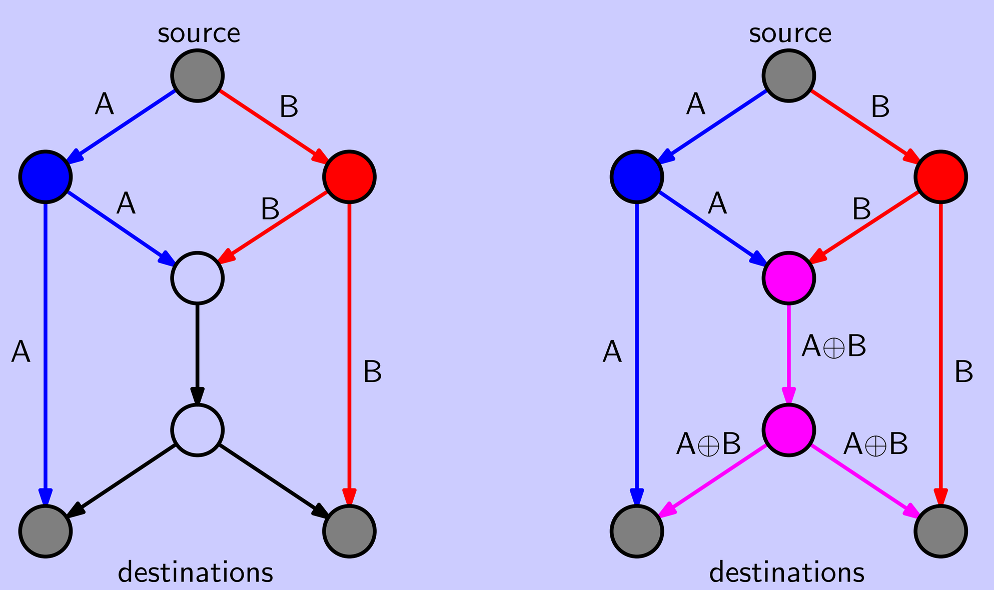
Projective Space Codes for the Injection Metric

Azadeh Khaleghi and Frank R. Kschischang
Department of Electrical and Computer Engineering
University of Toronto

Background and Motivation

Network Coding: Output at intermediate nodes are **functions** of their input packets.



Random Linear Network Coding: Each intermediate node outputs a **random linear combination** of its input packets.

Problem: Error Propagation → even a single corrupt packet, when combined with other packets in the network may render the entire transmission useless!

Adversarial Channel Model:

A source transmits source packets: $X_1, X_2, \cdots, X_m$. There exists a malicious node (an adversary) in the network that may inject (upto t) erroneous packets $E_1, E_2, \cdots, E_t$ at some or all of its outgoing links. A receiver receives

$$Y = AX + BE,$$

where $X = \begin{bmatrix} X_1 \\ X_2 \\ \vdots \\ X_m \end{bmatrix}$, $E = \begin{bmatrix} E_1 \\ E_2 \\ \vdots \\ E_t \end{bmatrix}$ and, A and B are the transfer matrices corresponding to the source and error packets respectively. Notice that in the absence of errors and if A is full-rank, $\langle Y \rangle = \langle AX \rangle$. Thus network coding is equivalent to transmission of vector-spaces.

Mathematical Preliminaries

Let W be an n-dimensional vector space over $\mathbf{F}_q$.

Projective Space: The set of all subspaces of W forms a projective space $\mathcal{P}_q(n)$.

Grassmannian: The set of all k-dimensional subspaces of W, $k \leq n$ forms a Grassmannian $\mathcal{G}_q(n,k)$.

Injection Distance: The injection distance between U, and $V \in \mathcal{P}_q(n)$ is defined as,

$$d_I(U,V) = \max\{\dim U, \dim V\} - \dim(U \cap V).$$

$d_I(\cdot,\cdot)$ is shown to be a suitable metric for adversarial error-control in network coding.

Spheres in Projective Space

Let V be a k-dimensional vector space in $\mathcal{P}_q(n)$. We define $B_V(t)$ to be the set of all spaces in $\mathcal{P}_q(n)$ at an injection distance at most t from V: $B_V(t) = \{W \in \mathcal{P}(n) | d_I(V,W) \leq t\}$

$\mathcal{P}_q(n)$ is a highly non-homogeneous space, in particular spheres of the same radius are not necessarily of the same size.

