On the minimal distance of a polynomial near-ring code

Péter Pál Pach

ELTE, Hungary

June 2010

Polynomial near-ring codes

The code $C(f, k)$.

Polynomial near-ring codes

The code $C(f, k)$.

$$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$$

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

The codewords

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

The codewords

- for $f = x + x^2 + \cdots + x^n$

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

The codewords

- for $f = x + x^2 + \cdots + x^n$

  $f \circ x^j = x^j + x^{2j} + \cdots + x^{nj}$

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

The codewords

- for $f = x + x^2 + \cdots + x^n$

  $f \circ x^j = x^j + x^{2j} + \cdots + x^{nj}$
- a codeword in C: $f \circ x^{b_1} + \cdots + f \circ x^{b_m}$

Polynomial near-ring codes

The code $C(f, k)$.

$f = x + x^2 + \cdots + x^n \in \mathbb{Z}_2[x]$

$C(f, k)$: linear code generated by $f \circ x$, $f \circ x^2$, $\ldots$, $f \circ x^k$

The codewords

- for $f = x + x^2 + \cdots + x^n$

  $f \circ x^j = x^j + x^{2j} + \cdots + x^{nj}$
- a codeword in C: $f \circ x^{b_1} + \cdots + f \circ x^{b_m}$

Example

$(x + x^2 + x^3 + x^4) \circ x + (x + x^2 + x^3 + x^4) \circ x^2 = x + x^3 + x^6 + x^8$

Near-rings

Near-rings

Near-rings

Near-rings

- $(\mathbb{Z}_2[x], +, \circ)$ is a near-ring

Near-rings

Near-rings

- $(\mathbb{Z}_2[x], +, \circ)$ is a near-ring
- not left distributive

Near-rings

Near-rings

- $(\mathbb{Z}_2[x], +, \circ)$ is a near-ring
- not left distributive
- effective linear codes

Near-rings

Near-rings

- $(\mathbb{Z}_2[x], +, \circ)$ is a near-ring
- not left distributive
- effective linear codes
- block designs

Number theoretic question

Minimal distance

$d_{\min}(C) = \min w$, minimal weight of a codeword in C

Number theoretic question

Minimal distance

$d_{\min}(C) = \min w$, minimal weight of a codeword in C

The exponents

Number theoretic question

Minimal distance

$d_{\min}(C) = \min w$, minimal weight of a codeword in C

The exponents

- $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_k\}$

Number theoretic question

Minimal distance

$d_{\min}(C) = \min w$, minimal weight of a codeword in C

The exponents

- $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_k\}$
- $A * B := \{a_1 b_1, a_2 b_1, \ldots, a_n b_1\} \Delta \cdots \Delta \{a_1 b_k, a_2 b_k, \ldots, a_n b_k\}$

Number theoretic question

Minimal distance

$d_{\min}(C) = \min w$, minimal weight of a codeword in C

The exponents

- $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_k\}$
- $A * B := \{a_1 b_1, a_2 b_1, \ldots, a_n b_1\} \Delta \cdots \Delta \{a_1 b_k, a_2 b_k, \ldots, a_n b_k\}$
- $A * B$: the set of elements that occur odd many times in $A \cdot B$

Number theoretic question

$$\min_K |N * K| = d_{\min}(C)$$

Number theoretic question

$$\min_K |N * K| = d_{\min}(C)$$

Conjecture (Pilz)

Number theoretic question

$$\min_K |N * K| = d_{\min}(C)$$

Conjecture (Pilz)

- $d_{\min}(C) = n$

Number theoretic question

$$\min_K |N * K| = d_{\min}(C)$$

Conjecture (Pilz)

- $d_{\min}(C) = n$
- Is it true that if $N = \{1, 2, \ldots, n\}$, then $|N * K| \geq n$ for all finite K?

Number theoretic question

$$\min_K |N * K| = d_{\min}(C)$$

Conjecture (Pilz)

- $d_{\min}(C) = n$
- Is it true that if $N = \{1, 2, \ldots, n\}$, then $|N * K| \geq n$ for all finite K?
- Is it true that $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, k\}| \geq n$?

Why $x + x^2 + \cdots + x^n$?

