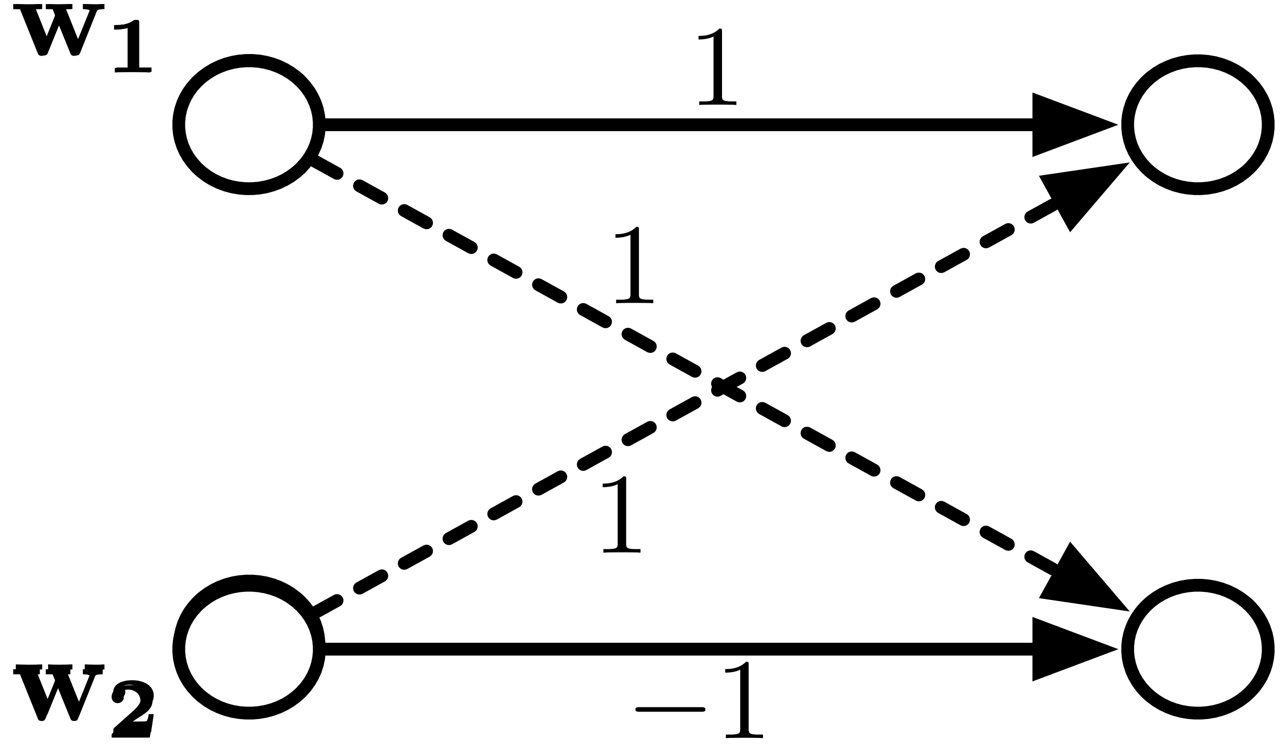
Inverse Compute-and-Forward: Extracting Messages from Simultaneously Transmitted Equations

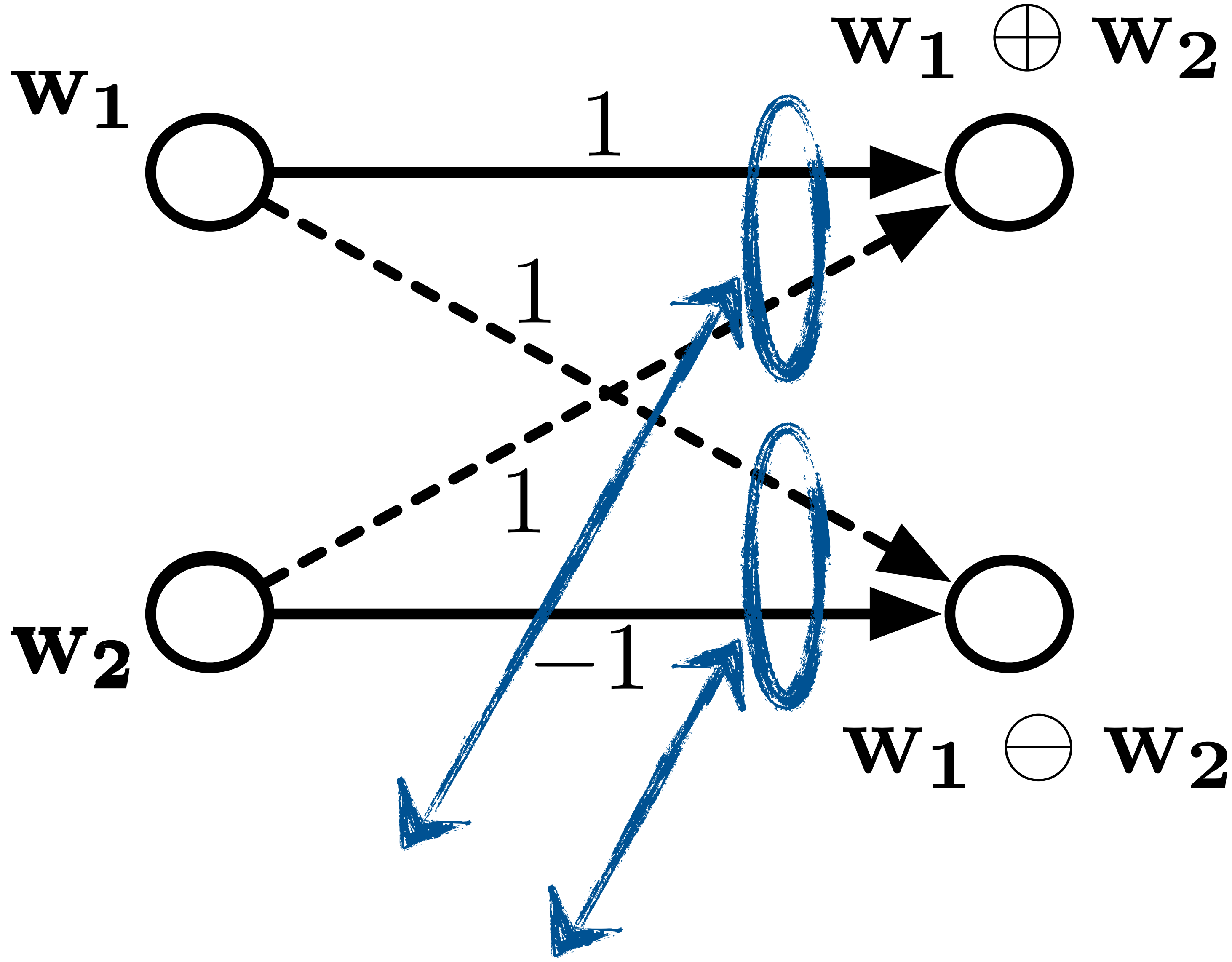
Yiwei Song, Natasha Devroye *(University of Illinois at Chicago)*
Bobak Nazer *(Boston University)*

BU Electrical & Computer Engineering

UIC UNIVERSITY OF ILLINOIS AT CHICAGO Department of Electrical and Computer Engineering
COLLEGE OF ENGINEERING

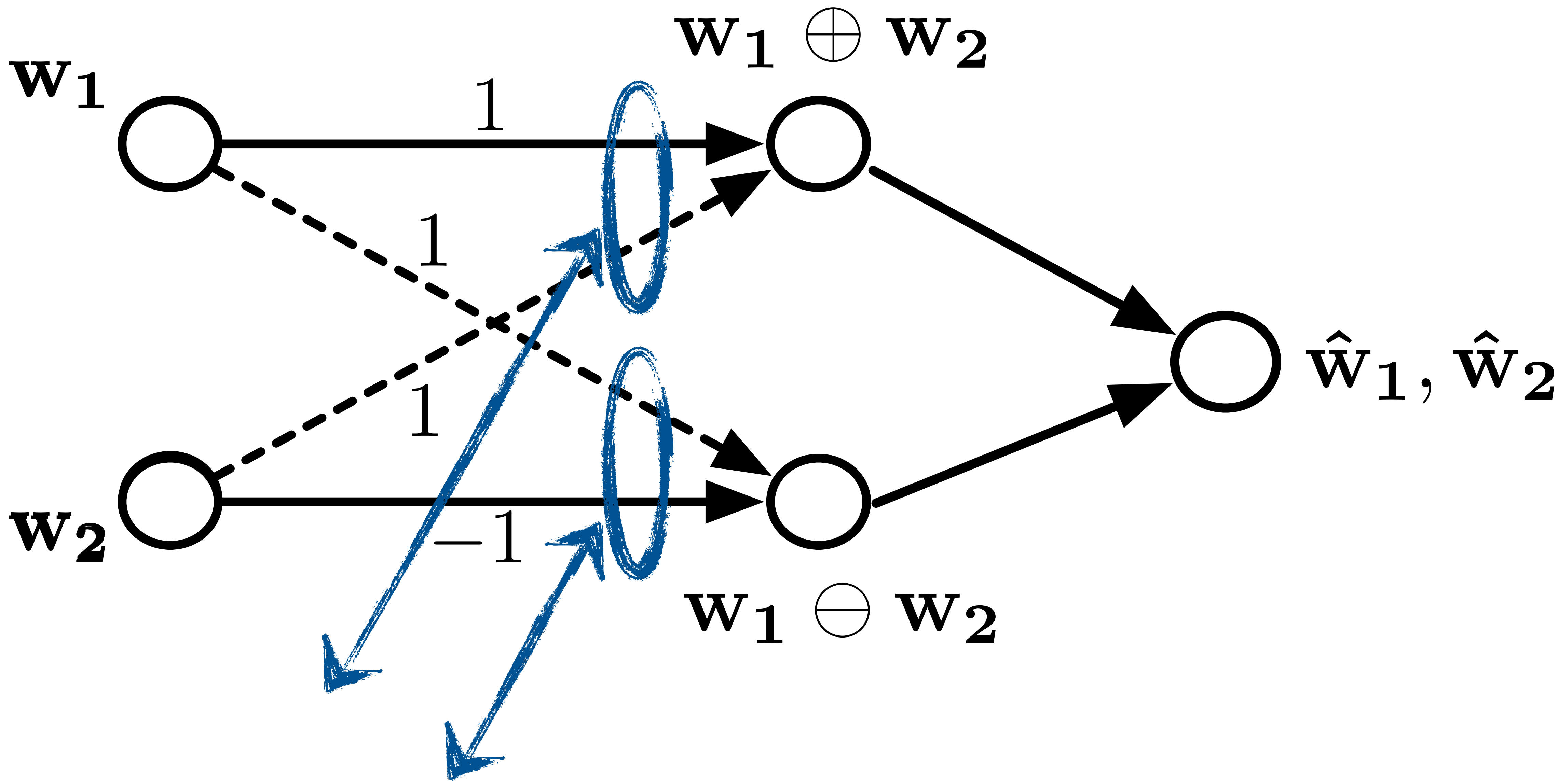

$\mathbf{w}_1$
$\mathbf{w}_2$


$\mathbf{w_1}$
1
1
1
$\mathbf{w_2}$
-1



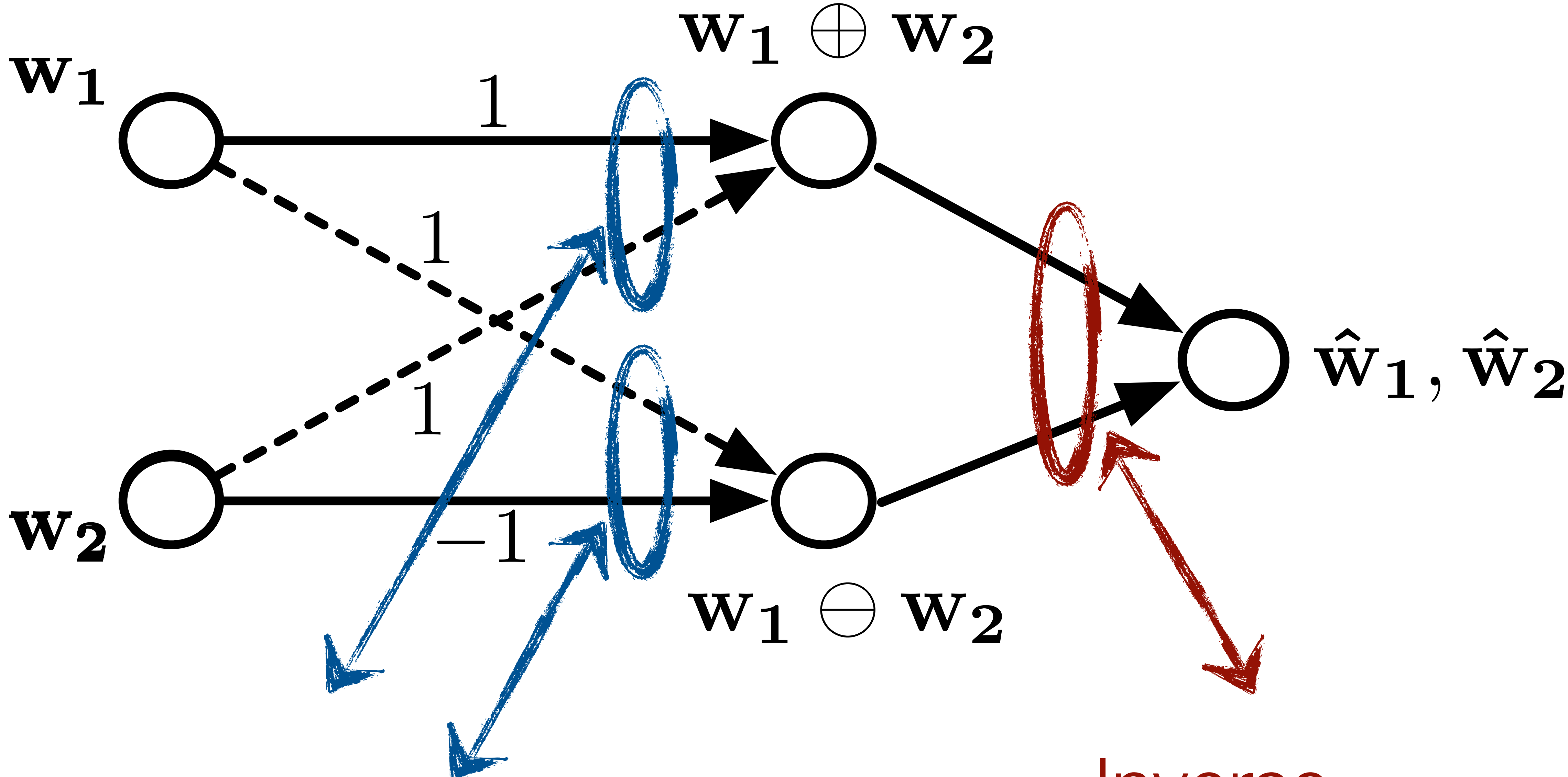
Compute and forward

[Nazer, Gastpar, 2011]



Compute and forward

[Nazer, Gastpar, 2011]



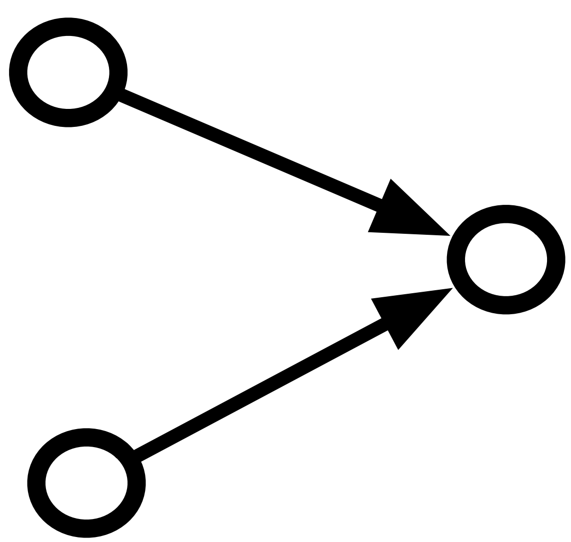
Compute and forward

[Nazer, Gastpar, 2011]

Inverse
Compute and forward

Key idea

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

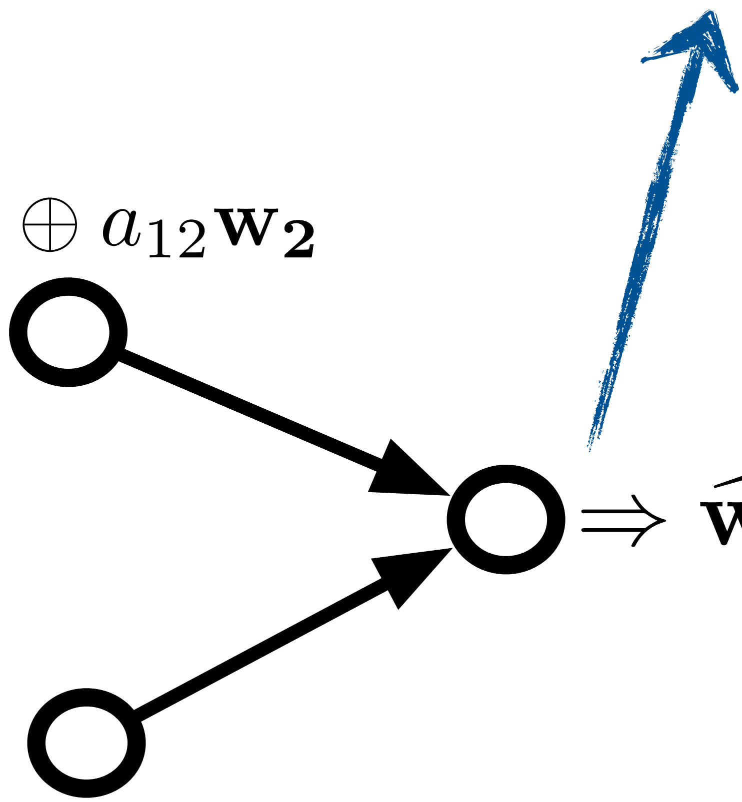
$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

Key idea

Option 1: transmit equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

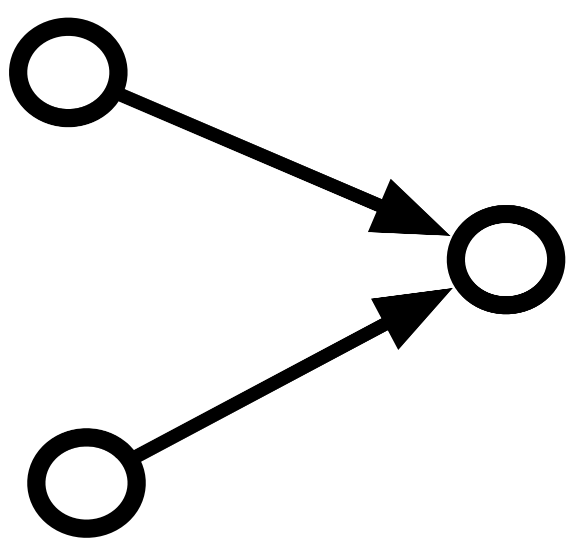
Key idea

Option 1: transmit equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

(if matrix A invertible)

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

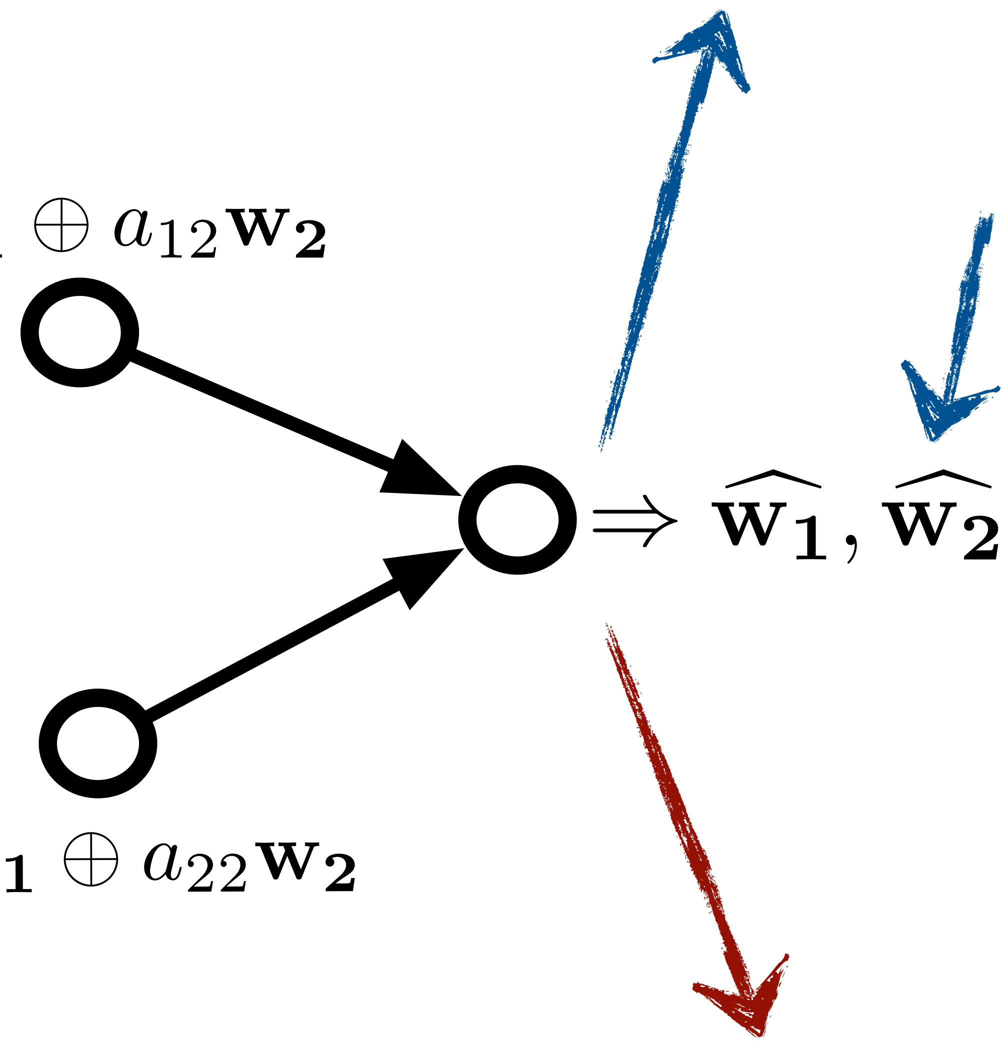
Key idea

Option 1: transmit equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

(if matrix A invertible)

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

Option 2: extract directly over the air!

