NEGIN KARIMI

UNIVERSITY OF MOHAGHEGH ARDABILI

19.9.2020

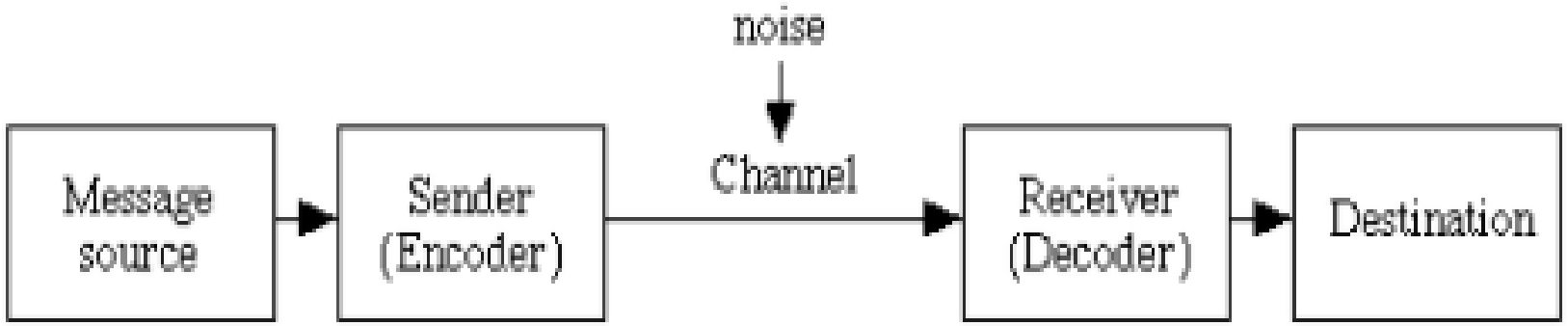
Linear And Cyclic Codes Over Finite Rings and Their Application over Distributed Storage Systems.

Outline

- **Distributed storage systems**
- **Replication erasure codes**
- **Regenerating codes and generalized regenerating codes.**
- **Information flow graph**
- **Generalized regenerating codes**

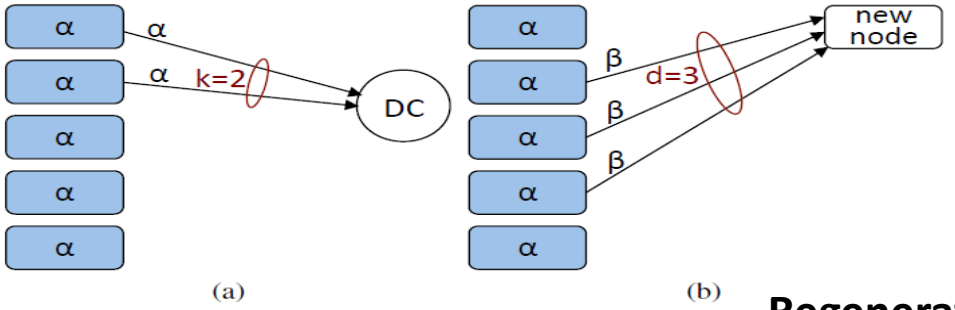
All communications involves three basic steps:

- Encoding a message at its source
- Transmitting that message through a communication medium
- Decoding the message at its destination



Distributed storage systems

Distributed storage provides a solution to the increased demand for long term data storage. In a distributed storage system (DSS), data is divided into small chunks and stored among different disks or nodes. When the user wants to retrieve the stored data, various blocks from individual nodes are accessed and the required data is reconstructed.

