THÈSE

présentée à

L'UNIVERSITE DES SCIENCES ET TECHNIQUES DE LILLE FLANDRES ARTOIS

pour obtenir le titre de

DOCTEUR EN ELECTRONIQUE

par

Abdel Hadi OUADGHIRI

Maître es Sciences

SUR LES CONDITIONS D'UTILISATION DES CODES DETECTEURS D'ERREURS DANS LES TRANSMISSIONS NUMERIQUES NECESSITANT UNE SECURITE QUASI ABSOLUE

Applications aux systèmes de transports et en particulier aux métros souterrains.

Corrections faites après avis du jury

Soutenue le 24 Juin 1986 devant la Commission d'Examen

Membres du Jury :	MM.	R.	GABILLARD	Président
		F.	LOUAGE	Rapporteur
		Y.	DAVID	Rapporteur
		J.F.	DHALLUIN	Invité
		B.	GUIEU	Invité
		C.	PONTIER	Invité

A mes Parents.

En témoignage de mon plus profond attachement et en reconnaissance de tout ce qu'ils ont fait pour moi

A mes frères, mes soeurs,

Vous avez été pour moi un soutien précieux durant toutes mes études. Je vous serai reconnaissant.

Avec mes souhaits de bonheur.

A la famille Jacquemin.

Avec mes souhaits de bonheur.

A tous mes ami(e)s.

A. Ouadghiri
Hadi

AVANT - PROPOS .

Cette étude a été réalisée au laboratoire de radiopropagation et Electronique de l'Université des Sciences et techniques de Lille sous la direction du Professeur Robert Gabillard .

Je tiens à le remercier pour l'opportunité qu'il m'a offerte en me proposant un sujet aussi passionnant que celui de la sécurité de la transmission numérique et pour l'honneur qu'il me fait en présidant le jury .

Je remercie Monsieur F.Louage , professeur à l'Université de Lille I ainsi que Monsieur Y.David , Directeur de l'Institut National de Recherche pour les Transports et leur Sécurité (I.N.R.E.T.S) qui ont bien voulu juger mon travail et être membres du jury .

Je remercie Monsieur J.F.Dhalluin,ingénieur à l'I.N.R.E.T.S. pour le soutien constant et les multiples conseils qu'il m'a apportés tout au long de ce travail .

Mes remerciements vont également à Monsieur Guieu , chef du service Recherche et Développement du département signalisation de la société Alsthom Atlantique et à Monsieur C.Pontier,ingénieur dans ce service ,pour l'honneur qu'ils me font en participant à mon jury .

Enfin , je remercie tous les membres du laboratoire qui par leur présence m'ont permis de mener à bien ce travail .

SOMMAIRE

INTRODUCTION

GENERALE

INTRODUCTION

Etant donné le développement de la technologie dans le contexte économique actuel , il s'avère de plus en plus important de connaître parfaitement le fonctionnement des différents systèmes à tout moment .

C'est pourquoi il est indispensable de s'intéresser aux échanges d'informations .

Actuellement les transferts d'informations entre les automatismes s'effectuent sous forme de liaisons numériques.
Un système de transmission d'information numérique utilise en tant que canal de transmission des lignes bifilaires , coaxiales ou hertziennes.

Le taux moyen d'erreurs dues aux perturbations de ces lignes est de l'ordre de 10^{-3} à 10^{-5} par bit.

Toutefois , dans la plupart des cas , l'échange des informations s'effectue sans tenir compte de la sécurité de ces dernières .

Or , dans certains domaines d'utilisation , il est indispensable de s'assurer un maximum de sécurité et par conséquent le taux moyen d'erreurs défini précédemment est inacceptable lorsque l'on veut un échange d'informations en sécurité .

Parmi les solutions retenues pour rendre une transmission en sécurité, une consiste à appliquer à l'information avant sa transmission, un codage particulier permettant de détecter à la réception la plupart des erreurs introduites par le support de transmission.

Notre travail vient s'insérer dans ce cadre.

Il s'agit en effet d'étudier les conditions d'utilisation des codes détecteurs d'erreurs dans les transmissions numériques nécessitant une sécurité quasi absolue .

Nous avons appliqué ce concept à deux domaines particuliers dans les transports et nous pensons toutefois que cette étude est applicable à d'autres domaines d'activité qui nécessitent l'échange des informations en sécurité .

Nous exposons dans un premier chapitre le principe général des codes de détection d'erreurs où nous définissons en particulier les codes linéaires et les codes cycliques de détection d'erreurs .

Nous décrivons ensuite dans le deuxième chapitre les conditions à respecter pour obtenir une sécurité de transmission prédéterminée .

Nous définissons ainsi une marge supérieure de la probabilité de non détection d'erreurs . Cette inégalité permet d'atteindre l'objectif de sécurité voulu sans que ceci dépende du code détecteur d'erreurs choisi,ce qui laisse une grande liberté sur le choix du code de détection d'erreurs ,(linéaire , cyclique , arithmétique ,...) .

Les deux derniers chapitres sont consacrés à l'application de cette étude aux systèmes de transport .
Dans le chapitre III , nous nous intéressons à une transmission interne à une rame de métro , commande des portes, tandis que dans le chapitre IV nous étudions une transmission sol-trains en tunnel .

Nous avons pensé qu'il était utile de développer en Annexes des exemples sur les codes de détection d'erreurs, de définir les moyens de mesure des qualités d'une transmismsion de données utilisant un code de détection d'erreur, et enfin de donner des outils mathématiques pour la démonstration de la sécurité de l'information.

C H A P I T R E   I

RAPPELS THEORIQUES ET GENERAUX SUR LES CODES DE DETECTION D'ERREURS .

I-INTRODUCTION .

Un système de transmission de données binaires qui utilise en tant que canal de transmission des lignes bifilaires ou coaxiales ou hertziennes n'est jamais parfait,il est donc inévitable qu'à la réception d'une telle transmission, quelques symboles binaires soient altérés.

Généralement le taux moyen d'erreurs par symbole (Bit) d'un système est de l'ordre de 10^{-3} à 10^{-5} (Réf 2).

Or dans certains domaines ,où il faut satisfaire un objectif de sécurité élevé ,en particulier dans celui des transports ce taux moyen d'erreurs devient inacceptable.

D'où la nécessité d'un code de détection d'erreurs ,capable de protéger les informations de sécurité contre les erreurs de transmission.

II-PRINCIPE GENERAL D'UN CODE DE DETECTION D'ERREURS (Réf 4) .

Le principe général d'un code de détection d'erreurs consiste à ajouter une certaine quantité d'informations supplémentaires à l'information utile proprement dite.
Ces bits d'information supplémentaires sont appelés **"bits de redondance"** ou **"bits de contrôle"**.

Ces bits de contrôle sont déterminés en fonction des bits d'information selon une loi **L** connue du récepteur comme de l'émetteur.

Ceci étant ,le mot obtenu grâce à cette loi **L** fait partie d'un ensemble appelé **"Ensemble des mots du code"**.

Un mot code est ainsi formé de **"m"** bits de contrôle et de **"k"** bits d'information utile.

Le nombre total de bits dans un mot code et donc **"n"**,avec **n=k+m.**

III- MECANISME GENERAL DE DETECTION D'ERREURS .

On se place à la réception où on reçoit un mot .
Si le mot reçu satisfait la loi **L** définie précédemment , on dit que le mot reçu est un " **mot du code**" ou "**mot code**". Dans le cas contraire , on détecte que le mot reçu a été entaché d'erreurs par la voie de transmission .

Dans la suite de notre travail , nous proposerons des codes de détection d'erreurs qui sont susceptibles de protéger l'information transmise contre les erreurs de transmission.

IV-CODES LINEAIRES DE DETECTION D'ERREURS .

IV-1 Définition.

Si la loi **L** de formation du code se réduit à des combinaisons linéaires permettant de déterminer à partir des positions et des valeurs (0 ou 1) des bits d'information **k** , la valeur des bits à placer en position de contrôle **m** ,on aura un code linéaire **L(n , k)** .

IV-2 Représentation matricielle .

Un message binaire non codé "N_i" composé de **k** symboles a_i (pouvant prendre les valeurs 0 ou 1) est représenté sous la forme matricielle :

$$\langle N_i \rangle = \langle a_0 \ldots\ldots a_{k-1} \rangle$$

$\langle N_i \rangle$ est appelée la matrice des symboles d'information utile ou vecteur des symboles d'information .

De même , un mot code M_i formé de **n** symboles binaires a_i est représenté sous la forme matricielle :

$$\langle M_i \rangle = \langle a_0 \ldots a_{k-1} \ldots a_{n-1} \rangle.$$

IV-3 Matrice génératrice d'un code linéaire de détection d'erreurs .

D'après la définition d'un code linéaire , il existe une relation entre l'ensemble de tous les mots d'information utiles N_i et l'ensemble des mots du code M_i .
Cette correspondance peut être établie en définissant un opérateur **g** qui soit tel que l'on ait :

$$g\ (N_i) = M_i\ .$$

Sa structure matricielle est la suivante :

$$< N_i > (\ G\ )_{k,n} = < M_i > \qquad (1)$$

Donc un code linéaire peut être représenté par une matrice de **k** lignes et **n** colonnes .
Cette matrice est appelée " **matrice génératrice** " du code d'ordre (**k** , **n**) .

Remarque : Si le code est systématique , c'est à dire si les bits d'informations, sont groupés ensemble et les bits de contrôle également , alors :

$$< M_i > = < N_i > (\ G\ )_{k,n}$$

$$= < \underbrace{a_o \ldots a_{k-1}}_{\substack{\text{k bits} \\ \text{d'information}}} \underbrace{c_o \ldots c_{m-1}}_{\substack{\text{m bits de} \\ \text{contrôle}}} >$$

avec :

$$(\ G\ )_{k,n} = (\ I_{k,k}\ P_{k,m}\ )$$

où $I_{k,k}$ est la matrice unité d'ordre (k , k)
et $P_{k,m}$ est une matrice d'ordre (k , m) .

IV-4 Matrice de contrôle d'un code de détection d'erreurs .

Soit $< M_i >$ un mot code transmis sur un canal de transmission . A la réception , on reçoit un mot $< M_i' >$.

Ce mot peut être défini par :

$$< M_i' > \; = \; < M_i > + < E_i >$$

$< E_i >$ étant une matrice appelée **"vecteur d'erreur"** représentant les erreurs introduites par le canal de transmission .

Le rôle d'un code de détection d'erreur est de déterminer si $< E_i > = 0$ ou si $< E_i > \, <> \, 0$, c'est à dire si le mot reçu $< M_i' >$ est bien le mot émis $< M_i >$.
Mais en fait , la seule certitude qu'il soit possible d'obtenir est celle que $< M_i' >$ est un mot du code .
Ceci peut signifier soit que $< E_i > = 0$ (il n'y a pas eu d'erreur de transmission) , ou bien que les erreurs ($<E_i> \, <> \, 0$) qui se sont produites ont réussi à transformer un mot du code en un autre mot code .
Dans la suite de notre travail , nous calculerons la probabilité de ce dernier évènement .

Pour déceler si le mot reçu $< M_i' >$ est un mot du code , on calcule à partir des mots reçus et de la loi de codage L (connue du récepteur) , un vecteur indicateur d' erreur $< S_i >$ appelé "syndrome" .
Ceci s'effectue à l'aide d'un opérateur H qui est défini par :

$$H \, (M_i') \; = S_i$$

La structure matricielle de cet opérateur est :

$$< M_i' >(H)^t \; = \; < S_i > \qquad (2)$$

$< S_i >$ est le syndrome d'erreurs comportant m bits .
$(H)^t$ est la matrice transposée de (H) .

La matrice (**H**) est appelée la matrice de contrôle ou matrice de vérification formée de **m** lignes et **n** colonnes .

Remarques: - Si le code est systématique alors :

$$(H)_{m,n} = (-P_{k,m}{}^{t}\ I_{mm})$$

I_{mm} est la matrice unité
et $P_{k,m}{}^{t}$ est la matrice transposée de $P_{k,m}$.

- On montre facilement que :

$$(G) . (H)^{t} = (0)_{k,m}$$

$(0)_{k,m}$ étant la matrice nulle .

IV-5 Mécanisme de détection d'un code linéaire détecteur d'erreurs .

Lors d'une transmission d'un mot **M** , le canal de transmission introduit un bruit caractérisé par :

$$< E_i > = <e_0 \ldots e_j \ldots e_n >$$

avec $e_j = \begin{cases} 0 \text{ si le } j^{\text{ième}} \text{ bit est transmis correctement} \\ 1 \text{ si le } j^{\text{ième}} \text{ bit est changé par le bruit du canal .} \end{cases}$

$< E_i >$ est le vecteur d'erreur .

Le mot reçu est alors : $< M_i'> = < M_i > + < E_i >$

A la réception , le décodeur peut calculer le "**syndrome**" qui est défini par l'équation :

$$< S_i > = < M_i'> (H)^{t}$$

Deux cas peuvent se présenter :

a) - Si le syndrome $< S_i > = 0$ alors le mot reçu a la configuration d'un mot du code , donc aucune erreur n'est décelée .

Ceci peut signifier qu'effectivement aucune erreur ne s'est produite ou bien que les erreurs du canal de transmission ont transformé le mot code émis en un autre mot du code .

b) - Si le syndrome $< S_i > \,<>\, 0$, $< M_i' >$ n'est pas un mot du code , donc le canal a introduit sûrement une erreur $<E_i><>0$.
Dans ce cas , le décodeur signale une détection d'erreur .

<u>IV-6 Procédure de construction d'un code linéaire L(n,k) .</u>

L'expression (2) peut s'écrire :

$$< S_i > = <M_i'> (H)^t \Longrightarrow < S_i >^t = (H) < M_i'>^t$$

La matrice (H) peut s'écrire sous la forme :

$$(H) = (h_o..h_i..h_{n-1})$$

où h_i représente une colonne de la matrice (H) .

Théorème : La distance minimale d'un code linéaire est le poids minimal d'un mot du code non nul .

Remarque : Pour la définition des concepts de "distance" et de "poids" , voir Annexe III .

Soit $< M_i >$ le mot code de poids minimal d , alors :

$$(H) < M_i >^t = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\sum_{i=\emptyset}^{i=n} a_i h_i = 0 \Longrightarrow h_{i1} + h_{i2} + \dots + h_{id} = 0$$

$$h_{id} = hi1 + \dots + hi(d-1) <> 0 .$$

C'est la relation d'indépendance linéaire de (d-1) colonnes de la matrice (H)

théorème :Pour détecter **t** erreurs ,il faut que la distance minimale entre les mots du code satisfasse l'équation :

$$d = t + 1 \quad .$$

Tenant compte de cette condition , les vecteurs colonnes de la matrice **(H)** devront satisfaire les relations suivantes :

$$h_{io} <> 0 \quad \text{pour } i_o = 0,1 \ldots., (n-1)$$

$$h_{io} + h_{i1} <> 0 \quad \text{pour } i_o \text{ , } i_1 = 0,1,2\ldots,(n-1) \text{ et } i_o <> i_1$$

....

$$h_{io} + h_{i1} + \ldots + h_{i(d-2)} <> 0$$

$$\text{pour } i_o \text{ ,} i_1 \ldots, i_{(d-2)} = 0 \text{ ,} \ldots,(n-1)$$

$$i_o \text{ ,} i_1 \ldots, i_{(d-2)} \text{ distincts.}$$

IV-7 Codes linéaires particuliers .

Parmi les codes linéaires , on distingue :

- Les codes de **Hamming**
- Les codes de **Reed - Muller**
- Les codes de **Mac Donald**
- Les codes dérivés des matrices d'**Hadamard** .

Des exemples de codes linéaires sont exposés en Annexe I .

V-CODES CYCLIQUES DE DETECTION D'ERREURS .(Réf : 1 , 2 , 4)

V-1 Définition.

Un code cyclique **C (n,k)** est un code linéaire possédant la propriété suivante :
Toute permutation cyclique d'un mot code est aussi un mot code.

Soit $< M_o >$ un mot code : $< M_o > = < a_o \, a_1 \ldots a_{n-1} >$
alors tous les mots de la forme :

$$< M_i > = < a_i a_{i+1} \ldots a_{n-1} a_o \ldots a_{i-1} >$$

sont aussi des mots codes .

V-2 Représentation polynômiale des codes cycliques .

Nous avons représenté les mots des codes linéaires par des vecteurs .
Une autre possibilité est de considérer les mots codes comme des éléments de l'ensemble des polynômes binaires de degré (n-1) .
Donc un mot code $< M_o > = < a_o \ldots a_{n-1} >$ est représenté par le polynôme binaire suivant :

$$M_o(x) = a_o + a_1 x + \ldots + a_{n-1} x^{n-1}$$
$$\text{modulo } x^n + 1$$

Cette représentation à l'aide des polynômes est très intéressante car les opérations sur les polynômes sont simples .
Bien entendu , la multiplication des polynômes donnera en général un polynôme de degré supérieur à (n-1) , mais il est facile de le réduire modulo un polynôme binaire de degré **n** .

Ainsi la définition du code cyclique peut être la suivante:

Soit un mot du code représenté par le polynôme **M(x)** ; Si **xM(x)** appartient aussi au code , alors celui-ci est un code cyclique .

En effet ,la multiplication du polynôme M(x) par x^i modulo ($x^n + 1$) correspond à i permutations successives des bits de M(x) et par conséquent , $x^iM(x)$ modulo (x^n+1) représente un mot appartenant au code .

V-3 Polynôme générateur.

Rappelons que la matrice génératrice (**G**) d'un code linéaire permet de déterminer tous les mots codes .

Pour un code cyclique , le calcul de la matrice génératrice **(G)** se ramène à la détermination d'un polynôme générateur **g(x)** de degré **m** = (**n-k**) , vérifiant les propriétés suivantes :

Propriété 1 : Tout mot d'un code cyclique **C (n,k)** est un multiple du polynôme générateur **g(x)** de degré **m.**

Propriété 2 : Le polynôme générateur d'un code cyclique **C(n,k)** est un polynôme qui divise ($x^n + 1$).

Remarque : Comme les codes linéaires , les codes cycliques contiennent **(2^k-1)** mots codes et chaque mot code est formé de **n** symboles (n bits) , **k** symboles étant réservés à l'information utile et **m=(n-k)** étant réservés au contrôle .

- Recherche des polynômes générateurs .

Le polynôme générateur d'un code **C (n,k)** est un diviseur de (x^n+1) , donc la recherche des polynômes générateurs susceptibles d'engendrer un code **C (n,k)** commence par la décomposition de (x^n+1) en produits de polynômes irréductibles de la forme :

$$(x^n+1) = m_1(x).m_2(x)...m_t(x)$$

Tous les polynômes irréductibles $m_1(x), m_2(x)$ ..etc sont capables d'engendrer des codes cycliques (n,k) .

Pour la définition d'un polynôme irréductible,voir Annexe II.

V-4 Mise en oeuvre des codes cycliques .

V-4-1 Codage

Lorsque l'on se donne **k** bits qui constituent l'information utile à transmettre , on peut former un mot :

$$< N > = <a_0 \ldots a_{k-1} > .$$

Ce mot est représentable par un polynôme :
$N(x) = a_0x^0 + a_1x^1 + \ldots + a_{k-1}x^{k-1}$ **de degré k-1.**

On obtient le polynôme du code en effectuant le produit $N(x)g(x) = M(x)$.
Cette procédure produit un code non systématique .

Pour obtenir un code cyclique systématique :
1°) On multiplie x^m par $N(x)$ ce qui donne $x^mN(x)$.
2°) On divise $x^mN(x)$ par $g(x)$ et on utilise le reste , changé de signe comme symbole de contrôle.

On peut toujours écrire :

$$x^mN(x) = Q(x)g(x) + C(x)$$

$C(x)$ est un polynôme de degré inférieur à **m** .
Par conséquent , le polynôme $M(x)$ de degré $n=m+k$ défini par : $M(x) = x^mN(x) - C(x) = Q(x)g(x)$ est bien divisible par g(x) et est par suite un polynôme du code .

Les **k** premiers symboles sont des bits d'information utile et les $m=(n-k)$ symboles suivants sont des bits de contrôle .

V-4-2 Décodage ou mécanisme de détection d'erreurs

Comme dans le cas des codes linéaires , on calcule à la réception le syndrome d'erreurs du message reçu .

Soit **M'(x)** le message reçu :

$$M'(x) = M(x) + E(x)$$

E(x) étant le polynôme d'erreurs introduit par le canal de transmission .
A la réception , le décodeur calcule le "syndrome" défini par :

$$S(x) = \text{Reste de} \left\{ \frac{M'(x)}{g(x)} \right\}$$

Si le syndrome n'est pas nul , il y a eu erreur et on a **E(x) <> 0** . Le décodeur signale ainsi une détection d'erreurs .
Si le syndrome est nul , on a la configuration d'un mot du code , donc aucune erreur n'est décelée .
Il n'y a donc pas eu d'erreur ou bien les erreurs qui se sont produites ont transformé le mot code émis en un autre mot du code .

