On Field Size and Success Probability in Network Coding

Olav Geil, Ryutaroh Matsumoto, Casper Thomsen

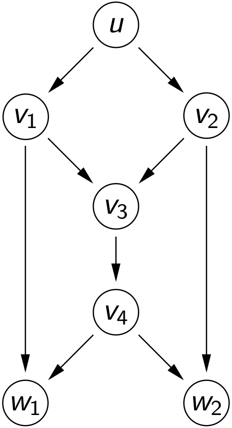
2008-07-09

Introduction

Results

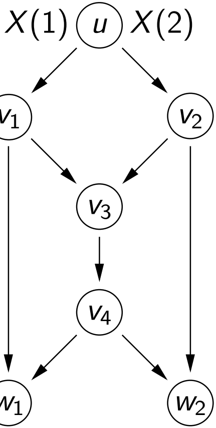
- Min. field size
- Improving bound
- Interpret $|M_w|$

The Usual Example



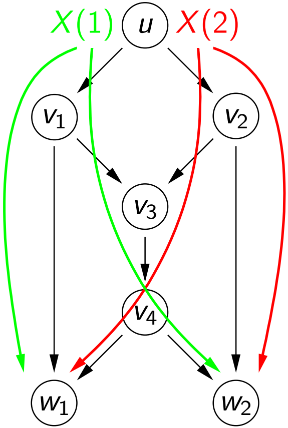
- Information network; DAG.
- Unit capacity edges
- Two unit source processes over $\mathbb{F}_{2^m}$ located at the source vertex u.
- Both receivers w_1 and w_2 wants information from both source processes.

The Usual Example



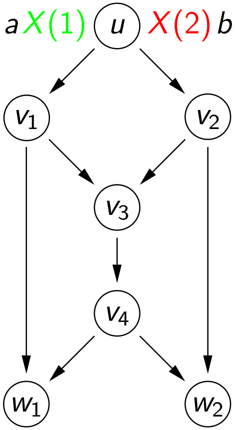
- Information network; DAG.
- Unit capacity edges
- Two unit source processes over $\mathbb{F}_{2^m}$ located at the source vertex u.
- Both receivers w_1 and w_2 wants information from both source processes.

The Usual Example

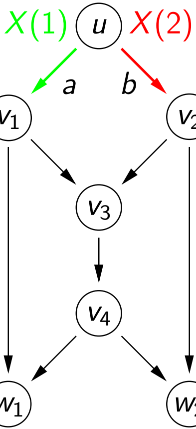


- Information network; DAG.
- Unit capacity edges
- Two unit source processes over $\mathbb{F}_{2^m}$ located at the source vertex u.
- Both receivers w_1 and w_2 wants information from both source processes.

