Upper bounds on the smallest size of a complete cap in $\mathrm{PG}(3, q)$ and $\mathrm{PG}(4, q)$

Daniele Bartoli* Alexander A. Davydov@ Alexey A. Kreshchuk@ Stefano Marcugini* Fernanda Pambianco*

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

XV International Workshop on Algebraic and Combinatorial Coding Theory, ACCT2016,Albena, Bulgaria, June 18-24, 2016

Outline

INTRODUCTION NOTATION

$\mathrm{PG}(N, q) \Leftrightarrow$ projective space of dimension N over Galois field $\mathbb{F}_q$

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

bisecant $\Leftrightarrow$ a line intersecting a cap in two points

a **point** A of $\mathrm{PG}(N, q)$ is **covered** by a cap $\Leftrightarrow$
the point A lies on a **bisecant** of the cap

complete cap $\Leftrightarrow$ all points of $\mathrm{PG}(N, q)$
are covered by bisecants of the cap
$\Leftrightarrow$ one may not add a new point to a complete cap

CONNECTIONS with CODING THEORY

complete n-cap in $\mathrm{PG}(N,q) \Leftrightarrow [n, n-(N+1), 4]_q 2$ code

point of the cap

$\Updownarrow$

column of a parity-check matrix of the code

LOWER BOUND

$t_2(N,q) \Leftrightarrow$ the smallest size of a complete cap in $\mathrm{PG}(N,q)$

exact values of $t_2(N,q)$ are known only for small q, N

LOWER BOUND: $t_2(N,q) > \sqrt{2}q^{\frac{N-1}{2}}$

results close to lower bound are known only for even q

$q = 2$, N odd & N even:
E.M. Gabidulin, A.A. Davydov, L.M. Tombak **1991**

$q = 2^h$, N odd: F. Pambianco, L. Storme **1996**; M. Giulietti **2007**
A.A. Davydov, M. Giulietti, S. Marcugini, F. Pambianco **2010**

PROBLEM: UPPER BOUND

$t_2(N,q) \Leftrightarrow$ the smallest size of a complete cap in $\mathrm{PG}(N,q)$

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

upper bound on $t_2(N,q)$

$$t_2(N,q) < cq^{\frac{N-1}{2}} \ln^{300} q$$

c - constant independent of q

D. Bartoli, S. Marcugini, F. Pambianco **ACCT2014** &
http://arxiv.org/pdf/1406.5060.pdf **2014**

probabilistic methods based on J.H. Kim, V. Vu for plane $\mathrm{PG}(2,q)$
2003

directions using computer for combinatorics

EXACT ANSWERS: Extremal and critical (or close to them) values and objects; classification; existence and nonexistence of objects with special properties or parameters; exhaustive search...
Usually this is investigated for relatively small fields and rings.

TRENDS, BOUNDS, ORDER of VALUES ...
This is studied for LARGE REGIONS of sizes of fields and rings.
Results can be represented in graphical forms.
Results are not the best or exact, but the results are "good", reasonable, they show "behavior" of values that we investigate...
This direction is developing in recent years, in particular, due to cluster-computers.

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.

D.Bartoli, A.A.Davydov, G.Faina, A.A.Kreshchuk, S.Marcugini, F.Pambianco
J. of Geometry, Discrete Mathematics, OC2013, arXiv.org **2005-2016**

Greedy algorithms give good results but take many computer time.

For $\mathrm{PG}(N, q)$ greedy algorithms are useful for relatively small q.

Algorithm FOP – fixed order of points

Algorithm FOP. We fix a particular order of points of $\mathrm{PG}(N, q)$. Algorithm FOP builds a complete cap *iteratively*, step-by-step. In the k-th step the first uncovered point in the fixed order is added to the $(k-1)$-cap obtained in the previous step. As the result we have a new k-cap. And so on ...

Lexicographical order of points. q **– prime.** The elements of the field $\mathbb{F}_q = \{0, 1, \ldots, q-1\}$ are integers modulo q. The homogeneous coordinates of a point A_i are treated as its number i written in the q-ary scale of notation: $x_j^{(i)} \in \mathbb{F}_q$,

$$A_i = (x_0^{(i)}, x_1^{(i)}, \ldots, x_N^{(i)}), \quad i = x_0^{(i)} q^N + x_1^{(i)} q^{N-1} + \ldots + x_N^{(i)}$$

FOP with lexicographical order forms LEXICAP.

