} \in \mathbb{F}_q^{|E|}$ と消失 $\vec{e'} \in \mathbb{F}_q^{|E|}$ は, $2w(\vec{e}) + w(\vec{e'}) \leq 2\alpha$ を満たすものとする.

式 (21) と (22) において, 消失 $\vec{e'}$ に対し $F(\vec{e'})$ と $U(\vec{e'})$ を定義したことと同様に, 誤り $\vec{e}$ に対しても以下を定義する.

$$\begin{aligned} F(\vec{e}) &= \{i \mid e_i \neq 0,\ 1 \leq i \leq |E|\}, \\ U_t(\vec{e}) &= \{\phi(\vec{0}, \vec{e}_i) \mid \vec{e}_i \in \mathbb{F}_2^{|E|}, w(\vec{e}_i) = 1 \text{ for } i \in F(\vec{e})\}. \end{aligned}$$

ただし, 説明を簡単にするため便宜上, $F(\vec{e}) \cap F(\vec{e'}) = \emptyset$ であると仮定する. さらに, $U_t(\vec{e})$ と $U_t(\vec{e'})$ のそれぞれの元によって張られる $\mathbb{F}_q$ 上の線型空間を

$$\begin{aligned} V_t &= \mathrm{spn}(U_t(\vec{e})), \\ V'_t &= \mathrm{spn}(U_t(\vec{e'})) \end{aligned}$$

と簡略して表す. そして, V'_t の次元を

$$m'_t = \mathrm{dim} V'_t$$

と表し,

$$m^*_t = \mathrm{dim} V_t - \mathrm{dim} V_t \cap V'_t$$

とする. これより, $\mathrm{dim}(V_t + V'_t) = m^*_t + m'_t$ である. 線型空間 V'_t の m'_t 個の基底を $U_t(\vec{e'})$ の中から選び,

$$u'_1, \ldots, u'_{m'_t} \in U_t(\vec{e'})$$

と表す. さらに, $u'_1, \ldots, u'_{m'_t}$ を拡張し, $V_t + V'_t$ の基底を

$$u'_1, \ldots, u'_{m'_t}, u^*_1, \ldots, u^*_{m^*_t}$$

と表す. ただし, $u^*_1, \ldots, u^*_{m^*_t} \in U_t(\vec{e})$ とする.

誤り $\vec{e}$ と消失 $\vec{e'}$ に対応するそれぞれのベクトルは $\phi(\vec{0}, \vec{e}) \in V_t$, $\phi(\vec{0}, \vec{e'}) \in V'_t$ を満たすから, $\phi(\vec{0}, \vec{e} + \vec{e'}) = \phi(\vec{0}, \vec{e}) + \phi(\vec{0}, \vec{e'}) \in V_t + V'_t$. したがって, $\phi(\vec{0}, \vec{e} + \vec{e'})$ は $V_t + V'_t$ の

基底である $u'_1,\ldots,u'_{m'_t},u^*_1,\ldots,u^*_{m^*_t}$ の線型結合で一意に表すことができる. すなわち,

$$\phi(\vec{0},\vec{e}+\vec{e'})=\sum_{i=1}^{m^*_t}v^*_iu^*_i+\sum_{i=1}^{m'_t}v'_iu'_i$$

と表すことができる $v'_1,\ldots,v'_{m'_t},v^*_1,\ldots,v^*_{m^*_t}\in\mathbb{F}_q$ が一意に定まる.

次に, シンク t での V_2 の検査行列 H_t について、その i 行目の行ベクトルを $h_i\in\mathbb{F}_q^{|\Gamma^-(t)|}$, $1\le i\le|\Gamma^-(t)|-k$ と表すことにする.

