

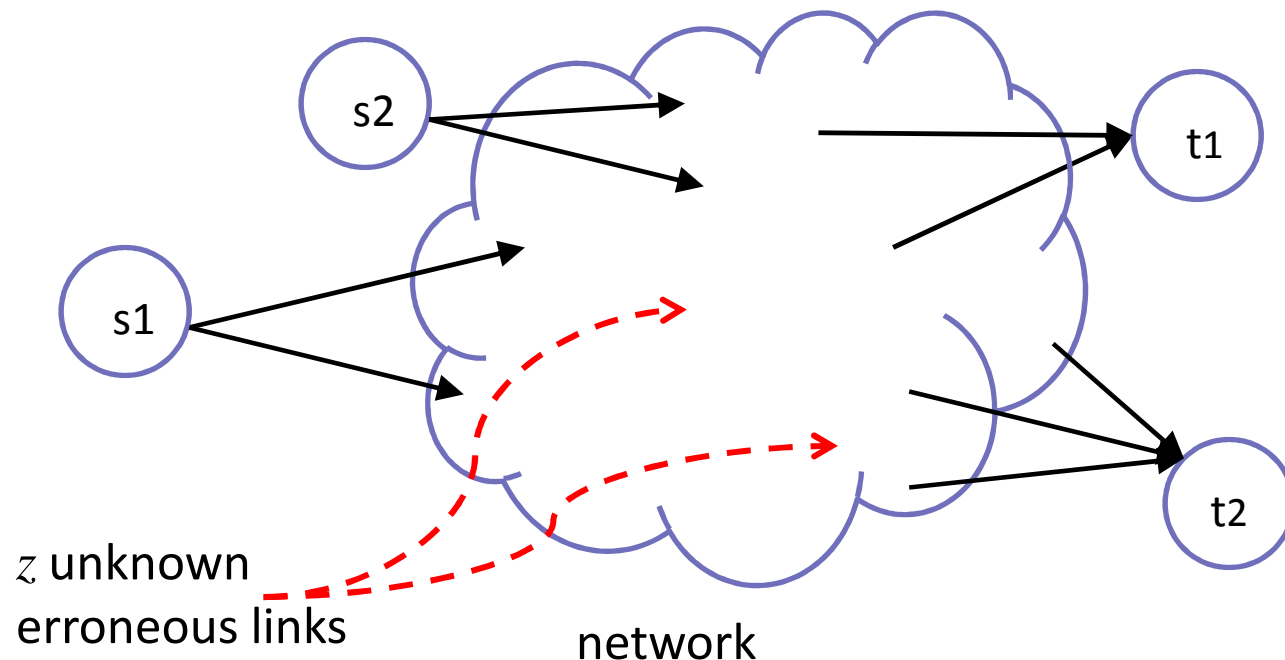


On error and erasure correction coding for networks and deadlines

Tracey Ho
Caltech

Stanford, October 2011

Network error correction problem



- Problem of reliable communication under arbitrary errors on z links (or packets)
- The set of erroneous links is fixed but unknown to the network user $\rightarrow$ cannot do error correction on individual links separately
- Erasure correction is a related problem

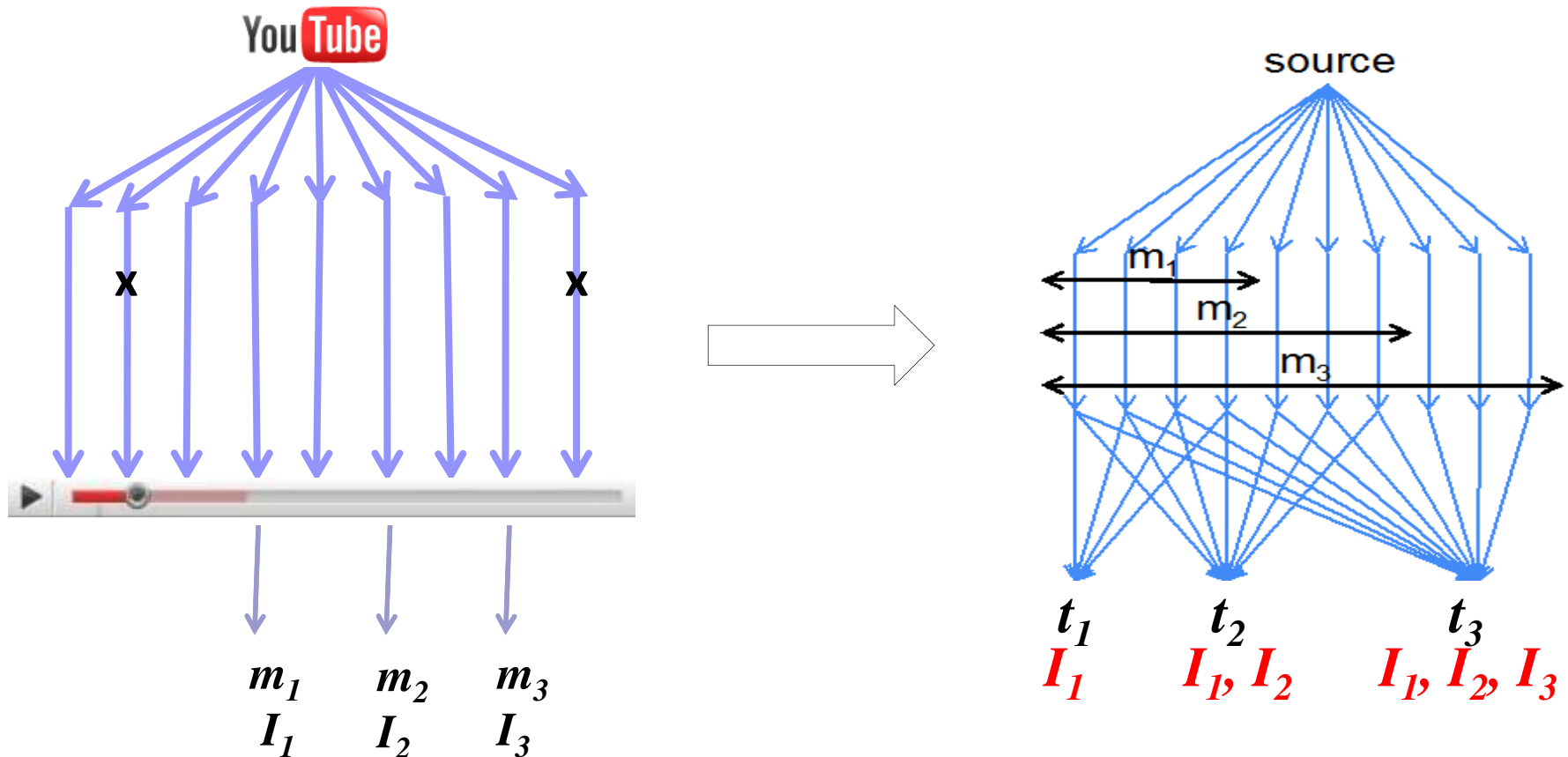


Background – network error correction

- The network error correction problem was introduced by [Cai & Yeung 03]
- Extensively studied in the single-source multicast case with uniform errors
 - Equal capacity network links (or packets), any z of which may be erroneous
 - Various capacity-achieving code constructions, e.g. [Cai & Yeung 03, Jaggi et al. 07, Zhang 08, Koetter & Kschischang 08]

This talk: two application domains and related theory

1. Network error/erasure correction as a model for analyzing reliable communication with deadlines





This talk: two application domains and related theory

1. Network error/erasure correction as a model for analyzing reliable communication with deadlines
2. Networks with active adversaries
 - Information theoretic security
 - Resources: path diversity and capacity
 - No computational assumptions on adversaries
 - Combining information theoretic and cryptographic security
 - For computationally limited nodes



Outline

- Coding for deadlines: non-multicast nested networks
- Combining information theoretic and cryptographic security: single-source multicast
- Multiple-source multicast, uniform errors
- Non-uniform errors: unequal link capacities



Outline

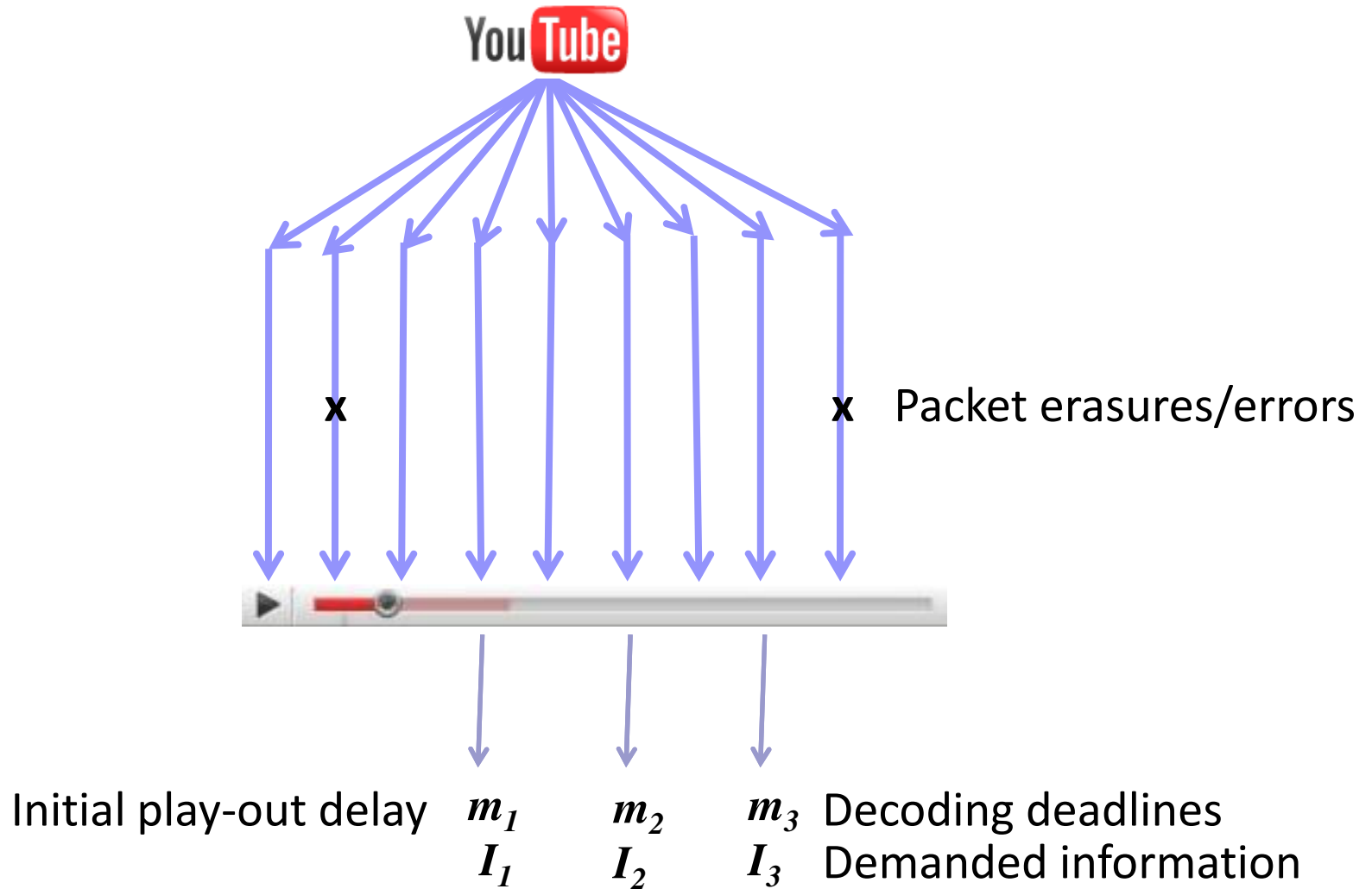
- Coding for deadlines: non-multicast nested networks
O. Tekin, S. Vyetrenko, T. Ho and H. Yao, Allerton 2011.
- Combining information theoretic and cryptographic security:
single-source multicast
- Multiple-source multicast, uniform errors
- Non-uniform errors: unequal link capacities



