Kneser's theorem for codes and ℓ-divisible set families

Gilles Zémor

joint work with Chenying Lin

Bordeaux Institute of Mathematics (IMB)

ICTS, May 2025

ℓ-divisible set families

Eventown problem: size of maximal collection $\mathcal{F}$ of subsets of $\{1, 2, \ldots, n\}$ such that $|A \cap B|$ even for all $A, B \in \mathcal{F}$?

View $\mathcal{F}$ as set of binary vectors. Let C be linear code generated by $\mathcal{F}$. Intersection property means $\mathbf{c}\mathbf{c}'$ has even weight for any $\mathbf{c}, \mathbf{c} \in C$. So $C \subset C^{\perp}$. So $\dim C \leqslant n/2$ and $|\mathcal{F}| \leqslant 2^{n/2}$.

Maximum size of $\mathcal{F}$ if any intersection of any two subsets has size $0 \bmod \ell$??

Not known: not $2^{\lfloor n/\ell \rfloor}$. Counter-example for $\ell = 3$: from Hadamard matrix of size 12 we get, for $n = 12$, a family $|\mathcal{F}| = 24 > 2^{12/3}$.

Gishboliner, Sudakov, Tomon (2022): there exists k depending only on ℓ such that if intersection of *any k subsets* has size $0 \bmod \ell$, then $|\mathcal{F}| \leqslant 2^{n/\ell}$. The guaranteed number k is exponential in ℓ. Solved conjecture Frankl Odlyzko 1983.

Results

Family $\mathcal{F} \subset 2^{[n]}$ is k-wise ℓ-divisible if intersection of any k subsets of $\mathcal{F}$ is ℓ-divisible.

Theorem:
For p prime, if family $\mathcal{F} \subset 2^{[n]}$ is p-wise p-divisible, then maximum size $|\mathcal{F}| \leqslant 2^{\lfloor n/p \rfloor}$.

For $p = 3$, optimal. Note that upper can always be achieved by *atomic* family: all unions of disjoint subsets of size p.

Companion result.

Theorem:
For p prime, if family $\mathcal{F} \subset 2^{[n]}$ is $p+1$-wise p-divisible, and $|\mathcal{F}| > 2^{\lfloor n/p \rfloor - 1}$, then atoms of $\mathcal{F}$ have size p.

Results

For arbitrary (composite) ℓ, looser result.

Theorem:
If family $\mathcal{F} \subset 2^{[n]}$ is $4\ell^2$-wise ℓ-divisible, then maximum size $|\mathcal{F}| \leqslant 2^{\lfloor n/\ell \rfloor}$. Furthermore, if $|\mathcal{F}| > 2^{\lfloor n/\ell \rfloor - 1}$, then atoms of $\mathcal{F}$ have size ℓ.

Note: brings down value of k from exponential in ℓ to polynomial in ℓ.

Key idea: Viewed as set of functions, or $\{0,1\}$ n-tuples, consider V code generated by $\mathcal{F}$ over $\mathbb{F}_p$. The family $\mathcal{F}$ is k-wise p-divisible iff

$$\langle \mathbf{x}, \mathbf{1} \rangle = 0 \quad \text{for every } \mathbf{x} \in V^{\langle k \rangle},$$

equivalently,

$$V^{\langle k \rangle} \subset \mathbf{1}^{\perp}$$

Code products

For $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$,

$$\mathbf{x} = [x_1, \ldots, x_n]$$
$$\mathbf{y} = [y_1, \ldots, y_n]$$

$$\mathbf{x} * \mathbf{y} = \mathbf{xy} := [x_1 y_1, \ldots, x_n y_n].$$

C, D two linear codes in $\mathbb{F}_q^n$, the product (Hadamard, Schur, star) is defined as the linear code $C * D = CD$ generated by

$$\mathbf{cd},$$

$$\text{for} \quad \mathbf{c} \in C, \ \mathbf{d} \in D.$$

Denote $C^{\langle k \rangle} = C * C * \cdots * C$.

Products of small dimension

We have

$$\dim CD \leqslant \dim C \dim D$$

(equality is typical case whenever $CD \neq \mathbb{F}_q^n$).

