Cyclic Redundancy Check (CRC)

Le codage de détection d'erreurs le plus utilisé est le Cyclic Redundancy Check ou CRC.
Nous allons d'abord démontrer son fonctionnement à l'aide d'un exemple.
Il est important de garder à l'esprit que la première partie de ce texte explique uniquement la mécanique du calcul du CRC. Celles qui sont curieuse de connaître les raisons derrière les étapes que nous allons suivre devront attendre les explication sur la logique derrière ce codage qui seront données dans une version ultérieure du document.

Représentation polynomiale de chaîne de bits

Ce codage représente les chaînes de bits sous la forme de polynômes.

Voici comment on procède pour exprimer des bits comme polynôme :

Pour représenter une chaîne de n bits $c = b_n\, b_{n-1}\, b_{n-2} \ldots b_2\, b_1\, b_0$ sous la forme d'un polynôme nous écrivons des puissances de x sur les bits correspondants de la manière suivante ;

$$\begin{array}{cccccccc} & x^n & x^{n-1} & x^{n-2} & \ldots x^2 & x^1 & x^0 \\ c = & b_n & b_{n-1} & b_{n-2} & \ldots b_2 & b_1 & b_0 \end{array}$$

Nous multiplions ensuite les bits de la chaîne par les termes en x et nous additionnons le résultats:

$$c(x) = b_n x^n + b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \ldots b_2 x^2 + b_1 x + b_0$$

Example

Voyons un exemple. Supposas que nous avons la chaîne $c = 10110101$.
Nous écrivons sur la chaîne les différentes puissances de x :

$$\begin{array}{cccccccc} & x^7 & x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 \\ c = & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{array}$$

Nous multiplions maintenant les bits par les puissances de x et additionnons les produits :

$$c(x) = x^7 + x^5 + x^4 + x^2 + 1$$

Représentation binaire de polynôme (processus inverse)

Dans cette section, nous voulons illustrer le processus inverse à celui de la section précédente, c'et à dire l'expression binaire d'une d'une chaîne qui a été exprimée comme un polynôme.

La conversion de polynôme en chaîne binaire se fait en écrivant d'abord le polynôme incluant les puissances de x manquants multipliés par 0.
Une bonne façon de comprendre ce processus inverse et d'utiliser un exemple.

Prenant le résultat de l'exemple précédent : $c(x) = x^7 + x^5 + x^4 + x^2 + 1$.
Ecrivons maintenant ce polynôme avec les puissance manquantes écrites avec un coefficient 0 :

$$c(x) = x^7 + 0x^6 + x^5 + x^4 + 0x^3 + x^2 + 0x + 1$$

Il suffit maintenant d'écrire la suite de coefficients :

$$c = 1 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0 \quad 1$$

Exercices

Exprimez les chaînes suivantes sous forme polynomiale

a) $c = 0110$
b) $c = 1101$
c) $c = 111$
d) $c = 11010010$

Exprimez les polynôme suivants sous la forme binaire

a) $c(x) = x^7 + x^6 + x^5 + x^4 + x + 1$
b) $c(x) = x^7 + x^6 + x^5 + x^4 + x + 1$
c) $c(x) = + x^4 + x$
d) $c(x) = x^9 + x^6 + x^5 + x$

Le CRC

Le CRC est utilisé de la façon suivante :

1. Une chaîne de bits d'information au niveau de la couche 2 va être transmise
2. Se basant sur les bits d'information et en utilisant un polynôme appelé le "polynôme générateur" $G(x)$, on calcule des bits de contrôle qui sont ajoutés à la fin de la chaîne de bits d'information. La procédure pour le calcul des bits de contrôle sera expliquée plus bas.
3. Le mot code (qui est formé par la concaténation des bits d'information et des bits de contrôle) est transmis.
4. L'entité de la couche 2 au niveau du système récepteur vérifie si le mot code a subit des erreurs ou pas.