Size of a complete lexicap in $\mathrm{PG}(N, q)$ is uniquely given by N, q. (unfortunately, we are able to find this size only by computer)

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

Journal of Geometry, ENDM, ACCT2012, OC2013, arXiv **2012-2016**

Region for computer search

FOP-caps $\Leftrightarrow$ Lexicaps. Sets L_N

$\mathrm{PG}(3,q)$ $L_3 = \{$**all prime** $q \le 4673$ **without gaps** & $q = 5003, 6007, 7001, 8009\}$

$\mathrm{PG}(4,q)$ $L_4 = \{$**all prime** $q \le 1301$ **without gaps** & $q = 1409\}$

for greedy algorithms the sets are smaller

$\#\mathrm{PG}(N,q) = q^N + q^{N-1} + \ldots + q + 1$ bit

$\#\mathrm{PG}(3,8009) \approx 60GB$ $\#\mathrm{PG}(4,1409) \approx 460GB$

parallel computations; up two months computer time for big q's

Resources of Multipurpose Computing Complex of National Research Centre "Kurchatov Institute" are used

Forms of bounds

For expressive graphical representation we write $t_2(N, q)$ as follows:

$$t_2(N, q) < q^{\frac{N-1}{2}} \ln^f q$$

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

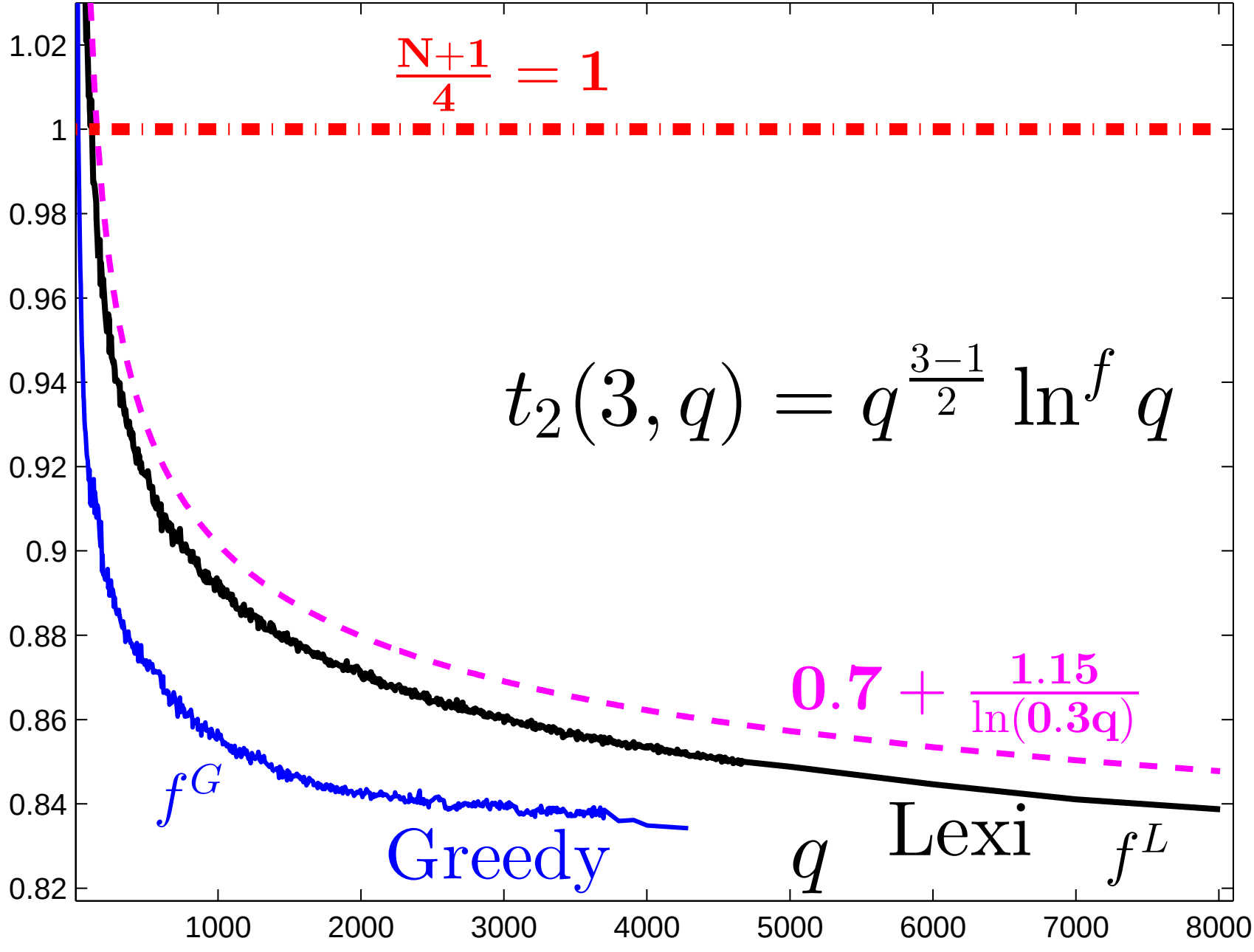
$$t_2(N, q) < d q^{\frac{N-1}{2}} \ln q$$

