Erasure resilient MDS code with four redundant packets

Emin Gabrielyan
EPFL / Switzernet Sàrl
2005-11-03

HTML – HTM (MS) – PDF – DOC

We are trying to build (11, 7), (10, 6) and (9, 5) MDS codes

Given are:

- 7, 6 or 5 information packets
- 4 redundant packets
- Packet sizes are identical and are divisible by 3, minimum 3 bits
- Information must be retrieved if number of losses does not exceed 4

We must check for which numbers of information packets we can build an MDS code.

Let (*a*,*b*,*c*) be a packet where *a*, *b* and *c* are its first, second and third portions. Let *f* be a function which applied to a packet (*a*,*b*,*c*) forms another packet of the same size, whose first, second and third elements are XOR results of some subsets given from {*a*,*b*,*c*}. Example: $f(x, y, z) = (x+y, z, x+z)$, where operation + is XOR.

We are interested in only invertible functions. There are 168 such functions producing 168 invertible packets. Each function can be represented by a binary 3 by 3 matrix.

Four redundant packets are constructed as follows

$$\sum_{i=1}^{k}(x_i, y_i, z_i)$$

$$\sum_{i=1}^{k} f_i(x_i, y_i, z_i)$$

$$\sum_{i=1}^{k} g_i(x_i, y_i, z_i)$$

$$\sum_{i=1}^{k} h_i(x_i, y_i, z_i)$$

where *k* is the number of information packets, i.e. is equal to 7, 6 or 5.
f, *g* and *h* are vectors whose elements are from the list of 168 invertible functions

Restoring two information packets from (1, *f*), (1, *g*) and (1, *h*)

In case, two information packets *i*, *j* are lost and we received the first and the second redundant packet (the other two are also lost). Then if $f_i^{-1} \cdot f_j(x_j, y_j, z_j) + (x_j, y_j, z_j)$ is invertible for any pair of *i* and *j* we can restore (x_j, y_j, z_j) and successively (x_i, y_i, z_i).

Similarly for the cases when two information packets must be restored from the first and third (g-redundant) packets or from the first and fourth (h-redundant) packets.

In the set of 168 invertible functions, there are 4032 subsets of the size of 5-functions, 1344 subsets of the size of 6-functions and 192 subsets of the size of 7-functions, for which the above condition ($f_i^{-1} \cdot f_j + 1$ is invertible) holds for any pair of the subset.

Restoring two information packets from (f, g)

Let us now examine valid combinations of f and g vectors. For the sizes of 5, 6 and 7 functions there are $4032 \times 4032 \times 5!$, $1344 \times 1344 \times 6!$ and $192 \times 192 \times 7!$ possible pairs of f and g vectors. An (f, g) pair is valid only if for any two i and j (the lost packets) the following function:

$$f_i^{-1} \cdot f_j + g_i^{-1} \cdot g_j$$

is invertible

Restoring three information packets from (1, f, g)

Additionally, an (f, g)-pair is valid only if it can retrieve, together with the first redundant packet, any three lost information packets.

For that the following function must be invertible for any i, j and k:

$$(f_i^{-1} \cdot f_j + 1)^{-1} \cdot (f_i^{-1} \cdot f_k + 1) + (g_i^{-1} \cdot g_j + 1)^{-1} \cdot (g_i^{-1} \cdot g_k + 1)$$

Instead of examining all possible pairs of vectors
$4032 \times 4032 \times 5!$ – for 5 information packets (codeword length = 9)
$1344 \times 1344 \times 6!$ – for 6 information packets (codeword length = 10)
$192 \times 192 \times 7!$ – for 7 information packets (codeword length = 11)

We fixed the f-vector on the first candidate

(11,73,140,167,198) – for 5 information packets
(11,73,140,167,198,292) – for 6
(11,73,140,167,198,292,323) – and for 7

Thus we limited our choice by the following number of pairs
$4032 \times 5!$ – for 5 information packets
$1344 \times 6!$ – for 6
$192 \times 7!$ – and for 7

for 7 information packets we have found 1680 valid (f, g)-pairs
for 6 information packets we have found 1680 valid (f, g)-pairs as well
and for 5 information packets also we have found 1680 valid (f, g)-pairs

Thus (10, 7)-code exists, which is an MDS code.

Choosing *h*-redundant packet, restoring two information packets from (*g*, *h*) and three information packets from (1, *g*, *h*)

For any of 1680 valid (*f*, *g*)-pairs we must examine a valid (*f*, *h*)-pair, thus there are 1680×(1680–1)/2 possible (*f*, *g*, *h*) combinations to examine.

