Tutorial on radio communications: From the basics to future developments

Part 2: Forward Error Correction in Radio Networks

Stefan Nowak
TU Dortmund, Germany
stefan.nowak@tu-dortmund.de
Outline

• Why do we need FEC?
• Classification of FEC codes
• Selected FEC coding schemes
• Automatic Repeat Request
• Conclusion
Why do we need FEC?

Add additional redundancy at the transmitter

Exploit it at the receiver for error detection and error correction

- FEC coding makes communication more robust or even enables it at all

Why do we need FEC?

Radio communication environment

- Time selectivity due to mobility
- Frequency selectivity due to multipath propagation
Classification of FEC Codes

FEC types

Block codes

- Hamming codes
- BCH codes
- RS codes

Convolutional codes

- Turbo codes
- LDPC codes

Decoding by

- Viterbi algorithm
- Iterative decoding

Algebraic coding and decoding

Concatenated Codes

Product Codes
Coding gain

$E_b/N_0$ (dB)

$P_b$

$10^{-8}$ $10^{-6}$ $10^{-4}$ $10^{-2}$ $10^0$

BPSK uncoded
Coding gain

\[ P_b \] vs. \( E_b/N_0 \) (dB)

- BPSK uncoded
- \( R = 1/4 \)
- \( R = 1/2 \)
- \( R = 3/4 \)
- \( R = 9/10 \)

Ultimate Shannon limit
Block Codes

- Code rate: \( R = \frac{k}{n} \)
- Code identification: \((n, k, d_{\text{min}})\) - block code
- Code capabilities of a linear block code with \(d_{\text{min}}\):
  - up to \(d_{\text{min}} - 1\) errors can be detected
  - up to \(\left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor\) errors can be corrected
Hamming Codes

• First non-trivial code to appear in literature:
  (7,4,3)-Hamming Code
• Infinite class of single error correcting binary linear codes
• Parameters:
  - Block length: $n = 2^m - 1$
  - Dimension: $k = n - m$
  - Minimum distance: $d_{\text{min}} = 3$
• Properties:
  - Low complexity
  - Can correct a single bit error
  - Can detect up to two bit errors
    (code extension by parity bit)
• Applications:
  - Computer memory (SECDED)
  - Teletext

<table>
<thead>
<tr>
<th>m</th>
<th>n</th>
<th>k</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>7</td>
<td>4</td>
<td>0.57</td>
</tr>
<tr>
<td>4</td>
<td>15</td>
<td>11</td>
<td>0.73</td>
</tr>
<tr>
<td>5</td>
<td>31</td>
<td>26</td>
<td>0.84</td>
</tr>
<tr>
<td>6</td>
<td>63</td>
<td>57</td>
<td>0.90</td>
</tr>
<tr>
<td>7</td>
<td>127</td>
<td>120</td>
<td>0.94</td>
</tr>
<tr>
<td>8</td>
<td>255</td>
<td>247</td>
<td>0.97</td>
</tr>
<tr>
<td>9</td>
<td>511</td>
<td>502</td>
<td>0.98</td>
</tr>
<tr>
<td>10</td>
<td>1023</td>
<td>1013</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Hamming Codes

![Diagram showing the performance of Hamming codes with different rates vs. Eb/N0. The diagram includes curves for BPSK uncoded and (7,4,3)-Hamming Code R=0.57, as well as the ultimate Shannon limit.]
Hamming Codes

\[ E_b/N_0 (dB) \]

\[ P_b \]

- (127,120,3)-Hamming Code
  - $R=0.94$ (SECDED)

- (7,4,3)-Hamming Code $R=0.57$
- BPSK uncoded

MobiLight 2010, 12 May 2010, Barcelona
BCH Codes

• Binary cyclic error correcting block codes

• Parameters:
  - Block length: \( n = 2^n - 1 \)
  - Dimension: \( k \)
  - Number of errors to be corrected: \( t \)
  - Distance: \( d = 2 \cdot t + 1 \)
  - Number of parity bits: \( n - k \leq m \cdot t \) (very often = is valid)

