Combinatorics of Euclidean spaces over finite fields

Semin Yoo (KIAS)

2023 FINITE GEOMETRY & FRIENDS
September 18-22, 2023

Motivation

Motivation

Recall. q - binomial coefficients (Gaussian binomial coefficients)

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} = \frac{[n]_q!}{[k]_q!\,[n-k]_q!}$$
$$= \text{the number of } k\text{-dimensional subspaces of } \mathbb{F}_q^n.$$

For example, if $q = 3$, $n = 3$, and $k = 2$,
the number of 2-dimensional subspaces of $\mathbb{F}_3^3$ is

$$\binom{3}{2}_3 = \frac{(3^3-1)(3^3-3)}{(3^2-1)(3^2-3)} = 13.$$

Motivation

Recall. q - binomial coefficients (Gaussian binomial coefficients)

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})} = \frac{[n]_q!}{[k]_q!\,[n-k]_q!}$$
$$= \text{the number of } k\text{-dimensional subspaces of } \mathbb{F}_q^n.$$

For example, if $q=3$, $n=3$, and $k=2$,

the number of 2-dimensional subspaces of $\mathbb{F}_3^3$ is

$$\binom{3}{2}_3 = \frac{(3^3-1)(3^3-3)}{(3^2-1)(3^2-3)} = 13.$$

	Lines in 2-space
p_1	$\{\langle(1,0,0)\rangle, \langle(0,1,1)\rangle, \langle(1,1,1)\rangle, \langle(1,2,2)\rangle\}$
p_2	$\{\langle(1,0,0)\rangle, \langle(0,1,2)\rangle, \langle(1,1,2)\rangle, \langle(1,2,1)\rangle\}$
p_3	$\{\langle(0,1,0)\rangle, \langle(1,0,1)\rangle, \langle(1,1,1)\rangle, \langle(1,2,1)\rangle\}$
p_4	$\{\langle(0,1,0)\rangle, \langle(1,0,2)\rangle, \langle(1,1,2)\rangle, \langle(1,2,2)\rangle\}$
p_5	$\{\langle(0,0,1)\rangle, \langle(1,1,0)\rangle, \langle(1,1,1)\rangle, \langle(1,1,2)\rangle\}$
p_6	$\{\langle(0,0,1)\rangle, \langle(1,2,0)\rangle, \langle(1,2,1)\rangle, \langle(1,2,2)\rangle\}$
p_7	$\{\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(1,1,0)\rangle, \langle(1,2,0)\rangle\}$
p_8	$\{\langle(1,0,0)\rangle, \langle(0,0,1)\rangle, \langle(1,0,1)\rangle, \langle(1,0,2)\rangle\}$
p_9	$\{\langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(0,1,1)\rangle, \langle(0,1,2)\rangle\}$
p_{10}	$\{\langle(1,0,1)\rangle, \langle(0,1,1)\rangle, \langle(1,2,0)\rangle, \langle(1,1,2)\rangle\}$
p_{11}	$\{\langle(1,0,1)\rangle, \langle(1,1,0)\rangle, \langle(0,1,2)\rangle, \langle(1,2,2)\rangle\}$
p_{12}	$\{\langle(1,1,0)\rangle, \langle(0,1,1)\rangle, \langle(1,0,2)\rangle, \langle(1,2,1)\rangle\}$
p_{13}	$\{\langle(0,1,2)\rangle, \langle(1,0,2)\rangle, \langle(1,2,0)\rangle, \langle(1,1,1)\rangle\}$

Table: The description of all 2-dimensional subspaces of $\mathbb{F}_3^3$.

Q. Can we always find an orthonormal basis in p_i?

	Lines in 2-space
p_1	$\{\langle(1,0,0)\rangle,\langle(0,1,1)\rangle,\langle(1,1,1)\rangle,\langle(1,2,2)\rangle\}$
p_2	$\{\langle(1,0,0)\rangle,\langle(0,1,2)\rangle,\langle(1,1,2)\rangle,\langle(1,2,1)\rangle\}$
p_3	$\{\langle(0,1,0)\rangle,\langle(1,0,1)\rangle,\langle(1,1,1)\rangle,\langle(1,2,1)\rangle\}$
p_4	$\{\langle(0,1,0)\rangle,\langle(1,0,2)\rangle,\langle(1,1,2)\rangle,\langle(1,2,2)\rangle\}$
p_5	$\{\langle(0,0,1)\rangle,\langle(1,1,0)\rangle,\langle(1,1,1)\rangle,\langle(1,1,2)\rangle\}$
p_6	$\{\langle(0,0,1)\rangle,\langle(1,2,0)\rangle,\langle(1,2,1)\rangle,\langle(1,2,2)\rangle\}$
p_7	$\{\langle(1,0,0)\rangle,\langle(0,1,0)\rangle,\langle(1,1,0)\rangle,\langle(1,2,0)\rangle\}$
p_8	$\{\langle(1,0,0)\rangle,\langle(0,0,1)\rangle,\langle(1,0,1)\rangle,\langle(1,0,2)\rangle\}$
p_9	$\{\langle(0,1,0)\rangle,\langle(0,0,1)\rangle,\langle(0,1,1)\rangle,\langle(0,1,2)\rangle\}$
p_{10}	$\{\langle(1,0,1)\rangle,\langle(0,1,1)\rangle,\langle(1,2,0)\rangle,\langle(1,1,2)\rangle\}$
p_{11}	$\{\langle(1,0,1)\rangle,\langle(1,1,0)\rangle,\langle(0,1,2)\rangle,\langle(1,2,2)\rangle\}$
p_{12}	$\{\langle(1,1,0)\rangle,\langle(0,1,1)\rangle,\langle(1,0,2)\rangle,\langle(1,2,1)\rangle\}$
p_{13}	$\{\langle(0,1,2)\rangle,\langle(1,0,2)\rangle,\langle(1,2,0)\rangle,\langle(1,1,1)\rangle\}$

Table: The description of all 2-dimensional subspaces of $\mathbb{F}_3^3$.