Using Switching

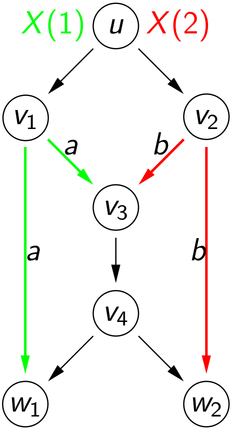


Using Switching



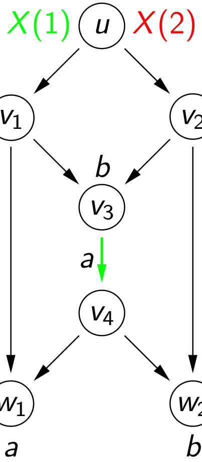
1
2
3
4
5

Using Switching



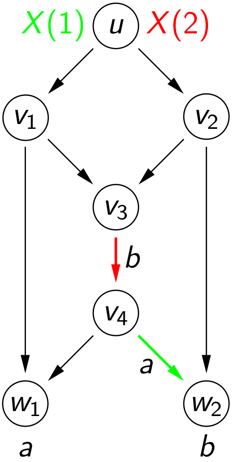
1
2
3
4
5

Using Switching



1
2
3
4
5

Using Switching



1

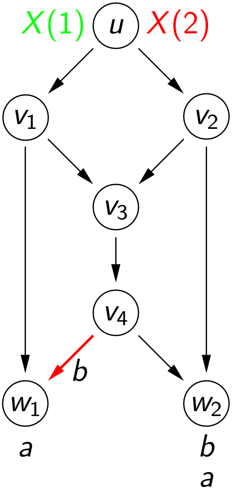
2

3

4

5

Using Switching



1

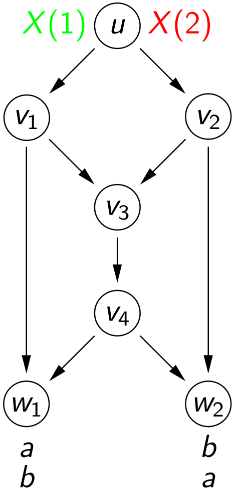
2

3

4

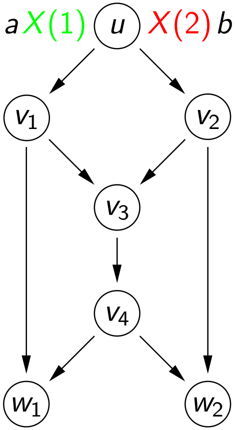
5

Using Switching



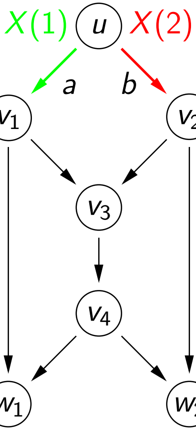
1
2
3
4
5

Using Network Coding



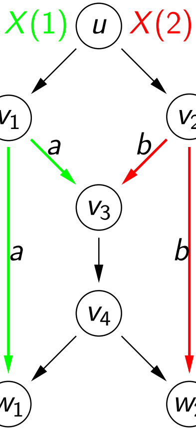
1
2
3
4

Using Network Coding



1
2
3
4

Using Network Coding



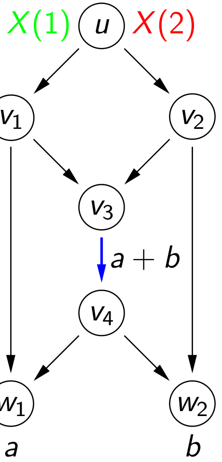
1

2

3

4

Using Network Coding



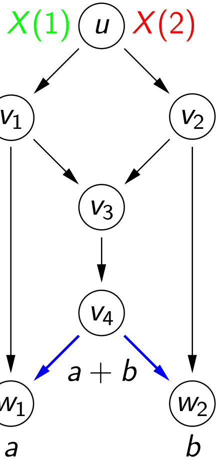
1

2

3

4

Using Network Coding



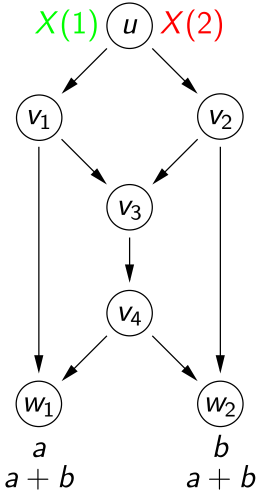
1

2

3

4

Using Network Coding



1

2

3

4

What About "Decoding"?

w_i must know how a and b is linearly combined.

$$\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = a + b$$

- Local coding vector

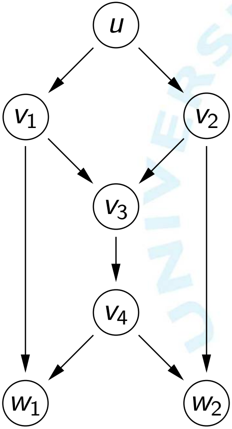
What About "Decoding"?

w_i must know how a and b is linearly combined.

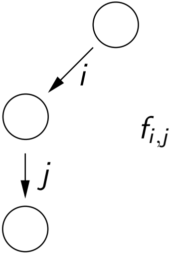
$$\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = a + b$$

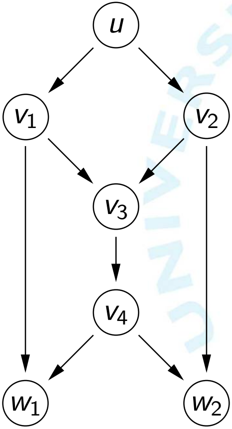
- Local coding vector

Formalizing . . .

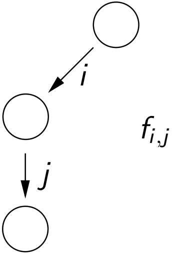


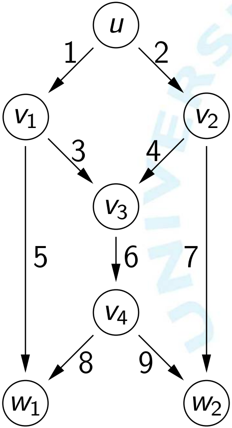
Formalizing . . .



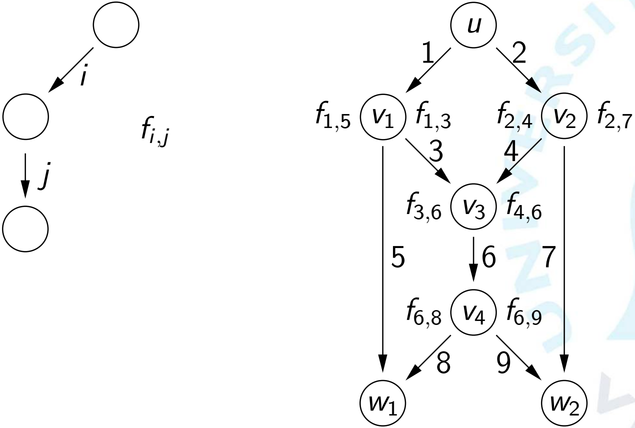


Formalizing . . .

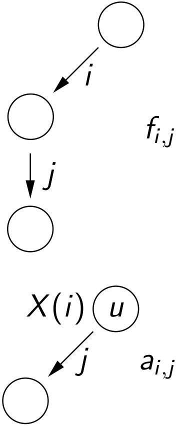


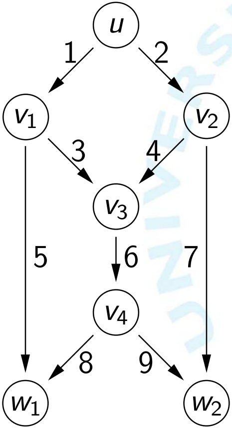


Formalizing . . .

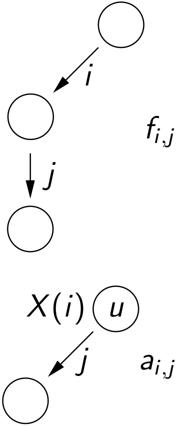


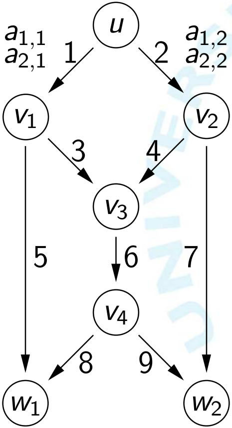
Formalizing . . .



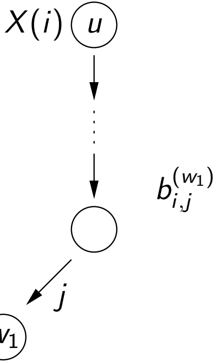


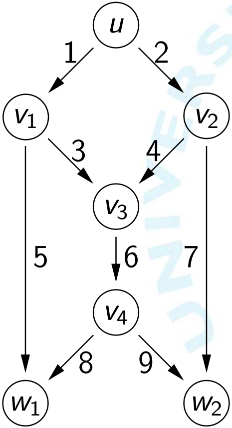
Formalizing . . .



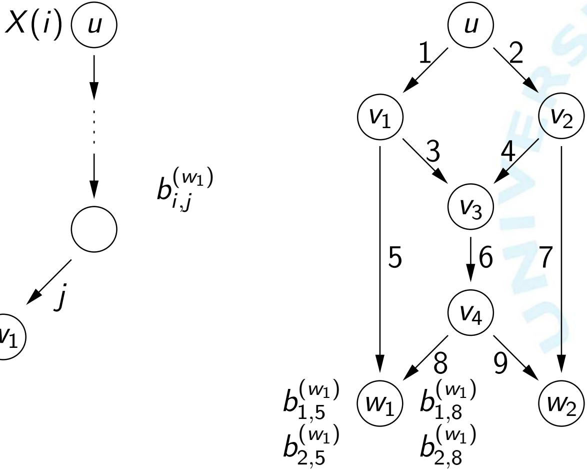


Formalizing . . .

