# ON THE STRUCTURE OF Q-STEINER SYSTEMS

Tuvi Etzion

Computer Science Department

TECHNION
Israel Institute of Technology

Istanbul, Turkey, November 4, 2015

# Outline

$q$-Steiner Systems

Punctured $q$-Steiner Systems

The $q$-Fano Plane

Open Problems and Future Research

# 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

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 $B$.

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

# $q$-Steiner Systems

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

**Theorem**

If an $S(t,k,n)_q$ exists then an $S(t-1,k-1,n-1)_q$ exists.

**Corollary**

A necessary condition for the existence of a Steiner system $S(t,k,n)_q$ is that for each $i$, $0 \le i \le t-1$, the numbers $\begin{bmatrix} n-i \\ t-i \end{bmatrix}_q \Big/ \begin{bmatrix} k-i \\ t-i \end{bmatrix}_q$ are integers.

# Spreads

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

spread

**Proof** $n = sk$

$\alpha$ primitive in $GF(q^n)$

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

$\alpha^r$ 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 $\Rightarrow S(1,k,n)_q$

# $q$-Steiner Systems

$S(2,3,13)_2$

$\alpha$ 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

Braun, E., Östergård, Vardy, Wassermann, 2013

# $q$-Steiner Systems

A $q$-packing system $P(t,k,n)_q$ 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 at most one block of $B$.

$$|P(t,k,n)_q| \leq {\begin{bmatrix} n \\ t \end{bmatrix}_q} \Big/ {\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

# 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

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

as $n \to \infty$.

**Blackburn, E., 2012**

# Punctured $q$-Steiner Systems

Given an $n \times m$ array $A$, the punctured array $A'$ is an $n \times (m-1)$ array obtained from $A$ by deleting one of the columns of $A$.

For a subspace $X \in G_q(n,k)$ the punctured subspace $X'$ by the $i$th coordinate of $X$ is the subspace obtained by deleting the $i$th coordinate from all the vectors of $X$.

**Lemma** A punctured $k$–subspace is either a $k$-subspace or a $(k-1)$-subspace.

# Punctured $q$-Steiner Systems

## Representation of a subspace

A $k$-subspace $X$ of $\mathbb{F}_q^n$ is represented by a $(q^k - 1) \times n$ matrix which contains the $q^k - 1$ nonzero vectors of $X$. Each nonzero vector of $X$ is a row in this matrix.

# Punctured $q$-Steiner Systems

**Lemma** A punctured $k$–subspace is either a $k$-subspace or a $(k-1)$-subspace.

If the punctured $k$-subspace $X$ contains the unity vector with a *one* in the $i$th coordinate then $X'$ is a $(k-1)$-subspace. Otherwise, $X'$ is a $k$-subspace.

For a set of subspaces $\mathbb{S}$, the punctured set $\mathbb{S}'$ is defined as $\mathbb{S}' = \{X' : X \in \mathbb{S}\}$.

Unless otherwise said, the last coordinate is the punctured one.

# Punctured $q$-Steiner Systems

A $t$-subspace $X$ of $\mathbb{F}_q^m$ is extended to a $t'$-subspace $Y$ of $\mathbb{F}_q^{m'}$, where $t' \geq t$, $m' > m$, $m' - m \geq t' - t$ if $X$ is the subspace obtained from $Y$ by puncturing $m' - m$ times.

**Lemma** If $X$ is a $t$-subspace of $\mathbb{F}_q^m$ then it can be extended in exactly $q^t$ distinct ways to a $t$-subspace of $\mathbb{F}_q^{m+1}$.

**Lemma** If $X$ is a $t$-subspace of $\mathbb{F}_q^m$ then it can be extended in exactly one way to a $(t+1)$-subspace of $\mathbb{F}_q^{m+1}$.

# Punctured $q$-Steiner Systems

## $p$–punctured $q$-Steiner system

$$S(t, k, n; m)\,,\, m = n - p$$

A system $\mathbb{S}$ of subspaces of $\mathbb{F}_q^m$, in which each $t$-subspace of $\mathbb{F}_q^n$ can be obtained exactly once by extending $p$ times all the subspaces of $\mathbb{S}$. This is done in parallel for all identical subspaces of $\mathbb{S}$.