• Properties:
  - Algebraic coding and decoding
  - Offer a large set of codes to choose from

• Applications:
  - Used rarely
  - DVB-T2/S2: Outer code for an LDPC Code
  - CRC: Cyclic-Redundancy-Check for error detection in automatic repeat request (ARQ) systems

RS Codes

- Non-binary cyclic error correcting block codes

**Parameters:**

- Number of bits per symbol: $m$
- Number of different symbols: $q = 2^m$
- Block length (symbols): $N = 2^m - 1$
- Number of parity symbols: $M$
- Code dimension: $K = N - M$
- Minimum distance: $d_{\text{min}} = N - K + 1$
- Number of errors to be corrected: $t = \left\lfloor \frac{M}{2} \right\rfloor$
- Number of erasures to be corrected: $e = M$

**Properties:**

- Decoding by the Berlekamp-Massey algorithm
- Matches perfectly representation of bytes ($m = 8$ Bit)
- Well suited for burst error correction: $b = \left( \frac{(N-K)}{2} \cdot q + 1 \right) = (t - 1) \cdot q + 1$
  (Maximum length of bit error burst)

RS Codes

• Some possible codes for $m = 8$:

<table>
<thead>
<tr>
<th>$N,K$</th>
<th>$n,k$</th>
<th>$t$</th>
<th>$R$</th>
<th>$b$</th>
</tr>
</thead>
<tbody>
<tr>
<td>255,247</td>
<td>2040,1976</td>
<td>4</td>
<td>0.97</td>
<td>25</td>
</tr>
<tr>
<td>255,239</td>
<td>2040,1912</td>
<td>8</td>
<td>0.94</td>
<td>57</td>
</tr>
<tr>
<td>255,223</td>
<td>2040,1784</td>
<td>16</td>
<td>0.84</td>
<td>121</td>
</tr>
</tbody>
</table>

• Applications:
  – Highly useful in practice (extended or shortened versions)
  – Used in many concatenated coding schemes (DVB-T/S)
  – Deep space communication (e.g. Voyager, Mars Pathfinder)
  – Data/audio/video storage systems (e.g. compact disc)

• Recent results on RS Codes:
  – List decoding beyond the guaranteed error-correction distance (Sudan, 1997)
  – Soft decision decoding (Kötter/Vardy, 2003)


RS Codes

\[ \frac{E_b}{N_0} \text{ (dB)} \]

\[ P_b \]

- BPSK uncoded
- (7,4,3)-Hamming Code R=0.57
- (127,120,3)-Hamming Code R=0.94 (SECDED)
- (255, 247) RS-Code R=0.97

\[ \text{Eb/N0 (dB)} \]

\[ P_b \]

\[ R=\frac{1}{4}, R=\frac{1}{2}, R=\frac{3}{4}, R=\frac{9}{10} \]

\[ \text{ultimate Shannon limit} \]

MobiLight 2010, 12 May 2010, Barcelona

ICT-213311 OMEGA
RS Codes

![Graph showing the performance of different codes with varying Eb/N0 (dB) and Pb (Error Probability). The graph includes lines for (255, 239) RS-Code R=0.94, (255, 247) RS-Code R=0.97, (127, 120, 3)-Hamming Code R=0.94 (SECDED), (7,4,3)-Hamming Code R=0.57, and BPSK uncoded. The Shannon limit is also marked.]

MobiLight 2010, 12 May 2010, Barcelona
Convolutional Codes

- Information is spread over the codeword by serial shift registers and XORs
- Parameters:
  - $n$ output bits are produced out of $k$ input bits $\Rightarrow$ code rate $R=k/n$
  - Constraint length $C$: number of bits in the input stream that affect one output bit
  - Generator polynomials define encoder structure
  - Many good generator polynomials available from literature
  - Many code rates adjustable by puncturing

- Example: IEEE 802.11a/g/n

\[
\begin{align*}
R &= 1/2 \\
C &= 7 \\
g &= \{133, 171\}_8
\end{align*}
\]