(*g*, *h*)-pair is valid only if:

$g_i^{-1} \cdot g_j + h_i^{-1} \cdot h_j$ is invertible for any two *i* and *j* (the case when two information packets must be retrieved from the *g* and *h*-redundant packets)

and if:

$(g_i^{-1} \cdot g_j + 1)^{-1} \cdot (g_i^{-1} \cdot g_k + 1) + (h_i^{-1} \cdot h_j + 1)^{-1} \cdot (h_i^{-1} \cdot h_k + 1)$ is also invertible for any three lost information packets *i*, *j* and *k* (the case when three information packets must be retrieved from the first redundant packets and from the *g* and *h*-redundant packets).

there are 28224 valid (*g*, *h*)-pairs for 7 information packets
there are also 28224 valid (*g*, *h*)-pairs with 6 information packets
and there are 56448 valid (*g*, *h*)-pairs with 5 information packets

Restoring three information packets from (*f*, *g*, *h*) and four information packets from (1, *f*, *g*, *h*)

Three lost information packets can be retrieved from *f*, *g* and *h*-redundant packets if the following function is invertible

$$(f_i^{-1} \cdot f_j + g_i^{-1} \cdot g_j)^{-1} \cdot (f_i^{-1} \cdot f_k + g_i^{-1} \cdot g_k) + (f_i^{-1} \cdot f_j + h_i^{-1} \cdot h_j)^{-1} \cdot (f_i^{-1} \cdot f_k + h_i^{-1} \cdot h_k)$$

for any three lost information packets *i*, *j* and *k*

Among 28224 (*g*, *h*)-pairs with 7 information packets and 28224 (*g*, *h*)-pairs with 6 information packets there were none, satisfying the above constraint, thus:

(11, 7) MDS code does not exist and
(10, 6) MDS code does not exist (at least with this method)

Additionally vector *h* is valid only if we can also restore any four *i*, *j*, *k* and *l* lost information packets from the four redundant packets. From the four redundant packets we can obtain these three (by eliminating (x_i, y_i, z_i) corposant)

$$(f_i^{-1} \cdot f_j + 1)(x_j, y_j, z_j) +$$
$$(f_i^{-1} \cdot f_k + 1)(x_k, y_k, z_k) +$$
$$(f_i^{-1} \cdot f_l + 1)(x_l, y_l, z_l)$$

$$(g_i^{-1}\cdot g_j+1)(x_j,y_j,z_j)+$$
$$(g_i^{-1}\cdot g_k+1)(x_k,y_k,z_k)+$$
$$(g_i^{-1}\cdot g_l+1)(x_l,y_l,z_l)$$

$$(h_i^{-1}\cdot h_j+1)(x_j,y_j,z_j)+$$
$$(h_i^{-1}\cdot h_k+1)(x_k,y_k,z_k)+$$
$$(h_i^{-1}\cdot h_l+1)(x_l,y_l,z_l)$$

From them we can obtain these two by eliminating the (x_j,y_j,z_j) composant:

$$((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_k+1)+(g_i^{-1}\cdot g_j+1)^{-1}\cdot(g_i^{-1}\cdot g_k+1))(x_k,y_k,z_k)\ +$$
$$((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_l+1)+(g_i^{-1}\cdot g_j+1)^{-1}\cdot(g_i^{-1}\cdot g_l+1))(x_l,y_l,z_l)$$

$$((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_k+1)+(h_i^{-1}\cdot h_j+1)^{-1}\cdot(h_i^{-1}\cdot h_k+1))(x_k,y_k,z_k)$$
$$((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_l+1)+(h_i^{-1}\cdot h_j+1)^{-1}\cdot(h_i^{-1}\cdot h_l+1))(x_l,y_l,z_l)$$

From the above two, we can eliminate (x_k,y_k,z_k) and obtain the below function applied to (x_l,y_l,z_l). If this function is invertible then we can retrieve (x_l,y_l,z_l) and consecutively all other information packets.

$$\begin{aligned}
&((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_k+1)+(g_i^{-1}\cdot g_j+1)^{-1}\cdot(g_i^{-1}\cdot g_k+1)\ )^{-1}\cdot\\
&\qquad((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_l+1)+(g_i^{-1}\cdot g_j+1)^{-1}\cdot(g_i^{-1}\cdot g_l+1))\\
&\qquad\qquad+\\
&((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_k+1)+(h_i^{-1}\cdot h_j+1)^{-1}\cdot(h_i^{-1}\cdot h_k+1)\ )^{-1}\cdot\\
&\qquad((f_i^{-1}\cdot f_j+1)^{-1}\cdot(f_i^{-1}\cdot f_l+1)+(h_i^{-1}\cdot h_j+1)^{-1}\cdot(h_i^{-1}\cdot h_l+1))
\end{aligned}$$

Among 56448 (g, h)-pairs we have found 28224 valid (f, g, h)-triplets with 5 information packets.

Thus (9, 5) MDS code exists with four redundant packets

All valid (1, f, g, h) redundant packets are presented here.

AMPL programs:

Trying to find (11, 7)-code

- step 1
- step 2
- step 3
- step 4
- step 5 and conclusions

Trying to find (10, 6)-code

- step 1
- step 2
- step 3
- step 4

Finding (9, 5) MDS code

- step 1
- step 2
- step 3
- step 4
- step 5

* * *

US – Mirror
CH – Mirror

Relevant links:

051025-erasure-resilient
051027-erasure-9-2-resilient
051031-erasure-10-3-resilient
051101-erasure-9-7-resilient
051102-erasure-10-7-resilient
051103-erasure-9-5-resilient