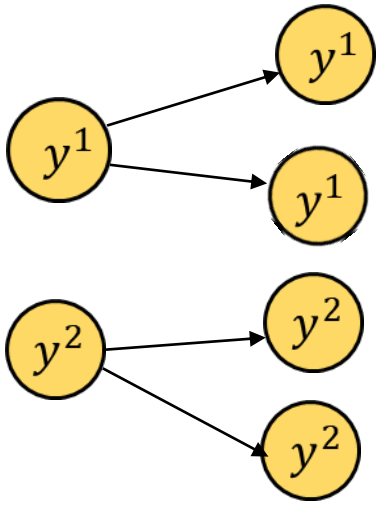


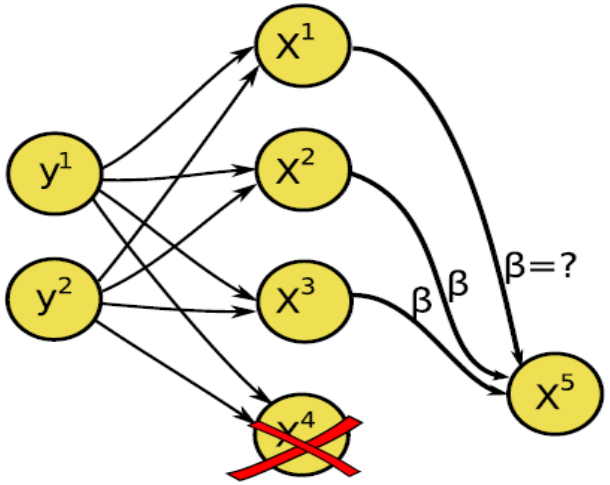
Reconstruction in DSS: When the user wants to retrieve the stored data, various blocks from individual nodes are accessed and the required data is reconstructed.

Regeneration in DSS: In order to ensure data availability, the data stored in failed nodes have to be reconstructed by accessing data from live nodes.

Replication and erasure coding:

In a DSS ensuring reliability requires the introduction of redundancy.





Replication: The simplest form of redundancy.

erasure coding: introduce redundancy in an optimal way.

$$y^1, y^2 = 1Mb$$

x^1, x^2, x^3, x^4 same size

Why regenerating codes?

Dimakis introduced a tradeoff between storage and repair bandwidth and show that codes exist that achieve every point on this optimal tradeoff curve.

Dimakis, Alexandros G., et al. "Network coding for distributed storage systems." IEEE transactions on information theory 56.9 (2010): 4539-4551.

Regenerating code: (n,k,d,α,γ)

