Optical Orthogonal Codes and Arcs in PG(d, q)

T. L. Alderson [1]

Department of Mathematical Sciences, University of New Brunswick, Saint John, New Brunswick, E2L 4L5, Canada

Abstract

We present a new construction for (n, w, λ)-optical orthogonal codes (OOCs). The construction is pleasingly simple, where codewords correspond to arcs, specifically normal rational curves. Moreover, our construction yields for each $\lambda > 1$ an infinite family of OOCs which are asymptotically optimal (with respect to the Johnson bound).

Key words: Optical orthogonal code, Normal rational curve, arc, cyclically permutable code
Subject Class: 94B27, 51E20

1 Introduction

An $(n, w, \lambda_a, \lambda_c)$-optical orthogonal code (OOC) is a family of binary sequences (codewords) of length n, with constant hamming weight w satisfying the following two conditions:

- (auto-correlation property) for any codeword $c = (c_0, c_1, \ldots, c_{n-1})$ and for any integer $1 \leq t \leq n-1$, there holds $\sum_{i=0}^{n-1} c_i c_{i+t} \leq \lambda_a$
- (cross-correlation property) for any two distinct codewords c, c' and for any integer $0 \leq t \leq n-1$, there holds $\sum_{i=0}^{n-1} c_i c'_{i+t} \leq \lambda_c$

Email address: talderso@unbsj.ca (T. L. Alderson).

[1] The author acknowledges support from the NSERC of Canada.

where each subscript is reduced modulo n.

One of the first proposed applications of optical orthogonal codes was to optical code-division multiple access communication systems where binary sequences with strong correlation properties are required [1–3]. Subsequently, OOCs have found application for multimedia transmissions in fiber-optic LANs [4]. Optical orthogonal codes have also been called cyclically permutable constant weight codes in the construction of protocol sequences for multiuser collision channels without feedback [5].

An $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a = \lambda_c$ is denoted (n, w, λ)-OOC. The number of codewords is the *size* of the code. For fixed values of n, w, and λ, the largest size of an (n, w, λ)-OOC is denoted $\Phi(n, w, \lambda)$. In general, $\Phi(n, w, \lambda)$ is difficult to compute. In [2] the Johnson bound for constant weight codes is used to derive the following upper bound on $\Phi(n, w, \lambda)$.

$$\Phi(n, w, \lambda) \leq \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \right\rfloor \cdots \right\rfloor \right\rfloor \tag{1}$$

If an (n, w, λ)-OOC meets the bound (1) then the code is said to be *optimal*. If C is an $(n, w, \lambda_a, \lambda_c)$-OOC with $\lambda_a \neq \lambda_c$ then we obtain a bound on the size of C by taking $\lambda = max\{\lambda_a, \lambda_c\}$ in (1).

For $\lambda = 1, 2$ optimal OOCs are known to exist [2,6]. It is still unknown as to whether optimal (n, w, λ)-OOCs exist with $\lambda > 2$. There is much interest in constructing optimal and asymptotically optimal OOCs. The concept of asymptotic optimality was introduced in [7].

Definition 1 *Let F be an infinite family of OOCs with $\lambda_a = \lambda_c$. For any (n, w, λ)-OOC $C \in F$ containing at least one codeword, the number of codewords in C is denoted by $M(n, w, \lambda)$ and the corresponding Johnson bound is denoted by $J(n, w, \lambda)$. F is called asymptotically optimal if*

$$\lim_{n\to\infty} \frac{M(n, w, \lambda)}{J(n, w, \lambda)} = 1. \tag{2}$$

There are many constructions of infinite families of (asymptotically) optimal (n, w, λ)-OOCs where $\lambda = 1$ or 2. However, for $\lambda > 2$ constructive examples seem scarce. In [2], lines of $PG(d, q)$ are used to construct optimal OOCs with $\lambda = 1$ (see Section 2). In [8], the methods of [2] are applied to certain families of conics in $PG(2, q)$ in order to construct asymptotically optimal OOCs with $\lambda = 2$. Our method generalizes the conic construction in [8] to one using normal rational curves in $PG(d, q)$. The new infinite families of OOCs constructed here are asymptotically optimal. Moreover, the construction is

pleasingly simple and serves to exemplify the beautiful relationship between these codes and finite projective geometries.

