Reconstruction of Constellation Labeling with Convolutional Coded Data

Marion Bellard   Nicolas Sendrier

INRIA-Rocquencourt, SECRET Project-Team

October 2012
1 Communication System

2 Convolutional codes

3 Reconstruction of Constellation Labeling
   - Method
   - Classes
   - Convolutional code reconstruction
   - Complexity
   - Further work
\[ x = x_1 \ldots x_k \rightarrow y = y_1 \ldots y_n \rightarrow z_t = (z_1 \ldots z_a)_t \rightarrow (A, \phi)_t \]

\[ x' = x'_1 \ldots x'_k \rightarrow y' = y'_1 \ldots y'_n \rightarrow z'_t = (z'_1 \ldots z'_a)_t \rightarrow (A', \phi')_t \]
Labeling: $P \in \mathcal{C} \rightarrow f(P) \in \mathbb{F}_2^a$

Constellation: Representation of the labeling in the plane

$P$
Gray labeling

\[ f \] is a Gray labeling if for all \( P_1 \) and \( P_2 \in \mathcal{C} \) such as
\[ d(P_1, P_2) = 1, \]
\[ d_{Hamming}(f(P_1), f(P_2)) = 1 \]
1 Communication System

2 Convolutional codes

3 Reconstruction of Constellation Labeling
   • Method
   • Classes
   • Convolutional code reconstruction
   • Complexity
   • Further work
Convolutional codes

$k : \text{number of inputs}$

$n : \text{number of outputs}$

The output $(y_1 \ldots y_n)_t$ depends on $(x_1 \ldots x_k)_t, (x_1 \ldots x_k)_{t-1}, \ldots, (x_1 \ldots x_k)_{t-M}$
1 Communication System

2 Convolutional codes

3 Reconstruction of Constellation Labeling
   - Method
   - Classes
   - Convolutional code reconstruction
   - Complexity
   - Further work
Exhaustive method

For all possible labelings, observe the signal $S_f$ with a default labeling $f$. Try to recognize a convolutional code $(n, k)$, $(\lambda n, \lambda k)$, $\emptyset$, $\emptyset$, and so on for all possible labelings.
Our method

Demodulation with a default labeling $f$

For all representative labelings, try to recognize a convolutional code

$(n, k)$

$(n, k)$

$(\lambda n, \lambda k)$
Linear and affine classes

- **Notation:**
  - \( C \) a constellation, \( a \) the number of bits per symbol.
  - \( C_L(f) \) the linear class of \( f \), \( C_A(f) \) the affine class of \( f \)

**Definitions**

- We say that two labelings \( f_1 \) and \( f_2 \) from \( C \) to \( \{0, 1\}^a \) are linearly equivalent if and only if there exists \( L \) a binary invertible \( a \times a \) matrix such as for all \( P \in C \), \( f_1(P) = f_2(P) \cdot L \).

- We say that two labelings \( f_1 \) and \( f_2 \) from \( C \) to \( \{0, 1\}^a \) are affine equivalent if and only if there exists \( L \) a binary invertible \( a \times a \) matrix and \( v \) a binary vector of length \( a \) such as for all \( P \in C \), \( f_1(P) = f_2(P) \cdot L + v \).
### Labeling distribution

#### Table: Number of labelings $a = 2, 3, 4$

<table>
<thead>
<tr>
<th>$a$</th>
<th>Number of labelings</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>40 320</td>
</tr>
<tr>
<td>4</td>
<td>$&gt; 2 \times 10^{13}$</td>
</tr>
</tbody>
</table>

#### Table: Labelings distribution for $a = 2, 3, 4$

<table>
<thead>
<tr>
<th>$a$</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>30</td>
<td>8</td>
<td>168</td>
</tr>
<tr>
<td>4</td>
<td>64 864 800</td>
<td>16</td>
<td>20 160</td>
</tr>
</tbody>
</table>

(1) Number of affine classes  
(2) Number of linear classes per affine class  
(3) Number of labelings per linear class
Gray labelings

The “Grayness” of the labelings is compatible to an extent with the linear and affine equivalence relations

**Property**

Let $f_1$ be a Gray labeling and let $f_2 \in C_A(f_1)$, then $f_2$ is a Gray labeling if and only if there exists $L$ a permutation matrix and $v$ a vector of $\{0, 1\}^a$ such as $\forall P \in C, f_2(P) = f_1(P) \cdot L + v$. 
Gray labelings

Table: Number of Gray labelings for square constellations 16- QAM, 64- QAM and 256- QAM

<table>
<thead>
<tr>
<th>a</th>
<th>Number of Gray labelings</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>384</td>
</tr>
<tr>
<td>6</td>
<td>414 720</td>
</tr>
<tr>
<td>8</td>
<td>584 674 836 480</td>
</tr>
</tbody>
</table>

