The dot-binomial coefficients

Semin Yoo

University of Rochester

7th annual Mississippi Discrete Math Workshop
October 27th, 2019

1. Motivation

Motivation

The Gaussian binomial coefficients (or q-binomial coefficients)

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

Motivation

The Gaussian binomial coefficients (or q-binomial coefficients)

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

- There are a lot of works associated with $\mathbb{F}_q^n$.
- We add one more algebraic structure, called quadratic form.
- We will count special quadratic subspaces of $(\mathbb{F}_q^n, Q)$, where $Q = x_1^2 + \cdots + x_n^2$.
- This count gives us a new binomial coefficients, called the **dot-binomial coefficients**.

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

Table: The q-analogues and the dot-analogues.

Combinatorics of quadratic spaces over finite fields.
Arxiv: 1910.03482

Outline

Outline

Preliminaries

- Let V be a n-dimensional vector space over a field F with $\mathrm{char} F \neq 2$.
- A quadratic form (symmetric bilinear form) is a kind of generalization of an inner product.

Definition (Coordinate dependent)

A **quadratic form** Q is a homogeneous polynomial of degree 2.

Preliminaries

- Let V be a n-dimensional vector space over a field F with $\mathrm{char} F \neq 2$.
- A quadratic form (symmetric bilinear form) is a kind of generalization of an inner product.

Definition (Coordinate dependent)

A **quadratic form** Q is a homogeneous polynomial of degree 2.

Definition (Coordinate independent)

A **quadratic form** Q on V is a function from V to F satisfying the following two conditions:
(1) $Q(cv) = c^2 Q(v)$ for any $v \in V, c \in F$;
(2) $B(v, w) := \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$ is bilinear.

Example

In $\mathbb{R}^n$, consider $Q(x_1, x_2, \cdots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$.
For $v = (v_1, \cdots, v_n), w = (w_1, \cdots, w_n)$ in $\mathbb{R}^n$,

- $B(v, w) := \langle v, w \rangle = v_1 w_1 + \cdots + v_n w_n$
- The matrix form associated with Q in the standard basis is

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Example

In $\mathbb{R}^n$, consider $Q(x_1, x_2, \cdots, x_n) = x_1^2 + x_2^2 + \cdots + x_n^2$.
For $v = (v_1, \cdots, v_n), w = (w_1, \cdots, w_n)$ in $\mathbb{R}^n$,

- $B(v, w) := \langle v, w \rangle = v_1 w_1 + \cdots + v_n w_n$
- The matrix form associated with Q in the standard basis is

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

In a chosen basis, there are canonical bijections:

quadratic form on V $\Leftrightarrow$ symmetric bilinear form on V $\Leftrightarrow$ symmetric $n \times n$ matrix

Definition

The quadratic forms Q_1, Q_2 on V are **equivalent** if $\exists$ a linear isomorphism $A : V \longrightarrow V$ s.t $Q_2(Av) = Q_1(v)$ for any $v \in V$.

e.g, $Q(x, y) = x^2 - y^2$ and $Q'(x, y) = xy$ are equivalent on $\mathbb{R}^2$.

Definition

The quadratic forms Q_1, Q_2 on V are **equivalent** if $\exists$ a linear isomorphism $A : V \longrightarrow V$ s.t $Q_2(Av) = Q_1(v)$ for any $v \in V$.

e.g, $Q(x, y) = x^2 - y^2$ and $Q'(x, y) = xy$ are equivalent on $\mathbb{R}^2$.

Definition

Q is called **nondegenerate** if a matrix representation M of Q is invertible. If $\det M = 0$, we call a quadratic form **degenerate**.

e.g., On $\mathbb{R}^2$, $Q(x, y) = x^2 - y^2$ is nondegenerate.
On $\mathbb{R}^3$, $Q(x, y, z) = x^2 - y^2$ is degenerate.

Theorem

Any nondegenerate quadratic form on $\mathbb{F}_q^n$ is equivalent to one of

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \quad \text{or} \quad x_1^2 + \cdots + x_{n-1}^2 + \lambda x_n^2$$

for some nonsqaure $\lambda \in \mathbb{F}_q$. Denote dot_n, λdot_n respectively.

Theorem

Any nondegenerate quadratic form on $\mathbb{F}_q^n$ is equivalent to one of

$$x_1^2 + \cdots + x_{n-1}^2 + x_n^2 \quad \textit{or} \quad x_1^2 + \cdots + x_{n-1}^2 + \lambda x_n^2$$

for some nonsqaure $\lambda \in \mathbb{F}_q$. Denote dot_n, λdot_n respectively.

In particular, there are three possible 1-dimensional quadratic subspaces in $(\mathbb{F}_q^n, \mathrm{dot}_n)$ up to equivalence:

(1) dot_1, (2) $\lambda\mathrm{dot}_1$, and the degenerate case (3) 0.

