数理解析研究所講究録
第 285 巻 1976 年 49-60

Nonexistence theorems of perfect codes and tight designs in distance transitive graphs

東大 理　坂内英一

§1. Perfect code problem in graphs

Γ を（方向を持たず loop や multiple edge を持たない）graph とする。$V(\Gamma)$ で Γ の頂点の集合をあらわす。2頂点 $x, y \in V(\Gamma)$ に対してその距離 $d(x, y)$ が i であるとは、x, y が i 個の edges からなる path で結べ、$i-1$ 個以下の edges からなる path では結べないことと定義する。頂点 x に対して、その i-近傍を $\Sigma_i(x) = \{y \in V(\Gamma) \mid d(x, y) \leq i\}$ で定義する。自然数 e に対して、$V(\Gamma)$ の部分集合 C が perfect e-code であるとは、c が C を動く時 $\Sigma_e(c)$ が $V(\Gamma)$ の partition を与えることと定義する。

graph Γ を与えた時、perfect e-code が存在するか否かを決める問題を perfect code problem と呼ぶことにする。この perfect code problem は graph Γ が arbitrary であればあまり興味はないかもしれない（実際不自然な graph を考えれば

perfect codes はいくらでも作れるであろう。) 問題は、Γ が regularity にみちている程興味があると考えてよいであろう。この種の問題の設定は N. Biggs [5] および P. Delsarte [6] の基本的な論文に負っている。N. Biggs [5] は perfect code problem を考えるべき graphs のクラスとして <u>distance transitive graphs</u> のクラスを提唱し、P. Delsarte [6] ではそれを含むもっと一般的なクラス(グラフだけでなく association schemes に対しても)を考えている。実際の所、distance transitive graphs のクラスは(特に組合せ論の立場からは)制限が強すぎると言えないこともないが、重要と思われる graphs の例は全て distance transitive であること、またいずれにせよこの場合が一番本質的であることから、ここでは一応 distance transitive graphs について考えることにする。なお、graph Γ が distance transitive であるとは、$d(x,y)=d(w,z)$ をみたす任意の $x,y,z,w \in V(\Gamma)$ に対して $\exists g \in \mathrm{Aut}(\Gamma)$ (= グラフ Γ の自己同型群) such that $x^g=z,\ y^g=w$ と定義する。

次の3つは重要な distance transitive graphs の例である。(他にも色々と重要な例があるがここでは略す)。

1. <u>Lattice graphs $\Gamma(n,q)$</u>

$Q = q$ 個の元からなる任意の集合. $(q \geq 2)$.

$V(\Gamma(n,q)) = \underbrace{Q \times \cdots \times Q}_{n}$ とおく $(n \geq 1)$.

2頂点 $\vec{x}=(x_1,\cdots,x_n)$, $\vec{y}=(y_1,\cdots,y_n)\in V(\Gamma(n,q))$ に対して

$d(\vec{x},\vec{y}) = \#$ of i such that $x_i \neq y_i$ と定義する。

この時 $\Gamma(n,q)$ が diameter $n+1$ の distance transitive graph であることは直ちに check される.

2. <u>Triangular graphs $J(v,k)$</u>

S = v 個の元からなる任意の集合.

$V(J(v,k))$ = k-element subsets of S とおく. $(k < \frac{v}{2})$

$\left(従って\ |V(J(v,k))| = \binom{v}{k}. \right)$

2頂点 $x, y \in V(J(v,k))$ に対して.

$d(x,y) = k - |x \cap y|$ とおく ($x \cap y$ は S の subset.)

この時 $J(v,k)$ が diameter $k+1$ の distance transitive graph であることは直ちに check される.

3. <u>Odd graphs O_k</u>

S = $2k$[redacted]1 個の元からなる任意の集合.

$V(O_k)$ = (k-1)element subsets of S とおく.

2頂点. $x, y \in V(O_k)$ に対して. x, y が edge である $(x \neq y)$ (i.e., $d(x,y)=1$) であるとは $x \cap y = \phi$ であることと定義する. この時 O_k が diameter k[redacted] の distance transitive graph となることは直ちに check される.

