

Leçon 7 - Contrôle des erreurs de transmission

Joël Adépo, UVCi

Table des matières



I - Objectifs	3
II - Introduction	4
III - Différents types de détection d'erreur	5
IV - Détection d'erreur par clé calculée	6
1. Principe de la détection d'erreur par clé calculée	6
2. Technique du bit de parité	6
3. Contrôle de parité par bloc	7
4. Contrôle par code cyclique (CRC)	8
5. Exercice : Exercices	10
V - Détection et correction d'erreur	12
1. Principe	12
2. Exercice	13



Objectifs

A la fin de cette leçon, vous serez capable de :

- Décrire les techniques de détection d'erreur lors d'une transmission
- Décrire les techniques de correction d'erreur.

Introduction



On doit s'assurer lors d'une transmission de données, que les données reçues n'ont pas été altérées durant la transmission. Plusieurs facteurs peuvent modifier le contenu des données. Les uns sont d'origine humaine, le contrôle d'intégrité concerne alors la sécurité des données. Les autres sont d'origine physique, le contrôle d'intégrité porte alors le nom de contrôle d'erreur.

Les rayonnements électromagnétiques, les perturbations propres au système (distorsions, bruit...), des intempéries, des tensions instables peuvent modifier les informations transmises (bits erronés).



Différents types de détection d'erreur

🔑 Définition : Taux d'erreur binaire

On appelle taux d'erreur binaire ou BER (Bit Error Rate) le rapport entre le nombre d'informations (bits) erronées reçues et le nombre d'informations (bits) transmises.

$teb = (\text{nombre bits erronés}) / (\text{nombre de bits transmis})$.

👉 Exemple

Soit à transmettre la suite de bits « 1001101 ». La suite de bits reçu après la transmission est « 1001001 ».

Le message reçu diffère d'*un bit* du message émis. Le nombre de bits émis étant 8 bits, le taux d'erreur binaire est $teb = 1/8 = 0,125$.

Il faut donc être capable de détecter ces erreurs de transmission et si possible les corriger ou demander une réémission des même données.

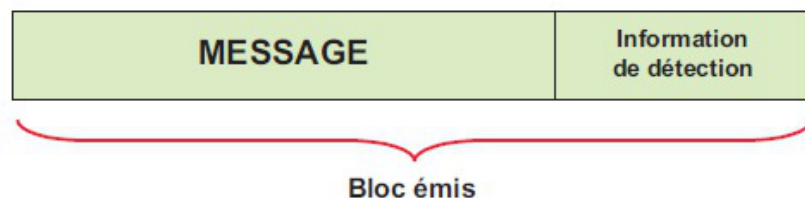
🔑 Définition : Détection d'erreur

On appelle *détection d'erreur* les mécanismes mis en œuvre pour que le système destinataire puisse vérifier la validité des données reçues.

La détection d'erreur repose sur l'introduction d'une certaine redondance dans l'information transmise.

Différentes techniques peuvent être mises en œuvre pour détecter et éventuellement corriger les erreurs. Parmi celles-ci, on a :

- *La détection d'erreur par clé calculée* : Une information supplémentaire (clé) déduite des informations transmises est ajoutée à celles-ci. En réception, le récepteur recalcule la clé. Si le résultat obtenu correspond à la clé reçue, les données sont réputées exactes, sinon le récepteur ignore les données reçues et éventuellement en demande la retransmission (*reprise sur erreur*).



Message avec information de détection d'erreur par clé

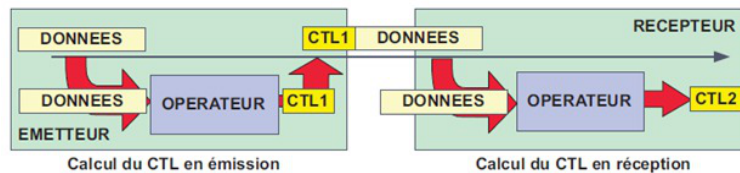
- *La détection et correction d'erreur par code* : cette technique consiste à substituer aux caractères à transmettre, une combinaison binaire différente du codage de base (code autocorrecteur).

