Low density quasi-perfect linear codes, small complete caps and symmetric surfaces

Fernanda Pambianco

University of Perugia (Italy)

co-authors: D. Bartoli, H. Kaneta, S. Marcugini

ACCT 2014

Svetlogorsk (Kaliningrad region), Russia, September 7-13

OUTLINE

- INTRODUCTION: LINEAR CODES AND CAPS
- A PROBABILISTIC METHOD
- A NEW UPPER BOUND ON THE SMALLEST SIZE OF COMPLETE CAPS IN $PG(N,q)$ AND ON THE MINIMAL LENGTH OF QUASI-PERFECT LINEAR CODES
- THE FIRST AND SECOND MOST SYMMETRIC NONSINGULAR CUBIC SURFACES

Linear Codes

$\mathbb{F}_q$: *Galois field of q elements*

Definition

$$\boxed{\mathcal{C}: \textit{ linear code } [n, k, d]_q}$$

$$\mathcal{C} \subset \mathbb{F}_q^n \qquad \dim(\mathcal{C}) = k \qquad d = \min_{x \in \mathcal{C} \setminus \{0\}} w(x)$$

$G_{k \times n}$: generator matrix of $\mathcal{C}$

Definition

$$\mathcal{C}^\perp = \{y \in \mathbb{F}_q^n | y \cdot x = 0 \quad \forall\, x \in \mathcal{C}\}$$

$$\boxed{\mathcal{C}^\perp: \textit{ linear code } [n, n-k, d']_q}$$

$G_{(n-k) \times n}$: generator matrix of $\mathcal{C}^\perp$ and parity check matrix of $\mathcal{C}$

Coding Theory and Projective Geometry: Connection

$\mathcal{C}$: $[n, k, d]_q$ $d \geq 3$ linear code

$$G_{(n-k)\times n} = (A^1, A^2, \ldots, A^n) \text{ parity check matrix}$$

$$\downarrow \quad \downarrow \qquad \quad \downarrow$$

$$\{P_1, P_2, \ldots, P_n\}$$

set of points in $PG(n-k-1, q)$

Linear Codes: error correction

$[n, k, d]_q$ linear code

$$\left\lfloor \frac{d-1}{2} \right\rfloor\text{-error correcting}$$

Theorem (Singleton bound)

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

Definition (MDS code)

$$d = n - k + 1 \iff \textit{MDS code}$$

Covering codes

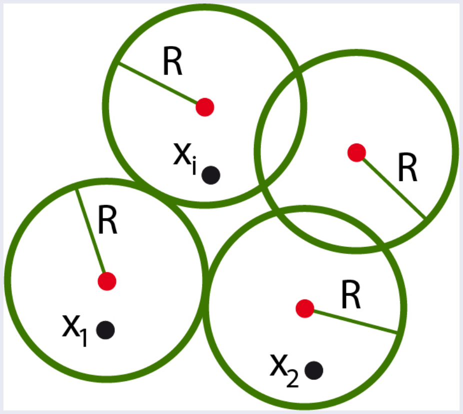
Definition

Covering code with covering radius R

$[n, k, d]_q R$ *linear code* $\mathcal{C}$

R covering radius

$$\forall x \in \mathbb{F}_q^n \implies d(x, \mathcal{C}) \leq R$$



Definition (Perfect code)

$$R(\mathcal{C}) = \left\lfloor \frac{d-1}{2} \right\rfloor \iff \mathcal{C} \text{ is } perfect$$

Covering Density

Definition (Covering Density)

$$\mu(\mathcal{C}) = \frac{1}{q^{n-k}} \sum_{i=0}^{R(\mathcal{C})} (q-1)^i \binom{n}{i}.$$

$$\boxed{\mu(\mathcal{C}) \geq 1}$$

$$\boxed{\mu(\mathcal{C}) = 1 \iff \mathcal{C} \text{ is perfect}}$$

Remark

Codes with the same codimension and covering radius

shortest ones $\Longrightarrow$ *best covering density*

Hamming codes and the Golay code are the only nontrivial examples of perfect codes

$$\Downarrow$$

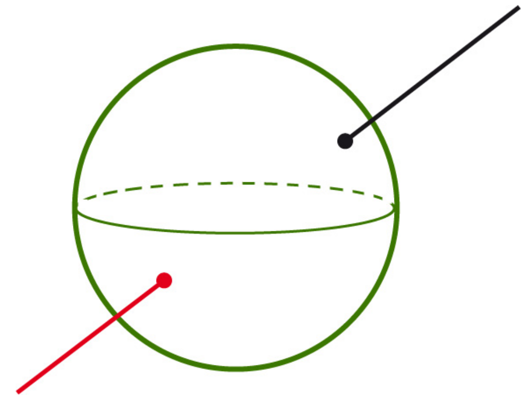
We are interested in quasi-perfect codes, i.e $R(\mathcal{C}) = \left\lfloor \frac{d-1}{2} \right\rfloor + 1.$

Coding Theory and Caps

$[n, k, d]R$
$d = 4$ and $R = 2$ $\longrightarrow$ quasi-perfect linear code 1-error correcting

Cap : *set $\mathcal{Q}$ no three points of which are collinear*

Complete: $\mathcal{Q} \not\subset \mathcal{Q}', |\mathcal{Q}| < |\mathcal{Q}'|$



quasi-perfect $[n, k, 4]_q 2$-*t code*	$\longleftrightarrow$	*complete n-cap in* $PG(n-k-1, q)$
Columns of the parity-check matrix	$\longleftrightarrow$	*points in* $PG(n-k-1, q)$

Remark

best covering density $\Longleftrightarrow$ *smallest complete caps*

Smallest Complete Caps

Remark

best covering density $\Longleftrightarrow$ *smallest complete caps*

Definition

$t_2(N, q)$: *Minimum size of complete caps in* $PG(N, q)$.

Trivial Lower Bound

$$t_2(N, q) \geq \sqrt{2} q^{\frac{N-1}{2}}$$

$N = 3 \longrightarrow t_2(3, q)$ known only for $q \leq 7$

$q \leq 5$	1998 G.Faina, S.Marcugini, A.Milani, F.P., Ars Combin.
$q = 7$	2006 J. Bierbrauer, S.Marcugini, F.P., Discrete Math.

Known constructions of infinite families of small complete caps in $PG(N, q)$

Trivial Lower Bound

$$t_2(N, q) \geq \sqrt{2}q^{\frac{N-1}{2}}$$

$$q \text{ even and } N \text{ odd} \longrightarrow 3(q^{\frac{N-1}{2}} + \ldots + q) + 2$$

- Gabidulin, Davydov, Tombak, "Linear codes with covering radius 2 and other new covering codes", *IEEE Trans. Inform. Theory*, 1991
- Pambianco, Storme, "Small complete caps in spaces of even characteristic", *J. Combin. Theory Ser. A*, 1996
- Giulietti, "Small complete caps in $PG(N, q)$, q even", *J. Combin. Des.*, 2007
- Davydov, Giulietti, Marcugini, Pambianco, "New inductive constructions of complete caps in $PG(N, q)$, q even", *J. Combin. Des.*, 2010

Known constructions of infinite families of small complete caps in $PG(N, q)$

Trivial Lower Bound

$$t_2(N, q) \geq \sqrt{2}q^{\frac{N-1}{2}}$$

N even $\longrightarrow cq^{N/2}$

- Pambianco, Storme, "Small complete caps in spaces of even characteristic", *J. Combin. Theory Ser. A*, 1996
- Davydov, Östergård, "Recursive constructions of complete caps", *J. Statist. Planning Infer.*, 2001
- Giulietti, "Small complete caps in $PG(N, q)$, q even", *J. Combin. Des.*, 2007
- Giulietti, "Small complete caps in Galois affine spaces", *J. Algebraic Combin.*, 2007
- Giulietti, Pasticci, "Quasi-perfect linear codes with minimum distance 4", *IEEE Trans. Inform. Theory*, 2007
- Davydov, Giulietti, Marcugini, Pambianco, "New inductive constructions of complete caps in $PG(N, q)$, q even", *J. Combin. Des.*, 2010

