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

栗原正純

電気通信大学

(UEC Tokyo)

SITA2008 **鬼怒川** 2008 **年** 10 **月** 8 **日**

kuri@ice.uec.ac.jp (2008/10/8/14:18)

目次

ネットワークコーディングにおける誤り訂正符号で扱う雑音の種類

1. 誤り
2. 消失
3. 誤り + 消失

本日の発表では、誤りのみを扱う。

$$H_t \begin{bmatrix} \vec{u}_1 \\ | \\ \vec{u}_\alpha \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_\alpha \end{bmatrix} = \sigma(\vec{z})^T \qquad \cdots\cdots \qquad (A)$$

符号の構成と復号

(しらみつぶし法, 列挙法 (exhausitive serach, enumeration method))

1. N. Cai and R.W. Yeung,
   "Network coding and error correction" (2002)
   "Network error correction, Part I, II" (2006)
2. Z. Zhang,
   "Network error correction coding in packetized networks"(2006)
   ("Linear network error correction coding in packetized networks"(2008))
3. S. Yang and R.W. Yeung,
   "Characterizations of network error correction/detection and erasure correction" (2007)
   "Construction of linear network codes that achieve a refined Singleton bound" (2007) with C.K. Ngai
4. R. Matsumoto, (Network α-Error-Correcting Codes)
   "Construction algorithm for network error-correcting codes attaining the Singleton bound" (2007)

符号の構成と復号

(パリティ検査行列 + しらみつぶし法, 列挙法)

時間計算量の評価において、 q^k の項が現れない。

1. H.Bahramgiri and F.Lahouti,
   "Block network error control codes and syndrome-based maximum likelihood decoding" (2008)
2. **本発表 (復号についてのみ)**
   " 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"

対象とする符号は、松本 (2007) **の構成法による**
Network α-Error-Correcting Codes (Nα-ECC)

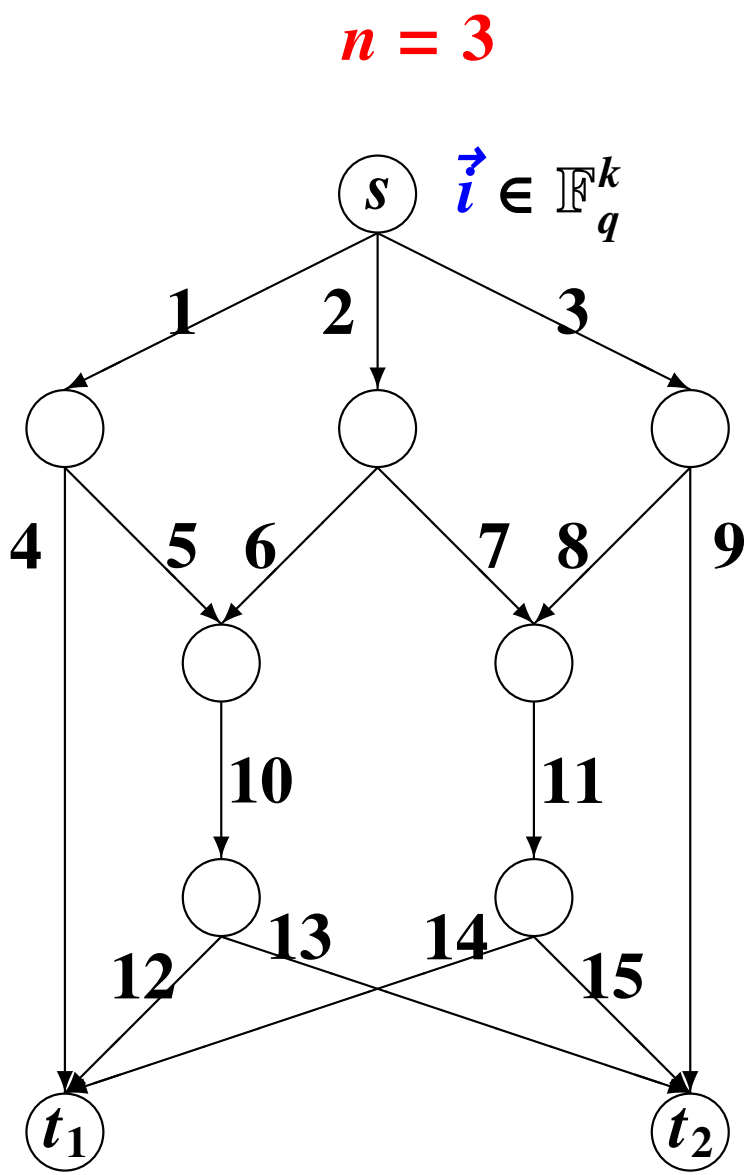
(本発表の研究は, 上記の H.Bahramgiri and F.Lahouti(2008) **とは独立に行なわれた研究)**

ネットワーク G と マルチキャスト

1. ネットワーク $G = (V, E)$
2. ソース $s \in V$
3. シンク t と シンクの集合 T
4. ソース s から 各シンク $t \in T$ への最大流の**最小値** n
5. ソース s から シンク $t \in T$ へのマルチキャスト
   ソースから **情報** $\vec{i} \in \mathbb{F}_q^k$ を送信する

$$n \geq k$$

6. 右図のネットワークでは、リンクの本数 $|E| = 15$.

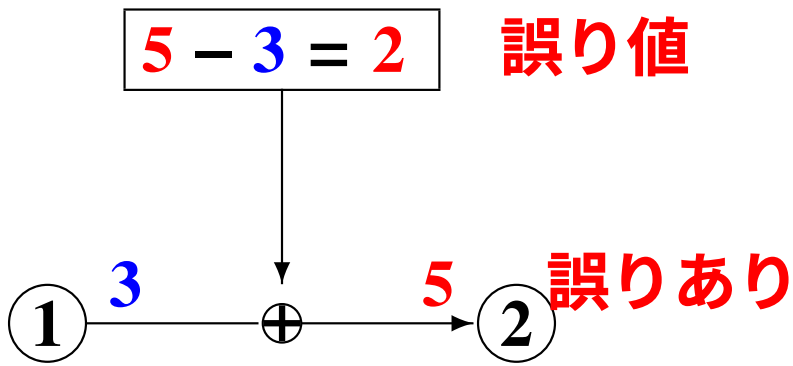


誤りと加法的離散通信路 (リンク $e \in E$)

- ネットワーク $G = (V, E)$ 上で発生する **誤り**

$$\vec{e} = (e_1, e_2, \ldots, e_i, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$$

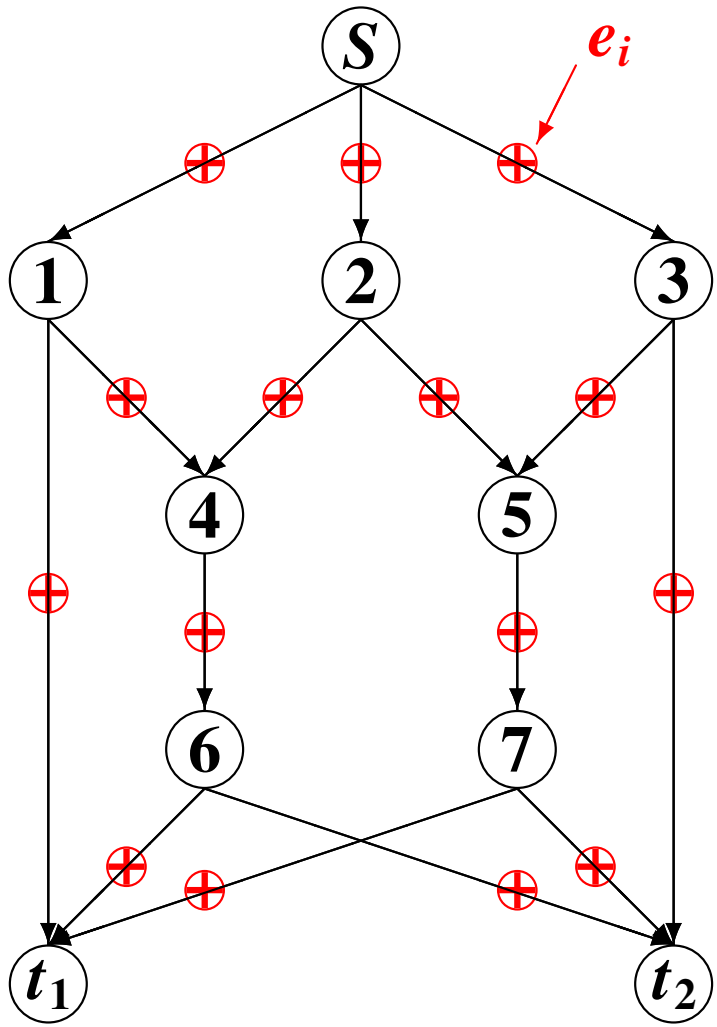
- i 番目のリンク上で発生した**誤り値** e_i



- 誤り $\vec{e}$ のハミング重み $w(\vec{e})$ が誤りの個数.

誤り $\vec{e}$

$$\vec{e}=(e_1,\ldots,e_i,\ldots,e_{|E|})\in \mathbb{F}_q^{|E|}$$



Network α-Error-Correcting Codes

- Network α-Error-Correcting Code とは,
  ネットワーク G の中で発生した誤り $\vec{e} \in \mathbb{F}_q^{|E|}$ が

$$w(\vec{e}) \leq \alpha$$

を満たすならば, シンク t での受信ベクトル $\vec{z} \in \mathbb{F}_q^n$ から送信情報 $\vec{i} \in \mathbb{F}_q^k$ を正しく復号できる線型なネットワークコーディングのこと. ただし,

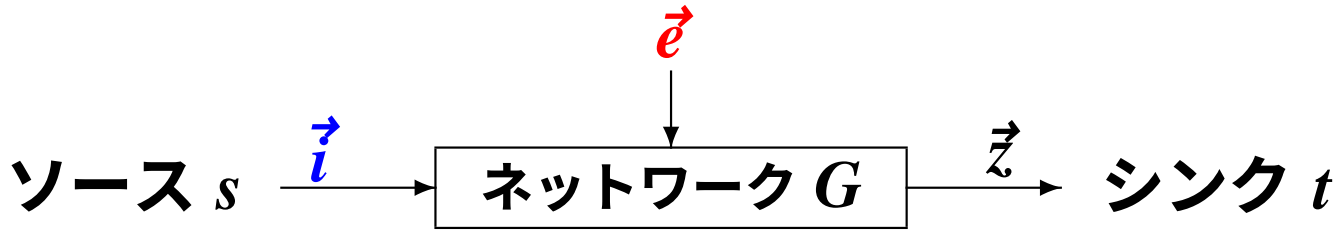
$$n - k \geq 2\alpha$$

が成り立つとする.

一般に、受信ベクトル $\vec{z}$ の長さは, $|\Gamma^-(t)| (\geq n)$ として扱えるが、ここでは、簡単のために、長さ n とする。

Network α-Error-Correcting Code [松本 (2007)]

- 通信モデル (情報 $\vec{i}$, 誤り $\vec{e}$, 受信ベクトル $\vec{z}$)



- $\mathbb{F}_q^k \times \mathbb{F}_q^{|E|}$ から $\mathbb{F}_q^n$ への写像 ϕ_t

$$\phi_t \quad : \quad \mathbb{F}_q^k \times \mathbb{F}_q^{|E|} \longrightarrow \mathbb{F}_q^n$$
$$(\vec{i}, \vec{e}) \longmapsto \vec{z} = \phi_t(\vec{i}, \vec{e})$$

Network α-Error-Correcting Code [松本 (2007)]

- **受信ベクトルのつくる 3 つの空間**

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

ただし、$\vec{e}$ は $w(\vec{e}) \leq 2\alpha$ を満たす。

- Network α-Error-Correcting Code **の条件**

次の条件を満たすように写像 ϕ_t を構成できれば、それが Network α-Error-Correcting Code **になる。**

1. $V_1 = V_2 + V_3$,
2. $\dim V_2 = k$,
3. $\dim V_2 \cap V_3 = 0$.

写像 ϕ_t

- 任意の $\vec{i}_1, \vec{i}_2 \in \mathbb{F}_q^k$, $\vec{e}_1, \vec{e}_2 \in \mathbb{F}_q^{|E|}$, $a_1, a_2, b_1, b_2 \in \mathbb{F}_q$ に対し,

$$\phi_t(a_1\vec{i}_1 + a_2\vec{i}_2,\ b_1\vec{e}_1 + b_2\vec{e}_2) = a_1\phi_t(\vec{i}_1, \vec{0}) + a_2\phi_t(\vec{i}_2, \vec{0}) + b_1\phi_t(\vec{0}, \vec{e}_1) + b_2\phi_t(\vec{0}, \vec{e}_2)$$

が成り立つ.

- 例えば、写像 ϕ_t は, $(k + |E|) \times n$ 伝送行列 B_t を用いて,

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

と表すことができる.

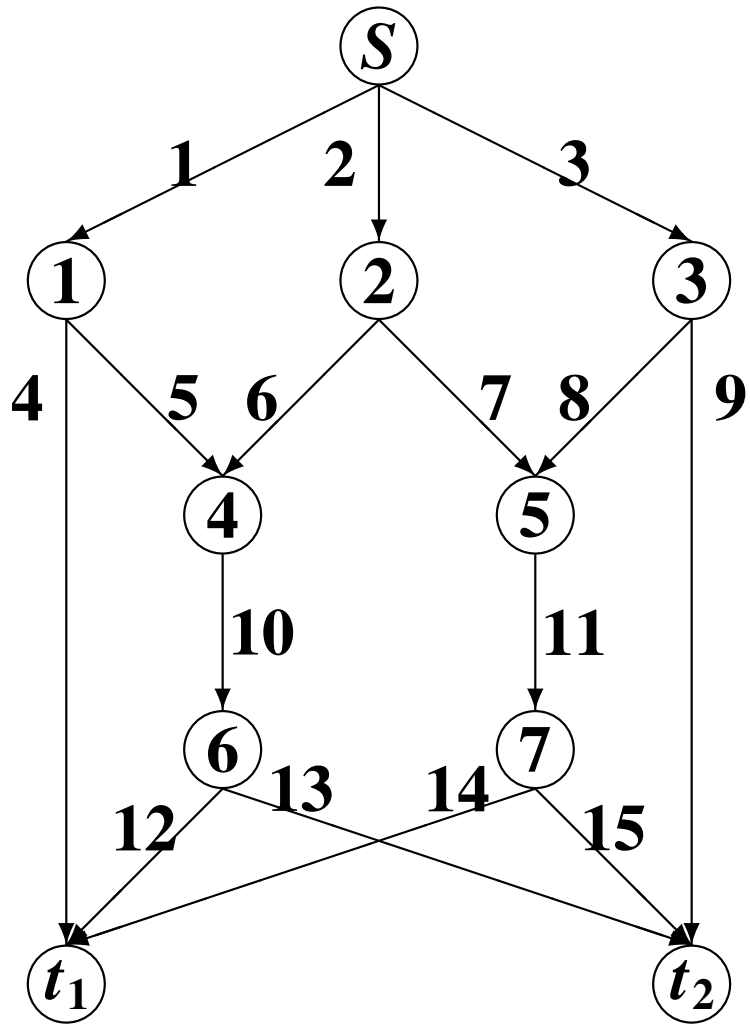
- 誤りのない受信ベクトル $\vec{z} = \phi_t(\vec{i}, \vec{0}) \in V_2$ に対応する送信情報は, B_t の逆行列のようなもの B_t^{-1} を用いて,

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

のように計算可能である.