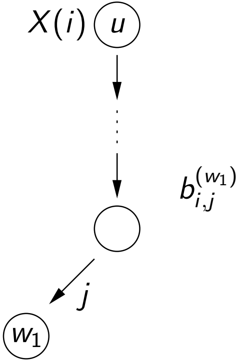


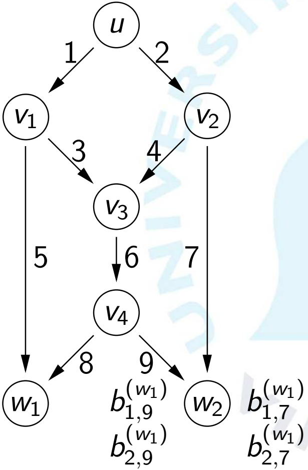


Formalizing . . .



Formalizing . . .





Formalizing . . . (contd)

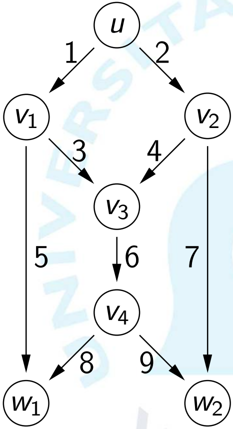
- $Y(1) = a_{1,1}X(1) + a_{2,1}X(2)$
- $Y(3) = f_{1,3}Y(1)$
- $Y(6) = f_{3,6}Y(3) + f_{4,6}Y(4)$

In general:

$$Y(j) = \sum_u a_{i,j}X(u) + \sum_i f_{i,j}Y(i)$$

"Decoding":

$$b_i^{(w)} = \sum_j b_{i,j}^{(w)}Y(j)$$



Formalizing . . . (contd)

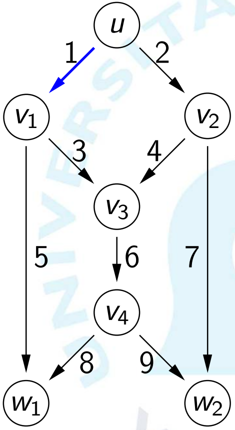
- $Y(1) = a_{1,1}X(1) + a_{2,1}X(2)$
- $Y(3) = f_{1,3}Y(1)$
- $Y(6) = f_{3,6}Y(3) + f_{4,6}Y(4)$

In general:

$$Y(j) = \sum_u a_{i,j}X(u) + \sum_i f_{i,j}Y(i)$$

"Decoding":

$$b_i^{(w)} = \sum_j b_{i,j}^{(w)}Y(j)$$



Formalizing . . . (contd)

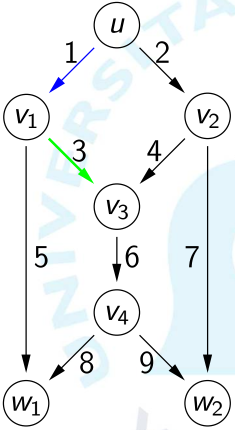
- $Y(1) = a_{1,1}X(1) + a_{2,1}X(2)$
- $Y(3) = f_{1,3}Y(1)$
- $Y(6) = f_{3,6}Y(3) + f_{4,6}Y(4)$

In general:

$$Y(j) = \sum_u a_{i,j}X(u) + \sum_i f_{i,j}Y(i)$$

"Decoding":

$$b_i^{(w)} = \sum_j b_{i,j}^{(w)} Y(j)$$



Formalizing . . . (contd)

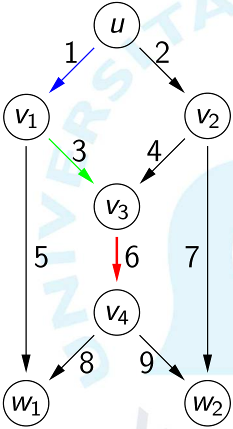
- $Y(1) = a_{1,1}X(1) + a_{2,1}X(2)$
- $Y(3) = f_{1,3}Y(1)$
- $Y(6) = f_{3,6}Y(3) + f_{4,6}Y(4)$

In general:

$$Y(j) = \sum_{u} a_{i,j}X(u) + \sum_{i} f_{i,j}Y(i)$$

"Decoding":

$$b_i^{(w)} = \sum_{j} b_{i,j}^{(w)} Y(j)$$



Formalizing . . . (contd)

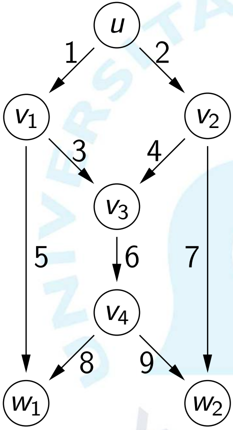
- $Y(1) = a_{1,1}X(1) + a_{2,1}X(2)$
- $Y(3) = f_{1,3}Y(1)$
- $Y(6) = f_{3,6}Y(3) + f_{4,6}Y(4)$

In general:

$$Y(j) = \sum_u a_{i,j}X(u) + \sum_i f_{i,j}Y(i)$$

"Decoding":

$$b_i^{(w)} = \sum_j b_{i,j}^{(w)} Y(j)$$



Success Criterion

Theorem

$$M_w := \begin{bmatrix} (a_{i,j}) & 0 \\ I - (f_{i,j}) & (b_{i,j}^{(w)})^T \end{bmatrix};$$

$$|M_w| \neq 0 \textit{ in } \mathbb{F}_{2^m} \quad \Longleftrightarrow \quad \textit{Receiver } w \textit{ can decode.}$$

(Koetter et al. (2003) and Ho et al. (2006))

$$P := \prod_w |M_w| \neq 0 \text{ in } \mathbb{F}_{2^m}?$$

Success Criterion

Theorem

$$M_w := \begin{bmatrix} (a_{i,j}) & 0 \\ I - (f_{i,j}) & (b_{i,j}^{(w)})^T \end{bmatrix};$$

$$|M_w| \neq 0 \text{ in } \mathbb{F}_{2^m} \iff \text{Receiver } w \text{ can decode.}$$

(Koetter et al. (2003) and Ho et al. (2006))

$$P := \prod_w |M_w| \neq 0 \text{ in } \mathbb{F}_{2^m}?$$

Results

1. Minimum field size of given characteristic. (Imply that finding the polynomial is NP-complete.)
2. Improving a bound for random network coding.
3. Topological interpretation of $|M_w|$.

