Packing sets

Arne Winterhof
(joint with Oliver Roche-Newton and Ilya Shkredov)

Austrian Academy of Sciences
Johann Radon Institute for Computational and Applied Mathematics
Linz

Irsee, September 14, 2017

Basics

A, B subsets of a finite abelian group $(G, \circ)$ with neutral element 1

Product set of A and B: $A \circ B := \{a \circ b : a \in A, b \in B\}$
Ratio set of A and B: $A \circ B^{-1} = \{a \circ b^{-1} : a \in A, b \in B\}$

Trivial bound: $|A \circ B| \leq \min\{|A||B|, |G|\}$

Problem:
Given $\emptyset \neq A \subseteq G$, what is the size of the largest set $B \subseteq G$ such that $|A \circ B| = |A||B|$?

Motivation: coding theory

Packing sets

A-packing set: any B with $|A \circ B| = |A||B|$

$\nu(A)$: maximal size of an A-packing set

$$\nu(A) := \max\{|B| : B \subseteq G, |A \circ B| = |A||B|\}$$

Trivial upper bound: $\nu(A) \leq \frac{|G|}{|A|}$

Example

A subgroup of G, $k = |G|/|A|$

k different cosets $x_1 \circ A, x_2 \circ A, \ldots, x_k \circ A$

$B = \{x_1, x_2, \ldots, x_k\}$

$|A \circ B| = |A||B| = |G|$

$\nu(A) = |B| = |G|/|A|$
$\nu(B) = |A| = |G|/|B|$

Upper bound is tight!

Lower bound

Rusza's Covering Lemma:

$$\nu(A) \geq \frac{|G|}{|A \circ A^{-1}|} \geq \frac{|G|}{|A|^2}$$

Proof. Choose $B \subseteq G$ with $\nu(A) = |B|$.
By maximality of B, for each $x \in G$: $(A \circ x) \cap (A \circ B) \neq \emptyset$,
that is, $G \subseteq A^{-1} \circ A \circ B$,
hence $|G| \leq |A^{-1} \circ A \circ B| \leq |A \circ A^{-1}||B|$. □

Example

$H = \{g, g^2, \dots, g^k\}$ cyclic subgroup of G, $d = \lceil \sqrt{k} \rceil \geq 2$

$$A = \{g, g^2, \dots, g^d\} \cup \{g^{2d}, \dots, q^{(d-1)d}, g^{d^2}\}$$

$|A| < 2d$, $A \circ A^{-1} = H$

$|A \circ B| = |A||B|$ is true iff there are no non-trivial solutions to the equation $a_1 \circ b_1 = a_2 \circ b_2, \quad (a_1, a_2, b_1, b_2) \in A \times A \times B \times B$:

$$\underbrace{(A \circ A^{-1})}_{H} \cap (B \circ B^{-1}) = \{1\}.$$

B cannot contain more than one element from each coset of H.

$$|B| \leq \frac{|G|}{k} < \frac{|G|}{(d-1)^2} \leq \frac{16|G|}{|A|^2}.$$

$$\nu(A) = \max\{|B| : |A \circ B| = |A||B|\}$$

$$\frac{|G|}{|A|^2} \leq \nu(A) \leq \frac{|G|}{|A|}$$

- upper bound is tight
- lower bound is tight (up to a multiplicative constant)
- adding more elements of H to A in the above example we can get: $|A \circ A^{-1}| \approx |A|^{1+\alpha}$ for any $0 \leq \alpha \leq 1$ and $\nu(A) \approx |G|/|A|^{1+\alpha}$

The case $G = \mathbb{F}_p^*$, p prime, and $A = \{1, 2, \ldots, \lambda\}$

- application: limited-magnitude error-correcting codes
- λ small, say, $\lambda < p^{1/2}$ for this application
- $\nu(A) \geq (p-1)/|AA^{-1}|$ is not better than $\nu(A) \gg p/\lambda^2$

$A_{\mathbb{Z}} = \{1, 2, \ldots, \lambda\} \subset \mathbb{Z}$

$$A_{\mathbb{Z}} A_{\mathbb{Z}}^{-1} = \left\{ ab^{-1} : a, b \in A_{\mathbb{Z}}, \gcd(a, b) = 1 \right\}$$

and thus

$$|AA^{-1}| = |A_{\mathbb{Z}} A_{\mathbb{Z}}^{-1}| = \varphi(1) + 2(\varphi(2) + \varphi(3) + \ldots + \varphi(\lambda))$$

$$= \frac{6}{\pi^2}\lambda^2 + O(\lambda \log \lambda)$$

Garaev, 2006: For $\lambda \geq p^{1/2} \log^{1+\varepsilon} p$ we have $|AA^{-1}| = (1 + o(1))p$.