Convolutional Codes

• Properties:
  – Decoding by the Viterbi algorithm (VA): soft decision decoding
    Estimates the most likely sequence of encoder register states based on the
    channel observation \( \rightarrow \) recovery of input bits
  – Traceback length \( t_b \): Number of decoding steps before deciding about a bit
    \( t_b \approx 5 \cdot (C - 1) \) and larger especially for punctured codes
  – Complexity of VA increases exponentially with \( C \)
  – Well suited for the correction of single bit errors
  – Bursty errors at the decoder input mostly result in decoding failure

• Applications:
  – Wireless LANs according to IEEE 802.11a/g/n
  – Deep space communication (e.g. Mars Pathfinder with \( C=15 \))
  – Part of concatenated coding schemes: e.g. DVB-T/S, NASA missions in the 1970s

A. J. Viterbi, “Error bounds for convolutional codes and asymptotically optimum decoding algorithm,”
Convolutional Codes

$\text{Eb/N0 (dB)}$

$P_b$

$10^{-8}$

$10^{-6}$

$10^{-4}$

$10^{-2}$

$10^{0}$

$10^{2}$

$10^{4}$

$10^{6}$

$10^{8}$

$20$ - $12$

$R=1/4$

$R=1/2$

$R=3/4$

$R=9/10$

$\text{BPSK uncoded}$

Conv. Code $g=(133,171)_g$

$R=1/2$ (IEEE 802.11a/g/n)

$(255, 223)$ RS-Code $R=0.84$

$(255, 239)$ RS-Code $R=0.94$

$(255, 247)$ RS-Code $R=0.97$

$(127,120,3)$-Hamming Code $R=0.94$ (SECDED)

$(7,4,3)$-Hamming Code $R=0.57$
Convolutional Codes

- Conv. Code $g=(133, 165, 171)_8$ R = 1/3 (ECMA-368, WiMedia)
- Conv. Code $g=(133, 171)_8$ R = 1/2 (IEEE 802.11a/g/n)
- (255, 223) RS-Code R=0.84
- (255, 239) RS-Code R=0.94
- (255, 247) RS-Code R=0.97
- (127,120,3)-Hamming Code R=0.94 (SECDED)
- (7,4,3)-Hamming Code R=0.57
- BPSK uncoded

$E_b/N_0$ (dB) vs. $P_b$
Concatenated Codes

- Concatenation of an outer and inner channel code
- Example: DVB-S, derived from a NASA coding scheme of the 1970s

```plaintext
Outer Encoder RS(204,188)  Convolutional Interleaver M=17, I=12  Inner Convolutional Encoder R = 1/2
```

- Inner convolutional code:
  - Well suited for single bit errors
  - In case of burst errors the Viterbi decoder produces burst errors as well

- Outer RS code:
  - Oversized for single bit errors, those are eliminated by the Viterbi decoder
  - Well suited for all burst errors at the output of the Viterbi decoder

- Convolutional interleaver:
  - Spreads neighboured RS symbols over several RS code words
Concatenated Codes

\[ DVB-S \text{ conc. code } R = 0.47 \]
\[ RS(204,188) + CC (R=1/2) \]
\[ \text{Conv. Code } g=(133, 165, 171)_8 \]
\[ R = 1/3 \ (ECMA-368, WiMedia) \]
\[ \text{Conv. Code } g=(133,171)_8 \]
\[ R = 1/2 \ (IEEE 802.11a/g/n) \]
\[ (255, 223) \text{ RS-Code } R = 0.84 \]
\[ (255, 239) \text{ RS-Code } R = 0.94 \]
\[ (255, 247) \text{ RS-Code } R = 0.97 \]
\[ (127,120,3)-\text{Hamming Code } R = 0.94 \ (\text{SECDED}) \]
\[ (7,4,3)-\text{Hamming Code } R = 0.57 \]
\[ \text{BPSK uncoded} \]
Turbo-Codes

- Invented by C. Berrou, A. Glavieux and P. Thitimajshima in 1993
- "Classical" Turbo-Encoder:
  - Parallel concatenation of recursive systematic convolutional codes (RSC)