Definition

The type of a line l through the origin in $(\mathbb{F}_q^n, \mathrm{dot}_n)$ is

- **spacelike** if $|l|$ is a square,
- **timelike** if $|l|$ is a nonsquare, and
- **lightlike** if $|l|$ is 0.

Here, $|l| := \mathrm{dot}_n(\mathbf{x})$ for any nonzero $\mathbf{x}$ in l.

- (V, Q) is called a **quadratic space**;
- (V_1, Q_1) and (V_2, Q_2) are **isometrically isomorphic** if $\exists$ a linear map $A : V_1 \to V_2$ s.t $Q_2(Av) = Q_1(v)$.
- For $W \subset V$, $(W, Q|_W)$ is a **quadratic subspace**.

- (V, Q) is called a **quadratic space**;
- (V_1, Q_1) and (V_2, Q_2) are **isometrically isomorphic** if $\exists$ a linear map $A : V_1 \to V_2$ s.t $Q_2(Av) = Q_1(v)$.
- For $W \subset V$, $(W, Q|_W)$ is a **quadratic subspace**.

Theorem (Witt's Cancellation Theorem)

Let U_1, U_2, V_1, V_2 be quadratic spaces where V_1 and V_2 are isometrically isomorphic. If $U_1 \oplus V_1 \cong U_2 \oplus V_2$, then $U_1 \cong U_2$.

- (V, Q) is called a **quadratic space**;
- (V_1, Q_1) and (V_2, Q_2) are **isometrically isomorphic** if $\exists$ a linear map $A : V_1 \to V_2$ s.t $Q_2(Av) = Q_1(v)$.
- For $W \subset V$, $(W, Q|_W)$ is a **quadratic subspace**.

Theorem (Witt's Cancellation Theorem)

Let U_1, U_2, V_1, V_2 be quadratic spaces where V_1 and V_2 are isometrically isomorphic. If $U_1 \oplus V_1 \cong U_2 \oplus V_2$, then $U_1 \cong U_2$.

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 $F(U_1) = U_2$.

Our interest: $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$ where $\mathrm{dot}(\mathbf{x}) = x_1^2 + \cdots + x_n^2$.

We call it a (nondegenerate) quadratic space of **Euclidean type**.

Our interest: $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$ where $\mathrm{dot}(\mathbf{x}) = x_1^2 + \cdots + x_n^2$.

We call it a (nondegenerate) quadratic space of **Euclidean type**.

Q. What about quadratic subspaces of $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$?

Our interest: $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$ where $\mathrm{dot}(\mathbf{x}) = x_1^2 + \cdots + x_n^2$.

We call it a (nondegenerate) quadratic space of **Euclidean type**.

Q. What about quadratic subspaces of $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$?

Possible k-dimensional quadratic subspaces:

$$\mathrm{dot}_k, \mathrm{dot}_{k-1} \oplus 0, \cdots, \mathrm{dot}_1 \oplus 0^{k-1}$$

$$\lambda\mathrm{dot}_k, \lambda\mathrm{dot}_{k-1} \oplus 0, \cdots, \lambda\mathrm{dot}_1 \oplus 0^{k-1}$$

$$0^k$$

Our interest: $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$ where $\mathrm{dot}(\mathbf{x}) = x_1^2 + \cdots + x_n^2$.

We call it a (nondegenerate) quadratic space of **Euclidean type**.

Q. What about quadratic subspaces of $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$?

Possible k-dimensional quadratic subspaces:

$$\mathrm{dot}_k, \mathrm{dot}_{k-1} \oplus 0, \cdots, \mathrm{dot}_1 \oplus 0^{k-1}$$

$$\lambda\mathrm{dot}_k, \lambda\mathrm{dot}_{k-1} \oplus 0, \cdots, \lambda\mathrm{dot}_1 \oplus 0^{k-1}$$

$$0^k$$

Let W be a **$\mathbf{dot_k}$-subspace** if W is isometrically isomorphic to dot_k with $\mathrm{dot}_n|_W$.

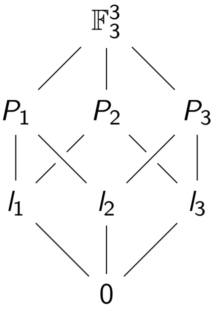
$\Rightarrow$ We are only looking at dot_k-subspaces of $(\mathbb{F}_q^n, \mathrm{dot}(\mathbf{x}))$.

Outline

- Define a poset $E_n(q) := (\mathrm{dot}_{k,n}, \subset)$.
- Call it the **Euclidean poset**.