各 ℓ, $1\le\ell\le|\Gamma^-(t)|-k-m'_t$ に対し, 検査行列 H_t の ℓ 行目から $\ell+m'_t$ 行目までの m'_t+1 個の行ベクトルを順に並べた $(m'_t+1)\times|\Gamma^-(t)|$ 部分行列を $H_t^{(\ell)}$ と表す. 受信ベクトル $\phi(\vec{i},\vec{e}+\vec{e'})$ と $H_t^{(\ell)}$ によるシンドローム $(\sigma_\ell,\ldots,\sigma_{\ell+m'_t})$ は次のように書ける.

$$\begin{aligned}(\sigma_\ell,\ldots,\sigma_{\ell+m'_t})^T &= H_t^{(\ell)}\phi(\vec{i},\vec{e}+\vec{e'})^T\\ &= H_t^{(\ell)}U^{*T}V^{*T}+H_t^{(\ell)}U'^TV'^T\end{aligned}\quad(31)$$

ただし, U^*, V^*, U', V' は, それぞれ以下のような $m^*_t\times|\Gamma^-(t)|$ 行列, $1\times m^*_t$ 行列, $m'_t\times|\Gamma^-(t)|$ 行列, $1\times m'_t$ 行列であるとする:

$$U^*=\begin{bmatrix}u^*_1\\|\\u^*_{m^*_t}\end{bmatrix},\qquad U'=\begin{bmatrix}u'_1\\|\\u'_{m'_t}\end{bmatrix},$$
$$V^*=[v^*_1,\ldots,v^*_{m^*_t}],\qquad V'=[v'_1,\ldots,v'_{m'_t}].$$

そして, 各 ℓ, $1\le\ell\le|\Gamma^-(t)|-k-m'_t$ に対し, 式 (31) の右辺の第 2 項に現れる $(m'_t+1)\times m'_t$ 行列 $H_t^{(\ell)}U'^T$ の転置行列 $(H_t^{(\ell)}U'^T)^T$ に関する次の連立一次方程式を考える.

$$(H_t^{(\ell)}U'^T)^T(\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})^T=0^T\quad(32)$$

転置行列 $(H_t^{(\ell)}U'^T)^T$ は $m'_t\times(m'_t+1)$ 行列であるから, $\tau_{m'_t+1}^{(\ell)}\neq0$ を満たす自明でない解 $\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)}\in\mathbb{F}_q$ を得ることができる.

各 ℓ, $1\le\ell\le|\Gamma^-(t)|-k-m'_t$ に対し, シンドローム $(\sigma_\ell,\ldots,\sigma_{\ell+m'_t})$ と $(\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})$ の内積を σ^*_ℓ と表すと, 式 (31) と (32) より, 修正シンドローム

$$\begin{aligned}\sigma^*_\ell &= (\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})(\sigma_\ell,\ldots,\sigma_{\ell+m'_t})^T\\ &= (\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})(H_t^{(\ell)}U^{*T}V^{*T}+H_t^{(\ell)}U'^TV'^T)\\ &= (\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})H_t^{(\ell)}U^{*T}V^{*T}\\ &= h^*_\ell U^{*T}V^{*T}=\sum_{i=1}^{m^*_t}v^*_ih^*_\ell u^{*T}_i\end{aligned}\quad(33)$$

を得ることができる. ただし, $h^*_\ell=(\tau_1^{(\ell)},\ldots,\tau_{m'_t+1}^{(\ell)})H_t^{(\ell)}\in\mathbb{F}_q^{|\Gamma^-(t)|}$. そして, すべての $1\le\ell\le|\Gamma^-(t)|-k-m'_t$ に対し, $\tau_{m'_t+1}^{(\ell)}\neq0$ としていることより, $h^*_1,\ldots,h^*_{|\Gamma^-(t)|-k-m'_t}$ は線型独立であることに注意する. 式 (33) より, 修正シンドローム σ^*_ℓ は, $u'_1,\ldots,u'_{m'_t}$ という消失 $\vec{e'}$ に関わる影響が取り除かれていることが分かる.

以上より, $|\Gamma^-(t)|-k$ 個のシンドローム $\sigma_1,\ldots,\sigma_{|\Gamma^-(t)|-k}$ から消失 $\vec{e'}$ の影響を取り除いた $|\Gamma^-(t)|-k-m'_t$ 個の修正シンドローム $\sigma^*_1,\ldots,\sigma^*_{|\Gamma^-(t)|-k-m'_t}$ を得ることができる.