Examples

Why $x + x^2 + \cdots + x^n$?

Examples

- $|N * K| \geq |N|$ is not true for arbitrary N

Why $x + x^2 + \cdots + x^n$?

Examples

- $|N * K| \geq |N|$ is not true for arbitrary N
  $N = \{1, 2, 2^2, \ldots, 2^{n-1}\}$, $K = \{1, 2\} \implies K * N = \{1, 2^n\}$

Why $x + x^2 + \cdots + x^n$?

Examples

- $|N * K| \geq |N|$ is not true for arbitrary N

  $N = \{1, 2, 2^2, \ldots, 2^{n-1}\}$, $K = \{1, 2\} \implies K * N = \{1, 2^n\}$

  $(x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x + (x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x^2 = x+x^{2^n}$

Why $x + x^2 + \cdots + x^n$?

Examples

- $|N * K| \geq |N|$ is not true for arbitrary N

  $N = \{1, 2, 2^2, \ldots, 2^{n-1}\}$, $K = \{1, 2\} \implies K * N = \{1, 2^n\}$

  $(x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x + (x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x^2 = x + x^{2^n}$

- $|N * K| \geq \min(|N|, |K|)$ is not true

Why $x + x^2 + \cdots + x^n$?

Examples

- $|N * K| \geq |N|$ is not true for arbitrary N

  $N = \{1, 2, 2^2, \ldots, 2^{n-1}\}$, $K = \{1, 2\} \implies K * N = \{1, 2^n\}$

  $(x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x + (x+x^2+x^4+\cdots+x^{2^{n-1}}) \circ x^2 = x + x^{2^n}$

- $|N * K| \geq \min(|N|, |K|)$ is not true

  $N = \{2^1, 2^2, 2^4, \ldots, 2^{2^n}\}$, $K = \{1\} \cup N \implies K * N = \{2^1, 2^{2^{n+1}}\}$

Upper bound on the minimal distance

Examples for $|N * K| = n$

Upper bound on the minimal distance

Examples for $|N * K| = n$

- $|\{1, 2, \ldots, n\} * \{a\}| = |\{a, 2a, \ldots, na\}| = n$

Upper bound on the minimal distance

Examples for $|N * K| = n$

- $|\{1, 2, \ldots, n\} * \{a\}| = |\{a, 2a, \ldots, na\}| = n$
- $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, n\}| = |\{1^2, 2^2, \ldots, n^2\}| = n$

Upper bound on the minimal distance

Examples for $|N * K| = n$

- $|\{1, 2, \ldots, n\} * \{a\}| = |\{a, 2a, \ldots, na\}| = n$
- $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, n\}| = |\{1^2, 2^2, \ldots, n^2\}| = n$
- $|\{1, 2, \ldots, 2k\} * \{1, 2\}| = |\{1, 3, 5, \ldots, 2k-1, 2k+2, \ldots, 4k\}| = 2k$

Upper bound on the minimal distance

Examples for $|N * K| = n$

- $|\{1, 2, \ldots, n\} * \{a\}| = |\{a, 2a, \ldots, na\}| = n$
- $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, n\}| = |\{1^2, 2^2, \ldots, n^2\}| = n$
- $|\{1, 2, \ldots, 2k\} * \{1, 2\}| = |\{1, 3, 5, \ldots, 2k-1, 2k+2, \ldots, 4k\}| = 2k$
- $|\{1, 2, 3, 4\} * \{1, 2, 3\}| = |\{1, 8, 9, 12\}| = 4$

Upper bound on the minimal distance

Examples for $|N * K| = n$

- $|\{1, 2, \ldots, n\} * \{a\}| = |\{a, 2a, \ldots, na\}| = n$
- $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, n\}| = |\{1^2, 2^2, \ldots, n^2\}| = n$
- $|\{1, 2, \ldots, 2k\} * \{1, 2\}| = |\{1, 3, 5, \ldots, 2k-1, 2k+2, \ldots, 4k\}| = 2k$
- $|\{1, 2, 3, 4\} * \{1, 2, 3\}| = |\{1, 8, 9, 12\}| = 4$
- these are the only examples for $|\{1, 2, \ldots, n\} * \{1, 2, \ldots, k\}| = n$

