Chambre de Commerce et d'Industrie de Paris ————— E.S.I.E.E.	Unité : TACN Partie J.-F. Bercher Date : décembre 2000	Classe I5

Tous documents (notes de cours, polys, livres, etc) autorisés

Remis par M. J.-F. BERCHER

Durée : 4 heures

Nom :

L'examen comporte deux parties : un partie QCM et deux exercices sur égalisation et diversité [1]. Vous rédigerez les exercices sur une copie séparéee. La partie QCM est de type « K bonnes réponses parmi N », $N \geq K \geq 0$. Sur chacune des réponses possibles, énumérées (a), (b), (c), etc, **entourez ou soulignez** la (les) lettre(s) correspondant à la (aux) bonne(s) réponse(s) (de manière non ambigüe). Bon courage.

N'oubliez pas d'indiquer votre nom sur le sujet...

Première partie – Répondre sur le sujet

Codage (C. Renaud)

1. Les codes convolutifs sont largement employés en radiocommunications car :
   - (a) Ils peuvent être décodés grâce à l'algorithme de Viterbi qui est simple à mettre en oeuvre soit dans un microprocesseur soit dans un circuit spécialisé
   - (b) Naturellement, ils sont insensibles aux paquets d'erreurs et les corrigent donc très bien, sans précaution supplémentaire
   - (c) Ils permettent d'obtenir d'excellents rendements et donc de hauts débits de transmission de données
   - (d) Ils ont naturellement une excellente capacité de détection d'erreurs et ne nécessitent pas l'emploi de CRC pour détecter que le nombre d'erreurs à corriger dépasse leur capacité de correction
2. Le soft decoding
   - (a) permet systématiquement un gain de 3 dB par rapport au hard decoding.
   - (b) n'est pas mis en œuvre pour les codes convolutifs car nécessite beaucoup de calculs supplémentaires par rapport au hard decoding .
   - (c) comporte une étape de calculs de syndromes.
   - (d) nécessite que la démodulation effectue un calcul de vraisemblance sur les bits décidés.
3. Les turbo codes
   - (a) ont l'inconvénient d'être plus complexes que les techniques de codage usuelles
   - (b) au fur et à mesure des itérations affinent l'estimation des bits d'information
   - (c) sont construits uniquement à partir de codes convolutifs
   - (d) parallèles ont un rendement R = R1 + R2, où R1 et R2 sont les rendements des codes constituants.
4. Afin de décorréler les erreurs et améliorer ainsi l'efficacité du décodage, il est important d'entrelacer les bits :
   - (a) à l'intérieur d'un bloc de Reed-Solomon

[1] les intervenants n'ayant pas retenu ou compris le concept de QCM

(b) à l'intérieur d'un bloc BCH
(c) après un codage convolutif
(d) avant de procéder au codage convolutif

5. Un code de Reed-Solomon de longueur 255 symboles de 8 bits (dimension du code = 8), comprenant 231 symboles utiles, peut :
   (a) corriger 8 symboles faux (la dimension) et en détecter 16 faux, au maximum
   (b) corriger 8 bits faux et en détecter 16 faux, au maximum
   (c) corriger 24 symboles faux (255 moins 231) et en détecter 48 faux, au maximum
   (d) corriger 12 symboles faux (255 moins 231, divisé par 2) et en détecter 24 faux, au maximum

Crypto (D. Samyde)

1. La cryptologie est composée de :
   (a) la cryptographie et de la cryptanalyse
   (b) la cryptanalyse et des attaques de protocoles
   (c) la cryptographie et de la fabrication des algorithmes ou des protocoles
   (d) du chiffrement
2. La sécurité cryptographique réside dans le fait que :
   (a) les algorithmes soient tenus secrets
   (b) les clés ne soient pas révélées
   (c) les méthodes soient obscures
   (d) les formules mathématiques mises en oeuvre sont très complexes
3. Les grands principes de base de la cryptographie symétriques sont :
   (a) les substitutions
   (b) le mélange des informations
   (c) les transpositions
   (d) l'arrangement aléatoire
4. Une clé de 1 367 500 000 de bits peut être attaquée par force brute (essais successifs exhaustifs) :
   (a) en un temps raisonable par des gens disposant de supercalculateurs existant aujourd'hui
   (b) en quelques dizaines d'années par l'humanité toute entière
   (c) en deux mois par un pc
   (d) ne peut pas être attaquée en temps raisonable

Séquences PN a bonnes propriétés.... (G. Baudoin)

1. Le polynôme P suivant permet-il de générer une séquence PN M à longueur maximale, avec un registre à décalage de longueur 2 ?
$$P = x^2 + x + 1.$$
   (a) Vrai
   (b) Faux

2. Le polynôme P suivant permet-il de générer une séquence PN M à longueur maximale, avec un registre à décalage de longueur 2 ?

$$P = x^2 + 1.$$

   (a) Vrai
   (b) Faux

3. Cocher la bonne réponse. La période L des séquences M à longueur maximale est de la forme :
   (a) $L = 2^r$
   (b) $L = 2^r - 1$
   (c) $L = 2^{r-1}$

