ネットワークコーディングにおける代数的誤り訂正符号とその構成法

栗原正純

電気通信大学

(UEC Tokyo)

IEICE 情報理論 (IT) 研究会 2009 年 7 月 24 日 関西学院大学 大阪梅田キャンパス

kuri@ice.uec.ac.jp

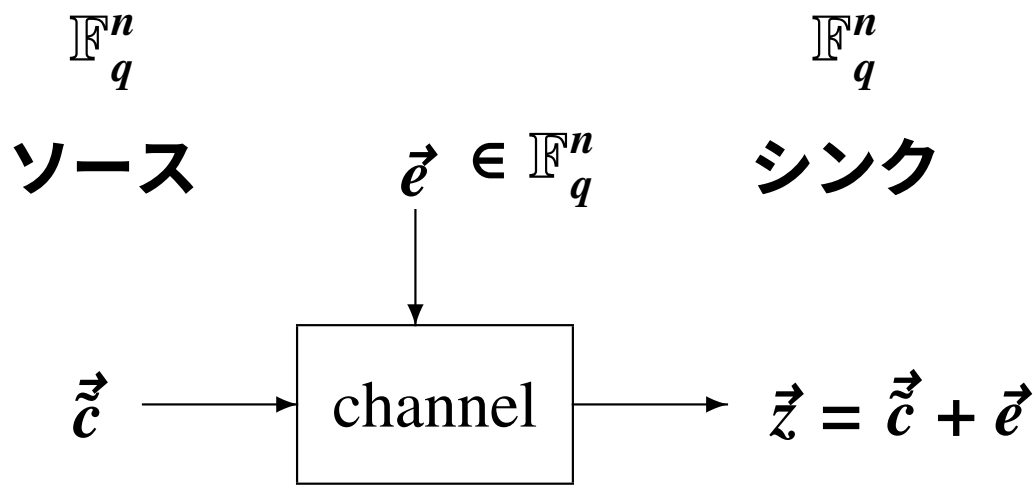
(2009/7/24/14:37)

キーワード

1. (情報伝送用) ネットワークコーディング
2. 伝送行列 H_t と テンプレート行列 T_t
3. テンプレート距離 d_{T_t} と 符号 C_t
4. マルチキャスト誤り訂正符号 $\widetilde{C}$
5. 生成行列 $\widetilde{G}$

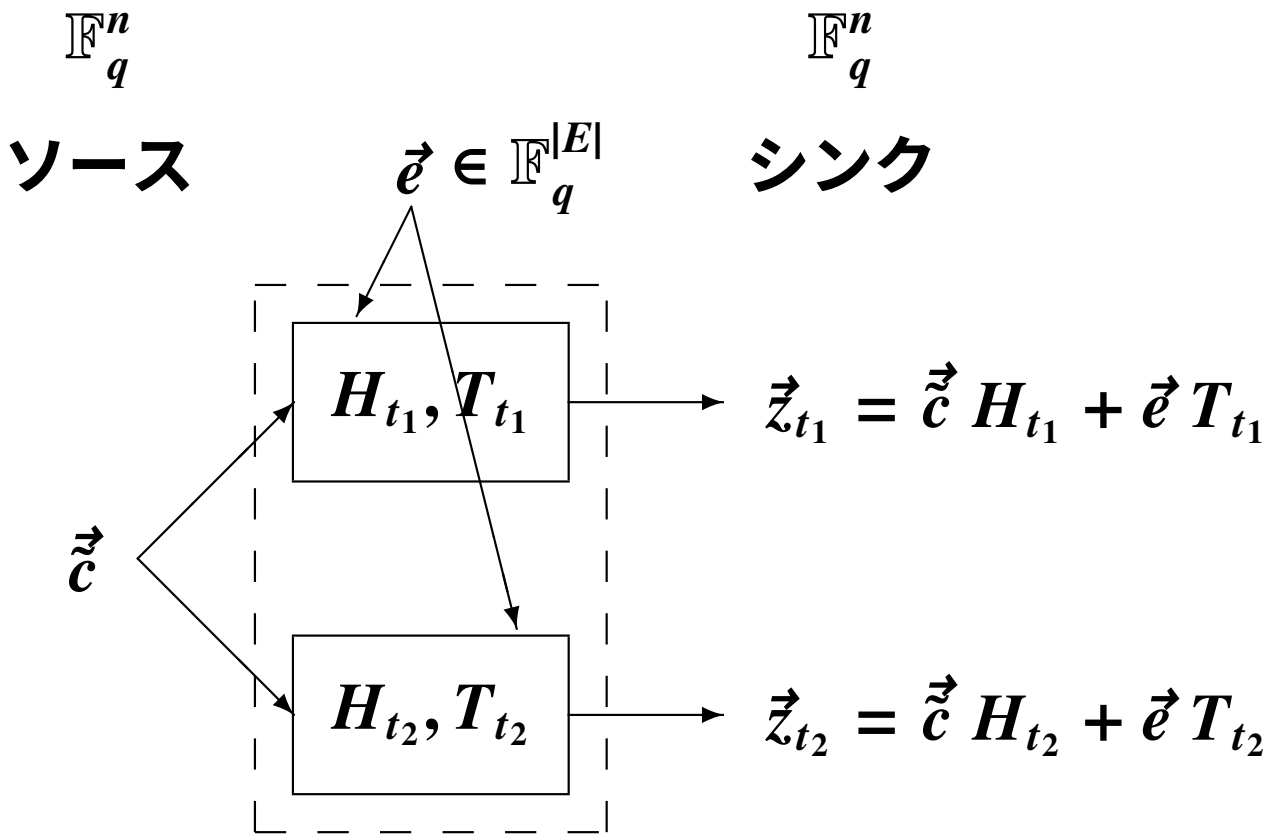
シングルユニキャスト (1 対 1 通信モデル) : 加法的離散通信路

従来のブロック誤り訂正符号



マルチキャスト (1 対多通信モデル) : 加法的離散通信路

Codes attaining the Singleton Bound

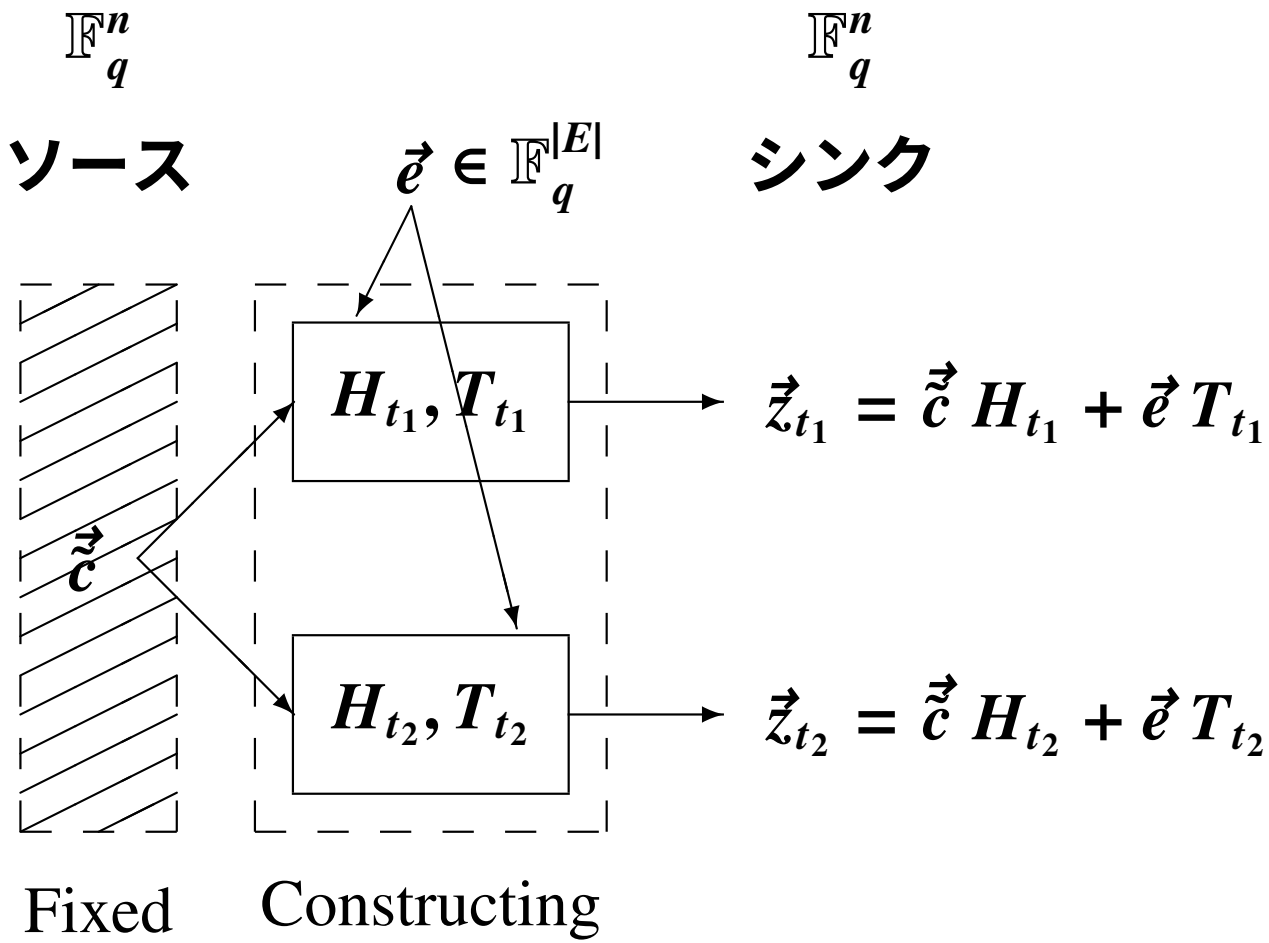


- $n = \min\{n_t \mid t \in T\}$
- H_t : 伝送行列 (情報 (送信シンボル列) を伝送する行列)
- T_t : テンプレート行列 (誤りを伝送する行列)

