

## Kontrollfragen zur Vorlesung ÜT-Technik I

Diese Fragen sollen beim Durcharbeiten / Wiederholen des Stoffes helfen. Sie sind nicht eine Sammlung, aus der dann einige Fragen einfach so für die Klausur ausgewählt werden. In der Klausur können dann andere Fragen gestellt werden, die natürlich auch zum Vorlesungsinhalt und dem Inhalt der Übungen passen, genau wie diese Kontrollfragen.

Die nachfolgenden Fragen sind immer im Kontext zur Übertragungstechnik zu sehen, auch wenn das nicht immer extra betont wird.

1. Was verstehen Sie unter „Nachricht“, „Signal“, „Information“ und „Redundanz“, „Kodierung“, „Symbol“, „Alphabet eines Codes“ und „Elementarsymbol“?
2. Was verstehen Sie unter „wertediskret“, „zeitdiskret“, „digital“ und „binär“?
3. Skizzieren Sie das Kanalmodell von der Quelle bis zur Senke.
4. Was verstehen Sie unter Quelle, Primärquelle, Sekundärquelle und Ersatzquelle?
5. Wie kann der Informationsgehalt eines wertediskreten Symbols bestimmt werden? Nennen Sie die beiden Grenzwerte.
6. Was ist die Entropie einer werte- und zeitdiskreten Quelle?
7. Wie wird die Entropie einer werte- und zeitdiskreten Quelle ermittelt?
8. Die Statistik einer binären Quelle ist gegeben. Schreiben Sie bitte die Formel zur Ermittlung der Entropie auf und setzen sie die statistischen Parameter ein.
9. Wie hoch ist die maximale Entropie einer binären Quelle? Nennen Sie die Formel und den Wert.
10. Wie kann bei einer binären Quelle die Redundanz ermittelt werden?
11. Was verstehen Sie unter dem Gedächtnis einer Quelle?
12. Welchen Einfluß auf die Entropie einer Quelle hat die Tatsache, daß die Quelle ein Gedächtnis hat?
13. Was versteht man unter einer Quelle mit Gedächtnis 5. Ordnung?
14. Wie wird die Wahrscheinlichkeit eines Symbols einer Quelle mit Gedächtnis 1. Ordnung geschrieben (math. Ausdruck)?
15. Was versteht man unter Übergangswahrscheinlichkeiten? Wie werden diese üblicherweise dargestellt? Schreiben Sie diese Darstellung für eine binäre Quelle mit Gedächtnis 1. Ordnung auf und erklären Sie die einzelnen Terme.
16. Gegeben sind die Matrix der Übergangswahrscheinlichkeiten einer binären Quelle mit Gedächtnis 1. Ordnung und die ergodischen Wahrscheinlichkeiten der Symbole dieser Quelle. Prüfen Sie bitte, ob die Werte plausibel sind.
17. Lassen sich beliebige werte- und zeitdiskrete Quellen auf binäre Symbole abbilden? Wenn ja, wie funktioniert das?
18. Gegeben ist eine Quelle mit einem Alphabet von  $N$  Symbolen. Wieviele binäre Elementarsymbole müssen die Worte eines gleichwertigen binären Codes mindestens aufweisen, wenn über den primären Code nichts weiter bekannt ist?
19. Welchen Einfluß hat die Kenntnis der Auftretenswahrscheinlichkeiten der Symbole des primären Codes auf die Beantwortung der vorherigen Frage?
20. Was ist grundsätzlich bei der Bildung von Kodeworten aus Elementarsymbolen zu beachten und wie kann das praktisch realisiert werden?
21. Was ist ein Binärbaum? Was sind seine Elemente?
22. Was kann mit Binärbäumen dargestellt werden?
23. Was ist ein Präfixkode?
24. Gegeben sind mehrere Kodealphabete.
  - Zeichnen Sie jeweils einen passenden Binärbaum.

