# Prüfungsprotokoll

|  |  |
|---|---|
| **Prüfung:** | Vordiplom Informatik |
|  | Teilprüfung Diskrete Mathematik, Logik |
| **Prüfer:** | Prof. Schmitt |
| **Termin:** | 1. Oktober 2001, 11:30 Uhr |
| **Note:** | 2,3 |

**Die Prüfung:**

*Womit wollen Sie anfangen?*
Algebra.
*Also Codierungen.*
Es folgten sehr ungenaue Fragen. Ich kann mich an wenig konkretes erinnern. Wir redeten einige Zeit über Dinge wie endliche Körper, Galoisfelder, Vektorräume über diesen Körpern, allgemeine Codes, Blockcodes, Hamming-Distanz, $r$-Kugeln um $a$, etc. Die "Fragen" waren für mich sehr verwirrend, ich wußte fast nie, was für eine Antwort Prof. Schmitt erwartete, geschweige denn worauf es hinauslaufen sollte. Einige Fragen, an die ich mich erinnern kann:
*Was für Eigenschaften haben endliche Zahlenkörper?*
Anzahl Elemente ist Primzahlpotenz ... Ringstrukur ... Nullteilerfreiheit ... irgendwann auch den Begriff "modulo" benutzt, das wollte er hören.
*Über welchem Alphabet werden Codierungen definiert?*
Über beliebigen? Es können Buchstaben, Ziffern, Bits sein.
*Was für eine Eigenschaft müssen Codierungen haben?*
Zuerst Ratlosigkeit und dann mein Tip: „Sie dürfen nicht surjektiv sein. Es müssen noch Falschworte im Vektorraum übrigbleiben, die nicht im Bild der Codierfunktion liegen, um Störungen bei der Übertragung zu bemerken.“ Mit dieser Antwort hatte ich zwar Glück, aber sie lag sicher nicht auf der Hand.

Nach einiger Zeit kamen wir zu dem, worauf Prof. Schmitt die ganze Zeit hinauswollte:
*Was sind Lineare Codes?*
Untervektorräume von $K^n$ wobei $K$ ein endlicher Körper.
*Wie sieht das nun mit den Begriff der Code-Distanz aus?*
Der vereinfacht sich aufgrund der Linearität. Da die Addition (und damit Subtraktion) im Vektorraum abgeschlossen ist, liegt die Differenz $b - a$ zweier Codeworte wieder im Vektorraum. Man kann daher die Hamming-Distanz $d(a, b)$ mit $g(b - a)$ ausdrücken, wobei $g(w) := |\{i : w_i \neq 0\}|$ das Gewicht von $w$ ist. Die Code-Distanz ist dann das minimale Gewicht aller Worte ungleich dem Nullwort.
*Wie geschieht der Codiervorgang?*
Eine Matrix $G$ ist genau dann eine Generatormatrix, wenn ihre Zeilenvektoren eine Basis des linearen Codes sind. Eine Nachricht $w$ wird mit $w \cdot G = a$ kodiert.
*Wie stellt man fest, ob ein Wort im Code liegt?*