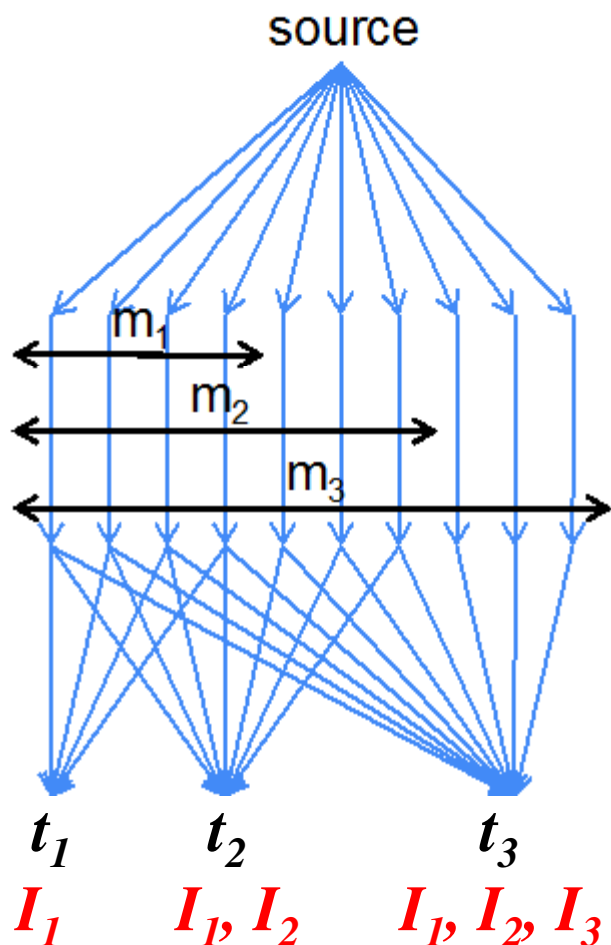
Background - non-multicast

- Finding the capacity region of a general non-multicast network even in the erasure-free case is an open problem
 - Coding across different sinks' packets (inter-session coding) is sometimes required
 - We don't know in general when intra-session coding is sufficient
- We can derive cut set bounds by analyzing three-layer networks (Vyetenko, Ho & Dikaliotis 10)

Motivation



Three-layer nested networks



- A model for temporal demands
 - Links $\leftrightarrow$ Packets
 - Sinks $\leftrightarrow$ Deadlines by which certain information must be decoded
- Each sink receives a subset of the information received by the next (nested structure)
- Packet erasures can occur
- Non-multicast problem

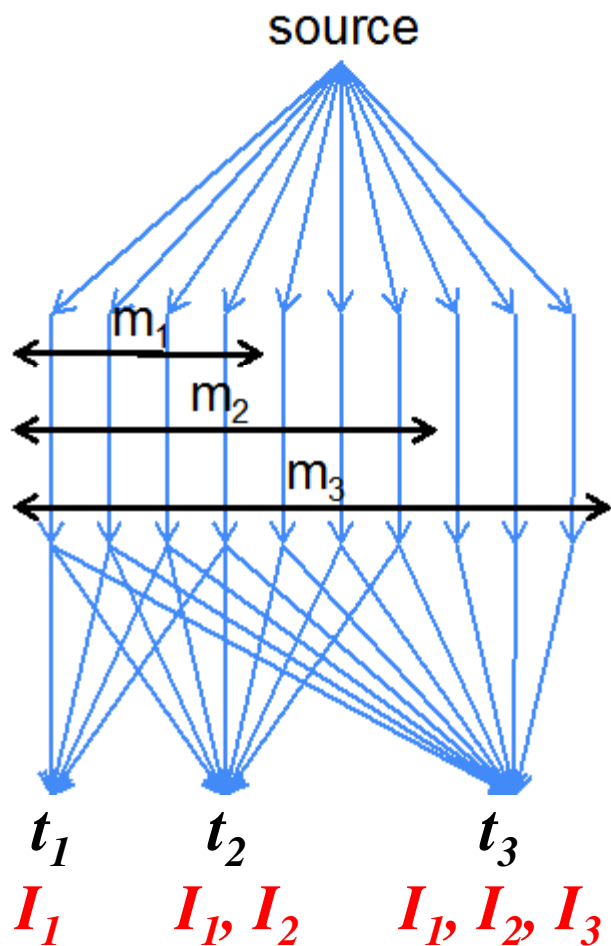


Erasure models

We consider two erasure models:

- z erasures (uniform model)
 - At most z links can be erased, locations are unknown *a priori*.
- Sliding window erasure model

z erasures – bounding capacity



- Want to find the capacity region of achievable rates $u_1, u_2, \dots, u_n$
- We can write a cut-set bound for each sink and erasure pattern (choice of z erased links)

$$u_1 \leq m_1 - z$$

$$u_1 + u_2 \leq m_2 - z$$

...

$$u_1 + u_2 + \dots + u_n \leq m_n - z$$

- Can we combine bounds for multiple erasure patterns and sinks to obtain tighter bounds?

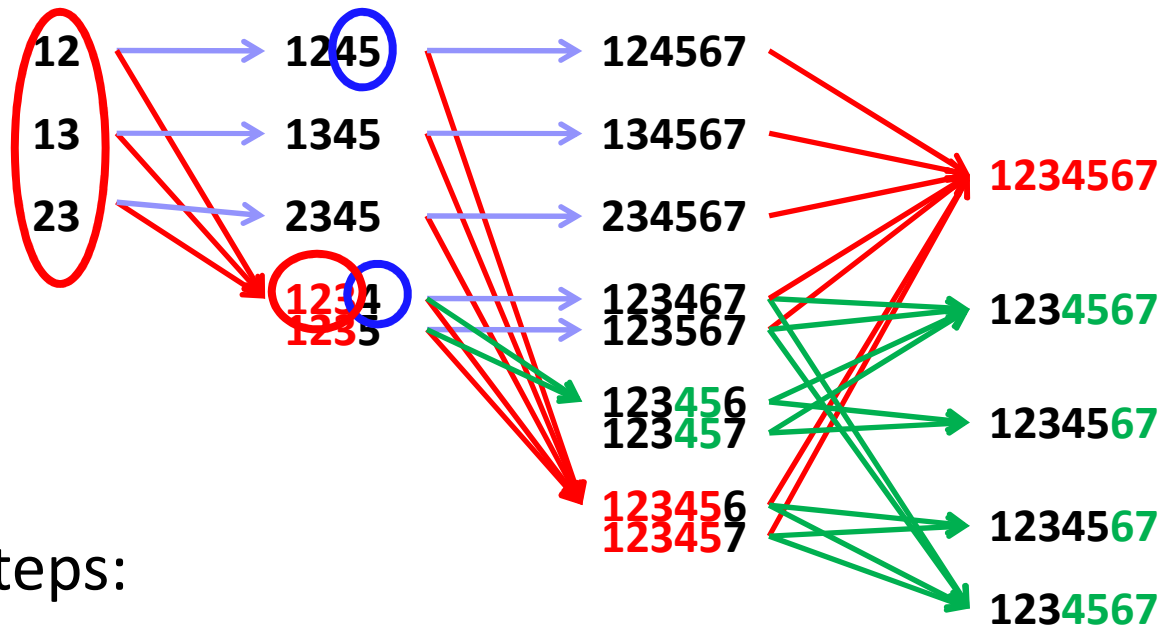
Cut-set combining procedure

Example: $m_1=3, m_2=5, m_3=7, m_4=11, z=1$

$$u_1 + H(X_1 X_2 | I_1) \leq 2$$

$$u_1 + H(X_1 X_3 | I_1) \leq 2$$

$$u_1 + H(X_2 X_3 | I_1) \leq 2$$



• Iteratively apply steps:

Extend: $H(X | I_1^{i-1}) + |Y| \geq H(X, Y | I_1^{i-1}) = H(X, Y | I_1^i) + u_i$

where X, Y is a decoding set for I_i

Combine:
$$\sum_{A: A \subset X, |A|=k} H(Z, A | I_1^i) \geq \binom{|X|-1}{k} H(Z, X | I_1^i)$$

Upper bound derivation graph

Example: $m_1=3, m_2=5, m_3=7, m_4=11, z=1$

Capacity region:

$$u_1 \leq 2$$

$$3u_1 + 2u_2 \leq 8$$

$$3u_1 + 2u_2 + u_3 \leq 9$$

$$6u_1 + 5u_2 + 4u_3 \leq 24$$

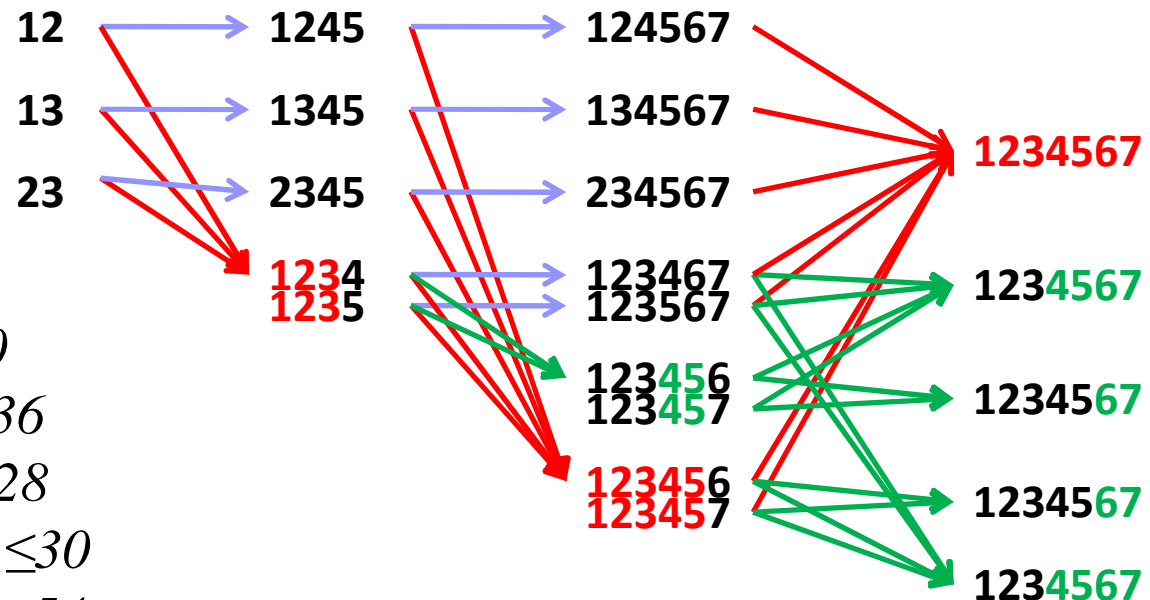
$$6u_1 + 4u_2 + 2u_3 + u_4 \leq 20$$

$$9u_1 + 6u_2 + 4u_3 + 3u_4 \leq 36$$

$$6u_1 + 5u_2 + 4u_3 + 2u_4 \leq 28$$

$$6u_1 + 4.5u_2 + 4u_3 + 3u_4 \leq 30$$

$$9u_1 + 7.5u_2 + 7u_3 + 6u_4 \leq 54$$



- Different choices of links at each step give different upper bounds
- Exponentially large number of bounds
- Only some are tight – how to find them?
- We use an achievable scheme as a guide and show a matching upper bound

Intra-session Coding

- $y_{j,k}$: capacity on k^{th} link allocated to j^{th} message
- We may assume $y_{j,k} = 0$ for $k > m_j$
- P : set of unerased links with at most z erasures
- A rate vector $(u_1, u_2, \dots, u_n)$ is achieved if and only if:

	1	2	$\dots$	m_n	Σ_P
I_1	$y_{1,1}$	$y_{1,2}$	$\dots$	y_{1,m_n}	$\geq u_1$
I_2	$y_{2,1}$	$y_{2,2}$	$\dots$	y_{2,m_n}	$\geq u_2$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	
I_n	$y_{n,1}$	$y_{n,1}$	$\dots$	y_{n,m_n}	$\geq u_n$
Σ	≤ 1	≤ 1		≤ 1	

“As uniform as possible” intra-session coding scheme

- Fill up each row as uniformly as possible subject to constraints from previous rows
- Example:

$$m_1 = 10, m_2 = 14, m_3 = 18, m_4 = 22, \\ u_1 = 6, u_2 = 3, u_3 = 3, u_4 = 4, z = 2$$

$$\begin{array}{r} u_4 - u_3^* = 0.25 \\ \frac{m_4 - m_3}{m_3} = \frac{4}{18} = 0.22 \\ \frac{m_3 - m_2}{m_2} = \frac{4}{14} = 0.29 \\ \frac{m_2 - m_1}{m_1} = \frac{4}{10} = 0.4 \end{array}$$

	1,2,...,9,10	11,12,13,14	15,16,17,18	19,20,21,22
I_1	0.75			
I_2	0.25	0.25		
I_3	0	0.5	0.5	
I_4	0	0.25	0.5	0.5

Can we do better?



