Classification of optimal \((v, 4, 1)\) optical orthogonal codes with \(v \leq 76\)

Tsonka Baicheva    Svetlana Topalova

Institute of Mathematics and Informatics
Bulgarian Academy of Sciences

September, 2010
Novosibirsk, Russia

- Optical code-division multiple-access communication systems
- Mobile radio
- Frequency-hopping spread spectrum communications
- Constructing protocol-sequence sets for the M-active-out-of-T users collision channel without feedback
- Radar and sonar signal design
- Public key algorithm for optical communication based on lattice cryptography
Optical orthogonal codes with specific parameters are closely related to

- Constant-weight error-correcting codes
- Difference sets
- Cyclic partial designs
- Well-correlated binary sequences
Basic definitions I

- $\mathbb{Z}_v$ the ring of integers modulo $v$

**Definition**

A $(v, k, \lambda_a, \lambda_c)$ optical orthogonal code (OOC) can be defined as a collection $\mathcal{C} = \{C_1, ..., C_s\}$ of $k$-subsets (codeword-sets) of $\mathbb{Z}_v$ such that any two distinct translates of a codeword-set share at most $\lambda_a$ elements while any two translates of two distinct codeword-sets share at most $\lambda_c$ elements:

\[
|C_i \cap (C_i + t)| \leq \lambda_a, \quad 1 \leq i \leq s, \quad 1 \leq t \leq v - 1 \quad (1)
\]
\[
|C_i \cap (C_j + t)| \leq \lambda_c, \quad 1 \leq i < j \leq s, \quad 0 \leq t \leq v - 1 \quad (2)
\]

- (1) is called the auto-correlation property
- (2) is called the cross-correlation property
The size of $C$ is the number $s$ of its codeword-sets.

A $(v, k, \lambda, \lambda)$ OOC is also denoted by $(v, k, \lambda)$ OOC.

$C = \{c_1, c_2, \ldots, c_k\}$ is a codeword-set

$\triangle' C$ is the multiset of the values of the differences $c_i - c_j, \ i \neq j, \ i, j = 1, 2, \ldots, k$

$\triangle C$ is the underlying set of $\triangle' C$

Autocorrelation property $\Rightarrow$ at most $\lambda_a$ differences are the same

Cross-correlation property $\Rightarrow$ if $\lambda_c = 1$ then $\triangle C_1 \cap \triangle C_2 = \emptyset$ for two codeword-sets $C_1$ and $C_2$ of the $(v, k, \lambda_a, 1)$ OOC
Definition

Two \((v, k, \lambda_a, \lambda_c)\) optical orthogonal codes are **equivalent** if they can be mapped to one another by an automorphism of \(Z_v\) and (or) replacement of codeword-sets by some of their translates.
Bound for the size of \((v, k, 1)\) OOC

\[
s \leq \left\lfloor \frac{(v - 1)}{k(k - 1)} \right\rfloor
\]

- \((v, k, 1)\) OOCs for which \(s = \left\lfloor \frac{(v - 1)}{k(k - 1)} \right\rfloor\) are called optimal
- If \(s = \frac{(v - 1)}{k(k - 1)}\) the \((v, k, 1)\) OOC is called perfect

A perfect \((v, k, 1)\) OOC corresponds to
- a cyclic 2-\((v,k,1)\) design
- a cyclic \((v,k,1)\) difference family
K. Chen and L. Zhu, Existence of \((q, k, 1)\) difference families with \(q\) a prime power and \(k = 4, 5\). *Combin. Des.* 7, 21–30, 1999.


M. Buratti and A. Pasotti, Further progress on difference families with block size 4 or 5, *Des. Codes Cryptogr*. Published online, doi:10.1007/s10623-009-9335-6.
An optimal \((v, 4, 1)\) OOC exists for all \(v \leq 1212, v \neq 25\).

Classification results for small \(v\) are only known for cyclic \(2 - (v, 4, 1)\) designs, namely for the perfect \((v, 4, 1)\) OOCs for \(v = 37, 49\) and \(61\).

- A table of optimal \((v, 4, 2)\) OOCs with \(v \leq 44\) (with 3 possible exceptions) is presented.
- Construction by an algorithm based on the maximum clique search problem.
We classify up to equivalence optimal $(v, 4, 1)$ OOCs with $v \leq 76$

**Our approach:**
ordering all possibilities for codeword-sets with respect to the action of the automorphisms of the cyclic group of order $v$, and then applying the well-known techniques of back-track search with minimality test on the partial solutions

We relate to each codeword-set \( C = \{c_1, c_2, c_3, c_4\} \) a codeword-set vector \( \vec{C} = (c_1, c_2, c_3, c_4) \) such that \( c_1 < c_2 < c_3 < c_4 \).

If we replace a codeword-set \( C \in \mathcal{C} \) with a translate \( C + t \in \mathcal{C} \), we obtain an equivalent OOC.

w.l.o.g. we assume that each codeword-set vector of the optimal \((v, 4, 1)\) OOC is lexicographically smaller than the codeword-set vectors of its translates.

