ISSN 2590-9770
The Art of Discrete and Applied Mathematics 1 (2018) #P2.02
https://doi.org/10.26493/2590-9770.1236.ce4
(Also available at http://adam-journal.eu)

On silver and golden optical orthogonal codes*

Marco Buratti

Dipartimento di Matematica e Informatica, Università di Perugia, via Vanvitelli 1

Received 1 January 2018, accepted 24 June 2018, published online 3 August 2018

Abstract

It is several years that no theoretical construction for optimal $(v, k, 1)$ optical orthogonal codes (OOCs) with new parameters has been discovered. In particular, the literature almost completely lacks optimal $(v, k, 1)$-OOCs with $k > 3$ which are not regular. In this paper we will show how some elementary difference multisets allow to obtain three new classes of optimal but not regular $(3p, 4, 1)$-, $(5p, 5, 1)$-, and $(2p, 4, 1)$-OOCs which are describable in terms of Pell and Fibonacci numbers. The OOCs of the first two classes (resp. third class) will be called *silver* (resp. *golden*) since they exist provided that the square of a *silver element* (resp. *golden element*) of $\mathbb{Z}_p$ is a primitive square of $\mathbb{Z}_p$.

Keywords: Silver and golden ratio, Pell and Fibonacci numbers, difference packing, optimal optical orthogonal code, strong difference family, difference multiset.

Math. Subj. Class.: 05B10, 94B25

1 Introduction

The real numbers $1 + \sqrt{2}$ (the *silver ratio*), $\frac{1+\sqrt{5}}{2}$ (the *golden ratio*) and their marvelous properties are very well known. Disregarding their geometrical meaning (see, e.g., [17]), they can be defined in the same algebraic way in any finite field $\mathbb{F}_q$ of an appropriate order q. By the Law of Quadratic Reciprocity (see, e.g., [20]), it is well known that 2 is a non-zero square in $\mathbb{F}_q$ if and only if $q \equiv 1$ or $7 \pmod 8$ and that 5 is a non-zero square in $\mathbb{F}_q$ if and only if $q \equiv 1$ or $4 \pmod 5$. Thus, for a prime $p \equiv 1$ or $7 \pmod 8$, we naturally define the *silver elements of* $\mathbb{Z}_p$ as the two elements $1 + x$ and $1 - x$ of $\mathbb{Z}_p$ where x and $-x$ are the square roots of 2 modulo p. Also, for a prime $p \equiv 1$ or $4 \pmod 5$, we naturally define the *golden elements of* $\mathbb{Z}_p$ as the two elements $2^{-1}(1 + x)$ and $2^{-1}(1 - x)$ of $\mathbb{Z}_p$ where x and $-x$ are the square roots of 5 modulo p.

We recall that the *Pell sequence* is the integer sequence $\{P_n\}$ defined by $P_0 = 0$, $P_1 = 1$ and by the recursive formula $P_n = 2P_{n-1} + P_{n-2}$ for $n \geq 2$, and that the

*This work has been performed under the auspices of the G.N.S.A.G.A. of the C.N.R. (National Research Council) of Italy.

E-mail address: buratti@dmi.unipg.it (Marco Buratti)

Fibonacci sequence is the integer sequence $\{F_n\}$ defined by $F_0 = 0$, $F_1 = 1$ and by the recursive formula $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

Two good textbooks on *Pell* and *Fibonacci numbers* are [19] and [18], respectively.

As in the real field, if θ is a silver element of $\mathbb{F}_q$ then we have

$$\theta^n = P_n\theta + P_{n-1} \quad \forall n \geq 1 \tag{1.1}$$

Also, if ϕ is a golden element of $\mathbb{F}_q$ then we have

$$\phi^n = F_n\phi + F_{n-1} \quad \forall n \geq 1 \tag{1.2}$$

An *optical orthogonal code* of *length* v, *weight* k, *auto-correlation* λ_a and *cross-correlation* λ_c – briefly, a $(v, k, \lambda_a, \lambda_c)$-OOC – can be seen as a set of k-subsets (*codeword-sets*) of $\mathbb{Z}_v$ such that

(i) any two distinct translates of a codeword-set share at most λ_a elements (*auto-correlation property*);

(ii) any two translates of two distinct codeword-sets share at most λ_c elements (*cross-correlation property*).

This topic, introduced by Chung, Salehi and Wei [12], has been well studied for a long time in view of its many applications (see, e.g., [13]).

In particular, a $(v, k, 1, 1)$-OOC – briefly, a $(v, k, 1)$-OOC – can be viewed as a set of k-subsets of $\mathbb{Z}_v$ (*codeword-sets*) such that no element of $\mathbb{Z}_v \setminus \{0\}$ can be represented as a difference of two elements of a codeword-set in more than one way. Such an OOC is said to be *optimal* when its *size* (that is the number of its codeword-sets) reaches the upper *Johnson bound* $\lfloor \frac{v-1}{k(k-1)} \rfloor$.

There is a huge literature on optical orthogonal codes but, as far as this author is aware, in the last seven years no theoretical construction for a class of optimal $(v, k, 1)$-OOCs with new parameters has been discovered. In this paper we find three classes of optimal OOCs with new parameters: an optimal $(3p, 4, 1)$-OOC and an optimal $(5p, 5, 1)$-OOC for each prime $p \equiv 7 \pmod 8$ such that the silver elements of $\mathbb{Z}_p$ are generators of $\mathbb{Z}_p^*/\{1, -1\}$ (both these codes will be called silver); an optimal $(2p, 4, 1)$-OOC for each prime $p \equiv 11$ or $29 \pmod{30}$ such that the golden elements of $\mathbb{Z}_p$ are generators of $\mathbb{Z}_p^*/\{1, -1\}$ (this code will be called golden).