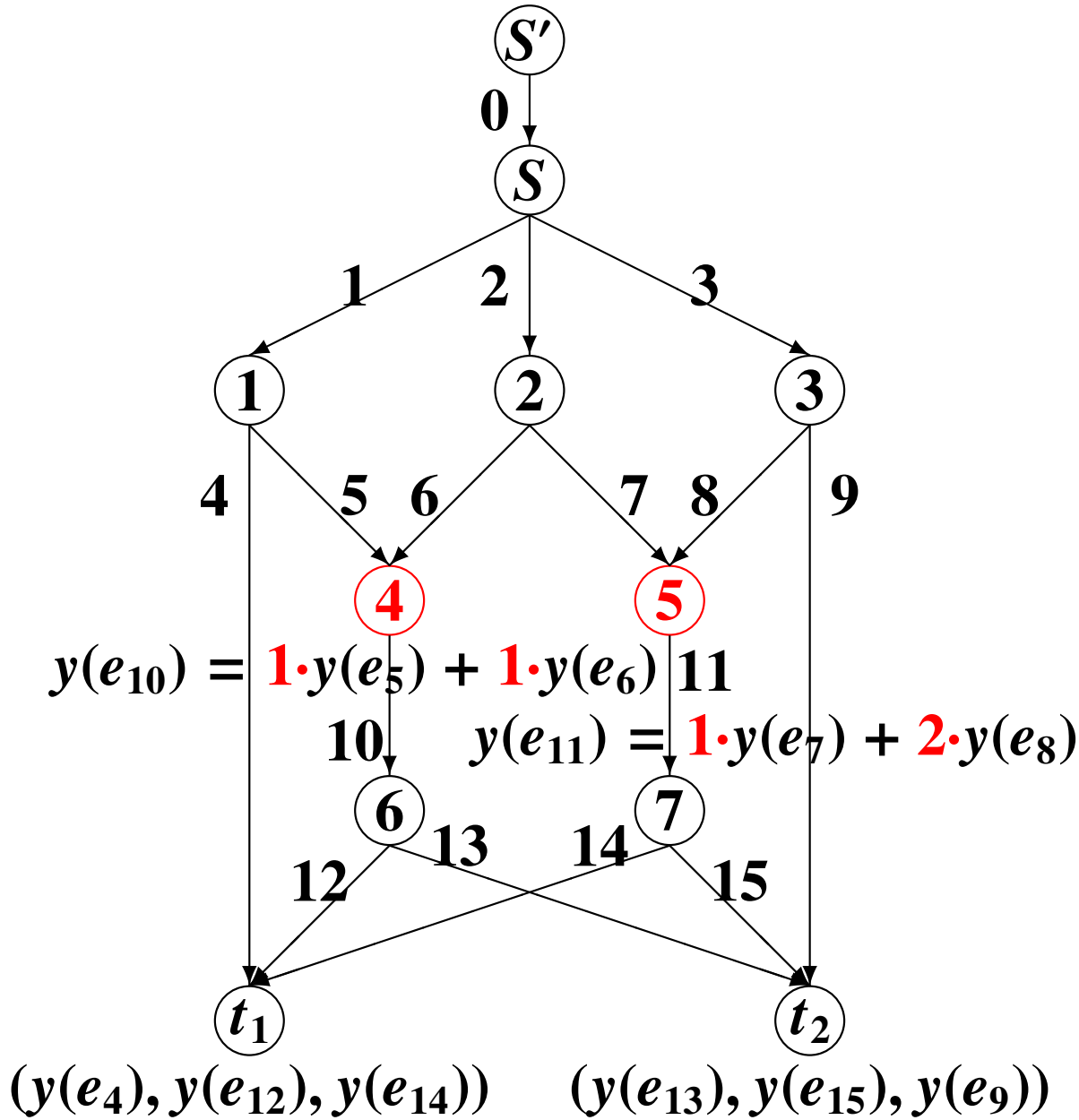
ネットワーク $G = (V, E)$

最大流 $n = 3$, $|E| = 15$



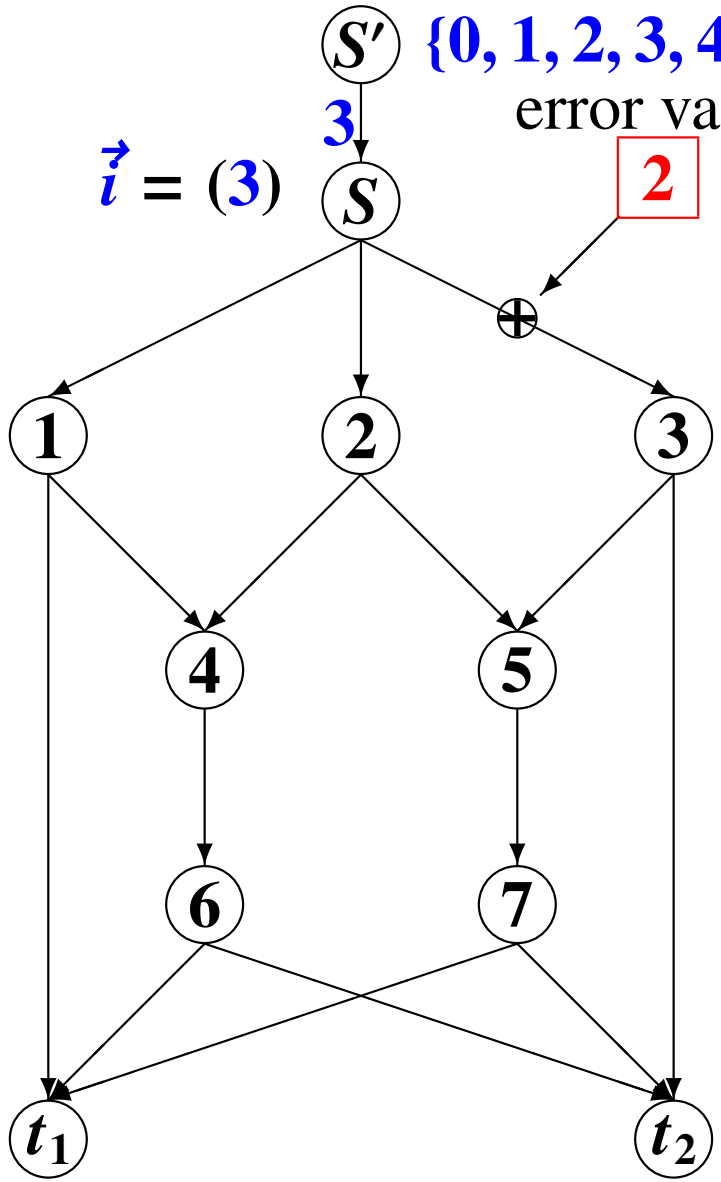
Network α-Error-Correcting Code

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



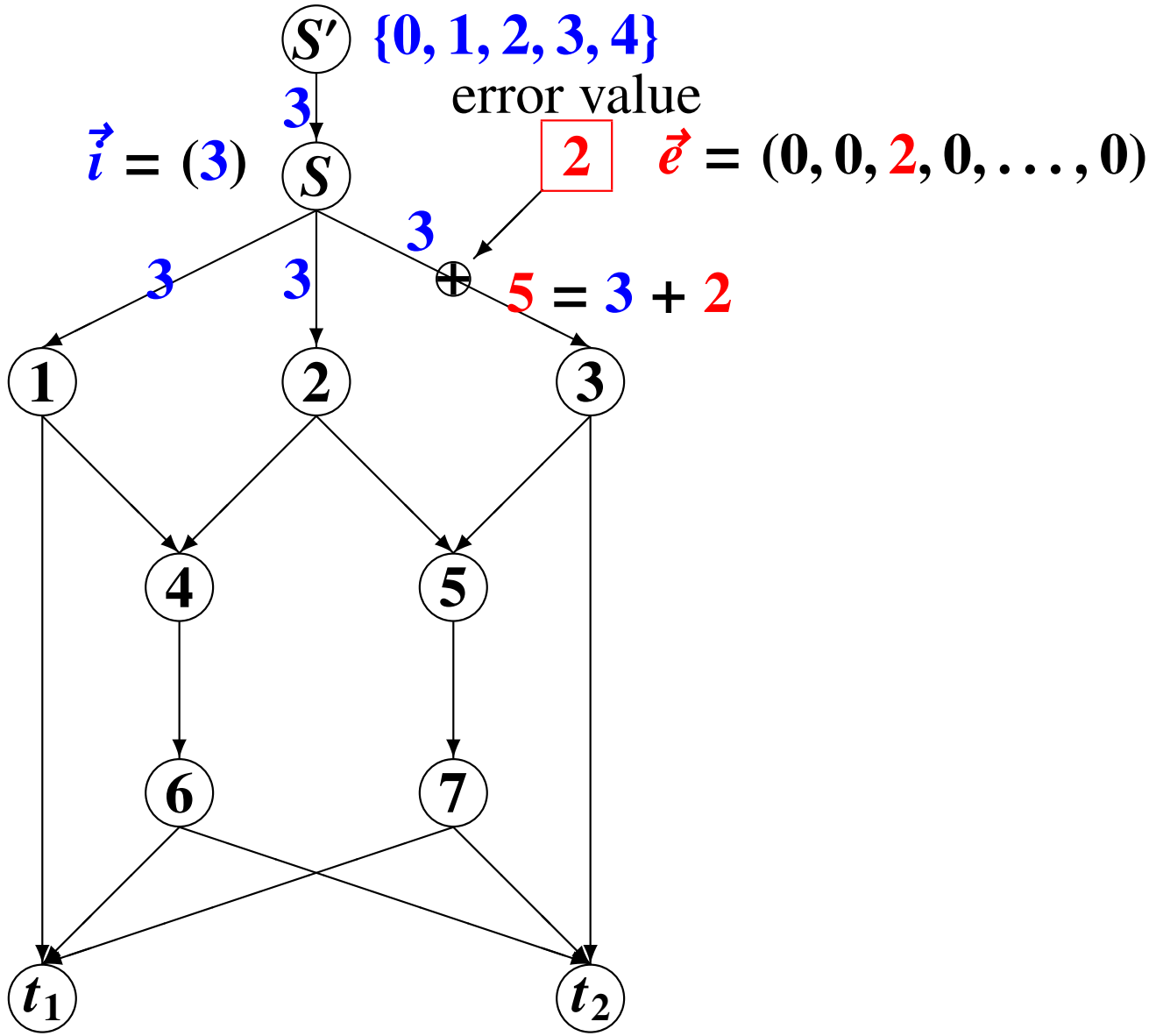
受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



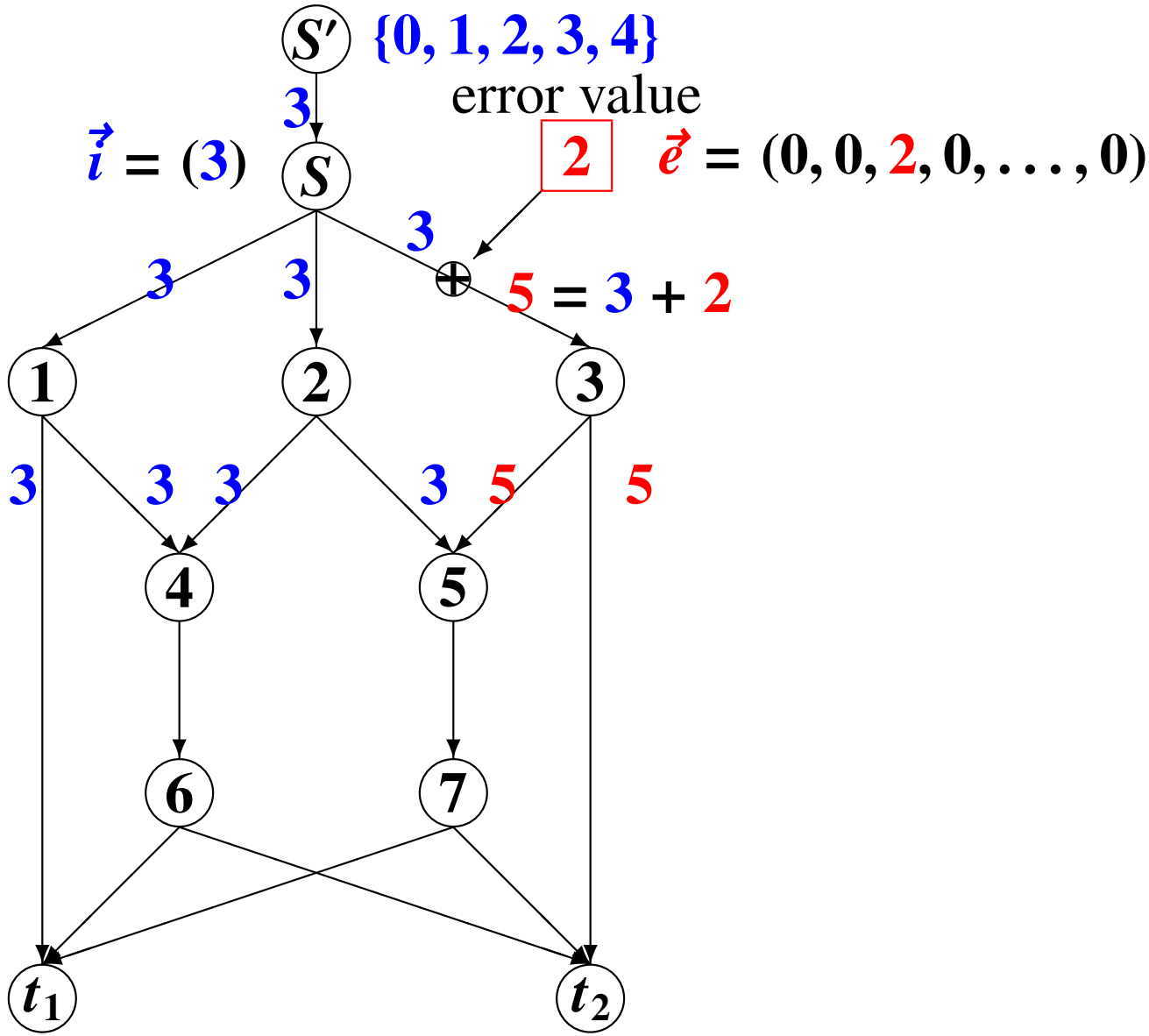
受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