This means that \( c_1 = 0 \).
We create an array $L$ of all 4-dimensional vectors over $Z_v$ which might become codeword-set vectors

- We construct the vectors of $L$ in lexicographic order
- To each vector we apply the automorphisms $\varphi_i$, $i = 1, 2, \ldots, m - 1$ of $Z_v$ and if some of them maps it to a smaller vector, we do not add this vector since it is already somewhere in the array
- If we add the current vector $\vec{C}$ to the list, we also add after it the $m - 1$ vectors to which $\vec{C}$ is mapped by $\varphi_i$, $i = 1, 2, \ldots, m - 1$.

This way we obtain the array $L$ whose elements $L_x$, $x = 0, 1, \ldots, f$ are all the possible codeword-set vectors
Classification algorithm III

Codewordsets with suitable autocorrelation

$L_0$
$L_1 = \varphi_1 L_0$
$L_2 = \varphi_2 L_0$
\ldots
$L_{m-1} = \varphi_{m-1} L_0$
$L_m$
$L_{m+1} = \varphi_1 L_m$
$L_{m+2} = \varphi_2 L_m$
\ldots
$L_{2m-1} = \varphi_{m-1} L_m$
\ldots
$L_{im}$
$L_{im+1} = \varphi_1 L_m$
$L_{im+2} = \varphi_2 L_m$
\ldots
$L_{(i+1)m-1} = \varphi_{m-1} L_m$
Classification algorithm IV

It is possible for two different automorphisms to map a codeword-set vector to one and the same codeword-set vector.

Example

The automorphism group of $Z_{30}$ is of order 8

$\varphi_0(a) = a$, $\varphi_1(a) = 7a$, $\varphi_2(a) = 11a$, $\varphi_3(a) = 13a$, $\varphi_4(a) = 17a$, $\varphi_5(a) = 19a$, $\varphi_6(a) = 23a$, $\varphi_7(a) = 29a$, where $a \in Z_{30}$.

$\vec{C}_1 = (0, 1, 3, 22) \xrightarrow{\varphi_1} (0, 7, 21, 4) \xrightarrow{+26} (26, 3, 17, 0) \rightarrow (0, 3, 17, 26) = \vec{C}_2$

$\vec{C}_1 = (0, 1, 3, 22) \xrightarrow{\varphi_3} (0, 13, 9, 16) \xrightarrow{+17} (17, 0, 26, 3) \rightarrow (0, 3, 17, 26) = \vec{C}_2$
We keep for each possible codeword-set vector $L_x$ the smallest number $a$, such that $L_x = L_y$ and $y = a \ (mod \ m)$

We keep this $a$ in place of the first codeword-set element $c_1$, which is always 0

This way for each $x$ we can directly obtain the smallest $y$, such that $L_y$ is obtained by applying on $L_x$ a given automorphism of $Z_v$. 
Classification algorithm VI

We construct the OOC choosing the codeword-sets among the elements of \( L \) by backtrack search until we find the \( s \) codeword-sets

\[ L_{x_1}, L_{x_2}, \ldots, L_{x_s} \]

- We choose the \( r + 1 \)-st element \( L_{x_{r+1}} \) \((x_{r+1} > x_r)\) of the codeword-set to have no common differences with the previous \( r \) ones
- When we add the \( r + 1 \)-st codeword-set number \( x_{r+1} \), we also find the \( r + 1 \) numbers obtained by applying \( \varphi_i, i = 1, 2, \ldots, m \) to the current partial solution and sort them
- If the obtained array is lexicographically smaller than the current one, it means that an equivalent sub-code with \( r + 1 \) codeword-sets has already been considered, and we look for the next possibility for the \( r + 1 \)-st codeword-set.
### Table: Inequivalent optimal \((v,4,1)\) OOCs