Capacity region

Theorem: The z -erasure (or error) correction capacity region of a 3-layer nested network is achieved by the “as uniform as possible” coding scheme.

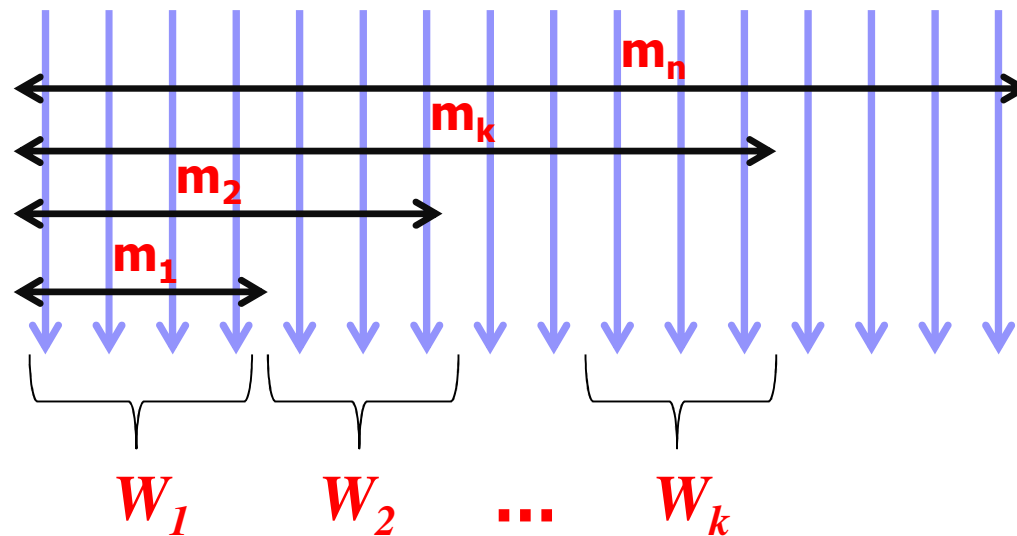
Proof Idea

- Consider any given rate vector $(u_1, u_2, \dots, u_n)$ and its corresponding “as uniform as possible” allocation:

	$1, 2, \dots, m_1$	$m_1 + 1, \dots, m_2$	$m_2 + 1, \dots, m_3$	...	$m_{n-1} + 1, \dots, m_n$
I_1	$T_{1,1}$				
I_2	$T_{2,1}$	$T_{2,2}$			
I_3	$T_{3,1}$	$T_{3,2}$	$T_{3,3}$		
...	...	...	...	...	
I_n	$T_{n,1}$	$T_{n,2}$	$T_{n,3}$	...	$T_{n,n}$

- Obtain matching information theoretic bounds, by using $T_{i,j}$ values to choose path through upper bound derivation graph

Proof Idea



- Consider any unerased set $W = W_1 \cup W_2 \dots \cup W_k$ with at most z erasures.
- **Show by induction:** The conditional entropy of W given messages $I_1, \dots, I_k$ matches the residual capacity in the table,

i.e.
$$H(W | I_1, \dots, I_k) \leq \sum_{i=1}^k |W_i| (1 - \sum_{j=1}^k T_{j,i})$$

Proof Idea

- For any set $V \subset W$ with $|V| = m_k - z$, an upper bound for $H(V | I_1^k)$ can be derived as follows:
 - let V' be the subset of V consisting of links upstream of t_{k-1}
 - obtain $H(V' | I_1^{k-1})$ from the table (induction hypothesis)
 - **extend** : $H(V | I_1^k) \leq H(V' | I_1^{k-1}) + |V \setminus V'| - u_k$
- For each row k , there exists a column k^* such that all $T_{i,j}$ are all equal for $j > k^*$
- **Combine** over all such $V \subset W$ having erasures on links $m_{k^*+1}, m_{k^*+2}, \dots, m_k$ to obtain:

$$H(W | I_1, \dots, I_k) \leq \sum_{i=1}^k |W_i| (1 - \sum_{j=1}^k T_{j,i})$$



z -error capacity region

- A linear non-multicast code that can correct $2z$ erasures can correct z errors [Vyetenko, Ho, Effros, Kliever & Erez 09]
- An arbitrary code for a three-layer network that can correct z errors can correct $2z$ erasures (Singleton-type argument)
- Since our capacity-achieving code is linear, the z -error capacity region is the same as the $2z$ -erasure capacity region



Sliding window erasure model

- Parameterized by erasure rate p and burst parameter T .
- For $y \geq T$, at most py out of y consecutive packets can be erased.
- Erasures occur with rate p in long term.
- Erasure bursts cannot be too long (controlled by T).



Sliding window erasure achievable region

- Theorem: Let the rate vector $\vec{u}$ be achievable. Then the rate vector*

$$\frac{1}{1 + \log\left(\frac{m_1 + T}{m_1}\right)} \frac{1 - p}{1 - p + \frac{1}{T}} \vec{u}$$

is achieved by “as uniform as possible” coding.

- Note: asymptotically optimal for $m_1 \gg T \gg 1$*



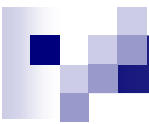
Outline

- Coding for deadlines: non-multicast nested networks
- Combining information theoretic and cryptographic security: single-source multicast
S. Vyetrenko, A. Khosla & T. Ho, Asilomar 2009.
- Multiple-source multicast, uniform errors
- Non-uniform errors: unequal link capacities



Problem statement

- Single source, multicast network
- Packets may be corrupted by adversarial errors
- Computationally limited network nodes (e.g. low-power wireless/sensor networks)



Background: information-theoretic and cryptographic approaches

- Information theoretic network error correction
 - Existing codes are designed for a given upper bound z_U on the number of errors, achieve rate $\text{mincut} - 2z_U$, e.g. [Yeung and Cai 03]
- Cryptographic signatures with erasure correction
 - Cryptographic signatures allow network coded packets to be validated, e.g. [Zhao et al. 07, Boneh et al. 09]
 - If all packets are signed and each network node checks all packets, then rate $\text{mincut} - z$ can be achieved, where z is the actual number of erroneous packets



Motivation for hybrid schemes

- Performing signature checks at network nodes requires significant computation
- Checking all packets at all nodes can limit throughput when network nodes are computationally weak
- Want to use both path diversity as well as cryptographic computation as resources, to achieve rates higher than with each separately

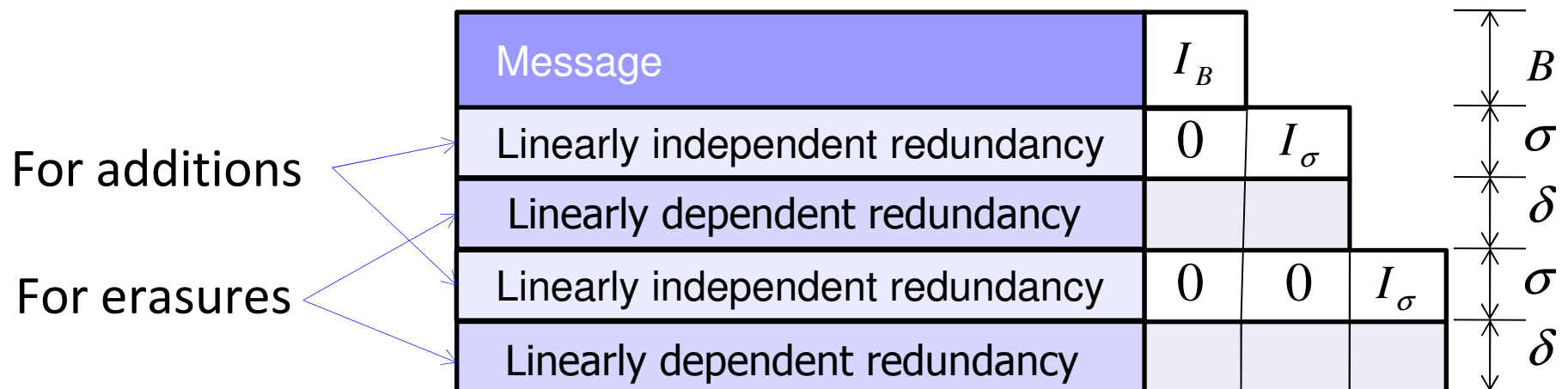


Approach

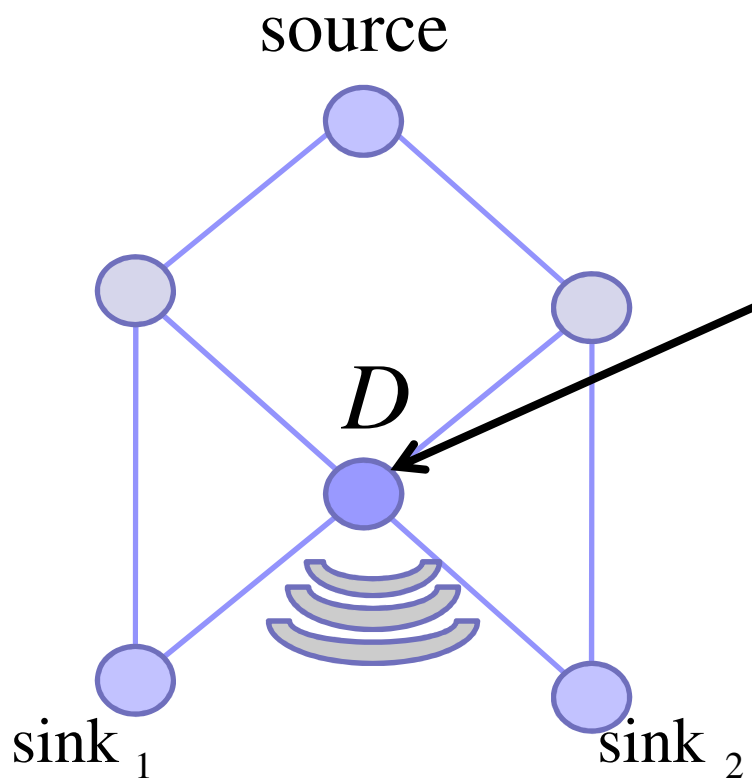
- Cannot afford to check all packets → use **probabilistic** signature checking
- **Deterministic** bound on number of erroneous packets is needed in existing network error correction code constructions
- Rather than have to choose a conservative bound, we want a code construction that does not require an upper bound on the number of errors to be known in advance

Fountain-like network error correction code

- We propose a fountain-like error-correcting code which incrementally sends redundancy until decoding succeeds (verified by signature checks)
- Each adversarial error packet can correspond to an addition (of erroneous information) and/or an erasure (of good information)
- Construction:



