WHAT IS OLD, WHAT IS NEW, AND WHAT TO DO?

Tuvi Etzion

Computer Science Department

TECHNION
Israel Institute of Technology

Dubrovnik, Croatia, April 8, 2016

To Honor the Memory

Rudolph Ahlswede 1938 -- 2010

Ralf Kötter 1963 -- 2009

And Our COST Friend

Axel Kohnert 1962 -- 2013

Outline

Outline

Before we knew on network coding

Outline

Before we knew on network coding

From network codes to subspace codes

Outline

Before we knew on network coding

From network codes to subspace codes

Codes and designs over vector spaces

Outline

Before we knew on network coding

From network codes to subspace codes

Codes and designs over vector spaces

Four years in the COST Action

Outline

Before we knew on network coding

From network codes to subspace codes

Codes and designs over vector spaces

Four years in the COST Action

Open problems and future research

Before Network Coding

Before Network Coding

The father of Projective Geometry

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Who else?

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Who else?

Blaise Pascal 1623 -- 1662

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Who else?

Blaise Pascal 1623 -- 1662

What next?

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Who else?

Blaise Pascal 1623 -- 1662

What next?

unfortuntely,

Before Network Coding

The father of Projective Geometry

Girard Desargues 1593 -- 1661

Grandfather?

Pappus 300 AD

Who else?

Blaise Pascal 1623 -- 1662

What next?

unfortuntely,

a clinical death

Projective Geometry Reborn

Projective Geometry Reborn

Hermann Grassmann 1809 – 1877

Projective Geometry Reborn

The Grassmann graph

Hermann Grassmann 1809 -- 1877

The Great Geometers

The Great Geometers

Julius Plücker 1801 -- 1868

The Great Geometers

Plücker coordinates

Julius Plücker 1801 -- 1868

The Great Geometers

The Great Geometers

Gino Fano 1871 -- 1952

The Great Geometers

Fano plane

Gino Fano 1871 -- 1952

The Great Geometers

The Great Geometers

Felix Klein 1849 -- 1925

The Great Geometers

Klein quartic

Felix Klein 1849 – 1925

And Block Designers

And Block Designers

Jakob Steiner 1796 – 1863

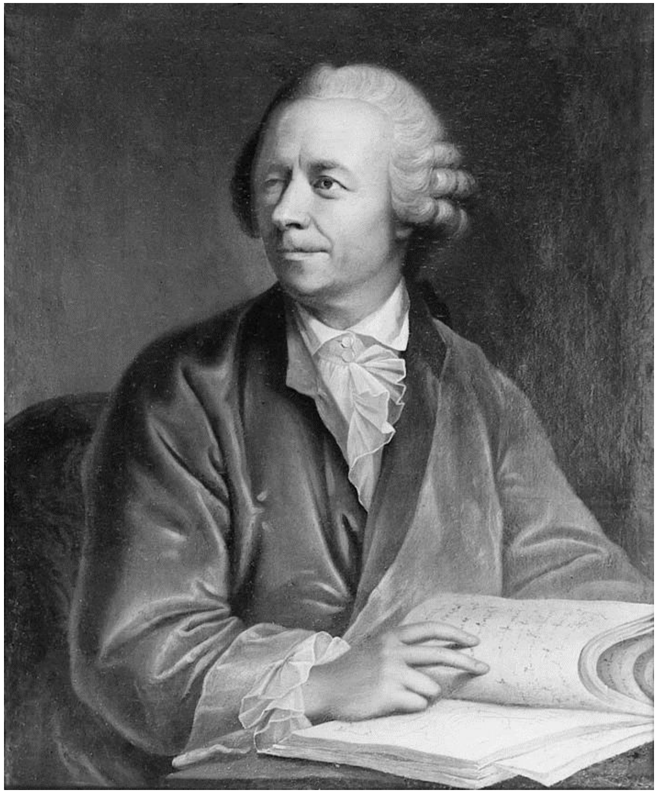
And Block Designers

Steiner systems

Jakob Steiner 1796 -- 1863

And The Great

And The Great



Leonhard Euler 1707 -- 1783

q-Analogs

q-Analogs

Jacques Tits 1930 -

1957

q-Analogs

Jacques Tits 1930 -

1957

Peter Cameron 1947 -

1974

q-Analogs

Jacques Tits 1930 -

1957

Peter Cameron 1947 -

1974

Philippe Delsarte 1942 -

1976

t-Designs Over Vector Spaces

t-Designs Over Vector Spaces

S. Thomas

1987, 1996

t-Designs Over Vector Spaces

S. Thomas

1987, 1996

D. K. Ray-Chaudhuri, N. M. Singhi

1989

t-Designs Over Vector Spaces

S. Thomas 1987, 1996

D. K. Ray-Chaudhuri, N. M. Singhi 1989

H. Susuki 1990, 1992

t-Designs Over Vector Spaces

S. Thomas 1987, 1996

D. K. Ray-Chaudhuri, N. M. Singhi 1989

H. Susuki 1990, 1992

M. Miyakawa, A. Munemasa, S. Yoshiara 1995

t-Designs Over Vector Spaces

S. Thomas — 1987, 1996

D. K. Ray-Chaudhuri, N. M. Singhi — 1989

H. Susuki — 1990, 1992

M. Miyakawa, A. Munemasa, S. Yoshiara — 1995

M. Braun, A. Kerber, R. Laue — 2005

Codes, Designs in Vector Spaces

Codes, Designs in Vector Spaces

L. Chihara

1987

Codes, Designs in Vector Spaces

L. Chihara 1987

W. J. Martin, X. J. Zhu 1995

Codes, Designs in Vector Spaces

L. Chihara 1987

W. J. Martin, X. J. Zhu 1995

R. Ahlswede, H. K. Aydinian, L. H. Khachatrian 2001

Codes, Designs in Vector Spaces

L. Chihara 1987

W. J. Martin, X. J. Zhu 1995

R. Ahlswede, H. K. Aydinian, L. H. Khachatrian 2001

M. Schwartz, T. E. 2002

Results in Projective geometry

Results in Projective geometry

Partial spread

Results in Projective geometry

Partial spread

A set of disjoint k-subspaces.

