

# Group factorisations applied to a Caching Problem

Simon R. Blackburn

Joint work with James F. McKee



31st August 2010

# Overview

- 1  $k$ -radius sequences
- 2 A construction and simple bounds
- 3 Asymptotics of 2-radius sequences
- 4 General values of  $k$
- 5 Tilings and group factorisations
- 6 Logarithms
- 7 Open problems

## An example

A 5-ary 2-radius sequence of length 5 is:

0, 1, 2, 3, 4, 0, 1

## An example

A 5-ary 2-radius sequence of length 5 is:

$$0, 1, 2, 3, 4, 0, 1$$

### Definition (Jaromczyk–Lonc 2004)

Let  $F = \{0, 1, \dots, n - 1\}$ . An  $n$ -ary  $k$ -radius sequence is a finite sequence

$$a_0, a_1, \dots, a_{m-1}$$

over the alphabet  $F$  with the following property:

For all  $x, y \in F$ , there exist  $i, j \in \{0, 1, \dots, m - 1\}$  such that  $a_i = x$ ,  $a_j = y$  and  $|i - j| \leq k$ .

## An application

An 8-ary 3-radius sequence:

0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 4, 5, 6, 3, 7

## An application

An 8-ary 3-radius sequence:

0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 4, 5, 6, 3, 7

### Application

- A cache holds 4 of 8 medical images at one time.
- We want to compute a function that depends on comparing pairs of images.
- We operate a FIFO caching strategy.

## An application

An 8-ary 3-radius sequence:

0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 4, 5, 6, 3, 7

### Application

- A cache holds 4 of 8 medical images at one time.
- We want to compute a function that depends on comparing pairs of images.
- We operate a FIFO caching strategy.

	Time													
Mem. 1	0	4	4	4	4	0	0	0	0	5	5	5	5	
Mem. 2	1	1	5	5	5	5	1	1	1	1	6	6	6	
Mem. 3	2	2	2	6	6	6	6	2	2	2	2	3	3	
Mem. 4	3	3	3	3	7	7	7	7	4	4	4	4	7	

# The main problem

When we hold  $k + 1$  of  $n$  images in cache, we can use an  $n$ -ary  $k$ -radius sequence.

The shorter the length of the sequence, the faster we can compute the function.

# The main problem

When we hold  $k + 1$  of  $n$  images in cache, we can use an  $n$ -ary  $k$ -radius sequence.

The shorter the length of the sequence, the faster we can compute the function.

## Main Question

Let  $f_k(n)$  be the length of the shortest  $n$ -ary  $k$ -radius sequence. What can we say about this function?

# 1-radius sequences

Theorem (Ghosh 1975)

$$f_1(n) = \begin{cases} \binom{n}{2} + 1 & \text{when } n \text{ is odd;} \\ \binom{n}{2} + n/2 & \text{when } n \text{ is even.} \end{cases}$$

## Simple bounds

For fixed  $k$ , the function  $f_k(n)$  grows like  $\binom{n}{2}$ :

### Lemma

*We have*

$$\frac{1}{k} \binom{n}{2} \leq f_k(n) \leq \binom{n}{2} + O(n)$$

## Simple bounds

For fixed  $k$ , the function  $f_k(n)$  grows like  $\binom{n}{2}$ :

### Lemma

We have

$$\frac{1}{k} \binom{n}{2} \leq f_k(n) \leq \binom{n}{2} + O(n)$$

### Proof.

**The upper bound:** A 1-radius sequence is a  $k$ -radius sequence: use Ghosh 1975.

## Simple bounds

For fixed  $k$ , the function  $f_k(n)$  grows like  $\binom{n}{2}$ :

### Lemma

We have

$$\frac{1}{k} \binom{n}{2} \leq f_k(n) \leq \binom{n}{2} + O(n)$$

### Proof.

**The upper bound:** A 1-radius sequence is a  $k$ -radius sequence: use Ghosh 1975.

**The lower bound:** There are less than  $kf_k(n)$  pairs  $\{a_i, a_{i+\delta}\}$  where  $1 \leq \delta \leq k$ . They must cover all  $\binom{n}{2}$  subsets of  $F$  of size 2. □

## A construction

Assume the alphabet size is prime:  $n = p$ . So  $F = \mathbb{Z}_p$ .

