# Upper bounds on the smallest sizes of a complete arc in $PG(2, q)$ based on computer search

Daniele Bartoli[*] Alexander A. Davydov[@] Giorgio Faina[*]
Alexey A. Kreshchuk[@] Stefano Marcugini[*]
Fernanda Pambianco[*] Igor A. Tkachenko[&]

@ Institute for Information Transmission Problems (Kharkevich Institute), Russian Academy of Science, Moscow, Russia
* Department of Mathematics and Informatics, Perugia University, Perugia, Italy
& National Research Centre "Kurchatov Institute", Moscow, Russia

XIV International Workshop on Algebraic and Combinatorial Coding Theory, ACCT-2014, Svetlogorsk, Russia, September 7-13, 2014

# Outline

# INTRODUCTION NOTATION

$PG(2,q)$ $\Leftrightarrow$ projective **space** of dimension 2 over Galois field $F_q$

$n$-**arc** $\Leftrightarrow$ a set of $n$ points no three of which are collinear

a line meeting an arc $\Leftrightarrow$ **tangent** or **bisecant**

bisecant $\Leftrightarrow$ a line intersecting an arc in two points

a **point** $A$ of $PG(2,q)$ is **covered** by an arc $\Leftrightarrow$
$A$ lies on a **bisecant** of the arc

**complete arc** $\Leftrightarrow$ all points of $PG(2,q)$ are covered
by bisecants of the arc

$\Leftrightarrow$ one may not add a new point to a complete arc

# INTRODUCTION NOTATION

$t_2(2, q) \Leftrightarrow$ the smallest size of a complete arc in $PG(2, q)$

**HARD OPEN CLASSICAL PROBLEM:** **1950** $\rightarrow$

**upper bound on** $t_2(2, q)$

$\bar{t}_2(2, q) \Leftrightarrow$ the smallest **known** size of a complete arc in $PG(2, q)$ including computer search

$$t_2(2, q) \leq \bar{t}_2(2, q)$$

theoretical bound $t_2(2, q) \leq d\sqrt{q} \log^c q, \quad c \leq 300$

$c, d \Leftrightarrow$ constants independent of $q$ J.H. Kim, V. Vu **2003**

# INTRODUCTION NOTATION

$t_2(2,q)$ ⇔ the smallest size of a complete arc in $PG(2,q)$

**HARD OPEN CLASSICAL PROBLEM:** **1950** →

**upper bound on** $t_2(2,q)$

$\bar{t}_2(2,q)$ ⇔ the smallest **known** size of a complete arc in $PG(2,q)$ including computer search

$$t_2(2,q) \le \bar{t}_2(2,q)$$

theoretical bound $t_2(2,q) \le d\sqrt{q}\log^c q, \quad c \le 300$

$c, d$ ⇔ constants independent of $q$ J.H. Kim, V. Vu **2003**

# INTRODUCTION NOTATION

$t_2(2,q) \Leftrightarrow$ the smallest size of a complete arc in $PG(2,q)$

**HARD OPEN CLASSICAL PROBLEM:** **1950** $\rightarrow$

**upper bound on** $t_2(2,q)$

$\bar{t}_2(2,q) \Leftrightarrow$ the smallest **known** size of a complete arc in $PG(2,q)$ including computer search

$$t_2(2,q) \leq \bar{t}_2(2,q)$$

theoretical bound $t_2(2,q) \leq d\sqrt{q}\log^c q, \quad c \leq 300$

$c, d \Leftrightarrow$ constants independent of $q$ J.H. Kim, V. Vu **2003**

# Randomized greedy algorithms

A greedy algorithm is an algorithm that makes the *locally optimal choice* at each stage with the hope of finding a global optimum or, at least, a global "good" solution.

A randomized greedy algorithm executes some stages in a random manner without the local optimum.