Q. Can we always find an orthonormal basis in p_i?

An **inner product** on V over $\mathbb{R}$ is a bilinear map $\langle \cdot, \cdot \rangle \; : \; V \times V \longrightarrow \mathbb{R}$ such that

1. $\langle v, w \rangle = \langle w, v \rangle$
2. $\langle v, v \rangle \geq 0$, $=$ holds $\Leftrightarrow$ $v = 0$.

Simply, $\langle \cdot, \cdot \rangle$ is a positive-definite symmetric bilinear form.

But we don't have positiveness and negativeness in $\mathbb{F}_3$!

$$\Downarrow$$

Consider a symmetric bilinear form, called a **quadratic form**.

$$\mathbb{R} \quad \Rightarrow \quad \mathbb{F}_3.$$

An **inner product** on V over $\mathbb{R}$ is a bilinear map $\langle \cdot, \cdot \rangle \;:\; V \times V \longrightarrow \mathbb{R}$ such that

1. $\langle v, w \rangle = \langle w, v \rangle$
2. $\langle v, v \rangle \geq 0$, $=$ holds $\Leftrightarrow$ $v = 0$.

Simply, $\langle \cdot, \cdot \rangle$ is a positive-definite symmetric bilinear form.

But we don't have positiveness and negativeness in $\mathbb{F}_3$!

$$\Downarrow$$

Consider a symmetric bilinear form, called a **quadratic form**.

$$\mathbb{R} \quad \Rightarrow \quad \mathbb{F}_3.$$

An **inner product** on V over $\mathbb{R}$ is a bilinear map $\langle\cdot,\cdot\rangle \; : \; V \times V \longrightarrow \mathbb{R}$ such that

1. $\langle v, w\rangle = \langle w, v\rangle$
2. $\langle v, v\rangle \geq 0$, $=$ holds $\Leftrightarrow$ $v = 0$.

Simply, $\langle\cdot,\cdot\rangle$ is a positive-definite symmetric bilinear form.

But we don't have positiveness and negativeness in $\mathbb{F}_3$!

$$\Downarrow$$

Consider a symmetric bilinear form, called a **quadratic form**.

$$\mathbb{R} \quad \Rightarrow \quad \mathbb{F}_3.$$

Consider $B(x, y) = x \cdot y$. Then B is a quadratic form on $\mathbb{F}_3^3$.

$\{v, w\}$ is an **orthonormal basis** of $(\mathbb{F}_3^3, B)$ if $B(v, w) = 0$, and $B(v, v) = B(w, w) = 1$, $v \neq w$.

	Lines in 2-space	$\exists$ ON basis?
p_1	$\{\langle(1,0,0)\rangle, \langle(0,1,1)\rangle, \langle(1,1,1)\rangle, \langle(1,2,2)\rangle\}$	No
p_2	$\{\langle(1,0,0)\rangle, \langle(0,1,2)\rangle, \langle(1,1,2)\rangle, \langle(1,2,1)\rangle\}$	No
p_3	$\{\langle(0,1,0)\rangle, \langle(1,0,1)\rangle, \langle(1,1,1)\rangle, \langle(1,2,1)\rangle\}$	No
p_4	$\{\langle(0,1,0)\rangle, \langle(1,0,2)\rangle, \langle(1,1,2)\rangle, \langle(1,2,2)\rangle\}$	No
p_5	$\{\langle(0,0,1)\rangle, \langle(1,1,0)\rangle, \langle(1,1,1)\rangle, \langle(1,1,2)\rangle\}$	No
p_6	$\{\langle(0,0,1)\rangle, \langle(1,2,0)\rangle, \langle(1,2,1)\rangle, \langle(1,2,2)\rangle\}$	No
p_7	$\{\langle(1,0,0)\rangle, \langle(0,1,0)\rangle, \langle(1,1,0)\rangle, \langle(1,2,0)\rangle\}$	Yes
p_8	$\{\langle(1,0,0)\rangle, \langle(0,0,1)\rangle, \langle(1,0,1)\rangle, \langle(1,0,2)\rangle\}$	Yes
p_9	$\{\langle(0,1,0)\rangle, \langle(0,0,1)\rangle, \langle(0,1,1)\rangle, \langle(0,1,2)\rangle\}$	Yes
p_{10}	$\{\langle(1,0,1)\rangle, \langle(0,1,1)\rangle, \langle(1,2,0)\rangle, \langle(1,1,2)\rangle\}$	No
p_{11}	$\{\langle(1,0,1)\rangle, \langle(1,1,0)\rangle, \langle(0,1,2)\rangle, \langle(1,2,2)\rangle\}$	No
p_{12}	$\{\langle(1,1,0)\rangle, \langle(0,1,1)\rangle, \langle(1,0,2)\rangle, \langle(1,2,1)\rangle\}$	No
p_{13}	$\{\langle(0,1,2)\rangle, \langle(1,0,2)\rangle, \langle(1,2,0)\rangle, \langle(1,1,1)\rangle\}$	No

Goal:

- Introduce a formula to count the number of k-dimensional subspaces of $\mathbb{F}_q^n$ which have an ON basis, where q is a prime power, char(q)$\neq 2$.
- This can be written by an analogue of binomial coefficient, $\binom{n}{k}_q^{\perp}$,
- Study its related combinatorial properties,
- Compare it with the q-binomial coefficient.
- One application

Outline

Outline

Theorem

Any non-degenerate quadratic form over $\mathbb{F}_q$ is equivalent to one of

$$\mathrm{Euc}_n := x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \quad \text{or} \quad \mathrm{Lor}_n := x_1^2 + \cdots + x_{n-1}^2 + \lambda x_n^2$$

for some non-square $\lambda \in \mathbb{F}_q$.

cf. The classification from finite geometers.