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$
- $2^3 \cdot 5^4 \cdot 11 \longrightarrow x_2^3 \cdot x_5^4 \cdot x_{11}$

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$
- $2^3 \cdot 5^4 \cdot 11 \longrightarrow x_2^3 \cdot x_5^4 \cdot x_{11}$

Set of natural numbers $\longrightarrow$ polynomial

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$
- $2^3 \cdot 5^4 \cdot 11 \longrightarrow x_2^3 \cdot x_5^4 \cdot x_{11}$

Set of natural numbers $\longrightarrow$ polynomial

- $N = \{1, 2, 3, 4\} \longrightarrow f_N = 1 + x_2 + x_3 + x_2^2$

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$
- $2^3 \cdot 5^4 \cdot 11 \longrightarrow x_2^3 \cdot x_5^4 \cdot x_{11}$

Set of natural numbers $\longrightarrow$ polynomial

- $N = \{1, 2, 3, 4\} \longrightarrow f_N = 1 + x_2 + x_3 + x_2^2$
- $|N|$: the number of terms in f_N

More examples when $|N * K| = n$

Natural number $\longrightarrow$ monomial

- $p_i \longrightarrow x_{p_i}$
- $2^3 \cdot 5^4 \cdot 11 \longrightarrow x_2^3 \cdot x_5^4 \cdot x_{11}$

Set of natural numbers $\longrightarrow$ polynomial

- $N = \{1, 2, 3, 4\} \longrightarrow f_N = 1 + x_2 + x_3 + x_2^2$
- $|N|$: the number of terms in f_N
- $f_{N*K} = f_N \cdot f_K$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

- $f_N^2 = 1 + x_2^2 + x_3^2 + x_2^4$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

- $f_N^2 = 1 + x_2^2 + x_3^2 + x_2^4$
- $f_N^{2^r} = 1 + x_2^{2^r} + x_3^{2^r} + x_2^{2^{r+1}}$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

- $f_N^2 = 1 + x_2^2 + x_3^2 + x_2^4$
- $f_N^{2^r} = 1 + x_2^{2^r} + x_3^{2^r} + x_2^{2^{r+1}}$
- e.g. $r = 2$: $f_N^4 = 1 + x_2^4 + x_3^4 + x_2^8$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

- $f_N^2 = 1 + x_2^2 + x_3^2 + x_2^4$
- $f_N^{2^r} = 1 + x_2^{2^r} + x_3^{2^r} + x_2^{2^{r+1}}$
- e.g. $r = 2$: $f_N^4 = 1 + x_2^4 + x_3^4 + x_2^8$
- $f_N^3 = 1 + x_2 + x_3 + x_2^3 + x_3^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^3 + x_2^5 + x_2^2 x_3^2 + x_2^4 x_3 + x_2^6$

More examples when $|N * K| = n$

Example: $N = \{1, 2, 3, 4\}$, $f_N = 1 + x_2 + x_3 + x_2^2$

- $f_N^2 = 1 + x_2^2 + x_3^2 + x_2^4$
- $f_N^{2^r} = 1 + x_2^{2^r} + x_3^{2^r} + x_2^{2^{r+1}}$
- e.g. $r = 2$: $f_N^4 = 1 + x_2^4 + x_3^4 + x_2^8$
- $f_N^3 = 1 + x_2 + x_3 + x_2^3 + x_3^2 + x_2^2 x_3 + x_2 x_3^2 + x_3^3 + x_2^5 + x_2^2 x_3^2 + x_2^4 x_3 + x_2^6$
- $\{1, 2, 3, 4\} * \{1, 2, 3, 8, 9, 12, 18, 27, 32, 36, 48, 64\} = \{1, 16, 81, 256\}$

Lower bound on the minimal distance

Theorem

$K \subseteq \mathbb{N}$ finite, $n \in \mathbb{N}$, then $|\{1, 2, \ldots, n\} * K| \geq \pi(n)$.

Lower bound on the minimal distance

Theorem

$K \subseteq \mathbb{N}$ finite, $n \in \mathbb{N}$, then $|\{1, 2, \ldots, n\} * K| \geq \pi(n)$.