V - 5 CODES CYCLIQUES PARTICULIERS .

- Les codes **B.C.H.** (Bose - Chaudhuri - Hocquenghem ,1960)
- Les codes de **Reed - Solomon** à structure binaire .
- Les codes de **Fire** (1959) .
- Les codes d'**Abranson** .

Pour un exemple de code cyclique , voir Annexe II .

C H A P I T R E I I

_°_°_°_°_°_°_°_°_°_°_

MISE EN EVIDENCE DES CONDITIONS A RESPECTER POUR OBTENIR UNE SECURITE DE TRANSMISSION PREDETERMINEE .

I-DEFINITION DE LA SECURITE PROBABILISTE

La **"sécurité probabiliste"** d'un système de transmission peut se définir à partir de la **"probabilité de non détection d'erreur"** (**PND**).
C'est la probabilité pour que les erreurs aléatoires qui se produisent dans le canal de transmission réussissent à transformer un mot code en un autre mot code .

On se définit un **"objectif de sécurité"** qui est une probabilité de valeur assez petite pour être jugée satisfaisante. Par exemple $q = 10^{-10}$.

Le système de transmission sera dit **"de sécurité"** si :

$(\mathbf{PND}) < q$

(**PND**) est aussi appelée :**"taux d'erreur global par message"** . Une définition plus précise est donnée en Annexe III.
La probabilité **(PND)** dépend de la probabilité élémentaire d'erreur du canal de transmission encore appelé " **Taux d'erreur brut** " et des caractéristiques du code de détection d'erreurs .

II-HYPOTHESES DE TRAVAIL PRISES EN CONSIDERATION .

a) Il faut connaître le nombre **N** de messages à transmettre dont on déduit le nombre de bits d'information utile **k** par la relation :

$$N \leqslant 2^k - 1$$

b) Nous considérons que les erreurs introduites par la transmission se manifestent de façon indépendante sur chacun des bits et sur chaque message transmis .

c) On note par **q "objectif de sécurité"** .

d) On note par **PND** le taux d'erreurs global par message ou probabilité de non détection d'erreurs .

e) On note par **P** , la probabilité d'erreurs par bit de la transmission

f) On note par **n** ,le nombre total de bits dans un mot code.

II-1 Rappel de la définition des erreurs individuelles .

On dit qu'il y a **"erreur individuelle"** lorsque l'on suppose que chaque symbole ou bit transmis est affecté de manière indépendante par les perturbations .
Dans ces conditions , la probabilité d'apparition de **e** erreurs indépendantes dans un message ou dans un mot est :

$$P(e) = C_n^e \, P^e \, (1 - P)^{n-e} \qquad (1) \qquad \text{(Réf 4)}$$

En supposant que les messages sont indépendants , on obtient comme pourcentage moyen de messages faux , la quantité :

$$\frac{\sum_{e=1}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e}}{2^n} \qquad (2)$$

III-MISE EN EVIDENCE DES CONDITIONS A RESPECTER POUR OBTENIR UNE SECURITE DE TRANSMISSION PREDETERMINEE.

Dans ce chapitre , nous allons tenter d'estimer la **sécurité probabiliste** de la transmission .
Cette estimation s'établit au moyen du calcul approximatif qui va suivre en tenant compte au départ de la définition de l'efficacité **E** d'un code de détection d'erreurs (voir Annexe III) soit :

$$E = \frac{\textbf{le nombre moyen de messages faux et détectés}}{\textbf{le nombre moyen total de messages faux}} \qquad \text{(Réf 2)}$$

Avec l'hypothèse du II b) , on peut écrire :

$$E \leqslant \frac{\sum_{e=1}^{e=d-1} C_n^e \, P^e \, (1 - P)^{n-e}}{\sum_{e=1}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e}} \qquad (3)$$

où **d** représente la distance minimale de Hamming entre les mots du code . (Voir définition en Annexe III) .

En effet , pour qu'un mot code transmis soit changé en un autre mot code , (et par conséquent que l'erreur de transmission ne soit pas détectée) , il faut qu'il soit affecté par un nombre d'erreurs individuelles au moins égal à **d** .

L'expression (3) peut encore s'écrire :

$$E < 1 - \frac{\sum_{e=d}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e}}{\sum_{e=1}^{e=n} C_n \, P^e \, (1 - P)^{n-e}}$$

Formule du binôme :

$$(a + b)^n = \sum_{e=0}^{e=n} C_n^e . a^{n-e} . b^e \, .$$

Grâce à cette formule , le dénominateur du deuxième membre de l'expression (3) devient :

$$\sum_{e=1}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e} \;\#\; n.P \qquad \text{pour } P \ll 1 \, .$$

L'expression (3) peut donc s'écrire :

$$E < 1 - \frac{\sum_{e=d}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e}}{nP} \qquad (4)$$

Or, d'après la référence (2) , la relation liant l'efficacité du code et le taux d'erreur global **PND** s'écrit :

$$E \leqslant 1 - \frac{PND}{nP} \quad (5)$$

Des expressions (4) et (5) , on en déduit la valeur suivante pour le taux d'erreur global **PND** :

$$PND \# \sum_{e=d}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e} \qquad (6)$$

Sachant que **"l'objectif de sécurité" q** doit être supérieur au **taux d'erreur global PND** , on doit avoir :

$$q \geqslant \sum_{e=d}^{e=n} C_n^e \, P^e \, (1 - P)^{n-e} \quad .$$

L'expression (6) exprime de façon approchée la valeur du taux d'erreur global **PND** en fonction de la distance minimale entre les mots code **d** , du nombre total des bits dans un mot code **n** et de la probabilité d'erreur par bit introduit par la trans mission **P.**

De même , on peut remarquer que le terme $\sum_{e=d}^{e=n} C_n^e \, P^e(1-P)^{n-e}$ représente un majorant du nombre de messages faux non détectés ,puisque tout le calcul précédent est basé sur l'hypothèse que toutes les erreurs affectant un nombre de bits compris entre **d** et **n** transforment le mot code émis en un autre mot code qui ne sera pas détecté .

Cette hypothèse est évidemment pessimiste .

Si , pendant la transmission d'un mot code de **n** bits ,il se produit **e** erreurs individuelles,(e>d),ceci peut transformer le mot émis en C_n^e mots différents .
Mais parmi ces mots différents , il n'y a eu que $A_e \leqslant C_n^e$ qui appartienne au code .
On peut donc écrire :

$$(PND) = \sum_{e=d}^{e=n} A_e \, P^e \, (1 - P)^{n-e} \qquad (\text{Réf } 25)$$

Malheureusement , on ne peut pas déterminer A_e avant de mettre en oeuvre le code de détection d'erreur choisi .

L'expression (6) contient deux inconnues **d** et **n** .
A la suite d'une série de calculs et de quelques estimations,(Voir Annexe IV) , nous nous ramenons à une seule inconnue **(d/n)** et parvenons à mettre en évidence une des conditions à respecter pour obtenir une sécurité de transmission prédéterminée

$$\frac{|\log_{10} q|}{n} < E\left(\frac{d}{n}, P\right) \qquad (7)$$

où $E\left(\frac{d}{n},P\right) = H(P) - H\left(\frac{d}{n}\right) + \left(\frac{d}{n} - P\right).H'(P)$

H(P) est l'entropie du canal de transmission définie par :

$$H(P) = - P.\log_{10}P - (1-P).\log_{10}(1-P)$$

$$H'(P) = - \log_{10} \frac{P}{1-P}$$

H'(P) est la dérivée par rapport à P de H(P) .
Les valeurs de H(P) et H'(P) se trouvent dans un tableau en Annexe V .
L'inégalité (7) permet donc de lier l'objectif de sécurité **"q"** au rapport **(d/n)** qui est une caractéristique du code de détection d'erreurs utilisé et à la probabilité d'errreurs par bit de la transmission **P** .

Afin d'encadrer le rapport **(d/n)** et de savoir si un code de détection d'erreurs existe pour **n** et **d** fixés , nous avons cherché une autre condition .
Pour cela , nous faisons appel à la marge inférieure de Hamming :

Pour corriger **e** erreurs , il faut que :

$$\sum_{i=0}^{i=e} C_n^i \leqslant 2^{n-k} \qquad (8)$$

e étant la partie entière de **(d-1)/2**

On note la partie entière de **(d-1)/2** par $\left[\frac{d-1}{2}\right]$

La condition (8) est nécessaire pour parvenir à trouver un code de détection d'erreur capable de corriger **e** erreurs mais elle n'est pas suffisante .

L'inégalité (8) peut donc s'écrire :

$$\sum_{i=0}^{i=\left[\frac{d-1}{2}\right]} C_n^i \leqslant 2^{n-k} \qquad (9)$$

L'expresion (9) peut encore s'écrire :

$$\sum_{i=n-\left[\frac{d-1}{2}\right]}^{i=n} C_n^i \leqslant 2^{n-k} \qquad (10)$$

De même on a :

$$\sum_{i=n-\left[\frac{d-1}{2}\right]}^{i=n} C_n^i < \sum_{i=n-\frac{d}{2}}^{i=n} C_n^i \qquad (11)$$

Suite à un calcul développé en Annexe IV , nous parvenons alors à trouver la deuxième condition qui est :

$$\frac{n-k}{n} \geqslant H_2\left(\frac{d}{2n}\right) \qquad (12)$$

avec :

$$H_2\left(\frac{d}{2n}\right) = -\left(\frac{d}{2n}\right).\log_2\left(\frac{d}{2n}\right) - \left(1 - \frac{d}{2n}\right).\log_2\left(1 - \frac{d}{2n}\right)$$

Si on veut obtenir une condition qui soit suffisante , il faut faire appel à la marge de Warchanov -Gilbert :

$$\sum_{i=0}^{i=2e-1} C_n^i < 2^{n-k} \qquad (13)$$

e étant la partie entière de (d-1)/2

L'inégalité (13) peut donc s'écrire :

$$\sum_{i=0}^{i=d-2} C_n^i < 2^{n-k}$$

Comme dans le calcul précédent , nous parvenons alors à trouver une autre condition qui est :

$$\frac{n-k}{n} > H_2\left(\frac{d}{n}\right)$$

avec :

$$H_2\left(\frac{d}{n}\right) = - \frac{d}{n} \operatorname{Log}_2\left(\frac{d}{n}\right) - \left(1 - \frac{d}{n}\right).\operatorname{Log}_2\left(1 - \frac{d}{n}\right)$$

IV-CONCLUSION.

Nous pensons que l'étude mathématique du problème de la sécurité de la transmission telle que nous l'avons développée dans ce chapitre nous a permis de mettre en évidence des conditions à respecter pour obtenir une transmission satisfaisant un objectif de sécurité donné .

Il faut donc s'assurer que les conditions (7) et (12) sont satisfaites avant de mettre en oeuvre un code de détection d'erreurs .

Les expressions (7) et (12) montrent que la sécurité d'une transmission numérique est indépendante du type de codage du code de détection d'erreurs choisi , (indépendante de la formation du code) , ce qui laisse une grande liberté sur le choix du code .

Sous réserve que les relations (7) et (12) entre les données "k","P" et "q" et les caractéristiques "d" et "n" du code soient satisfaites , on peut choisir n'importe quel type de formation de code .

On peut encore dire qu'un code linéaire , cyclique , arithmétique ou autre permet d'atteindre l'objectif de sécurité "q" sous réserve qu'il respecte les relations (7) et (12) et que l'hypothèse d'indépendance des erreurs introduites par le canal de transmission sur les bits individuels soit bien respectée .

Dans ces conditions , la probabilité de non détection d'erreurs (PND) est :

$$\mathbf{PND} < 10^{-n.E(d/n,P)} \qquad (14)$$

C H A P I T R E   I I I

APPLICATION AUX TRANSMISSIONS INTERNES D'UNE RAME DE METRO : COMMANDE DES PORTES .

I INTRODUCTION.

Cette application se situe dans le cadre d'une étude portant sur la possibilité de commander les portes des véhicules d'une rame de métro par microprocesseur .

La structure choisie pour cette commande reposant sur un réseau de microprocesseurs , il est apparu nécessaire d'étudier la sécurité des transferts d'informations entre le calculateur central et les cartes de commande de chacune des portes et de définir un code susceptible de répondre à l'objectif de sécurité fixé pour cette application .

II SITUATION DU PROBLEME.

La structure choisie pour la commande des 6 portes d'un , véhicule consiste en un réseau local de type étoile , (Réf 16 ,18) .
La transmission des informations entre le système central et les cartes de commande est réalisée par des liaisons bifilaires .

Rappel sur le réseau : Voir Figure I

Les messages envoyés du système central vers les cartes de commande de porte ou télécommande sont au nombre de 7 :

- **TCO** : Télécommande d'ouverture
- **TCF** : Télécommande de fermeture
- **TCP** : Télécommande de préparation
- **TCI** : Télécommande d'initialisation
- **TCA** : Télécommande véhicule en ligne
- **TCM** : Télécommande véhicule en station
- **TCT** : Télémesure .

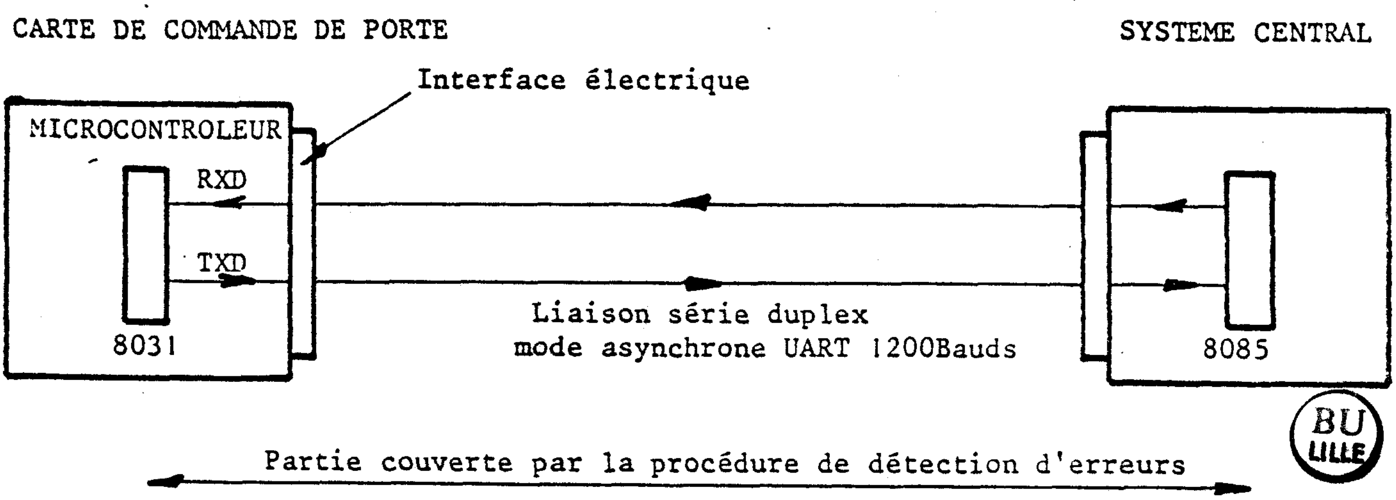
Ces messages sont complétés par le numéro de la porte à laquelle ils s'adressent et sont diffusés simultanément sur les 6 cartes de commande de porte . Seule la porte qui reconnaît son numéro obéira au message .

Les messages envoyés par les cartes de commande vers le système central , appelés messages de télémesure , sont au nombre de 50 .
Une partie des messages de télémesure est utilisée par l'exploitation (indications : porte ouverte ,porte fermée porte verrouillée) .
Une autre partie indique l'état de fonctionnement des systèmes de porte ; ces messages servent d'aide à la maintenance .

Dans ce qui suit , nous proposons un code de détection d'erreurs applicable aux messages de télécommande et aux messages de télémesure .

III-DESCRIPTION D'UNE LIAISON .

Chaque liaison du réseau peut être représentée individuellement par le schéma suivant :



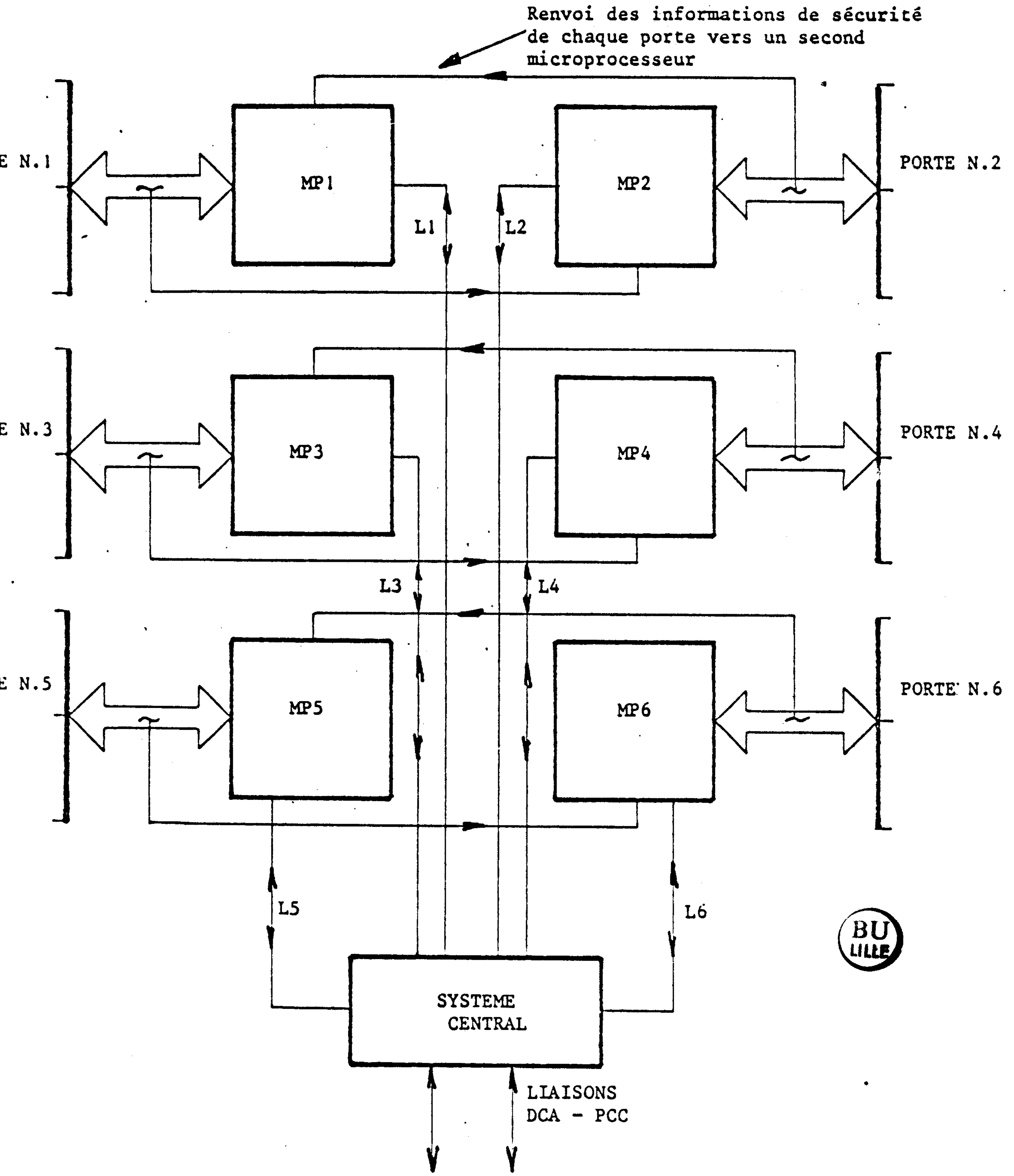


Figure 1 SCHEMA DE PRINCIPE DU RESEAU LOCAL
DE COMMANDE-CONTROLE DE PORTE EN SECURITE
BILAN DE LIAISON

Les procédures de détection d'erreurs que nous allons mettre en oeuvre couvrent l'ensemble :" liaison et interfaces électriques d'attaque de la transmission." .

Les défaillances entraînant un taux d'erreurs de transmission anormal : coupure , court-circuit , dérive des interfaces ou diaphonie , sont détectées par ailleurs.

D'autre part , nous considérons dans ce qui va suivre , que les blocs fonctionnels (UART) appartenant aux systèmes microprocesseurs placés aux deux extrêmités de la liaison sont en fonctionnement correct .