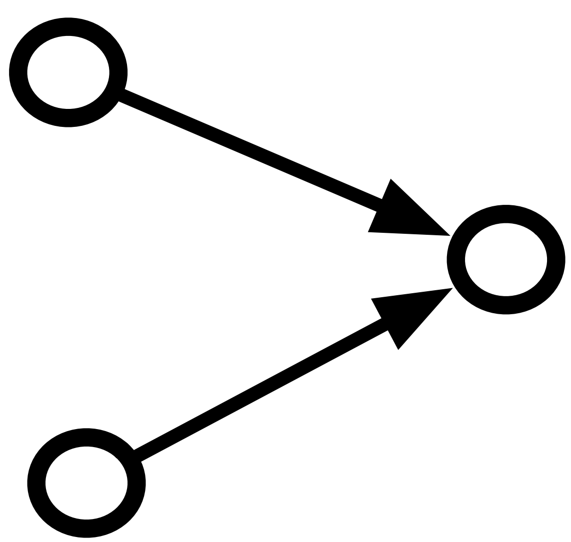
Key idea

Option 1: transmit equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

(if matrix A invertible)

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

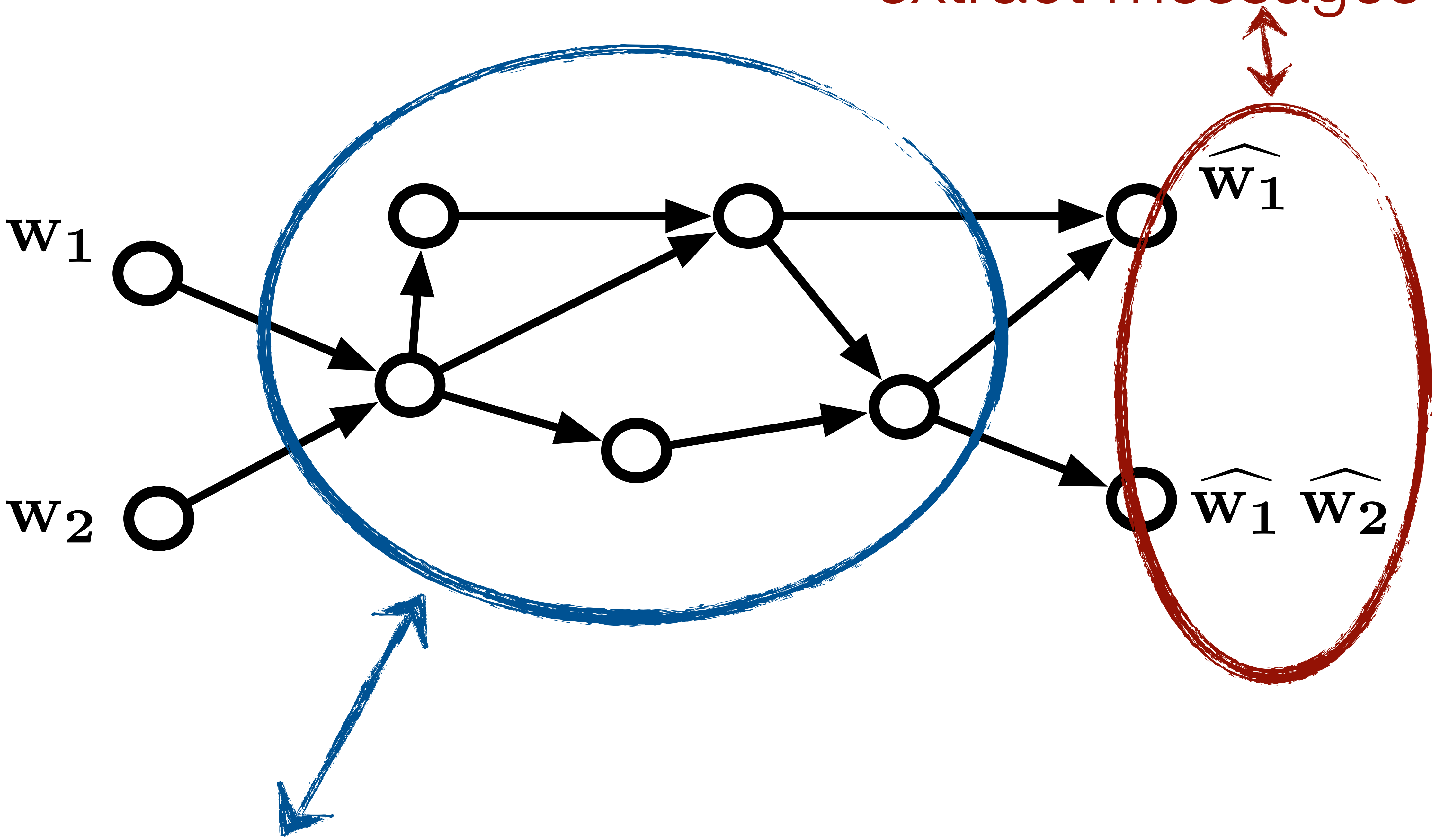
$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

(allowable equations or MAC with common messages)

Option 2: extract directly over the air!

Combine for a unified rate region!

Inverse
Compute and forward to extract messages



Compute and forward to decode $a\mathbf{w_1} \oplus b\mathbf{w_2}$

Outline

Outline

- Problem statement

Outline

- Problem statement

- Approach 1: allowable equations

Outline

- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages

Outline

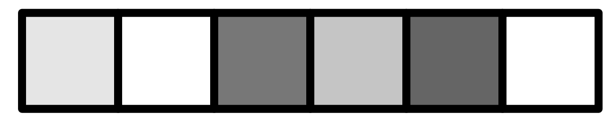
- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users

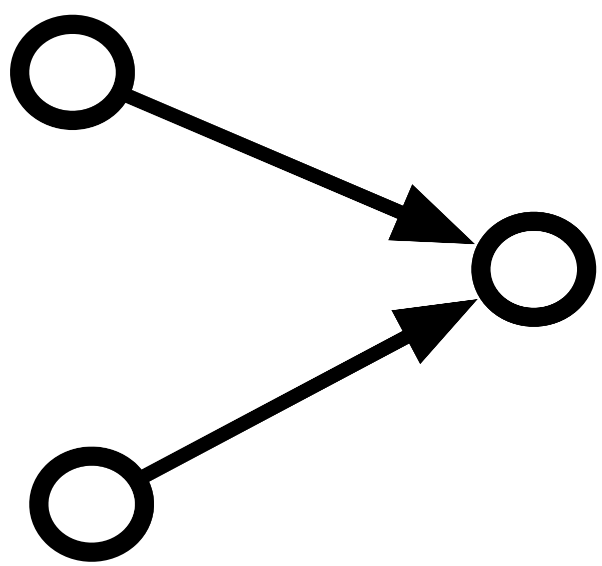
Outline

- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users
- Case study

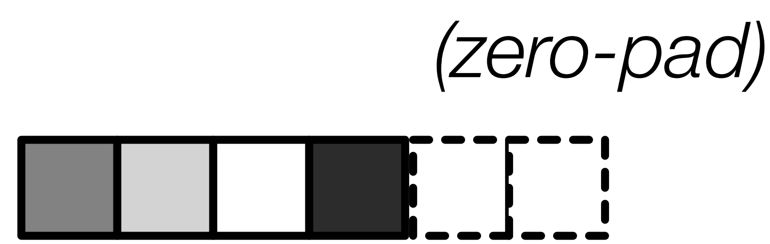
Problem statement

$\mathbf{w}_1 \in \mathbb{F}_q^{k_1}$, for q prime, $k_1 = \frac{nR_1}{\log_2 q}$



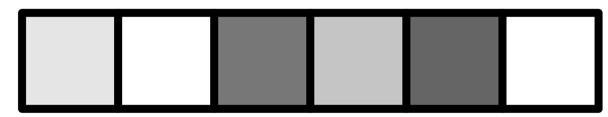


$\mathbf{w}_2 \in \mathbb{F}_q^{k_2}$, for q prime, $k_2 = \frac{nR_2}{\log_2 q}$

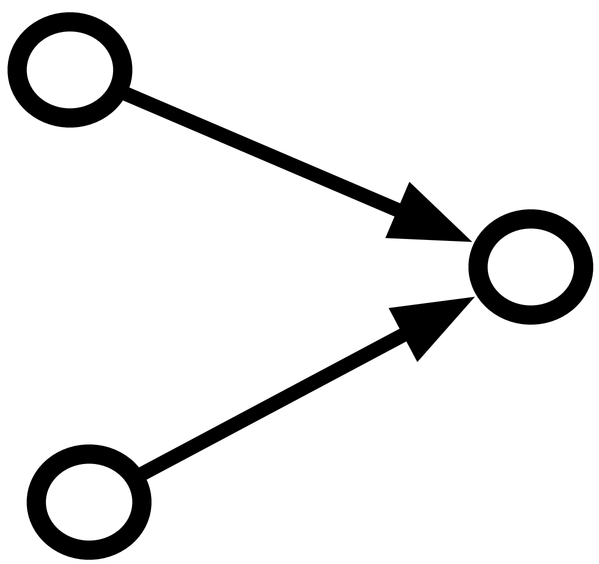


Problem statement

$\mathbf{w}_1 \in \mathbb{F}_q^{k_1}$, for q prime, $k_1 = \frac{nR_1}{\log_2 q}$



$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

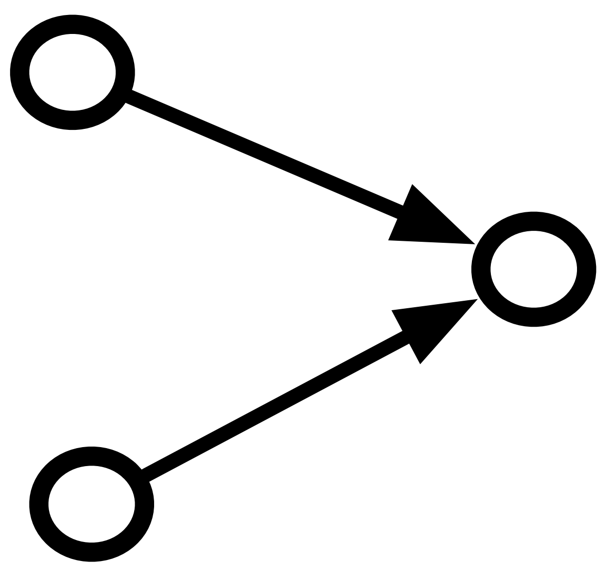
(zero-pad)

$\mathbf{w}_2 \in \mathbb{F}_q^{k_2}$, for q prime, $k_2 = \frac{nR_2}{\log_2 q}$

Problem statement

$\mathbf{w}_1 \in \mathbb{F}_q^{k_1}$, for q prime, $k_1 = \frac{nR_1}{\log_2 q}$

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



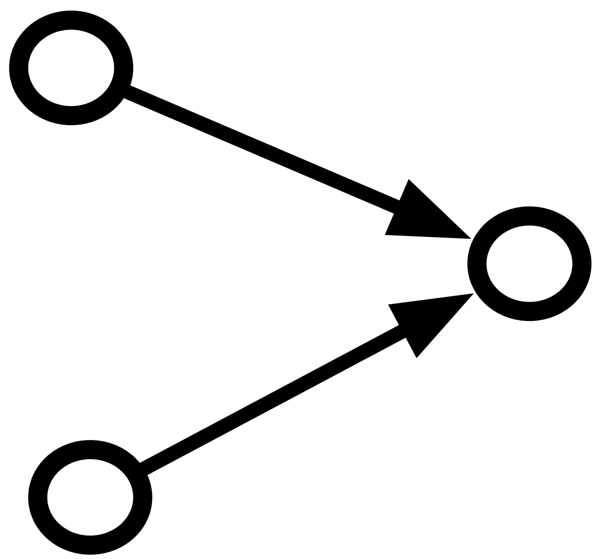
$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

- $\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ is full rank over $\mathbb{F}_q$.
- $\oplus$ denotes finite field addition

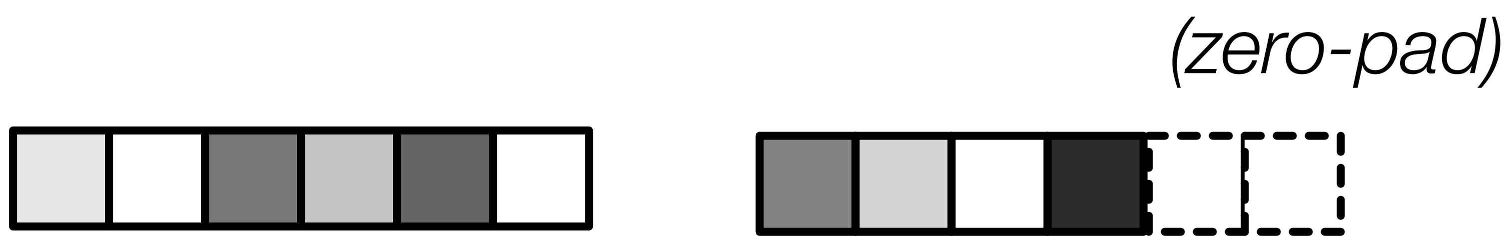
$\mathbf{w}_2 \in \mathbb{F}_q^{k_2}$, for q prime, $k_2 = \frac{nR_2}{\log_2 q}$

Problem statement

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



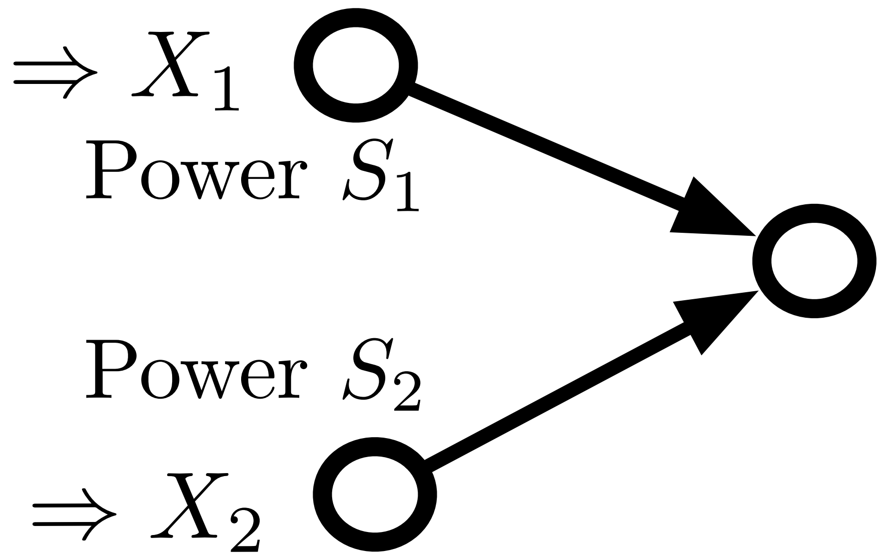
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$



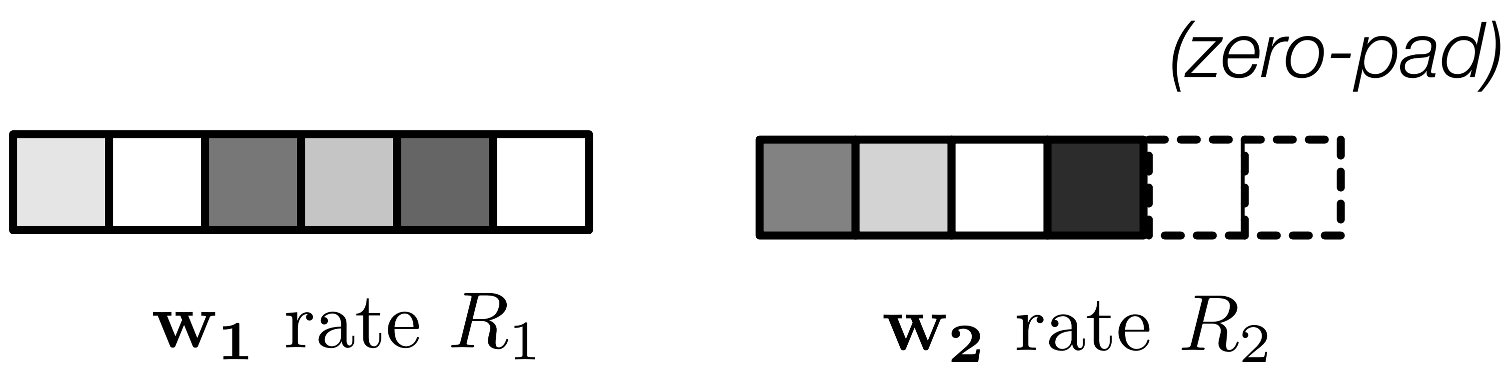
$\mathbf{w_1}$ rate R_1 $\mathbf{w_2}$ rate R_2

Problem statement

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

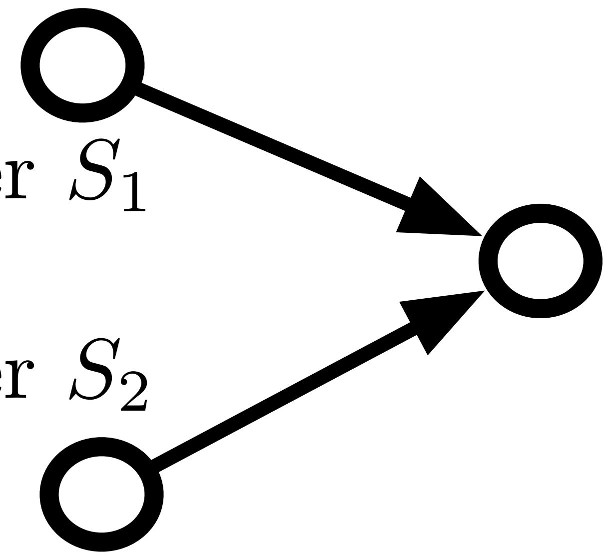


Problem statement

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$

$\Rightarrow X_1$

Power S_1



Power S_2

$\Rightarrow X_2$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

$$Y = X_1 + X_2 + Z$$

$$Z \sim \mathcal{N}(0,1)$$

(zero-pad)

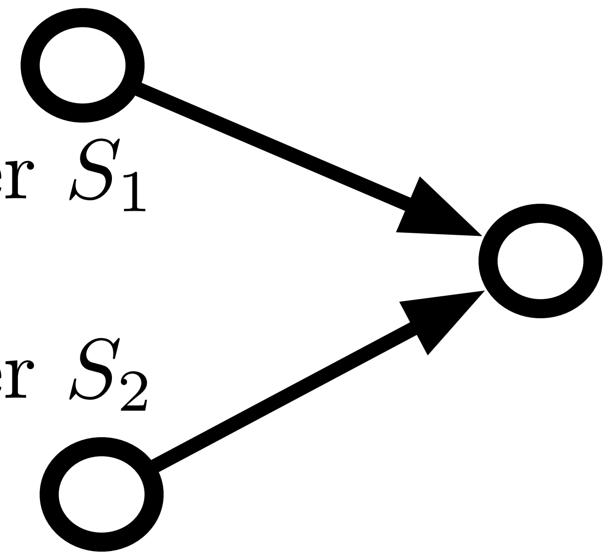
$\mathbf{w_1}$ rate R_1 $\mathbf{w_2}$ rate R_2

Problem statement

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$

$\Rightarrow X_1$

Power S_1



Power S_2

$\Rightarrow X_2$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

$$Y = X_1 + X_2 + Z$$

$$Z \sim \mathcal{N}(0,1)$$

$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\Pr((\hat{\mathbf{w}}_1, \hat{\mathbf{w}}_2) \neq (\mathbf{w}_1, \mathbf{w}_2)) < \epsilon\ .$$

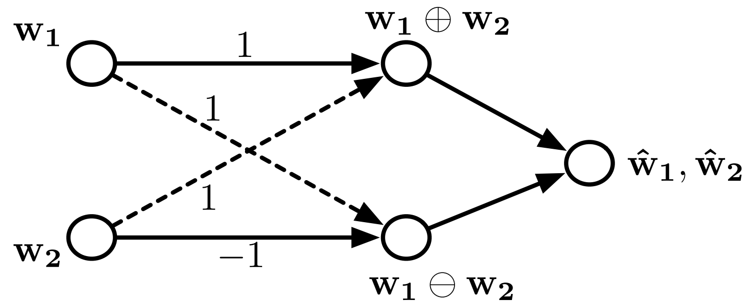
(zero-pad)

