

# Erasure resilient systematic code with two information packets and up to 7 redundant packets

emin.gabrielyan@{epfl.ch, switzernet.com}

2005-10-27

[HTML](#) - [PDF](#) - [DOC](#)

Given is the problem:

- The receiver needs to receive any two packets out of all transmitted packets (information and redundancy) in order to completely recover the two information packets.
- Length of the packets must be equal and divisible to 3 (minimum 3 bits).

Let the first packet's first, second and third components be  $a$ ,  $b$  and  $c$ , and the second packet's components be correspondingly  $x$ ,  $y$  and  $z$ .

We will use the following notation:

$\boxed{abc}$  – denotes the first packet

$\boxed{xyz}$  – denotes the second packet

$\begin{array}{|c|} \hline xyz \\ \hline abc \\ \hline \end{array}$  – denotes a bitwise XOR result of the first and second packets (we mean an XOR results when we put the components vertically)

The redundant packets produced by this code are XOR results of the first packet  $\boxed{abc}$  with some derivative obtained from the second packet  $\boxed{xyz}$ . The derivatives are obtained by reordering and XOR-ing the three components of the second packet.

Example of a (4,2) code:

$\boxed{abc}$ ,  $\boxed{xyz}$ ,  $\begin{array}{|c|} \hline zyx \\ \hline abc \\ \hline \end{array}$ ,  $\begin{array}{|c|} \hline x \\ \hline yzy \\ \hline abc \\ \hline \end{array}$

In case if  $\boxed{xyz}$  is received with one of the redundant packets, we can produce from  $\boxed{xyz}$  the corresponding derivative and extract  $\boxed{abc}$  from the redundant packet. In case we received  $\boxed{abc}$  with one of redundant packets, we extract the derivative from which (as

you can see) we are capable to build back  $xyz$ . Finally if we received the two redundant packets:

$x$   
 $yzx$   
 $zyx$

We XOR them and obtain  $xyz$ . It is another derivative of  $xyz$ , which can be also converted back to  $xyz$ . Once  $xyz$  is found we can restore  $abc$  from any redundant packet.

This example can be generalized:

- The redundant packets must be built from such *self-containing* derivatives of  $xyz$ , from which we can fully restore back  $xyz$  (needed in the case when we receive  $abc$  with one redundant packet). I.e. the derivative of  $xyz$  must be reversible.
- The XOR result of two self-containing derivatives must be also a self-containing reversible derivative of  $xyz$  (we need this when two redundant packets are received).

Equipped with the above formulated point of view we first obtain all reversible derivatives of  $xyz$ .

A derivative of  $xyz$  may have one of the following 7 components:

$x$   
 $yzx$   
 $zyx$   
 $xzy$   
 $yxz$   
 $zxy$   
 $x, y, z, y, z, x$

Thus we have  $\frac{7!}{(7-3)!} = 210$  candidates

The derivative is not reversible and must be removed from the list, if the XOR result of any of two of its components is equal to the third component.

From 210 candidates we obtain 168 self-containing reversible derivatives of  $xyz$ .

These 168 self-containing results consist of the re-ordered versions of the following 28 distinct derivatives:

| <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|--------------------|--------------------|--------------------|
| $x$                | $y$                | $z$                |
| $x$                | $y$                | $x+z$              |
| $x$                | $y$                | $y+z$              |
| $x$                | $y$                | $x+y+z$            |

|       |       |         |
|-------|-------|---------|
| $x$   | $x+y$ | $z$     |
| $x$   | $x+y$ | $x+z$   |
| $x$   | $x+y$ | $y+z$   |
| $x$   | $x+y$ | $x+y+z$ |
| $x$   | $z$   | $y+z$   |
| $x$   | $z$   | $x+y+z$ |
| $x$   | $x+z$ | $y+z$   |
| $x$   | $x+z$ | $x+y+z$ |
| $y$   | $x+y$ | $z$     |
| $y$   | $x+y$ | $x+z$   |
| $y$   | $x+y$ | $y+z$   |
| $y$   | $x+y$ | $x+y+z$ |
| $y$   | $z$   | $x+z$   |
| $y$   | $z$   | $x+y+z$ |
| $y$   | $x+z$ | $y+z$   |
| $y$   | $y+z$ | $x+y+z$ |
| $x+y$ | $z$   | $x+z$   |
| $x+y$ | $z$   | $y+z$   |
| $x+y$ | $x+z$ | $x+y+z$ |
| $x+y$ | $y+z$ | $x+y+z$ |
| $z$   | $x+z$ | $y+z$   |
| $z$   | $x+z$ | $x+y+z$ |
| $z$   | $y+z$ | $x+y+z$ |
| $x+z$ | $y+z$ | $x+y+z$ |

where the operation  $+$  is a binary XOR

Let us enumerate the list of all derivatives and build a directed Graph whose vertices are the 168 self-containing reversible derivatives of  $\boxed{xYZ}$  and there is an arc from one self-containing derivative of  $\boxed{xYZ}$  to another one, if the sequential number of the first is smaller the number of the second one and if the XOR result of these two reversible derivatives is also reversible (i.e. is in the set of the 168 derivatives).