Minimum field size of given characteristic

What Is known

Choose $a_{i,j}$'s, $f_{i,j}$'s and $b_{i,j}^{(w)}$'s from a finite field.

Field size $\geq$ no. of receivers

(Koetter et al. (2003))

- Utilizing the fact that for

$$F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$$

then there exists

$$(x_1, \ldots, x_n) \in \mathbb{F}_q^n \quad \text{such that} \quad F(x_1, \ldots, x_n) \neq 0$$

if and only if

$$F(X_1, \ldots, X_n) \text{ rem } (X_1^q - X_1, \ldots, X_n^q - X_n) \neq 0.$$

- Reduce P modulo

$$\{a_{i,j}^q - a_{i,j}, \ldots, f_{i,j}^q - f_{i,j}, \ldots, (b_{i,j}^{(w)})^q - b_{i,j}^{(w)}\}.$$

(Fast!)

- Utilizing the fact that for

$$F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$$

then there exists

$$(x_1, \ldots, x_n) \in \mathbb{F}_q^n \quad \text{such that} \quad F(x_1, \ldots, x_n) \neq 0$$

if and only if

$$F(X_1, \ldots, X_n) \text{ rem } (X_1^q - X_1, \ldots, X_n^q - X_n) \neq 0.$$

- Reduce P modulo

$$\{a_{i,j}^q - a_{i,j}, \ldots, f_{i,j}^q - f_{i,j}, \ldots, (b_{i,j}^{(w)})^q - b_{i,j}^{(w)}\}.$$

(Fast!)

- Utilizing the fact that for

$$F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$$

then there exists

$$(x_1, \ldots, x_n) \in \mathbb{F}_q^n \quad \text{such that} \quad F(x_1, \ldots, x_n) \neq 0$$

if and only if

$$F(X_1, \ldots, X_n) \text{ rem } (X_1^q - X_1, \ldots, X_n^q - X_n) \neq 0.$$

- Reduce P modulo

$$\{a_{i,j}^q - a_{i,j}, \ldots, f_{i,j}^q - f_{i,j}, \ldots, \cancel{(b_{i,j}^{(w)})^q - b_{i,j}^{(w)}}\}.$$

(Fast!)

The Method

- For characteristic p: If P rem p reduces to 0 modulo the $a_{i,j}$'s and $f_{i,j}$'s in $\mathbb{F}_p$, then try $\mathbb{F}_{p^2}$. Etc.
- Max $\lfloor \log_p(\text{no. receivers}) \rfloor$ trials.
- Easy to find the $a_{i,j}$'s and $f_{i,j}$'s afterwards:
  - $\mathbb{F}_q$ large enough.
  - $F \in \mathbb{F}_q(X_1, \ldots, X_{n-1})[X_n]$.
  - Choose $X_n = z_n$ s.t. F is nonzero; possible because $\deg_{X_n}(F) \leq q - 1$.
  - Find $F(X_1, \ldots, X_{n-1}, z_n) \in \mathbb{F}_q[X_1, \ldots, X_{n-1}]$.
  - Continue.
- Quite fast. (Finding P is NP-complete.)

The Method

- For characteristic p: If P rem p reduces to 0 modulo the $a_{i,j}$'s and $f_{i,j}$'s in $\mathbb{F}_p$, then try $\mathbb{F}_{p^2}$. Etc.
- Max $\lfloor \log_p(\text{no. receivers}) \rfloor$ trials.
- Easy to find the $a_{i,j}$'s and $f_{i,j}$'s afterwards:
  - $\mathbb{F}_q$ large enough.
  - $F \in \mathbb{F}_q(X_1, \ldots, X_{n-1})[X_n]$.
  - Choose $X_n = z_n$ s.t. F is nonzero; possible because $\deg_{X_n}(F) \leq q - 1$.
  - Find $F(X_1, \ldots, X_{n-1}, z_n) \in \mathbb{F}_q[X_1, \ldots, X_{n-1}]$.
  - Continue.
- Quite fast. (Finding P is NP-complete.)

The Method

- For characteristic p: If P rem p reduces to 0 modulo the $a_{i,j}$'s and $f_{i,j}$'s in $\mathbb{F}_p$, then try $\mathbb{F}_{p^2}$. Etc.
- Max $\lfloor \log_p(\text{no. receivers}) \rfloor$ trials.
- Easy to find the $a_{i,j}$'s and $f_{i,j}$'s afterwards:
  - $\mathbb{F}_q$ large enough.
  - $F \in \mathbb{F}_q(X_1, \ldots, X_{n-1})[X_n]$.
  - Choose $X_n = z_n$ s.t. F is nonzero; possible because $\deg_{X_n}(F) \leq q - 1$.
  - Find $F(X_1, \ldots, X_{n-1}, z_n) \in \mathbb{F}_q[X_1, \ldots, X_{n-1}]$.
  - Continue.
- Quite fast. (Finding P is NP-complete.)

Improving a bound for random network coding

Introducing Randomized Network Coding

Choose the $a_{i,j}$'s and $f_{i,j}$'s uniformly i.i.d.

- ...then hope that you can choose the $b_{i,j}^{(w)}$'s such that P is nonzero.
- Success probability.

Introducing Randomized Network Coding

Choose the $a_{i,j}$'s and $f_{i,j}$'s uniformly i.i.d.

- ...then hope that you can choose the $b_{i,j}^{(w)}$'s such that P is nonzero.
- Success probability.

Introducing Randomized Network Coding

Choose the $a_{i,j}$'s and $f_{i,j}$'s uniformly i.i.d.

- ... then hope that you can choose the $b_{i,j}^{(w)}$'s such that P is nonzero.
- Success probability.