Table: Gray labelings distribution for \(a = 4, 6, 8\)

<table>
<thead>
<tr>
<th>a</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>6</td>
<td>9</td>
<td>64</td>
<td>720</td>
</tr>
<tr>
<td>8</td>
<td>56 644</td>
<td>256</td>
<td>40 320</td>
</tr>
</tbody>
</table>

(1) Number of affine classes containing Gray labelings
(2) Number of linear classes per affine class
(3) Number of Gray labelings per linear class
Representatives of classes

- Representatives of affine classes: There exist \( f_1, \ldots, f_N \) such as
  \[
  \bigcup_{i=1\ldots N} C_A(f_i) = M_a
  \]
  and
  \[ f_i \notin C_A(f_j) \]

- We find them:
  - Not Gray: by fixing the values of several points of \( C \) and carry out a backtrack search
  - Gray: with the direct product of two Gray codes (Wesel, Liu, Cioffi, Komminakakis)

- Representatives of linear classes:
  \[
  \bigcup_{\nu \in \mathbb{F}_2^a} C_L(f_i + \nu) = C_A(f_i)
  \]
Convolutional code reconstruction

\[ n : \text{code length} \]
\[ k : \text{code dimension} \]
\[ S_f : \text{the binary sequence observed with labeling } f \]
\[ R(S_f) = (n, k, G) \text{ is the result of convolutional code reconstruction} \]
Test on linear and affine classes

- \( (f \in C_L(f')) \Rightarrow (R(S_f) = \emptyset \iff R(S_{f'}) = \emptyset) \)

- \( S \ll \delta \) the sequence \( S \) shifted by \( \delta \geq 0 \) left positions and 
  \( D_\delta(S) = S - (S \ll \delta) \).

  if \( \delta \) is a multiple of \( \text{lcm}(n, a) \) we have :
- \( (f' \in C_A(f)) \Rightarrow (R(D_\delta(S_f)) = \emptyset \iff R(D_\delta(S_{f'})) = \emptyset) \)
Test on linear class

<table>
<thead>
<tr>
<th>Property</th>
</tr>
</thead>
<tbody>
<tr>
<td>((f \in C_L(f')) \Rightarrow (R(S_f) = \emptyset \iff R(S_{f'}) = \emptyset)).</td>
</tr>
</tbody>
</table>

Let \(S_f\) be a binary sequence produced by an \((n, k, m)\) convolutional encoder using the labeling \(f\)

Let \(\text{lcm}(a, n) = \lambda n = \mu a\).

We have \(\forall P \in C, \ f'(P) = f(P) \cdot \mathcal{L}\)

Note that \(R(S_f) = (\lambda n, \lambda k, G[^\lambda]) \Rightarrow R(S_{f'}) = (\lambda n, \lambda k, G[^\lambda] \mathcal{L}[\mu])\)
Test on affine class

- \((f' \in C_A(f)) \not\Rightarrow (R(S_f) = \emptyset \iff R(S_{f'}) = \emptyset)\)

- \(S \ll \delta\) the sequence \(S\) shifted by \(\delta \geq 0\) left positions and \(D_\delta(S) = S - (S \ll \delta)\).

Property

*If \(\delta\) is a multiple of \(\text{lcm}(n, a)\) we have

\[ (f' \in C_A(f)) \Rightarrow (R(D_\delta(S_f)) = \emptyset \iff R(D_\delta(S_{f'})) = \emptyset). \]

Proof: \(\forall P \in C, f'(P) = f(P) \cdot \mathcal{L} + \nu\)

- \(\delta\) multiple of \(a\): the affine part \(\nu\) cancels with the difference.
- \(\delta\) multiple of \(n\): the sequence \(D_\delta(S) = S - (S \ll \delta)\) remains a sequence from a convolutional encoder.
$N$ : the number of affine classes
We denote $C_A(x_1), \ldots, C_A(x_s)$ the affine classes selected, $n_i$ the number of linear classes selected in $C_A(x_i)$.

Number of code reconstruction :

- Non gray : $N + s2^a + (n_1 + n_2 + \cdots + n_s) \# GL(a, \mathbb{F}_2)$
- Gray : $N + s2^a + (n_1 + n_2 + \cdots + n_s)a!$
Further work

- Use the relation between linear classes:
  Let $f_1 \in C_A(f)$ be a linear representative such as $R(S_{f_1}) = (G[^\lambda], \lambda n, \lambda k)$. Then $R(S_{(f_1+v)\cdot L}) = R(S_{f_1\cdot L}) = (G[^\lambda L[^\mu], \lambda n, \lambda k)$

- Use the ratio $\frac{k}{n}$ to select the best affine classes
  Example: $(n, k) = (3, 1)$ we can find $(3, 2)$ codes
Thanks for your attention
Any questions?