§2. Nonexistence theorem of perfect codes in the lattice graphs

先ず lattice graph $\Gamma(n,q)$ における perfect code problem を考えよう。この問題は coding theory における通常の perfect code problem として有名なものである。この方面では、次の Tietäväinen の結果が重要かつ有名である。

定理 (Tietäväinen, 部分的には Van Lint etc.) $e \geqslant 2$ かつ q が素数巾の時、lattice graph $\Gamma(n,q)$ における perfect e-code は次のいずれかに限る。(i.e. $\mathrm{Aut}(\Gamma)$ で次のいずれかにうつる。)

(i) $e \geqslant n$, $|C|=1$ (trivial perfect codes)

(ii) $e=$ arbitrary $q=2$, $n=2e+1$ (almost trivial perfect codes)

(iii) $e=3$, $q=2$, $n=23$, the binary Golay code (M_{23} と関連)

(iv) $e=2$, $q=3$, $n=11$, the ternary Golay code (M_{11} と関連)

上の定理は重要であり、その証明は巧妙であるが、それを拡張して、q が素数巾でない場合を取り扱うことは難かしいと考えられていた。何故なら、Tietäväinen–Van Lint の証明法では次の2つの必要条件を同時に用い、その際 sphere packing condition を用いる際に $q=$ 素数巾であることを本質的に用いなければならないからである。

(I) Sphere packing condition: $|\Sigma_e(c)| \mid |V(\Gamma(n,q))|$.
(i.e. $1+n(q-1)+\cdots+\binom{n}{k}(q-1)^k \mid q^n$).

(II) Lloyd Theorem: 次のe次の多項式(Lloyd polynomial と呼ばれる) $\Psi_e(X)$ の零点は全て相異なり、かつ整数でなければならない。

$$\Psi_e(X)=\sum_{i=0}^{e}(-1)^i\binom{n-X}{e-i}\binom{X-1}{i}(q-1)^{e-i}$$

さて、ここでは q が(必ずしも素数巾でない)一般の場合を考えよう。次の結果が基本的である。

定理1([1]) 各 $e\geq 3$ に対して、lattice graphs $\Gamma(n,q)$ (n, q は任意)における nontrivial (i.e., $n>e$) perfect e-codes は高々有限個である。

Remark e が小さい時(但、$e\geq 3$)、e を決めれば、全ての perfect e-codes を決めることは容易である($e=3, 4, 5$ etc.) 実際、この定理1の方向を発展させて、perfect e-codes ($e\geq 3$) が完全に決定出来るかもしれないと思うが、まだ出来ていない。

定理1の証明の概略は次の通りである。まず、今までの常識に反して、sphere packing condition は一切用いず、Lloyd Theorem のみを用いることにする。根本方針は、Lloyd 多項式 $\Psi_e(X)$ の零点の値を(正確な値を求めることは不可能だが)近似的に求め、その情報からある零点が整数でないことを導き、Lloyd Theorem に矛盾することを言う。この近似

値をもとめる際に、$\Psi_e(x)$ を Hermite 多項式を使って近似する idea が新らしくかつ一番重要であり、Hermite 多項式の理論が重要な役を演ずる。次にこれらのことをもう少し詳しく言うと、

(1) $q>2$ の時のみ考える。($q=2$ の時は既に分類済 Tietäväinen 他)

(2) $\beta = \frac{\sqrt{(n-e)(q-1)}}{q}$ という値を考え、β が bounded されている時、perfect e-codes が高々有限個しか存在しないことをいうのはさほど難かしくない。(ここでは Lloyd 多項式を monic にした時の係数が整数という条件を用いる。)

(3) $\beta \longrightarrow +\infty$ という条件のもとで、$\Psi_e(x)$ の零点の分布を調べる。(この step が一番やっかいで、$\Psi_e(x)$ の generating function を考え、その formal な微分を考えたりして、$\Psi_e(x)$ を Hermite poly. を用いて近似したりする必要がある。) さて、

$$x_{-[\frac{e}{2}]} < x_{-[\frac{e}{2}]+1} < \cdots < x_{-1} < (x_0) < x_1 < \cdots < x_{[\frac{e}{2}]}$$

を大きさの順にならべた $\Psi_e(x)$ の零点とする。(但 x_0 は $e=\mathrm{odd}$ の時のみ存在する。) この時、$\beta \longrightarrow +\infty$ の時、

$$x_i \longrightarrow \alpha + \beta \xi_i + \lambda_i \qquad \left(i = -[\tfrac{e}{2}], \cdots, -1, (0), 1, \cdots, [\tfrac{e}{2}]\right)$$

但、$\alpha = \frac{(n-e)(q-1)}{q} + \frac{e+1}{2}$ (e 個の零点の算術平均)

