Higher Dimensional Optical Orthogonal Codes

Finite Geometries 2017
5th Irsee Conference

Tim Alderson [1]

University of New Brunswick

September 12, 2017.

[1]Supported by the NSERC of Canada Discovery Grants Program.

Table of contents

In Optical code-division multiple access (OCDMA) applications, the number of codewords in an OOC corresponds to possible number of asynchronous users able to transmit information efficiently and reliably.

1D-OOCs suffer from small cardinality (need long codewords or relaxed correlations).

3D-OOCs or space/wavelength/time OOCs encode the data bits in spatial, wavelength and time domains, overcoming the 1D-OOC shortcomings.

3D OOCs

We denote by $(\Lambda \times S \times T, w, \lambda_a, \lambda_c)$ a 3D-OOC with constant weight w, Λ wavelengths, space spreading length S, and time-spreading length T (hence, each codeword may be considered as an $\Lambda \times S \times T$ binary array) subject to the following properties.

- (auto-correlation property) for any codeword $A = (a_{i,j,k})$ and for any integer $1 \leq t \leq T-1$, we have
$$\sum_{i=0}^{S-1}\sum_{j=0}^{\Lambda-1}\sum_{k=1}^{T-1} a_{i,j,k}a_{i,j,k+t} \leq \lambda_a,$$
- (cross-correlation property) for any two distinct codewords $A = (a_{i,j,k})$, $B = (b_{i,j,k})$ and for any integer $0 \leq t \leq T-1$, we have $$\sum_{i=0}^{S-1}\sum_{j=0}^{\Lambda-1}\sum_{k=0}^{T-1} a_{i,j,k}b_{i,j,k+t} \leq \lambda_c,$$

where each subscript is reduced modulo T.

Example

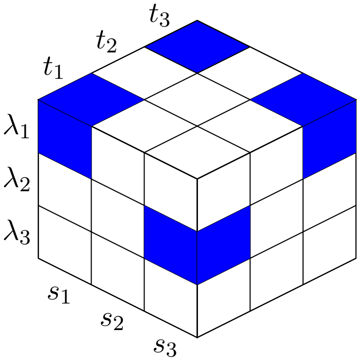


Figure: Autocorrelation $\lambda_a = 1$

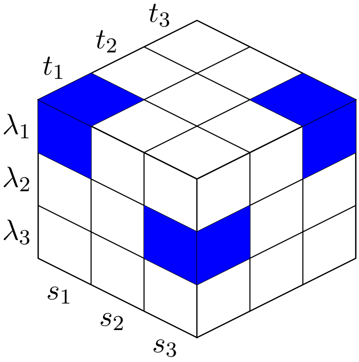
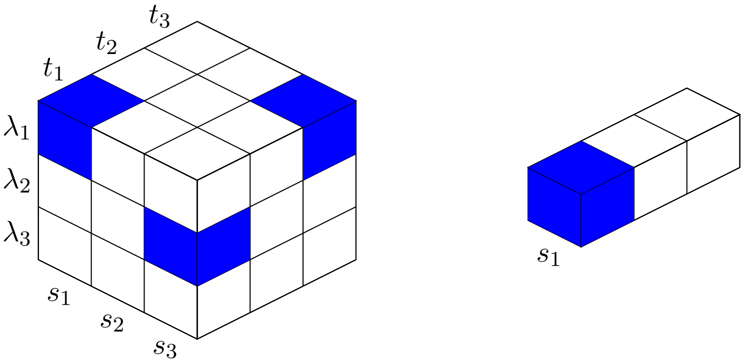


Figure: Autocorrelation zero!

Codes with $\lambda_a = 0$ are called **ideal codes**.

Bounds



A codeword from an ideal 3-D OOC, black cubes indicate 1, white indicate 0. (b) Each of the ΛS space/wavelength sections correspond to an element from an alphabet of size $T+1$.