- hyperbolic : $k\mathbb{H}$ if $n = 2k$ and $\mathbb{H}$ is the hyperbolic plane,
- elliptic : $(k-1)\mathbb{H} \oplus (x^2 - \lambda y^2)$ if $n = 2k, \lambda$ is a non-square,
- parabolic : $k\mathbb{H} \oplus cx^2$ if $n = 2k+1, c$ is 1 or a non-square .

Corollary

Two non-degenerate quadratic forms over a finite field are equivalent iff they have the same dimension and same discriminant.

Theorem

Any non-degenerate quadratic form over $\mathbb{F}_q$ is equivalent to one of

$$\mathrm{Euc}_n := x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \text{ or } \mathrm{Lor}_n := x_1^2 + \cdots + x_{n-1}^2 + \lambda x_n^2$$

for some non-square $\lambda \in \mathbb{F}_q$.

cf. The classification from finite geometers.

- hyperbolic : $k\mathbb{H}$ if $n = 2k$ and $\mathbb{H}$ is the hyperbolic plane,
- elliptic : $(k-1)\mathbb{H} \oplus (x^2 - \lambda y^2)$ if $n = 2k, \lambda$ is a non-square,
- parabolic : $k\mathbb{H} \oplus cx^2$ if $n = 2k+1, c$ is 1 or a non-square .

Corollary

Two non-degenerate quadratic forms over a finite field are equivalent iff they have the same dimension and same discriminant.

Theorem

Any non-degenerate quadratic form over $\mathbb{F}_q$ is equivalent to one of

$$\mathrm{Euc}_n := x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \quad \text{or} \quad \mathrm{Lor}_n := x_1^2 + \cdots + x_{n-1}^2 + \lambda x_n^2$$

for some non-square $\lambda \in \mathbb{F}_q$.

cf. The classification from finite geometers.

- hyperbolic : $k\mathbb{H}$ if $n = 2k$ and $\mathbb{H}$ is the hyperbolic plane,
- elliptic : $(k-1)\mathbb{H} \oplus (x^2 - \lambda y^2)$ if $n = 2k, \lambda$ is a non-square,
- parabolic : $k\mathbb{H} \oplus cx^2$ if $n = 2k+1, c$ is 1 or a non-square .

Corollary

Two non-degenerate quadratic forms over a finite field are equivalent iff they have the same dimension and same discriminant.

Definition

Let us call a k-dimensional quadratic subspace $W \subset (\mathbb{F}_q^n, \mathrm{Euc}_n)$ a **Euclidean** k-subspace (or Lorentzian k-subspace) if $(W, \mathrm{Euc}_n|_W)$ is isometrically isomorphic to $(\mathbb{F}_q^k, \mathrm{Euc}_k)$ (or $(\mathbb{F}_q^k, \mathrm{Lor}_k)$).

For a k-dimensional W in $(\mathbb{F}_q^n, Q)$,

$$(W, Q|_W) \text{ has an ON basis} \Leftrightarrow (W, Q|_W) \text{ is a Euclidean } k\text{-subspace.}$$

Definition

Let us call a k-dimensional quadratic subspace $W \subset (\mathbb{F}_q^n, \mathrm{Euc}_n)$ a **Euclidean** k-subspace (or Lorentzian k-subspace) if $(W, \mathrm{Euc}_n|_W)$ is isometrically isomorphic to $(\mathbb{F}_q^k, \mathrm{Euc}_k)$ (or $(\mathbb{F}_q^k, \mathrm{Lor}_k)$).

For a k-dimensional W in $(\mathbb{F}_q^n, Q)$,

$$(W, Q|_W) \text{ has an ON basis} \Leftrightarrow (W, Q|_W) \text{ is a Euclidean } k\text{-subspace.}$$

Example. Let us consider $W = \langle (1,0,0),(0,1,1)\rangle$ in $(\mathbb{F}_3^3, \mathrm{Euc}_3)$.

Then $(W, B = \mathrm{Euc}_3|_W)$ is a Lorentzian 2-subspace.

$(\because e_1 = (1,0,0), e_2 = (0,1,1)$

$$\mathrm{Euc}_3|_W = \begin{pmatrix} B(e_1,e_1) & B(e_1,e_2)/2 \\ B(e_2,e_1)/2 & B(e_2,e_2) \end{pmatrix}$$
$$= \begin{pmatrix} (1,0,0)\cdot(1,0,0) & (1,0,0)\cdot(0,1,1)/2 \\ (0,1,1)\cdot(1,0,0)/2 & (0,1,1)\cdot(0,1,1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

$\Rightarrow \mathrm{disc}(\mathrm{Euc}_3|_W) = 2.)$

Example. Let us consider $W = \langle (1,0,0), (0,1,1) \rangle$ in $(\mathbb{F}_3^3, \mathrm{Euc}_3)$.

Then $(W, B = \mathrm{Euc}_3|_W)$ is a Lorentzian 2-subspace.