Results in Projective geometry

Partial spread

A set of disjoint k-subspaces.

Blocking set

Results in Projective geometry

Partial spread

A set of disjoint k-subspaces.

Blocking set

A set of k-subspaces which are incident to each t-subspace, $t > k$.

Results in Projective geometry

Results in Projective geometry

Albrecht Beutelspacher 1950 -

Results in Projective geometry

The size of a partial spreads

Albrecht Beutelspacher 1950 -

Results in Projective geometry

The size of a partial spreads

1-parallelisms - partitions of all 1-subspaces into spreads.

Albrecht Beutelspacher 1950 -

Results in Projective geometry

Albrecht Beutelspacher 1950 -

The size of a partial spreads

1-parallelisms - partitions of all 1-subspaces into spreads.

Geometric spreads - optimal q-covering designs.

Hamming and Preparata Codes

Hamming and Preparata Codes

The codewords of weight three in the Hamming code correspond to 1-dimensional subspaces. The union of words of weight three in certain translates of the Preparata code consists of exactly these codewords. These words in each such translate corresponds to a 1-spread. Thus, we have a 1-parallelism for the 1-dimensional subspaces.

Rank-Metric Codes

Rank-Metric Codes

Rank-metric codes played an important role in error-correcting codes for network codes and in error-correcting codes for network coding. Comprehensive work, upper bounds on their size and constructions which attain these bounds were found.

Rank-Metric Codes

Rank-metric codes played an important role in error-correcting codes for network codes and in error-correcting codes for network coding. Comprehensive work, upper bounds on their size and constructions which attain these bounds were found.

P. Delsarte 1978, E. M. Gabidulin 1985, R. M. Roth 1991

Routing

Routing

min-cut/max-flow Theorem

Routing

min-cut/max-flow Theorem

For any maximum flow problem for which a feasible flow exists, we have that the maximum $s-t$ flow value is equal to the minimum capacity of any $s-t$ cut.

Routing

min-cut/max-flow Theorem

For any maximum flow problem for which a feasible flow exists, we have that the maximum $s-t$ flow value is equal to the minimum capacity of any $s-t$ cut.

L. R. Ford Jr. and D. R. Fulkerson 1956

Routing

min-cut/max-flow Theorem

For any maximum flow problem for which a feasible flow exists, we have that the maximum $s-t$ flow value is equal to the minimum capacity of any $s-t$ cut.

L. R. Ford Jr. and D. R. Fulkerson 1956

Menger's Theorem

Routing

min-cut/max-flow Theorem

For any maximum flow problem for which a feasible flow exists, we have that the maximum $s-t$ flow value is equal to the minimum capacity of any $s-t$ cut.

L. R. Ford Jr. and D. R. Fulkerson 1956

Menger's Theorem

Let $G=(V,E)$ be a unit capacity flow network. There are k edge disjoint paths in G from s to t if and only if the maximum value of an $s-t$ flow in G' is at least k.

Routing

min-cut/max-flow Theorem

For any maximum flow problem for which a feasible flow exists, we have that the maximum $s-t$ flow value is equal to the minimum capacity of any $s-t$ cut.

L. R. Ford Jr. and D. R. Fulkerson 1956

Menger's Theorem

Let $G=(V,E)$ be a unit capacity flow network. There are k edge disjoint paths in G from s to t if and only if the maximum value of an $s-t$ flow in G' is at least k.

K. Menger 1927

Routing

Routing

For broadcasting

Routing

Edmonds Theorem

For broadcasting

Routing

For broadcasting

Edmonds Theorem

In a directed graph $G = (V, E)$ there are k edge disjoint spanning trees rooted at $r \in V$ if and only if $k \leq C_G(r, V \setminus \{r\})$.

Routing

For broadcasting

Edmonds Theorem

In a directed graph $G = (V, E)$ there are k edge disjoint spanning trees rooted at $r \in V$ if and only if $k \leq C_G(r, V \setminus \{r\})$.

J. Edmonds 1972

Routing

For broadcasting

Edmonds Theorem

In a directed graph $G = (V, E)$ there are k edge disjoint spanning trees rooted at $r \in V$ if and only if $k \leq c_G(r, V \setminus \{r\})$.

J. Edmonds 1972

Maximaizing the multicast rate is an NP-hard problem with reduction to the Steiner tree problem.

Routing

For broadcasting

Edmonds Theorem

In a directed graph $G = (V, E)$ there are k edge disjoint spanning trees rooted at $r \in V$ if and only if $k \leq C_G(r, V \setminus \{r\})$.

J. Edmonds 1972

Maximaizing the multicast rate is an NP-hard problem with reduction to the Steiner tree problem.