Bounds

Let $\Phi(C)$ denote the theoretical upper bound on the capacity of C. After adapting the Johnson Bound for non-binary alphabets we obtain the following bound for ideal 3-D OOCs.

Theorem

[Johnson Bound for Ideal 3D OOC]
Let C be an $(\Lambda \times S \times T, w, 0, \lambda)$-OOC, then

$$\Phi(C) \leq J(\Lambda \times S \times T, w, 0, \lambda_c)$$
$$= \left\lfloor \frac{\Lambda S}{w} \left\lfloor \frac{T(\Lambda S - 1)}{w-1} \left\lfloor \cdots \left\lfloor \frac{T(\Lambda S - \lambda)}{w - \lambda} \right\rfloor \right\rfloor \cdots \right\rfloor\right.$$

Note thatif C is an ideal 3D OOC of maximal weight ($w = \Lambda S$) then $\Phi(C) \leq T^{\lambda}$.
Codes meeting the bound will be said to be *J-optimal*.

Bounds

One way to achieve $\lambda_a = 0$ is to select codes with at most one pulse per spatial plane. Such codes are referred to as *at most one pulse per plane* (AMOPP) codes. AMOPP codes of maximal weight S have a single pulse per spatial plane, and are referred to as SPP codes.

Bounds

Using similar methods as above we are able to establish that for fixed dimensions, weight, and correlation

$$
\begin{aligned}
\Phi(SPP) &\leq \Lambda^{\lambda} T^{\lambda-1} \\
&\leq \Phi(AMOPP) \\
&\leq \left\lfloor \frac{1}{T} \left\lfloor \frac{\Lambda ST}{w} \left\lfloor \frac{\Lambda T(S-1)}{w-1} \left\lfloor \cdots \left\lfloor \frac{\Lambda T(S-\lambda)}{w-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor \\
&\leq \Phi(Ideal) \\
&\leq \left\lfloor \frac{\Lambda S}{w} \left\lfloor \frac{T(\Lambda S-1)}{w-1} \left\lfloor \cdots \left\lfloor \frac{T(\Lambda S-\lambda)}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor
\end{aligned}
$$

Known families of optimal ideal 3D OOC, $\lambda_c = 1$.

p a prime, q a prime power, $\theta(k,q) = \frac{q^{k+1}-1}{q-1}$

Conditions	Type	Ref.
$w = S \leq p$ for all p dividing ΛT	SPP	Kim,Yu,Park, (2000)
$w = S = \Lambda = T = p$	SPP	Li, Fan, Shum (2012)
$w = S = 4 \leq \Lambda = q$, $T \geq 2$	SPP	Li, Fan, Shum (2012)
$w = S = q+1$, $\Lambda = q > 3$, $T = p > q$	SPP	Li, Fan, Shum (2012)
$w = S = 3$ $\Lambda \equiv T \mod 2$	SPP	Shum (2015)
$w = 3$, $\Lambda T(S-1)$ even, $\Lambda T(S-1)S \equiv 0$ mod 3, and $S \equiv 0, 1$ mod 4 if $T \equiv 2$ mod 4 and Λ is odd.	AMOPP	Shum(2015)

Projective Spaces: Notation

- $PG(k,q)$: The finite projective geometry of dimension k and order q.
- The number of points of $PG(k,q)$:

$$\theta(k,q) = \theta(k) = \frac{q^{k+1}-1}{q-1}.$$

- Number of lines on $PG(k,q)$: $\mathcal{L}(k)$
- The number of d-flats in $PG(k,q)$:

$$\begin{bmatrix} k+1 \\ d+1 \end{bmatrix}_q = \frac{(q^{k+1}-1)(q^{k+1}-q)\cdots(q^{k+1}-q^d)}{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}.$$

Singer representation

A **Singer group** is a cyclic group acting sharply transitively on the points of $PG(k,q)$. A generator is a **Singer cycle**.
Let β be a primitive element of $GF(q^{k+1})$. Then the powers of β:

$$\beta^0, \beta^1, \beta^2, \ldots, \beta^{q^k+q^{k-1}+\cdots+q^2+q(=\theta(k,q)-1)}$$

represent the projective points of $\Sigma = PG(k,q)$.