$(\because e_1 = (1,0,0), e_2 = (0,1,1)$

$$\begin{aligned}\mathrm{Euc}_3|_W &= \begin{pmatrix} B(e_1,e_1) & B(e_1,e_2)/2 \\ B(e_2,e_1)/2 & B(e_2,e_2) \end{pmatrix} \\ &= \begin{pmatrix} (1,0,0)\cdot(1,0,0) & (1,0,0)\cdot(0,1,1)/2 \\ (0,1,1)\cdot(1,0,0)/2 & (0,1,1)\cdot(0,1,1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\end{aligned}$$

$\Rightarrow \mathrm{disc}(\mathrm{Euc}_3|_W) = 2.)$

Here is the fundamental theorem in the theory of quadratic forms over any fields.

Theorem (Witt's Extension Theorem)

Let $X_1 \cong X_2$, $X_1 = U_1 \oplus V_1, X_2 = U_2 \oplus V_2, f : V_1 \longrightarrow V_2$ an isometry. Then there is an isomtery $F : X_1 \longrightarrow X_2$ such that $F|_{V_1} = f$ and $F(U_1) = U_2$.

$\Rightarrow$ $O(n, q)$ acts on $\left\{\text{Euclidean } k\text{-subspaces of } (\mathbb{F}_q^n, \mathrm{Euc}_n)\right\}$ transitively.

cf.

- S_n acts on $\{k\text{-sets of } [n]\}$ transitively.
- $GL_n(\mathbb{F}_q)$ acts on $\left\{k\text{-dim'l subspaces of } \mathbb{F}_q^n\right\}$ transitively.

Here is the fundamental theorem in the theory of quadratic forms over any fields.

Theorem (Witt's Extension Theorem)

Let $X_1 \cong X_2$, $X_1 = U_1 \oplus V_1, X_2 = U_2 \oplus V_2, f : V_1 \longrightarrow V_2$ *an isometry. Then there is an isomtery* $F : X_1 \longrightarrow X_2$ *such that* $F|_{V_1} = f$ *and* $F(U_1) = U_2$.

$\Rightarrow O(n, q)$ acts on $\left\{\text{Euclidean } k\text{-subspaces of } (\mathbb{F}_q^n, \mathrm{Euc}_n)\right\}$ transitively.

cf.

- S_n acts on $\{k\text{-sets of } [n]\}$ transitively.
- $GL_n(\mathbb{F}_q)$ acts on $\left\{k\text{-dim'l subspaces of } \mathbb{F}_q^n\right\}$ transitively.

Outline

1. Motivation
2. Preliminaries
   - The theory of quadratic forms
3. Combinatorial properties related to $\binom{n}{k}_q^{\perp}$
   - Formula for $\binom{n}{k}_q^{\perp}$
   - Combinatorial properties of $\binom{n}{k}_q^{\perp}$
4. Comparison
   - $\binom{n}{k}_q$ vs. $\binom{n}{k}_q^{\perp}$
   - $\binom{n}{k}$ vs. $\binom{n}{k}_q^{\perp}$
5. An application
   - Clique-free pseudorandom graphs

Theorem (Y., 2023)

For any n and k, we define **Euclidean-analogues** *as follows:*

$$|\mathrm{Euc}_k, \mathrm{Euc}_n|_q := \frac{|\mathrm{Euc}_1, \mathrm{Euc}_n|_q |\mathrm{Euc}_1, \mathrm{Euc}_{n-1}|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_{n-k+1}|_q}{|\mathrm{Euc}_1, \mathrm{Euc}_k|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_1|_q}.$$

- $[k]_q^{\perp} := |\mathrm{Euc}_1, \mathrm{Euc}_k|_q$,
- $[n]_q^{\perp}! := [n]_q^{\perp}[n-1]_q^{\perp} \cdots [1]_q^{\perp}$,
- $\binom{n}{k}_q^{\perp} := |\mathrm{Euc}_k, \mathrm{Euc}_n|_q = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![n-k]_q^{\perp}!}$.

We call these **Euclidean-analogues**. *In particular, we call $\binom{n}{k}_q^{\perp}$ the* **Euclidean-binomial coefficient**. *We adopt the convention that $|\mathrm{Euc}_0, \mathrm{Euc}_n|_q := 1$.*

Theorem (Y., 2023)

For any n and k, we define **Euclidean-analogues** *as follows:*

$$|\mathrm{Euc}_k, \mathrm{Euc}_n|_q := \frac{|\mathrm{Euc}_1, \mathrm{Euc}_n|_q |\mathrm{Euc}_1, \mathrm{Euc}_{n-1}|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_{n-k+1}|_q}{|\mathrm{Euc}_1, \mathrm{Euc}_k|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_1|_q}.$$

- $[k]_q^{\perp} := |\mathrm{Euc}_1, \mathrm{Euc}_k|_q$,
- $[n]_q^{\perp}! := [n]_q^{\perp}[n-1]_q^{\perp} \cdots [1]_q^{\perp}$,
- $\binom{n}{k}_q^{\perp} := |\mathrm{Euc}_k, \mathrm{Euc}_n|_q = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![n-k]_q^{\perp}!}$.