Le polynôme générateur

Le calcul du CRC requière que les entités paire de la couche 2 soient d'accord su l'utilisation d'un polynôme appelé le "polynôme générateur" $G(x)$ mentionné à la section précédente.
Il existe de bons et de moins bins polynômes générateurs. Nous en parlerons d'avantage plus tard.

Calcul du CRC et mot code à transmettre

Pour calculer le CRC, on fait au total 5 pas qui seront décrits à l'aide d'un exemple concret en ce qui suit.

Le mot information que nous allons utiliser est $i = 10111$.
Le polynôme générateur que nous allons utiliser est $G(x) = x^3 + x + 1$.

Pas 1 : Exprimez le mot information sus forme polynomiale. Nous avant vu comment le faire précédemment. Le résultat est

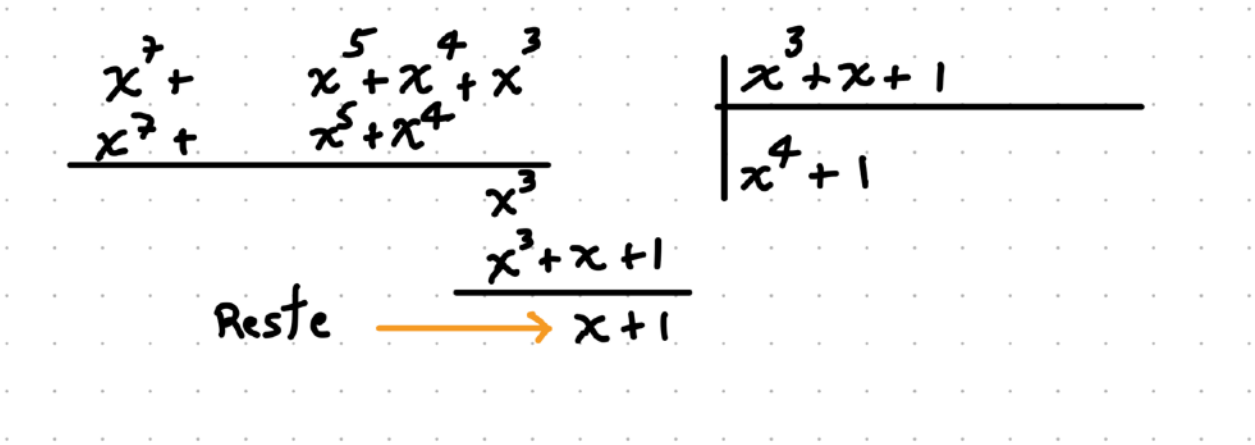
$$i(x) = x^4 + x^2 + x + 1$$

Pas 2 : Multiplier $i(x)$ par x^p où p est le degré du polynôme générateur (le degré de $G(x)$ est 3 dans notre cas).

$$i(x)x^p = (x^4 + x^2 + x + 1)x^3 = x^7 + x^5 + x^4 + x^3$$

Pas 3 : Diviser $i(x)x^p$ par $G(x)$ et trouve le reste de la division.
$x^7 + x^5 + x^4 + x^3 \div x^3 + x + 1$

Pour effectuer cette division, nous commençons par diviser le term avec le plus haut exposant dans le dividend (dans ce cas-ci c'est x^7) par le term avec le plus haut exposant dans le diviseur (dans ce cas-ci c'est x^3). La division a été expliquée en classe. Ci-dessous le résultat. Vous pouvez bien-sûr demander au personnel enseignant si vous avez des doutes concernant la procédure qui sera évaluée au travail écrit.



Le reste est donc $Reste(x) = x + 1$

Pas 4 : Additionner $i(x)x^p$ et le reste $Reste(x)$. Le résultat et le mot code à transmettre mais pour l'instant exprimé sous forme polynomiale.

$$c(x) = i(x)x^p + Reste(x) = x^7 + x^5 + x^4 + x^3 + x + 1$$

Pas 5 : Exprimer $c(x)$ sous forme binaire.
Nous avons vu précédemment comment passer de la forme polynomiale en forme binomiale.
Le résultat pour $c(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ est :

$c = 10111011$

On remarque que le mot code est composé de deux parties, le mot information $i = 10111$ suivi de trois bits de contrôle 011. Ces trois bits de contrôle sont appelé le CRC. Le nombre de bits de contrôle est toujours égal au degré du polynôme générateur qui, dans ce cas-si, est 3.