Such a graph has 4032 edges.

Any two adjacent vertices of this Graph can be used for production of two redundant packets and we have a (2,2) erasure resilient code.

A 3-complete sub-graph of our Graph consist of three distinct reversible derivatives of  $\boxed{xYZ}$ , such that an XOR of any of two of these derivatives gives us also a reversible derivative of  $\boxed{xYZ}$ . It means that if our Graph has 3-complete sub-graph we can create a (5,2) erasure resilient code.

Indeed, our Graph has 16128 such 3-complete sub-graphs.

Similarly, if we have a  $k$ -complete sub-graph in our Graph we can create  $(k + 2, 2)$  erasure resilient code. Hopefully we have also 4-complete sub-graphs and more ...

Here are the numbers of the  $k$ -complete sub-graphs in our Graph

|                       |       |
|-----------------------|-------|
| vertices              | 168   |
| arcs                  | 4032  |
| 3-complete sub-graphs | 16128 |
| 4-complete sub-graphs | 6720  |
| 5-complete sub-graphs | 4032  |
| 6-complete sub-graphs | 1344  |
| 7-complete sub-graphs | 192   |
| 8-complete sub-graphs | 0     |

Thus with this scheme we have 192 possible  $(9, 2)$  erasure resilient codes, which can restore the original two information packets from any two received packets (out of 9 transmitted). Note that with three bits symbols the Reed Solomon code can produce only blocks of  $2^3 - 1 = 7$  packets. I.e. the largest Reed-Solomon code is RS(7,2).

Below are a few of our codes (the full list is in the [output](#) of the AMPL program):

- (11,73,140,167,198,292,323)
- (11,75,134,182,241,247,314)
- (11,78,145,153,212,273,332)
- (12,71,137,163,203,290,328)
- (12,77,135,178,244,249,309)
- (12,80,146,149,217,267,333)

The numbers above refer to a reversible derivative of  $\boxed{xyz}$  from the table below. The derivative must be XOR-ed with  $\boxed{abc}$  in order to obtain the instance of the corresponding redundant packet.

| <i>Number</i> | <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|---------------|--------------------|--------------------|--------------------|
| 11            | $x$                | $y$                | $z$                |
| 12            | $x$                | $y$                | $x+z$              |
| 13            | $x$                | $y$                | $y+z$              |
| 14            | $x$                | $y$                | $x+y+z$            |
| 18            | $x$                | $x+y$              | $z$                |
| 19            | $x$                | $x+y$              | $x+z$              |
| 20            | $x$                | $x+y$              | $y+z$              |
| 21            | $x$                | $x+y$              | $x+y+z$            |
| 23            | $x$                | $z$                | $y$                |
| 24            | $x$                | $z$                | $x+y$              |
| 27            | $x$                | $z$                | $y+z$              |
| 28            | $x$                | $z$                | $x+y+z$            |
| 30            | $x$                | $x+z$              | $y$                |

