Galois geometries and Random network coding

Leo Storme

Ghent University
Dept. of Mathematics
Krijgslaan 281
9000 Ghent
Belgium

Buenos Aires, July 29, 2016

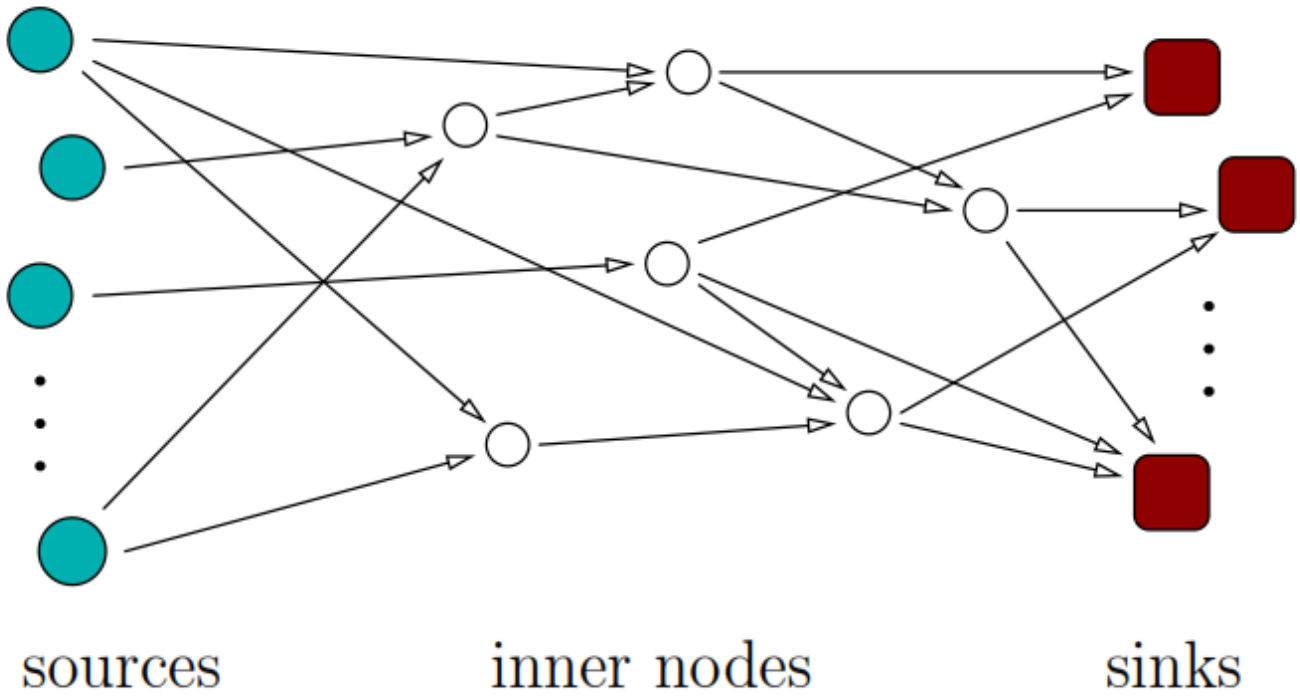
UNIVERSITEIT GENT

OUTLINE

OUTLINE

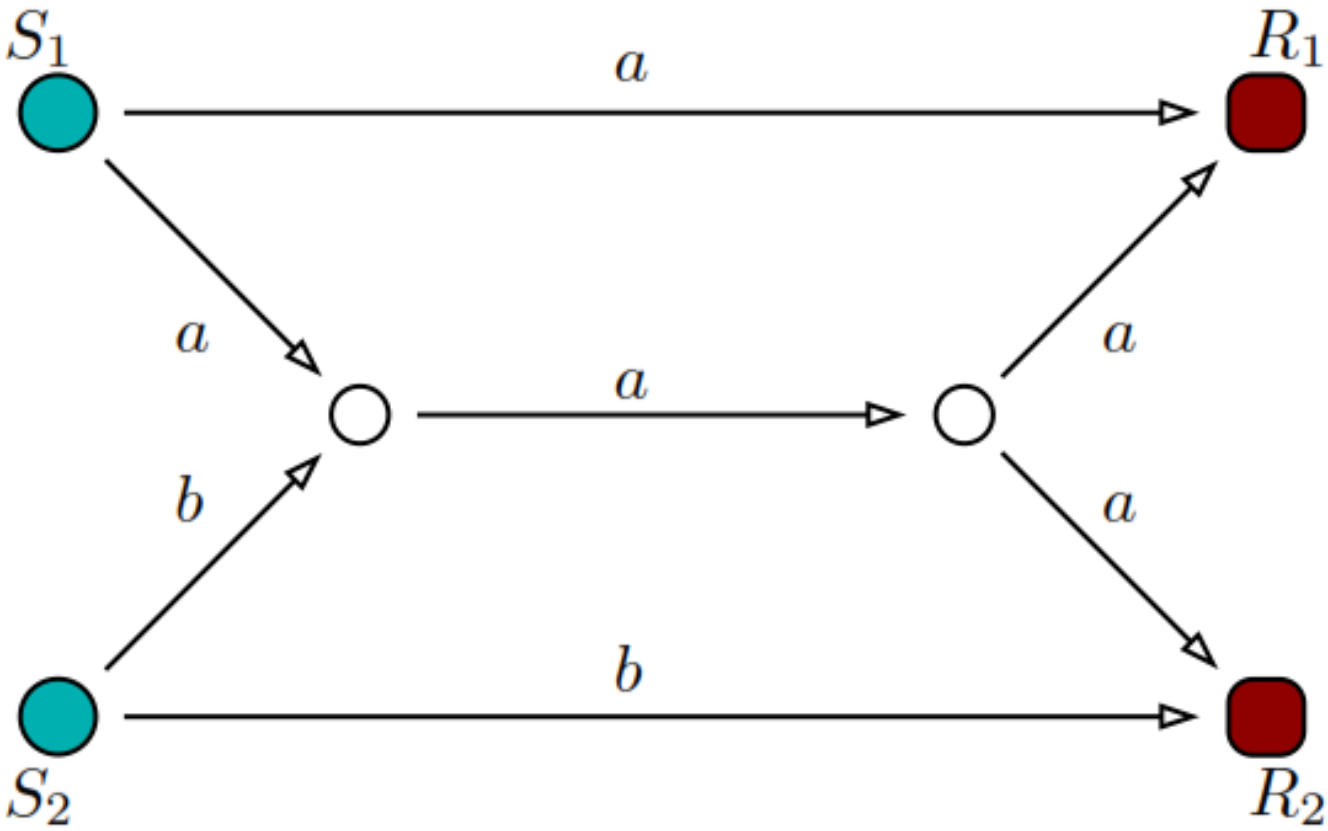
RANDOM NETWORK CODING

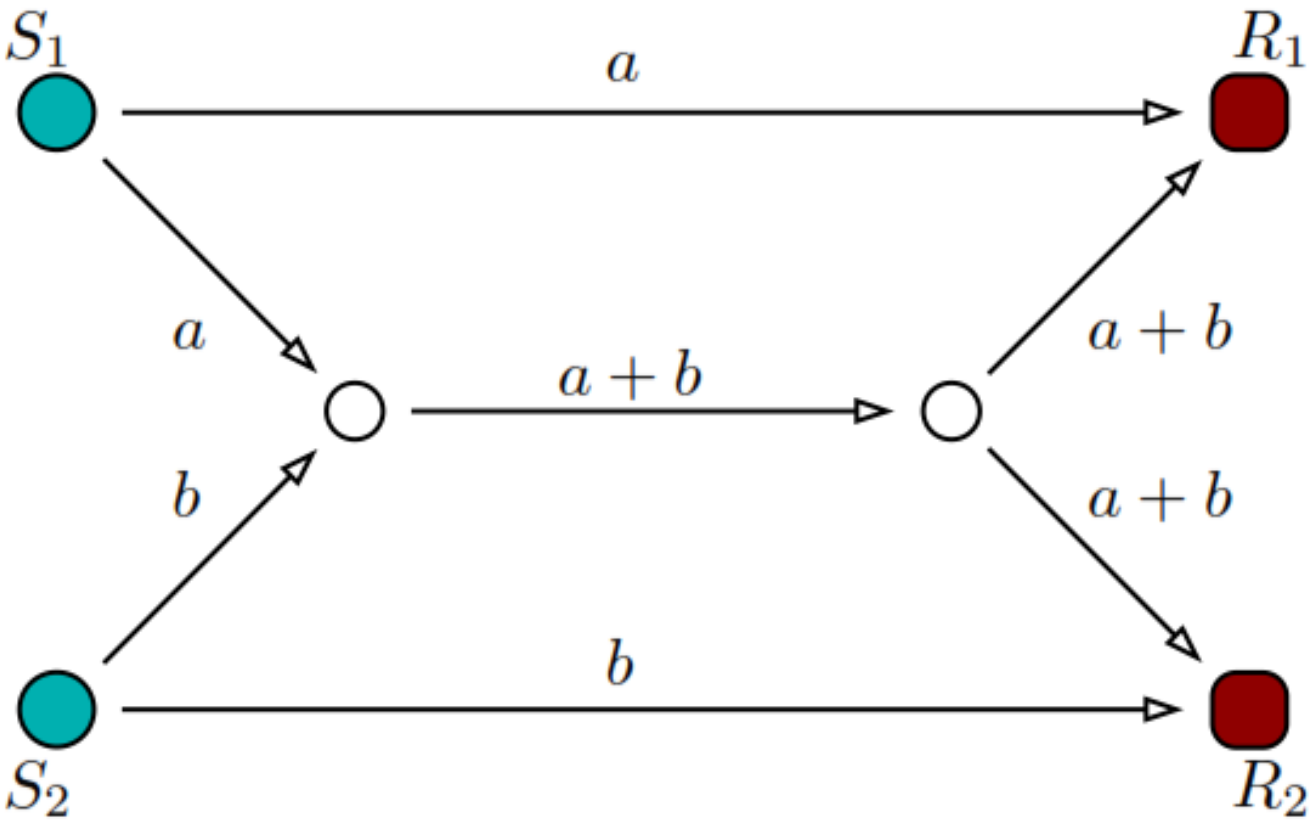
- Consider network with varying topology: users come and go.
- How to transmit quickly information through the network?


sources
inner nodes
sinks

RANDOM NETWORK CODING

- Kötter and Kschischang: use *network codes*,
- Codewords: k-dimensional subspaces U of $V(n, q)$ (n-dimensional vector space over the finite field $\mathbb{F}_q$).
- Transmit basis of U, but:
  - intermediate nodes transmit linear combinations of incoming basis vectors.
- Kötter and Kschischang noticed this speeds up the transmission.