# Punctured $q$-Steiner Systems

**Theorem**

If $\mathbb{S}$ is a $q$-Steiner system $S(t,k,n)_q$ then the punctured system $\mathbb{S}'$ has ${\begin{bmatrix} n-1 \\ t-1 \end{bmatrix}_q} \Big/ {\begin{bmatrix} k-1 \\ t-1 \end{bmatrix}_q}$ distinct $(k-1)$-subspaces which form a $q$-Steiner system $S(t-1,k-1,n-1)_q$, $\hat{\mathbb{S}}$. Each $t$-subspace which is contained in a $(k-1)$-subspace of $\hat{\mathbb{S}}$ is not contained in the $k$-subspaces of $\mathbb{S}'$. Each $t$-subspace which is not contained in a $(k-1)$-subspace of $\hat{\mathbb{S}}$, appears exactly $q^t$ times in the other $k$-subspaces of $\mathbb{S}'$.

# $S(t,k,n;m)_q$-Necessary Conditions

## System of Equations

Variables – one for each possible $p$–punctured $k$–subspaces of $S(t,k,n)_q$.

Equations – one for each possible $p$–punctured $t$-subspace of $\mathbb{F}_q^n$.

# $S(t,k,n;m)_q$-Necessary Conditions

## Dimension of subspaces to be covered

In a $p$-punctured $q$-Steiner system $S(t,k,n;m)_q$, the $t$-subspaces which should be covered by $k$-subspaces, were punctured and reduced to $s$-subspaces, where $\max\{0, t-p\} \leq s \leq \min\{t, m\}$.

## Dimension of subspaces to cover an $s$-subspace

In a $p$-punctured $q$-Steiner system $S(t,k,n;m)_q$, an $s$-subspaces which was $p$ -punctured from a $t$-subspace, is covered by an $r$-subspace, where $\max\{s, k-p\} \leq r \leq \min\{k-t+s, m\}$.

# $S(t,k,n;m)_q$-Necessary Conditions

$N_{(s,m),(t,n)}$ - the number of $t$-subspaces in $\mathbb{F}_q^n$ which are formed by extending a given $s$-subspace $X$ of $\mathbb{F}_q^m$.

$$N_{(s,m),(t,n)} = q^{s(n-m-t+s)} \begin{bmatrix} n-m \\ t-s \end{bmatrix}_q$$

$C_{(s,t),(r,k)}$ - number of $t$-subspaces in $\mathbb{F}_q^n$ extended from a given $s$-subspace $X$ of $\mathbb{F}_q^m$, contained in an $r$-subspace $Y \supseteq X$ of $\mathbb{F}_q^m$, which are contained in the $k$-subspace of $\mathbb{F}_q^n$ extended from $Y$.

$$C_{(s,t),(r,k)} = q^{s(k-r-t+s)} \begin{bmatrix} k-r \\ t-s \end{bmatrix}_q$$

# $S(t,k,n;m)_q$-Necessary Conditions

$D_{s,r,m}$ - number of $r$-subspaces in $\mathbb{F}_q^m$ which contain a given $s$-subspace $X$ of $\mathbb{F}_q^m$.

$$D_{s,r,m} = \begin{bmatrix} m-s \\ r-s \end{bmatrix}_q$$

Uniform design - each $r$-subspace of $\mathbb{F}_q^m$ appears in $S(t,k,n,;m)_q$ with the same amount.

$X_{r,m}$ - number of $r$-subspaces in a uniform $S(t,k,n;m)_q$ for any given $r$-subspace of $\mathbb{F}_q^m$.

$$\max\{0, t-p\} \le s \le \min\{t,m\}$$

$$N_{(s,m),(t,n)} = \sum_{max\{s,k-p\}}^{min\{k-t+s,m\}} D_{s,r,m} \cdot C_{(s,t)(r,k)} \cdot X_{r,m}$$

