FIVE DAYS INTRODUCTION TO THE THEORY OF DESIGNS

at OSAKA CITY UNIVERSITY

December 4-8, 1989

by Hiroshi SUZUKI

INTRODUCTION.

Since I started studying combinatorics, I have been attracted by the beautifulness of the Delsarte theory in designs and codings and the difficulty of the constructions.

When I was given a previledge of giving a series of lectures on design theory, I decided to present Delsarte theory (Theorem 3.2) by the original Ray-Chaudhuri and Wilson version. There are two reasons why I didn't use association schemes. Firstly because of my limited knowledge it seemed impossible to go through the basics of association schemes and to develop it to Delsarte theory in five lectures. Secondly, I thought it is important to see the results in each individual association scheme to consider extremal problems such as the existence problem of tight t-designs. (See Remarks on DAY 3 and Theorem 4.1.) I believe that we can appreciate Delsarte theory better, after going through the original Ray-Chaudhuri and Wilson version. So I wish that this note serves as an introduction to the paper [12].

I also attempted to write an 'easy to read' proof of the existence of t-designs by Teirlinck. This proof was introduced in a book [1], written in Japanese. Since the theorem itself is epoch making, I thought it is important to write down the translation of the proof in English.

I included the topics from the designs over a finite field, or equivalently the designs in the Q-polynomial association scheme called the q-analogue of Johnson. Recently the first nontrivial examples were constructed. It is a new area and there are a lot of

interesting problems to be considered.

I thank the members of the department of mathematics at Osaka City University, especially Professor Tsushima, Professor Okuyama and Professor Kawata who gave me the opportunity of giving this lecture. I am much indebted to Professor T. Ito for encouraging me to write this note and giving me valuable comments.

DAY 1.

Let $V = \{ 1, 2, \ldots, v \}$ and $\binom{V}{k}$ be the family of all k-element subsets of V.

Definition 1.1. $\phi \neq \mathcal{B} \subset \binom{V}{k}$ is a t-(v,k,λ) design (or t-design for short, $S_\lambda(t,k,v)$ in some literature) if $0 \leq t \leq k \leq v$ and

$\lambda(\alpha) = |\{ B \in \mathcal{B} \mid \alpha \subset B \}| = \lambda$ for all $\alpha \in \binom{V}{t}$,

i.e., the number $\lambda(\alpha)$ does not depend on the choice of a t-element subset α of V.

The design is nontrivial if $\mathcal{B} \neq \binom{V}{k}$ and $0 < t < k < v$.

For finite sets A and B let Mat(A,B) denote the set of all matrices over the real numbers $\mathbb{R}$ having A and B as row and column labeling sets. For $M \in Mat(A,B)$ and $(\alpha,\beta) \in A \times B$, $M[\alpha,\beta]$ denotes the (α,β) entry of M. Let $\mathbb{1}_A$ denote the all one column vector whose rows are indexed by the set A. By abuse of notation $\mathbb{1}_A$ may denote the characteristic vector of A. Let $\mathbb{1}_i$ be $\mathbb{1}\binom{V}{i}$.

Let W_{ik}^j be a matrix in $Mat(\binom{V}{i},\binom{V}{k})$ whose (α,β) entry $W_{ik}^j[\alpha,\beta]$ is 1 if $\alpha \cap \beta \in \binom{V}{j}$ and is 0 otherwise.

For $\mathcal{B} \subset \binom{V}{k}$, let N_i^j be a matrix in $Mat(\binom{V}{i},\mathcal{B})$, whose (α,B) entry $N_i^j[\alpha,B]$ is 1 if $\alpha \cap B \in \binom{V}{j}$ and is 0 otherwise.

We write W_{ik} for W_{ik}^i and N_i for N_i^i. Clearly we have $W_{ik}^j N_k = N_i^j$ and if $\mathcal{B} = \binom{V}{k}$, $N_i^j = W_{ik}^j$.

By the definition of t-designs, it is easy to see that $\phi \neq \mathcal{B} \subset \binom{V}{k}$ is a t-(v,k,λ) design if and only if $N_t \mathbb{1}_{\mathcal{B}} = \lambda \mathbb{1}_t$ (or we may write $W_{tk} \mathbb{1}_{\mathcal{B}} = \lambda \mathbb{1}_t$).

Example 1.1. Let $V = PG(m-1,q)$ be the set of projective points of an m-1 dimensional projective space, i.e., the set of 1 dimensional subspaces of an m dimensional vector space U over a finite field $GF(q)$. Let $\mathcal{B}$ be the collection of r-1 dimensional projective subspaces in $PG(m-1,q)$, i.e., the collection of subsets of V corresponding to r dimensional vector subspaces of U. Then $\mathcal{B}$ is a 2-$\left(\binom{m}{1}_q, \binom{r}{1}_q, \binom{m-2}{r-2}_q\right)$ design, where

$$\binom{n}{s}_q = \prod_{i=0}^{s-1} \frac{q^{n-i}-1}{q^{s-i}-1}$$

is the number of s dimensional subspaces in an n dimensional vector space over $GF(q)$.

Let $\binom{V}{r}_q$ denote the collection of r-1 dimensional projective subspaces. Then $\phi \neq \mathcal{B} \subset \binom{V}{r}_q$ is called a t-$(m,r,\lambda;q)$ design if $0 \leq t \leq r \leq m$ and

$$\lambda(\alpha) = |\{ B \in \mathcal{B} \mid \alpha \subset B\}| = \lambda \quad \text{for all} \quad \alpha \in \binom{V}{t}_q.$$

Note that $\binom{V}{k}_q$ is a t-$(m,k,\lambda;q)$ design for all possible t by this definition. We may discuss the theory of t-$(m,r,\lambda;q)$ design in a similar way, and in most cases we can obtain the assertions of classical t-(m,r,λ) designs just by taking the limit as q tends to 1. But to avoid confusion we discuss the classical t-designs defined in Definition 1.1 only and discuss t-$(m,r,\lambda;q)$ designs separately on Day 4. Note that

$$\lim_{q \to 1} \binom{n}{s}_q = \binom{n}{s}.$$

Example 1.2. Let $V = GF(q)$ with $q \equiv 3 \pmod 4$ and $R = GF(q)^{\times 2} = \{ a^2 \mid a \in GF(q) - \{0\} \}$ the set of quadratic residues of $GF(q)$. Let $\mathcal{B} = \{ R + a \mid a \in GF(q) \}$. Then $\mathcal{B}$ is a $2\text{-}(q,\frac{1}{2}(q-1),\frac{1}{4}(q-3))$ design. A $2\text{-}(v,\frac{1}{2}(v-1),\frac{1}{4}(v-3))$ design is called a Hadamard 2-design. A $\{1,-1\}$ square matrix H of size $v+1$ is called a Hadamard matrix if $HH^T = (v+1)I$. It is easy to check that, if $\mathcal{B}$ is a Hadamard 2-design, i.e., $2\text{-}(v,\frac{1}{2}(v-1),\frac{1}{4}(v-3))$ design and N_1 is the matrix defined above then the matrix

$$H = \begin{pmatrix} 1_0 & 1_{\mathcal{B}}^T \\ 1_1 & 2N_1 - J \end{pmatrix}$$

becomes a Hadamard matrix, where $J = 1_1 1_{\mathcal{B}}^T$, the all one matrix of the suitable size. Moreover if there is a Hadamard matrix we can always obtain Hadamard 2-designs. It is easy to see that if $\mathcal{B}$ is a Hadamard $2\text{-}(v,\frac{1}{2}(v-1),\frac{1}{4}(v-3))$ design with $v \geq 3$, then $v \equiv 3 \pmod 4$. The converse is the Hadamard conjecture, i.e., if $v \equiv 3 \pmod 4$ then there is a Hadamard $2\text{-}(v,\frac{1}{2}(v-1),\frac{1}{4}(v-3))$ design!? If $q = 7$, the matrix N_1 of the design given above is the following.

$$N_1^T = \begin{array}{c} \begin{pmatrix} 0&1&1&0&1&0&0 \\ 0&0&1&1&0&1&0 \\ 0&0&0&1&1&0&1 \\ 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 1&0&1&0&0&0&1 \\ 1&1&0&1&0&0&0 \end{pmatrix} \\ \overline{0}\ \overline{1}\ \overline{2}\ \overline{3}\ \overline{4}\ \overline{5}\ \overline{6} \end{array} \begin{array}{l} R + \overline{0} \\ R + \overline{1} \\ R + \overline{2} \\ R + \overline{3} \\ R + \overline{4} \\ R + \overline{5} \\ R + \overline{6} \end{array}$$

With the suitable ordering of the columns and the rows we obtain the same matrix N_1 for the design given in Example 1.1 with $m = 3$, $r = 2$, $q = 2$.

Exercise. Check the assertions in Example 1.2.

Hint: Let χ be the Legendre symbol of $GF(q)$, q odd, i.e., $\chi(a) = 1$ if $a \in R = GF(q)^{\times 2}$, $\chi(a) = -1$ if $a \in GF(q)^{\times} - R$ and $\chi(0) = 0$. Then for $b \neq c$

$$\sum_{y\in GF(q)} \chi(y+b)\chi(y+c) = \sum_{\substack{y\in GF(q)\\ y+c\neq 0}} \chi\left(\frac{y+b}{y+c}\right)\chi(y+c)^2$$

$$= \sum_{\substack{y\in GF(q)\\ y+c\neq 0}} \chi\left(\frac{y+b}{y+c}\right) = \sum_{\substack{y\in GF(q)\\ z\neq 1}} \chi(z) = \sum_{z\in GF(q)} \chi(z) - 1 = -1.$$

Use the identity above.

Lemma 1.1. *Let* $\mathcal{B} \subset \binom{V}{k}$. *Then*

$W_{is}N_s = \binom{k-i}{s-i} N_i$.

Proof. $W_{is}N_s[\alpha,B] = |\{\ \beta \in \binom{V}{s} \mid \alpha \subset \beta \subset B\ \}| = \binom{k-i}{s-i}$.

Lemma 1.2. *Let* $\mathcal{B}$ *be a* t-(v,k,λ) *design. Then* $\mathcal{B}$ *is a* i-(v,k,λ_i) *design with*

$$\lambda_i = \lambda\frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}} = \lambda\frac{\binom{v-i}{k-i}}{\binom{v-t}{k-t}} = \lambda\frac{(v-i)\cdots(v-t+1)}{(k-i)\cdots(k-t+1)} = \frac{\binom{v-i}{k-i}|\mathcal{B}|}{\binom{v}{k}},$$

$i = 0, 1, 2, \ldots, t$. *In particular these numbers are integers.*

Proof. Let $0 \le i \le t$. Since $\binom{k-i}{t-i} \neq 0$,

$$N_i\mathbb{1}_{\mathcal{B}} = \frac{1}{\binom{k-i}{t-i}} W_{it}N_t\mathbb{1}_{\mathcal{B}} = \frac{\lambda}{\binom{k-i}{t-i}} W_{it}\mathbb{1}_t = \lambda\frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}\mathbb{1}_i.$$

Since $\binom{v-i}{t-i}\binom{v-t}{k-t} = \binom{k-i}{t-i}\binom{v-i}{k-i}$ and $\lambda_0 = |\mathcal{B}|$, the assertion holds. Note that for $\alpha \in \binom{V}{i}$,

$$(W_{it}\mathbb{1}_t)[\alpha] = |\{\ \beta \in \binom{V}{t} \mid \alpha \subset \beta\ \}| = \binom{v-i}{t-i}.$$

Corollary 1.1. *Let* $\mathcal{B}$ *be a* t-(v,k,λ) *design. Then*

$$|\mathcal{B}| = \lambda\frac{\binom{v}{t}}{\binom{k}{t}} \geq \frac{\binom{v}{t}}{\binom{k}{t}}.$$

A t-design with $\lambda = 1$ is called a Steiner system.

Let $\mathcal{B}$ be a t-(v,k,λ) design and $x \in V$, $V_1 = V - \{x\}$. Let

$\mathcal{B}_1 = \{ B \cap V_1 \mid x \in B \in \mathcal{B} \}$,

$\mathcal{B}_2 = \{ B \cap V_1 \mid x \in V - B, B \in \mathcal{B} \}$,

then it is easy to see that $\mathcal{B}_1$ is a (t-1)-(v-1,k-1,λ) design and $\mathcal{B}_2$ is a (t-1)-(v-1,k,λ_{t-1}-λ) design. $\mathcal{B}_1$ is called a derived design and $\mathcal{B}_2$ is a residual design. $\mathcal{B}$ is called an extension of $\mathcal{B}_1$.

Let $\mathcal{P} = \bigcup_{i=0}^{v} \binom{V}{i}$ and G a subgroup of $S^V = S_v$, the symmetric group on V. Then G is a permutation group on $\mathcal{P}$, i.e., a subgroup of $S^{\mathcal{P}}$. So G can be embedded as a subgroup in $\mathrm{Mat}(\mathcal{P},\mathcal{P})$ as follows; for $a \in G$, P(a) is a matrix in $\mathrm{Mat}(\mathcal{P},\mathcal{P})$, whose $(\alpha,\beta) \in \mathcal{P} \times \mathcal{P}$ entry $P(a)[\alpha,\beta]$ is 1 if $\alpha^a = \beta$ and is 0 otherwise. Now $\mathcal{P}/G$ denotes the set of orbits of G on $\mathcal{P}$. Let

$$\mathrm{Mat}_G(\mathcal{P},\mathcal{P}) = \{ M \in \mathrm{Mat}(\mathcal{P},\mathcal{P}) \mid P(a)M = MP(a) \text{ for all } a \in G \}.$$

We define an algebra homomorphism

$$\tau : \mathrm{Mat}_G(\mathcal{P},\mathcal{P}) \to \mathrm{Mat}(\mathcal{P}/G,\mathcal{P}/G).$$

Let F be a matrix in $\mathrm{Mat}(\mathcal{P},\mathcal{P}/G)$ whose (α,Δ) entry $F[\alpha,\Delta]$ is $|\Delta|^{-\frac{1}{2}}$ if $\alpha \in \Delta$ and is 0 otherwise. Let D be a matrix in $\mathrm{Mat}(\mathcal{P}/G,\mathcal{P}/G)$, whose (Δ,Γ) entry $D[\Delta,\Gamma]$ is $|\Delta|$ if $\Delta = \Gamma$ and is

0 otherwise. Let $\tau(M) = D^{-\frac{1}{2}}F^{T}MFD^{\frac{1}{2}}$. Then the following hold.

Proposition 1.1. *(1) FF^{T} is in the center of $Mat_{G}(\mathcal{P},\mathcal{P})$.*

(2) $F^{T}F = I$ in $Mat(\mathcal{P}/G,\mathcal{P}/G)$.

(3) τ is a surjective algebra homomorphism from $Mat_{G}(\mathcal{P},\mathcal{P})$ to $Mat(\mathcal{P}/G,\mathcal{P}/G)$.

Proof. (1) Let $M \in Mat_{G}(\mathcal{P},\mathcal{P})$ and $\alpha, \beta \in \mathcal{P}$. Then

$$\begin{aligned} MFF^{T}[\alpha,\beta] &= \sum_{\delta\in\mathcal{P}} \sum_{\Delta\in\mathcal{P}/G} M[\alpha,\delta]F[\delta,\Delta]F[\beta,\Delta] \\ &= \sum_{\delta\in\beta^{G}} M[\alpha,\delta]/|\beta^{G}| = \frac{1}{|G|}\sum_{g\in G} M[\alpha,\beta^{g}] \\ &= \frac{1}{|G|}\sum_{g\in G} M[\alpha^{g},\beta] = \sum_{\gamma\in\alpha^{G}} M[\gamma,\beta]/|\alpha^{G}| \\ &= \sum_{\Delta\in\mathcal{P}/G} \sum_{\gamma\in\mathcal{P}} F[\alpha,\Delta]F[\gamma,\Delta]M[\gamma,\beta] \\ &= FF^{T}M[\alpha,\beta]. \end{aligned}$$

(2) Clear.