K. Jain, M. Mahdian, M. R. Salavatipour 2003

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Multicast Network

Network Codes to Subspace Codes

Multicast Network

A multicast network is a directed acyclic graph containing a single source node and a collection of N destination nodes. The source node has a set of h messages from a fixed alphabet and each destination node tries to recover all the messages.

Network Codes to Subspace Codes

Network Codes to Subspace Codes

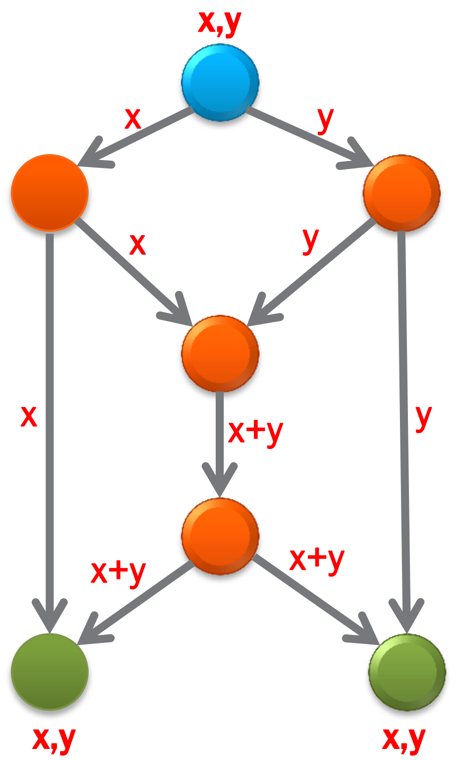
Multicast Network

Network Codes to Subspace Codes

Multicast Network

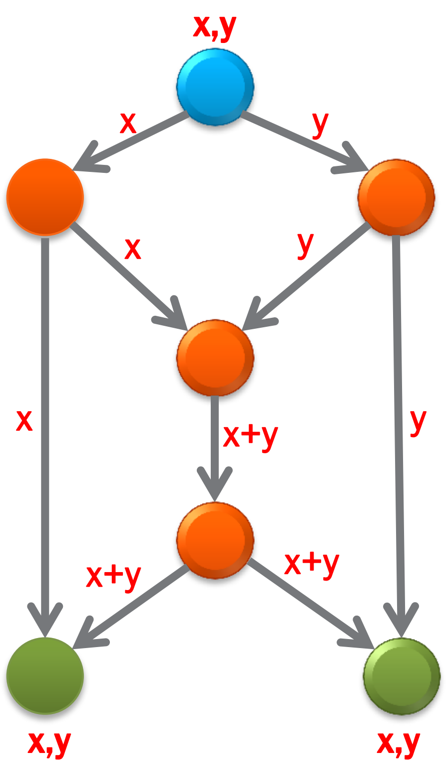
A multicast network is a directed acyclic graph containing h source nodes and a collection of N destination nodes. Each source node has one message from a fixed alphabet and each destination node tries to recover all the messages.

Network Codes to Subspace Codes



Network Codes to Subspace Codes

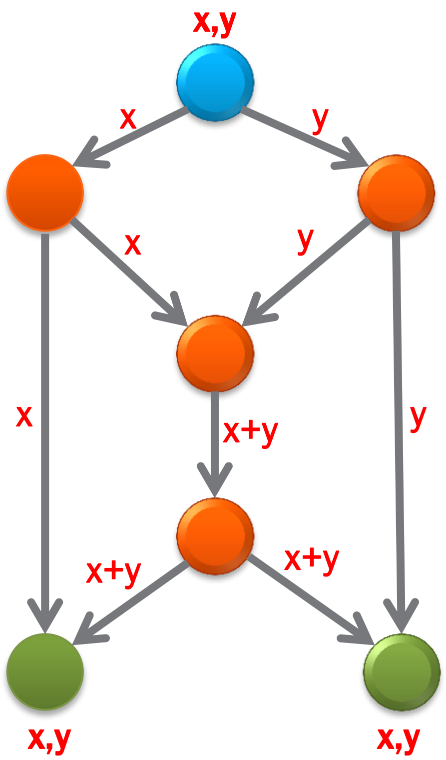
The butterfly network



Network Codes to Subspace Codes

The butterfly network

$\mathbf{x}, \mathbf{y} \in \{\mathbf{0}, \mathbf{1}, \dots, \boldsymbol{n} - \mathbf{1}\}$

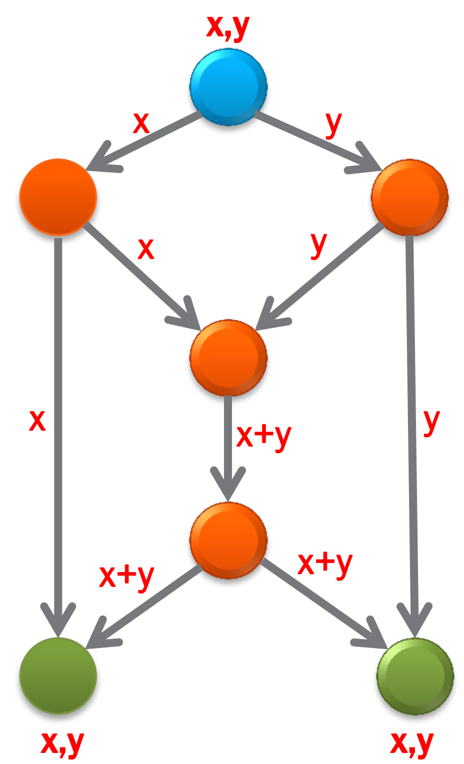


Network Codes to Subspace Codes

The butterfly network

$\mathbf{x}, \mathbf{y} \in \{\mathbf{0}, \mathbf{1}, \dots, \boldsymbol{n} - \mathbf{1}\}$

