Orthogonal Arrays & Quantum Error Correcting Codes

Jakub Bielawski [1]

[1]Wydział Fizyki, Astronomii i Informatyki
Uniwersytetu Jagiellońskiego

14 grudnia 2015

Outline

Orthogonal Arrays

Definition

An Orthogonal Array of strength k with r rows N columns and based on d symbols is an $r \times N$ array with entries $0, 1, \ldots, d-1$ such that every $r \times k$ subarray contains each of the s^k possible k-tuples equally often (say λ times) as a row.

- $\lambda = r/s^k$ is the index of the array
- Notation: $\mathrm{OA}(r, N, d, k)$
- Terminology:
  - r: number of rows or runs
  - N: number of columns of factors
  - d: number of symbols of levels
  - k: strength

$\mathrm{OA}(4, 3, 2, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal Arrays

Definition

An Orthogonal Array of strength k with r rows N columns and based on d symbols is an $r \times N$ array with entries $0, 1, \ldots, d-1$ such that every $r \times k$ subarray contains each of the s^k possible k-tuples equally often (say λ times) as a row.

- $\lambda = r/s^k$ is the index of the array
- Notation: $\mathrm{OA}(r, N, d, k)$
- Terminology:
  - r: number of rows or runs
  - N: number of columns of factors
  - d: number of symbols of levels
  - k: strength

$\mathrm{OA}(4, 3, 2, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal Arrays

Definition

An Orthogonal Array of strength k with r rows N columns and based on d symbols is an $r \times N$ array with entries $0, 1, \ldots, d-1$ such that every $r \times k$ subarray contains each of the s^k possible k-tuples equally often (say λ times) as a row.

- $\lambda = r/s^k$ is the index of the array
- Notation: $\mathrm{OA}(r, N, d, k)$
- Terminology:
  - r: number of rows or runs
  - N: number of columns of factors
  - d: number of symbols of levels
  - k: strength

$\mathrm{OA}(4, 3, 2, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

Orthogonal Arrays

Definition

An Orthogonal Array of strength k with r rows N columns and based on d symbols is an $r \times N$ array with entries $0, 1, \ldots, d-1$ such that every $r \times k$ subarray contains each of the s^k possible k-tuples equally often (say λ times) as a row.

- $\lambda = r/s^k$ is the index of the array
- Notation: $\mathrm{OA}(r, N, d, k)$
- Terminology:
  - r: number of rows or runs
  - N: number of columns of factors
  - d: number of symbols of levels
  - k: strength

$\mathrm{OA}(4, 3, 2, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

Classical Error Correcting Codes

Let S be a set of symbols of size d and let S^N denotes the set of all d^N vectors of length N. An linear error-correcting code, or simply a code is a vector subspace C of S^N. This implies that C has size $r = d^n$ for some $0 \leqslant n \leqslant N$, this is called the dimension of the code.

Notation: $(N, r, k)_d$

The Hamming weight $w(u)$ of a vector $u = (u_1, \ldots, u_N) \in S^N$ is defined to be the number of nonzero components u_i. The Hamming distance between two vectors $u, v \in S^N$ is defined by $\mathrm{dist}(u, v) = w(u - v)$ and the minimal distance of a code C is the minimal distance between codewords

$$k = \min\{\mathrm{dist}(u, v) : u, v \in C, u \neq v\}.$$

A code of minimal distance k can correct any number from 1 to $\lfloor \frac{k-1}{2} \rfloor$ of errors when used on a noisy channel.

Orthogonal arrays & Classical Error Correcting Codes

Example

The set $\{00000, 11111\}$ is a $(5, 2, 5)_2$ code.

Associated with any linear code C is another code called its dual, and denoted by $C^{\perp}$. The dual code consist of all vectors $v \in S^N$ such that

$$uv^T = 0 \text{ for all } u \in C.$$

Theorem

If C is a $(N, r, k)_d$ linear code with dual distance $k^{\perp}$ then the codewords of C form the rows of an $\mathrm{OA}(r, N, d, k^{\perp} - 1)$.
Conversely, the rows of an $\mathrm{OA}(r, N, d, k)$ form a $(N, r, l)_d$ linear code with dual distance $l^{\perp} \geqslant k + 1$. If the orthogonal array has strength k but not $k + 1$ then $l^{\perp} = k + 1$.

