Determination of Suitable CRC Polynomials for Functional Safe Communication
Determination of Suitable CRC Polynomials for Functional Safe Communication

Prof. Dr.-Ing. Frank Schiller
Beckhoff Automation
Scientific Safety & Security

F.Schiller@beckhoff.com
+49 911 54056 244
1. Introduction

2. Requirements to Data Integrity Measures
   - Residual Error Probability
   - Deterministic Criteria

3. Generator Polynomials for Cyclic Redundancy Check (CRC)
   - Meaning of the Generator Polynomial
   - Determination of the Generator Polynomial

4. Examples

5. Conclusion
1. Introduction

Why (still) to deal with Cyclic Redundancy Check?

- easy to implement
- operates potentially fast
- does not need too much memory
- mathematically clear

Implementations:

- Linear Feedback Shift Register in hardware
- Linear Feedback Shift Register in software
- Table method

\[(nd'(x) \cdot x^r + fcs'(x)) \mod g(x) = 0?\]
Overall Schema of CRC:

Sender

ND
net data, information bits of length $m$

FCS
frame check sequence of length $r$

message $T$ of length $n$

Receiver

ND'
net data, information bits of length $m$

FCS'
frame check sequence of length $r$

message $T'$ of length $n$
1. Introduction

2. Requirements to Data Integrity Measures
   - Residual Error Probability
   - Deterministic Criteria

3. Generator Polynomials for Cyclic Redundancy Check (CRC)
   - Meaning of the Generator Polynomial
   - Determination of the Generator Polynomial

4. Examples

5. Conclusion
The **Residual Error Probability** $P_{re}$ is the probability that any non-detectable erroneous message is received.

The Residual Error Probability depends on:

- number of FCS bits $r$,
- number of ND bits $m$,
- generator polynomial $g(x)$,
- bit error probability $p$.

The Binary Symmetric Channel is assumed:

- bits are corrupted independently and with the same probability,
- falsification from 0 to 1 occurs with the same probability as from 1 to 0.
Remark: Residual Error Probability of CRC compared to other approaches:
Deterministic Criteria are independent of the assumption of the BSC:

- Hamming Distance (minimum 4 has been required so far)
- Detectability of odd bit errors (since even one parity bit enables that)
- Detectability of complete one-telegrams (failure in a component)
- Detectability of complete zero-telegrams (failure in a component)
- Detectability of completely inverted telegrams (failure in a component)
- Detectability of burst errors (transmission error, meaning for data)
- Detectability of slip errors (failure in a component)

Not all criteria should be fulfilled by 100% but should be included into the overall assessment in order to justify the Residual Error Probability based on BSC.

The check for Deterministic Criteria can be implemented very easily and the check is implicitly realized in well-known algorithms like CRC.
Remark: Effects of Hamming Distance on the Residual Error Probability of CRC:

Polynomial $1\text{FFEDh} / 1\text{6FFFh}$: residual error probability for $m=8, 80, 800$

$0 < p \leq 0.5$

Residual error probability $P_{re}$

HD=3
HD=4
HD=6

$2^{-16}$
2. Requirements to Data Integrity Measures

Remark: Effects of Hamming Distance on the Residual Error Probability of CRC:

Polynomial 14EABh / 1AAE5h: residual error probability for m=8, 80, 800

- HD=2
- HD=6
- HD=8
1. Introduction

2. Requirements to Data Integrity Measures
   - Residual Error Probability
   - Deterministic Criteria

3. Generator Polynomials for Cyclic Redundancy Check (CRC)
   - Meaning of the Generator Polynomial
   - Determination of the Generator Polynomial

4. Examples

5. Conclusion
3. Generator Polynomials for CRC

Meaning of the generator polynomial for probabilistic and deterministic criteria:

Given:
- number of ND bits \( m \),
- generator polynomial \( g(x) \)

Find:
- Residual Error Probability \( P_{re} \) for \( 0 \leq p \leq 0.5 \)
- deterministic criteria

\[
(n_d'(x) \cdot x^r + fcs'(x)) \mod g(x) = 0? 
\]
Examples: $m = 112$, $r = 16$, $n = 128$ different generator polynomials
3. Generator Polynomials for CRC

Determination of the generator polynomial:

Given:
- number of ND bits $m$,
- generator polynomial $g(x)$

Find:
- Residual Error Probability $P_{re}$ for $0 \leq p \leq 0.5$
- deterministic criteria

Solution:
- by means of deterministic and stochastic automata
- (direct code analysis, transformed code analysis, Monte Carlo Method)

Given:
- number of ND bits $m$,
- degree $r$ of generator polynomial $g(x)$
- maximum Residual Error Probability $P_{re}$ for $0 \leq p \leq 0.5$

Find:
- generator polynomial $g(x)$
  - with lowest Residual Error Probability $P_{re}$ for $0 \leq p \leq 0.5$
  - and fulfilling deterministic criteria

Solution:
- combination of algorithms
- by means of deterministic and stochastic automata
3. Generator Polynomials for CRC

Determination of the generator polynomial, algorithm in principle:

\[ n, r, \text{maximum} \quad P_{re} \]

1. Identify all generator polynomials causing the maximum Hamming Distance \( d(1) \) for message length \( n(1) \)

1. Choose those polynomials causing the next lower Hamming Distance \( d(i+1) < d(i) \) for maximum message length \( n(i+1) < n(i) \)