The strategy to get our silver/golden OOCs is to use some elementary *difference multisets* (which are *strong difference families* with only one block) but, in the end, we will show that all these codes can be presented in terms of *Pell/Fibonacci numbers*.

2 Difference packings via strong difference families

Given a k-multisubset, in particular a k-subset, $B = \{b_1, \ldots, b_k\}$ of an additive group G, we call list of differences from B the multiset ΔB of all possible differences $b_i - b_j$ with (i, j) an ordered pair of distinct elements of $\{1, \ldots, k\}$. One calls $(G, k, 1)$ *difference packing* any set $\mathcal{D}$ of k-subsets of G (*blocks*) with the property that its list of differences, namely the multiset sum

$$\Delta\mathcal{D} := \biguplus_{B \in \mathcal{D}} \Delta B,$$

does not have repeated elements. It is evident that the size of $\mathcal{D}$ cannot exceed $\lfloor \frac{|G|-1}{k(k-1)} \rfloor$. For this reason, one says that $\mathcal{D}$ is *optimal* when its size reaches this value. The *difference leave* of a $(G,k,1)$ difference packing $\mathcal{D}$ is defined to be the set of all elements of G not appearing in $\Delta\mathcal{D}$. Thus $\mathcal{D}$ is optimal provided that its difference leave has size less or equal to $k(k-1)$. The difference packing is a *relative difference family* [5] if its difference leave is a subgroup H of G. In this case someone also speaks of a r-*regular* difference packing if H has order r (see, e.g., [24]). Note that a $(\mathbb{Z}_v,k,1)$ difference packing is nothing but a $(v,k,1)$-OOC.

The problem of factoring a group into subsets and its variants [23] could play a crucial role in the construction of difference packings. Also, the construction of a $|G|$-regular $(G\times\mathbb{F}_q,k,1)$ difference packing can be facilitated by a suitable *strong difference family* in G, a concept formally introduced in [6] but implicitly used for a long time. A t-(G,k,μ) *strong difference family* is a t-multiset $\mathcal{S}$ of k-multisubsets (blocks) of a group G such that $\Delta\mathcal{S}$ covers all elements of G exactly μ times. The parameter μ is called the *index* of the strong difference family and a trivial counting shows that it is necessarily equal to $\frac{k(k-1)t}{|G|}$. Of course it is possible to consider, more generally, strong difference families whose blocks have variable sizes [7].

In order to explain why strong difference families might be good to construct relative difference families and more generally OOCs, we have to introduce some notation and terminology.

Denote by $\mathbb{F}_q^*$ the multiplicative group of the field $\mathbb{F}_q$. Given a subset B of a direct product $G\times\mathbb{F}_q$ and given $c\in\mathbb{F}_q^*$, denote by $(1,c)\cdot B$ the subset of $G\times\mathbb{F}_q$ obtained from B by multiplying the second coordinates of all its elements by c and leaving invariant their first coordinates. If $\mathcal{B}$ is a set of subsets of $G\times\mathbb{F}_q$ and $g\in G$, we denote by $\Delta_g\mathcal{B}$ the list of the second coordinates of all elements of $\Delta\mathcal{B}$ whose first coordinate is g so that one can write

$$\Delta\mathcal{B}=\bigcup_{g\in G}\{g\}\times\Delta_g\mathcal{B}.$$

Let us say that two subsets C and Δ of $\mathbb{F}_q^*$ are *companions* if the list $C\cdot\Delta:=\{c\delta \mid c\in C;\delta\in\Delta\}$ does not have repeated elements. In this case it is evident that the size of C cannot exceed $\lfloor\frac{q-1}{|\Delta|}\rfloor$. Thus we say that C is an *optimal* companion of Δ when its size reaches this value. In particular, we say that C is a *perfect* or *near-perfect* companion of Δ when its size is exactly equal to $\frac{q-1}{|\Delta|}$ or $\frac{q-2}{|\Delta|}$, respectively. In these last two cases we have $C\cdot\Delta=\mathbb{F}_q^*$ or $C\cdot\Delta=\mathbb{F}_q^*\setminus\{x\}$ for some $x\in\mathbb{F}_q^*$ and one says that $C\cdot\Delta$ is a *factorization* of $\mathbb{F}_q^*$ in the former case and that $\frac{1}{x}C\cdot\Delta$ is a *near factorization* of $\mathbb{F}_q^*$ in the latter (see [23]).

The next proposition is very elementary.

Proposition 2.1. *Let $\mathcal{B}=\{B_1,\dots,B_t\}$ be a set of k-subsets of $G\times\mathbb{F}_q$ such that all $\Delta_g\mathcal{B}$ are sets admitting a common companion C. Then $\mathcal{D}:=\{(1,c)\cdot B \mid c\in C, B\in\mathcal{B}\}$ is a $(G\times\mathbb{F}_q,k,1)$ difference packing.*

The proof is straightforward; indeed, by assumption, $C\cdot\Delta_g\mathcal{B}$ does not have repeated elements, hence $\Delta\mathcal{D}=\bigcup_{g\in G}\{g\}\times(C\cdot\Delta_g\mathcal{B})$ is also without repeated elements.

Now we show that the above proposition cannot give optimal optical orthogonal codes for arbitrarily high values of q unless the projection of $\mathcal{B}$ on G is a strong difference family.

