”Gauss sums and Legendre polynomials” in algebraic combinatorics

Eiichi Bannai

Shanghai Jiao Tong University

Talk at “Modular functions and Quadratic forms
—— Number theoretic delights”

Osaka Japan, Dec 23, 2013

§1. Introduction

Takashi Ono: Gauss sums and Legendre polynomials, Sugaku Seminar, Nov. 1986— April 1987 (in Japanese)

小野孝、ガウスの和とルジャドル多項式、
数学セミナー、1986 年 11 月号ーー1987 年 4 月号

This became the Part I of the book: Gauss sums and Poicaré sums (in Japanese) Nihon Hyoronsha (2009) by Takashi Ono,
小野孝：ガウスの和とポアンカレ級数、日本評論社 (2009) (第 1 部)

In the Preface of the book, Professor Takashi Ono kindly mentioned our book: "Algebraic Combinatorics on Spheres" (球面上の代数的組合せ論), Springer-Tokyo (1999), by Eiichi Bannai and Etsuko Bannai, quoting a part of Introduction of our book.

「この本の最初の３つの章で書いたことは、小野 [356] の雑誌数学セミナー (1986 年 11 月号から 1987 年 4 月号まで）での主題の取り扱いと非常に近いものがある。事実我々がこの連載記事を知ったとき（1988年頃)、これらの主題に関して書きためてあった我々の原稿との数学的類似に驚いたことを覚えている。しかしこれは偶然ではないのである。小野 [356] の記事においては、球面上の調和解析と、有限体上の調和解析ともいえるガウス和などとの関連性が主題であった。この有限体上の調和解析は、アソシエーションスキームの上の表現論（調和解析）の特別な一例であるからである。.........」

「The contents in the first three chapters of our book are very closely related to the contents of the series of articles by Ono [356] in Sugaku Seminar (1986.11 to 1987.4). When we knew this series of articles (around 1988), we were very surprised with the similarities with our manuscripts. But this is not an accident. One of the main topics of the articles of Ono [356] was the relations between the harmonic analysis on the spheres and the harmonic analysis on the finite fields including Gauss sums. In fact, the harmonic analysis on finite fields can be regarded as a special case of the representation theory (harmonic analysis) on the association schemes...... 」

Anyway, we were very much encouraged by the articles of Ono, to learn that there are some people who are thinking similar things. (Of course this viewpoint itself is far older, and perhaps many people may now think that this is rather obvious. But I was very glad that the philosophy was clearly manifested in the articles of Ono at that time.)

§2. Association schemes

Definition (Association Scheme) $\mathfrak{X} = (X, \{R\}_{0\leq i\leq d})$**, where** X **is a finite set and** $R_i \subset X \times X$ $(i = 0, 1, 2, \ldots, d)$**, is called an association scheme, if the following conditions are satisfied.**

(i) $R_0 = \{(x, x) \mid x \in X\}$**,**
(ii) $R_0 \cup R_1 \cup \cdots \cup R_d = X \times X$ **(disjoint),**
(iii) For each $i \in \{0, 1, \ldots, d\}$,
$^tR_i = \{(y, x) \mid (x, y) \in R_i\} = R_j$**, for some** $j \in \{0, 1, \ldots, d\}$
(iv) For each $i, j, h \in \{0, 1, \ldots, d\}$**,**

$$|\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}| = p^h_{i,j} \quad \textbf{(constant)},$$

whenever $(x, y) \in R_h$.

Let A_i **be the adjacency matrix with respect to** R_i $(i = 0, 1, \ldots, d)$, **namely**

$$A_i = (A_i)_{x \in X, y \in X} = \begin{cases} 1 & \textbf{if } (x, y) \in R_i \\ 0 & \textbf{if } (x, y) \notin R_i \end{cases}$$

We say the assoc. schemes $\mathfrak{X} = (X, \{R\}_{0 \le i \le d})$ **is commutative, if and only if** $A_i A_j = A_j A_i$ **for all** $i, j \in \{0, 1, \ldots, d\}$.

Let $\mathfrak{X} = (X, \{R_i\}_{0 \le i \le d})$ **be a commutative assoc. scheme.**
Then $A_0, A_1, \ldots A_d$ **act on** $V = \mathbb{R}^X$ **(So, dim** $V = |X|$**).**
Let $V_0, V_1, \ldots, V_d$ **be the maximal common eigensubspaces of** V**.**
(Here we can take $V_0 = \langle {}^t(1, 1, \ldots, 1) \rangle$**)**
Let E_i **be the projection map** $V \to V_i$.
So, the Bose-Mesner algebra $\mathfrak{A} = \langle A_0, A_1, \ldots, A_d \rangle$ **has another basis (of primitive idempotents)** $E_0, E_1, \ldots, E_d$.

