# Fooling-sets and Rank in Nonzero Characteristic


Mirjam Friesen
University of Magdeburg
Germany

Dirk Oliver Theis
University of Tartu
Estonia



UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE


EuroComb'13
Pisa, Sep 9–14, 2013

# What is a fooling-set matrix?

**Definition.**

$M$ $n \times n$-matrix over field $\mathbb{k}$ is called

*fooling-set matrix of size $n$*

if

- $M_{k,k} \neq 0 \quad \forall k$
- $M_{k,\ell} M_{\ell,k} = 0 \quad \forall\, k \neq \ell$

# Why bother about them? — Communication Complexity

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

# Why bother about them? — Communication Complexity

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Communication complexity

- **Given:**
  - Alice & Bob
  - 0/1-matrix $A$ (known to both Alice & Bob)

# Why bother about them? — Communication Complexity

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Communication complexity

- **Given:**
  - Alice & Bob
  - 0/1-matrix $A$ (known to both Alice & Bob)
- Alice only gets a row idx $k$; Bob gets a column idx $\ell$

# Why bother about them? — Communication Complexity

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Communication complexity

- **Given:**
  - Alice & Bob
  - 0/1-matrix $A$ (known to both Alice & Bob)
- Alice only gets a row idx $k$; Bob gets a column idx $\ell$
- Alice & Bob want to output the entry $A_{k,\ell}$

# Why bother about them? — Communication Complexity

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Communication complexity

- **Given:**
  - Alice & Bob
  - 0/1-matrix $A$ (known to both Alice & Bob)
- Alice only gets a row idx $k$; Bob gets a column idx $\ell$
- Alice & Bob want to output the entry $A_{k,\ell}$
- How many bits do they have to exchange for that?

Log of size of a fooling-set sub-matrix in $A$
is a lower bound to the # bits.

# Why bother about them? — Polytope extension problem

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

**Example: Polytope extension problem**

*) The *vertex-facet slack matrix* of the polytope.

# Why bother about them? — Polytope extension problem

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Example: Polytope extension problem

- $P$ a polytope

*) The *vertex-facet slack matrix* of the polytope.

# Why bother about them? — Polytope extension problem

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Example: Polytope extension problem

- $P$ a polytope
- $Q$ another polytope, $\pi$ a projective mapping taking $Q$ *onto* $P$

*) The *vertex-facet slack matrix* of the polytope.

# Why bother about them? — Polytope extension problem

- Find fooling-set sub-matrix in a (larger) matrix $A$
  $\rightsquigarrow$ size is lower bound on properties of $A$.

## Example: Polytope extension problem

- $P$ a polytope
- $Q$ another polytope, $\pi$ a projective mapping taking $Q$ *onto* $P$
- Geometric problem:
  Find such $Q$ with minimum number of facets.

Size of a fooling-set sub-matrix in some matrix* $A(P)$ defined by $P$ is a lower bound to this number.

*) The *vertex-facet slack matrix* of the polytope.

# What's with the rank?

- Have: large matrix $A$

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)
- Are: Lazy! Is that worth all the work?

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)
- Are: Lazy! Is that worth all the work?
- Need: *A priori* upper bound on size of fooling-set sub-matrix.

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)
- Are: Lazy! Is that worth all the work?
- Need: *A priori* upper bound on size of fooling-set sub-matrix.

**Theorem (Dietzfelbinger, Hromkovič, Schnitger 1996).**

$M$ fooling-set matrix.

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, A)^2$$

The ieq holds over every field $\mathbb{k}$.

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)
- Are: Lazy! Is that worth all the work?
- Need: *A priori* upper bound on size of fooling-set sub-matrix.

**Theorem (Dietzfelbinger, Hromkovič, Schnitger 1996).**

$M$ fooling-set matrix.

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, A)^2$$

The ieq holds over every field $\mathbb{k}$.

- Rank of $A$ is often generally known

# What's with the rank?

- Have: large matrix $A$
- Want: large fooling-set sub-matrix
  (its size is lower bound to something)
- Are: Lazy! Is that worth all the work?
- Need: *A priori* upper bound on size of fooling-set sub-matrix.