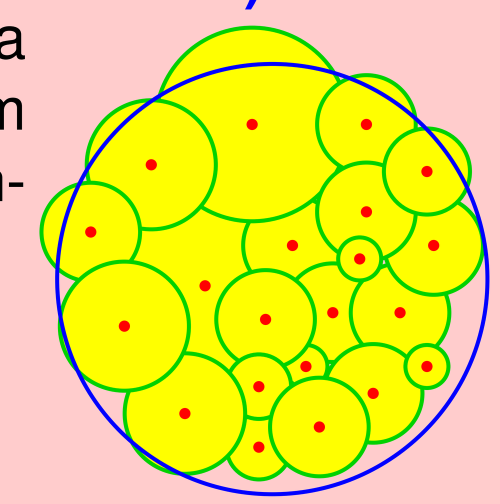
Theorem: The size of $B_V(t)$ depends on $\dim V$ and is given by,

$$|B_V(t)| = \sum_{i=1}^{t} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q + \sum_{j=1}^{i} q^{i(i-j)} \left(\begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i-j \end{bmatrix}_q + \begin{bmatrix} n-k \\ i \end{bmatrix}_q \begin{bmatrix} k \\ i-j \end{bmatrix}_q \right)$$

Theorem: (Gilbert-Varshamov Bound)

The maximum size $A_q(n,d)$ of a code $C \subseteq \mathcal{P}_q(n)$ with minimum injection distance d is guaranteed to be at least,

$$A_q(n,d) \geq \frac{|\mathcal{P}_q(n)|^2}{\sum\limits_{X \in \mathcal{P}_q(n)} |B_X(d-1)|}.$$



Code Design

Objective: Construct a set $\mathcal{C} \subseteq \mathcal{P}_q(n)$ such that,

for all $U, V \in \mathcal{C}, d_I(U,V) \geq d.$

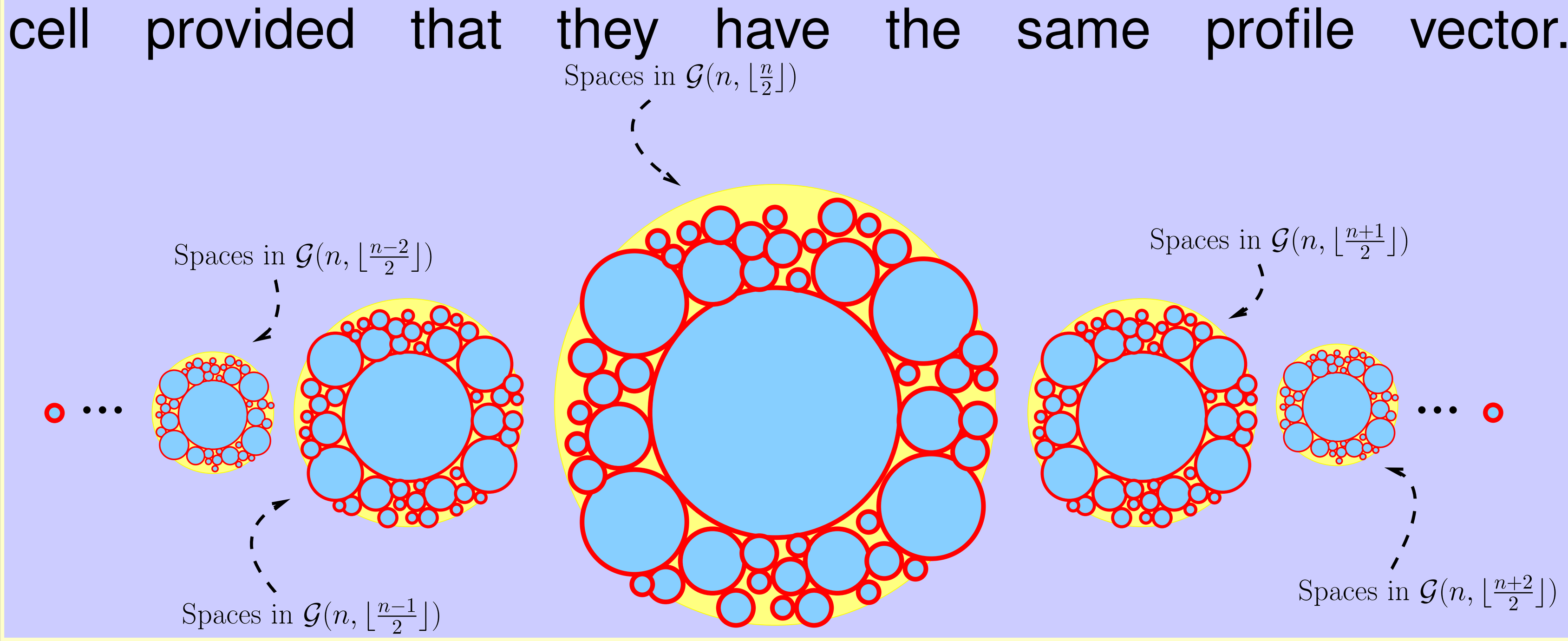
Every vector space in $\mathcal{P}_q(n)$ arises **uniquely** as the row-space of a matrix in **Reduced Row Echelon Form (RREF)**.