(3) It is clear that τ is a linear mapping. Let $M, N \in Mat_{G}(\mathcal{P},\mathcal{P})$. Then

$$\begin{aligned} \tau(M\cdot N) &= D^{-\frac{1}{2}}F^{T}MNFD^{\frac{1}{2}} = D^{-\frac{1}{2}}F^{T}MNFF^{T}FD^{\frac{1}{2}} \\ &= D^{-\frac{1}{2}}F^{T}MFF^{T}NFD^{\frac{1}{2}} = \tau(M)\tau(N). \end{aligned}$$

For $M \in Mat(\mathcal{P}/G,\mathcal{P}/G)$ define $N \in Mat_{G}(\mathcal{P},\mathcal{P})$ by $N[\alpha,\beta] = M[\alpha^{G},\beta^{G}]/|\beta^{G}|$. Then

$$\begin{aligned} \tau(N)[\Delta,\Gamma] &= (D^{-\frac{1}{2}}F^{T}NFD^{\frac{1}{2}})[\Delta,\Gamma] \\ &= \left(\frac{|\Gamma|}{|\Delta|}\right)^{\frac{1}{2}} \sum_{\alpha\in\mathcal{P}} \sum_{\beta\in\mathcal{P}} F[\alpha,\Delta]N[\alpha,\beta]F[\beta,\Gamma] \\ &= \frac{1}{|\Delta|}\sum_{\alpha\in\Delta} \sum_{\beta\in\Gamma} N[\alpha,\beta] = M[\Delta,\Gamma]. \end{aligned}$$

Hence τ is surjective.

By abuse of notations we view W^j_{ik} and N^j_i as matrices in $\mathrm{Mat}(\mathcal{P},\mathcal{P})$, i.e., the matrix such that the $\binom{V}{i} \times \binom{V}{k}$ block is W^j_{ik} (or N^j_i respectively) and the other blocks are 0 matrices. Let A^j_{tk} and B^j_{tk} be matrices in $\mathrm{Mat}(\binom{V}{t}/G, \binom{V}{k}/G)$ defined as follows.

$$A^j_{tk}[\Delta,\Gamma] = |\{ \alpha \in \Gamma \mid \beta \cap \alpha \in \binom{V}{j} \}|, \text{ where } \beta \in \Delta,$$
$$B^j_{tk}[\Delta,\Gamma] = |\{ \beta \in \Delta \mid \beta \cap \alpha \in \binom{V}{j} \}|, \text{ where } \alpha \in \Gamma.$$

Proposition 1.2. *(1)* $B^j_{tk}D_{kk} = D_{tt}A^j_{tk}$, *where* D_{ij} *is the* $\binom{V}{i}/G \times \binom{V}{j}/G$ *block of* D.

(2) $\tau(W^j_{ik}) = A^j_{ik}$.

(3) $\tau(W^j_{ik}{}^T) = B^j_{ik}{}^T$.

Proof. (1) $B^j_{tk}D_{kk}[\Delta,\Gamma]$

$$= \sum_{E \in \binom{V}{k}/G} B^j_{tk}[\Delta,E]D_{kk}[E,\Gamma] = B^j_{tk}[\Delta,\Gamma]|\Gamma|$$
$$= |\Gamma||\{ \delta \in \Delta \mid \delta \cap \gamma \in \binom{V}{j}\}|, \text{ where } \gamma \in \Gamma$$
$$= |\{ (\delta,\gamma) \in \Delta \times \Gamma \mid \delta \cap \gamma \in \binom{V}{j} \}|$$
$$= |\Delta||\{ \gamma \in \Gamma \mid \delta \cap \gamma \in \binom{V}{j} \}|, \text{ where } \delta \in \Delta$$
$$= |\Delta|A^j_{tk}[\Delta,\Gamma] = D_{tt}A^j_{tk}[\Delta,\Gamma].$$

(2) $\tau(W^j_{ik})[\Delta,\Gamma]$

$$= \frac{1}{|\Delta|}\sum_{\delta\in\Delta}\sum_{\gamma\in\Gamma} W^j_{ik}[\delta,\gamma] = \frac{1}{|\Delta|}|\{ (\delta,\gamma) \in \Delta \times \Gamma \mid \delta \cap \gamma \in \binom{V}{j} \}|$$
$$= A^j_{ik}[\Delta,\Gamma].$$

(3) Similar to (2).

Since $\mathcal{B}$ is a G-invariant t-(v,k,λ) design, i.e., the members of $\mathcal{B}$ are permuted by the elements of G, if and only if

$A_{tk}\mathbb{1}_{\mathcal{B}} = \lambda\mathbb{1}_t$, or $\mathcal{B} = \Gamma_1 \cup \ldots \cup \Gamma_u$ ($\Gamma_i \in \binom{V}{k}/G$) is a t-(v,k,λ) design if and only if

$$\sum_{i=1}^{u} A_{tk}[\Delta,\Gamma] = \lambda \quad \text{for all} \quad \Delta \in \binom{V}{t}/G,$$

we can investigate the existence of G-invariant t-designs using the matrix A_{tk}, which is possibly much smaller than W_{tk}. In particular if G is transitive on $\binom{V}{t}$, i.e., t-homogeneous, A_{tk} is a $1 \times |\binom{V}{k}/G|$ matrix. So every collection of G orbits on $\binom{V}{k}$ yields a t-design.

Example 1.3. Let $G = M_{24}$, $V = \{ 1,2,\ldots,24 \}$. Then G is 5-transitive on V. Hence any collection of G orbits on $\binom{V}{k}$ other than $\binom{V}{k}$ with $5 < k < 24-5$ becomes a nontrivial 5-design. For example we have 5-(24,8,1) design, which is called a Witt design.

Example 1.4. Let G be an abelian group of order v. If $(v,(2r)!) = 1$, then

$$\mathcal{B}_r = \{ L_r(U) \mid U \in \binom{G}{2} \}, \text{ where}$$

$$L_r(U) = \{ a_1 \cdots a_r \mid a_i \in U \} = \{ a^i b^{r-i} \mid i=0,1,\ldots,r \}$$

with $U = \{ a,b \}$,

is a 2-$(v,r+1,\binom{r+1}{2})$ design.

Example 1.5. Let $G = < (1,2,\ldots,7) >$. Then

$$A_{23} = \begin{array}{c} \begin{matrix} \Gamma_1 & \Gamma_2 & \Gamma_3 & \Gamma_4 & \Gamma_5 \\ \{123\} & \{124\} & \{125\} & \{126\} & \{135\} \end{matrix} \\ \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 2 \\ 0 & 1 & 2 & 1 & 1 \end{pmatrix} \end{array} \begin{matrix} \{12\} \\ \{13\} \\ \{14\} \end{matrix}$$

and Γ_2 and Γ_4 both correspond to a 2-(7,3,1) design obtained in

Example 1.2, $\Gamma_1 \cup \Gamma_3 \cup \Gamma_5$ corresponds to a 2-(7,3,3) design in Example 1.4 with $v = 7$, $r = 2$.

Note for DAY 1.

The most of the results discussed here is standard and can be found in any standard textbooks, see for example [1], [17], [20], [26]. The higher incidence matrices W_{ik} are introduced and discussed in [37].

The study of t-designs with a group action is an old subject but is formulated using the homomorphism τ by Kreher in [23], [24].

Example 1.4 was taken from [31], where it is discussed as a limiting case of the design over GF(q) with $q = 1$. See DAY 4.

DAY 2.

We shall prove the Ray-Chaudhuri Wilson inequality on the number of blocks of t-designs and the Bruck-Ryser-Chowla's theorem on symmetric designs. As an introduction we give another definition of t-designs.

For $V = \{ 1,2,\ldots,v \}$, let $\mathbb{R}[V] = \mathbb{R}[x_1,\ldots,x_v]$ be the polynomial ring over $\mathbb{R}$ with v indeterminates. Let $\mathbb{R}[V]_s$ denote the set of polynomials in $\mathbb{R}[V]$ of degree at most s. We identify $\mathbb{R}[V]$ as the set of polynomial functions on $\mathcal{P}$ by embedding $\alpha \in \mathcal{P}$ into $\mathbb{R}^V$ in such a way that the i-th coordinate α_i is 1 if $i \in \alpha$ and is 0 otherwise, i.e, 1_α. For a subset S of $\mathbb{R}^V$ let S^* denote the set of functions from S to $\mathbb{R}$. Then there is a natural homomorphism φ_k from $\mathbb{R}[V]$ to $\binom{V}{k}^*$, which is defined by the restriction of the domain from $\mathbb{R}^V$ to $\binom{V}{k}$.

$$\varphi_k : \mathbb{R}[V] \to \mathcal{P}^* \to \binom{V}{k}^* = \{ g \mid \binom{V}{k} \to \mathbb{R} \}.$$

Then the following hold.

Lemma 2.1. *(1)* $Ker\varphi_k \supset < x_i^2 - x_i,\ x_1+\ldots+x_v-k \mid i=1,\ldots,v >$.

(2) $\varphi_k(\mathbb{R}[V]_s) = \varphi_k(< x_{i_1}\cdots x_{i_s} \mid i_1<\ldots<i_s >_{\mathbb{R}})$ *if* $k \geq s$.

(3) $dim\varphi_k(\mathbb{R}[V]_s) \leq \binom{k}{s}$ *if* $k \geq s$.

Proof. (1) Clear.

(2) Let Y be the right hand side of the equality. By induction on $s-t$ we show that for $i_1<\ldots<i_t$, $t \leq s$, $\varphi_k(x_{i_1}\cdots x_{i_t}) \in Y$. For $s = t$, there is nothing to prove. Let $t < s \leq k$. Let m be different from $i_1,\ldots,i_t$. Then

$$\varphi_k(x_{i_1}\cdots x_{i_t}x_m)$$
$$= \varphi_k(x_{i_1}\cdots x_{i_t}(k-(x_1+\ldots+x_{m-1}+x_{m+1}+\ldots+x_v))$$
$$= (k-t)\varphi_k(x_{i_1}\cdots x_{i_t}) - \sum_{j\neq i_1,\ldots,i_t,m}\varphi_k(x_{i_1}\cdots x_{i_t}x_j).$$

Since the last sum is in Y by the induction hypothesis, $\varphi_k(x_{i_1}\cdots x_{i_t})$ belongs to Y as $k - t \neq 0$.

(3) This follows immediately from (2).

For $i_1<\ldots<i_t$ and $\alpha = \{ i_1,\ldots,i_t \}$, let $x_\alpha = x_{i_1}\cdots x_{i_t}$. Then $x_\alpha(B)$ is 1 if $\alpha \subset B$, and is 0 otherwise for all B in $\mathcal{P}$. Hence $\phi \neq \mathcal{B} \subset \binom{V}{k}$ is a t-(v,k,λ) design if and only if

$$\sum_{B\in\mathcal{B}} x_\alpha(B) = \lambda_t(\alpha) = \lambda \quad \text{for all } \alpha \text{ in } \binom{V}{t}.$$

By Lemma 1.2, $\lambda/|\mathcal{B}| = \binom{v-t}{k-t}/\binom{v}{k}$. So

$$\frac{1}{|\mathcal{B}|}\sum_{B\in\mathcal{B}} x_\alpha(B) = \frac{1}{\binom{v}{k}}\sum_{\beta\in\binom{V}{k}} x_\alpha(\beta).$$

Now by Lemma 2.1.(2)

$$\frac{1}{\binom{v}{k}}\sum_{\alpha\in\binom{V}{k}} f(\alpha) = \frac{1}{|\mathcal{B}|}\sum_{B\in\mathcal{B}} f(B) \quad \text{for all } f \text{ in } \mathbb{R}[V]_t.$$

Let $\frac{1}{|\mathcal{B}|}\sum_{B\in\mathcal{B}} f(B)g(B) = \langle f,g \rangle_{\mathcal{B}}$ be an inner product on $\mathcal{B}^*$.

Then $\langle\ ,\ \rangle_{\mathcal{B}}$ is nondegenerate. Hence by the equation above we have that

$$|\mathcal{B}| = \dim \mathcal{B}^* \geq \dim \varphi_k(\mathbb{R}[V]_s), \text{ where } 2s \leq t,$$

we obtained a bound for $|\mathcal{B}|$.

It will be shown later that $\dim \varphi_k(\mathbb{R}[V]_s) = \binom{v}{s}$ if $k + s \leq v$.

Recall that $\phi \neq \mathcal{B} \subset \binom{V}{k}$ is a t-(v,k,λ) design if and only if

$$\sum_{B\in\mathcal{B}} x_\alpha(B) = \lambda = |\mathcal{B}|\binom{v-t}{k-t}/\binom{v}{k} \quad \text{for all } \alpha \text{ in } \binom{V}{t}.$$

Since $\frac{1}{n}\sum_{i=1}^{n} x_i^2 \geq (\frac{1}{n}\sum_{i=1}^{n} x_i)^2$ and the equality holds if and only if $x_1 = x_i$ for all i, in $\mathbb{R}$, we have that

$$\frac{1}{\binom{v}{t}}\sum_{\alpha\in\binom{V}{t}}(\sum_{B\in\mathcal{B}} x_\alpha(B))^2 \geq (\frac{1}{\binom{v}{t}}\sum_{\alpha\in\binom{V}{t}}(\sum_{B\in\mathcal{B}} x_\alpha(B)))^2 = (\frac{1}{\binom{v}{t}}|\mathcal{B}|\binom{k}{t})^2,$$

and the equality holds if and only if $\mathcal{B}$ is a t-design.

Let $a_i = \frac{1}{|\mathcal{B}|}|\{ (B_1,B_2) \in \mathcal{B}\times\mathcal{B} \mid B_1 \cap B_2 \in \binom{V}{k-i} \}|$, then

$$\sum_{\alpha\in\binom{V}{t}}(\sum_{B\in\mathcal{B}} x_\alpha(B))^2 = \sum_{\alpha\in\binom{V}{t}}\sum_{B_1\in\mathcal{B}}\sum_{B_2\in\mathcal{B}} x_\alpha(B_1)x_\alpha(B_2)$$

$$= \sum_{\alpha\in\binom{V}{t}}\sum_{(B_1,B_2)\in\mathcal{B}\times\mathcal{B}} x_\alpha(B_1\cap B_2) = |\mathcal{B}|\sum_{i=0}^{k} a_i\binom{k-i}{t}.$$

Proposition 2.1. *Let* $\phi \neq \mathcal{B} \subset \binom{V}{k}$.

(1) $$\sum_{i=0}^{k}\binom{k-i}{t}a_i \geq \binom{k}{t}^2|\mathcal{B}|/\binom{v}{t}.$$

(2) The equality holds in (1) if and only if $\mathcal{B}$ *is a t-design and*

$$\sum_{i=0}^{k}\binom{k-i}{u}a_i = \binom{k}{u}\lambda_u, \quad u = 0, 1, \ldots, t.$$

Proof. The last equations can be derived using Lemma 1.2.

Lemma 2.2. *For a* t-(v,k,λ) *design* $\mathcal{B}$, *let* $\alpha \in \binom{V}{r}$ *and* $\beta \in \binom{V}{s}$ *with* $\alpha \cap \beta = \phi$ *and* $r + s \leq t$, *and*

$$\Lambda_r^s(\alpha,\beta) = \{ B \in \mathcal{B} \mid \alpha \subset B,\ B \cap \beta = \phi \}.$$

Let $|\Lambda_r^s(\alpha,\beta)| = \lambda_r^s$. *Then* λ_r^s *does not depend on the choices of* α, β *and the following hold.*

(1) $\lambda_r^s = \lambda_r^{s+1} + \lambda_{r+1}^s$.

(2) $\lambda_r^s = \sum_{u=0}^{s} (-1)^u \binom{s}{u} \lambda_{r+u} = \lambda \binom{v-r-s}{k-r} / \binom{v-t}{k-t}$.

Proof. We prove (1) by induction on s. Note that for s = 0, $\lambda_r^0 = \lambda_r$ and λ_r does not depend on the choice of α by Lemma 1.2. Let $a \in V - (\alpha \cup \beta)$. Then for each $B \in \Lambda_r^s(\alpha, \beta)$, either $B \in \Lambda_{r+1}^s(\alpha \cup \{a\}, \beta)$ or $B \in \Lambda_r^{s+1}(\alpha, \beta \cup \{a\})$ and

$$\Lambda_{r+1}^s(\alpha \cup \{a\}, \beta) \cap \Lambda_r^{s+1}(\alpha, \beta \cup \{a\}) = \phi.$$

Hence we have (1) and we can show that λ_r^s does not depend on the choices of α and β by induction.