We call these **Euclidean-analogues**. *In particular, we call $\binom{n}{k}_q^{\perp}$ the* **Euclidean-binomial coefficient**. *We adopt the convention that $|\mathrm{Euc}_0, \mathrm{Euc}_n|_q := 1$.*

Theorem (Y., 2023)

If $q \equiv 1 \pmod 4$ and n is odd, the the number of Euclidean lines S, and Lorentzian lines T in $(\mathbb{F}_q^n, \mathrm{Euc}_n)$ are

$$S = \frac{q^{n-1} + q^{\frac{n-1}{2}}}{2}, T = \frac{q^{n-1} - q^{\frac{n-1}{2}}}{2}.$$

If n is even,

$$S = \frac{q^{n-1} - q^{\frac{n-2}{2}}}{2}, T = \frac{q^{n-1} - q^{\frac{n-2}{2}}}{2}.$$

Definition (Y., 2023)

Let n, k be positive integers with $k \leq n$. Then we have

$$|\mathrm{Euc}_k, \mathrm{Euc}_n|_q = \frac{|\mathrm{Euc}_1, \mathrm{Euc}_n|_q |\mathrm{Euc}_1, \mathrm{Euc}_{n-1}|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_{n-k+1}|_q}{|\mathrm{Euc}_1, \mathrm{Euc}_k|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_1|_q},$$

$$|\mathrm{Euc}_k, \mathrm{Lor}_n|_q = \frac{|\mathrm{Euc}_1, \mathrm{Lor}_n|_q |\mathrm{Euc}_1, \mathrm{Lor}_{n-1}|_q \cdots |\mathrm{Euc}_1, \mathrm{Lor}_{n-k+1}|_q}{|\mathrm{Euc}_1, \mathrm{Euc}_k|_q \cdots |\mathrm{Euc}_1, \mathrm{Euc}_1|_q},$$

$$|\mathrm{Lor}_k, \mathrm{Euc}_n|_q = \frac{|\mathrm{Lor}_1, \mathrm{Euc}_n|_q}{|\mathrm{Lor}_1, \mathrm{Lor}_k|_q} \binom{\overline{n-1}}{k-1}_q^{\perp},$$

$$|\mathrm{Lor}_k, \mathrm{Lor}_n|_q = \frac{|\mathrm{Lor}_1, \mathrm{Lor}_n|_q}{|\mathrm{Lor}_1, \mathrm{Lor}_k|_q} \binom{n-1}{k-1}_q^{\perp}.$$

Outline

Theorem (Y., 2023)

- $\binom{n}{k}_q^{\perp}$ *can be written by the q-binomial coefficients. When* $q \equiv 1 \pmod 4$, *and* n, k *are odd,*

$$\binom{n}{k}_q^{\perp} = \frac{1}{2} q^{\frac{k(n-k)}{2}} (q^{\frac{n-k}{2}} + 1) \binom{\frac{n-1}{2}}{\frac{k-1}{2}}_{q^2}$$

- *There are* 4 *cases if* $q \equiv 1 \pmod 4$,
  16 *cases if* $q \equiv 3 \pmod 4$.

- $\binom{n}{k}_q^{\perp}$ *are polynomials of degree* $k(n-k)$ *in* $\frac{1}{2}\mathbb{Z}[q]$.

Theorem (Y., 2023)

- $\binom{n}{k}_q^{\perp}$ *can be written by the q-binomial coefficients. When* $q \equiv 1 \pmod 4$, *and* n, k *are odd,*

$$\binom{n}{k}_q^{\perp} = \frac{1}{2} q^{\frac{k(n-k)}{2}} (q^{\frac{n-k}{2}} + 1) \binom{\frac{n-1}{2}}{\frac{k-1}{2}}_{q^2}$$

- *There are* 4 *cases if* $q \equiv 1 \pmod 4$,
  16 *cases if* $q \equiv 3 \pmod 4$.
- $\binom{n}{k}_q^{\perp}$ *are polynomials of degree* $k(n-k)$ *in* $\frac{1}{2}\mathbb{Z}[q]$.

Theorem (Y., 2023)

- *$\binom{n}{k}_q^{\perp}$ can be written by the q-binomial coefficients. When $q \equiv 1 \pmod 4$, and n, k are odd,*

$$\binom{n}{k}_q^{\perp} = \frac{1}{2} q^{\frac{k(n-k)}{2}} (q^{\frac{n-k}{2}} + 1) \binom{\frac{n-1}{2}}{\frac{k-1}{2}}_{q^2}$$

- *There are 4 cases if $q \equiv 1 \pmod 4$,*

  16 cases if $q \equiv 3 \pmod 4$.

- *$\binom{n}{k}_q^{\perp}$ are polynomials of degree $k(n-k)$ in $\frac{1}{2}\mathbb{Z}[q]$.*

Theorem (Y., 2023)

- $|O(n,q)| = 2^n\,[n]_q^{\perp}!.$

  cf. $|S_n| = n!$ and $|GL(n,q)| = q^{n(n-1)/2}(q-1)^n\,[n]_q!$

- $$\binom{n}{k}_q^{\perp} = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![n-k]_q^{\perp}!} = \left|\frac{O(n,q)}{O(k,q)\times O(n-k,q)}\right|.$$

- $\binom{n}{k}_q^{\perp} = |Gr_q^{\perp}(n,k)| < |Gr_q(n,k)| = \binom{n}{k}_q.$

- c.f. Over $\mathbb{R}$, $Gr_{\mathbb{R}}(n,k) = \frac{O(n)}{O(k)\times O(n-k)}.$

Theorem (Y., 2023)

- $|O(n,q)| = 2^n \, [n]_q^{\perp}!$.

  cf. $|S_n| = n!$ *and* $|GL(n,q)| = q^{n(n-1)/2}(q-1)^n \, [n]_q!$

- $$\binom{n}{k}_q^{\perp} = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![n-k]_q^{\perp}!} = \left| \frac{O(n,q)}{O(k,q) \times O(n-k,q)} \right|.$$

- $\binom{n}{k}_q^{\perp} = |Gr_q^{\perp}(n,k)| < |Gr_q(n,k)| = \binom{n}{k}_q$.

- *c.f. Over* $\mathbb{R}$, $Gr_{\mathbb{R}}(n,k) = \frac{O(n)}{O(k) \times O(n-k)}$.

Theorem (Y., 2023)

- $|O(n,q)| = 2^n \, [n]_q^{\perp}!$.