Proposition 2.2. *Let $\mathcal{D}$ be a difference packing as in Proposition 2.1 and set $\mu=\frac{k(k-1)t}{|G|}$. Then, for $q>k(k-1)\mu$, $\mathcal{D}$ is optimal if and only if the following conditions hold:*

(i) The projection of $\mathcal{B}$ on G is a t-(G,k,μ) strong difference family;

(ii) C is an optimal companion of $\Delta_g\mathcal{B}$ for every $g \in G$;

(iii) the remainder of the Euclidean division of q by μ does not reach $\frac{\mu}{t}$.

Proof. ($\Longrightarrow$): The size of $\mathcal{D}$ is $|C| \cdot t$, therefore we have $|C| \cdot t = \lfloor \frac{|G|q-1}{k(k-1)} \rfloor$ because $\mathcal{D}$ is optimal. This gives $|C| \geq k(k-1)$ in view of the hypothesis $q > k(k-1)\mu$.

For each $g \in G$, let $L_g(\mathcal{B})$ be the complement of $C \cdot \Delta_g\mathcal{B}$ in $\mathbb{F}_q$. We have $|L_g(\mathcal{B})| = q - |C| \cdot |\Delta_g\mathcal{B}|$ for each $g \in G$. This implies that $|L_g(\mathcal{B})| = |L_h(\mathcal{B})| + |C| \cdot (|\Delta_h\mathcal{B}| - |\Delta_g\mathcal{B}|)$ for any pair of elements g and h of G. Thus, if $|\Delta_g\mathcal{B}| < |\Delta_h\mathcal{B}|$ we would have $|L_g(\mathcal{B})| > |C|$ and then $L_g(\mathcal{B})$ would have size greater than $k(k-1)$ in view of the previous paragraph. This is clearly absurd since $\{g\} \times L_g(\mathcal{B})$ is contained in the difference leave of $\mathcal{D}$ whose size is at most $k(k-1)$.

We conclude that $|\Delta_g\mathcal{B}|$ is a constant, i.e., the projection of $\mathcal{B}$ on G is a strong difference family with t blocks of size k. This implies that its index is $\frac{k(k-1)t}{|G|}$ which is equal to μ. Thus $|\Delta_g\mathcal{B}| = \mu$ for every $g \in G$.

Now assume that C is not optimal. In this case the size of $L_g(\mathcal{B})$ would be a constant at least equal to μ, hence the difference leave of $\mathcal{D}$, which is clearly given by $\bigcup_{g \in G} \{g\} \times L_g(\mathcal{B})$, would have size greater than $\mu|G| = tk(k-1)$, therefore greater than $k(k-1)$ contradicting the optimality of $\mathcal{D}$.

If r is the remainder of the Euclidean division of q by μ, then the difference leave of $\mathcal{D}$ has size $r \cdot |G|$. Thus, since $\mathcal{D}$ is optimal, we must have $r \cdot |G| \leq k(k-1)$ which means $r < \frac{\mu}{t}$.

($\Longleftarrow$): Straightforward. □

Note that condition (iii) is certainly satisfied when $t = 1$, namely when $\mathcal{B}$ is a singleton $\{B\}$. In this case one says that the projection of B on G, say $\pi(B)$, is a (G,k,μ) *difference multiset* (also called a *difference cover* in [3]) rather than to say that $\{\pi(B)\}$ is a 1-(G,k,μ) strong difference family.

The above proposition suggests the following strategy for getting families of optimal difference packings. Start with a t-(G,k,μ) strong difference family $\mathcal{S}$ which will be used as "skeleton" of the desired optimal difference packing. Then take a prime power $q = \mu n + r$ with $1 \leq r \leq \frac{\mu}{t}$ and try to "lift" $\mathcal{S}$ to a suitable t-set $\mathcal{B}$ of k-subsets of $G \times \mathbb{F}_q$ in such a way that all $\Delta_g\mathcal{B}$ admit a common optimal companion C. For $r = 1$ this strategy has been used (sometimes implicitly) in many papers to construct relative difference families and, in particular, regular OOCs. The elder constructions are surveyed in [2]. More recent constructions can be found in [8, 9, 11, 14, 15, 21, 22, 25]. Here one often tries to have each $\Delta_g\mathcal{B}$ a complete system of representatives for the cosets of the subgroup of $\mathbb{F}_q^*$ of index μ, namely the group C^μ of non-zero μ-th powers of $\mathbb{F}_q$. Indeed in this case a common companion of each $\Delta_g\mathcal{B}$ is clearly given by C^μ itself.

On the other hand, as far as this author is aware, the above strategy has been never applied with $r > 1$ probably because the existence of a common optimal but not perfect companion of all the set $\Delta_g\mathcal{B}$ seems to be almost a miracle. Indeed, the probability that even a single set $\Delta \subset \mathbb{F}_q^*$ admits an optimal companion C diminishes dramatically if $|\Delta|$ is not a divisor of $q-1$. Consider, for instance, that Theorem 2.8 and Theorem 2.9 in [4] imply that for $q \equiv 1 \pmod 3$ the number of 3-subsets of $\mathbb{F}_q^*$ admitting a perfect companion is at least equal to $q(\frac{q-1}{3})^3$, while for $q \equiv 2 \pmod 3$ the number of 3-subsets of $\mathbb{F}_q^*$ admitting a near-perfect companion is less or equal to $q \cdot \Phi(q-1)$ with Φ the *Euler totient function*.