Denote by ϕ the Singer cycle of Σ defined by $\beta^i \mapsto \beta^{i+1}$.

Codewords from Orbits

Let $n = \theta(k) = \Lambda \cdot S \cdot T$ where G is the Singer group of $\Sigma = PG(k, q)$. Since G is cyclic there exists a unique subgroup H of order T (H is the subgroup with generator $\phi^{\Lambda S}$).

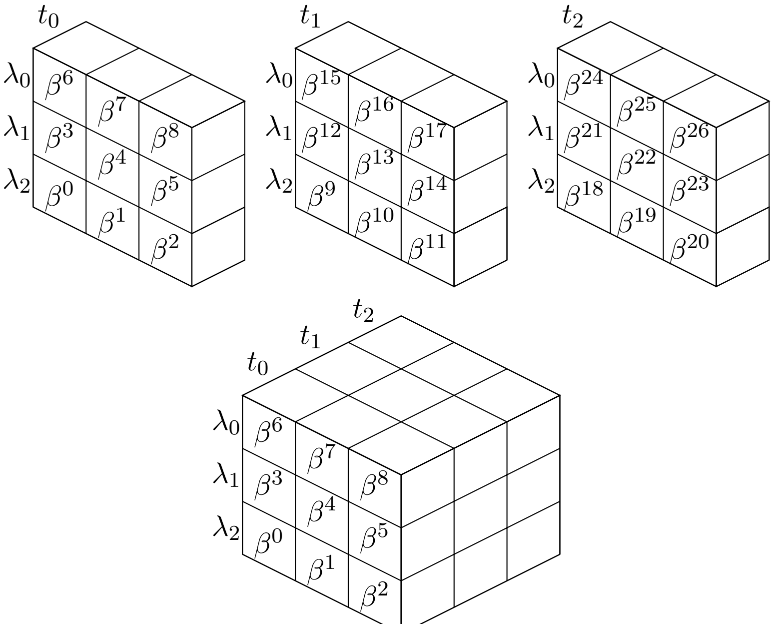
Definition (Projective Incidence Array)

Let Λ, S, T be positive integers such that $\theta(k, q) = \Lambda \cdot S \cdot T$. For an arbitrary pointset $\mathcal{A}$ in $\Sigma = PG(k, q)$ we define the $\Lambda \times S \times T$ incidence array $A = (a_{i,j,k})$, $0 \leq i \leq \Lambda - 1$, $0 \leq j \leq S - 1$, $0 \leq k \leq T - 1$ where $a_{i,j,k} = 1$ if and only if the point corresponding to $\beta^{i+j\cdot\Lambda+k\cdot S\Lambda}$ is in $\mathcal{A}$.

Note that a cyclic shift of the temporal planes of A is the incidence array corresponding to $\sigma(\mathcal{A})$.

UNB Saint John

β^9 induces a cyclic shift of the temporal planes.



If $\mathcal{A}$ is a pointset of Σ, consider its orbit $Orb_H(\mathcal{A})$ under the group H generated by $\phi^{\Lambda S}$.
The set $\mathcal{A}$ has *full H-orbit* if $|Orb_H(\mathcal{A})| = T = \frac{n}{\Lambda S}$ and *short H-orbit* otherwise.
If $\mathcal{A}$ has full H-orbit then a representative member of the orbit and corresponding 3-D codeword is chosen. The collection of all such codewords gives rise to a $(\Lambda \times S \times T, w, \lambda_a, \lambda_c)$-3D-OOC, where

$$\lambda_a = \max_{0 \leq i < j \leq T-1} \left\{ |\phi^{\Lambda S \cdot i}(\mathcal{A}) \cap \phi^{\Lambda S \cdot j}(\mathcal{A})| \right\} \tag{1}$$

and

$$\lambda_c = \max_{0 \leq i, j \leq T-1} \left\{ |\phi^{\Lambda S \cdot i}(\mathcal{A}) \cap \phi^{\Lambda S \cdot j}(\mathcal{A}')| \right\} \tag{2}$$

ranging over all $\mathcal{A}$, $\mathcal{A}'$ with full H-orbit.