What Is Known

- q The field size.
- d The number of receivers.
- μ The number of randomly chosen variables.
- η The number of edges j where $Y(j)$ depends on randomly chosen $a_{i,j}$'s and $f_{i,j}$'s.

$$\text{Success probability} \geq \frac{(q-d)^\eta}{q^\eta}$$

(Ho et al. (2006))

What Is Known

- q The field size.
- d The number of receivers.
- μ The number of randomly chosen variables.
- η The number of edges j where $Y(j)$ depends on randomly chosen $a_{i,j}$'s and $f_{i,j}$'s.

$$\text{Success probability} \geq \frac{(q-d)^\eta}{q^\eta}$$

(Ho et al. (2006))

$$\text{Success probability} \geq \frac{(q-1)^\eta}{q^\eta}$$

What Is Known

- q The field size.
- d The number of receivers.
- μ The number of randomly chosen variables.
- η The number of edges j where $Y(j)$ depends on randomly chosen $a_{i,j}$'s and $f_{i,j}$'s.

$$\text{Success probability} \geq \frac{(q-d)^\eta}{q^\eta}$$

(Ho et al. (2006))

~~$$\text{Success probability} \geq \frac{(q-1)^\eta}{q^\eta}$$~~

Our bound

- $\widehat{P} \in \mathbb{F}_q[X_1, \ldots, X_\mu]$ the remainder of P modulo $X_1^q - X_1, \ldots, X_\mu^q - X_\mu$.
- Assume $\mathrm{LM}(\widehat{P}) = X_1^{j_1} \cdots X_\mu^{j_\mu}$. (Any monomial ordering.)

$$\text{Success probability} \geq \frac{(q - j_1) \cdots (q - j_\mu)}{q^\mu}$$

since $\frac{(q-j_1)\cdots(q-j_\mu)}{q^\mu} \geq \frac{q-(j_1+\cdots+j_\mu)}{q}$.

Our bound

- $\widehat{P} \in \mathbb{F}_q[X_1, \ldots, X_\mu]$ the remainder of P modulo $X_1^q - X_1, \ldots, X_\mu^q - X_\mu$.
- Assume $\mathrm{LM}(\widehat{P}) = X_1^{j_1} \cdots X_\mu^{j_\mu}$. (Any monomial ordering.)

$$\text{Success probability} \geq \frac{(q - j_1) \cdots (q - j_\mu)}{q^\mu}$$

since $\frac{(q-j_1)\cdots(q-j_\mu)}{q^\mu} \geq \frac{q-(j_1+\cdots+j_\mu)}{q}$.

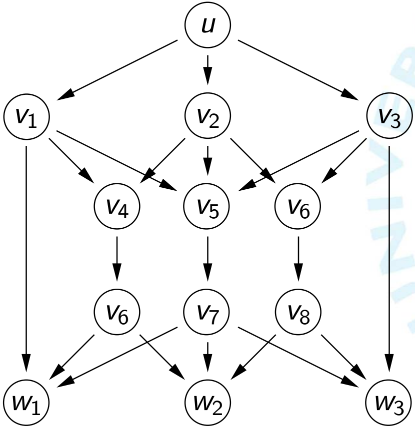
Our bound

- $\widehat{P} \in \mathbb{F}_q[X_1, \ldots, X_\mu]$ the remainder of P modulo $X_1^q - X_1, \ldots, X_\mu^q - X_\mu$.
- Assume $\mathrm{LM}(\widehat{P}) = X_1^{j_1} \cdots X_\mu^{j_\mu}$. (Any monomial ordering.)

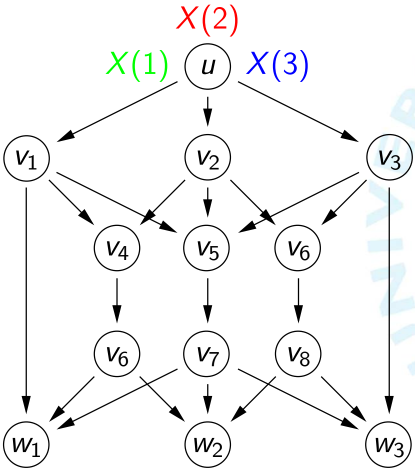
$$\text{Success probability} \geq \frac{(q-j_1)\cdots(q-j_\mu)}{q^\mu} \geq \frac{(q-d)^\eta}{q^\eta}$$

since $\frac{(q-j_1)\cdots(q-j_\mu)}{q^\mu} \geq \frac{q-(j_1+\cdots+j_\mu)}{q}$.

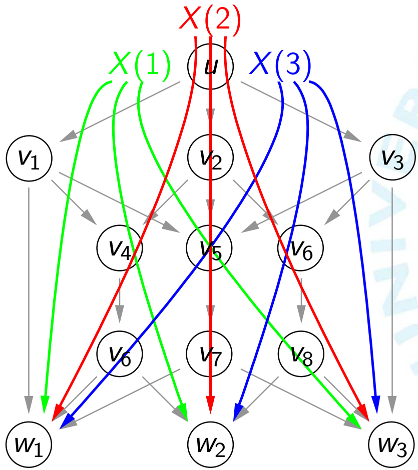
Improvement?



Improvement?

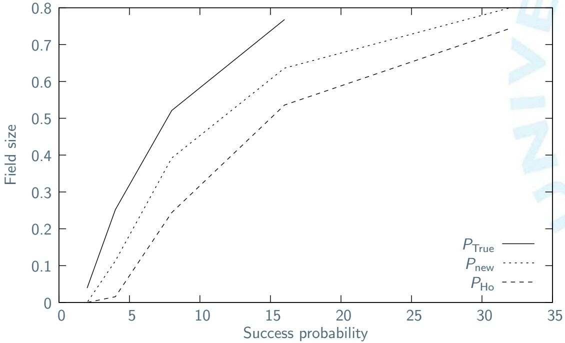


Improvement?