Theorem (PPP)

$K \subseteq \mathbb{N}$ finite, $n \in \mathbb{N}$, then $|\{1, 2, \ldots, n\} * K| \geq \frac{n}{\log^{0.223} n}$.

Results

Theorem (PPP)

For a fixed $K = \{a_1, \ldots, a_k\}$ set we have $|\{1, 2, \ldots, n\} * K| = cn + O_k(1)$, where $c = c(K) > 0$.

Results

Theorem (PPP, Huang-Ke-Pilz)

$|\{1, 2, \ldots, n\} * \{1, 2, \ldots, k\}| \geq n$

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Case 2. $9 \leq k \leq 1.34 \log n$

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Case 2. $9 \leq k \leq 1.34 \log n$

Lemma: if $1 \leq i \leq k$, $n/2 < t \leq n$ and $(t, a) = 1$ for every $1 \leq a \leq k$, then it appears once in $\underline{k} \cdot \underline{n}$.

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Case 2. $9 \leq k \leq 1.34 \log n$

Lemma: if $1 \leq i \leq k$, $n/2 < t \leq n$ and $(t, a) = 1$ for every $1 \leq a \leq k$, then it appears once in $\underline{k} \cdot \underline{n}$.

$D :=$ the number of such t-s

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Case 2. $9 \leq k \leq 1.34 \log n$

Lemma: if $1 \leq i \leq k$, $n/2 < t \leq n$ and $(t, a) = 1$ for every $1 \leq a \leq k$, then it appears once in $\underline{k} \cdot \underline{n}$.

$D :=$ the number of such t-s

inclusion-exclusion principle $\implies$ $D \geq \frac{0.245n}{\log k} - 2^{\pi(n)} \geq \frac{0.2445}{\log k} n$

Proof

Notation

$\{1, 2, ..., k\} = \underline{k}$, $\{1, 2, ..., n\} = \underline{n}$

Case 1. $k \leq 8$

Easy to check.

Case 2. $9 \leq k \leq 1.34 \log n$

Lemma: if $1 \leq i \leq k$, $n/2 < t \leq n$ and $(t, a) = 1$ for every $1 \leq a \leq k$, then *it* appears once in $\underline{k} \cdot \underline{n}$.

$D :=$ the number of such t-s

inclusion-exclusion principle $\implies D \geq \frac{0.245n}{\log k} - 2^{\pi(n)} \geq \frac{0.2445}{\log k} n$

$\implies |\underline{k} * \underline{n}| \geq Dk \geq \frac{0.2445k}{\log k} n > n.$

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}, n \geq 1410$

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}, n \geq 1410$

$k_1 := \max(k, n/7)$, $k_1 < p$ prime

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}$, $n \geq 1410$

$k_1 := \max(k, n/7)$, $k_1 < p$ prime

$k < p \implies \{a : a \in \underline{k} * \underline{n}, p|a\} = \underline{k} * \{p, 2p, ..., [n/p]p\}$

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}$, $n \geq 1410$

$k_1 := \max(k, n/7)$, $k_1 < p$ prime

$k < p \implies \{a : a \in \underline{k} * \underline{n}, p|a\} = \underline{k} * \{p, 2p, ..., [n/p]p\}$

$\underline{k} * \underline{n}$ has at least k elements divisible by p

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}, n \geq 1410$

$k_1 := \max(k, n/7)$, $k_1 < p$ prime

$k < p \implies \{a : a \in \underline{k} * \underline{n}, p|a\} = \underline{k} * \{p, 2p, ..., [n/p]p\}$

$\underline{k} * \underline{n}$ has at least k elements divisible by p

$\implies |\underline{k} * \underline{n}| \geq (\pi(n) - \pi(k_1))k > n$

Proof

Case 3. $1.34 \log n \leq k \leq n - \frac{0.22n}{\log n}, n \geq 1410$

$k_1 := \max(k, n/7)$, $k_1 < p$ prime

$k < p \implies \{a : a \in \underline{k} * \underline{n}, p|a\} = \underline{k} * \{p, 2p, ..., [n/p]p\}$