## A construction

Assume the alphabet size is prime:  $n = p$ . So  $F = \mathbb{Z}_p$ .

Define, for  $d \in \mathbb{Z}_p^*$ ,

$$\mathbf{t}_d = 0, d, 2d, 3d, \dots, (p-1)d, 0, d, \dots, (k-1)d.$$

## A construction

Assume the alphabet size is prime:  $n = p$ . So  $F = \mathbb{Z}_p$ .

Define, for  $d \in \mathbb{Z}_p^*$ ,

$$\mathbf{t}_d = 0, d, 2d, 3d, \dots, (p-1)d, 0, d, \dots, (k-1)d.$$

Distinct  $x, y \in F$  occur within a distance  $k$  of each other in  $\mathbf{t}_d$  whenever

$$x - y \in \{\pm d, \pm 2d, \pm 3d, \dots, \pm kd\} = d \cdot \pm[1, k].$$

## A construction

Let  $D \subseteq \mathbb{Z}_p^*$  be such that

$$\mathbb{Z}_p^* = \bigcup_{d \in D} d \cdot \pm[1, k].$$

## A construction

Let  $D \subseteq \mathbb{Z}_p^*$  be such that

$$\mathbb{Z}_p^* = \bigcup_{d \in D} d \cdot \pm[1, k].$$

### Theorem

*There exists a  $p$ -ary  $k$ -radius sequence of length  $|D|(p + k)$*

## A construction

Let  $D \subseteq \mathbb{Z}_p^*$  be such that

$$\mathbb{Z}_p^* = \bigcup_{d \in D} d \cdot \pm[1, k].$$

### Theorem

*There exists a  $p$ -ary  $k$ -radius sequence of length  $|D|(p + k)$*

### Proof.

Concatenate the sequences  $\mathbf{t}_d$  where  $d \in D$ . □

## A construction

Let  $D \subseteq \mathbb{Z}_p^*$  be such that

$$\mathbb{Z}_p^* = \bigcup_{d \in D} d \cdot \pm[1, k].$$

### Theorem

*There exists a  $p$ -ary  $k$ -radius sequence of length  $|D|(p + k)$*

### Proof.

Concatenate the sequences  $\mathbf{t}_d$  where  $d \in D$ . □

**Remark:** Can easily improve the length to  $|D|(p + k - 1) + 1$ .

# Coverings and group factorisations

## Goal

Construct good coverings of  $\mathbb{Z}_p^*$  by sets of the form  $d \cdot \pm[1, k]$ .

# Coverings and group factorisations

## Goal

Construct good coverings of  $\mathbb{Z}_p^*$  by sets of the form  $d \cdot \pm[1, k]$ .

## Ideal situation

Find a group factorisation  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .

# Coverings and group factorisations

## Goal

Construct good coverings of  $\mathbb{Z}_p^*$  by sets of the form  $d \cdot \pm[1, k]$ .

## Ideal situation

Find a group factorisation  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .

Then  $|D| = (p-1)/2k$  and

$$f_k(p) = |D|(p+k) = \frac{(p+k)(p-1)}{2k} = \frac{1}{k} \binom{p}{2} + O(p).$$

## A good covering

Consider  $k = 2$ . Suppose that  $p \equiv 5 \pmod{8}$ .

## A good covering

Consider  $k = 2$ . Suppose that  $p \equiv 5 \pmod{8}$ .

The order  $\ell$  of 2 in  $\mathbb{Z}_p^*$  is divisible by 4, so  $2^{\ell/2} = -1$ .

## A good covering

Consider  $k = 2$ . Suppose that  $p \equiv 5 \pmod{8}$ .

The order  $\ell$  of 2 in  $\mathbb{Z}_p^*$  is divisible by 4, so  $2^{\ell/2} = -1$ .

Write  $S = \{2^0, 2^2, 2^4, 2^6, \dots, 2^{\ell/2-2}\}$ . Then  $\langle 2 \rangle = S \cdot \pm[1, 2]$ .

## A good covering

Consider  $k = 2$ . Suppose that  $p \equiv 5 \pmod{8}$ .