S_1
R_1
a
a
a
a
b
a
b
S_2
R_2


S_1
R_1
a
a
$a+b$
$a+b$
b
$a+b$
b
S_2
R_2

COMPLETE NEW THEORY

Complete new theory opens: from classical coding theory to random network coding

Constant dimension code: all codewords have same dimension k.

Subspace distance:

- U, V subspaces of $V(n, q)$:

$$d(U, V) = \dim(U) + \dim(V) - 2\dim(U \cap V).$$

- Minimum distance $d(C) = \min_{\{U,V \in C, U \neq V\}} d(U, V)$.
- So the larger d, the smaller $\dim(U \cap V)$.

JOHNSON BOUND FOR RANDOM NETWORK CODES

Notations:

- $\mathcal{A}_q(n, d, k)$: largest number of codewords in random network code of k-dimensional codewords in $V(n, q)$ having minimum distance d.
- $$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

(number of $V(k, q)$ in $V(n, q)$)

JOHNSON BOUND FOR RANDOM NETWORK CODES

1. $$\mathcal{A}_q(n,d,k) \leq \frac{q^n-1}{q^k-1}\mathcal{A}_q(n-1,d,k-1).$$
2. Let $t = k - d/2 + 1$.
$$\mathcal{A}_q(n,d,k) \leq \frac{\begin{bmatrix} n \\ t-1 \end{bmatrix}_q}{\begin{bmatrix} k \\ t-1 \end{bmatrix}_q}\mathcal{A}_q(n-k+d/2,d,d/2).$$
3. $$\mathcal{A}_q(n-k+d/2,d,d/2)$$
equals the maximum size of partial $(d/2-1)$-spread in $\mathrm{PG}(n-k+d/2-1,q)$ (= set of pairwise disjoint $d/2$-dimensional subspaces of $V(n-k+d/2,q)$).

EXAMPLE

- $$\mathcal{A}_q(6,4,3) \leq (q^3+1)^2.$$
- Vector meaning: Upper bound on number of 3-dimensional subspaces of $V(6,q)$ pairwise intersecting in at most a 1-dimensional subspace is $(q^3+1)^2$.
- Projective meaning: Upper bound on number of planes in PG$(5,q)$ pairwise intersecting in at most a projective point is $(q^3+1)^2$.

SHARP RESULT

$$\mathcal{A}_2(6,4,3) \leq (2^3+1)^2 = 81.$$

THEOREM (HONOLD, KIERMAIER, KURZ)

$$\mathcal{A}_2(6,4,3) = 77.$$

Maximal number of planes in $PG(5,2)$ pairwise intersecting in at most a point is 77.

THEOREM (HONOLD, KIERMAIER, KURZ, COSSIDENTE, PAVESE)

$$q^6+2q^2+2q+1 \leq \mathcal{A}_q(6,4,3) \leq (q^3+1)^2.$$

Example of q^6+2q^2+2q+1 planes in $PG(5,q)$ pairwise intersecting in at most a point.

OUTLINE

t-INTERSECTING CONSTANT DIMENSION RANDOM NETWORK CODES

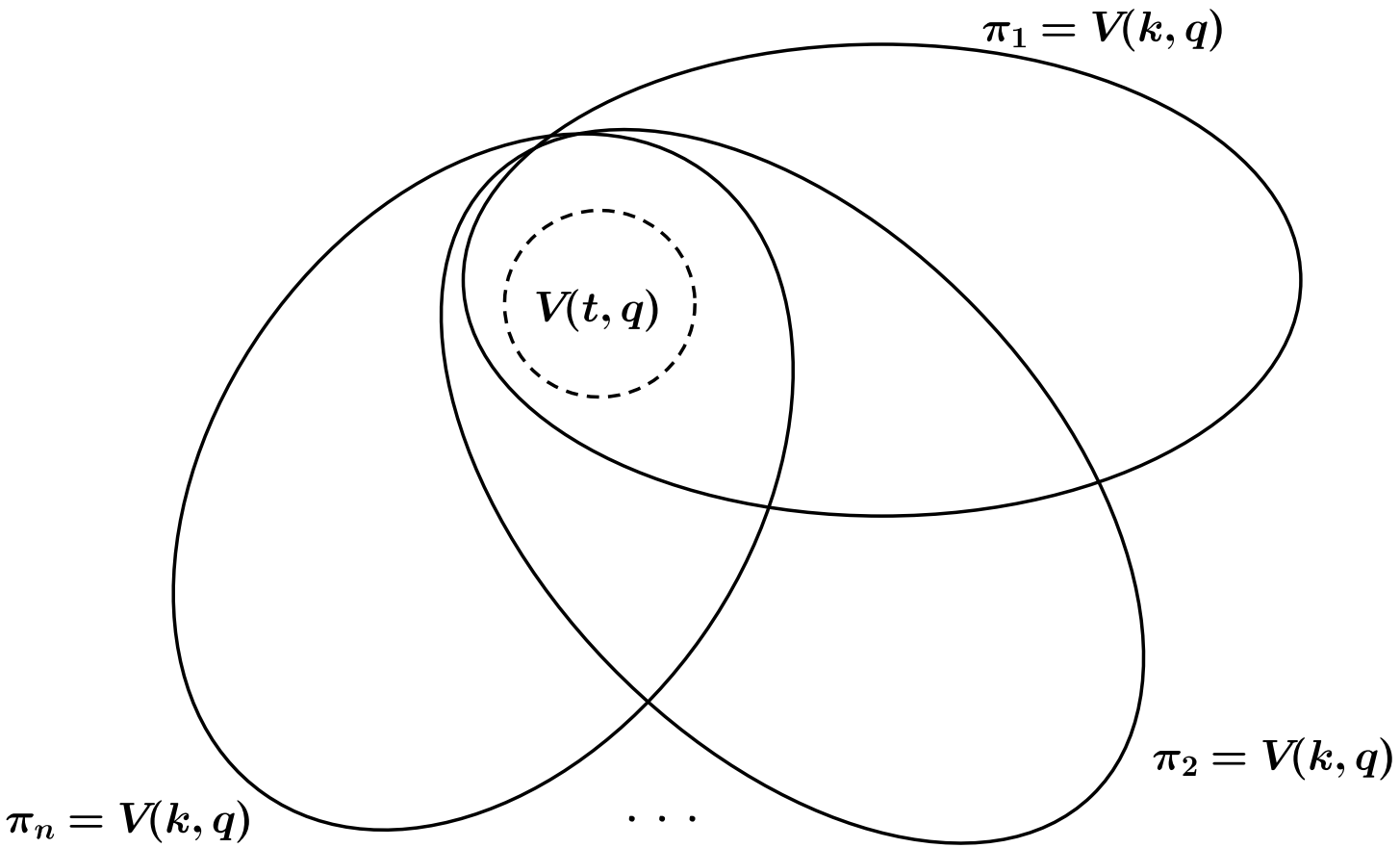
t-Intersecting constant dimension random network code:

