早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

論　文　題　目

A Study on Extension of Orthogonal Arrays and its Application to Experimental Designs and Unequal Error Protection Codes

直交配列の拡張及びその実験計画法と不均一誤り訂正符号への応用に関する研究

申　請　者

斉藤	友彦
SAITO	Tomohiko

2010 年　7 月

直交配列（Orthogonal Array: OA）は統計学における実験計画法を中心にコンピュータサイエンス，暗号学など幅広く応用されている．また，OA の数理モデルはラテン方格，アダマール行列などと関連があり，中でも誤り訂正符号とは特に密接な関連があることが知られている．

OA の定義は次の通りである．OA とは F_q 上 N×k 配列であり，かつ，“任意の t 列からなる N×t 部分配列の N 個の行ベクトルに全ての t 組が同数回現れる”ものである．以下ではこれを“強さ t”の OA と呼ぶ．このとき，OA の構成問題は次のように定式化される．

・配列の列数 k，有限体の位数 q，強さ t が与えられた下で，配列の行数 N が最小となる OA を求める問題．

この構成問題に伴い，次の OA の下界を求める問題も重要なものとなる．

・配列の列数 k，水準数 q，強さ t が与えられた下で，配列の行数 N の下界を求める問題．

得られた下界値は，構成された OA の評価に用いられるだけでなく，OA の構成に関する指針を与える意味でも重要な値となる．

OA は実験計画法において主要な役割を果たしている．実験計画法とは，少ない実験回数で，より多くの情報を実験から得るための技術である．例えば,次のような例を考える.ある化学製品の強度がその製造過程で反応温度，反応炉，触媒などの要因に影響を受けるものとする．このとき各要因に複数の水準を設定する．例えば反応温度を 800℃と 900℃，反応炉を 1 号炉と 2 号炉，触媒も 2 種類などのように設定する．なお，本研究では各要因に対して同じ水準数で実験を行う場合のみを扱っている．このとき全ての水準組合せで実験を行うことで各要因効果（要因の水準を変更することにより現れる効果），及び，交互作用効果（ある要因と要因の水準を組み合わせると現れる効果）を推定することができるが，これでは実験回数が膨大になってしまうため，その中の一部の実験でこれらを推定する必要がある．これは OA を用いることによって実現することができる．このとき，OA の各行は一つの水準組合せに対応する．従って，OA の列数は要因数，行数は実験回数，有限体の位数は水準数に対応する．また実験において存在が仮定される交互作用効果に対して，必要とされる OA の強さが定まる．正確には全ての e 次交互作用（e 要因間で現れる交互作用効果）が存在するとき強さ 2e の OA が必要となる．

従来,OA と誤り訂正符号には密接な関係があることが Delsarte や Sloane らによって示されている．誤り訂正符号は，通信途中で生じる雑音を訂正するために用いられる符号であり，次のように定義される．誤り訂正符号（もしくは単に符号と呼ぶ）とは F_q 上 k 次元ベクトル空間の部分集合であり，その要素数が N，かつ，符号の任意の要素間のハミング距離が d 以上であるとき，これを符号長 k，符号語数 N，最小距離 d の q 元符号と呼ぶ．このとき符号構成問題，符号の上界を求める問題は次のように定式化される．

・符号長 k，有限体の位数 q，最小距離 d が与えられた下で，符号語数 N が最大となる符号を求める問題．

・符号長 k，有限体の位数 q，最小距離 d が与えられた下で，符号語数 N の上界を求める問題．

符号の上界も，OA の下界と同様，符号の評価及び符号構成の指針を与える意味で重要な値となる．

Delsarte は OA 及び符号に対して，距離分布，双対距離分布と呼ばれるパラメータを導入し，OA と符号の関係を明確にした．ここで，符号長 k の 2 元符号 C（$\subseteq F_2{}^k$）の距離分布 A_i, i=0,1,...,k，双対距離分布 $A_i^{\perp}$, i=0,1,...,k，を

定義すると次のようになる.

$$A_i = \frac{1}{|C|}\sum_{x\in C}|\{y \in C \mid \mathrm{dist}(x,y) = i\}| \ ,$$

$$A_i^{\perp} = \frac{1}{|C|}\sum_{j=0}^{k} A_j P_i(j) \ .$$

但し$\mathrm{dist}(x,y)$は x, y のハミング距離であり，$P_i(j)$は次のように定義される.

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

さらに，Delsarte は OA と符号の関係を用い，OA の必要条件（OA の線形制約）を導いた．この必要条件を用いることによって，OA の下界を求める問題は線形計画（Linear Programming: LP）問題に帰着される．この LP 問題の解を LP 限界と呼び，LP 限界は現在最も強い OA の下界として知られている.

本論文では，OA を拡張し，部分的な強さを持つ OA（OA with Partial strength: POA）を導入している．POA の定義は次の通りである．部分的な強さ S（$\subseteq F_2{}^k$）を持つ POA とは F_q 上 N×k 配列であり，かつ，$i_1, i_2, \ldots, i_h$ 列目（$\{i_1, i_2, \ldots, i_h\} \in S'$）からなる N×h 部分配列の N 個の行ベクトルに全ての h 組が同数回現れるものである．但し，$v(a) = \{ i \mid a_i \neq 0 \}$ $(a = (a_1, a_2, \ldots, a_k,) \in F_2{}^k)$, $S' = \{v(a) \mid a \in S\}$とする．ここで $S = \{ a \in F_2{}^k \mid w(a) \leq t \}$（但し，$w(a)$は a のハミング重みとする）であるとき，この部分的な強さ S を持つ POA は強さ t の OA と等しい．また，POA の構成問題，下界を求める問題は次のように定式化される.