Détection d'erreur par clé calculée



1. Principe de la détection d'erreur par clé calculée

Dans les systèmes à clé calculée, une séquence de contrôle (CTL1) déduite d'une opération mathématique appliquée au message à émettre est envoyée avec le message. Le récepteur effectue la même opération. Si le résultat trouvé (CTL2) est identique à la clé calculée par la source (CTL1) le bloc est réputé exact, dans le cas contraire le bloc est rejeté.



Principe de la détection par clé calculée

2. Technique du bit de parité

La technique du bit de parité consiste à ajouter, à la séquence binaire à protéger, un bit, telle que la somme des bits à 1 transmis soit paire (bit de parité) ou impaire (bit d'impairité). L'émetteur et le récepteur s'entendent sur la parité utilisée pour les transmissions les concernant.

1) Parité paire

Si le nombre de 1 est impair, le bit de parité prend la valeur 1 ; sinon il prend la valeur 0.

Exemple

Le bit de contrôle est en gras dans chaque cas :

010010**1**1

0100001**0**

2) Parité impaire

Si le nombre de 1 est impair, le bit de contrôle est 0 sinon le bit de contrôle est 1.

Exemple

Le bit de contrôle est en gras dans chaque cas :

0100101**0**

0100001**1**

3) Fiabilité

S'il existe des erreurs lors de la transmission, la valeur du bit de parité peut aussi changer.

Si la valeur de la parité a changé, il y a eu sûrement erreur de transmission, sinon il se peut qu'il y ait erreurs mais difficile à détecter par ce moyen.

Exemple

Cas 1

Transmis (01001011)

Reçu (01001001)

En parité paire, il y a erreur.

Cas 2

Transmis (01001011)

Reçu (10001011)

En parité paire, la parité est correcte pourtant il y a deux erreurs.

On transmet le caractère complété par le bit de parité. La détection d'erreur est donc sûre lorsque l'altération ne concerne qu'un seul bit et que le bit de parité n'est pas lui-même altéré. Le contrôle est donc peu fiable avec ces techniques.

3. Contrôle de parité par bloc

Pour améliorer le contrôle des erreurs utilisant la parité, on utilise les contrôles par VRC et LRC.

VRC : Vertical Redundancy Check), vérification par redondance vertical

LRC: Longitudinal Redundancy Check, vérification par redondance longitudinal.

Principe du contrôle par bloc

Le contrôle de l'intégrité du bloc se fait de manière verticale (VRC) où on contrôle l'intégrité caractère par caractère et de manière longitudinale (LRC) par bit de même rang dans les caractères.

Exemple

le mot « OSI », avec un caractère codé sur 7 bits.

Parité paire

O	1	0	0	1	1	1	1	1	
S	1	0	1	0	0	1	1	0	
I	1	0	0	1	0	0	1	1	
	1	0	1	0	1	0	1	0	LRC
								VRC	

Mot OSI et les contrôles VRC et LRC

On transmet chaque caractère complété par le code de parité du caractère. Puis à la fin, on transmet le caractère LRC du bloc.

Caractère à transmettre	bit de parité	Caractère à transmettre	bit de parité	...	Caractère LRC	bit de parité
-------------------------------	---------------------	-------------------------------	---------------------	-----	------------------	---------------------

*Exemple de transmission de mot**Contrôle des erreurs à la réception*

Cas 1 avec une erreur : Les bits reçus sont ci-dessous, avec une erreur de transmission en gras dans le caractère O.

O	1	0	0	1	0	1	1	1	
S	1	0	1	0	0	1	1	0	
I	1	0	0	1	0	0	1	1	
	1	0	1	0	1	0	1	0	LRC
								VRC	

Bits reçus avec une erreur

La parité de la première ligne et celle de la cinquième colonne ne correspondent pas aux éléments correspondants des VRC et LRC. Il y a eu erreur de transmission. Cette erreur est située à la position (1 ;5) dans le tableau de données.

Une erreur par caractère est aussi détectable et on peut les corriger en supposant que les bits de contrôle (colonne VRC et ligne LRC) ne sont pas altérés.

Cas 2 avec deux erreurs de transmission: Les bits reçus sont dans le tableau ci-dessous, avec deux erreurs de transmission.