Then there exist $(d+1) \times (d+1)$ **matrice** P **and** Q **such that**

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d) P,$$

$$(E_0, E_1, \ldots, E_d) = \frac{1}{|X|} (A_0, A_1, \ldots, A_d) Q.$$

These two matrices

$$P = (P_j(i))_{0 \le i \le d,\ 0 \le j \le d} \quad \text{and} \quad Q = (Q_j(i))_{0 \le i \le d,\ 0 \le j \le d}$$

(called the character tables of assoc. scheme $\mathfrak{X}$) play very important roles.

Note that

$$P = \begin{bmatrix} 1 & k_1 & k_2 & \cdots & k_d \\ 1 & P_1(1) & P_2(1) & \cdots & P_d(1) \\ 1 & P_1(2) & P_2(2) & \cdots & P_d(2) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & P_1(d) & P_2(d) & \cdots & P_d(d) \end{bmatrix}, \quad Q = \begin{bmatrix} 1 & m_1 & m_2 & \cdots & m_d \\ 1 & Q_1(1) & Q_2(1) & \cdots & Q_d(1) \\ 1 & Q_1(2) & Q_2(2) & \cdots & Q_d(2) \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & Q_1(d) & Q_2(d) & \cdots & Q_d(d) \end{bmatrix}$$

$(k_i = P_i(0) = \text{column sum of } A_i)$ $\qquad$ $(m_i = Q_i(0) = \text{rank}(E_i) = \dim(V_i))$

$$PQ = |X| I$$

Example 0. (Transitive permutation group)
Let G be a transitive permutation group on X, and let

$$R_0 = \{(x, x) \mid x \in X\}, R_1, R_2, \ldots, R_d$$

be all the orbits of G on $X \times X$. Then $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is an association scheme.

Remark. $\mathfrak{X}$ is commutative, if and only if the permutation character π of G on X is multiplicity-free.

Example 1. (Johnson assoc. scheme $J(v, d)$)
Let V be a set with $|V| = v$, and let $X = \binom{V}{d}$ be the set of all the d-element subset of V. For $x, y \in X$, let

$$(x, y) \in R_i \Leftrightarrow |x \cap y| = d - i \quad (i = 0, 1., \ldots, d).$$

Then $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is a commutative assoc. scheme.

Remark. This assoc. scheme $\mathfrak{X} = J(v,d)$ is the assoc. scheme of permutation group $G = S_v$ acting on the set $X = S_v/(S_d \times S_{v-d})$. For $J(v,d)$ **we have**

$$P_j(i) = \sum_{\nu=0}^{j} (-1)^{j-\nu} \binom{d-\nu}{d-j} \binom{d-i}{\nu} \binom{v-d+\nu-i}{\nu}. \quad \textbf{(Hahn polynomial)}$$

$$Q_j(i) = m_j k_i^{-1} P_i(j). \qquad \textbf{(dual Hahn polynomial)}$$

with $$m_j = \binom{v}{j} - \binom{v}{j-1}, \quad k_i = \binom{d}{i}\binom{v-d}{i}$$

Example 2. (Hamming assoc. scheme $H(d,q)$)
Let $X = \mathbb{F}_q^d$, or we take any finite set of size q instead of $\mathbb{F}_q$.
For $x = (x_1, x_2, \ldots, x_d), y = (y_1, y_2, \ldots, y_d) \in X$, let

$$(x, y) \in R_i \Leftrightarrow |\{j \mid x_j \neq y_j\}| = i \quad (i = 0, 1., \ldots, d).$$

Then $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is a commutative assoc. scheme.

Remark. This assoc. scheme $\mathfrak{X}$ is the assoc. scheme of permutation group $\boldsymbol{G} = \boldsymbol{S_q}\mathrm{wr}\boldsymbol{S_d}$ acting on the set $X = (S_q\mathbf{wr}S_d)/(S_{q-1}\mathbf{wr}S_d)$.