ネットワークコーディング

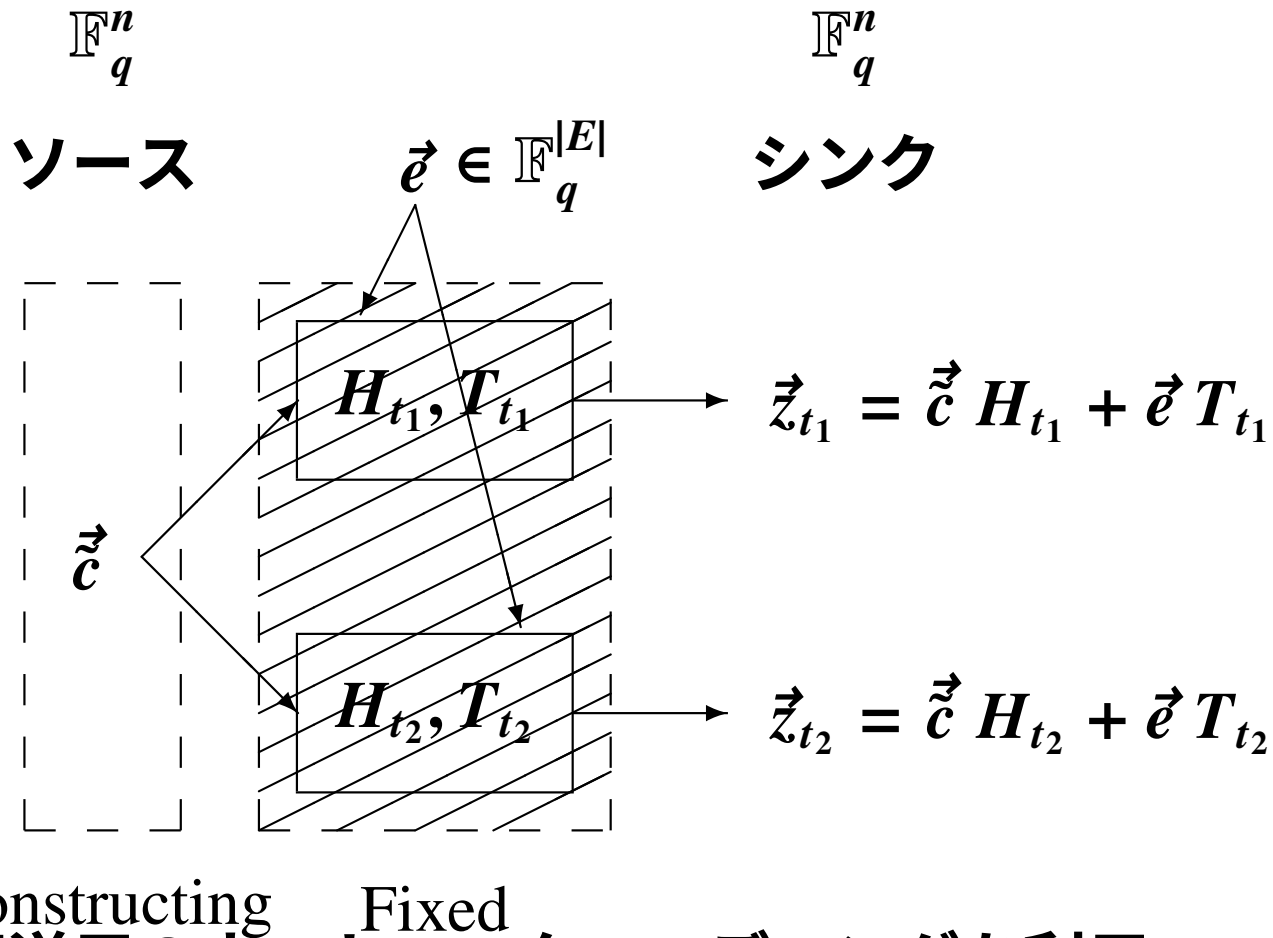
1. **ネットワークコーディングの提案**
   [1](R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, 2000)
2. **線形ネットワークコーディングの提案**
   [2](S.-Y. R. Li, R. W. Yeung, and N. Cai, 2003)
3. **線形ネットワークコーディングの構成法**
   [3](R. Koetter and M. Medard, 2003), [4](S.Jaggi, P.Sanders, P.A.Chou, M.Effros, S. Egner, K.Jain, and L.M.G.M.Tolhuizen, 2005)
4. **ネットワークコーディングの誤り訂正符号**
   [5](N. Cai and R.W. Yeung, 2002), [6](R.W. Yeung and N. Cai, 2006), [7](N. Cai and R.W. Yeung, 2006), [8](Z. Zhang, 2008)
5. **ネットワークコーディングの誤り訂正符号の構成法**
   [9](S. Yang, C.K. Ngai, and R.W. Yeung, 2007)
   [10](R. Matsumoto, 2007)

従来方法 [9,10]：マルチキャスト (1 対多通信モデル)



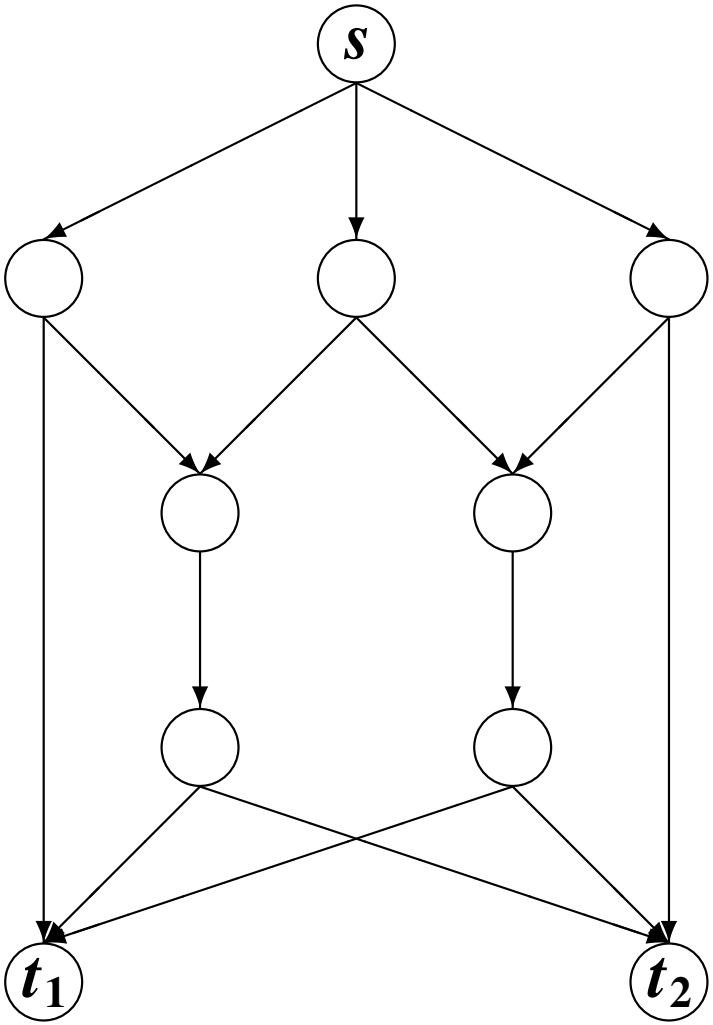
- 誤り訂正用のネットワークコーディングを構成

提案方法：マルチキャスト(1対多通信モデル)



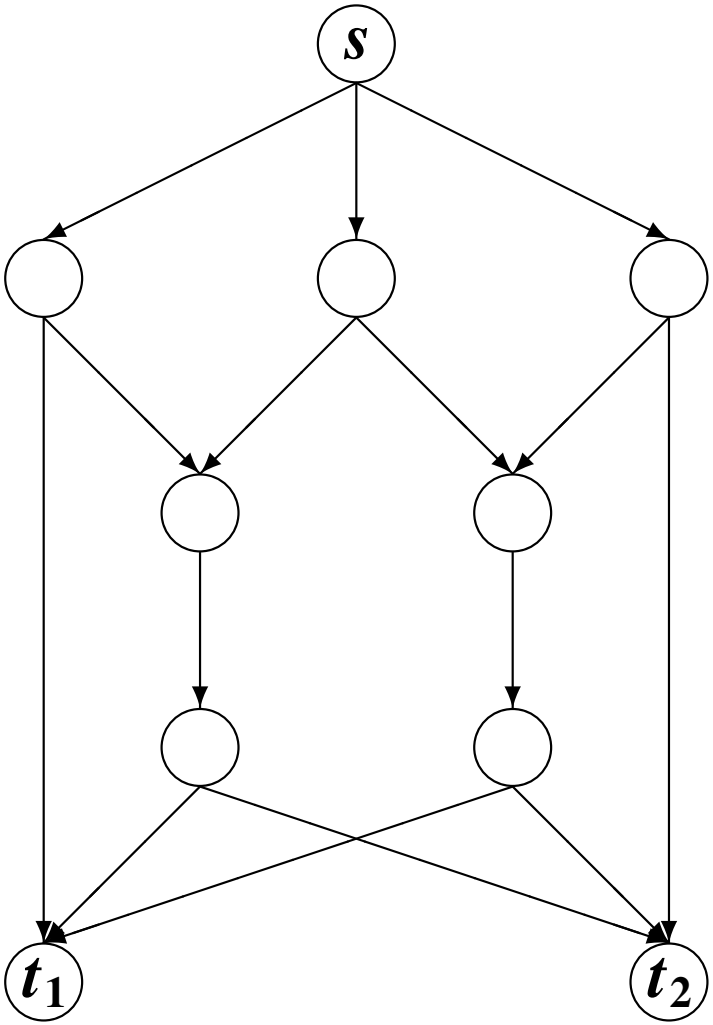
- 情報伝送用のネットワークコーディングを利用
- 送信シンボル列の符号化を工夫して、誤り訂正能力をもたせる
- 誤り訂正能力のパラメータごとに、ネットワークコーディングを再構成する必要がない

ネットワーク $(V, E, s, T = \{t_1, t_2\})$



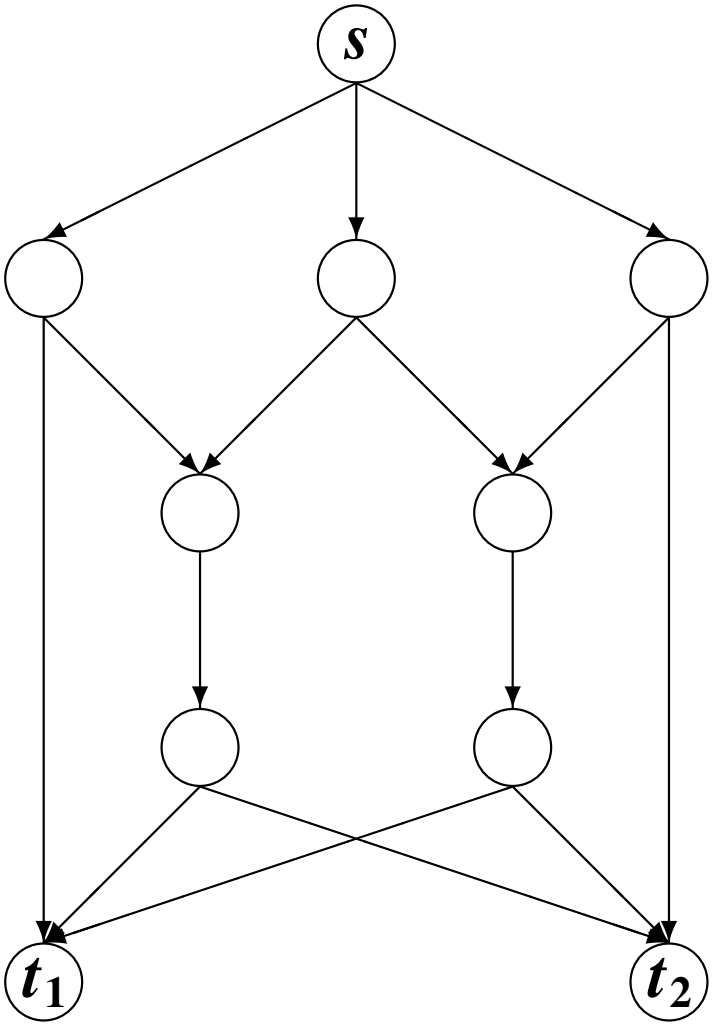
1. ネットワーク (V, E)
2. ソース $s \in V$
3. シンクの集合 $T = \{t_1, t_2\}$
4. ソースからシンクへの最大流
   n_{t_1} =maxflow$(s, t_1) = 3$
   n_{t_2} =maxflow$(s, t_2) = 3$
5. マルチキャスト可能な伝送量
   $n = \min\{n_{t_1}, n_{t_2}\} = 3$
6. リンクに番号付け $1 \sim |E|$