Known constructions of infinite families of small complete caps in $PG(N,q)$

Trivial Lower Bound

$$t_2(N,q) \geq \sqrt{2}q^{\frac{N-1}{2}}$$

$$\boxed{N \equiv 0 \pmod 4 \text{ and } q \text{ odd} \longrightarrow q^{(N/2-1/8)}}$$

- Giulietti, “Small complete caps in Galois affine spaces”, *J. Algebraic Combin.*, 2007
- Anbar, Bartoli, Giulietti, Platoni, “Small Complete Caps from Singular Cubics”, *J. Combin. Des.*, 2013
- Anbar, Bartoli, Giulietti, Platoni, “Small Complete Caps from Singular Cubics II”, J. Algebraic Combin., 2014

Main result

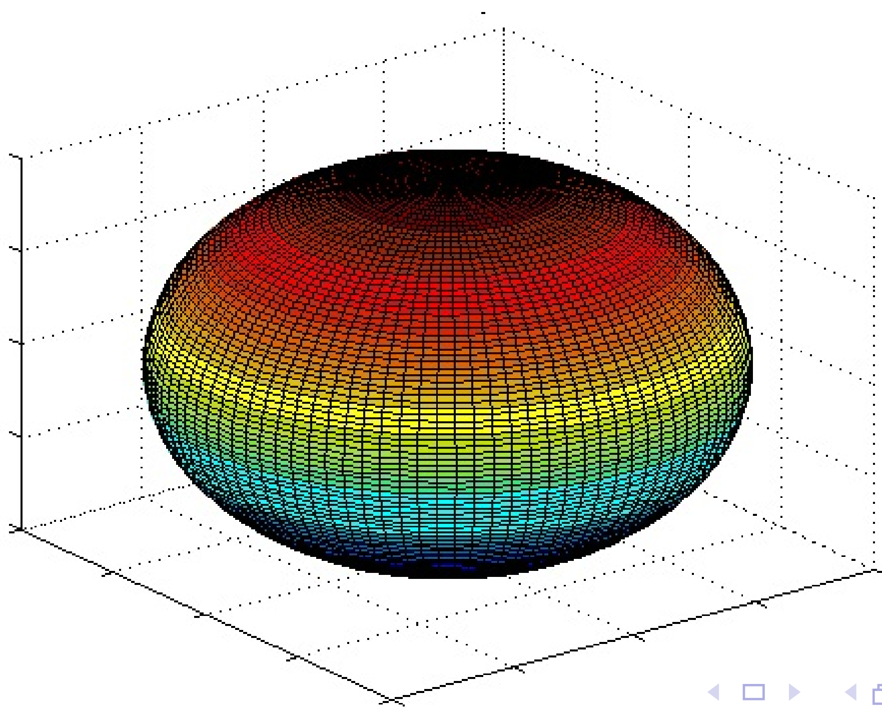
Theorem

$PG(N, q)$

$$\exists\ c > 0 \text{ and } M > 0:$$

$q \geq M \implies \exists$ *a complete cap of size*

$$O\left(q^{\frac{N-1}{2}} \log^c q\right).$$



Main result

Theorem

$\mathcal{C}$: $[n, n-(N+1), 4]_{q^2}$ *linear code*

$\exists$ $c > 0$ *and* $M > 0$:

$$q \geq M \implies \boxed{n = O\left(q^{\frac{N-1}{2}} log^c q\right)}$$

Probabilistic methods in Combinatorics

- **Graph Theory**

- **Graph Theory**
- **Blocking sets**

- **Graph Theory**
- **Blocking sets**
- **Saturating sets**

- **Graph Theory**
- **Blocking sets**
- **Saturating sets**
- **Complete arcs in projective planes**

The probabilistic construction of small complete arcs of J.H. Kim and W.H. Vu, *Combinatorica*, 2003

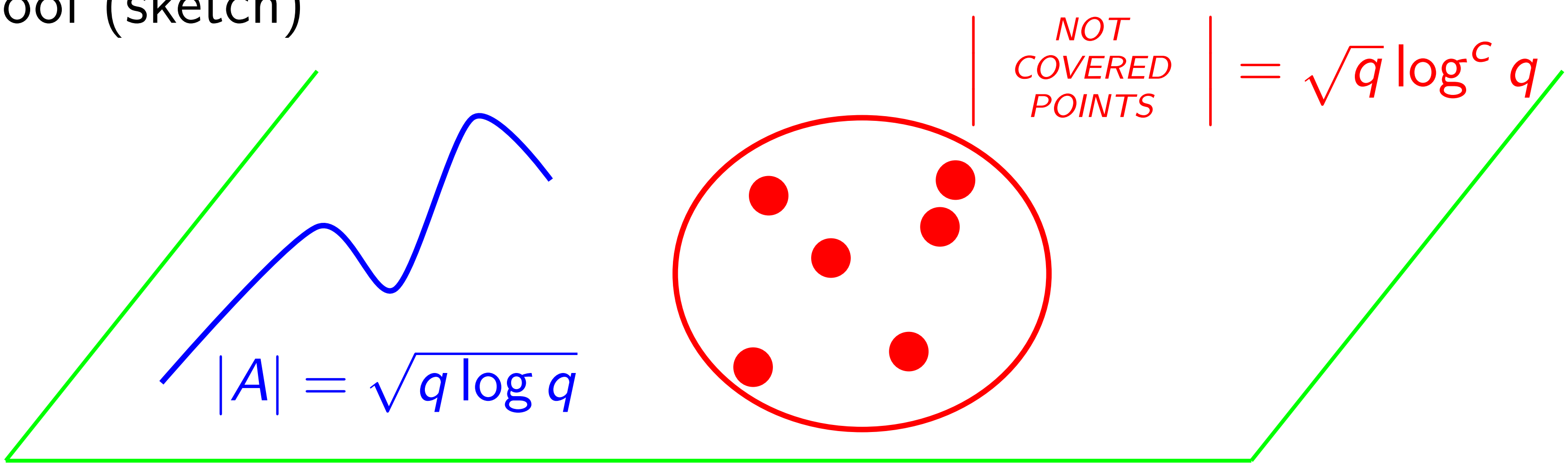
Theorem

$PG(2,q)$ $\quad \exists\ c > 0$ *and* $M > 0$:

$$q \geq M \implies \exists \text{ a complete arc of size}$$

$$O\left(q^{\frac{1}{2}} \log^c q\right).$$

Proof (sketch)



randomized algorithm with probability close to 1	$\Longrightarrow$	complete arcs in $\Theta(\log^{5/2} q)$ steps

Nibble method vs Point-by-point method

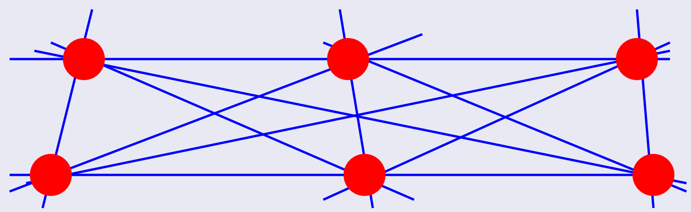
Point-by-point construction

1. *Select a new element among those which* **do not cause** *any conflict*
   - **Random**
   - **Greedy**
   - **According a certain ordering**
2. *Discard all elements that* **cause** *any conflict*

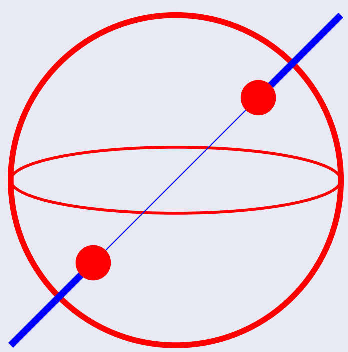
Nibble method vs Point-by-point method

Example

1. *At the beginning the cap being constructed is empty*
2. *Select one non-discarded point according to the criterion*
3. *At each step, discard all points contained in any secant of already selected points*