Let $V = \langle X \rangle \in \mathcal{P}_q(n)$ where X is in RREF. The **profile vector** of V is a binary vector of length n, whose non-zero elements appear **only** in positions where X has a **leading** 1.

For example, $U = \left\langle \begin{bmatrix} \mathbf{1} & u_{12} & \mathbf{0} & u_{14} & \mathbf{0} & \mathbf{0} & u_{17} \\ \mathbf{0} & 0 & \mathbf{1} & u_{24} & \mathbf{0} & \mathbf{0} & u_{27} \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{1} & \mathbf{0} & u_{37} \\ \mathbf{0} & 0 & \mathbf{0} & 0 & \mathbf{0} & \mathbf{1} & u_{47} \end{bmatrix} \right\rangle \rightarrow p(U) = 1010110$

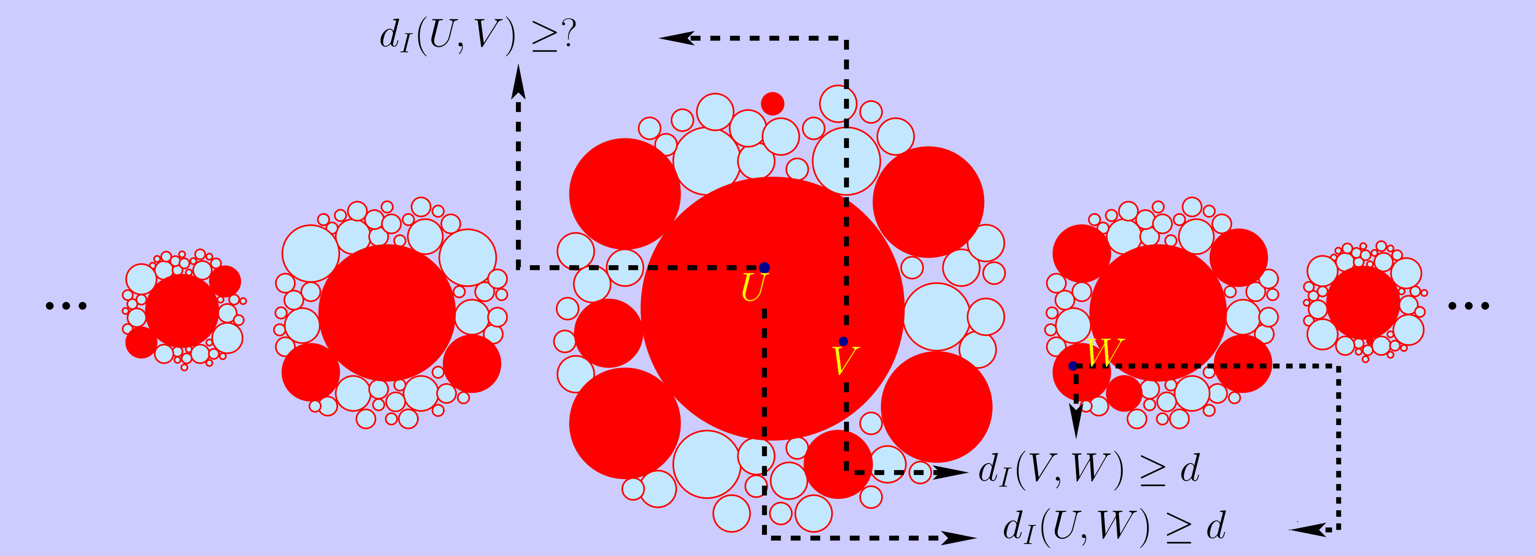
In fact all spaces of the form $\left\langle \begin{bmatrix} 1 & \bullet & 0 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 1 & \bullet & 0 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{bmatrix} \right\rangle$, have 1010110 as their profile vector.

The set of all binary vectors $v \in \{0,1\}^n$ partition $\mathcal{P}_q(n)$, in which two space belong to the same cell provided that they have the same profile vector.



Construction Procedure

Step I: Select a set of *cells* with *minimum inter-cell distance* d.