HUGE region $T = \{\textbf{all} \quad q \leq 150001 \ \ \textbf{without gaps}\} \cup$

$\{41 \ \ \text{sporadic} \ \ q's \text{ in } [150503 \ldots 430007]\}$

D.Bartoli, A.A.Davydov, G.Faina, A.A.Kreshchuk, S.Marcugini, F.Pambianco
*J. of Geometry, Discrete Mathematics, OC2013, arXiv* **2005-2014**

Many arcs have been obtained using resources of Multipurpose Computing Complex of National Research Centre "Kurchatov Institute"

## Theorem

$$t_2(2,q) < \min\{\sqrt{q}\ln^{0.7295} q,\ 0.6\sqrt{q}\ln^{\varphi(q)} q,\ 1.745\sqrt{q\ln q}\}$$

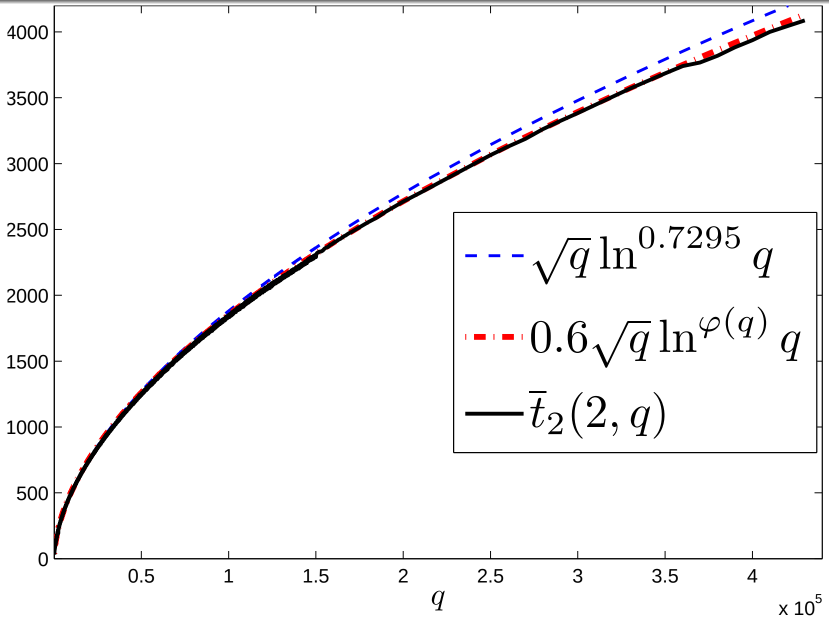
$$q \in T, \quad \varphi(q) = \frac{1.5}{\ln q} + 0.802$$

$$\min = \begin{cases} \sqrt{q}\ln^{0.7295} q & \textit{if} \quad q < 9500 \\ 0.6\sqrt{q}\ln^{\varphi(q)} q & \textit{if} \quad 9500 < q < 310000 \\ 1.745\sqrt{q\ln q} & \textit{if} \quad 310000 < q \end{cases}$$

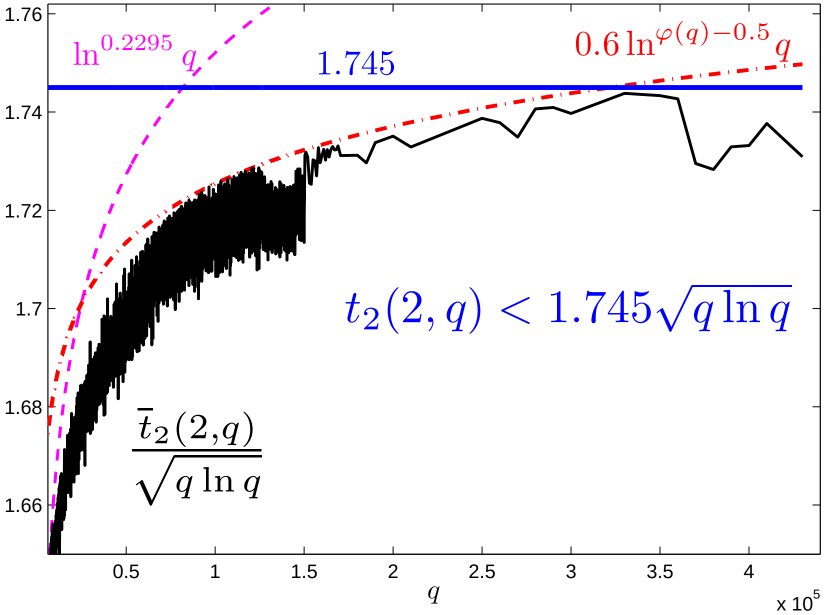
$\varphi(q)$ – decreasing function of $q$

an exotic form of the bound

"good" for $q < 310000$



4000
3500
3000
2500
2000
1500
1000
500
0
0.5
1
1.5
2
2.5
3
3.5
4
q
x 10^5
$\sqrt{q}\ln^{0.7295} q$
$0.6\sqrt{q}\ln^{\varphi(q)} q$
$\bar{t}_2(2,q)$