This probably explains why, at the moment, we have only a few known classes of optimal but not regular $(v,k,1)$-OOCs with $k>3$ (see [1, 4, 10]).

Anyway in this paper we manage to find three new classes of optimal but not regular OOCs adopting the strategy described above with $\mathcal{S}$ equal to one the following very elementary strong difference families:

(a) the $(\mathbb{Z}_3,4,4)$ difference multiset $\{0,0,1,1\}$ for getting an optimal $(3p,4,1)$-OOC with $p=8n+7$ a prime whose silver elements are generators of $\mathbb{Z}_p^*/\{1,-1\}$;

(b) the $(\mathbb{Z}_5,5,4)$ difference multiset $\{0,1,1,4,4\}$ for getting an optimal $(5p,5,1)$-OOC with p a prime as above;

(c) the $(\mathbb{Z}_2,4,6)$ difference multiset $\{0,1,1,1\}$ for getting an optimal $(2p,4,1)$-OOC with $p=30n+11$ or $p=30n+29$ a prime whose golden elements are generators of $\mathbb{Z}_p^*/\{1,-1\}$.

3 On the silver $(3p,4,1)$ and $(5p,5,1)$ optical orthogonal codes

Note that the silver elements of $\mathbb{Z}_p$ are precisely the solutions of the congruence $x^2-2x-1\equiv 0 \pmod p$, i.e., the elements θ of $\mathbb{Z}_p$ such that $\theta+1=\theta(\theta-1)$. This property is crucial for getting the following construction.

Theorem 3.1. *Let $p=8n+7$ be a prime and let θ be a silver element of $\mathbb{Z}_p$. If θ is a generator of $\mathbb{Z}_p^*/\{1,-1\}$, then there exists an optimal $(3p,4,1)$-OOC and an optimal $(5p,5,1)$-OOC.*

Proof. By the Chinese Remainder Theorem, $\mathbb{Z}_{3p}$ and $\mathbb{Z}_{5p}$ are isomorphic to $\mathbb{Z}_3\times\mathbb{Z}_p$ and $\mathbb{Z}_5\times\mathbb{Z}_p$, respectively. So it is enough to show that, under the given assumption, there exists an optimal $(\mathbb{Z}_3\times\mathbb{Z}_p,4,1)$ difference packing and an optimal $(\mathbb{Z}_5\times\mathbb{Z}_p,5,1)$ difference packing.

The assumption on θ implies that $\{\theta^i \mid 0\le i\le 4n+2\}$ is a complete system of representatives for the cosets of $\{1,-1\}$ in $\mathbb{Z}_p^*$ so that we have

$$\mathbb{Z}_p^*=\{1,-1\}\cdot\{1,\theta,\theta^2,\dots,\theta^{4n+1},\theta^{4n+2}\}$$

and then $\{\theta^{2i}\mid 0\le i\le 2n\}\cdot\{\pm\theta,\pm\theta^2\}=\mathbb{Z}_p^*\setminus\{1,-1\}$. Thus we can claim that

$$C:=\{\theta^{2i}\mid 0\le i\le 2n\} \text{ is an optimal companion of } \{\pm\theta,\pm\theta^2\}. \tag{3.1}$$

Let us lift the $(\mathbb{Z}_3,4,4)$ difference multiset $\{0,0,1,1\}$ to the following 4-subset of $\mathbb{Z}_3\times\mathbb{Z}_p$

$$B=\{(0,\theta),(0,-\theta),(1,\theta^2),(1,-\theta^2)\}.$$

The *difference table* of B (see Table 1) shows that we can write:

$$\Delta_0B=\{\pm2\theta,\pm2\theta^2\};\quad \Delta_1B=\Delta_2B=\{\pm\theta(\theta-1),\pm\theta(\theta+1)\}. \tag{3.2}$$

Then, recalling that $\theta+1=\theta(\theta-1)$, we have:

$$\Delta_0B=2\{\pm\theta,\pm\theta^2\};\quad \Delta_1B=\Delta_2B=(\theta-1)\{\pm\theta,\pm\theta^2\}.$$

We conclude, by (3.1), that C is an optimal companion of Δ_gB for every $g\in\mathbb{Z}_3$ and then $\mathcal{D}=\{(1,c)\cdot B\mid c\in C\}$ is the desired optimal $(\mathbb{Z}_3\times\mathbb{Z}_p,4,1)$ difference packing by Proposition 2.2.

Table 1: The difference table of $B = \{(0,\theta),(0,-\theta),(1,\theta^2),(1,-\theta^2)\}$.

	$(0,\theta)$	$(0,-\theta)$	$(1,\theta^2)$	$(1,-\theta^2)$
$(0,\theta)$	•	$(0,2\theta)$	$(2,\theta-\theta^2)$	$(2,\theta+\theta^2)$
$(0,-\theta)$	$(0,-2\theta)$	•	$(2,-\theta-\theta^2)$	$(2,-\theta+\theta^2)$
$(1,\theta^2)$	$(1,\theta^2-\theta)$	$(1,\theta^2+\theta)$	•	$(0,2\theta^2)$
$(1,-\theta^2)$	$(1,-\theta^2-\theta)$	$(1,-\theta^2+\theta)$	$(0,-2\theta^2)$	•

Now, let us lift the $(\mathbb{Z}_5,5,4)$ difference multiset $\{0,1,1,4,4\}$ to the following 5-subset of $\mathbb{Z}_5 \oplus \mathbb{Z}_p$

$$B = \{(0,0),(1,\theta),(1,-\theta),(4,\theta^2),(4,-\theta^2)\}.$$

Table 2 is its difference table.