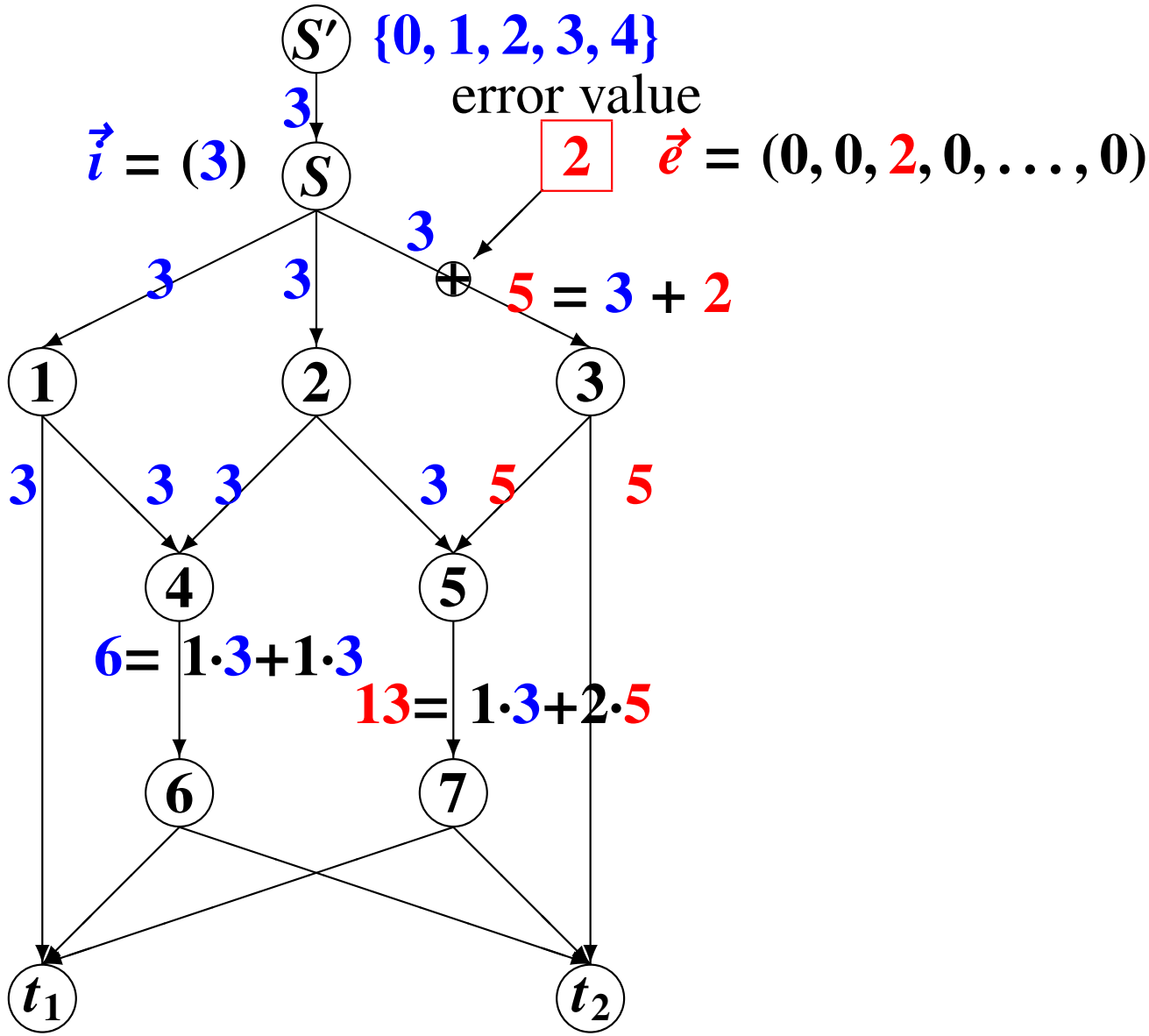
受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



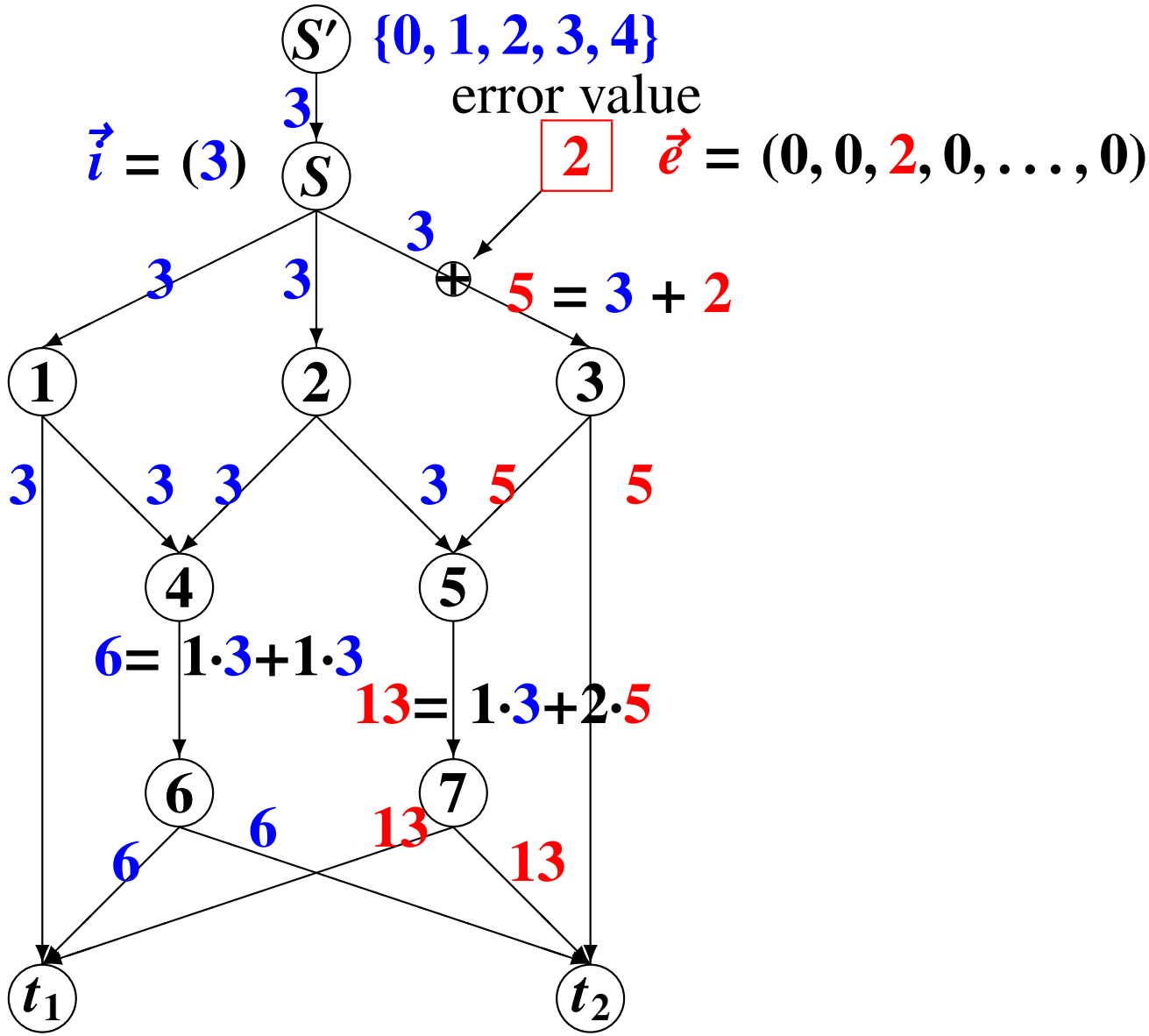
受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



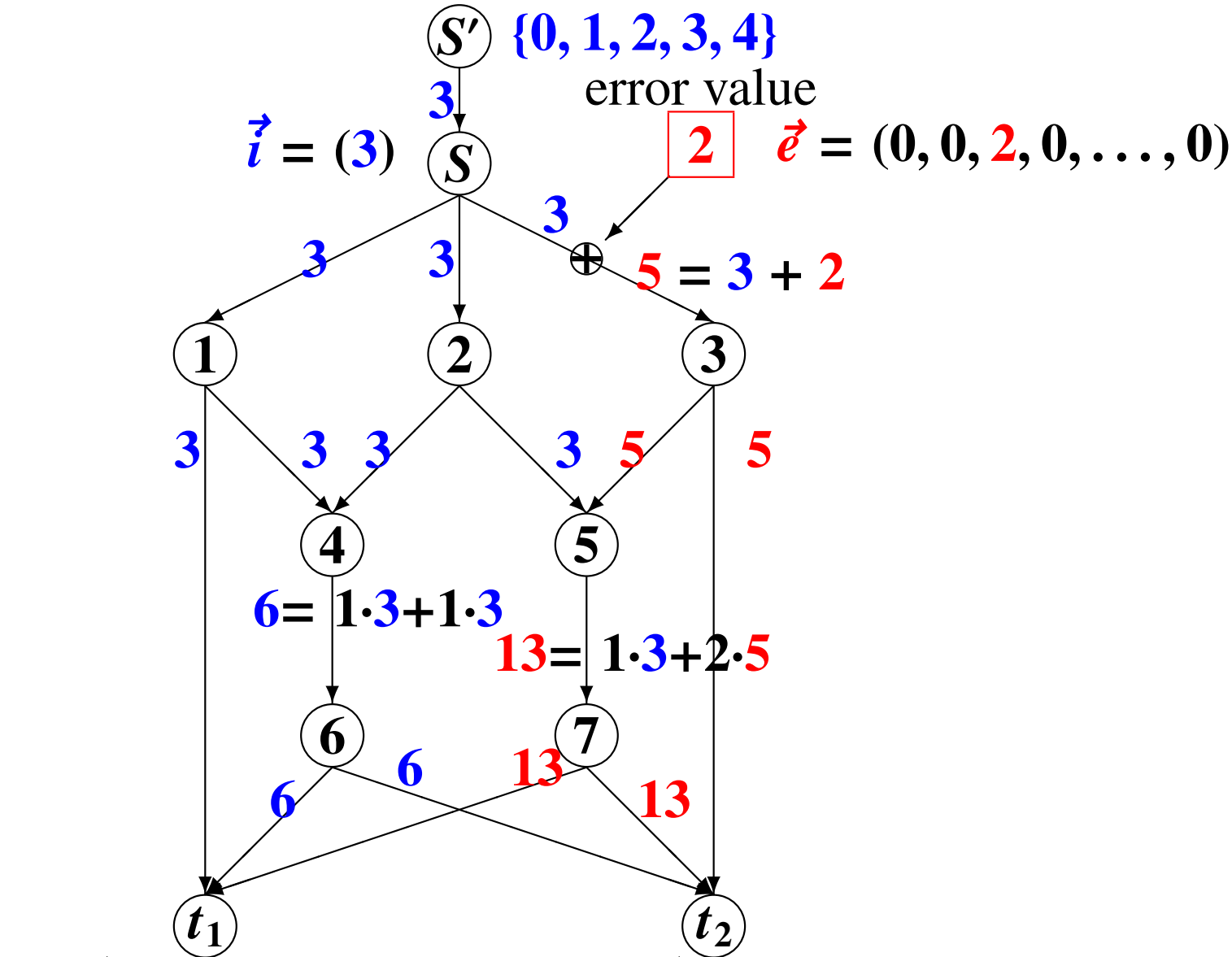
受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



受信ベクトル $\phi_t(\vec{i}, \vec{e})$

$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



$\phi_{t_1}(\vec{i}, \vec{e}) = (3, 6, 13)$ $\phi_{t_2}(\vec{i}, \vec{e}) = (6, 13, 5)$

検査行列とシンドローム

1. 空間 $V_2 = \{\phi_t(\vec{i}, \vec{0}) \mid \vec{i} \in \mathbb{F}_q^k\}$ の直交補空間 $V_2^{\perp}$
2. $\dim V_2^{\perp} = n - k$ が成り立つ.
3. 空間 V_2 の検査行列 H_t

空間 $V_2^{\perp}$ を張る $n - k$ 個の基底ベクトルより、
$(n - k) \times n$ 行列 H_t を構成する。

任意の $\vec{z} \in \mathbb{F}_q^n$ に対し、

$$H_t \vec{z}^T = \vec{0}^T \quad \text{(if } \vec{z} \in V_2\text{)},$$
$$H_t \vec{z}^T \neq \vec{0}^T \quad \text{(otherwise).}$$

検査行列とシンドローム

1. 任意の $\vec{i} \in \mathbb{F}_q^k$ と $\vec{e} \in \mathbb{F}_q^{|E|}$ に対し,

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

が成り立つ.

2. シンドローム $\sigma(\vec{z}) = (\sigma_1(\vec{z}), \ldots, \sigma_{n-k}(\vec{z}))$

任意の $\vec{z} \in \mathbb{F}_q^n$ に対し, シンドローム $\sigma(\vec{z}) \in \mathbb{F}_q^{n-k}$ を

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

と定義する。

誤りによる空間 V_3 の部分集合 U_t

1. 空間 $V_3 = \{\phi_t(\vec{0}, \vec{e}) \mid \vec{e} \in \mathbb{F}_q^{|E|}\}$ の部分集合：

$$U_t = \{\phi_t(\vec{0}, \vec{e}_i) \mid \vec{e}_i \in \mathbb{F}_2^{|E|},\ w(\vec{e}_i) = 1\} \setminus \{\vec{0}\} \subseteq V_3$$

2. 誤り $\vec{e} = (e_1, \ldots, e_i, \ldots, e_{|E|})$ に対する、シンク t での受信ベクトル $\phi_t(\vec{0}, \vec{e}) \in V_3$ の表現

$$V_3 \ni \phi_t(\vec{0}, \vec{e}) = \sum_{i=1}^{|E|} e_i \phi_t(\vec{0}, \vec{e}_i) = \sum_i v_i \vec{u}_i$$

ただし、

$$\phi_t(\vec{0}, \vec{e}_i),\ \vec{u}_i \in U_t,$$
$$\vec{e}_i = (0, \ldots, 0, 1_i, 0, \ldots, 0) \in \mathbb{F}_2^{|E|},$$
$$v_i \in \mathbb{F}_q \text{ for all } i.$$

α 個以下の誤り訂正 (位置 と 値)

1. 受信ベクトル $\vec{z} = \phi_t(\vec{i}, \vec{e})$ に対し、連立一次方程式

$$H_t \begin{bmatrix} \vec{u}_1 \\ | \\ \vec{u}_\alpha \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_\alpha \end{bmatrix} = \sigma(\vec{z})^T \qquad \cdots\cdots \qquad (A)$$

を満たすような

$$\vec{u}_1, \ldots, \vec{u}_\alpha \in U_t \quad \text{と} \quad v_1, \ldots, v_\alpha \in \mathbb{F}_q$$

(位置) (値)

の組を求める。

2. $w(\vec{e}) \leq \alpha$ ならば、式 (A) を満たす
$\vec{u}_1, \ldots, \vec{u}_\alpha \in U_t$ と $v_1, \ldots, v_\alpha \in \mathbb{F}_q$
の組が存在する。

α 個以下の誤り訂正 (位置 と 値)

1. ある $\vec{u}_1, \ldots, \vec{u}_\alpha \in U_t$ と $v_1, \ldots, v_\alpha \in \mathbb{F}_q$ の組が式 (A) を満たすならば、

$$\vec{z} - \sum_{i=1}^{\alpha} v_i \vec{u}_i \in V_2$$

が成り立つ.