Turbo-Codes

- **Turbo-Decoding**
  - Based on iterative processing of extrinsic information
  - Stops if process has converged or maximum number of iterations is reached
  - Soft-decision decoding algorithm needed providing posteriori probabilities per bit
    Most common: BCJR algorithm (MAP, sum-product algorithm on a trellis)

- Poor minimum distance $\rightarrow$ error floor
- Applications:
  - B3G mobile telephony (HSPA + LTE), NASA deep space missions, IEEE 802.16 (WiMAX)

---

Turbo-Codes

"Original" Turbo-Code R=1/2
RSC (37,21)_8, N=65536

DVB-S conc. code R=0.47
RS(204,188) + CC (R=1/2)

Conv. Code g=(133, 165, 171)_8
R =1/3 (ECMA-368, WiMedia)
Conv. Code g=(133,171)_8
R =1/2 (IEEE 802.11a/g/n)

(255, 223) RS-Code R=0.84
(255, 239) RS-Code R=0.94
(255, 247) RS-Code R=0.97
(127,120,3)-Hamming Code
R=0.94 (SECDED)

(7,4,3)-Hamming Code R=0.57

BPSK uncoded

MobiLight 2010, 12 May 2010, Barcelona
Turbo-Codes

- LTE Turbo-Code $R=1/2$
  - RSC (13,15)$_b$, $N=6144$
- "Original" Turbo-Code $R=1/2$
  - RSC (37,21)$_b$, $N=65536$
- DVB-S conc. code $R=0.47$
- RS(204,188) + CC ($R=1/2$)
- Conv. Code $g=(133, 165, 171)_h$
  - $R=1/3$ (ECMA-368, WiMedia)
- Conv. Code $g=(133,171)_h$
  - $R=1/2$ (IEEE 802.11a/g/n)
- (255, 223) RS-Code $R=0.84$
- (255, 239) RS-Code $R=0.94$
- (255, 247) RS-Code $R=0.97$
- (127,120,3)-Hamming Code
  - $R=0.94$ (SECDED)
- (7,4,3)-Hamming Code $R=0.57$
- BPSK uncoded

**Graph:**
- $E_b/N_0$ (dB) vs. $P_b$ for various codes and rates.
- Shown are curves for different rates ($R=1/4, 1/2, 3/4, 9/10$) and codes.
- Ultimate Shannon limit marked at $E_b/N_0 = 2.4$ dB.
LDPC Codes

• Linear block codes described by a sparse parity-check matrix
  → LDPC: Low-Density Parity-Check

\[
H = \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
\end{bmatrix}
\]

• Properties:
  – Regular and irregular LDPC Codes
  – Irregularity can be described by (optimized) degree distributions
  – Decoded iteratively (sum-product algorithm)
    Processing of soft-information, girth should be as large as possible
  – Performance close to the Shannon limit for large block lengths
  – Error floors can occur (due to low weight near codewords)

LDPC Codes

• Some notes:
  – LDPC Codes which approach the Shannon limit within 0.0045 dB have been designed theoretically
  – Performance within 0.04 dB of the Shannon limit has been reached practically for a code with $R=1/2$ and $N=10^7$
  – Non-binary codes show a better performance for small block lengths

• Applications:
  – DVB-S2 in combination with an outer BCH code
  – IEEE 802.11n (optional coding scheme)
  – 10GBase-T Ethernet (IEEE 802.3an)


LDPC Codes

- DVB-S2 LDPC Code R=1/2, N=64800 (eIRA)
- LTE Turbo-Code R=1/2
- "Original" Turbo-Code R=1/2
- DVB-S conc. code R=0.47
- RS(204,188) + CC (R=1/2)
- Conv. Code g=(133,165,171) R=1/3 (ECMA-368, WiMedia)
- Conv. Code g=(133,171) R=1/2 (IEEE 802.11a/g/n)
- (255, 223) RS-Code R=0.84
- (255, 239) RS-Code R=0.94
- (255, 247) RS-Code R=0.97
- (127,120,3)-Hamming Code R=0.94 (SECDED)
- (7,4,3)-Hamming Code R=0.57
- BPSK uncoded

