k-radius Sequences

Simon R. Blackburn

Joint work with James F. McKee

16th February 2011

Overview

An example

A 5-ary 2-radius sequence of length 7 is:

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

An example

A 5-ary 2-radius sequence of length 7 is:

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

Definition (Jaromczyk–Lonc 2004)

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

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

over the alphabet F with the following property:
For all $x, y \in F$, there exist $i, j \in \{0, 1, \ldots, m-1\}$ 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 cache replacement policy.

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 cache replacement policy.

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?

What if we don't use a FIFO cache replacement policy?

What if we don't use a FIFO cache replacement policy?

A good technique:

- Load the first k images into cache.
- In the final position, load all the remaining images in turn.
- Load the next k images into cache.
- In the final postion, load the later images in turn.
- ...

What if we don't use a FIFO cache replacement policy?

A good technique:

- Load the first k images into cache.
- In the final position, load all the remaining images in turn.
- Load the next k images into cache.
- In the final postion, load the later images in turn.
- ...

All pairs occur in cache at some time. The total time required is

$$\approx \sum_{i=1}^{n/k}(k+n-ki) = \frac{1}{k}\binom{n}{2} + O(n).$$

What if we don't use a FIFO cache replacement policy?

A good technique:

- Load the first k images into cache.
- In the final position, load all the remaining images in turn.
- Load the next k images into cache.
- In the final postion, load the later images in turn.
- ...

All pairs occur in cache at some time. The total time required is

$$\approx \sum_{i=1}^{n/k}(k+n-ki) = \frac{1}{k}\binom{n}{2} + O(n).$$

Essentially best possible: at most k new pairs 'covered' with each new caching.

1-radius sequences

Theorem (Ghosh 1975)

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

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

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

A construction

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

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

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

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

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

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

Goal

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

Coverings

Goal

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

When $k = 2$: easy to construct optimal coverings when $p \equiv 5 \mod 8$.

Coverings

Goal

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

When $k = 2$: easy to construct optimal coverings when $p \equiv 5 \bmod 8$.

Theorem

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

Coverings

Goal

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

When $k = 2$: easy to construct optimal coverings when $p \equiv 5 \bmod 8$.

Theorem

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

Proof.

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

Coverings

Goal

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

When $k = 2$: easy to construct optimal coverings when $p \equiv 5 \bmod 8$.

Theorem

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

Proof.

For all sufficiently large n, there is a prime $p \equiv 5 \bmod 8$ with $n \leq p \leq n + n^{0.525}$. Our optimal covering 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 $\mathbb{Z}_p^* = D \cdot \pm[1, k]$.
- Problem: we don't know much about $\langle 2, 3, \ldots, k \rangle$.

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 $\mathbb{Z}_p^* = D \cdot \pm[1, k]$.
- Problem: we don't know much about $\langle 2, 3, \ldots, k \rangle$.
- Solution: construct tilings of $\mathbb{Z}^r$, where $r = \pi(k)$.

Logarithms

Definition (Galovich and Stein, 1981)

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

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

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

Logarithms

Definition (Galovich and Stein, 1981)

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

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

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

Example

Suppose $k + 1$ is prime, and let α 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 $i = \alpha^x$.

Finding suitable tilings of $\mathbb{Z}^r$

Theorem

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

Finding suitable tilings of $\mathbb{Z}^r$

Theorem

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

Corollary

If a logarithm of length k exists, then

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

Finding suitable tilings of $\mathbb{Z}^r$

Theorem

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

Corollary

If a logarithm of length k exists, then

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

Remark: We can get a better error term when a logarithm with an extra property 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.

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

No explicit constructions of good k-radius sequences are known for these values. Can probabilistic methods help?

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- The hypergraph (V, E) is *r-uniform* if all hyperedges have cardinality r.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- The hypergraph (V, E) is r-uniform if all hyperedges have cardinality r.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- The hypergraph (V, E) is r-uniform if all hyperedges have cardinality r.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$.

Hypergraphs

Let V be a set of vertices, and E be a set of hyperedges.

- The hypergraph (V, E) is r-uniform if all hyperedges have cardinality r.
- The degree $\deg(v)$ of a vertex v is the number of hyperedges containing v.
- The hypergraph (V, E) is d-regular if $\deg(v) = d$ for all $v \in V$.
- The codegree $\mathrm{codeg}(u, v)$ of a pair of vertices is the number of hyperedges containing both u and v.

The Rödl Nibble

Suppose we have a large r-uniform d-regular hypergraph Γ. Suppose the codegree of a pair of vertices is always much smaller than d. Then there is a covering of the vertices by hyperedges that is about as small as we could hope for (about $|V|/r$ hyperedges).