The order  $\ell$  of 2 in  $\mathbb{Z}_p^*$  is divisible by 4, so  $2^{\ell/2} = -1$ .

Write  $S = \{2^0, 2^2, 2^4, 2^6, \dots, 2^{\ell/2-2}\}$ . Then  $\langle 2 \rangle = S \cdot \pm[1, 2]$ .

Write

$$\mathbb{Z}_p^* = C_1 \cup C_2 \cup \dots \cup C_{(p-1)/\ell}$$

where  $C_i = c_i \langle 2 \rangle$ .

## A good covering

Consider  $k = 2$ . Suppose that  $p \equiv 5 \pmod{8}$ .

The order  $\ell$  of 2 in  $\mathbb{Z}_p^*$  is divisible by 4, so  $2^{\ell/2} = -1$ .

Write  $S = \{2^0, 2^2, 2^4, 2^6, \dots, 2^{\ell/2-2}\}$ . Then  $\langle 2 \rangle = S \cdot \pm[1, 2]$ .

Write

$$\mathbb{Z}_p^* = C_1 \cup C_2 \cup \dots \cup C_{(p-1)/\ell}$$

where  $C_i = c_i \langle 2 \rangle$ .

Define

$$D = \bigcup_{i \in [1, (p-1)/\ell]} c_i S$$

Then  $D \cdot \pm[1, 2]$  is a group factorisation.

## 2-radius sequences

### Theorem

$$f_2(n) = \frac{1}{2} \binom{n}{2} + O(n^{1.525}).$$

## 2-radius sequences

### Theorem

$$f_2(n) = \frac{1}{2} \binom{n}{2} + O(n^{1.525}).$$

### Proof.

For all sufficiently large  $n$ , there is a prime  $p \equiv 5 \pmod{8}$  with  $n \leq p \leq n + n^{0.525}$ .

## 2-radius sequences

### Theorem

$$f_2(n) = \frac{1}{2} \binom{n}{2} + O(n^{1.525}).$$

### Proof.

For all sufficiently large  $n$ , there is a prime  $p \equiv 5 \pmod{8}$  with  $n \leq p \leq n + n^{0.525}$ . Our group factorisation shows

$$f_2(n) \leq f_2(p) \leq \frac{1}{2} \binom{p}{2} + O(p) = \frac{1}{2} \binom{n}{2} + O(n^{1.525}).$$



## Generalising to other values of $k$

- We can restrict to alphabets of size  $p$  (with mild restrictions on  $p$ ).

## Generalising to other values of $k$

- We can restrict to alphabets of size  $p$  (with mild restrictions on  $p$ ).
- It is sufficient to construct (small) sets  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .

## Generalising to other values of $k$

- We can restrict to alphabets of size  $p$  (with mild restrictions on  $p$ ).
- It is sufficient to construct (small) sets  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .
- Suppose  $-1 \notin \langle 2, 3, \dots, k \rangle$  (true under a mild restriction on  $p$ ):
  - ▶ If we can construct a small cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$ , then  $E \cdot \pm[1, k]$  is a small cover for  $\langle -1, 2, 3, \dots, k \rangle$ .

## Generalising to other values of $k$

- We can restrict to alphabets of size  $p$  (with mild restrictions on  $p$ ).
- It is sufficient to construct (small) sets  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .
- Suppose  $-1 \notin \langle 2, 3, \dots, k \rangle$  (true under a mild restriction on  $p$ ):
  - ▶ If we can construct a small cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$ , then  $E \cdot \pm[1, k]$  is a small cover for  $\langle -1, 2, 3, \dots, k \rangle$ .
  - ▶ Then we can construct  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .

## Generalising to other values of $k$

- We can restrict to alphabets of size  $p$  (with mild restrictions on  $p$ ).
- It is sufficient to construct (small) sets  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .
- Suppose  $-1 \notin \langle 2, 3, \dots, k \rangle$  (true under a mild restriction on  $p$ ):
  - ▶ If we can construct a small cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$ , then  $E \cdot \pm[1, k]$  is a small cover for  $\langle -1, 2, 3, \dots, k \rangle$ .
  - ▶ Then we can construct  $D$  such that  $\mathbb{Z}_p^* = D \cdot \pm[1, k]$ .
- So we need to construct small covers of  $\langle 2, 3, \dots, k \rangle \subset \mathbb{Z}_p^*$  using sets of the form  $d \cdot [1, k]$ .