2 OOCs from lines of $PG(k,q)$

In [2] Chung, Salehi, and Wei provide a method for constructing $(n,w,1)$-OOCs using lines of the projective geometry $PG(k,q)$. Briefly, let ω be a primitive element of $GF(q^{k+1})$. The points of $\Sigma = PG(k,q)$ can be represented as $\omega^0 = 1, \omega, \omega^2, \ldots, \omega^{n-1}$ where $n = \frac{q^{k+1}-1}{q-1}$. Hence, in a natural way a point set A of $PG(k,q)$ corresponds to a binary n-tuple (or codeword) $(a_0, a_1, \ldots, a_{n-1})$ where $a_i = 1$ if and only if $\omega^i \in A$.

Denote by ϕ the collineation of Σ defined by $\omega^i \mapsto \omega^{i+1}$, a Singer group acting on Σ. The map ϕ acts transitively on the points (and dually on the hyperplanes) of Σ. If A is a point set of Σ corresponding to the codeword $c = (a_0, a_1, \ldots, a_{n-1})$, then ϕ induces a cyclic shift on the entries of c.

For each line ℓ of Σ, consider the orbit $\mathcal{O}_\ell$ under ϕ. If $\mathcal{O}_\ell$ is a full orbit (has size n) then a representative line and corresponding codeword is chosen. Short orbits are discarded. Let $\mathcal{L}(k,q)$ represent the cardinality of this set of chosen lines. Two lines of Σ intersect in at most one point and each line contains $q+1$ points. It follows that the codewords satisfy both $\lambda_a \leq 1$ and $\lambda_c \leq 1$ and by counting the number of full orbits under ϕ the following is obtained.

Theorem 2 *For any prime power q and any positive integer k, there exists a $\left(\frac{q^{k+1}-1}{q-1}, q+1, 1\right)$-OOC consisting of $\mathcal{L}(k,q) = \left\lfloor \frac{q^k-1}{q^2-1} \right\rfloor$ codewords.*

3 OOCs from arcs of $PG(k,q)$

An *m-arc* in $PG(d,q)$ is a collection of $m > d$ points such that no $d+1$ are incident with a common hyperplane. It follows that if $\mathcal{K}$ is an m-arc in $PG(d,q)$ then no $d+1$ points of $\mathcal{K}$ lie on a hyperplane, no d lie on a $(d-2)$-flat,..., no 3 lie on a line. An arc is called *complete* if it is maximal with respect to inclusion.

In $PG(2,q)$, a (non-degenerate) conic is a $(q+1)$-arc and elementary counting shows that this arc is complete when q is odd. The $(q+2)$-arcs (hyperovals) exist in $PG(2,q)$ if q is even and they are necessarily complete. Conics are a special case of the so called normal rational curves. A *rational curve* $\mathcal{C}_n$ of order n in $PG(d,q)$ is a set of points

$$\{P(t) = P\left(g_0(t_0, t_1), \ldots, g_d(t_0, t_1)\right) \mid t_0, t_1 \in GF(q)\}$$

where each g_i is a binary form of degree n and the highest common factor of $g_0, g_1, \ldots, g_d$ is 1. The curve $\mathcal{C}_n$ may also be written

$$\{P(t) = P\left(f_0(t), \ldots, f_d(t)\right) \mid t \in GF(q) \cup \{\infty\}\} \tag{3}$$

where $f_i(t) = g_i(1, t)$.

Definition 3 *A normal rational curve (NRC) in $PG(d, q)$, $2 \leq d \leq q-2$ is a rational curve (of order d) projectively equivalent to the $(q+1)$-arc*

$$\{(1, t, \ldots, t^d) \mid t \in GF(q)\} \cup \{(0, \ldots, 0, 1)\}.$$

If $\mathcal{C}$ is an NRC in $PG(d, q)$ then the subgroup of $PGL(d+1, q)$ leaving $\mathcal{C}$ fixed is (isomorphic to) $PGL(2, q)$. It follows that if $\nu(d, q)$ denotes the number of distinct normal rational curves in $PG(d, q)$ then

$$\nu(d, q) = \frac{|PGL(d+1, q)|}{|PGL(2, q)|} = \frac{(q^{d+1}-1)(q^{d+1}-q)\cdots(q^{d+1}-q^d)}{(q^2-1)(q^2-q)} \tag{4}$$

The following is a well known property of NRCs (see [9]).