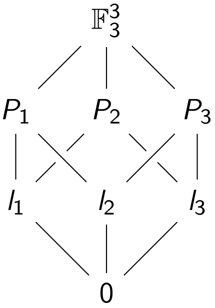
- Define a poset $E_n(q) := (\mathrm{dot}_{k,n}, \subset)$.
- Call it the **Euclidean poset**.
- We do not consider the empty set to be a subspace.
- We consider the zero space as the least element of the Euclidean poset.

Example. In $E_3(q) = (\mathbb{F}_3^3, \mathrm{dot}_3(\mathbf{x}))$,



$$P_1 = \langle (1,0,0),(0,1,0) \rangle \,, \;\; P_2 = \langle (1,0,0),(0,0,1) \rangle \,,$$
$$P_3 = \langle (0,1,0),(0,0,1) \rangle \,,$$
$$l_1 = \langle (1,0,0) \rangle \,, \;\; l_2 = \langle (0,1,0) \rangle \,, \;\; l_3 = \langle (0,0,1). \rangle$$

Example. In $E_3(q) = (\mathbb{F}_3^3, \mathrm{dot}_3(\mathbf{x}))$,



$$
\begin{aligned}
&P_1 = \langle (1,0,0),(0,1,0) \rangle\,,\;\; P_2 = \langle (1,0,0),(0,0,1) \rangle\,,\\
&P_3 = \langle (0,1,0),(0,0,1) \rangle\,,\\
&\;l_1 = \langle (1,0,0) \rangle\,,\;\; l_2 = \langle (0,1,0) \rangle\,,\;\; l_3 = \langle (0,0,1).\rangle
\end{aligned}
$$

Notice that any vertex in $E_n(q)$ has the same degree by Witt's Theorems.

Lemma

For each k and n, the number of dot_k subspaces in dot_n containing a spacelike line is $|\mathrm{dot}_{k-1,n-1}|$.

Proof.

This counting is independent of which spacelike line is chosen by Witt's Extension Theorem. Let L be a spacelike line. Then we get the following bijection map.

$$\begin{array}{ccc} (\mathrm{dot}_{k-1} \text{ subspaces in } (\mathrm{dot}_n/L)) & \longrightarrow & (\mathrm{dot}_k \text{ containing } L) \\ WL & \mapsto & L \oplus W \end{array}$$

It is easy to show that this map is bijective by its definition. □

Euclidean flag is a (maximal) chain in a poset $E_n(q)$. We count flags in two different ways.

Theorem

For each n, we have

$$|dot_{1,k}||dot_{k,n}| = |dot_{1,n}||dot_{k-1,n-1}|.$$

Proof.

Note that

$$\begin{aligned} |\mathrm{dot}_{1,k}| &= \text{spacelike lines in a fixed } \mathrm{dot}_n \text{ subspace} \\ |\mathrm{dot}_{k,n}| &= \text{the number of } \mathrm{dot}_k \text{ subspaces in a fixed } \mathrm{dot}_n \\ |\mathrm{dot}_{1,n}| &= \text{the number of spacelike lines in fixed a } \mathrm{dot}_n \\ |\mathrm{dot}_{k-1,n-1}| &= \text{the number of } \mathrm{dot}_k \text{ subspaces containing a spacelike line.} \end{aligned}$$

□

- $|\mathrm{dot}_{2,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}|}{|\mathrm{dot}_{1,2}|}$.
- $|\mathrm{dot}_{3,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{2,n-1}|}{|\mathrm{dot}_{1,3}|} = \frac{|\mathrm{dot}_{1,n}|}{|\mathrm{dot}_{1,3}|}\frac{|\mathrm{dot}_{1,n-1}||\mathrm{dot}_{1,n-2}|}{|\mathrm{dot}_{1,2}|} = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}||\mathrm{dot}_{1,n-2}}{|\mathrm{dot}_{1,3}||\mathrm{dot}_{1,2}|}$

Therefore, we have

$$|\mathrm{dot}_{k,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}|\cdots|\mathrm{dot}_{1,n-k+1}|}{|\mathrm{dot}_{1,k}|\cdots|\mathrm{dot}_{1,1}|}. \tag{1}$$

- $|\mathrm{dot}_{2,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}|}{|\mathrm{dot}_{1,2}|}$.
- $|\mathrm{dot}_{3,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{2,n-1}|}{|\mathrm{dot}_{1,3}|} = \frac{|\mathrm{dot}_{1,n}|}{|\mathrm{dot}_{1,3}|}\frac{|\mathrm{dot}_{1,n-1}||\mathrm{dot}_{1,n-2}|}{|\mathrm{dot}_{1,2}|} = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}||\mathrm{dot}_{1,n-2}|}{|\mathrm{dot}_{1,3}||\mathrm{dot}_{1,2}|}$

Therefore, we have

$$|\mathrm{dot}_{k,n}| = \frac{|\mathrm{dot}_{1,n}||\mathrm{dot}_{1,n-1}| \cdots |\mathrm{dot}_{1,n-k+1}|}{|\mathrm{dot}_{1,k}| \cdots |\mathrm{dot}_{1,1}|}. \tag{1}$$

Definition

For any n and k, we define

- $[k]_d := |\mathrm{dot}_{1,k}|$;
- $[n]_d! := [n]_d \cdots [1]_d$;
- $\binom{n}{k}_d := |\mathrm{dot}_{k,n}| = \frac{[n!]_d}{[k!]_d[(n-k)!]_d}$.