- Codewords are k-dimensional vector spaces.
- Distinct codewords intersect in t-dimensional vector spaces.

Classical example:

- **Sunflower:** all codewords pass through same t-dimensional vector space.

SUNFLOWER



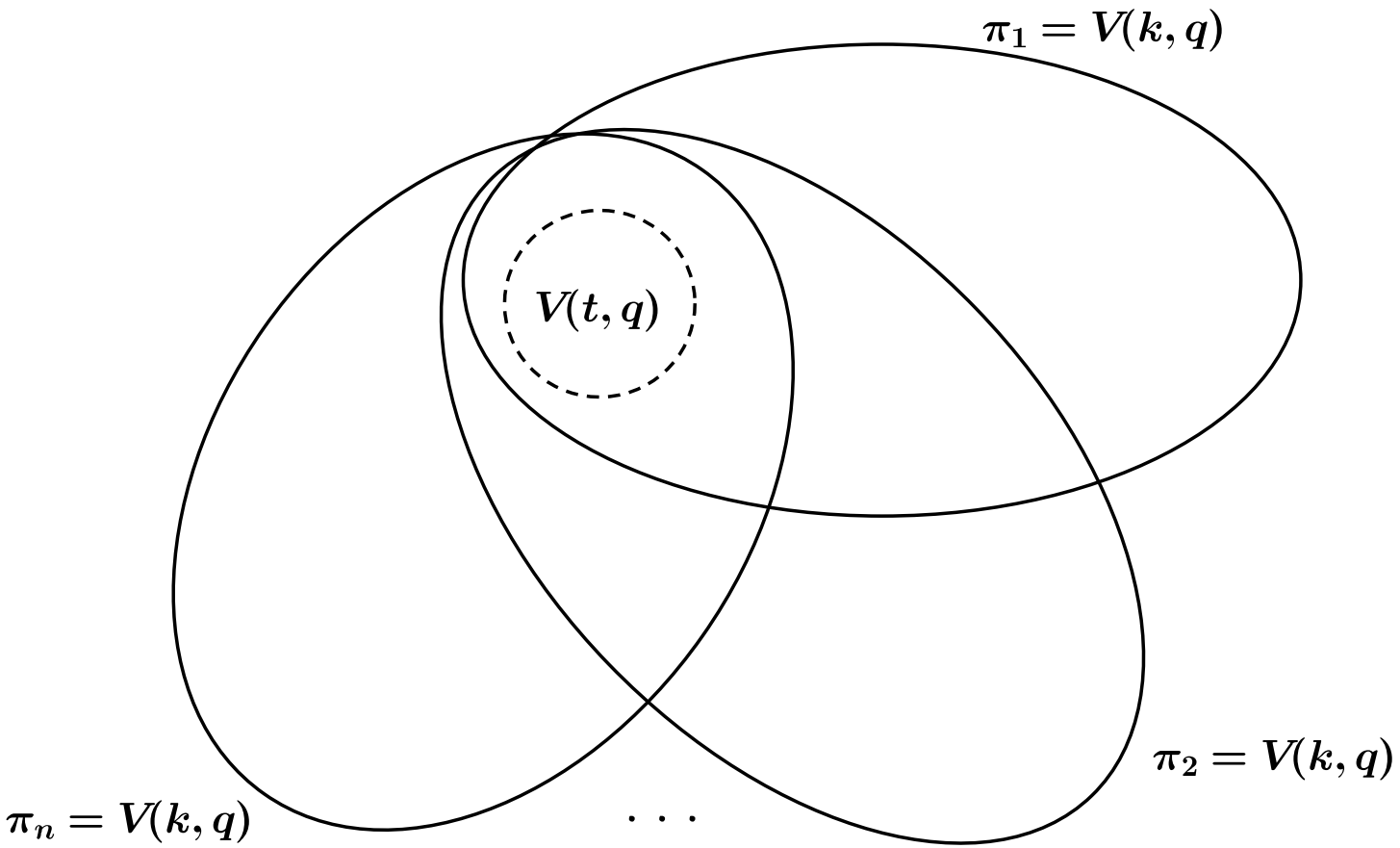
Large t-intersecting constant dimension random network codes

Large t-intersecting constant dimension random network codes are sunflowers.