Theorem 4 *A $(d+3)$-arc in $PG(d, q)$ is contained in a unique normal rational curve.*

Definition 5 *Let $\pi = PG(d, q)$. A d-family $\mathcal{F}$ of m-arcs in π is a collection of m-arcs mutually meeting in at most d points.*

Theorem 6 *In $\pi = PG(d, q)$ let $\mathcal{F}$ be a d-family of m-arcs, $m \leq q+1$. Then there exists a $\left(\frac{q^{d+2}-1}{q-1}, m, d\right)$-OOC C consisting of $|\mathcal{F}| + \mathcal{L}(d+1, q)$ codewords.*

PROOF. Consider $\pi = PG(d, q)$ as embedded in $\Sigma = PG(d+1, q)$ and let ω be a primitive element of $GF(q^{d+2})$. Let $\mathcal{F}$ be a d-family of m-arcs in π. Identify each arc in $\mathcal{F}$ with the corresponding codeword of length $\frac{q^{d+2}-1}{q-1}$ and weight m. As before, let $\phi : \omega^i \mapsto \omega^{i+1}$ be a Singer group acting on Σ. Let $\mathcal{K}$ be an arc in $\mathcal{F}$. Then we have

$$\lambda_a = \max\left|\{\mathcal{K} \cap \phi^i(\mathcal{K}) | 1 \leq i \leq n-1\}\right|.$$

As $\mathcal{K} \cap \phi^i(\mathcal{K}) \subset \pi \cap \phi^i(\pi)$ (a hyperplane of π), and an arc in π intersects a hyperplane of π in at most d points, we get $\lambda_a \leq d$. Similarly, for two distinct arcs $\mathcal{K}$ and $\mathcal{K}'$ in $\mathcal{F}$

$$\lambda_c = \max|\{\mathcal{K} \cap \phi^i(\mathcal{K}')|\mathcal{K} \neq \mathcal{K}', 0 \leq i \leq n-1\}|.$$

If $i \neq 0$ then (as above) this number is at most d. If $i = 0$ then $\mathcal{K}$ and $\phi^i(\mathcal{K}')$ are in π and can therefore share as many as d points so $\lambda_c = d$.
If $m = q + 1$ then the $\mathcal{L}(d+1, q)$ codewords obtained from lines of Σ in Theorem 2 may be added to the code (Two lines intersect in at most one point and a line intersects an arc in at most two points). If $m < q + 1$ we may arbitrarily remove $q + 1 - m$ points from each of the $\mathcal{L}(d+1, q)$ lines and then add the corresponding codewords to the code. Thus we construct a $\left(\frac{q^{d+2}-1}{q-1}, m, d\right)$-OOC consisting of $|\mathcal{F}| + \mathcal{L}(d+1, q)$ codewords.

Theorem 7 *In $\pi = PG(d, q)$, $d \geq 2$, there exists a d-family $\mathcal{F}$ of $(q-1)$-arcs where $|\mathcal{F}| = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d)$.*

PROOF. In $\pi = PG(d, q)$ fix two points P and Q. Denote by X_d the number of NRCs containing P and Q. By counting ordered triples $(\mathcal{N}, P_1, P_2)$ where $\mathcal{N}$ is a NRC in π and P_1 and P_2 are distinct points of $\mathcal{N}$ we get

$$\frac{|PGL(d+1, q)|}{|PGL(2, q)|}(q+1)(q) = \left(\frac{q^{d+1}-1}{q-1}\right)\left(\frac{q^{d+1}-1}{q-1} - 1\right) X_d,$$

which gives

$$X_d = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d).$$

Hence, removing P and Q from each of the X_d NRCs through P and Q we arrive at a d-family $\mathcal{F}$ of $(q-1)$-arcs.

In [8] (Lemma 5) a large 2-family of conics is constructed. We generalize this result using analogous arguments in higher dimensions to get a slight improvement to Theorem 7.

Theorem 8 *In $\pi = PG(d, q)$, $d \geq 2$, there exists a d-family $\mathcal{F}$ of $(q+1)$-arcs where $|\mathcal{F}| = (q^{d+1} - q^2)(q^{d+1} - q^3) \cdots (q^{d+1} - q^d)$.*

PROOF. Consider $\pi = PG(d, q)$ as a (Baer) subspace of $\Pi = PG(d, q^2)$. Let $\Pi^* = \Pi \setminus \pi$. Choose a point $P = (\alpha_0, \alpha_1, \ldots, \alpha_d) \in \Pi^*$.