4. *At the end the set of all selected points is a complete cap*



Nibble method vs Point-by-point method

Ajtai, Komlós, Szemerédi, "A dense infinite Sidon sequence", *Eur. J. Comb.*, 1981

Rödl, "On a packing and covering problem", European J. Comb., 1985

Nibble method

1. *Select a bunch of elements together with some probability (a nibble)*

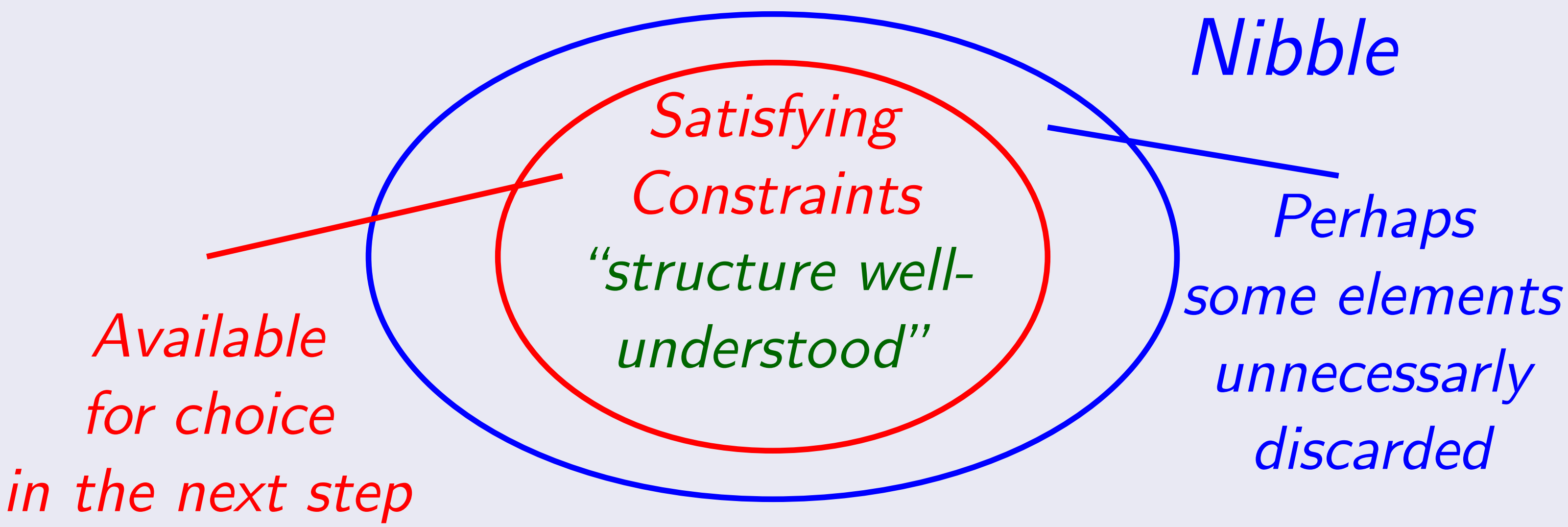
Nibble method vs Point-by-point method

Ajtai, Komlós, Szemerédi, “A dense infinite Sidon sequence”, *Eur. J. Comb.*, 1981

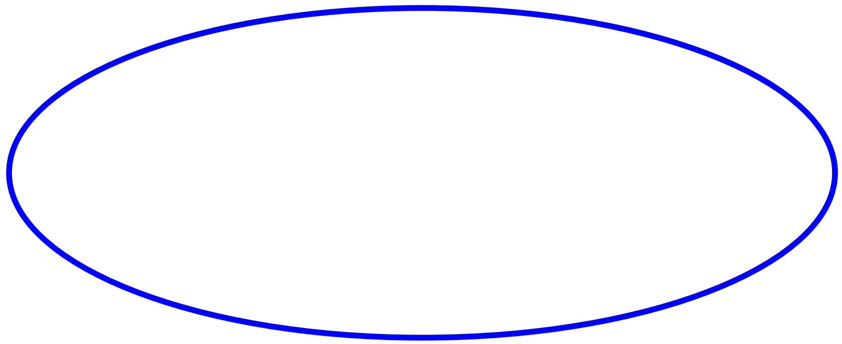
Rödl, “On a packing and covering problem”, European J. Comb., 1985

Nibble method

1. *Select a bunch of elements together with some probability (a nibble)*
2. *Select a subset of the nibble satisfying some constraints*



Nibble method vs Point-by-point method



NIBBLE

"Convenient Size?"

NO
TOO BIG $\Longrightarrow$

- too many elements would be unnecessarily discarded
- hard to predict the structure of its elements

YES
SMALL ENOUGH $\Longrightarrow$

- no conflict occurs for most chosen elements
- only few elements would be unnecessarily discarded

Algorithm: START

$$\boxed{PG(N, q)}$$

$A_i \rightarrow$ the cap at step i

Algorithm: START

$$\boxed{PG(N, q)}$$

$A_i \longrightarrow$ the cap at step i

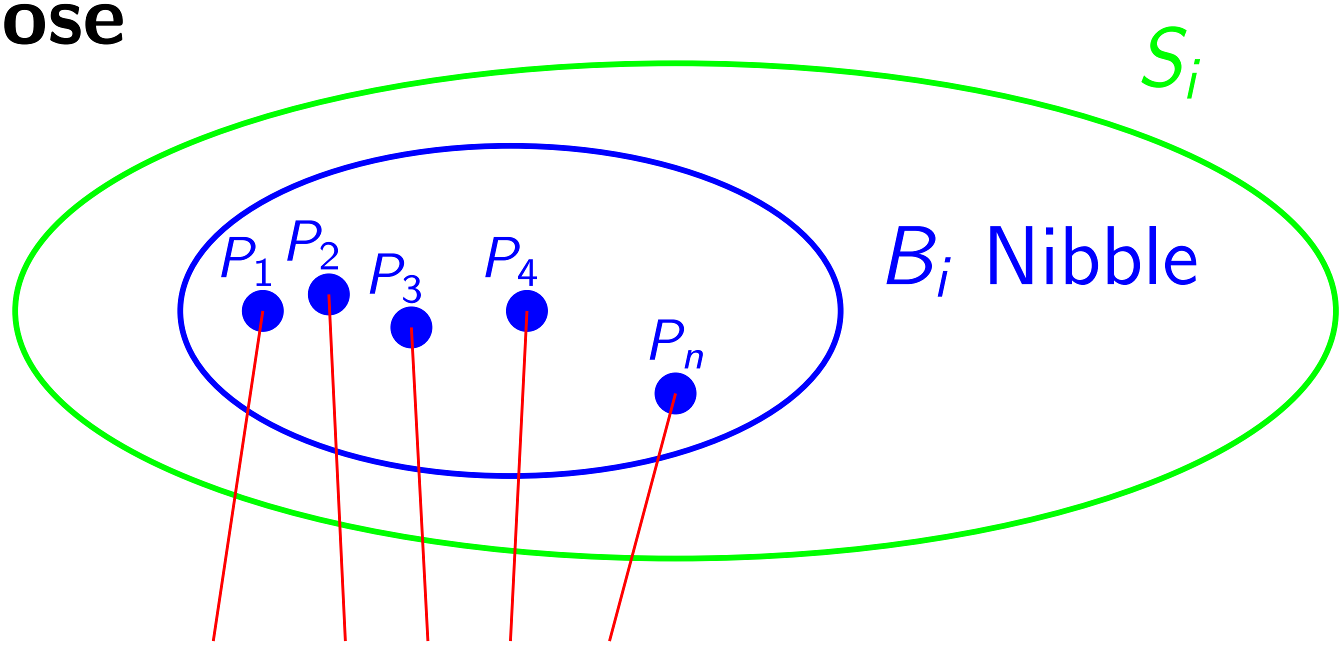
START :