(2) It is easily proved by induction but we give alternative proof. Let μ_r^s be the corresponding constants for the trivial design $\binom{V}{k}$. Since $\mu_t^0 = \binom{v-t}{k-t}$, $\lambda_i = \frac{\lambda}{\mu_t^0} \mu_i^0$. So by (1),

$$\lambda_r^s = \frac{\lambda}{\mu_t^0} \mu_r^s = \lambda \frac{\binom{v-r-s}{k-r}}{\binom{v-t}{k-t}},$$

as $\mu_r^s = \binom{v-r-s}{k-r}$.

Proposition 2.2. *Let $\mathcal{B}$ be a t-(v, k, λ) design and N_i be the matrices defined on Day 1, $i = 0, 1, \ldots, k$.* Then

$$N_e N_f^T = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i}^i W_{ie}^T W_{if}, \quad \text{if } e + f \le t.$$

Proof. For $(\alpha, \beta) \in \binom{V}{e} \times \binom{V}{f}$, with $\alpha \cap \beta \in \binom{V}{i}$,

$$N_e N_f^T[\alpha, \beta] = |\{ B \in \mathcal{B} \mid B \supset \alpha \cup \beta \}| = \lambda_{e+f-i},$$

we have

$$N_e N_f^T = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i} W_{ef}^i.$$

On the other hand, since

$$W_{ie}{}^{T}W_{if}[\alpha,\beta] = |\{\ \gamma \in \binom{V}{i} \mid \gamma \subset \alpha \cap \beta\ \}|,$$

$$W_{ie}{}^{T}W_{if} = \sum_{i=0}^{\min\{e,f\}} \binom{u}{i} W_{ef}^{u}.$$

Claim 1 $\quad \sum_{j=i}^{u} (-1)^{j-i}\binom{j}{i}\binom{u}{j} = \delta_{ui}.$

(For) $\quad \sum_{j=i}^{u} (-1)^{j-i}\binom{j}{i}\binom{u}{j} = \sum_{j=i}^{u} (-1)^{j-i}\binom{u-i}{j-i}\binom{u}{i}$

$$= (\sum_{j=0}^{u-i} (-1)^{j}\binom{u-i}{j})\binom{u}{i} = \binom{u}{i}(1-1)^{u-i}.$$

Claim 2 $\quad W_{ef}^{u} = \sum_{i=u}^{\min\{e,f\}} (-1)^{i-u}\binom{i}{u} W_{ie}{}^{T}W_{if}.$

(For) $\quad \sum_{i=u}^{\min\{e,f\}} (-1)^{i-u}\binom{i}{u} \sum_{w=i}^{\min\{e,f\}} \binom{w}{i} W_{ef}^{w}$

$$= \sum_{w=0}^{\min\{e,f\}} (\sum_{i=u}^{w} (-1)^{i-u}\binom{i}{u}\binom{w}{i}) W_{ef}^{w}$$

$$= W_{ef}^{u}.$$

Therefore

$$N_e N_f{}^{T} = \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i} W_{ef}^{i}$$

$$= \sum_{i=0}^{\min\{e,f\}} \lambda_{e+f-i} \sum_{u=i}^{\min\{e,f\}} (-1)^{u-i}\binom{u}{i} W_{ue}{}^{T}W_{uf}$$

$$= \sum_{u=0}^{\min\{e,f\}} (\sum_{j=0}^{u} (-1)^{j}\binom{u}{j}\lambda_{e+f-u+j}) W_{ue}{}^{T}W_{uf}$$

$$= \sum_{u=0}^{\min\{e,f\}} \lambda_{e+f-u}^{u} W_{ue}{}^{T}W_{uf}.$$

Theorem 2.1. *Let $\mathcal{B}$ be a t-(v,k,λ) design. If $2s \le t$ and $k + s \le v$, $|\mathcal{B}| \ge \binom{v}{s}$.*

Proof. Let $e = f = s$ in Proposition 2.2. Then

$$N_s N_s^T = \sum_{i=0}^{s} \lambda_{2s-i}^{i} W_{is}^T W_{is}.$$

For each i, $\lambda_{2s-i}^{i} \geq 0$ and $W_{is}^T W_{is}$ is positive semidefinite. Moreover for $i = s$, $\lambda_{2s-s}^{s} = \lambda_s^s = \lambda\binom{v-2s}{k-s}/\binom{v-t}{k-t} \neq 0$, as $k - s \leq v-2s$ and $W_{ss} = I$. Consequently, $N_s N_s^T$ is positive definite and N_s is of full row rank, which implies $|\mathcal{B}| \geq \binom{v}{s}$.

Theorem 2.2. *Let $\mathcal{B}$ be a t-(v,k,λ) design such that $\mathcal{B}^\sigma = \mathcal{B}$ for all σ in $G \leq S^V$. If $2s \leq t$, $k + s \leq v$,*

$$|\mathcal{B}/G| \geq |\binom{V}{s}/G|.$$

In particular, if G is transitive on $\mathcal{B}$ then G is transitive on $\binom{V}{s}$.

Proof. Let τ be the mapping defined on Day 1. Then

$$A_{s\mathcal{B}} B_{s\mathcal{B}}^T = \sum_{i=0}^{s} \lambda_{2s-i}^{i} B_{is}^T A_{is}.$$

Since $B_{s\mathcal{B}} D_{\mathcal{B}\mathcal{B}} = D_{ss} A_{s\mathcal{B}}$ and $B_{is} D_{ss} = D_{ii} A_{is}$,

$$B_{s\mathcal{B}} D_{\mathcal{B}\mathcal{B}} B_{s\mathcal{B}}^T = D_{ss} A_{s\mathcal{B}} B_{s\mathcal{B}}^T = \sum_{i=0}^{s} \lambda_{2s-i}^{i} D_{ss} B_{is}^T A_{is}$$

$$= \sum_{i=0}^{s} \lambda_{2s-i}^{i} A_{is}^T D_{ii} A_{is}.$$

Hence we can argue similarly as in the proof of Theorem 2.1. We have that $B_{s\mathcal{B}} D_{\mathcal{B}\mathcal{B}} B_{s\mathcal{B}}^T$ is positive definite, which implies the inequality in the theorem.

Definition 2.1. A $2s$-(v,k,λ) design is called tight if $|\mathcal{B}| = \binom{v}{s}$ and $k + s \leq v$.

A tight 2-(v,k,λ) design is called a symmetric (v,k,λ) design.

A symmetric $(v,k,1)$ design is called a projective plane.

Remark. If $\mathcal{B}$ is a G-invariant tight 2s-design, then N_s is a nonsingular square matrix inducing a G-isomorphism from $\binom{V}{s}^*$ to $\mathcal{B}^*$. $|\mathcal{B}/G| = |\binom{V}{s}/G|$ in this case.

The equation

$$N_s N_s^T = \sum_{i=0}^{s} \lambda_{2s-i} W_{is}^T W_{is}$$

indicates that if $\mathcal{B}$ is a tight 2s-design the quadratic form

$$x_1^2 + x_2^2 + \ldots + x_{\binom{v}{s}}^2$$

is rationally equivalent to the form defined by the symmetric matrix

$$\sum_{i=0}^{s} \lambda_{2s-i} W_{is}^T W_{is}.$$

This is the basic observation which leads to the Bruck-Ryser-Chowla's theorem on symmetric designs.

Theorem 2.3. *Let $\mathcal{B}$ be a symmetric (v,k,λ) design. Then the following hold.*

(1) $(v-1)\lambda = k(k-1)$, $\lambda_0 = v$ *and* $\lambda_1 = k$.

(2) (Schutzenberger) If v is even, then $k-\lambda$ is a square.

(3) (Bruck-Ryser-Chowla) If v is odd then the equation

$$nX^2 + (-1)^{(v-1)/2}\lambda Y^2 = Z^2$$

must have a solution in integers X, Y, Z not all zero, where $n = k-\lambda$ and is called the order of the design.

Proof. (1) By Lemma 1.2, $|\mathcal{B}| = \lambda v(v-1)/k(k-1)$. Since the design is symmetric, $|\mathcal{B}| = v$ and we have the assertion.

(2) Let $N_1 = N$. Then the equation in Proposition 2.2 yields

$$NN^T = \lambda W_{01}{}^T W_{01} + \lambda_1^1 W_{11}{}^T W_{11}$$
$$= \lambda J + (k-\lambda)I = \lambda J + nI,$$

where J is the all 1 matrix of size v. Since the eigenvalues of J are v with multiplicity 1 and 0 with multiplicity $v-1$,

$$\det(N)^2 = \det(NN^T) = (\lambda v+n)n^{v-1} = k^2 n^{v-1},$$

as $\lambda v + n = k^2$ by (1). Since N is an integer matrix $k^2 n^{v-1}$ is a square. Thus n is a square if $v-1$ is odd.

(3) Let

$$B = \begin{pmatrix} N & \mathbb{1}_1 \\ \lambda \mathbb{1}_{\mathcal{B}}{}^T & k \end{pmatrix}, \quad \Psi = \begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix},$$

where I_v is the identity matrix of size v and 0 is the 0 matrix of suitable size. Since $NN^T = nI_v + \lambda J$ and $\lambda v - k^2 = -n$, letting $\mathbb{1} = \mathbb{1}_1 = \mathbb{1}_{\mathcal{B}}$, we have

$$B\Psi B^T = \begin{pmatrix} N & \mathbb{1} \\ \lambda \mathbb{1}^T & k \end{pmatrix}\begin{pmatrix} I_v & 0 \\ 0 & -\lambda \end{pmatrix}\begin{pmatrix} N^T & \lambda \mathbb{1} \\ \mathbb{1}^T & k \end{pmatrix}$$
$$= \begin{pmatrix} NN^T - \lambda J & \lambda N\mathbb{1} - \lambda k \mathbb{1} \\ \lambda \mathbb{1}^T N^T - k\lambda \mathbb{1}^T & \lambda^2 v - k^2\lambda \end{pmatrix} = \begin{pmatrix} nI_v & 0 \\ 0 & -n\lambda \end{pmatrix}$$
$$= n\Psi.$$

Hence the quadratic forms

$$Q_1 = y_1^2 + \ldots + y_v^2 - \lambda y_{v+1}^2 \quad \text{and}$$
$$Q_2 = nx_1^2 + \ldots + nx_v^2 - n\lambda x_{v+1}^2$$

are rationally equivalent. In other words $Q_1 = Q_2$, where each x_i is a rational linear combination of $y_1, \ldots, y_{v+1}$.

Sublemma (Lagrange). *For any positive integer t, $tx_1^2 + tx_2^2 + tx_3^2 + tx_4^2$ can be written as $y_1^2 + y_2^2 + y_3^2 + y_4^2$,*

where each y_i *is an integral linear combination of* x_1, x_2, x_3 *and* x_4.

Proof. By a theorem of Lagrange any positive integer t can be written as a sum of 4 squares. (See Hardy and Wright "An Introduction to the Theory of Numbers", Oxford University Press, 302-303). So let $t = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Then

$$t(x_1^2+x_2^2+x_3^2+x_4^2) = (a_1^2+a_2^2+a_3^2+a_4^2)(x_1^2+x_2^2+x_3^2+x_4^2)$$

$$= y_1^2+y_2^2+y_3^2+y_4^2,$$

where

$$y_1 = a_1x_1 - a_2x_2 - a_3x_3 - a_4x_4,$$

$$y_2 = a_1x_2 + a_2x_1 + a_3x_4 - a_4x_3,$$

$$y_3 = a_1x_3 + a_3x_1 + a_4x_2 - a_2x_4,$$

$$y_4 = a_1x_4 + a_4x_1 + a_2x_3 - a_3x_2.$$

Hence using the Witt's cancellation theorem or the specialization we can cancel terms, four at a time.

Case 1 $v \equiv 1 \pmod 4$.

After cancellation we find $y_v^2 - \lambda y_{v+1}^2$ and $nx_v^2 - n\lambda x_{v+1}^2$ are equivalent quadratic forms. Hence they represent the same numbers. The latter represents n at the point (1,0), so there exists a rational point (z,y) such that $z^2 - \lambda y^2 = n$. We have (3) in this case as $(-1)^{(v-1)/2} = 1$.

Case 2 $v \equiv 3 \pmod 4$.

Adding the quadratic form $u^2 + nw^2$ to each of the quadratic forms, we find that $nw^2 - \lambda y_{v+1}^2$ and $u^2 - n\lambda x_{v+1}^2$ are equivalent. So as before, $nw^2 - \lambda y_{v+1}^2$ represents 1 and we have the assertion.

Remark. If $G \leq S^V$ stabilizes $\mathcal{B}$, we can obtain the following matrix equation by applying τ.

$$\begin{pmatrix} B_{1\mathcal{B}} & A_{01}^T \\ \lambda B_{0\mathcal{B}} & k \end{pmatrix}\begin{pmatrix} D_{\mathcal{B}\mathcal{B}} & 0 \\ 0 & -\lambda \end{pmatrix}\begin{pmatrix} B_{1\mathcal{B}}^T & \lambda B_{0\mathcal{B}}^T \\ A_{01} & k \end{pmatrix}$$

$$= \begin{pmatrix} A_{11}^T & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} nD_{11} & 0 \\ 0 & -n\lambda \end{pmatrix}\begin{pmatrix} A_{11} & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\{ \Gamma_1, \ldots, \Gamma_s \} = \mathcal{B}/G$ and $\{ \Delta_1, \ldots, \Delta_s \} = \begin{pmatrix} V \\ 1 \end{pmatrix}/G$, with $\gamma_i = |\Gamma_i|$ and $\delta_j = |\Delta_j|$. Then the quadratic forms

$$Q_1 = \gamma_1 x_1^2 + \ldots + \gamma_s x_s^2 - \lambda x_{s+1}^2 \quad \text{and}$$

$$Q_2 = n\delta_1 y_1^2 + \ldots + n\delta_s y_s^2 - n\lambda y_{s+1}^2$$

are rationally equivalent. So we can discuss similarly if we know γ_i, δ_j explicitly.

Note for DAY 2.

Proposition 2.2 is proved in [37] and is used to show Theorem 2.1. The original proof of it is in [28].

Theorem 2.2 is taken from [23].

Theorem 2.3.(3) was first proved for the case $\lambda = 1$ in [7], and generalized for all λ in [11]. The proof here is taken from [25], which has deeper discussions on symmetric designs with a group action.

DAY 3.

We shall discuss the duality theorem of Ray-Chaudhuri and Wilson. As an introduction we give a definition of s-distance set and the bound of it using the polynomial function ring introduced in the begining of Day 2.

Definition 3.1. A family $\mathcal{B}$ of subsets of V, i.e., $\mathcal{B} \subset \mathcal{P}$, is an s-distance set if $s = |\{\ |B_1 \cap B_2|\ |\ B_1, B_2 \in \mathcal{B},\ B_1 \neq B_2\ \}|$.

Proposition 3.1. *Let $\mathcal{B}$ be an s-distance set of V.*

(1) $|\mathcal{B}| \leq \binom{v}{s} + \ldots + \binom{v}{0}$.

(2) *If* $\mathcal{B} \subset \binom{V}{k}$, *then* $|\mathcal{B}| \leq \binom{v}{s}$.

