Erasure resilient (10,3) checksum codes

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

HTML – PDF – DOC

Given is the problem:

- Packets of equal length divisible by 3 (minimum 3 bit)
- 3 information packets
- 7 redundant packets
- Information must be restored upon successful reception of any of three packets out of 10

How to construct:

Let (a,b,c) be the first packet, where a, b and c represent the first, second and third portions of the packet

Let (x,y,z) and (t,v,w) bet the second and third packets

A redundant packet is formed as follows:
$(a,b,c)+(x',y',z')+(t',v',w')$
where

$(a,b,c)+(x,y,z)=(a+x,b+y,c+z)$
Henceforth, operation + is an XOR
$(x',y',z')=f(x,y,z)$
$(t',v',w')=g(t,v,w)$

Each of x', y' and z' is obtained by XOR-ing a subset from x, y and z (same is for t', v' and w'). Thus the functions f and g can be defined via 3 by 3 binary matrices.

Functions f and g are invertible, such that you can always obtain (x,y,z) from (x',y',z') and (t,v,w) from (t',v',w').

There are 168 invertible (x',y',z') packets (or functions). They are listed here with some IDs and we will further refer to them by these IDs.

The codeword consists of three information packets (the code is systematic) and a block of 7 distinct redundant packets. For each of 7 redundant packets we need to have a distinct pair of f_i and g_i functions:

$(a,b,c)+f_1(x,y,z)+g_1(t,v,w)$
$(a,b,c)+f_2(x,y,z)+g_2(t,v,w)$
…
$(a,b,c)+f_7(x,y,z)+g_7(t,v,w)$

The set of seven *f* (or *g*) functions has the following properties
$f_i(x,y,z)+f_j(x,y,z)\in F$, for any $i\neq j$, where *F* is the set of all 168 invertible packets

In 051027-erasure-9-2-resilient we obtained 192 different 7-member subsets satisfying this property: an XOR of two members is invertible. Let us denote the set of these 192 subsets of *F* as *G*.

Here is the list of these 192 subsets. Elements of the subsets are the IDs of the invertible functions.

Now let us analyze how the decoding works in a simple cases, when (*x*,*y*,*z*) is received with the following two redundant packets:
$(a,b,c) + f_i(x,y,z) + g_i(t,v,w)$
$(a,b,c) + f_j(x,y,z) + g_j(t,v,w)$

By XOR-ing the redundant packets we eliminate (*a*,*b*,*c*) and obtain:
$f_i(x,y,z) + g_i(t,v,w) + f_j(x,y,z) + g_j(t,v,w)$

Since (*x*,*y*,*z*) is known, we compute $f_i(x,y,z) + f_j(x,y,z)$ and XOR it with the previous result, obtaining:
$g_i(t,v,w) + g_j(t,v,w)$

Since, by the choice of the 7-member subset $g_i(t,v,w) + g_j(t,v,w)$ is invertible we can obtain (*t*,*v*,*w*), then $g_i(t,v,w)$ or $g_j(t,v,w)$ and then by using one of the redundant packets finally (*a*,*b*,*c*).

The same reasoning works when (*t*,*v*,*w*) is received with two redundant packets.

The case is obvious when we are receiving two information packets with a redundant packet: $(a,b,c) + f_i(x,y,z) + g_i(t,v,w)$, since (*a*,*b*,*c*), $f_i(x,y,z)$ and $g_i(t,v,w)$ are all invertible.

It is more complicated when (*a*,*b*,*c*) is received with two redundant packets:

We have shown that by applying any inverse function to any other invertible packet we obtain always another invertible packet

if

$$f^{-1}(f(x,y,z)) = (x,y,z)$$

where $(x,y,z)\in F$

then

$$f^{-1}(t,v,w) \in F$$

for any $(t,v,w) \in F$

F is the set of all 168 invertible packets

The block of redundant packets is represented by a pair of two 7-tuples

$$\begin{pmatrix} f_1 & f_2 & \dots & f_7 \\ g_1 & g_2 & \dots & g_7 \end{pmatrix}$$

Where $\{f_1 \quad f_2 \quad \dots \quad f_7\}$ is one of the possible 192 members of G (such that $f_i + f_j$ is also in F, for any $i \neq j$) and $(g_1 \quad g_2 \quad \dots \quad g_7)$ is any re-ordering of a member of the same set G.