Mit einer Kontrollmatrix $H$, es muß $a \cdot H = 0$ gelten. (Dann dualen Code und Kontrollmatrix erklärt.)
*In welchem Zusammenhang stehen die Generatormatrix und die Kontrollmatrix?*
Es gilt ja $w \cdot G = a$ und $a \cdot H = 0$, also $w\,GH = 0$. Da $w$ beliebig, muß $GH = 0$ sein.
*Wie wird das Wort wieder dekodiert?*
Es muß das LGS $w \cdot G = a$ gelöst werden (hier war ich unbegründet etwas verwirrt). Es geht aber auch einfacher, wenn die Generatormatrix systematisch ist, also der Form $G = (E, G')$. Dann ist das Codewort $a$ der Form $(w, wG')$ und man kann die Nachricht $w$ direkt ablesen. Die zugehörige Kontrollmatrix $H$ hat die Form $\begin{pmatrix} -G' \\ E \end{pmatrix}$. Habe dann noch versucht zu erklären, warum sie so aussieht, aber es interessierte wohl wenig...
*Wann ist ein Code $r$-fehlererkennend?*
Wenn $d(C) \geq r + 1$. Man kann an der Anzahl der paarweise linear unabhängigen Zeilenvektoren der Kontrollmatrix erkennen, ob dies der Fall ist. (Das Wort "paarweise" störte ihn.)
*Wieviel Prüfzeichen muß das Codewort mindestens enthalten?*
Mindestens $r$ Prüfzeichen. (Hier herrschte wieder etwas Verwirrung.)
*Eigenschaften von Einwegfunktionen?*
Habe die drei Punkte aus dem Skript wiedergegeben.
*Wie funktioniert das RSA-Verfahren?*
Man faßt die Nachricht als eine große Zahl auf und [blabla...] (Das war's nicht, er wollte was anderes hören. Schließlich:) Da gibt es eine Codier-Abbildung $c\colon x \mapsto x^s \equiv y \pmod m$ und die dazu inverse Decodier-Abbildung $d\colon y \mapsto y^g \equiv x \pmod m$. $m$ muß dabei das Produkt zweier großer Primzahlen $p$ und $q$ sein, um die Sicherheit zu gewährleisten. Soll ich den zugrunde liegenden Satz beweisen?
*[...]*
Habe dann gezeigt, wann und warum $x^{sg} \equiv x \pmod m$ gilt.
*Können Sie etwas zu Stirling-Zahlen sagen?*
Ich erklärte die kombinatorischen Bedeutungen der Stirlingzahlen 1. und 2. Art ($s_{nk}$ = Anzahl der $n$-Permutationen mit genau $k$ Zyklen, $S_{nk}$ = Anzahl der $k$-Partitionen einer $n$-elementigen Menge), ihre Rekursionsformeln und die Polynomidentitäten. Ich habe dann gezeigt, daß man den Satz über die Polynomidentitäten mit dem Basiswechselsatz aus der Linearen Algebra einfacher beweisen kann, als es im Skript bewiesen wurde. Wieder kein merkliches Interesse...
*... Surjektive Abbildungen?...*
Ich bot an, zuerst die die Anzahlen aller Abbildungen von $N$ nach $K$ und aller injektiven Abbildungen herzuleiten, wollte Prof. Schmitt aber nicht haben. Es gilt $|Sur(N, K)| = k!\, S_{nk}$. Habe es mit Bällen und Fächern erklärt: „Eine surjektive Abbildung verteilt $n$ Bälle auf $k$ Fächer, wobei in jedes Fach mindestens ein Ball kommen muß, also eine $k$-Partition der Menge $N$. Und da die Zuordnungen der $k$ Fächer zu den Partitionen permutierbar sind, das Ganze mal $k!$."
*Derangement-Zahlen?*
$D_n$ = Anzahl fixpunktfreier $n$-Permutationen.
*Herleitung?*

Das geht über die Ein-Ausschalt-Formel von Sylvester, oder genauer: mit dem Korollar aus dem Satz. Habe dann zuerst die Formel von Sylvester aufgeschrieben. Dann die Vereinfachung, wenn die Größe der Schnittmengen nur von der Anzahl der zu schneidenden Mengen abhängt. Damit wollte ich $D_n$ herleiten. Ich habe aber die Bedeutung von $A_i := \{\pi\colon \pi(i) = i\}$ nicht richtig erklärt. Prof. Schmitt mußte mich korrigieren. Zwischendurch habe ich die Indizes ungeschickt gewählt, aber nichts spektakuläres. Als ich die Formel für $D_n$ stehen hatte, sollte ich noch etwas dazu sagen. Ich erwähnte die Ähnlichkeit zur Exponentialreihe, und daß $\frac{1}{n!}D_n \cong \frac{1}{e}$ für große $n$ ist.

*Rekursionsformel für $D_n$?*

$D_n = (n-1)(D_{n-1} + D_{n-2})$

*Was ist das?*

Das ist eine 2-stufige lineare Differenzengleichung.

*Kann man das anders schreiben? [o.ä. Frage]*

Habe zuerst behauptet, daß es dafür ein Lösungsverfahren gibt, so daß man $D_n = \beta_1(z_1)^n\beta_2(z_2)^n$ schreiben kann. Mir fiel auf, daß dies nicht stimmt. Das Lösungsverfahren gilt nur für Differenzengleichungen mit konstanten Koeffizienten, aber $(n-1)$ ändert sich in jeder Rekursionsstufe. Habe meine Aussage korrigiert. Prof. Schmitt bemängelte aber noch etwas an meiner Schreibweise, ich korrigierte: $\beta_1(z_1^n)\beta_2(z_2^n)$ (*?*)

*Wann kann man dieses Lösungsverfahren anwenden?*

Bei linearen Differenzengleichungen mit konstanten Koeffizienten.