Proof. We identify elements of $\mathcal{P}$ with $\{0,1\}$-vectors in $\mathbb{R}^V$ as before. Let φ be the restriction homomorphism from $\mathbb{R}[V]$ to $\mathcal{P}^*$. Let $\mathcal{B} = \{ B_1,\ldots,B_m \}$ with $|B_1| \leq \ldots \leq |B_m|$ and

$$\{\ |B_1 \cap B_2|\ |\ B_1, B_2 \in \mathcal{B},\ B_1 \neq B_2\ \} = \{ k_1,\ldots,k_s \},$$

with $k_1 < \ldots < k_s$. Let

$$f_i(x) = \prod_{k_j < |B_i|} (B_i \cdot x - k_j),$$

where $B_i \cdot x$ denotes the dot product, i.e., if $B_i = (b_{i1},\ldots,b_{iv})$, $x = (x_1,\ldots,x_v)$, $B_i \cdot x = b_{i1}x_1 + \ldots + b_{iv}x_v$. Then

$$f_i(B_j) = \begin{cases} 0, & \text{if } 1 \leq j < i \leq m, \\ \text{nonzero}, & \text{if } i = j. \end{cases}$$

So $\{ \varphi(f_1),\ldots,\varphi(f_m) \}$ is linearly independent subset of $\varphi(\mathbb{R}[V]_s)$. Since $\mathrm{Ker}\varphi \supset \langle x_i^2 - x_i \mid i = 1,\ldots,v \rangle$,

$$\varphi(\mathbb{R}[V]_s) = \varphi(\langle x_{i_1} \cdots x_{i_r} \mid 0 \leq r \leq s \rangle_{\mathbb{R}}).$$

Hence

$$|\mathcal{B}| = m \le \dim \varphi(\mathbb{R}[V]_s) \le \binom{v}{s} + \cdots + \binom{v}{0}.$$

If $\mathcal{B} \subset \binom{V}{k}$, we have

$$|\mathcal{B}| = m \le \dim \varphi_k(\mathbb{R}[V]_s) \le \binom{v}{s}$$

by Lemma 2.1.

Proposition 3.2. *(1) Let $\mathcal{B}$ be a t-(v,k,λ) design. If $e + f \le t$ and $u \le f$, then*

$$N_e(N_f^u)^T = \sum_{i=0}^{u} \binom{f-i}{u-i} \lambda_{e+f-i}^{f-u} W_{ef}^i.$$

(2) Let $\mathcal{B}$ be an s-distance set in $\binom{V}{k}$ and $\{ |B_1 \cap B_2| \mid B_1 \neq B_2 \in \mathcal{B} \} = \{ \mu_1, \ldots, \mu_s \}$, $\mu_0 = k$, then

$$N_e^T N_e^u = \sum_{i=0}^{s} \binom{\mu_i}{u} \binom{k-\mu_i}{e-u} N^{\mu_i},$$

where $N^{\mu_i} = N_k^T W_{kk}^{\mu_i} N_k$.

Proof. (1) Let $(\alpha,\beta) \in \binom{V}{e} \times \binom{V}{f}$ with $\alpha \cap \beta \in \binom{V}{i}$. Then by Lemma 2.2,

$$N_e(N_f^u)^T[\alpha,\beta] = |\{ B \in \mathcal{B} \mid \alpha \subset B,\ \beta \cap B \in \binom{V}{u} \}|$$

$$= \sum_{\gamma \in \binom{\beta-\alpha}{u-i}\binom{\beta-\alpha}{f-u}} |\Lambda_{e+f-i}^{f-u}(\alpha \cup (\beta-\gamma), \gamma)|$$

$$= \binom{f-i}{u-i} \lambda_{e+f-i}^{f-u}.$$

(2) Firstly note that

$$N^{\mu_i}[B_1,B_2] = \begin{cases} 1, & \text{if } B_1 \cap B_2 \in \binom{V}{\mu_i}, \\ 0, & \text{otherwise.} \end{cases}$$

Let $B_1, B_2 \in \mathcal{B}$ with $B_1 \cap B_2 \in \binom{V}{\mu}$. Then

$$N_e^T N_e^u[B_1,B_2] = |\{ \alpha \in \binom{V}{e} \mid \alpha \subset B_1,\ \alpha \cap B_2 \in \binom{V}{u} \}|$$
$$= \binom{\mu}{u}\binom{k-\mu}{e-u}.$$

2nd Proof of Theorem 2.1.

Let $e = f = s \leq [t/2]$ in Proposition 3.2.(1). Then

$$N_s(N_s^0)^T = \lambda_s^s W_{ss}^0,$$

.....

$$N_s(N_s^u)^T = \sum_{i=0}^{u-1} \binom{s-i}{u-i} \lambda_{s+u-i}^{s-u} W_{ss}^i + \lambda_s^{s-u} W_{ss}^u,$$

.....

$$N_s(N_s^s)^T = \sum_{i=0}^{s-1} \lambda_{2s-i}^0 W_{ss}^i + \lambda_s^i W_{ss}^s.$$

Since $\lambda_s^i \neq 0$, $0 \leq i \leq s$, by the condition $k + s \leq v$, and $W_{ss}^s = I$,

$$< N_s(N_s^0)^T, \ldots, N_s(N_s^s)^T > = < W_{ss}^0, \ldots, W_{ss}^s >.$$

In particular there is a matrix M in $\mathrm{Mat}(\binom{V}{s}, \mathcal{B})$ such that $I = N_s M^T$. So $\binom{v}{s} \leq |\mathcal{B}|$, as desired.

Remark. By the same argument we can verify a slightly more general theorem.

RESULT Let X and Y be finite sets, $I \subset X \times Y$ and $s \geq 0$. Suppose $\mathcal{B} \subset Y$ satisfy the following.

(i) $|\{ B \in \mathcal{B} \mid \alpha_i \times \{B\} \subset I \}|$ does not depend on the choice of $\alpha_i \in \binom{X}{i}$, for $i = s, \ldots, 2s$.

(ii) For some $\alpha, \beta \in \binom{X}{s}$, $\alpha \cap \beta = \phi$, there is $B \in \mathcal{B}$ such

that $\alpha \times \{B\} \subset I$ and $\beta \times \{B\} \cap I = \phi$.

Then $|\mathcal{B}| \geq \binom{|X|}{s}$.

Proposition 3.3. *Let $\mathcal{B}$ be a 2s+1 design.* If $v-1 \geq k+s$,

$$|\mathcal{B}| = \lambda \frac{\binom{v}{2s+1}}{\binom{k}{2s+1}} \geq \lambda \frac{\binom{v-1}{2s}}{\binom{k-1}{2s}} + \binom{v-1}{s} \geq 2\binom{v-1}{s} > \binom{v}{s}.$$

Moreover if $|\mathcal{B}| = 2\binom{v-1}{s}$, the residual design is a tight 2s-desegn.

Proof. The first equality is from Corollary 1.1. Let $x \in V$, $\mathcal{B}_1 = \Lambda_1^0(\{x\},\phi)$ and $\mathcal{B}_2 = \Lambda_0^1(\phi,\{x\})$. By Lemma 2.2, $\mathcal{B}_1$ defines a $2s\text{-}(v-1,k-1,\lambda)$ design and $\mathcal{B}_2$ defines a $2s\text{-}(v-1,k,\lambda_{2s}^1)$ design. Now the assertion easily follows.

2nd Proof of Proposition 3.1.(2).

Let $e = s$ in Proposition 3.2.(2). Then we have $s+1$ equations.

$$N_s{}^T N_s^u = \sum_{i=0}^{s} \binom{\mu_i}{u}\binom{k-\mu_i}{s-u} N^{\mu_i}, \quad u = 0,\ldots,s.$$

Suppose the matrix P, whose (i,j) entry is $\binom{\mu_i}{j}\binom{k-\mu_i}{s-j}$ is singular. Then there are $c_0,\ldots,c_s$, not all zero such that the polynomial

$$p(x) = c_0\binom{x}{0}\binom{k-x}{s} + c_1\binom{x}{1}\binom{k-x}{s-1} + \ldots + c_s\binom{x}{s}\binom{k-x}{0}$$

has $s+1$ roots, $\mu_0,\ldots,\mu_s$. Since the degree of $p(x)$ is at most s, we have a contradiction. Hence the matrix P is nonsingular and

$$< N_s{}^T N_s^0,\ldots,N_s{}^T N_s^s > = < N^{\mu_0},\ldots,N^{\mu_s} >.$$

Since $N^{\mu_0} = N^k = I$, there is a matrix M' in $\mathrm{Mat}(\binom{V}{s},\mathcal{B})$ such

that $N_s{}^T M' = I$. So $\binom{v}{s} \geq |\mathcal{B}|$.

Lemma 3.1. *For $0 \leq i \leq s \leq k$ the following hold.*

(1) $$W_{is}N_s^j = \sum_{u=0}^{j} \binom{k-u}{j-u}\binom{v-k-i+u}{s-j-i+u} N_i^u.$$

In particular

$$W_{is}N_s = \binom{k-i}{s-i} N_i, \text{ and}$$

$$W_{is}N_s^0 = \binom{v-k-i}{s-i} N_i^0.$$

(2) $$W_{is}{}^T N_i^j = \sum_{u=j}^{s} \binom{u}{j}\binom{s-u}{i-j} N_s^u.$$

In particular

$$W_{is}{}^T N_i = \sum_{u=i}^{s} \binom{u}{i} N_s^u, \text{ and}$$

$$W_{is}{}^T N_i^0 = \sum_{u=0}^{s-i} \binom{s-u}{i} N_s^u.$$

(3) $$N_s^0 = \sum_{i=0}^{s} (-1)^i W_{is}{}^T N_i.$$

(4) $$N_s = \sum_{i=0}^{s} (-1)^i W_{is}{}^T N_i^0.$$

(5) $$I = W_{ss} = \sum_{i=0}^{s} (-1)^i W_{is}^0{}^T W_{is} = \sum_{i=0}^{s} (-1)^i W_{is}{}^T W_{is}^0.$$

Proof. (1) Let $(\alpha, B) \in \binom{V}{i} \times \mathcal{B}$, $\alpha \cap B \in \binom{V}{u}$. Then

$$W_{is}N_s^j[\alpha, B] = |\{ \beta \in \binom{V}{s} \mid \alpha \subset \beta,\ \beta \cap B \in \binom{V}{j} \}|$$

$$= \binom{k-u}{j-u}\binom{v-k-i+u}{s-j-i+u}.$$

Similarly we have (2).

Since $\sum_{j=0}^{u} (-1)^{j-i}\binom{j}{i}\binom{u}{j} = \delta_{iu}$ (see Claim 1 in Proposition

2.2),

$$\sum_{i=0}^{s}(-1)^i W_{is}\,{}^{T}N_i = \sum_{i=0}^{s}(-1)^i \sum_{u=i}^{s}\binom{u}{i}N_s^u = \sum_{u=0}^{s}\Big(\sum_{i=0}^{s}(-1)^i\binom{u}{i}\Big)N_s^u = N_s^0.$$

$$\sum_{i=0}^{s}(-1)^i W_{is}\,{}^{T}N_i^0 = \sum_{i=0}^{s}(-1)^i \sum_{u=0}^{s-i}\binom{s-u}{i}N_s^u = \sum_{u=0}^{s}\Big(\sum_{i=0}^{s}(-1)^i\binom{s-u}{i}\Big)N_s^u =$$

$N_s^s = N_s$.

(5) follows from (4) by setting $k = s$ and $\mathcal{B} = \binom{V}{k}$.

Corollary 3.1. *(1) If $s + k \le v$ and $s \le k$, then rank $W_{sk} = \binom{v}{s}$, and rank $A_{sk} = |\binom{V}{s}/G|$.*

(2) If $s + k \ge v$ and $s \le k$, then rand $W_{sk} = \binom{v}{k}$, and rank $A_{sk} = |\binom{V}{k}/G|$.

Proof. Let $2s \le v$. Then by Lemma 3.1.(5),

$$I = W_{v-s\ v-s}^{v-s} = \sum_{i=0}^{v-s}(-1)^i W_{i\ v-s}^{0}\,{}^{T}W_{i\ v-s}.$$

Since $W_{i\ v-s}^{0} = 0$ if $i \ge s$,

$$I = \sum_{i=0}^{s}(-1)^i W_{i\ v-s}^{0}\,{}^{T}W_{i\ v-s}$$

$$= \Big(\sum_{i=0}^{s}\frac{(-1)^i}{\binom{v-k-i}{k-i}}W_{i\ v-s}^{0}\,{}^{T}W_{is}\Big)W_{s\ v-s}.$$

Hence $W_{s\ v-s}$ is a nonsingular matrix and

$$I = W_{ss}^{s} = W_{s\ v-s}\Big(\sum_{i=0}^{s}\frac{(-1)^i}{\binom{v-k-i}{k-i}}W_{i\ v-s}^{0}\,{}^{T}W_{is}\Big).$$

Applying τ on the equations above, we have that $A_{s\ v-s}$ is nonsingular.

(1) $|\binom{V}{s}/G| = \text{rank } A_{s\ v-s} = \text{rank } A_{s\ k}A_{k\ v-s} \le \text{rank } A_{s\ k}$

$$\leq |\binom{v}{s}/G|.$$

(2) $$|\binom{v}{k}/G| = \text{rank } A_{v-k\ k} = \text{rank } A_{v-k\ s}A_{s\ k} \leq \text{rank } A_{s\ k} \leq |\binom{v}{k}/G|.$$

Lemma 3.2. *Let U_i denote the row space of N_i, i.e., the vector space in $\mathbb{R}^{|\mathcal{B}|}$ spanned by the rows of N_i. Let U_i' denote the row space of N_i^0. Then the following hold.*

(1) $U_0 \subset U_1 \subset \ldots \subset U_k$.

(2) $U_i = U_i'$.

(3) If $\mathcal{B}$ is a 2s-design and $k + s \leq v$, then

$\dim U_i = \binom{v}{i}$ for all $i \leq s$.

Proof. Lemma 3.1.(1) implies that every row of N_i is written as a linear combination of the rows of N_s if $i \leq s$. So we have (1). Similarly we have

$U_0' \subset U_1' \subset \ldots \subset U_k'$.

Now by Lemma 3.1.(3), $U_s' \subset < U_0, \ldots, U_s > = U_s$, and by Lemma 3.1.(4), $U_s \subset < U_0', \ldots, U_s' > = U_s'$. So we have $U_s' = U_s$. If $\mathcal{B}$ is a 2s-design and $k + s \leq v$, N_s is of full row rank $\binom{v}{s}$ (see the proof of Theorem 2.1). Hence we have (3).

Theorem 3.1. *Let $\mathcal{B}$ be a t-(v,k,λ) design. Let $U = \mathbb{R}^{|\mathcal{B}|}$ and U_s denote the row space of N_s in U and P_s the orthogonal projection onto U_s. If $v \geq k + s$ and $2s \leq t$, then*

$$P_s = \sum_{i=0}^{s} (-1)^i \frac{\binom{k-i}{s-i}}{\lambda_s^i} N_i^{0T} N_i$$

$$= \sum_{j=0}^{s'} \Big(\sum_{i=0}^{s} (-1)^i \frac{\binom{k-i}{s-i}}{\lambda_s^i} \binom{k-\mu_j}{i} \Big) N^{\mu_j}$$

$$= \frac{\binom{v-t}{k-t}}{\lambda} \sum_{j=0}^{s'} p_s(\mu_j) N^{\mu_j}$$

with

$$p_s(x) = \sum_{i=0}^{s} (-1)^i \frac{\binom{k-i}{s-i}}{\binom{v-i-s}{k-s}} \binom{k-x}{i}.$$

Here $\{ |B_1 \cap B_2| \mid B_1, B_2 \in \mathcal{B}, B_1 \neq B_2 \} = \{ \mu_1, \ldots, \mu_{s'} \}$ *and* $k = \mu_0$.

Proof. It suffices to prove that $N_s P_s = N_s$ and if $x \in U_s^{\perp}$ then $xP_s = 0$.

Let $x \in U_s^{\perp} \subset U_i^{\perp} = U_{i'}^{\perp}$, $i \leq s$. Then $xN_i^{0T} = 0$. So $xP_s = 0$.

$$N_s P_s = \sum_{i=0}^{s} (-1)^i \frac{\binom{k-i}{s-i}}{\lambda_s^i} N_s N_i^0 N_i = \sum_{i=0}^{s} (-1)^i \binom{k-i}{s-i} W_{is}^{0\,T} N_i$$

$$= \sum_{i=0}^{s} (-1)^i W_{is}^{0\,T} W_{is} N_s = N_s.$$

For the second equality we used $N_s N_i^{0T} = \lambda_s^i W_{is}^{0\,T}$. Since

$$N_i^{0T} N_i = \sum_{j=0}^{s'} \binom{k-\mu_j}{i} N^{\mu_j},$$

we have the assertion.