$$A_0 = \emptyset.$$

$$\Omega_0 = S_0 = PG(N, q).$$

Algorithm: AT EACH STEP

- **Choose**



Chosen independently with the same probability

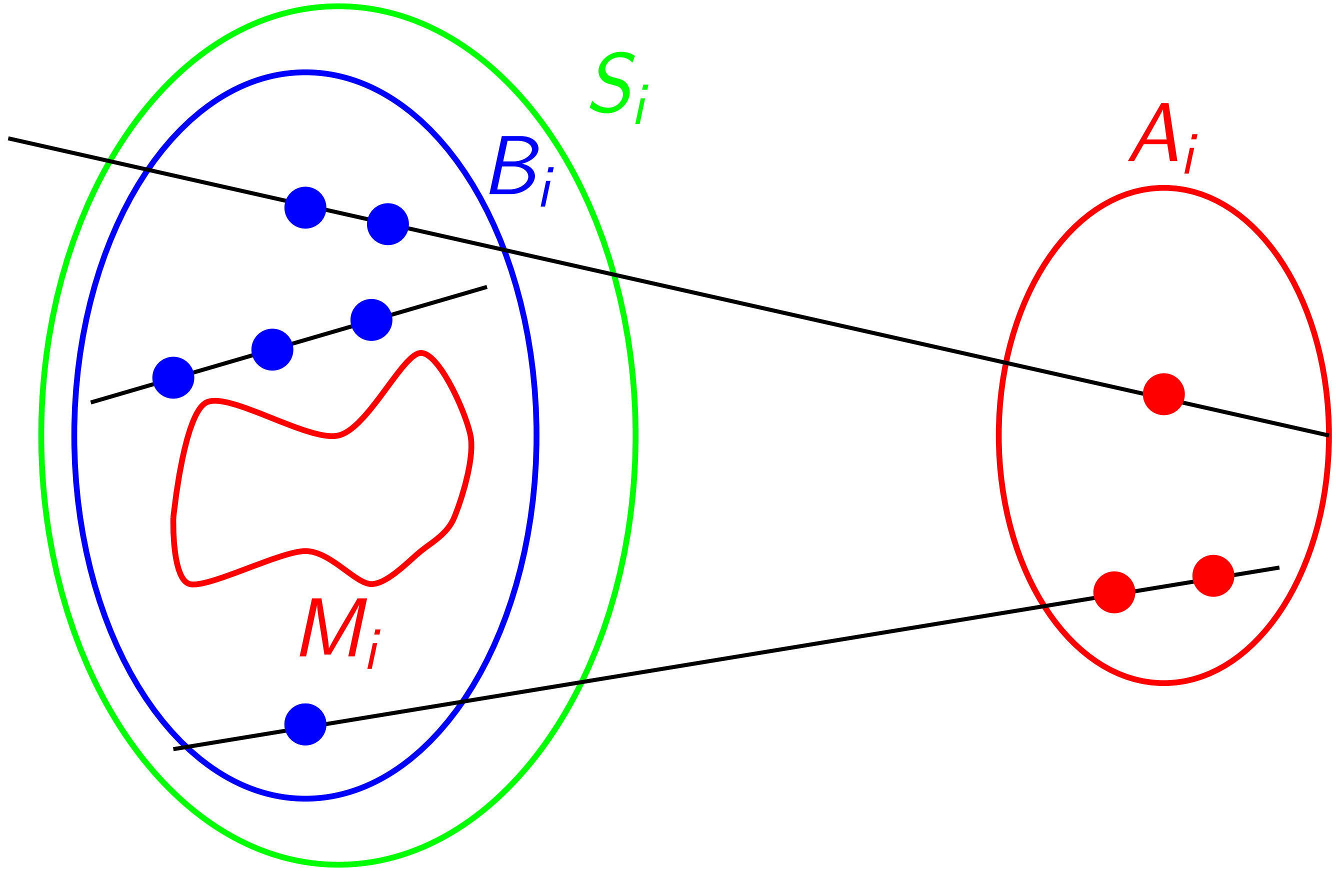
$$p_i = (b_i q^{\frac{N+1}{2}} log^2 q)^{-1},$$

where $b_i = \frac{|S_i|}{q^N + q^{N-1} + \ldots + q + 1}$

Algorithm: AT EACH STEP

- **Choose**

$$M_i = \{P \in B_i : \nexists Q, R \in A_i \cup B_i : P, Q, R \text{ are collinear } \}$$



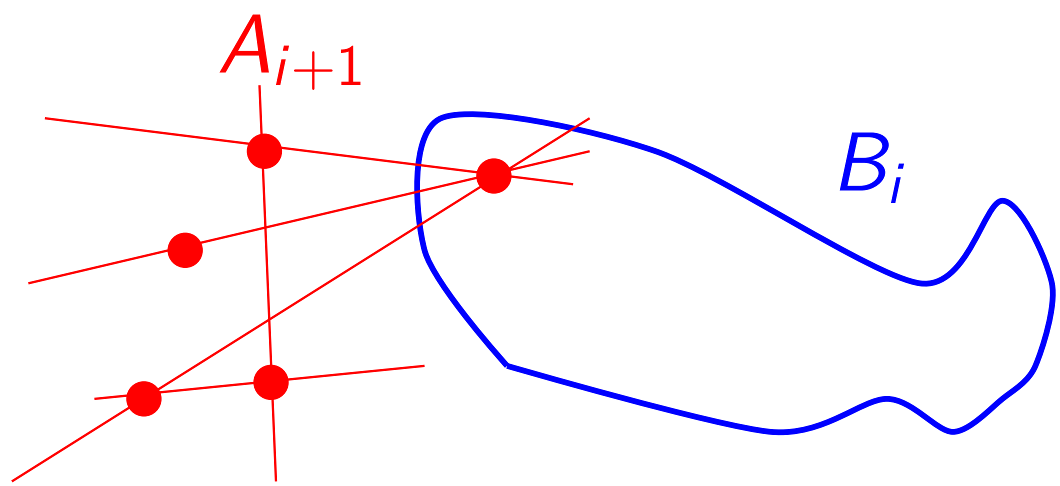
Definition

$$A_{i+1} = A_i \cup M_i.$$

Algorithm: AT EACH STEP

- **Delete**

$$D_i = \{\text{the set of points on bisecants of } A_{i+1}\} \cup B_i$$



Definition

$$\Omega_{i+1} = \Omega_i \setminus D_i.$$

$$P \in \Omega_i, \quad p_i(P) = Pr(P \in D_i), \quad p_i^u \text{ upper bound}$$

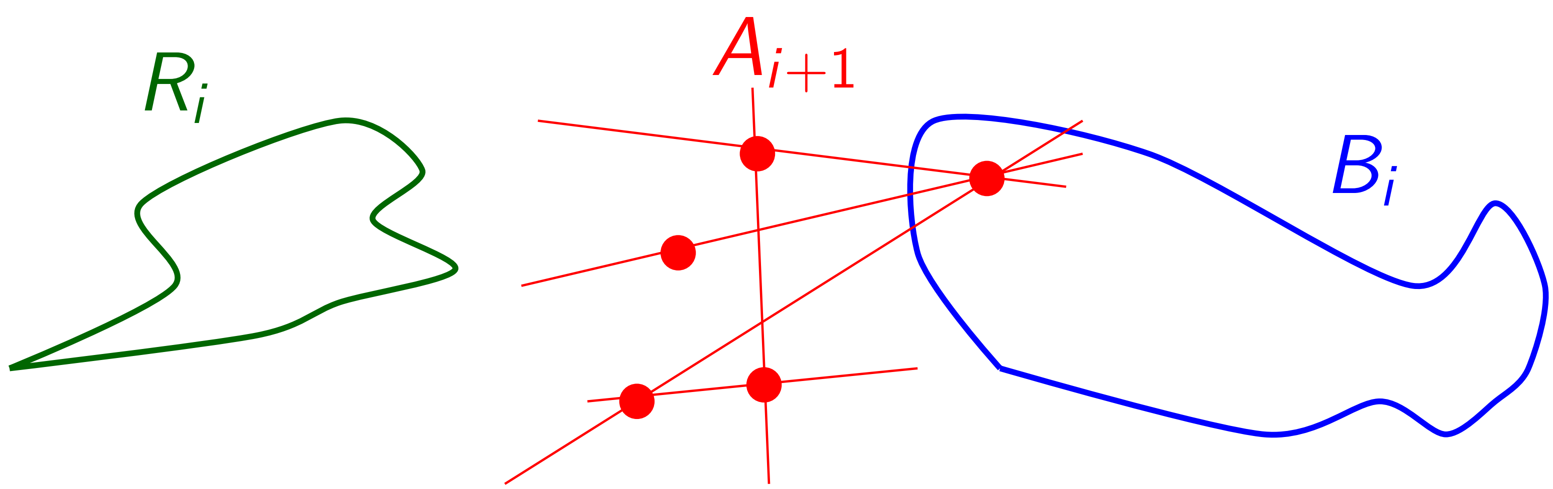
Algorithm: AT EACH STEP

- **Compensate**

$$P \in \Omega_i, \quad p_i(P) = Pr(P \in D_i), \quad p_i^u \text{ upper bound}$$