2. したがって、送信情報 $\phi_t^{-1}(\vec{z} - \sum_{i=1}^{\alpha} v_i \vec{u}_i)$ が求まる.
3. 式 (A) を満たす異なる 2 つの組 :

$$\vec{u}_1, \ldots, \vec{u}_\alpha \in U_t, \qquad v_1, \ldots, v_\alpha \in \mathbb{F}_q$$
$$\vec{u}'_1, \ldots, \vec{u}'_\alpha \in U_t, \qquad v'_1, \ldots, v'_\alpha \in \mathbb{F}_q$$

に対し、

$$\sum_{i=1}^{\alpha} v_i \vec{u}_i = \sum_{i=1}^{\alpha} v'_i \vec{u}'_i$$

が成り立つ.

$\vec{u}_1, \ldots, \vec{u}_\alpha$ の選定

- 集合 U_t から α 個の要素数を取り出した部分集合 $\{\vec{u}_1, \ldots, \vec{u}_\alpha\}$ の全体からなる集合：

$$\wp_\alpha(U_t) = \{\{\vec{u}_1, \ldots, \vec{u}_\alpha\} \mid \{\vec{u}_1, \ldots, \vec{u}_\alpha\} \subseteq U_t\}$$

- 濃度は, $|\wp_\alpha(U_t)| = \binom{|U_t|}{\alpha} \leq \binom{|E|}{\alpha}$ である.
- 順序集合 $(\wp_\alpha(U_t), \preceq)$

$\{\vec{u}_1, \ldots, \vec{u}_\alpha\}$ と $\{\vec{u}'_1, \ldots, \vec{u}'_\alpha\} \in \wp_\alpha(U_t)$ に対応し、

$$\begin{array}{c} \{\vec{u}_1, \ldots, \vec{u}_\alpha\} \preceq \{\vec{u}'_1, \ldots, \vec{u}'_\alpha\} \\ \Updownarrow \\ \mathrm{spn}(\{\vec{u}_1, \ldots, \vec{u}_\alpha\}) \subseteq \mathrm{spn}(\{\vec{u}'_1, \ldots, \vec{u}'_\alpha\}) \end{array}$$

$\vec{u}_1, \ldots, \vec{u}_\alpha$ の選定

- 1. $\{\vec{u}_1, \ldots, \vec{u}_\alpha\} \preceq \{\vec{u}'_1, \ldots, \vec{u}'_\alpha\}$

  かつ

  2. $\{\vec{u}_1, \ldots, \vec{u}_\alpha\}$ に対し、式 (A) を満たす $v_1, ..., v_\alpha$ が存在する

  ならば、$\{\vec{u}'_1, \ldots, \vec{u}'_\alpha\}$ にも 式 (A) を満たす $v'_1, ..., v'_\alpha$ が存在する.

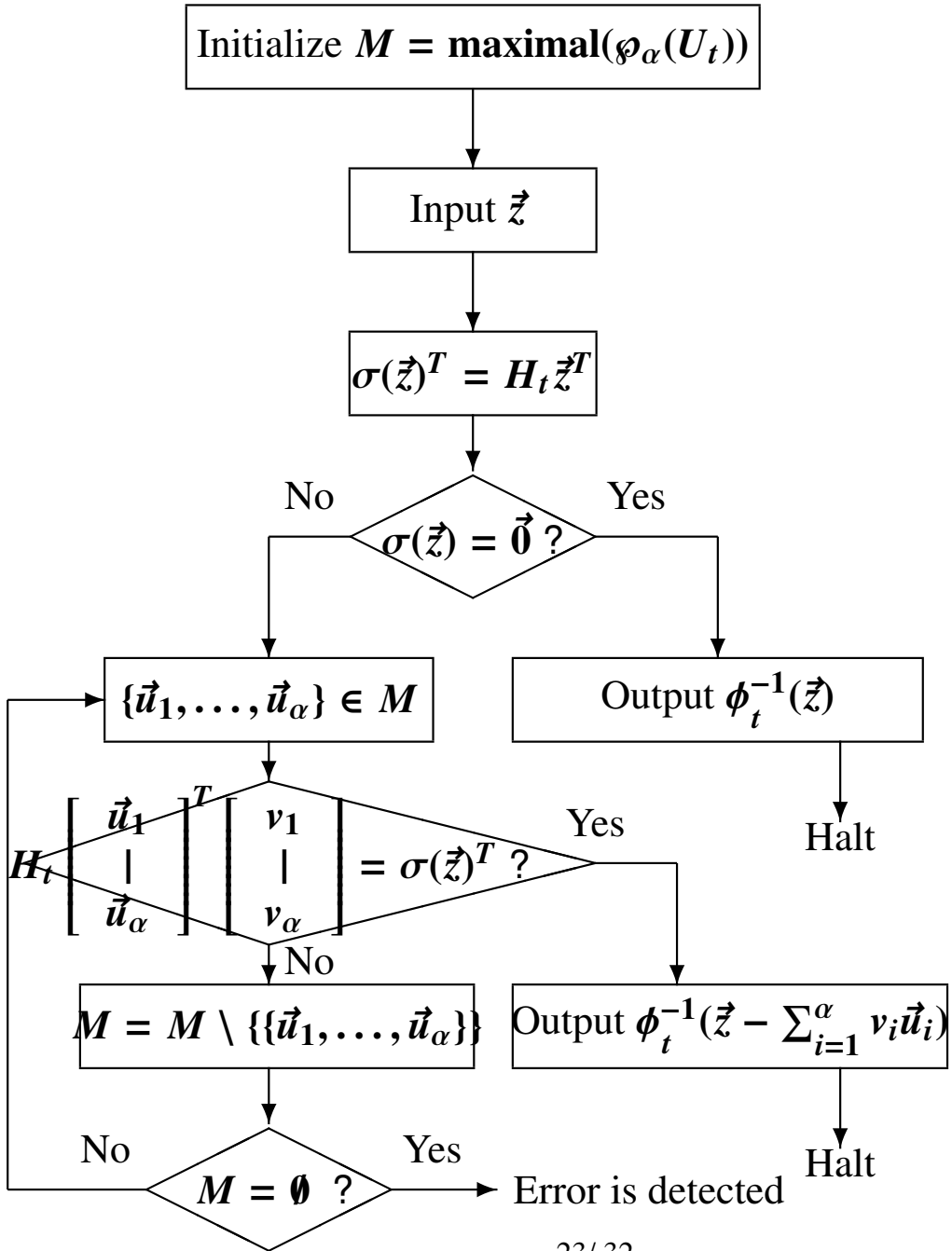
$$H_t \begin{bmatrix} \vec{u}_1 \\ | \\ \vec{u}_\alpha \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_\alpha \end{bmatrix} = \sigma(\vec{z})^T \qquad \cdots\cdots \qquad (A)$$

- 順序集合 $(\wp_\alpha(U_t), \preceq)$ の **極大元** のみからなる集合を

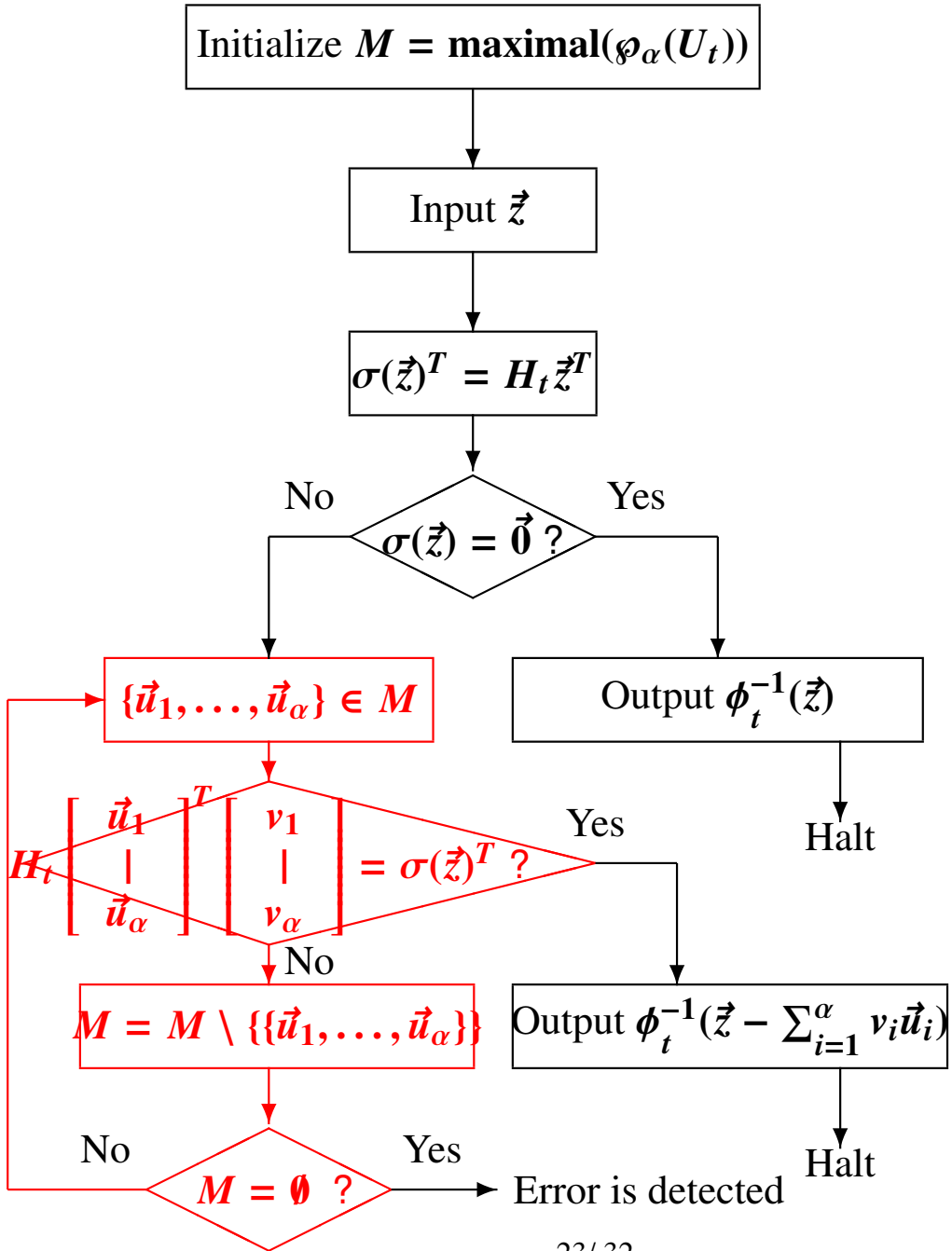
$$\mathbf{maximal}(\wp_\alpha(U_t))$$

と表す.

復号アルゴリズム (Flowchart)



復号アルゴリズム (Flowchart)



結論

1. 式 (A) を満たす $|\mathrm{maximal}(\wp_\alpha(U_t))|$ の要素 $\{\vec{u}_1, \ldots, \vec{u}_\alpha\}$ を求めることで復号するアルゴリズムを示した.

$$H_t \begin{bmatrix} \vec{u}_1 \\ | \\ \vec{u}_\alpha \end{bmatrix}^T \begin{bmatrix} v_1 \\ | \\ v_\alpha \end{bmatrix} = \sigma(\vec{z})^T \qquad \cdots\cdots \qquad (A)$$

2. 復号アルゴリズムの時間計算量の主要な因子は、ループの回数の上限 $|\mathrm{maximal}(\wp_\alpha(U_t))|$:

$$|\mathrm{maximal}(\wp_\alpha(U_t))| \leq |\wp_\alpha(U_t)| = \binom{|U_t|}{\alpha} \leq \binom{|E|}{\alpha}$$

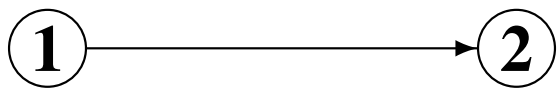
3. 今後の課題として、基本方程式 (A) を満たす解を、効率よく求めることが可能な (代数的な) 構造を入れた符号化と復号の導出が必要である。

誤りと加法的離散通信路 (リンク $e \in E$)

- ネットワーク $G = (V, E)$ 上で発生する **誤り**

$$\vec{e} = (e_1, e_2, \ldots, e_i, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$$

- i 番目のリンク上で発生した**誤り値** e_i



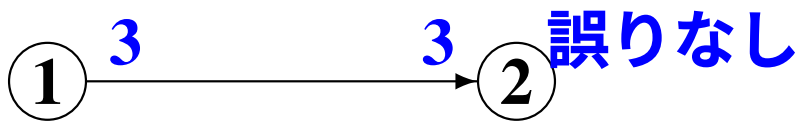
- 誤り $\vec{e}$ のハミング重み $w(\vec{e})$ が誤りの個数.

誤りと加法的離散通信路 (リンク $e \in E$)

- ネットワーク $G = (V, E)$ 上で発生する 誤り

$$\vec{e} = (e_1, e_2, \ldots, e_i, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$$

- i 番目のリンク上で発生した誤り値 e_i



- 誤り $\vec{e}$ のハミング重み $w(\vec{e})$ が誤りの個数.

誤りと加法的離散通信路 (リンク $e \in E$)

- ネットワーク $G = (V, E)$ 上で発生する 誤り

$$\vec{e} = (e_1, e_2, \ldots, e_i, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$$

- i 番目のリンク上で発生した誤り値 e_i

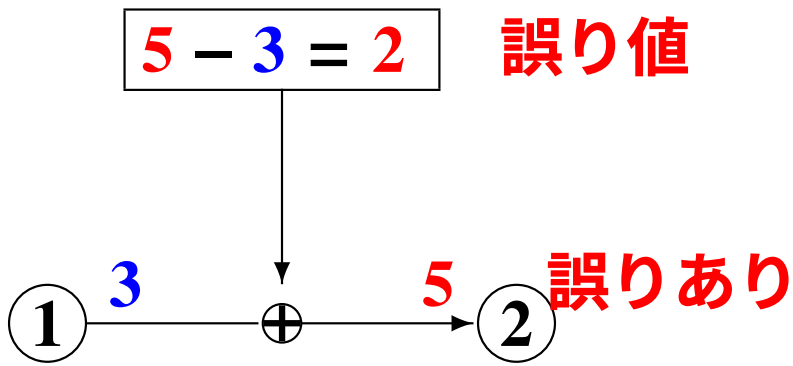
- 誤り $\vec{e}$ のハミング重み $w(\vec{e})$ が誤りの個数.