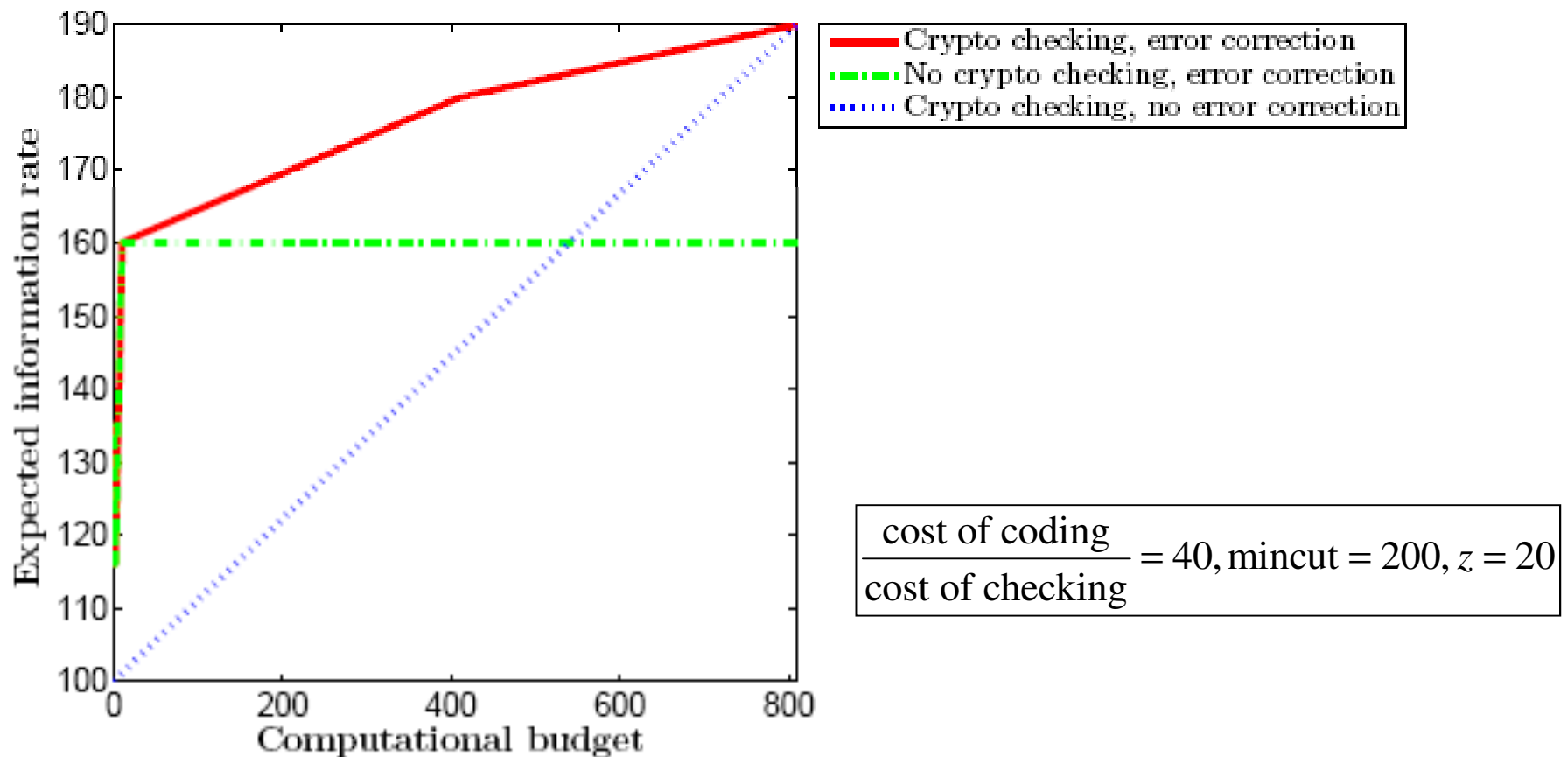
Example: simple hybrid strategy on wireless butterfly network



Node D has limited computation and outgoing capacity

- Carries out probabilistic signature checking/coding
- Proportion of packets checked/coded chosen to maximize expected information rate subject to computational budget

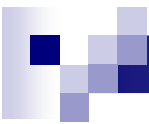
Example: simple hybrid strategy on wireless butterfly network





Outline

- Coding for deadlines: non-multicast nested networks
- Combining information theoretic and cryptographic security: single-source multicast
- **Multiple-source multicast, uniform errors**
T. Dikaliotis, T. Ho, S. Jaggi, S. Vyetrenko, H. Yao, M. Effros, J. Kliewer and E. Erez, IT Transactions 2011.
- Non-uniform errors: unequal link capacities

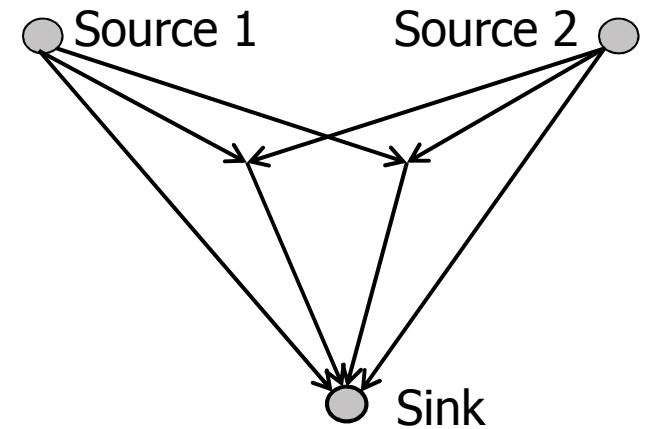


Background – single-source multicast, uniform z errors

- Capacity = min cut – $2z$, achievable with linear network codes (Cai & Yeung 03)
- Capacity-achieving codes with polynomial-time decoding:
 - Probabilistic construction (Jaggi, Langberg, Katti, Ho, Katabi & Medard 07)
 - Lifted Gabidulin codes (Koetter & Kschischang 08, Silva, Kschischang & Koetter 08)

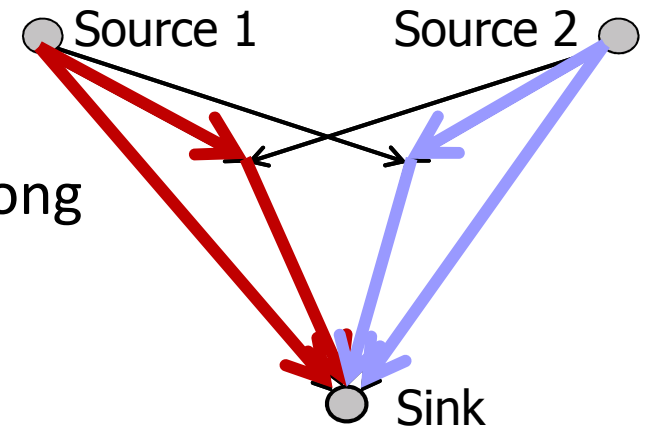
Multiple-source multicast, uniform z errors

- Sources with independent information



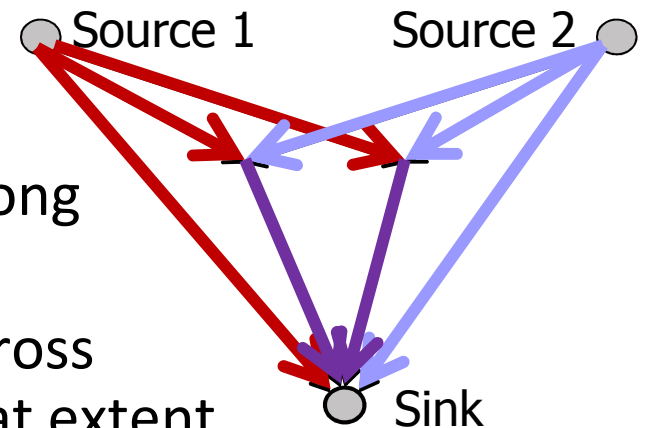
Multiple-source multicast, uniform z errors

- Sources with independent information
- We could partition network capacity among different sources...



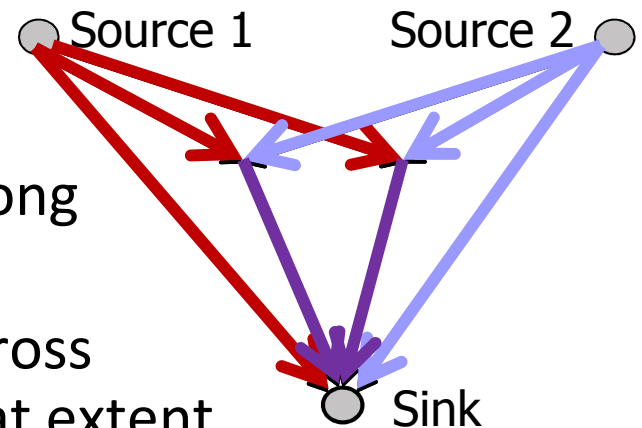
Multiple-source multicast, uniform z errors

- Sources with independent information
- We could partition network capacity among different sources...
- But could rate be improved by coding across different sources in the network? To what extent can different sources share network capacity?



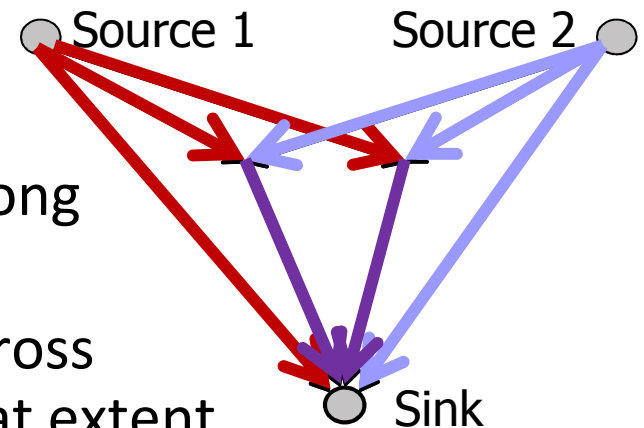
Multiple-source multicast, uniform z errors

- Sources with independent information
- We could partition network capacity among different sources...
- But could rate be improved by coding across different sources in the network? To what extent can different sources share network capacity?
- Challenge: owing to the need for coding across sources in the network and independent encoding at sources, straightforward extensions of single-source codes are suboptimal



Multiple-source multicast, uniform z errors

- Sources with independent information
- We could partition network capacity among different sources...
- But could rate be improved by coding across different sources in the network? To what extent can different sources share network capacity?
- Challenge: owing to the need for coding across sources in the network and independent encoding at sources, straightforward extensions of single-source codes are suboptimal
- Related work: code construction in (Siavoshani, Fragouli & Diggavi 08) achieves capacity for $C1+C2=C$



Capacity region

- U = set of source nodes
- m_S = min cut capacity between sources in subset S of U and each sink
- r_i = rate from the i^{th} source
- **Theorem:** The capacity region (coherent & non-coherent) under any z link errors is given by the cut set bounds

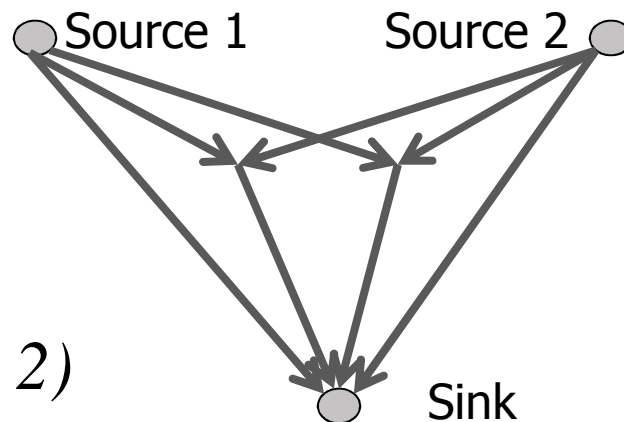
$$\sum_{i \in S} r_i \leq m_S - 2z, \forall S \subseteq U$$

- Example: $z = 1$

$$r_1 \leq m_1 - 2z = 1$$

$$r_2 \leq m_2 - 2z = 1$$

$$(r_1 + r_2 \leq m - 2z = 2)$$



Capacity region

- U = set of source nodes
- m_S = min cut capacity between sources in subset S of U and each sink
- r_i = rate from the i^{th} source
- **Theorem:** The capacity region (coherent & non-coherent) under any z link errors is given by the cut set bounds

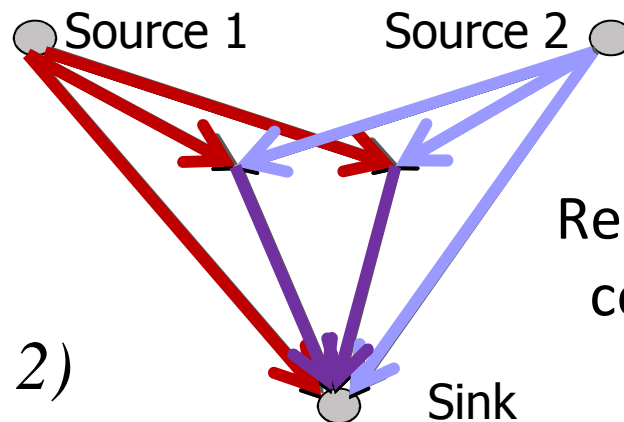
$$\sum_{i \in S} r_i \leq m_S - 2z, \forall S \subseteq U$$