We call these **dot-analogs**. In particular, we call $\binom{n}{k}_d$ **dot-binomial coefficients**. We adopt the convention that $|\mathrm{dot}_{1,0}| := 1$.

- The number of maximal Euclidean flags in $E_n(q)$ is $[n]_d! = [n]_d\,[n-1]_d \cdots [1]_d$

- The number of maximal Euclidean flags in $E_n(q)$ is $[n]_d! = [n]_d\,[n-1]_d \cdots [1]_d$
- Note that Euclidean flags are bijective up to a factor of 2^n with ON basis.

$$(\because \mathrm{span}(e_1) \subset \mathrm{span}(e_1, e_2) \subset \cdots \subset \mathrm{span}(e_1, e_2, \cdots, e_n).)$$

- The number of maximal Euclidean flags in $E_n(q)$ is $[n]_d! = [n]_d\,[n-1]_d\cdots[1]_d$
- Note that Euclidean flags are bijective up to a factor of 2^n with ON basis.

$$(\because \mathrm{span}(e_1) \subset \mathrm{span}(e_1, e_2) \subset \cdots \subset \mathrm{span}(e_1, e_2, \cdots, e_n).)$$

-

$$\begin{aligned} [n]_d! &= \text{the number of the Euclidean flags} \\ &= \text{the number of orthonormal bases up to } \pm \\ &= \frac{|O(n,q)|}{2^n} \end{aligned}$$

$$\Rightarrow |O(n,q)| = 2^n\,[n]_d!.$$

- $$\begin{aligned}\binom{n}{k}_d &= \frac{[n]_d!}{[k]_d!\,[n-k]_d!} \\ &= \frac{|O(n,q)|}{|O(k,q)\times O(n-k,q)|}\cdot\frac{2^k\cdot 2^{n-k}}{2^n} \\ &= \left|\frac{O(n,q)}{O(k,q)\times O(n-k,q)}\right|.\end{aligned}$$

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

Table: The q-analogues and the dot-analogues.

Question. How to count $|\mathrm{dot}_{1,k}|$?

Theorem

In $(\mathbb{F}_q^n, x_1^2 + x_2^2 + \cdots + x_n^2)$, *the number of spacelike lines,* $|dot_{1,n}|$, *is following:*

<table>
<tr><th>Spacelike</th><th>q ≡ 1 mod 4</th><th>q ≡ 3 mod 4</th></tr>
<tr><td>$n = 4k+3$</td><td rowspan="2">$\frac{q^{n-1}+q^{\frac{n-1}{2}}}{2}$</td><td>$\frac{q^{n-1}-q^{\frac{n-1}{2}}}{2}$</td></tr>
<tr><td>$n = 4k+1$</td><td>$\frac{q^{n-1}+q^{\frac{n-1}{2}}}{2}$</td></tr>
<tr><td>$n = 4k+2$</td><td rowspan="2">$\frac{q^{n-1}-q^{\frac{n-2}{2}}}{2}$</td><td>$\frac{q^{n-1}+q^{\frac{n-2}{2}}}{2}$</td></tr>
<tr><td>$n = 4k$</td><td>$\frac{q^{n-1}-q^{\frac{n-2}{2}}}{2}$</td></tr>
</table>

Table: *The number of spacelike lines in* dot_n.

Outline

More results

- A new isometric invariant of combinatorial type on quadratic spaces over finite fields. It can distinguish even degenerate cases.
- Recover the size of Minkowski's sphere.
- Existence of types of quadratic subspaces in $\mathbb{F}_q^n$.
- $E_n(q)$ is rank symmetric, rank unimodal, log-concave, and Sperner.
- Compute the Mobius function for $E_n(q)$.
- We study its combinatorial properties such as Pascal's triangle, the dot-binomial coefficients are rational in q, compute $\lim_{q\to 1} \binom{n}{k}_d$.

Question. Can we find other combinatorial descriptions of dot-binomial coefficients?

References

Pete L. Clark
Quadratic forms chapter I: Witt's theory
http://math.uga.edu/~pete/quadraticforms.pdf

Keith Conrad
Bilinear Forms
https://kconrad.math.uconn.edu/blurbs/linmultialg/bilinearform.pdf

Semin Yoo (2019)
Combinatorial structures of quadratic spaces over finite fields
Preprint

Thank you for your attention!