## Covers of $\langle 2, 3, \dots, k \rangle$

### Problem

We do not know much about  $\langle 2, 3, \dots, k \rangle$ .

## Covers of $\langle 2, 3, \dots, k \rangle$

### Problem

We do not know much about  $\langle 2, 3, \dots, k \rangle$ .

Let  $r = \pi(k)$  and let  $p_1, p_2, \dots, p_r$  be the primes in  $[1, k]$ .

We know that  $\langle 2, 3, \dots, k \rangle$  is generated by  $p_1, p_2, \dots, p_r$ .

## Covers of $\langle 2, 3, \dots, k \rangle$

### Problem

We do not know much about  $\langle 2, 3, \dots, k \rangle$ .

Let  $r = \pi(k)$  and let  $p_1, p_2, \dots, p_r$  be the primes in  $[1, k]$ .

We know that  $\langle 2, 3, \dots, k \rangle$  is generated by  $p_1, p_2, \dots, p_r$ .

So  $\langle 2, 3, \dots, k \rangle$  is a quotient of  $\mathbb{Z}^r$  by some lattice (i.e. subgroup)  $L$ .

Let  $\phi : \mathbb{Z}^r \rightarrow \langle 2, 3, \dots, k \rangle$  be the natural homomorphism. Then

$$\phi(i_1, i_2, \dots, i_r) = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r} \bmod p$$

(and  $L$  is the kernel of  $\phi$ ).

## Covers of $\langle 2, 3, \dots, k \rangle$

### Problem

We do not know much about  $\langle 2, 3, \dots, k \rangle$ .

Let  $r = \pi(k)$  and let  $p_1, p_2, \dots, p_r$  be the primes in  $[1, k]$ .

We know that  $\langle 2, 3, \dots, k \rangle$  is generated by  $p_1, p_2, \dots, p_r$ .

So  $\langle 2, 3, \dots, k \rangle$  is a quotient of  $\mathbb{Z}^r$  by some lattice (i.e. subgroup)  $L$ .

Let  $\phi : \mathbb{Z}^r \rightarrow \langle 2, 3, \dots, k \rangle$  be the natural homomorphism. Then

$$\phi(i_1, i_2, \dots, i_r) = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r} \bmod p$$

(and  $L$  is the kernel of  $\phi$ ).

Define  $\mathcal{C}_k \subseteq \mathbb{Z}^r$  by

$$\mathcal{C}_k = \{(i_1, i_2, \dots, i_r) \mid p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r} \in [1, k]\}.$$

Then  $|\mathcal{C}_k| = k$  and  $\phi(\mathcal{C}_k) = [1, k] \bmod p$ .

## Group factorisations (tilings) of $\mathbb{Z}^r$

### Idea

If a group factorisation  $T + C_k$  of  $\mathbb{Z}^r$  exists, we always have a good cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$  (for *any*  $p$ ).

## Group factorisations (tilings) of $\mathbb{Z}^r$

### Idea

If a group factorisation  $T + C_k$  of  $\mathbb{Z}^r$  exists, we always have a good cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$  (for *any*  $p$ ).

Example:  $k = 4$ . So  $r = 2$ ,  $p_1 = 2$ ,  $p_2 = 3$  and  $C_4 = \{(0, 0), (1, 0), (0, 1), (2, 0)\}$ .

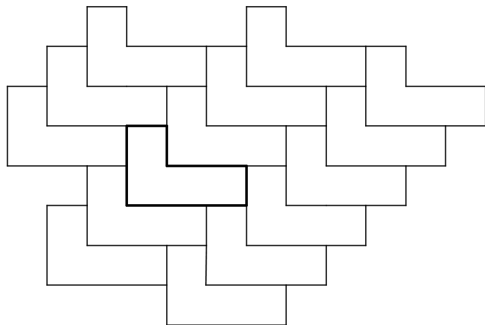
# Group factorisations (tilings) of $\mathbb{Z}^r$

## Idea

If a group factorisation  $T + \mathcal{C}_k$  of  $\mathbb{Z}^r$  exists, we always have a good cover  $E \cdot [1, k]$  for  $\langle 2, 3, \dots, k \rangle$  (for any  $p$ ).