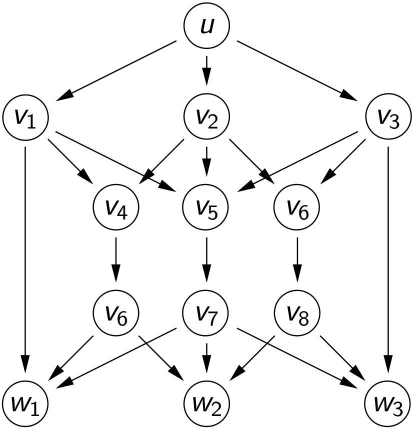


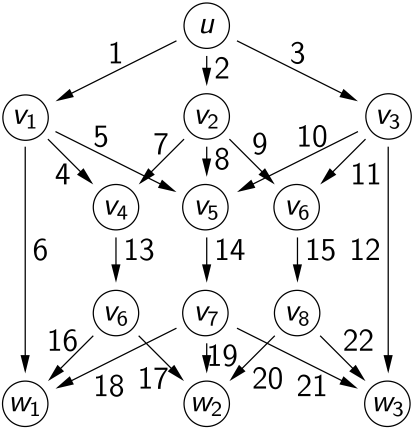
Improvement? (contd)

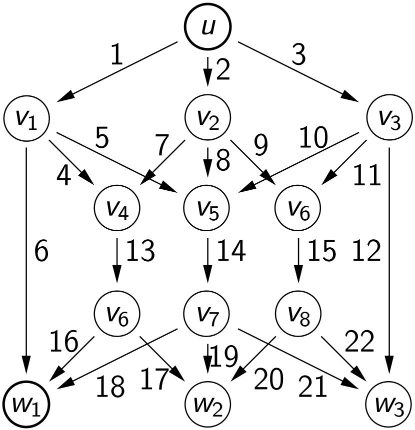
q	2	4	8	16	32
$P_{\text{true}}(q)$	0.039	0.252	0.521	0.768	?
$P_{\text{new}}(q)$	$0.610 \cdot 10^{-4}$	0.133	0.392	0.636	0.800
$P_{\text{Ho}}(q)$	0	$0.156 \cdot 10^{-1}$	0.244	0.536	0.744



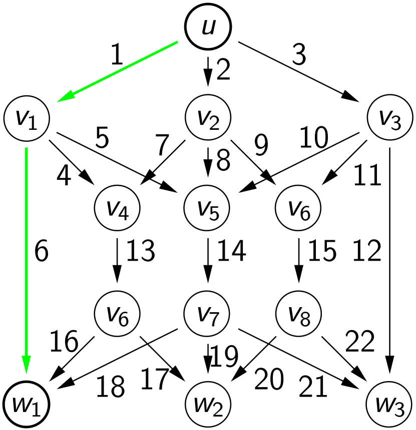
Topological Interpretation of $|M_w|$


u
v1
v2
v3
v4
v5
v6
v6
v7
v8
w1
w2
w3

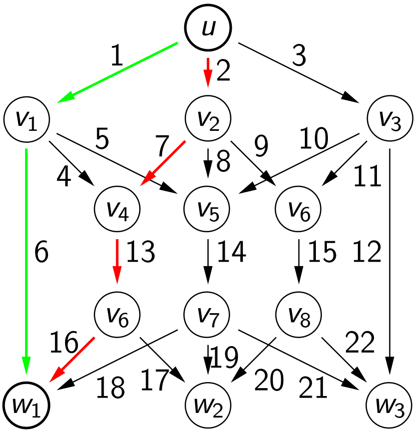

u
1
2
3
v_1
v_2
v_3
5
7
9
10
8
4
11
v_4
v_5
v_6
6
13
14
15
12
v_6
v_7
v_8
16
19
22
18
17
20
21
w_1
w_2
w_3


u
1
2
3
v_1
v_2
v_3
5
7
9
10
8
4
11
v_4
v_5
v_6
6
13
14
15
12
v_6
v_7
v_8
16
19
22
18
17
20
21
w_1
w_2
w_3

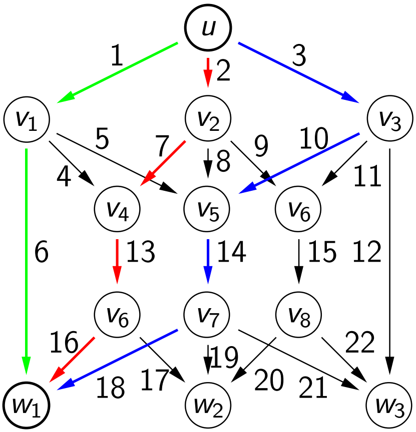
$$|M_{w_1}| = Q_1$$


u
1
2
3
v1
v2
v3
5
7
9
10
4
8
11
v4
v5
v6
6
13
14
15
12
v6
v7
v8
16
19
22
18
17
20
21
w1
w2
w3

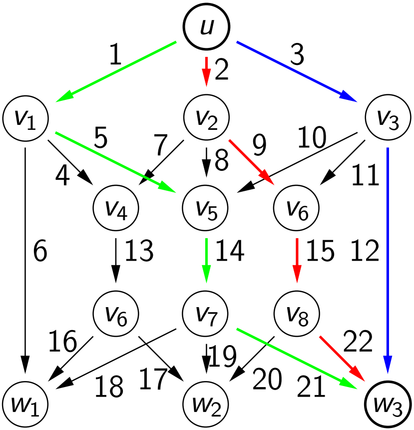
$|M_{w_1}| = Q_1 \; f_{1,6}$



$|M_{w_1}| = Q_1 \; f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$

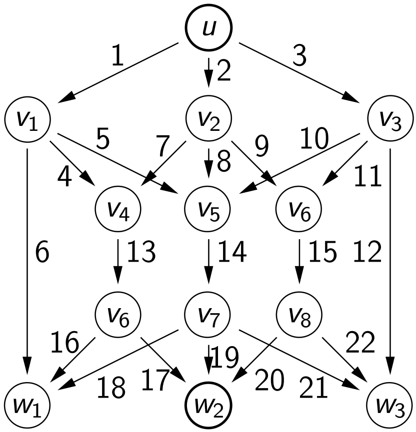


$|M_{w_1}| = Q_1 \; f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$



$$|M_{w_1}| = Q_1 \; f_{1,6} \cdot f_{2,7} f_{7,13} f_{13,16} \cdot f_{3,10} f_{10,14} f_{14,18}$$