| <i>Number</i> | <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|---------------|--------------------|--------------------|--------------------|
| 31            | $x$                | $x+z$              | $x+y$              |
| 34            | $x$                | $x+z$              | $y+z$              |
| 35            | $x$                | $x+z$              | $x+y+z$            |
| 37            | $x$                | $y+z$              | $y$                |
| 38            | $x$                | $y+z$              | $x+y$              |
| 39            | $x$                | $y+z$              | $z$                |
| 40            | $x$                | $y+z$              | $x+z$              |
| 44            | $x$                | $x+y+z$            | $y$                |
| 45            | $x$                | $x+y+z$            | $x+y$              |
| 46            | $x$                | $x+y+z$            | $z$                |
| 47            | $x$                | $x+y+z$            | $x+z$              |
| 53            | $y$                | $x$                | $z$                |
| 54            | $y$                | $x$                | $x+z$              |
| 55            | $y$                | $x$                | $y+z$              |
| 56            | $y$                | $x$                | $x+y+z$            |
| 67            | $y$                | $x+y$              | $z$                |
| 68            | $y$                | $x+y$              | $x+z$              |
| 69            | $y$                | $x+y$              | $y+z$              |
| 70            | $y$                | $x+y$              | $x+y+z$            |
| 71            | $y$                | $z$                | $x$                |
| 73            | $y$                | $z$                | $x+y$              |
| 75            | $y$                | $z$                | $x+z$              |
| 77            | $y$                | $z$                | $x+y+z$            |
| 78            | $y$                | $x+z$              | $x$                |
| 80            | $y$                | $x+z$              | $x+y$              |
| 81            | $y$                | $x+z$              | $z$                |
| 83            | $y$                | $x+z$              | $y+z$              |
| 85            | $y$                | $y+z$              | $x$                |
| 87            | $y$                | $y+z$              | $x+y$              |
| 89            | $y$                | $y+z$              | $x+z$              |
| 91            | $y$                | $y+z$              | $x+y+z$            |
| 92            | $y$                | $x+y+z$            | $x$                |
| 94            | $y$                | $x+y+z$            | $x+y$              |
| 95            | $y$                | $x+y+z$            | $z$                |
| 97            | $y$                | $x+y+z$            | $y+z$              |
| 102           | $x+y$              | $x$                | $z$                |
| 103           | $x+y$              | $x$                | $x+z$              |
| 104           | $x+y$              | $x$                | $y+z$              |
| 105           | $x+y$              | $x$                | $x+y+z$            |
| 109           | $x+y$              | $y$                | $z$                |
| 110           | $x+y$              | $y$                | $x+z$              |
| 111           | $x+y$              | $y$                | $y+z$              |
| 112           | $x+y$              | $y$                | $x+y+z$            |
| 120           | $x+y$              | $z$                | $x$                |

| <i>Number</i> | <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|---------------|--------------------|--------------------|--------------------|
| 121           | $x+y$              | $z$                | $y$                |
| 124           | $x+y$              | $z$                | $x+z$              |
| 125           | $x+y$              | $z$                | $y+z$              |
| 127           | $x+y$              | $x+z$              | $x$                |
| 128           | $x+y$              | $x+z$              | $y$                |
| 130           | $x+y$              | $x+z$              | $z$                |
| 133           | $x+y$              | $x+z$              | $x+y+z$            |
| 134           | $x+y$              | $y+z$              | $x$                |
| 135           | $x+y$              | $y+z$              | $y$                |
| 137           | $x+y$              | $y+z$              | $z$                |
| 140           | $x+y$              | $y+z$              | $x+y+z$            |
| 141           | $x+y$              | $x+y+z$            | $x$                |
| 142           | $x+y$              | $x+y+z$            | $y$                |
| 145           | $x+y$              | $x+y+z$            | $x+z$              |
| 146           | $x+y$              | $x+y+z$            | $y+z$              |
| 149           | $z$                | $x$                | $y$                |
| 150           | $z$                | $x$                | $x+y$              |
| 153           | $z$                | $x$                | $y+z$              |
| 154           | $z$                | $x$                | $x+y+z$            |
| 155           | $z$                | $y$                | $x$                |
| 157           | $z$                | $y$                | $x+y$              |
| 159           | $z$                | $y$                | $x+z$              |
| 161           | $z$                | $y$                | $x+y+z$            |
| 162           | $z$                | $x+y$              | $x$                |
| 163           | $z$                | $x+y$              | $y$                |
| 166           | $z$                | $x+y$              | $x+z$              |
| 167           | $z$                | $x+y$              | $y+z$              |
| 177           | $z$                | $x+z$              | $y$                |
| 178           | $z$                | $x+z$              | $x+y$              |
| 181           | $z$                | $x+z$              | $y+z$              |
| 182           | $z$                | $x+z$              | $x+y+z$            |
| 183           | $z$                | $y+z$              | $x$                |
| 185           | $z$                | $y+z$              | $x+y$              |
| 187           | $z$                | $y+z$              | $x+z$              |
| 189           | $z$                | $y+z$              | $x+y+z$            |
| 190           | $z$                | $x+y+z$            | $x$                |
| 191           | $z$                | $x+y+z$            | $y$                |
| 194           | $z$                | $x+y+z$            | $x+z$              |
| 195           | $z$                | $x+y+z$            | $y+z$              |
| 198           | $x+z$              | $x$                | $y$                |
| 199           | $x+z$              | $x$                | $x+y$              |
| 202           | $x+z$              | $x$                | $y+z$              |
| 203           | $x+z$              | $x$                | $x+y+z$            |
| 204           | $x+z$              | $y$                | $x$                |