Table 2: The difference table of $B = \{(0,0),(1,\theta),(1,-\theta),(4,\theta^2),(4,-\theta^2)\}$.

	$(0,0)$	$(1,\theta)$	$(1,-\theta)$	$(4,\theta^2)$	$(4,-\theta^2)$
$(0,0)$	•	$(4,-\theta)$	$(4,\theta)$	$(1,-\theta^2)$	$(1,\theta^2)$
$(1,\theta)$	$(1,\theta)$	•	$(0,2\theta)$	$(2,\theta-\theta^2)$	$(2,\theta+\theta^2)$
$(1,-\theta)$	$(1,-\theta)$	$(0,-2\theta)$	•	$(2,-\theta-\theta^2)$	$(2,-\theta+\theta^2)$
$(4,\theta^2)$	$(4,\theta^2)$	$(3,\theta^2-\theta)$	$(3,\theta^2+\theta)$	•	$(0,2\theta^2)$
$(4,-\theta^2)$	$(4,-\theta^2)$	$(3,-\theta^2-\theta)$	$(3,-\theta^2+\theta)$	$(0,-2\theta^2)$	•

Recalling again that $\theta+1 = \theta(\theta-1)$, we can write

$$\begin{aligned}\Delta_0 B &= 2\{\pm\theta,\pm\theta^2\},\\ \Delta_1 B &= \Delta_4 B = \{\pm\theta,\pm\theta^2\},\\ \Delta_2 B &= \Delta_3 B = (\theta-1)\{\pm\theta,\pm\theta^2\}\end{aligned}$$

so that, by (3.1), C is an optimal companion of $\Delta_g B$ for each $g \in \mathbb{Z}_5$. We conclude that $\mathcal{D} = \{(1,c)\cdot B \mid c \in C\}$ is the desired optimal $(\mathbb{Z}_5 \times \mathbb{Z}_p, 5, 1)$ difference packing by Proposition 2.2. The assertion follows. □

The optimal OOCs arising from the above result will be called *silver*. We remark that the assumption on θ is equivalent to ask that θ^2, that is $2\theta+1$, is a primitive square of $\mathbb{Z}_p$ and that this assumption does not depend on the chosen silver element; indeed the product of the two silver elements is -1, hence they have the same orders in $\mathbb{Z}_p^*/\{1,-1\}$. We also note that the difference leaves of the constructed pakings are

$$\{0\}\times\{0,2,-2\} \cup \{1,2\}\times\{0,\theta-1,1-\theta\}$$

for the $(\mathbb{Z}_3 \times \mathbb{Z}_p, 4, 1)$ difference packing and

$$\{0\}\times\{0,2,-2\} \cup \{1,4\}\times\{0,1,-1\} \cup \{2,3\}\times\{0,\theta-1,1-\theta\}$$

for the $(\mathbb{Z}_5 \times \mathbb{Z}_p, 5, 1)$ difference packing.

Among the 2399 primes p congruent to 7 modulo 8 and not exceeding 100 000 we have checked that θ is not a generator of $\mathbb{Z}_p^*/\{1,-1\}$ in "only" 599 cases. Thus, roughly speaking, it seems that the two constructions succeed three times out of four.

Remark 3.2. Using formula (1.1), the optimal difference packings constructed in Theorem 3.1 can be more explicitly written in terms of Pell numbers. They are of the form $\mathcal{D} = \{B_i \mid 0 \le i \le 2n\}$ with

$$B_i = \{(0, P_{2i+1}\theta + P_{2i}),\ (0, -P_{2i+1}\theta - P_{2i}),\ (1, P_{2i+2}\theta + P_{2i+1}),\ (1, -P_{2i+2}\theta - P_{2i+1})\}$$

when $\mathcal{D}$ is a $(\mathbb{Z}_3 \times \mathbb{Z}_p, 4, 1)$ difference packing and with

$$B_i = \{(0,0),\ (1, P_{2i+1}\theta + P_{2i}),\ (1, -P_{2i+1}\theta - P_{2i}),\ (4, P_{2i+2}\theta + P_{2i+1}),\ (4, -P_{2i+2}\theta - P_{2i+1})\}$$

when $\mathcal{D}$ is a $(\mathbb{Z}_5 \times \mathbb{Z}_p, 5, 1)$ difference packing.

By way of illustration we explicitly construct a silver $(141, 4, 1)$-OOC.

We have $141 = 3p$ with $p = 47 = 8n + 7$ prime, $n = 5$. A silver element of $\mathbb{Z}_p$ is $\theta = 8$; indeed we have $8 + 1 \equiv 8^2 - 8 \pmod{47}$. Here the group $\mathbb{Z}_p^*/\{1,-1\}$ has prime order 23, hence θ is certainly a generator of it and Theorem 3.1 can be applied. The reduction modulo p of the Pell sequence up to its 22-nd term is

$$(0, 1, 2, 5, 12, 29, 23, 28, 32, 45, 28, 7, 42, 44, 36, 22, 33, 41, 21, 36, 46, 34, 20).$$