With reference to Equation (3), consider the collection of NRCs in Π having polynomial coefficients in $GF(q)$. Denote by X_P the number of such NRCs containing P. Note that any such NRC intersects π in an NRC of π. To determine X_P, we count ordered pairs $(\mathcal{N}, Q)$ where $\mathcal{N}$ is an NRC of Π over $GF(q)$ and Q is a point of $\mathcal{N}$ in Π^*. This gives us the following.

$$\frac{|PGL(d+1,q)|}{|PGL(2,q)|}[(q^2+1)-(q+1)] = \left[\left(\frac{(q^2)^{d+1}-1}{q^2-1}\right) - \left(\frac{(q)^{d+1}-1}{q-1}\right)\right] X_P.$$

After some simplification we arrive at

$$X_P = (q^{d+1}-q^2)(q^{d+1}-q^3)\cdots(q^{d+1}-q^d).$$

Let $\mathcal{C}$ be an NRC in Π over $GF(q)$ containing P. Then the point $P^q = (\alpha_0^q, \alpha_1^q, \ldots, \alpha_d^q)$ is also contained in $\mathcal{C}$ (and is also in Π^*). As such, any two of the NRCs counted above have at most d common points in π. Hence, by restricting to the intersection of these NRCs with π we have a d-family of $(q+1)$-arcs in π having size X_P.

This following theorem is an immediate consequence of Theorems 8 and 6.

Theorem 9 *For $\lambda > 1$ and $q > \lambda$ a prime power, there exists a $(\frac{q^{\lambda+2}-1}{q-1}, q+1, \lambda)$-OOC consisting of $(q^{\lambda+1}-q^2)(q^{\lambda+1}-q^3)\cdots(q^{\lambda+1}-q^\lambda) + \mathcal{L}(\lambda+1, q)$ codewords.*

4 Optimality

Fix $\lambda > 1$ and consider the infinite family of (n, w, λ)-OOCs constructed as for Theorem 9. The Johnson bound for these codes is

$$J(n,w,\lambda) = \left\lfloor \frac{1}{q+1} \left\lfloor \frac{q^{\lambda+1}+q^\lambda+\cdots+q}{q} \left\lfloor \frac{q^{\lambda+1}+q^\lambda+\cdots+q-1}{q-1} \left\lfloor \cdots \left\lfloor \frac{q^{\lambda+1}+q^\lambda+\cdots+q-\lambda}{q+1-\lambda} \right\rfloor \right\rfloor \right\rfloor \right\rfloor .$$

With reference to Definition 1 we see that the codes constructed as in Theorem 9 satisfy the following limit.

$$\lim_{n\to\infty} \frac{M(n,w,\lambda)}{J(n,w,\lambda)} = \lim_{n\to\infty} \frac{q^{\lambda^2-1}}{q^{\lambda^2-1}} = 1.$$

Hence, we get the following Theorem.

Theorem 10 *For each $\lambda > 1$, the corresponding infinite family of OOCs in Theorem 9 is asymptotically optimal.*

Acknowledgements

The author thanks Professor Tim Penttila for his enlightening discussions and in particular for pointing out the elegant formula (4).

References

[1] Bird, C. M. and Keedwell, A. D., Design and applications of optical orthogonal codes—a survey, Bull. Inst. Combin. Appl., 11, 1994, 1183-1287.

[2] Chung, Fan R.K. and Salehi, Jawad A. and Wei, Victor K., Optical orthogonal codes: design, analysis, and applications, IEEE Trans. Inform. Theory, 35, 1989, 595-604.

[3] Healy, Timothy J., Coding and decoding for code division multiple user communication systems, IEEE Trans. Comm., 33, 1985, no. 4, 310-316.

[4] Maric S. V, Moreno O., and Corrada,C., Multimedia transmission in fiber-optic LANs using optical CDMA, J. Lightwave Technol., 14, 1996, 2149-2153.

[5] Nguyen Q. A and Györfi, László and Massey, James L., Constructions of binary constant-weight cyclic codes and cyclically permutable codes, IEEE Trans. Inform. Theory, 38, 1992, no. 3, 940-949.

[6] Chung, Habong and Kumar, P. Vijay, Optical orthogonal codes—new bounds and an optimal construction, IEEE Trans. Inform. Theory, 36, 1990, no. 4, 866-873.

[7] Moreno, Oscar and Zhang, Zhen and Kumar, P. Vijay and Zinoviev, Victor A., New constructions of optimal cyclically permutable constant weight codes, IEEE Trans. Inform. Theory, 41, 1995, no. 2, 448-455.

[8] Miyamoto, Nobuko and Mizuno, Hirobumi and Shinohara, Satoshi, Optical orthogonal codes obtained from conics on finite projective planes, Finite Fields Appl., 10, 2004, no. 3, 405-411.

[9] Thas, Joseph A., Projective geometry over a finite field, Handbook of incidence geometry, North-Holland, Amsterdam, 1995, 295–347.