n: fils's size

k: the number of reconstruction sets

d: the number of regeneration sets

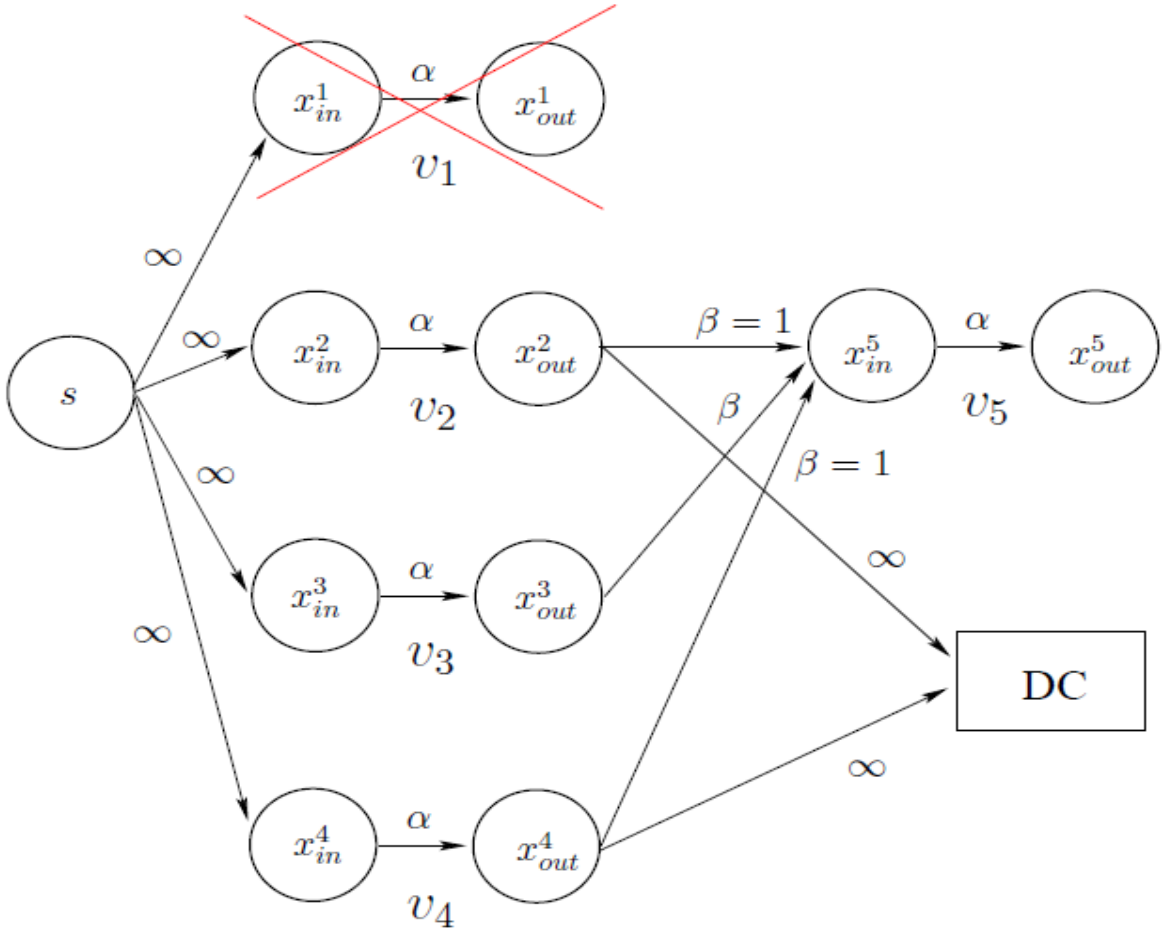
α: capacity of each storage node

γ: repair bandwidth

Analysis of regenaring codes:

At any given time, each vertex in the graph is either active or inactive, depending on whether it is available in the network.

- At the initial time, only the source node S is active
- At the next time step, the initially chosen storage nodes become now active
- Data collectors connect to subsets of active nodes through edges with infinite capacity