computation modulo n

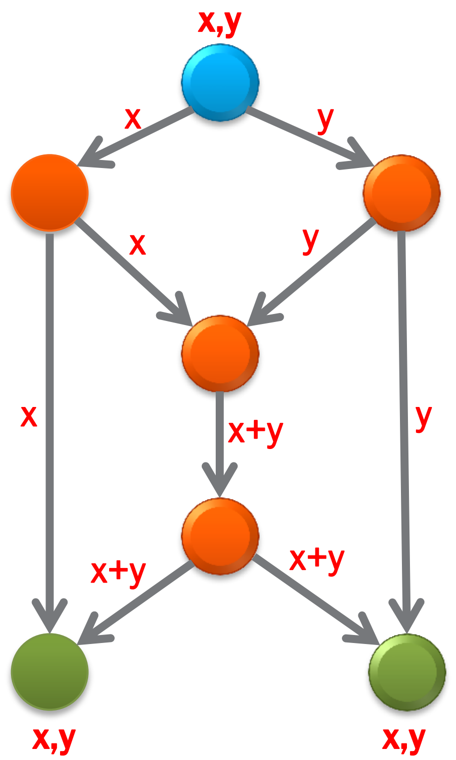


Network Codes to Subspace Codes

The butterfly network

$\mathbf{x}, \mathbf{y} \in \{\mathbf{0}, \mathbf{1}, \ldots, \boldsymbol{n}-\mathbf{1}\}$

computation modulo n



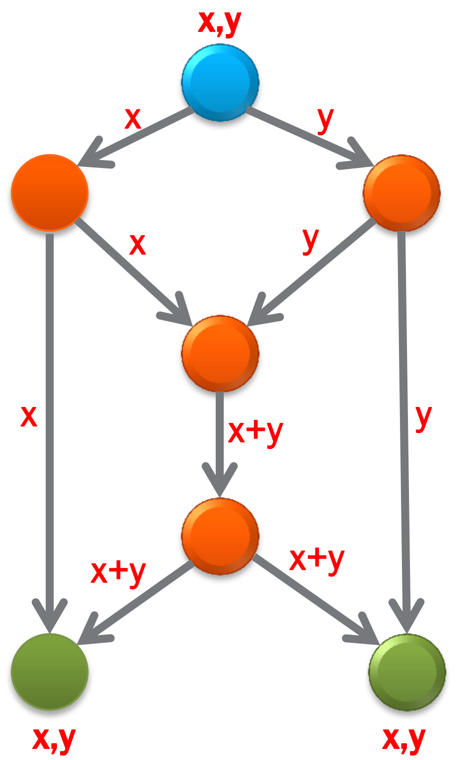
R. Ahlswede, N. Cai, S.-Y. Li, R. W. Yeung 2000

Network Codes to Subspace Codes

The butterfly network

$\mathbf{x}, \mathbf{y} \in \{\mathbf{0}, \mathbf{1}, \dots, \boldsymbol{n} - \mathbf{1}\}$

computation modulo n



R. Ahlswede, N. Cai, S.-Y. Li, R. W. Yeung 2000

S.-Y. Li, R. W. Yeung, N. Cai 2003

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Min-Cut/Max-Flow Theorem for Multicast Networks

Network Codes to Subspace Codes

Min-Cut/Max-Flow Theorem for Multicast Networks

A multicast network is solvable if there exist h edge disjoint paths, starting at the h sources, to each one of the N destination nodes.

Network Codes to Subspace Codes

Min-Cut/Max-Flow Theorem for Multicast Networks

A multicast network is solvable if there exist h edge disjoint paths, starting at the h sources, to each one of the N destination nodes.

A multicast network is solvable if the min-cut to each destination is h.

Network Codes to Subspace Codes

Network Codes to Subspace Codes

R. Kötter, M. Médard 2003

Network Codes to Subspace Codes

Algebraic Approach for Network Coding

R. Kötter, M. Médard 2003

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Polynomial Time Algorithm for Solvable Multicast Networks

Network Codes to Subspace Codes

Polynomial Time Algorithm for Solvable Multicast Networks

A polynomial time algorithm to find the network code of a solvable multicast network with N receivers. The solution is over any field $\mathbb{F}_q$ such that $q \geq N$.

Network Codes to Subspace Codes

Polynomial Time Algorithm for Solvable Multicast Networks

A polynomial time algorithm to find the network code of a solvable multicast network with N receivers. The solution is over any field $\mathbb{F}_q$ such that $q \geq N$.

S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, L. M. G. M. Tolhuizen 2005

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Random Network Coding

Network Codes to Subspace Codes

Random Network Coding

Network nodes independently and randomly select linear mappings from inputs links onto outputs links over some field.

Network Codes to Subspace Codes

Random Network Coding

Network nodes independently and randomly select linear mappings from inputs links onto outputs links over some field.

T. Ho, M. Medard, R. Kötter, D. R. Karger, M. Effros, J. Shi, B. Leong 2006

Network Codes to Subspace Codes

Network Codes to Subspace Codes

R. Kötter, and F. Kschischang, 2008

Network Codes to Subspace Codes

The Operator Channel

R. Kötter, and F. Kschischang, 2008

Network Codes to Subspace Codes

The Operator Channel

Subspace codes for error-correction in random network coding.