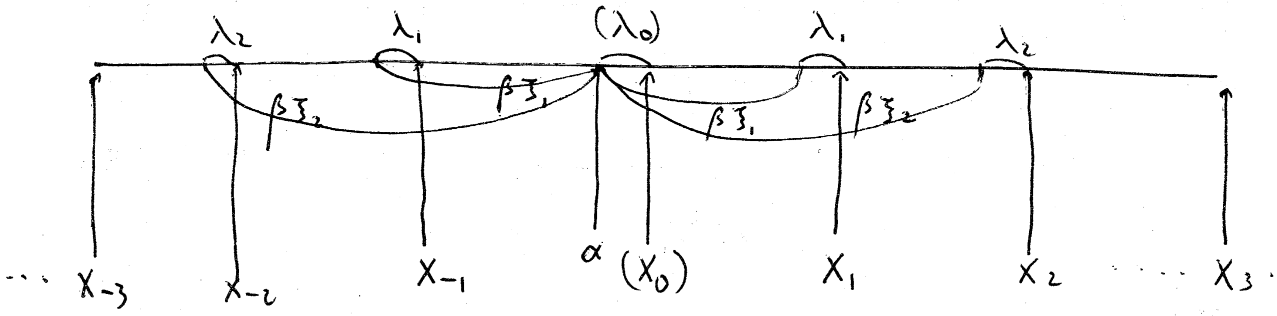
ξ_i $\left(i = -[\frac{e}{2}], \cdots, -1, (0), 1, \cdots, [\frac{e}{2}]\right)$ は Hermite 多項式

$$He(x) = \sum_{r=0}^{[\frac{e}{2}]} (-1)^r \, 1\cdot 3\cdot 5 \cdots (2r-1) \binom{e}{2r} x^{e-2r}$$

の零点。

$$\lambda_i = \frac{q-2}{q}\left(\frac{e-1}{6} - \frac{\xi_i^2}{6}\right).$$

なお、Hermite多項式の零点は原点を中心に対称なことに注意。
従って、$\lambda_i = \lambda_{-i}$、$-\xi_i = \xi_{-i}$。従って、$\Psi_e(x)$の零点は（$\beta \to +\infty$の時）次のようになる。



(4) 上のことから $X_1 + X_{-1} - X_2 - X_{-2} \longrightarrow \frac{q-2}{q}\cdot\frac{2}{6}(\xi_2^2 - \xi_1^2)$ が言え、この右辺は e が大きい時 strictly に 0と1の間にあることが（Hermite多項式の根の近似的評価が得られていることから）言え、Lloyd Theorem に矛盾することがわかる。e が小さい時は少し別に考察を加えなければならないが、いずれにせよ Lloyd Theorem に矛盾することが言え、定理1の証明が完了する。（なお $q=2$ の時、零点の分布は完全に対称になり、上の方法が使えないことに注意されたい。）

<u>Remark</u> 定理1の証明法は多くの (distance transitive) graphs の perfect code problem に応用出来る。今までにいくつかの場合を考えてみたが、いずれも成功するようである。

大ていの場合、Lloyd多項式(distance transitive graphsに対してそれは定義出来る)の零点はほぼ(零点の算術平均αに関して)対称であるが、完全には対称でない。(従って定理1の証明のようにそのずれを調べることにより矛盾が得られる。)ただし特別な場合(lattice graphsにおける$q=2$の場合にあたる)は完全に対称となり、上の方法は用いられない。但、この場合は

$$\prod_{\substack{i=-[\frac{e}{2}]\\ i\neq 0}}^{[\frac{e}{2}]}(x_i-\alpha)\cdot(-1)^{[\frac{e}{2}]}$$

が平方数とならなければならないことから、Thue-Siegel-Bakerなどによる不定方程式の整数解に関する深い結果を用いて、非存在が証明される場合もある。次の定理はその一例である。

定理2([4]) 各$e\geqq 4$に対して、odd graphs O_kにおけるperfect e-codesは高々有限個しか存在しない。また$e=4$のnontrivial perfect e-codeは存在しない。

問題(未解決と思う。何か御存知の方がいらっしゃいましたら是非教えて下さい)

(1) $\binom{x}{4}=\binom{y}{2}$ の整数解をもとめよ。(これが出来るとO_kのperfect 5-codesの非存在が言えると思う。なお上の式のかわりに$3(z^2-5)^2+96=w^2$ (z=odd) を考えてもよい。

(2) $$\frac{x(x+2)(x+4)\cdots(x+2(r-1))}{1\cdot3\cdot5\cdot\cdots\cdot(2r-1)}=y^2 \quad (r\geqq 3)$$ の整数解をもとめよ。但、必要なら、xはrにくらべてかなり大(e.g. $x>4r$)と仮定してよい。これについてはrが十分大の時非存在が証明出来たと思う。これは後述のtight spherical designsの存在問題および他にも色々関連する。

§3. Tight designs

Tight design の概念は perfect code の dual とも言えるもので、perfect code と同様、かなり広いクラスの graphs (あるいは association schemes) に対して定義が可能である。(Delsarte [6] 参照) 但、ここでは一般の場合を考えず、通常の tight designs についてまず考えることにする。通常の意味の t-(v, k, λ) design に対して、次の不等式が知られている。