Dans ce cas, le bit de parité est correct, donc VRC est correct. C'est les bits LRC qui ne correspondent pas. Mais on ne pourra pas localiser les erreurs. On pourra juste trouver les deux colonnes comportant des erreurs. Ici, c'est les colonnes 3 et 5.

O	1	0	1	1	0	1	1	1	
S	1	0	1	0	0	1	1	0	
I	1	0	0	1	0	0	1	1	
	1	0	1	0	1	0	1	0	LRC
								VRC	

Bits reçus avec deux erreurs

4. Contrôle par code cyclique (CRC)

1) Principe

Une trame ou ensemble de trames de bis est considéré comme un polynôme dont les coefficients des termes sont des valeurs de bits.

Par exemple :

Trame : 1101011 sera représentée par $X^6 + X^5 + X^3 + X + 1$.

$P(X) = X^6 + X^5 + X^3 + X + 1$ est un polynôme représentant la trame.

- On utilise un polynôme générateur $G(X)$ avec lequel Emetteur et Récepteur se sont entendus pour tout envoi et réception. On note k le degré de G .
- Pour permettre une division, on décale $P(X)$ vers la gauche de d^0P+k . On obtient le polynôme $T(X)$.
- On divise (en arithmétique booléenne) $T(X)$ par $G(X)$ et on retient le reste $R(X)$ de cette division
- On remplace les k bits à 0 de $T(X)$ par les coefficients de $R(X)$. Cela donne la trame $T'(X)$ à émettre.

Remarque : En arithmétique booléenne, l'addition et la soustraction sont la même opération.

Addition			Soustraction		
+	0	1	−	0	1
0	0	1	0	0	1
1	1	0	1	1	0

Addition et soustraction

Exemple

Exemple : Soit à transmettre la trame 1101011011.

$$P(X) = X^9 + X^8 + X^6 + X^4 + X^3 + X + 1.$$

Le polynôme générateur choisi est $G(X) = X^4 + X + 1$ (10011) et $d^0G = k = 4$.

Le nouveau message est 11010110110000.

Ce nouveau message est représenté par $T(X) = P(X) * X^4 = X^{13} + X^{12} + X^{10} + X^8 + X^7 + X^5 + X^4$.

On effectue ensuite la division par G .

Le reste obtenu est $R(X) = X^3 + X^2 + X$ qui correspond à 1110.

Le message final à transmettre est 11010110111110 correspondant à $T'(X) = X^{13} + X^{12} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^3 + X^2 + X$.

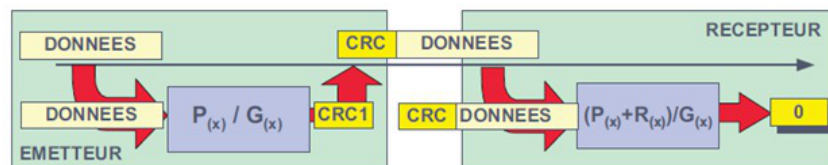
A la réception, le récepteur divise $T'(X)$ par $G(X)$ et s'attend à trouver un polynôme divisible par $G(X)$ (reste 0). Si le reste est 0, on estime qu'il n'y a pas eu erreur de transmission ; sinon il y a eu erreur.

Ce qui est envoyé est donc $T'(X)$. $G(X)$ est déjà connu par le destinataire.

Remarque

$T'(X) = 11010110111110$ et $G(X) = 10011$

Après la division de $T'(X)$ et $G(X)$, on trouvera que le reste est nul.



Exemple de contrôle de message

Remarque

Quelques polynômes générateurs

CRC-12 : $X^{12} + X^{11} + X^3 + X^2 + X + 1$

CRC-16 : $X^{16} + X^{15} + X^2 + 1$ ou $X^{16} + X^{12} + X^5 + 1$.

5. Exercice : Exercices

Exercice : Question 1

La détection d'erreur dans une transmission permet :

Choisir une réponse

- ☐ A) D'éviter la transmission de bits erronés
- ☐ B) De vérifier que les bits reçus sont bien ceux qui ont été émis
- ☐ C) De déterminer les bits en erreur dans une transmission et de les corriger.