But notable exceptions: Reed-Solomon codes C, D are such that $\dim CD = \mathbb{F}_q^n$ or

$$\dim CD = \dim C + \dim D - 1.$$

Structure of pairs of codes C, D s.t. products CD have small dimension ?

Many applications (Decoding, Multiplicative secret sharing, MPC protocols, cryptanalysis, quantum computing ...)

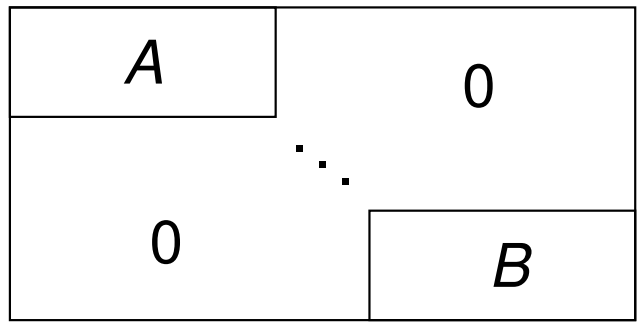
Kneser's Theorem for codes

Theorem (Mirandola, Z.)

$$\dim CD \geqslant \dim C + \dim D - s$$

where s is such that CD decomposes into a direct sum of s codes with disjoint supports.

CD generated by $G =$



Compare with Kneser's theorem:

Theorem

$A, B \subset G$ Abelian group.

$$|A + B| \geqslant |A| + |B| - \#\mathrm{St}(A + B)$$

where $\mathrm{St}(A + B) = \{g \in G,\ g + (A + B) = A + B\}$.

Kneser's Theorem for codes (2)

More precisely,

$$\dim CD \geqslant \dim C + \dim D - \dim \mathrm{St}(CD)$$

Stabiliser algebra of a code C: $\mathrm{St}(C) = \{\mathbf{x} \subset \mathbb{F}_p^n, \mathbf{x}C \subset C\}$.

It is generated by a set of constant vectors of disjoint supports.

Improving result of Gishboliner et al.

For $\mathcal{F}$ k-wise p-divisible family. Introduce $V = \langle \mathcal{F} \rangle$ over $\mathbb{F}_p$.

Consider the sequence $V, V^{\langle 2 \rangle}, \ldots, V^{\langle k \rangle}$. If it grows too quickly it eventually fills up the whole space, contradiction. Else, Kneser's theorem implies that $V^{\langle k \rangle}$ splits into direct sum of spaces, each orthogonal to $\mathbf{1}$.

The family $\mathcal{F}$, restricted to the support of a component code must also be k-wise ℓ-divisible. Use induction argument.

Dimension argument

Need largest possible dimension for V to start with. If V has dimension r, generator matrix

$$\mathbf{G} = \begin{bmatrix} I_r & \mathbf{A} \end{bmatrix}$$

we see that $|V \cap \{0,1\}^n| \leqslant 2^r$. Almost gives the result. But need improvement.

If $V^{\langle 3 \rangle}$ has trivial stabiliser then

$$|V \cap \{0,1\}^n| \leqslant 2^{r-1}$$

Composite ℓ

$\ell = p_1 p_2 \dots p_m$.

Need somewhat different strategy, since $V^{\langle k \rangle}$, with V vector space generated by $\mathcal{F}$ over $\mathbb{F}_{p_i}$ may decompose differently for different primes.

Look for an atom of $\mathcal{F}$ that is p_i-divisible for all prime factors of ℓ. Argue that for k large enough,

$$V^{\langle k \rangle} = C_1 \oplus C_2 \oplus \cdots \oplus C_h$$

with many C_i's of dimension 1. Their supports must be atoms of $\mathcal{F}$. If V is defined over $\mathbb{F}_p$, then these atoms are p-divisible. The remaining C_i's have small dimension, so $\mathcal{F}$ restricted to their support contains few functions. Looking at all these restricted functions simultaneously for all prime factors of ℓ, we get that they cannot cover the whole support of $\mathcal{F}$. There must exist an atom outside which must be p_i-divisible for every p_i.

Some open problems

- Largest non-atomic 3-wise 3-divisible set families?
- Beyond Kneser's theorem for binary codes. Codes with a small product which is not a direct sum are hard to come by if one wants a small codimension.