**Theorem (Dietzfelbinger, Hromkovič, Schnitger 1996).**

$M$ fooling-set matrix.

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, A)^2$$

The ieq holds over every field $\mathbb{k}$.

- Rank of $A$ is often generally known
- If $(\mathrm{rk}\, A)^2$ is good lower bound, go find fooling-set sub-matrix!

# Q: Can the exponent 2 be improved — or not?

**Open Problem (Dietzfelbinger, Hromkovič, Schnitger 1996)**

Can the exponent 2 in the inequality

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, M)^2$$

be improved — or not?

# Our result

**Dietzfelbinger et al. ieq:**

$$n \leq (\mathrm{rk}_{\mathbb{k}} M)^2$$

# Our result

**Dietzfelbinger et al. ieq:**

$$n \leq (\mathrm{rk}_{\mathbb{k}}\, M)^2$$

**Theorem (Friesen & T. 2012+).**

For each prime number $p$, there exists a family $M(t)$ of fooling-set matrices over $\mathbb{k} = \mathbb{F}_p$ of size $n = n(t)$ and rank $r = r(t)$, with $n(t) \to \infty$ as $t \to \infty$, and such that

$$\frac{n(t)}{r(t)^2} \to 1$$

- In short: the inequality $n \leq \left(\mathrm{rk}_{\mathbb{F}_p}\, M\right)^2$ is best possible

# Our result

**Dietzfelbinger et al. ieq:**

$n \leq (\mathrm{rk}_{\mathbb{k}} M)^2$

**Theorem (Friesen & T. 2012+).**

For each prime number $p$, there exists a family $M(t)$ of fooling-set matrices over $\mathbb{k} = \mathbb{F}_p$ of size $n = n(t)$ and rank $r = r(t)$, with $n(t) \to \infty$ as $t \to \infty$, and such that

$$\frac{n(t)}{r(t)^2} \to 1$$

- In short: the inequality $n \leq \left(\mathrm{rk}_{\mathbb{F}_p} M\right)^2$ is best possible
- . . . including the constant (one) inf front of $(\mathrm{rk}\, M)^2$

# Outline

# How to prove this

Easy approach to lower bounds on exponent:

- Find *one* good matrix $M$, e.g.,

$$M := \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & -1 & 0 \\ -1 & 1 & 1 & 0 & -1 & 0 \\ -1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

- It is a fooling-set matrix of size $a = 6$ with rank $b = 3$
- Hence $n \leq \mathrm{rk}^{\log_b a} = \mathrm{rk}^{\log_3 6} = \mathrm{rk}^{1.63\ldots}$
- For an infinite family of matrices: take $M^{\otimes k}$ ($k$-fold tensor product)
  - is a fooling set matrix of size $a^k$
  - with rank $b^k$

# Bounds achieved in this way

| Year | Authors | Exponent |
|---|---|---|
| 1996 | Dietzfelbinger et al. | $\log_3 4 = 1.26\ldots$ |
| 1996 | Hühne | $\log_4 6 = 1.29\ldots$ |
| 2012 | Klauck & de Wolf | $\log_3 6 = 1.63\ldots$ |
| 2013 | Lee | $\log_5 15 = 1.68\ldots$ |

# Outline

# How we proved this

- $p$ prime, $\Bbbk := \mathbb{F}_p$
- $r$ integer $r \geq 2$

We define $f\colon \mathbb{Z} \to \Bbbk$ by linear recurrence relation

- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.

Define $n \times n$ matrix $M$ by

# How we proved this

- $p$ prime, $\Bbbk := \mathbb{F}_p$
- $r$ integer $r \geq 2$

We define $f\colon \mathbb{Z} \to \Bbbk$ by linear recurrence relation

- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.

Define $n \times n$ matrix $M$ by

- $M_{k,\ell} = f(k-\ell)$

# How we proved this

- $p$ prime, $\Bbbk := \mathbb{F}_p$
- $r$ integer $r \geq 2$

We define $f\colon \mathbb{Z} \to \Bbbk$ by linear recurrence relation

- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.

Define $n \times n$ matrix $M$ by

- $M_{k,\ell} = f(k-\ell)$

- We don't yet know how to choose $r$ and $n$.