ネットワーク $(V, E, s, T = \{t_1, t_2\})$



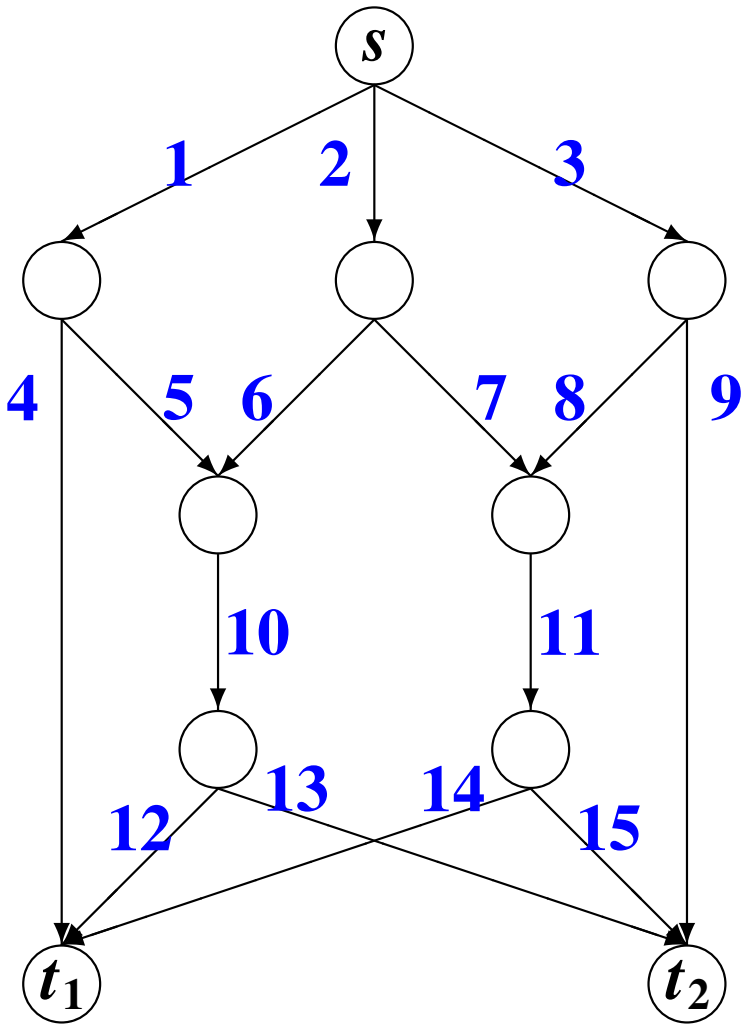
1. ネットワーク (V, E)
2. ソース $s \in V$
3. シンクの集合 $T = \{t_1, t_2\}$
4. ソースからシンクへの最大流
   n_{t_1} =maxflow$(s, t_1) = 3$
   n_{t_2} =maxflow$(s, t_2) = 3$
5. マルチキャスト可能な伝送量
   $n = \min\{n_{t_1}, n_{t_2}\} = 3$
6. リンクに番号付け $1 \sim |E|$

ネットワーク $(V, E, s, T = \{t_1, t_2\})$



1. ネットワーク (V, E)
2. ソース $s \in V$
3. シンクの集合 $T = \{t_1, t_2\}$
4. ソースからシンクへの最大流
   n_{t_1} =maxflow$(s, t_1) = 3$
   n_{t_2} =maxflow$(s, t_2) = 3$
5. マルチキャスト可能な伝送量
   $n = \min\{n_{t_1}, n_{t_2}\} = 3$
6. リンクに番号付け $1 \sim |E|$

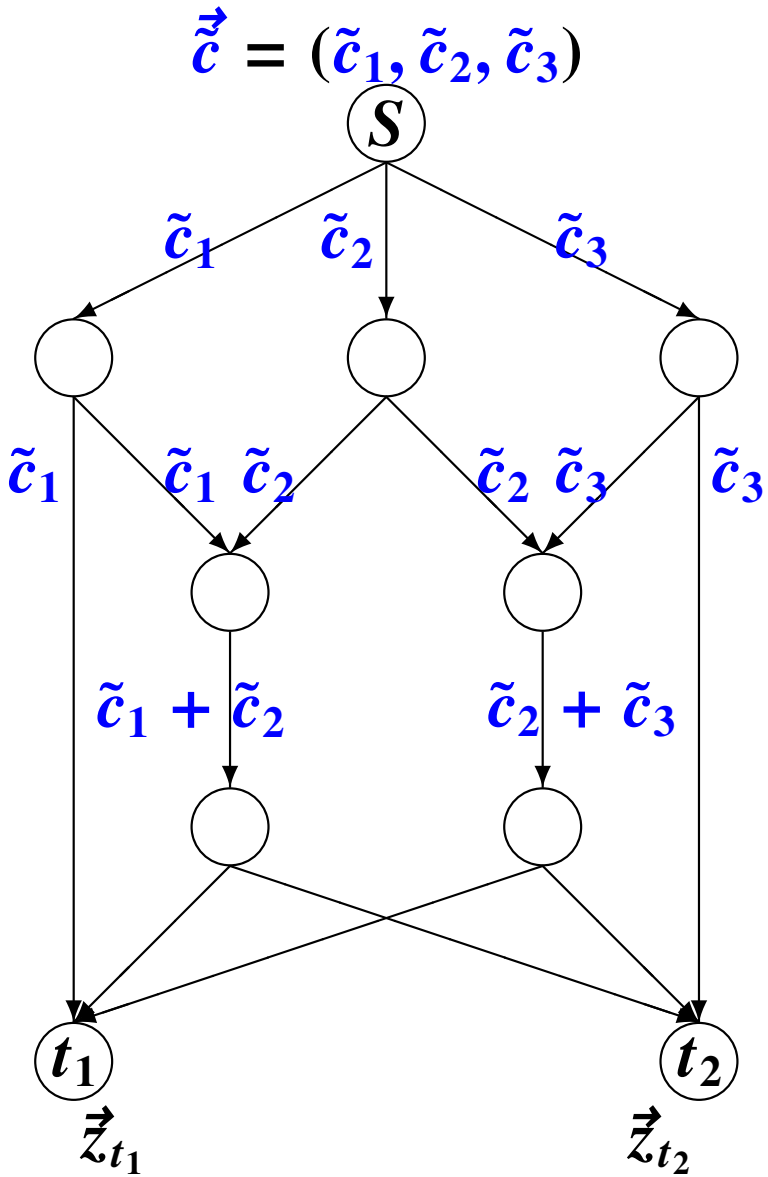
ネットワーク $(V, E, s, T = \{t_1, t_2\})$



1. ネットワーク (V, E)
2. ソース $s \in V$
3. シンクの集合 $T = \{t_1, t_2\}$
4. ソースからシンクへの最大流
   n_{t_1} =maxflow$(s, t_1) = 3$
   n_{t_2} =maxflow$(s, t_2) = 3$
5. マルチキャスト可能な伝送量
   $n = \min\{n_{t_1}, n_{t_2}\} = 3$
6. リンクに番号付け $1 \sim |E|$

(情報伝送用) ネットワークコーディング

ソースからシンクへの情報伝送



1. 各シンクの伝送行列 H_t が定まる

$$H_{t_1} = \begin{bmatrix} 110 \\ 011 \\ 001 \end{bmatrix}, \quad H_{t_2} = \begin{bmatrix} 010 \\ 011 \\ 101 \end{bmatrix}$$

2. $\vec{\tilde{c}}$, $\vec{z}_t$, H_t の関係:

$$\vec{z}_t = \vec{\tilde{c}}\, H_t$$

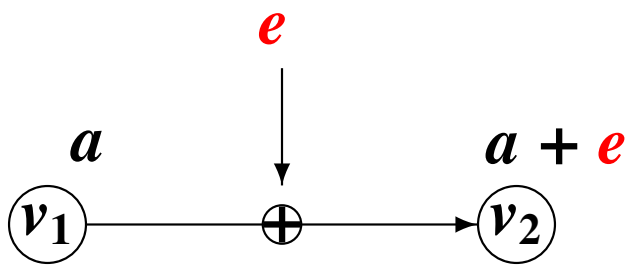
3. $\vec{z}_t$ から $\vec{\tilde{c}}$ の復元:

$$\vec{z}_t\, H_t^{-1} = \vec{\tilde{c}}$$

4. 同時に、各シンクの テンプレート行列 T_t も定まる

ネットワーク上で発生する誤りについて

- ネットワーク上の各リンクを加法的離散通信路として考える。
  - ノード v_1 からリンクにシンボル a を送信。
  - リンク上で**誤り値** e の誤りが発生。
  - ノード v_2 はリンクからシンボル $a + e$ を受信。



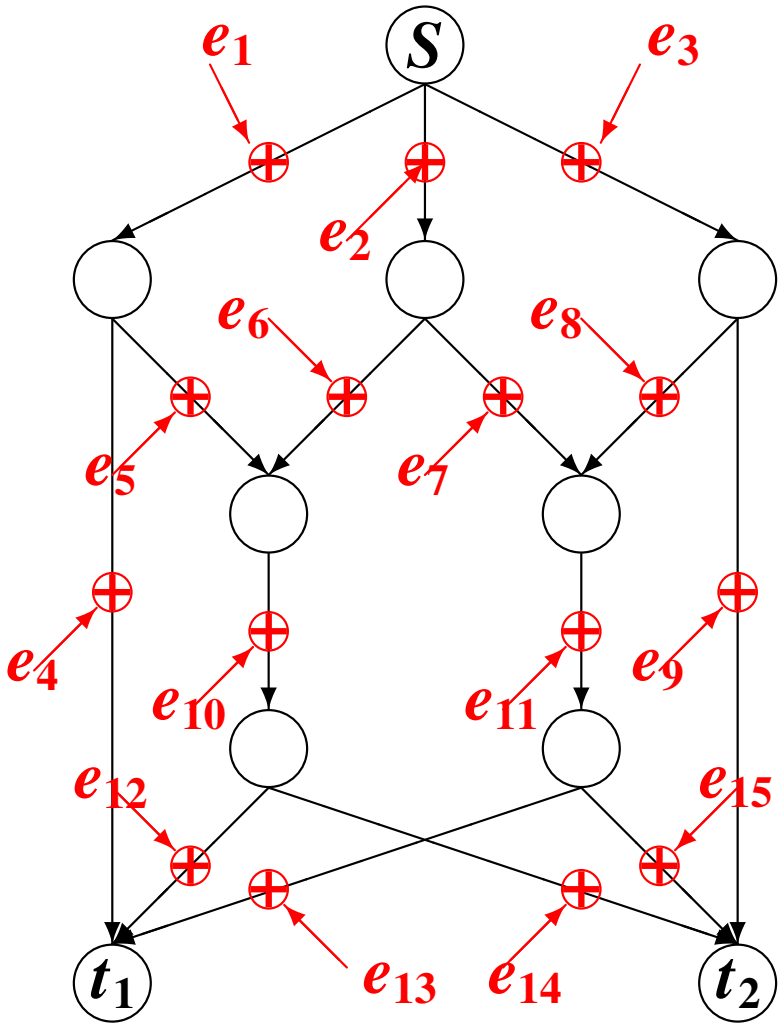
- これより、ネットワーク上の誤り $\vec{e}$ は

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

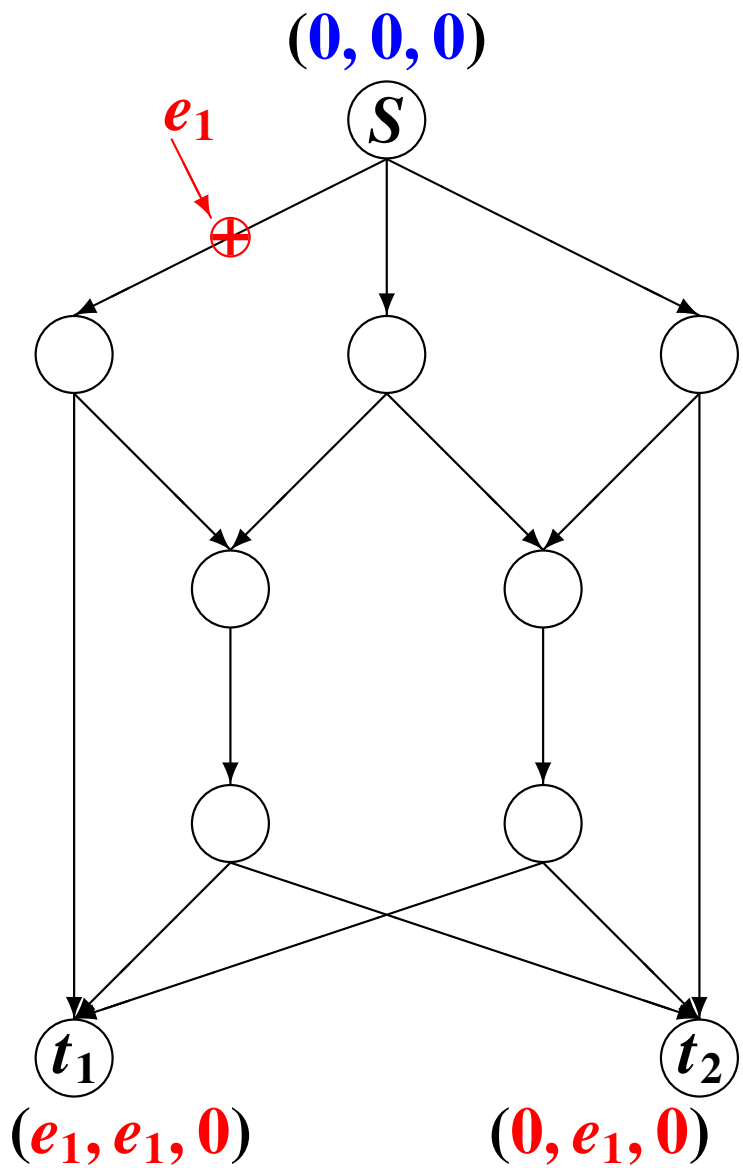
と表され、$w_{\mathrm{H}}(\vec{e}\,) =$ { 誤りの発生したリンクの本数 } となる。