IV ETABLISSEMENT DU CODAGE DES INFORMATIONS DE TELEMESURE ET DE TELECOMMANDE D'UN MECANISME DE PORTE .

IV-1 Détermination du nombre de bits d'information

A partir de l'étude fonctionnelle du système , nous avons vu que **7** messages de télécommande suffisaient à piloter un microprocesseur de commande de porte .

De par la constitution physique du réseau d'interconnexion au sein d'un véhicule , il faut utiliser **42** messages différents (pour 6 portes) .

De même , nous avons vu qu'il fallait **50** messages différents pour rendre compte de toutes les télémesures .

De par l'indépendance dans le traitement logiciel des messages et des unités de décodage (Hard) , on peut envisager d'utiliser la même partition de messages codés auxquels on accordera , selon le sens de transfert , une signification particulière .

Soit **k** le nombre de bits d'information . On a :

$$2^5 < 42 < 2^6 \Longrightarrow k = 6$$

IV-2 Hypothèses prises pour la recherche d'un code .

Ces hypothèses sont les suivantes :

- Nous considérons que les erreurs introduites par la transmission se manifestent de façon indépendante .

- Afin de rendre la chaîne de transmission en sécurité , la probabilité de non détection d'erreurs doit être inférieure à 10^{-10} , " **objectif de sécurité** " .

La probabilité d'erreur moyenne par bit **P** est de l'ordre de 10^{-3} .

IV-3 Calcul du nombre de bits de contrôle et de la distance minimale entre les mots du code .

En tenant compte de ces hypothèses , nous pouvons utiliser les deux conditions (7) et (12) de la deuxième partie pour déterminer la distance entre les mots du code et le nombre de bits de contrôle **m** , dans un mot du code .

En répondant à l'objectif de sécurité fixé (q = 10),on a:

$$\frac{|\log_{10} q|}{n} \leqslant E\left(\frac{d}{n}, P\right)$$

$$\frac{n-k}{n} \geqslant H_2\left(\frac{d}{2n}\right)$$

Nous traçons les fonctions $E\left(\frac{d}{n}, P\right)$, $\frac{|\log_{10} q|}{n}$, $\frac{n-k}{n}$ et $H_2\left(\frac{d}{2n}\right)$ dans un plan d'ordonnée 0,1 et d'abscisse représentant le rapport $\left(\frac{d}{2n}\right)$.

Pour satisfaire le problème , plusieurs valeurs de **n** ont été essayées . Voir figures 2 , 3 , 4 .

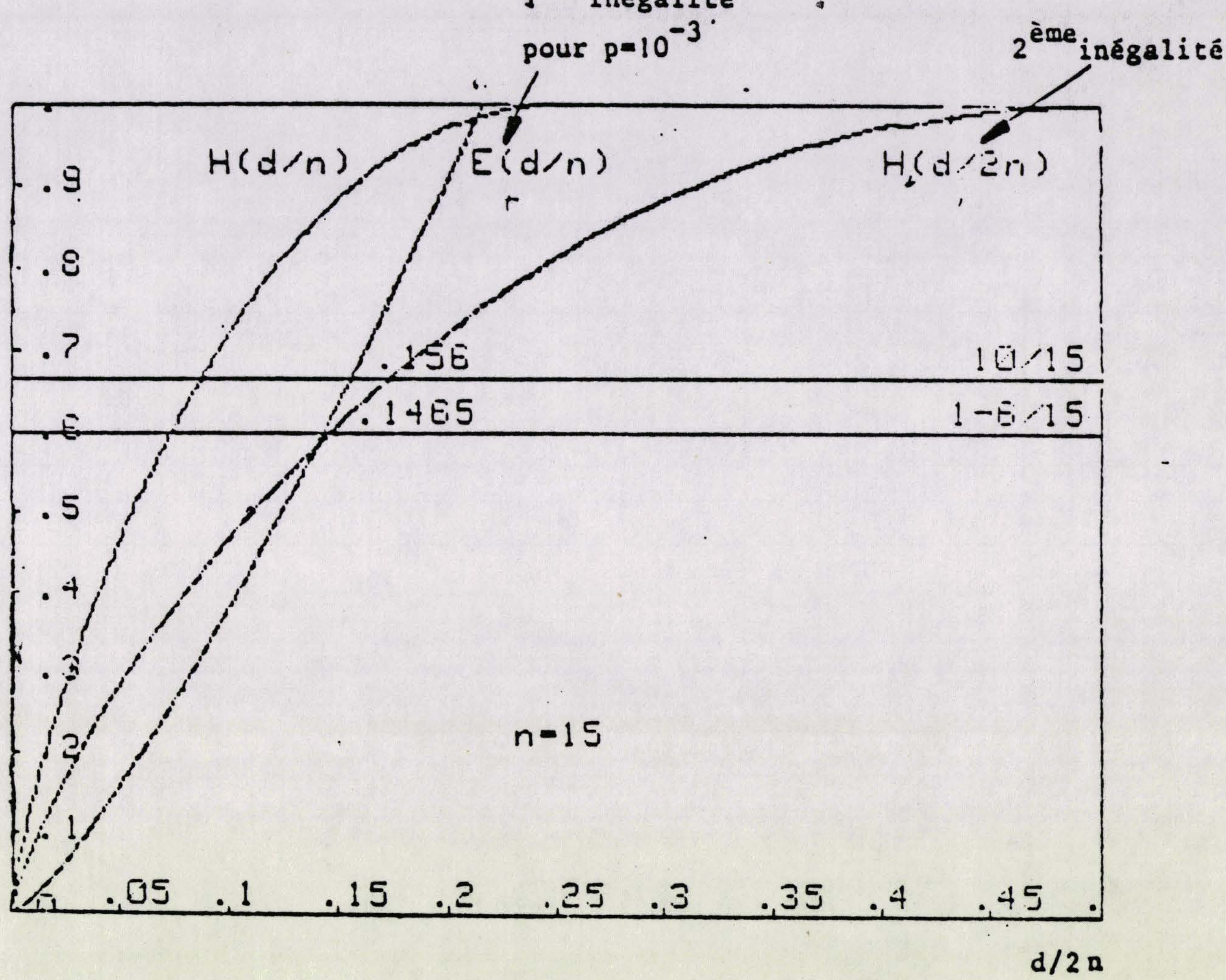


Figure 2

Sur la figure 2, nous voyons que pour n = 15, soit
n = m+k avec k = 6, soit m = 9 ou 9 bits de contrôle
les marges se recoupent, en toute rigueur il n'existe pas de solution. Toutefois, les approximations étant très pessimistes, la valeur n = 15 constitue une solution limite.

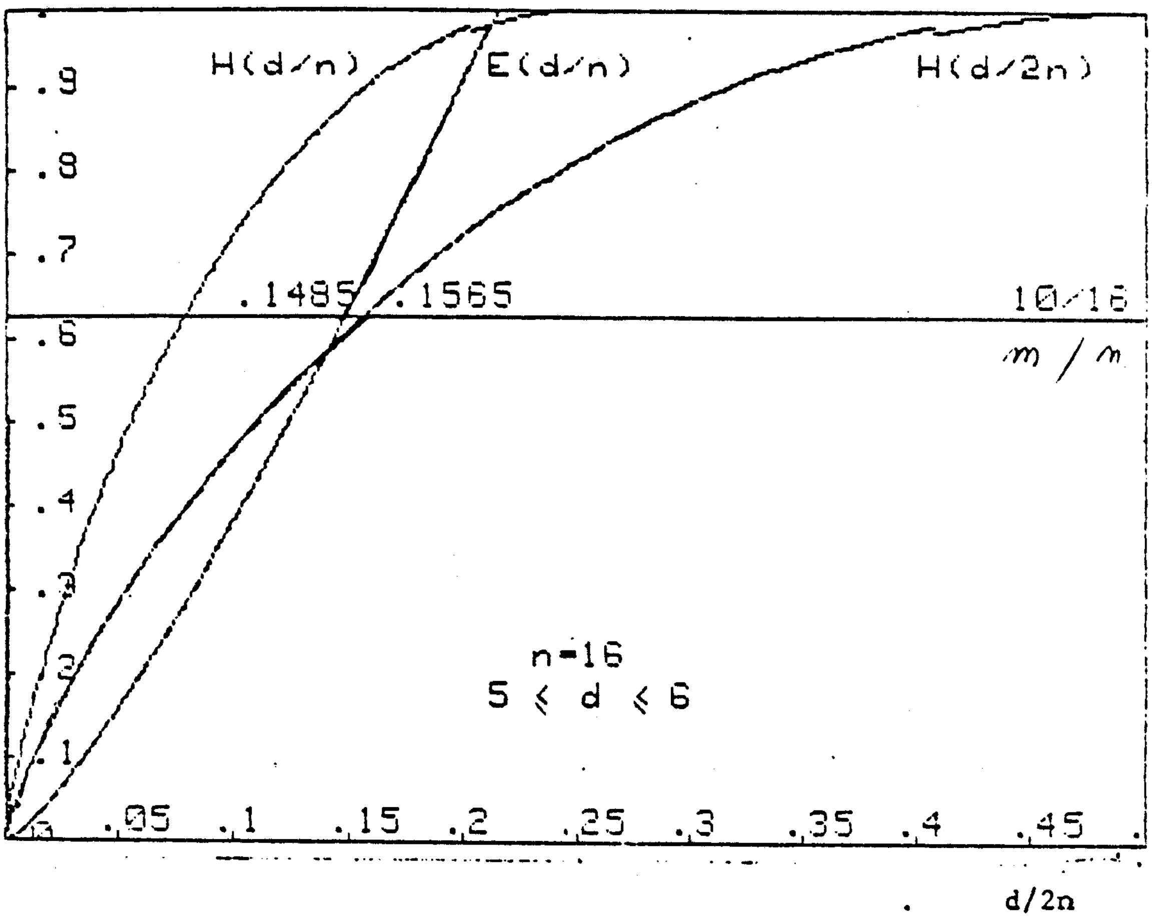


Figure 3

Sur la figure 3, pour n = 16, soit 10 bits de contrôle, les deux marges se joignent.

m = 10 constitue une solution. Il faut, dans ce cas, prendre la distance d entre les messages :

$5 \leqslant d \leqslant 6$

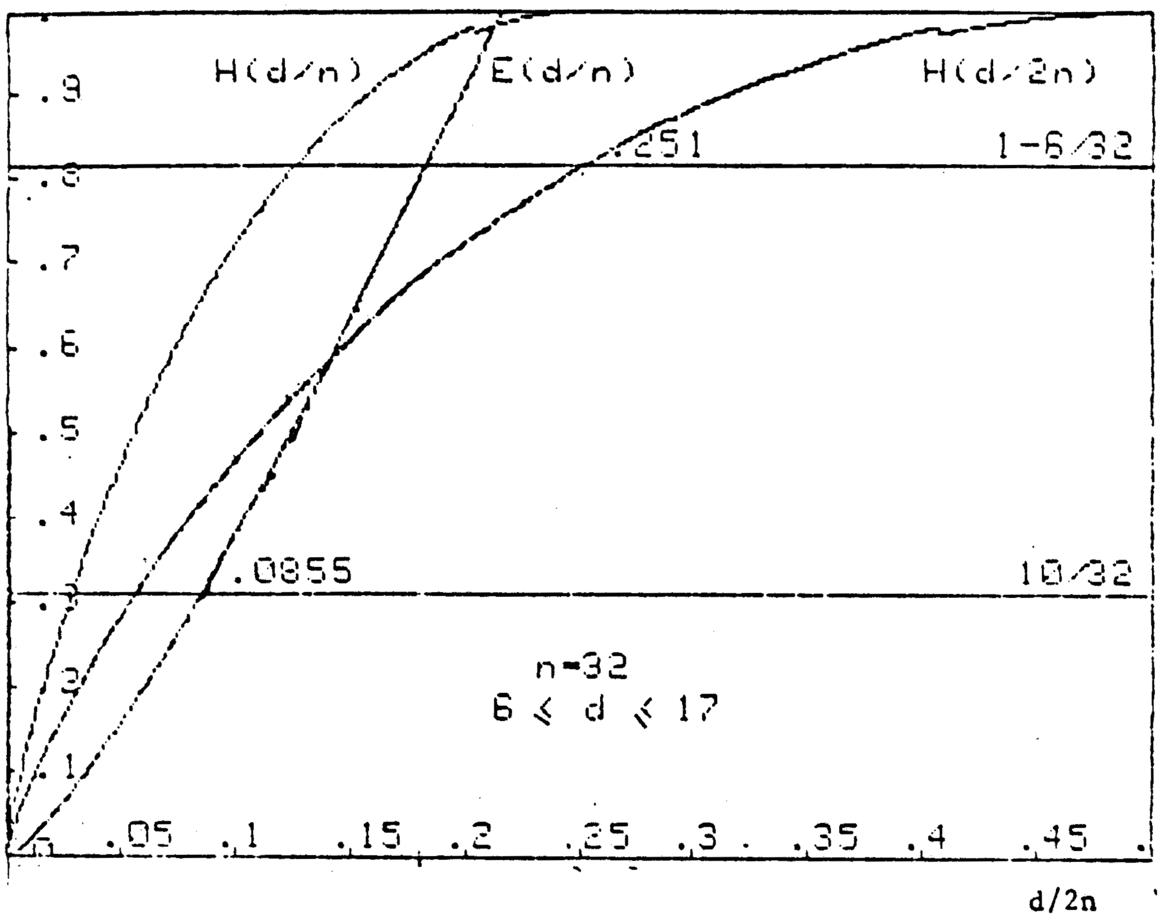


Figure 4

Pour n = 32, figure 4 les marges s'éloignent. Le problème a plusieurs solutions possibles, mais le nombre de bits de contrôle est surabondant (m = 2(
La distance entre les messages peut être comprise :

$6 \leqslant d \leqslant 17$

La solution retenue en fonction des objectifs fixés au départ est donc :

- Nombre maximum d'informations à transmettre , 63 , soit $k = 6$.

- La probabilité d'erreurs par bit dans les voies de transmission , $P = 10^{-3}$.

- Objectif de sécurité par message , $q = 10^{-10}$.

- Le nombre de bits de contrôle est de $m = 10$.

-La distance entre les messages est de $d = 6$.

Les caractéristiques physiques du code étant connues , on peut à présent mettre en oeuvre un code satisfaisant aux conditions établies précédemment .

IV-4 Codes choisis .

IV-4-1 Code linéaire .

Le code choisi est un code linéaire dont la distance minimale est $d = 6$ et le nombre total de bits dans un mot du code est $n = 16$.

Si on appelle <M> le mot du code , alors :

$$\langle M \rangle = \langle k_0 k_1 \ldots k_5 , m_0 m_1 \ldots m_9 \rangle$$

avec $k_0, k_1, \ldots, k_5$: bits d'information utile
et $m_0, m_1, \ldots, m_9$: bits de contrôle .

Les bits de contrôle sont choisis de telle sorte que l'on respecte la distance minimale entre les mots du code ,(d=6).

$m_0 = k_2+k_3+k_4+k_5$	$m_5 = k_0+k_3+k_4+k_5$
$m_1 = k_1+k_3+k_4+k_5$	$m_6 = k_0+k_1+k_4$
$m_2 = k_1+k_2+k_4+k_5$	$m_7 = k_0+k_1+k_2+k_5$
$m_3 = k_1+k_2+k_3+k_5$	$m_8 = k_0+k_1+k_2+k_3$
$m_4 = k_0+k_2+k_4$	$m_9 = k_0+k_1+k_2+k_3+k_4$.

La matrice génératrice des mots du code est la suivante :
(On notera que le code choisi est un code systématique)

$$(G) = \begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1 \\ 0&1&0&0&0&0&0&1&1&1&0&0&1&1&1&1 \\ 0&0&1&0&0&0&1&0&1&1&1&0&0&1&1&1 \\ 0&0&0&1&0&0&1&1&0&1&0&1&0&0&1&1 \\ 0&0&0&0&1&0&1&1&1&0&1&1&1&0&0&1 \\ 0&0&0&0&0&1&1&1&1&1&0&1&0&1&0&0 \end{bmatrix}$$

Un mot code est obtenu par :

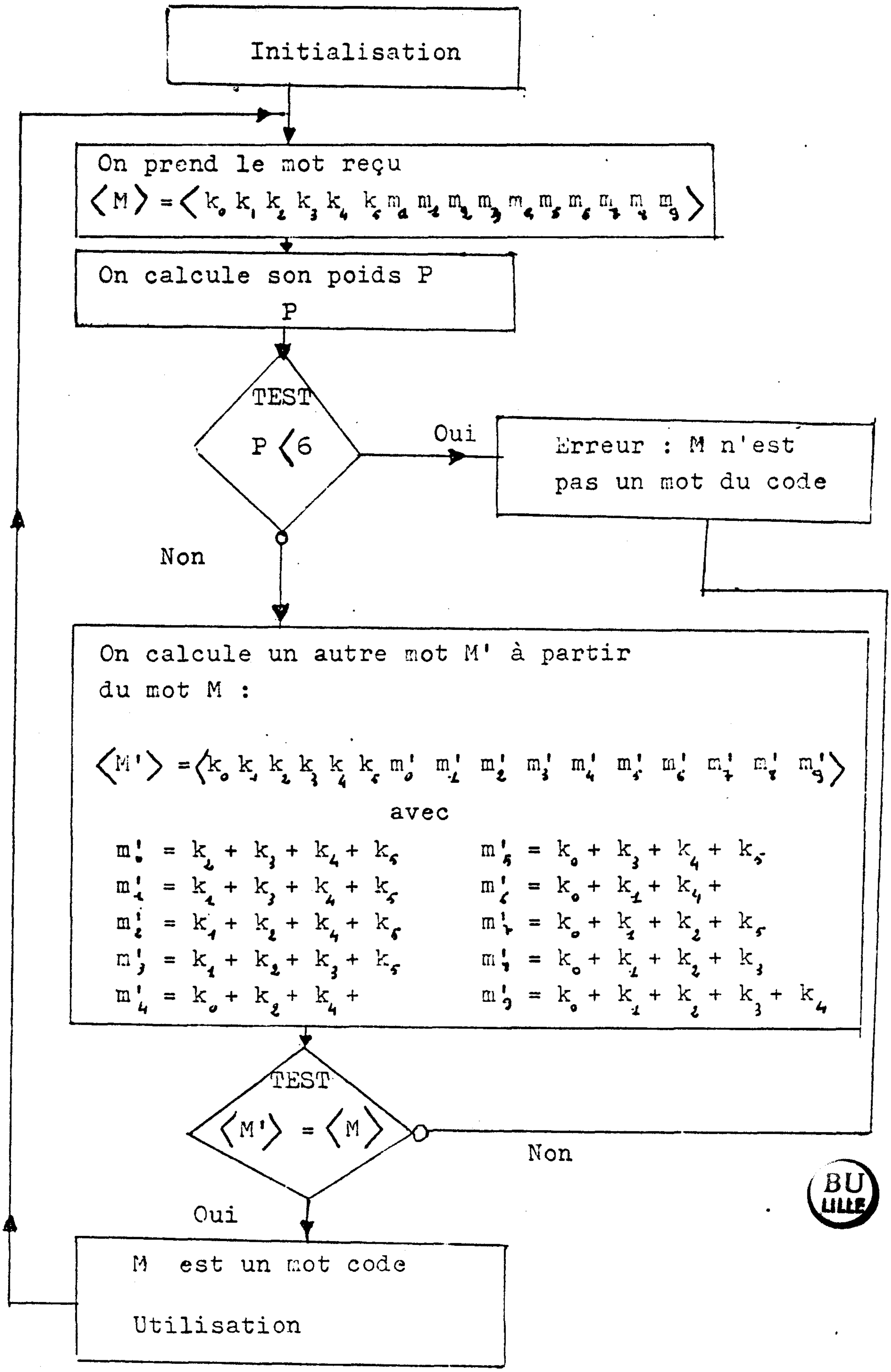
$$\langle k_0k_1k_2k_3k_4k_5\rangle \; . \; G = \langle k_0k_1k_2k_3k_4k_5m_0m_1m_2m_3m_4m_5m_6m_7m_8m_9\rangle$$

<u>Performance du code **L(16,6)**</u>.

Le code **L(16,6)** est capable de détecter jusqu'à **5** erreurs indépendantes ou bien un paquet d'erreurs de longueur **1** , inférieure à **10** .