Note that

$$P_k(i) = Q_k(i) = K_k(i).$$

$$K_k(u) = \sum_{i=0}^{k} (-q)^i (q-1)^{k-i} \binom{d-i}{k-i} \binom{u}{i} \quad \textbf{(Krawtchouk polynomial)}$$

§3. Cyclotomic assoc. schemes and Gauss periods

Let $\mathbb{F}_q$ be a finite field with $q = p^r$ elements. Let G be the multiplicative group of $\mathbb{F}_q^*$, and let H be the subgroup of G with $|G : H| = e$ (let $q-1 = ef$).
Let $C_1 (= H), C_2, \ldots, C_d$ be the cosets of G by H. Let $C_0 = \{0\}$. Let $X = \mathbb{F}_q$, and for $x, y \in X$, define

$$(x, y) \in R_i \Leftrightarrow x - y \in C_i \quad (i = 0, 1, \ldots, e).$$

Then $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq e})$ is a commutative assoc. scheme.

What are the character tables P and Q of this assoc. scheme?

They are described using Gauss periods!
(Cf. 数理解析研究所講究録 Vol 1564 (2007), 172-183, Some remarks on pseudo-cyclic association schemes)

(Moreover, the parameters $p_{i,j}^h$ of this cyclotomic assoc. scheme are so called cyclotomic numbers in the "theory of cyclotomy" in number theory (L.E. Dickson, M. Hall, Jr, T. Storer, K. Yamamoto, etc.)

Let $\xi_p = e^{\frac{2\pi\sqrt{-1}}{p}}$. **and** $\psi : \mathbb{F}_q \longrightarrow \mathbb{C}^*$ **be defined by** $\psi(x) = \xi_p^{Tr_{q/p}(x)}$**. While let** χ **be an (irreducible) character of** $\mathbb{F}_q^*$**. Then, Gauss sum** $G(\chi)$ **is defined by**

$$g(\chi) = \sum_{a \in \mathbb{F}_q^*} \chi(a)\psi(a).$$

Moreover, if χ **is a character of** G/H**, then**

$$g(\chi) = \sum_{i=1}^{e} \chi(c_i)\eta_i$$

where $c_i \in C_i$ **and**

$$\eta_i = \sum_{a \in C_i} \psi(a).$$

The numbers $\eta_1, \eta_2, \ldots, \eta_e$ **are called Gauss periods.**

Moreover, we have

$$\boldsymbol{P}=\begin{bmatrix} 1 & f & f & \cdots & \cdots & f \\ 1 & \eta_1 & \eta_2 & \cdots & \cdots & \eta_e \\ 1 & \eta_e & \eta_1 & \eta_2 & \cdots & \eta_{e-1} \\ \vdots & \vdots & \eta_e & \ddots & \ddots & \vdots \\ \vdots & \eta_3 & & \ddots & \ddots & \eta_2 \\ 1 & \eta_2 & \eta_3 & \cdots & \eta_e & \eta_1 \end{bmatrix}$$

If we write

$$\boldsymbol{P}=\begin{bmatrix} 1 & f\cdots \\ \vdots & P_0 \end{bmatrix}$$

with essential part

$$\boldsymbol{P}_0=\begin{bmatrix} \eta_1 & \eta_2 & \cdots & \cdots & \eta_e \\ \eta_e & \eta_1 & \eta_2 & \cdots & \eta_{e-1} \\ \vdots & \eta_e & \ddots & \ddots & \vdots \\ \eta_3 & & \ddots & \ddots & \eta_2 \\ \eta_2 & \eta_3 & \cdots & \eta_e & \eta_1 \end{bmatrix}$$

then e eigenvalus of P_0 are Gauss sums $g(\chi)$ corresponding to e characters of G/H.

§4. Spherical harmonics and Gegenbauer polynomials

$S^{n-1} = \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^n \mid x_1^2 + x_2^2 + \cdots + x_n^2 = 1\}$ $(\subset \mathbb{R}^n)$
$Harm_i(\mathbb{R}^n) =$ **the space of homogeneous harmonic polynomials of degree** i**.**
(Then dim$(Harm_i(\mathbb{R}^n)) = N_i = \binom{n-1+i}{i} - \binom{n-1+i-2}{i-2}$**.)**

Let $\phi_1, \phi_2, \dots, \phi_{N_i}$ **be an orthonormal basis of** $Harm_i(S^{n-1})(= Harm_i(\mathbb{R}^n))$, **with respect to the inner product:**

$$< f, g >= \frac{1}{|S^{n-1}|} \int_{S^{n-1}} f(x)g(x)d\sigma(x).$$

Then, for $x, y \in S^{n-1}$**, we have (Addition theorem):**

$$\sum_{j=1}^{N_i} \phi_j(x)\phi_j(y) = G_i(x \cdot y),$$

where $G_i(x)$ **is the Gegenbauer (Legendre) polynomials defined by**

$$\int_{-1}^{1} G_i(x)G_j(x)(1 - x^2)^{\frac{n-3}{2}} dx = \alpha_i \delta_{ij}$$

and $G_i(1) = N_i \quad (i = 0, 1, \dots)$.