$\ln^{0.2295} q$
1.745
$0.6 \ln^{\varphi(q)-0.5} q$
$t_2(2,q) < 1.745\sqrt{q \ln q}$
$\frac{\bar{t}_2(2,q)}{\sqrt{q \ln q}}$
1.76
1.74
1.72
1.7
1.68
1.66
0.5
1
1.5
2
2.5
3
3.5
4
$q$
x $10^5$

# Algorithm FOP – fixed order of points

**Algorithm FOP.** We fix a particular order of points of $PG(2,q)$.

$$PG(2,q)=\{A_1,A_2,\dots,A_{q^2+q+1}\}$$

Algorithm FOP builds a complete arc *iteratively*, step-by-step

$K^{(i-1)}\Leftrightarrow$ the arc obtained on the $(i-1)$-th step.

On the next $i$-th step, the first uncovered point in the fixed order is added to $K^{(i-1)}$ that gives $K^{(i)}$

**Lexicographical order of points.** $q$ – **prime** The elements of the field $\mathbb{F}_q=\{0,1,\dots,q-1\}$ are integers modulo $q$

The homogenous coordinates of a point $A_i$ are treated as its number $i$ written in the $q$-ary scale of notation:

$$A_i=(x_0^{(i)},x_1^{(i)},x_2^{(i)}),\quad x_j^{(i)}\in\mathbb{F}_q,\qquad i=x_0^{(i)}q^2+x_1^{(i)}q+x_2^{(i)}$$

D.Bartoli, A.A.Davydov, G.Faina, S.Marcugini, F.Pambianco

*Journal of Geometry, ENDM, ACCT2012, OC2013, arXiv* **2012-2014**

# FOP vs lexicographical codes (greedy codes, lexicodes)

A (rare and insufficiently studied) variant of the lexicodes: a parity check matrix (PCM) of an $[n, n-r, d]_q$ code is created step-by-step. All $q$-ary column $r$-vectors are written in a list in some order. On every step we include to PCM the 1-st column from the list which cannot be represented as a linear combination of $d-2$ or smaller columns already included to PCM.

A point of $PG(2, q) \Leftrightarrow$ a column 3-vector.
FOP algorithm creates a PCM of $[n, n-3, 4]_q$ lexicode.

But in Coding Theory, for given $r, d$ the aim is to get a long code while our goal is to obtain a short complete arc.

For $r = 3, d = 4$, FOP algorithm gives "bad" codes that are essentially shorter than "good" codes corresponding to ovals.