誤りと加法的離散通信路 (リンク $e \in E$)

- ネットワーク $G = (V, E)$ 上で発生する **誤り**

$$\vec{e} = (e_1, e_2, \ldots, e_i, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$$

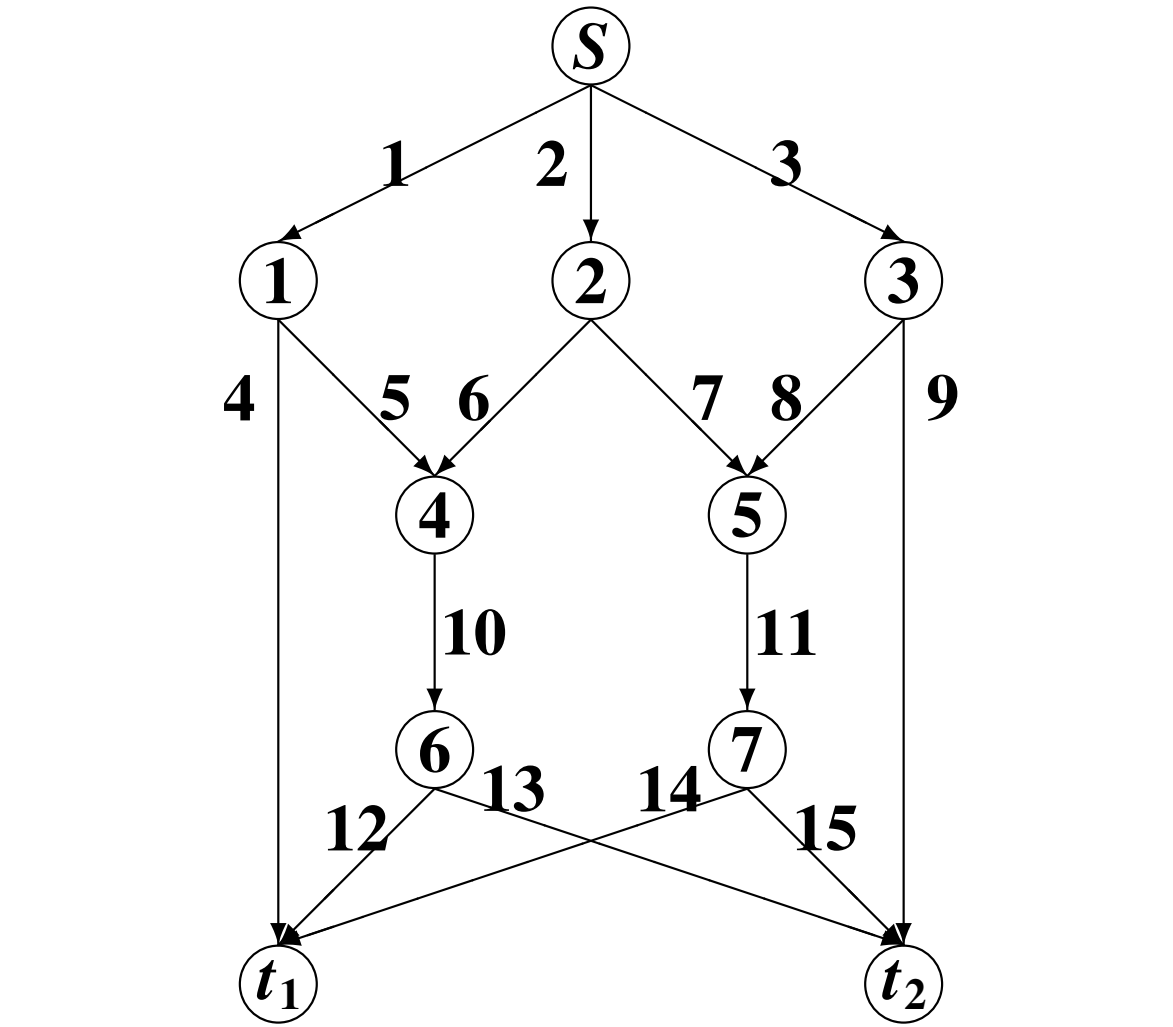
- i 番目のリンク上で発生した**誤り値** e_i



- 誤り $\vec{e}$ のハミング重み $w(\vec{e})$ が誤りの個数.

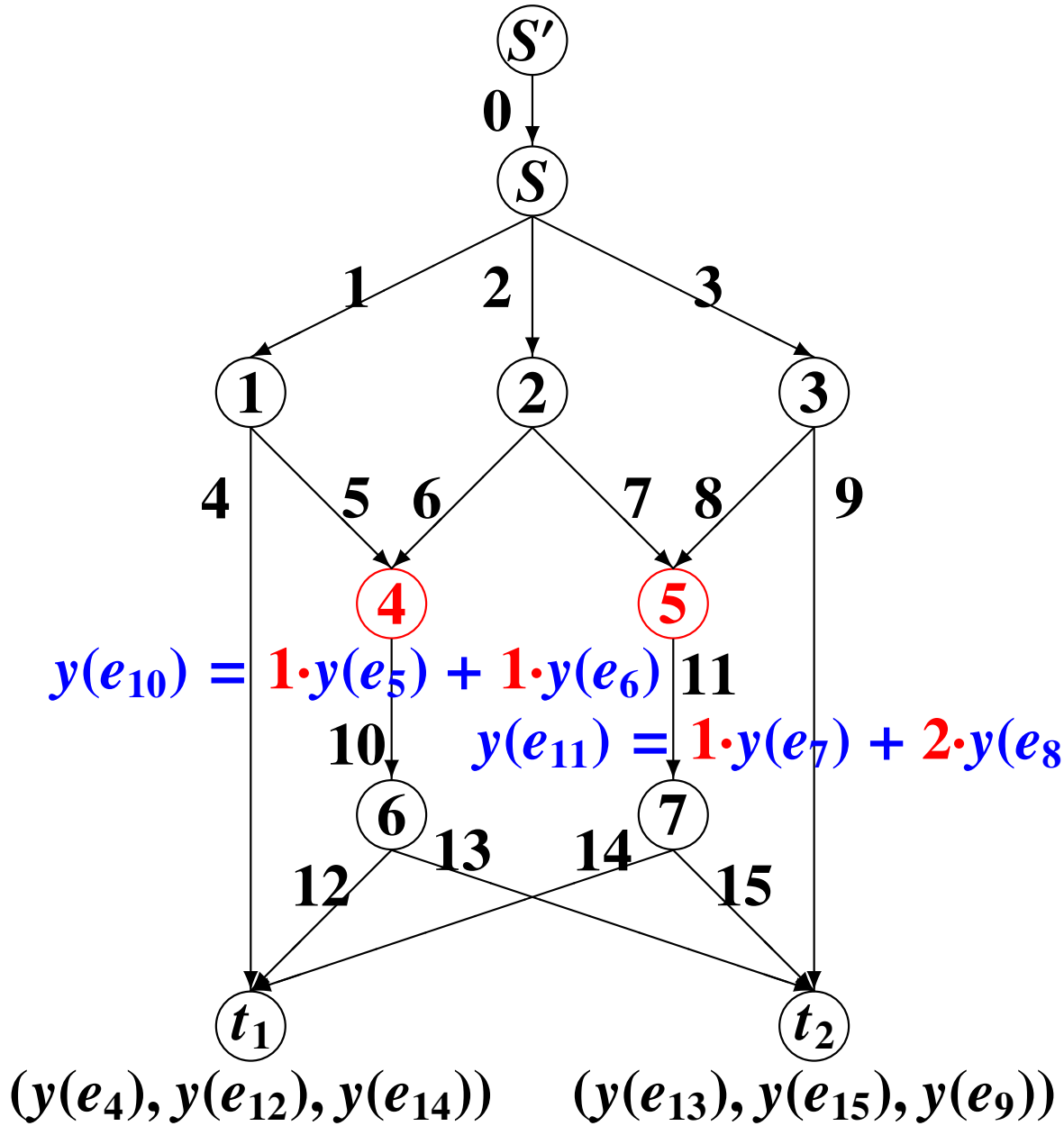
ネットワーク $G = (V, E)$

最大流 $n = 3$, $|E| = 15$

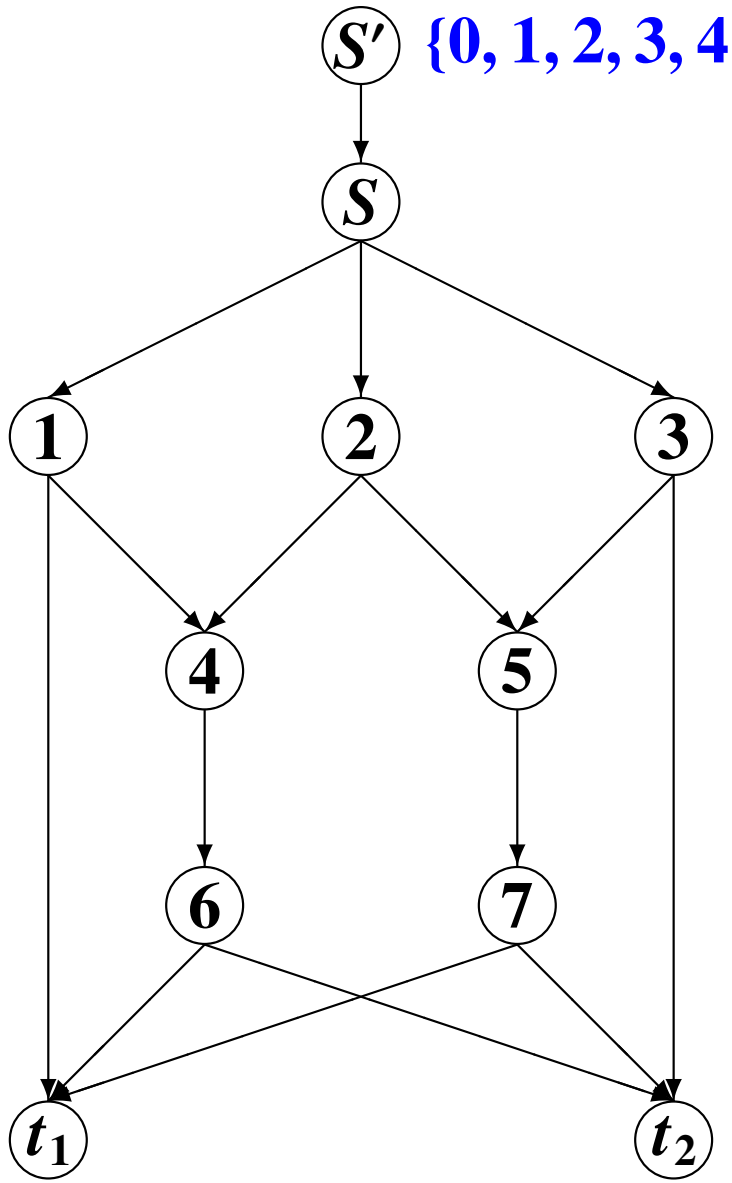


Network α-Error-Correcting Code

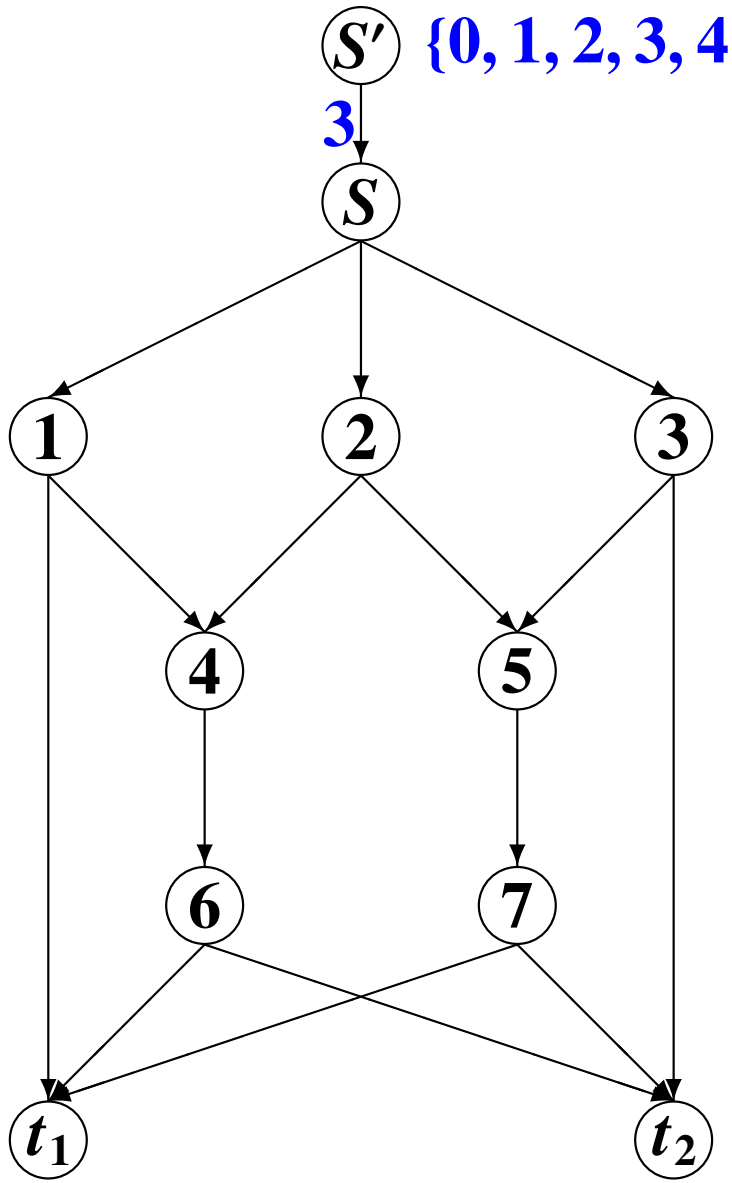
$(n, k, \alpha) = (3, 1, 1)$ — $n - k \geq 2\alpha$ — over $\mathbb{F}_5$