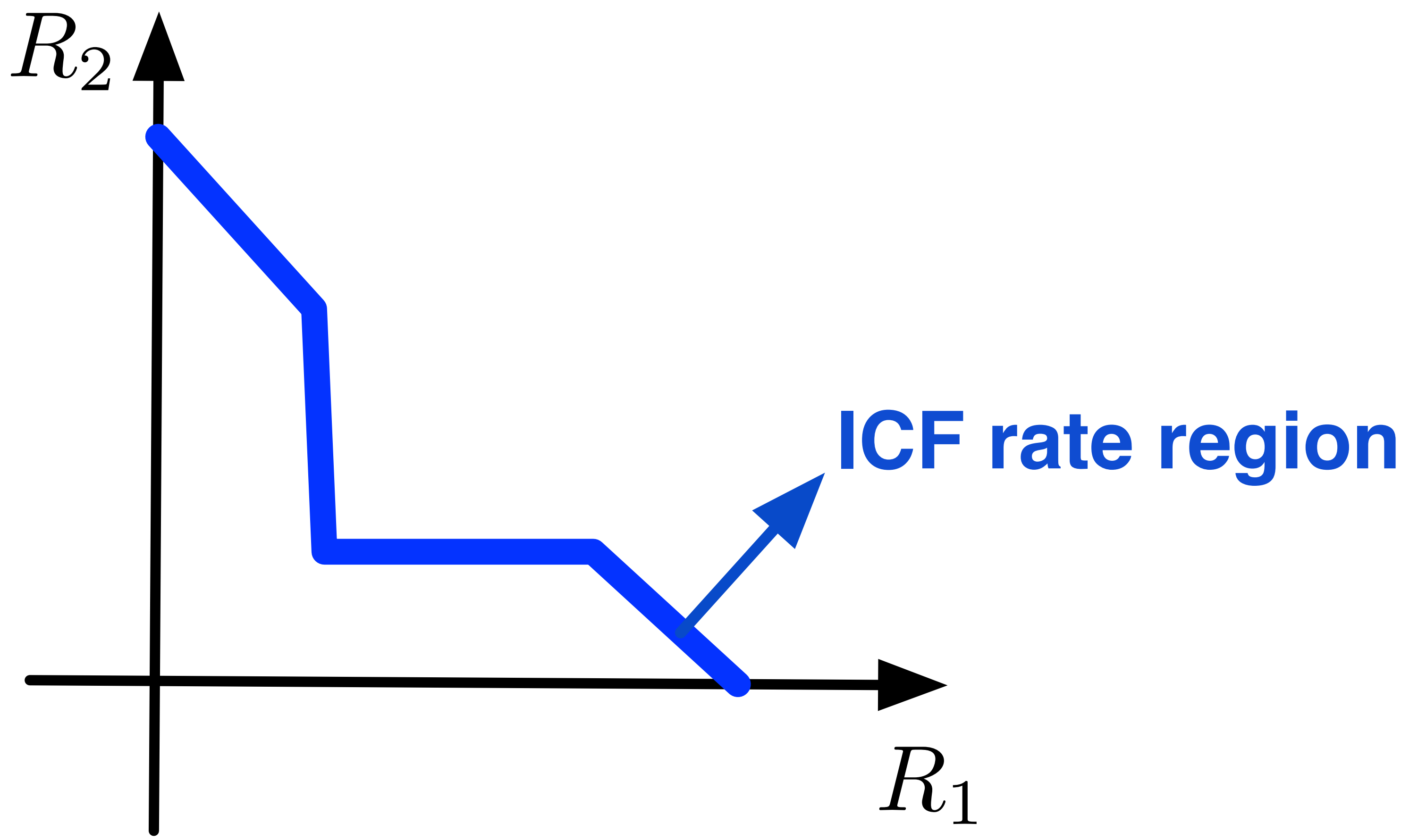
$\mathbf{w_1}$ rate R_1 $\qquad$ $\mathbf{w_2}$ rate R_2

Outline

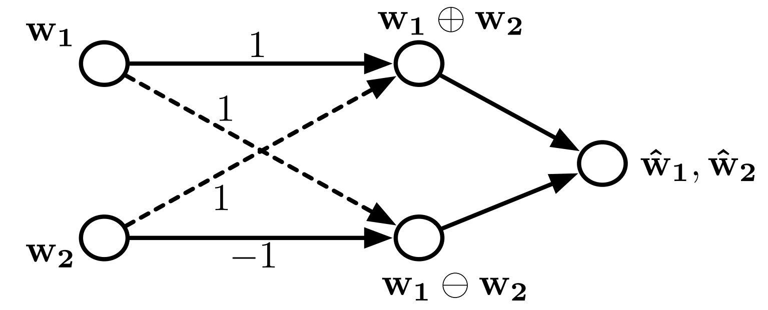
- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users
- Case study

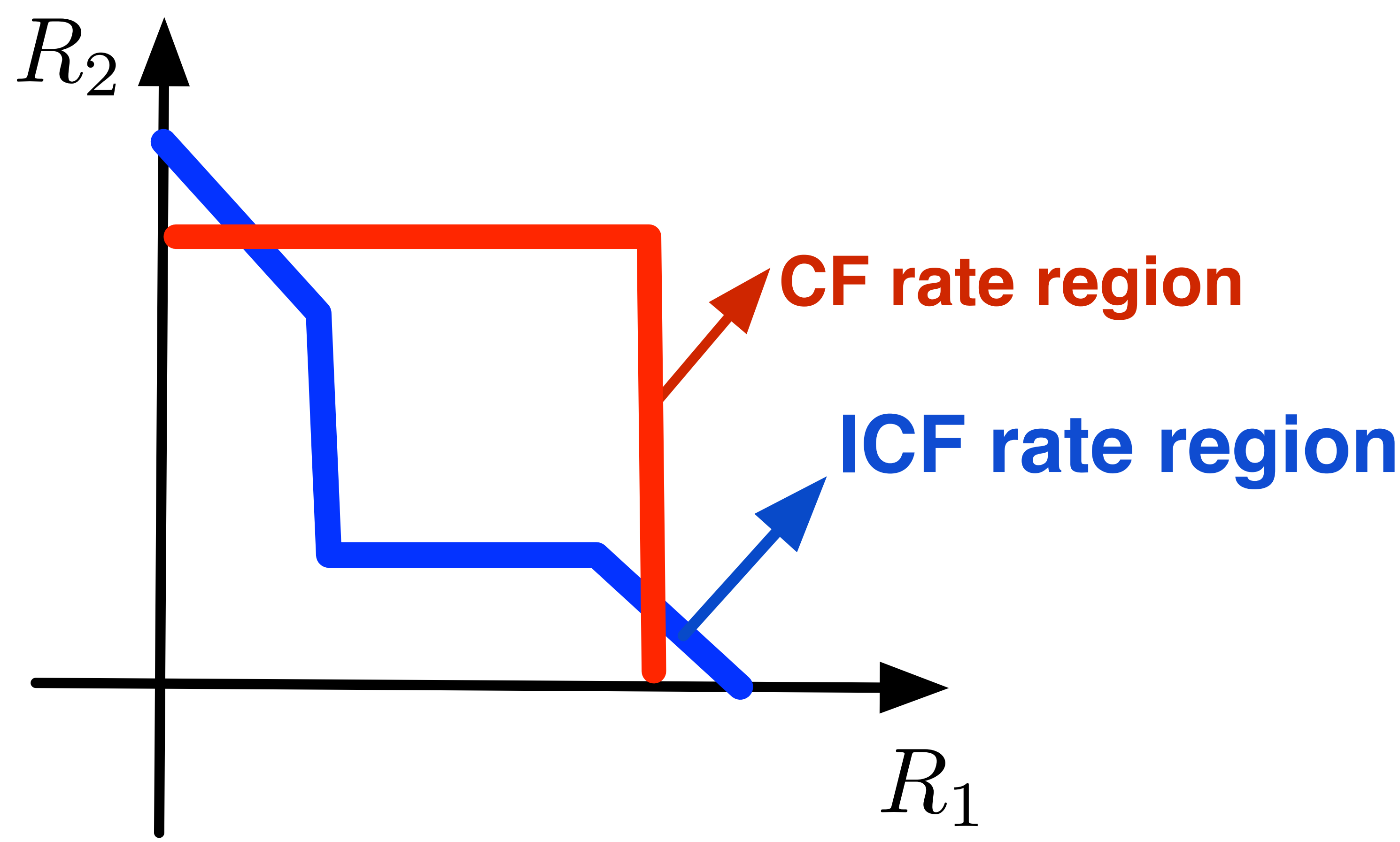
Goal - derive ICF rate region



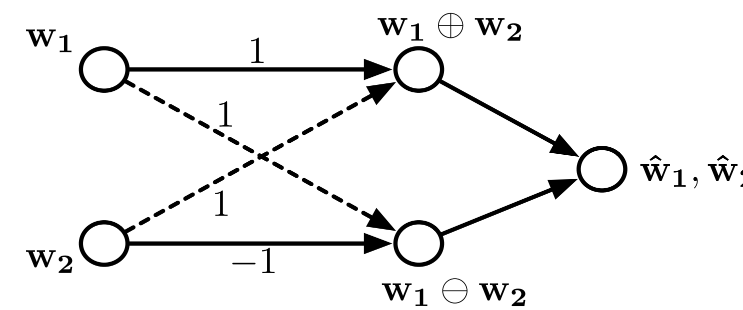


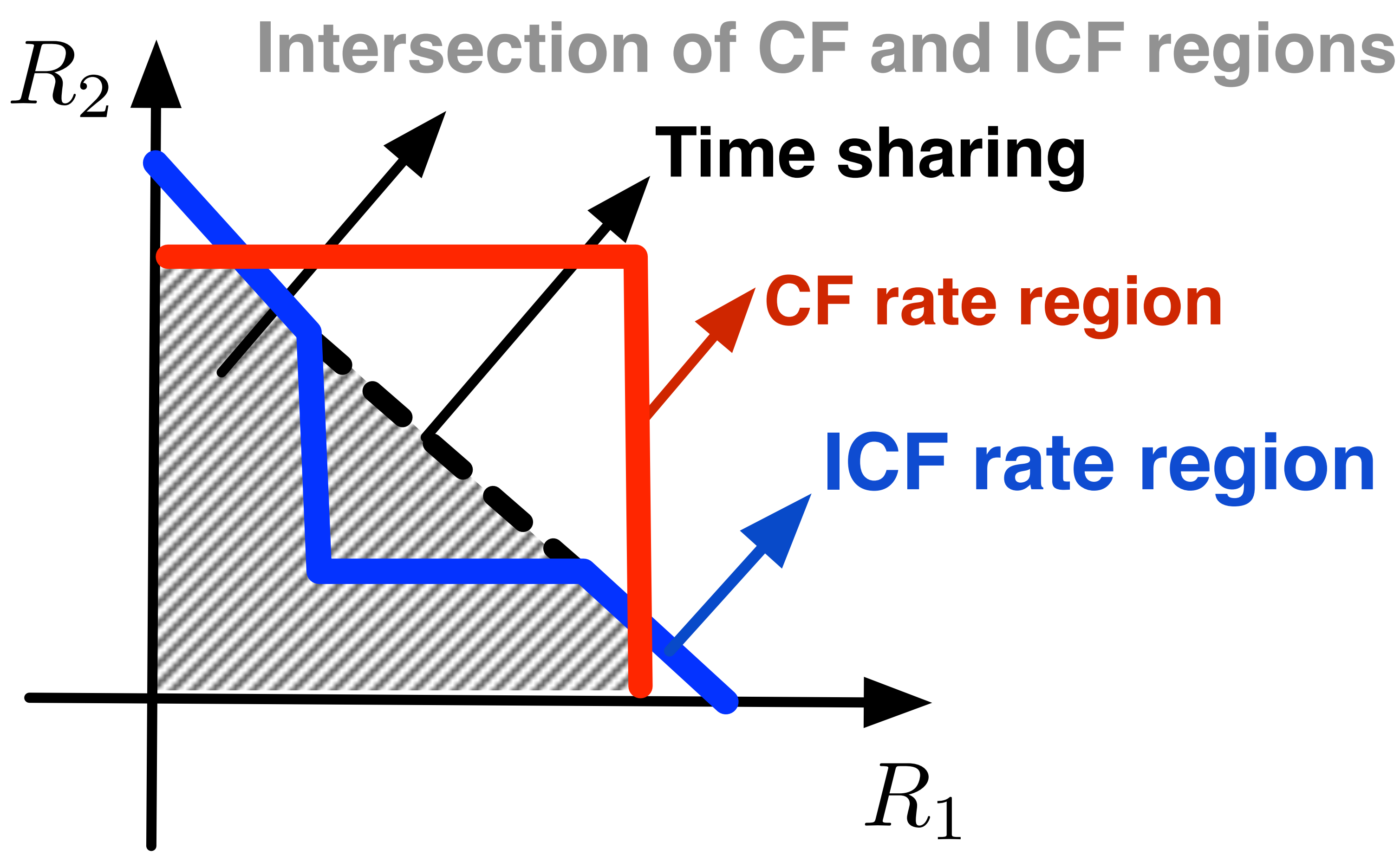
Goal - derive ICF rate region



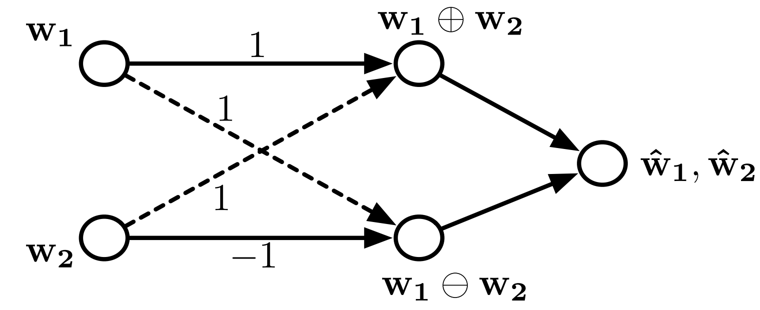


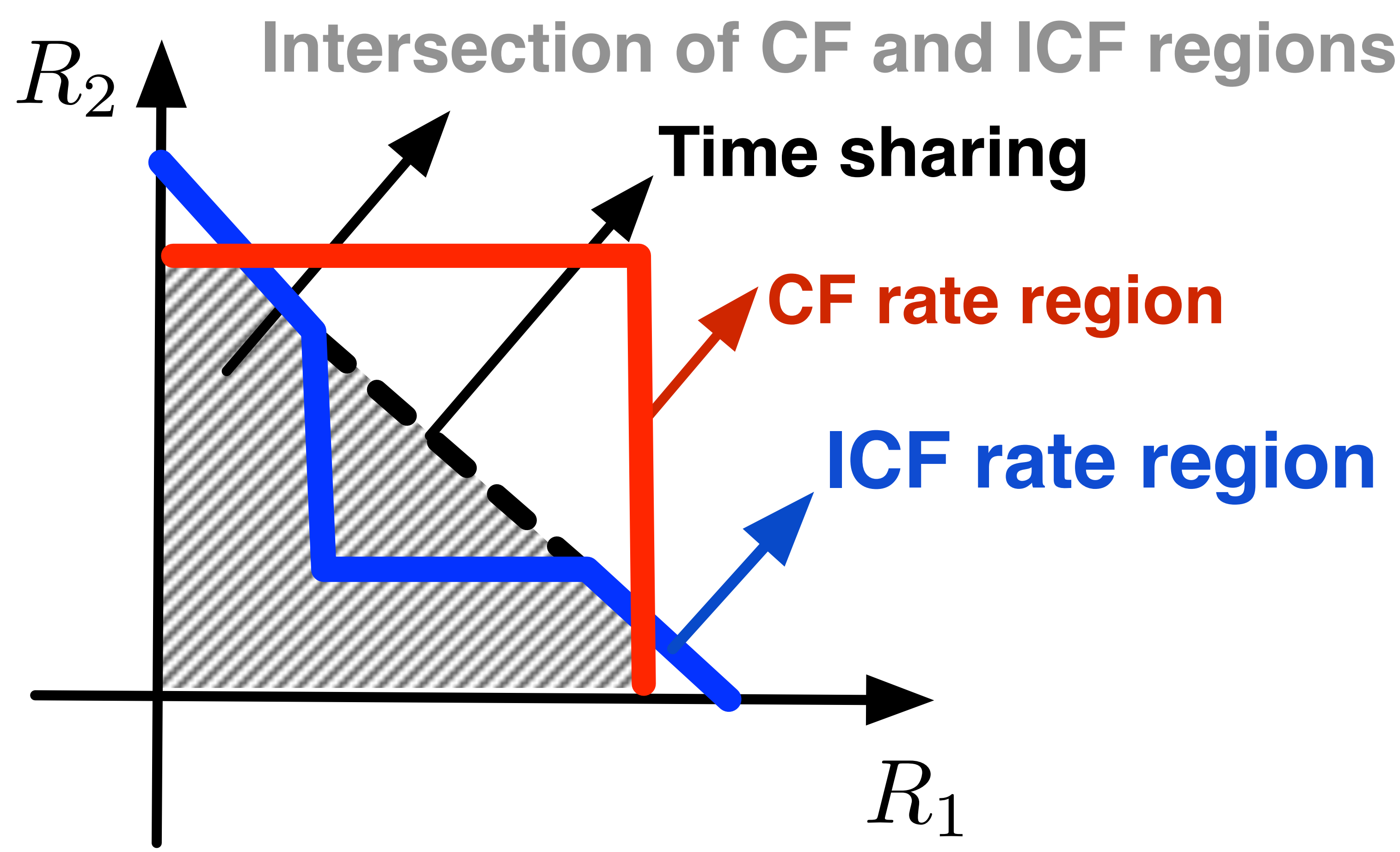
Goal - derive ICF rate region





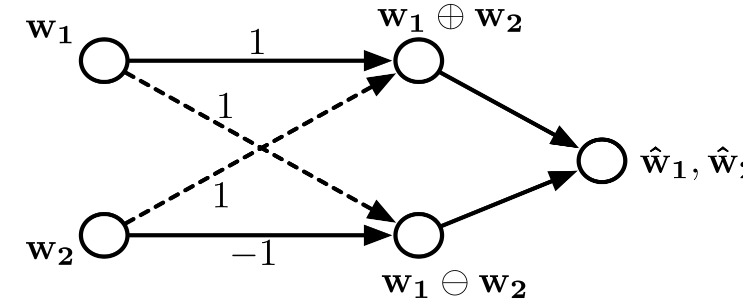
Goal - derive ICF rate region

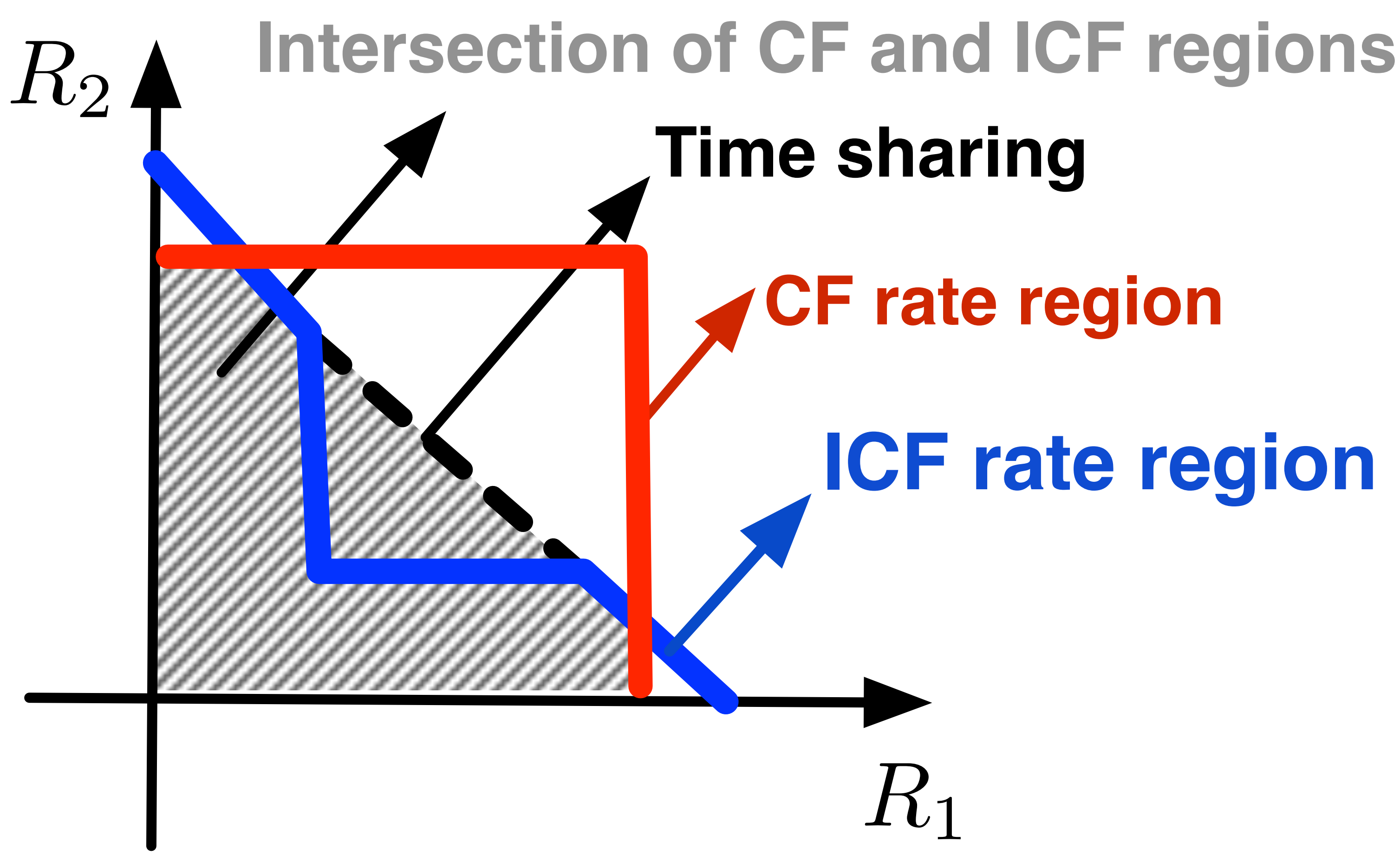




- Approach 1: allowable equations *(independent messages at Txs)*

Goal - derive ICF rate region

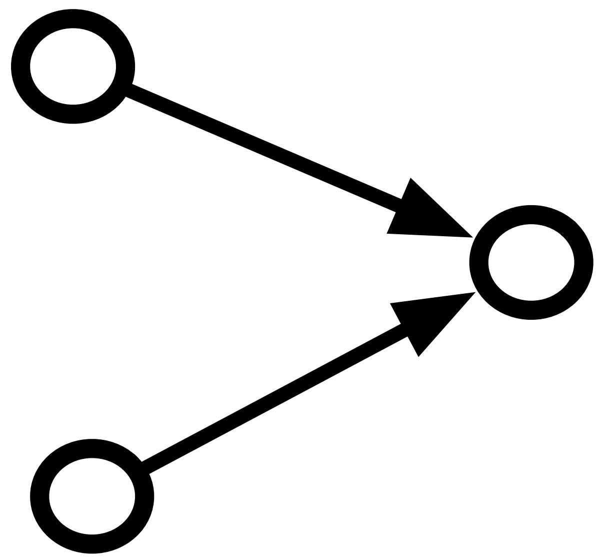




- Approach 1: allowable equations *(independent messages at Txs)*
- Approach 2: MAC with common messages *(correlated messages at Txs)*

Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$

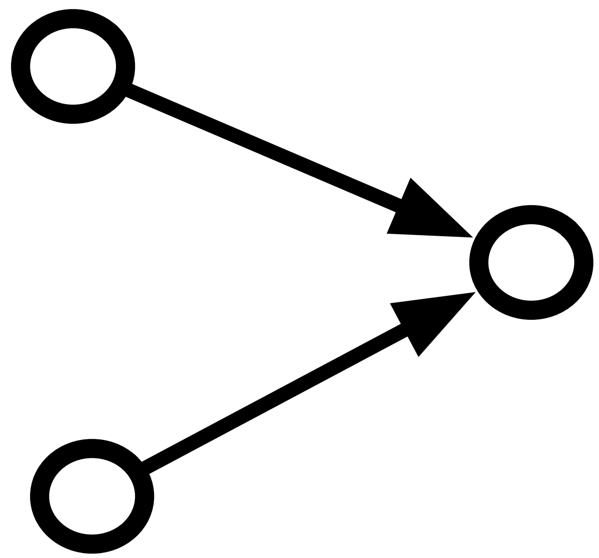


$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

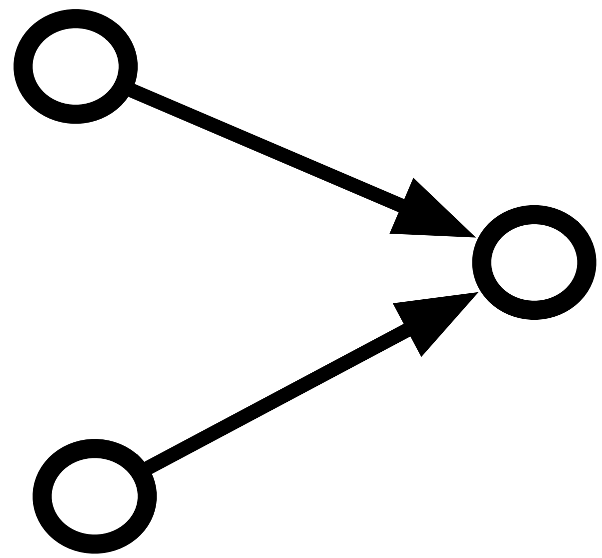
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

$\mathbf{w_1}$ rate R_1

$\mathbf{w_2}$ rate R_2

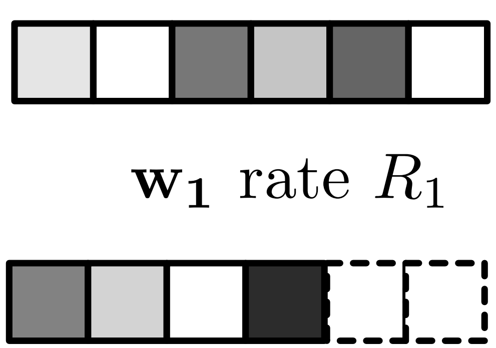
Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$



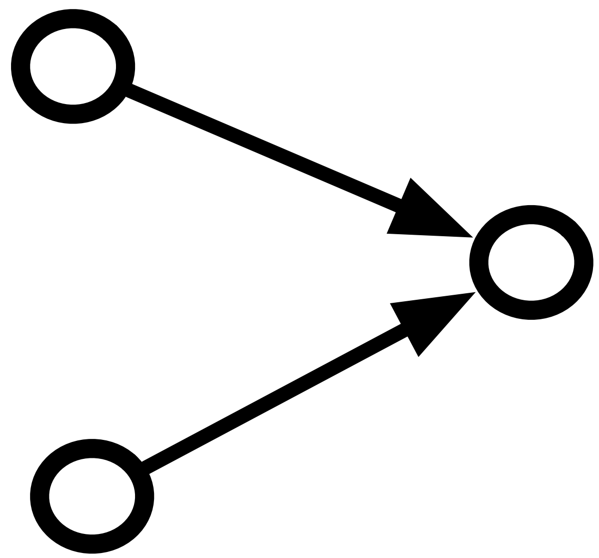
$\mathbf{w_1}$ rate R_1

$\mathbf{w_2}$ rate R_2

$$|\mathbf{u_1}| = |\mathbf{u_2}| = 2^{nR_{MAX}}$$

Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

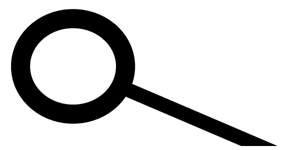
$\mathbf{w_1}$ rate R_1

$\mathbf{w_2}$ rate R_2

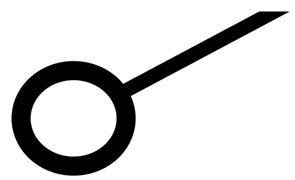
→ $|\mathbf{u_1}| = |\mathbf{u_2}| = 2^{nR_{MAX}}$ → $2R_{MAX} \geq R_1 + R_2$

Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



Key idea: if one equation is fixed, limits the number of possibilities of the other!



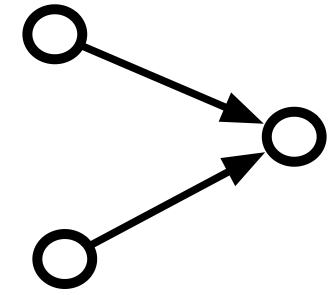
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

$\mathbf{w_1}$ rate R_1

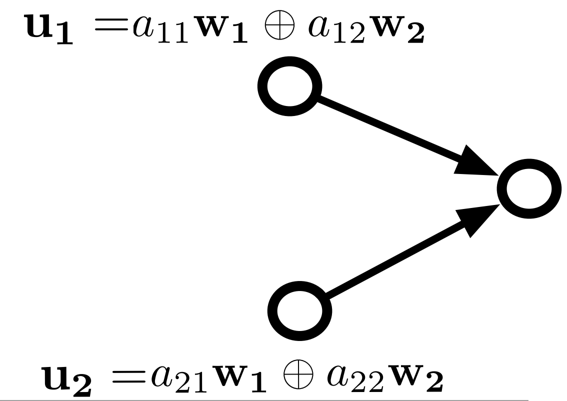
$\mathbf{w_2}$ rate R_2

$\rightarrow$ $|\mathbf{u_1}| = |\mathbf{u_2}| = 2^{nR_{MAX}}$ $\rightarrow$ $2R_{MAX} \geq R_1 + R_2$

Approach 1: allowable equations

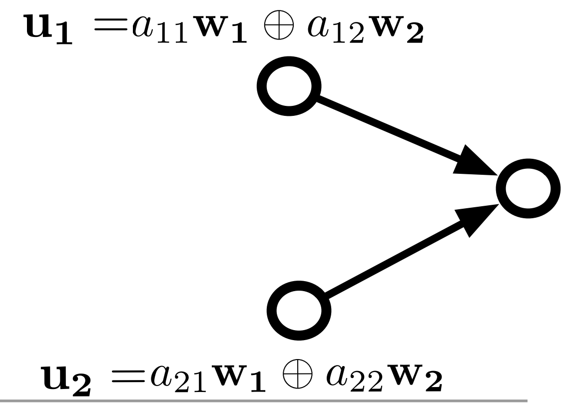


- Generate $2^{nR_{\mathrm{MAX}}}$ codewords of length n, X_1^n i.i.d $\sim \mathcal{N}(0, S_1)$.
- Generate $2^{nR_{\mathrm{MAX}}}$ independent codewords X_2^n i.i.d. $\sim \mathcal{N}(0, S_2)$.
- Transmit $X_1^n(\mathbf{u}_1)$ and $X_2^n(\mathbf{u}_2)$.



Approach 1: allowable equations

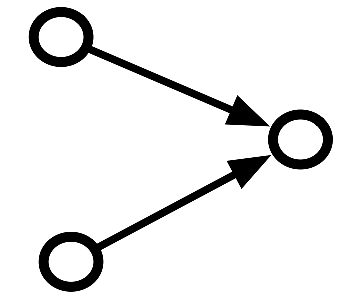
- Generate $2^{nR_{\mathrm{MAX}}}$ codewords of length n, X_1^n i.i.d $\sim \mathcal{N}(0, S_1)$.
- Generate $2^{nR_{\mathrm{MAX}}}$ independent codewords X_2^n i.i.d. $\sim \mathcal{N}(0, S_2)$.
- Transmit $X_1^n(\mathbf{u}_1)$ and $X_2^n(\mathbf{u}_2)$.
- Receive $Y^n = X_1^n(\mathbf{u}_1) + X_2^n(\mathbf{u}_2) + Z^n$ and decode $(\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2)$ such that $(X_1^n(\hat{\mathbf{u}}_1), X_2^n(\hat{\mathbf{u}}_2), Y^n)$ is jointly typical



Approach 1: allowable equations

- Generate $2^{nR_{\text{MAX}}}$ codewords of length n, X_1^n i.i.d $\sim \mathcal{N}(0, S_1)$.
- Generate $2^{nR_{\text{MAX}}}$ independent codewords X_2^n i.i.d. $\sim \mathcal{N}(0, S_2)$.
- Transmit $X_1^n(\mathbf{u}_1)$ and $X_2^n(\mathbf{u}_2)$.
- Receive $Y^n = X_1^n(\mathbf{u}_1) + X_2^n(\mathbf{u}_2) + Z^n$ and decode $(\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2)$ such that $(X_1^n(\hat{\mathbf{u}}_1), X_2^n(\hat{\mathbf{u}}_2), Y^n)$ is jointly typical
- P_e proceeds as in MAC channel EXCEPT that need to carefully count

• $(\mathbf{u_1} = \mathbf{0}, \mathbf{u_2} \neq \mathbf{0})$		• $\lvert\mathcal{M}_{\mathbf{A}}(U_2\lvert\mathbf{0})\rvert$
• $(\mathbf{u_1} \neq \mathbf{0}, \mathbf{u_2} = \mathbf{0})$	→	• $\lvert\mathcal{M}_{\mathbf{A}}(U_1\lvert\mathbf{0})\rvert$
• $(\mathbf{u_1} \neq \mathbf{0}, \mathbf{u_2} \neq \mathbf{0})$		• $\lvert\mathcal{M}_{\mathbf{A}}(U_1, U_2)$



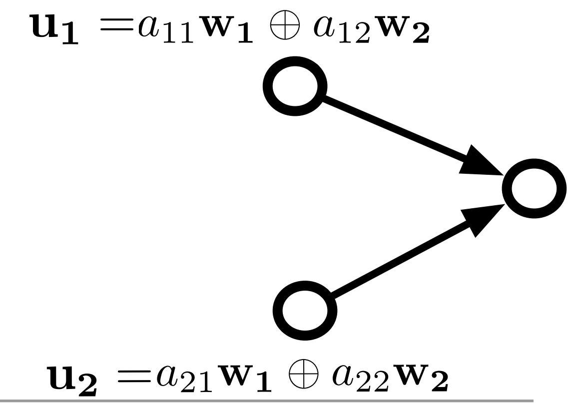
Approach 1: allowable equations

- Generate $2^{nR_{\text{MAX}}}$ codewords of length n, X_1^n i.i.d $\sim \mathcal{N}(0, S_1)$.
- Generate $2^{nR_{\text{MAX}}}$ independent codewords X_2^n i.i.d. $\sim \mathcal{N}(0, S_2)$.
- Transmit $X_1^n(\mathbf{u}_1)$ and $X_2^n(\mathbf{u}_2)$.
- Receive $Y^n = X_1^n(\mathbf{u}_1) + X_2^n(\mathbf{u}_2) + Z^n$ and decode $(\hat{\mathbf{u}}_1, \hat{\mathbf{u}}_2)$ such that $(X_1^n(\hat{\mathbf{u}}_1), X_2^n(\hat{\mathbf{u}}_2), Y^n)$ is jointly typical
- P_e proceeds as in MAC channel EXCEPT that need to carefully count

• $(\mathbf{u_1} = \mathbf{0}, \mathbf{u_2} \neq \mathbf{0})$		• $\lvert\mathcal{M}_{\mathbf{A}}(U_2 \lvert \mathbf{0})\rvert$
• $(\mathbf{u_1} \neq \mathbf{0}, \mathbf{u_2} = \mathbf{0})$	→	• $\lvert\mathcal{M}_{\mathbf{A}}(U_1 \lvert \mathbf{0})\rvert$
• $(\mathbf{u_1} \neq \mathbf{0}, \mathbf{u_2} \neq \mathbf{0})$		• $\lvert\mathcal{M}_{\mathbf{A}}(U_1, U_2)$

Count the number of allowable equations!

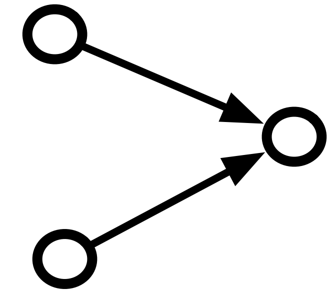
Cardinality Lemma



$$\mathcal{M}_{\mathbf{A}}(U_1, U_2) = \Big\{(\mathbf{u}_1, \mathbf{u}_2) : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2, \quad \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2, \ \text{for some } \mathbf{w}_1, \mathbf{w}_2\Big\} \ .$$

$$\mathcal{M}_{\mathbf{A}}(U_1 | \mathbf{u}_2) = \Big\{\mathbf{u}_1 : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2 \text{ for some } \mathbf{w}_1, \mathbf{w}_2 \quad \text{satisfying } \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2\Big\} \ ,$$

Cardinality Lemma



$$\mathcal{M}_{\mathbf{A}}(U_1, U_2) = \Big\{(\mathbf{u}_1, \mathbf{u}_2) : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2, \\ \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2, \text{ for some } \mathbf{w}_1, \mathbf{w}_2\Big\} .$$

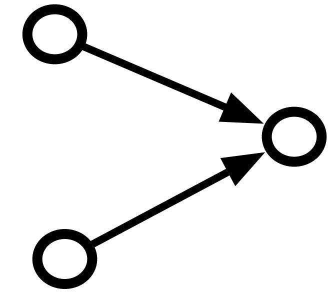
$$\mathcal{M}_{\mathbf{A}}(U_1 | \mathbf{u}_2) = \Big\{\mathbf{u}_1 : \ \mathbf{u}_1 = a_{11}\mathbf{w}_1 + a_{12}\mathbf{w}_2 \text{ for some } \mathbf{w}_1, \mathbf{w}_2 \\ \text{satisfying } \mathbf{u}_2 = a_{21}\mathbf{w}_1 + a_{22}\mathbf{w}_2\Big\} ,$$

Cardinality lemma. The set of allowable equations $\mathcal{M}_{\mathbf{A}}(U_1, U_2)$ and the set of conditionally allowable equations $\mathcal{M}_{\mathbf{A}}(U_\ell | \mathbf{u}_m)$ have the following cardinalities:

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2)| = 2^{n(R_1+R_2)}$$
$$|\mathcal{M}_{\mathbf{A}}(U_1 | \mathbf{u}_2)| = 2^{nR_{\mathrm{MIN}}}$$
$$|\mathcal{M}_{\mathbf{A}}(U_2 | \mathbf{u}_1)| = 2^{nR_{\mathrm{MIN}}} \ .$$

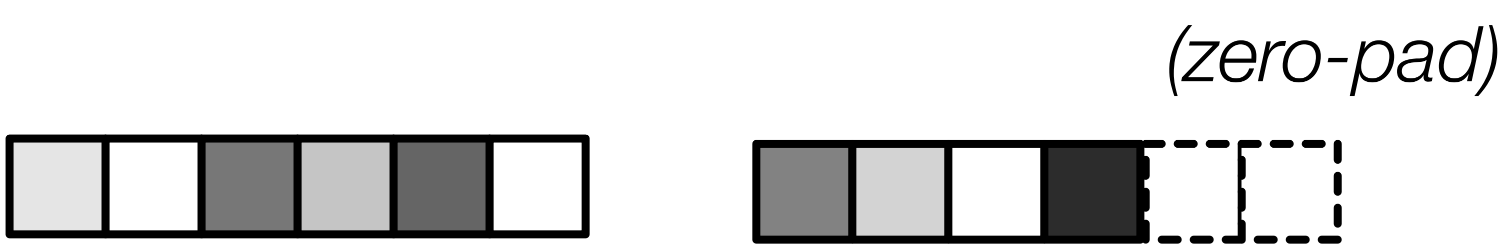
Proof of Cardinality Lemma

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



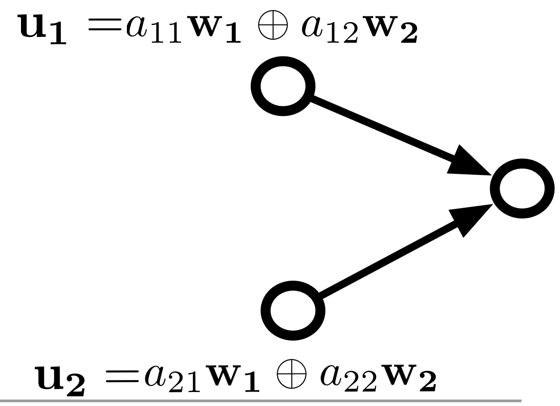
$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

- $|\mathcal{M}_{\mathbf{A}}(U_1, U_2)| = 2^{n(R_1+R_2)}$ as $\begin{bmatrix} \mathbf{u_1} \\ \mathbf{u_2} \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathbf{w_1} \\ \mathbf{w_2} \end{bmatrix}$



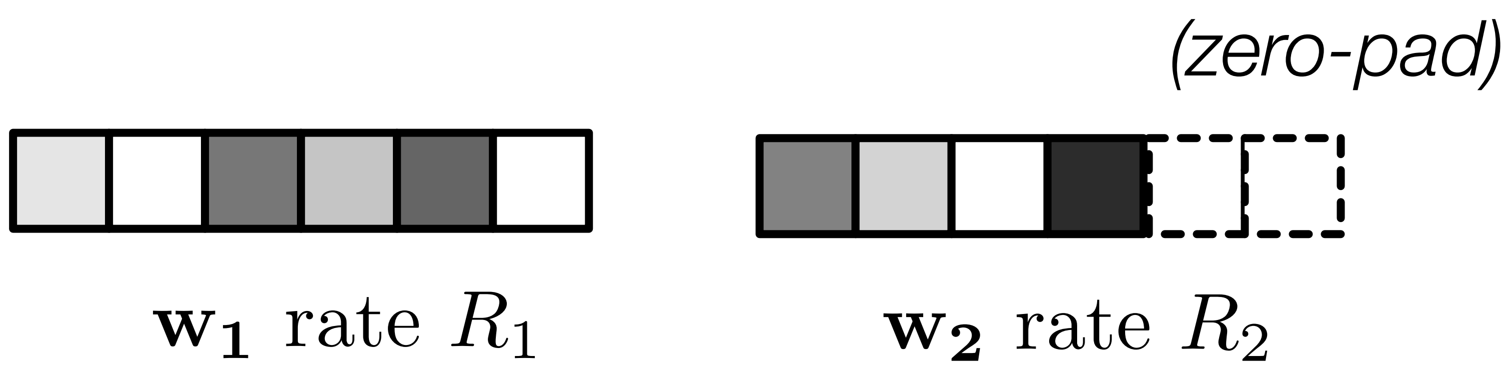
$\mathbf{w_1}$ rate R_1 $\quad$ $\mathbf{w_2}$ rate R_2

Proof of Cardinality Lemma



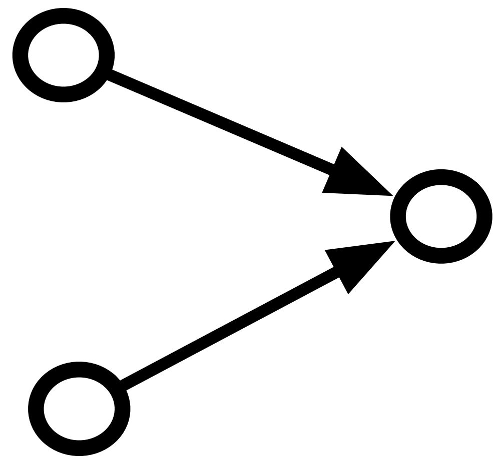
- $|\mathcal{M}_{\mathbf{A}}(U_1, U_2)| = 2^{n(R_1+R_2)}$ as $\begin{bmatrix} \mathbf{u_1} \\ \mathbf{u_2} \end{bmatrix} = \mathbf{A} \begin{bmatrix} \mathbf{w_1} \\ \mathbf{w_2} \end{bmatrix}$

- $|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u_2})| = 2^{n\min(R_1,R_2)}$. Assume WLOG $R_1 > R_2$.
Each $\mathbf{w_2}$ has *one* $\mathbf{w_1}$ such that $a_{21}\mathbf{w_1} + a_{22}\mathbf{w_2} = \mathbf{u_2}$.
Since $\mathbf{u_1} \perp \mathbf{u_2} \Rightarrow 2^{nR_2}$ solutions.