L'organigramme de détection d'erreurs est représenté à la page suivante .
Cet organigramme a été programmé sur microcontrôleur 8031 de Intel , en langage Assembleur , (270 octets environ).
Pour des questions de fonctionnement du microprocesseur , l'exécution de ce programme a été réalisée de telle sorte

- Organigramme de la détection des erreurs :



que l'on puisse générer un créneau équitemps conforme aux principes de sécurité développés par ailleurs , (Ref 19) . Le programme a été testé avec les 2^n ou 2^{16} messages possibles en réception au format de 2 octets chacun . La réception étant supposée faite à partir de l'UART de microcontrôleur , seuls les 63 messages appartenant au code sont ressortis validés .

IV-4-2 Code cyclique .

Le code cyclique choisi est défini par son polynôme générateur **g(x)** :

$$g(x) = x^9 + x^6 + x^5 + x^4 + x + 1 .$$

Sa distance minimale est **d = 6** et le nombre total de bits dans un mot du code est **n = 15** .

Si on appelle **M(x)** le polynôme du code , alors :

M(x) = g(x).N(x) ,avec **N(x)** polynôme d'information

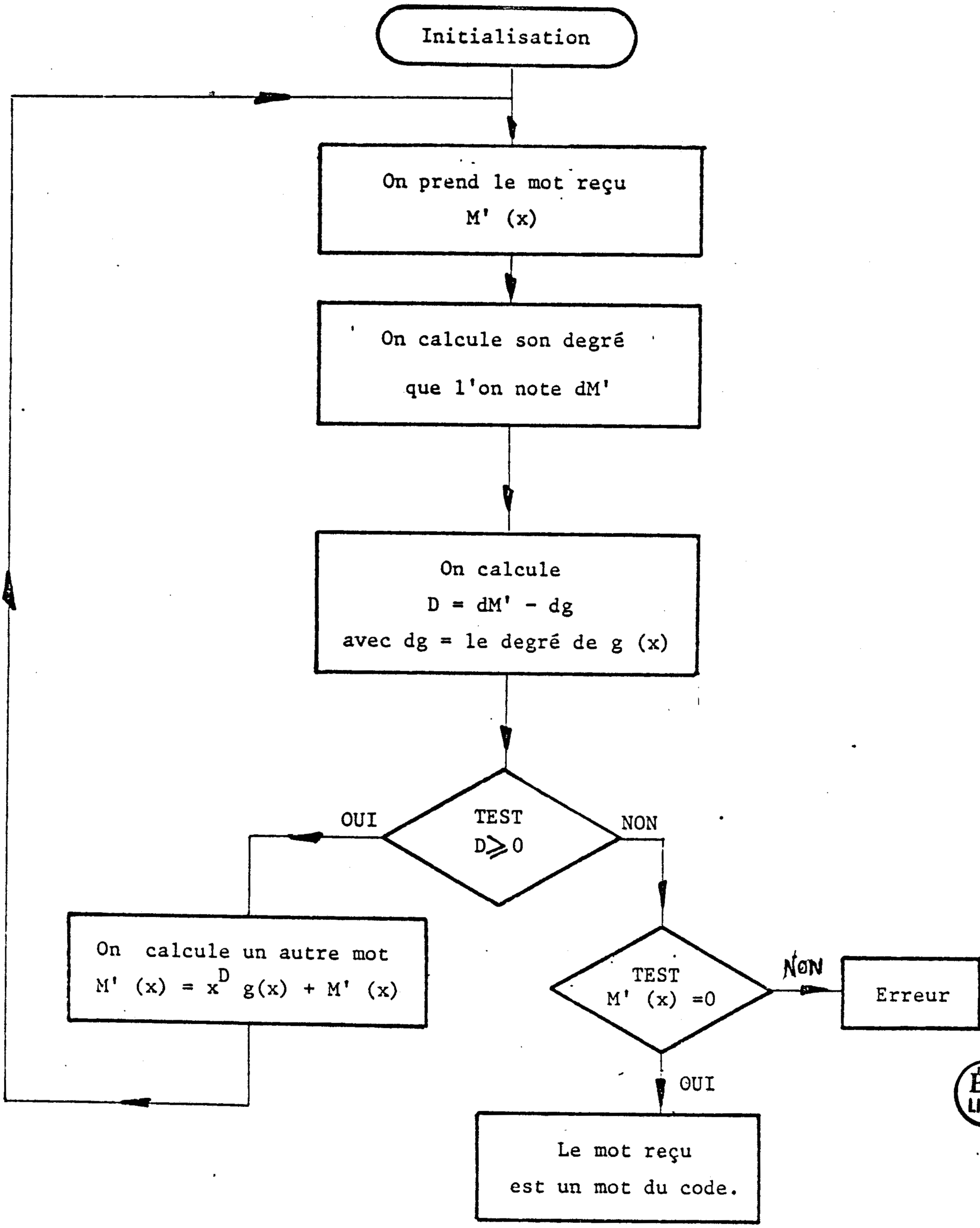
Si le processus de transmission n'introduit pas d'erreur , le polynôme **M'(x)** qui représente le mot reçu divisé par **g(x)** donnera un reste nul . Si des erreurs étaient introduites , le reste serait différent de zéro.

Performance du code C(15,6).

Le code **C(15,6)** est capable de détecter jusqu'à **5** erreurs indépendantes ou bien un paquet d'erreurs de longueur **1** , inférieure à **9** .

Il nous a semblé utile de mentionner toutes les performances de ce code , même en ce qui concerne les paquets d'erreurs , bien que nous ne les ayons pas pris en compte dans l'estimation de la probabilité de non détection d'erreurs . (La définition d'un paquet d'erreurs se trouve en Annexe III) .

Organigramme de la détection des erreurs:



De la même façon que précédemment , cet organigramme a été écrit en assembleur sur microcontrôleur 8031 , (environ 100 octets d'occupation de mémoire) . On y génère un créneau équitemps .

Le programme a également été testé de façon satisfaisante pour les 2^{16} combinaisons possibles de messages reçus .

Cette procédure de détection d'erreurs est donc également utilisable pour notre problème .

IV-5 Remarques sur le choix du code .

Après avoir établi les caractéristiques physiques des informations à transmettre , (format des messages) , nous avons mis en oeuvre et testé les procédures de détec tion d'erreurs utilisant un code cyclique et un code linéaire .
Notre choix final s'est porté sur **l'emploi du code linéaire** et ceci pour deux raisons .

1°) - **Au niveau du principe** , en débordant un peu de nos hypothèses de travail et en considérant que la transmission asynchrone de messages série peut , en cas de panne présenter une sorte de glissement dans la reconstitution des octets , il se peut qu'un message reçu corresponde à un message émis mais décalé de un ou plusieurs bits .
Or , de par les propriétés des codes cycliques , ce mot décalé peut justement appartenir au code .
Ce modèle d'erreur n'est pas valable si on utilise un code linéaire .

2°) - **Au niveau de la mise en application** . Bien que l'occupation mémoire du programme soit plus importante , le temps d'exécution de la routine de détection d'erreurs par code linéaire est plus rapide , (300 µ sec au lieu de 600 avec le code cyclique) .

D'autre part , la normalisation des séquences équitemps est plus aisée .

Ces caractéristiques sont importantes pour notre application , compte tenu des contraintes apportées par la sécurité où l'on observe temporellement le bon fonctionnement du microprocesseur .

V-CALCUL DE LA PROBABILITE DE NON DETECTION D'ERREUR UTILISANT LE CODE LINEAIRE.

Ce calcul revient à vérifier a posteriori que l'on tient bien l'objectif de sécurité que l'on s'était fixé initialement , soit **q** , à partir de la connaissance de la portion des mots du code . (Voir tableau n° 1) .

Nous avons vu dans le paragraphe précédent que la probabilité de non détection d'erreur avait pour expression :

$$\mathbf{PND} = \sum_{e=d}^{e=n} A_e\, p^e\,(1-p)^{n-e} \qquad (\text{ Réf } 25)\ .$$

où A_e représente le nombre de mots du code dont le poids est égal à **e** .

Le tableau n° 2 nous donne les valeurs de A_e :

e	6	7	8	9	10	11	12	13	14	15	16
A_e	9	20	13	8	6	4	2	0	1	0	0

(Tableau n° 2)

On a alors :

$$\text{PND} = 9\,p^6(1-p)^{10} + 20p^7(1-p)^9 + 13p^8(1-p)^8 + 8p^9(1-p)^7 + 6\,p^{10}(1-p)^6 + 4p^{11}(1-p)^5 + 2p^{12}(1-p)^4 + 1p^{14}(1-p)^2.$$

En prenant les valeurs numériques correspondant à notre problème , soit $p = 10^{-3}$, on obtient :

$$PND = 9{,}2 \,.\, 10^{-18}$$

$$= 10^{-17} < 10^{-10} \text{ " Objectif de sécurité " .}$$

Autrement dit , l'objectif de sécurité fixé est largement satisfait .

A titre indicatif , nous avons tracé sur la Figure 5 , la valeur de **PND** en fonction de la probabilité d'erreurs par bit de la transmission **p** .

Si on veut tenir compte de l'objectif fixé , on voit que la probabilité d'erreur par bit peut fluctuer dans l'intervalle :

$$0 \leqslant p \leqslant 1{,}52 \,.\, 10^{-2} \,.$$

TABLEAU N° 1

CALCUL DU POIDS DES MOTS CODES

Mots du code en Hexa	Poids du mot code	Mots du code en Hexa	Poids du mot code	Mots du code en Hexa	Poids du mot code	Mots du code en Hexa	Poids du mot code
07D4	7	461B	7	803F	7	C1F0	7
0BB9	8	4A76	8	87EB	10	C624	6
0C6D	7	4DA2	7	8B86	7	CA49	7
1353	7	5296	7	8C52	6	CD9D	10
1487	6	5548	6	936C	8	D2A3	8
18EA	7	5925	7	94B8	7	D577	11
1F3E	10	5EF1	10	98D5	8	D91A	8
22E7	8	6328	6	9F01	7	DECE	11
2533	7	64FC	9	A2D8	7	E317	9
295E	8	6891	6	A50C	6	E4C3	8
2E8A	7	6F45	9	A961	7	E8AE	9
31B4	7	707B	9	AEB5	10	EF7A	12
3660	6	77AF	12	B65F	11	F044	6
3A0D	7	7BC2	9	BA32	8	E790	9
3DD9	10	7C16	8	BDE6	11	FBFD	14
41CF	8			B18B	8	FC29	9

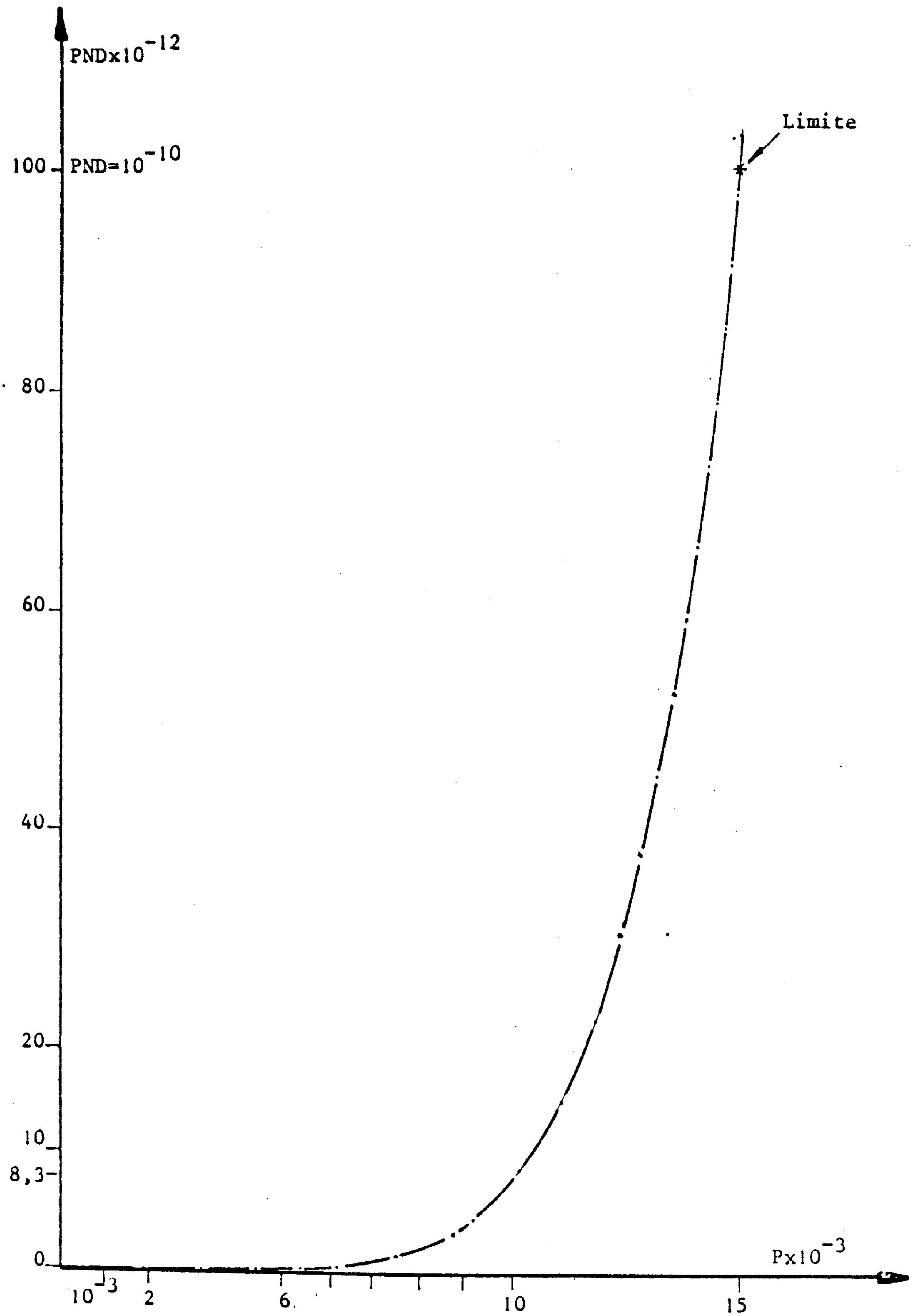


Figure 5 : PROBABILITE DE MESSAGES FAUX ET NON DETECTES (PND) EN FONCTION DE LA PROBABILITE DES ERREURS INTRODUITES PAR LA TRANSMISSION P PAR BIT

C H A P I T R E   I V

_°_°_°_°_°_°_°_°_°_°_

APPLICATION AUX TRANSMISSIONS NUMERIQUES SOL - TRAINS EN TUNNEL .

I INTRODUCTION.

La chaîne de transmission envisagée dans ce chapitre sert à l'envoi d'informations de sécurité entre les automatismes de pilotage fixe et embarqués .

Une voie de recherche consiste aujourd'hui à développer des procédés de transmission d'informations numériques sol - véhicules sans support matériel , ceci dans le but de simplifier les équipements et de les adapter au traitement par microprocesseur .

L'étude proposée par l'**INRETS - CRESTA*** associé à l'**USTL**** consiste à rendre cette transmission en sécurité en utilisant des codes de détection d'erreur , (sécurité probabiliste) .

Or , nous avons besoin de connaître le taux moyen d'erreur de cette transmission ainsi que les modèles d'erreurs prédominants afin de mettre en oeuvre un code de détection d'erreurs .

Malheureusement , nous ne possédons pas encore suffisamment de résultats expérimentaux sur ce type de transmission .

---

* Institut National de Recherche sur les Transports et leur Sécurité .
Centre de Recherche et d'Evaluation des Systèmes de Transport Automatisés .

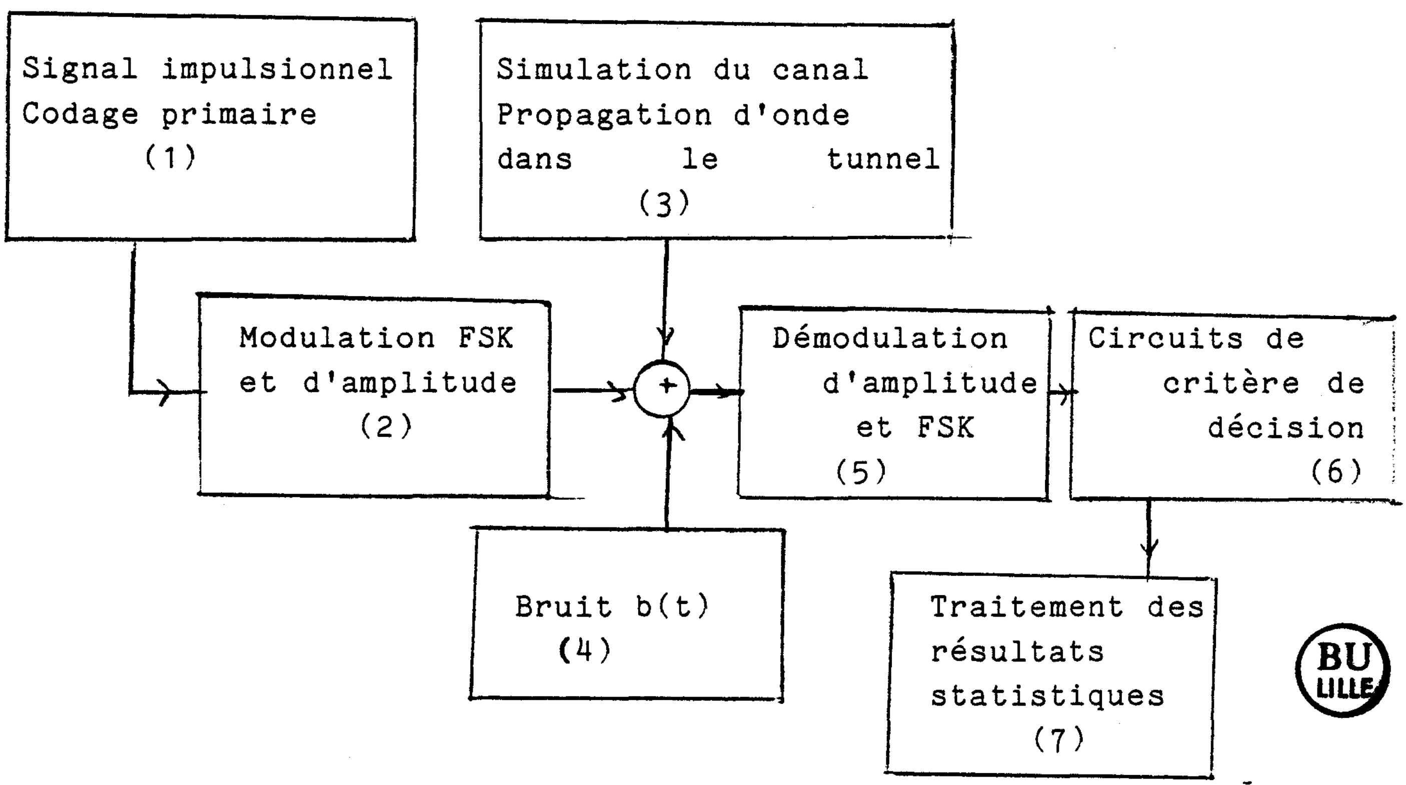
** Université des Sciences et Techniques de Lille .

C'est pourquoi , il nous a paru judicieux de mettre en oeuvre une simulation de cette chaîne de transmission afin d'estimer le taux moyen d'erreurs dépendant des grandeurs caractéristiques de la liaison , telles que la modulation de l'onde porteuse , la démodulation et le critère de décision .

II SIMULATION THEORIQUE DE LA CHAINE DE TRANSMISSION.

Notre premier travail consiste à simuler la chaîne de transmission complète en remplaçant les divers éléments par leur modèle mathématique , proche de la réalité physique et ceci afin d'utiliser la simulation comme aide à la conception ,(optimisation de la chaîne de réception).

Nous obtenons ainsi un schéma équivalent de la transmission simplifiée :



II-1 Caractéristiques du signal de données.

Le codage primaire utilisé pour l'émission du signal de données est du type binaire avec retour à zéro (RZ) .
Le "(1)" logique est émis sous forme d'une impulsion et le "(0)" logique correspond à l'absence d'impulsion .

II-2 Modulation FSK et d'amplitude .

Notre choix expérimental s'est porté sur une modulation d'amplitude par saut de fréquence , (Basse fréquence) , **ASFK**[1] .

A la succession d'états logiques d'entrée (0) et (1) , nous associons deux fréquences **BF** (12 Khz et 22 Khz) qui modulent en amplitude la porteuse hyperfréquence avec un indice de modulation voisin de 0,8 .

A la sortie du modulateur , on obtient donc l'un des deux signaux suivants :

$$a(t) = (1 + m.\sin(2\pi f_o.t)).\sin(2\pi F_p.t)$$

ou bien :

$$a(t) = (1 + m.\sin(2\pi f_1.t)) .\sin(2\pi F_p.t) .$$

avec :

f_o : Fréquence associée à l'état logique 0
f_1 : Fréquence associée à l'état logique 1
F_p : Fréquence porteuse
m : Indice de modulation

(1) AFSK Audio Frequency Shift Keying .