# Punctured $q$-Steiner Systems

$$S(3,4,8;4)_q$$

**Uniform solution**

$$X_{0,4} = 1, X_{1,4} = 0, \quad X_{2,4} = q^2(q^2+1)$$

$$X_{3,4} = q^4(q^4-1), \quad X_{4,4} = q^{12} - q^{11} + q^7$$

# Punctured $q$-Steiner Systems

$S(4,5,11;6)_q$

**Uniform solution**

$X_{0,6} = 1, X_{1,6} = 0, \quad X_{2,6} = q^2(q^2+1)$

$X_{3,6} = q^9 + q^7 - q^4, \quad X_{4,6} = q^{14} - q^9 + q^7$

$X_{5,6} = (q^{18} + q^{11})(q-1)$

# Punctured $q$-Steiner Systems

$$S(5,6,12;6)_q$$

**Uniform solution**

$$X_{0,6}=1,\ X_{1,6}=0,\quad X_{2,6}=q^2(q^4+q^2+1)$$

$$X_{3,6}=q^4(q^8+q^6+q^5-1),\ X_{4,6}=q^7(q^{11}+q^9+q^7-q^6+1)$$

$$X_{5,6}=q^{11}(q^{13}-q^7+q^6-1),\ X_{6,6}=q^{16}(q^{14}-q^{13}+q^7-q^6+1)$$

# Punctured $q$-Steiner Systems

$$S(3,4,2k;k)_q$$
$$k \equiv 2 \text{ or } 4 \pmod 6$$

**Uniform solution**

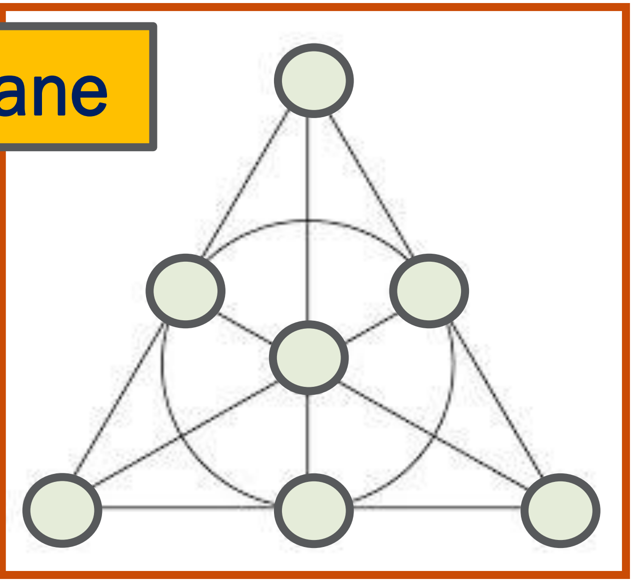
$$X_{0,k} = {\begin{bmatrix} k \\ 3 \end{bmatrix}_q} \Big/ {\begin{bmatrix} 4 \\ 3 \end{bmatrix}_q}, \quad X_{1,k} = 0, \quad X_{2,k} = q^{k-2}\frac{q^k - 1}{q^2 - 1}$$

$$X_{3,k} = q^k(q^k - 1), \quad X_{4,k} = \frac{(q^{3k} - q^{2k+3} + q^{k+3})(q-1)}{q^{k-3} - 1}$$

# $q$-Fano Plane

Steiner system $S(2,3,7)$

Fano Plane



What about $S(2,3,7)_q$?

$S(2,3,7)_q$ is a $q$-Fano plane

# $q$-Fano Plane

$S(2,3,7;4)_q$

**Uniform solution**

$X_{0,4} = 1, X_{1,4} = 0, X_{2,4} = q^2, X_{3,4} = q^4(q-1)$

# $q$-Fano Plane

## Column operations

1. Exchange of two columns.
2. Replace a column with a linear combination which consists of the replaced column with other columns.

## Theorem

If $\mathbb{S}$ is a $q$-Steiner system $\boldsymbol{S(t,k,n)_q}$ then any system obtained from $\mathbb{S}$ by the same column operations on all its $\boldsymbol{k}$-subspaces is also a $q$-Steiner system $\boldsymbol{S(t,k,n)_q}$.

# $q$-Fano Plane

Let $\mathbb{S}$ be a $q$-Fano Plane.

$Z_1$ - the unique $3$-subspace of $\mathbb{F}_q^7$ which starts with four all-zero columns.
$Z_2$ - the unique $3$-subspace of $\mathbb{F}_q^7$ which ends with four all-zero columns.

**Lemma** Without loss of generality we can assume that $Z_1, Z_2 \in \mathbb{S}$.

**Proof** Using column operations on a $3$-subspace whose first three columns have rank 3.

# $q$-Fano Plane

$\mathbb{S}$ – $S(2,3,7;4)_q$

$X_{0,4} = 1, X_{1,4} = 0$,
$X_{2,4} = q^2, X_{3,4} = q^4(q-1)$

$q^2 + q + 1$ 1-subspaces with four zeroes in specified positions.