- Prüfen Sie, ob der einzelne Kode jeweils ein Präfixkode ist.
- 25. Bilden Sie zu vorgegebenen Alphabeten den Binärbaum und umgekehrt.
- 26. Ein Quellkode mit unterschiedlich langen Kodeworten wird gebildet. Wie werden die Symbole der Quelle sinnvoll auf diese Kodeworte abgebildet, um die Redundanz im Quellkode zu minimieren?
- 27. Was ist ein idealer und was ein kompakter Kode?
- 28. Wie wird ein Huffmankode gebildet?
- 29. Gegeben ist eine Quelle mit ihren Symbolen und Symbolwahrscheinlichkeiten. Bilden Sie den Huffmankode.
- 30. Ermitteln Sie zum Kode aus dem vorherigen Punkt die Entropie der Quelle und die Effizienz des Quellkodes.
- 31. Nennen Sie die wesentlichen Ziele der Kanalkodierung und der Sicherheitskodierung.
- 32. Welches sind die drei Schutzziele der Sicherheitskodierung. Erläutern Sie kurz jedes Ziel.
- 33. Nennen Sie drei Angriffsstrategien auf die Sicherheitskodierung und charakterisieren Sie jede kurz.
- 34. Was versteht man bei der Sicherheitskodierung unter Substitution und was unter Permutation?
- 35. Was ist das Feistel-Netzwerk?
- 36. Was ist beim Feistelzyklus der spezielle „Trick“?
- 37. Nennen Sie zwei Verschlüsselungsverfahren, bei denen das Feistel-Netzwerk angewendet wird.
- 38. Was versteht man bei der Sicherheitskodierung unter einem Brut-Force-Angriff?
- 39. Was verstehen Sie unter symmetrischer und was unter unsymmetrischer Verschlüsselung?
- 40. Was ist ein Public Key und was ein Private Key? Welches ist der entscheidende Unterschied zwischen beiden?
- 41. Wie wird bei der unsymmetrischen Verschlüsselung vom privaten und vom öffentlichen Schlüssel Gebrauch gemacht? Wie erfolgt das bei der Signierung (z. B. von Mails)?
- 42. Nennen Sie zwei mathematische Objekte bzw. Verfahren, die wichtige Basis für die unsymmetrische Ver- und Entschlüsselung sind.
- 43. Was versteht man unter einer Hash-Funktion und einem Hash-Wert? Was stellt der Hash-Wert dar?
- 44. Wozu kann ein Hash-Wert verwendet werden?
- 45. Welche zwei Möglichkeiten kennen Sie, die den Nutzen eines Hash-Wertes reduzieren oder zunichte machen?
- 46. Was versteht man unter Authentifizierung und was unter Autorisierung?
- 47. Was versteht man unter schwacher und was unter starker Authentifizierung?
- 48. Was ist ein Zertifikat? Nennen Sie mindestens 4 besonders wichtige Bestandteile.
- 49. Wofür steht die Abkürzung PKI. Welches ist der hauptsächlichliche Nutzen einer PKI?
- 50. Was versteht man unter Kanalkodierung? Was sind die Hauptziele der Kanalkodierung?
- 51. Nennen Sie zwei Arten von Kanalkodes.
- 52. Wie funktionieren prinzipiell Blockcodes? Nennen Sie mindestens ein Beispiel für einen Blockcode.
- 53. Was kennzeichnet lineare Blockcodes?
- 54. Was versteht man unter Hamming-Metrik, Hamming-Gewicht, Hamming-Distanz, Gewichtsverteilung und Distanzverteilung?
- 55. Was macht die Mindestdistanz besonders interessant und das minimale Gewicht besonders nützlich?

56. Aus welchem Wert der Hamming-Metrik kann die Anzahl der garantiert erkennbaren Fehler im Empfangswort ermittelt werden? Erklären Sie diesen Zusammenhang prinzipiell und anhand eines selbst gewählten Beispiels.
57. Aus welchem Wert der Hamming-Metrik kann die Anzahl der garantiert korrigierbaren Fehler im Empfangswort ermittelt werden? Erklären Sie diesen Zusammenhang prinzipiell und anhand eines selbst gewählten Beispiels.
58. Aus einem gegebenen minimalen Gewicht soll die Anzahl der im Empfangswort sicher erkennbaren und der sicher korrigierbaren Fehler ermittelt werden.
59. Was kennzeichnet einen perfekten Code?
60. Mit welchem Mittel können Kodeverletzungen erkannt werden?
61. Welche beiden alternativen Aussagen kann die Prüfung eines Empfangswortes auf Kodeverletzungen liefern? Achten Sie auf die exakte Formulierung.
62. Interpretieren Sie zu einem binären Blockcode die Angabe  $C(7, 3, 3)$ . Welche Dimension hat die Generatormatrix? Welchem Teil der Generatormatrix können Sie ohne weitere Kenntnis des konkreten Codes bilden? Führen Sie das aus.
63. Gegeben ist eine konkrete Generatormatrix  $G$ . Bilden Sie daraus alle Codeworte und bestimmen Sie die minimale Distanz.
64. Bilden Sie zum Leitungskode im vorherigen Punkt die Prüfmatrix  $H$ .
65. Was verstehen Sie unter einem zyklischen Code? Was ist das wesentliche Merkmal?
66. Beschreiben Sie die Bildhaft und eventuell über eine Analogie die Wirksamkeit zyklischer Codes zur Korrektur von Übertragungsfehlern.
67. Mit welcher schaltungstechnischen Struktur wird eine zyklische Kodierung vorzugsweise realisiert? Wie wird in den meisten Fällen der vordere und wie der hintere Teil des Codewortes prinzipiell gebildet?
68. Gegeben sind zwei binäre Polynome. Dividieren Sie das erste Polynom durch das zweite und ermitteln Sie den Divisionsrest.
69. Gegeben ist das Generatorpolynom eines zyklischen Codes. Ermitteln Sie daraus eine Generatormatrix. Ermitteln Sie die Generatormatrix in der systematischen Form.
70. Womit und wie (prinzipiell) kann bei einem zyklischen Code das Empfangswort auf Fehler geprüft werden?
71. Wie können im Bezug auf vorher behandelte Kanalkodes Reed-Solomon-Kodes eingeordnet werden?
72. Was ist bei Faltungskodes prinzipiell anders als bei Blockcodes?
73. Was versteht man unter Kodeverkettung?
74. Was versteht man bei der Informationsübertragung unter Interleaving? Wie funktioniert dieses Verfahren und was ist der Nutzen? Klären Sie, ob es sich um eine Kanalkodierung im strengen Sinne handelt.