Informatik Diplomprüfung: Anwendungsfach Elektrotechnik

19. Mai 2009

Zusammenfassung

Fächer

- Nachrichtentechnik 1 (Prof. Ohm, SS 08)
- Nachrichtensysteme 1 (Prof. Vary, WS 07/08)
- Nachrichtensysteme 2 (Prof. Vary, SS 08)
- Digitale Sprachverarbeitung 1 (Prof. Vary, WS 08/09)
- Cryptography 1 (Prof. Mathar, WS 08/09)

Prüfer

- Prof. Vary
- Prof. Mathar

Empfohlene Literatur

- Digital Speech Transmission (Vary, Martin)
- Signalübertragung (Ohm, Lüke)

1 NT1

- Wie lautet das Differentiationstheorem und wie beweist man es?
- Wie ist die FT allgemein definiert?
- Wie sieht die komplexwertige Basisbandmodulation aus?
  - Was ist der Hintergrund der Basisbandmodulation? (äquivalentes TP-System)
  - Wie ist die Quadraturmodulation definiert (Gleichung mit I- und Q-Anteilen)
  - Blockschaltbild der Quadraturmodulation
  - Wie funktioniert die Modulation in der Praxis? (I und Q durch Signalraumabbildung erzeugen)

2 NS1

- Definition und Herleitungsskizze der Kanalkapazität nach Shannon
- Bedeutung für die praktische Umsetzung? (habe ich nicht verstanden, aber es lief auf das Einstellen von B gegen SNR hinaus)
- Quantisierungsrauschen bei gleichmäßiger Quantisierung angeben und herleiten
- Daraus SNR und die 6-dB-pro-Bit-Regel herleiten

3 NS2

- Thema: Faltungsdekodierung
  - Wie funktioniert Faltungskodierung?
  - Wie dekodiert man? (Zustandsdiagramm, Trellisdiagramm)
  - Wie funktioniert Viterbi-Dekoder? Welches Kriterium optimiert man damit (Max. Likelihood, Bayes-Thm. zur Umformung)
  - Was ist die Idee hinter MAP-Dekoder?
  - Ist er besser als Viterbi? (kaum)
  - Wozu braucht man es dann? (Zuverlässigkeiten für Turbo-Dekodierung)

4 DSV1

- Wie wird FFT (Radix-2, decimation-in-time) hergeleitet?
- Wie ist die Komplexität und warum?
- Wie ist der Gewinnfaktor? ($\frac{O(FFT_M)}{O(MFT_M)}$ für $M = 1024$)

5 Crypto1

- Wie modelliert und definiert Shannon die perfekte Sicherheit?
  - Zufallsvariablen für Klartext/Schlüssel/Geheimtext
  - Definition über Entropie (dabei habe ich nicht erwähnt, dass es stochastische Unabhängigkeit bedeutet, daraus ergab sich die nächste Frage)
  - Gilt denn für ein perfekt sicheres Kryptosystem auch $H(C|M) = H(C)$? (hier war klar, dass man mit stochastischer Unabhängigkeit argumentieren muss)
  - Blöd ist bei Vernam, dass der Schlüssel so lang sein muss, wie der Klartext. Da wird folgende Modifikation vorgeschlagen: generiere einen Zufallsstring der Länge $n/2$, benutze ihn für ungerade Key-Indices; berechne gerade Key-Indices als Summe der benachbarten Buchstaben im Schlüssel. Ist das System noch perfekt sicher? (Nein, denn die Anzahl der Schlüssel ist geringer, als die Anzahl der Klartexte)
- Thema: diskreter Logarithmus
  - Gegeben beliebige Zahlen $a, x, n, y = a^x$: ist $log_a(y) = x \ mod \ n$ immer eindeutig lösbar? (nein, a muss ein primitives Element modulo n sein)
  - Wie findet man primitive Elemente? Wieviele gibt es? Für welche n?
- Wie funktioniert ein Schlüsselaustausch-Protokoll, welches auf diskr. Log. basiert? (DH erklärt, mit Skizze)
- Wie funktioniert ein Public-Key-Protokoll (El-Gamal) und worin besteht seine Ähnlichkeit zu DH?
- *Flexibilitätsfrage (war wohl nicht mehr so ernst gemeint): Wie ist die "örtliche Ausdehnung eines Bits"bei einer Übertragung mit GSM und hypothetischen 300 kbit/s? (ein Bit wird in* $1/300000s$ *übertragen. GSM: Lichtgeschwindigkeit annehmen.* $S = t * v = 1 \ km$*)*