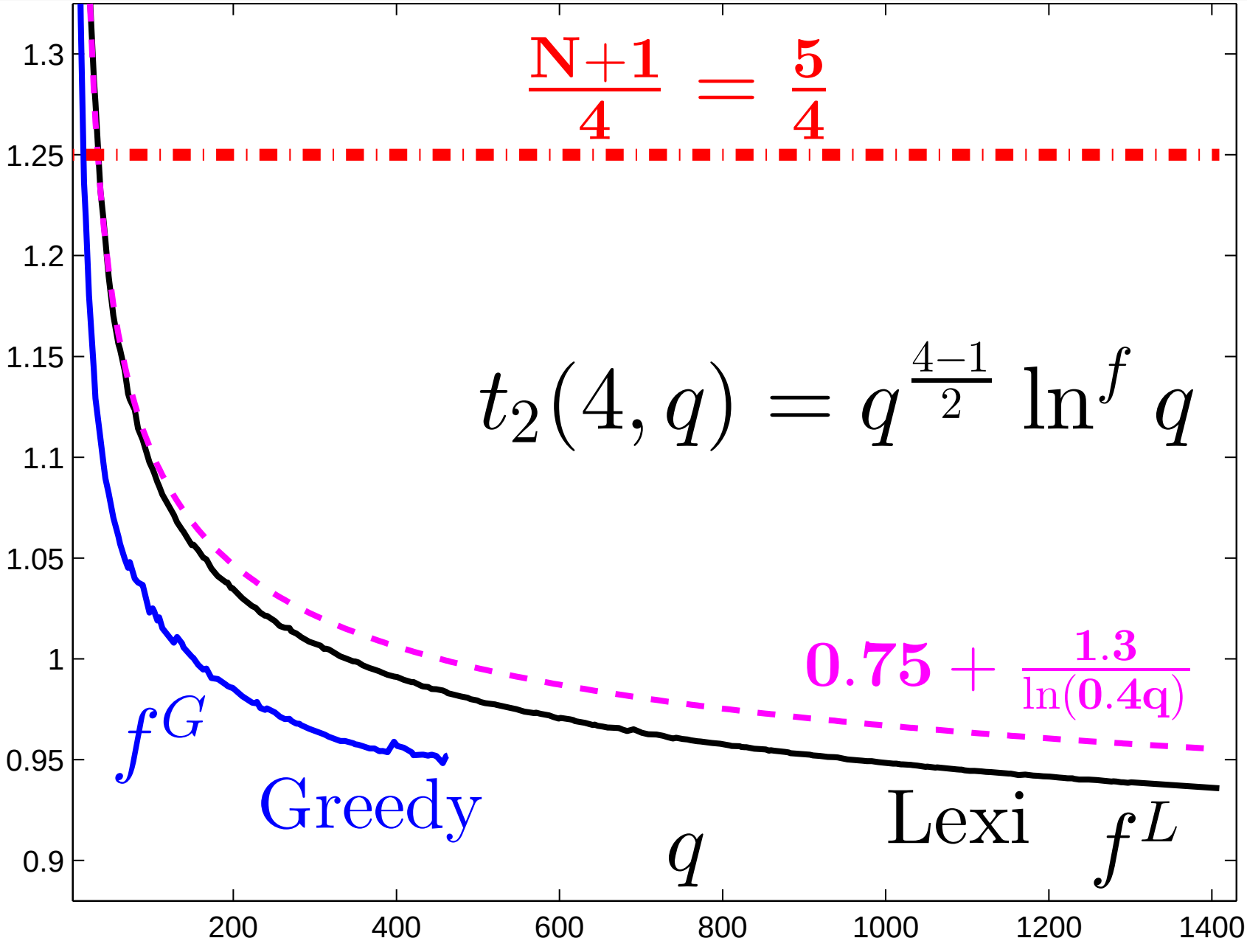
$q^{\frac{N-1}{2}}$ - the main term; $\ln q$ to a small power; β, d small factor