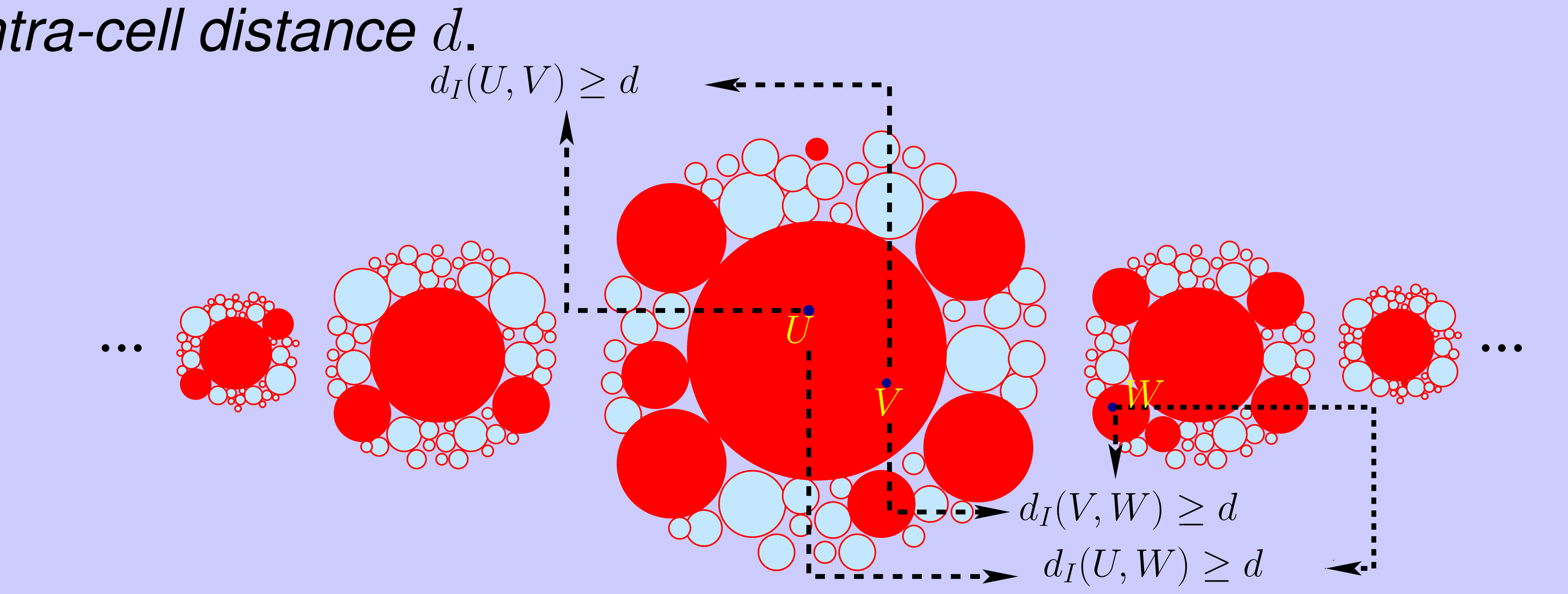
Theorem: Let U and V be two vector spaces in $\mathcal{P}_q(n)$, with profile vectors u and v, respectively. Then,

$$d_I(U,V) \geq \max\{N(u,v), N(v,u)\} = d_a(u,v)$$

where $N(x,y)$ the number of $1 \rightarrow 0$ transitions from x to y.

→ we select the profile vectors according to a **binary asymmetric code** with minimum distance $d_a \geq d$.

Step II: Select a **subset** of spaces **within each cell** with *minimum intra-cell distance* d.



If $p(\langle X \rangle) = p(\langle Y \rangle)$, then $d_I(\langle X \rangle, \langle Y \rangle) = \mathrm{rank}(X - Y) = d_R(X,Y)$.

→ we use Rank-Metric Codes to preserve the intra-cell distance.

Theorem: Let M be an $m \times n$ matrix in RREF, with a total of w •'s. Let C be a subcode of a linear Maximum-Rank-Distance code that fits M with $d_R(C) \geq \delta$. Then,

$$\dim C \geq w - \max\{m,n\}(\delta - 1)$$

Selecting the Profile Vectors

Given a minimum injection distance d we calculate for each vector $v \in \{0,1\}^n$, $\mathrm{score}(v,d) = \sum_{i=1}^{n} \sum_{j=1}^{i} \bar{v}_i v_j - \max\{m(v), \eta(v)\}(d-1)$, where, $\eta(v) = n - (wt(v) + \min_{t \in \mathrm{supp}(v)} t) + 1$, and $m(v) = wt(v) - (n - \max_{t \in \mathrm{supp}(\bar{v})} t)$.

We use a standard greedy algorithm to select a set of profile vectors at a minimum asymmetric distance d.

1. R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Trans. Inf. Theory*, 2008.
2. D. Silva, F. R. Kschischang, and R. Kötter, "A rank-metric approach to error control in random network coding," *IEEE Trans. Inf. Theory*, 2008.
3. D. Silva and F. R. Kschischang, "On metrics for error correction in network coding," submitted for publication, 2008.
4. T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," submitted for publication, 2009.
5. T. Etzion and A. Vardy, "Error-correcting codes in projective space," *ISIT*, 2008.
6. A. Khaleghi and F. R. Kschischang, " Projective Space Codes for the Injection Metric,"Canadian Workshop on Inf. Theory, 2009.