- Example: $z = 1$

$$r_1 \leq m_1 - 2z = 1$$

$$r_2 \leq m_2 - 2z = 1$$

$$(r_1 + r_2 \leq m - 2z = 2)$$





Achievable constructions

1. Probabilistic construction, joint decoding of multiple sources
 - Requires a different distance metric for decoding than single source multicast decoding metric from Koetter & Kschischang 08
2. Gabidulin codes in nested finite fields, successive decoding

Background - Gabidulin codes

$$M = \left[\begin{array}{c|c|c} & 1 & \\ \hline & F_{q^n} & \\ \hline & & \end{array} \right]_{r \times r}$$

Background - Gabidulin codes

$$GM = \left[\begin{array}{c|c|c} \overbrace{}^n & \overbrace{}^l & \overbrace{\phantom{F_{q^n}}}^1 \\ \hline M & F_q^r & F_{q^n} \end{array} \right]_{r+t}$$

$$GM \xrightarrow{\text{Channel}} GM + E$$

- Transmit $[I \ x]$, where x is a codeword of a Gabidulin code
- Achieves capacity $C - 2z$ for single-source multicast with efficient decoding algorithms (Koetter & Kschischang 08, Silva, Kschischang & Koetter 08)



Nested Gabidulin codes for multiple source multicast

- Interior nodes do random linear network coding in $GF(q)$
- Sources encode with Gabidulin codes over nested extension fields $GF(q^{n_1}), GF(q^{n_1 n_2}), \dots, GF(q^{n_1 n_2 \dots n_k})$ where $n_i \geq r_i + 2z$
- Enables successive decoding at the sinks, starting from outermost source k

Nested Gabidulin codes - 2 sources

$$Y = T_1 G_1 M_1 + T_2 G_2 M_2 + E \quad (1)$$

$$\Leftrightarrow Y = \begin{bmatrix} T_1 & G_1 & T_2 \end{bmatrix} \cdot \begin{bmatrix} M_1 \\ G_2 M_2 \end{bmatrix} + E \quad (2)$$

$$D = \begin{bmatrix} T_1 & G_1 & T_2 \end{bmatrix} \in F_{q^{n_1}}^{m \times m} \text{ invertible whp for RLNC}$$

$$\Leftrightarrow (D^{-1}Y) = \begin{bmatrix} M_1 \\ G_2 M_2 \end{bmatrix} + D^{-1}E \quad \begin{array}{l} \text{lowest } r_2 + 2z \\ \text{rows} \end{array}$$

$$\Rightarrow (D^{-1}Y)_\ell = G_2 M_2 + (D^{-1}E)_\ell \quad (3)$$

Matrix of rank z over $F_q^{n_1}$  Matrix of rank z over F_q 



Outline

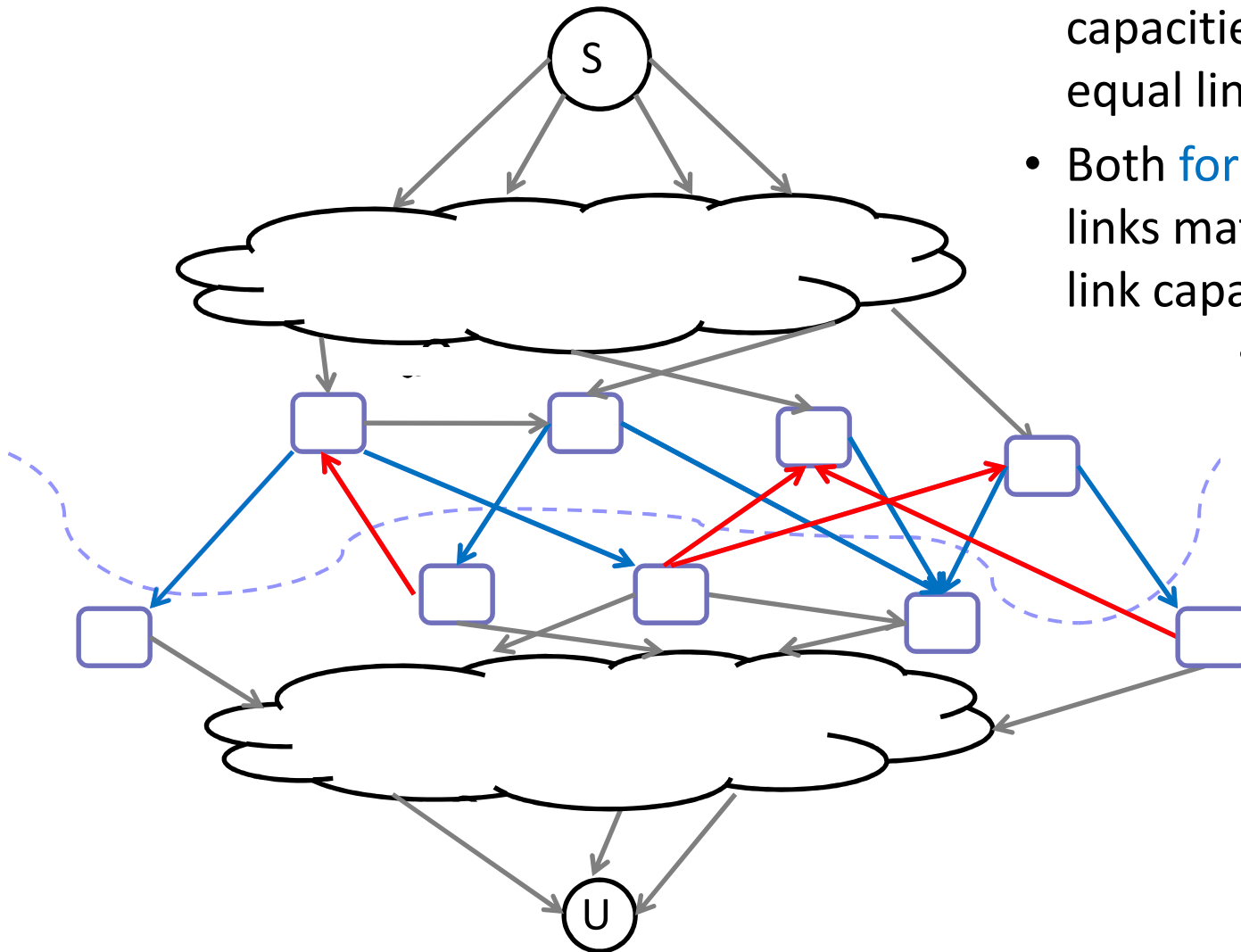
- Coding for deadlines: non-multicast nested networks
- Combining information theoretic and cryptographic security: single-source multicast
- Multiple-source multicast, uniform errors
- **Non-uniform errors: unequal link capacities**
 - S. Kim, T. Ho, M. Effros and S. Avestimehr, IT Transactions 2011.
 - T. Ho, S. Kim, Y. Yang, M. Effros and A. S. Avestimehr, ITA 2011.



Uniform and non-uniform errors

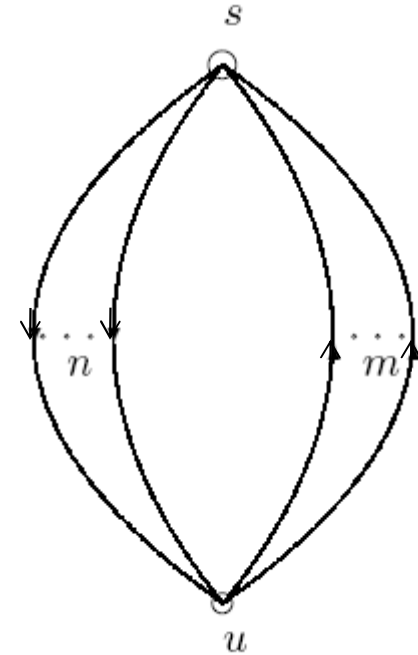
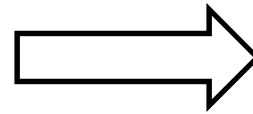
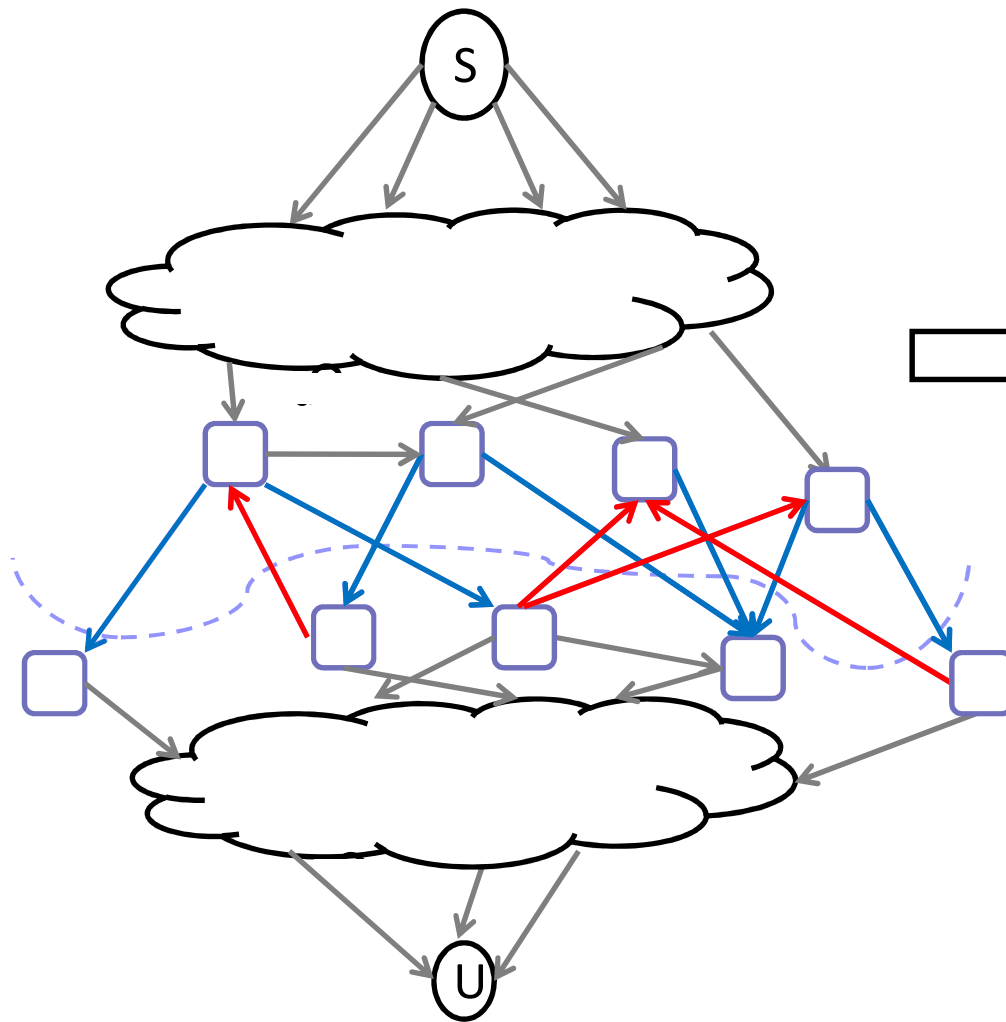
- Uniform errors:
 - Multicast error correction capacity = min cut $- 2z$
 - Worst-case errors occur on the min cut
- Non-uniform errors:
 - Model: network with unequal link capacities, adversarial errors on any z fixed but unknown links
 - Not obvious what are worst-case errors
 - Cut size versus link capacities
 - Feedback across cuts matters
 - Related work: Adversarial nodes (Kosut, Tong & Tse 09)

Network cuts



- Only **forward** link capacities matter in the equal link capacity case
- Both **forward** and **feedback** links matter in the unequal link capacity case
 - Feedback can provide information about errors on upstream links