II-3 Propagation d'onde dans le tunnel .

Afin de tenir compte de la propagation du champ en tunnel et surtout des variations d'amplitude , des chercheurs du laboratoire ont élaboré des programmes numériques permettant de simuler cette propagation .
(Pour davantage de détails , voir Réf 32) .

Ainsi , nous pouvons calculer le signal présent dans le plan du récepteur par la connaissance de l'état logique ("0" ou "1") émis , l'expression analytique du signal modulé et l'atténuation en tunnel subie par ce signal , soit :

$$a(t) = A\ (\ 1 + m.\sin(2\pi f.t)\ ).\sin(2\pi F_p.t)$$

avec :

$f = f_0$ pour l'état logique "0" émis
$f = f_1$ pour l'état logique "1" émis
A coefficient d'atténuation .

Nous négligeons tous les parasites de type naturel ou industriel .

II-4 Le bruit .

Dans notre étude , nous ne considérons que le bruit thermique apparaissant dans les préamplificateurs du récepteur.

Nous négligeons le bruit de grenaille et le bruit de génération - recombinaison .

Ce bruit vient donc se superposer au signal reçu au niveau de l'entrée du récepteur .

Le bruit thermique est défini comme un processus aléatoire stationnaire décrit par une fonction aléatoire **b(t)** , de moyenne nulle et de variance σ_b^2.

Le modèle mathématique de bruit utilisé dans notre application est un bruit à bande étroite .

Dans ces conditions , on montre facilement que la fonction aléatoire b(t) (Générateur du bruit) peut s'écrire sous la forme :

$$b(t) = E\ (\ U(t).\cos(2\pi F_p.t) - V(t).\sin(2\pi F_p.t)\ )$$

où **U(t)** et **V(t)** sont des variables aléatoires Gaussiennes normalisées , c'est à dire de moyenne nulle et de variance unitaire .

E est la tension efficace du bruit thermique de l'étage d'entrée du récepteur . Cette tension peut être exprimée par l'équation :

$$E = \sqrt{P.Z_e}\ ,$$

avec :

Z_e : impédance d'entrée du récepteur
P : puissance thermique d'équation :

$$P = \overline{V_b}^{2} = (\ G.K.T.B\ )\ (\ \text{Watt}\ )$$

avec :

G : Gain de l'étage d'entrée du récepteur
K : Constante de Boltzman , soit $1,37 \ .\ 10^{-23}$
T : Température du bruit global de l'étage d'entrée .
B : Bande passante de l'étage .

Les constructeurs donnent plus souvent le facteur de bruit des étages d'amplificateur en dB , noté FB .
Il est possible de passer de l'un à l'autre par l'expression :

$$T = 290 \left(e^{\frac{1}{\log_{10}(e)} \cdot \frac{FB}{10}} - 1 \right)$$

Remarque :

Nous avons généré les deux variables aléatoires gaussiennes normalisées , U(t) et V(t) , suivant la méthode de Bose et Muller (Réf 21) .

II-5 Démodulation d'amplitude et FSK .

II-5-1 Démodulation d'amplitude.

A l'entrée du démodulateur d'amplitude , le signal s'écrit:

$$s(t) = A.(1 + m.\sin(2\pi f.t)).\sin(2\pi F_p.t) + b(t)$$

avec :

$f = f_0$ pour l'état logique "0"
$f = f_1$ pour l'état logique "1".

Si nous supposons que la démodulation d'amplitude est parfaite , nous obtenons :

$$s(t) = A.m.\sin(2\pi f.t) + b(t) .$$

Cette supposition est due à la limitation du temps d'exécution du programme . (F_p = 10 Ghz) .

II-5-2 Démodulation FSK .

La démodulation FSK s'effectue à l'aide de deux filtres passe - bande de deuxième ordre accordés aux fréquences f_0= 12 Khz et f_1 = 22 Khz .

Pour un traitement par des calculateurs , nous avons dû simuler les deux filtres réels par des filtres numériques . Le modèle de simulation choisi est tel que l'on s'approche de la réalité physique . (Voir Figure 6) .

II-6 Critère de décision .

On simule le circuit de décision par :

- Le calcul des valeurs absolues des signaux à la sortie des 2 filtres , ce qui est équivalent à un circuit à double redressement .

- Le calcul de leur intégrale sur une période T , qui est la durée du bit .

- Le calcul de la différence entre les intégrales de ces 2 signaux .

- La définition d'un critère de décision à seuil .

Donc à l'une des sorties des deux filtres f_0 et f_1 et sans bruit , le signal est de la forme :

$$s'(t) = A'.m'.\sin(2\pi f.t)$$

avec :

$f = f_0$ pour l'état "0"
$f = f_1$ pour l'état "1" .

On calcule la valeur moyenne sur la durée du bit :

$$S = \int_0^T s'(t)\,dt = 2T.f \int_0^{\frac{1}{2.f}} A'.m'.\sin(2\pi f.t)\,dt$$

$$= \frac{2T.m'.A'}{\pi}$$

Supposons que l'état logique "1" ait été émis .
A la sortie du filtre f_1 , on a alors :

$$A'.m' \neq A.m$$

Avec :
A : coefficient d'atténuation
m : indice de modulation : 0,8 .

De même à la sortie du filtre f_0 , on a :

$$A'.m' = A_0'.m_0' \ll A.m$$

$$S_1 - S_0 = (2T/\pi).(A.m - A_0'.m_0') = (2T/\pi).A.(m - m_0')$$

Nous dirons que l'état logique "1" a été émis lorsque $S_1 - S_0 > E_{min} + 0$,avec une certaine zone d'interdiction sur l'incertitude .

De la même façon , lorsque $S_1 - S_0 < 0 - E_{min}$, avec une certaine zone d'interdiction , nous dirons que l'état logique "0" a été émis .

Les deux régions de décision D_0 et D_1 sont donc définies par :

	S_1-S_0	
		Zone interdite
$10.A(\frac{2T}{\pi}(m-m_0''))$	E_{max}	
		Zone D_1
$\frac{1}{10}.A(\frac{2T}{\pi}(m-m_0''))$	E_{min}	
		Zone interdite
	0	
		Zone interdite
	$-E_{min}$	
		Zone D_0
	$-E_{max}$	
		Zone interdite

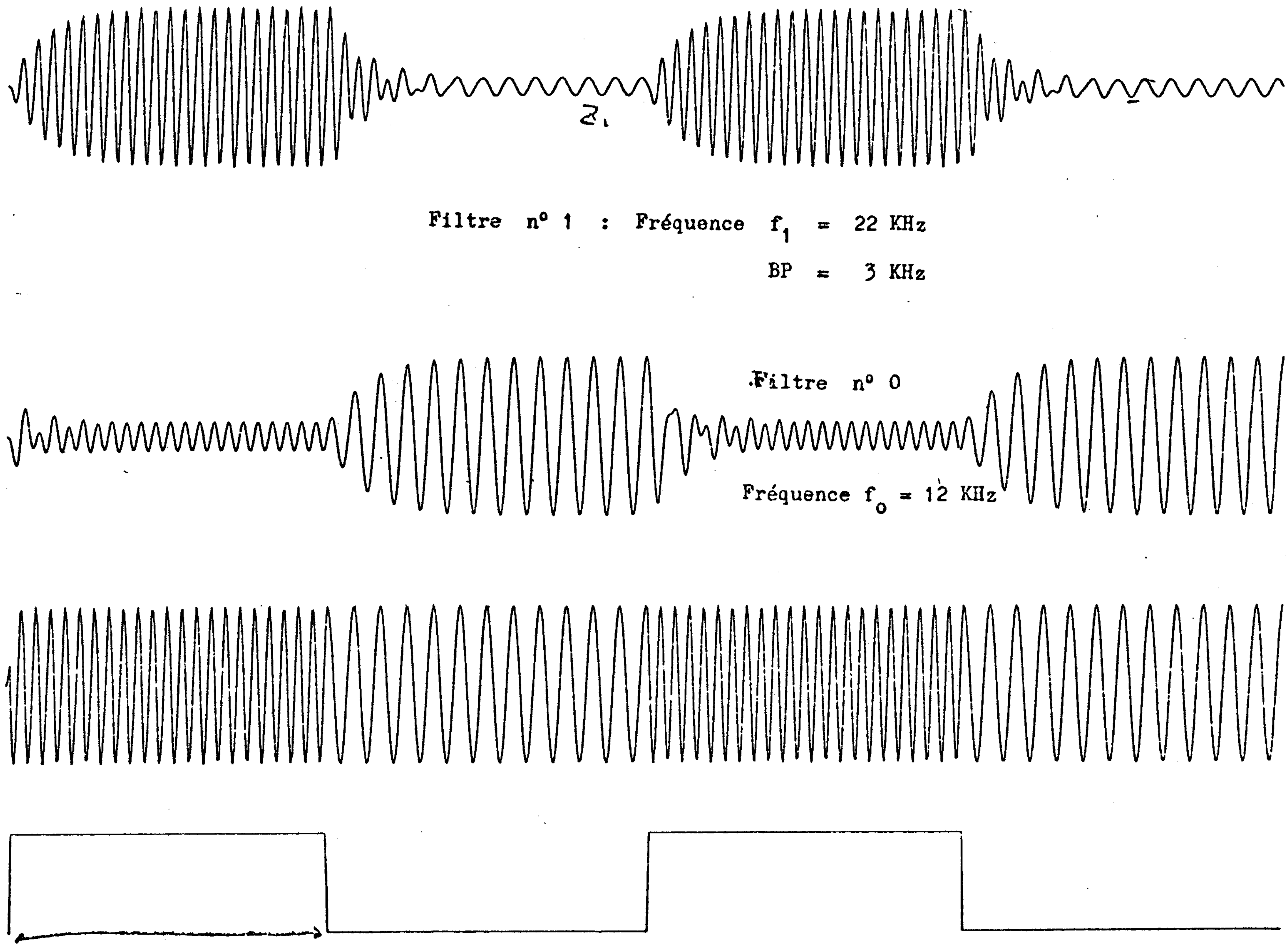


Figure 6 : Courbe de réponse de deux filtres numériques .
Fréquence d'échantillonnage f_e = 250 KHz .

II-7 Mise en oeuvre du programme de simulation .

Les différentes parties de la chaîne ayant été modélisées selon la description donnée précédamment , nous avons pour chacune développé un module de programme spécifique .

Un programme principal , définissant le cadre de l'étude ou l'objet de la simulation , vient employer tout ou une partie des programmes .

L'étude a été organisée de la façon suivante :

1°) - Détermination des caractéristiques des filtres de démodulation FSK .

Nous avons tout d'abord utilisé le programme de simulation des filtres numériques afin de déterminer un couple de filtres optimum à la démodulation du signal FSK .

Pour un débit de transmission **1/T** de 1 KBand , nous avons en effet à optimiser les caractéristiques des filtres et des fréquences porteuses f_0 et f_1 .

Les caractéristiques de ces filtres sont :

- Fréquence centrale f_c .
- Coefficient de qualité **Q** .
- Bande passante **BP** .
- Temps de montée du signal .

Suite à cette étude , nous avons choisi les filtres suivants :

- Premier filtre passe-bande :

$$f_c = f_1 = 22 \text{ KHz}$$
$$BP = 3 \text{ KHz}$$
$$Q = 22/3 = 7,3 .$$

- Deuxième filtre passe-bande :

$$f_c = f_0 = 12 \text{ KHz}$$
$$BP = 3 \text{ KHz}$$
$$Q = 4 .$$

Le choix de ces filtres résulte d'un compromis entre le temps d'établissement du signal et l'atténuation qu'ils apportent lorsque l'on n'est pas sur la bonne fréquence .

2°) Etude sans les perturbations apportées par la propaga--tion en tunnel .

Cette étude ne considère comme source d'erreur que le bruit du récepteur .
Le paramètre de l'étude est donc ici le rapport signal sur bruit que nous considérons varier dans une dynamique de 40 dB .
Les résultats obtenus sont des valeurs moyennes des taux d'erreurs .
Ces valeurs sont valables dans le cas général d'une transmission à point fixe .

3°) Etude avec les perturbations apportées par la propagation en tunnel .

On se place dans le cas où le milieu de propagation est un tunnel dont les dimensions transversales de la galerie sont très grandes par rapport à la longueur d'onde du signal radioélectrique .

La figure (7) montre un tracé expérimental du champ reçu en fonction de la distance émetteur-récepteur sur laquelle on peut constater une absorption quasi-totale du module du champ reçu .

Des recherches dans ce domaine ont montré que l'on n'excède pas une dynamique de 40 dB en utilisant une technique de diversité des antennes à l'émission ou à la réception .

évolution expérimentale du module du champ électrique à 10 GHz en fonction de la distance émetteur-récepteur

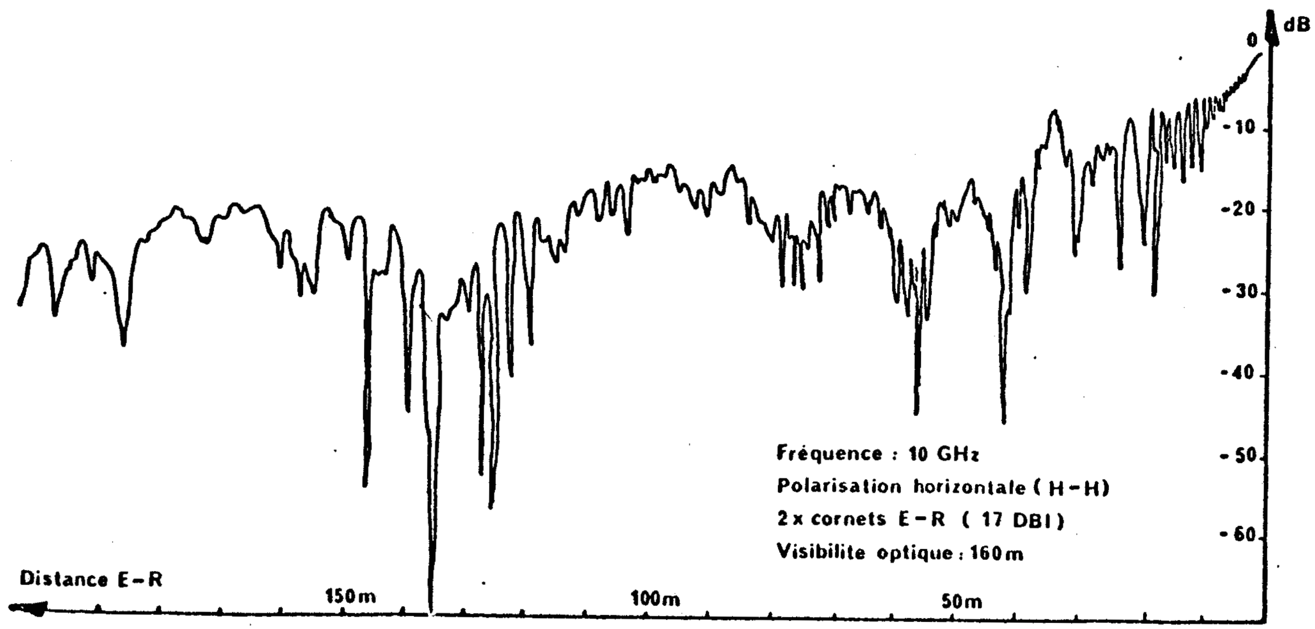


Figure 7

Dans ce cas , on effectue la simulation d'une transmission dans le cas réel d'une transmission en tunnel où l'on tient compte des fluctuations rapides du niveau reçu .

Pour ce faire , on intègre dans le programme principal la modélisation de la transmission en tunnel selon un procédé cinématique d'une rame de métro comparable à celle du Val .

La portion de tunnel parcourue est telle que les fluctuations de propagation n'excèdent pas 40 dB de dynamique .

Ceci nous permet dans un cas particulier de transmission à point mobile (récepteur fixe , émetteur embarqué) de vérifier que le taux d'erreur instantané n'excède pas le taux d'erreur moyen .

II-8 Estimation du taux d'erreur moyen de la transmission.

II-8-1 Définition.

Avant de donner les résultats des erreurs fournies par la simulation de la chaîne de transmission , il est important de préciser la définition du rapport signal sur bruit car elle a une grande importance pour le taux d'erreur .

Tout d'abord , on considère la puissance du signal et celle du bruit avant le passage du couple de filtres passe-bande. C'est le bruit de l'étage d'entrée du récepteur à la fréquence porteuse de 10 GHz .

Nous définissons le signal par la valeur crête du niveau reçu juste après la démodulation d'amplitude le bruit par sa tension crête :

$$\sqrt{2} \cdot E = \sqrt{2 . G . K . T . Z_c . B}$$

donc :
$$\left(\frac{S}{B}\right) = \left(\frac{m.A}{\sqrt{2}.E}\right)$$

où **m** est l'indice de modulation
et **A** est l'amplitude du signal reçu à l'entrée du récepteur .

$$\left(\frac{S}{B}\right) = 20.\mathrm{Log}_{10}\left(\frac{m.A}{\sqrt{2}.E}\right)$$

II-8-2 Résultats des erreurs données par simulation.

a) Sans tunnel.

Le calcul de la probabilité d'erreur pour tout symbole (bit) émis est une propriété statique .
Elle a pour expression :

$$P = \frac{\text{Nombre d'erreurs comptées dans un intervalle de temps fixé}}{\text{Nombre total de bits émis pendant le même intervalle de temps}}$$

Il est clair que le résultat présentera une variance statique à partir du taux moyen d'erreur à long terme en fonction de la taille de l'échantillon prélevé sur la population .

$\left(\frac{S}{B}\right)$ dB	5 dB	10 dB	20 dB	40 dB
Nbre d'erreurs sur 2700 bits	8 à 12	6	3	2 à 3

Au dessus de 40 dB , il n'y a pas d'erreur sur 2700 bits .

b) Avec tunnel:

Après les résultats des erreurs données sans tunnel , nous avons effectué le procédé de calcul des erreurs en tenant compte des fluctuations de l'onde hyperfréquence dans le tunnel et du profil cinématique de la partie mobile .

Nous avons choisi la cinématique suivante :

$$y = \frac{1}{2} \gamma t^2 + x_o$$

$$\gamma = 1{,}3 \quad m/s^2$$

$$x_o = 2 \text{ m} .$$

En faisant varier le temps **t** de 4,5 à 6 secondes , nous parvenons à obtenir un profil d'atténuation de l'amplitude de l'onde hyperfréquence variant entre - 15 et - 40 dB .

Ces résultats nous semblent satisfaisants car le nombre d'erreurs ne dépasse pas celui du rapport signal sur bruit à 40 dB , lorsque l'on ne tient pas compte de l'atténuation de l'amplitude de l'onde hyperfréquence .

II-9 Conclusion.

Le modèle de simulation que nous avons développé indique qu'il existe des erreurs de transmission et que la probabilité d'erreur de la transmission est de l'ordre de 10^{-3}.

Cette valeur est sous réserve du fait que notre simulation a demandé un temps considérable pour extraire un résultat et que par conséquent nous n'avons pas pu aller plus loin pour confirmer la probabilité obtenue .

Le but de notre étude étant par ailleurs d'avoir une idée de l'ordre de grandeur de cette probabilité d'erreurs afin de mettre en oeuvre un code de détection d'erreurs qui puisse rendre la transmission en sécurité .

III-CODES DE DETECTION D'ERREURS ADAPTES A LA TRANSMISSION.

L'étude qui suit consiste à trouver des codes de détection d'erreurs capables de s'affranchir d'un majorant d'erreurs dues au bruit et à la propagation d'onde dans le tunnel .

Afin de rendre la chaîne de transmission en sécurité , la probabilité de non détection d'erreur doit être inférieure à 10^{-10} par message .

III-1 Code de détection d'erreurs en cas de diffusion d'une donnée par un seul paquet.

III-1-1 Détermination des paramètres du codage.

Pour la transmission envisagée , les messages échangés entre les automatismes de pilotage fixe et embarqués ont un nombre de bits d'information **k** de l'ordre de 90 à 100 bits.

.

Les hypothèses prises pour la recherche d'un code de détection d'erreurs sont les suivantes :

- La probabilité d'erreur moyenne par bit ,P, est de l'ordre de 10^{-3} .

- Nous considérons dans ce qui va suivre que la distribution des erreurs est indépendante sur les bits .