R. Kötter, and F. Kschischang, 2008

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Lifted Rank-Metric Codes

Network Codes to Subspace Codes

Lifted Rank-Metric Codes

Large constant dimension codes can be constructed by lifting rank-metric codes, especially maximum rank distance (MRD) codes.

Network Codes to Subspace Codes

Lifted Rank-Metric Codes

Large constant dimension codes can be constructed by lifting rank-metric codes, especially maximum rank distance (MRD) codes.

D. Silva, F. Kschischang, R. Kötter 2008

Network Codes to Subspace Codes

Network Codes to Subspace Codes

Metrics for Error-Correcting Network Codes

Network Codes to Subspace Codes

Metrics for Error-Correcting Network Codes

Which metric to use: rank distance, subspace distance, or injection distance.

Network Codes to Subspace Codes

Metrics for Error-Correcting Network Codes

Which metric to use: rank distance, subspace distance, or injection distance.

D. Silva, F. Kschischang 2009

Codes and Designs Over GF(q)

Codes and Designs Over GF(q)

Error-correcting codes in the projective space

Codes and Designs Over GF(q)

Error-correcting codes in the projective space

Basic bounds, linear programming, cyclic codes, perfect codes.

Codes and Designs Over GF(q)

Error-correcting codes in the projective space

Basic bounds, linear programming, cyclic codes, perfect codes.

Constant dimension codes and general subspace codes.

Codes and Designs Over GF(q)

Error-correcting codes in the projective space

Basic bounds, linear programming, cyclic codes, perfect codes.

Constant dimension codes and general subspace codes.

T. E. and A. Vardy 2008, 2011

Codes and Designs Over GF(q)

Codes and Designs Over GF(q)

Covering Designs in the Grassmann space

Codes and Designs Over GF(q)

Covering Designs in the Grassmann space

Basic bounds and constructions for covering designs over GF(q).

Codes and Designs Over GF(q)

Covering Designs in the Grassmann space

Basic bounds and constructions for covering designs over GF(q).

T. E. and A. Vardy 2011

Codes and Designs Over GF(q)

Subspace Codes via Ferrers Diagram and Rank-Metric Codes

Codes and Designs Over GF(q)

Subspace Codes via Ferrers Diagram and Rank-Metric Codes

Representation of subspaces, Ferrers diagram rank-metric codes, punctured codes.

Codes and Designs Over GF(q)

Subspace Codes via Ferrers Diagram and Rank-Metric Codes

Representation of subspaces, Ferrers diagram rank-metric codes, punctured codes.

T. E. and N. Silberstein 2009

Codes and Designs Over GF(q)

Codes based on Lifted MRD Codes

Codes and Designs Over GF(q)

Codes based on Lifted MRD Codes

The lifted MRD codes are viewed as designs, bounds and constructions for codes which contain the related lifted MRD code.

Codes and Designs Over GF(q)

Codes based on Lifted MRD Codes

The lifted MRD codes are viewed as designs, bounds and constructions for codes which contain the related lifted MRD code.

T. E. and N. Silberstein 2011, 2013

Codes and Designs Over GF(q)

Codes and Designs Over GF(q)

Cyclic Orbit Codes

Codes and Designs Over GF(q)

Cyclic Orbit Codes

Properties of Grassmannian codes which are defined as orbits of a subgroup of the general linear group.

Codes and Designs Over GF(q)

Cyclic Orbit Codes

Properties of Grassmannian codes which are defined as orbits of a subgroup of the general linear group.

A.-L. Trautmann, F. Manganiello, M. Braun, J. Rosenthal 2013

Codes and Designs Over GF(q)

Codes and Designs Over GF(q)

Covering Codes

Codes and Designs Over GF(q)

Covering Codes

New constructions (upper bounds), mainly ones based on lifted MRD codes.

Codes and Designs Over GF(q)

Covering Codes

New constructions (upper bounds), mainly ones based on lifted MRD codes.

T. E. 2014

The Grassmannian

The Grassmannian

$\mathbb{F}_q^n$ - vector space of dimension n over $\mathbb{F}_q$ $(= \mathbf{GF}(q)$).

The Grassmannian

$\mathbb{F}_q^n$ - vector space of dimension n over $\mathbb{F}_q$ $(= \mathbf{GF}(q)$).

$G_q(n,k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ (the Grassmannian).

The Grassmannian

$\mathbb{F}_q^n$ - vector space of dimension n over $\mathbb{F}_q$ $(= \mathbf{GF}(q)\ )$.

$G_q(n,k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ (the Grassmannian).

Gaussian coefficients (q-binomial coefficient)

The Grassmannian

$\mathbb{F}_q^n$ - vector space of dimension n over $\mathbb{F}_q$ $(= \mathbf{GF}(q)\ )$.

$G_q(n,k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ (the Grassmannian).

Gaussian coefficients (q-binomial coefficient)

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

The Grassmannian

$\mathbb{F}_q^n$ - vector space of dimension n over $\mathbb{F}_q$ $(= \mathbf{GF}(q)$ $)$.

$G_q(n,k)$ is the set of all k-dimensional subspaces of $\mathbb{F}_q^n$ (the Grassmannian).