A handy Theorem

Theorem (Rao (1969), Drudge (2002))

In $\Sigma = PG(k,q)$, there exists a short G-orbit of d-flats if and only if $gcd(k+1, d+1) \neq 1$. In the case that $d+1$ divides $k+1$ there is a short orbit $\mathcal{S}$ which partitions the points of Σ (i.e. constitutes a d-spread of Σ). There is precisely one such orbit, and the G-stabilizer of any $\Pi \in \mathcal{S}$ is $Stab_G(\Pi) = \langle \phi^{\frac{\theta(k)}{\theta(d)}} \rangle$.

Codes from projective lines, $\lambda_c = 1$

In $PG(k,q)$, k odd, let $\mathcal{S}$ be the line spread determined by G where say $Stab_G(\ell) = H$ for $\ell \in \mathcal{S}$ (so $|H| = q+1$).

It follows that any pointset meeting each line of the spread in at most one point will be of full H-orbit, and moreover, that members of the orbit will be mutually disjoint.

(Consequently, if $\Lambda S = \frac{\theta(k,q)}{q+1}$, then the corresponding $\Lambda \times S \times (q+1)$ incidence array will satisfies $\lambda_a = 0$).

Clearly, each line $\ell \notin \mathcal{S}$ meets each spread line in at most one point.

For each full H-orbit of lines, select a representative member and corresponding $\Lambda \times S \times (q+1)$ incidence array (3D-codeword). The collection of all such codewords comprises a $(\Lambda \times S \times (q+1), q+1, 0, \lambda_c)$-3DOOC C.

As two lines intersect in at most one point we have $\lambda_c = 1$.

Each $\ell \notin \mathcal{S}$ is of full H-orbit, that is $|Orb_H(\ell)| = q+1$, and the lines in $Orb_H(\ell)$ are disjoint. It follows that the number of full H-orbits of lines is

$$\begin{aligned}
\#\text{ orbits} &= \frac{\mathcal{L}(k) - |\mathcal{S}|}{q+1} \\
&= \frac{1}{q+1} \cdot \left[\frac{(q^{k+1}-1)(q^{k+1}-q)}{(q^2-1)(q^2-q)} - \frac{\theta(k)}{q+1} \right] \\
&= \frac{q \cdot \theta(k,q) \cdot \theta(k-2,q)}{(q+1)^2} \qquad (3)
\end{aligned}$$

Comparing this with our established bounds we see that C is in fact optimal.

Theorem

Let q be a prime power and let k be odd. For any factorisation $\Lambda ST = \theta(k,q)$ where T divides $q+1$ there exists a J-optimal $(\Lambda \times S \times T, q+1, 0, 1)$-OOC.

In an analogous way we may generalize whereby codewords correspond to lines that are not contained in any element of a d-spread of Σ.

Theorem

For $d \geq 1$, $m > 1$, and for any factorisation $\Lambda ST = \theta(m-1, q^{d+1}) \cdot \theta(d, q)$ where T divides $\theta(d, q)$, there exists a J-optimal $(\Lambda \times S \times T, q+1, 0, 1)$-OOC .

Affine Analogue

There exists an affine analogue of the Singer automorphism, denoted $\hat{G} = \langle \hat{\psi} \rangle$. The following follows from Theorem 8 of (Bose, 1942).

Theorem (Bose (1942))

A d-flat Π in $PG(k, q)$ is of full $\hat{G}$-orbit if and only if the origin $P_0 \notin \Pi$ and Π is not a subset of Π_∞.

Utilizing this theorem we are able to contruct more 3D-OOCs.