Orthogonal arrays & Classical Error Correcting Codes

Example

Code $(5, 2, 5)_2$ from the previous example has its dual code $(5, 16, 2)_2$. The codewords of C form an $\mathrm{OA}(2, 5, 2, 1)$

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{array}$$

while the codewords of $C^{\perp}$ form an $\mathrm{OA}(16, 5, 2, 4)$ (transposed)

$$\begin{array}{ccccccccccccccc} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Irredundant Orthogonal Arrays

Definition

An array $A \in \mathrm{OA}(r, N, d, k)$ is called irredundant if every $r \times (N-k)$ subarray of A contains no repetitions of any of its $(N-k)$-tuple.

Notation: $\mathrm{IrOA}(r, N, d, k)$.

k-uniform states

Definition

A pure quantum state of N subsystems with d levels each is called k-uniform if every reduction to k qudits is maximally mixed.

Remark

Consider the following measure of entanglement

$$Q_k(\psi) = \frac{D^k}{D^k - 1}\left(1 - \frac{k!(n-k)!}{n!}\sum_{|S|=k} \mathrm{tr}\rho_S^2\right), \quad \text{for } k = 1, \ldots, \left\lfloor \frac{n}{2} \right\rfloor,$$

where $|\psi\rangle \in (C^D)^{\otimes n}$, $S \subset \{1, \ldots, n\}$ and $\rho_S = \mathrm{tr}_{S'}|\psi\rangle\langle\psi|$.
Then $Q_k(\psi) = 1$ if and only if $|\psi\rangle$ is k-uniform.

♦ A. J. Scott, *Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions*, PHYSICAL REVIEW A 69, 052330 (2004)

k-uniform states

- For 2 qubits there are four 1-uniform states, these are the Bell states:

$$|\Phi_2^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right) \qquad \text{and} \qquad |\Psi_2^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$$

- For 3 qubits there is only one 1-uniform state, the GHZ state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$$

- For N qudits the GHZ state

$$|GHZ_N^d\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes N}$$

  is 1-uniform.
- Although the $|W\rangle = \frac{1}{\sqrt{3}}\left(|100\rangle + |010\rangle + |001\rangle\right)$ state is maximally entangled it is not 1-uniform.

k-uniform states & Irredundant Orthogonal Arrays

Consider a superposition of r product states

$$|\Phi\rangle = |s_1^1 s_2^1 \dots s_N^1\rangle + |s_1^2 s_2^2 \dots s_N^2\rangle + \dots + |s_1^r s_2^r \dots s_N^r\rangle,$$

where we assume for simplicity that every coefficients is zero or one. Arrange the symbols in an array as follows

$$A_\Phi = \begin{matrix} s_1^1 & s_2^1 & \dots & s_n^1 \\ s_1^2 & s_2^2 & \dots & s_N^2 \\ \vdots & \vdots & \vdots & \vdots \\ s_1^r & s_2^r & \dots & s_N^r \end{matrix}$$

k-uniform states & Irredundant Orthogonal Arrays

Theorem

1. *If the array A_Φ is an $\mathrm{OA}(r, N, d, k)$ then after tracing out all but k qudits the reduction has all elements on the diagonal equal.*
2. *If the array A_Φ has no repetitions of rows in every $r \times (N - k)$ subarray then after tracing out all but k qudits the reduction has all off-diagonal elements equal zero.*

Consequently, if the array A_Φ is an $\mathrm{IrOA}(r, N, d, k)$ then the state $|\Phi\rangle$ is k-uniform.

k-uniform states & Irredundant Orthogonal Arrays

Example

- $$\mathrm{IrOA}(2,2,2,1) = \begin{matrix} 0 & 0 \\ 1 & 1 \end{matrix}$$

  corresponds to the Bell state $|\Phi_2^+\rangle = |00\rangle + |11\rangle$;