誤り $\vec{e}$

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

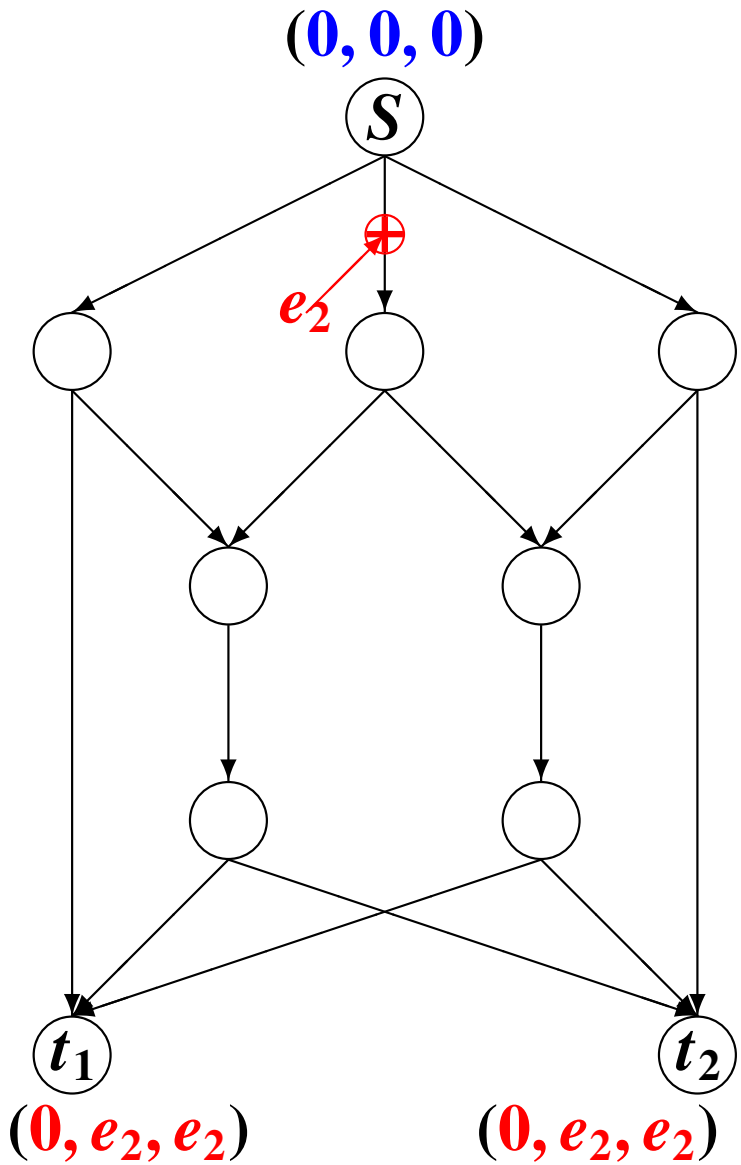


誤りと受信ベクトル



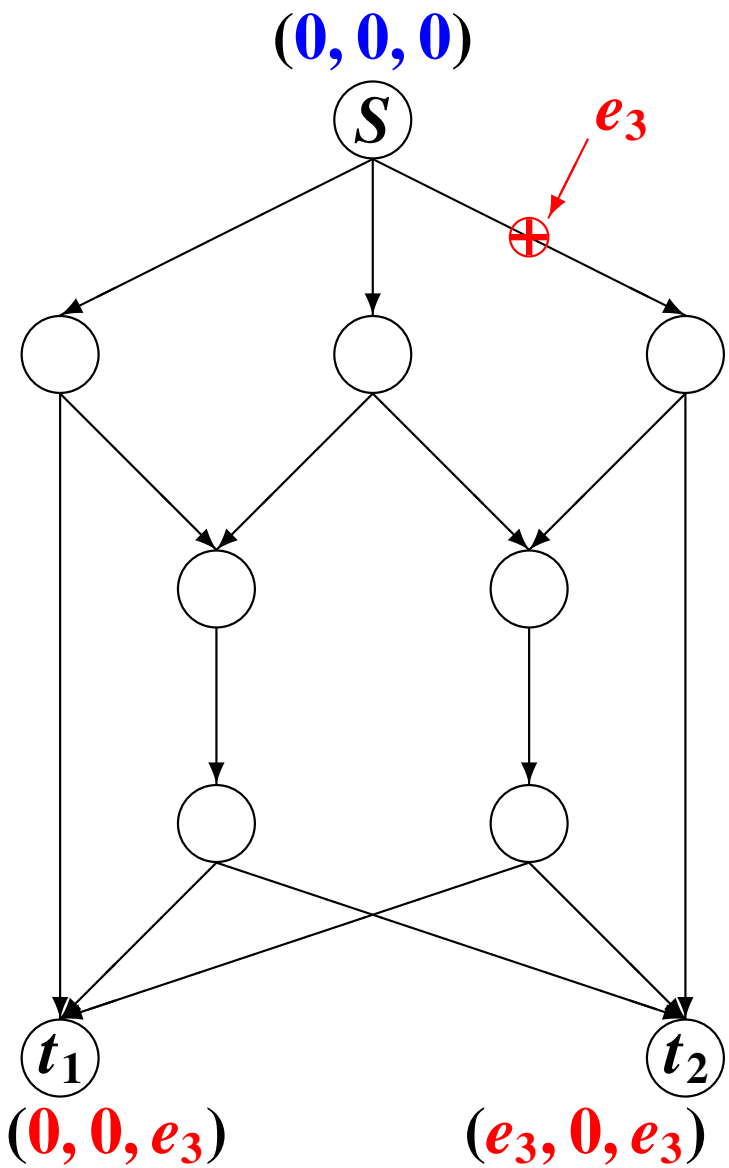
シンク t_1	シンク t_2
$e_1(110)$	$e_1(010)$
$e_2(011)$	$e_2(011)$
$e_3(001)$	$e_3(101)$
$e_4(100)$	$e_4(000)$
$e_5(010)$	$e_5(010)$
$e_6(010)$	$e_6(010)$
$e_7(001)$	$e_7(001)$
$e_8(001)$	$e_8(001)$
$e_9(000)$	$e_9(100)$
$e_{10}(010)$	$e_{10}(010)$
$e_{11}(001)$	$e_{11}(001)$
$e_{12}(010)$	$e_{12}(000)$
$e_{13}(000)$	$e_{13}(010)$
$e_{14}(001)$	$e_{14}(000)$
$e_{15}(000)$	$e_{15}(001)$

誤りと受信ベクトル



シンク t_1	シンク t_2
$e_1(110)$	$e_1(010)$
$e_2(011)$	$e_2(011)$
$e_3(001)$	$e_3(101)$
$e_4(100)$	$e_4(000)$
$e_5(010)$	$e_5(010)$
$e_6(010)$	$e_6(010)$
$e_7(001)$	$e_7(001)$
$e_8(001)$	$e_8(001)$
$e_9(000)$	$e_9(100)$
$e_{10}(010)$	$e_{10}(010)$
$e_{11}(001)$	$e_{11}(001)$
$e_{12}(010)$	$e_{12}(000)$
$e_{13}(000)$	$e_{13}(010)$
$e_{14}(001)$	$e_{14}(000)$
$e_{15}(000)$	$e_{15}(001)$

誤りと受信ベクトル



シンク t_1	シンク t_2
$e_1(110)$	$e_1(010)$
$e_2(011)$	$e_2(011)$
$e_3(001)$	$e_3(101)$
$e_4(100)$	$e_4(000)$
$e_5(010)$	$e_5(010)$
$e_6(010)$	$e_6(010)$
$e_7(001)$	$e_7(001)$
$e_8(001)$	$e_8(001)$
$e_9(000)$	$e_9(100)$
$e_{10}(010)$	$e_{10}(010)$
$e_{11}(001)$	$e_{11}(001)$
$e_{12}(010)$	$e_{12}(000)$
$e_{13}(000)$	$e_{13}(010)$
$e_{14}(001)$	$e_{14}(000)$
$e_{15}(000)$	$e_{15}(001)$

誤り $\vec{e}$ とテンプレート行列 T_t

$$
\begin{array}{ll}
e_1 & (110) \\
e_2 & (011) \\
e_3 & (001) \\
e_4 & (100) \\
e_5 & (010) \\
e_6 & (010) \\
e_7 & (001) \\
e_8 & (001) \\
e_9 & (000) \\
e_{10} & (010) \\
e_{11} & (001) \\
e_{12} & (010) \\
e_{13} & (000) \\
e_{14} & (001) \\
e_{15} & (000)
\end{array}
\quad \Longrightarrow \quad
\vec{e} = (e_1, \ldots, e_{15}) \text{ and } T_{t_1} = \left[\begin{array}{l}
110 \\ 011 \\ 001 \\ 100 \\ 010 \\ 010 \\ 001 \\ 001 \\ 000 \\ 010 \\ 001 \\ 010 \\ 000 \\ 001 \\ 000
\end{array}\right]
$$

送信ベクトル $\vec{c}$, 誤り $\vec{e}$, 受信ベクトル $\vec{z}$ の関係

1. $\vec{c} \in \mathbb{F}_q^n$: ソースからの送信ベクトル
2. $\vec{e} \in \mathbb{F}_q^{|E|}$: ネットワーク上で発生した誤り
3. H_t : $n \times n$ 伝送行列 (情報を伝送する行列)
4. T_t : $|E| \times n$ テンプレート行列 (誤りを伝送する行列)
5. $\vec{z} \in \mathbb{F}_q^n$: 受信ベクトル

$$\vec{z} = \vec{c} H_t + \vec{e} T_t$$

(テンプレート行列 T_t に関する) テンプレート距離 d_{T_t}

1. テンプレート行列 T_t
   $\vec{t}_{t,1}, \ldots, \vec{t}_{t,|E|}$ は T_t の行ベクトル (テンプレート) を表す。
2. テンプレート行列の条件
   $\mathrm{spn}(T_t) = \mathrm{spn}(\{\vec{t}_{t,1}, \ldots, \vec{t}_{t,|E|}\}) = \mathbb{F}_q^n$
3. 任意の $\vec{x}, \vec{y} \in \mathbb{F}_q^n$ に対し, $\vec{x}$ と $\vec{y}$ のテンプレート行列 T_t に関するテンプレート距離を

$$d_{T_t}(\vec{x}, \vec{y}) = \min\{w_{\mathrm{H}}(\vec{e}) \mid \vec{e} \in \mathbb{F}_q^{|E|}, \sum_{i=1}^{|E|} e_i \vec{t}_{t,i} = \vec{x} - \vec{y}\} \quad (1)$$

と定義する.
ただし, $\vec{e}$ は $\vec{e} = (e_1, \ldots, e_{|E|}) \in \mathbb{F}_q^{|E|}$ であり, $w_{\mathrm{H}}(\vec{e})$ は $\vec{e}$ のハミング重みを表す.