Thus, applying Remark 3.2, the blocks of a $(\mathbb{Z}_3 \times \mathbb{Z}_{47}, 4, 1)$ difference packing are the following:

$$\{(0,\theta), (0,-\theta), (1, 2\theta+1), (1, -2\theta-1)\}$$
$$\{(0, 5\theta+2), (0, -5\theta-2), (1, 12\theta+5), (1, -12\theta-5)\}$$
$$\{(0, 29\theta+12), (0, -29\theta-12), (1, 23\theta+29), (1, -23\theta-29)\}$$
$$\{(0, 28\theta+23), (0, -28\theta-23), (1, 32\theta+28), (1, -32\theta-28)\}$$
$$\{(0, 45\theta+32), (0, -45\theta-32), (1, 28\theta+45), (1, -28\theta-45)\}$$
$$\{(0, 7\theta+28), (0, -7\theta-28), (1, 42\theta+7), (1, -42\theta-7)\}$$
$$\{(0, 44\theta+42), (0, -44\theta-42), (1, 36\theta+44), (1, -36\theta-44)\}$$
$$\{(0, 22\theta+36), (0, -22\theta-36), (1, 33\theta+22), (1, -33\theta-22)\}$$
$$\{(0, 41\theta+33), (0, -41\theta-33), (1, 21\theta+41), (1, -21\theta-41)\}$$
$$\{(0, 36\theta+21), (0, -36\theta-21), (1, 46\theta+36), (1, -46\theta-36)\}$$
$$\{(0, 34\theta+46), (0, -34\theta-46), (1, 20\theta+34), (1, -20\theta-34)\}$$

The isomorphism $f\colon (x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_{47} \to 48y - 47x \in \mathbb{Z}_{141}$ turns the above blocks into the following eleven codeword-sets forming the desired silver $(141, 4, 1)$-OOC with difference leave $\{0, 7, 40, 45, 47, 94, 96, 101, 134\}$:

$$\{102, 39, 64, 124\},\quad \{42, 99, 7, 40\},\quad \{9, 132, 25, 22\},\quad \{12, 129, 49, 139\},$$
$$\{63, 78, 34, 13\},\quad \{84, 57, 61, 127\},\quad \{18, 123, 97, 91\},\quad \{24, 117, 4, 43\},$$
$$\{126, 15, 115, 73\},\quad \{27, 114, 28, 19\},\quad \{36, 105, 100, 88\}.$$

As far as this author is aware, the above optimal OOC is new but the same cannot be said for its parameters. Indeed it was proved in [16] that there exists a *perfect* $(v,4,1)$ *difference family* for all $v \equiv 1 \pmod{12}$ not exceeding 10 000 except $v = 25$ and $v = 37$. Also, according to Remark 1.4 in [1], any perfect $(v,4,1)$ difference family can be also seen as an optimal $(w,k,1)$-OOC for all w's between v and $v + k(k-1)$ included. Thus we have the existence of an optimal $(v,4,1)$-OOC for all v's not exceeding 10 012 except $v = 25$ (indeed an optimal $(v,4,1)$-OOC with $26 \le v \le 48$ is known to exist anyway).

4 On the golden $(2p,4,1)$ optical orthogonal codes

Note that the golden elements of $\mathbb{Z}_p$ are precisely the solutions of the congruence $x^2 - x - 1 \equiv 0 \pmod{p}$, i.e., the elements ϕ of $\mathbb{Z}_p$ such that $\phi + 1 = \phi^2$. This property is crucial for getting the following construction.

Theorem 4.1. *Let $p \equiv 11$ or $29 \pmod{30}$ be a prime and let ϕ be a golden element of $\mathbb{Z}_p$. If ϕ is a generator of $\mathbb{Z}_p^*/\{1,-1\}$, then there exists an optimal $(2p,4,1)$-OOC.*

Proof. We have to show that, under the given assumption, there exists an optimal $(\mathbb{Z}_2 \times \mathbb{Z}_p, 4, 1)$ difference packing. Indeed $\mathbb{Z}_2 \times \mathbb{Z}_p$ is isomorphic to $\mathbb{Z}_{2p}$ by the Chinese Remainder Theorem.

We can write $p = 6n + 5$ for a suitable n, hence $\frac{p-1}{2} = 3n + 2$, and the assumption on ϕ implies that we have

$$\mathbb{Z}_p^* = \{1,-1\} \cdot \{1, \phi, \phi^2, \dots, \phi^{3n}, \phi^{3n+1}\}.$$

It is then clear that

$$C := \{\phi^{3i-1} \mid 1 \le i \le n\} \text{ is an optimal companion of } \{\pm 1, \pm\phi, \pm\phi^2\}. \tag{4.1}$$

Indeed we have $C \cdot \{\pm 1, \pm\phi, \pm\phi^2\} = \mathbb{Z}_p^* \setminus \{\pm 1, \pm\phi\}$.

Let us lift the $(\mathbb{Z}_2, 4, 6)$ difference multiset $\{0,1,1,1\}$ to the 4-subset B of $\mathbb{Z}_2 \oplus \mathbb{Z}_p$

$$B = \{(0,0), (1,1), (1,\phi), (1,\phi^2\}.$$

Looking at the difference table of B (see Table 3) we see that we have

$$\Delta_0 B = \{\pm(\phi-1), \pm\phi(\phi-1), \pm(\phi+1)(\phi-1)\}; \quad \Delta_1 B = \{\pm 1, \pm\phi, \pm\phi^2\}.$$

Thus, recalling that $\phi + 1 = \phi^2$, we can write

$$\Delta_0 B = (\phi-1)\{\pm 1, \pm\phi, \pm\phi^2\}, \qquad \Delta_1 B = \{\pm 1, \pm\phi, \pm\phi^2\}$$

so that, by (4.1), C in an optimal companion of $\Delta_g B$ for each $g \in \mathbb{Z}_2$. We conclude that $\mathcal{D} = \{(1,c) \cdot B \mid c \in C\}$ is the desired optimal $(\mathbb{Z}_5 \times \mathbb{Z}_p, 5, 1)$ difference packing by Proposition 2.2. □