An almost best possible construction

Let $A = \{1, 2 \ldots, \lambda\} \subset \mathbb{F}_p^*$ with $\lambda \leq 0.9\sqrt{p}$. Then

$$\nu(A) \gg \frac{p}{\lambda \log p}.$$

Proof. $B := \left\{x \in \mathbb{F}_p : \lambda < x < \frac{p}{\lambda}, x \text{ is prime}\right\}$
Verify $|AB| = |A||B|$:

$$ab = a'b', \quad (a, a', b, b') \in A \times A \times B \times B.$$

No modulo reduction because of the sizes of a, a', b, b'.
unique factorisation: only solutions are trivial
Prime Number Theorem: $|B| \gg \frac{p/\lambda}{\log(p/\lambda)} - \frac{\lambda}{\log \lambda}$

Limited-magnitude error correcting codes

sent symbol: $c \in \mathbb{F}_p$

received symbol: $c + e \in \mathbb{F}_p$ with $e \in A = \{1, 2, \ldots, \lambda\}$

For $B = \{b_1, \ldots, b_n\} \subseteq \mathbb{F}_p$ with $n \geq 2$, we define the linear code

$$C = \{(c_1, \ldots, c_n) \in \mathbb{F}_p^n : c_1 b_1 + \cdots + c_n b_n = 0\}.$$

If a single error $e \in A$ occurs at position j, that is, we receive $(v_1, \ldots, v_n) = (c_1, \ldots, c_j + e, \ldots, c_n)$, then we get the syndrome

$$\sum_{i=1}^{n} v_i b_i = e b_j.$$

set of possible syndromes: AB

If B is an A-packing set, then the syndromes are distinct and C can correct any single limited-magnitude error $e \in A$ since the syndrome uniquely determines e and j.

Covering sets

For $A \subset G$ a set $B \subset G$ is an A-covering set if

$$A \circ B = G.$$

$$cov(A) = \min\{|B| : A \circ B = G\}$$

$$cov(A) \geq \frac{|G|}{|A|}$$

Bollobás et al., 2011:

$$cov(A) \leq \frac{|G|}{|A|}(\log(|A| + 1)$$

not constructive, not best possible

$G = \mathbb{F}_p^*$, $A = \{1, \ldots, \lambda\}$

Chen, Shparlinski, W., 2014: $cov(A) < 2p/\lambda$ (constructive!)

$$B = \{\pm b^{-1} \bmod p : b = 1, \ldots, \lfloor p/\lambda \rfloor\}$$

application: rewriting schemes

Rewriting schemes

- n memory cells, each capable of storing an element of $\mathbb{F}_p$
- $B = \{b_1, \ldots, b_n\} \subset \mathbb{F}_p$ of size n identified with the vector $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{F}_p^n$
- store a value $v \in \mathbb{F}_p$ in the n memory cells by storing $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_p^n$ with $\mathbf{xb} = x_1 b_1 + \ldots + x_n b_n = v$
- for rewriting v by any $v' \in \mathbb{F}_p$ we have to choose $\mathbf{x}' = (x_1', \ldots, x_n') \in \mathbb{F}_p^n$ with $\mathbf{x}'\mathbf{b} = v'$ and $x_i' \in \{x_i, x_i + 1, \ldots, x_i + \lambda\}$ due to the limitations of flash memory
- for efficiency we may allow only a single cell change
- if B is a $\{1, \ldots, \lambda\}$-covering set, we can write $v' - v = ab_i$ with $a \in \{1, \ldots, \lambda\}$ and $b_i \in B$ and then change only x_i to $x_i + a$ to derive $\mathbf{x}'$ from $\mathbf{x}$
- for efficiency we are interested in covering sets of smallest possible size

Thank you for your attention.