符号 C_t と最小距離 $d_{T_t}(C_t)$

1. 符号 $C_t \subseteq \mathbb{F}_q^n$
2. 符号 C_t のテンプレート行列 T_t に関する最小テンプレート距離 $d_{T_t}(C_t)$ を

$$d_{T_t}(C_t) = \min\{d_{T_t}(\vec{x}, \vec{y}) \mid \vec{x}, \vec{y} \in C,\ \vec{x} \neq \vec{y}\} \qquad (2)$$

と定義する.
3. テンプレート行列 T_t に関する $(n, \log_q|C_t|, d_{T_t}(C_t))$ 符号 C_t
4. 線形符号の場合, $\mathbb{F}_q$ 上の生成行列 $k \times n$ 行列 G_t を用いて、

$$C_t = \mathrm{spn}(G_t) = \{\vec{i}G_t \mid \vec{i} \in \mathbb{F}_q^k\}$$

と定義される。

符号のパラメータ (n, k, d), $n - k \geq d - 1$

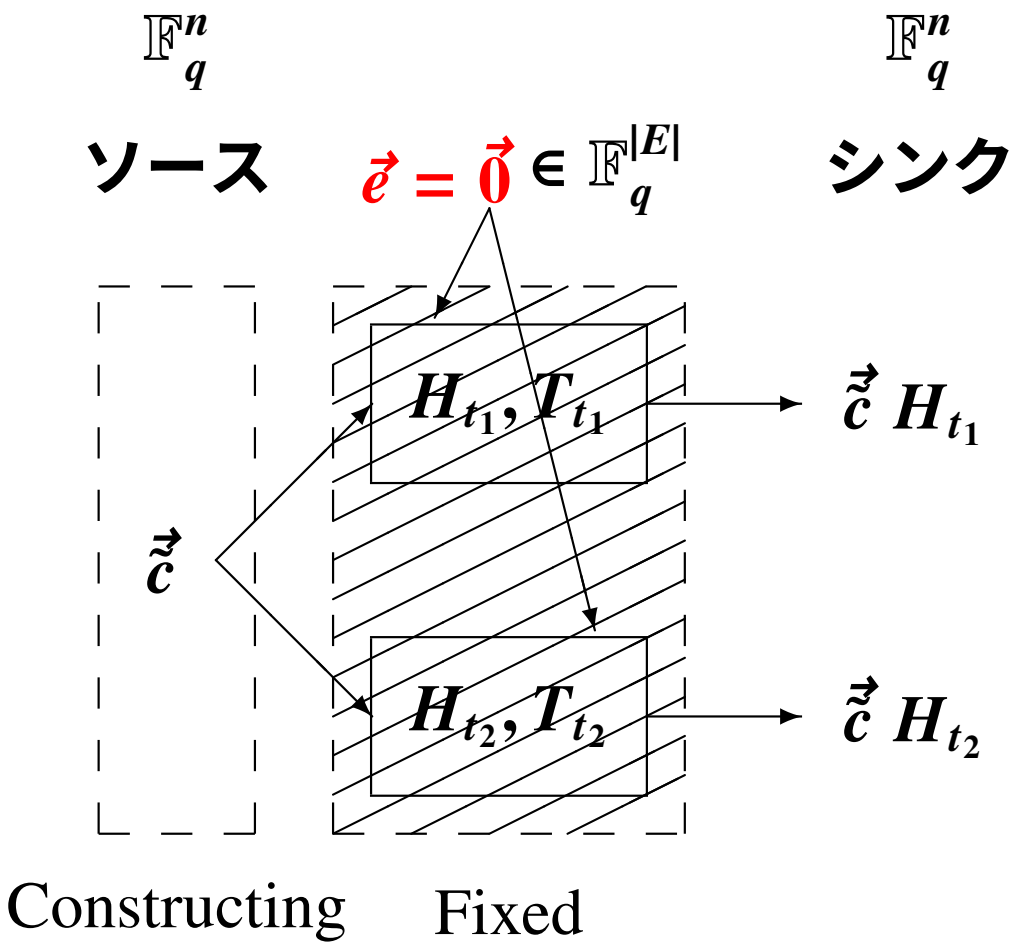
1. 与えられたパラメータ (k, d) に対し、テンプレート行列 T_t に関する $(n, k, d_{T_t}(C_t) \geq d)$ 符号 C_t を構成したい。
2. (定理)[11]
   符号 C_t の生成行列 G_t が次の (条件) を満たすならば、C_t は テンプレート行列 T_t に関する $(n, k, d_{T_t}(C_t) \geq d)$ 符号となる。
   (条件)
   1. $\mathrm{rank} G_t = k$
   2. すべての $I \in \mathcal{I}$ に対し,

$$\mathrm{spn}(G_t) \cap \mathrm{spn}(\{\vec{t}_{t,i} \mid i \in I\}) = \{\vec{0}\} \tag{3}$$

   が成り立つ.
   ただし、$\mathcal{I}$ は、添字集合 $\{1, \ldots, |E|\}$ の中から異なる $d-1$ 個を取り出して得られる部分集合 $\{i_1, \ldots, i_{d-1}\}$ の全体、すなわち、集合族である。

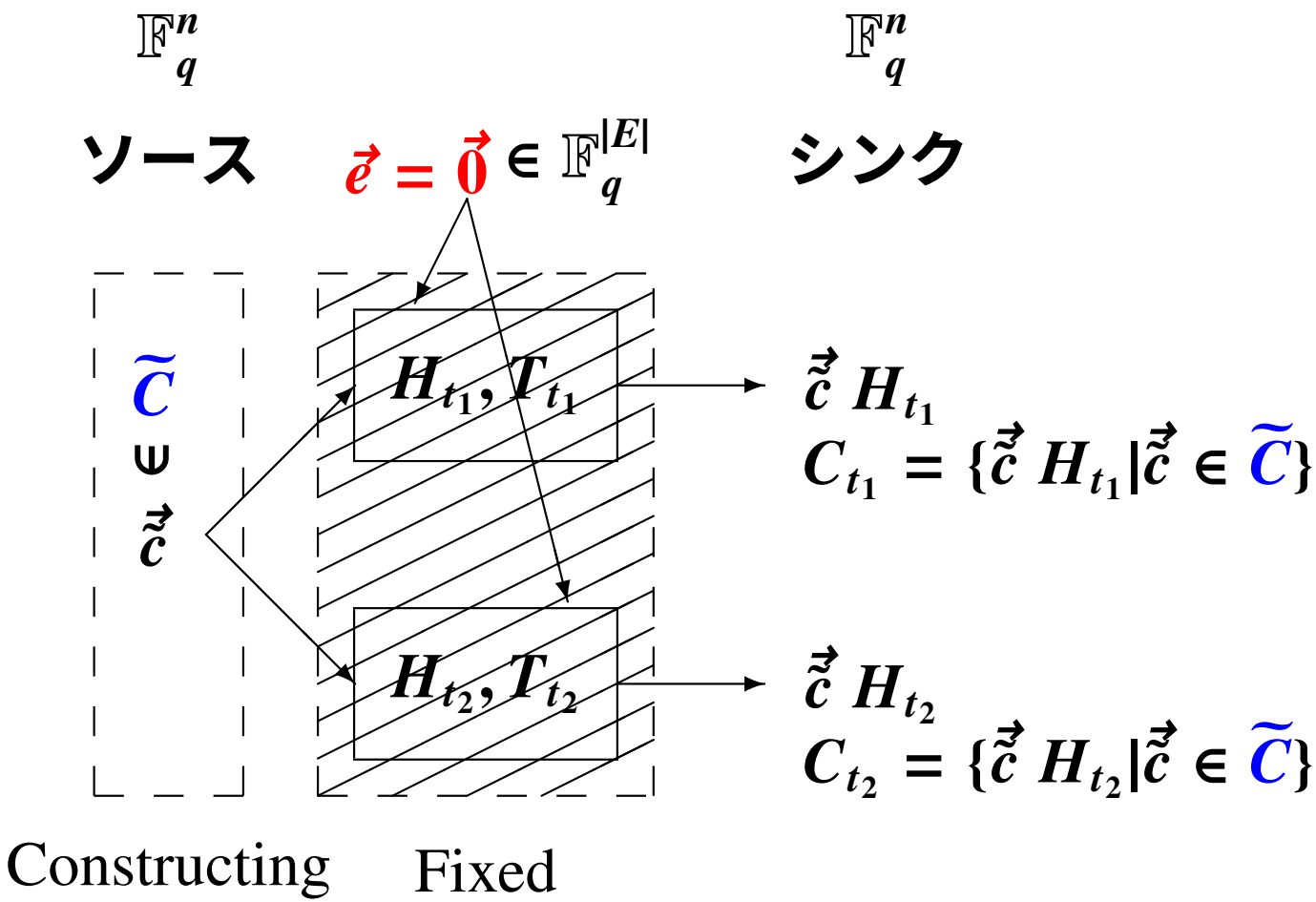
提案方法：マルチキャスト (1 対多通信モデル)

マルチキャスト誤り訂正符号 $\widetilde{C}$



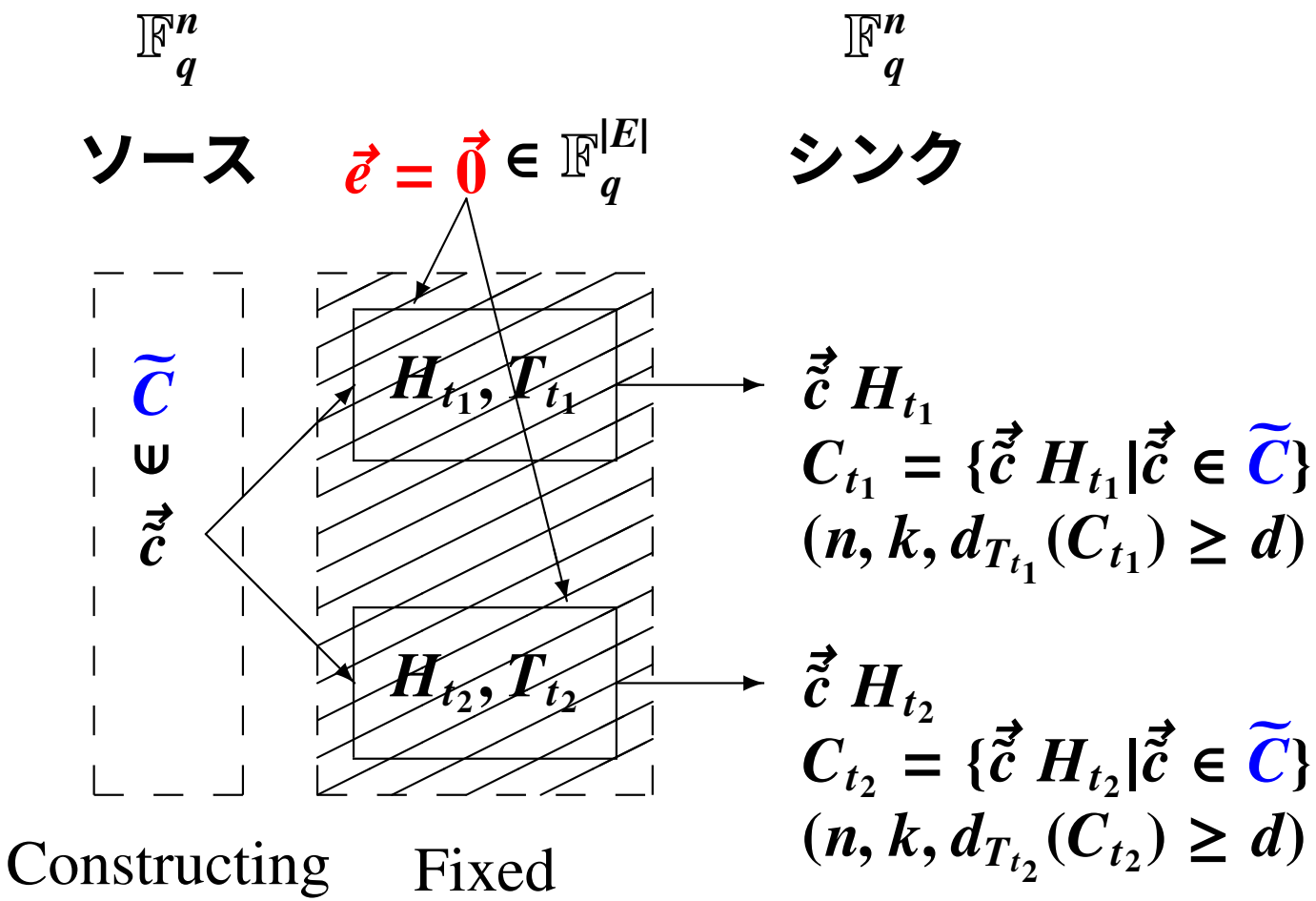
提案方法：マルチキャスト (1 対多通信モデル)