Corollary 3.2. *Let* $\mathcal{B}$ *be a* t-(v, k, λ) *design with* $t \geq 2s$, $v \geq k + s$ *and* $\{ B_1, \ldots, B_m \} \subset \mathcal{B}$. *Let* $\mu_{ij} = |B_i \cap B_j|$. *Then the* $m \times m$ *matrix* $I - \left(\frac{\binom{v-t}{k-t}}{\lambda} p_s(\mu_{ij}) \right)$ *is positive semidefinite and is singular if* $m > |\mathcal{B}| - \binom{v}{s}$.

Proof. Let $Q_s = I - P_s$. Then Q_s is the orthogonal projection onto $U_s^{\perp}$ of rank $|\mathcal{B}| - \binom{v}{s}$. Hence its principal submatrix is positive semidefinite.

3rd proof of Theorem 2.1.

Let $m = 1$. Since $p_s(k) = \dfrac{\binom{k}{s}}{\binom{v-s}{k-s}}$, $\dfrac{\binom{v-t}{k-t}}{\lambda} p_s(k) = \dfrac{\binom{v}{s}}{|\mathcal{B}|}$.

Applying Theorem 3.1, we have

$$1 - \frac{\binom{v}{s}}{|\mathcal{B}|} \geq 0, \text{ or } |\mathcal{B}| \geq \binom{v}{s}.$$

Corollary 3.3. *Let $\mathcal{B}$ be a t-(v,k,λ) design with $v \geq k + s$, $2s \leq t$. Let B_1, B_2 be distinct elements in $\mathcal{B}$. If the design is tight $|B_1 \cap B_2| = \mu$ is a root of the polynomial $p_s(x)$.*

In particular $s' \leq s$ in this case.

Proof. Let $c = \binom{v-t}{k-t}/\lambda$. By Lemma 3.1 with $m = 2$,

$$\begin{vmatrix} 1-c\cdot p_s(k) & -c\cdot p_s(\mu) \\ -c\cdot p_s(\mu) & 1-c\cdot p_s(k) \end{vmatrix} = 0,$$

or

$$|c\cdot p_s(\mu)| \leq 1 - c\cdot p_s(k) = 0.$$

Since the degree of $p_s(x)$ is s, the number of roots does not exceed s.

Theorem 3.2. *Let $\mathcal{B}$ be a nontrivial t-(v,k,λ) design and an s-distance set. Then $k - [t/2] < v$ and the following hold.*

(1) $\binom{v}{s} \geq |\mathcal{B}| \geq \binom{v}{[t/2]}$.

(2) If $|\mathcal{B}| = \binom{v}{[t/2]}$, *$t$ is even and $s = t/2$.*

(3) If $|\mathcal{B}| = \binom{v}{s}$, *then* $t = 2s$.

Proof. Let $s' = [t/2]$. Suppose $k + s' \geq v$. Then $t \geq 2s' \geq 2(v-k)$. So $\mathcal{B}$ is a $2(v-k)$ design. By Theorem 2.1,

$$\binom{v}{k} > |\mathcal{B}| \geq \binom{v}{v-k} = \binom{v}{k}.$$

A contradiction.

(1) We have proved the inequalities in Theorem 2.1 and Theorem 3.1.

(2) By Proposition 3.3 t is even. Since $\mathcal{B}' = \{ V-B \mid B \in \mathcal{B} \}$ is a nontrivial t-design and s-distance set we may assume that $2k \leq v$. Then $s \geq s'$ by (1). On the other hand we have $s \leq s'$ by Corollary 3.3. Hence we have $2s = t$.

(3) Suppose $|\mathcal{B}| = \binom{v}{s}$. Then by the second proof of Proposition 3.2.(2), there are constants $c_0, \ldots, c_s$ such that

$$N_s^T(c_0N_s^0 + \ldots + c_sN_s^s) = N^{\mu_0} = I.$$

Since N_s is a square matrix, N_s^T is nonsingular. So

$$(c_0N_s^0 + \ldots + c_sN_s^s)N_s^T = I.$$

Since Lemma 3.1 implies

$$W_{is}N_s^j \in \langle N_s^0, \ldots, N_s^j \rangle,$$

$W_{is} = (c_0^iN_i^0 + \ldots + c_i^iN_i^i)N_s^T$, with some constants $c_0^i, \ldots, c_i^i$.

Claim $\langle N_i^0N_s^T, \ldots, N_i^iN_s^T \rangle = \langle W_{is}^0, \ldots, W_{is}^i \rangle$.

(For) We prove the claim above by induction. For $i = 0$,

$$W_{0s} = c_0^0N_0^0N_s^T.$$

Suppose the claim holds for i, then

$$W_{i\ i+1}{}^TW_{is}^j = \sum_{u=j}^{i+1} \binom{u}{j}\binom{i+1-u}{i-j}W_{i+1\ s}^u.$$

Suppose

$$\sum_{j=0}^{i} \alpha_j W_{i\ i+1}{}^{T}W_{is}^{j} + \alpha_{i+1}W_{i+1\ s} = 0$$

Then

$$\sum_{u=0}^{i+1} \Big(\sum_{j=0}^{i} \alpha_j \binom{u}{j}\binom{i+1-u}{i-j} \Big) W_{i+1\ s}^{u} + \alpha_{i+1}W_{i+1\ s} = 0.$$

Since $W_{i+1\ s}^{u}$'s are linearly independent {0,1} matrices, the polynomial

$$f(x) = \sum_{j=0}^{i} \alpha_j \binom{x}{j}\binom{i+1-x}{i-j} + \alpha_{i+1}\binom{x}{i+1}.$$

of degree at most $i+1$ has $i+2$ roots. Hence $f(x) = 0$, and $\alpha_j = 0$ follows easily. Moreover since $W_{i\ i+1}{}^{T}N_i^j$ is in $< N_{i+1}^0, \ldots, N_{i+1}^j >$, we have

$$< W_{i+1\ s}^0, \ldots, W_{i+1\ s}^{i+1} > = < W_{i\ i+1}{}^{T}W_{is}^0, \ldots, W_{i\ i+1}{}^{T}W_{is}^i, W_{i+1\ s} >$$

$$= < W_{i\ i+1}{}^{T}N_i^0 N_s{}^{T}, \ldots, W_{i\ i+1}{}^{T}N_i^i N_s{}^{T}, W_{i+1\ s} >$$

$$\subset < N_{i+1}^0 N_s{}^{T}, \ldots, N_{i+1}^{i+1} N_s{}^{T} >.$$

Since the dimension of the last space is at most $i + 2$, we have the claim.

Hence there are constants $a_0, \ldots, a_s$ such that

$$N_s N_s{}^{T} = \sum_{i=0}^{s} a_i W_{ss}^i.$$

In particular $\lambda_{2s}(\alpha \cup \beta) = a_0$ for all α, β in $\binom{V}{s}$ with $\alpha \cap \beta = \phi$, which shows that $\mathcal{B}$ is a 2s-design.

Remark (1) N. Ito and others showed that the only tight 4-designs are the unique 4-(23,7,1) design and its complement. See [6], [15], [21], [22]. 4-(23,7,1) design is a derived

design of 5-(24,8,1) design in Example 3 on Day 1.

In [27], C. Peterson showed that there are no tight 6-designs using the fact that the polynomial $p_3(x)$ in Corollary 3.3 must have integral roots only. E. Bannai developed this argument and showed that there are only finitely many tight 2s designs for each fixed $s \geq 5$. See [5].

(2) The polynomial used by C. Peterson and E. Bannai has a little different form $\psi_s(x)$. As a closing remark we show it is essentially the same as $p_s(x)$.

Let

$$p_s(x) = \sum_{i=0}^{s} (-1)^i \frac{\binom{k-i}{s-i}}{\binom{v-i-s}{k-s}} \binom{k-x}{i},$$

and

$$\psi_s(x) = \sum_{i=0}^{s} (-1)^{s-i} \frac{\binom{v-s}{i}\binom{k-i}{s-i}\binom{k-1-i}{s-i}}{\binom{s}{i}} \binom{x}{i}.$$

Then

$$\binom{v-2s}{k-s}\binom{v-s}{s} p_s(x) = \psi_s(x).$$

(For) Since

$$P_s = \sum_{j=0}^{k} p_s(j) W_{kk}^{j} = \sum_{j=0}^{k} p_s(j) \sum_{u=0}^{k} (-1)^{r-j} \binom{r}{j} W_{rk}{}^{T} W_{rk},$$

it suffices to show the following.

$$\binom{v-2s}{k-s}\binom{v-s}{s} \sum_{j=0}^{k} p_s(j)(-1)^{r-j}\binom{r}{j}$$

equals 0 if $r > s$ and if $r \leq s$,

$$(-1)^{s-r}\binom{v-s}{r}\binom{k-r}{s-r}\binom{k-1-r}{s-r} / \binom{s}{r}.$$

$$\binom{v-2s}{k-s}\binom{v-s}{s} \sum_{j=0}^{k} p_s(j)(-1)^{r-j}\binom{r}{j}$$

$$= \sum_{j=0}^{k} \sum_{i=0}^{s} (-1)^{i+r-j} \frac{\binom{v-2s}{k-s}\binom{v-s}{s}\binom{k-i}{s-i}\binom{k-j}{i}\binom{r}{j}}{\binom{v-i-s}{k-s}}$$

$$= \sum_{i=0}^{s} (-1)^{i+r} \frac{\binom{v-2s}{k-s}\binom{v-s}{s}\binom{k-i}{s-i}}{\binom{v-i-s}{k-s}} \sum_{j=0}^{k} (-1)^{j} \binom{k-j}{i}\binom{r}{j}. \qquad \ldots(\#)$$

Since it is easy to see by induction on r that

$$\sum_{u=0}^{k-i} (-1)^{u} \binom{k-u}{i}\binom{r}{u} = \binom{k-r}{i-r},$$

(#) yields

$$\sum_{i=0}^{s} (-1)^{i+r} \frac{\binom{v-2s}{k-s}\binom{v-s}{s}\binom{k-i}{s-i}}{\binom{v-i-s}{k-s}} \binom{k-r}{i-r}$$

$$= \sum_{i=0}^{s} (-1)^{i+r} \frac{\binom{v-2s}{k-s}\binom{v-s}{s}\binom{k-i}{k-s}\binom{k-r}{k-i}}{\binom{v-i-s}{k-s}}$$

$$= \binom{k-r}{k-s}\binom{v-2s}{k-s}\binom{v-s}{s} \sum_{i=0}^{s} (-1)^{i+r} \frac{\binom{s-r}{s-i}}{\binom{v-i-s}{k-s}}$$

$$= \binom{k-r}{s-r}\binom{v-2s}{k-s}\binom{v-s}{s} \sum_{i=0}^{s} (-1)^{i+r} \frac{\binom{s-r}{s-i}}{\binom{v-i-s}{k-s}}. \qquad \ldots(\#\#)$$

In particular, if $r > s$, then this is 0. Since

$$\sum_{i=0}^{s} (-1)^{i} \frac{\binom{s-r}{s-i}}{\binom{v-i-s}{k-s}} = (-1)^{s} \frac{\binom{k-1-r}{s-r}}{\binom{v-2s}{k-s}\binom{v-s-r}{s-r}} = (-1)^{s} \frac{k-s}{(k-r)\binom{v-s-r}{k-r}},$$

(##) yields

$$\frac{\binom{k-r}{s-r}\binom{v-2s}{k-s}\binom{v-s}{s}(-1)^{s+r}\binom{k-1-r}{s-r}}{\binom{v-2s}{k-s}\binom{v-s-r}{s-r}}$$

$$= (-1)^{s-r} \frac{\binom{v-s}{r}\binom{k-r}{s-r}\binom{k-1-r}{s-r}\binom{v-s}{s}\binom{s}{r}}{\binom{v-s}{r}\binom{v-s-r}{s-r}\binom{s}{r}}$$

$$= (-1)^{s-r}\frac{\binom{v-s}{r}\binom{k-r}{s-r}\binom{k-1-r}{s-r}\binom{v-s}{s}\binom{s}{s-r}}{\binom{s}{r}\binom{v-s}{v-s-r}\binom{v-s-r}{s-r}}$$

$$= (-1)^{s-r}\frac{\binom{v-s}{r}\binom{k-r}{s-r}\binom{k-1-r}{s-r}}{\binom{s}{r}}.$$

Note for DAY 3.

Proposition 3.1.(1) is in [16] and further discussion on s-distance sets is in [14]. The concept of s-distance sets is introduced and the duality theorem 3.2 except (3) is proved in [28]. Today's material is mainly an introduction of [28]. The duality theorem 3.2 was clarified by the work of Delsarte [12], [13], which uses the duality theorem in linear programing.

For the result quoted in Remark following the 2nd proof of theorem 2.1, see [8], [29], [32].

DAY 4.

We descuss the q-analogue of t-designs. It is easy to see that most of the results obtained for classical t-designs can be translated into the terms of its q-analogue by changing the usual binomial coefficients $\begin{pmatrix} r \\ m \end{pmatrix}$ to $\begin{pmatrix} r \\ m \end{pmatrix}_q$ and putting the appropriate power of q. In stead of stating the corresponding results we show that the Ray-Chaudhuri Wilson type inequality does not give an efficient bound and we present some attempt to construct the q-analogue of t-designs.

We begin with the definition.

Let V be a v-dimensional vector space over a finite field $GF(q)$ with q-elements. Let $\begin{pmatrix} V \\ r \end{pmatrix}_q$ denote the family of all r-dimensional subspaces of V and $\begin{pmatrix} v \\ r \end{pmatrix}_q$ be its number. Then it is easy to see that

$$\begin{pmatrix} v \\ r \end{pmatrix}_q = \prod_{i=0}^{r-1} \frac{q^{n-i}-1}{q^{r-i}-1}.$$

Definition 4.1. $\phi \neq \mathcal{B} \subset \begin{pmatrix} V \\ k \end{pmatrix}_q$ is a t-$(v,k,\lambda;q)$ design (or t-design over $GF(q)$), if $0 \leq t \leq k \leq v$ and

$\lambda(\alpha) = |\{ B \in \mathcal{B} \mid \alpha \subset B \}| = \lambda$ for all α in $\begin{pmatrix} V \\ t \end{pmatrix}_q$,

i.e., the number $\lambda(\alpha)$ does not depend on the choice of the t-dimensional subspace α of V.

The design is nontrivial if $\mathcal{B} \neq \begin{pmatrix} V \\ k \end{pmatrix}_q$ and $0 < t < k < v$.

Just for the technical advantage we adopt a nonsingular bilinear form. So if α is in $\begin{pmatrix} V \\ r \end{pmatrix}_q$, $\alpha^{\perp} = \{ a \in V \mid (a,b) = 0$ for all b

in $\alpha\ \} \in \begin{pmatrix} V \\ v-r \end{pmatrix}_q$. For $\mathcal{B} \subset \begin{pmatrix} V \\ r \end{pmatrix}_q$, $\mathcal{B}^{\perp} = \{\ \alpha^{\perp} \mid \alpha \in \mathcal{B}\ \}$.

The following lemma corresponds to Lemma 1.2 and 2.2.

Lemma 4.2. *Let $\mathcal{B}$ be a t-$(v,k,\lambda;q)$ design. For s and r with $s + r \leq t$, let $\alpha \in \begin{pmatrix} V \\ r \end{pmatrix}_q$, $\beta \in \begin{pmatrix} V \\ s \end{pmatrix}_q$ and $\gamma \in \begin{pmatrix} V \\ v-s \end{pmatrix}_q$ such that $\alpha \cap \beta = 0$ and $\alpha \subset \gamma$. Then we have*

$$\lambda_r^s = \lambda_r^s(\alpha,\beta) = |\{\ B \in \mathcal{B} \mid \alpha \subset B,\ \beta \cap B = 0\ \}|$$

$$= \lambda \cdot \frac{q^{s(k-r)} \begin{pmatrix} v-r-s \\ k-s \end{pmatrix}_q}{\begin{pmatrix} v-t \\ k-t \end{pmatrix}_q}, \text{ and}$$

$$\mu_r^s = \mu_r^s(\alpha,\gamma) = |\{\ B \in \mathcal{B} \mid \alpha \subset B \subset \gamma\ \}|$$

$$= \lambda \cdot \frac{\begin{pmatrix} v-r-s \\ k-s \end{pmatrix}_q}{\begin{pmatrix} v-t \\ k-t \end{pmatrix}_q},$$

and they do not depend on the choices of α, β and γ. They satisfy

$$\lambda_r^s = \lambda_r^{s+1} + q^s \lambda_{r+1}^s,\quad \mu_r^s = \mu_r^{s+1} + q^{v-k-s} \mu_{r+1}^s.$$

Moreover $\lambda_r^0 = \mu_r^0$ and $\mathcal{B}$ is an r-$(v,k,\lambda_r^0;q)$ design for all r with $0 \leq r \leq t$.