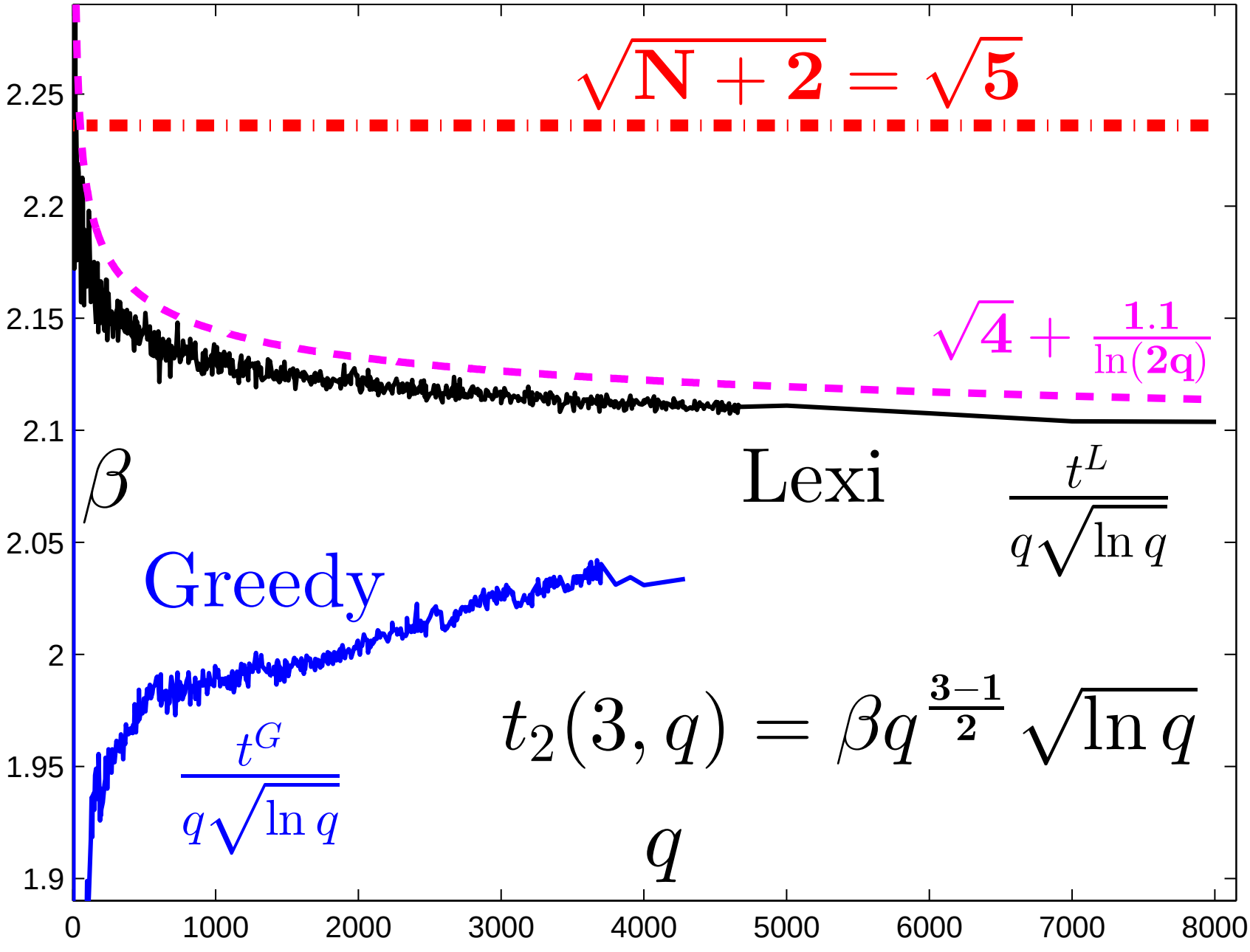
we find upper bounds on f, β, d

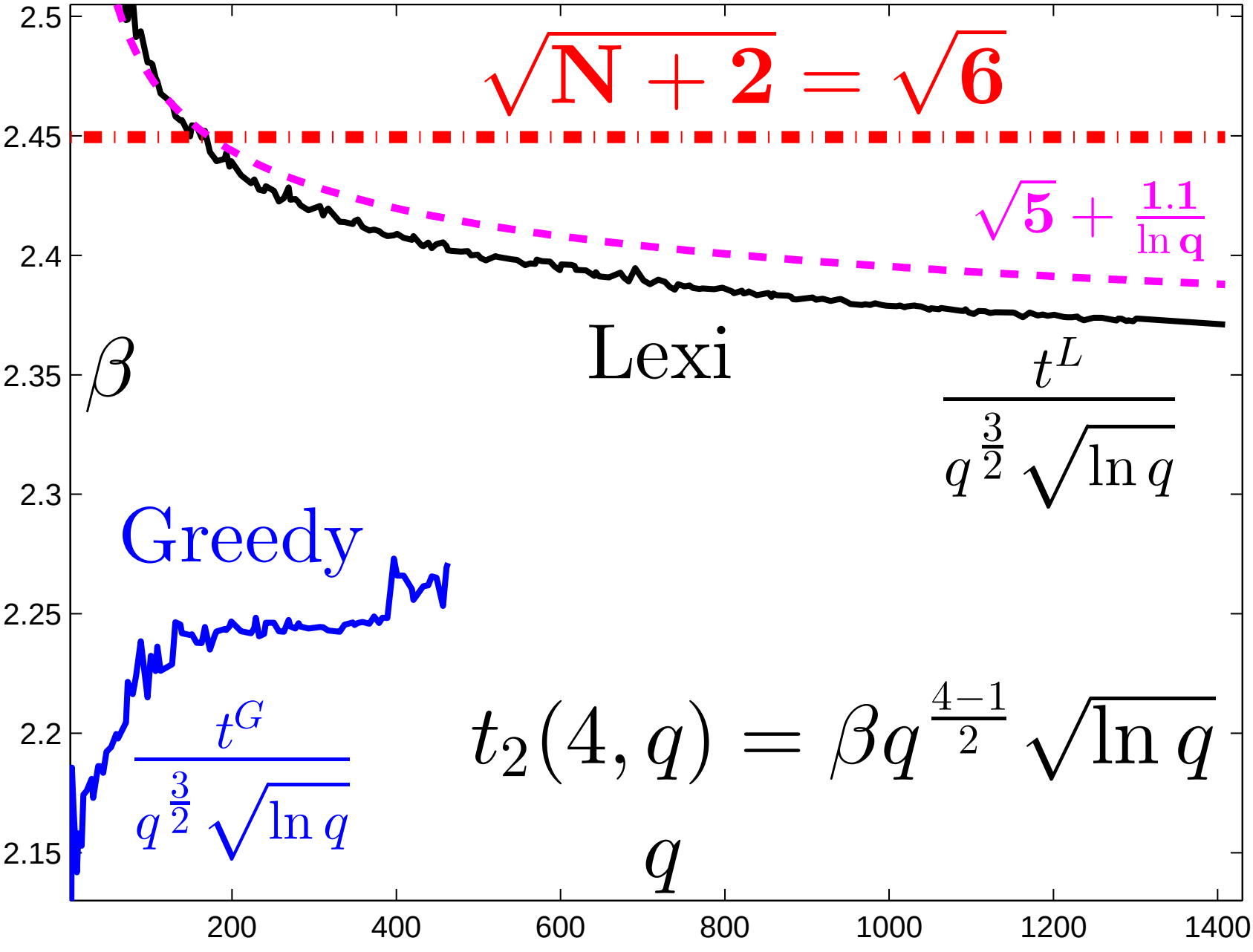
A) f, β, d are constants

B) f, β, d are decreasing functions of q


1.02
1
0.98
0.96
0.94
0.92
0.9
0.88
0.86
0.84
0.82
1000
2000
3000
4000
5000
6000
7000
8000
$\frac{N+1}{4} = 1$
$t_2(3,q) = q^{\frac{3-1}{2}} \ln^f q$
$0.7 + \frac{1.15}{\ln(0.3q)}$
f^G
Greedy
q
Lexi
f^L