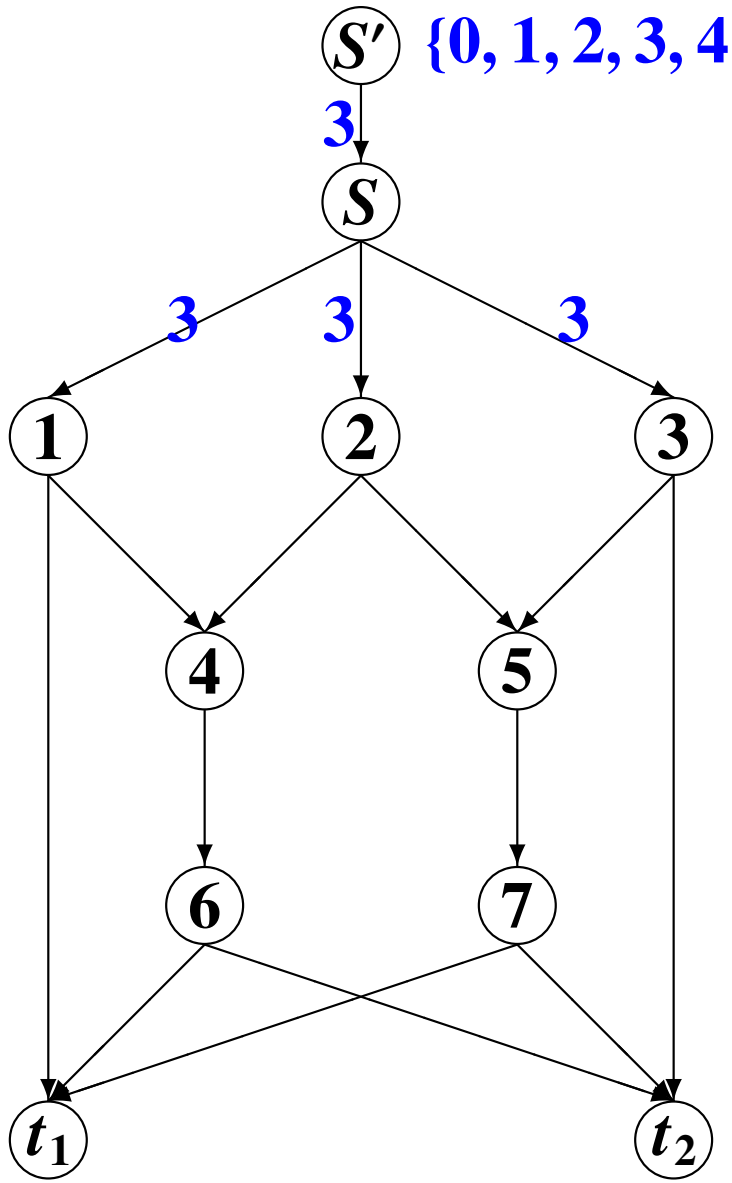
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



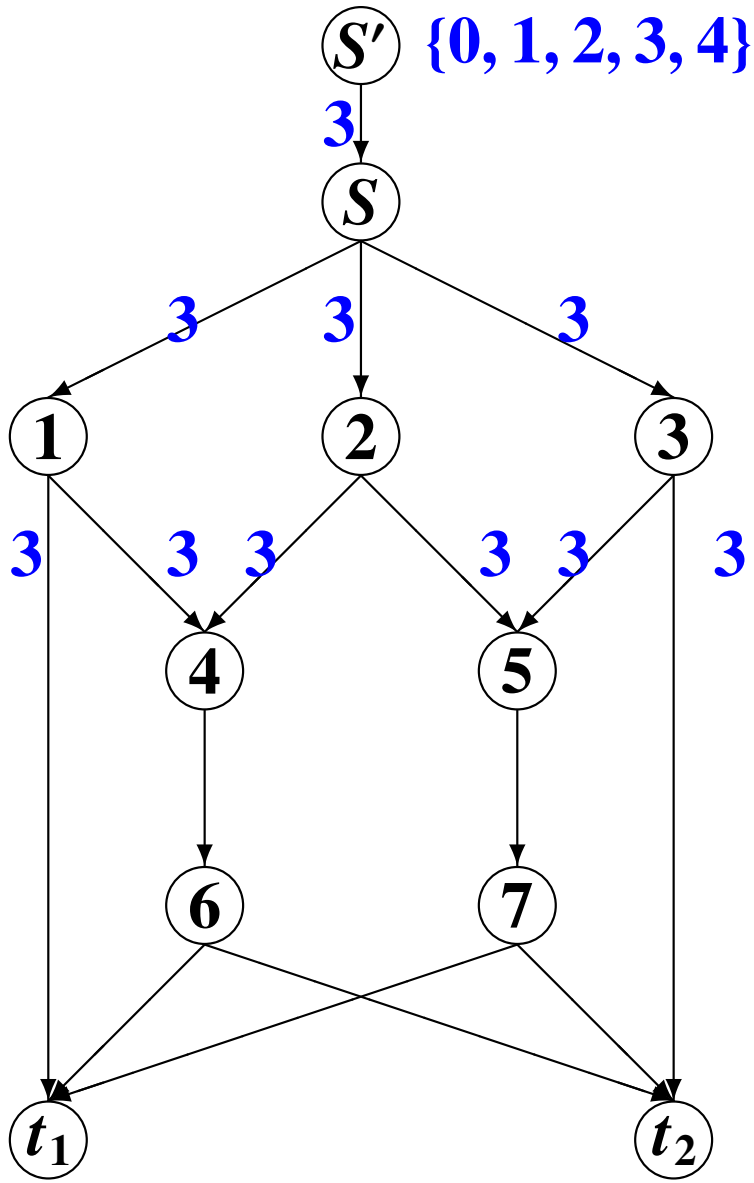
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



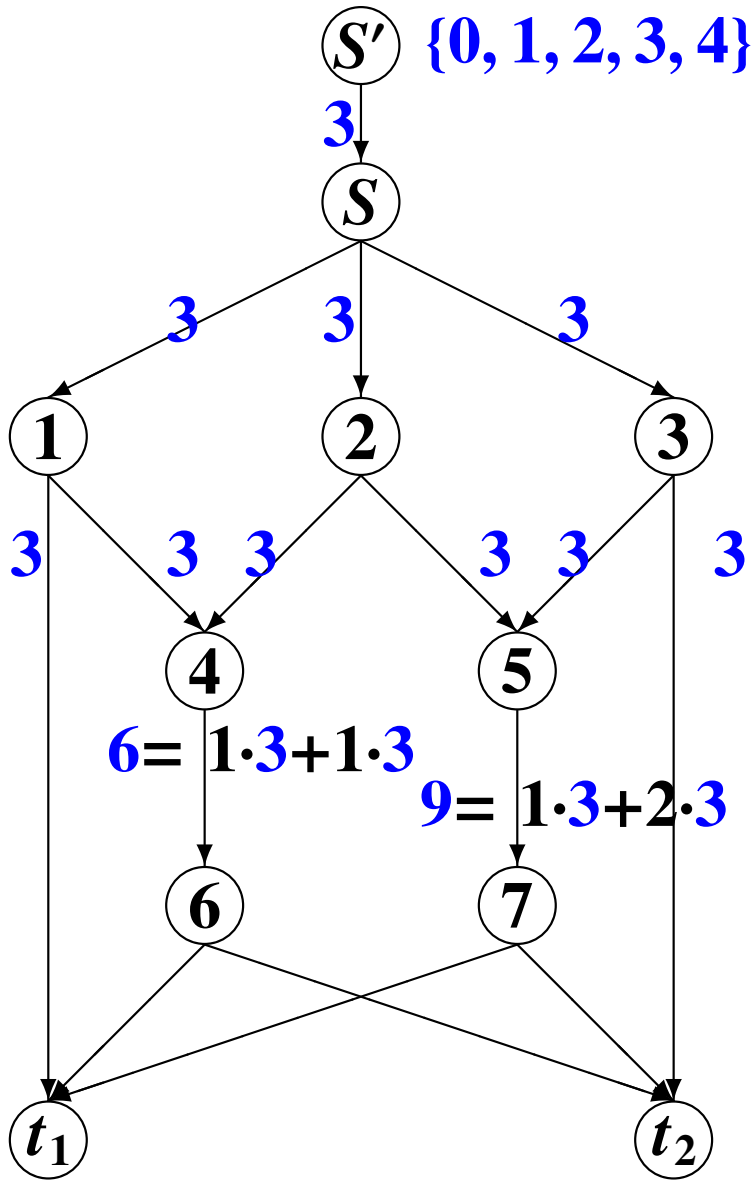
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



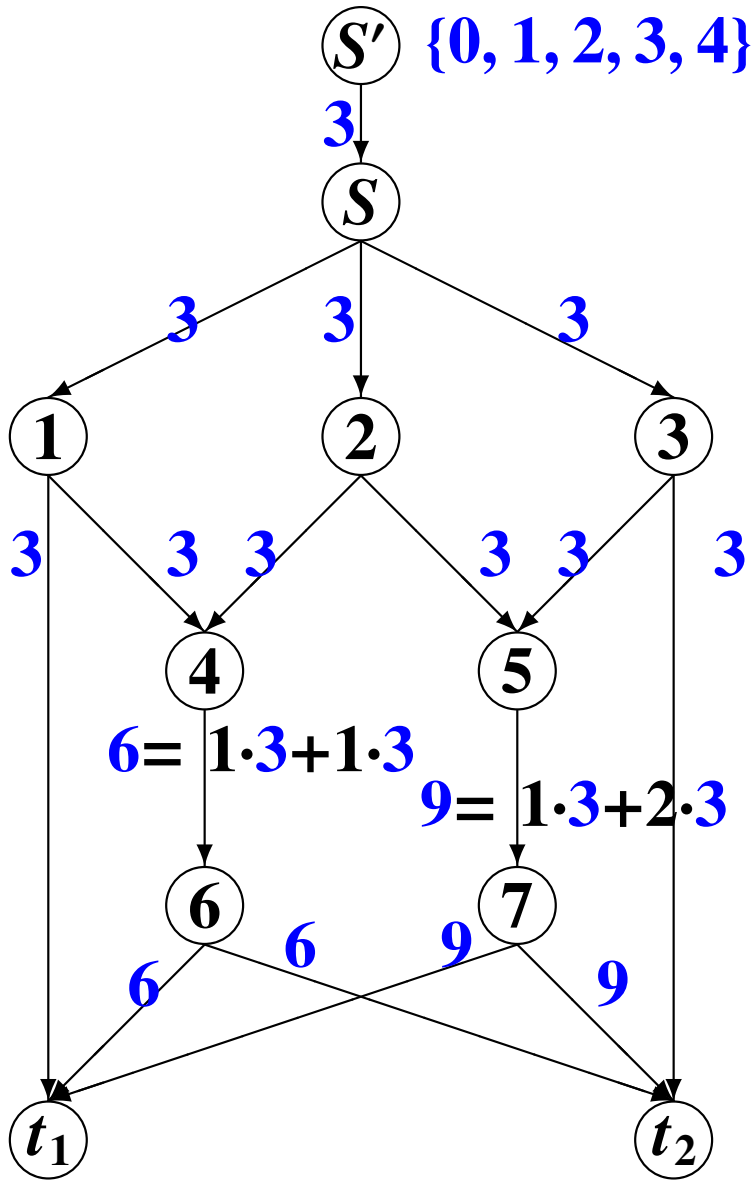
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



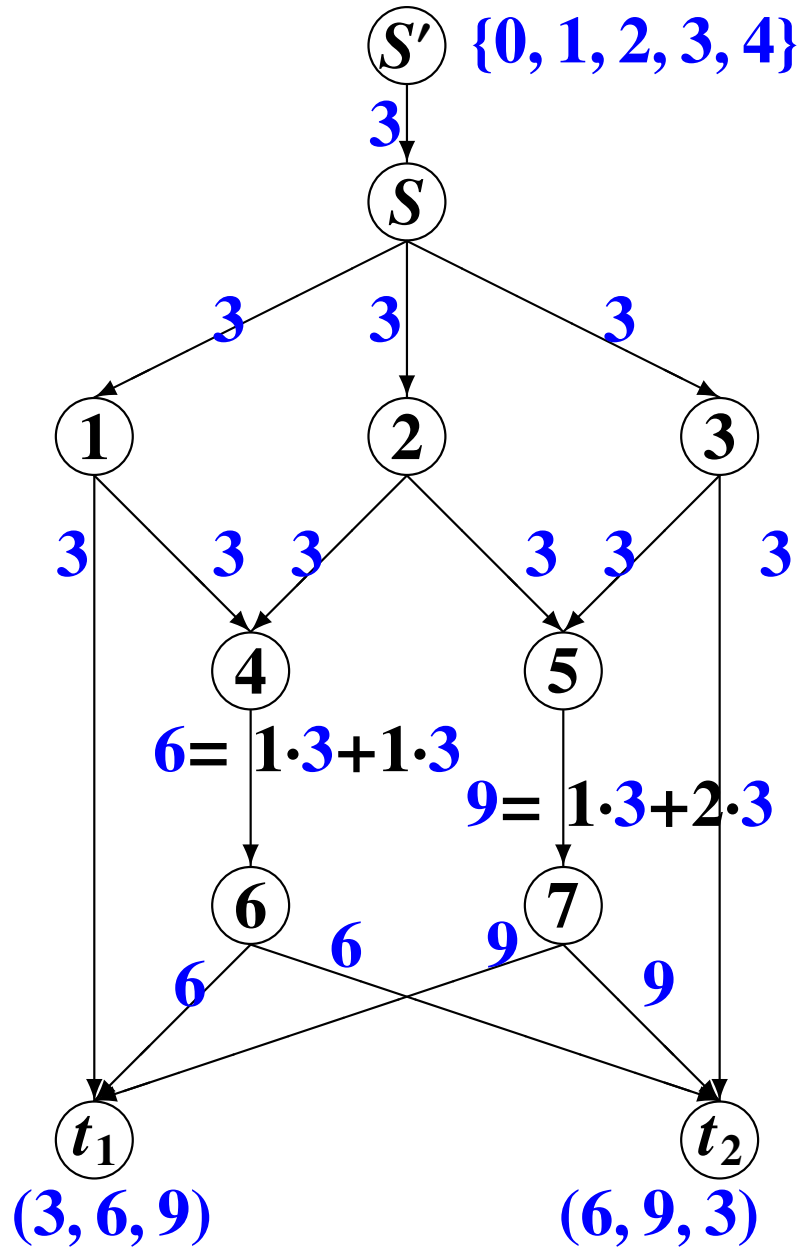
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



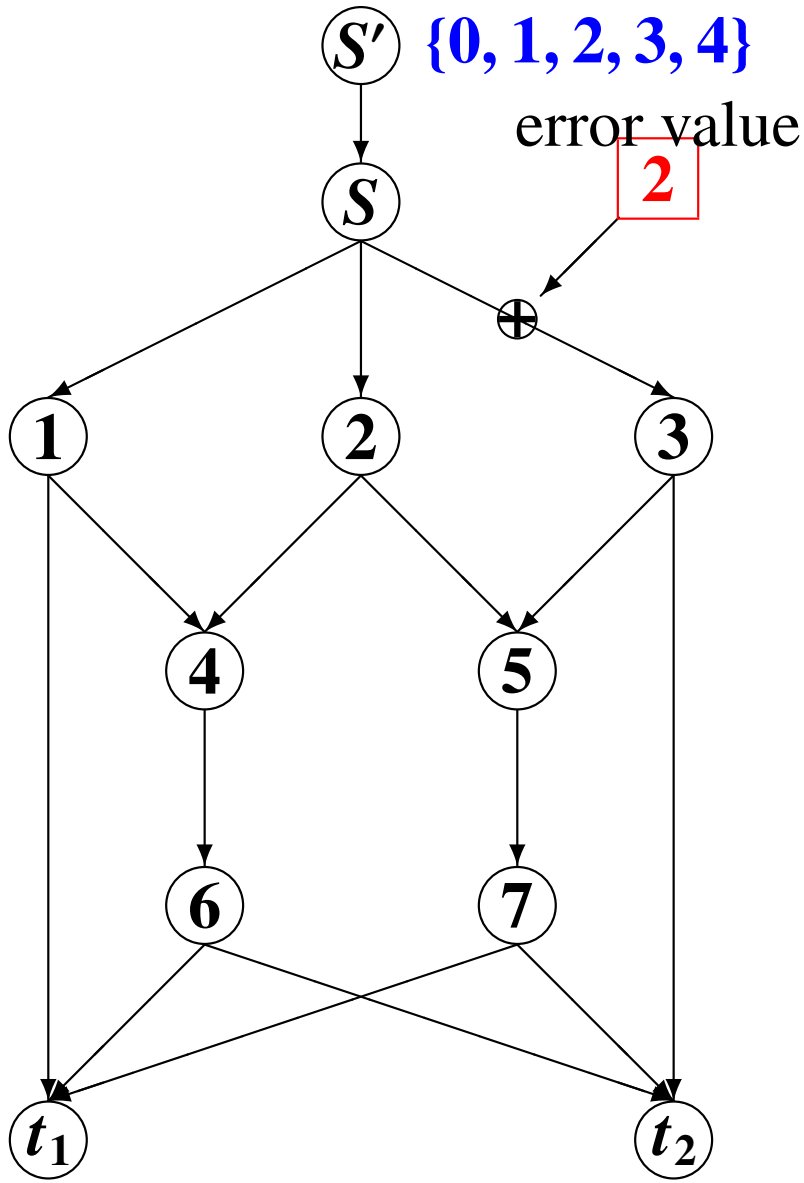
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