$\mathbb{A}$ - set of 3-subspaces of $\mathbb{S}$ which form the $q^2(q^2+1)(q^2+q+1)$ 2-subspaces of $S(2,3,7;4)_q$ obtained by puncturing the last three columns.

$\mathbb{B}$ - set of 3-subspaces of $\mathbb{S}$ which form the $q^2(q^2+1)(q^2+q+1)$ 2-subspaces of $S(2,3,7;4)_q$ obtained by puncturing the first three columns.

$|\mathbb{A}| = |\mathbb{B}| = q^2(q^2+1)(q^2+q+1)$ $\quad |\mathbb{A} \cap \mathbb{B}| = (q^2+q+1)^2$

# $q$-Fano Plane

$\mathbb{A}$ - set of $\mathbf{3}$-subspaces of $\mathbb{S}$ which form the $q^2(q^2+1)(q^2+q+1)$ $\mathbf{2}$-subspaces of $S(2,3,7;4)_q$ obtained by puncturing the last three columns.

$\mathbb{B}$ - set of $\mathbf{3}$-subspaces of $\mathbb{S}$ which form the $q^2(q^2+1)(q^2+q+1)$ $\mathbf{2}$-subspaces of $S(2,3,7;4)_q$ obtained by puncturing the first three columns.

$$|\mathbb{A}| = |\mathbb{B}| = q^2(q^2+1)(q^2+q+1) \qquad |\mathbb{A} \cap \mathbb{B}| = \left(q^2+q+1\right)^2$$

$$|\mathbb{A} \setminus \mathbb{B}| = |\mathbb{B} \setminus \mathbb{A}| = (q^2+q+1)(q^4-q-1)$$

# $q$-Fano Plane

$S(2,3,7;5)_q$

Start with uniform solution for $S(2,3,7;4)_q$

$X_{0,4} = 1$, $X_{1,4} = 0$, $X_{2,4} = q^2$, $X_{3,4} = q^4(q-1)$

# $q$-Fano Plane

$\mathbb{S} \; - \; S(2,3,7;4)_q$

$X_{0,4} = 1$, $X_{1,4} = 0$ , $X_{2,4} = q^2$, $X_{3,4} = q^4(q-1)$

$\mathbb{T} \quad - \quad S(2,3,7;5)_q$

A $3$-subspace of $\mathbb{F}_q^4$ can be extended in $q^3$ different ways to a $3$-subspace of $\mathbb{F}_q^5$.

Each $3$-subspace of $\mathbb{F}_q^5$ extended from a $3$-subspace of $\mathbb{F}_q^4$ appears $q(q-1)$ times in $\mathbb{T}$.

# $q$-Fano Plane

$\mathbb{S} - S(2,3,7;4)_q$

$X_{0,4} = 1, X_{1,4} = 0, X_{2,4} = q^2, X_{3,4} = q^4(q-1)$

$\mathbb{T} - S(2,3,7;5)_q$

There are $(q^2+1)(q^2+q+1)$ $2$-subspaces in $\mathbb{F}_q^4$, each one appears $q^2$ times in $\mathbb{S}$.

$q^2(q^2+1)q^2$ should be extended to $3$-subspaces.

$q^2(q^2+1)(q+1)$ should be extended to $2$-subspaces.

# $q$-Fano Plane

$\mathbb{S}$ – $S(2,3,7;4)_q$

$X_{0,4} = 1, X_{1,4} = 0, X_{2,4} = q^2, X_{3,4} = q^4(q-1)$

$\mathbb{T}$ – $S(2,3,7;5)_q$

The $(q^2+1)(q^2+q+1)$ 2-subspaces in $\mathbb{F}_q^4$ are partitioned into $q^2+q+1$ spreads, each one of size $q^2+1$.

Beutelspacher 1974
Baker 1976

**Two sets**

$A$ - $q^2$ spreads.
$B$ - $q+1$ spreads.

# $q$-Fano Plane

$\mathbb{S}$ – $S(2,3,7;4)_q$

$X_{0,4} = 1, X_{1,4} = 0, X_{2,4} = q^2, X_{3,4} = q^4(q-1)$

$\mathbb{T}$ – $S(2,3,7;5)_q$

**Two sets**

$A$ - $q^2$ spreads.
$B$ - $q+1$ spreads.

2-subspace from $A$ is extended into a unique 3-subspace in $\mathbb{T}$.