Example:  $k = 4$ . So  $r = 2$ ,  $p_1 = 2$ ,  $p_2 = 3$  and  $\mathcal{C}_4 = \{(0, 0), (1, 0), (0, 1), (2, 0)\}$ .

We can take  $T = \{a(4, 0) + b(1, 1) \mid a, b \in \mathbb{Z}\}$ .



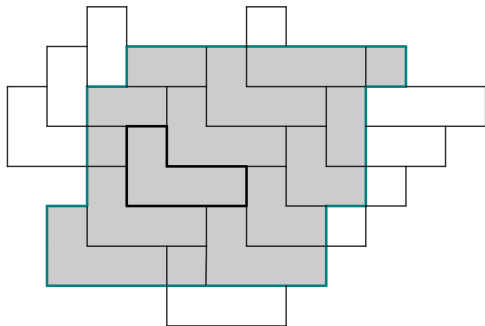
## Constructing covers of $\langle 2, 3, \dots, k \rangle$

Recall:  $\langle 2, 3, \dots, k \rangle$  is the quotient of  $\mathbb{Z}^r$  by a lattice  $L$ .

## Constructing covers of $\langle 2, 3, \dots, k \rangle$

Recall:  $\langle 2, 3, \dots, k \rangle$  is the quotient of  $\mathbb{Z}^r$  by a lattice  $L$ .

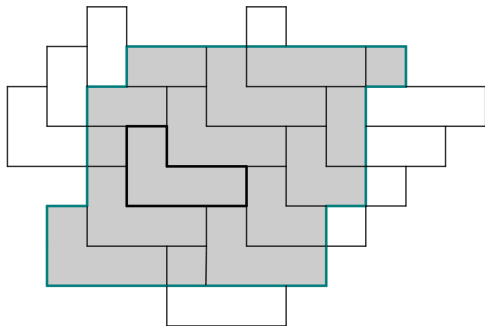
Choose a fundamental region for  $L$ :



## Constructing covers of $\langle 2, 3, \dots, k \rangle$

Recall:  $\langle 2, 3, \dots, k \rangle$  is the quotient of  $\mathbb{Z}^r$  by a lattice  $L$ .

Choose a fundamental region for  $L$ :



The images under  $\phi$  of the tiles intersecting the fundamental region form a covering  $E \cdot [1, k]$  of  $\langle 2, 3, \dots, k \rangle$ .

# The main theorem

- $E$  is not quite a group factorisation: some overlapping at the boundary of fundamental region.
- So choose a fundamental region that has small surface when compared to its volume (use LLL).

# The main theorem

- $E$  is not quite a group factorisation: some overlapping at the boundary of fundamental region.
- So choose a fundamental region that has small surface when compared to its volume (use LLL).

## Theorem

Suppose there exists a tiling  $T$  of  $\mathbb{Z}^r$  by  $C_k$ . Then

$$f_k(n) = \frac{1}{k} \binom{n}{2} + O(n^2 / \log n).$$

# The main theorem

- $E$  is not quite a group factorisation: some overlapping at the boundary of fundamental region.
- So choose a fundamental region that has small surface when compared to its volume (use LLL).

## Theorem

Suppose there exists a tiling  $T$  of  $\mathbb{Z}^r$  by  $C_k$ . Then

$$f_k(n) = \frac{1}{k} \binom{n}{2} + O(n^2 / \log n).$$

When do tilings of  $\mathbb{Z}^r$  by  $C_k$  exist?

# Logarithms

## Definition (Galovich and Stein, 1981)

A **logarithm of length  $k$**  is a bijection  $f : [1, k] \rightarrow \mathbb{Z}_k$  such that for all  $a, b \in [1, k]$

$$f(ab) = f(a) + f(b) \pmod k$$

whenever this makes sense (so whenever  $ab \in [1, k]$ ).

# Logarithms

## Definition (Galovich and Stein, 1981)

A **logarithm of length  $k$**  is a bijection  $f : [1, k] \rightarrow \mathbb{Z}_k$  such that for all  $a, b \in [1, k]$

$$f(ab) = f(a) + f(b) \pmod k$$

whenever this makes sense (so whenever  $ab \in [1, k]$ ).