| <i>Number</i> | <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|---------------|--------------------|--------------------|--------------------|
| 206           | $x+z$              | $y$                | $x+y$              |
| 207           | $x+z$              | $y$                | $z$                |
| 209           | $x+z$              | $y$                | $y+z$              |
| 211           | $x+z$              | $x+y$              | $x$                |
| 212           | $x+z$              | $x+y$              | $y$                |
| 214           | $x+z$              | $x+y$              | $z$                |
| 217           | $x+z$              | $x+y$              | $x+y+z$            |
| 219           | $x+z$              | $z$                | $y$                |
| 220           | $x+z$              | $z$                | $x+y$              |
| 223           | $x+z$              | $z$                | $y+z$              |
| 224           | $x+z$              | $z$                | $x+y+z$            |
| 232           | $x+z$              | $y+z$              | $x$                |
| 233           | $x+z$              | $y+z$              | $y$                |
| 235           | $x+z$              | $y+z$              | $z$                |
| 238           | $x+z$              | $y+z$              | $x+y+z$            |
| 239           | $x+z$              | $x+y+z$            | $x$                |
| 241           | $x+z$              | $x+y+z$            | $x+y$              |
| 242           | $x+z$              | $x+y+z$            | $z$                |
| 244           | $x+z$              | $x+y+z$            | $y+z$              |
| 247           | $y+z$              | $x$                | $y$                |
| 248           | $y+z$              | $x$                | $x+y$              |
| 249           | $y+z$              | $x$                | $z$                |
| 250           | $y+z$              | $x$                | $x+z$              |
| 253           | $y+z$              | $y$                | $x$                |
| 255           | $y+z$              | $y$                | $x+y$              |
| 257           | $y+z$              | $y$                | $x+z$              |
| 259           | $y+z$              | $y$                | $x+y+z$            |
| 260           | $y+z$              | $x+y$              | $x$                |
| 261           | $y+z$              | $x+y$              | $y$                |
| 263           | $y+z$              | $x+y$              | $z$                |
| 266           | $y+z$              | $x+y$              | $x+y+z$            |
| 267           | $y+z$              | $z$                | $x$                |
| 269           | $y+z$              | $z$                | $x+y$              |
| 271           | $y+z$              | $z$                | $x+z$              |
| 273           | $y+z$              | $z$                | $x+y+z$            |
| 274           | $y+z$              | $x+z$              | $x$                |
| 275           | $y+z$              | $x+z$              | $y$                |
| 277           | $y+z$              | $x+z$              | $z$                |
| 280           | $y+z$              | $x+z$              | $x+y+z$            |
| 289           | $y+z$              | $x+y+z$            | $y$                |
| 290           | $y+z$              | $x+y+z$            | $x+y$              |
| 291           | $y+z$              | $x+y+z$            | $z$                |
| 292           | $y+z$              | $x+y+z$            | $x+z$              |
| 296           | $x+y+z$            | $x$                | $y$                |

| <i>Number</i> | <i>Component 1</i> | <i>Component 2</i> | <i>Component 3</i> |
|---------------|--------------------|--------------------|--------------------|
| 297           | $x+y+z$            | $x$                | $x+y$              |
| 298           | $x+y+z$            | $x$                | $z$                |
| 299           | $x+y+z$            | $x$                | $x+z$              |
| 302           | $x+y+z$            | $y$                | $x$                |
| 304           | $x+y+z$            | $y$                | $x+y$              |
| 305           | $x+y+z$            | $y$                | $z$                |
| 307           | $x+y+z$            | $y$                | $y+z$              |
| 309           | $x+y+z$            | $x+y$              | $x$                |
| 310           | $x+y+z$            | $x+y$              | $y$                |
| 313           | $x+y+z$            | $x+y$              | $x+z$              |
| 314           | $x+y+z$            | $x+y$              | $y+z$              |
| 316           | $x+y+z$            | $z$                | $x$                |
| 317           | $x+y+z$            | $z$                | $y$                |
| 320           | $x+y+z$            | $z$                | $x+z$              |
| 321           | $x+y+z$            | $z$                | $y+z$              |
| 323           | $x+y+z$            | $x+z$              | $x$                |
| 325           | $x+y+z$            | $x+z$              | $x+y$              |
| 326           | $x+y+z$            | $x+z$              | $z$                |
| 328           | $x+y+z$            | $x+z$              | $y+z$              |
| 331           | $x+y+z$            | $y+z$              | $y$                |
| 332           | $x+y+z$            | $y+z$              | $x+y$              |
| 333           | $x+y+z$            | $y+z$              | $z$                |
| 334           | $x+y+z$            | $y+z$              | $x+z$              |