§§ Similarity with association scheme situation.

Let $\mathfrak{X} = (X, \{R_i\}_{0\le i\le d})$ **be a commutative association scheme.**

Let $L_i(X)$ **be the space spanned by the column vectors of** E_i.
($\longleftrightarrow Harm_i(S^{n-1})$.**) (also note that dim** $L_i =$ **rank** $E_i = m_i$.

Let $\phi_1, \phi_2, \ldots, \phi_{m_I}$ **be an orthonormal basis of** $L_i(X)$ **with respect to the inner product:**

$$< f, g >= \frac{1}{|X|}\sum_{x\in X} f(x)g(x).$$

Then for $x, y \in X$, **we have**

$$\sum_{j=1}^{m_i} \phi_j(x)\phi_j(y) = Q_i(u)$$

where $(x, y) \in R_u$, **and** Q **is the character table of the assoc. scheme** $\mathfrak{X}$.
(In the case of cyclotomic association schemes, $Q_i(u)$ **are Gauss periods!**
Moreover, $Q_i(x)$ **are good orthogonal polynomials for good assoc. schemes** $\mathfrak{X}$.

§5. Spherical designs and combinatorial designs

Definition (Spherical designs).
A finite subset $Y \subset S^{n-1}$ is called a spherical t-design, if and only if

$$\frac{1}{|S^{n-1}|}\int_{S^{n-1}} f(x)d\sigma(x) = \frac{1}{|X|}\sum f(x)$$

for any polynomials $f(x) = f(x_1, x_2, \ldots, x_n)$ of degree $\leq t$.

Examples.

- 12 **vertices of a regular icosahedron make a** 5**-design in** $S^2(\subset \mathbb{R}^3)$.
- 240 **roots of type** E_8 **make a** 7**-design in** $S^7(\subset \mathbb{R}^8)$.
- 196560 **min. vectors of Leech lattice make an** 11**-design in** $S^{23}(\subset \mathbb{R}^{24})$.

We are interested in t-designs Y on S^{n-1} with Y smaller as possible.

(Fisher type inequality)

- Y **is a** $2e$**-design on** S^{n-1}**, then**

$$|Y| \geq \binom{n-1+e}{e} + \binom{n-1+e-1}{e-1}$$

$= m_e + m_{e-1} + \cdots + m_1 + m_0,$

where $m_i = \mathbf{dim} Harm_i(\mathbb{R}^n) = N_i = \binom{n-1+i}{i} - \binom{n-1+i-2}{i-2}$.

(If Y **is a** $(2e+1)$**-design, then** $|Y| \geq 2\binom{n-1+e}{e}$.**)**

Y **is called a tight spherical** t**-design, if the above possible smallest value for** $|Y|$ **is attend. Some examples do exist, but not many examples. We are interested in the classification problem of tight spherical** t**-designs.**

Definition (Combinatorial t-designs, i.e. t-(v,k,λ) designs)

Let $X = \binom{V}{k}$ be the point set of all k-element subsets of V, i.e. the set X of Johnson assoc. scheme $J(v,k)$.
A subset Y of X is called a t-(v,k,λ) design, if and only if

$$|\{y \in Y \mid T \subset y\}| = \lambda \quad \textbf{(constant), for any } T \in \binom{V}{t}.$$

Again, we are interested in t-(v,k,λ) designs with $|Y|$ as smaller as possible.

(Fisher type lower bound)
If Y is a $2e$-(v,k,λ) design, then

$$|Y| \geq \binom{v}{e} = m_e + m_{e-1} + \cdots + m_1 + m_0$$

where $m_i =$ ‘rank$(E_i) = Q_i(0) = \binom{v}{i} - \binom{v}{i-1}$.

Those Y which attain the above lower bound is called tight t-designs.
Again, we are interested in the classification problem of tight t-designs.