Gaussian coefficients (q-binomial coefficient)

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

$$|G_q(n,k)| = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

q-Steiner Systems

q-Steiner Systems

A q-Steiner system $S(t,k,n)_q$ is a pair (N,B), where N is an n-dimensional space over $\mathbb{F}_q$ and B is set of k-dimensional subspaces (called blocks) of N such that each t-dimensional subspace of N is contained in exactly one block of B.

q-Steiner Systems

A q-Steiner system $S(t,k,n)_q$ is a pair (N,B), where N is an n-dimensional space over $\mathbb{F}_q$ and B is set of k-dimensional subspaces (called blocks) of N such that each t-dimensional subspace of N is contained in exactly one block of B.

$$\left|S(t,k,n)_q\right| = {\begin{bmatrix} n \\ t \end{bmatrix}_q} \Big/ {\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

Codes and Designs Over GF(q)

Codes and Designs Over GF(q)

Algebraic, Combinatorics, and Applications, Thurnau, Germany 2010

Codes and Designs Over GF(q)

Algebraic, Combinatorics, and Applications, Thurnau, Germany 2010

Castle Meeting on Coding Theory and Applications, Cardona, Spain 2011

Asymptotic Behavior

Asymptotic Behavior

$A(n) \sim B(n)$ if $\lim {}^{A(n)}/_{B(n)} = 1$ as $n \to \infty$.

Asymptotic Behavior

Theorem

$A(n) \sim B(n)$ if $\lim {}^{A(n)}/_{B(n)} = 1$ as $n \to \infty$.

Asymptotic Behavior

$A(n) \sim B(n)$ if $\lim {}^{A(n)}/_{B(n)} = 1$ as $n \to \infty$.

Theorem

If q, k, and t are fixed integers with $0 \leq t \leq k$, q a prime power, then the size $P(t,k,n)$ (the largest size of a set with k–subspaces (blocks) of an n-space N such that each t-subspace of N appears in exactly one block) satisfies

$$P(t,k,n) \sim {}^{\begin{bmatrix} n \\ t \end{bmatrix}_q}\Big/_{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

as $n \to \infty$.

Asymptotic Behavior

$A(n) \sim B(n)$ if $\lim {}^{A(n)}/_{B(n)} = 1$ as $n \to \infty$.

Theorem

If q, k, and t are fixed integers with $0 \le t \le k$, q a prime power, then the size $P(t,k,n)$ (the largest size of a set with k–subspaces (blocks) of an n-space N such that each t-subspace of N appears in exactly one block) satisfies

$$P(t,k,n) \sim {}^{\begin{bmatrix} n \\ t \end{bmatrix}_q} \Big/ {}_{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

as $n \to \infty$.

S.Blackburn, T. E. 2012

Asymptotic Behavior

$A(n) \sim B(n)$ if $\lim {}^{A(n)}/_{B(n)} = 1$ as $n \to \infty$.

Theorem

If q, k, and t are fixed integers with $0 \leq t \leq k$, q a prime power, then the size $P(t,k,n)$ (the largest size of a set with k-subspaces (blocks) of an n-space N such that each t-subspace of N appears in exactly one block) satisfies

$$P(t,k,n) \sim {}^{\begin{bmatrix} n \\ t \end{bmatrix}_q} \Big/ {}_{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

as $n \to \infty$.

S.Blackburn, T. E. 2012

Same result for covering.

Spreads

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

spread

Spreads

Theorem A q-Steiner system $S(1, k, n)_q$ exists if and only if k divides n.

spread

Proof

Spreads

Theorem A q-Steiner system $S(1, k, n)_q$ exists if and only if k divides n.

spread

Proof $n = sk$

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

spread

Proof $n = sk$

α primitive in $GF(q^n)$

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

spread

Proof $n = sk$

α primitive in $GF(q^n)$

$$r = \frac{q^n - 1}{q^k - 1}$$

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

spread

Proof

$n = sk$

α primitive in $GF(q^n)$

$$r = \frac{q^n - 1}{q^k - 1}$$

α^r is primitive in the subfield $GF(q^k)$ of $GF(q^n)$

Spreads

Theorem A q-Steiner system $S(1,k,n)_q$ exists if and only if k divides n.

spread

Proof

$n = sk$

α primitive in $GF(q^n)$

$$r = \frac{q^n - 1}{q^k - 1}$$

α^r is primitive in the subfield $GF(q^k)$ of $GF(q^n)$

$\{0, \alpha^i, \alpha^{i+r}, \alpha^{i+2r}, \ldots, \alpha^{i+(2^k-2)r}\}, 0 \le i \le r-1,$ are closed under addition in $GF(q^n)$ $\Rightarrow$ subspaces $\Rightarrow$ $S(1,k,n)_q$

Four Years of the COST Action

Four Years of the COST Action

$S(2, 3, 13)_2$

Four Years of the COST Action

$S(2, 3, 13)_2$

Ascona 2012

Four Years of the COST Action

$S(2,3,13)_2$

Ascona 2012





M. Braun, T. E., P. Östergård, A. Vardy, A. Wassermann, 2013

Four Years of the COST Action

$S(2,3,13)_2$

Ascona 2012

Bergen 2013

M. Braun, T. E., P. Östergård, A. Vardy, A. Wassermann, 2013

Four Years of the COST Action

Four Years of the COST Action

$\boldsymbol{S(2,3,13)_2}$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

Frobenius map

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

Frobenius map

$F(V) = \{0, \alpha^{2 \cdot i_1}, \alpha^{2 \cdot i_2}, \alpha^{2 \cdot i_3}, \alpha^{2 \cdot i_4}, \alpha^{2 \cdot i_5}, \alpha^{2 \cdot i_6}, \alpha^{2 \cdot i_7}\}$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