定理 (Generalized Fisher の不等式) t-(v, k, λ) design (但、$t < k < v - [\frac{t}{2}]$) において、blocks の個数 b は

$$b \geqq \binom{v}{[\frac{t}{2}]}.$$

上で等式が成り立つ時、その design を tight design と呼ぶ。tight design が存在すれば $t = 2s$ (偶数) でなければならない。$t < k < v - t$ の design を nontrivial design と呼ぶ。

さて、Nontrivial tight 4-design は Ito [7] により Witt design 4-(23, 7, 1) 又はその complementary design 4-(23, 16, 52) に限ることが示されている。また Nontrivial tight 6-design の非存在は Peterson [8] により示されている。ここでは前の定理 1 と同様の方法を用いることにより、次の結果が得られることに注意しよう

定理3*([3]) 各 $s \geq 4$ に対して, nontrivial tight $2s$-design は高々有限個しか存在しない.

* 上の定理の証明の中で一ヶ所だけ(ある種の複雑な combinatorial identities について)きちんと証明していない所があるので厳密には定理といわない方がいいかもしれない。しかしいずれにせよ. その部分の証明はすぐ出来ると思うし. また小さい s, ($s=4, 5$ etc) の場合 あるいは $v > k \cdot f(e)$ ((但 $f(e)$ は e のみにより決まるある函数) という条件のもとでは完全な定理である.

定理3の証明は次の s次の多項式の零点が全て整数でなければならないという必要条件([6], [8] etc)をもちいる. この場合も Hermite 多項式が(定理1の証明におけるのと同様のいみで)本質的な役を演ずる:

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

Remark 上の通常の tight designs は Triangular graphs (= Johnson schemes) における "tight design" と考えられる. さて lattice graphs (= Hamming schemes) における "tight design" は Rao's bound を attain する orthogonal array と考えられる. なお q 個の元からなる alphabet の上に定義された length n, strength τ の orthogonal array Y に対して

$$|Y| \geq 1 + n(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{\tau}(q-1)^{\tau}$$

が知られており、上で等号が成り立つ時、Rao's bound を attain すると呼ぶことにする。定理1の証明の直接の系として、次の結果が得られる。

定理4　各 $\tau \geqq 3$ に対して、Rao's bound を attain する strength τ の orthogonal arrays (n, q は任意) は高々有限個しか存在しない。

§4. Concluding Remarks

Remark　ここで述べた方法は更に他の種類の問題、例えば tight spherical designs (Euclid 空間内の点の作るある種の集合) の存在問題にも有効である。ここではページ数の制限もあり、それについて詳しくは述べないが、興味のある方は [2] の preprint を著者まで請求されたい。ここでも Hermite 多項式が本質的な役割を演ずる。

Remark　ここで述べたことからもわかるように、組み合せ論と Orthogonal polynomials の理論には密接な関連がある。この原稿ではあまり直交多項式のことをおもてに出さなかったが、これらの問題と関連して、多くの(ありとあらゆる)直交多項式があらわれてくる。このことのさきがけは Delsarte [6] による。[6] での関係は多分に形式的な面にとどまっていたともいえなくないが、ここで述べた

ことは、それを越えて、これら2つに実質的な関係があることを表していると思う。なおここで取り扱った問題の中で本質的な役割を演じたのはいつも<u>Hermite多項式</u>であったが、例えばMoore graphsに近いようなグラフのクラス（そのようなgraphsの存在は不明だが）でperfect code problemを考えると、そこで本質的に出てくるのはHermite多項式でなく<u>Tchebycheff多項式</u>である。Hermite多項式、Tchebycheff多項式以外に本質的にあらわれる多項式としてどのようなものがあるかもっと知りたいが、今の所、この種の研究はまだはじまったばかりである。

References

[1] E. Bannai : On perfect codes in the Hamming schemes $H(n,q)$ with q arbitrary. (To appear in J.C.T.(A))

[2] ——— : On tight spherical designs (To appear)

[3] ——— : On tight designs (In preparation)

[4] ——— and D.H. Smith : On the nonexistence of perfect codes in the odd graphs O_k (to appear)

[5] N. Biggs : Perfect codes in graphs. J. Comb. Th. B (1973) vol 15. 289-296

[6] P. Delsarte : An algebraic approach to the association schemes of coding theory : Philip Res. Repts. Suppl. 10 (1973)

[7] N. Ito : On tight 4-designs. Osaka J. Math 12 (1975), 493-522

[8] C. Peterson : On tight 6-designs. To appear in Osaka J. Math.

（他にCameron・Van Lintによる最近の本（London Math. Soc Lecture series）などに関連した解説記事などがみられる。）