Theorem

If $|C| > (\frac{q^k-q^t}{q-1})^2 + (\frac{q^k-q^t}{q-1}) + 1$, *then* C *is sunflower.*

SUNFLOWER



A DIMENSION RESULT

- Let C be $(k-t)$-intersecting constant dimension random network code of k-dimensional codewords.
- Let $C = \{\pi_1, \ldots, \pi_n\}$.
- Maximal dimension for sunflower is

$$\dim\langle \pi_1, \ldots, \pi_n \rangle = k + t(n-1).$$

Question: From which dimension for $\langle \pi_1, \ldots, \pi_n \rangle$ are we sure that C is sunflower?

A DIMENSION RESULT

THEOREM (BARROLLETA, STORME, SUAREZ-CANEDO, VANDENDRIESSCHE)

Let $C = \{\pi_1, \ldots, \pi_n\}$ be $(k-t)$-intersecting constant dimension random network code of k-dimensional codewords.
If $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 2$, *then C is sunflower.*

PROOF:

- Order codewords.
- $$\delta_i = \dim\langle \pi_1, \ldots, \pi_i \rangle - \dim\langle \pi_1, \ldots, \pi_{i-1} \rangle.$$
- Order codewords so that $\delta_2 \geq \delta_3 \geq \cdots \geq \delta_n$.
- Sequence $(\delta_2, \ldots, \delta_n)$.
- $\delta_2, \ldots, \delta_{n-1} \geq t-1$.

Dimension result is sharp

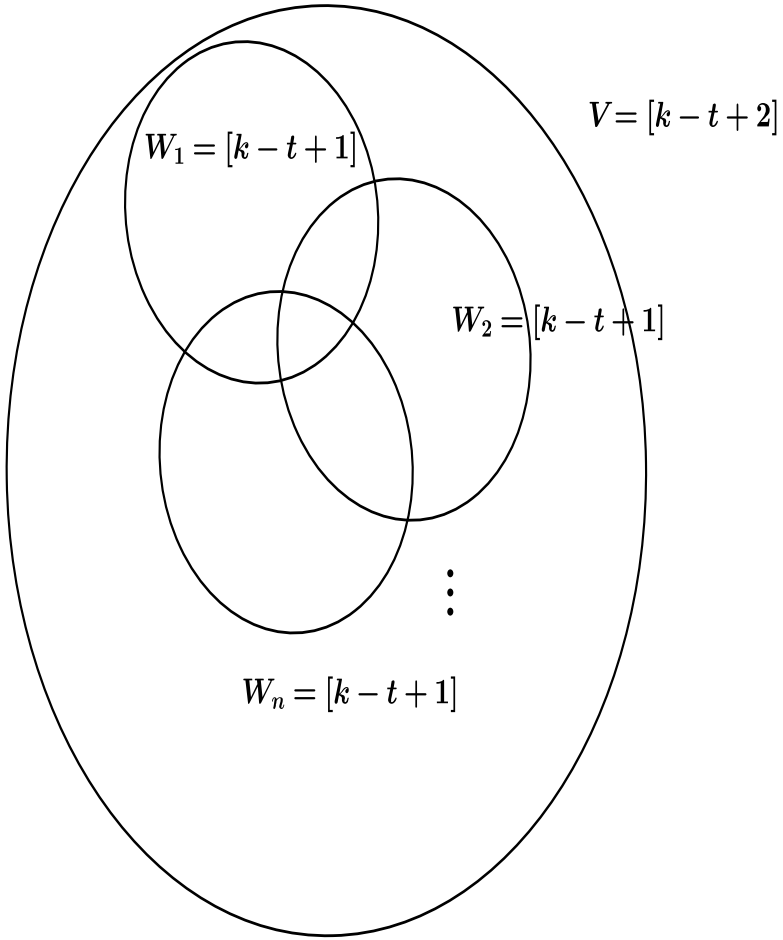
Theorem (Barrolleta, Storme, Suarez-Canedo, Vandendriessche)

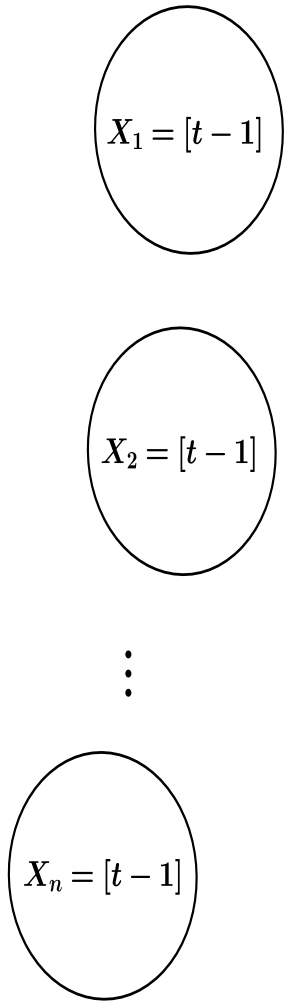
Let $C = \{\pi_1, \ldots, \pi_n\}$ be $(k-t)$-intersecting constant dimension random network code of k-dimensional codewords.
If $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 2$, then C is sunflower.

Theorem (Barrolleta, Storme, Suarez-Canedo, Vandendriessche)

If $\dim\langle \pi_1, \ldots, \pi_n \rangle = k + (t-1)(n-1) + 1$, then C is sunflower, or one of two other types of examples.