Regenerating codes

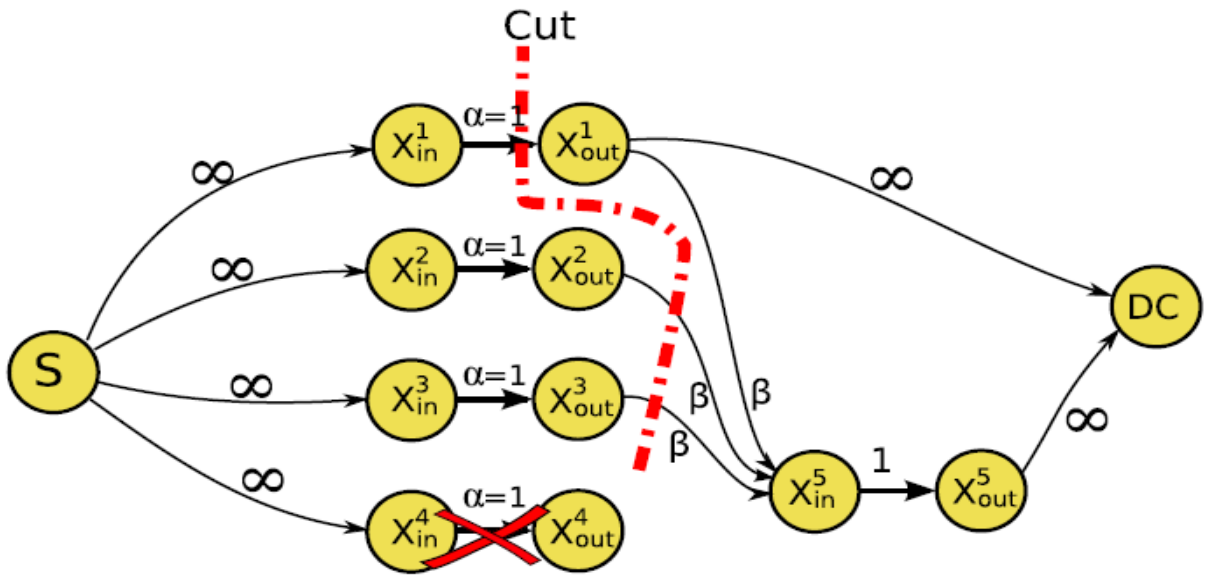


Illustration of the information flow graph G corresponding to the (4,2) regenerating code

The min-cut separating the source and the data collector must be larger than M = 2Mb for reconstruction to be possible. For this graph, the min-cut value is given by $1 + 2\beta$, implying that 0.5Mb is sufficient and necessary.

Storage-Bandwidth Tradeoff:

For each set of parameters (n, k, d, α, γ), there is a family of information flow graphs, each of which corresponds to a particular evolution of node failures/repairs.

An (n, k, d, α, γ) tuple will be feasible, if a code with storage α and repair bandwidth γ exists.

Generalized regenerating code:

Regenerating codes: $\aleph_H = C_{n-1}^{d}$, $\aleph_R = C_n^k$

Generalized regenerating codes: $1 \leq \aleph_R \leq C_n^k$, $1 \leq \aleph_H \leq C_{n-1}^{d}$

- MDS code
- Fractional Repetition Code

Generalized regenerating codes

MDS codes: A linear code which meets the singleton bound is called a Maximum Distance Separable (MDS) code .

$$d \leq n - k + 1$$

Fractional Repetition Codes: A FR code C with repetition degree ρ for an (n, k, d) DSS is a collection of n subsets $v_1, v_2, \ldots, v_n$ of a set $\Omega = \{1, \ldots, \theta\}$

And of cardinality d such that each element of Ω belongs to exactly ρ sets in the collection.

$$\rho\theta = nd$$

Intruder Model:

- Passive Eavesdropper:
- Active Omniscient Adversary:
- Active Limited-Knowledge Adversary:

Generalized regenerating codes

v_1	:	x_1	x_2	$\ldots x_\alpha$	
v_2	:	$x_{\alpha+1}$	$x_{\alpha+2}$	$\ldots x_{2\alpha}$	
		$\vdots$	$\vdots$	$\vdots$	
v_k	:	$x_{(k-1)\alpha+1}$	$\cdots$	$x_{k\alpha}$	
v_{k+1}	:	$x_{k\alpha}$	x_1	$\cdots$	$x_{\alpha-1}$
v_{k+2}	:	x_α	$x_{\alpha+1}$	$\cdots$	$x_{2\alpha-1}$
	$\vdots$	$\vdots$	$\vdots$		
v_{2k}	:	$x_{(k-1)\alpha}$	$x_{(k-1)\alpha+1}$	$\cdots$	$x_{k\alpha-1}$
		$\vdots$	$\vdots$	$\vdots$	

REFERENCES

1. Dimakis, Alexandros G., et al. "Network coding for distributed storage systems." *IEEE transactions on information theory* 56.9 (2010): 4539-4551.

2. Rashmi, K. V., et al. "Regenerating codes for errors and erasures in distributed storage." *2012 IEEE International Symposium on Information Theory Proceedings*. IEEE, 2012.

3. K. V. Rashmi, N. B. Shah, P. V. Kumar, and K. Ramchandran, "Explicit construction of optimal exact regenerating codes for distributed storage," in Proc. Allerton Conf., Urbana-Champaign, Sep. 2009.

4. N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran, "Explicit codes minimizing repair bandwidth for distributed storage," in Proc.IEEE ITW, Cairo, Jan. 2010.

5. S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing dynamic distributed storage systems against eavesdropping and adversarial attacks," IEEE Trans. Inf. Theory, vol. 57, no. 10, pp. 6734–6753, 2011.