$R_i \subset S_i$ set of points chosen with probability

$$p_i^{com}(P) = \frac{p_i^u - p_i(P)}{1 - p_i(P)}.$$



Definition

$$S_{i+1} = S_i \setminus (D_i \cup R_i).$$

Algorithm

Remark

Compensation is made in order to give the

same probability

to the points in S_i to be in S_{i+1}.

In fact, if $p_i(P) = Pr(P \in D_i)$, then

$$Pr(P \notin S_{i+1} | P \in S_i) = p + (1-p)\frac{p_i^u - p}{1-p} = p_i^u.$$

So,

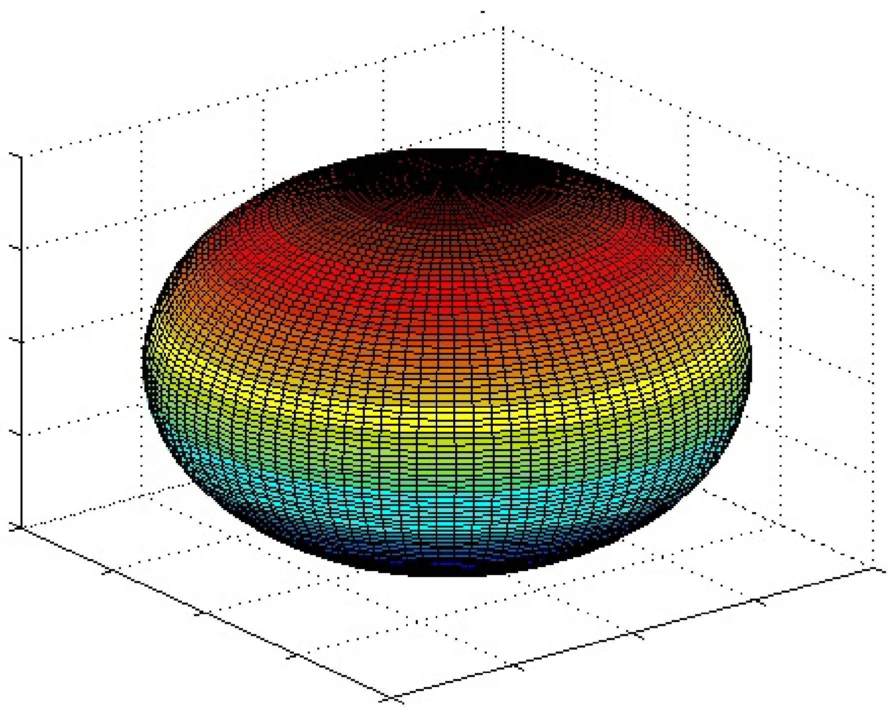
$$\mathbb{E}(|S_{i+1}|) = |S_i|(1 - p_i^u).$$

Algorithm: STOP

STOP : after k steps if k is the smallest integer such that

$$\frac{|S_k|}{q^N + q^{N-1} + \ldots + q + 1} = b_k \leq q^{-\frac{N+1}{2}} \log^c q,$$

for some constant c (we set $c = 300$).



Concentration of Measure

Problem

X random variable with mean $\mathbb{E}[X]$.

What is the probability that X deviates far from $\mathbb{E}[X]$?

random variable X_i, $i = 1, \ldots, n$	$\leftrightarrow$	Success of a trial with probability p_i

$\downarrow$

Estimate the number of successes

Theorem (Chernoff Bound)

Let $X = \sum_{i=1}^{n} X_i$, $p = \frac{\sum_{i=1}^{n} p_i}{n}$, $q = 1 - p$. Then for any t

$$Pr(X > (p+t)n) \leq e^{\left(-(p+t)\ln\frac{p+t}{p} - (q-t)\ln\frac{q-t}{t}\right)^n}.$$

New Concentration Results

t_P is the binary event:
the point $P \in S_i$ is chosen to be in the nibble B_i or not

Definition

$\bar{t} = (t_1, \ldots, t_n)$ independent binary random variables
$Y(t_1, \ldots, t_n)$ function

discrete Lipschitz coefficient of Y := smallest integer r
$$|Y(\bar{t}) - Y(\bar{t}')| \le r$$
$$\bar{t} = (t_1, \ldots, t_i, \ldots, t_n)$$
$$\bar{t}' = (t_1, \ldots, t_i', \ldots, t_n)$$

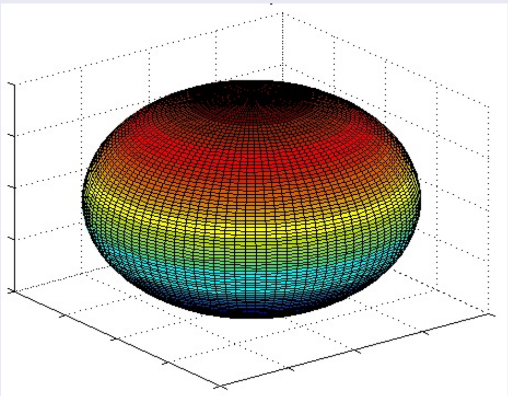
Theorem (J.H. Kim, W.H. Vu, *Combinatorica*, 2000)

r sufficiently small with respect to n and the mean of Y
$$\Downarrow$$
Y is strongly concentrated with variance of order at most $r^2 n$.

Main result

Theorem

$\exists\ M > 0$:
in $PG(N,q)$ $q \geq M$ *there exists*
a complete cap of size
$$O\left(q^{\frac{N-1}{2}} log^{300} q\right).$$