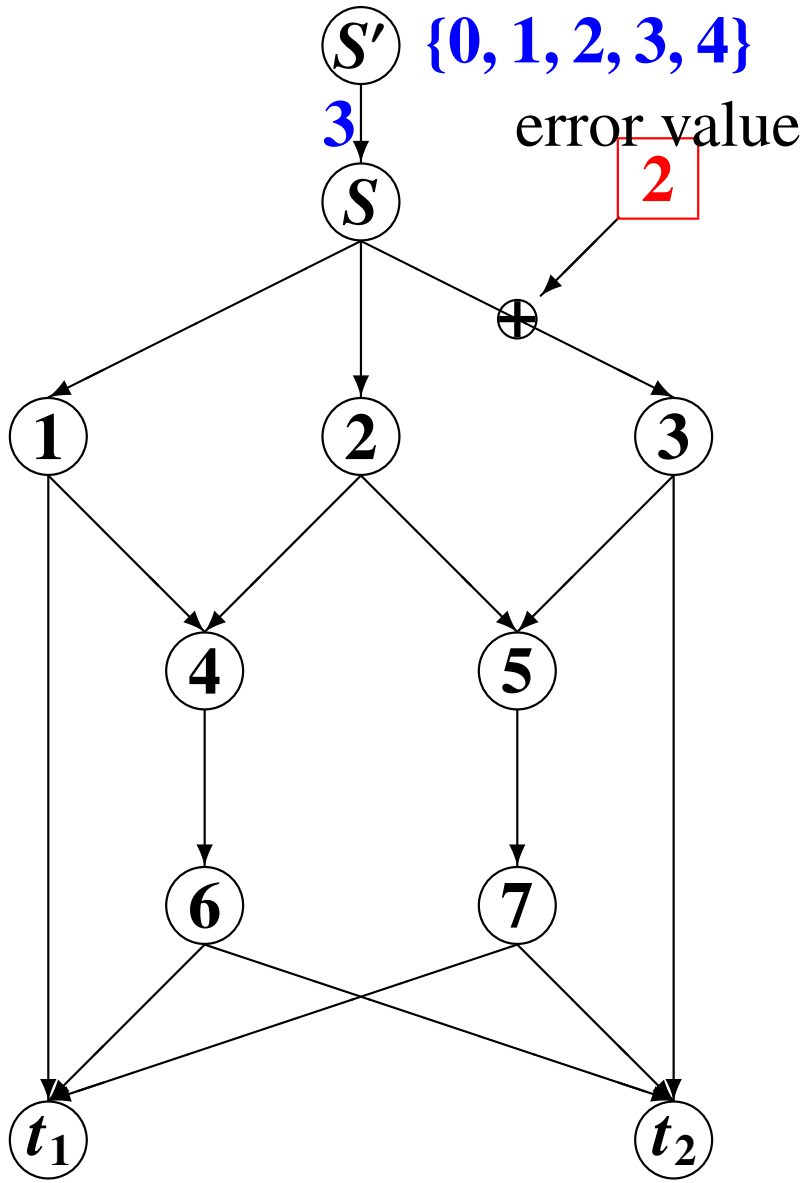
受信ベクトル $\phi_t(\vec{i}, \vec{0})$ — 誤りなし —



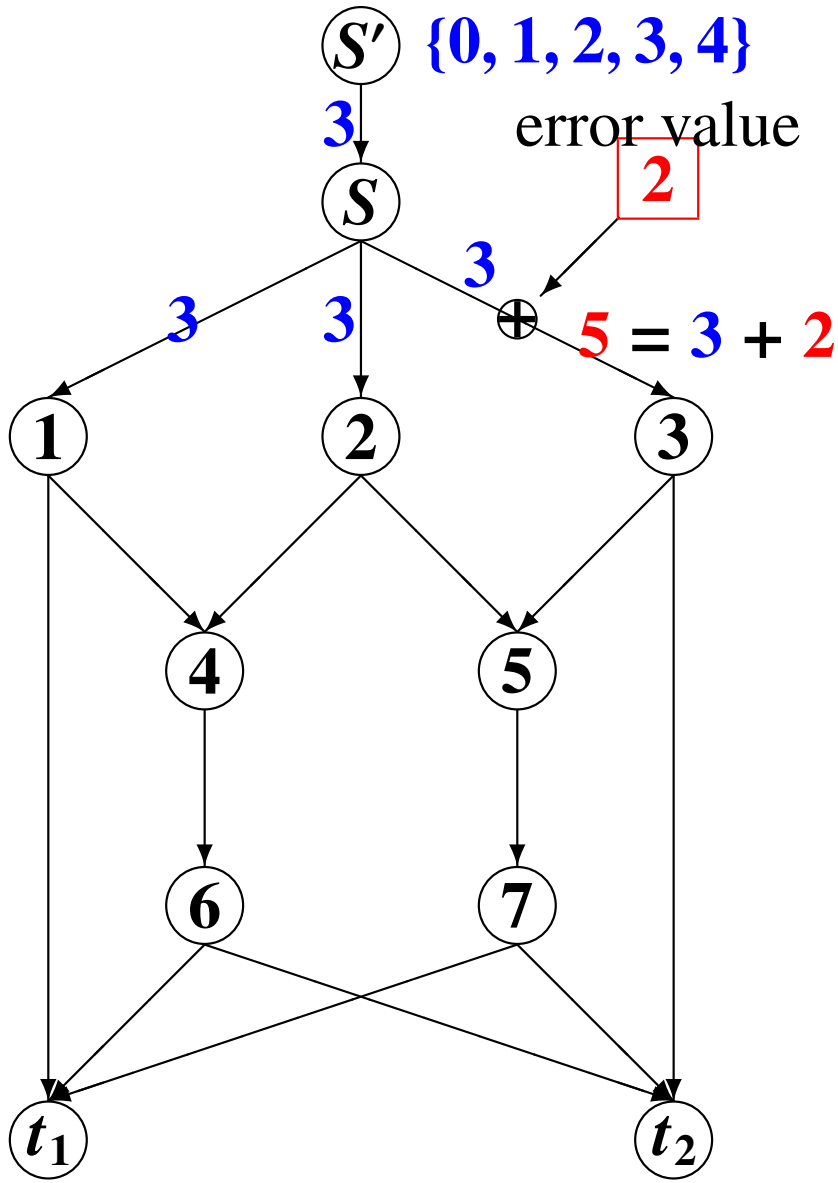
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



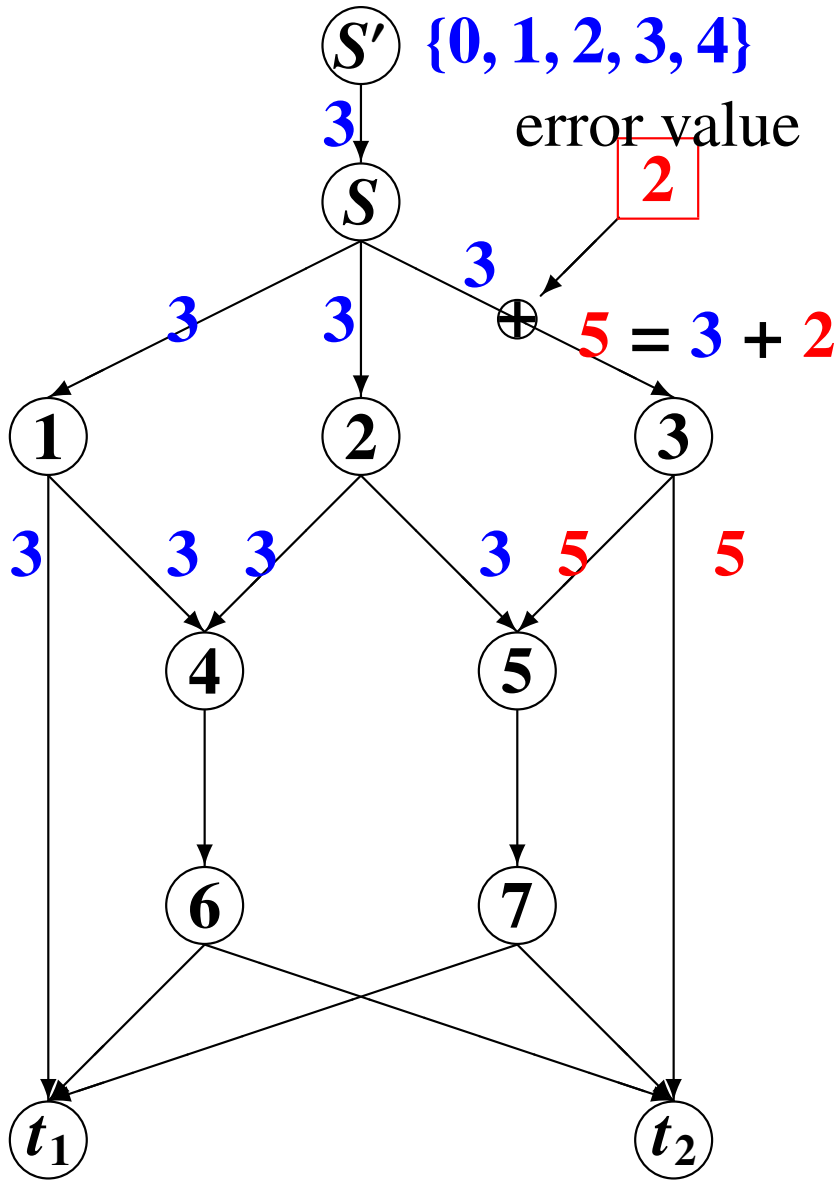
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



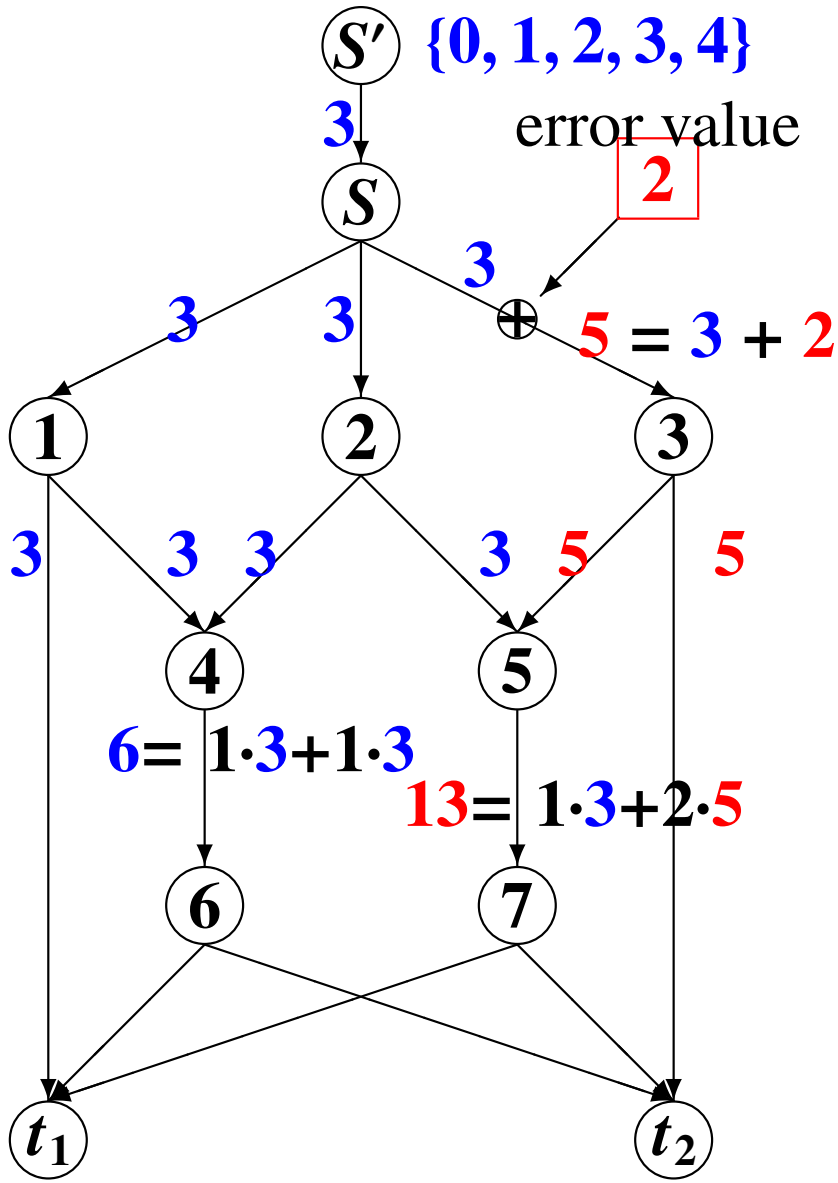
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