Proof. Firstly just as in the proof of Lemma 1.2 we obtain that

$$|\{\ (\delta,B) \in \begin{pmatrix} V \\ t \end{pmatrix}_q \times \mathcal{B} \mid \alpha \subset \delta \subset B\ \}|$$

$$= \lambda_r^0 \cdot \begin{pmatrix} k-r \\ t-r \end{pmatrix}_q = \lambda \cdot \begin{pmatrix} v-r \\ t-r \end{pmatrix}_q.$$

As $\begin{pmatrix} m \\ r \end{pmatrix}_q \begin{pmatrix} n \\ m \end{pmatrix}_q = \begin{pmatrix} n \\ r \end{pmatrix}_q \begin{pmatrix} n-r \\ m-r \end{pmatrix}_q$,

$$\lambda_r^0 = \mu_r^0 = \lambda \cdot \frac{\begin{pmatrix} v-r \\ t-r \end{pmatrix}_q}{\begin{pmatrix} k-r \\ t-r \end{pmatrix}_q} = \lambda \cdot \frac{\begin{pmatrix} v-r \\ k-r \end{pmatrix}_q}{\begin{pmatrix} v-t \\ k-t \end{pmatrix}_q}.$$

Then we have the assertion by a little modification of the proof of

Lemma 2.2.

Proposition 4.1. *Let $\mathcal{B}$ be a t-$(v,k,\lambda;q)$ design.*

(1) $$|\mathcal{B}| = \lambda\cdot\frac{\begin{bmatrix}v\\t\end{bmatrix}_q}{\begin{bmatrix}k\\t\end{bmatrix}_q} \geq \frac{\begin{bmatrix}v\\t\end{bmatrix}_q}{\begin{bmatrix}k\\t\end{bmatrix}_q}.$$

(2) $|\mathcal{B}| = \begin{bmatrix}v\\s\end{bmatrix}_q$, *if* $2s \leq t$ *and* $s + k \leq v$.

Proof. (1) Let $r = s = 0$ in Lemma 4.2. Then we have (1).

(2) It is easy to see that we have the equation

$$N_s(N_s^u)^T = \sum_{i=0}^{u}\begin{bmatrix}s-i\\u-i\end{bmatrix}_q\lambda_{2s-i}^{s-u}W_{ss}^i,$$

where the matrices N_s, N_s^u and W_{ss}^i are those defined on Day 1 just by replacing $\begin{pmatrix}V\\m\end{pmatrix}$ by $\begin{pmatrix}V\\m\end{pmatrix}_q$. So we have the assertion by simply following the proof of Theorem 2.1 given on Day 2.

Remark. Using the matrix equation similar to Lemma 3.1.(5)

$$I = W_{ss} = \sum_{i=0}^{s}(-1)^i q^{-is+\binom{i+1}{2}}W_{is}^0{}^T W_{is},$$

we can show the q-analogue of Corollary 3.1 easily. Note that

$$\sum_{i=0}^{r}(-1)^i q^{-ir+\binom{i+1}{2}}\begin{bmatrix}r\\i\end{bmatrix}_q = \delta_{r,0},$$

$$\begin{bmatrix}i\\j\end{bmatrix}_q = \begin{bmatrix}i-1\\j-1\end{bmatrix}_q + q^j\cdot\begin{bmatrix}i-1\\j\end{bmatrix}_q = \begin{bmatrix}i-1\\j\end{bmatrix}_q + q^{i-j}\cdot\begin{bmatrix}i-1\\j-1\end{bmatrix}_q.$$

Lemma 4.3. *Let $\mathcal{B}$ be a t-$(v,k,\lambda;q)$ design. Then $\mathcal{B}^\perp$ is a t-$(v,v-k,\mu_0^t;q)$ design.*

Proof. Let α be in $\begin{pmatrix}V\\t\end{pmatrix}_q$. Then

$$\lambda(\alpha) = |\{\, B \in \mathcal{B}^\perp \mid \alpha \subset B \,\}|$$
$$= |\{\, B \in \mathcal{B}^\perp \mid \alpha^\perp \supset B^\perp \,\}|$$

$$= |\{ B \in \mathcal{B} \mid B \subset \alpha^{\perp} \}| = \mu_0^t.$$

Lemma 4.4. *If* $0 < t < k \leq v/2$ *and* $2s \leq t$, *then*

$$\frac{\begin{pmatrix} v \\ t \end{pmatrix}_q}{\begin{pmatrix} k \\ t \end{pmatrix}_q} > \begin{pmatrix} v \\ s \end{pmatrix}_q.$$

Proof. We may assume that $s = [t/2]$.

$$\frac{\binom{v}{t}_q}{\binom{k}{t}_q} = \frac{(q^v-1)\cdots(q^{v-t+1}-1)}{(q^k-1)\cdots(q^{k-t+1}-1)}$$

$$= \binom{v}{s}_q \cdot \frac{(q^{v-s}-1)\cdots(q^{v-t+1}-1)(q^s-1)\cdots(q-1)}{(q^k-1)(q^{k-1}-1)\cdots(q^{k-t+1}-1)}$$

$$\geq \binom{v}{s}_q \cdot \frac{(q^{v-s}-1)(q^s-1)(q^{v-s-1}-1)(q^{s-1}-1)\cdots(q^{v-2s+1}-1)(q-1)}{(q^k-1)(q^{k-1}-1)(q^{k-2}-1)(q^{k-3}-1)\cdots(q^{k-2s+2}-1)(q^{k-2s+1}-1)}$$

$$\geq \binom{v}{s}_q \cdot \frac{(q^{2k-s}-1)(q^s-1)}{(q^k-1)(q^{k-1}-1)} \cdot \frac{(q^{2k-s-1}-1)(q^{s-1}-1)}{(q^{k-2}-1)(q^{k-3}-1)} \cdots \frac{(q^{2k-2s+1}-1)(q-1)}{(q^{k-2s+2}-1)(q^{k-2s+1}-1)}$$

as $\dfrac{q^{v-t+1}-1}{q^{k-t+1}-1} \geq 1$.

It is enough to show

$$\frac{(q^{2k-s-i}-1)(q^{s-i}-1)}{(q^{k-2i}-1)(q^{k-2i-1}-1)} > 1, \text{ for all } i \text{ with } 0 \leq i \leq s-1,$$

or

$$q^{2k-2i} - q^{2k-s-i} - q^{s-i} + 1 > q^{2k-4i-1} - q^{k-2i-1} - q^{k-2i} + 1,$$

or

$$(q^{2k-2i-1}-q^{2k-4i-1}) + ((q-1)q^{2k-2i-1}-q^{2k-s-i}) + q^{k-2i-1}+q^{k-2i}-q^{s-i}$$

$$\geq 0 + (q^{2k-2i-1}-q^{2k-s-i}) + (q^{k-2i-1}-q^{s-i}) + q^{k-2i} \geq q^{k-2i} > 0.$$

The last statement is valid as

$2k-2i-1 \geq 2k-i-(s-1)-1 = 2k-i-s$, and

$k-2i-1 \geq 2s-2i-1 \geq (s-i)+s-(s-1)-1 = s-i$.

Theorem 4.1. *There is no t-$(v,k,\lambda;q)$ design which attain the bound in Proposition 4.1.(2) if $2s \le t$ and $s+k \le v$.*

Proof. By Lemma 4.3, we may assume that $k \le v/2$. Then by Lemma 4.4 and Proposition 4.1.(1)

$$|\mathcal{B}| \ge \frac{\begin{bmatrix} v \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q} > \begin{bmatrix} v \\ s \end{bmatrix}_q .$$

Thus for the q-analogue there are no designs corresponding to symmetric designs or tight t-designs. Theorem 4.1 was first proved by L. Chihara by the investigation of the roots of polynomials corresponding to $p_s(x)$ in Corollary 3.2.

We now turn to the attempt to construct t-designs over GF(q). In the history of the construction of classical t-designs, most of the designs were constructed by the following observation.

Let $G \le S^X$, $X = \{1,2,\dots,v\}$. Suppose G is transitive on $\begin{pmatrix} X \\ t \end{pmatrix}$ but not on $\begin{pmatrix} X \\ k \end{pmatrix}$, then the union of orbits of G on $\begin{pmatrix} V \\ k \end{pmatrix}$ becomes a t-design. (See the remark preceeding Example 1.3.)

So it is natural to ask the following question:

Is there a subgroup G of $P\Gamma L(V)$ which acts transitively on $\begin{bmatrix} V \\ t \end{bmatrix}_q$ but not on $\begin{bmatrix} V \\ k \end{bmatrix}_q$, with $1 < t < k$?

The answer is given by the following deep result of W. Kantor.

Result (W. Kantor [9]).

If a subgroup G of $P\Gamma L(V)$ is transitive on $\begin{bmatrix} V \\ r \end{bmatrix}_q$ for some r with $2 \le r \le v-2$, then G is transitive on $\begin{bmatrix} V \\ k \end{bmatrix}_q$ for all k with $1 \le k \le v-1$.

Thus it is impossible to use the observation above, if $t \geq 2$. We note here that there are many examples of 1-design over GF(q), especially a 1-(v,k,1;q) design is called a spread.

Though the direct application of the observation above failed, it may still be a good idea to use a group G in $P\Gamma L(V)$ which has small number of orbits on $\begin{pmatrix} V \\ t \end{pmatrix}_q$.

Example 4.1. Let $v = 2m$, $G = Sp(2m,2)$, and $t = 2$. There are two orbits Δ_2^0 and Δ_2^1 of G on $\begin{pmatrix} V \\ 2 \end{pmatrix}_2$, and $[k/2]+1$ orbits of G on $\begin{pmatrix} V \\ k \end{pmatrix}_2$, where the superfix is given by the Witt index. Then

$$|\Delta_k^u| = \frac{2^{2u(m-k+u)} \prod_{i=0}^{k-u-1} (2^{2m-2i}-1)}{\prod_{i=0}^{u-1} (2^{k-2u-2i}-1) \prod_{j=0}^{k-2u-j} (2^{k-2u-j}-1)}$$

$$B(\Delta_2^0, \Delta_k^u) = \frac{2^{2k-2u-2} + 2^{2k-2} - 2^k - 2^{k-1} + 1}{2^2 - 1}$$

$$B(\Delta_2^1, \Delta_k^u) = \frac{2^{2k-2u-2}(2^{2u}-1)}{2^2 - 1}$$

$$A(\Delta_2^i, \Delta_k^u) = |\Delta_k^u| B(\Delta_2^i, \Delta_k^u) / |\Delta_2^i|.$$

Let $\phi \neq \Delta = \Delta_k^{i_1} \cup \ldots \cup \Delta_k^{i_u} \subset \begin{pmatrix} V \\ k \end{pmatrix}_2$. Suppose Δ is a nontrivial 2-(2m,k,λ;2) design. We may assume that $0 < i_1 < \ldots < i_u$, replacing by the complement if necessary. Then we have

$$\sum_{j=1}^{u} A(\Delta_2^0, \Delta_k^{i_j}) = \sum_{j=1}^{u} A(\Delta_2^1, \Delta_k^{i_j}).$$

So

$$(|\Delta_k^{i_1}|B(\Delta_2^0,\Delta_k^{i_1}) + \ldots + |\Delta_k^{i_u}|B(\Delta_2^0,\Delta_k^{i_u}))|\Delta_2^1|$$

$$= (|\Delta_k^{i_1}|B(\Delta_2^1,\Delta_k^{i_1}) + \ldots + |\Delta_k^{i_u}|B(\Delta_2^1,\Delta_k^{i_u}))|\Delta_2^0|.$$

Since the power of 2 dividing $|\Delta_k^w|B(\Delta_2^0,\Delta_k^w)|\Delta_2^1|$ is $2w(m-k+w)+2m-2$, and the power of 2 dividing $|\Delta_k^w|B(\Delta_2^1,\Delta_k^w)|\Delta_2^0|$ is $2w(m-k+w)+2k-2w-2 = 2(w^2+(m-k-1)+k-1)$. So considering modulo $2^{2w(m-k+u)+2k-2u-1}$ with $w = i_1$, the only nonzero term is $|\Delta_k^{i_1}|B(\Delta_2^1,\Delta_k^{i_1})|\Delta_2^0|$. A contradiction. Hence we conclude that there is no nontrivial t-$(2m,k,\lambda;2)$ design such that $\mathcal{B}^\sigma = \mathcal{B}$ for all σ in $Sp(2m,2)$.

The first nontrivial 2-designs over $GF(q)$ were constructed by S. Thomas for $q = 2$ and extended to all q by E. Schram and the author.

Let $K = GF(q^v)$, $F = GF(q)$ and view K as a v-dimensional vector space over F.

For each U in $\begin{bmatrix} K \\ 2 \end{bmatrix}_q$ and a natural number r, let

$$L_r(U) = \langle a_1 \cdot a_2 \cdots a_r \mid a_i \in U,\ i=1,\ldots,r \rangle,$$

i.e., the subspace of K spanned by the products of r-elements in U. Let

$$\mathcal{B}_r = \{ L_r(U) \mid U \in \begin{bmatrix} K \\ 2 \end{bmatrix}_q \}.$$

Question. Suppose $(v,(2r)!) = 1$. When does $\mathcal{B}_r$ become a 2-$(v,r+1,\begin{bmatrix} r+1 \\ 2 \end{bmatrix}_q;q)$ design ?

We do not have the complete answer. We give a partial answer to it in the following. For the case $q = 1$, see Example 1.4.

Lemma 4.5. *If* $(v, r!) = 1$, *then* $\dim L_r(U) = r+1$.

Proof. Let $U = \langle a,b \rangle$. Then $L_r(U) = \langle a^r, a^{r-1}b, \ldots, b^r \rangle$. Suppose $\{ a^r, a^{r-1}b, \ldots, b^r \}$ is linearly dependent over F. Then a/b is a root of a nonzero polynomial of degree at most r. So $[F(a/b), F] \leq r$. By the assumption we have $F(a/b) = F$ and $Fa = Fb$. A contradiction.

Lemma 4.6. *Suppose* $(v, (2r)!) = 1$. *Let* U *and* W *be in* $\begin{pmatrix} K \\ 2 \end{pmatrix}_q$. *If* $L_r(U) = L_r(W)$, *then* $U = W$.

Proof. We may assume that 1 is in U. Let $U = \langle 1,a \rangle$ and $W = \langle x,y \rangle$. Since $L_r(U) = \langle 1, a, \ldots, a^{r-1}, a^r \rangle$, there are polynomials $f_0, \ldots, f_r$ in $F[t]$ of degree at most r satisfying $f_i(a) = x^{r-i}y^i$. Since $\langle 1, a, \ldots, a^{r-1} \rangle \cap \langle x^r, x^{r-1}y \rangle \neq 0$, we may assume that either $\deg f_0 \leq r-1$ or $\deg f_1 \leq r-1$ by a suitable change of the basis of W. Moreover $f_i(t) \cdot f_{i+2}(t) = f_{i+1}(t)^2$ in $F[t]$, where $i=0,1,\ldots,r-2$. Suppose not. Then $f_i(t)f_{i+2}(t) - f_{i+2}(t)^2$ is a nonzero polynomial of degree at most $2r$ and a is its root. So $[F(a):F] \leq 2r$. A contradiction.