$\underline{k} * \underline{n}$ has at least k elements divisible by p

$\implies |\underline{k} * \underline{n}| \geq (\pi(n) - \pi(k_1))k > n$

$\left(n - \frac{0.22n}{\log n}, n\right)$ contains at least two primes

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

$$|\underline{k} * \underline{n}| = |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$$

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

$$|\underline{k} * \underline{n}| = |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$$

$$|\underline{k} * \underline{k}| = k$$

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

$|\underline{k} * \underline{n}| = |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$

$|\underline{k} * \underline{k}| = k$

$i \leq \frac{k}{n-k}, k+1 \leq j \leq n \implies ij$ appears once in $\underline{k} \cdot (\underline{n} \setminus \underline{k})$

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

$|\underline{k} * \underline{n}| = |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$

$|\underline{k} * \underline{k}| = k$

$i \leq \frac{k}{n-k}, k+1 \leq j \leq n \implies ij$ appears once in $\underline{k} \cdot (\underline{n} \setminus \underline{k})$

$\implies |\underline{k} * (\underline{n} \setminus \underline{k})| \geq 2k - n$

Proof

Case 4. $n - \frac{0.22n}{\log n} \leq k \leq n, n \geq 350$

For $k = n$: $\underline{n} * \underline{n} = \{1^2, ..., n^2\}$. Assume $k < n$.

$|\underline{k} * \underline{n}| = |\underline{k} * \underline{k}| + |\underline{k} * (\underline{n} \setminus \underline{k})| - 2|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))|$

$|\underline{k} * \underline{k}| = k$

$i \leq \frac{k}{n-k}, k+1 \leq j \leq n \implies ij$ appears once in $\underline{k} \cdot (\underline{n} \setminus \underline{k})$

$\implies |\underline{k} * (\underline{n} \setminus \underline{k})| \geq 2k - n$

$|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))| < 0.436k$

Proof

Proof

- if among the numbers $1^2, 2^2, ..., k^2$ at most $0.436k$ many has a divisor in $[k+1, n]$, then $|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))| < 0.436k$

Proof

- if among the numbers $1^2, 2^2, ..., k^2$ at most $0.436k$ many has a divisor in $[k+1, n]$, then $|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))| < 0.436k$
- $k+1 \leq m \leq n$, $m = a_m b_m^2$ (b_m^2: largest square divisor), $m | i^2$ iff $a_m b_m | i$

Proof

- if among the numbers $1^2, 2^2, ..., k^2$ at most $0.436k$ many has a divisor in $[k+1, n]$, then $|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))| < 0.436k$
- $k+1 \leq m \leq n$, $m = a_m b_m^2$ (b_m^2: largest square divisor), $m | i^2$ iff $a_m b_m | i$
- $$S = \sum_{m=k+1}^{n} \left[\frac{k}{a_m b_m} \right] \leq \sum_{m=k+1}^{n} \frac{k}{a_m b_m} = k \sum_{m=k+1}^{n} \frac{b_m}{m}$$

Proof

- if among the numbers $1^2, 2^2, ..., k^2$ at most $0.436k$ many has a divisor in $[k+1, n]$, then $|(\underline{k} * \underline{k}) \cap (\underline{k} * (\underline{n} \setminus \underline{k}))| < 0.436k$
- $k+1 \leq m \leq n$, $m = a_m b_m^2$ (b_m^2: largest square divisor), $m | i^2$ iff $a_m b_m | i$
- $$S = \sum_{m=k+1}^{n} \left[\frac{k}{a_m b_m} \right] \leq \sum_{m=k+1}^{n} \frac{k}{a_m b_m} = k \sum_{m=k+1}^{n} \frac{b_m}{m}$$

  Summing by $j = b_m$: $$S \leq k \sum_{j=1}^{[\sqrt{n}]} \sum_{\substack{j^2 | m, \\ k+1 \leq m \leq n, \\ |\mu(m/j^2)|=1}} \frac{j}{m} \leq k \sum_{j=1}^{[\sqrt{n}]} j \sum_{\substack{j^2 | m, \\ k+1 \leq m \leq n}} \frac{1}{m}.$$