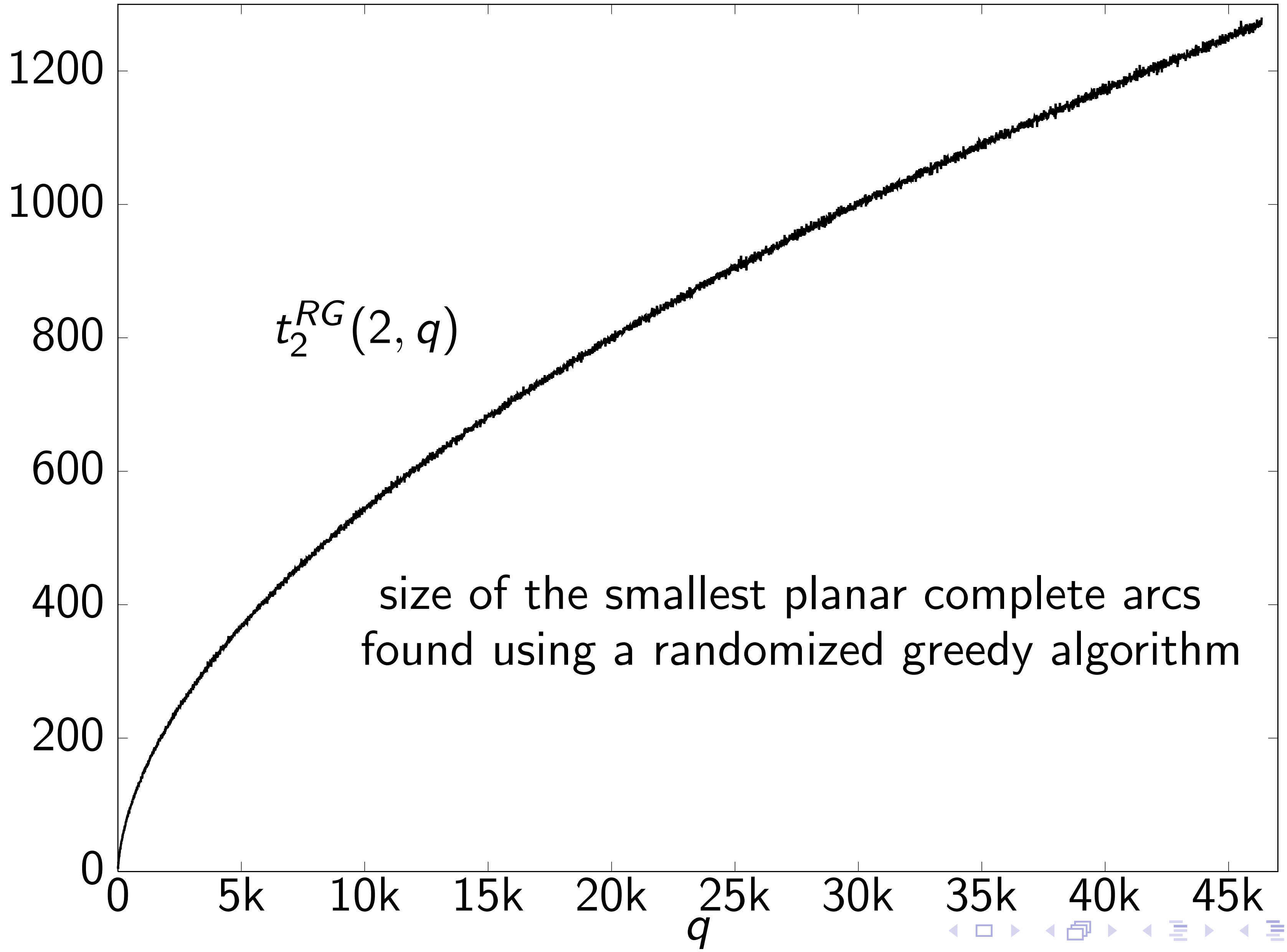
$$\Updownarrow$$

Theorem

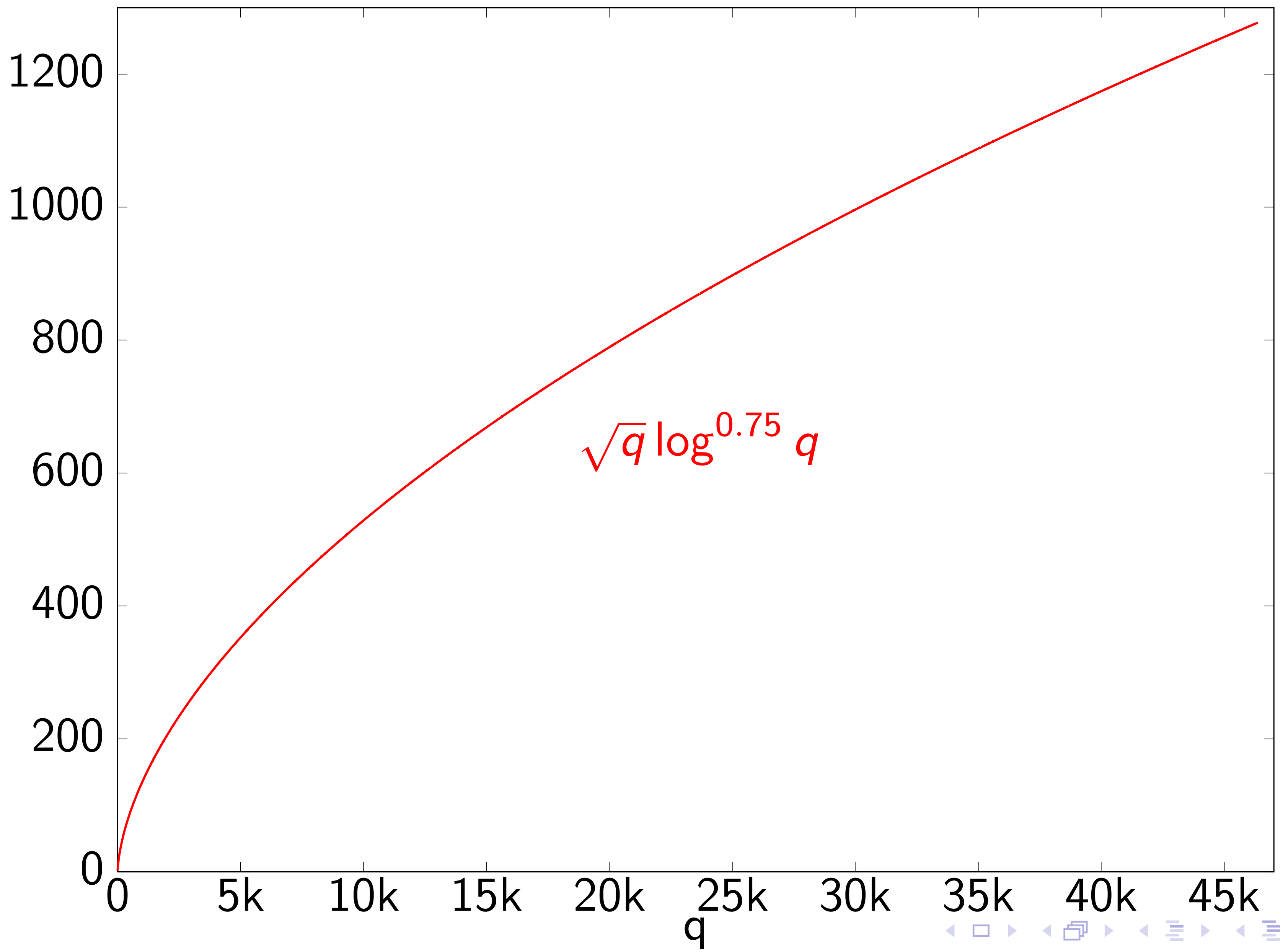
$\mathcal{C}$: $[n, n-(N+1), 4]_q 2$ *linear code*

$\exists\ M > 0$:
$$q \geq M \Longrightarrow n = O\left(q^{\frac{N-1}{2}} log^{300} q\right).$$