+

Frobenius map

$F(V) = \{0, \alpha^{2\cdot i_1}, \alpha^{2\cdot i_2}, \alpha^{2\cdot i_3}, \alpha^{2\cdot i_4}, \alpha^{2\cdot i_5}, \alpha^{2\cdot i_6}, \alpha^{2\cdot i_7}\}$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

$+$

Frobenius map

$F(V) = \{0, \alpha^{2\cdot i_1}, \alpha^{2\cdot i_2}, \alpha^{2\cdot i_3}, \alpha^{2\cdot i_4}, \alpha^{2\cdot i_5}, \alpha^{2\cdot i_6}, \alpha^{2\cdot i_7}\}$

$=$

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

$+$

Frobenius map

$F(V) = \{0, \alpha^{2\cdot i_1}, \alpha^{2\cdot i_2}, \alpha^{2\cdot i_3}, \alpha^{2\cdot i_4}, \alpha^{2\cdot i_5}, \alpha^{2\cdot i_6}, \alpha^{2\cdot i_7}\}$

$=$

normalizer of Singer subgroup automoprphism

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

+

Frobenius map

$F(V) = \{0, \alpha^{2\cdot i_1}, \alpha^{2\cdot i_2}, \alpha^{2\cdot i_3}, \alpha^{2\cdot i_4}, \alpha^{2\cdot i_5}, \alpha^{2\cdot i_6}, \alpha^{2\cdot i_7}\}$

=

normalizer of Singer subgroup automoprphism

15 representatives

Four Years of the COST Action

$S(2,3,13)_2$

α primitive in $GF(2^{13})$

$V = \{0, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3}, \alpha^{i_4}, \alpha^{i_5}, \alpha^{i_6}, \alpha^{i_7}\}$

cyclic shift

$\alpha V = \{0, \alpha^{i_1+1}, \alpha^{i_2+1}, \alpha^{i_3+1}, \alpha^{i_4+1}, \alpha^{i_5+1}, \alpha^{i_6+1}, \alpha^{i_7+1}\}$

+

Frobenius map

$F(V) = \{0, \alpha^{2\cdot i_1}, \alpha^{2\cdot i_2}, \alpha^{2\cdot i_3}, \alpha^{2\cdot i_4}, \alpha^{2\cdot i_5}, \alpha^{2\cdot i_6}, \alpha^{2\cdot i_7}\}$

=

normalizer of Singer subgroup automoprphism

15 representatives

1 597 245
3–dimensional subspaces

Four Years of the COST Action

Designs Over Vector Spaces

Four Years of the COST Action

Designs Over Vector Spaces

Ghent 2013

Four Years of the COST Action

Designs Over Vector Spaces

Ghent 2013

Derived and residual subspace designs.

Four Years of the COST Action

Designs Over Vector Spaces

Ghent 2013

Derived and residual subspace designs.

M. Kiermaier and R. Laue 2015

Four Years of the COST Action

Four Years of the COST Action

Fano Plane

Four Years of the COST Action

Fano Plane

Ghent 2013

Four Years of the COST Action

Fano Plane

Ghent 2013

If a 2-Fano plane exists it does not have a large automorphism group.

Four Years of the COST Action

Fano Plane

Ghent 2013

If a 2-Fano plane exists it does not have a large automorphism group.

M. Braun, M. Kiermaier, N. Nakić 2015

Four Years of the COST Action

Fano Plane

Ghent 2013

If a 2-Fano plane exists it does not have a large automorphism group.

M. Braun, M. Kiermaier, N. Nakić 2015

Istanbul 2015

Four Years of the COST Action

Fano Plane

Ghent 2013

If a 2-Fano plane exists it does not have a large automorphism group.

M. Braun, M. Kiermaier, N. Nakić 2015

The structure of the q-Fano plane if exists.

Istanbul 2015

Four Years of the COST Action

Fano Plane

Ghent 2013

If a 2-Fano plane exists it does not have a large automorphism group.

M. Braun, M. Kiermaier, N. Nakić 2015

The structure of the q-Fano plane if exists.

Istanbul 2015

T. E. 2015

Four Years of the COST Action

Four Years of the COST Action

Rank-Metric Codes

Four Years of the COST Action

Rank-Metric Codes

Bordeaux 2014

Four Years of the COST Action

Rank-Metric Codes

Bordeux 2014

Palmela 2014

Four Years of the COST Action

Rank-Metric Codes

Bordeux 2014

Palmela 2014

Constructions of Ferrers diagram rank-metric codes and a related Anticode bound.

Four Years of the COST Action

Rank-Metric Codes

Bordeux 2014

Palmela 2014

Constructions of Ferrers diagram rank-metric codes and a related Anticode bound.

T. E., E. Gorla, A. Ravagnani, A. Wachter-Zeh 2014

Four Years of the COST Action

Four Years of the COST Action

New Codes

Four Years of the COST Action

New Codes

Bordeux 2014

Four Years of the COST Action

New Codes

Bordeux 2014

ALCOMA 2015

Four Years of the COST Action

New Codes

Bordeaux 2014

ALCOMA 2015

Large constant dimension codes of length 6 and length 8 over any given finite field.

Four Years of the COST Action

New Codes

Bordeaux 2014 | **ALCOMA 2015**

Large constant dimension codes of length 6 and length 8 over any given finite field.

A. Cossidente, F. Pavese 2014
A. Cossidente, F. Pavese 2015

Four Years of the COST Action

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Subspace polynomial, cyclic mapping, Frobenius mapping, relatively large cyclic subspace codes.