マルチキャスト誤り訂正符号 $\widetilde{C}$



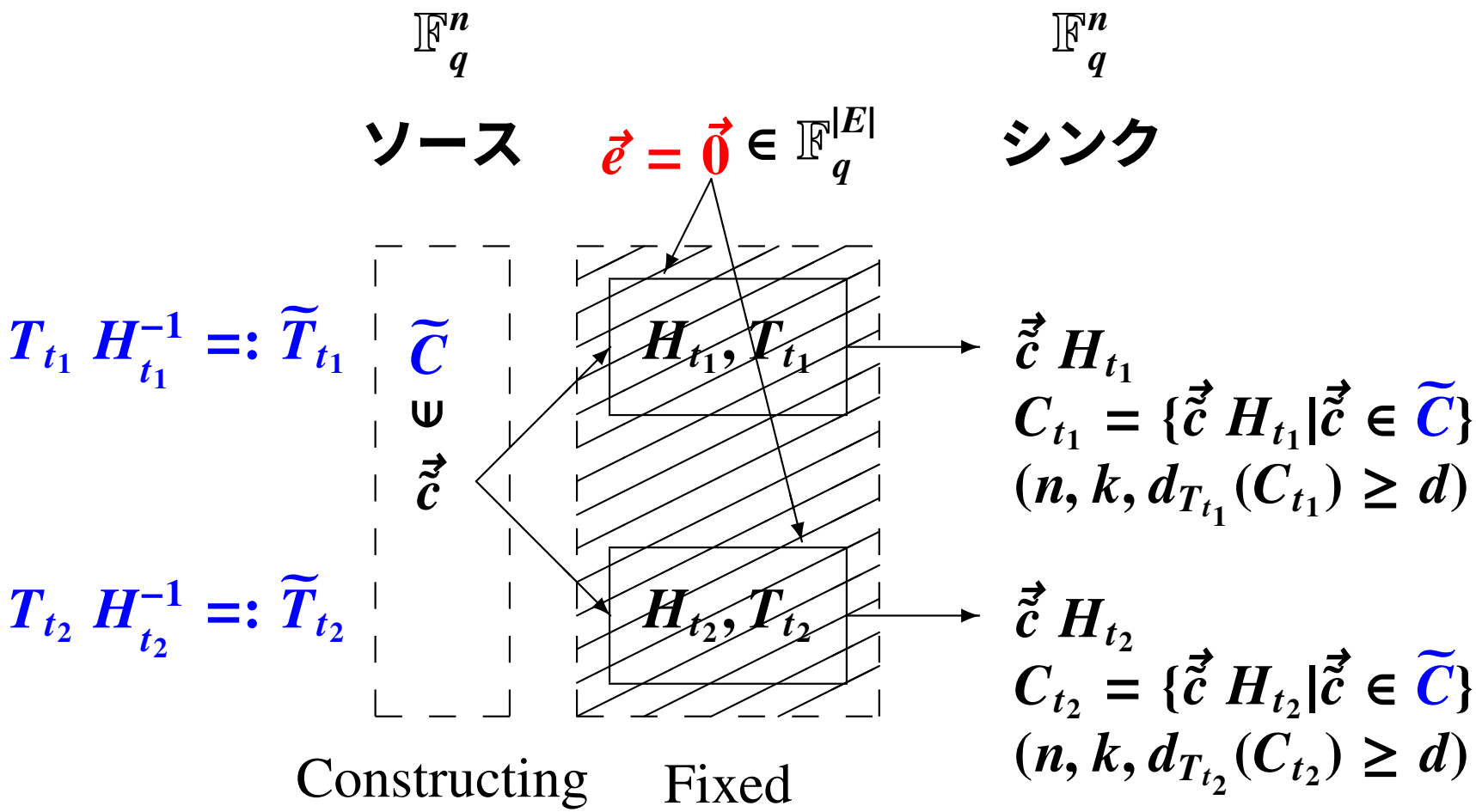
提案方法：マルチキャスト (1 対多通信モデル)

マルチキャスト誤り訂正符号 $\widetilde{C}$



提案方法：マルチキャスト (1 対多通信モデル)

マルチキャスト誤り訂正符号 $\widetilde{C}$



マルチキャスト誤り訂正符号 $\widetilde{C}$ (4 つの同値命題) 1/2

1. 符号 $\widetilde{C}$ は (n, k, d) マルチキャスト誤り訂正符号である.
2. 各シンク $t \in T$ の符号 C_t は,
   テンプレート行列 T_t に関する $(n, k, d_{T_t}(C_t) \geq d)$ 符号である.
   すなわち, 各シンク $t \in T$ に対し,
   1. $\dim C_t = k$,
   2. $d_{T_t}(C_t) \geq d$.

   が成り立つ.

マルチキャスト誤り訂正符号 $\widetilde{C}$ (4つの同値命題)2/2

1. 符号 $\widetilde{C}$ は,
   1. $\dim\widetilde{C} = k$,
   2. 各テンプレート距離 $d_{\widetilde{T}_t}$, $t \in T$, において, $d_{\widetilde{T}_t}(\widetilde{C}) \geq d$ が成り立つ

   を満たす. ただし、$\widetilde{T}_t := T_t H_t^{-1}$, $t \in T$.
2. 符号 $\widetilde{C}$ の生成行列 $\widetilde{G}$ は,
   1. $\mathrm{rank}\widetilde{G} = k$.
   2. すべての $(t, I) \in T \times \mathcal{I}$ に対し,

$$\mathrm{spn}(\widetilde{G}) \cap \mathrm{spn}(\{\vec{\widetilde{t}}_{t,i} | i \in I\}) = \{\vec{0}\} \tag{4}$$

   が成り立つ

   を満たす. ただし、$\vec{\widetilde{t}}_{t,i}$ は $\widetilde{T}_t$ の行ベクトルを表す。

生成行列 $\widetilde{G}$ の構成アルゴリズム

1. 符号 $\widetilde{C}$ の生成行列 $\widetilde{G}$ は, 次の条件を満たす.
   1. $\mathrm{rank}\widetilde{G} = k$.
   2. すべての $(t, I) \in T \times \mathcal{I}$ に対し,

$$\mathrm{spn}(\widetilde{G}) \cap \mathrm{spn}(\{\vec{\tilde{t}}_{t,i} | i \in I\}) = \{\vec{0}\} \tag{5}$$

      が成り立つ.
2. [12] 栗原正純,
   “セキュアネットワーク符号化アルゴリズム
   —条件付き正則行列の構成アルゴリズム (I)— ,”
   SITA2006 予稿集, pp.763–766, 函館, 12 月 1 日, 2006.

まとめ

1. ネットワークコーディングにおける誤り訂正に対応するテンプレート距離を示した。
2. (n, k, d) マルチキャスト誤り訂正符号 $\widetilde{C}$ とその生成行列 $\widetilde{G}$ を示した。
3. 生成行列 $\widetilde{G}$ の構成アルゴリズムはセキュアネットワーク符号の構成アルゴリズムを利用できることを説明した。

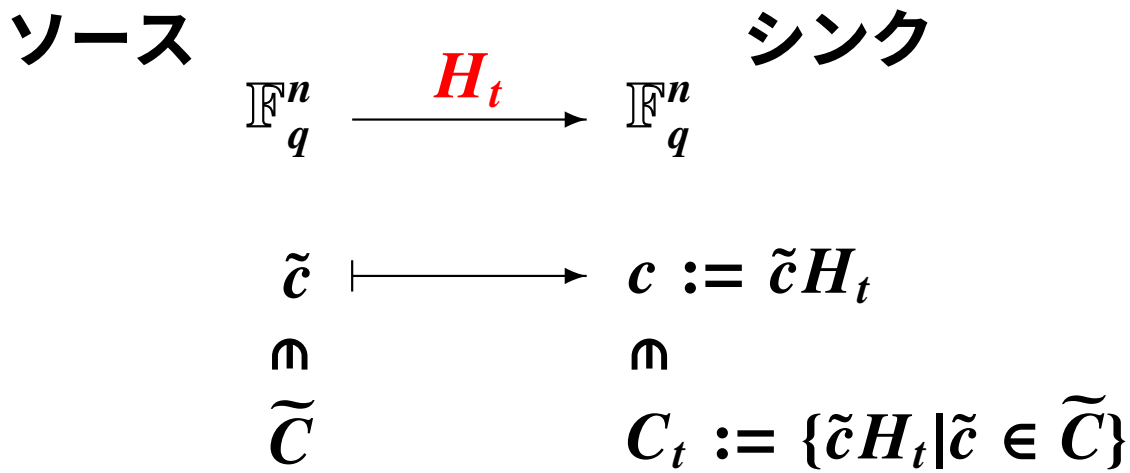
ソース s とシンク t のそれぞれの符号の関係 additional sheet