From all possible $\#(\mathrm{G}) \cdot \#(\mathrm{G}) \cdot 7!$ combinations (where #(G)=192) the codeword can recover information when (a,b,c) survived with two redundant packets, only if:

$$\{f_1^{-1}(g_1) \quad f_2^{-1}(g_2) \quad \dots \quad f_7^{-1}(g_7)\} \in G$$

If we received the following three packets:

(a,b,c)

$(a,b,c) + f_i(x,y,z) + g_i(t,v,w)$

$(a,b,c) + f_j(x,y,z) + g_j(t,v,w)$

We obtain these two:

$f_i(x,y,z) + g_i(t,v,w)$

$f_j(x,y,z) + g_j(t,v,w)$

Then these two:

$f_i^{-1} \cdot f_i(x,y,z) + f_i^{-1} \cdot g_i(t,v,w) = (x,y,z) + f_i^{-1} \cdot g_i(t,v,w)$

$f_j^{-1} \cdot f_j(x,y,z) + f_j^{-1} \cdot g_j(t,v,w) = (x,y,z) + f_j^{-1} \cdot g_j(t,v,w)$

Then this one:

$f_i^{-1} \cdot g_i(t,v,w) + f_j^{-1} \cdot g_j(t,v,w)$

And since

$$\{f_1^{-1}(g_1) \quad f_2^{-1}(g_2) \quad \dots \quad f_7^{-1}(g_7)\} \in G$$

then

$f_i^{-1} \cdot g_i(t,v,w) + f_j^{-1} \cdot g_j(t,v,w) \in F$

Therefore we can recover (t,v,w) and successively (x,y,z)

Assuming that $f_1 = g_1$ =1 we obtained 152 pairs of 7-tuples (out of 46080 possible candidates)

$$\begin{pmatrix} f_1 & f_2 & \cdots & f_7 \\ g_1 & g_2 & \cdots & g_7 \end{pmatrix}$$

Satisfying the following constraint for successful decoding when (*a*,*b*,*c*) survives with any two redundant packets:

$$\{f_1^{-1}(g_1) \quad f_2^{-1}(g_2) \quad \cdots \quad f_7^{-1}(g_7)\} \in G$$

When receiving only redundant packets …

Take (*i*,*j*,*k*) triplet from the 7 redundant packets and take two pairs from this triplet, e.g (*i*,*j*) and (*i*,*k*).

We can eliminate (*a*,*b*,*c*) composant and obtain these two packets:

$f_i(x,y,z) + f_j(x,y,z) + g_i(t,v,w) + g_j(t,v,w)$

$f_i(x,y,z) + f_k(x,y,z) + g_i(t,v,w) + g_k(t,v,w)$

Since $\{f_1 \quad f_2 \quad \cdots \quad f_7\}$ is in *G* (7-member subsets, such that the XOR of any pair from it is invertible),

$f_i(x,y,z) + f_j(x,y,z)$ and $f_i(x,y,z) + f_k(x,y,z)$ are in *F* (162 invertibles)

Similarly

$g_i(t,v,w) + g_j(t,v,w)$ and $g_i(t,v,w) + g_k(t,v,w)$ are also in *F*

Thus

$(f_i + f_j)^{-1} \cdot (g_i + g_j)$ and $(f_i + f_k)^{-1} \cdot (g_i + g_k)$ are in *F* as well

If we find

$$\begin{pmatrix} f_1 & f_2 & \cdots & f_7 \\ g_1 & g_2 & \cdots & g_7 \end{pmatrix}$$

Such that any triplet (*i*,*j*,*k*) contains a pair, e.g (*i*,*j*) and (*i*,*k*), such that

$(f_i + f_j)^{-1} \cdot (g_i + g_j) + (f_i + f_k)^{-1} \cdot (g_i + g_k)$ is in *F*, then we have a (10,3)-code

(The two other possible pairs of the triplet are (*i*,*j*) and (*j*,*k*) or (*i*,*k*) and (*j*,*k*))

80 out of 152 candidates satisfied this triplet constraint

Pair of the following tuple:

11 73 140 167 198 292 323

With any of these 10 tuples

(11,140,198,73,292,323,167)   (11,198,323,140,167,73,292)
(11,140,292,198,323,167,73)   (11,292,167,198,73,323,140)
(11,167,73,323,140,198,292)   (11,292,323,73,140,167,198)

(11,167,198,292,323,73,140)   (11,323,73,292,167,140,198)
(11,198,292,323,73,140,167)   (11,323,167,140,292,198,73)

Is an example of a (10,3)-code
(As everywhere, the numbers are IDs of invertible packets, from here)

All possible 80 pairs of tuples (always assuming that $f_1 = g_1 = 1$) are given here

Note that we exceed the limit of Reed-Solomon code $2^3 - 1$ by 3 and the usual limit of MDS codes $2^3 + 1$ by 1, since our codeword can be as long as 10 packets, with *s=3*.

AMPL programs generating the examples

- Step1
- Step2
- Step3
- Data

*   *   *

US – Mirror
CH – Mirrors

Relevant links:

051025-erasure-resilient
051027-erasure-9-2-resilient