  $cf.\ |S_n| = n! \quad and \quad |GL(n,q)| = q^{n(n-1)/2}(q-1)^n \, [n]_q!$

- $$\binom{n}{k}_q^{\perp} = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![n-k]_q^{\perp}!} = \left| \frac{O(n,q)}{O(k,q) \times O(n-k,q)} \right|.$$

- $\binom{n}{k}_q^{\perp} = |Gr_q^{\perp}(n,k)| < |Gr_q(n,k)| = \binom{n}{k}_q$.

- $c.f.\ Over\ \mathbb{R},\ Gr_{\mathbb{R}}(n,k) = \frac{O(n)}{O(k)\times O(n-k)}$.

Outline

$$\text{Connection: } \lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$$

	Field with one element	$\mathbb{F}_q$ (q-analogues)
object	$[n] = \{1, 2, \cdots, n\}$	$\mathbb{F}_q^n$
subobject	a k set in $[n]$	a k-dimensional subspace of $\mathbb{F}_q^n$
bracket	n	the number of lines in $\mathbb{F}_q^n$
factorial	$n!$	$[n]_q!$
poset	B_n	$L_n(q)$
group	$\lvert S_n\rvert = n!$	$\lvert GL(n,q)\rvert = q^{n(n-1)/2}(q-1)^n\,[n]_q!$
flag	flags in $[n]$	flags in $\mathbb{F}_q^n$
binomial coefficient	$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \left\lvert\frac{S_n}{S_k\times S_{n-k}}\right\rvert$	$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![(n-k)]_q!} = \left\lvert\frac{GL(n,q)}{\begin{pmatrix} A & C \\ \mathbf{0} & B\end{pmatrix}}\right\rvert$
connection	$\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$	

Table: Example of Field with one element analogues.

$\binom{n}{k}_q$ vs. $\binom{n}{k}_q^{\perp}$

	q-analogues	Euclidean-analogues
space	$\mathbb{F}_q^n$	$(\mathbb{F}_q^n, \mathrm{Euc}_n)$
subspace	a k-dimensional subspace of $\mathbb{F}_q^n$	a Euc_k-subspace of Euc_n
bracket	the number of lines in $\mathbb{F}_q^n$	the number of Euclidean lines in $(\mathbb{F}_q^n, \mathrm{Euc}_n)$
factorial	$[n]_q!$	$[n]_q^{\perp}!$
poset	$L_n(q)$	$E_n(q)$
group	$\lvert GL(n,q)\rvert = q^{n(n-1)/2}(q-1)^n\,[n]_q!$	$\lvert O(n,q)\rvert = 2^n\,[n]_q^{\perp}!$
flag	flags in $\mathbb{F}_q^n$	Euclidean flags in $(\mathbb{F}_q^n,\mathrm{Euc}_n)$
binomial coefficient	$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![(n-k)]_q!} = \left\lvert \frac{GL(n,q)}{\begin{pmatrix} A & C \\ \mathbf{0} & B \end{pmatrix}} \right\rvert$	$\binom{n}{k}_q^{\perp} = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![(n-k)]_q^{\perp}!} = \left\lvert \frac{O(n,q)}{O(k,q)\times O(n-k,q)} \right\rvert$

Table: The q-analogues and the Euclidean-analogues (Y., 2023).

Question.

$$\begin{array}{ccc} ?? & \text{———} & \binom{n}{k}_q^{\perp} \\ \Big| & & \Big| \\ \binom{n}{k} & \text{———} & \binom{n}{k}_q \end{array}.$$

	q-analogues	Euclidean-analogues
space	$\mathbb{F}_q^n$	$(\mathbb{F}_q^n, \mathrm{Euc}_n)$
subspace	a k-dimensional subspace of $\mathbb{F}_q^n$	a Euc_k-subspace of Euc_n
bracket	the number of lines in $\mathbb{F}_q^n$	the number of Euclidean lines in $(\mathbb{F}_q^n, \mathrm{Euc}_n)$
factorial	$[n]_q!$	$[n]_q^{\perp}!$
poset	$L_n(q)$	$E_n(q)$
group	$\lvert GL(n,q)\rvert = q^{n(n-1)/2}(q-1)^n\,[n]_q!$	$\lvert O(n,q)\rvert = 2^n\,[n]_q^{\perp}!$
flag	flags in $\mathbb{F}_q^n$	Euclidean flags in $(\mathbb{F}_q^n,\mathrm{Euc}_n)$
binomial coefficient	$\binom{n}{k}_q = \frac{[n]_q!}{[k]_q![(n-k)]_q!} = \left\lvert \frac{GL(n,q)}{\begin{pmatrix} A & C \\ \mathbf{0} & B \end{pmatrix}} \right\rvert$	$\binom{n}{k}_q^{\perp} = \frac{[n]_q^{\perp}!}{[k]_q^{\perp}![(n-k)]_q^{\perp}!} = \left\lvert \frac{O(n,q)}{O(k,q)\times O(n-k,q)} \right\rvert$

Table: The q-analogues and the Euclidean-analogues (Y., 2023).

Question.

$$\begin{tikzcd}
?? \arrow[r, dash] \arrow[d, dash] & \binom{n}{k}_q^{\perp} \arrow[d, dash] \\
\binom{n}{k} \arrow[r, dash] & \binom{n}{k}_q
\end{tikzcd}.$$

Outline

1. Motivation
2. Preliminaries
   - The theory of quadratic forms
3. Combinatorial properties related to $\binom{n}{k}_q^{\perp}$
   - Formula for $\binom{n}{k}_q^{\perp}$
   - Combinatorial properties of $\binom{n}{k}_q^{\perp}$
4. Comparison
   - $\binom{n}{k}_q$ vs. $\binom{n}{k}_q^{\perp}$
   - $\binom{n}{k}$ vs. $\binom{n}{k}_q^{\perp}$
5. An application
   - Clique-free pseudorandom graphs

Recall $\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$ gives a connection between $\binom{n}{k}_q$ and $\binom{n}{k}$.