ソース　　シンク

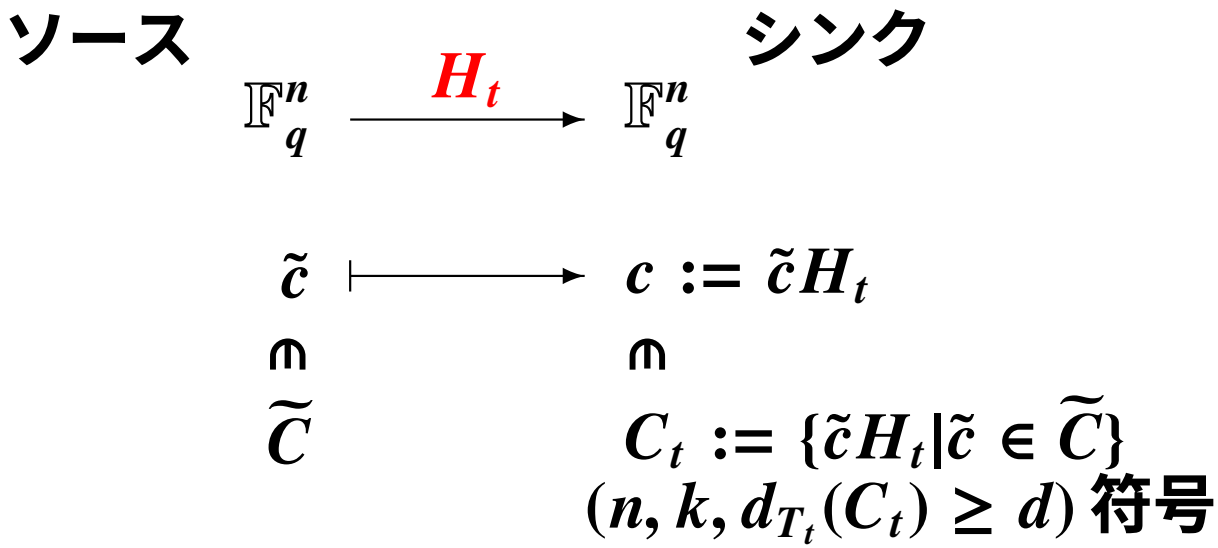
$$\mathbb{F}_q^n \xrightarrow{H_t} \mathbb{F}_q^n$$

$$\tilde{c} \longmapsto c := \tilde{c}H_t$$

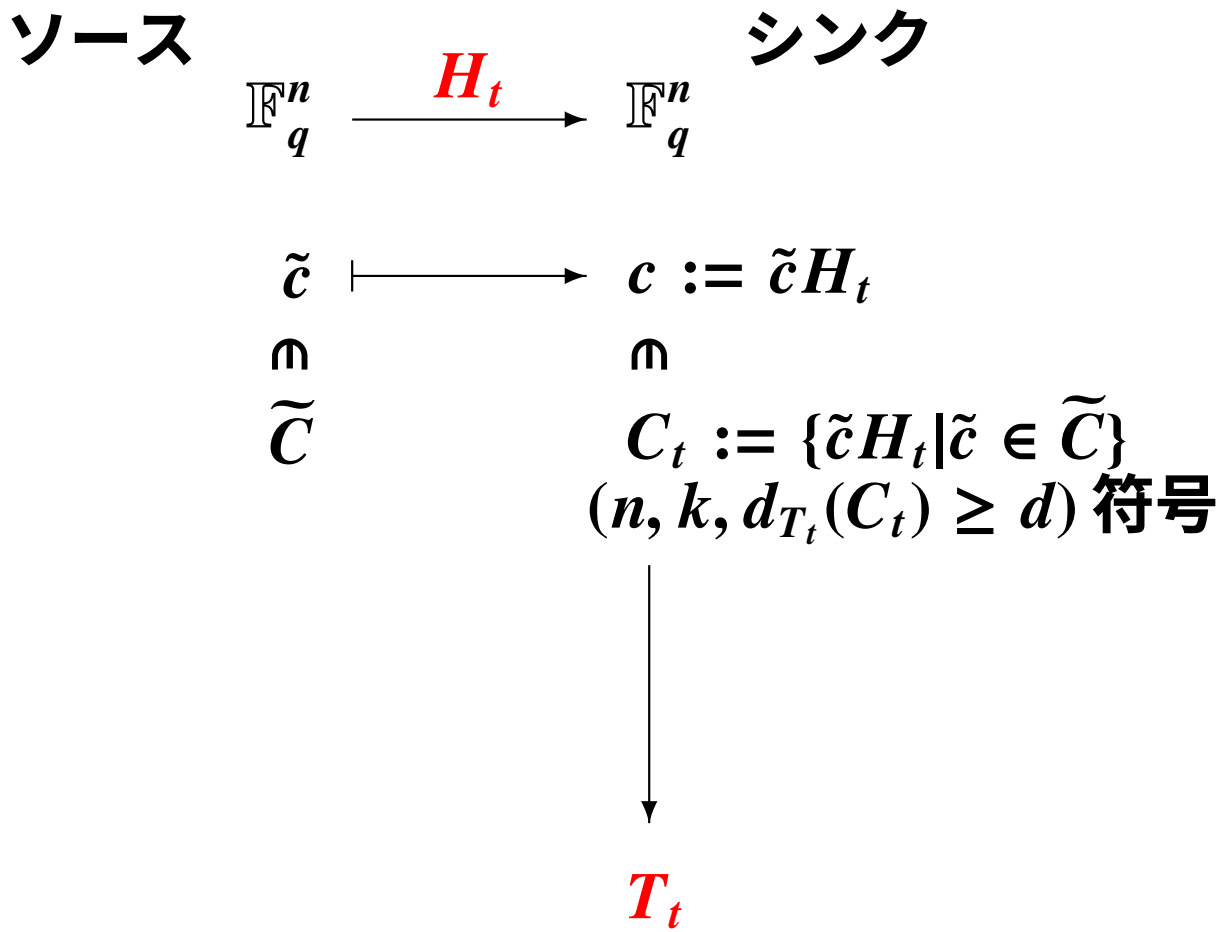
ソース s とシンク t のそれぞれの符号の関係 additional sheet



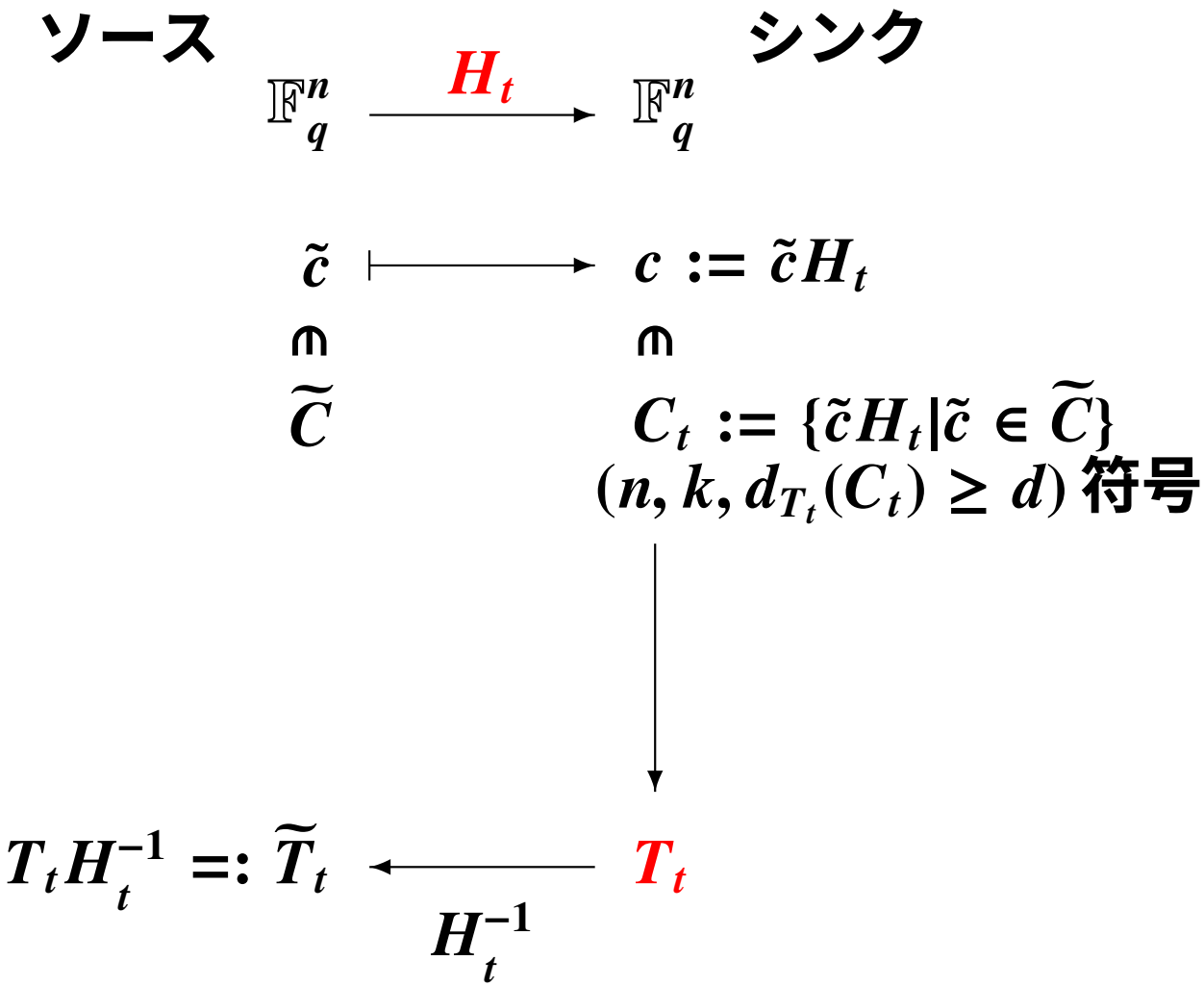
ソース s とシンク t のそれぞれの符号の関係 additional sheet



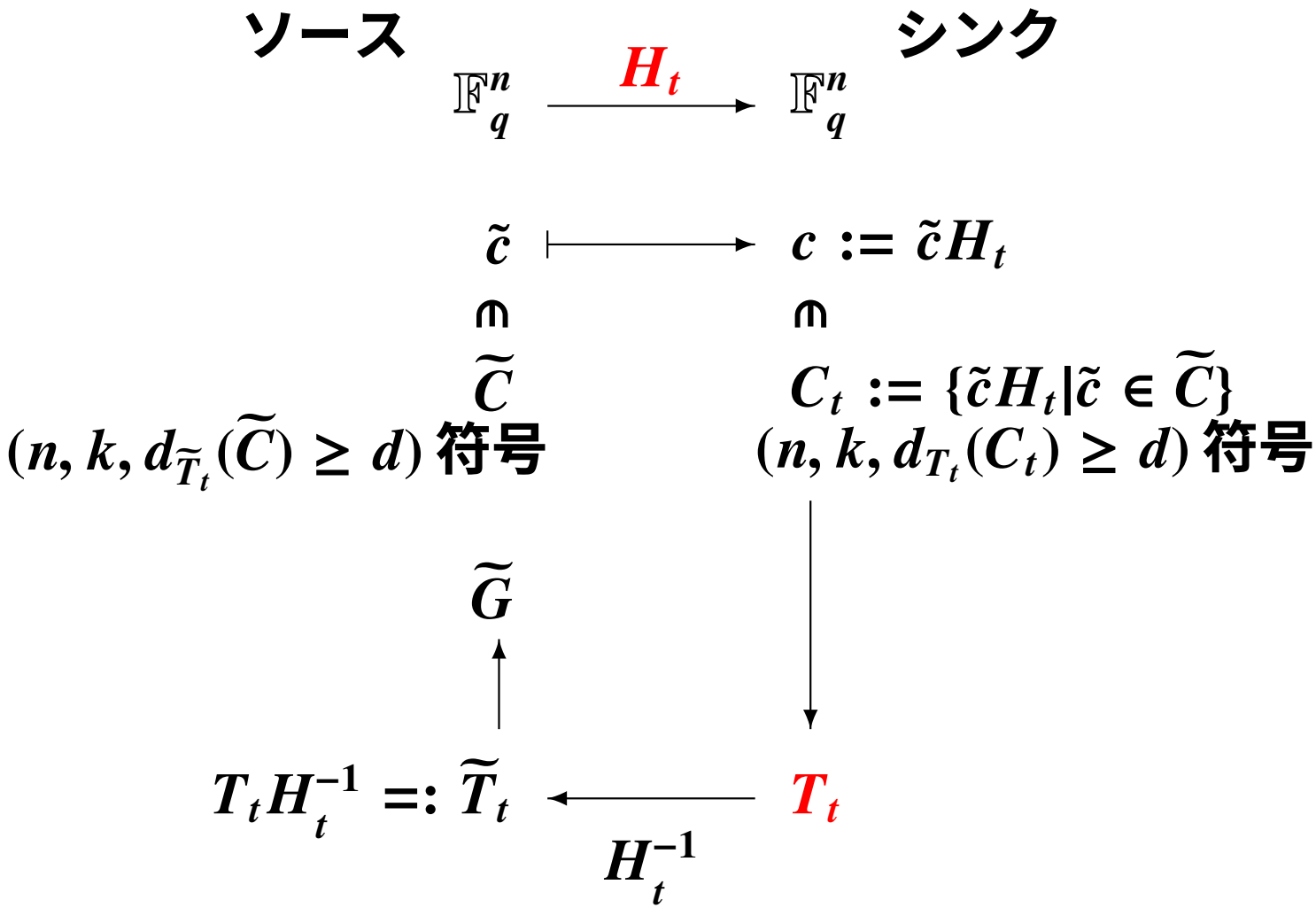
ソース s とシンク t のそれぞれの符号の関係 additional sheet