Each $q^2$ copies of a 2-subspace from $B$ are extended into the $q^2$ possible 2-subspaces in $\mathbb{T}$.

# Recursive Construction

$k \equiv 1$ or $3 \pmod 6$

$p$-punctured $q$-Steiner system

$S\left(2, 3, k; \left\lfloor \frac{k+1}{3} \right\rfloor\right)_q$, $p = k - \left\lfloor \frac{k+1}{3} \right\rfloor$ .

# Recursive Construction

$$S(2,3,2k+1;k+1)_q$$

$k \equiv 1$ or $3 \pmod 6$

$\sum_{i=0}^{2} \begin{bmatrix} k+1 \\ i \end{bmatrix}_q$ equations

$\sum_{i=0}^{3} \begin{bmatrix} k+1 \\ i \end{bmatrix}_q$ variables

# Recursive Construction

$$S(2,3,2k+1;k+1)_q$$

$k \equiv 1$ or $3 \pmod 6$

Uniform solution

$$X_{0,k+1} = \begin{bmatrix} k \\ 2 \end{bmatrix}_q \Big/ \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q$$

$$X_{1,k+1} = 0,\ X_{2,k+1} = q^{k-1},\ X_{3,k+1} = q^{k+1}(q-1)$$

# Recursive Construction

$\mathbb{S}$ - $k$-punctured $q$-Steiner system $S(2,3,2k+1;k+1)_q$..

$\mathbb{T}$ - $p$-punctured $q$-Steiner system $S\left(2,3,2k+1;k+1+\left\lfloor\frac{k+1}{3}\right\rfloor\right)_q$,. $p = k - \left\lfloor\frac{k+1}{3}\right\rfloor$.

$r = \left\lfloor\frac{k+1}{3}\right\rfloor$ columns should be added to each subspace of $\mathbb{S}$ to obtain $\mathbb{T}$.

$S(2,3,k;r)_q$ exists.

# Recursive Construction

$r = \left\lfloor \frac{k+1}{3} \right\rfloor$ columns should be added to each subspace of $\mathbb{S}$ to obtain $\mathbb{T}$.

$\begin{bmatrix} k+1 \\ 3 \end{bmatrix}_q$ distinct $3$–subspaces in $\mathbb{S}$, each one appears $q^{k+1}(q-1)$ times in $\mathbb{S}$.

A $3$-subspace of $\mathbb{F}_q^m$ has $q^3$ distinct extension to a $3$-subspace in $\mathbb{F}_q^{m+1}$.

Each $3$-subspace of $\mathbb{F}_q^{k+1+r}$ extended from a $3$-subspace of $\mathbb{F}_q^{k+1}$ will appear in $\mathbb{T}$ $q^{k+1-3r}(q-1)$ times.

# Recursive Construction

$r = \left\lfloor \frac{k+1}{3} \right\rfloor$ columns should be added to each subspace of $\mathbb{S}$ to obtain $\mathbb{T}$.

The $\mathbf{0}$–subspace appears ${\left[{k \atop 2}\right]_q}\Big/{\left[{3 \atop 2}\right]_q}$ times in $\mathbb{S}$.

Recursive step

The ${\left[{k \atop 2}\right]_q}\Big/{\left[{3 \atop 2}\right]_q}$ subspaces of an $S(2,3,k;r)_q$ are appended to the $\mathbf{0}$-subspaces of $\mathbb{S}$.

# Recursive Construction

Large set (1-parallelism) of spreads in $G_q(k+1,2)$ - $\frac{q^k-1}{k-1}$ spreads of size $\frac{q^{k+1}-1}{q^2-1}$.

$q = 2$

$2^r$ sets

One set - $2^{k-r}-1$ spreads.

$2^r-1$ sets - each one $2^{k-r}$ spreads.

# Recursive Construction

$q = 2$

$2^r$ sets

One set - $2^{k-r} - 1$ spreads.

$2$-subspaces $\Rightarrow$ $2$-subspaces

$2^r - 1$ sets - each one $2^{k-r}$ spreads.

$2$-subspaces $\Rightarrow$ $3$-subspaces

# Open Problems

Find new $q$-Steiner systems.

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

Analyze the 1-punctured $q$-Steiner system $S(2,3,7;6)_q$.

Find new $p$-punctured $q$-Steiner systems.

# THANK YOU