Chambre de Commerce et d'Industrie de Paris ——— E.S.I.E.E.	Unité : TACN Partie J.-F. Bercher Date : décembre 2001	Classe I5

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

---

Remis par M. J.-F. BERCHER

Durée : 4 heures

Nom :

L'examen est un QCM 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...

Codage (C. Renaud/F. Gabin)

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
   (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

Égalisation (C. Vignat)

1. les critères ”Zero-Forcing” et ”Erreur Quadratique Minimale” sont, en absence de bruit
   (a) équivalents
   (b) asymptotiquement équivalents
   (c) distincts
2. l’égalité des filtres d’émission et de réception permet d’obtenir, en sortie du filtre de réception
   (a) un rapport signal à bruit optimal
   (b) un taux d’erreur par bit minimal
   (c) une erreur de prédiction minimale
3. en absence de bruit, quel que soit le canal, et avec un égaliseur linéaire :
   (a) on peut toujours reconstituer exactement les symboles
   (b) on peut reconstituer exactement les symboles s’ils sont Gaussiens
   (c) on peut reconstituer les symboles émis sous certaines hypothèses
4. afin d’éviter les interférences intersymboles, il suffit
   (a) d’utiliser un filtre émetteur en cosinus surélevé
   (b) d’utiliser un filtre émetteur qui vérifie le critère de Nyquist
   (c) d’utiliser des filtres émetteurs et récepteur en racine de cosinus surélevé
   (d) d’utiliser un équaliseur linéaire optimisé selon le critère ”Zéro Forcing”
5. lorsque le critère de Nyquist n’est pas vérifié,
   (a) on peut transmettre les données à un débit quelconque
   (b) il est impossible, sans autres hypothèses, de reconstituer avec une erreur arbitrairement faible les données émises
   (c) il est possible, sous certaines hypothèses, de reconstituer les données émises avec une erreur arbitrairement faible
6. dans le cas non-bruité, et sans aucune autre hypothèse, le récepteur optimal est
   (a) un filtre linéaire à réponse impulsionnelle finie
   (b) un filtre linéaire à réponse impulsionnelle infine
   (c) un filtre non-linéaire instantané

Crypto (D. Samyde)

1. La génération de nombres pseudo-aléatoires en quantité peut s’effectuer grâce au résultat partiel d’une fonction de hachage reconnue comme sûre (Exemple SHA) ?
   (a) Oui en prenant des bits quelconques dans le résultat du hachage et en ayant une entrée non constante (Heure ou Timer, Intervalle entre deux interruptions,...).

(b) Oui en prenant des bits fixes et en maintenant toujours la même entrée. Car une fonction de hachage n'est pas déterministe.

(c) Non, une fonction de hachage ne permet pas d'obtenir des nombres pseudo-aléatoires. Car elle est déterministe et l'on peut prévoir sa sortie aisément.

(d) Non, car on peut inverser n'importe quelle fonction de hachage de manière simple et donc il n'y a pas de pseudo-aléa.

2. Une machine parcourant par force brute (totalité du parcours par essais successifs) un espace de clés de 512 bits est réalisable :

   (a) Oui, grâce à un supercalculateur de type Cray

   (b) Oui, en parallélisant des PC monoprocesseurs (Pentium III 500) pendant environ 1 mois.

   (c) Oui, car une clé RSA de 512 bits a été cassée par force brute en juillet dernier (Equipe française liée à Polytechnique).

   (d) Non, les lois de la thermodynamique l'interdisent (Impossible de dépasser 220 bits).

3. L'algorithme RSA est un algorithme a clé publique,clé privée, inconditionnellement sûr :

   (a) Oui, RSA est sûr dans tous les cas

   (b) Non RSA nécessite juste une taille de clé supérieure à 512 bits.

   (c) Non RSA, n'est pas sûr lors de signatures provenant de l'extérieur et n'ayant pas utilisé de fonction de hachage sûre pour générer le résidu à signer. De plus la taille des clés doit être supérieure à 512 bits.

   (d) Non, RSA est un algorithme à clé secrète.