The optimal OOCs arising from the above result will be called *golden*. We remark that the assumption on ϕ is equivalent to ask that ϕ^2, that is $\phi + 1$, is a primitive square of $\mathbb{Z}_p$ and it does not depend on the chosen golden element; indeed the product of the two golden elements is -1, hence their orders in $\mathbb{Z}_p^*/\{1,-1\}$ are the same. We also note that the difference leave of the constructed difference packing is

$$\{0\} \times \{0, 1, -1, \phi-1, 1-\phi\} \cup \{1\} \times \{0, 1, -1, \phi, -\phi\}.$$

Table 3: The difference table of $B = \{(0,0),(1,1),(1,\phi),(1,\phi^2\}$.

	$(0,0)$	$(1,1)$	$(1,\phi)$	$(1,\phi^2)$
$(0,0)$	$\bullet$	$(1,-1)$	$(1,-\phi)$	$(1,-\phi^2)$
$(1,1)$	$(1,1)$	$\bullet$	$(0,1-\phi)$	$(0,1-\phi^2)$
$(1,\phi)$	$(1,\phi)$	$(0,\phi-1)$	$\bullet$	$(0,\phi-\phi^2)$
$(1,\phi^2)$	$(1,\phi^2)$	$(0,\phi^2-1)$	$(0,\phi^2-\phi)$	$\bullet$

We have checked that in the range $[1,10^5]$, Theorem 4.1 works in 1533 out of 2399 of the cases.

Remark 4.2. Using formula (1.2), the optimal difference packing $\mathcal{D}$ constructed in Theorem 4.1 can be more explicitly written in terms of Fibonacci numbers. Indeed we have $\mathcal{D} = \{B_i \mid 1 \le i \le n\}$ with

$$B_i = \{(0,0),\ (1,F_{3i-1}\phi + F_{3i-2}),\ (1,F_{3i}\phi + F_{3i-1}),\ (1,F_{3i+1}\phi + F_{3i})\}.$$

By way of illustration we explicitly construct a golden $(142,4,1)$-OOC using the above remark.

We have $142 = 2p$ with $p = 71 \equiv 11 \pmod{30}$ prime, and we can write $p = 6n+5$ with $n = 11$. A golden element of $\mathbb{Z}_p$ clearly is $\phi = 9$; indeed we have $9^2 \equiv 10 \pmod{71}$. The maximal proper divisors of $(p-1)/2$ are 5 and 7 and neither 10^5 nor 10^7 is $1 \pmod{p}$. This guarantees that 10 has order $(p-1)/2$ in $\mathbb{Z}_p^*$, namely $\phi+1$ is a primitive square of $\mathbb{Z}_p$. Thus Theorem 4.1 can be applied. The reduction modulo p of the Fibonacci sequence up to its 34-th term is

$$(0,1,1,2,3,5,8,13,21,34,55,18,2,20,22,42,64,35,28,63,20,$$
$$12,32,44,5,49,54,32,15,47,62,38,29,67,25).$$

Thus, applying Remark 4.2, the blocks of an optimal $(\mathbb{Z}_2 \times \mathbb{Z}_{71},4,1)$ difference packing are the following:

$$\{(0,0),(1,\phi+1),(1,2\phi+1),(1,3\phi+2)\}$$
$$\{(0,0),(1,5\phi+3),(1,8\phi+5),(1,13\phi+8)\}$$
$$\{(0,0),(1,21\phi+13),(1,34\phi+21),(1,55\phi+34)\}$$
$$\{(0,0),(1,18\phi+55),(1,2\phi+18),(1,20\phi+2)\}$$
$$\{(0,0),(1,22\phi+20),(1,42\phi+22),(1,64\phi+42)\}$$
$$\{(0,0),(1,35,\phi+64),(1,28\phi+35),(1,63\phi+28)\}$$
$$\{(0,0),(1,20\phi+63),(1,12\phi+20),(1,32\phi+12)\}$$
$$\{(0,0),(1,44\phi+32),(1,5\phi+44),(1,49\phi+5)\}$$
$$\{(0,0),(1,54\phi+49),(1,32\phi+54),(1,15\phi+32)\}$$
$$\{(0,0),(1,47\phi+15),(1,62\phi+47),(1,38\phi+62)\}$$
$$\{(0,0),(1,29\phi+38),(1,67\phi+29),(1,25\phi+67)\}$$

The isomorphism $f\colon (x,y) \in \mathbb{Z}_2 \times \mathbb{Z}_{71} \to 71x + 72y \in \mathbb{Z}_{142}$ turns the above blocks into the following eleven codeword-sets forming the desired golden $(142, 4, 1)$-OOC with difference leave $\{0, 1, 8, 9, 70, 71, 72, 133, 134, 141\}$:

$$\{0, 81, 19, 29\}, \quad \{0, 119, 77, 125\}, \quad \{0, 131, 43, 103\}, \quad \{0, 75, 107, 111\},$$
$$\{0, 5, 45, 121\}, \quad \{0, 95, 3, 27\}, \quad \{0, 101, 57, 87\}, \quad \{0, 73, 89, 91\},$$
$$\{0, 109, 129, 25\}, \quad \{0, 83, 37, 49\}, \quad \{0, 15, 135, 79\}.$$

Although the above optimal OOC is probably new, the same cannot be said for its parameters for the same reason explained in the end of Section 3.