## Example

Suppose  $k + 1$  is prime, and let  $\alpha$  be a primitive root modulo  $k + 1$ . The 'discrete logarithm' map  $f$  is a logarithm, where  $f$  maps  $i \in [1, k]$  to the unique  $x \in \mathbb{Z}_k$  such that  $i = \alpha^x$ .

## When do tilings of $\mathbb{Z}^r$ by $C_k$ exist?

### Theorem

*If a logarithm of length  $k$  exists, then a tiling of  $\mathbb{Z}^r$  by  $C_k$  exists.*

## When do tilings of $\mathbb{Z}^r$ by $C_k$ exist?

### Theorem

*If a logarithm of length  $k$  exists, then a tiling of  $\mathbb{Z}^r$  by  $C_k$  exists.*

### Proof.

$T$  is the kernel of the map  $\phi : \mathbb{Z}^r \rightarrow \mathbb{Z}_k$  given by

$$\phi(i_1, i_1, \dots, i_r) = i_1 f(p_1) + i_2 f(p_2) + \dots + i_r f(p_r).$$



## When do tilings of $\mathbb{Z}^r$ by $C_k$ exist?

### Theorem

*If a logarithm of length  $k$  exists, then a tiling of  $\mathbb{Z}^r$  by  $C_k$  exists.*

### Proof.

$T$  is the kernel of the map  $\phi : \mathbb{Z}^r \rightarrow \mathbb{Z}_k$  given by

$$\phi(i_1, i_1, \dots, i_r) = i_1 f(p_1) + i_2 f(p_2) + \dots + i_r f(p_r).$$



### Corollary

*If a logarithm of length  $k$  exists, then*

$$f_k(n) = \frac{1}{k} \binom{n}{2} + O(n^2 / \log n).$$

## A better error term

### Definition

Let  $f$  be a logarithm of length  $k$ . Then  $f$  is a **KM-logarithm** if there exists a prime  $p$  and a primitive  $k$ -th root  $\alpha \bmod p$  such that

$$x^{(p-1)/k} = \alpha^{f(x)} \bmod p$$

for all  $x \in \mathbb{Z}_p^*$ .

# A better error term

## Definition

Let  $f$  be a logarithm of length  $k$ . Then  $f$  is a **KM-logarithm** if there exists a prime  $p$  and a primitive  $k$ -th root  $\alpha \bmod p$  such that

$$x^{(p-1)/k} = \alpha^{f(x)} \bmod p$$

for all  $x \in \mathbb{Z}_p^*$ .

A KM-logarithm  $f$  is **special** if (i)  $k$  is odd, or (ii)  $k$  is even and  $f(x)$  is even whenever  $x$  divides  $k/2$ .

## A better error term

### Definition

Let  $f$  be a logarithm of length  $k$ . Then  $f$  is a **KM-logarithm** if there exists a prime  $p$  and a primitive  $k$ -th root  $\alpha \bmod p$  such that

$$x^{(p-1)/k} = \alpha^{f(x)} \bmod p$$

for all  $x \in \mathbb{Z}_p^*$ .

A KM-logarithm  $f$  is **special** if (i)  $k$  is odd, or (ii)  $k$  is even and  $f(x)$  is even whenever  $x$  divides  $k/2$ .

### Corollary

*If a special KM-logarithm of length  $k$  exists, then*

$$f_k(n) = \frac{1}{k} \binom{n}{2} + O(n^2 \log n \exp(-a_k \sqrt{\log n}))$$

*where  $a_k$  is a positive constant.*

# Computational results on logarithms

Logarithms of length  $k$  exist when  $k + 1$  is prime, and when  $2k + 1$  is prime.

Forcade and Pollington (1990), motivated by a problem in number theory, showed that logarithms of length  $k$  exist for all  $k \leq 194$ , but no logarithm of length 195 exists.

# Computational results on logarithms

Logarithms of length  $k$  exist when  $k + 1$  is prime, and when  $2k + 1$  is prime.

Forcade and Pollington (1990), motivated by a problem in number theory, showed that logarithms of length  $k$  exist for all  $k \leq 194$ , but no logarithm of length 195 exists.