4. Le seul chiffrement inconditionnellement sûr est le chiffrement de Vernam ou OTP ou encore appelé Masque Jetable :

   (a) Oui, car la taille de la clé (clé purement aléatoire et utilisable une fois et une seule), égale la taille du message. Toutefois il pose le problème de l'acheminement préalable des clés.

   (b) Non, ce chiffrement est facilement cassable par collisions même avec des clés purement aléatoires (Attaques des anniversaires).

5. L'algorithme DES (Data Encryption System) est un algorithme actuellement sûr, et résistant aux plus grandes puissances de calcul connues :

   (a) Oui, DES est encore sûr, son utilisation massive le prouve.

   (b) Non, il a été récemment prouvé que cet algorithme n'est pas sûr.

6. Un protocole utilisant une fonction de hachage permet à Alice et Bob ne s'assurer qu'Estelle (Espion actif) ne modifie pas le message :

   (a) Vrai, car Alice envoie d'abord le hachage d'une question avant de poser cette dernière.

   (b) Faux, car Estelle utilisant l'attaque (*Man in the middle*) , ne peut jamais être contournée.

Séquences à bonnes propriétés... (G. Baudoin)

1. Le polynôme P suivant est un polynôme primitif : $P = x^2+x+1$.

   (a) Vrai

   (b) Faux

2. Le polynôme P suivant est un polynôme primitif : $P = x^3+1$.

   (a) Vrai

   (b) Faux

3. Le polynôme P(x)= P = x^3+x+1 permet de générer une séquence PN M à longueur maximale, avec un registre à décalage de longueur 3. Cette séquence est de période égale à :
   (a) 15
   (b) 7
   (c) 2
4. On note Φ(n) la fonction de Euler de l'entier n.
   (a) Φ (31) vaut 30
   (b) Φ (31) vaut 31
   (c) Φ (31) vaut 32
   (d) Φ (31) vaut 28
5. Le nombre de polynômes minimaux primitifs de degré r vaut :
   (a) Φ (r)
   (b) Φ (r)/r
   (c) Φ (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 2 est une séquence de Gold
7. Pour une même périodicité, les séquences de Gold sont :
   (a) plus nombreuses que les séquences m
   (b) ont de meilleures propriétés d'autocorrélation que les séquences m
   (c) ont de meilleures propriétés d'intercorrélation que les séquences m.

Multiporteuses (R. Samy)

1. Débit maximal du flux descendant de l'ADSL
   (a) 56 Kbps
   (b) 512 Kbps
   (c) 1 Mbps
   (d) 8 Mbps
2. Débit maximal du flux descendant du VDSL sur une distance de 2 km
   (a) 8 Mbps
   (b) 30 Mbps
   (c) 50 Mbps
   (d) 100 Mbps
3. Quels sont les 2 égaliseurs mis en oeuvre dans l'ADSL
   (a) FFE+ DFE
   (b) TEQ + FEQ
4. Quel le code correcteur d'erreur utilisé dans l'ADSL

(a) Read-Solomon

(b) turbo-code

Architecture et performances (G. Martinez)

A – Convertisseur analogique/numérique (abaques pp 16-17)

On souhaite spécifier un convertisseur analogique/numérique pour un démodulateur numérique.
- La fréquence symbole est de 5 Mbaud.
- La modulation est une MAQ-64.
- Le rapport signal sur bruit minimum de fonctionnement est de 20 dB.
- La fréquence d'échantillonage est de 10 MHz.

1. Combien de bits le convertisseur peut-il avoir pour que la dégradation de rapport signal bruit soit inférieure à 0.1 dB.

   (a) 7 bits

   (b) 8 bits

   (c) 9 bits

2. Quel niveau d'harmonique d'ordre 3 faut-il au minimum pour qu'avec un convertisseur de 10 bits la dégradation soit inférieure à 0.5dB.

