

info528 : Mathématiques pour l'informatique
TD 3 : codes de Reed-Solomon (QR-codes)

Pierre Hyvernat
 Laboratoire de mathématiques de l'université de Savoie
 bâtiment Chablais, bureau 22, poste : 94 22
 email : Pierre.Hyvernat@univ-savoie.fr
 www : <http://www.lama.univ-savoie.fr/~hyvernat/>

Exercice 1 : préliminaires

Nous allons regarder les codes correcteurs utilisés dans le QR codes dans une version plus simple : au lieu de considérer des octets (entre 0x01 et 0xff), nous allons considérer des demi-octets (entre 0x1 et 0xf).

Les opérations d'addition et de multiplication sont notées \oplus et \otimes . L'addition \oplus est simplement le XOR...

Question 1. Combien valent

- $0x3 \oplus 0x3$
- $0x3 \oplus 0x7$
- $0x3 \oplus 0x4$
- $0x5 \oplus 0xf$

Question 2. Il y a plusieurs manières de calculer (et programmer) la multiplication \otimes

- en considérant les demi-octets comme des polynômes à coefficients booléens, et en effectuant la multiplication *modulo* $X^4 \oplus X \oplus 1$,
- en codant en dur la table de multiplication,
- en utilisant le *logarithme*.

Quelle taille en mémoire fera la table de multiplication pour les demi-octets et pour les octets ?

Question 3. Le demi octet 0x5 (0101 en binaire) représente le polynome $0X^3 \oplus 1X^2 \oplus 0X^1 \oplus 1X^0$, c'est à dire $X^2 \oplus 1$.

- calculez le polynôme obtenu en multipliant $X^2 \oplus 1$ par 0x6,
- divisez le résultat obtenu (division euclidienne) par $X^4 \oplus X \oplus 1$,
- déduisez-en le résultat de $0x5 \otimes 0x6$.

Question 4. Le tableau suivant contient les puissances successive $0x2^n$ pour n variant de 0 à 15. Complétez le.

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

EXP = [0x1 0x2 ___ ___ ___ ___ 0xc 0xb 0x5 ___ 0x7 0xe 0xf 0xd 0x9 ___]

Question 5. Donnez le tableau de LOG des logarithmes correspondants

Question 6. En utilisant les tables de logarithmes / puissances, calculez

- $0x5 \otimes 0x6$
- $0x2 \otimes 0x7$
- $0x3 \otimes 0x7$

Quel est l'inverse de 0x9 ?

Question 7. Parmi les 3 méthodes pour calculer la multiplication, laquelle vous paraît-elle la meilleure ?

Exercice 2 : codage

Nous allons maintenant coder des suites de 3 demi-octets en ajoutant 2 demi-octets...

La suite "0x1 0x0 0x7" sera interprétée comme le polynôme $P = 0x1X^2 \oplus 0x0X \oplus 0x7$.

Question 1. Calculez les coefficients du polynôme $G = (X \oplus 0x2^0)(X \oplus 0x2^1)$.

Question 2. Calculez les coefficients de $M = PG$. Il s'agit du message qu'on enverra.

Question 3. Calculez le reste de $R = X^2P/G$ et le polynôme $M' = X^2P \oplus R$.

Question 4. Calculez les syndromes : $M(0x2^0)$ et $M(0x2^1)$, idem pour M' .

Question 5. On suppose que le coefficient de degré 2 subit une erreur de 0x3, c'est à dire que ce c_2 coefficient est remplacé par $c_2 \oplus 0x3$.

Calculez les syndromes des polynômes M et M' modifiés. Que constatez vous ?