The values of  $k$  with  $k \leq 300$  with no logarithm of length  $k$  are:

195, 205, 208, 211, 212, 214, 217, 218, 220, 227, 229, 235, 242, 244, 246, 247, 248, 252, 253, 255, 257, 258, 259, 263, 264, 265, 266, 267, 269, 271, 274, 275, 279, 283, 286, 287, 289, 290, 291, 294, 295, 297, 298

## Computational results on logarithms

Logarithms of length  $k$  exist when  $k + 1$  is prime, and when  $2k + 1$  is prime.

Forcade and Pollington (1990), motivated by a problem in number theory, showed that logarithms of length  $k$  exist for all  $k \leq 194$ , but no logarithm of length 195 exists.

The values of  $k$  with  $k \leq 300$  with no logarithm of length  $k$  are:

195, 205, 208, 211, 212, 214, 217, 218, 220, 227, 229, 235, 242, 244, 246, 247, 248, 252, 253, 255, 257, 258, 259, 263, 264, 265, 266, 267, 269, 271, 274, 275, 279, 283, 286, 287, 289, 290, 291, 294, 295, 297, 298

There is no special KM-logarithm for  $k = 4, 12, 60, 180, 182, 184, 190, 196, 222, 234, 236, 238, 268, 276, 282, 292$ .

## Open problems

- Determine  $\lim f_k(n)/\binom{n}{2}$  (if this limit exists). We know that

$$\frac{1}{k} \leq f_k(n)/\binom{n}{2} \leq \frac{1}{k + o(k)}$$

for all sufficiently large  $n$ .

## Open problems

- Determine  $\lim f_k(n)/\binom{n}{2}$  (if this limit exists). We know that

$$\frac{1}{k} \leq f_k(n)/\binom{n}{2} \leq \frac{1}{k + o(k)}$$

for all sufficiently large  $n$ .

- In particular, what is the behaviour of  $f_{195}(n)$ ?

## Open problems

- Determine  $\lim f_k(n)/\binom{n}{2}$  (if this limit exists). We know that

$$\frac{1}{k} \leq f_k(n)/\binom{n}{2} \leq \frac{1}{k + o(k)}$$

for all sufficiently large  $n$ .

- In particular, what is the behaviour of  $f_{195}(n)$ ?
- Are there tilings of  $\mathbb{Z}^r$  by  $\mathcal{C}_k$  when no logarithms of length  $k$  exist? If not, do there exist good coverings?

## Open problems

- Determine  $\lim f_k(n)/\binom{n}{2}$  (if this limit exists). We know that

$$\frac{1}{k} \leq f_k(n)/\binom{n}{2} \leq \frac{1}{k + o(k)}$$

for all sufficiently large  $n$ .

- In particular, what is the behaviour of  $f_{195}(n)$ ?
- Are there tilings of  $\mathbb{Z}^r$  by  $\mathcal{C}_k$  when no logarithms of length  $k$  exist? If not, do there exist good coverings?
- For which  $k$  do logarithms of length  $k$  exist? Is it the case that they exist only when  $k + 1$  or  $2k + 1$  is prime, when  $k$  is sufficiently large?

## Open problems

- Determine  $\lim f_k(n)/\binom{n}{2}$  (if this limit exists). We know that

$$\frac{1}{k} \leq f_k(n)/\binom{n}{2} \leq \frac{1}{k + o(k)}$$

for all sufficiently large  $n$ .

- In particular, what is the behaviour of  $f_{195}(n)$ ?
- Are there tilings of  $\mathbb{Z}^r$  by  $\mathcal{C}_k$  when no logarithms of length  $k$  exist? If not, do there exist good coverings?
- For which  $k$  do logarithms of length  $k$  exist? Is it the case that they exist only when  $k + 1$  or  $2k + 1$  is prime, when  $k$  is sufficiently large?
- Are there other ways of constructing good  $k$ -radius sequences?

## Some Links

This talk will appear soon on my home page:

<http://www.ma.rhul.ac.uk/sblackburn>

S.R. Blackburn and J.F. McKee, 'Constructing  $k$ -radius sequences' is available at:

<http://arxiv.org/abs/1006.5812>