# The rank

- $p, r, n$ fixed.
- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.
- $M_{k,\ell} = f(k-\ell)$

**Lemma (easy).**

$$\operatorname{rk} M \leq r$$

(In fact, $\operatorname{rk} M = r$ if $n \geq r$.)

# The fooling-set property

- $p, r, n$ fixed.
- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.
- $M_{k,\ell} = f(k-\ell)$

**Trivial:**

$$M_{k,k} = 1 \text{ for } k = 0, \ldots, n-1.$$

# The fooling-set property

- $p, r, n$ fixed.
- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.
- $M_{k,\ell} = f(k-\ell)$

**Trivial:**

$$M_{k,k} = 1 \text{ for } k = 0, \ldots, n-1.$$

**Not trivial:**

$$M_{k,\ell} M_{\ell,k} \stackrel{!}{=} 0 \text{ whenever } k \neq \ell.$$

# Fooling-set property in terms of $f$

- $p, r, n$ fixed.
- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.
- $M_{k,\ell} = f(k-\ell)$

**Lemma (easy).**

$M$ is fooling-set matrix, if and only if,

$$f(k)f(-k) = 0 \quad \text{for all } k \in \{1, \ldots, n-1\}.$$

# Fooling-set property in terms of $f$

- $p, r, n$ fixed.
- $f(k+r) = -f(k) - f(k+1)$ for all $k \in \mathbb{Z}$
- $f(0) = 1$, and $f(1) = \cdots = f(r-1) = 0$.
- $M_{k,\ell} = f(k-\ell)$

**Lemma (easy).**

$M$ is fooling-set matrix, if and only if,

$$f(k)f(-k) = 0 \quad \text{for all } k \in \{1, \ldots, n-1\}.$$

Mini proof.

$M_{k,\ell}M_{\ell,k} = f(k-\ell)f(\ell-k)$

# Main lemma

**Lemma.**

For all integers $t \geq 1$, if we let

- $r := p^t + 1$ and
- $n := r(r-1) + 1$,

then $f(k)f(-k) = 0$ for all $k \in \mathbb{Z} \setminus n\mathbb{Z}$.

This lemma proves the main theorem.

# How to prove the main lemma

**Lemma 1 (Combinatorial part).**

"Something about blocks of zero."

**Lemma 2 (Algebraic part).**

If $r = p^t + 1$ for some integer $t \geq 1$,
then $n := r(r-1) + 1$ is a period of the function $f$.

Finally: Putting together part.

# How to prove the main lemma

**Lemma 1 (Combinatorial part).**

"Something about blocks of zero."

**Lemma 2 (Algebraic part).**

If $r = p^t + 1$ for some integer $t \geq 1$,
then $n := r(r-1) + 1$ is a period of the function $f$.

Proof.

...
Prove that values of $f$ are (more or less) binomials $\binom{r}{j}$. ...

Finally: Putting together part.