Theorem

For q a prime power, and for any factoristion $\Lambda ST = q^k - 1$ where T divides $q - 1$ there exists a J-optimal $(\Lambda \times S \times T, q, 0, 1)$-OOC.

New families of optimal ideal 3D OOC, $\lambda_c = 1$.

p a prime, q a prime power, $\theta(k,q) = \frac{q^{k+1}-1}{q-1}$

Conditions	Type	Ref.
$w = S \leq p$ for all p dividing ΛT	SPP	Kim, Yu, and Park (2000)
$w = S = \Lambda = T = p$	SPP	Li, Fan, and K. W. Shum (2012)
$w = S = 4 \leq \Lambda = q$, $T \geq 2$	SPP	Li, Fan, and K. W. Shum (2012)
$w = S = q+1$, $\Lambda = q > 3$, $T = p > q$	SPP	Li, Fan, and K. W. Shum (2012)
$w = S = 3$ $\Lambda \equiv T \mod 2$	SPP	Kenneth W. Shum (2015)
$w = 3$, $\Lambda T(S-1)$ even, $\Lambda T(S-1)S \equiv 0$ mod 3, and $S \equiv 0, 1$ mod 4 if $T \equiv 2$ mod 4 and Λ is odd.	AMOPP	Shum(2015)
$w = q+1, T \vert \theta(d,q)$, $\Lambda ST = \theta(m-1, q^{d+1})\theta(d,q)$, $d > 0, m > 1$		TLA (2017)
$w = q$, $\Lambda ST = q^k - 1, T \vert (q-1)$		TLA 2017

Conclusion and further work

- Provided constructions of infinite families of optimal ideal 3-dimensional OOC's.
- Constructions involve two or more parameters that may grow without bound.
- FUTURE:
  1. Consider orbits of further algebraic or geometric objects (curves, arcs, subgeometries etc.) .
  2. If desired, construct codes without the ideal constraints (much larger families).
  3. Possible generalize methods to (periodic) (multidimensional) Costas Arrays.
  4. Complete generalizations to D-dimensional codes.

UNB Saint John

Alderson, T. L. (2017). "3-Dimensional Optical Orthogonal Codes with Ideal Autocorrelation-Bounds and Optimal Constructions". In: *Information Theory, IEEE Transactions on* in press, pp. 1–7. ISSN: 0018-9448. DOI: 10.1109/TIT.2017.2717538.

Bose, R. C. (1942). "An affine analogue of Singer's theorem". In: *J. Indian Math. Soc. (N.S.)* 6, pp. 1–15.

Drudge, Keldon (2002). "On the orbits of Singer groups and their subgroups". In: *Electron. J. Combin.* 9.1, Research Paper 15, 10 pp. (electronic). ISSN: 1077-8926.

Kim, Sangin, Kyungsik Yu, and N. Park (2000). "A new family of space/wavelength/time spread three-dimensional optical code for OCDMA networks". In: *Journal of Lightwave Technology* 18.4, pp. 502–511. ISSN: 0733-8724. DOI: 10.1109/50.838124.

Li, X., P. Fan, and K. W. Shum (2012). "Construction of Space/Wavelength/Time Spread Optical Code with Large Family Size". In: *IEEE Communications Letters* 16.6, pp. 893–896. ISSN: 1089-7798. DOI: 10.1109/LCOMM.2012.040912.112296.

Rao, C. Radhakrishna (1969). "Cyclical generation of linear subspaces in finite geometries". In: *Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967)*. Chapel Hill, N.C.: Univ. North Carolina Press, pp. 515–535.

Shum, Kenneth W. (2015). "Optimal three-dimensional optical orthogonal codes of weight three". In: *Des. Codes Cryptogr.* 75.1, pp. 109–126. ISSN: 0925-1022. DOI: 10.1007/s10623-013-9894-4. URL: http://dx.doi.org/10.1007/s10623-013-9894-4.

Danke,

Lass uns essen!