En tenant compte de ces hypothèses , nous pouvons utiliser les inégalités (7) et (12) pour déterminer la distance entre les mots du code et le nombre de bits de contrôle **m** dans un message .

$$\frac{|\mathrm{Log}_{10}\, q|}{n} \leqslant E\left(\frac{d}{n}, p\right) \qquad (7)$$

$$\frac{n-k}{n} \geqslant H_2\left(\frac{d}{2n}\right) \qquad (12)$$

Nous traçons les fonctions ci-dessus pour **n = 127** et **k=99** .

Nous constatons que la probabilité de non détection d'erreurs est respectée , c'est à dire inférieure à 10^{-10} , pour une distance minimale entre les mots du code d_{min} vérifiant :

. $8 < d_{min} < 10$ (Voir Figure 8)

Par la suite , nous chercherons un code de détection d'erreurs de distance minimale vérifiant les inégalités ci-dessus .

III-1-2 Code de détection d'erreurs choisi.

Le code choisi est un code cyclique défini par son polynôme générateur g(x).(Le lecteur se reportera au chapitre I pour la définition des codes cycliques).

$$g(x) = x^{28} + x^{27} + x^{23} + x^{21} + x^{18} + x^{16} + x^{14} + x^{13} + x^{12} + x^{11} + x^{8} + x^{5} + x^{4} + x^{3} + x^{2} + x + 1 .$$

a)_Codage .

Si on appelle **N(x)** le polynôme d'information utile à coder, de degré maximal **(k-1) = 98** , alors le polynôme code **M(x)** est égal à :

$$M(x) = g(x).N(x) .$$

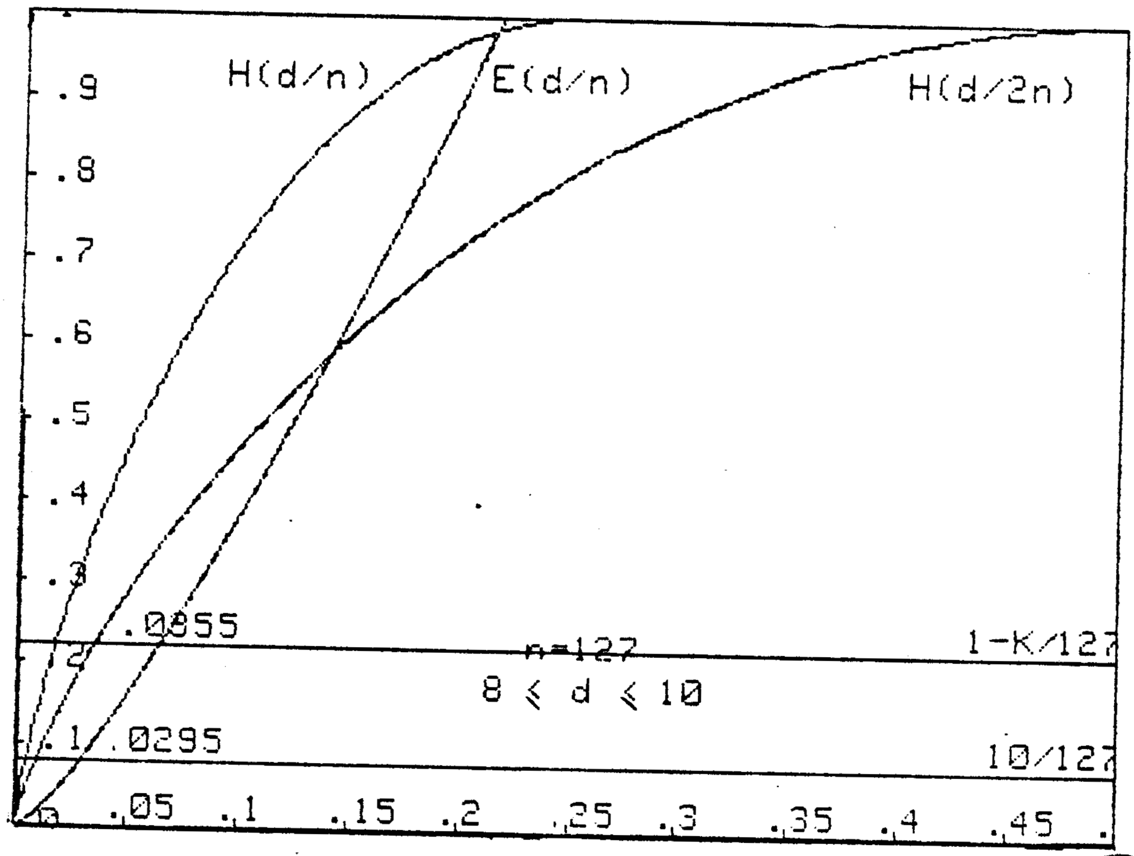

H(d/n)
E(d/n)
H(d/2n)
.9
.8
.7
.6
.5
.4
.3
.2
.1
.0855
.0295
n=127
8 ⩽ d ⩽ 10
1-K/127
10/127
.05
.1
.15
.2
.25
.3
.35
.4
.45

Figure 8

Pour rendre ce code systématique , on effectue les étapes suivantes :

1°) On multiplie **N(x)** par $x^m = x^{28}$.

2°) On effectue la division de $x^{28}.N(x)$ par **g(x)**.

3°) On additionne le reste **R(x)** de degré maximal 27 au polynôme $x^{28}.N(x)$.
On obtient le mot code :

$M(x) = x^{28}.N(x) + R(x)$.

M(x) sera le message transmis à travers le canal de transmission .

b) Décodage du code C(127,99) .

Si le processus de transmission n'introduit pas d'erreur , le polynôme **M'(x)** qui représente le mot reçu , divisé par **g(x)** donnera un reste nul .

Si le reste est différent de zéro , alors **M'(x)** n'est pas un mot du code .

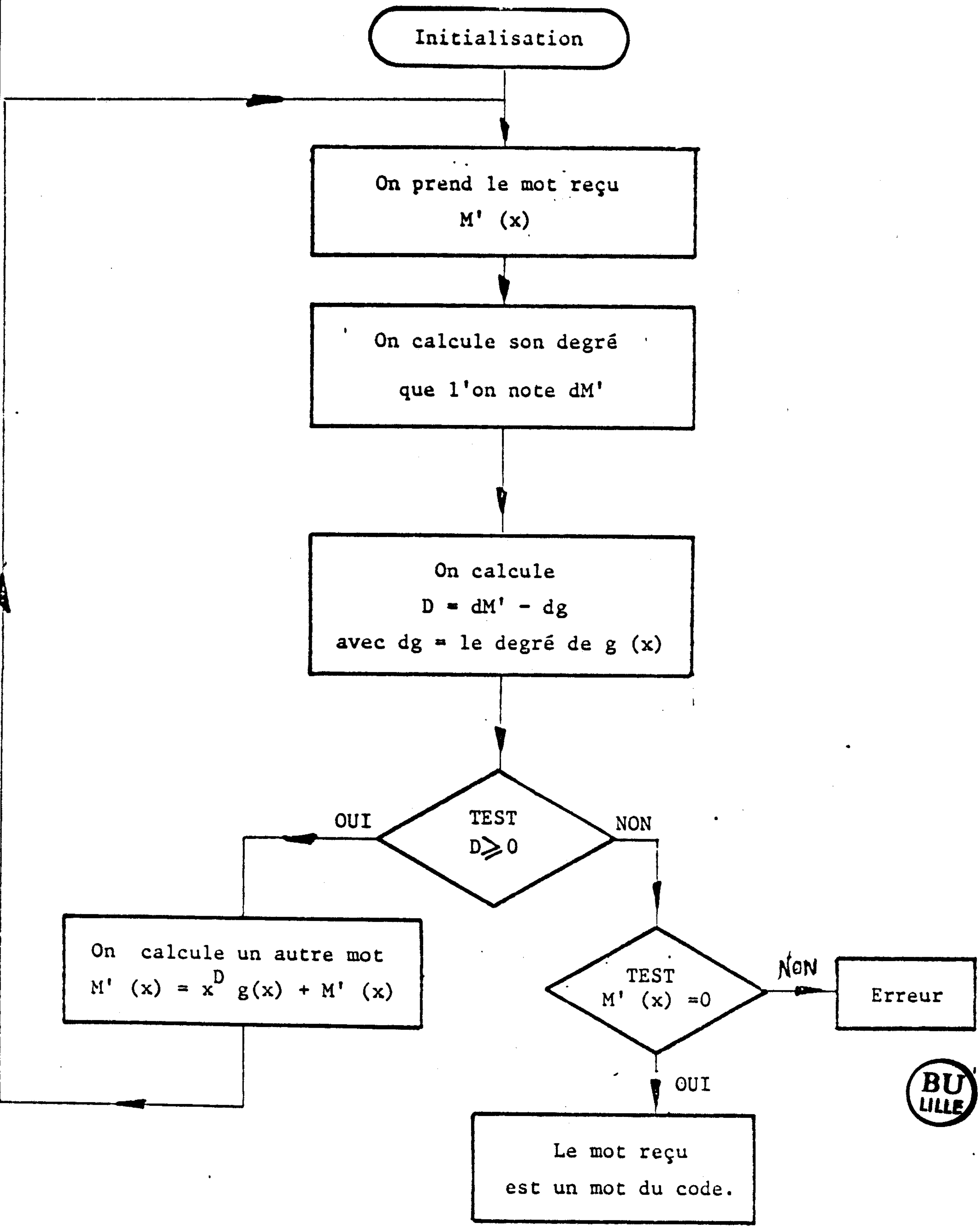
(Voir page suivante pour l'organigramme de détection des erreurs)

c) Capacité de détection d'erreurs .

Le code choisi est un code de distance minimale entre les mots du code de $d_{min} = 9$.
Il peut donc détecter jusqu'à **8 erreurs** indépendantes et il peut détecter un paquet d'erreurs de longueur $l < 28$.
Il nous a semblé utile de mentionner la détection des paquets d'erreurs bien que nous ne les ayons pas pris en considération dans l'estimation de la probabilité de non détection d'erreurs .

d) Rendement du code de détection d'erreurs .

Le rendement d'un code est par définition :



Organigramme de la détection des erreurs

$$R = \frac{k}{n(1+np)} = \frac{99}{127(1+127.10^{-3})} \# \ 69\ \%$$

donc 69 % sont alloués à l'information utile .
Il reste 31 % du nombre total de symboles pour la redondance .

e) Estimation de la probabilité de non détection d'erreurs .

Nous avons montré dans le Chapitre II que l'estimation de la probabilité de non détection d'erreurs est donnée par l'équation :

$$PND \lesssim 10^{-E(d/n,P)\cdot n}$$

$H(P) = H(10^{-3}) = 0{,}00343$

$H'(P) = 2{,}9996$

$H(d/n) = H(9/127) = 0{,}11015$

Ce qui donne : **PND** $< 1{,}15 \cdot 10^{-13}$.

Remarque:

Afin d'améliorer encore la sécurité de la transmission , on peut envisager un autre code de distance minimale entre les mots du code, $d_{min} = 11$ et dont le polynôme générateur est :

$$g_n(x) = g(x).(x^7 + x^5 + x^4 + x^3 + 1)$$

où $g(x)$ est l'ancien polynôme générateur .

Dans ce cas l'estimation de **PND** est donnée par :

PND $< 1{,}59 \cdot 10^{-17}$.

Malheureusement , on perd sur le rendement et sur le nombre de bits d'information .

n = 127 bits
m = 35 bits
k = 92 bits .

Le rendement est :

$$R = \frac{92}{127.(1+127.10^{-3})} \# 64\ \%$$

III-2 Code de détection d'erreurs en cas de diffusion d'une donnée par des paquets de 8 bits (octets).

III-2-1 Introduction.

Les microprocesseurs sécuritaires à 8 ,16 ou 32 bits , utilisés dans le domaine des transports peuvent être envisagés dans la transmission des messages de sécurité entre les pilotages automatiques fixe et embarqués .

Ceci nous a amené à considérer un autre code basé sur l'hypothèse suivante :

- Les messages sont émis en séquences dans un format de base , chaque format comportant un nombre fixe d'octets .

La structure du message peut donc être la suivante :

Format 1	......	Format R	Format R+1 ......

Comme le nombre de bits d'information est de l'ordre de 100, alors le nombre de bits d'information **k** peut prendre un nombre fixe d'octets que l'on considérera n'excédant pas 15 .

Avec cette condition , la numérotation des octets peut prendre **4 bits** ($2^4 - 1 = 15$) , ce qui donne une information de la forme :

numéro d'octet sur 4 bits	Octet d'information utile	....

Pour l'ensemble "information utile et sa numérotation " il faut 12 bits .

Avec les mêmes hypothèses que pour l'autre code, nous pouvons utiliser les inégalités (7) et (12) du chapitre II afin de déterminer la distance entre les mots du code et le nombre de bits de contrôle **m** dans un message .

On constate sur la figure 9 que l'objectif de sécurité peut être obtenu pour **n=24** lorsque la distance minimale entre les mots du code est :

$$6 \leqslant d_{min} \leqslant 6$$

Donc les mots du code peuvent être émis dans un format de base de 3 octets , (3 . 8 = 24) .

III-2-2 Code de détection d'erreurs choisi.

Le code choisi est un code de Golay modifié , (Réf 2) , dont la distance minimale est $d_{min} = 8$ pour $n = 24$ bits et dont le polynôme générateur est :

$$g(x) = x^{12} + x^{10} + x^7 + x^4 + x^3 + x^2 + x + 1.$$

Le nombre de bits d'information est $k = 12$, se qui représente l'information utile et son numéro .

Le nombre de bits de redondance est $m = 12$.

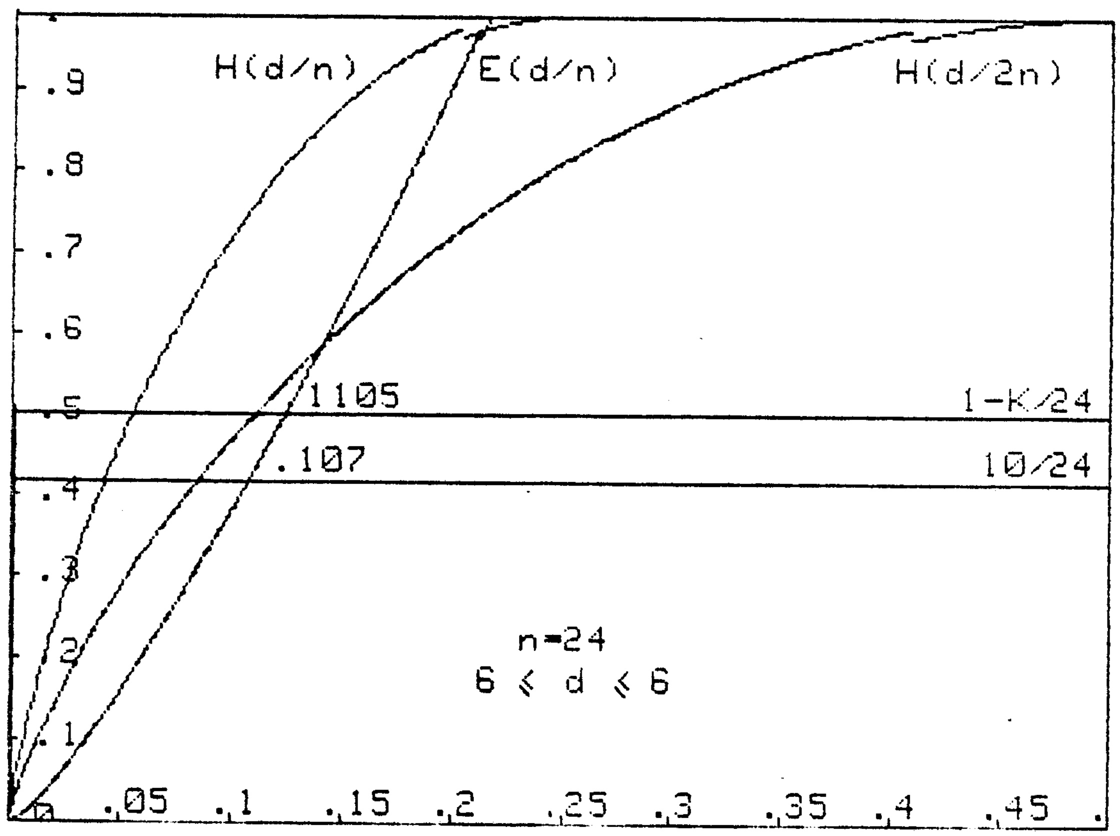

H(d/n)
E(d/n)
H(d/2n)
.9
.8
.7
.6
.5
.4
.3
.2
.1
.1105
1-K/24
.107
10/24
n=24
6 ≤ d ≤ 6
.05
.1
.15
.2
.25
.3
.35
.4
.45

Figure 9

a) Codage et décodage.

Les codage et décodage de ce code sont les mêmes que ceux explicités précédemment .

b) Capacité de détection .

Le code choisi peut détecter jusqu'à 7 **erreurs** indépendantes sur un message de 24 bits .
Il peut de même détecter un paquet d'erreurs de longueur **$l < 12$.**

c) Rendement du code .

Le rendement du code est :

$$R = \frac{k}{n(1+np)} = \frac{12}{24.(1+24.10^{-3})} \# 1/2 = 50\%$$

Le code choisi est efficace pour la détection d'erreur mais il possède un rendement faible .

d) Estimation de la probabilité de non détection d'erreurs par message .

Nous avons montré dans la partie II que l'estimation de la probabilité de non détection d'erreur est donnée par :

$$PND < 10^{-E(d/n,P).n}$$

$$H(P)=H(10^{-3})=0{,}00343$$

$$H'(P)=2{,}9996$$

$$H(d/n)=H(8/24)= 0{,}27542$$

Ce qui donne : $PND < 1{,}26 \,.\, 10^{-14} < 10^{-10}$.

La probabilité de non détection d'erreur , **PND** , est estimée sur un message de 24 bits mais pas sur un message de 15.8 = 120 bits .

III-3 Remarque.

Les codes présentés dans ce chapitre sont des codes qui détectent des erreurs indépendantes et un paquet d'erreurs de longueur $l < m$.

Dans le cas de la détection des paquets d'erreurs seulement on peut envisager les codes de Fire et alors il faut revoir l'estimation de la probabilité de non détection d'erreurs.
Les codes de Fire sont définis par leur polynôme générateur de la forme :

$$g(x) = P(x) . (x^c + 1) ,$$

où $P(x)$ est un polynôme irréductible de degré b .

L'ordre e du polynôme irréductible n'est pas divisible par c .
La longueur n d'un code ainsi défini est le plus petit commun multiple de e et c :

$$n = PPCM (e,c) .$$

Les codes de Fire sont capables de détecter n'importe quelle combinaison de deux paquets , si la longueur du plus petit des deux ne dépasse pas b et que la somme des deux longueurs ne dépasse pas $c+1$.

Il peuvent également détecter tout paquet unique de longueur $l < m$ avec $m = c+b$.

Exemple d'un code de Fire.

Le code de Fire choisi est un code défini par :

$$g(x) = (x^{13} + 1).(x^6 + x^3 + 1) .$$

L'ordre du polynôme irréductible (x^6+x^3+1) est **9** .

Le nombre total **n** dans un mot code est :

n = PPCM (13,9) = 117 .

Il détecte un paquet d'erreurs de longueur $1 < 13+6$ et il peut également détecter n'importe quelle combinaison de deux paquets , si la longueur du plus petit des deux ne dépasse pas **6** et que la somme des deux longueurs ne dépasse pas **13+1 = 14** .

C O N C L U S I O N

CONCLUSION .

L'objectif de l'étude proposée dans cette thèse est d'apporter une solution au problème de la sécurité des transmissions numériques .

Parmi les solutions envisagées , nous avons retenu celle qui consiste à utiliser les codes de détection d'erreurs puisque ceux-ci permettent d'effectuer une démonstration mathématique de la sécurité de la transmission .

Le principe général des codes de détection d'erreurs consiste à ajouter aux symboles d'information utiles , des symboles supplémentaires permettant à la réception de détecter des erreurs introduites par le canal de transmission.

Nous avons pu ainsi établir une relation liant l'objectif de sécurité , la probabilité d'erreurs du canal de transmission ,le nombre de symboles d'information utiles ,aux caractéristiques du code ,soit la distance minimale entre les mots du code et le nombre total de symboles contituant le mot code .

Nous concluons alors que toute transmission utilisant les codes de détection d'erreurs et qui satisfait à la relation précédemment définie sera en sécurité , sous réserve qu'elle vérifie les hypothèses prises en considération .

Une hypothèse de travail reste en effet à vérifier : Il s'agit de la modélisation des erreurs que nous avons considérées comme apparaissant individuellement par bit .

Pour compléter cette étude , des travaux restent donc à effectuer notamment lorsque l'on considère que les erreurs se manifestent sous forme de "paquets d'erreurs" .