Approach 1: allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$$

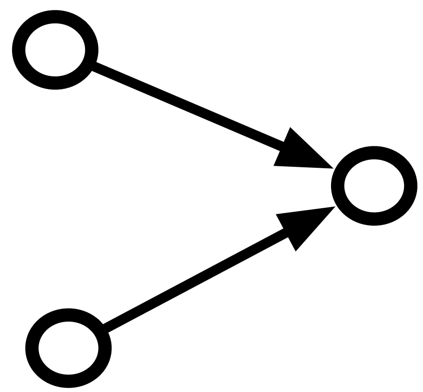
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$

$$\min(R_1, R_2) < \min(C(S_1), C(S_2))$$
$$R_1 + R_2 < C(S_1 + S_2).$$

$$P_e \leq \epsilon \ + \ |\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{0})| 2^{-n(I(X_1;Y|X_2)-\epsilon)} + \ |\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{0})| 2^{-n(I(X_2;Y|X_1)-\epsilon)} + \ |\mathcal{M}_{\mathbf{A}}(U_1, U_2)| 2^{-n(I(X_1,X_2;Y)-\epsilon)}$$
$$= \epsilon + 2^{nR_{\text{MIN}}} 2^{-n(I(X_1;Y|X_2)-\epsilon)} + 2^{nR_{\text{MIN}}} 2^{-n(I(X_2;Y|X_1)-\epsilon)} + 2^{n(R_1+R_2)} 2^{-n(I(X_1,X_2;Y)-\epsilon)}.$$

What if coefficients are zero?

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



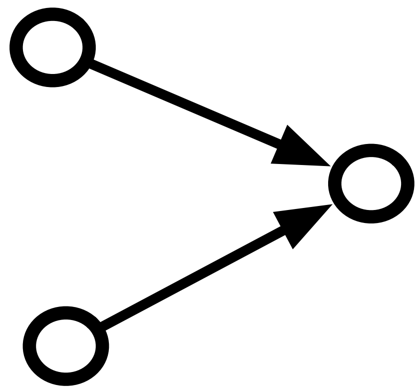
$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

$$R_{min} < I(X_1; Y | X_2) = C(S_1)$$
$$R_{min} < I(X_2; Y | X_1) = C(S_2)$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2).$$

What if coefficients are zero?

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$

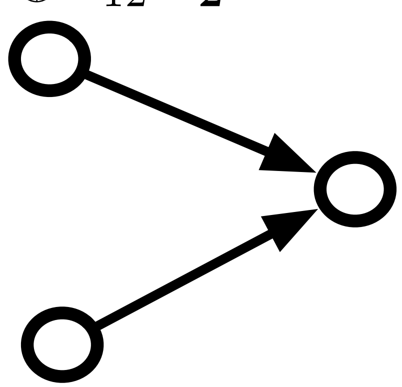


$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

$$R_{min} < I(X_1; Y|X_2) = C(S_1)$$
$$R_{min} < I(X_2; Y|X_1) = C(S_2)$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2).$$

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



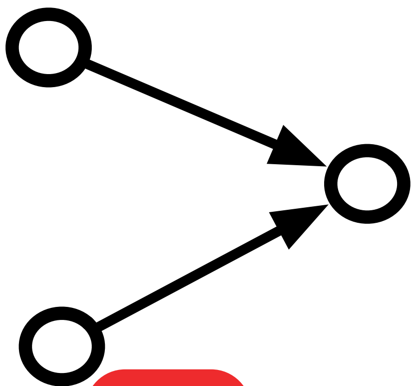
$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

$\mathbf{u_2} = a_{21}\mathbf{w_1}$

$$R_2 < I(X_1; Y|X_2) = C(S_1)$$
$$R_{min} < I(X_2; Y|X_1) = C(S_2)$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2).$$

What if coefficients are zero?

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$

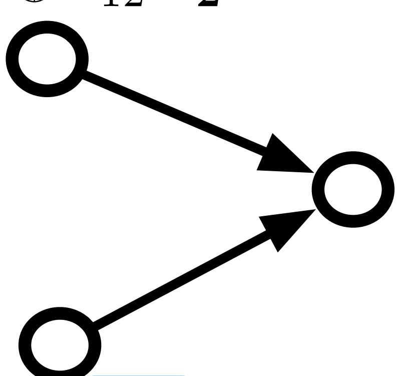


$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$

$$R_{min} < I(X_1; Y | X_2) = C(S_1)$$
$$R_{min} < I(X_2; Y | X_1) = C(S_2)$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2).$$

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$



$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}$

$\mathbf{u_2} = a_{21}\mathbf{w_1}$

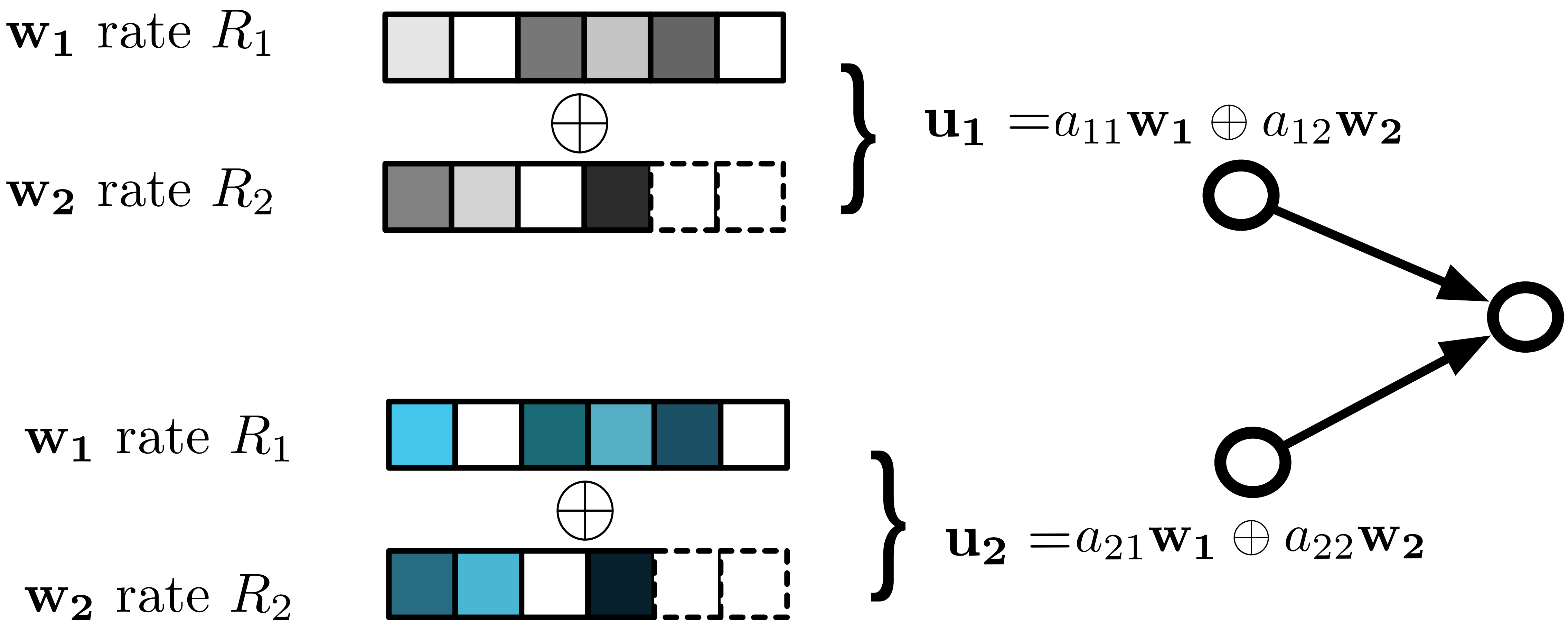
$$R_2 < I(X_1; Y | X_2) = C(S_1)$$
$$R_{min} < I(X_2; Y | X_1) = C(S_2)$$
$$R_1 + R_2 < I(X_1, X_2; Y) = C(S_1 + S_2).$$

Outline

- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users
- Case study

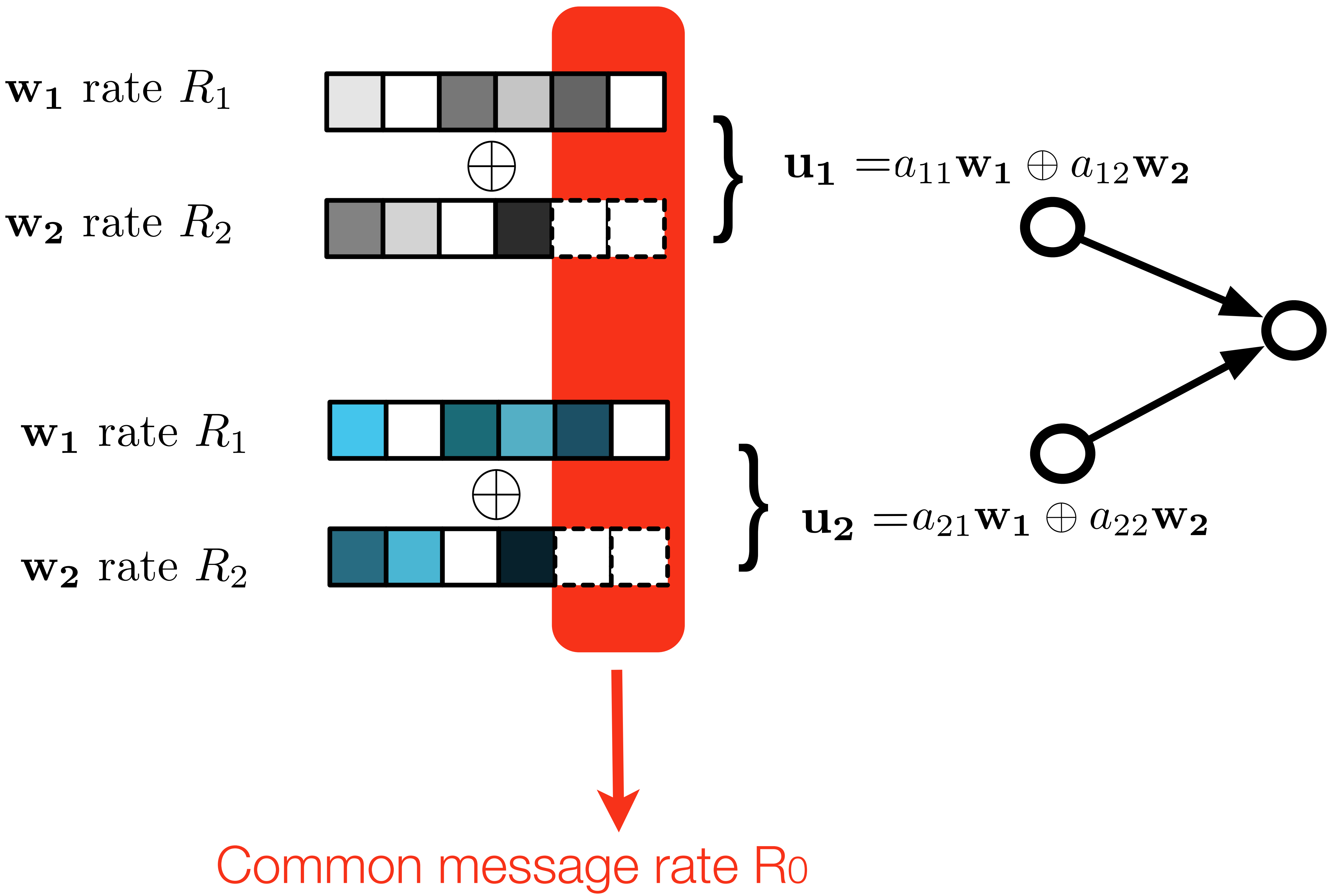
[Slepian, Wolf, 1973], [Han, 1979]

Approach 2: MAC with common messages



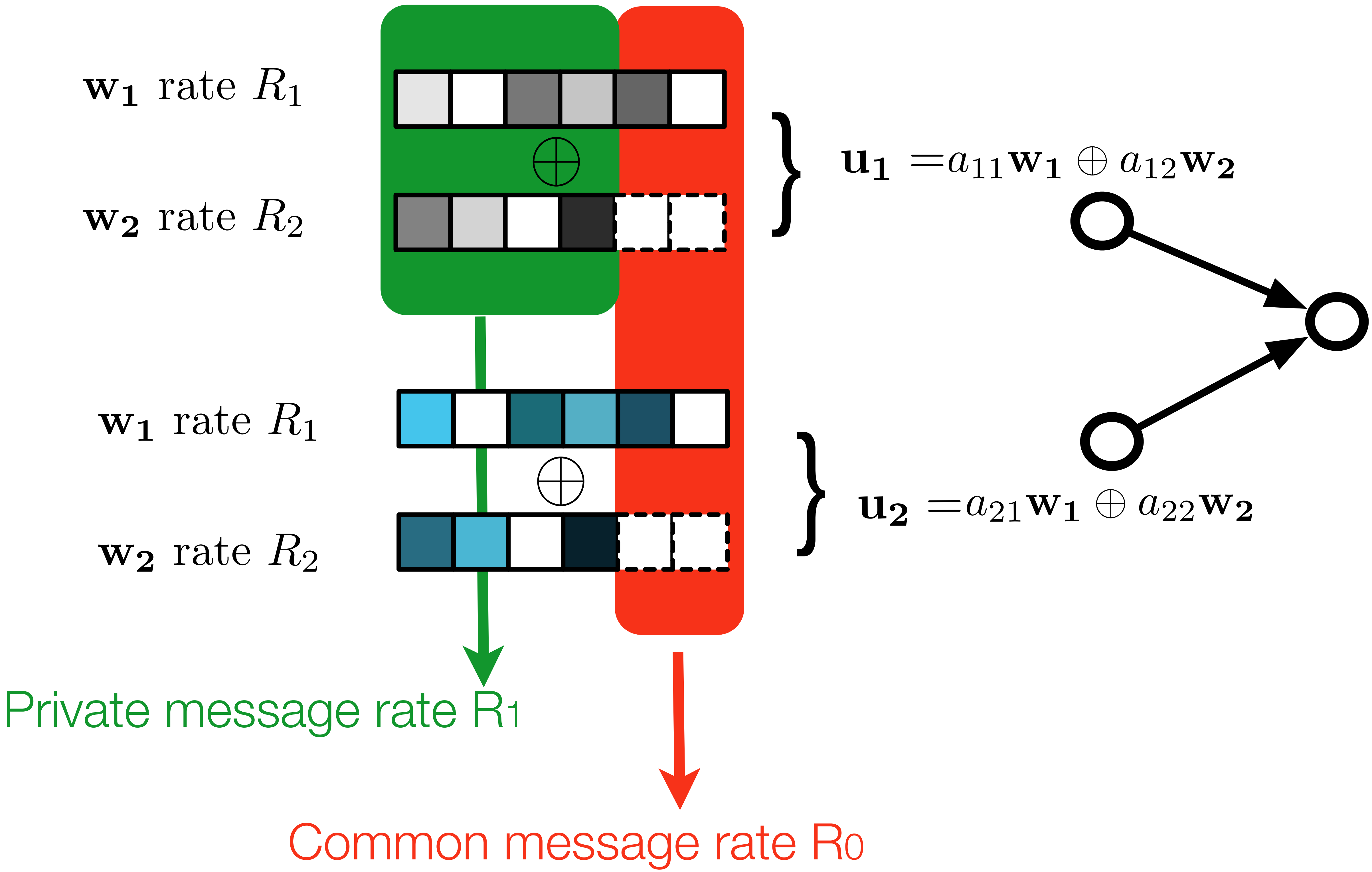
[Slepian, Wolf, 1973], [Han, 1979]

Approach 2: MAC with common messages



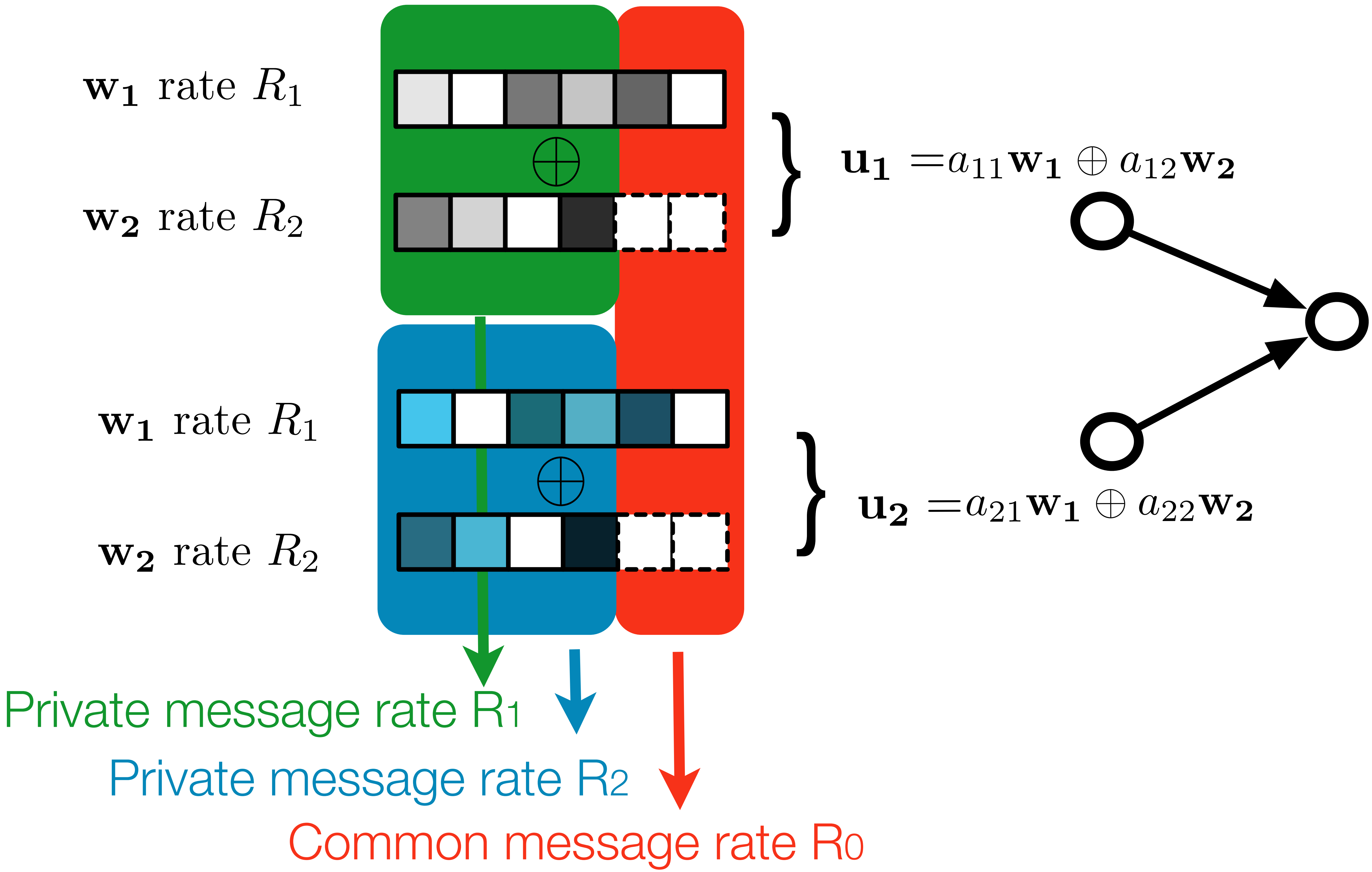
[Slepian, Wolf, 1973], [Han, 1979]

Approach 2: MAC with common messages



[Slepian, Wolf, 1973], [Han, 1979]

Approach 2: MAC with common messages



[Slepian, Wolf, 1973], [Han, 1979]