where operation + is a binary XOR

Here is an implementation of the algorithm in AMPL:

```

reset;

set B ordered = {"x","y","z"};

set A{i in 1..7} within B =
  (if i div 1 mod 2 then {member(1,B)} else {}) union
  (if i div 2 mod 2 then {member(2,B)} else {}) union
  (if i div 4 mod 2 then {member(3,B)} else {});

set S{n in 1..7^3,p in 0..2} within B =
  A[(n-1) div 7^p mod 7 + 1];

#210 members according to Binomial Coefficient (7 over 3) multiplied by
3!
set Binomial =
  {
    n in 1..7^3:
      (S[n,0] symdiff S[n,1] not within {}) and
      (S[n,1] symdiff S[n,2] not within {}) and
      (S[n,2] symdiff S[n,0] not within {})
  }

```



```

};

set Codes ordered =
{ n in Binomial:
  not (
    ( (S[n,0] symdiff S[n,1]) symdiff S[n,2] within {} ) or
    ( (S[n,1] symdiff S[n,2]) symdiff S[n,0] within {} ) or
    ( (S[n,2] symdiff S[n,0]) symdiff S[n,1] within {} )
  )
};

set Graph =
{
  n in Codes, m in Codes:
  {
    k in Codes:
      ( (S[n,0] symdiff S[m,0]) symdiff S[k,0] within {} ) and
      ( (S[n,1] symdiff S[m,1]) symdiff S[k,1] within {} ) and
      ( (S[n,2] symdiff S[m,2]) symdiff S[k,2] within {} )
    } not within {}
};

set Codes2 = { (n1,n2) in Graph: n2>n1};

set Codes3 =
{
  (n1,n2) in Codes2, n3 in Codes:
    n3>n2 and
    (n1,n3) in Codes2 and
    (n2,n3) in Codes2
};

set Codes4 =
{
  (n1,n2,n3) in Codes3, n4 in Codes:
    n4>n3 and
    (n1,n4) in Codes2 and
    (n2,n4) in Codes2 and
    (n3,n4) in Codes2
};

set Codes5 =
{
  (n1,n2,n3,n4) in Codes4, n5 in Codes:
    n5>n4 and
    (n1,n5) in Codes2 and
    (n2,n5) in Codes2 and
    (n3,n5) in Codes2 and
    (n4,n5) in Codes2
};

set Codes6 =
{
  (n1,n2,n3,n4,n5) in Codes5, n6 in Codes:
    n6>n5 and
    (n1,n6) in Codes2 and
    (n2,n6) in Codes2 and

```

```

        (n3,n6) in Codes2 and
        (n4,n6) in Codes2 and
        (n5,n6) in Codes2
    };

set Codes7 =
{
    (n1,n2,n3,n4,n5,n6) in Codes6, n7 in Codes:
        n7>n6 and
        (n1,n7) in Codes2 and
        (n2,n7) in Codes2 and
        (n3,n7) in Codes2 and
        (n4,n7) in Codes2 and
        (n5,n7) in Codes2 and
        (n6,n7) in Codes2
};

set Codes8 =
{
    (n1,n2,n3,n4,n5,n6,n7) in Codes7, n8 in Codes:
        n8>n7 and
        (n1,n8) in Codes2 and
        (n2,n8) in Codes2 and
        (n3,n8) in Codes2 and
        (n4,n8) in Codes2 and
        (n5,n8) in Codes2 and
        (n6,n8) in Codes2 and
        (n7,n8) in Codes2
};

display card(Codes);
display card(Codes2);
display card(Codes3);
display card(Codes4);
display card(Codes5);
display card(Codes6);
display card(Codes7);
display card(Codes8);

for
    {n in Codes:
        (n-1) div 7^0 mod 7 + 1 > (n-1) div 7^1 mod 7 + 1 > (n-1) div 7^2
mod 7 + 1
    }
    display n,S[n,2],S[n,1],S[n,0];

display Codes7;

```

\* \* \*

© 2005 – Switzernet ([www.switzernet.com](http://www.switzernet.com))

[US – Mirror](#)

[CH – Mirror](#)