Dans ces conditions , il reste à vérifier que la formule liant l'objectif de sécurité aux caractéristiques du code est toujours adaptée .

Nous pensons cependant que l'étude mathématique du problème telle que nous l'avons développée est généralisable , attendu que nous n'avons employé que peu d'hypothèses restrictives .

Nous avons utilisé les conclusions de cette étude pour deux applications dans le domaine des transports et nous pensons qu'elles peuvent être utilisées pour toute transmission utilisant des informations de sécurité .

ANNEXES

ANNEXE I

EXEMPLES DE CODES LINEAIRES : CODES DE HAMMING .

I-DEFINITION.

Les codes de Hamming sont des codes linéaires **L(n,k)**, de distance minimale 3 , définis par :

$n = (2^m - 1)$, **m** étant le nombre de bits de contrôle .

$k = n - m$, **k** étant le nombre de bits d'information .

Ces codes sont capables de corriger une erreur simple et de détecter 2 erreurs .

Les colonnes de la matrice de contrôle **(H)** satisfont aux relations :

$h_{i_o} \neq 0$ pour $i_o = 0 , \ldots , (n-1)$.

$h_{i_o} + h_{i_1} \neq 0$ pour $i_o , i_1 = 0 , \ldots , (n-1)$
$i_o = i_1$.

Pour cela , il suffit de donner aux colonnes de la matrice (H) les valeurs 1 , 2 ,...,**jusqu'à n** , en représentation binaire sur **m** positions .

II-EXEMPLE.

Construction d'un code de Hamming **L(7,4)** .

$n = 2^3 - 1 = 7$

$k = 7 - 3 = 4$

La matrice de contrôle est de la forme :

$$(H) = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Pour avoir un code de Hamming systématique , on remplace la matrice **(H)** par **(H_S)** .

$$(H_S) = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

La matrice génératrice associée à **(H_S)** est :

$$(G_S) = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

III-CODAGE.

Un mot **$\langle M_i \rangle$** est de la forme :

$$\langle M_i \rangle = \langle a_0 a_1 a_2 a_3 c_0 c_1 c_2 \rangle .$$

Pour obtenir les mots du code **$\langle M_i \rangle$** , on multiplie les mots d'information **$\langle N_i \rangle$** par la matrice **(G_S)** .

Soit à coder le mot <1000> , on a :

$$\langle M_i \rangle = \langle N_i \rangle \cdot (G_S) .$$

On trouve alors le mot suivant :

$$\langle 1000110 \rangle .$$

IV-DECODAGE.

A la réception , on obtient un mot $\langle M_i' \rangle = \langle M_i \rangle + \langle E_i \rangle$.

On étudie les deux cas suivants :

1°) $\langle E_i \rangle = 0$ $\langle M_i' \rangle = \langle 1000110 \rangle = \langle M_i \rangle$

On calcule le syndrome d'erreurs :

$\langle S_i \rangle = \langle M_i' \rangle.(H)^t$.

Si on trouve $\langle S_i \rangle = \langle 0 \rangle$ alors le mot reçu est correct.

2°) $\langle E_i \rangle \neq 0$, $\langle E_i \rangle = \langle 0010000 \rangle$

$\langle M_i' \rangle = \langle 1010110 \rangle$.

On calcule le syndrome d'erreurs :

$\langle S_i \rangle = \langle M_i' \rangle.(H)^t = \langle 011 \rangle$.

Si on trouve $\langle S_i \rangle \neq \langle 0 \rangle$ alors le mot reçu est erroné.

ANNEXE II

I-DEFINITION D'UN POLYNOME IRREDUCTIBLE.

Un polynôme **f(x)** de degré **N** qui n'est divisible par aucun polynôme de degré inférieur à N dans le même corps est dit **irréductible** .

II-NOMBRE DE POLYNOMES IRREDUCTIBLES.

Le nombre **Nb(r)** de polynômes irréductibles de degré **r** dans un corps de Galois 2 , (**CG(2)**) satisfait à la relation :

$$\sum_{r=1}^{r=N} r.Nb(r) = 2^N .$$

III-DECOMPOSITION DE (X^n+1) EN POLYNOMES IRREDUCTIBLES.

Les racines de (x^n+1) sont des racines de l'unité .
Si **n** est pair , (n=2p) , alors :

$$x^n + 1 = x^{2p} + 1$$
$$= (x^p + 1).(x^p + 1) \text{ dans } CG(2).$$

Donc l'étude de (x^n+1) se ramène à celle pour laquelle **n** est impair .

Soit un polynôme **f(x)** , irréductible , de degré **m** et qui divise (x^n+1) , n impair .
Ses **m** racines sont : $\beta^{2^0}, \beta^{2^1}, \ldots, \beta^{2^{(m-1)}}$
et qui sont aussi racines de (x^n+1) .
Autrement dit , elles appartiennent à l'ensemble des racines de (x^n+1) , soit :

$$S = \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}\}$$

donc $\beta = \alpha^j \Rightarrow \beta^2 = \alpha^{2j} \Rightarrow \beta^{2^i} = \alpha^{2^i j} = \alpha^r$,

r étant le reste de la division de $2^i. j$ **par n** .

Pour la pratique de la décomposition de (x^n+1) , on débute par $j=1$ .On divise par n les puissances successives de $2^i.j$. On arrête la division lorsque l'on obtient un reste déjà trouvé .
Les racines α^{r_1}, α^{r_2}...etc obtenues sont celles d'un polynôme partiel cherché .
On recommence l'opération pour une nouvelle valeur de j qui donne des restes différents de ceux déjà trouvés .

Exemple :Décomposition de (x^7+1) en polynôme irréductible.

$j=1$

$$2^0 = 1 \quad \text{modulo } 7$$
$$2^1 = 2 \quad \text{modulo } 7$$
$$2^2 = 4 \quad \text{modulo } 7$$
$$2^3 = 1 \quad \text{modulo } 7 .$$

Ce qui donne le polynôme cherché $f_1(x)$:

$$f_1(x) = (x + \alpha).(x + \alpha^2).(x + \alpha^4),\text{de degré } 3.$$

Puis on passe à :

$j=3$

$$3.2^0 = 3 \quad \text{modulo } 7$$
$$3.2^1 = 6 \quad \text{modulo } 7$$
$$3.2^2 = 5 \quad \text{modulo } 7$$
$$3.2^3 = 3 \quad \text{modulo } 7 .$$

Ce qui donne le polynôme cherché $f_3(x)$:

$$f_3(x) = (x + \alpha^3).(x + \alpha^6).(x + \alpha^5),\text{de degré } 3.$$

Donc : $(x^7 + 1) = f_1(x).f_3(x).(x+1)$.

$f_1(x)$ s'écrit :

$$f_1(x) = x^3 + A.x^2 + B.x + 1 .$$

Pour calculer les coefficients **A** et **B** , on cherche les restes de la division de x^n ,$(0<n<7)$ par $x^3 + x^2 + 1$.

On trouve : $A = 1$ et $B = 0$, d'où :

$$f_1(x) = x^3 + x^2 + 1 \quad .$$

De même , pour $f_3(x) = x^3 + A'.x^2 + b'.x + 1$, on trouve :

$A' = 0$ et $B' = 1$, d'où :

$$f_3(x) = x^3 + x + 1 \ .$$

$$\begin{aligned}(x^7+1) &= (x+1).(x^3+x+1).(x^3+x^2+1) \\ &= (x+1).(x^6+x^5+x^4+x^3+x^2+x+1) = A(x).B(x) \\ &= (x^3+x^2+1).(x^4+x^3+x^2+1) = C(x).D(x) \ .\end{aligned}$$

Les 4 polynômes **A(x)** , **B(x)** , **C(x)** et **D(x)** sont des polynômes générateurs de 4 codes cycliques différents

A(x) pour le code cyclique C(7,6) ,
B(x) " " " " " C(7,1) ,
C(x) " " " " " C(7,4) ,
D(x) " " " " " C(7,3) .

IV-EXEMPLE DU CODE CYCLIQUE C(7,3).

Il y a 3 bits d'information et 4 bits de contrôle .

$g(x) = x^4 + x^3 + x^2 + 1$.

Pour un code C(7,3) non systématique,les mots codes sont :

Bits de message	polynôme associé N(x)	polynôme du code N(x).g(x)= M(x)	mots codes
001	1	$x^4+x^3+x^2+1$	0011101
010	x	$x^5+x^4+x^3+x$	0111010
011	x+1	x^5+x^2+x+1	0100111
100	x^2	$x^6+x^5+x^4+x^2$	1110100
101	x^2+1	$x^6+x^5+x^3+1$	1101001
110	x^2+x	$x^6+x^3+x^2+x$	1001110
111	x^2+x+1	x^6+x^4+x+1	1010011

Pour un code C(7,3) systématique , les mots codes sont:

Bits de message	$x^4.N(x)$	$C(x)=x^4.N(x)$ modulo $g(x)$	Polynôme du code	Mots codes
001	x^4	x^3+x^2+1	$x^4+x^3+x^2+1$	0011101
010	x^5	x^2+x+1	x^5+x^2+x+1	0100111
011	x^5+x^4	x^3+x	$x^5+x^4+x^3+x$	0111010
100	x^6	x^3+x^2+x	$x^6+x^3+x^2+x$	1001110
101	x^6+x^4	$x+1$	x^6+x^4+x+1	1010011
110	x^6+x^5	x^3+1	$x^6+x^5+x^3+1$	1101001
111	$x^6+x^5+x^4$	x^2	$x^6+x^5+x^4+x^2$	1110100

Décodage :

Supposons que l'on ait émis un mot du code :
$\langle M_i \rangle = \langle 0111010 \rangle$.

A la réception on obtient un mot :
$\langle M_i' \rangle = \langle M_i \rangle + \langle E_i \rangle$.

Deux cas peuvent se présenter :

a) $\langle E_i \rangle = 0 \qquad \langle M_i' \rangle = \langle M_i \rangle = \langle 0111010 \rangle$.

Le polynôme associé est : $x^5 + x^4 + x^3 + x$

On calcule le syndrome d'erreurs par :

$$S(x) = \text{Reste}\left\{\frac{x^5 + x^4 + x^3 + x}{x^4 + x^3 + x^2 + 1}\right\}$$
$$= 0 .$$

Puisque $S(x) = 0$ alors le mot reçu est correct .

b) $\langle E_i \rangle \neq 0 \qquad \langle M_i' \rangle = \langle M_i \rangle + \langle E_i \rangle$.

Si on suppose que $\langle E_i \rangle = \langle 0010000 \rangle$ alors :

$\langle M_i' \rangle = \langle 0101010 \rangle$, son polynôme associé est :

$M'(x) = x^5 + x^3 + x$.

On calcule le syndrome d'erreurs $S(x)$ défini par :

$$S(x) = \text{Reste}\left\{\frac{x^5 + x^3 + x}{x^4 + x^3 + x^2 + 1}\right\}$$

$$= x^3 + x^2 + 1 \ .$$

Puisque $S(x) \neq 0$, le mot reçu est erroné .

ANNEXE III

MESURE DES QUALITES D'UNE TRANSMISSION DE DONNEES UTILISANT UN CODE DE DETECTION D'ERREURS.

I-NECESSITE DE LA DETECTION.

Quelle que soit la qualité de la transmission d'information , il est inévitable qu'à la réception , quelques symboles , (bits) , binaires soient altérés .
D'où la nécessité d'un code redondant pour la détection d'erreurs .

II-RAPPELS SUR LA MESURE DES QUALITES D'UNE TRANSMISSION.

Pour mesurer les qualités d'une transmission de données, il est nécessaire de définir les grandeurs suivantes , qui sont relatives aux codes et au canal .

II-1 Efficacité E d'un code de détection d'erreurs.

L'efficacité **E** d'un code est le rapport moyen du nombre de messages faux et détectés au nombre total de messages faux.

II-2 Taux d'erreur brut τ.

C'est la proportion moyenne de messages faux reçus qu'ils soient détectés ou non .
Le taux d'erreur brut mesure la qualité intrinsèque de la transmission et il est indépendant du code de détection d'erreurs choisi .
Par contre , il dépend de la loi de probabilité de répartition des erreurs sur le canal .
Si ces erreurs sont indépendantes et ont pour probabilité d'erreur **P** par bit sur un message de longueur **n** bits , on a :

$$\tau = n.P .$$

II-3 Taux d'erreur global par message.

Ce taux d'erreur global **PND** est défini comme étant la proportion de messages finalement faux après épuisement de la procédure de détection .
il mesure la qualité finale de la transmission , c'est à dire celle qui intéresse l'utilisateur .
Donc **PND** est la garantie que nous avons de ne pas laisser passer un message faux .

Il existe une relation liant l'efficacité **E** , le taux d'erreur brut τ et le taux d'erreur global **PND** :

$$PND = \tau(1 - E) + \tau^2 E.(1 - E) + \tau^3 E^2.(1 - E)$$

$$PND \# \tau(1 - E) \quad \text{, pour E voisine de 1 .}$$

III-CARACTERISTIQUES DES CODES DE DETECTION D'ERREURS.

III-1 Nòtion de poids et de distance.

III-1-1 Poids d'un message.

On appelle **poids** d'un message , le nombre de "1" qu'il contient .

III-1-2 Distance entre 2 messages :Distance de Hamming.

On appelle **distance** $d(V_i,V_j)$ entre 2 messages V_i et V_j , la quantité :

$$d(V_i,V_j) = \sum_{k=1}^{k=n} (a_{ik} \oplus a_{jk})$$

$\oplus$ étant l'addition modulo 2

avec : $V_i = < a_{i1} \ldots a_{ik} \ldots a_{in} >$
$V_j = < a_{j1} \ldots a_{jk} \ldots a_{jn} >$.

On note **d** la distance minimale entre les mots d'un code .

La distance minimale entre les mots d'un code est un paramètre qui conditionne la capacité de détection et de correction d'un code .

III-2 Relation entre la distance minimale entre les mots d'un code et le nombre de corrections ou de détection des erreurs dans un mot code .

III-2-1 Détection des erreurs.

Pour détecter **t** erreurs , il faut que la distance minimale entre les mots du code soit :

$$d = t + 1 .$$

III-2-2 Correction des erreurs.

Un code est capable de corriger **e** erreurs si la distance minimale entre les mots du code **d** est au moins égale à :

$$d = 2e + 1 .$$

III-3 Relation entre le nombre de bits de contrôle et le nombre de bits d'information.

III-3-1 Condition nécessaire.

Pour corriger **e** erreurs , il est nécessaire d'avoir :

$$2^{n-k} \geq \sum_{i=0}^{i=e} C_n^i$$

C'est la **marge inférieure de Hamming** .

k est le nombre de bits d'information .

n est le nombre total des bits dans un mot du code

III-3-2 Condition suffisante.

Pour corriger e erreurs , il suffit d'avoir :

$$2^m \geq \sum_{i=0}^{i=2e-1} C_n$$

C'est la **marge de Warchanov - Gilbert** .

Cette condition n'est pas nécessaire .

V- LES DIFFERENTES SORTES D'ERREURS .

IV-1 Les erreurs individuelles :

Si on suppose que chaque symbole transmis est affecté de manière indépendante par les perturbations , les erreurs qui apparaissent seront indépendantes les unes des autres.

IV-2 Paquets d'erreurs :

Si les perturbations ont une durée plus longue que la durée d'un bit ,les erreurs apparaîtront groupées.
On dit alors qu'il se présente " des paquets d'erreurs".
On définit un paquet d'erreurs de la façon suivante :

-Deux séquences en erreurs correspondent à des paquets d'erreurs séparés s'il existe au moins entre ces deus paquets 10 bits binaires consécutifs non erronés.

-Pour une séquence d'erreurs correspondant à un seul paguet ,la longueur du paquet , l ,est le nombre binaire qui constitue cette séquence.

-A l'intérieur d'un paquet d'erreurs ,il peut exister des bits binaires non erronés.

ANNEXE IV

Cette annexe contient une inégalité utile pour la démonstration de l'expression (7) de ce document estimant la sécurité probabiliste d'une transmission numérique utilisant un code de détection d'erreurs .

De même , elle est utile pour la démonstration de l'expression (12) de ce document justifiant l'existence d'un code de détection d'erreurs , (condition nécessaire mais pas suffisante) .

Cette inégalité est la suivante :

$$\sum_{i=\lambda.n}^{i=n} C_i^n.P^i.Q^{n-i} \leqslant (\lambda)^{-\lambda n}.(\mu)^{-\mu n}.P^{\lambda n}.(1-P)^{\mu n} \quad . \qquad (\textbf{A.1})$$

$$C_i^n = \frac{n!}{i!.(n-i)!} \qquad ; \quad \lambda \leqslant 1 \quad .$$

L'inégalité est vraie pour $\lambda > P$, $Q = (1-P)$ et $\lambda = 1-\mu$.

En posant **P = 1/2** et en multipliant les 2 membres de cette inégalité par 2^n , on obtient :

$$\sum_{i=\lambda n}^{i=n} C_i^n \leqslant (\lambda)^{-\lambda n}.(1-\lambda)^{-n(1-\lambda)} \qquad (\text{A.2})$$

Pour $\lambda > 1/2$.

L'inégalité **(A.1)** est un cas particulier de l'inégalité de **Chernoff** .
La démonstration de l'inégalité **(A.1)** peut se faire en majorant la distribution binômiale par une suite géométrique puis en surestimant le coefficient C_n (0< <1) La démonstration de l'inégalité **(A.1)** se fait donc en deux étapes :

<u>1°) Majoration de la distribution binômiale</u> :

La distribution binômiale peut être majorée de la façon suivante :

$$\sum_{i=\lambda n}^{i=n} C_i^n.P^i.Q^{n-i} < \frac{\lambda.Q}{\lambda - P} C_n^{\lambda n}.P^{\lambda n}.Q^{\mu n} \qquad (\text{A.3})$$

L'inégalité (A.3) est obtenue en majorant cette somme par une série géométrique . En effet :

$$\sum_{i=\lambda n}^{i=n} C_i^n.P^i.Q^{n-i} = C_{\lambda n}^n.P^{\lambda n}.Q^{\ n} + C_{\lambda n+1}^n.P^{\ n+1}.Q^{\ n-1}+\ldots+C_n^n.P^n$$

$$= C_{\lambda n}^n.P^{\lambda n}.Q^{\mu n}.(1+ \frac{C_{\lambda n+1}^n}{C_n}.(\frac{P}{Q}) +\ldots+\frac{C_n^n}{C_{\lambda n}^n}(\frac{P}{Q})^{\mu n})$$

Une estimation de $\frac{C_{\lambda n+i}^n}{C_{\lambda n}^n}$ est :

$$\frac{C_{\lambda n+i}^n}{C_{\lambda n}^n} = \frac{(\ n)!.(\mu n)!}{(\lambda n+i)!.(\mu n-i)!}$$

$$= \frac{(\mu n-i+1).(\mu n-i+2)\ldots.(\mu n)}{(\lambda n+1).(\lambda n+2)\ldots.(\lambda n+i)}$$

$$= \frac{(\mu-(i-1)/n).(\mu-(i-2)/n)\ldots.(\mu\ )}{(\lambda+1/n).(\lambda+2/n)\ldots\ldots (\lambda+i/n)}$$

$$\leqslant \underbrace{(\mu/\lambda).(\mu/\lambda)\ \ldots\ldots\ldots\ldots\ldots.(\mu/\lambda)}_{\text{i fois}} = (\mu/\lambda)^i .$$

Donc :

$$\sum_{i=\lambda n}^{i=n} C_i^n.P^i.Q^{n-i} \leqslant C_{\lambda n}^n.P^{\ n}.Q^{\ n}.(1+(\mu/\lambda).(P/Q)+\ldots+(\mu/\lambda)(P/Q)^{\mu n})$$

$$\leqslant C_{\lambda n}^n.P^{\lambda n}.Q^{\mu n}.(\frac{1-(\mu/\lambda).(P/Q)^{\mu n}}{1-(\mu/\lambda).(P/Q)})$$

$$\leqslant \frac{\lambda Q}{\lambda - P}.C_{\lambda n}^n.P^{\lambda n}.Q^{\mu n} \qquad \text{avec } \lambda > P$$

<u>2°) Surestimation du coefficient</u> : $C_{\lambda n}^n = \frac{n!}{(\lambda n)!(\mu n)!}$

On utilise l'approximation de Stirling soit :

$$n! = \sqrt{2\pi n}.n^n.e^{-n}.\exp(\frac{1}{12n} - \frac{1}{360n^3} + \ldots.) \qquad (A.4)$$

Il est connu que **n!** est sous estimé si l'expression (A.4) s'arrête au terme $(-1/360n^3)$ et **n!** est surestimé si l'expression s'arrête au terme $(1/12n)$.