<table>
<thead>
<tr>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>2</td>
<td>1</td>
<td>43</td>
<td>3</td>
<td>1772</td>
<td>60</td>
<td>4</td>
<td>7585950</td>
</tr>
<tr>
<td>27</td>
<td>2</td>
<td>4</td>
<td>44</td>
<td>3</td>
<td>3208</td>
<td>61p</td>
<td>5</td>
<td>18132</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>4</td>
<td>45</td>
<td>3</td>
<td>12428</td>
<td>62</td>
<td>5</td>
<td>20736</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>11</td>
<td>46</td>
<td>3</td>
<td>9999</td>
<td>63</td>
<td>5</td>
<td>529996</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>41</td>
<td>47</td>
<td>3</td>
<td>20692</td>
<td>64</td>
<td>5</td>
<td>409632</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>42</td>
<td>48</td>
<td>3</td>
<td>51510</td>
<td>65</td>
<td>5</td>
<td>3774498</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>64</td>
<td>49p</td>
<td>4</td>
<td>224</td>
<td>66</td>
<td>5</td>
<td>6512840</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
<td>196</td>
<td>50</td>
<td>4</td>
<td>336</td>
<td>67</td>
<td>5</td>
<td>18814608</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>181</td>
<td>51</td>
<td>4</td>
<td>5530</td>
<td>68</td>
<td>5</td>
<td>27675160</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
<td>378</td>
<td>52</td>
<td>4</td>
<td>6382</td>
<td>69</td>
<td>5</td>
<td>153524880</td>
</tr>
<tr>
<td>36</td>
<td>2</td>
<td>731</td>
<td>53</td>
<td>4</td>
<td>28672</td>
<td>70</td>
<td>5</td>
<td>204850952</td>
</tr>
<tr>
<td>37p</td>
<td>3</td>
<td>2</td>
<td>54</td>
<td>4</td>
<td>56064</td>
<td>71</td>
<td>5</td>
<td>425759570</td>
</tr>
<tr>
<td>38</td>
<td>3</td>
<td>12</td>
<td>55</td>
<td>4</td>
<td>213662</td>
<td>72</td>
<td>5</td>
<td>979134632</td>
</tr>
<tr>
<td>39</td>
<td>3</td>
<td>96</td>
<td>56</td>
<td>4</td>
<td>263102</td>
<td>73p</td>
<td>6</td>
<td>1426986</td>
</tr>
<tr>
<td>40</td>
<td>3</td>
<td>86</td>
<td>57</td>
<td>4</td>
<td>1105056</td>
<td>74</td>
<td>6</td>
<td>2140556</td>
</tr>
<tr>
<td>41</td>
<td>3</td>
<td>338</td>
<td>58</td>
<td>4</td>
<td>1011104</td>
<td>75</td>
<td>6</td>
<td>59992260</td>
</tr>
<tr>
<td>42</td>
<td>3</td>
<td>998</td>
<td>59</td>
<td>4</td>
<td>2575944</td>
<td>76</td>
<td>6</td>
<td>42145856</td>
</tr>
</tbody>
</table>
**Table: Inequivalent optimal \((v, 4, 1)\) OOCs**

<table>
<thead>
<tr>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
<th>(v)</th>
<th>(s)</th>
<th>OOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>2</td>
<td>1</td>
<td>43</td>
<td>3</td>
<td>1772</td>
<td>60</td>
<td>4</td>
<td>7585950</td>
</tr>
<tr>
<td>27</td>
<td>2</td>
<td>4</td>
<td>44</td>
<td>3</td>
<td>3208</td>
<td>61</td>
<td>5</td>
<td>18132</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>4</td>
<td>45</td>
<td>3</td>
<td>12428</td>
<td>62</td>
<td>5</td>
<td>20736</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>11</td>
<td>46</td>
<td>3</td>
<td>9999</td>
<td>63</td>
<td>5</td>
<td>529996</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>41</td>
<td>47</td>
<td>3</td>
<td>20692</td>
<td>64</td>
<td>5</td>
<td>409632</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>42</td>
<td>48</td>
<td>3</td>
<td>51510</td>
<td>65</td>
<td>5</td>
<td>3774498</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>64</td>
<td>49</td>
<td>4</td>
<td>224</td>
<td>66</td>
<td>5</td>
<td>6512840</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
<td>196</td>
<td>50</td>
<td>4</td>
<td>336</td>
<td>67</td>
<td>5</td>
<td>18814608</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>181</td>
<td>51</td>
<td>4</td>
<td>5530</td>
<td>68</td>
<td>5</td>
<td>27675160</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
<td>378</td>
<td>52</td>
<td>4</td>
<td>6382</td>
<td>69</td>
<td>5</td>
<td>153524880</td>
</tr>
<tr>
<td>36</td>
<td>2</td>
<td>731</td>
<td>53</td>
<td>4</td>
<td>28672</td>
<td>70</td>
<td>5</td>
<td>204850952</td>
</tr>
<tr>
<td><strong>37p</strong></td>
<td><strong>3</strong></td>
<td><strong>2</strong></td>
<td><strong>54</strong></td>
<td><strong>4</strong></td>
<td><strong>56064</strong></td>
<td><strong>71</strong></td>
<td><strong>5</strong></td>
<td><strong>425759570</strong></td>
</tr>
<tr>
<td>38</td>
<td>3</td>
<td>12</td>
<td>55</td>
<td>4</td>
<td>213662</td>
<td>72</td>
<td>5</td>
<td><strong>979134632</strong></td>
</tr>
<tr>
<td>39</td>
<td>3</td>
<td>96</td>
<td>56</td>
<td>4</td>
<td>263102</td>
<td>73</td>
<td>6</td>
<td><strong>1426986</strong></td>
</tr>
<tr>
<td>40</td>
<td>3</td>
<td>86</td>
<td>57</td>
<td>4</td>
<td>1105056</td>
<td>74</td>
<td>6</td>
<td>2140556</td>
</tr>
<tr>
<td>41</td>
<td>3</td>
<td>338</td>
<td>58</td>
<td>4</td>
<td>1011104</td>
<td>75</td>
<td>6</td>
<td>59992260</td>
</tr>
<tr>
<td>42</td>
<td>3</td>
<td>998</td>
<td>59</td>
<td>4</td>
<td>2575944</td>
<td>76</td>
<td>6</td>
<td>42145856</td>
</tr>
</tbody>
</table>