4. On note $\Phi(n)$ la fonction de Euler de l'entier n.
   (a) $\Phi(63)$ vaut 6
   (b) $\Phi(63)$ vaut 8
   (c) $\Phi(63)$ vaut 36
   (d) $\Phi(63)$ vaut 48

5. Le nombre de polynômes minimaux primitifs de degré r vaut :
   (a) $\Phi(r)$
   (b) $\Phi(r)/r$
   (c) $\Phi(r) - 1$

6. Les séquences de Gold :
   (a) sont des séquences à longueur maximale
   (b) ont une intercorrélation prenant 5 valeurs différentes
   (c) ont une intercorrélation prenant 3 valeurs différentes
   (d) si a et b sont 2 séquences PN à longueur maximales, leur somme modulo 2est une séquence de Gold

Modulations codées, multiporteuses et applications (F. Belveze)

1. Un récepteur pour un système OFDM :
   (a) doit mettre en oeuvre un égaliseur pour réponse impulsionnelle longue, sur chaque sous-porteuse
   (b) utilise des FFT inverses
   (c) n'égalise pas mais doit compenser le canal de propagation réduit à un seul coefficient, sur chaque sous-porteuse
   (d) repose principalement sur l'algorithme de Viterbi

2. Dans le système DAB, on trouve une fonction d'embrouillage :
   (a) elle sert à briser le caractère éventuellement régulier des informations modulantes, de manière à équilibrer le spectre résultant
   (b) elle sert à crypter l'information, pour ne permettre qu'aux auditeurs ayant contracté l'abonnement adéquat d'accéder au service offert
   (c) elle réalise un entrelacement temporel après codage canal, pour mieux corriger les paquets d'erreurs
   (d) elle réalise un entrelacement fréquentiel des informations, pour lutter contre les évanouissements localisés sur certaines sous-porteuses

3. A quoi sert le temps de garde en OFDM :
   (a) à assurer l'orthogonalité des sous-porteuses entre elles
   (b) à répartir uniformément le spectre du signal dans la bande occupée
   (c) à accroître l'efficacité spectrale
   (d) à éviter d'avoir de l'interférence entre symboles

4. En modulation codée, la méthode du Set Partitioning :
    (a) classe l'ensemble des signaux possibles en niveaux successifs de sous-ensembles, de distances euclidiennes internes *décroissantes*
    (b) est un algorithme de calcul rapide de treillis de modulation
    (c) permet d'optimiser séparément la modulation et le code convolutif
    (d) attribue des labels voisins à des sous-ensembles éloignés (n'étant pas inclus dans le même sur-ensemble de niveau immédiatement supérieur), à l'inverse du codage de Gray
5. Le treillis d'une modulation codée
    (a) est toujours plus simple que le treillis du code convolutif servant à sa construction
    (b) a une taille nécessairement supérieure au produit du nombre d'états du code et du nombre d'états de la modulation
    (c) a une taille au plus égale au produit du nombre d'états du code et du nombre d'états de la modulation
    (d) est variant dans le temps, comme celui des codes en bloc.

Synchronisation (W. Hachem)

1. On transmet des données sur un canal de Nyquist et on s'intéresse à l'incidence des perturbations de phase et d'horloge sur la constellation reçue.

    (a) En présence d'un effet Doppler, la constellation subit un décalage angulaire.
    (b) En présence d'un effet Doppler, la constellation tourne autour de l'origine.
    (c) Si l'instant d'échantillonnage subit un décalage fixe par rapport à l'instant optimal, la constellation subit un décalage angulaire.
    (d) Si l'instant d'échantillonnage subit un décalage fixe par rapport à l'instant optimal, les points de la constellation deviennent des nuages de points.

2. On cherche à compenser l'offset de fréquence de la fréquence porteuse. Pour ceci, on dispose uniquement d'une Boucle à Verrouillage de Phase d'ordre 1.

    (a) Un gain de boucle élevé réduit l'erreur en régime permanent (*i.e.*, le biais).
    (b) Un gain de boucle élevé accroît le biais.
    (c) Un gain de boucle élevé réduit le bruit de phase.
    (d) Un gain de boucle élevé accroît le bruit de phase.

3. On compense les ambiguïtés de phase en réception

    (a) Par un bon choix du filtre de la boucle à verrouillage de phase.
    (b) Par l'usage d'un codage différentiel.
    (c) Par l'usage d'une constellation MDP (en anglais PSK).
    (d) Par l'usage d'un détecteur de phase de caractéristique proche de celle d'un détecteur linéaire.

4. Si le coefficient d'excès de bande α d'un filtre en cosinus surélevé est grand

    (a) L'ouverture horizontale de l'œil est grande.
    (b) L'ouverture horizontale de l'œil est petite.
    (c) L'ouverture verticale de l'œil est grande.
    (d) L'ouverture verticale de l'œil est petite.

5. Un égaliseur dont l'entrée respecte le théorème de Shannon (*i.e.*, un égaliseur "fractionnaire") peut compenser

   (a) Un décalage constant de l'instant d'échantillonnage.
   (b) Un offset de la fréquence d'horloge.
   (c) Un décalage constant de la phase de la porteuse.
   (d) Un offset de la fréquence porteuse.