D'où la formule (A.5) :

$$\sqrt{2\pi n}\,.n^n.e^{-n}.\exp\left(\frac{1}{12n}-\frac{1}{360n^3}\right) < n! < \sqrt{2\pi n}.n^n.e^{-n}.\exp\left(\frac{1}{12n}\right)$$

Pour obtenir une surestimation de C_n ,on minore $(\lambda n)!$ et $(\mu n)!$ et on majore le numérateur soit n! en utilisant l'expression (A.5).

On obtient donc :

$$\frac{n!}{(\lambda n)!.(\mu n)!} < \frac{(\lambda)^{-\lambda n}.(\mu)^{-\mu n}}{\sqrt{2\pi n\lambda\mu}}.\exp\left(\frac{1}{12n}-\frac{1}{12\ n}-\frac{1}{12\ n}+\frac{1}{360(\ n)^3}+\frac{1}{360(\ n)^3}\right)$$

Cette expression est symétrique en λ et μ .

Si on suppose que $\lambda > \mu$ alors :

$$\frac{1}{360(\lambda n)^3} < \frac{1}{360(\mu n)^3} < \frac{1}{360(\mu n)}$$

et on a : $\frac{1}{12n} < \frac{1}{12\lambda n}$ puisque $0 < \lambda < 1$.

donc :

$$\frac{1}{12n}-\frac{1}{12\lambda n}-\frac{1}{12\mu n}+\frac{1}{360(\lambda n)^3}+\frac{1}{360(\mu n)^3} < \frac{1}{12n}-\frac{1}{12\lambda n}-\frac{1}{12\mu n}+\frac{1}{180\mu n}$$

$$< \frac{1}{12n}-\frac{1}{12\lambda n}-\frac{7}{90\mu n}$$

$$< 0$$

Une surestimation de $C^n_{\lambda n}$ est alors :

$$C^n_{\lambda n} < \frac{1}{\sqrt{2\pi n\lambda\mu}}.\lambda^{-\lambda n}.\mu^{-\mu n} \qquad (\text{A.6})$$

En tenant compte des inégalités (A.3) et (A.6),on obtient :

$$\sum_{i=\lambda n}^{i=n} C^n_i.P^i.Q^{n-i} \leqslant \lambda^{-\lambda n}.\mu^{-\mu n}.(P)^{\lambda n}.(Q)^{\mu n} \qquad (\text{C.Q.F.D}) .$$

La démonstration de l'estimation de la sécurité probabiliste , expression (7) , s'appuie sur l'inégalité (A.1) que nous venons de démontrer .

Nous avons montré dans ce document que le taux d'erreurs global était approximé à :

$$\mathbf{PND} \# \sum_{i=d}^{i=n} C_i^n . P^i . (1 - P)^{n-i} .$$

En utilisant l'inégalité **(A.1)** et en posant : $\lambda n = d$, on obtient :

$$\sum_{i=d}^{i=n} C_i^n . P^i . (1-P)^{n-i} < (d/n)^{-d} . (1-d/n)^{-(n-d)} . P^d . (1-P)^{(n-d)} .$$

L'inégalité est vraie pour **(d/n) > P** .

Donc pour tenir compte de **"l'objectif de sécurité" q** , il faut parvenir à une valeur de probabilité de non détection d'erreurs **(PND)** telle que :

$$\mathbf{PND} < q .$$

Pour s'assurer de cela , on doit avoir :

$$(d/n)^{-d} . (1-d/n)^{-(n-d)} . P^d . (1-P)^{(n-d)} < q \qquad (A.7) .$$

La suite du calcul fait appel à l'entropie , celle-ci étant égale à la quantité d'information moyenne contenue dans l'apparition d'un symbole .

On rappelle que l'entropie d'une source binaire , (valeurs émises 0 ou 1) , ayant une probabilité d'erreurs **P** sur les valeurs émises , s'écrit :

$$H(P) = -P . \log P - (1-P) . \log(1-P) \qquad (A.8) .$$

La dérivée de **H(P)** par rapport à **P** est :

$$H'(P) = - \log (P/(1-P)) \qquad (A.9) .$$

Donc le logarithme à base 10 de l'expression **(A.7)** s'écrit

$$-d.\log(d/n) - (n-d).\log(1-d/n) + d.\log P + (n-d).\log(1-P) < \log q \; .$$

En multipliant les 2 membres par **1/n** , on obtient :

$$-(d/n).\log(d/n) - (1-d/n).\log(1-d/n) + d/n.\log P + (1-d/n).\log(1-P) \leqslant 1/n.\log q \; .$$

Par la suite , on va essayer de faire apparaître : **H(d/n)**, **H(P)** et **H'(P)** . D'où l'inégalité :

$$H(d/n) + (d/n).\log P + (1-d/n).\log(1-P) \leqslant (1/n).\log q \; .$$

En ajoutant **P.logP** et **(1-P).log(1-P)** puis en les retranchant au premier membre de l'inégalité , on obtient à l'aide des expressions **(A.8)** et **(A.9)** :

$$H(d/n) - H(P) - (d/n - P).H'(P) \leqslant (1/n).\log q \; ;$$

Comme **q<1** , on a **logq < 0** , donc on obtient :

$$\boxed{\frac{|\log q|}{n} \leqslant E(d/n\, , P) \qquad (\text{C.Q.F.D.})}$$

$$\boxed{\text{Avec : } E(d/n,P) = -H(d/n) + h(P) + (d/n - P).H'(P)} \; .$$

Il reste à montrer l'expression (12) de ce document , soit :

$$\frac{n-k}{n} \leqslant H_2(d/2n) \qquad (12)$$

Avec **k** : Nombre de bits d'information dans un message .
n : Nombre total de bits dans un message .

La démonstration de cette inégalité s'appuie sur la marge inférieure de **Hamming** qui est :

$$\sum_{i=0}^{i=\left[\frac{d-1}{2}\right]} C_i^n < 2^{n-k}$$

L'expression $\sum_{i=0}^{i=\left[\frac{d-1}{2}\right]} C_n^i$ peut s'écrire :

$$\sum_{i=0}^{i=\frac{d-1}{2}} C_n^i = \sum_{i=n-\left[\frac{d-1}{2}\right]}^{i=n} C_n^i < \sum_{i=n-\frac{d}{2}}^{i=n} C_n^i$$

De même , on a :

$$\sum_{i=n-\frac{d}{2}}^{i=n} C_n^i \leqslant (1-d/2n)^{-(n-d/2)} \cdot (d/2n)^{-n(d/2n)} .$$

$$\leqslant (1-d/2n)^{-(n-d/2)} \cdot (d/2n)^{-d/2} .$$

Cette inégalité est vraie pour : $1-\frac{d}{2n} > 1/2$

$$(1-d/2n) > 1/2$$
$$d/2n < 1/2$$
$$d < n \quad \text{toujours vrai} ..$$

Comme précédemment et en utilisant le logarithme à base 2, on a :

$$\log_2(2^{n-k}) \geqslant \log_2 \quad (1-d/2n)^{-(n-d/2)} \cdot (d/2n)^{-d/2} .$$

$$\frac{n-k}{n} \geqslant -(1-d/2n).\log_2(1-d/2n) - (d/2n).\log_2(d/2n)$$

De par la définition de l'entropie , on peut écrire :

$$\boxed{\frac{n-k}{n} \geqslant H_2(d/2n) \qquad (\text{ C.Q.F.D.})}$$

Avec :

$$H_2(d/2n) = -(d/2n).\log_2(d/2n) - (1-d/2n).\log_2(1-d/2n).$$

ANNEXE V

A SHORT TABLE OF THE ENTROPY FUNCTION (BASE 10) AND ITS FIRST DERIVATIVE

P	H	DH/DX	P	H	DH/DX	P	H	DH/DX	P	H	DH/DX
.00001	.00005	5.0000	.0001	.00044	4.0000	.001	.00343	2.9996	.01	.02432	1.9956
00002	.00010	4.6990	0002	.00083	3.6989	002	.00627	2.6981	02	.04258	1.6902
00003	.00015	4.5229	0003	.00119	3.5227	003	.00887	2.5216	03	.05852	1.5097
00004	.00019	4.3979	0004	.00153	3.3978	004	.01133	2.3962	04	.07274	1.3802
00005	.00024	4.3010	0005	.00187	3.3008	005	.01367	2.2989	05	.08621	1.2788
00006	.00028	4.2218	0006	.00219	3.2216	006	.01593	2.2192	06	.09857	1.1950
00007	.00032	4.1549	0007	.00251	3.1546	007	.01811	2.1519	07	.11015	1.1234
00008	.00036	4.0969	0008	.00282	3.0966	008	.02024	2.0934	08	.12107	1.0607
00009	.00040	4.0457	0009	.00313	3.0454	009	.02230	2.0418	09	.13139	1.0048
00010	.00044	4.0000	0010	.00343	2.9996	010	.02432	1.9956	10	.14118	0.9542
00011	.00048	3.9586	0011	.00373	2.9581	011	.02630	1.9538	11	.15049	0.9080
00012	.00052	3.9208	0012	.00403	2.9203	012	.02823	1.9156	12	.15935	0.8653
00013	.00056	3.8860	0013	.00432	2.8855	013	.03013	1.8804	13	.16781	0.8256
00014	.00060	3.8538	0014	.00460	2.8533	014	.03199	1.8477	14	.17587	0.7884
00015	.00064	3.8238	0015	.00489	2.8233	015	.03382	1.8173	15	.18358	0.7533
00016	.00068	3.7958	0016	.00517	2.7952	016	.03563	1.7889	16	.19095	0.7202
00017	.00071	3.7695	0017	.00545	2.7688	017	.03740	1.7621	17	.19799	0.6886
00018	.00075	3.7447	0018	.00572	2.7439	018	.03915	1.7368	18	.20472	0.6585
00019	.00079	3.7212	0019	.00599	2.7204	019	.04088	1.7129	19	.21116	0.6297
00020	.00083	3.6989	0020	.00627	2.6981	020	.04258	1.6902	20	.21732	0.6021
00021	.00086	3.6777	0021	.00653	2.6769	021	.04426	1.6686	21	.22321	0.5754
00022	.00090	3.6575	0022	.00680	2.6566	022	.04592	1.6479	22	.22863	0.5497
00023	.00094	3.6382	0023	.00707	2.6373	023	.04755	1.6282	23	.23420	0.5248
00024	.00097	3.6197	0024	.00733	2.6187	024	.04917	1.6092	24	.23933	0.5006
00025	.00101	3.6020	0025	.00759	2.6010	025	.05077	1.5911	25	.24422	0.4771
00026	.00105	3.5849	0026	.00785	2.5839	026	.05235	1.5736	26	.24888	0.4543
00027	.00108	3.5685	0027	.00811	2.5675	027	.05392	1.5567	27	.25331	0.4320
00028	.00112	3.5527	0028	.00836	2.5516	028	.05547	1.5405	28	.25752	0.4102
00029	.00115	3.5375	0029	.00862	2.5363	029	.05700	1.5248	29	.26151	0.3889
00030	.00119	3.5227	0030	.00887	2.5216	030	.05852	1.5097	30	.26530	0.3680
00031	.00122	3.5085	0031	.00912	2.5073	031	.06002	1.4950	31	.26887	0.3475
00032	.00126	3.4947	0032	.00937	2.4935	032	.06151	1.4807	32	.27225	0.3274
00033	.00129	3.4813	0033	.00962	2.4801	033	.06298	1.4669	33	.27542	0.3076
00034	.00133	3.4684	0034	.00987	2.4670	034	.06444	1.4535	34	.27840	0.2881
00035	.00136	3.4558	0035	.01011	2.4544	035	.06589	1.4405	35	.28118	0.2688
00036	.00140	3.4435	0036	.01036	2.4421	036	.06732	1.4278	36	.28378	0.2499
00037	.00143	3.4316	0037	.01060	2.4307	037	.06874	1.4154	37	.28618	0.2311
00038	.00146	3.4201	0038	.01084	2.4186	038	.07015	1.4034	38	.28840	0.2126
00039	.00150	3.4088	0039	.01109	2.4072	039	.07155	1.3917	39	.29043	0.1943
00040	.00153	3.3978	0040	.01133	2.3962	040	.07294	1.3802	40	.29229	0.1761
00041	.00157	3.3870	0041	.01156	2.3854	041	.07431	1.3690	41	.29396	0.1581
00042	.00160	3.3766	0042	.01180	2.3749	042	.07568	1.3581	42	.29545	0.1402
00043	.00163	3.3663	0043	.01204	2.3647	043	.07703	1.3474	43	.29676	0.1224
00044	.00167	3.3564	0044	.01228	2.3546	044	.07837	1.3370	44	.29790	0.1047
00045	.00170	3.3466	0045	.01251	2.3448	045	.07970	1.3268	45	.29865	0.0872
00046	.00173	3.3370	0046	.01274	2.3352	046	.08102	1.3168	46	.29964	0.0696
00047	.00177	3.3277	0047	.01298	2.3259	047	.08234	1.3070	47	.30025	0.0522
00048	.00180	3.3186	0048	.01321	2.3167	048	.08364	1.2974	48	.30068	0.0348
00049	.00183	3.3096	0049	.01344	2.3077	049	.08493	1.2880	49	.30094	0.0174
00050	.00187	3.3008	0050	.01367	2.2989	050	.08621	1.2788	50	.30103	0.0000
00051	.00190	3.2922	0051	.01390	2.2902	051	.08749	1.2697			
00052	.00193	3.2838	0052	.01413	2.2817	052	.08875	1.2608			
00053	.00197	3.2755	0053	.01436	2.2734	053	.09001	1.2521			
00054	.00200	3.2674	0054	.01458	2.2653	054	.09126	1.2435			
00055	.00203	3.2594	0055	.01481	2.2572	055	.09250	1.2351			
00056	.00206	3.2516	0056	.01504	2.2494	056	.09373	1.2268			
00057	.00210	3.2439	0057	.01526	2.2416	057	.09495	1.2186			
00058	.00213	3.2363	0058	.01548	2.2340	058	.09617	1.2106			
00059	.00216	3.2289	0059	.01571	2.2266	059	.09737	1.2027			
00060	.00219	3.2216	0060	.01593	2.2192	060	.09857	1.1950			

BIBLIOGRAPHIE

REFERENCES BIBLIOGRAPHIQUES

(1) **G.Cullman**
"Codes détecteurs et correcteurs d'erreurs".
Dunod 1967.

(2) **J.Clavier,G.Coffinet,N.Niquil,F.Behr**
"Théorie et technique de la transmission des données"

(3) **Peterson Wesly**
"Error correcting code".
M.I.T Press 1961 .

(4) **A.Spataru**
"Théorie de la transmission de l'information".
Tome 2 : Codes et Décisions .
Masson et Cie 1973 .

(5) **F.Corr , E.Gorog**
"Les codes capables d'assurer une sécurité contre les erreurs dans la transmission des données" .
Revue "Onde électrique" , Année 1963 n°431 .

(6) **Sikk Leung Yan Cheong , Martin E.Hellman**
"Concerning a bound on undetected error probability".
Revue IEEE Transactions on information theory ,
Vol : IT 22 , pp 235-237 , Mars 1976 .

(7) **J.P Dubus**
"Cours sur la théorie de transmission de l'information et le traitement du signal" .
Fascicules 1 , 2 et 3 . U.S.T.L , UER I.E.E.A.

(8) **Abdellah Mahdi**
"Codes auto-correcteurs d'erreurs adaptés à la protection d'informations numériques sur vidéo--disque analogique".
Thèse présentée à l'université de Rennes I en 1982 .

(9) **Jean Vignolle**
"Les codes binaires cycliques" .
Thèse présentée à l'université Paul Sabatier de Toulouse en 1973 .

(10) **Marc Heddebaut**
"Transports automatiques et transmissions électro--magnétiques en tunnel" .
Revue "Recherche,Transports,Sécurité" n°4 .

(11) **Alain Segui**
"Etude et réalisation d'un système de transmission d'information en présence de trajet et de bruit parasite" .
Thèse présentée à l'université de Rennes en 1972 .

(12) **Sikk Leung Yan Cheong**
"On some properties of the undetected error probabi--lity of linear codes" .
Revue IEEE Transactions on information Theory , Vol IT 25 , pp 110-112 , Janvier 1979 .

(13) **AbelHadi Ouadghiri**
"Application de la théorie des codages au traitement d'informations de sécurité analysées par microproces--seur" .
D.E.A d'électronique 1983 , U.S.T.L .

(14) **Marc Heddebaut**
"Transmissions numériques en tunnel" .
Note GRRI-IRT-CRESTA , Septembre 1985 .

(15) **AbelHadi Ouadghiri , J.F.Dhalluin**
"Sécurité des transmissions d'information"
Note CRESTA et U.S.T.L , Juillet 1984 .

(16) **M.El Koursi , Ch.Magniez , J.F.Dhalluin**
"Commande des portes VAL . Rapport d'avancement au 1er Mars 1984" .
Note GRRT-LRPE .

(17) **CH.Magniez**
"Commande d'un ensemble de processus en sécurité . Application à la commande d'un système de portes de métro" .
D.E.A , U.S.T.L , Juillet 1983 .

(18) **J.F.Dhalluin**
"Commande contrôle de processus en sécurité . Application à la commande d'un ensemble de portes véhicule VAL".
Thèse de Docteur Ingénieur , Décembre 1983 .

(19) **Ph.Delanghe**
"Commande de processus en sécurité par microproces--seur . Rapport d'avancement" .
Juillet 1984 .

(20) **P.Huckett , G.Thow**
"Analyse des performances en fonction des erreurs des systèmes de transmission numérique" .
Électronique,Technique et Industries (Paris) .
1984 n°5 , pp 35-43 .

(21) **J.P.Asselin de Beauville**
"Les sous-programmes **usuels** de simulation statistique"
Revue de statistique appliquée,1974 ,Vol XXII,n°4 .

(22) **Jack.Wolf , Fellow**
"On the probability of undetected error for linear block codes" .
Revue IEEE transactions on communication , Vol COM 30 n°2 , Février 1982 .

(23) **Tadao Kasami**
"Linear block codes for error detection" .
Revue IEEE Transactions on information theory ,
Vol IT 29 n°1 , Janvier 1983 .

(24) **Cyril Leung**
"Evaluation of the undetected error probability of single parity-check product codes" .

Revue IEEE Transactions on communications ,
Vol COM 31 n°2 , Février 1983 .

(25) **Roberto Padovani , Jack Keilwolf**
"Poor error correction codes are poor error detection codes" .
Revue IEEE Transactions on information theory ,
Vol IT 30 n°1 , Janvier 1984 .

(26) **P.Fondanèdre , P.Gilbertas**
"Filtres numériques . Principes et réalisation" .
Masson 1981 .

(27) **Jacques Hervé**
"Electronique appliquée à l'information" .
Tomes 1 et 2 . Masson 1981 .

(28) **M.Dreyfus**
"Fortran IV" .
5ième édition , Dunod 1972 .

(29) **Paul Bildstein**
"Filtres actifs" .
2ième édition , edition Radio 1976 .

(30) **Dominique Soufflet**
"Comportement d'un signal modulé en phase et en amplitude dans un canal de transmission numérique" .
Thèse présentée à l'université de Rennes en 1978 .

(31) **Benjamin Arazi**
"The optimal burst-error correcting capability of the codes generated by $f(x) = (x^p+1).(x^q+1) / (x+1)$.
Revue IEEE Information and controle n°39 , pp 303-314
1978 .

(32) **Mamadou Mbath**
"Contribution à l'étude théorique et éxperimentale de la propagation d'ondes haute fréquence en tunnel."
Thèse présentée à l'université de Lille I en 1985.

RESUME .

Les travaux présentés dans le cadre de cette thèse consti- -tuent une contribution à l'étude de la sécurité des trans- -missions numériques utilisant des codes de détection d'er- -reurs .

Dans un premier temps , nous exposons de façon générale le principe des codes de détection d'erreurs en définissant notamment les codes linéaires et cycliques .

Ensuite , après avoir rappelé la définition de la sécurité probabiliste dans les transmissions numériques , nous avons mis en évidence les conditions d'utilisation de ces codes afin d'atteindre un objectif de sécurité jugé satisfaisant .

Enfin , nous avons utilisé ces codes de détection d'erreurs pour la sécurité des transmissions numériques dans le domai- -ne des transports et en particulier aux métros souterrains.

La première application concerne la transmission des com- -mandes des portes d'une rame de métro .

La seconde s'applique à la transmission sol-véhicules en tunnel (messages télémesure et télécommande) .

MOTS CLES :

- Transmission numérique .
- Objéctif de sécurité ·
- Sécurité de l'information .
- Probabilité de non détection d'erreurs .
- Codes détecteurs d'erreurs .