DIMENSION RESULT IS SHARP



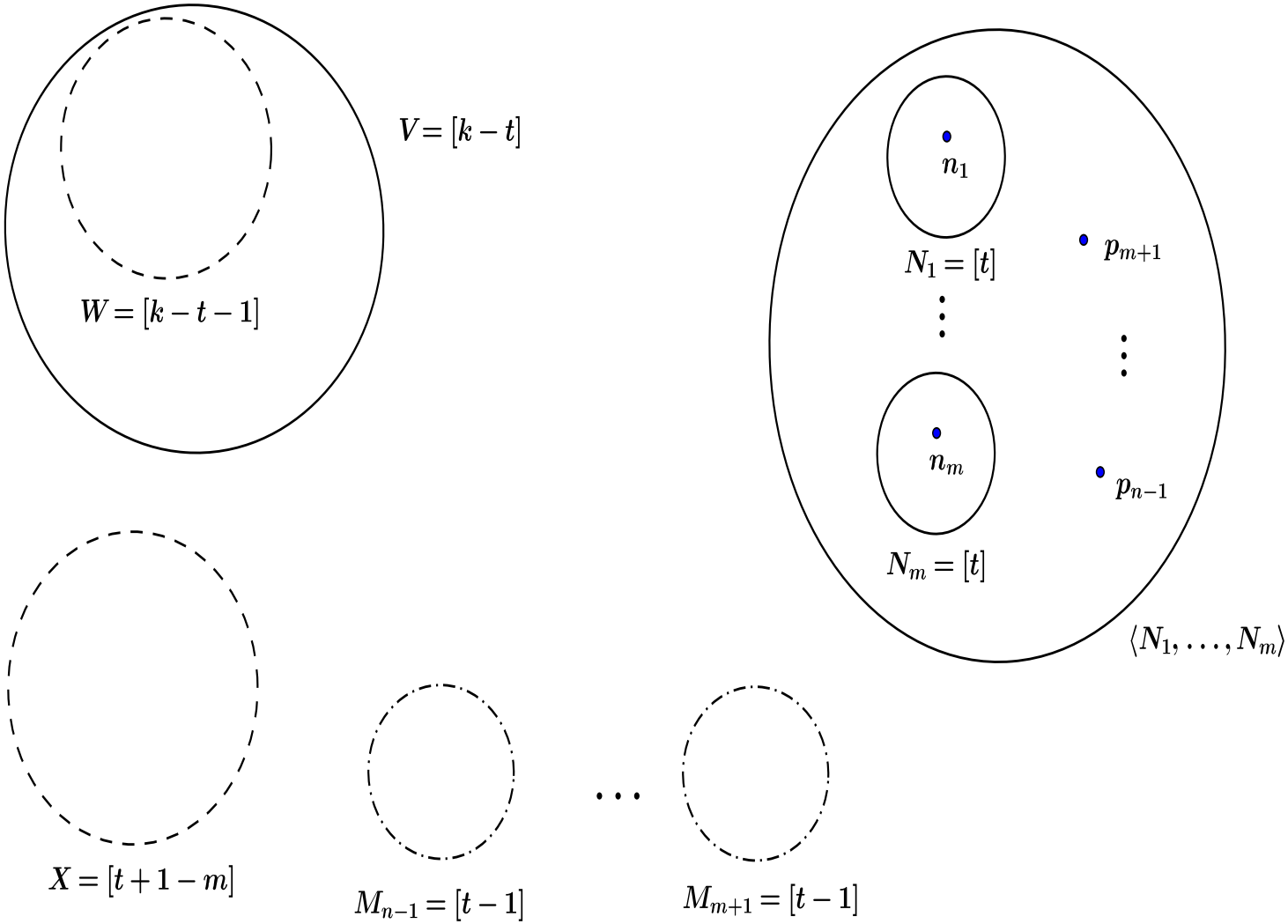


DIMENSION RESULT IS SHARP

- $V = [k - t + 2]$ fixed.
- $W_1, \ldots, W_n$ are $[k - t + 1]$ in V, not through common $[k - t]$.
- $X_1, \ldots, X_n$ are $[t - 1]$, and
- codewords are $\pi_i = \langle W_i, X_i \rangle$, $i = 1, \ldots, n$.

$$(\delta_2, \ldots, \delta_n) = (t, t - 1, \ldots, t - 1).$$

DIMENSION RESULT IS SHARP



Dimension result is sharp

- Type 1: $\pi_1 = \langle V, N_1 \rangle, \ldots, \pi_m = \langle V, N_m \rangle$.
- Type 2:
  $\pi_{m+1} = \langle V, M_{m+1}, p_{m+1} \rangle, \ldots, \pi_{n-1} = \langle V, M_{n-1}, p_{n-1} \rangle$.
- Type 3: $\pi_n = \langle W, X, n_1, \ldots, n_m \rangle$.

$$(\delta_2, \ldots, \delta_n) = (t, \ldots, t, t-1, \ldots, t-1, t+1-m).$$

Dimension result is sharp

Theorem (Barrolleta, Storme, Suarez-Canedo, Vandendriessche)

Let $C = \{\pi_1, \ldots, \pi_n\}$ be $(k-t)$-intersecting constant dimension random network code of k-dimensional codewords.
If $\dim\langle \pi_1, \ldots, \pi_n \rangle \geq k + (t-1)(n-1) + 2$, then C is sunflower.