§6. Further generalizations of designs

(i) For different spaces.

For other compact symmetric spaces of rank 1. For other association schemes, in particular for those called Q-polynomial association schemes, i.e. $Q_i(u)$ is a polynomial of degree i in (namely $|X|E_i = Q_i(|X|E_1)$, where multiplication is an entry wise product of matrices).

(There are many good families of such association schemes. The most interesting class of such association schemes is called P-and Q-polynomial association schemes, where both $P_i(x)$ and $Q_i(x)$ are polynomials of degree exactly i. These polynomials are described by Askey-Wilson polynomials or their special cases or their limiting cases. (The classification of such association schemes is one of the most important problems in algebraic combinatorics.)

(ii) Designs which allow weight functions. $Y \subset S^{n-1}$ **or** $Y \subset \binom{V}{k}$ **and**

$$w : Y \longrightarrow \mathbb{R}_{>0}$$

Consider a pair (Y, w)**.**
(This is equivalent to consider cubature formulas in numerical analysis.)

(iii) Designs which allow several spheres (Euclidean designs), and combinatorial designs which allow several block sizes (regular t**-wise designs and equivalent to the concept of relative** t**-designs in** $H(v, 2)$**).**

I will not discuss further details, but there are close similarities (and some differences) between the theory of Euclidean t**-designs and the theory of relative** t**-designs on** $H(v, 2)$**, say. (This is our current research topic, and see [1] and [2] for more details.**

[1] Eiichi Bannai, Etsuko Bannai, Hideo Bannai, On the existence of tight relative 2-designs on binary Hamming association schemes, Discrete Mathematics. 314 (2014), 17–37.

[2] Eiichi Bannai, Etsuko Bannai, Sho Suda, Hajime Tanaka, On relative t-designs in polynomial association schemes, (arXiv:1303.7163)

(iv) One extreme of association schemes are the cases where $P_i(x)$ and/or $Q_i(x)$ are polynomials.

Another extreme is just the opposite case where all the relations are similar, i.e. the most extremal case is cyclotomic assoc. schemes, or pseudo-cyclic assoc. schemes.

So, the Gauss periods or their generalization would be interesting from the view point of association schemes and algebraic combinatorics.

Moreover, finite groups, in particular finite simple groups, should be looked at from the viewpoint of algebraic combinatorics. This is far more difficult, but we hope we can study them from this viewpoint.

§§ Let me finish my talk by quoting a paragraph from the article of T. Ono (in Sugaku seminar, April 1987).

「この反省によってルジャンドル多項式とガウスの和がある意味で同じ仕掛けで定義されていることがわかりました。もちろん K や S や Φ のとり方はいろいろありますから、それらに応じて P を拾集すれば面白い変種も見つかるでしょう。こうなると別々に整数論とか解析とか幾何とかいっていられません。$K = \mathbb{F}_q$ (や p-進体) にとれば整数論でしょうし、$K = \mathbb{R}$ (や $\mathbb{C}$) にとれば解析でしょうし、図形 S をいろいろと考えれば幾何が入ってまいります。また、ガウスの和やルジャンドル多項式が、より内容のある相互律やラプラス方程式に使用される道具であったように、いろいろの K, S, Φ から得られる変り種の P が役に立つような (相互律やラプラス方程式に類する) 面白い応用はないでしょうか？それとも、いくらガンバッても、ガウスの和やルジャンドル多項式を本質的に凌ぐものはないのでしょうか？」

「From this reflection it can be seen that the definitions of both Legendre polynomials and Gauss sums are, in a sense, coming from the same technique. Of course, we can take K and S and Φ to be many different objects, so accordingly we can surely find intriguing variations of P as well. This then means we can no longer be bothered by our usual distinctions such as "number theory", "analysis", or "geometry"! After all, if we take $K = \mathbb{F}_q$ (or p-adic field) then it may be number theory, and if we take $K = \mathbb{R}$ or $\mathbb{C}$ then this may be analysis, and if we take different configurations S, then geometry also comes in to play. Moreover, just as both Gauss sums and Legendre polynomials were tools used in the study of the reciprocity law and Laplace equation, we can wonder whether the variants on P obtained from different choices of K, S, and Φ have other interesting applications. Or, perhaps there is no single object that can substantially enhance or replace the richness of that of Gauss sums and Legendre polynomials? 」

(translated by Megumi Harada)