Question. $\lim_{q\to 1}\binom{n}{k}_q^{\perp} =?$

Big Trouble:

- There are 4 cases of $\binom{n}{k}_d$ when $q \equiv 1 \pmod 4$ and 16 cases when $q \equiv 3 \pmod 4$.
- $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 1 \pmod 4$ is NOT the same with $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 3 \pmod 4$.

Solution: $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 1 \pmod 4$ is the same with $\lim_{q\to -1}\binom{n}{k}_q^{\perp}$ when $q \equiv 3 \pmod 4$.

Recall $\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$ gives a connection between $\binom{n}{k}_q$ and $\binom{n}{k}$.

Question. $\lim_{q\to 1}\binom{n}{k}_q^\perp = ?$

Big Trouble:

- There are 4 cases of $\binom{n}{k}_d$ when $q \equiv 1 \pmod 4$ and 16 cases when $q \equiv 3 \pmod 4$.
- $\lim_{q\to 1}\binom{n}{k}_q^\perp$ when $q \equiv 1 \pmod 4$ is NOT the same with $\lim_{q\to 1}\binom{n}{k}_q^\perp$ when $q \equiv 3 \pmod 4$.

Solution: $\lim_{q\to 1}\binom{n}{k}_q^\perp$ when $q \equiv 1 \pmod 4$ is the same with $\lim_{q\to -1}\binom{n}{k}_q^\perp$ when $q \equiv 3 \pmod 4$.

Recall $\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}$ gives a connection between $\binom{n}{k}_q$ and $\binom{n}{k}$.

Question. $\lim_{q\to 1}\binom{n}{k}_q^{\perp} = ?$

Big Trouble:

- There are 4 cases of $\binom{n}{k}_d$ when $q \equiv 1 \pmod 4$ and 16 cases when $q \equiv 3 \pmod 4$.
- $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 1 \pmod 4$ is NOT the same with $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 3 \pmod 4$.

Solution: $\lim_{q\to 1}\binom{n}{k}_q^{\perp}$ when $q \equiv 1 \pmod 4$ is the same with $\lim_{q\to -1}\binom{n}{k}_q^{\perp}$ when $q \equiv 3 \pmod 4$.

Proposition (Y., 2023)

- *If n, k are odd,*

$$\lim_{q\to 1}\binom{n}{k}_q^{\perp}=\binom{(n-1)/2}{(k-1)/2}=\lim_{q\to -1}\binom{n}{k}_q^{\perp}.$$

- *If n, k are even,*

$$\lim_{q\to 1}\binom{n}{k}_q^{\perp}=\binom{n/2}{k/2}=\lim_{q\to -1}\binom{n}{k}_q^{\perp}.$$

- *If n is odd and k is even,*

$$\lim_{q\to 1}\binom{n}{k}_q^{\perp}=\binom{(n-1)/2}{k/2}=\lim_{q\to -1}\binom{n}{k}_q^{\perp}.$$

Definition

A set S in $\mathbb{Z}/(n+1)\mathbb{Z}$ is called **symmetric** if $S = -S$ and $0 \notin S$.

Proposition (Y., 2023)

$\lim_{q\to\pm1} \binom{n}{k}_q^{\perp}$ *is the number of symmetric k-sets in* $\mathbb{Z}/(n+1)\mathbb{Z}$.

For example, if $n = 8$ and $k = 4$,

$$\mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$\Rightarrow \quad |\text{symmetric 4-sets in } \mathbb{Z}/9\mathbb{Z}| = \binom{8/2}{4/2} = \binom{4}{2} = 6.$$

$$\lim_{q\to1} \binom{8}{4}_q^{\perp} = \lim_{q\to1} \frac{1}{2} q^8 (q^2+1)^2 (q^2-q+1)(q^2+q+1) = 6.$$

Definition

A set S in $\mathbb{Z}/(n+1)\mathbb{Z}$ is called **symmetric** if $S = -S$ and $0 \notin S$.

Proposition (Y., 2023)

$\lim_{q\to\pm 1} \binom{n}{k}_q^{\perp}$ is the number of symmetric k-sets in $\mathbb{Z}/(n+1)\mathbb{Z}$.

For example, if $n = 8$ and $k = 4$,

$$\mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$\Rightarrow \quad |\text{symmetric 4-sets in } \mathbb{Z}/9\mathbb{Z}| = \binom{8/2}{4/2} = \binom{4}{2} = 6.$$

$$\lim_{q\to 1} \binom{8}{4}_q^{\perp} = \lim_{q\to 1} \frac{1}{2} q^8 (q^2+1)^2 (q^2-q+1)(q^2+q+1) = 6.$$

Definition

A set S in $\mathbb{Z}/(n+1)\mathbb{Z}$ is called **symmetric** if $S = -S$ and $0 \notin S$.

Proposition (Y., 2023)

$\lim_{q\to\pm 1} \binom{n}{k}_q^{\perp}$ is the number of symmetric k-sets in $\mathbb{Z}/(n+1)\mathbb{Z}$.