Vérifiez que vous avez bien indiqué votre nom sur le sujet...

Deuxième partie - À rédiger sur une copie séparée

Diversité (A. Chevreuil)

Question 1 On observe la variable aléatoire

$$Y_n = As + W_n$$

où A est un canal de Rayleigh à P composantes indépendantes Enfin W_n est une suite de vecteurs Gaussiens, blancs spatialement et temporellement de variance $\sigma^2 I_P$. $s = + - 1$ est un symbole à estimer. Pourquoi le fait d'avoir un modèle de diversité permet-il d'obtenir de meilleures probabilités d'estimation du symbole s ?

Question 2 Dans un modèle de transmission de symboles binaires où l'on suppose disposer de P canaux de Rayleigh indépendants (le bruit additif est supposé Gaussien, blanc spatialement et temporellement), la probabilité d'erreur est

1. une fonction croissante de P
2. une fonction décroissante de P
3. de l'ordre de $(\frac{1}{\gamma})^P$ où γ est le rapport signal-sur-bruit moyen sur chaque voie.

Question 3 Dans un modèle de diversité d'antennes (le bruit additif est toujours Gaussien et blanc), le nombre de ces antennes

1. laisse invariante la capacité de Shannon
2. permet d'éviter les phénomènes d'évanouissements dans une bande de fréquences
3. augmente les performances d'un récepteur MMSE-DFE

Question 4 Il est courant en communications numériques de modéliser le processus observé par le récepteur comme

$$y_n = \sum_k h_k s_{n-k} + w_k$$

où (h_k) est une suite finie inconnue, (s_n) la suite des symboles, supposée i.i.d. de variance 1 et (w_n) un bruit Gaussien, blanc. Dans la suite, on se restreint au cas où le bruit est nul.
Soit $h(z)$ la Transformée en z de (h_k). On filtre y_n par un filtre $g(z)$ stable. Caractériser le filtre g tel que la filtrée de y_n par g s'écrit

$$\sum g_k y_{n-k} = s_n.$$

On dit qu'il y a un évanouissement fréquentiel lorsque $h(z)$ s'annule en un point du cercle unité. La méthode de restitution des symboles par filtrage inverse telle que décrite précédemment s'applique-t-elle encore ?
Si maintenant on observe sur une deuxième voie $\tilde{y}_n = \sum \tilde{h}_k s_{n-k}$, où $\tilde{h}_k$ est une autre suite finie, on note $\tilde{h}(z)$ la transformée en z de $\tilde{h}_k$. On considère alors la filtrée des deux voies définie par

$$\sum g_k y_{n-k} + \sum \tilde{g}_k \tilde{y}_{n-k}.$$

Trouver une condition pour qu'il existe $g(z)$ et $g(z)'$ deux polynômes tels que la filtrée des deux voies soit exactement s_n. Montrer que le premier canal peut infliger un évanouissement fréquentiel sans que, du fait de la présence de la seconde voie, la restitution des symboles par filtrage ne soit compromise.

Égalisation (C. Vignat)

Soit un filtre G de fonction de transfert

$$G(z) = 1 - \mu z^{-1}$$

où $|\mu| > 1$.

1. caractériser le filtre de fonction de transfert $1/G(z)$
2. Soit N un entier positif fixé. On s'intéresse au filtre H_{opt} solution du problème suivant

$$\begin{cases} H_{opt} = \arg\min_H C(H) \\ H \text{ est tel que } h(k) = 0 \text{ si } k < 0 \text{ ou } k \geq N \end{cases}$$

avec

$$C(H) = \sum_{k=-\infty}^{+\infty} |1 - (g * h)(k)|^2$$

- quel est l'intérêt de ce problème ?
- quelle est l'expression **fréquentielle** de la fonction de coût $C(H)$?

3. on montre que H_{opt} est solution du système linéaire

$$R_{gg} h = r_g$$

où
- $h = [h(0), \ldots, h(N-1)]^T$ est le vecteur $(N \times N)$ composé des échantillons de la réponse impulsionnelle de H_{opt}
- R_{gg} est une matrice Toeplitz $N \times N$ dont l'entrée (i, j) vaut

$$R_{gg}(i, j) = \sum_{k=-\infty}^{+\infty} g(k-i) g(k-j)$$

- r_g est un vecteur $N \times 1$ tel que [2]

$$r_g(i) = \sum_{k=-\infty}^{+\infty} \delta(k) g(k-i)$$

* expliciter le vecteur r_g et la matrice R_{gg}
* en admettant que la solution de ce système est donnée par

$$h(k) = \frac{\mu^{N-k} - \mu^{-(N-k)}}{\mu^{N+2} - \mu^{-N}} \, \forall 0 \leq k \leq N-1$$

en déduire la fonction de transfert du filtre noté H_∞ obtenu comme la solution de ce problème lorsque $N \to +\infty$

4. caractériser le filtre

$$G(z) H_\infty(z)$$

(on pourra représenter ses pôles et zéros)

5. conclure

[2] $\delta(k)$ est la suite de Kronecker