早稲田大学大学院　基幹理工学研究科

博 士 論 文 概 要

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
Tomohiko	Saito

2010 年　5 月

直交配列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，直交配列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．

直交配列の定義は次の通りである.直交配列とは F_q 上 $N \times k$ 配列であり,かつ，“任意の t 列からなる $N \times t$ 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”の直交配列と呼ぶ．このとき，直交配列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 が最小となる直交配列を求める問題．

また，この構成問題に伴い，次の行数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，構成された直交配列の評価に用いられるだけでなく，直交配列の構成に関する指針を与える意味でも重要な値となる．

従来，直交配列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考える．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，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．これは直交配列を用いることによって実現することができる．このとき，直交配列の各行は一つの水準組合せに対応する．従って，直交配列の列数は要因数，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，必要とされる直交配列の強さが定まる．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 の直交配列が必要となる．

また，直交配列はディジタル通信における誤り訂正符号と密接な関連がある．誤り訂正符号とはディジタル情報を通信・記録する際に生じる誤りを訂正するための符号化に関する技術である．誤り訂正符号において，符号構成問題は最も基本的な問題の一つである.符号とは 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.

また, 符号構成問題に伴い, 次の符号語数の上界を求める問題も重要である.

・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 の上界を求める問題.

直交配列, 及び, 誤り訂正符号はそれぞれ別々に発展した分野であるが, Delsarte や Sloane らの研究などによって, その対応関係が明らかにされた. 特に, Delsarte によって示された, 直交配列における強さと符号における双対距離と呼ばれるパラメータの対応関係は重要なものである. これらの対応関係を用いることによって, どちらか一方の成果をもう一方に応用することが可能である.

従来, 直交配列における行数の下界（及び, 符号における符号語数の上界）を求める問題に対して, Delsarte は線形計画限界を提案している. これによって, 行数の下界を求めることは線形計画問題を解くことに帰着される. また, Sloane らはこの線形計画問題を実際に解くことによって, いくつかのパラメータにおける下界値を実際に求め, 他の下界との比較を行っている. これらの結果から線形計画限界は現在最も優れた下界として知られている.

本研究では直交配列における強さの概念を拡張し, 部分的な強さ S（$\subseteq F_2^k$）を持つ直交配列（Orthogonal Arrays with Partial Strength: POA）を提案する. POA においても構成問題, 及び, 行数の下界を求める問題が重要なテーマとなり, それぞれ以下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.

本研究ではこれらの問題に対して, いくつかの提案を行う.

強さの概念を拡張し, POA を提案する意義は次の二点である.

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 のある部分クラスは誤り訂正符号における不均一誤り訂正符号に対応する.

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 の直交配列が必要となる. 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, 従来の直交配列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. 次に二点目の意義について述べる. これは本研究の成果の一つであるが, POA のある部分クラ

スは，Masnick らによって提案された不均一誤り訂正符号と対応する．このことから POA に関して得られた成果は不均一誤り訂正符号に応用することが可能である．

本研究では，まず POA の定義を行い，その実験計画法への応用，及び，POA と符号の関係について述べる．次に POA の行数の下界（及び，POA に対応する符号の符号語数の上界）を求める問題に対して，線形計画限界の拡張を行う．これによって，POA においても，行数の下界を求めることは線形計画問題を解くことに帰着される．但し，ここで得られた線形計画問題は変数，及び，制約式の数が多すぎるため，列数が大きいとき，この問題を解くことは困難である．そのため，線形計画問題が解け，かつ実験計画法への応用に即した，POA の部分クラスについて考えることが重要である．

次に，上記で述べた POA の部分クラスの一つとして，列ごとに強さが異なる直交配列の定義を行う．そして，これが不均一誤り訂正符号と対応していることを示し，これを用いて不均一誤り訂正符号における線形計画限界を提案する．さらに不均一誤り訂正符号における符号語数の上界として知られる Masnick らの修正ハミング限界と本研究による線形計画限界との比較を行う．

最後に，不均一誤り訂正符号の構成法として知られる Masnick らや Boyarinov らの手法を利用した，新たな POA（列ごとに強さが異なる直交配列）の構成法を提案する．ここでは上で述べた，列ごとに強さが異なる直交配列と不均一誤り訂正符号との関係を利用する．

本論文の構成は次の通りである．

第 1 章では本研究の序論として，研究背景，目的について述べる．

第 2 章では準備として，本研究で用いる基本事項，及び従来研究について述べる．まず，直交配列の定義，性質について述べる．次に直交配列の実験計画法への応用，及び，直交配列と誤り訂正符号の関係について述べる．最後に直交配列，及び，符号における線形計画限界について述べる．

第 3 章では POA について述べる．まず POA の定義，性質について述べる．次に POA の実験計画法への応用，POA と符号の対応関係について述べる．最後に POA，及び，POA に対応する符号の線形計画限界を提案する．

第 4 章では列ごとに強さが異なる直交配列，及び，不均一誤り訂正符号について述べる．まずこれらの定義を述べ，次にその線形計画限界を提案する．そして，Masnick らの修正ハミング限界との比較を行う．