Let $\deg f_i = r_i$. Then $r_i + r_{i+2} = 2r_{i+1}$ or $r_i - r_{i+1} = r_{i+1} - r_{i+2}$. Suppose $r = r_0$. Then

$$r = r_0 > r-1 \geq r_1 > \ldots > r_r.$$

Hence we have $r_i = r-i$. Similarly if $r > r_0$, we have $r_j = j$. So by replacing x and y if necessary, we may assume that

$$x^{r-i}y^i \in \langle 1, a, \ldots, a^i \rangle.$$

In particular x^r is in F. So x is in F by our condition.

Since $x^{r-1}y$ is in $\langle 1,a\rangle$, y belongs to U.

Therefore U = W.

Corollary 4.1. *$|\mathcal{B}_r| = \begin{pmatrix} v \\ 2 \end{pmatrix}_q$ and if $\mathcal{B}_r$ is a 2-design it is a 2-$(v, r+1, \begin{pmatrix} r+1 \\ 2 \end{pmatrix}_q; q)$ design.*

The design is nontrivial if $2 \le r \le r-4$.

Proof. Since the correspondence U to $L_r(U)$ defines a monomorphism by Lemma 4.6, we have the cardinality of $\mathcal{B}_r$. Now the latter half is immediate.

In the following we show that it is a design if r = 2. Let $\mathcal{B} = \mathcal{B}_2$ and $L(U) = L_2(U)$. Let $W \in \begin{pmatrix} V \\ 2 \end{pmatrix}_q$ and

$$\lambda(W) = |\{ U \in \begin{pmatrix} K \\ 2 \end{pmatrix}_q \mid L(U) \supset W \}|.$$

We need to show that $\lambda(W) = \begin{pmatrix} 2+1 \\ 1 \end{pmatrix}_q = q^2+q+1$.

Let $U = \langle x,y\rangle$, $L(U) = \{ sx^2+ty^2+uxy \mid s,t,u \in F \}$ and $f = st-u^2$. Then GL(U) is embedded as a subgroup in $O_f(L(U))$, the orthogonal group defined by f. So we have the following.

$$\begin{pmatrix} L(U) \\ 2 \end{pmatrix}/GL(U) \sim \begin{pmatrix} L(U) \\ 1 \end{pmatrix}/GL(U)$$

$= \{ \langle x^2\rangle, \langle xy\rangle, \langle x^2-\varepsilon y^2\rangle \}$ if q is odd, and

$= \{ \langle x^2\rangle, \langle xy\rangle, \langle x(x+y)\rangle \}$ if q is even.

Hence we have three types.

I. $W = \langle x^2, y^2\rangle = \langle xy\rangle^{\perp}$.

II. $W = \langle x^2, xy\rangle = \langle x^2\rangle^{\perp}$.

III. $W = \langle xy, x^2+\varepsilon y^2\rangle = \langle x^2-\varepsilon y^2\rangle^{\perp}$, with q odd. Here ε is a fixed element in $F - F^2$.

III'. $W = \langle x^2, y(x+y) \rangle = \langle x(x+y) \rangle^{\perp}$, q even.

Let $\lambda[T] = |\{ L(U) \in \mathcal{B} \mid W \subset L(U), W \text{ is of type } T \}|$.

Then it is easy to get the following.

$$\lambda[I] = \begin{cases} q(q+1)/2, & q \text{ odd}, \\ 1, & q \text{ even}. \end{cases}$$

$\lambda[II] = q+1$.

Let $W = \langle xy, x^2+\varepsilon y^2 \rangle$. Then

$$(x^2-\varepsilon y^2)^2 = (x^2+\varepsilon y^2)^2 - 4\varepsilon(xy)^2.$$

So $\lambda[III] = |\{ \langle a^2-\varepsilon b^2 \rangle \mid \langle a,b \rangle = W \}| = q(q-1)/2$.

Suppose $W = \langle x^2, y(x+y) \rangle$ with q even. Then considering the solution of the following equation applying Hilbert's Theorem 90, we have $\lambda[III'] = (q-1)(q+1)$.

$z^2 + z + c = 0$, where $c = ba^{-1}$ or $ba^{-1}+1$.

Taking the sum of three numbers in each case, we have the assertion.

Note for DAY 4.

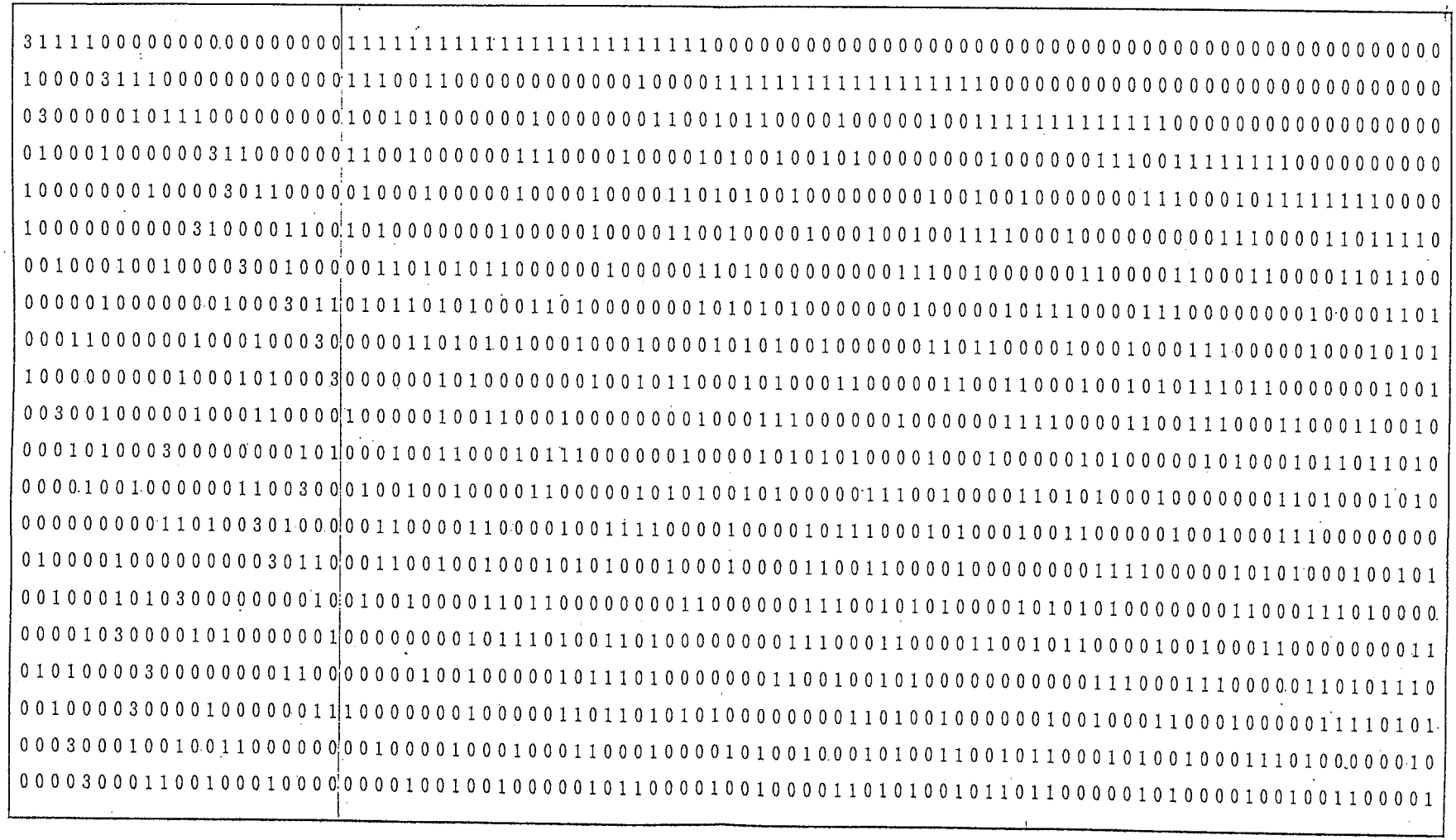
The Ray-Chaudhuri and Wilson type inequality for t-designs over GF(q) is discussed in [8]. See also [13], [32].

Theorem 4.1 is a special case of the results of Chihara in [10]. She showed the nonexistence of tight t-designs for every known Q-polynomial schemes with $q > 1$. Here we followed [32].

The first construction of t-designs over GF(q) is in [35] for $q = 2$, $q = 2^m$ case is in [30] and q odd case is in [31]. E. Schram at the Ohio State University seems to obtain the similar results.

The table following this note is the matrix A_{23} where V is a 7 dimensional vector space over $GF(2)$ and G is the so-called Singer group, a cyclic gorup of order 127. It was computed by Kawamoto and Yoshikura. It is easy to check that there are no 2-(7,3,1;2) designs with G as an automorphism group. See [35]. The first 21 columns corresponds to a 2-(7,3,7;2) design constructed by Thomas [35].

ON 2− (7, 3, 1 ; 2) Design



DAY 5.

The today's goal is to prove the following theorem of L. Teirlinck. It gives a constructive proof of the existence of (classical) nontrivial t-designs for all t. For $t \geq 7$ the only nontrivial t-designs known are those constructed in the theorem below within the author's knowledge.

Theorem 5.1. (L. Teirlinck) *Let v, k be positive integers such that $m = (v-k+1)/(k!)^{2k-1}$ is an integer, and $V = \{1, 2, \ldots, v\}$. Then there exist m disjoint families $\mathcal{F}_1, \ldots, \mathcal{F}_m$ in $\binom{V}{k}$ such that $\binom{V}{k} = \mathcal{F}_1 \cup \ldots \cup \mathcal{F}_m$ and that each $\mathcal{F}_i$ is a $(k-1)$-(v, k, λ) design with $\lambda = (k!)^{2k-1}$.*

Remark 5.1. Since the union of disjoint families of t-designs with same k is a t-design, Theorem 5.1 implies the following:

Suppose $(k!)^{2k-1}$ divides λ and λ divides $v-k+1$. Then there exist $m = (v-k+1)/\lambda$ disjoint families $\mathcal{F}_1, \ldots, \mathcal{F}_m$ in $\binom{V}{k}$ such that $\binom{V}{k} = \mathcal{F}_1 \cup \ldots \cup \mathcal{F}_m$ and that each $\mathcal{F}_i$ is a $(k-1)$-(v,k,λ) design.

Lemma 5.1. *Let $E_s = \{ (e_1, \ldots, e_s) \mid e_i \in \mathbb{N}, e_1 + \ldots + e_s = k \}$. Then $|E_s| = \binom{k-1}{s-1}$.*

Proof. $|E_s|$ is the number of ways of dividing k 1's into s nonempty parts. So $|E_s| = \binom{k-1}{s-1}$.

In the following

$(a,b) = \{ x \in \mathbb{Z} \mid a < x < b \}$,

$[a,b) = \{ x \in \mathbb{Z} \mid a \leq x < b \}$, and

$I(s,p) = \{ (i_1,\ldots,i_s) \mid 0 \leq i_1 < \ldots < i_s < p \} \subset \mathbb{Z}^s$.

For $a \in [0,m)$, $\mathbf{i} \in I(s,(k!)m) = I_s$ and $\mathbf{e} \in E_s$, let

$$B_a(\mathbf{i}) = \{ \mathbf{e} \in E_s \mid \sum_{j=1}^{s} e_j i_j \in [k!a,k!(a+1)) \pmod{k!m} \}.$$

We write $\mathbf{i} = (i_1,\ldots,i_s) < \mathbf{j} = (j_1,\ldots,j_{s+1})$ if $\{i_1,\ldots,i_s\} \subset \{j_1,\ldots,j_{s+1}\}$.

Lemma 5.2. *Let m, k and s be positive integers and a be in $[0,m)$. For each $\mathbf{i} = (i_1,\ldots,i_s)$ in $I(s,k!\cdot m)$,*

$$\sum_{\mathbf{i}<\mathbf{j}} |B_a(\mathbf{j})| + (k-s)|B_a(\mathbf{i})| = \binom{k-1}{s}\cdot k!.$$

Proof. Let $p = k!\cdot m$ and

$$S = \{ (f,x) \mid f \in E_{s+1},\ x \in [0,p),\ \sum_{j=1}^{s} f_j i_j + f_{s+1}x \in [k!\cdot a,k!\cdot(a+1)) \pmod{p} \}.$$

Since f_{s+1} divides $k!$, $f_{s+1}\cdot x+b \in [k!\cdot a,k!\cdot(a+1)) \pmod{p}$ has $k!$ solutions for each a with $b = \sum_{j=1}^{s} f_j\cdot i_j$,

$$|S| = |E_{s+1}|\cdot k! = \binom{k-1}{s}\cdot k!.$$

On the other hand let

$S_0 = \{ (f,x) \in S \mid x \text{ is not in } \{i_1,\ldots,i_s\} \}$, and

$S_r = \{ (f,x) \in S \mid x = i_r \}$.

Then S is a disjoint union of $S_0,S_1,\ldots,S_s$. Moreover

$$|S_0| = \sum_{\mathbf{i}<\mathbf{j}} |B_a(\mathbf{j})|.$$

Let φ be a mapping from $\bigcup_{r=1}^{s} S_r$ to $B_a(\mathbf{i})$ defined as follows.

For each $(f,x) \in S_r$, let

$$\varphi(f,x) = (f_1,\ldots,f_{r-1},f_r+f_{s+1},f_{r+1},\ldots,f_s).$$

Then φ is surjective and for each $e \in B_a(\mathbf{i})$

$$|\varphi^{-1}(e) \cap S_r| = e_r - 1.$$

Hence $|\varphi^{-1}(e)| = \sum_{r=1}^{s} (e_r - 1) = k - s$. Therefore we have the assertion.

Proof of Theorem 5.1.

We proceed by induction on k. If $k = 1$, $m = v$ and we may take $\mathcal{F}_i = \{x_i\}$. Assume $k > 1$ and Theorem 5.1 is valid for all $k' < k$. Let $p = k!\cdot m$ and

$$V = T \cup U_0 \cup \ldots \cup U_{p-1}$$

be a partition of V such that $T = \{1,2,\ldots,k-1\}$ and $|U_r| = (k!)^{2k-2}$, $r = 0,\ldots,p-1$. Note that $v = (k-1) + (k!)^{2k-1}\cdot k!\cdot m$. For each e in E_s let $T_1(e) = (0,e_1)$ and $T_r(e) = (e_1+\ldots+e_{r-1},e_1+\ldots+e_r)$. Then $|T_r(e)| = e_r - 1$, $T_r(e) \subset T$ and $\left|\bigcup_{r=1}^{s} T_r(e)\right| = k - s$. For each e in E_s and $\mathbf{i} = (i_1,\ldots,i_s)$ in $I_s = I(s,p)$, let

$$V_r(e,\mathbf{i}) = U_{i_r} \cup T_r(e), \text{ and}$$

$$R(e,\mathbf{i}) = \prod_{r=1}^{s} \binom{V_r(e,\mathbf{i})}{e_r}$$

$$= \binom{(0,e_1)\cup U_{i_1}}{e_1} \times \binom{(e_1,e_1+e_2)\cup U_{i_2}}{e_2} \times \cdots \times \binom{(e_1+\ldots+e_{s-1},k)\cup U_{i_s}}{e_s}$$

$$= \{ F \in \binom{V}{k} \mid |F \cap V_r(e,\mathbf{i})| = e_r,\ 1 \le r \le s \}$$

Sublemma 1. $\binom{V}{k} = \bigcup_{s=1}^{k} \bigcup_{\mathbf{e}\in E_s} \bigcup_{\mathbf{i}\in I_s} R(\mathbf{e},\mathbf{i})$, *(disjoint)*.

Proof. Since $R(\mathbf{e},\mathbf{i}) \subset \binom{V}{k}$, it suffices to show that each $F \in \binom{V}{k}$ uniquely determines $s \in \{1,\ldots,k\}$, $\mathbf{e}$ in E_s and $\mathbf{i}$ in I_s and that $F \in R(\mathbf{e},\mathbf{i})$. Let

$$\{ i_1,\ldots,i_s \} = \{ j \mid F \cap U_j \neq \phi \}.$$

Claim 1. Let $G \in R(\mathbf{e},\mathbf{i})$ with $\mathbf{i} = (i_1,\ldots,i_s)$, then

$$\{ i_1,\ldots,i_s \} = \{ j \mid G \cap U_j \neq \phi \}.$$

(For) By the definition of $R(\mathbf{e},\mathbf{i})$, it is clear that if $G \cap U_j \neq \phi$, $j \in \{ i_1,\ldots,i_s \}$. On the other hand

$$|G \cap U_{i_r}| = |G \cap V_r(\mathbf{e},\mathbf{i})| - |G \cap T_r(\mathbf{e})|$$

$$\geq e_r - |T_r(\mathbf{e})| = e_r - (e_r - 1) = 1.$$

Hence we have the claim.