The Rödl Nibble

Suppose we have a large r-uniform d-regular hypergraph Γ. Suppose the codegree of a pair of vertices is always much smaller than d. Then there is a covering of the vertices by hyperedges that is about as small as we could hope for (about $|V|/r$ hyperedges).

Theorem

Fix an integer r and a positive real number δ. Then there exists an integer n_0 and a positive real number δ' with the following property.
Let Γ be an r-uniform hypergraph on n vertices, where $n \geq n_0$. Suppose that all vertices of Γ have degree d for some integer d. Let $c = \max \mathrm{codeg}(u, v)$, where the maximum is taken over all pairs of distinct vertices $u, v \in \Gamma$. If $c \leq \delta' d$, then there exists a hyperedge cover consisting of at most $(1 + \delta)n/r$ hyperedges.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.
Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.

Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^{\ell}$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- Γ is r-uniform, where $r = r(\ell, k)$ is fixed.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.

Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- Γ is r-uniform, where $r = r(\ell, k)$ is fixed.
- When ℓ is big, $r \approx \ell k$.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.

Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- Γ is r-uniform, where $r = r(\ell, k)$ is fixed.
- When ℓ is big, $r \approx \ell k$.
- Γ is d-regular, where d is of the order of $n^{\ell-2}$.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.

Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- Γ is r-uniform, where $r = r(\ell, k)$ is fixed.
- When ℓ is big, $r \approx \ell k$.
- Γ is d-regular, where d is of the order of $n^{\ell-2}$.
- The codegree of any pair of vertices is $O(n^{\ell-3}) = o(d)$.

Defining a hypergraph

Fix a large integer ℓ. We want to build a k-radius sequence from 'partial permutations' of length ℓ.

Let F be such that $|F| = n$. Define a hypergraph $\Gamma = (V, E)$ as follows:

- The vertices are the $\binom{n}{2}$ unordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^{\ell}$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- Γ is r-uniform, where $r = r(\ell, k)$ is fixed.
- When ℓ is big, $r \approx \ell k$.
- Γ is d-regular, where d is of the order of $n^{\ell-2}$.
- The codegree of any pair of vertices is $O(n^{\ell-3}) = o(d)$.
- So we can apply the Rödl Nibble to Γ.

The existence of k-radius sequences

- The vertices are the $\binom{n}{2}$ ordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.

The existence of k-radius sequences

- The vertices are the $\binom{n}{2}$ ordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- We have a covering by approximately $|V|/r \approx \binom{n}{2}/(\ell k)$ hyperedges.

The existence of k-radius sequences

- The vertices are the $\binom{n}{2}$ ordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- We have a covering by approximately $|V|/r \approx \binom{n}{2}/(\ell k)$ hyperedges.
- Coverings of V by x hyperedges give rise to k-radius sequences of length $x\ell$. (Concatenate the sequences.)

The existence of k-radius sequences

- The vertices are the $\binom{n}{2}$ ordered pairs of elements of F.
- The hyperedges are the $n(n-1)\cdots(n-(\ell-1)) \approx n^\ell$ sequences of ℓ distinct elements over F.
- A vertex v is contained in a hyperedge e if the pair v occurs within a distance of k somewhere in the sequence e.
- We have a covering by approximately $|V|/r \approx \binom{n}{2}/(\ell k)$ hyperedges.
- Coverings of V by x hyperedges give rise to k-radius sequences of length $x\ell$. (Concatenate the sequences.)
- We get a k-radius sequence of length approximately $\binom{n}{2}/k$.

A probabilistic result

Theorem

Let k be fixed and $n \to \infty$. Then

$$f_k(n) \sim \frac{1}{k}\binom{n}{2}$$

A probabilistic result

Theorem

Let k be fixed and $n \to \infty$. Then

$$f_k(n) \sim \frac{1}{k}\binom{n}{2}$$

Remark: Same as non-FIFO case.

A probabilistic result

Theorem

Let k be fixed and $n \to \infty$. Then

$$f_k(n) \sim \frac{1}{k}\binom{n}{2}$$

Remark: Same as non-FIFO case.

Open Problem

Construct k-radius sequences of length approximately $\frac{1}{k}\binom{n}{2}$. (In particular, $k = 195$ is interesting.)

A probabilistic result

Theorem

Let k be fixed and $n \to \infty$. Then

$$f_k(n) \sim \frac{1}{k}\binom{n}{2}$$

Remark: Same as non-FIFO case.

Open Problem

Construct k-radius sequences of length approximately $\frac{1}{k}\binom{n}{2}$. (In particular, $k = 195$ is interesting.)

Open Problem

Generalise constructions from pairs of elements of F to larger subsets of F.

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', *Mathematics of Computation* to appear:

http://arxiv.org/abs/1006.5812

S.R. Blackburn, ‘The existence of k-radius sequences’:

http://arxiv.org/abs/1101.1172