- $$\mathrm{IrOA}(2,2,2,1) = \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$$

  corresponds to the Bell state $|\Psi_2^+\rangle = |01\rangle + |10\rangle$;

- $$\mathrm{IrOA}(2,3,2,1) = \begin{matrix} 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix}$$

  corresponds to the $|GHZ\rangle = |000\rangle + |111\rangle$ state;

k-uniform states & Irredundant Orthogonal Arrays

Example

- the following array found in the catalog of Kuhfeld (http://support.sas.com/techsup/technote/ts723.html)

$$\begin{array}{ccc} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

is $\mathrm{OA}(4,3,2,2)$ but it is not $\mathrm{IrOA}(4,3,2,2)$. However this array can be regarded as $\mathrm{IrOA}(4,3,2,1)$ and consequently it can be used to construct 1-uniform state $|\psi\rangle = |000\rangle + |011\rangle + |101\rangle + |110\rangle$;

k-uniform states & Irredundant Orthogonal Arrays

Example

- the following array found in the catalog of Kuhfeld (http://support.sas.com/techsup/technote/ts723.html)

$$\begin{array}{cccc} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 \\ 0 & 2 & 1 & 2 \\ 1 & 0 & 2 & 2 \\ 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 2 & 1 & 0 & 2 \\ 2 & 2 & 2 & 0 \end{array}$$

is $\mathrm{IrOA}(9, 4, 3, 2)$ and can be used to construct 2-uniform state $|\psi\rangle = |0000\rangle + |0121\rangle + |0212\rangle + |1022\rangle + |1110\rangle + |1201\rangle + |2011\rangle + |2102\rangle + |2220\rangle$.

k-uniform states & Quantum Error Correcting Codes

An encoding of a K-dimensional quantum state into N qudits is a linear map from $\mathbb{C}^K$ to subspace $\mathcal{Q}$ of $(\mathbb{C}^D)^N$. An error operator E is a linear map acting on $(\mathbb{C}^D)^N$.

Theorem

Let $|\psi\rangle$ be a pure quantum state of N subsystems with d levels each. The state $|\psi\rangle$ is k-uniform if and only if the subspace generated by $|\psi\rangle$ is $((N, 1, k+1))_d$ quantum error correcting code.

♦ A. J. Scott, *Multipartite entanglement, quantum-error-correcting codes, and entangling power of quantum evolutions*, PHYSICAL REVIEW A 69, 052330 (2004)

Mixed Orthogonal Arrays

Definition

1. An $r \times N$ array A with entries in the first N_1 columns taken from $\{0, 1, \ldots, d_1 - 1\}$, entries in the next N_2 columns taken from $\{0, 1, \ldots, d_2 - 1\}$, and so on, where $N = N_1 + N_2 + \ldots + N_n$ is the total number of columns, is said to be a mixed orthogonal array with r runs, N factors, d_i levels in N_i factors for $i = 1, 2, \ldots, n$, and strength k if every $r \times k$ subarray of A contains each possible k-tuple an equal number of times as a row.
2. A mixed orthogonal array is called irredundant if every $r \times (N - k)$ subarray contains no repetitions of any of its $(N - k)$-tuple.

Notation:

1. $\mathrm{MOA}(r, d_1^{N_1} \ldots d_n^{N_n}, k)$
2. $\mathrm{IrMOA}(r, d_1^{N_1} \ldots d_n^{N_n}, k)$

Irredundant Mixed Orthogonal Arrays

Example

$$\mathrm{IrMOA}(12, 2^6 3^1, 2) = \begin{array}{ccccccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 2 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 2 \end{array}$$

Irredundant Mixed Orthogonal Arrays

Theorem

An array $A \in \mathrm{IrMOA}(2n, 2^n\ n^1, 2)$ exists if there exists a Hadamard matrix of size n.

Construction

$$A = \begin{array}{|c|c|} \hline & 0 \\ \overline{H_n} & 1 \\ & \dots \\ & n-1 \\ \hline & 0 \\ H_n & 1 \\ & \dots \\ & n-1 \\ \hline \end{array}$$

Open problem

Existence of irredundant mixed orthogonal array of strength 3.