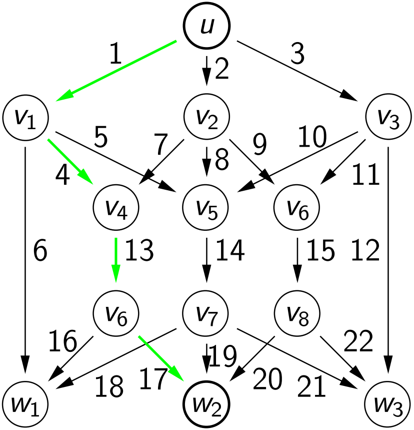
$$|M_{w_3}| = Q_2 \; f_{1,5} f_{5,14} f_{14,21} \cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$$



$$|M_{w_1}| = Q_1 \; f_{1,6} \cdot f_{2,7} f_{7,13} f_{13,16} \cdot f_{3,10} f_{10,14} f_{14,18}$$

$$|M_{w_3}| = Q_2 \; f_{1,5} f_{5,14} f_{14,21} \cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$$

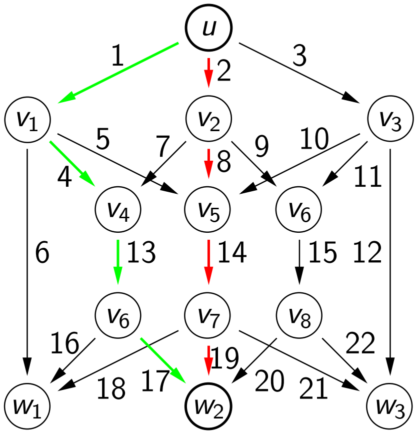
$$|M_{w_2}| = Q_3$$



$|M_{w_1}| = Q_1 \; f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

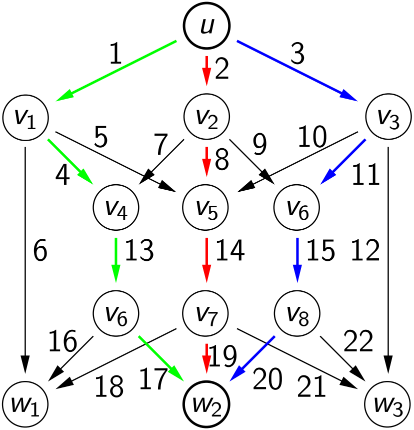
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$



$|M_{w_1}| = Q_1\ f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

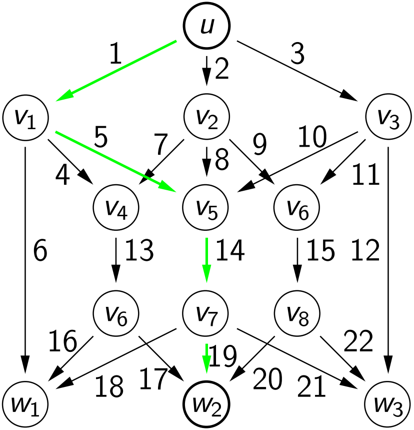
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$



$|M_{w_1}| = Q_1 \ f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

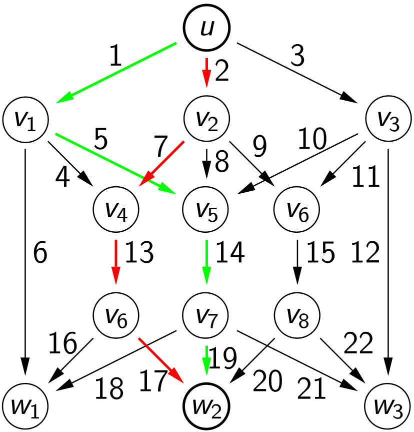
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$



$|M_{w_1}| = Q_1\ f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

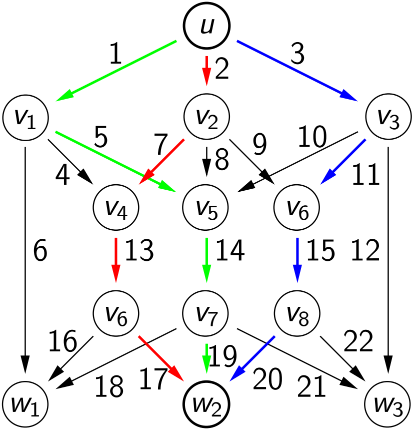
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$
$+ f_{1,5} f_{5,14} f_{14,19}$



$|M_{w_1}| = Q_1 \; f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

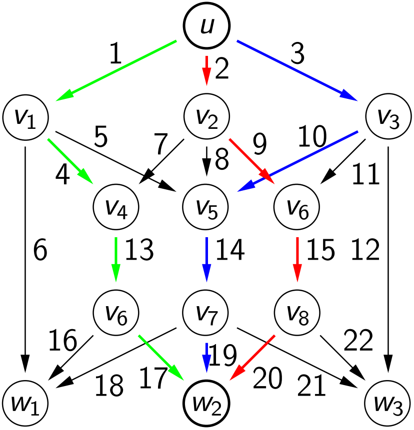
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$
$+ f_{1,5} f_{5,14} f_{14,19}$
$\cdot f_{2,7} f_{7,13} f_{13,17}$



$|M_{w_1}| = Q_1 \; f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

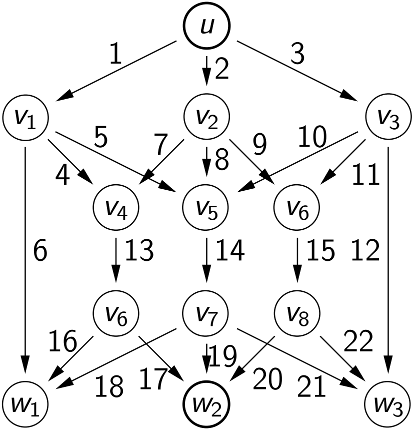
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$
$+ f_{1,5} f_{5,14} f_{14,19}$
$\cdot f_{2,7} f_{7,13} f_{13,17}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$



$|M_{w_1}| = Q_1 \ f_{1,6}$
$\cdot f_{2,7} f_{7,13} f_{13,16}$
$\cdot f_{3,10} f_{10,14} f_{14,18}$