For example, if $n = 8$ and $k = 4$,

$$\mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$$

$$\Rightarrow \quad |\text{symmetric 4-sets in } \mathbb{Z}/9\mathbb{Z}| = \binom{8/2}{4/2} = \binom{4}{2} = 6.$$

$$\lim_{q\to 1} \binom{8}{4}_q^{\perp} = \lim_{q\to 1} \frac{1}{2} q^8 (q^2+1)^2 (q^2-q+1)(q^2+q+1) = 6.$$

Outline

An application

- Finding the conjectured lower bound of off-diagonal Ramsey numbers can be replaced by constructing clique-free pseudorandom graphs under some required conditions. (D. Mubayi and J. Verstraete, 2019+) As $t \to \infty$,

$$c_s \frac{t^{s-1}}{(\log t)^{s-2}} \leq r(s,t) \leq c_s' \frac{t^{s-1}}{(\log t)^{s-2}}.$$

- A. Bishnoi, F. Inhringer, and V. Pepe (2020) constructed clique-free pseudorandom graphs and improved the lower bound of off-diagonal Ramsey numbers a little bit.
- I found that their vertices are 1-dimensional Euclidean lines in my language, so I generalized the vertices of the graphs.

An application

- Finding the conjectured lower bound of off-diagonal Ramsey numbers can be replaced by constructing clique-free pseudorandom graphs under some required conditions. (D. Mubayi and J. Verstraete, 2019+) As $t \to \infty$,

$$c_s \frac{t^{s-1}}{(\log t)^{s-2}} \leq r(s,t) \leq c_s' \frac{t^{s-1}}{(\log t)^{s-2}}.$$

- A. Bishnoi, F. Inhringer, and V. Pepe (2020) constructed clique-free pseudorandom graphs and improved the lower bound of off-diagonal Ramsey numbers a little bit.
- I found that their vertices are 1-dimensional Euclidean lines in my language, so I generalized the vertices of the graphs.

An application

- Finding the conjectured lower bound of off-diagonal Ramsey numbers can be replaced by constructing clique-free pseudorandom graphs under some required conditions. (D. Mubayi and J. Verstraete, 2019+) As $t \to \infty$,

$$c_s \frac{t^{s-1}}{(\log t)^{s-2}} \leq r(s,t) \leq c_s' \frac{t^{s-1}}{(\log t)^{s-2}}.$$

- A. Bishnoi, F. Inhringer, and V. Pepe (2020) constructed clique-free pseudorandom graphs and improved the lower bound of off-diagonal Ramsey numbers a little bit.
- I found that their vertices are 1-dimensional Euclidean lines in my language, so I generalized the vertices of the graphs.

I studied the graph $\Gamma^{\square}(n,k,q)$ defined as follows:

- The vertex set is the set of Euclidean k-subspaces in $(\mathbb{F}_q^n, \mathrm{Lor}_n)$,
- Two vertices x, y are adjacent if $x \subseteq y^{\perp}$,
- By the transitivity, the graph $\Gamma^{\square}(n,k,q)$ is vertex-transitive. Thus it is regular.
- We know the size of the vertex set n, the degree of the graph d, and the 2nd largest eigenvalue λ such that $\lambda = O(\sqrt{d})$ by using an interlacing lemma.

I studied the graph $\Gamma^{\square}(n,k,q)$ defined as follows:

- The vertex set is the set of Euclidean k-subspaces in $(\mathbb{F}_q^n, \mathrm{Lor}_n)$,
- Two vertices x, y are adjacent if $x \subseteq y^{\perp}$,
- By the transitivity, the graph $\Gamma^{\square}(n,k,q)$ is vertex-transitive. Thus it is regular.
- We know the size of the vertex set n, the degree of the graph d, and the 2nd largest eigenvalue λ such that $\lambda = O(\sqrt{d})$ by using an interlacing lemma.

	The results in BIP	The results in my paper
ambient space	$(\mathbb{F}_q^n, \mathrm{Lor}_n)$	$(\mathbb{F}_q^n, \mathrm{Lor}_n)$
vertex set	Euclidean lines	Euclidean k-subspaces
number of vertices	$(1+o(1))q^{n-1}/2$	$(1+o(1))q^{k(n-k)}/2$
adjacency relation	$x \sim y \;\Leftrightarrow\; x \subseteq y^{\perp}$	$x \sim y \;\Leftrightarrow\; x \subseteq y^{\perp}$
graph	$\Gamma^{\square}(n,q)$	$\Gamma^{\square}(n,k,q)$
properties of the graph	(1) vertex-transitive (2) K_2-free for any $n=2$ (3) K_n-free for all $n \geq 2$ (4) (n', d', λ')-graph	(1) vertex and arc-transitive (2) K_2-free for any $k \geq n/2$ (3) K_l-free for all $l > \left[\frac{n-1}{k}\right]$ (4) (n'', d'', λ'')-graph

Table: Comparison of the results in BIP with mine.

$$\text{where } n' = \Theta(q^{n-1}), d' = \Theta(q^{n-2}), \lambda' = \Theta(q^{(n-2)/2}),$$
$$n'' = \Theta(q^{k(n-k)}), d'' = \Theta(q^{k(n-2k)}), \lambda'' = \Theta(q^{k(n-2k)/2}).$$

$$d'/n' = \Theta(n'^{-1/(n-1)}) \quad \text{and} \quad d''/n'' = \Theta(n''^{-k/(n-k)}).$$

References

A. Bishnoi, F. Inhringer, V. Pepe,
Construction for clique-free pseudorandom graphs,
Combinatorica, 40, pages 307–314 (2020)

S. Yoo,
Combinatorics of Euclidean spaces over finite fields
To appear in Annals of Combinatorics (2023)

S. Yoo,
Graphs associated with orthogonal collections of k-planes over finite fields
Discrete Mathematics, 344, no. 9, 112496 (2021)

Thank you for your attention!