MobiLight 2010, 12 May 2010, Barcelona
LDPC Codes

IEEE 802.11n LDPC Code R=1/2, N=1944 (QC)
DVB-S2 LDPC Code R=1/2, N=64800 (eIRA)
LTE Turbo-Code R=1/2, RSC (13,15)_8, N=6144
"Original" Turbo-Code R=1/2, RSC (37,21)_8, N=65536
DVB-S conc. code R=0.47
RS(204,188) + CC (R=1/2)
Conv. Code g=(133, 165, 171)_8, R =1/3 (ECMA-368, WiMedia)
Conv. Code g=(133,171)_8, R =1/2 (IEEE 802.11a/g/n)
(255, 223) RS-Code R=0.84
(255, 239) RS-Code R=0.94
(255, 247) RS-Code R=0.97
(127,120,3)-Hamming Code R=0.94 (SECDED)
(7,4,3)-Hamming Code R=0.57
BPSK uncoded

MobiLight 2010, 12 May 2010, Barcelona
ICT-213311 OMEGA
LDPC Codes

- LDPC Code: Chung et al. R=1/2, N=10^7, Shannon-Gap=0.04 dB @ P_b=10^{-6}
- IEEE 802.11n LDPC Code R=1/2, N=1944 (QC)
- DVB-S2 LDPC Code R=1/2, N=64800 (eIRA)
- DVB-S conc. code R=0.47
- LTE Turbo-Code R=1/2 RSC (13,15)_8, N=6144
- "Original" Turbo-Code R=1/2 RSC (37,21)_8, N=65536
- DVB-S conc. code R=0.47
- RS(204,188) + CC (R=1/2)
- Conv. Code g=(133, 165, 171)_8 R =1/3 (ECMA-368, WiMedia)
- Conv. Code g=(133, 171)_8 R =1/2 (IEEE 802.11a/g/n)
- (255, 223) RS-Code R=0.84
- (255, 239) RS-Code R=0.94
- (255, 247) RS-Code R=0.97
- (127,120,3)-Hamming Code R=0.94 (SECDED)
- (7,4,3)-Hamming Code R=0.57
- BPSK uncoded

MobiLight 2010, 12 May 2010, Barcelona
ICT-213311 OMEGA
Automatic Repeat Request

- **Drawbacks of FEC:**
  - Decoded information is delivered to the user whether it is correct or not.
  - Probability of a decoding error is much greater than the probability of an undetected error.
  - To obtain high system reliability: Long powerful codes must be used and a large set of error patterns must be corrected.

- **Automatic Repeat Request (ARQ) in packet-switching systems with two-way communication:**
  - Use of error detection capabilities of FEC codes in retransmission schemes.
  - Probability of undetected errors has to be very small (e.g. CRC codes).
  - e.g. WLAN according to IEEE 802.11.
  - Most common:
    - Stop-And-Wait
    - Go-Back-N
    - Selective Repeat
Conclusion

• FEC coding makes communication systems robust against errors and increases their efficiency
• Today, there is a rich FEC coding toolbox available
• Modern FEC codes practically reach the Shannon limit

• Some current and future research topics:
  – Reduction of complexity at constant performance
  – Redefinition of complexity and efficiency measures for future generations of technology?
  – Coding for multi-user channels and networks
Thank you for your attention!
Some useful references

- Nice review of the trip on “The Road to Channel Capacity” given by two distinguished contributors in this field:
  D. J. Costello and G. D. Forney, Jr., “Channel Coding: The Road to Channel Capacity,”

- Comprehensive textbooks on classical and modern channel coding:
  D. J. C. MacKay, “Information Theory, Inference and Learning Algorithms,”
  Cambridge University Press, 2003
  Available at: http://www.inference.phy.cam.ac.uk/mackay/itila/book.html

  S. Lin and D. J. Costello, Jr., “Error Control Coding,”

  T. K. Moon, “Error Correction Coding: Mathematical Methods and Algorithms,”
  John Wiley & Sons, 2005

  T. Richardson and R. Urbanke, “Modern Coding Theory,”
  Cambridge University Press, 2008

  (contains many recent developments on LDPC coding)