第 5 章では不均一誤り訂正符号構成法を利用した，POA の構成について述べる．まず Masnick らや Boyarinov らの手法を利用した構成法を提案し，次にその有効性を数値例によって検証する．

第 6 章では結論として，本研究のまとめについて述べる．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　斉藤　友彦　　印

（２０１０年　４月　現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
1.論文	A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes Journal of Discrete Mathematical Sciences & Cryptography (掲載決定) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
2.論文	A Note on a Sampling Theorem for Functions over GF(q)^n Domain IEICE Trans. Fundamentals (掲載決定) Yoshifumi Ukita, Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
3.○論文	Linear Programming Bounds of Orthogonal Arrays for Experimental Designs Proceedings of IEEE African Winter School on Information Theory and Communications 2010 (掲載決定) Tomohiko Saito, Yoshifumi Ukita, Toshiyasu Matsushima and Shigeichi Hirasawa
4.論文	A Description of Experimental Design using an Orthonormal System Proceeding of 2010 RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing, pp.429-432 (2010-3) Yoshifumi Ukita, Tomohiko Saito and Toshiyasu Matsushima
5.○論文	A Linear Programming Bound for Unequal Error Protection Codes Proceedings of the 2010 Australian Communications Theory Workshop, pp.24-29 (2010-2) Tomohiko Saito, Yoshifumi Ukita, Toshiyasu Matsushima and Shigeichi Hirasawa
6.論文	A Note on the Relation between a Sampling Theorem for Functions over a GF(q)^n Domain and Linear Codes 2009 IEEE International Conference on Systems, Man, and Cybernetics, pp.2665-2670 (2009-10) Yoshifumi Ukita, Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
7.論文	A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes Proceeding of Pre-ICM International Convention on Mathematical Sciences, p.112 (2008-12) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
8.○論文	A Note on Construction of Orthogonal Arrays with Unequal Strength from Error-Correcting Codes IEICE Trans. Fundamentals, Vol.E89-A, No.5, pp.1307-1315 (2006-5) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
9．論文	ストリーム暗号における擬似乱数生成器の構成に関する一考察 電子情報通信学会論文誌(Ａ)，Vol.J90-A，No.5，pp.470-476 (2007-5) 三上暢仁，斉藤友彦，松嶋敏泰
10．論文	ストリーム暗号への攻撃法の改良に関する一考察－多次元の相関を利用した攻撃－ 電子情報通信学会論文誌(Ａ)，Vol.J89-A，No.2，pp.121-128 (2006-2) 細渕智史，斉藤友彦，松嶋敏泰
11.講演	A Linear Programming Bound for Unequal Error Protection Codes 第 32 回情報理論とその応用シンポジウム予稿集(SITA),pp.359-364 (2009-12) Tomohiko Saito, Yoshifumi Ukita, Toshiyasu Matsushima and Shigeichi Hirasawa
12.講演	A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes 第 31 回情報理論とその応用シンポジウム予稿集(SITA)，pp.939-944 (2008-10) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
13.講演	On Factorial Effects Corresponding to Orthogonal Arrays with Unequal Strength Proceeding of 2006 Hawaii, IEICE and SITA Joint Conference on Information Theory (HISC2006)，pp.53-58 (2006-5) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
14.講演	A Note on Construction of Nonlinear Unequal Orthogonal Arrays from Error-Correcting Codes Proceeding of 2005 Hawaii, IEICE and SITA Joint Conference on Information Theory (HISC2005)，pp.13-18 (2005-5) Tomohiko Saito, Toshiyasu Matsushima and Shigeichi Hirasawa
15.講演	誤り訂正符号を利用した直交計画の構成法に関する一考察 ～逐次実験に適した直交計画について～ 第 27 回情報理論とその応用シンポジウム予稿集(SITA)，pp.463-466 (2004-12) 斉藤友彦，松嶋敏泰，平澤茂一
16.講演	誤り訂正符号を利用した直交計画の構成法に関する一考察 第 25 回情報理論とその応用シンポジウム予稿集(SITA)，pp.663-666 (2002-12) 斉藤友彦，吉田 隆弘，松嶋敏泰
17.講演	ランプ型 Robust 秘密分散法に関する一考察 2007 年暗号と情報セキュリティシンポジウム予稿集(SCIS) (2007-1) 宍戸大介，斉藤友彦，松嶋敏泰

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
18.講演	ID 情報に基づくランプ型非対称鍵配送方式について 2006 年暗号と情報セキュリティシンポジウム予稿集(SCIS) (2006-1) 海上勇二，斉藤友彦，松嶋敏泰
19.講演	Fast Correlation Attack の改良法に関する一考察 第 27 回情報理論とその応用シンポジウム予稿集(SITA)，pp.37-40 (2004-12) 細渕智史，斉藤友彦，松嶋敏泰
20.講演	衝突困難ハッシュ関数の安全性について 第 26 回情報理論とその応用シンポジウム予稿集(SITA)，pp.609-612 (2003-12) 渋谷知成，斉藤友彦，松嶋敏泰