Comment détermine-t-on à la réception s'il y a eu des erreurs ?

Lorsque le mot-code est reçu, la procédure pour savoir s'il y a eu des erreurs est simple. On divise le mot code reçu par le polynôme générateur et or regarde le reste de la division. Si le reste est 0, on conclut quel n'y a pas eu d'erreur. Si au contraire, les reste est différent de 0, la trame reçue est considérée comme erronée et elle est écartée.

Voyons ceci avec un example. Le mot code transmis dans l'exemple de la section précédente est $c = 10111011$. Supposons qu'aucune erreur ne s'est produite. Dans ces conditions, le mot code reçu c' est identique au mot code transmis :

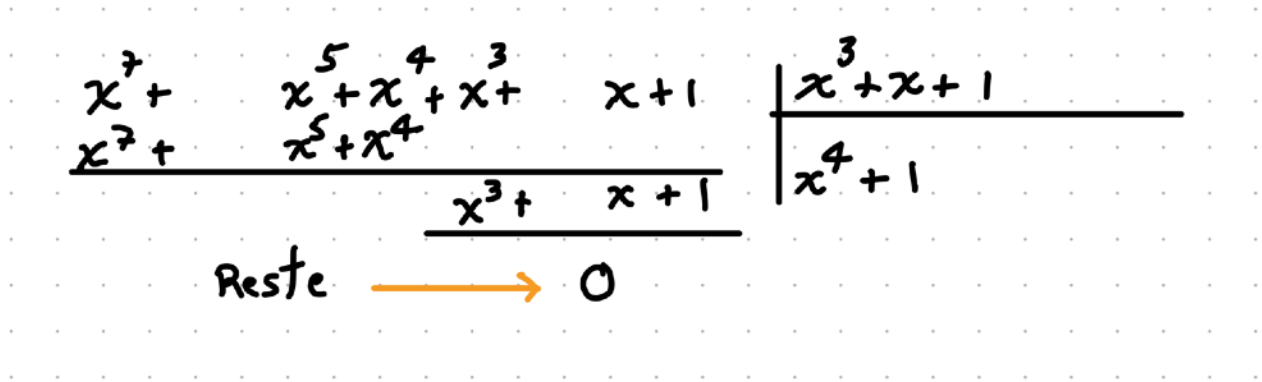
$c' = 10111011.$

Selon la procédure expliquée tout à l'heure, nous devons diviser $c'(x)$ par $G(x)$ et observer le reste $Reste(x)$.

Exprimons d'abord c' sous forme polynomiale (nous avons déjà le résultat à la section précédente puisque $c'(x) = c(x)$ dans le cas que nous considérons, sans erreurs) :

$c'(x) = x^7 + x^5 + x^4 + x^3 + x + 1$

Divisons maintenant $c'(x)$ par $G(x)$:



Nous voyons que le reste est égal à 0, ce qui indique qu'il n'y a pas eu d'erreur. Ceci est cohérent avec le fait que nous ayons supposé que le mot code reçu est identique au mot code transmis.

Si le mot code reçu est différent du mot code transmis, le reste de la division ne sera pas égal à 0 et nous pourrons conclure que un ou plusieurs bits ont changé depuis la transmission de c et jusqu'à la réception de c'. Autrement dit, qu'il y a eu des erreurs.

Exercices

a) Trouver le mot code correspondant au mot information $i = 011001$ si le codage CRC est utilisé et le polynôme générateur est $G(x) = x^4 + x + 1$.

b) Si le mot code reçu dans le système du point a) est $c' = 0100010010$, déterminez s'il y a eu des erreurs.