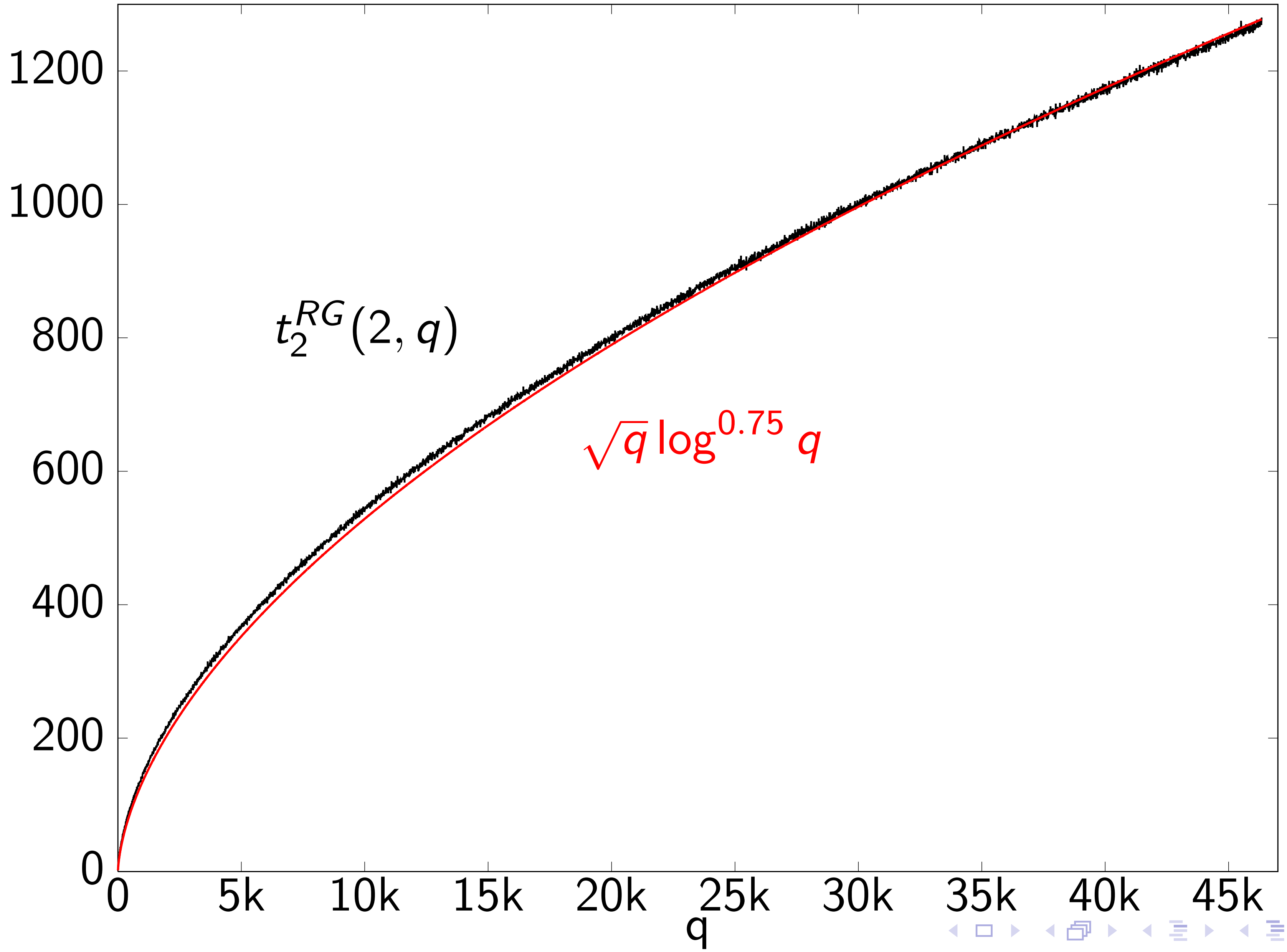
Something better?



Something better?



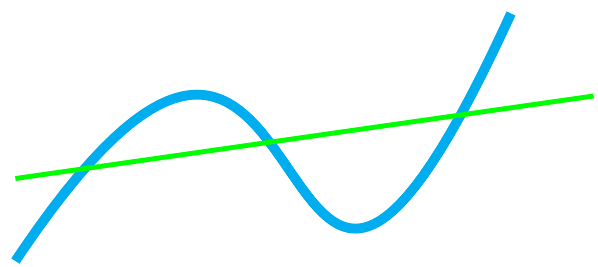
Something better?



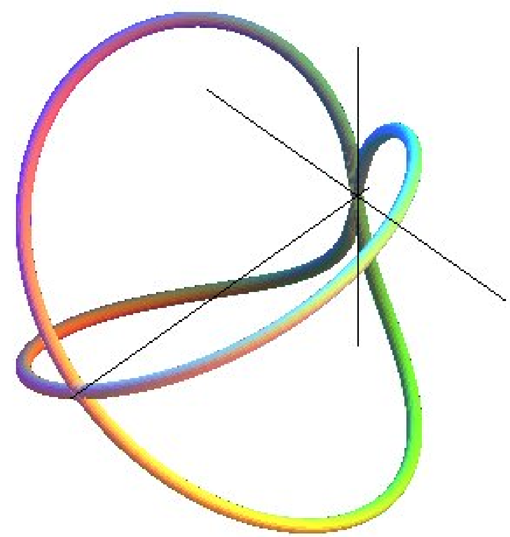
To do

- computer search using a nibble algorithm

- bounds for the sizes of complete (n,r)-arcs in projective planes



- bounds for the sizes of complete arcs in projective spaces



SYMMETRIC SURFACES

$\mathbb{K}$ algebraically closed field $char(\mathbb{K}) = 0$

$$\mathbb{P}^3(\mathbb{K})$$

What are the maximally symmetric nonsingular algebraic surfaces?

SYMMETRIC SURFACES

$\mathbb{K}$ algebraically closed field $char(\mathbb{K}) = 0$

$\mathbb{P}^3(\mathbb{K})$

What are the maximally symmetric nonsingular algebraic surfaces?

$\mathbb{P}^2(\mathbb{K})$

What are the maximally symmetric nonsingular algebraic curves?

The Fermat curve

[Characterization of the Fermat curve as the most symmetric nonsingular algebraic plane curve, F.P., Mathematische Zeitschrift 2014]

The most symmetric nonsingular plane curve

THEOREM

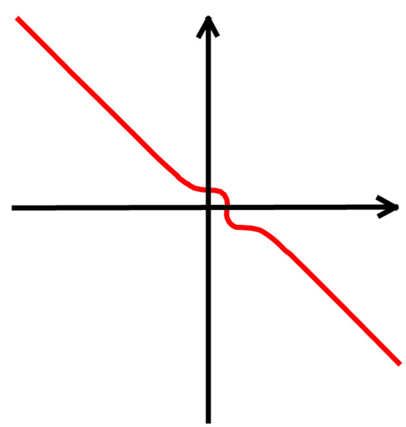
$\mathbb{K}$ algebraically closed field $\qquad char(\mathbb{K}) = 0$

$f \in \mathbb{K}[x, y, t]$, homogeneous of degree $d > 4, \quad d \neq 6$

$V(f)$: nonsingular algebraic curve in $\mathbb{P}^2(\mathbb{K})$

$$\Downarrow$$

- $|\mathrm{Aut}(V(f))| \leq 6d^2$
- $|\mathrm{Aut}(V(f))| = 6d^2 \iff V(f)$ projectively equivalent to Fermat curve



$$x^d + y^d + t^d = 0$$

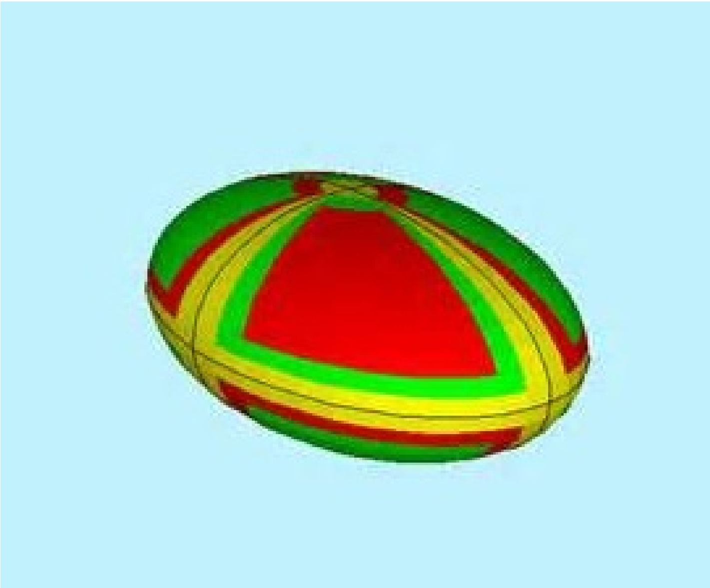
$\mathbb{P}^3(\mathbb{K})$, $\mathbb{K}$ algebraically closed field $char(\mathbb{K}) = 0$

What are the maximally symmetric nonsingular algebraic surfaces $\mathcal{S}_{\mathbf{d}}$?

$$d = 2 \qquad x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$$

the unique non-singular quadric

Automorphism group:
INFINITE



$\mathbb{K}$ algebraically closed field $char(\mathbb{K}) = 0$

$\mathbb{P}^3(\mathbb{K})$

What are the maximally symmetric nonsingular algebraic surfaces $\mathcal{S}_{\mathbf{d}}$?