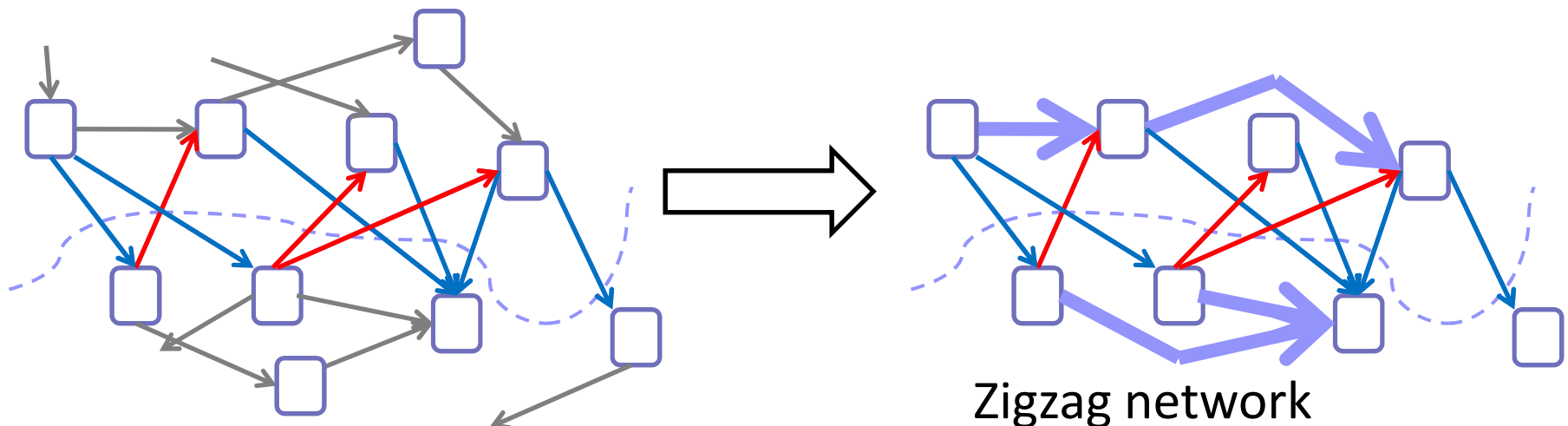
Two-node cut set bounding approach



Two-node network with n forward links and m feedback links

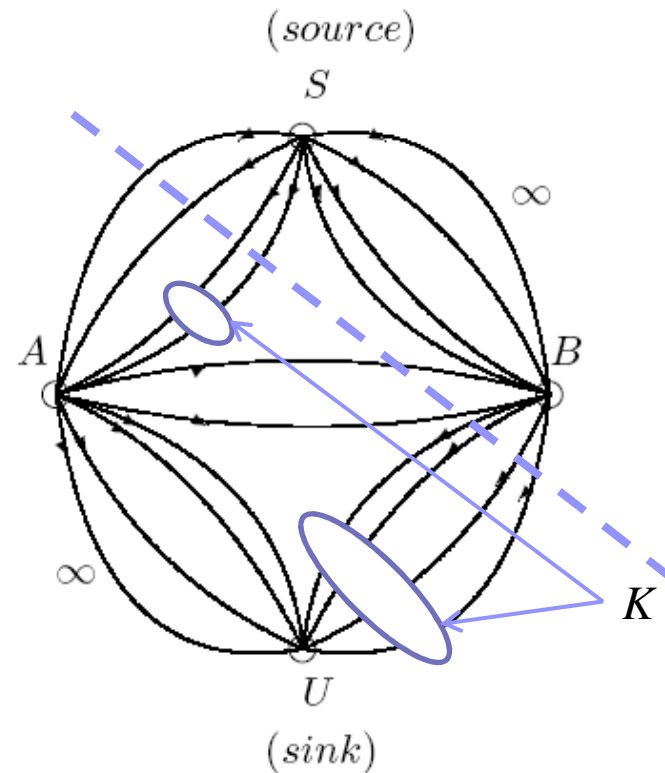
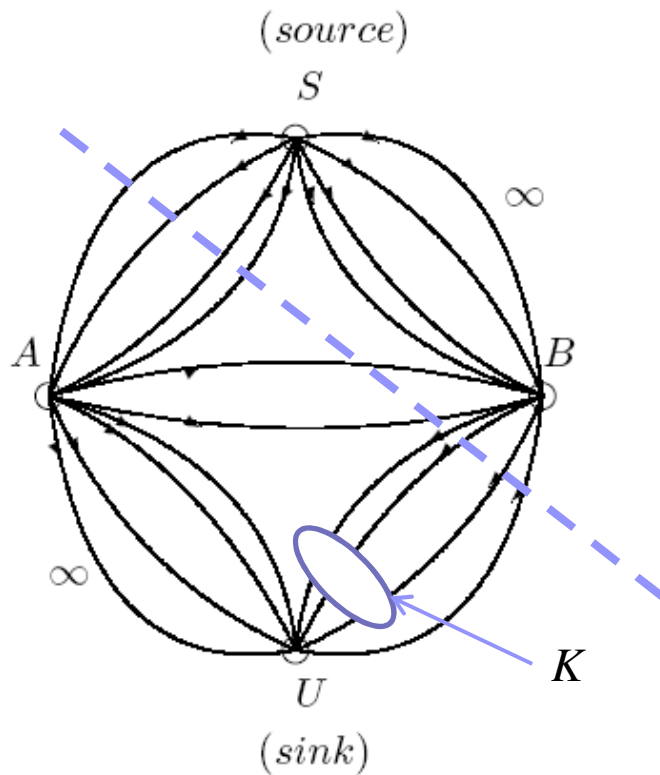
Tighter cut set bounding approach

- The two-node cut set bounding approach is equivalent to adding reliable, infinite-capacity bidirectional links between each pair of nodes on each side of the cut
- Tighter bounds can be obtained by taking into account which forward links affect or are affected by which feedback links
- Equivalent to adding a link (i,j) only if there is a directed path from node i to node j on that does not cross the cut



Downstream condition

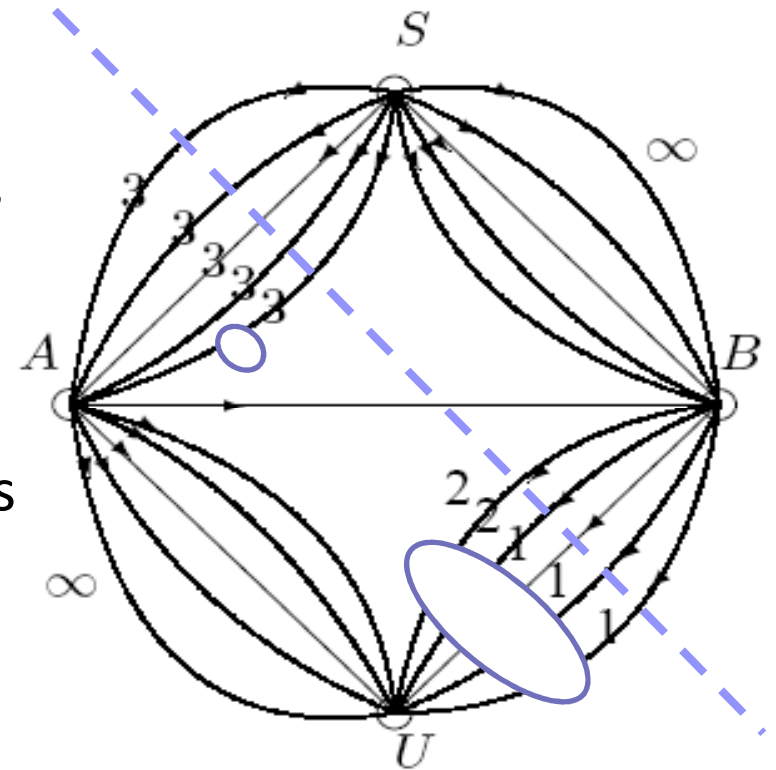
- A set of links K on a cut Q is said to satisfy the *downstream condition* if none of the remaining links on the cut Q are downstream of any link in K .



Generalized Singleton bound

Generalized Singleton bound [Kim, Ho, Effros & Avestimehr 09, Kosut, Tong & Tse 09]:

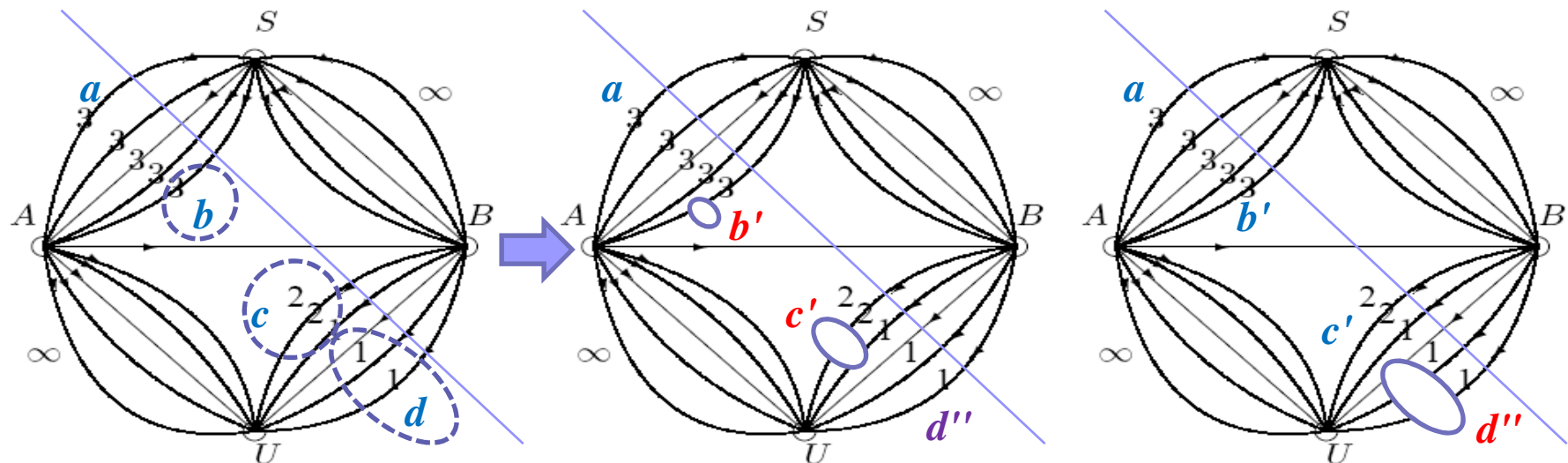
For any cut Q , after erasing any $2z$ links satisfying the downstream condition, the total capacity of the remaining links in Q is an upper bound on error correction capacity.



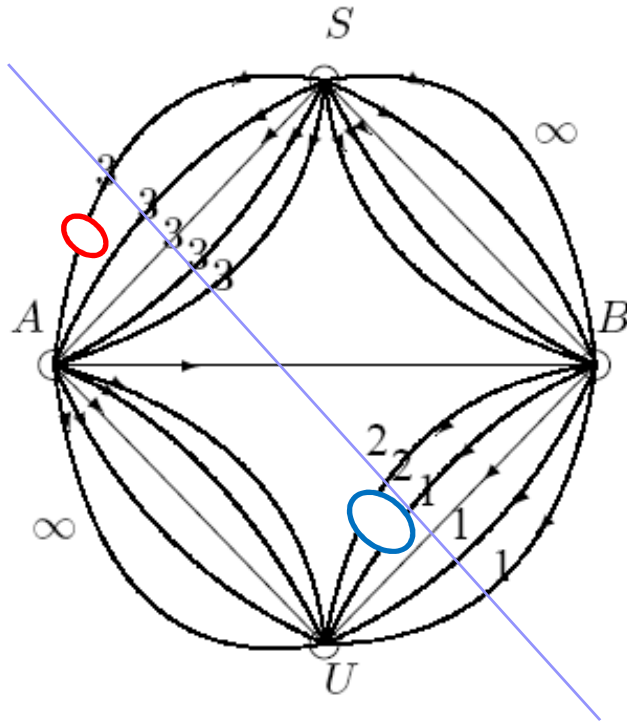
When $z=3$, generalized Singleton bound is
 $3+3+3+3=12$

Generalized Singleton bound - intuition

- Suppose the bound is violated. Then there exist two codewords x, x' that differ in $2z$ links satisfying the downstream condition and agree on the remaining links
- There exist error values e, e' such that sink U cannot distinguish (x, e) and (x', e')