$\frac{N+1}{4} = \frac{5}{4}$
$t_2(4,q) = q^{\frac{4-1}{2}} \ln^f q$
$0.75 + \frac{1.3}{\ln(0.4q)}$
f^G
Greedy
Lexi
f^L
q
1.3
1.25
1.2
1.15
1.1
1.05
1
0.95
0.9
200
400
600
800
1000
1200
1400


$\sqrt{N+2} = \sqrt{5}$
$\sqrt{4} + \frac{1.1}{\ln(2q)}$
β
Lexi
$\frac{t^L}{q\sqrt{\ln q}}$
Greedy
$\frac{t^G}{q\sqrt{\ln q}}$
$t_2(3,q) = \beta q^{\frac{3-1}{2}} \sqrt{\ln q}$
q
2.25
2.2
2.15
2.1
2.05
2
1.95
1.9
0
1000
2000
3000
4000
5000
6000
7000
8000


2.5
2.45
2.4
2.35
2.3
2.25
2.2
2.15
200
400
600
800
1000
1200
1400
$\sqrt{N+2} = \sqrt{6}$
$\sqrt{5} + \frac{1.1}{\ln q}$
β
Lexi
$\frac{t^L}{q^{\frac{3}{2}}\sqrt{\ln q}}$
Greedy
$\frac{t^G}{q^{\frac{3}{2}}\sqrt{\ln q}}$
$t_2(4,q) = \beta q^{\frac{4-1}{2}}\sqrt{\ln q}$
q

Analysis of figures

Greedy algorithms provide bounds for small q.

The nature and behavior of the curves for Lexi-caps are similar for $\mathrm{PG}(3, q)$ and $\mathrm{PG}(4, q)$.

The curves for lexicaps have a clearly expressed decreasing trend.

The curves for lexicaps are relatively "smooth".

The curves for lexicaps give us the confidence that bounds with constant parameters hold for all q.

Bounds with decreasing parameters seem to be similar to the truth; but these bounds need additional investigations

Upper bounds with constant parameters. $N = 3, 4$

Theorem

$$t_2(N,q) < q^{\frac{N-1}{2}} \ln^{\frac{N+1}{4}} q, \qquad q \in L_N.$$

$$t_2(N,q) < \frac{N+1}{4} q^{\frac{N-1}{2}} \ln q, \qquad q \in L_N.$$

$$t_2(N,q) < \sqrt{N+2} \cdot q^{\frac{N-1}{2}} \sqrt{\ln q}, \quad q \in L_N.$$

Conjecture. In $\mathrm{PG}(N,q)$, $N = 3, 4$, the bounds with constant parameters written above hold for all q.

Upper bounds with decreasing parameters. $N = 3, 4$

Theorem

$$t_2(N, q) < q^{\frac{N-1}{2}} \ln^{f_N(q)} q, \quad q \in L_N,$$

$$f_3(q) = 0.7 + \frac{1.15}{\ln(0.3q)},$$

$$f_4(q) = 0.75 + \frac{1.3}{\ln(0.4q)};$$

$$t_2(N, q) < \beta_N(q) \cdot q^{\frac{N-1}{2}} \sqrt{\ln q}, q \in L_N,$$

$$\beta_3(q) = \sqrt{3+1} + \frac{1.1}{\ln(2q)},$$

$$\beta_4(q) = \sqrt{4+1} + \frac{1.1}{\ln q}.$$

Thank you Spasibo

Premnogo blagodarya

Mille grazie

!‘Muchas gracias

Toda raba

Merci beaucoup

Dankeschön

Dank u wel

Domo arigato

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 $\mathrm{PG}(N, q) \Leftrightarrow$ a column N-vector.

FOP algorithm creates a PCM of $[n, n-(N+1), 4]_q$ 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 cap.

For $r = N+1, d = 4$, FOP algorithm gives "bad" codes that are essentially shorter than the known "good" codes.