So F determines s and $\mathbf{i}$ in I_s uniquely. Note that $|T| = k-1$ implies $s \geq 1$.

Claim 2. Let $G \in R(\mathbf{e},\mathbf{i})$ with $\mathbf{i} = (i_1,\ldots,i_s)$, $\mathbf{e} = (e_1,\ldots,e_s)$ and $|U_{i_1} \cap G| + \ldots + |U_{i_r} \cap G| = g_r$. Then the g_rth member not in G is $e_1+\ldots+e_r$.

(For) Since $|(0,e_1+\ldots+e_r) \cap G| + g_r = e_1+\ldots+e_r$, we have the assertion.

Hence F determines $\mathbf{e}$ uniquely and we have Sublemma 1.

Let $s \geq 2$ and $\mathbf{e} \in E_s$, $\mathbf{i} \in I_s$. Then

$$|V_r(\mathbf{e},\mathbf{i})| = |T_r(\mathbf{e})| + |U_{i_r}| = e_r - 1 + (k!)^{2k-2}, \quad e_r < k.$$

Since $(e_r!)^{2e_r-1}$ divides $\mu = (k!)^{2k-3}$ and μ divides $(e_r - 1 + (k!)^{2k-2}) - e_r + 1$, there exist k! disjoint families $\mathcal{F}_r^{(\alpha)}$

$(0 \le \alpha \le k!)$ of $\binom{V_r(\mathbf{e},\mathbf{i})}{e_r}$ such that

$$\binom{V_r(\mathbf{e},\mathbf{i})}{e_r} = \mathcal{P}_r^{(0)} \cup \ldots \cup \mathcal{P}_r^{(k!-1)}$$

and that each $\mathcal{P}_r^{(\alpha)}$ is a (e_r-1)-$(e_r-1+(k!)^{2k-2}, e_r, \mu)$ design.

Since $B_a(\mathbf{i})$ $(0 \le a < m)$ gives a partition of E_s, there is a partition

$$[0,k!) = B_0 \cup B_1 \cup \ldots \cup B_{m-1}$$

such that $|B_a| = k! \cdot |B_a(\mathbf{i})| / \binom{k-1}{s-1}$, as $|E_s| = \binom{k-1}{s-1}$.

This partition is also possible for $s = 1$ in which case $B_a = \phi$ except one a satisfying $k \cdot i \in [k! \cdot a, k! \cdot (a+1))$ $(\mathrm{mod}\ p)$.

Now let

$$R_a(\mathbf{e},\mathbf{i}) = \bigcup_{\substack{(\alpha_1,\ldots,\alpha_s) \\ \alpha_1+\ldots+\alpha_s \in B_a \ (\mathrm{mod}\ k!)}} \mathcal{P}_1^{(\alpha_1)} \times \ldots \times \mathcal{P}_s^{(\alpha_s)}.$$

For $s = 1$ let

$$R_a((k),(i)) = \binom{T \cup U_i}{k}$$

for a satisfying $k \cdot i \in [k! \cdot a, k! \cdot (a+1))$ and ϕ otherwise.

Sublemma 2. *Let* $R \in \binom{V}{k-1}$ *such that* $R \subset T'$ *for some* $T' \in R(\mathbf{e},\mathbf{i})$. *Then*

$$|\{ S \in R_a(\mathbf{e},\mathbf{i}) \mid R \subset S \}| = \frac{(k!)^{2k-2} |B_a(\mathbf{i})|}{\binom{k-1}{s-1}}.$$

Proof. Suppose $s = 1$. Then

$V_1((k),(i)) = T \cup U_i$, $|U_i| = (k!)^{2k-2}$ and

$$R_a((k),(i)) = \begin{cases} \binom{V_1((k),(i))}{k}, & \text{if } |B_a(\mathbf{i})| = 1, \\ \phi, & \text{otherwise.} \end{cases}$$

So if $|B_a(\mathbf{i})| = 1$, the left hand side is

$$\left(\begin{matrix} (k-1) + (k!)^{2k-2} - (k-1) \\ k - (k-1) \end{matrix} \right) = (k!)^{2k-2}$$

and is equal to the right hand side.

Suppose $s \geq 2$. Then we have $R \neq T$, as otherwise we have $s = 1$. Since $|T' \cap V_r(\mathbf{e},\mathbf{i})| = e_r$ and $k-1 = |R| = |T'| - 1$, there is a unique r such that

$$|R \cap V_r(\mathbf{e},\mathbf{i})| = e_r - 1 < e_r.$$

So $|R \cap V_j(\mathbf{e},\mathbf{i})| = e_j$ if $j \neq r$, and so there is a unique $\alpha_j = \alpha_j(R)$ such that $R \cap V_j \in \mathcal{P}_j^{(\alpha_j)}$. Hence R is contained in $\mu = (k!)^{2k-3}$ members of $\mathcal{P}_1^{(\alpha_1)} \times \ldots \times \mathcal{P}_s^{(\alpha_s)}$, where $\alpha_j = \alpha_j(R)$ if $j \neq r$ and α_r is arbitrary. In order to have that member in $R_a(\mathbf{e},\mathbf{i})$, α_r must satisfy

$$\alpha_r + \Big(\sum_{j \neq r} \alpha_j(R) \Big) \in B_a \pmod{k!}.$$

Hence there are

$$|B_a| = \frac{k! \cdot |B_a(\mathbf{i})|}{\left(\begin{matrix} k-1 \\ s-1 \end{matrix} \right)}$$

α_r among $\{ 0,\ldots,k!-1 \}$ satisfying the condition. Hence R is contained in

$$\mu \cdot |B_a| = \frac{(k!)^{2k-2} \cdot |B_a(\mathbf{i})|}{\left(\begin{matrix} k-1 \\ s-1 \end{matrix} \right)}$$

members of k-subsets in $R_a(\mathbf{e},\mathbf{i})$ as desired.

Let

$$\mathcal{F}_a = \bigcup_{s=1}^{k} \bigcup_{\mathbf{e} \in E_s} \bigcup_{\mathbf{i} \in I_s} R_a(\mathbf{e},\mathbf{i}).$$

By sublemma 1,

$$\binom{V}{k} = \bigcup_{a=0}^{m-1} \mathcal{F}_a \quad \text{(disjoint)}.$$

Hence we need to show that for each a, $\mathcal{F}_a$ is a $(k-1)$-(v,k,λ) design with $\lambda = (k!)^{2k-1}$.

Let $R \in \binom{V}{k-1}$, and $\mathbf{i} = (i_1,\ldots,i_s)$ with

$$I = \{ i_1,\ldots,i_s \} = \{ i \mid R \cap U_i \neq \phi \},\ 0 \leq i_1 < \ldots < i_s < p.$$

Let $r_u = |R \cap U_{i_u}|$. Then $|T - R| = \sum_{u=1}^{s} r_u$. Let

$$T-R = \{ x_1^{(1)},\ldots,x_{r_1}^{(1)},x_1^{(2)},\ldots,x_{r_2}^{(2)},\ldots,x_1^{(s)},\ldots,x_{r_s}^{(s)} \}$$

with $x_1^{(1)} < x_2^{(1)} < \ldots < x_{r_1}^{(1)} < x_1^{(2)} < \ldots < x_{r_s}^{(s)}$.

Claim 3. $|\{ Q \in \mathcal{F}_a \mid R \subset Q,\ Q \cap U_i = \phi \text{ if } i \text{ is not in } I \}|$

$$= \frac{s\cdot(k!)^{2k-2}\cdot|B_a(\mathbf{i})|}{\binom{k-1}{s-1}}.$$

(For) Let $\{x\} = Q - R$. Then either $x \in U_{i_u} - R$ for some u with $1 \leq u \leq s$ or $x = x_j^{(u)}$ for some u with $1 \leq u \leq s$ and $1 \leq j \leq r_u$. Let $e_1 = x_{r_1}^{(1)},\ldots,e_1+e_2+\ldots+e_{u-1} = x_{r_{u-1}}^{(u-1)}$, $e_1+e_2+\ldots+e_u = x_1^{(u+1)},\ldots,e_1+e_2+\ldots+e_{s-1} = x_1^{(s)}$, $e_1+e_2+\ldots+e_s = k$. See Claim 2 in the proof of Sublemma 1. Then $Q \in R(\mathbf{e},\mathbf{i})$ as $\{ i \mid U_i \cap Q \neq \phi \} = I$. Since there are s choices of u, the assertion of Claim 3 follows from Sublemma 2.

Claim 4. For some j not in I, let $\{j_1,\ldots,j_{s+1}\} = I \cup \{j\}$, $\mathbf{j} = (j_1,\ldots,j_{s+1}) \in I_{s+1}$. Then

$$|\{ Q \in \mathcal{F}_a \mid R \subset Q,\ Q \cap U_j \neq \phi \}| = \frac{(k!)^{2k-2}|B_a(\mathbf{j})|}{\binom{k-1}{s}}.$$

(For) For each $x \in U_j$, $R \cup \{x\}$ is in $R(\mathbf{e},\mathbf{i})$ for some $\mathbf{e}$ and $\mathbf{e}$ is determined by j uniquely, i.e., if $i_{u-1} < j < i_u$,

$$e_1 = x_{r_1}^{(1)}, \ldots, \quad e_1+\ldots+e_{u-1} = x_{r_{u-1}}^{(u-1)}, \quad e_1+\ldots+e_u = x_{r_{u-1}}^{(u-1)}+1,$$

$$e_1+\ldots+e_{u+1} = x_{r_u}^{(u)}+1, \ldots, \quad e_1+\ldots+e_{s+1} = k.$$

Hence by Sublemma 2, the left hand side is equal to

$$\frac{(k!)^{2k-2}\cdot|B_a(\mathbf{j})|}{\binom{k-1}{s}}.$$

Therefore

$$|\{ Q \in \mathcal{F}_a \mid R \subset Q \}|$$

$$= \frac{s\cdot(k!)^{2k-2}\cdot|B_a(\mathbf{i})|}{\binom{k-1}{s-1}} + \sum_{\mathbf{j}>\mathbf{i}} \frac{(k!)^{2k-2}\cdot|B_a(\mathbf{j})|}{\binom{k-1}{s}}$$

$$= (k!)^{2k-2}\cdot(k!) = (k!)^{2k-1} = \lambda$$

by Lemma 5.2 as desired.

Note for DAY 5.

The theorem is taken from [33]. In [34], Teirlinck discusses the general construction of t-designs using arrays. The original construction was introduced by T. Ito at a seminar in Tokyo and the proof was written by P. Frankl and others and included in the book [1]. The proof demonstrated here follows [1].

There are a lot of papers dealing with the constructions of t-designs, for example [2], [3], [4], [18], [19] and [36]. [4] gives an infinite series of 3-(v,6,1) designs and [18], [19], [36] also give examples of Steiner systems.

We do not have any nontrivial Steiner systems for $t \geq 6$, nor

infinite series of Steiner systems for $t \geq 4$, within the author's knowledge.

The determination of the existence or nonexistence of Steiner systems for all t seems to be one of the most interesting problems in design theory.

REFERENCES

1. Akiyama, J., P. Frankl : 'Gendai-Kumiawase-Ron', Kyoritsu-Shuppan, 1987, in Japanese.
2. Alltop, W. O. : 5-designs in affine spaces, Pacific J. of Math. 39, 1971, 547-551.
3. Alltop, W. O. : An infinite class of 5-designs, J. Comb. Th. (A) 12, 1972, 390-395.
4. Assmus Jr., E. F., J. D. Key : On an infinite class of Steiner systems with $t = 3$ and $k = 6$, J. Comb. Th. (A) 42, 1986, 55-60.
5. Bannai, E. : On tight designs, Quart. J. Math. (Oxford) 28, 1977, 433-448.
6. Bremner, A. : A diophantine equation arizing from tight 4-designs, Osaka J. Math. 16, 1979, 353-356.
7. Bruck, R. H., H. J. Ryser : The nonexistence of certain projective planes, Canad. J. Math. 1, 1949, 88-93.
8. Cameron, P. J. : Generalisation of Fisher's inequality to fields with more than one element, London Math. Soc. Lecture Note Ser. 13, 1973, 9-13.
9. Cameron, P. J., W. M. Kantor : 2-transitive and antiflag transitive collineation groups of finite projective spaces, J. Alg. 60, 1979, 384-422.
10. Chihara, L. : Applications of the Askey-Wilson polynomials to association schemes, Ph. D. Thesis, Univ. of Minnesota 1985.
11. Chowla, S., H. J. Ryser : Combinatorial problems, Canad. J. Math 2, 1950, 93-99.

12. Delsarte, P. : An algebraic approach to the association schemes of coding theory, Philips Research Reports, supplements 10, 1973.

13. Delsarte, P. : Association schemes and t-designs in regular semilattices, J. Comb. Th. (A) 20, 1976, 240-243.

14. Deza, M., P. Erdos, P. Frankl : Intersection properties of systems of finite sets, Proc. London Math. Soc. (3) 36, 1978, 369-384.

15. Enomoto, H, N. Ito, R. Noda : Tight 4-designs, Osaka J. Math 16, 1979, 39-43.

16. Frankl, P., R. M. Wilson : Intersection theorems with geometric consequences, Combinatorica 1, 1981, 357-368.

17. Hall Jr.,M. : 'Combinatorial Theory', second edition, John Wiley and Sons Inc., 1986.

18. Hanani, H. : The existence and construction of balanced imcomplete block designs, Ann. Math. Stat. 32, 1961, 361-386.

19. Hanani, H. : A class of three designs, J. Comb. Th. (A) 26, 1979, 1-19.

20. Hughes, D. R., F. C. Piper : 'Design Theory', Cambridge U. P. 1985.

21. Ito, N. : On tight 4-designs, Osaka J. Math. 12, 1975, 493-522.

22. Ito, N. : Corrections and supplements to 'On tight 4-designs', Osaka J. Math. 15, 1978, 693-697.

23. Kreher, D. L. : An incidence algebra for t-designs with automorphisms, J. Comb. Th. (A) 42, 1986, 239-251.

24. Kreher, D. L. : A generalization of Connor's inequality to t-designs with automorphisms, J. Comb. Th. (A) 50, 1989, 259-268.

25. Lander, E. S. : 'Symmetric Designs, an algebraic approach',

London Math. Soc. Lecture Note Ser. 74, Cambridge U. P., 1983.

26. Nagao, H. : 'Gun-To-Dezain', Iwanami-Shoten, 1974, in Japanese.

27. Peterson, C. L. : On tight 6-designs, Osaka J. Math. 14, 1977, 417-435.

28. Ray-Chaudhuri, D. K., R. M. Wilson : On t-designs, Osaka J. Math. 12, 1975, 737-744.

29. Suzuki, H. : t-designs in H(d,q), to appear in Hokkaido Math. J.

30. Suzuki, H. : 2-designs over $GF(2^m)$, preprint.

31. Suzuki, H. : 2-designs over GF(q), preprint.

32. Suzuki, H. : On the inequalities of t-designs over a finite field, preprint.

33. Teirlinck, L. : Nontrivial t-designs without repeated blocks exist for all t, Discrete Math. 65, 1987, 301-311.

34. Teirlinck, L. : On the use of regular arrays in the construction of t-designs, London Math. Soc. Lecture Note Ser. , 1989.

35. Thomas, S. : Designs over finite fields, Geometricae Dedicata 24, 1987, 237-242.

36. Wilson, R. M. : An existence theory for pairwise balanced designs I, II, J. Comb. Th. (A) 13, 1972, 220-273.

37. Wilson, R. M. : Incidence matrices of t-designs, Linear Alg. and its applications 46, 1982, 73-82.