Singer difference sets and difference system of sets

東北大学・情報科学　　宗政昭弘

1　序

有限射影空間における射影直線の集合、または超平面の集合はいずれも BIBD をなすが、これら相互の関係について考える。特に、Singer cycle で不変な構造から、差集合の一般化である difference system of sets が得られるが、実際に計算機を用いて、$PG(4,8)$ 等について実例が見つかったことを報告する。

まず有限射影空間に関する基本的な用語を説明する。$PG(n,q)$ は、有限体 $GF(q)$ 上の n 次元射影空間を表す。その元は点と呼び、直線は射影直線を意味することとする。$PG(n,q)$ における spread とは、互いに交わらない直線の集合で $PG(n,q)$ 全体の分割になっているものである。Spread が存在するために必要十分条件は n が奇数であることである。Packing （または resolution, parallelism）とは、直線全体の集合の、spread への分割である。n が奇数のとき packing が存在するかどうかは、一般には未解決問題である。

一方、n が偶数のとき、$PG(n,q)$ には spread が存在しないので、当然 packing も存在しないのだが、$PG(n,q)$ の余次元 1 の超平面には spread が存在するので、直線全体の集合をそのような spread に分割することが可能か、という問題は意味を持つ。これが可能なとき、$PG(n,q)$ は $(n-1)$-partitionable であるという。$PG(n,q)$ における直線の総数は

$$\frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)} = \frac{(q^{n+1}-1)}{(q-1)} \cdot \frac{(q^n-1)}{(q^2-1)}$$

であり、右辺の第一因子は $PG(n,q)$ における余次元 1 の超平面の総数、第二因子は余次元 1 の超平面における spread を構成する直線の数であるから、上の問題には肯定的な解が期待される。この問題を提起したのは藤原–神保–Vanstone [2] であり、彼らは例えば $(n,q) = (4,2), (4,3), (6,q)$ 等について肯定的に解決している。問題を若干言い換えると、以下のようになる。

問題 1. $PG(2n,q)$ の余次元 1 の各超平面 H に対して、spread S_H が存在して、直線全体の集合を S_H たちの、互いに交わらない和集合として分割することが可能か。

この問題でにおいて、今まで未解決であった $(2n,q)$ の値は例えば $(4,4), (4,5), (4,7)$ 等がある。

このような問題を肯定的に解決する常套手段は、すべての超平面を考えるかわりに、超平面全体の集合に可移に作用する自己同型を用意して、ただ一つの超平面に関する問題に帰着することである。そのような自己同型として、よく知られた Singer cycle というものがある。Singer cycle とは、射影空間の巡回的な自己同型で、点集合にも、余次元 1 の超平面の集合にもただひとつの軌道を持っている。以下、射影空間の次元は偶数 $2n$ とし、$PG(2n,q)$ の Singer cycle を σ とする。今、H を余次元 1 の超平面とし、

$$H = L_1 \cup L_2 \cup \cdots \cup L_s$$

を H の spread とすると、

$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma$$

は H^σ の spread になる。さらに続けて σ を作用させることによって、すべての超平面の spread が得られる。ただ、これだけでは問題 1 の解になるとは限らない。なぜなら、上記の方法で得られた直線がすべて異なるという保証がないからである。その保証をするためには、H の spread を構成する

$L_1, L_2, \ldots, L_s$ がすべて異なる $\langle\sigma\rangle$ 軌道に属していれば十分である。したがって、Singer cycle を使って問題 1 の解を得るためには、次の問題を解けばよいことになる。

問題 2. $PG(2n, q)$ の余次元 1 の任意の超平面を H とする。H の spread S で、S に属する直線がすべて異なる $\langle\sigma\rangle$ 軌道に属しているようなものが存在するか。

このような spread は、以下に定義する、difference system of sets を与えることがわかる。

定義 3. G を位数 v の有限群、$\mathcal{S} = \{B_1, B_2, \ldots, B_k\}$ を G の k 個の m 元部分集合とする。Multiset として

$$\{gh^{-1} \mid g \in B_i,\ h \in B_j,\ 1 \le i, j \le k,\ i \ne j\}$$

が $\lambda(G - \{1\})$ に一致するとき、$\mathcal{S}$ を $(v, k, \lambda; m)$ difference system of sets と呼ぶ。

実際、$PG(2n, q)$ とその Singer cycle $G = \langle\sigma\rangle$ を同一視すれば、H の spread $H = L_1 \cup \cdots \cup L_s$ は G の $s = (q^{2n} - 1)/(q^2 - 1)$ 個の $q + 1$ 元部分集合の族と考えることができて、

$$(\frac{q^{2n+1} - 1}{q - 1}, \frac{q^{2n} - 1}{q - 1}, \frac{q^{2n-1} - q}{q - 1}; q + 1) \text{ difference system of sets}$$

になることが簡単にわかる。その証明で重要なことは、H が Singer difference set になることと、$\{L_1, \ldots, L_s\}$ が difference family になることである。後者は、$\{L_1, \ldots, L_s\}$ の展開が $PG(2n, q)$ の直線全体の集合に一致することによる。

2 得られた結果

定理 4. $PG(4, 4)$ には問題 2 の条件を満たす spread は存在しない。

定理 5. $PG(4, 8), PG(4, 9)$ には問題 2 の条件を満たす spread が存在する。

いずれも、計算機によって確かめられた。ここでは、定理 4 の確認方法を簡単に述べる。$PG(4, 4)$ の余次元 1 の任意の超平面を H とする。グラフ Γ を次のように定義する。Γ の頂点集合としては H に含まれる直線全体をとる。2 つの直線 L, L' に対して、L, L' が交わらず、また L, L' が同じ $\langle\sigma\rangle$ 軌道に属していないとき、L, L' は Γ において辺で結ぶことにする。このように定義したグラフ Γ においては、17 点の完全部分グラフが問題 2 の条件を満たす spread に対応する。計算代数システム magma [1] を用いて、グラフ Γ を実際に構成し、magma のビルトイン関数 `HasClique` を用いて 17 点完全部分グラフが存在しないことを確認した。

同様の方法で $PG(4, q)$ $(q > 4)$ の場合に exhaustive search をするには時間がかかりすぎるため、$\langle\sigma\rangle$ の代わりに $\langle\sigma\rangle$ と Frobenius automorphism で生成された、より大きい群で不変な line partition を探すことにより、定理 5 を得た。

参考文献

[1] Computer Algebra System Magma, `http://magma.maths.usyd.edu.au/`.

[2] R. Fuji-hara, M. Jimbo and S. Vanstone, Some results on the line partitioning problem in $PG(2k, q)$, Utilitas Math. 30 (1986), 235–241.