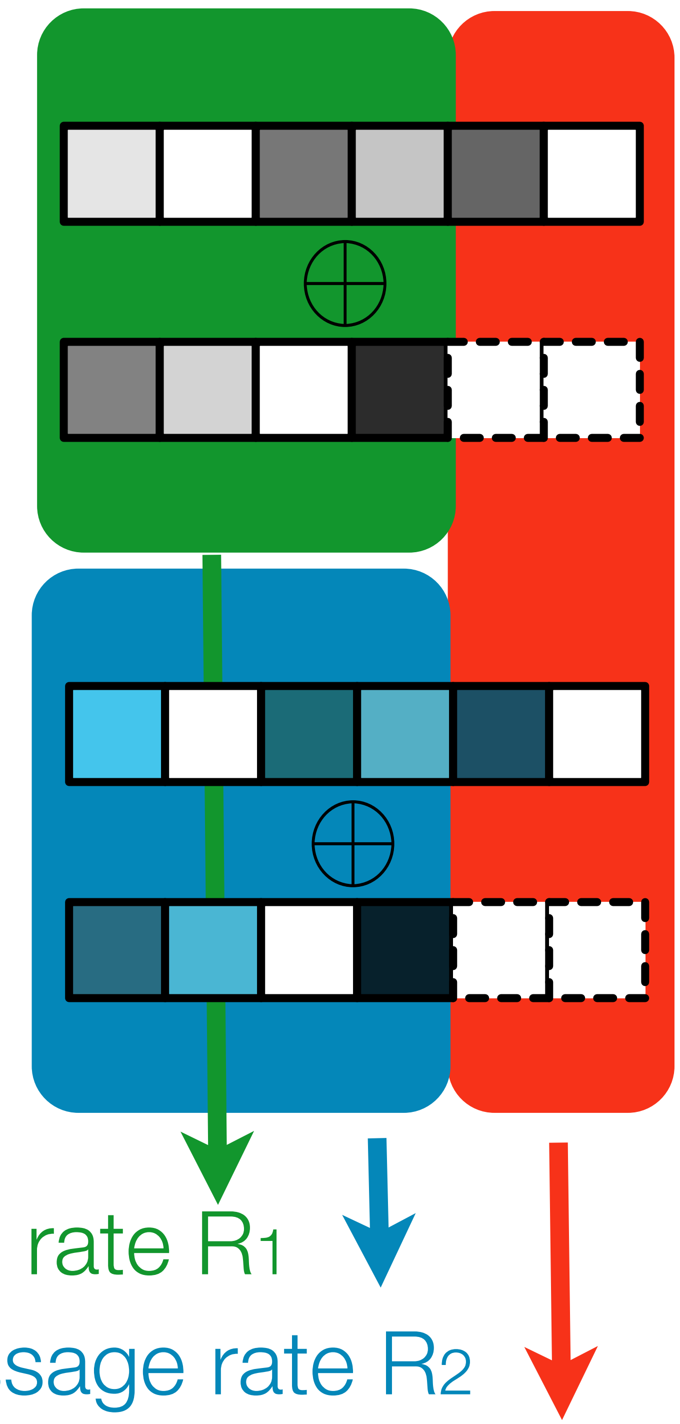
Approach 2: MAC with common messages

$\mathbf{w_1}$ rate R_1

$\mathbf{w_2}$ rate R_2

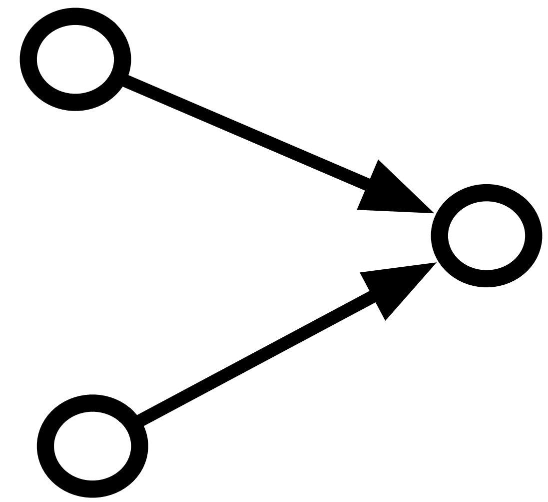
$\mathbf{w_1}$ rate R_1

$\mathbf{w_2}$ rate R_2



$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2}$$



Private message rate R_1

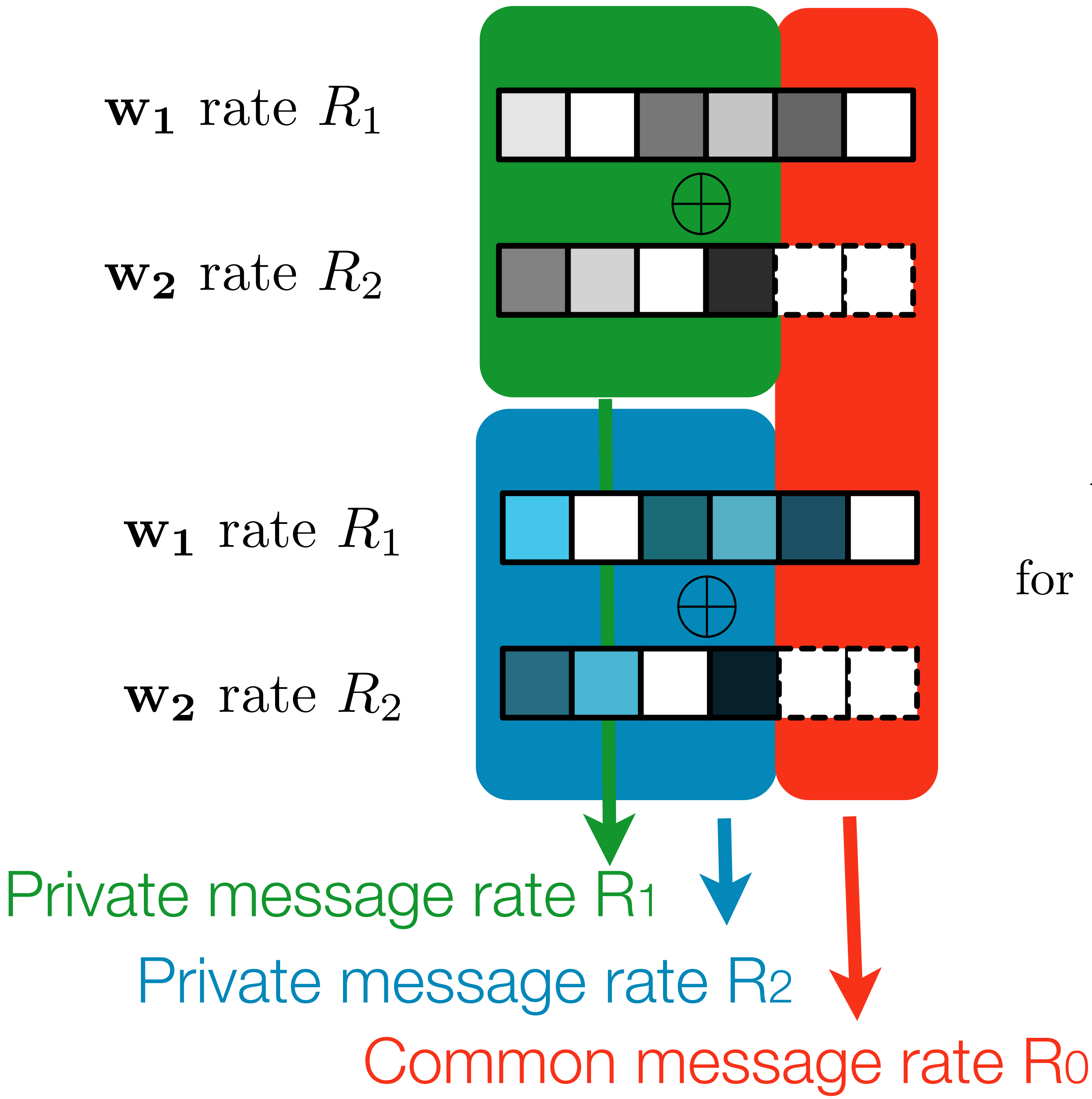
Private message rate R_2

Common message rate R_0

Decoding all parts yields **$\mathbf{w_1}$** and **$\mathbf{w_2}$**

[Slepian, Wolf, 1973], [Han, 1979]

Approach 2: MAC with common messages



$$R_1 < I(X_1; Y | X_2, V)$$
$$R_2 < I(X_2; Y | X_1, V)$$
$$R_1 + R_2 < I(X_1, X_2; Y | V)$$
$$R_0 + R_1 + R_2 < I(X_1, X_2; Y)$$

for some $p_V(v) p_{X_1|V}(x_1|v) p_{X_2|V}(x_2|v)$.

} Decoding all parts yields **w1** and **w2**

Outline

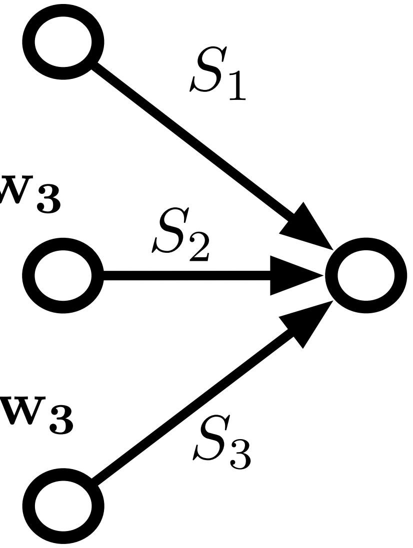
- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users
- Case study

Beyond 2 users - allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$



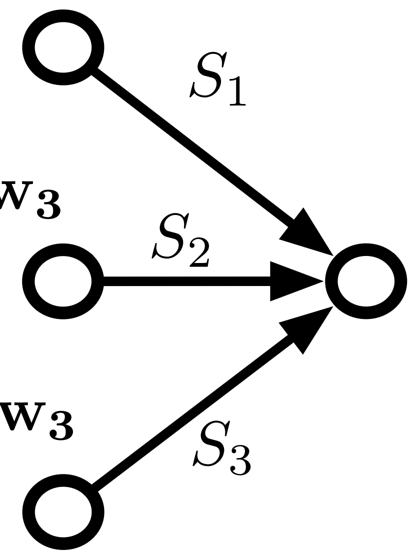
$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}, \widehat{\mathbf{w_3}}$$

Beyond 2 users - allowable equations

$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$

$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$

$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$



$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}, \widehat{\mathbf{w_3}}$

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2, U_3)| = 2^{n(R_1+R_2+R_3)}$$

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2|\mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_1, U_3|\mathbf{u}_2)| = |\mathcal{M}_{\mathbf{A}}(U_2, U_3|\mathbf{u}_1)| = 2^{n(R_{\mathrm{MID}}+R_{\mathrm{MIN}})}$$

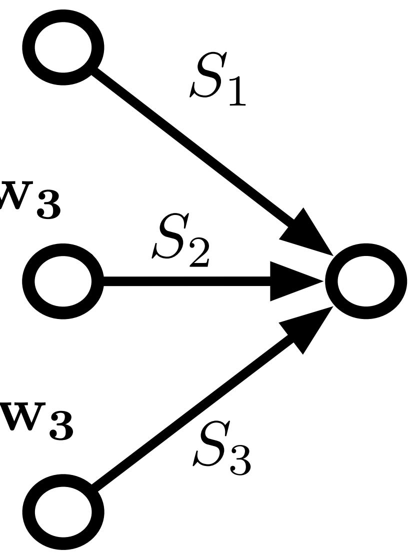
$$|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{nR_{\mathrm{MIN}}}$$

Beyond 2 users - allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$



$$\Rightarrow \widehat{\mathbf{w_1}}, \widehat{\mathbf{w_2}}, \widehat{\mathbf{w_3}}$$

Use in MAC Pe calculations

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2, U_3)| = 2^{n(R_1+R_2+R_3)}$$

$$|\mathcal{M}_{\mathbf{A}}(U_1, U_2|\mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_1, U_3|\mathbf{u}_2)| = |\mathcal{M}_{\mathbf{A}}(U_2, U_3|\mathbf{u}_1)| = 2^{n(R_{\text{MID}}+R_{\text{MIN}})}$$

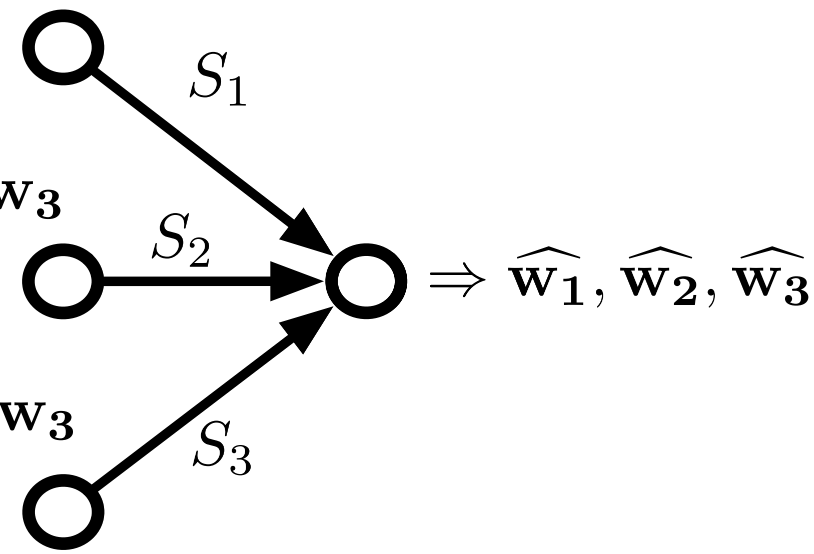
$$|\mathcal{M}_{\mathbf{A}}(U_1|\mathbf{u}_2, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_2|\mathbf{u}_1, \mathbf{u}_3)| = |\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{nR_{\text{MIN}}}$$

Beyond 2 users - allowable equations

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$

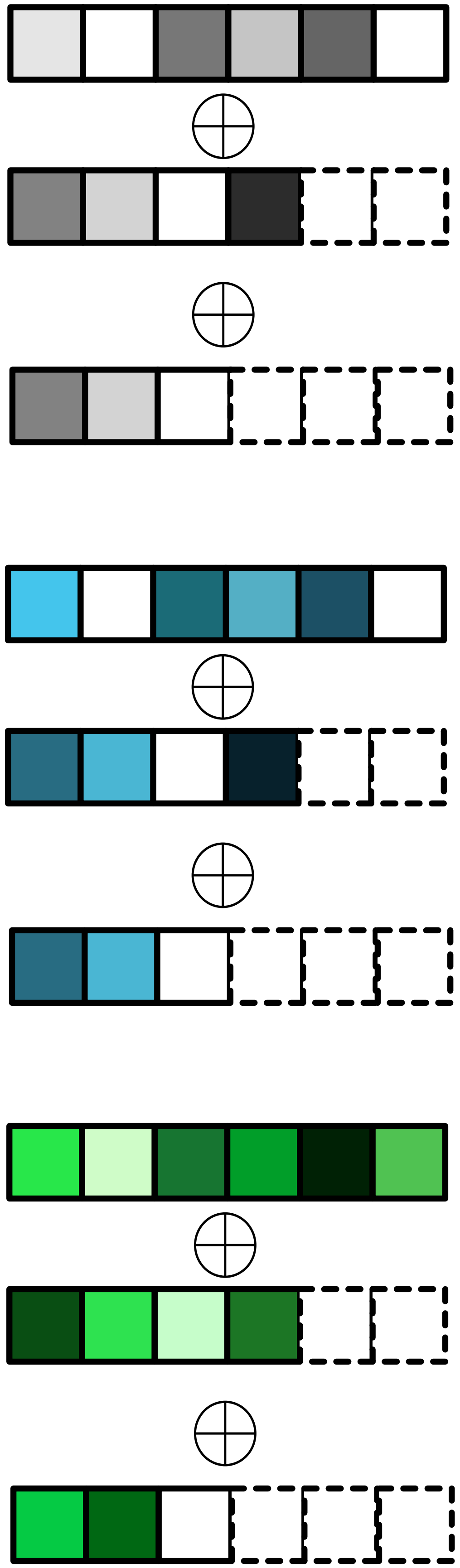


$$R_{\text{MIN}} \leq \min\{C(S_1), C(S_2), C(S_3)\}$$

$$R_{\text{MIN}} + R_{\text{MID}} \leq \min\{C(S_1 + S_2), C(S_1 + S_3), C(S_2 + S_3)\}$$

$$R_{\text{MIN}} + R_{\text{MID}} + R_{\text{MAX}} \leq C(S_1 + S_2 + S_3)$$

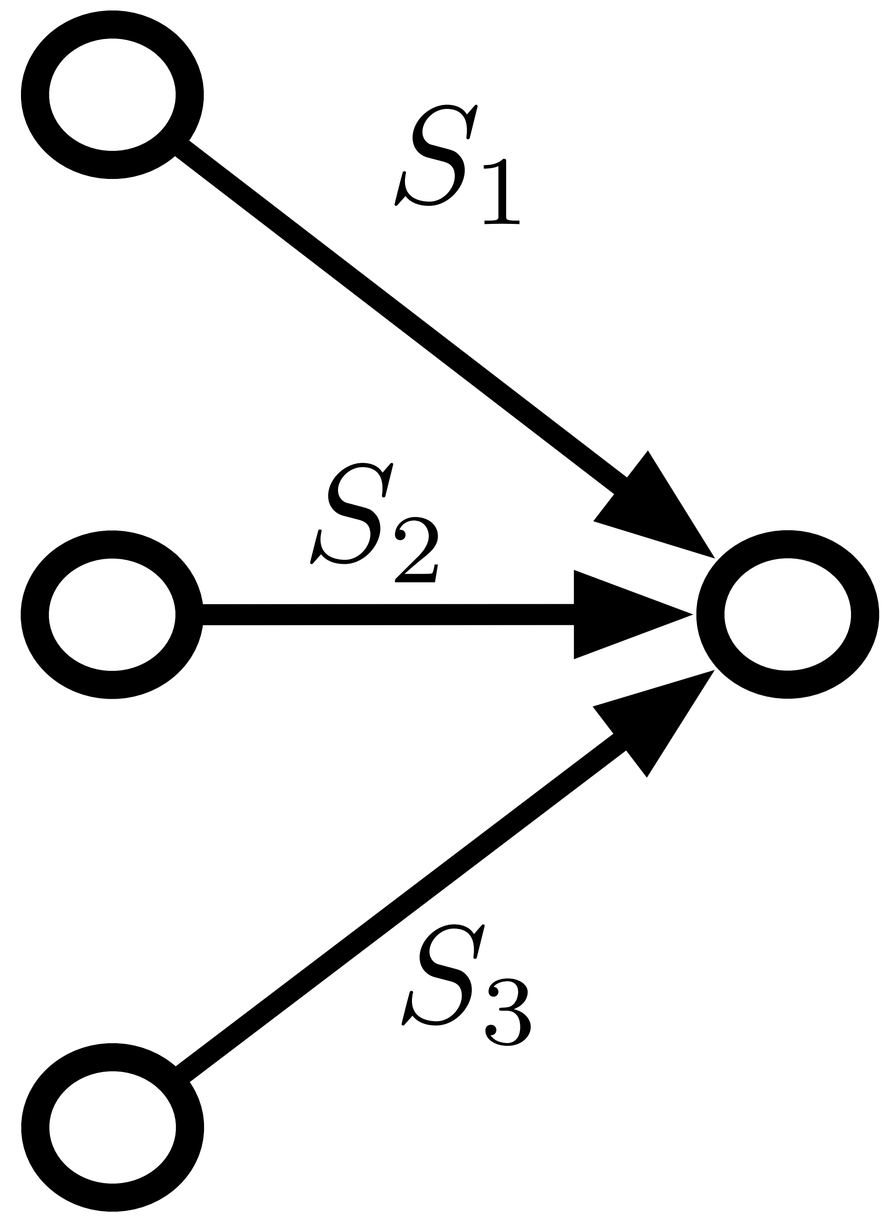
Beyond 2 users - MAC with common messages



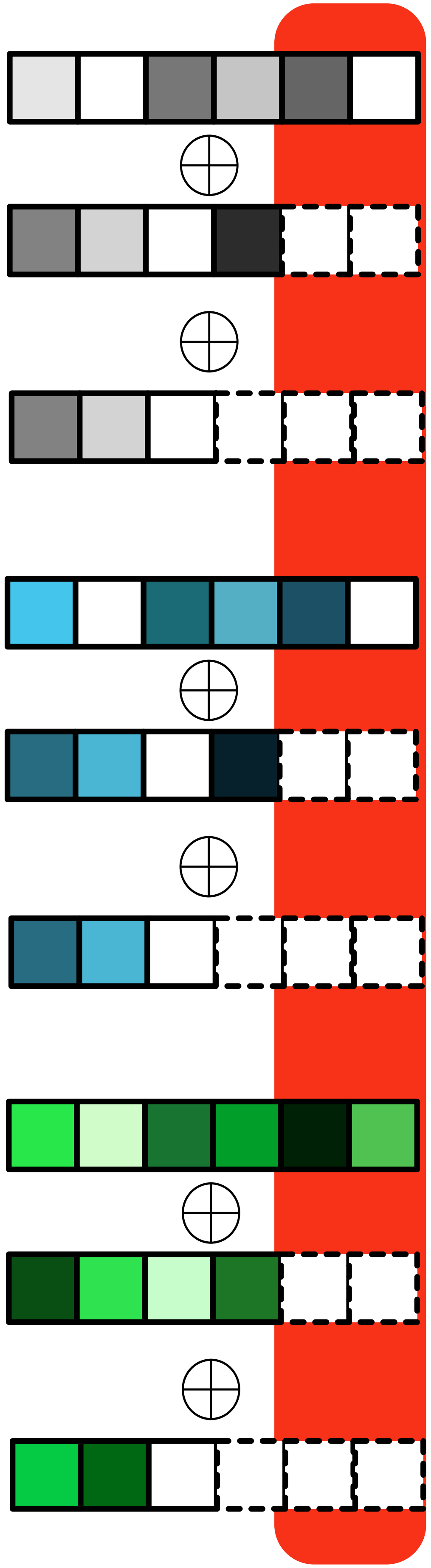
$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$



