Description of items of the Master's Thesis Project

Construction of Hadamard $Z_2Z_4Q_8$-codes

Màster interuniversitari de seguretat de les tecnologies de la informació i de les comunicacions.

Author: Pere Montolio Aranda
Thesis director: Jose Rifà Coma

February, 2014

Table of Contents

Included deliverables:

- pmaTFM0214readme (pdf): this document
- pmaTFM0214paper (pdf): Research paper with the master results.
- pmaTFM0214lib (text/sage): Sage librarian with the implementation of algorithms used in the research (see below).
- pmaTFM0214abstract (pdf): Anonymous ready to print extract of the paper abstract.

Sage librarian description:

During execution of this project several algorithms has been implemented in the Sage mathematics environment. These algorithms can be found in the related librarian. All them contains a sage help ready to be displayed inside the environment. Main user functions are:

- Constants:
  - Q8: The Quaternion group.
  - a,b,a2,a3,ab,a2b,a3b: Quaternion elements (short form of a^2*b, ...).
- Functions:
  - c2G(v): makes new G element
  - G2str(x): prints G elements

- Gu(): Element of order 2
- commutator(x,y): commutator
- swapper(x,y): swapper
- wt(bl,x): weight
- T(C): Subgroup of order 2
- K(C): Kernel
- S(C): Lineal spawn
- c_type(C): type of C
- is_hadamard(C,bl): verifies if Hadamard code
- shape(C): shape of C
- analysis(C,bl): utility, main C characteristics

Basic example:

```
load "pmaTFM0214lib.sage"

G=direct_product_permgroups( [Q8]*8 ) # init group structure
bl=[8]*8 # all elements are Quaternions

r1=c2G( [ 1,a,a2,a3,1,a,a2,a3 ] ); # first subgroup generator
s1=c2G( [ 1,b,a2,b,a2,ab,1,ab ] ); # second subgroup generator
C=G.subgroup([r1,s1]) # init subgroup
analysis(C,bl) # main analysis of subgroup properties
```