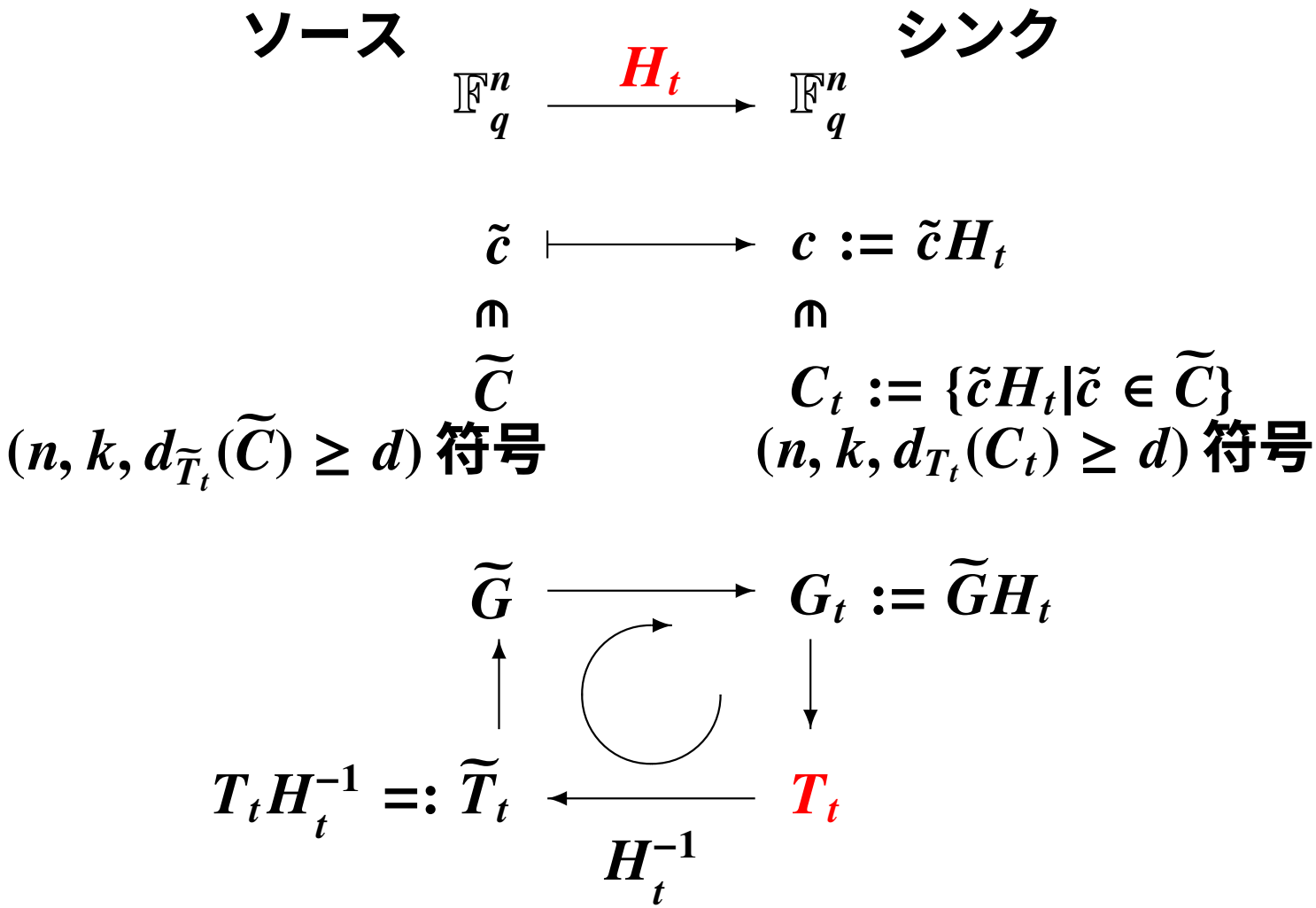
ソース s とシンク t のそれぞれの符号の関係 additional sheet



ソース s とシンク t のそれぞれの符号の関係 additional sheet

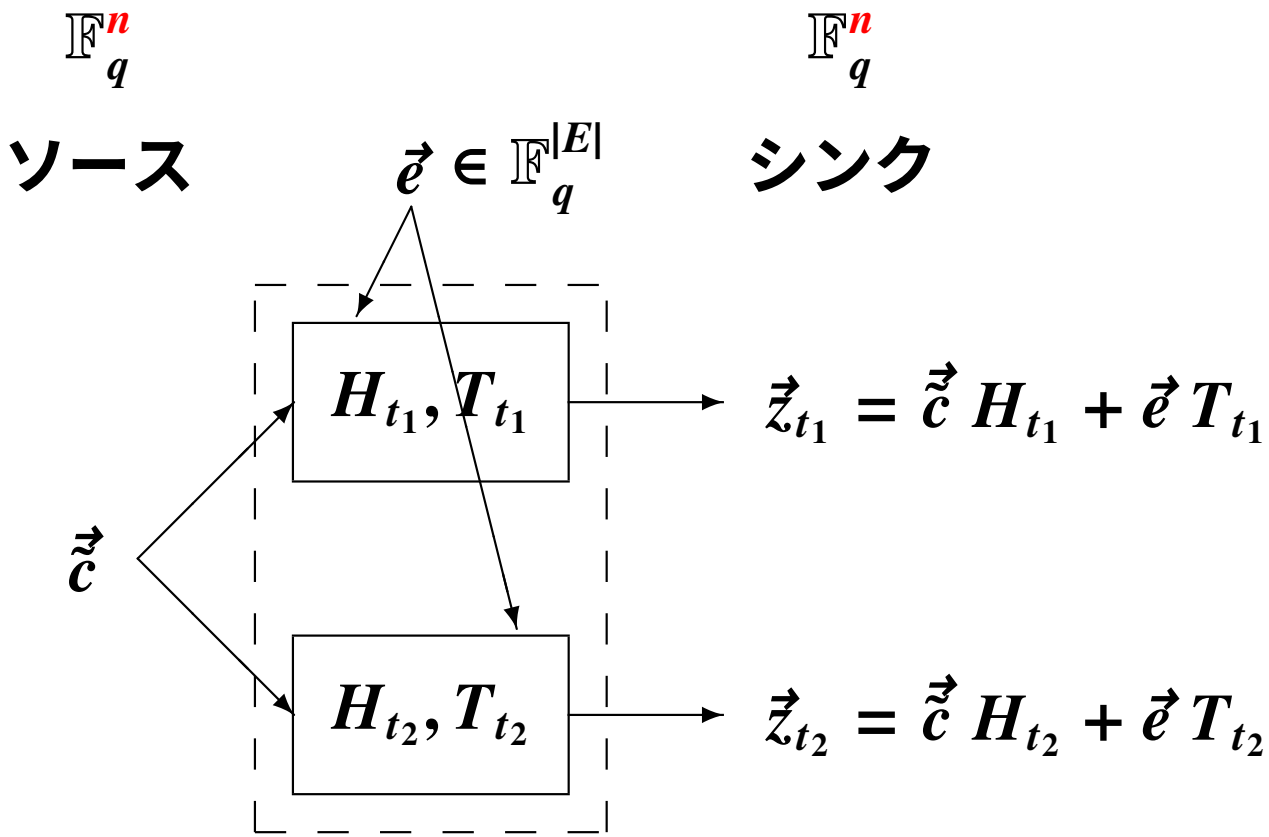


ソース s とシンク t のそれぞれの符号の関係 additional sheet



マルチキャスト (1 対多通信モデル) additional sheet

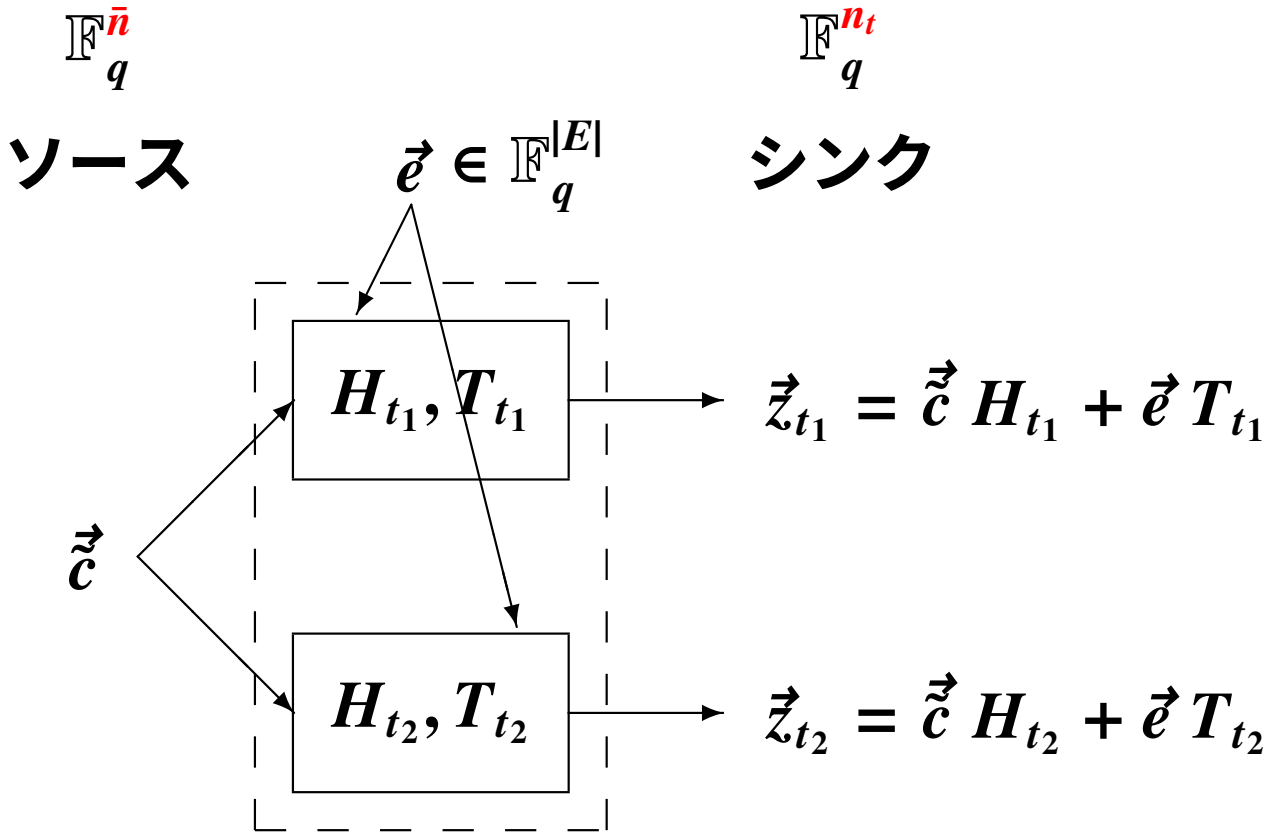
Codes attaining the Singleton Bound



- $n = \min\{n_t \mid t \in T\}$
- H_t : 伝送行列 (情報 (送信シンボル列) を伝送する行列)
- T_t : テンプレート行列 (誤りを伝送する行列)

一般化マルチキャスト (1 対多通信モデル) additional sheet

Codes attaining the Redefined Singleton Bound



- $\bar{n} = \max\{n_t \mid t \in T\}$
- H_t : 伝送行列 (情報 (送信シンボル列) を伝送する行列)
- T_t : テンプレート行列 (誤りを伝送する行列)