Idea 1



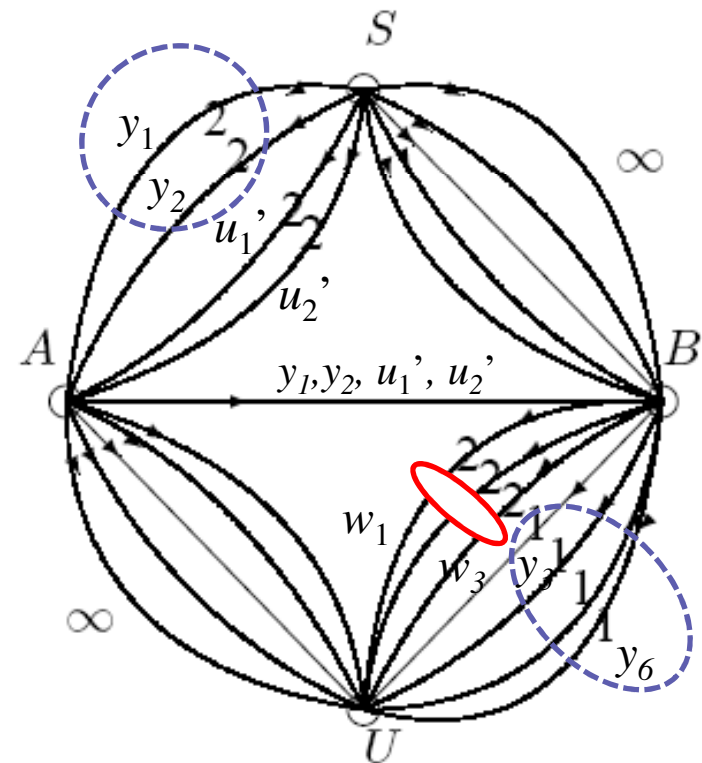
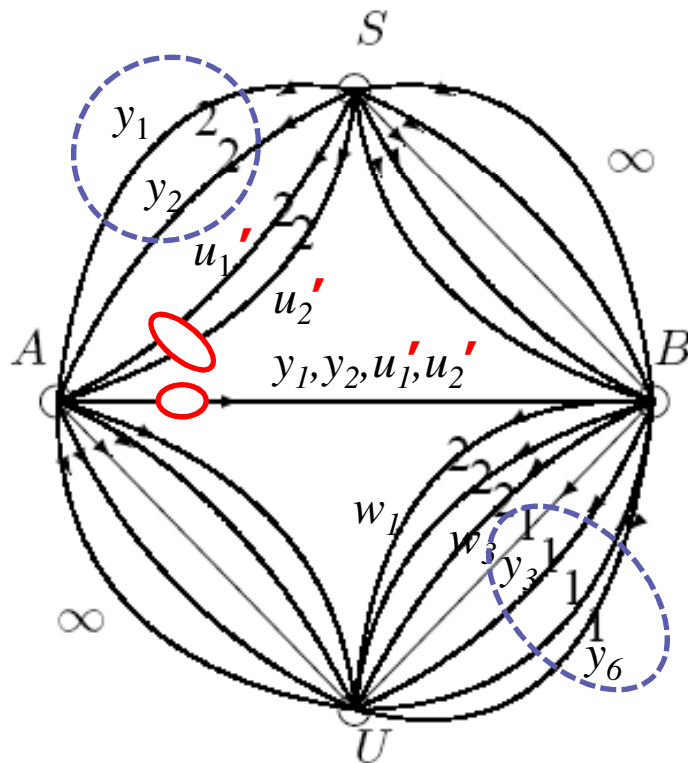
- Observation: generalized Singleton bound is not tight when downstream links have smaller capacities.



Idea 1: erase any $k \leq z$ largest capacity links and apply Singleton bound with $z-k$ adversarial links on remaining network.

Idea 2

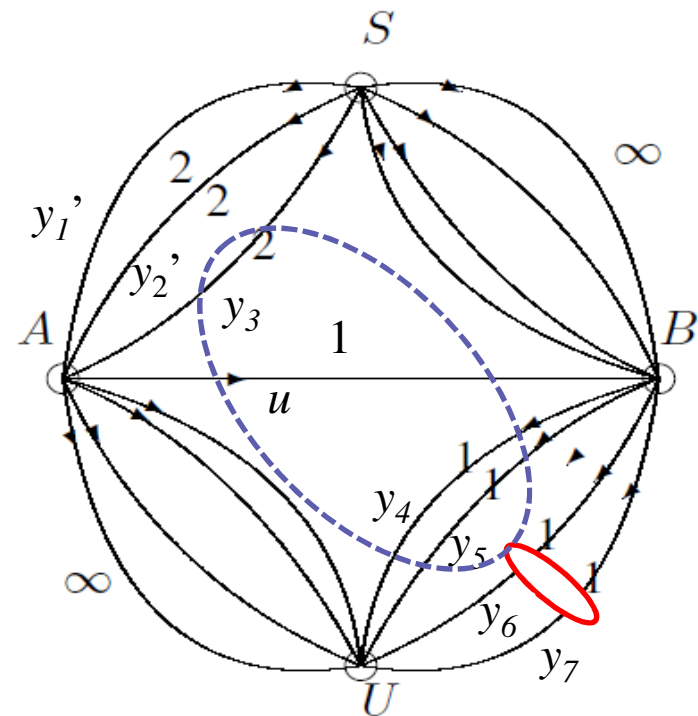
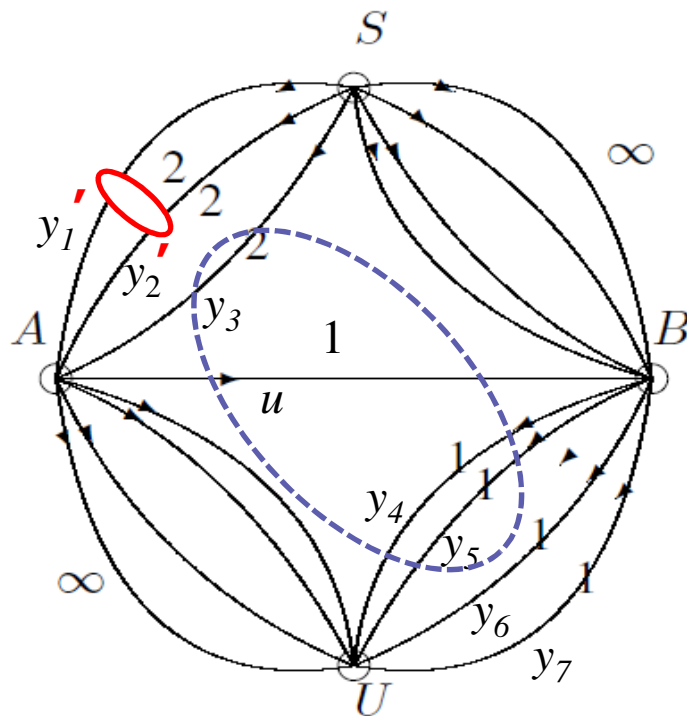
If adversary controls some forward links as well as their downstream feedback links, he can hide his errors



Idea 3

Observation: For small feedback link capacities, distinct codewords have the same feedback link values

➡ Idea 3: adversary can cause confusion between codewords that agree on the feedback links





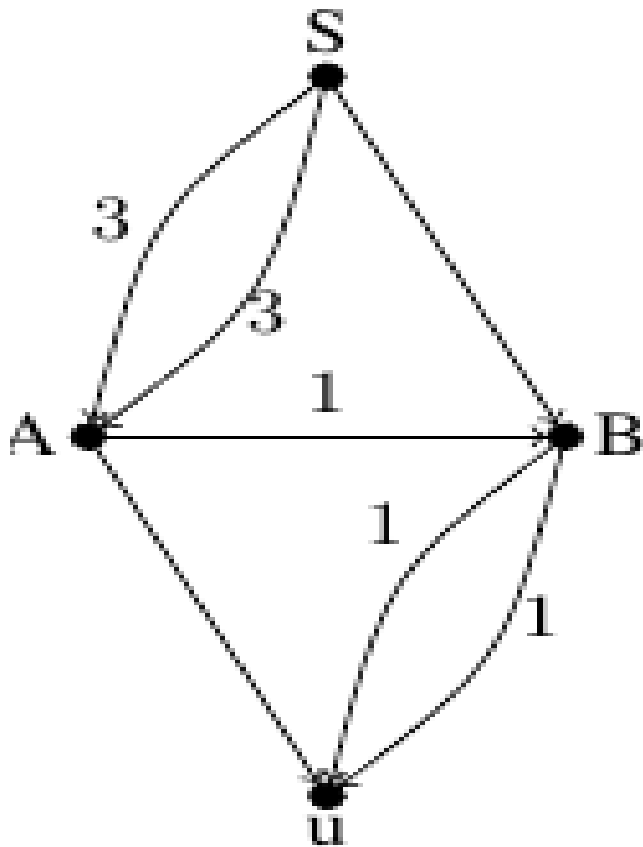
New cut-set bound

For any cut Q ,

- adversary first erases a set of $k \leq z$ forward links (idea 1)
- adversary then chooses two sets Z_1, Z_2 of $z-k$ links such that any feedback link directly downstream of links in both Z_1 and Z_2 and upstream of a forward link in $Q \setminus Z_1 \setminus Z_2$ is included in both Z_1 and Z_2 (idea 2)
- let W_i be the set of feedback links not in Z_i (idea 2) that are directly downstream of a link in Z_i and upstream of a forward link in $Q \setminus Z_1 \setminus Z_2$ (idea 3)
- sum of capacities of remaining forward links + capacities of links in W_1, W_2 is an upper bound

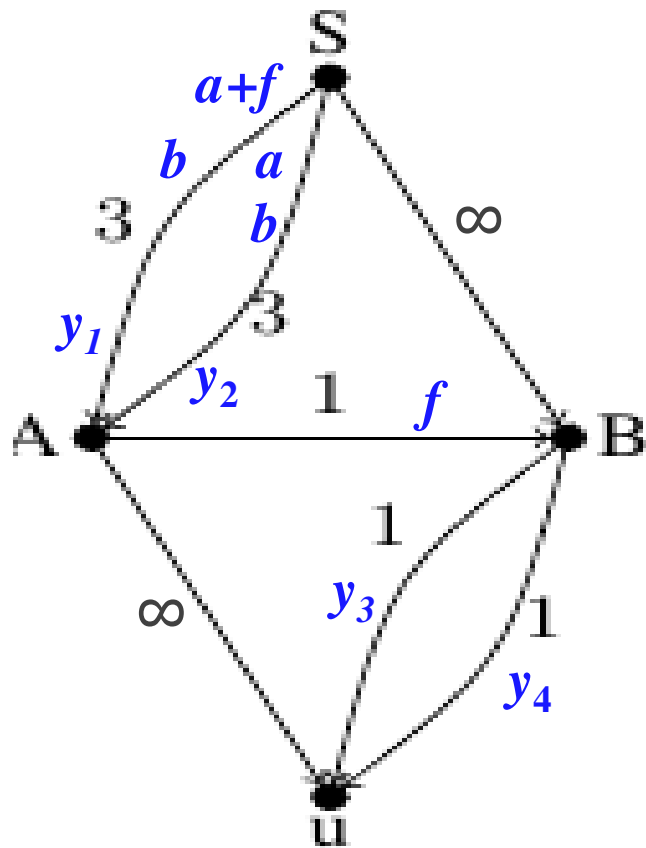
Bound is tight on some families of zig-zag networks

Achievability - example



- For $z=1$, upper bound = 5
- Without feedback link, capacity = 2
- Can we use feedback link to achieve rate 5?

“Detect and forward” coding strategy



$z=1$
capacity= 5

- Some network capacity is allocated to redundancy enabling partial error detection at intermediate nodes
- Nodes that detect errors forward additional information allowing the sink to locate errors
- Use feedback capacity to increase the number of symbols transmitted with error detection
- Remaining network capacity carries generic linear combinations of information symbols, serving as an MDS error correction code



Conclusion

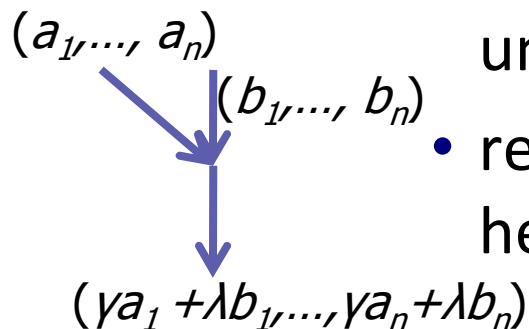
- Network error correction as a model for analyzing and designing codes for robust streaming
- Coding for adversaries: Information theoretic and hybrid cryptographic approaches
- New codes and outer bounds for more general networks and communication demands



- Thank you!