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Subspace polynomial, cyclic mapping, Frobenius mapping, relatively large cyclic subspace codes.

E. Ben Sasson, T. E., A. Gabizon, N. Raviv 2015

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Subspace polynomial, cyclic mapping, Frobenius mapping, relatively large cyclic subspace codes.

E. Ben Sasson, T. E., A. Gabizon, N. Raviv 2015

Istanbul 2015

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Subspace polynomial, cyclic mapping, Frobenius mapping, relatively large cyclic subspace codes.

E. Ben Sasson, T. E., A. Gabizon, N. Raviv 2015

New bounds

Istanbul 2015

Four Years of the COST Action

Subspace Polynomial and Cyclic Subspace Codes

Palmela 2014

Subspace polynomial, cyclic mapping, Frobenius mapping, relatively large cyclic subspace codes.

E. Ben Sasson, T. E., A. Gabizon, N. Raviv 2015

New bounds

Istanbul 2015

K. Otal and F. Özbudak 2015

Four Years of the COST Action

Four Years of the COST Action

Equidistant Codes

Four Years of the COST Action

Equidistant Codes

Bordeaux 2014

Four Years of the COST Action

Equidistant Codes

Theory for equidistant Grassmannian codes and rank-metric codes

Bordeux 2014

Four Years of the COST Action

Equidistant Codes

Theory for equidistant Grassmannian codes and rank-metric codes

T. E. and N. Raviv 2015

Bordeux 2014

Four Years of the COST Action

Equidistant Codes

Theory for equidistant Grassmannian codes and rank-metric codes

T. E. and N. Raviv 2015

Bordeux 2014

Istanbul 2015

Four Years of the COST Action

Equidistant Codes

Theory for equidistant Grassmannian codes and rank-metric codes

T. E. and N. Raviv 2015

Bordeaux 2014

New bounds

Istanbul 2015

Four Years of the COST Action

Equidistant Codes

Theory for equidistant Grassmannian codes and rank-metric codes

T. E. and N. Raviv 2015

Bordeaux 2014

New bounds

R.D. Barrolleta, D. Bartoli, M. De Boeck, E. Suárez Canedo, L. Storme, A.-E. Riet, P. Vandendriessche

Istanbul 2015

Four Years of the COST Action

Four Years of the COST Action

Vector Network Coding Outperforms Scalar Network Coding

Four Years of the COST Action

Vector Network Coding Outperforms Scalar Network Coding

Multicast network which is solved with vectors of length t over $\mathbb{F}_q$ and can be solved with scalar linear network coding only over a field of order $q^{(\ell-1)t^2/\ell}$, where 2ℓ is the number of messages.

Four Years of the COST Action

Vector Network Coding Outperforms Scalar Network Coding

Multicast network which is solved with vectors of length t over $\mathbb{F}_q$ and can be solved with scalar linear network coding only over a field of order $q^{(\ell-1)t^2/\ell}$, where 2ℓ is the number of messages.

T. E. and A. Wachter-Zeh 2016

Vector Network Coding Outperforms Scalar Network Coding

Multicast network which is solved with vectors of length t over $\mathbb{F}_q$ and can be solved with scalar linear network coding only over a field of order $q^{(\ell-1)t^2/\ell}$, where 2ℓ is the number of messages.

T. E. and A. Wachter-Zeh 2016

Constructions and bounds are based on rank-metric codes and subspace codes.

Open Problems, Future Reseach

Open Problems, Future Reseach

Bounds on the Alphabet size for a given number h of messages and N receivers.

Open Problems, Future Reseach

Bounds on the Alphabet size for a given number h of messages and N receivers.

Does there exist a multicast network with two messages in which vector network coding outperforms scalar network coding?

Open Problems, Future Reseach

Bounds on the Alphabet size for a given number h of messages and N receivers.

Does there exist a multicast network with two messages in which vector network coding outperforms scalar network coding?

Is there a multicast network in which exactly h edge disjoint paths are used to each receiver, and vector network coding outperforms scalar network coding.

Open Problems, Future Reseach

Open Problems, Future Reseach

Find new q-Steiner systems.

Open Problems, Future Reseach

Find new q-Steiner systems.

Prove the nonexistence of some currently possible q-Steiner systems.

Open Problems, Future Reseach

Find new q-Steiner systems.

Prove the nonexistence of some currently possible q-Steiner systems.

Does there exists q-Steiner system $S(2,3,7)_q$ (q-Fano plane).

Open Problems, Future Reseach

Find new q-Steiner systems.

Prove the nonexistence of some currently possible q-Steiner systems.

Does there exists q-Steiner system $S(2,3,7)_q$ (q-Fano plane).

Improve the bounds on the sizes of partial spreads.

Open Problems, Future Reseach

Open Problems, Future Reseach

Constructions for large cyclic codes.

Open Problems, Future Reseach

Constructions for large cyclic codes.

New constructions and bounds on subspaces codes which are not constant dimension codes.

Open Problems, Future Reseach

Constructions for large cyclic codes.

New constructions and bounds on subspaces codes which are not constant dimension codes.

Prove that current upper bounds are asymptotically optimal for new parameters.

Open Problems, Future Reseach

Constructions for large cyclic codes.

New constructions and bounds on subspaces codes which are not constant dimension codes.

Prove that current upper bounds are asymptotically optimal for new parameters.

Find new applications for subspace codes.

My Former Students, Postdocs

Moshe Schwartz, Natalia Silberstein, Netanel Raviv, Antonia Wachter-Zeh

THANK YOU