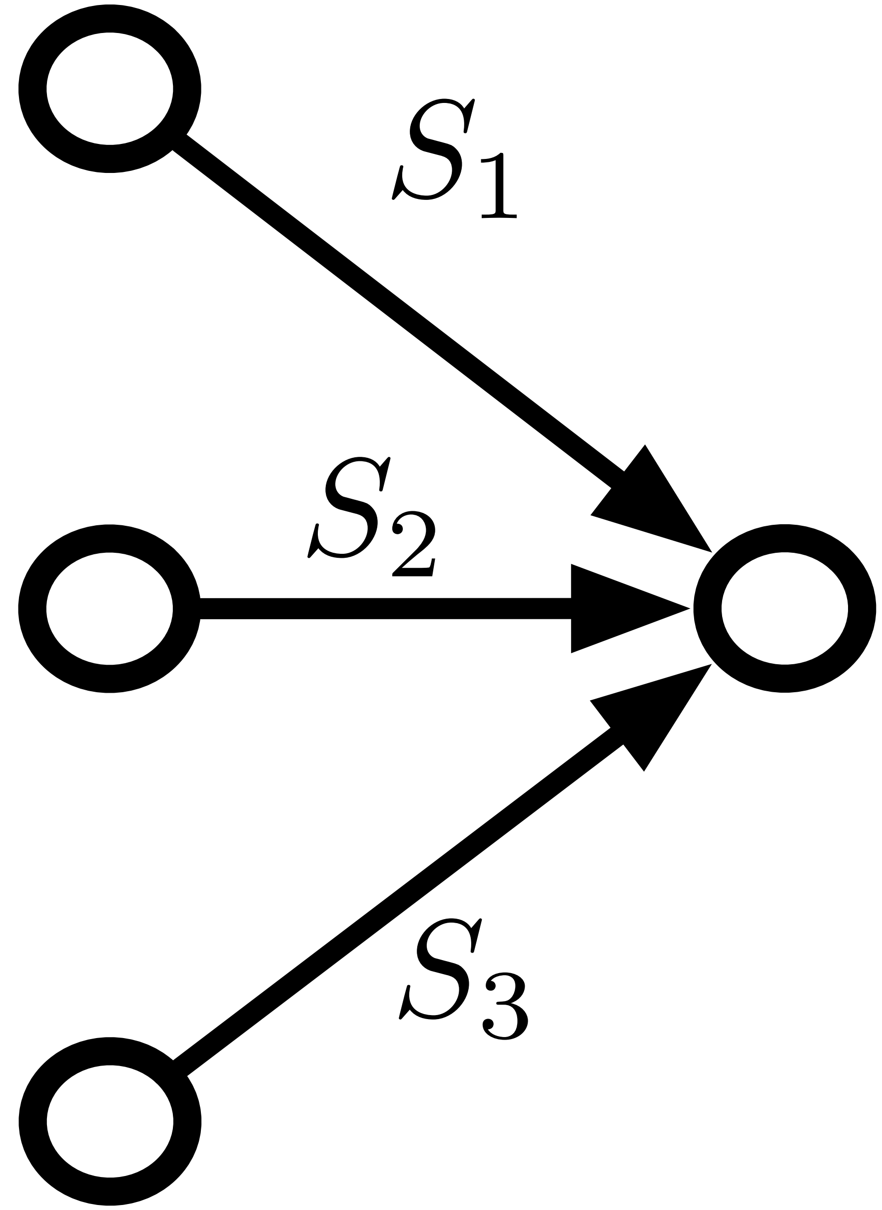
Beyond 2 users - MAC with common messages



$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

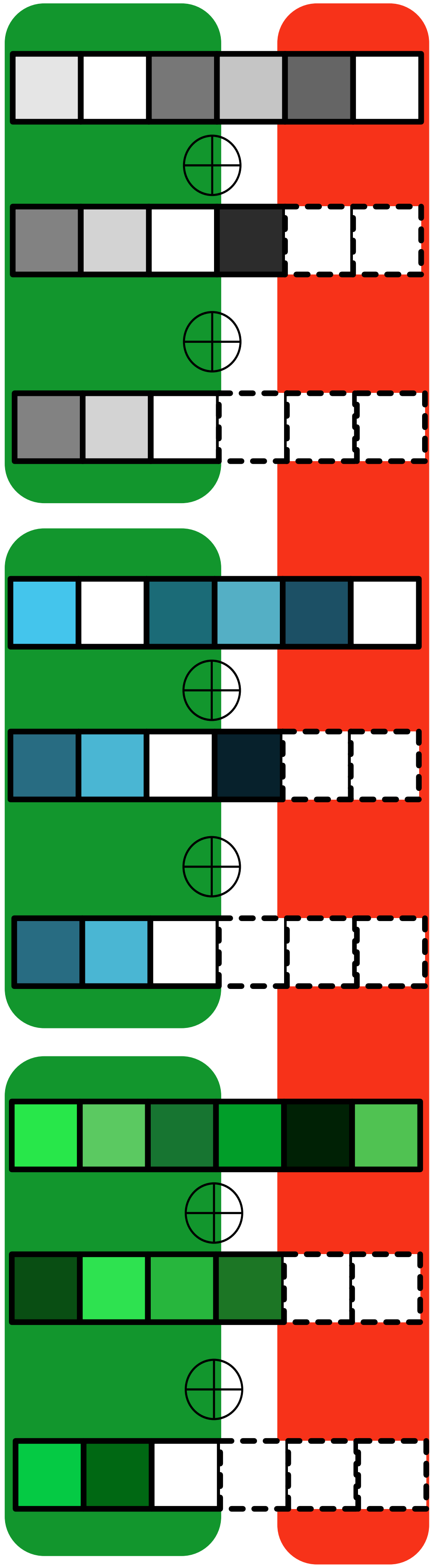
$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$



Common message

Beyond 2 users - MAC with common messages



Private message

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

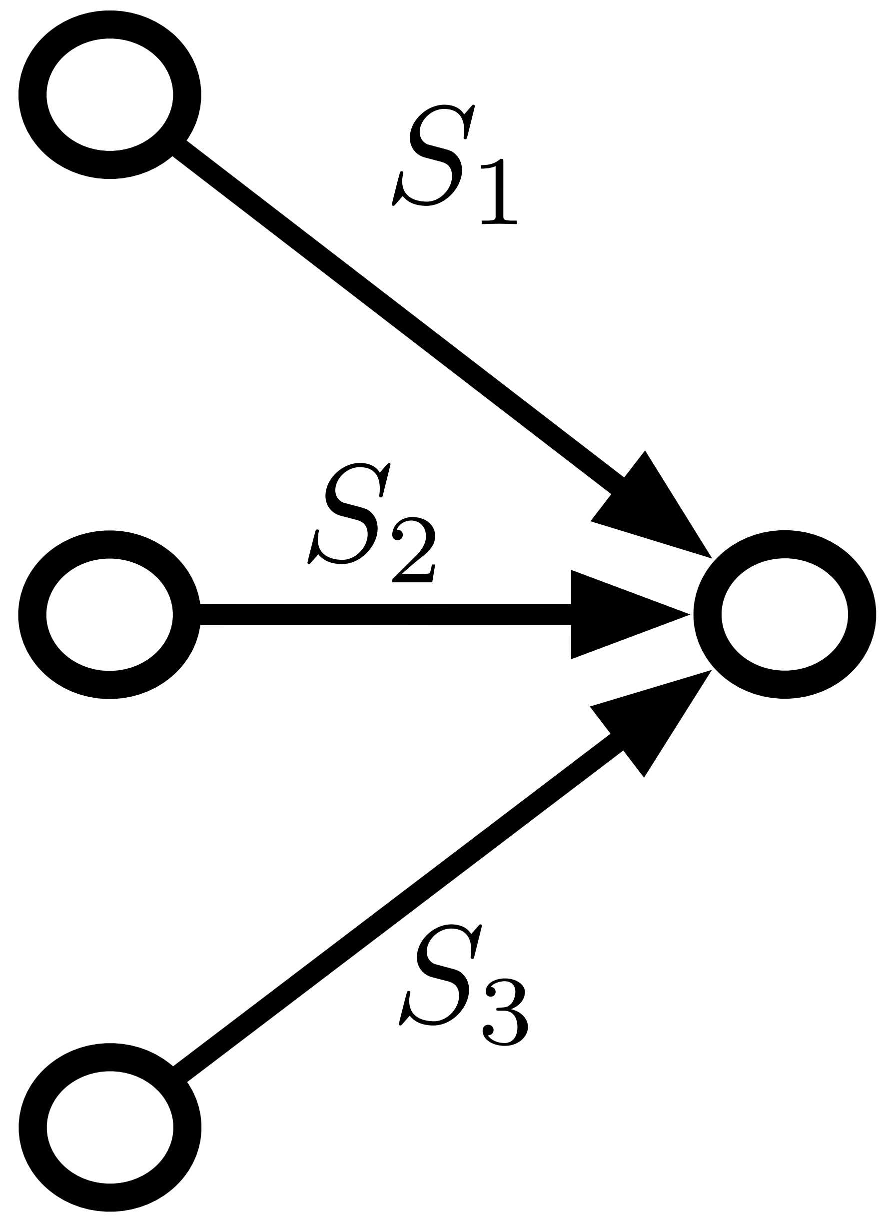
Private message

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

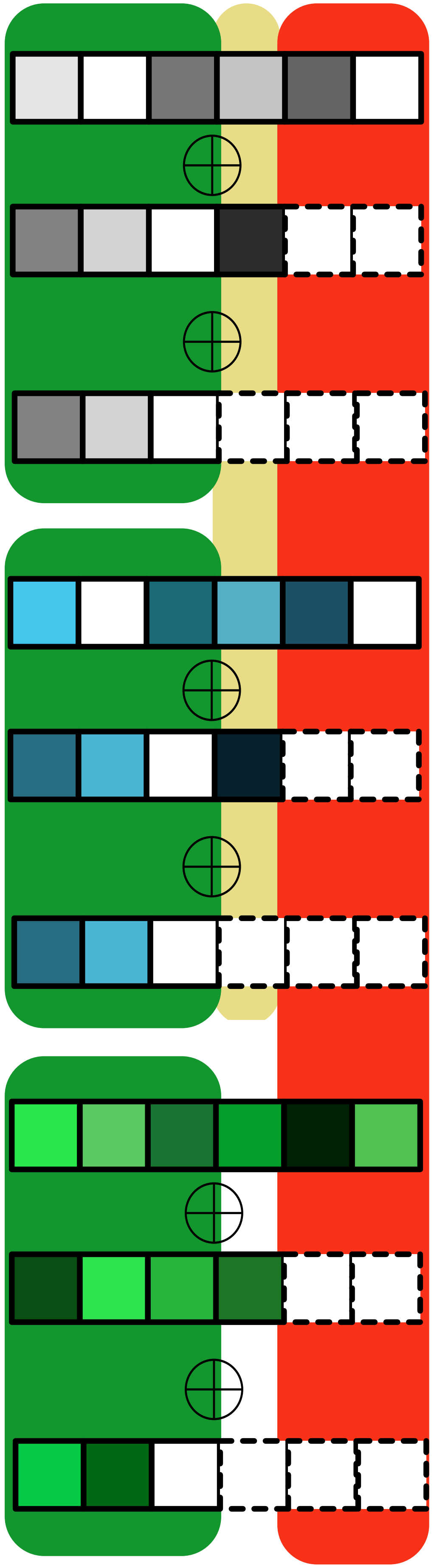
Private message

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$

Common message



Beyond 2 users - MAC with common messages



Private message

$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

Common message (1,2)

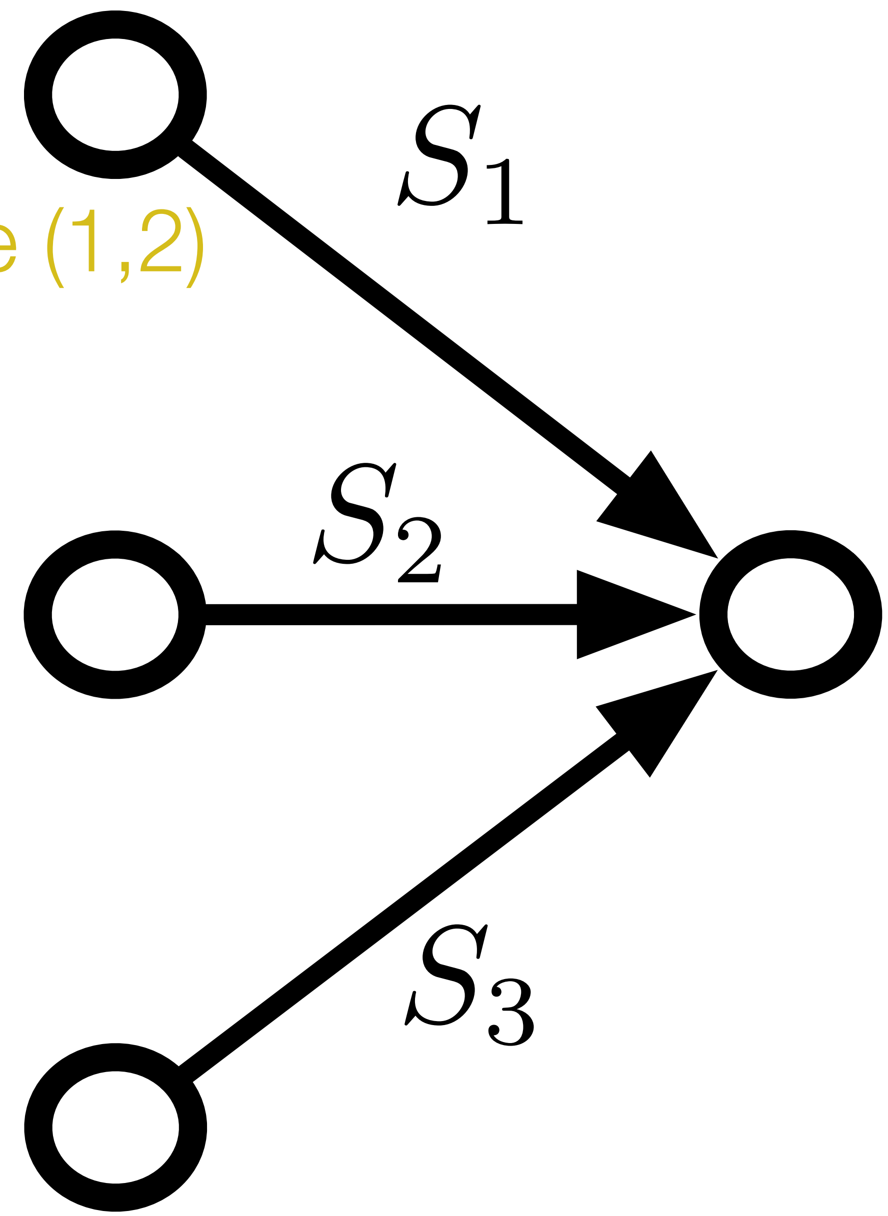
Private message

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

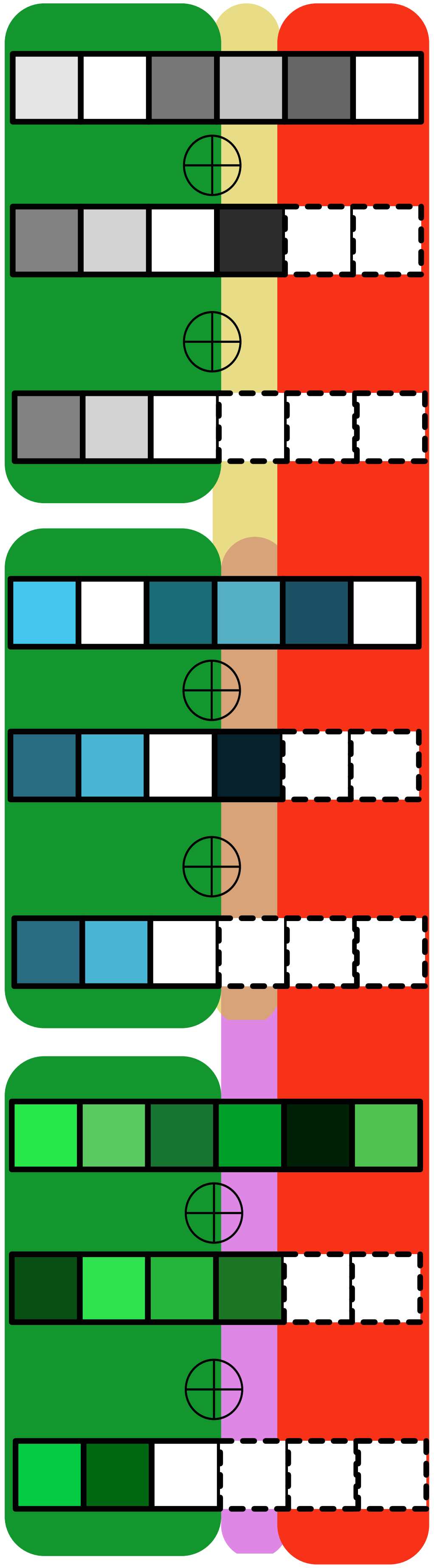
Private message

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$

Common message



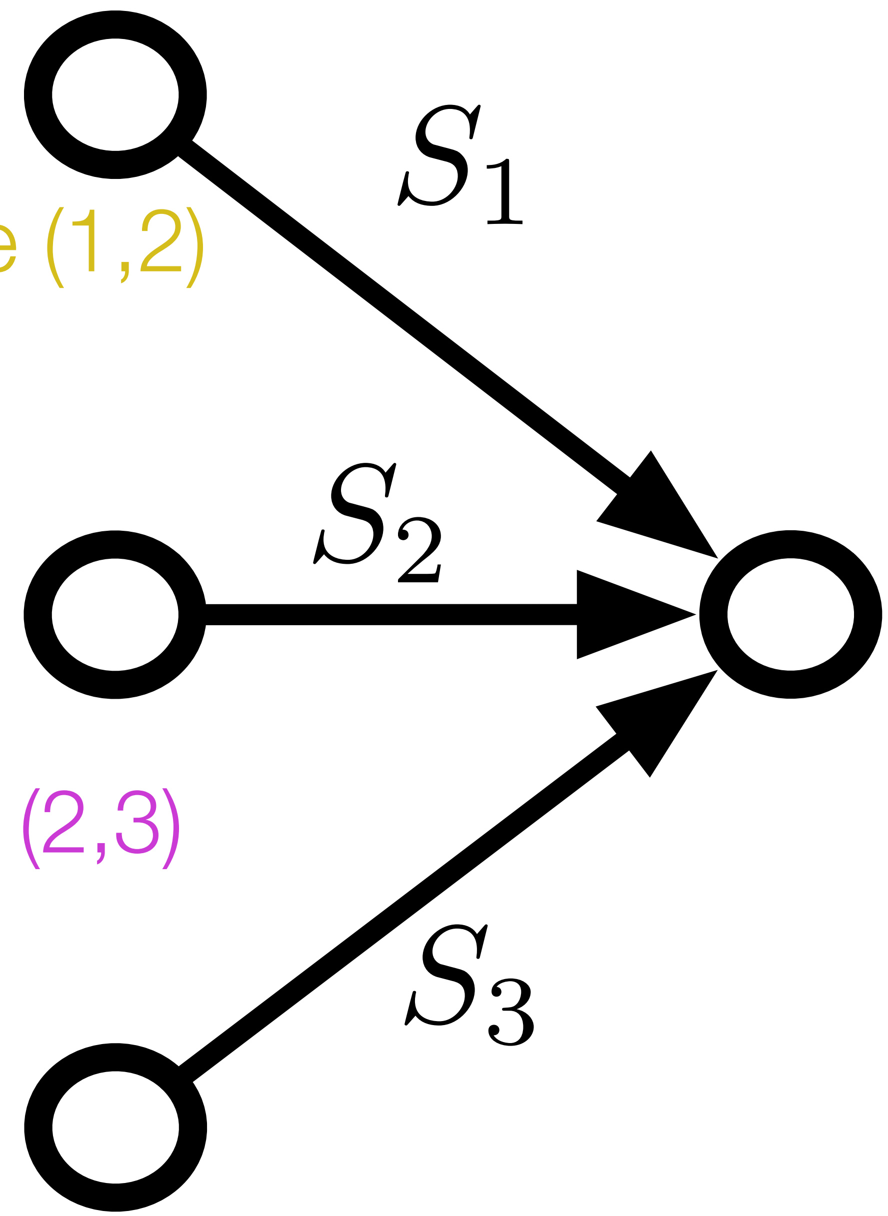
Beyond 2 users - MAC with common messages



$$\mathbf{u_1} = a_{11}\mathbf{w_1} \oplus a_{12}\mathbf{w_2} \oplus a_{13}\mathbf{w_3}$$

$$\mathbf{u_2} = a_{21}\mathbf{w_1} \oplus a_{22}\mathbf{w_2} \oplus a_{23}\mathbf{w_3}$$

$$\mathbf{u_3} = a_{31}\mathbf{w_1} \oplus a_{32}\mathbf{w_2} \oplus a_{33}\mathbf{w_3}$$