$\mathcal{S}_{\mathbf{d}} \subset \mathbb{P}^3(\mathbb{K}) \quad d \geq 3,\ d \neq 4$

$\Downarrow$

$Aut(\mathcal{S}_{\mathbf{d}})$ FINITE $< PGL(4, \mathbb{K})$

H. Matsumura and P. Monsky, 1964

CUBIC SURFACES

$$\mathbb{P}^3(\mathbb{K})$$

$d = 3$	Nonsingular algebraic cubic surfaces $\mathcal{S}_3$

Complete classification of automorphism groups (T. Hosoh, 1997)

$Aut(\mathcal{S}_3) = (\mathbb{Z}_3)^3 \times_s \mathbf{S}_4$	MAXIMUM ORDER
$Aut(\mathcal{S}_3) = \mathbf{S}_5$	SECOND MAXIMUM ORDER

CUBIC SURFACES

$$\mathbb{P}^3(\mathbb{K})$$

$d = 3$	Nonsingular algebraic cubic surfaces $\mathcal{S}_3$

Complete classification of automorphism groups (T. Hosoh, 1997)

$Aut(\mathcal{S}_3) = (\mathbb{Z}_3)^3 \times_s \mathbf{S}_4$	MAXIMUM ORDER
$Aut(\mathcal{S}_3) = \mathbf{S}_5$	SECOND MAXIMUM ORDER

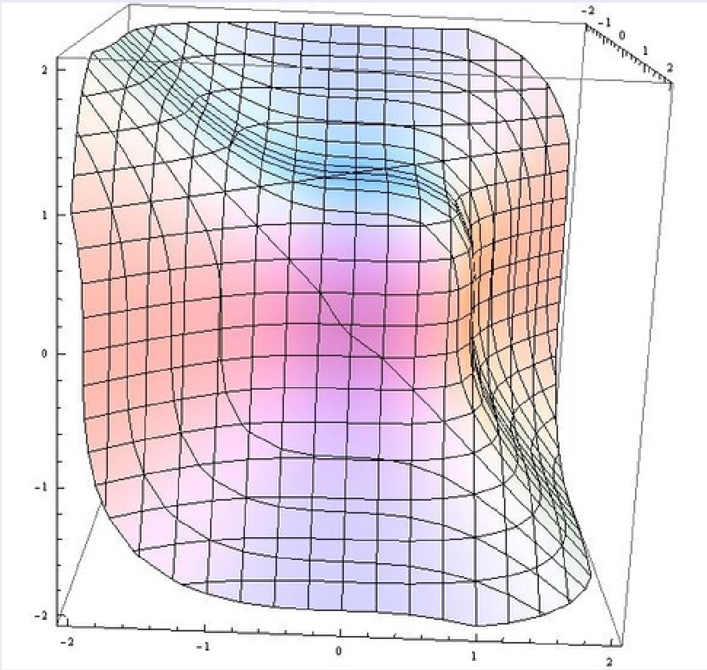
Theorem (H. Kaneta, S. Marcugini, F. P., 2014)

Up to equivalence

the Fermat surface

$$\mathcal{S}_3 = V(x^3 + y^3 + z^3 + t^3)$$

UNIQUE MAXIMALLY SYMMETRIC nonsingular algebraic cubic surface



THE MAXIMALLY SYMMETRIC

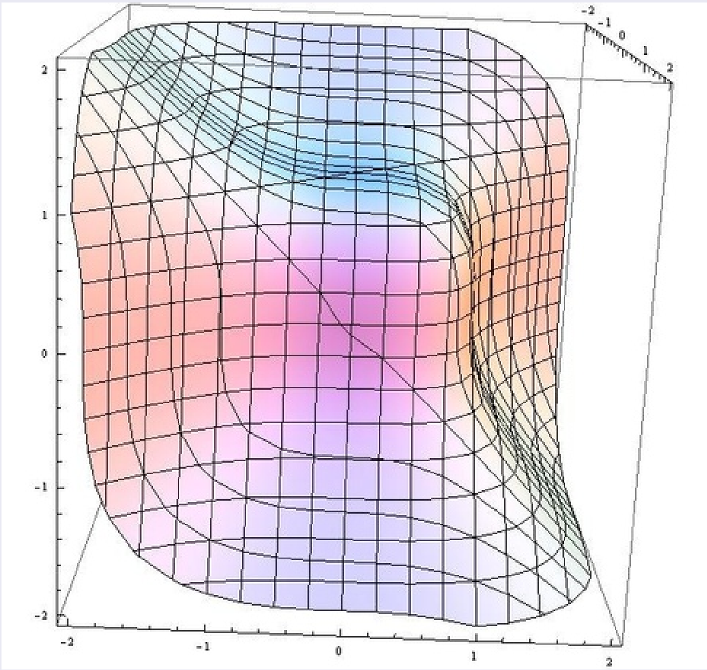
Theorem (H. Kaneta, S. Marcugini, F. P., 2014)

Up to equivalence

the Fermat surface

$$\mathcal{S}_3 = V(x^3 + y^3 + z^3 + t^3)$$

UNIQUE MAXIMALLY SYMMETRIC
nonsingular algebraic cubic surface



Proof (sketch)

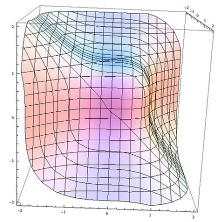
(1) $\mathcal{G} < PGL(4, \mathbb{K})$ $\quad \mathcal{G} \cong \mathbb{Z}_3^3$ conjugate to
$\mathcal{G}_{27} = \langle (\mathrm{diag}[\omega, 1, 1, 1]), (\mathrm{diag}[1, \omega, 1, 1]), (\mathrm{diag}[1, 1, \omega, 1]) \rangle$

(2) Any $\mathcal{G}_{27}-$invariant nonsingular algebraic cubic surface is
$V(ax^3 + by^3 + cz^3 + dt^3) \quad a, b, c, d \in \mathbb{K}^*$

FERMAT CUBIC SURFACE

(2) Any $\mathcal{G}_{27}$−invariant nonsingular algebraic cubic surface is

$$V(ax^3 + by^3 + cz^3 + dt^3) \qquad a, b, c, d \in \mathbb{K}^*$$



f homogeneous polynomial of degree 3

$V(f)$ $\mathcal{G}_{27}$−invariant nonsingular algebraic cubic surface

$$A_1 = \mathrm{diag}[\omega, 1, 1, 1],\ A_2 = \mathrm{diag}[1, \omega, 1, 1],\ A_3 = \mathrm{diag}[1, 1, \omega, 1]$$

$$ord(A_i) = 3$$

$$(A_i) \subset \mathcal{G}_{27} \Rightarrow f((x, y, z, t)A_i) \in \{f, \omega f, \omega^2 f\}$$

- $f((x, y, z, t)A_i) \in \{\omega f, \omega^2 f\} \Rightarrow V(f)$ **singular**
- $f((x, y, z, t)A_i) = f \Rightarrow \quad f = ax^3 + by^3 + cz^3 + dt^3$

  $V(ax^3 + by^3 + cz^3 + dt^3)$ **nonsingular** $\Leftrightarrow \quad a, b, c, d \in \mathbb{K}^*$

THE SECOND MAXIMALLY SYMMETRIC

Theorem (H. Kaneta, S. Marcugini, F. P., 2014)

Up to equivalence

$$\mathcal{S}_3 = V(x^2y + y^2z + z^2t + t^2x)$$

UNIQUE SECOND MAXIMALLY SYMMETRIC

nonsingular algebraic cubic surface

Proof (sketch)

$\mathbf{S}_5$ up to conjugacy

$\nearrow$ $\mathcal{C}_{5!}$ I $\Longrightarrow$ any $\mathcal{C}_{5!}$I-invariant nonsingular algebraic cubic surface is $V(x^2y + y^2z + z^2t + t^2x)$

$\longrightarrow$ $\mathcal{C}_{5!}$ II $\Longrightarrow$ $\nexists$ nonsingular

$\searrow$ $\mathcal{C}_{5!}$ III $\Longrightarrow$ $\nexists$ nonsingular

Representations

Thank you

for your attention!