Theorem (Barrolleta, Storme, Suarez-Canedo, Vandendriessche)

If $\dim\langle \pi_1, \ldots, \pi_n \rangle = k + (t-1)(n-1) + 1$, then C is sunflower, or one of two other types of examples.

Improvement to upper bound for $t = 1$

Large t-intersecting constant dimension random network codes are sunflowers.

- **Known result (Sunflower bound):**
  If
  $$|C| > \left(\frac{q^k - q^t}{q-1}\right)^2 + \left(\frac{q^k - q^t}{q-1}\right) + 1,$$
  then C is sunflower.

Improvement to upper bound for $t = 1$

- For $t = 1$ (k-dimensional subspaces pairwise intersecting in 1-dimensional subspaces), if

$$|C| > \left(\frac{q^k - q}{q - 1}\right)^2 + \left(\frac{q^k - q}{q - 1}\right) + 1,$$

  then C is sunflower.
- **Question:** Can this bound be improved?

Improvement to upper bound for $t = 1$

See codeword $c \in C$ as PG$(k-1, q)$.
Define

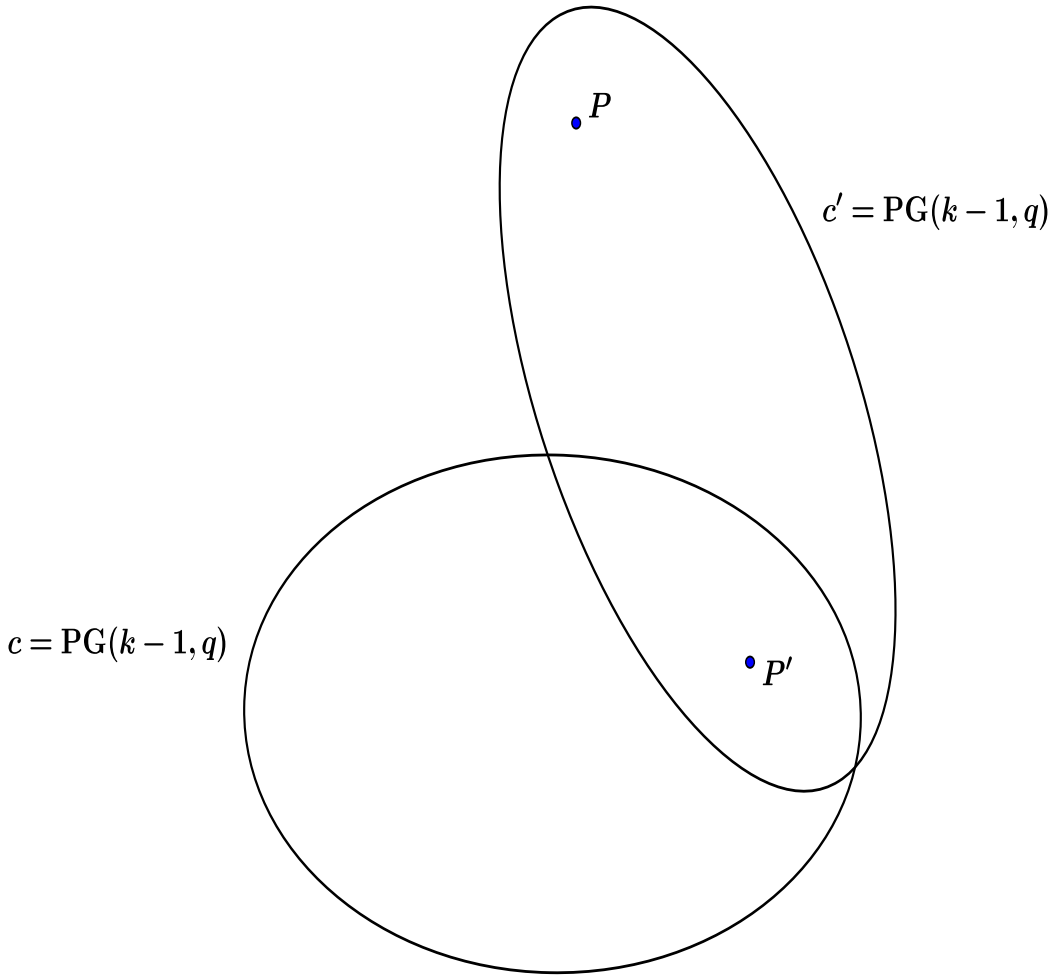
$$\mathcal{S} = \cup_{c \in C} c.$$

Lemma

Point $P \in \mathcal{S}$ belongs to at most $\frac{q^k-1}{q-1}$ codewords.