- 配列の列数 k，水準数 q，部分的な強さ S が与えられた下で，配列の行数 N が最小となる POA を求める問題.
- 配列の列数 k，水準数 q，部分的な強さ S が与えられた下で，配列の行数 N の下界を求める問題.

本論文ではこれらの問題に対していくつかの提案を行っている.

本論文ではまず POA と符号の関係について述べている．このとき距離分布，双対距離分布を拡張した m 分割距離分布，双対 m 分割距離分布（$1 \leq m \leq k$）と呼ばれるパラメータを導入し，POA と符号との関係を明確にしている．ここで符号長 $k(=\kappa_1 + \kappa_2 + \cdots + \kappa_m)$の 2 元符号 C の m 分割距離分布 $A_{i_1,i_2,\ldots,i_m}$, $i_g = 0,1,..,\kappa_g$, $1 \leq g \leq m$, 双対 m 分割距離 $A^{\perp}_{i_1,i_2,\ldots,i_m}$, $i_g = 0,1,..,\kappa_g$, $1 \leq g \leq m$を定義すると次のようになる.

$$A_{i_1,i_2,\ldots,i_m} = \frac{1}{|C|}\sum_{x\in C}|\{y \in C \mid \mathrm{dist}(x_1,y_1) = i_1, \mathrm{dist}(x_2,y_2) = i_2, \ldots, \mathrm{dist}(x_m,y_m) = i_m\}| \ ,$$

$$A^{\perp}_{i_1,i_2,\ldots,i_m} = \frac{1}{|C|}\sum_{j_1=0}^{\kappa_1}\sum_{j_2=0}^{\kappa_2}\cdots\sum_{j_m=0}^{\kappa_m} A_{i_1,i_2,\ldots,i_m} P_{i_1,i_2,\ldots,i_m}(j_1, j_2, \ldots, j_m) \quad ,$$

但し $x = (x_1, x_2, \ldots, x_m)$, $y = (y_1, y_2, \ldots, y_m) \in F_2^{\kappa_1} \times F_2^{\kappa_2} \times \ldots \times F_2^{\kappa_m}$であり，また

$$P_{i_1,i_2,\ldots,i_m}(j_1, j_2, \ldots, j_m) = P_{i_1}(j_1) P_{i_2}(j_2) \ldots P_{i_m}(j_m),$$

である．ここで，m=1 のとき，m 分割距離分布，双対 m 分割距離分布は距離分布，双対距離分布に一致する．さらに，本論文では POA と符号の関係を利用し，POA の必要条件（POA の線形制約）を導いている．この必要条件を用いることによって，POA の下界を求める問題も LP 問題に帰着される．この LP 問題の解を POA の LP 限界と呼ぶ．さらに，計算機を用いることに

よって，いくつかの LP 限界を実際に求めその有効性について検証している．

しかし，ここで示された LP 問題はその変数もしくは制約式の数が多すぎるため，列数 k が大きいとき，その LP 問題を解くことは困難である．そのため，LP 問題が解け，また実験計画法などへの応用に即した POA の部分クラスを考えることが次に重要となる．本論文ではこのような部分クラスの一つとして“列ごとに強さが異なる OA”を定義し，その LP 限界，さらにはその構成法について提案を行っている．

最後に，本論文の工学的意義についてまとめる．本論文では POA を導入する工学的意義として以下の二点を挙げている．

1．POA は複雑な交互作用に対応することができるため，実験計画法の問題により適している．

2．POA の部分クラス（列ごとに強さが異なる OA）は不均一誤り訂正（Unequal Error Protection: UEP）符号に対応する．

まず一点目の意義について述べる．上でも述べた通り，実験において全ての e 次交互作用が存在するとき，強さ 2e の OA が必要となる．しかし，実験計画法では，ある一部の e 次交互作用のみが存在する，など複雑な交互作用効果の存在を仮定することが一般的である．このような仮定に対して，OA では対応できないのに対して，POA では対応することが可能である．そのため，従来から実験計画法が実際に用いられる現場では POA のような配列が考えられており，その構成法については多くの提案がなされている．本論文ではそれらの構成法に関し，POA の下界という視点から評価を行っている．

次に二点目の意義について述べる．UEP 符号とは Masnick らによって提案された，符号のビットごとに最小距離（誤り訂正能力）が異なる符号である．UEP 符号は数値情報など位置（数値情報の場合は桁）によって情報の重要度が異なるものの符号化に有効であるとされている．この UEP 符号は上で述べた，列ごとに強さが異なる OA と対応している．そのため，これと同様に LP 問題を定式化し，その LP 限界を求めることができる．本論文では UEP 符号の LP 限界を提案し，修正ハミング限界と呼ばれる他の UEP 符号の限界と理論的な側面から比較をしている．さらに，計算機を用いることによって，UEP 符号の LP 限界を実際に求め，数値例からもその有効性を検証している．

以上を総括すると，本研究は従来の OA を一般化した POA を定義し，POA と符号の関係，POA の限界，POA の構成法について提案を行うと共に，これらの実験計画法や UEP 符号への応用について論じている．本研究の結果は OA，実験計画法，誤り訂正符号の各分野において理論的かつ実用的に重要な結果であると言える．よって本論文は博士（工学）の学位論文として価値のあるものと認める．

2010 年 7 月

審査員（主査）	早稲田大学教授	博士(工学)早稲田大学	松嶋 敏泰
	早稲田大学教授	工学博士(早稲田大学)	大石 進一
	早稲田大学名誉教授	工学博士(大阪大学)	平澤 茂一
	早稲田大学教授	理学博士(東京大学)	橋本 喜一朗