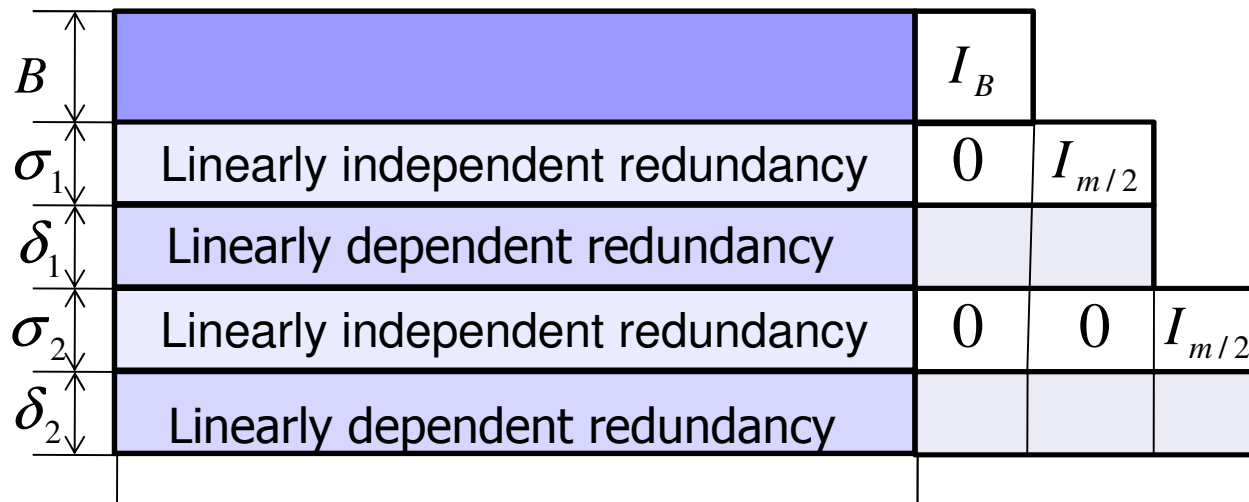
Coherent & non-coherent models

- **Coherent:** network topology known, centralized code design
- **Non-coherent (multicast):** network topology unknown, use distributed random linear network coding (RLNC)
 - each packet comprises a vector of symbols from a finite field F_q
 - each node sends linear combinations of its received packets with coefficients chosen uniformly at random from F_q
 - record network transformation in packet headers, or encode information in subspaces



Coding and decoding

- Coding over blocks (generations) of B source packets
- Phase $i = 0$: transmit B source packets
- Phase $i > 0$: transmit $\sigma_i = m/2$ linearly independent redundant packets and $\delta_i = m/2$ linearly dependent redundant packets
- At each phase the sink tries to decode (using a polynomial-time decoding algorithm similar to [Jaggi et al., 2007]), and performs signature checks on the decoded packets
- If the decoded packets pass the signature checks, the sink sends feedback telling the source to move on to the next block



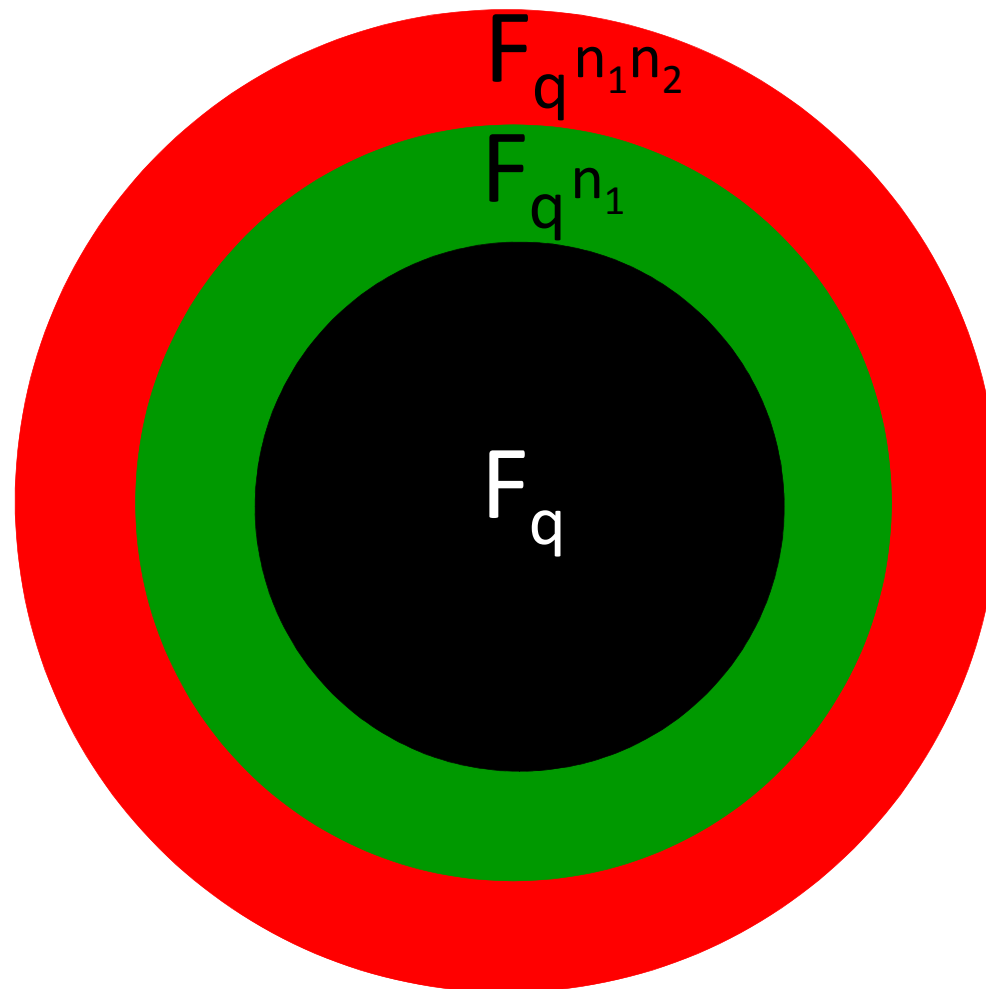


Field Extensions: example

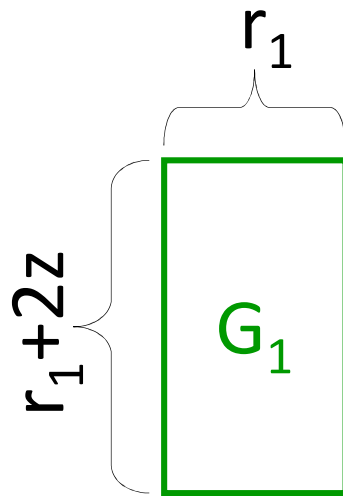
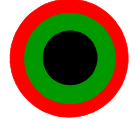
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \in F_2^{2 \times 4} \Leftrightarrow \begin{bmatrix} 2 & 0 \\ 3 & 1 \end{bmatrix} \in F_4^{2 \times 2} \Leftrightarrow \begin{bmatrix} 8 \\ 13 \end{bmatrix} \in F_{16}^{2 \times 1}$$



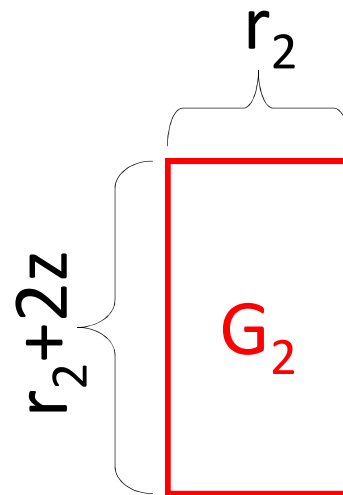
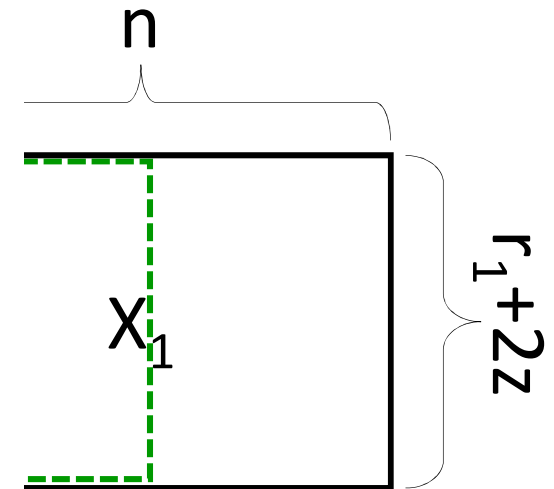
Field Extensions



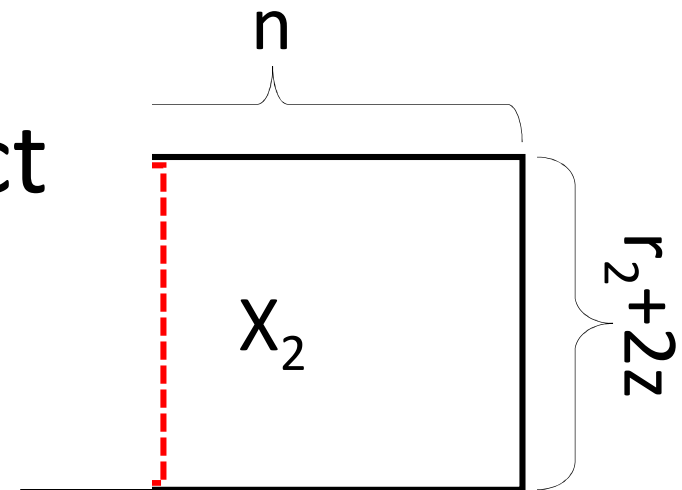
Encoding



G_1 can correct
rank z errors
over F_q

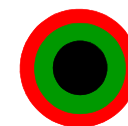


G_2 can correct
rank z errors
over $F_{q^{n_1}}$



$$n = kn_1n_2 \text{ where } n_i \geq r_i + 2z$$

Decoding



Matrix of rank z over F_q

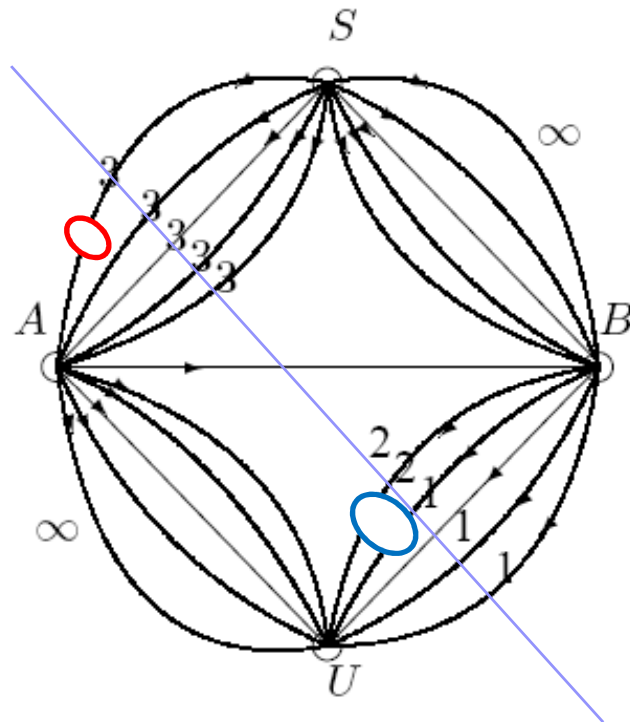
$$(D^{-1}Y)_\ell = G_2 M_2 + (D^{-1}E)_\ell$$

Matrix of rank z over $F_{q^{n_1}}$

(This is why we need the extension field)

- M_2 can be decoded (same as single-source decoding problem)
- Decoder then subtracts effect of M_2 and decodes M_1

Idea 1 - example



Four-node network with $z=2$.
 Singleton bound is $3 \times 5 + 1 = 16$.
 a) First erase one link with largest capacity.

b) Apply Singleton bound on remaining network for $z=1$.
 New bound is
 $3+3+3+3+1+1+1=15 < 16$