$|M_{w_3}| = Q_2$
$f_{1,5} f_{5,14} f_{14,21}$
$\cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$

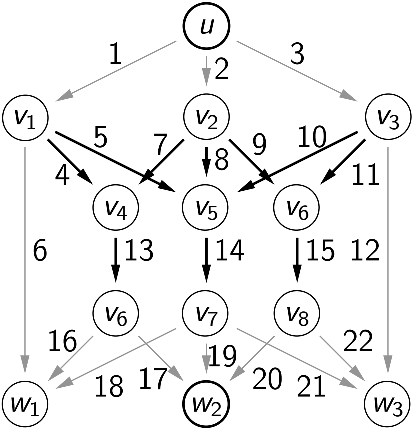
$|M_{w_2}| = Q_3$
$f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,8} f_{8,14} f_{14,19}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$
$+ f_{1,5} f_{5,14} f_{14,19}$
$\cdot f_{2,7} f_{7,13} f_{13,17}$
$\cdot f_{3,11} f_{11,15} f_{15,20}$
$+ f_{1,4} f_{4,13} f_{13,17}$
$\cdot f_{2,9} f_{9,15} f_{15,20}$
$\cdot f_{3,10} f_{10,14} f_{14,19}$



$$|M_{w_1}| = Q_1 \ f_{1,6} \cdot f_{2,7} f_{7,13} f_{13,16} \cdot f_{3,10} f_{10,14} f_{14,18}$$

$$|M_{w_3}| = Q_2 \ f_{1,5} f_{5,14} f_{14,21} \cdot f_{2,9} f_{9,15} f_{15,22} \cdot f_{3,12}$$

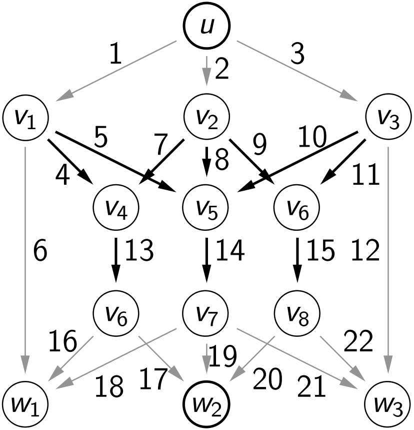
$$|M_{w_2}| = Q_3 \ f_{1,4} f_{4,13} f_{13,17} \cdot f_{2,8} f_{8,14} f_{14,19} \cdot f_{3,11} f_{11,15} f_{15,20} + f_{1,5} f_{5,14} f_{14,19} \cdot f_{2,7} f_{7,13} f_{13,17} \cdot f_{3,11} f_{11,15} f_{15,20} + f_{1,4} f_{4,13} f_{13,17} \cdot f_{2,9} f_{9,15} f_{15,20} \cdot f_{3,10} f_{10,14} f_{14,19}$$



$$|M_{w_1}| = Q_1 \; \cancel{f_{1,6}} \cdot \cancel{f_{2,7}} f_{7,13} \cancel{f_{13,16}} \cdot \cancel{f_{3,10}} f_{10,14} \cancel{f_{14,18}}$$

$$|M_{w_3}| = Q_2 \; \cancel{f_{1,5}} f_{5,14} \cancel{f_{14,21}} \cdot \cancel{f_{2,9}} f_{9,15} \cancel{f_{15,22}} \cdot \cancel{f_{3,12}}$$

$$|M_{w_2}| = Q_3 \; \cancel{f_{1,4}} f_{4,13} \cancel{f_{13,17}} \cdot \cancel{f_{2,8}} f_{8,14} \cancel{f_{14,19}} \cdot \cancel{f_{3,11}} f_{11,15} \cancel{f_{15,20}} + \cancel{f_{1,5}} f_{5,14} \cancel{f_{14,19}} \cdot \cancel{f_{2,7}} f_{7,13} \cancel{f_{13,17}} \cdot \cancel{f_{3,11}} f_{11,15} \cancel{f_{15,20}} + \cancel{f_{1,4}} f_{4,13} \cancel{f_{13,17}} \cdot \cancel{f_{2,9}} f_{9,15} \cancel{f_{15,20}} \cdot \cancel{f_{3,10}} f_{10,14} \cancel{f_{14,19}}$$



$|M_{w_1}| = Q_1 \quad f_{7,13} \cdot f_{10,14}$

$|M_{w_3}| = Q_2 \; f_{5,14} \cdot f_{9,15}$

$|M_{w_2}| = Q_3$
$f_{4,13} \cdot f_{8,14} \cdot f_{11,15}$
$+ f_{5,14} \cdot f_{7,13} \cdot f_{11,15}$
$+ f_{4,13} \cdot f_{9,15} \cdot f_{10,14}$

$$P = Q_1 Q_2 Q_3 \cdot f_{7,13} f_{10,14} \cdot f_{5,14} f_{9,15} \cdot (f_{4,13} f_{8,14} f_{11,15} + f_{5,14} f_{7,13} f_{11,15} + f_{4,13} f_{9,15} f_{10,14})$$

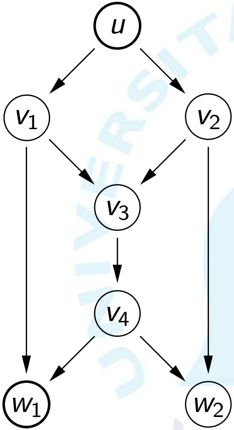
End

Theorem

Given a network connection problem as outlined above where the min-cut from the source vertex u to each receiver w_i is at least h, the number of sources processes. Then there exists a large enough finite field $\mathbb{F}_q$ in which inner vertices linearly combine the input symbols and send the linear combination to the out-edges such that each receiver w_i receive information at a rate equal to h.

Definition (min-cut)

The min-cut from a vertex u to a vertex w in a directed graph is the least number of edges that can be removed from the graph such that there is no path from u to w.



Theorem

Given a network connection problem as outlined above where the min-cut from the source vertex u to each receiver w_i *is at least h, the number of sources processes. Then there exists a large enough finite field* $\mathbb{F}_q$ *in which inner vertices linearly combine the input symbols and send the linear combination to the out-edges such that each receiver* w_i *receive information at a rate equal to h.*