References

[1] R. J. R. Abel and M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Comb. Theory Ser. A* **106** (2004), 59–75, doi:10.1016/j.jcta.2004.01.003.

[2] R. J. R. Abel and M. Buratti, Difference families, in: C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, Boca Raton, FL, Discrete Mathematics and its Applications (Boca Raton), pp. 392–410, 2nd edition, 2007.

[3] K. T. Arasu and S. Sehgal, Cyclic difference covers, *Australas. J. Combin.* **32** (2005), 213–223, https://ajc.maths.uq.edu.au/pdf/32/ajc_v32_p213.pdf.

[4] M. Buratti, A packing problem and its application to Bose's families, *J. Combin. Des.* **4** (1996), 457–472, doi:10.1002/(sici)1520-6610(1996)4:6⟨457::aid-jcd6⟩3.0.co;2-e.

[5] M. Buratti, Recursive constructions for difference matrices and relative difference families, *J. Combin. Des.* **6** (1998), 165–182, doi:10.1002/(sici)1520-6610(1998)6:3⟨165::aid-jcd1⟩3.0.co;2-d.

[6] M. Buratti, Old and new designs via difference multisets and strong difference families, *J. Combin. Des.* **7** (1999), 406–425, doi:10.1002/(sici)1520-6610(1999)7:6⟨406::aid-jcd2⟩3.3.co;2-l.

[7] M. Buratti, Hadamard partitioned difference families and their descendants, *Cryptogr. Commun.* (2018), doi:10.1007/s12095-018-0308-3.

[8] M. Buratti and L. Gionfriddo, Strong difference families over arbitrary graphs, *J. Combin. Des.* **16** (2008), 443–461, doi:10.1002/jcd.20201.

[9] M. Buratti and A. Pasotti, Combinatorial designs and the theorem of Weil on multiplicative character sums, *Finite Fields Appl.* **15** (2009), 332–344, doi:10.1016/j.ffa.2008.12.007.

[10] M. Buratti and A. Pasotti, Further progress on difference families with block size 4 or 5, *Des. Codes Cryptogr.* **56** (2010), 1–20, doi:10.1007/s10623-009-9335-6.

[11] M. Buratti, J. Yan and C. Wang, From a 1-rotational RBIBD to a partitioned difference family, *Electron. J. Combin.* **17** (2010), #R139, http://www.combinatorics.org/ojs/index.php/eljc/article/view/v17i1r139.

[12] F. R. K. Chung, J. A. Salehi and V. K. Wei, Optical orthogonal codes: design, analysis, and applications, *IEEE Trans. Inform. Theory* **35** (1989), 595–604, doi:10.1109/18.30982.

[13] C. J. Colbourn, J. H. Dinitz and D. R. Stinson, Applications of combinatorial designs to communications, cryptography, and networking, in: J. D. Lamb and D. A. Preece (eds.), *Surveys in Combinatorics, 1999*, Cambridge University Press, Cambridge, volume 267 of *London Mathematical Society Lecture Note Series*, pp. 37–100, 1999, doi:10.1017/cbo9780511721335.004, papers from the British Combinatorial Conference held at the University of Kent at Canterbury, Canterbury, 1999.

[14] S. Costa, T. Feng and X. Wang, Frame difference families and resolvable balanced incomplete block designs, *Des. Codes Cryptogr.* (2018), doi:10.1007/s10623-018-0472-7.

[15] S. Costa, T. Feng and X. Wang, New 2-designs from strong difference families, *Finite Fields Appl.* **50** (2018), 391–405, doi:10.1016/j.ffa.2017.12.011.

[16] G. Ge, Y. Miao and X. Sun, Perfect difference families, perfect difference matrices, and related combinatorial structures, *J. Combin. Des.* **18** (2010), 415–449, doi:10.1002/jcd.20259.

[17] J. Kapusta, The square, the circle and the golden proportion: a new class of geometrical constructions, *Forma* **19** (2004), 293–313, http://www.scipress.org/journals/forma/abstract/1904/19040293.html.

[18] T. Koshy, *Fibonacci and Lucas numbers with applications*, Pure and Applied Mathematics (New York), Wiley-Interscience, New York, 2001, doi:10.1002/9781118033067.

[19] T. Koshy, *Pell and Pell-Lucas numbers with applications*, Springer, New York, 2014, doi:10.1007/978-1-4614-8489-9.

[20] F. Lemmermeyer, *Reciprocity Laws*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000, doi:10.1007/978-3-662-12893-0.

[21] K. Momihara, Strong difference families, difference covers, and their applications for relative difference families, *Des. Codes Cryptogr.* **51** (2009), 253–273, doi:10.1007/s10623-008-9259-6.

[22] R. Pan and Y. Chang, Combinatorial constructions for maximum optical orthogonal signature pattern codes, *Discrete Math.* **313** (2013), 2918–2931, doi:10.1016/j.disc.2013.09.005.

[23] S. Szabó and A. D. Sands, *Factoring Groups into Subsets*, volume 257 of *Lecture Notes in Pure and Applied Mathematics*, CRC Press, Boca Raton, FL, 2009, doi:10.1201/9781420090475.

[24] J. Yin, Some combinatorial constructions for optical orthogonal codes, *Discrete Math.* **185** (1998), 201–219, doi:10.1016/s0012-365x(97)00172-6.

[25] J. Yin, X. Yang and Y. Li, Some 20-regular $\mathrm{CDP}(5,1;20u)$ and their applications, *Finite Fields Appl.* **17** (2011), 317–328, doi:10.1016/j.ffa.2011.01.002.