# Outlook

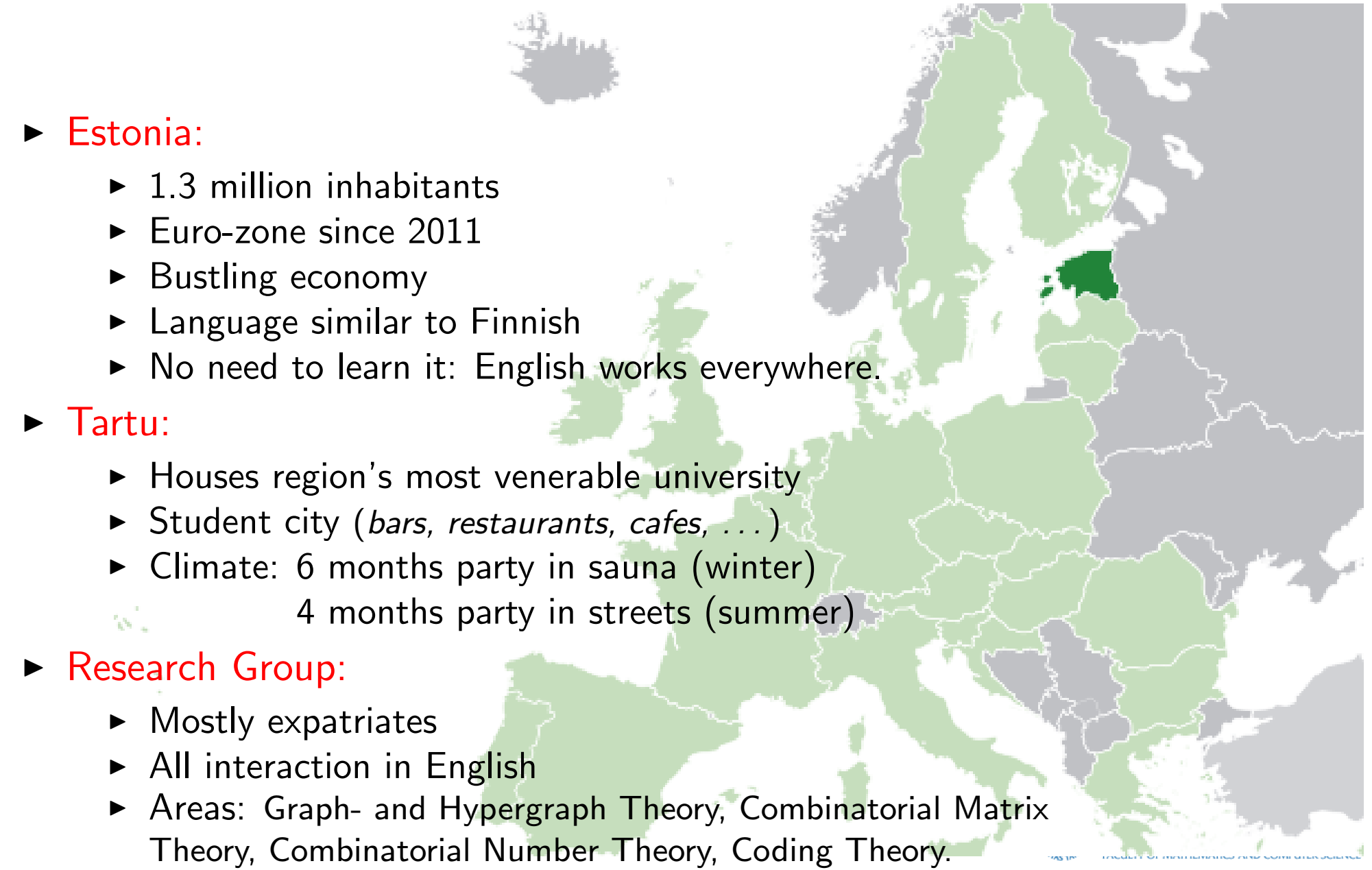
| Field | Entries | Result |
|---|---|---|
| $\chi(\mathbb{k}) = 2$ | $0/1$ | ieq asymptotically best possible |
| $\chi(\mathbb{k}) > 2$ | general | ieq asymptotically best possible |
| $\chi(\mathbb{k}) > 2$ | $0/1$ | ?!?? |
| $\chi(\mathbb{k}) = 0$ | general | up to constant<br>(very recently—will be in full version of paper) |
| $\chi(\mathbb{k}) = 0$ | $0/1$ | ?!?? |
| $\chi(\mathbb{k}) = 0$ | polytope | ?!?? |

**Open problems.**

1. Prove tightness with constant 1 in characteristic 0!
2. Prove tightness for $0/1$ matrices!
3. Prove tightness for matrices defined by polytopes!

# Discrete Math in Tartu

UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE



- Estonia:
  - 1.3 million inhabitants
  - Euro-zone since 2011
  - Bustling economy
  - Language similar to Finnish
  - No need to learn it: English works everywhere.
- Tartu:
  - Houses region's most venerable university
  - Student city (*bars*, *restaurants*, *cafes*, ...)
  - Climate: 6 months party in sauna (winter)
    4 months party in streets (summer)
- Research Group:
  - Mostly expatriates
  - All interaction in English
  - Areas: Graph- and Hypergraph Theory, Combinatorial Matrix Theory, Combinatorial Number Theory, Coding Theory.