# Region for computer search

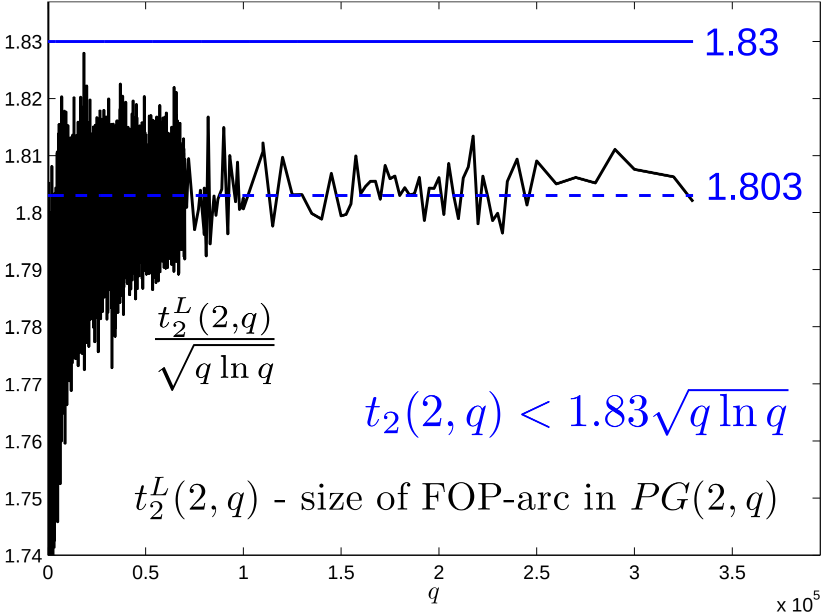
FOP-arcs

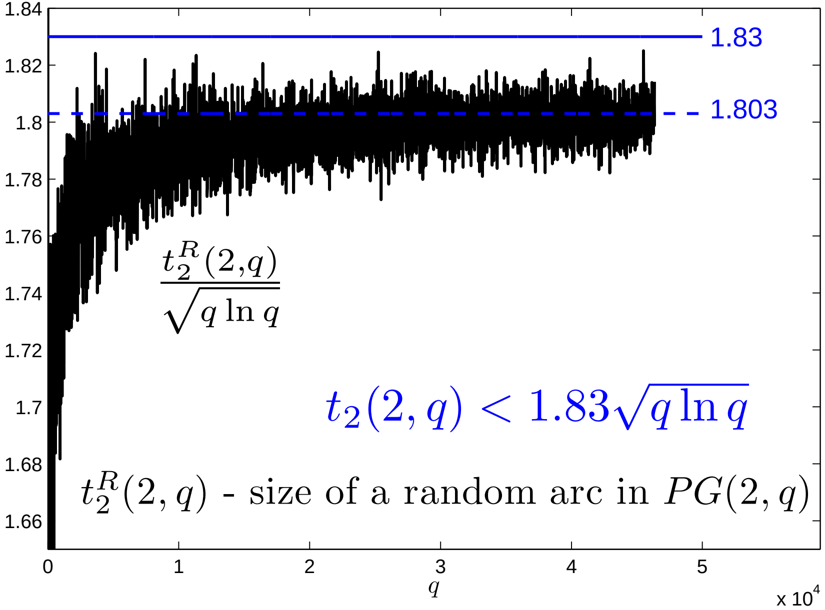
**all prime** $q \leq 70001$ **without gaps**

82 sporadic $q$'s in $[71001 \ldots 330017]$

Random arcs

**all prime** $q \leq 46337$ **without gaps**


1.83
1.803
$\frac{t_2^L(2,q)}{\sqrt{q \ln q}}$
$t_2(2,q) < 1.83\sqrt{q \ln q}$
$t_2^L(2,q)$ - size of FOP-arc in $PG(2,q)$
1.74
1.75
1.76
1.77
1.78
1.79
1.8
1.81
1.82
1.83
0
0.5
1
1.5
2
2.5
3
3.5
$q$
x $10^5$


1.84
1.82
1.8
1.78
1.76
1.74
1.72
1.7
1.68
1.66
1.83
1.803
$\frac{t_2^R(2,q)}{\sqrt{q \ln q}}$
$t_2(2,q) < 1.83\sqrt{q \ln q}$
$t_2^R(2,q)$ - size of a random arc in $PG(2,q)$
0
1
2
3
4
5
$q$
x $10^4$

# Conclusion

1. Lexicographical order is a random order in the geometrical sense.
   Graphics for FOP-arcs and random arcs are very similar

2. Mystery: Graphics $\frac{t_2^L(2,q)}{\sqrt{q \ln q}}$ and $\frac{t_2^R(2,q)}{\sqrt{q \ln q}}$ oscillate around line
   $y = 1.803$ parallel to the axis of abscissas

3. Greedy bound $1.745\sqrt{q \ln q}$
   FOP bound = random bound $1.830\sqrt{q \ln q}$

FOP – exact construction without random components;
computer time for FOP essentially smaller than for Greedy;
FOP bound is only slightly worse than Greedy bound;
computer search for very big $q$ should use FOP

Thank you Spasibo

Mille grazie

Premnogo blagodarya

!‘Muchas gracias

Toda raba

Merci beaucoup

Dankeschön

Dank u wel

Domo arigato