   (a) -87 dB

   (b) -67 dB

   (c) -47 dB

3. Quelle non-linéarité intégrale (INL) maximale peut-on alors spécifier ?

   (a) 0.2 bits

   (b) 0.5 bits

   (c) 0.8 bits

B – Boucle numérique à verrouillage de phase (pp 21-22)

On souhaite dimensionner une boucle numérique à verrouillage de phase pour une boucle de récupération de porteuse.
- La fréquence symbole est de 5 Mbaud.
- La modulation est une MAQ-64.
- Le rapport signal sur bruit minimum de fonctionnement est de 20 dB.
- La fréquence d'échantillonage est de 10 MHz.
- L'écart maximum de fréquence à récupérer est de +-100 KHz.
- Le gain du détecteur de phase est de 5V/rd.
- La fréquence naturelle choisie pour la boucle est de 10 KHz.

1. Combien de bits faut-il pour le registre stockant l'écart de fréquence (Xk)

   (a) 11 bits

   (b) 12 bits

   (c) 13 bits

2. Combien de bits conviennent pour représenter la phase régénérée dans la boucle.

   (a) 10 bits

   (b) 11 bits

   (c) 12 bits

C – Méthodes et modèle de simulation

1. La méthode de simulation qui présente le plus de fléxibilité pour estimer les performances d'un modem est :
   (a) la méthode Monte-Carlo
   (b) la méthode semi-analytique
   (c) la méthode analytique
2. On doit simuler la récupération de rythme d'un système dont la fréquence symbole est de 5 MBaud et le coefficient d'excès de bande du filtre de Nyquist est de 0.125 (ou 12.5
   (a) 5 MHz
   (b) 5.625 MHz
   (c) 20 MHz

Synchronisation (W. Hachem)

1. Pour compenser un offset de fréquence, la fonction de transfert $f(z) = \sum_k f_k z^{-k}$ du filtre de boucle de la PLL doit
   (a) avoir un zéro en $z = 1$.
   (b) avoir un pôle en $z = 1$.
   (c) avoir au moins un pôle dans le disque ouvert unité.
   (d) ne pas avoir de pôle en dehors du disque ouvert unité.
2. Les performances de la méthode de la raie spectrale dépendent
   (a) des performances de l'égaliseur.
   (b) du choix du filtre d'émission.
   (c) du choix du roll-off α.
   (d) des performances de l'algorithme de récupération de la porteuse.
3. La fonction de transfert globale du canal est une fonction en cosinus surélevé. T est la période symbole. $y(t)$ est le signal de sortie du filtre de réception et $a(n)$ est la séquence des symboles détectés. Le retard à l'échantillonnage est estimé itérativement selon
   $$\tau(n+1) = \tau(n) + \gamma f(n, \tau, y, a)$$
   où $\gamma > 0$. Fonction(s) f pertinente(s) ?
   (a) $f(n, \tau, y, a) = y(nT + \tau)a^*(n-1)$.
   (b) $f(n, \tau, y, a) = -y(nT + \tau)a^*(n-1)$.
   (c) $f(n, \tau, y, a) = y(nT + \tau)a^*(n-1) - y(nT + \tau)a^*(n+1)$.
   (d) $f(n, \tau, y, a) = y(nT + \tau)a^*(n+1)$.
4. La constellation émise est une constellation MDP2 (à valeurs dans $\{-1, 1\}$). $y(n)$ est l'entrée du détecteur des symboles et $\hat{a}(n)$ est le symbole détecté. L'estimée de l'erreur de phase est fournie par
   (a) $\mathrm{Re}(y(n)\hat{a}^*(n))$ avec une ambiguïté de $\pi/2$.
   (b) $\mathrm{Im}(y(n)\hat{a}^*(n))$ avec une ambiguïté de $\pi/2$.
   (c) $\mathrm{Re}(y(n)\hat{a}^*(n))$ avec une ambiguïté de π.
   (d) $\mathrm{Im}(y(n)\hat{a}^*(n))$ avec une ambiguïté de π.

5. Le codage différentiel

   (a) Compense la distorsion due à l'approximation $\sin(x) \approx x$ due au détecteur de phase.
   (b) Affecte les bits émis d'une redondance.
   (c) Fait en sorte que suite à un saut de phase (click) les bits détectés suivants ne sont pas tous erronés.
   (d) Modifie la Densité Spectrale de Puissance du signal émis.