1. Determine and evaluate Residual Error Probability w.r.t. maximum \( P_{re} \)

1. Apply deterministic Criteria

\[ g(x) \]
Determination of the generator polynomial, algorithm in principle:

\[ n(i), d(i) \]

\[ n(i+1) < n(i), d(i+1) < d(i) \]

\[ n(i+1) < n(i), d(i+1) < d(i) \]

\[ n(i+1) < n(i), d(i+1) < d(i) \]

\[ n(i+1) < n(i), d(i+1) < d(i) \]
1. Introduction

2. Requirements to Data Integrity Measures
   - Residual Error Probability
   - Deterministic Criteria

3. Generator Polynomials for Cyclic Redundancy Check (CRC)
   - Meaning of the Generator Polynomial
   - Determination of the Generator Polynomial

4. Examples

5. Conclusion
4. Examples

Achievable Hamming Distance

\( r = 8 \)

<table>
<thead>
<tr>
<th>Hamming Distance ( d \geq )</th>
<th>Message Length ( n \leq )</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>5</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>127</td>
</tr>
<tr>
<td>3</td>
<td>255</td>
</tr>
</tbody>
</table>
4. Examples

Best polynomial

\[ r = 8, \ m = 112 \]
4. Examples

Best polynomial

\( r = 8, m = 1..112 \)
4. Examples

Best polynomial

\( r = 8, \ m = 1..128 \)

**Polynomial 137h / 1D9h**: deterministic analysis for \( m=1..128 \)

- 1 to 4: \( HD=6 \)
- 5 to 118: \( HD=4 \)
- 119 to \( \infty \): \( HD=2 \)

Inversion detectable for all \( k \)

Polynomial is divisible by \( x+1 \).
All odd bit errors are detectable.
### Achievable Hamming Distance

**$r = 16$**

<table>
<thead>
<tr>
<th>Hamming Distance $d \geq$</th>
<th>Message Length $n \leq$</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td>15</td>
<td>17</td>
</tr>
<tr>
<td>14</td>
<td>17</td>
</tr>
<tr>
<td>13</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td>11</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>21</td>
</tr>
<tr>
<td>9</td>
<td>22</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
</tr>
<tr>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>151</td>
</tr>
<tr>
<td>5</td>
<td>257</td>
</tr>
<tr>
<td>4</td>
<td>32767</td>
</tr>
<tr>
<td>3</td>
<td>65535</td>
</tr>
</tbody>
</table>
4. Examples

Best polynomial

\[ r = 16, \ m = 112 \]

Polynomial 19AF7h / 1DEB3h: residual error probability for m=112

\[ 0 < p \leq 0.5 \]

\[ P_{re} = 112 \]
4. Examples

Best polynomial

\[ r = 16, \ m = 1..112 \]

Polynomial 19AF7h / 1DEB3h: residual error probability for \( m = 1..112 \)

\[ 0 < p \leq 0.5 \]

residual error probability \( P_{re} \)

\[ 2^{-16} \]

\[ P_{re} \]
Best polynomial

\( r = 16, \ m = 112 \)

Polynomial 19AF7h / 1DEB3h: deterministic analysis for \( m = 1 \ldots 120 \)

- 
  - at 1: HD=12
  - at 2: HD=10
  - 3 to 13: HD=8
  - 14 to 112: HD=6
  - 113 to 120: HD=4

Inversion detectable for all \( k \)

Polynomial is divisible by \( x+1 \).

All odd bit errors are detectable.
4. Examples

Achievable Hamming Distance

\( r = 24 \)

<table>
<thead>
<tr>
<th>Hamming Distance ( d \geq )</th>
<th>Message Length ( n \leq )</th>
</tr>
</thead>
<tbody>
<tr>
<td>…</td>
<td>…</td>
</tr>
<tr>
<td>6</td>
<td>2050</td>
</tr>
<tr>
<td>5</td>
<td>4097</td>
</tr>
<tr>
<td>4</td>
<td>( 8388607 = 2^{23} - 1 )</td>
</tr>
<tr>
<td>3</td>
<td>( 16777215 = 2^{24} - 1 )</td>
</tr>
</tbody>
</table>
4. Examples

Good polynomial

\( r = 24, \ m = 2026 \)
4. Examples

Good polynomial

\[ r = 24, \ m = 1..2026 \]
Good polynomial

\( r = 24, \ m = 1..2050 \)

Polynomial 1A3EF8Bh / 1A3EF8Bh: deterministic analysis for \( m = 1..2050 \)

- Number of information bits \( m \)
- Minimum Hamming distance \( HD \)

- At 1: \( HD = 16 \)
- 2 to 7: \( HD = 12 \)
- 8: \( HD = 10 \)
- 9 to 49: \( HD = 8 \)
- 50 to 2026: \( HD = 6 \)
- 2027 to 2050: \( HD = 4 \)

Inversion detectable for all \( k \)

Polynomial is divisible by \( x + 1 \).
All odd bit errors are detectable.
1. Introduction

2. Requirements to Data Integrity Measures
   - Residual Error Probability
   - Deterministic Criteria

3. Generator Polynomials for Cyclic Redundancy Check (CRC)
   - Meaning of the Generator Polynomial
   - Determination of the Generator Polynomial

4. Examples

5. Conclusion
5. Conclusion

- CRC is an efficient method to achieve a low Residual Error Probability with reasonable effort and a relatively low number of checksum bits.

- Residual Error Probability and Deterministic Criteria can be determined.

- Hamming Distance of the actual message length as well as Hamming Distance of smaller lengths effect the Residual Error Probability tremendously.

- This characteristic can be used to identify suitable generator polynomials according to the proposed new method.