$\dim V'_t=m'_t$ と $m^*_t+m'_t=\dim(V_t+V'_t)\le\dim V_t+\dim V'_t$ より, $m^*_t\le\dim V_t\le|U_t(\vec{e})|\le w(\vec{e})$ が成り立つ. そして, $2\alpha\le n-k\le|\Gamma^-(t)|-k$, $2w(\vec{e})+w(\vec{e'})\le2\alpha$, $m'_t\le w(\vec{e'})$ より, $2m^*_t\le2w(\vec{e})\le|\Gamma^-(t)|-k-m'_t$ が成り立つ. したがって, 式 (18) に対応する誤り $\vec{e}$ に関わる影響のみの連立一次方程式

$$\begin{bmatrix}h^*_1\\|\\h^*_{|\Gamma^-(t)|-k-m'_t}\end{bmatrix}U^{*T}V^{*T}=\begin{bmatrix}\sigma^*_1\\|\\\sigma^*_{|\Gamma^-(t)|-k-m'_t}\end{bmatrix}\quad(34)$$

を得ることができる.

消失の影響を取り除いた修正シンドロームを用いた復号の一つとして, 例えば, 探索的な復号法となる次の方法が考えられる. 式 (28) の定義より, $m^*_t\le w(\vec{e})\le\beta$ が成り立つ. また, $2\beta\le2\alpha-w(\vec{e'})\le|\Gamma^-(t)|-k-m'_t$ も成り立つ. これより, 連立一次方程式 (34) における m^*_t 個の $u^*_1,\ldots,u^*_{m^*_t}$ と $v^*_1,\ldots,v^*_{m^*_t}$ をそれぞれ β 個の $u_1,\ldots,u_\beta\in U_t\setminus U_t(\vec{e'})$ と $v_1,\ldots,v_\beta\in\mathbb{F}_q$ に拡張することで, 5 節と 7 節にて提案した探索的な方法による多重誤り訂正の復号法も利用することができることが分かる.

9 結論

Nα-ECC に対する検査行列とシンドロームを定義し, それらを利用した幾つかの探索的な復号法を示した. そして, 粗い計算量評価も行なった. 今後の課題として, 復号法およびその計算量評価のさらなる精査が必要である. また, 代数的な復号法を適用できるようなある種の構造をもたせた符号化の研究が必要である.

参考文献

[1] N. Cai and R.W. Yeung, "Network coding and error correction," Proc. ITW'02, 2002.

[2] R.W. Yeung and N. Cai, "Network error correction, Part I: Basic concept and upper bounds," Communications in Information and Systems, vol.6, no.1, pp.19-36, 2006.

[3] N. Cai and R.W. Yeung, "Network error correction, Part II: Lower bounds," Communications in Information and Systems, vol.6, no.1, pp.37-54, 2006.

[4] Z. Zhang, "Network error correction coding in packetized networks," Proc. ITW'06, Chengdu, China, pp.433-437, Oct. 2006.

[5] Z. Zhang, "Linear network error correction coding in packetized networks," IEEE Trans., on IT, Vol.54, No.1, pp.209-218, Jan. 2008.

[6] S. Yang and R.W. Yeung, "Characterizations of network error correction/detection and erasure correction," Proc. NetCod 2007, UCSD, San Diego, California, USA, Jan. 2007.

[7] S. Yang, C.K. Ngai, and R.W. Yeung, "Construction of linear network codes that achieve a refined Singleton bound," Proc. ISIT 2007, pp.1576-1580, Mice, France, June 2007.

[8] R. Matsumoto, "Construction Algorithm for Network Error-Correcting Codes Attaining the Singleton Bound," IEICE Trans., Fundamentals, Vol.E90-A, No.9, pp.1729-1735, Setp. 2007.

[9] H.Bahramgiri and F.Lahouti, "Block network error control codes and syndrome-based maximum likelihood decoding," Proc. ISIT 2008, pp.807-811, Toronto, Canada, July 6-11, 2008.

[10] R. Koetter and M. Medard, "An algebraic approach to network coding," IEEE/ACM Trans. Networking, vol.11, no.5, pp.782-795, Oct. 2003.

[11] G.D.Forney, "On decoding BCH codes," IEEE Trans. on IT, vol.IT-11, no.4, pp.549-557, Oct. 1965.