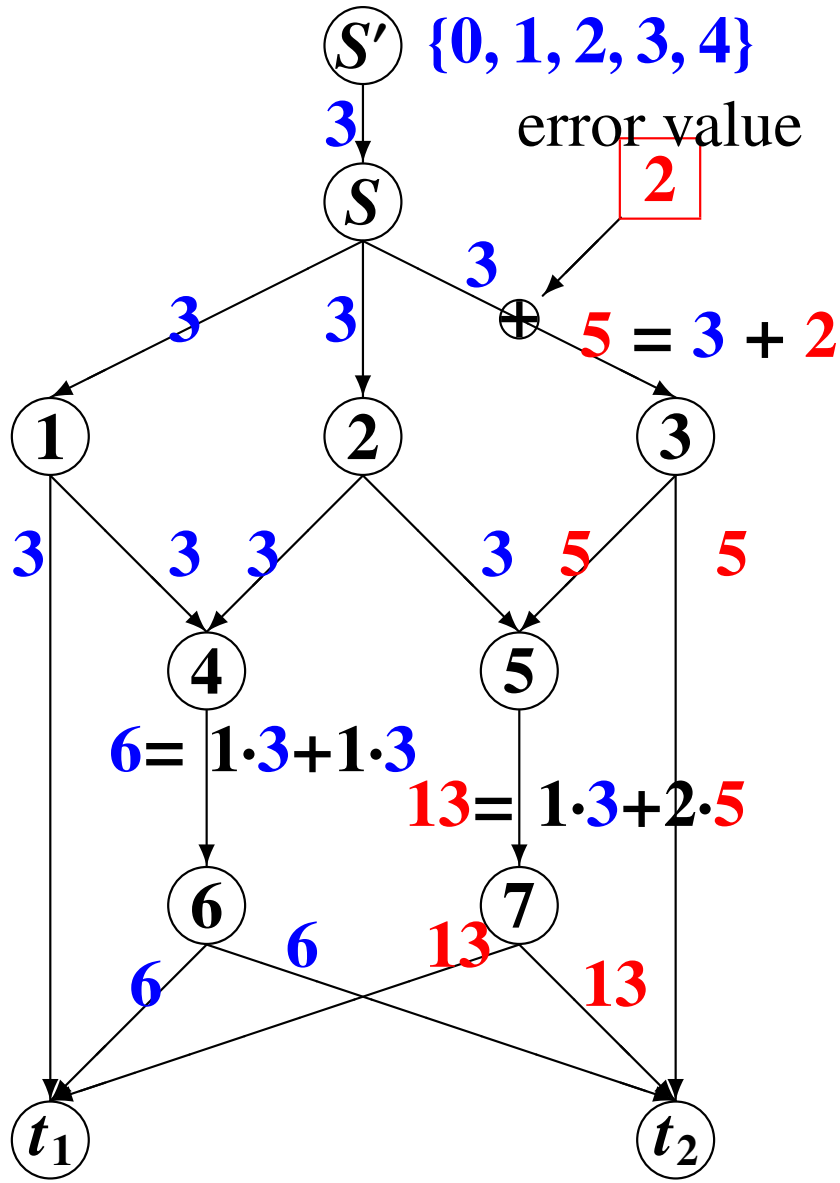
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



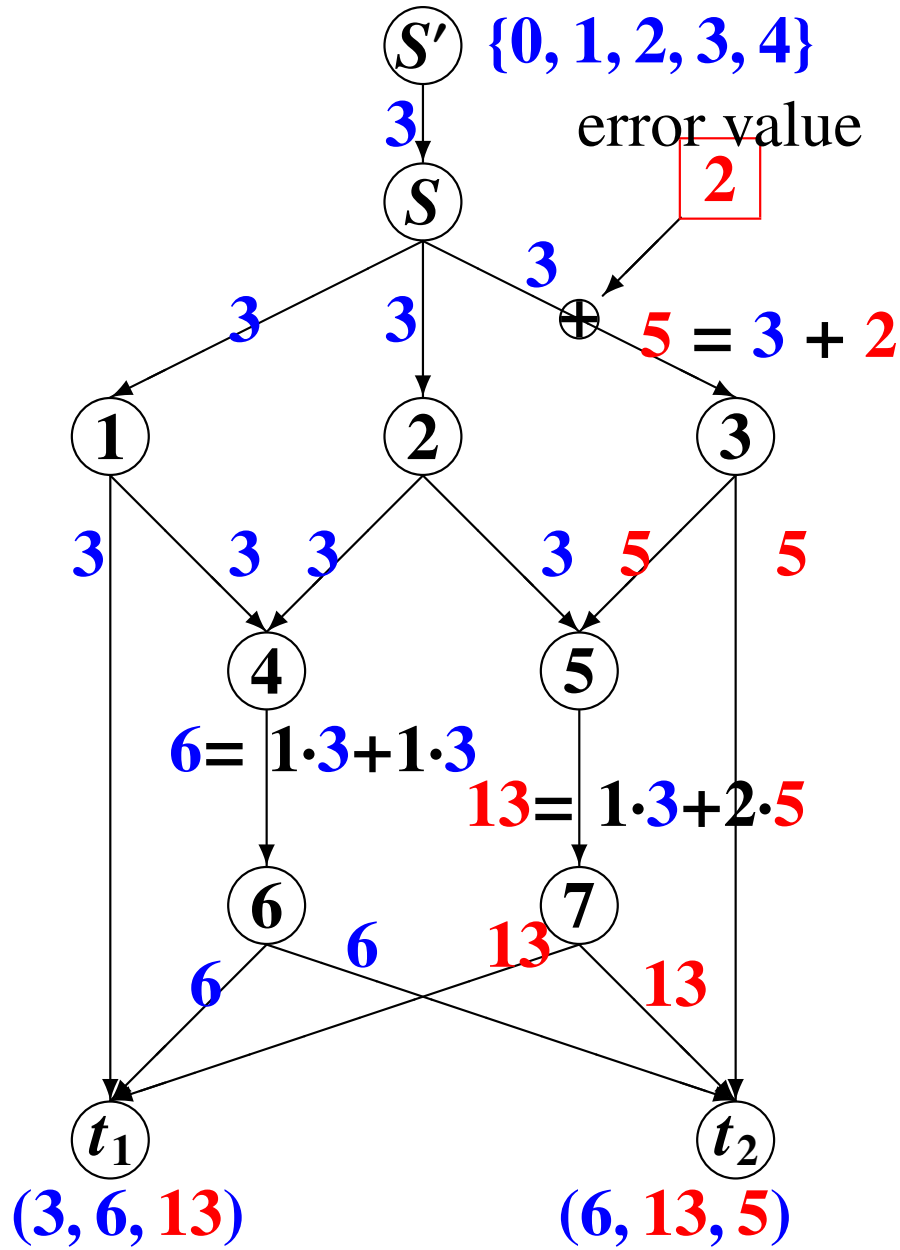
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



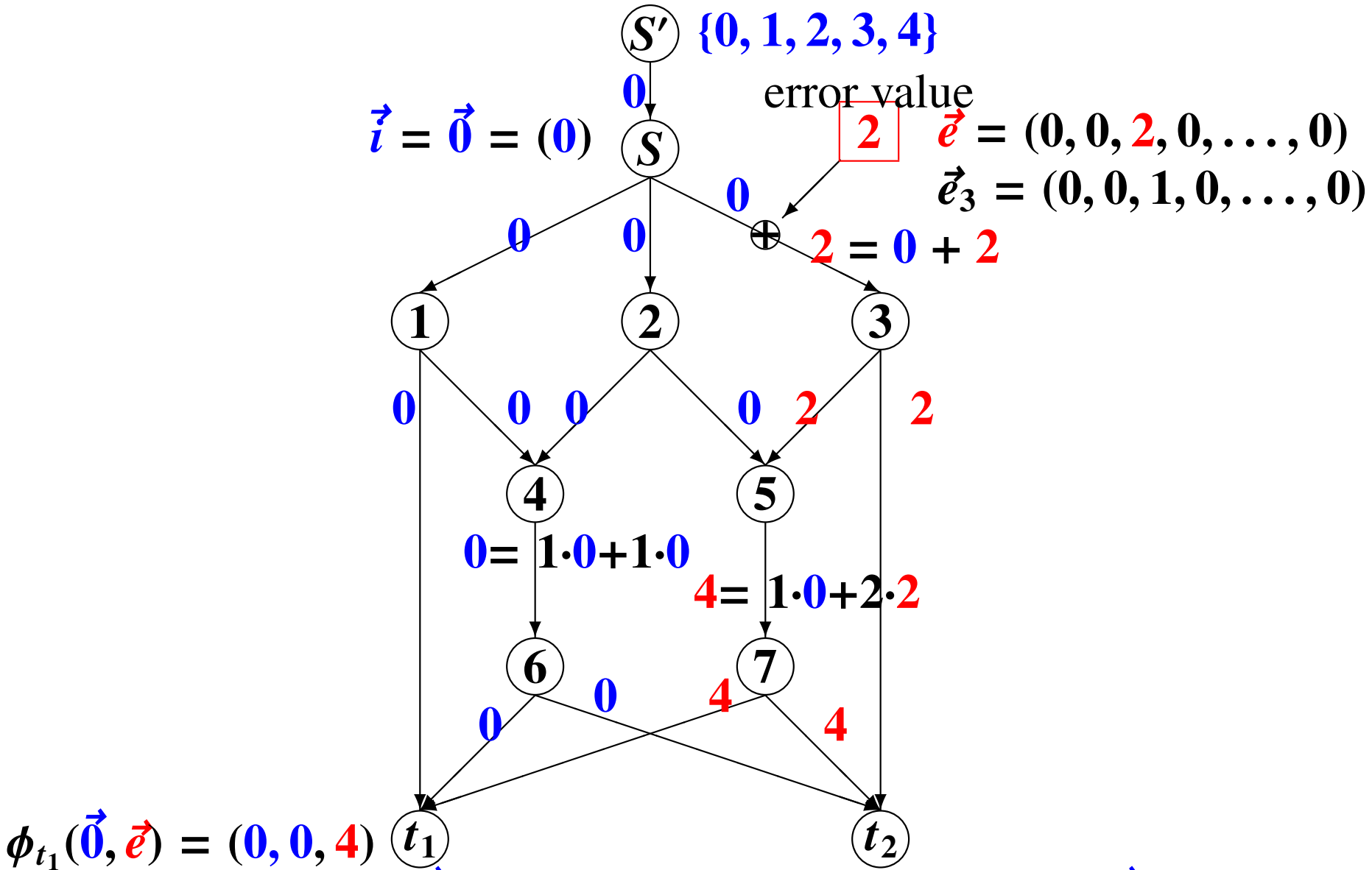
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



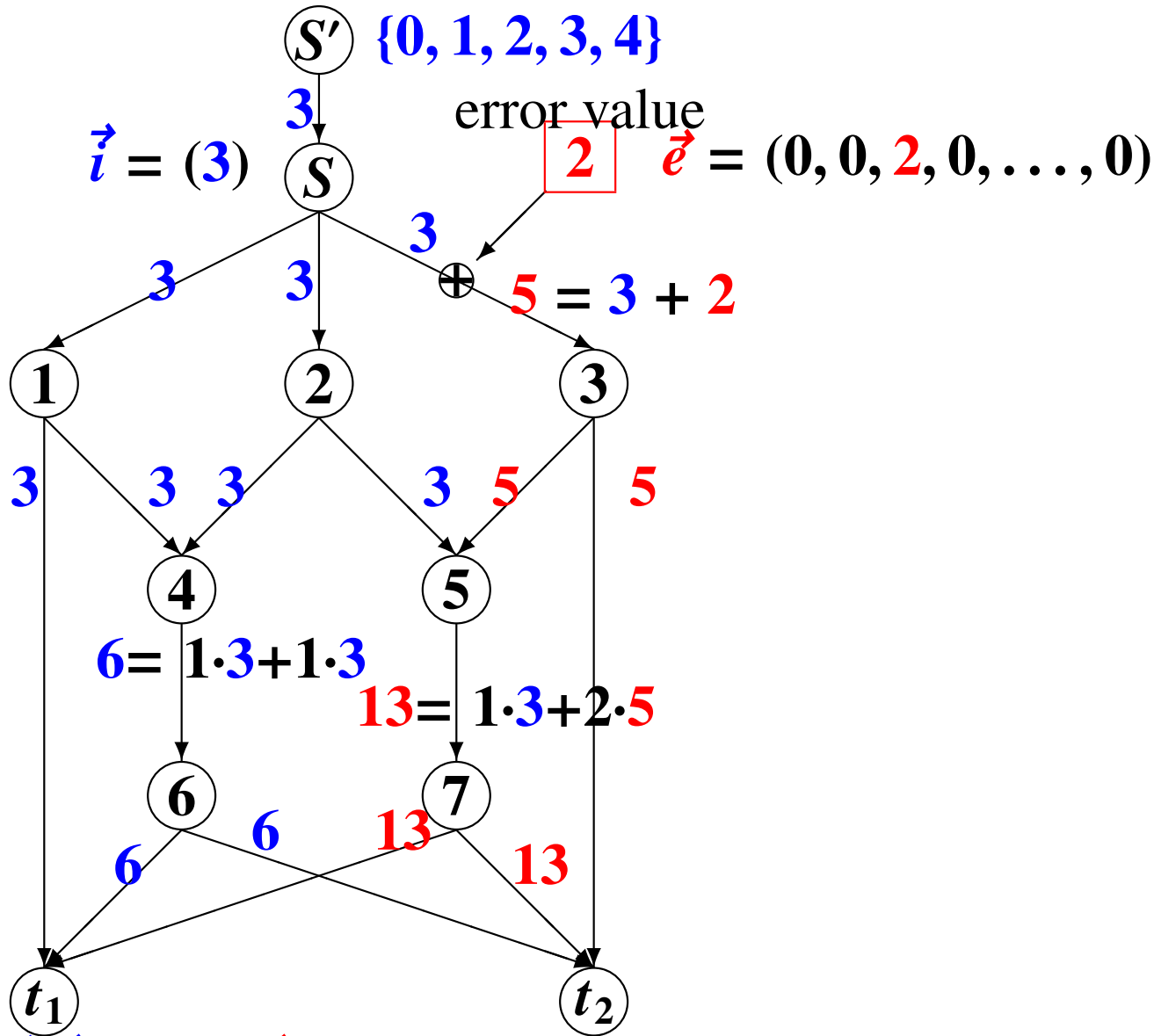
受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



受信ベクトル $\phi_t(\vec{0}, \vec{e})$ —誤りのみ—



受信ベクトル $\phi_t(\vec{i}, \vec{e})$ — 誤りあり —



$$\phi_{t_2}(\vec{i}, \vec{e}) = \phi_{t_2}(\vec{i}, \vec{0}) + \phi_{t_2}(\vec{0}, \vec{e}) = (6, 9, 3) + (0, 4, 2) = (6, 13, 5)$$

復号アルゴリズム (List)

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

1. Input the received vector $\vec{z}$.
2. Compute $\sigma(\vec{z})^T = H_t \vec{z}^T$.
3. If $\sigma(\vec{z}) = \mathbf{0}$ then output the information vector $\phi_t^{-1}(\vec{z})$ and halt else goto 4.
4. Choose an $\{\vec{u}_1, \ldots, \vec{u}_\alpha\} \in M$.
5. If the solution $v_1, \ldots, v_\alpha$ of the linear system (A) for $\vec{u}_1, \ldots, \vec{u}_\alpha$ can be found then goto 6 else goto 7.
6. Output the information vector $\phi_t^{-1}(\vec{z} - \sum_{i=1}^{\alpha} v_i \vec{u}_i)$ and halt.
7. Update $M = M \setminus \{\{\vec{u}_1, \ldots, \vec{u}_\alpha\}\}$. If $M = \emptyset$ then output "Error is detected" and halt else goto 4.