Exercice : Question 2

Un BER de 10^{-9} signifie que :

Choisir une bonne réponse

- ☐ A) Sur 10^{-9} bits transmis, il y a un bit erroné
- ☐ B) Sur 10^9 bits transmis, il y a un bit erroné
- ☐ C) Sur tous les bits transmis, il y a 10^9 bits erronés.

Exercice : Question 3

On veut transmettre le mot UVCI. On a en binaire :

U : 1010101

V : 1010110

C : 1000011

I : 1001001

Après l'ajout du bit de contrôle au caractère U (le bit de contrôle étant en gras), on a la suite de bits suivante :

10101011.

Quelle est la technique de détection d'erreur par contrôle de parité utilisée?

- ☐ A) Parité paire
- ☐ B) Parité impaire

Exercice : Question 4

Toujours dans le mot UVCI de la question 3, quelle est la suite de bits à émettre pour la lettre C en ajoutant le bit de contrôle avec la parité paire ?

- ☐ A) 10000111
- ☐ B) 10000110

Exercice : Question 5

Voici les tableaux représentant les bits émis et bits reçus avec un contrôle par blocs, utilisant la parité paire.

Y'a-t-il eu erreur de transmission si on suppose que les bits de contrôle ne sont pas erronés?

Bits émis

U	1	0	1	0	1	0	1	0	
V	1	0	1	0	1	1	0	0	
C	1	0	0	0	0	1	1	1	
I	1	0	0	1	0	0	1	1	
	0	0	0	1	0	0	1	0	LRC
								VRC	

Bits reçus

U	1	0	1	0	1	0	1	0	
V	1	1	1	0	1	1	0	0	
C	1	0	0	0	0	1	0	1	
I	1	0	0	1	0	0	1	1	
	0	0	0	1	0	0	1	0	LRC
								VRC	

- ☐ A) oui car le VRC n'est pas correct
- ☐ D) non car le VRC est correct
- ☐ E) non car le LRC est correct
- ☐ F) non car le VRC et le LRC sont corrects.

Détection et correction d'erreur



1. Principe

La détection et la correction des erreurs sont indispensables sur les supports de mauvaise qualité ou pour des applications qui demandent le transport de données précieuses.

Les deux grandes possibilités de reprise sur erreur sont :

- l'envoi de l'information en redondance
- l'utilisation d'un seul code détecteur d'erreur.

1) Envoi de l'information en redondance

Cette technique permet de détecter et de corriger les erreurs dans un même temps.

2) Utilisation d'un code détecteur d'erreur

Cette technique permet de récupérer les trames en erreur et de demander leur retransmission.

Un code à la fois détecteur et correcteur d'erreur nécessite d'envoyer en moyenne la moitié de l'information transportée en plus. Pour envoyer par exemple 2000 bits en sécurité, il faut émettre 3000 bits au total.

3) Correction d'erreur

La détection d'erreur suivie d'une transmission est la solution la plus utilisée en matière de transmission.

La détection et la correction des erreurs sur le même temps est souvent utilisée.

Parmi les algorithmes permettant de corriger les erreurs, on peut citer :

- la technique simple qui consiste à envoyer trois fois la même information et à choisir au recepateur l'information la plus probable.
- la technique FEC (Forward Error Correction) utilisant des algorithmes plus complexes.

Ces techniques demande un débit beaucoup plus important car on ajoute au message de l'information redondante.

2. Exercice

Exercice : Question 1

La correction d'erreur consiste à :

- ☐ A) Demander une retransmission de la trame contenant des erreurs
- ☐ B) Détecter et corriger dans un même temps la trame contenant des erreurs
- ☐ C) Ignorer la trame contenant des erreurs
- ☐ D) Demander une retransmission de la trame contenant des erreurs ou détecter et corriger dans un même temps la trame contenant des erreurs

Exercice : Question 2

Choisissez le cas où la détection et la correction d'erreur est peu exigée :

- ☐ A) Application multimédia sur support avec BER de 10^{-9} car elle est exigeante en temps.
- ☐ C) transmission de données bancaires