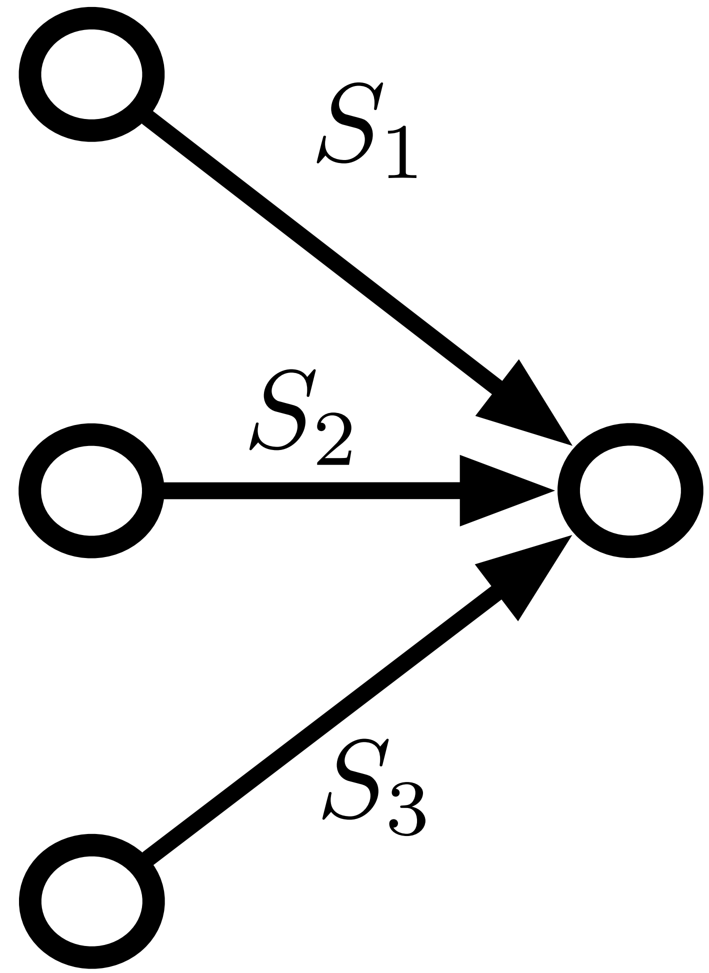


Beyond 2 users - Message and equation alignment

$$\mathbf{u_1} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \mathbf{w}_3$$

$$\mathbf{u_2} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus 3\mathbf{w}_3$$

$$\mathbf{u_3} = \mathbf{w}_1 \oplus 2\mathbf{w}_2 \oplus 3\mathbf{w}_3$$



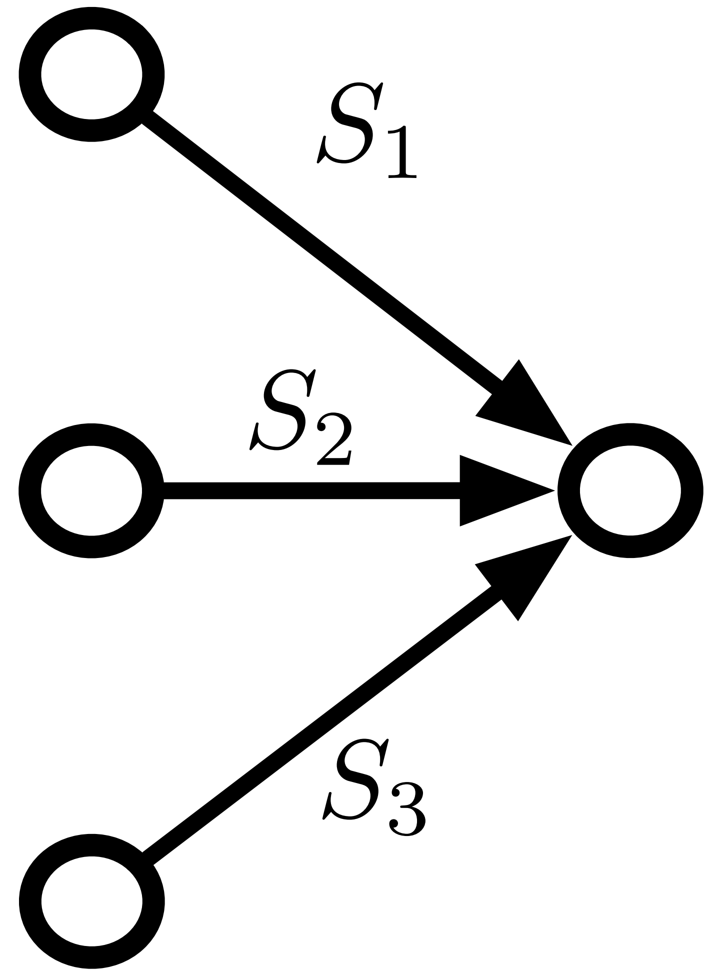
Beyond 2 users - Message and equation alignment

$$\mathbf{u_1} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \mathbf{w}_3$$

Sub-equation alignment

$$\mathbf{u_2} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus 3\mathbf{w}_3$$

$$\mathbf{u_3} = \mathbf{w}_1 \oplus 2\mathbf{w}_2 \oplus 3\mathbf{w}_3$$



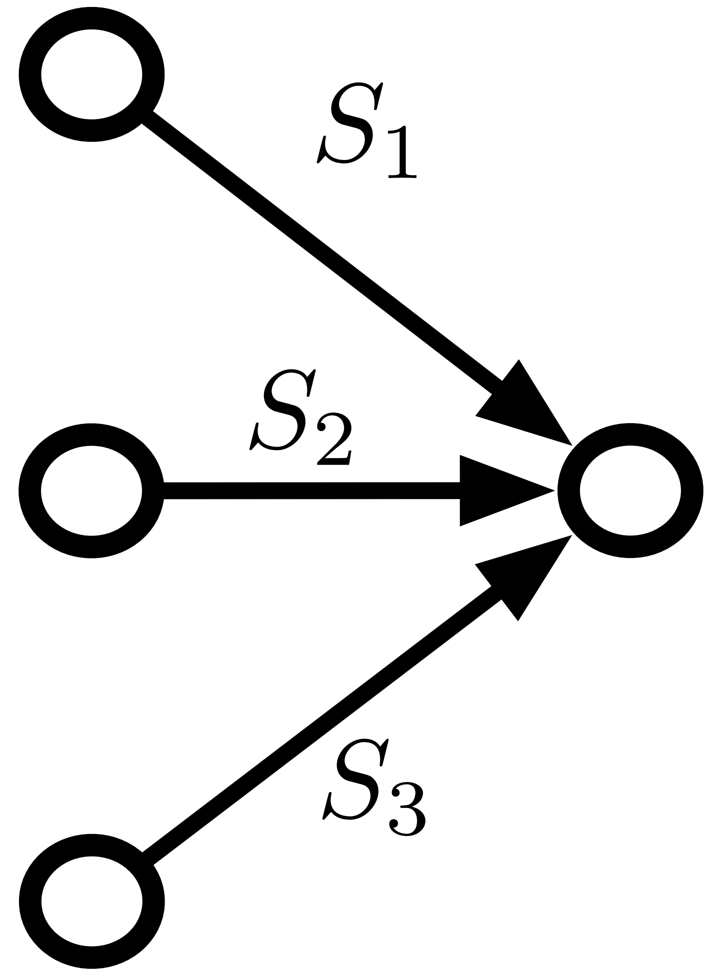
Beyond 2 users - Message and equation alignment

$$\mathbf{u_1} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \mathbf{w}_3$$

Sub-equation alignment

$$\mathbf{u_2} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus 3\mathbf{w}_3$$

$$\mathbf{u_3} = \mathbf{w}_1 \oplus 2\mathbf{w}_2 \oplus 3\mathbf{w}_3$$



$$\longrightarrow \quad |\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{n\,\min(R_1,R_2)} \text{ instead of } 2^{nR_{\mathrm{MIN}}}$$

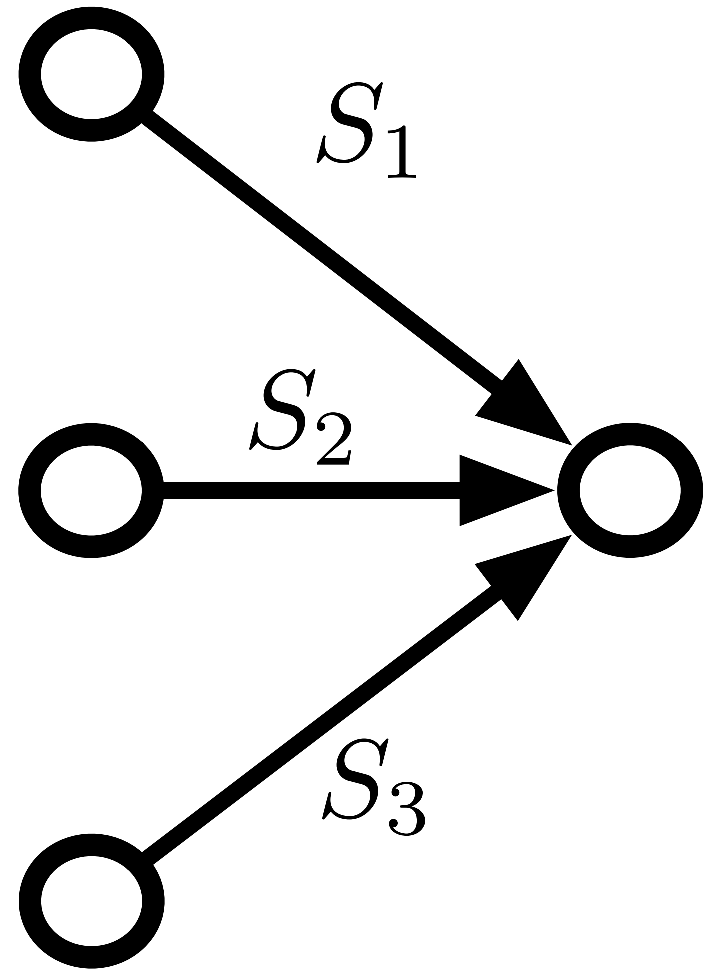
Beyond 2 users - Message and equation alignment

$$\mathbf{u_1} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus \mathbf{w}_3$$

Sub-equation alignment

$$\mathbf{u_2} = \mathbf{w}_1 \oplus \mathbf{w}_2 \oplus 3\mathbf{w}_3$$

$$\mathbf{u_3} = \mathbf{w}_1 \oplus 2\mathbf{w}_2 \oplus 3\mathbf{w}_3$$



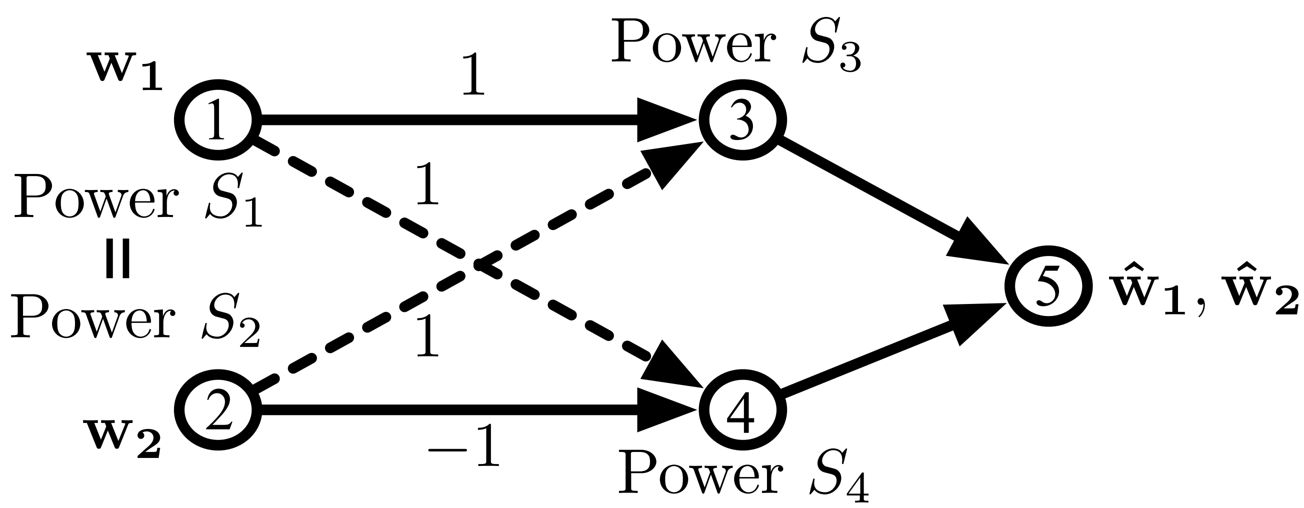
$|\mathcal{M}_{\mathbf{A}}(U_3|\mathbf{u}_1, \mathbf{u}_2)| = 2^{n \min(R_1, R_2)}$ instead of $2^{nR_{\text{MIN}}}$

Changes region!

Outline

- Problem statement
- Approach 1: allowable equations
- Approach 2: MAC with common messages
- Beyond 2 users
- Case study

Case study: exploiting interference



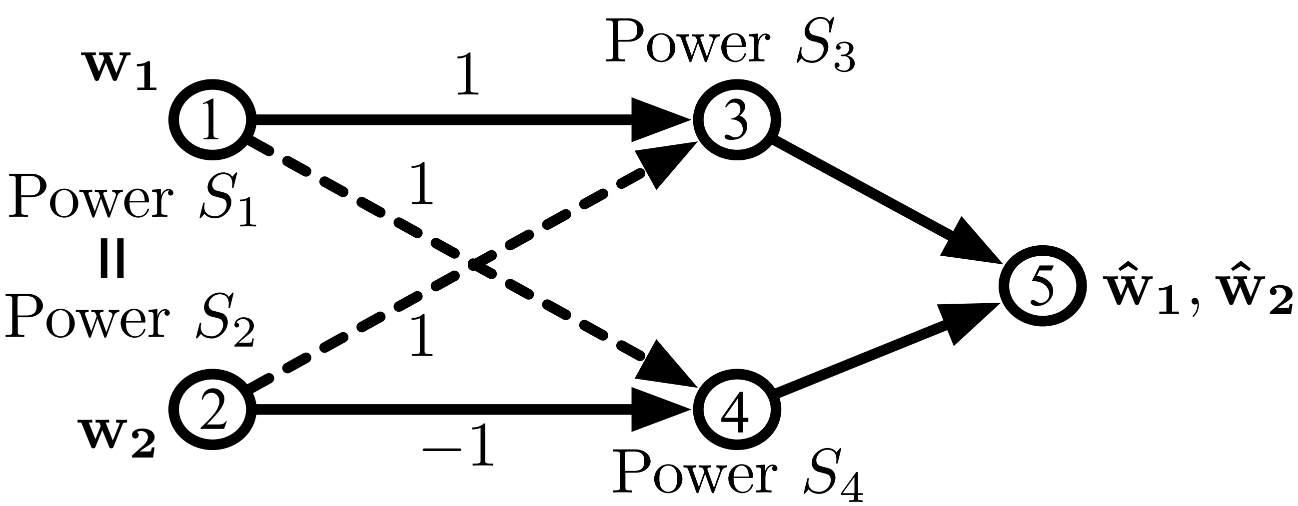
CF

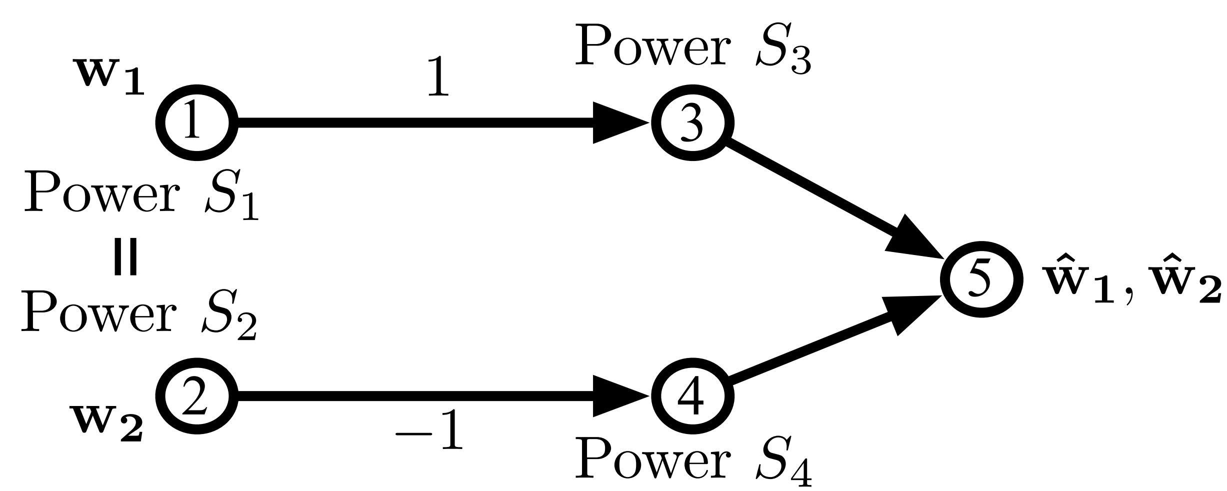
$$R_1 < \frac{1}{2}\log\left(\frac{1}{2} + S\right),$$
$$R_2 < \frac{1}{2}\log\left(\frac{1}{2} + S\right),$$

$$\min(R_1, R_2) < \min\left(\frac{1}{2}\log(1+S_3), \frac{1}{2}\log(1+S_4)\right)$$
$$R_1 + R_2 < \frac{1}{2}\log(1+S_3+S_4).$$

ICF

Case study: exploiting interference





CF

$$R_1 < \frac{1}{2}\log\left(\frac{1}{2} + S\right),$$

$$R_2 < \frac{1}{2}\log\left(\frac{1}{2} + S\right),$$

$$\min(R_1, R_2) < \min\left(\frac{1}{2}\log(1+S_3), \frac{1}{2}\log(1+S_4)\right)$$

$$R_1 + R_2 < \frac{1}{2}\log(1+S_3+S_4).$$

ICF

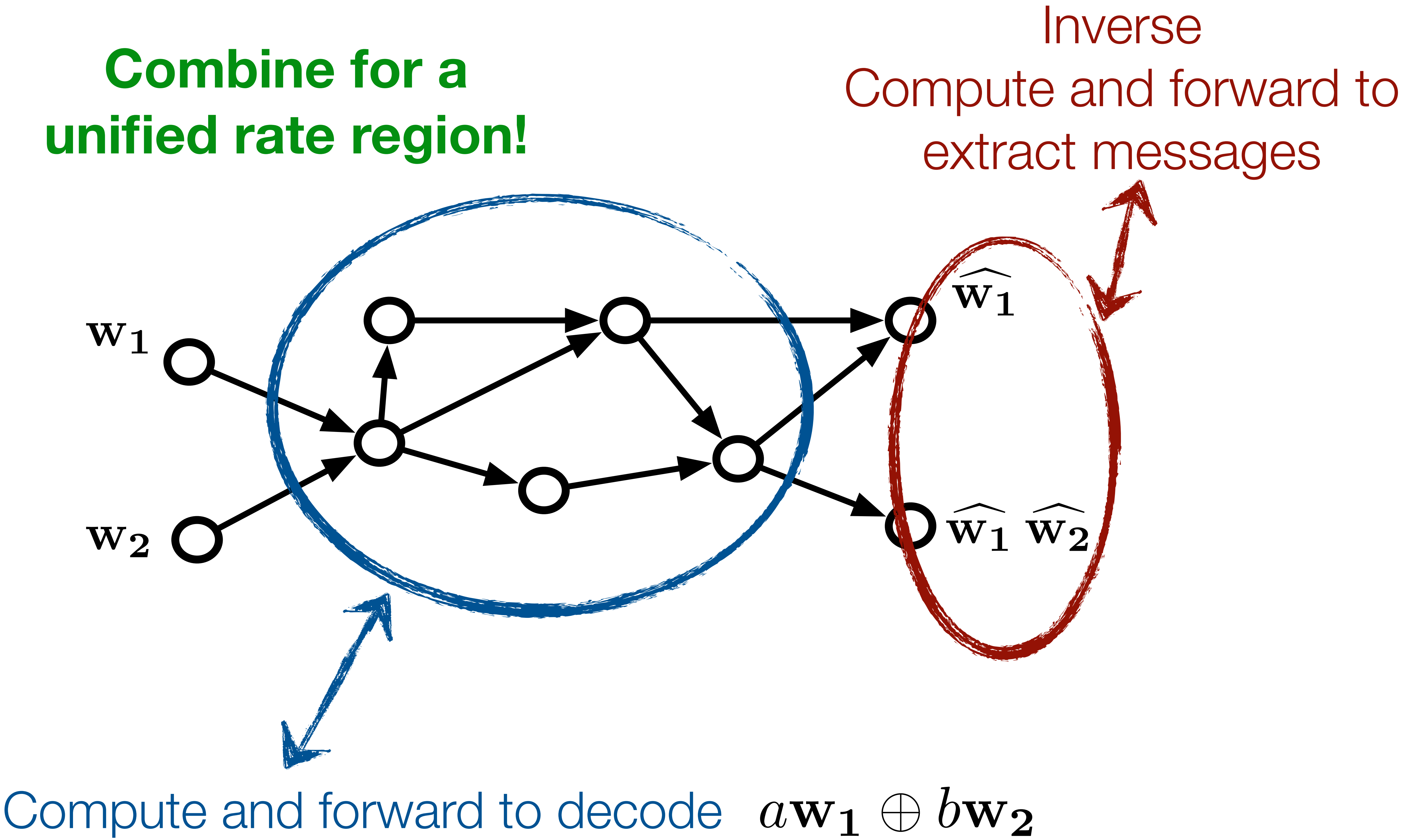
No interference

$$R_1 < \min\left\{\frac{1}{2}\log(1+S), \frac{1}{2}\log(1+S_3)\right\}$$

$$R_2 < \min\left\{\frac{1}{2}\log(1+S), \frac{1}{2}\log(1+S_4)\right\}$$

$$R_1 + R_2 < \frac{1}{2}\log(1+S_3+S_4).$$

Conclusion



Combine for a
unified rate region!
Inverse
Compute and forward to
extract messages
$\mathbf{w_1}$
$\mathbf{w_2}$
$\widehat{\mathbf{w_1}}$
$\widehat{\mathbf{w_1}}$ $\widehat{\mathbf{w_2}}$
Compute and forward to decode $a\mathbf{w_1} \oplus b\mathbf{w_2}$