-

IMPROVEMENT TO UPPER BOUND FOR $t = 1$



Improvement to upper bound for $t = 1$

Lemma

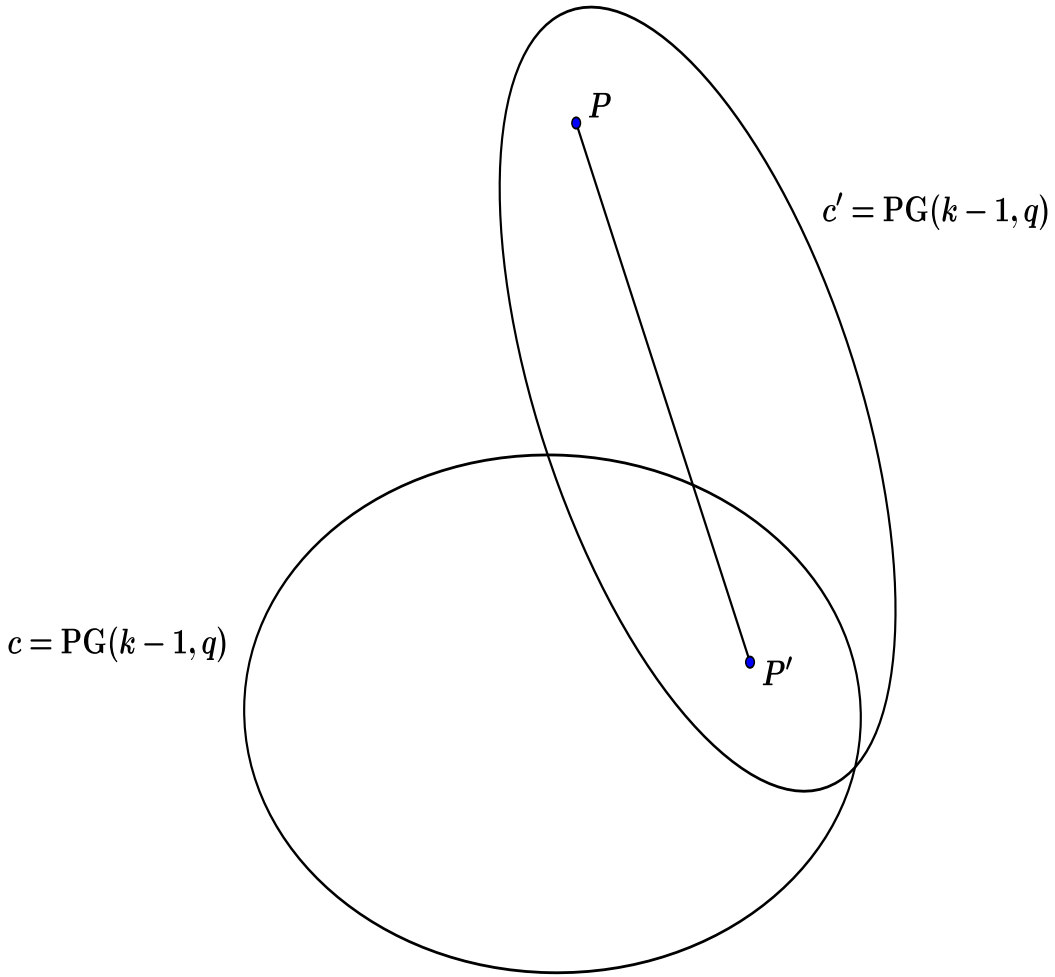
If $|C| > (\frac{q^k-q}{q-1})^2$, then every codeword in C has at least one point in $\frac{q^k-1}{q-1}$ codewords.

Lemma

If point P lies in $\frac{q^k-1}{q-1}$ codewords, then line through P and other point of $\mathcal{S}$ is completely contained in $\mathcal{S}$.

$$(\mathcal{S} = \cup_{c \in C} c)$$

IMPROVEMENT TO UPPER BOUND FOR $t = 1$



Improvement to upper bound for $t = 1$

Lemma

If point P lies in $\frac{q^k-1}{q-1}$ *codewords, then*

$$|\mathcal{S}| = |\cup_{c\in C} c| = \left(\frac{q^k-q}{q-1}\right)^2 + \left(\frac{q^k-q}{q-1}\right) + 1.$$

REMARK:

$$\left(\frac{q^k-q}{q-1}\right)^2 + \left(\frac{q^k-q}{q-1}\right) + 1 \neq |\mathrm{PG}(T,q)|.$$

$$|\mathrm{PG}(2k-2,q)| < |\mathcal{S}| < |\mathrm{PG}(2k-1,q)|.$$

Improvement to upper bound for $t = 1$

Theorem (Bartoli, Riet, Storme, Vandendriessche)

Every 1-intersecting constant dimension code C of codewords of dimension k of size

$$|C| = \left(\frac{q^k - q}{q-1}\right)^2 + \left(\frac{q^k - q}{q-1}\right) + 1 - q^{k-2},$$

is sunflower.

Three largest $(k-2)$-intersecting constant dimension codes

Theorem (Bartoli, Riet, Storme, Vandendriessche)

Largest $(k-2)$-intersecting constant dimension codes C of codewords of dimension k are:

- *code of codewords $\langle \pi_{k-1}, e \rangle$, where the spaces π_{k-1} are $(k-1)$-dimensional subspaces in a given $V(k,q)$, and e are vectors lying outside of $V(k,q)$.*
  (size: $q^{k-1} + \cdots + q + 1$)
- *set of k-subspaces in $V(k+2,q)$ which is dual of partial spread of 2-dimensional subspaces of $V(k+2,q)$:*
  (size: $\Theta(q^k)$)
- *sunflower.*

Two types of $(k-1)$-intersecting constant dimension codes

Theorem

There exist only two types of $(k-1)$-intersecting constant dimension codes C of codewords of dimension k:

- *set of k-dimensional subspaces in given $V(k+1,q)$.*
- *sunflower.*

COST PROJECT

- COST project IC-1104: *Random network coding and designs over GF(q)*
- `http://www.network-coding.eu/`
- Tuvi Etzion: *Problems on q-Analogs in Coding Theory*. More than 100 research problems.
- Lien Lambert: *Random network coding and designs over* $\mathbb{F}_q$.
  Master Thesis: Introduction to random network coding.

Thank you very much for your attention!