*Führen Sie mal das Verfahren an einem Beispiel vor.*

Habe die Fibonacci-Folge herangezogen, das charakteristische Polynom aufgestellt, dann versucht zu erläutern, daß die Nullstellen $z_1$, $z_2$ in der Form $(z_1^n)_n, (z_2^n)_n$ Lösungen der Differenzengleichungen darstellen. Dabei habe ich mich wohl etwas mißverständlich ausgedrückt.

*Was ist mit den Betas?*

Da muß man noch die Startwerte $F_1 = 1$ und $F_0 = 0$ der Folge miteinbeziehen. Dann liefert das Verfahren die explizite Darstellung für die Fibonacci-Folge.

*So, jetzt erzählen Sie mir etwas zu Logik: Substitution?*

Die an einen Quantor $Q$ gebundene Variable $y$ darf nicht substituiert werden, daher zuerst Ersetzung durch eine andere Variable $\xi$ , die nicht in der Zeichenfolge $Z$ vorkommt. Ich schrieb auf: $Qy(U)(x|Z) = Q\xi(U(y|\xi)(x|Z))$. Irgendetwas gefiel Prof. Schmitt daran nicht ... Verwirrung ... nächste Frage...

*Welche Beweiskriterien gibt es?*

Wir hatten ca. 24. Die am häufigsten genutzten waren der Syllogismus (= Modus Ponens = Schnittregel) und der Deduktionssatz. (beide erläutert)

*Wann heißt eine Theorie logisch?*

Wenn die folgenden Schemata gelten:

$S_1 : A \Rightarrow A \vee A$

$S_2 : A \Rightarrow A \vee B$

$S_3 : (A \vee B) \Rightarrow (B \vee A)$

$S_4 : (A \Rightarrow B) \Rightarrow ((C \vee A) \Rightarrow (C \vee B))$

*Warten Sie jetzt bitte draußen.*

**Zur Prüfungsatmosphäre:**

Die Prüfung ist alles andere als "rund" verlaufen. Wie oben geschildert, wußte ich oftmals nicht, was Prof. Schmitt genau von mir wollte. Gegenfragen meinerseits oder Antworten der Form „Ich verstehe Ihre Frage nicht“ haben sicherlich nicht zu einem guten Gesamteindruck beigetragen.

Prof. Schmitt drückt sich sehr zurückhaltend aus. Die Fragen am Anfang der Prüfung zum Thema Codierungen waren beispielsweise so allgemein gehalten, daß ich nicht wußte, womit ich anfangen sollte. Zu dem Zeitpunkt habe ich versucht, auch nur allgemein und nur auf die Fragen zu antworten. Ich dachte, Prof. Schmitt würde von alleine immer mehr ins Detail gehen bzw. das Gespräch selber auf andere wichtige Dinge lenken. Dies ist aber nicht eingetroffen. Scheinbar hat er meine spärlichen Antworten auf seine spärlichen Fragen mit Unwissenheit meinerseits gedeutet. Ich hätte wohl etwas mehr von mir aus erzählen müssen. Allerdings erhält man sehr wenig Feedback von Prof. Schmitt. Man weiß nie genau, ob er gerade das hören möchte, was man erzählt. Das hat mich sehr verunsichert. Er macht auch wenig Anstalten, um einen auf die richtige Spur zu bringen. Meine Antworten kamen mir die ganze Zeit etwas unbeholfen vor, weil ich mir nie sicher war, was ich sagen sollte. Um die Situation zu retten, habe ich einige Male versucht, einfach ein paar Zusammenhänge bzw. Hintergründe zu erwähnen. Es war für mich aber stets frustrierend festzustellen, daß dies Prof. Schmitt offenbar nicht hören wollte.

Bei Beweisen oder Herleitungen darf man nicht viel Hilfestellungen von Herrn Schmitt erwarten. Wenn man etwas falsch gemacht hat oder nicht weiterkommt, läßt er einen ziemlich lange zappeln, anstatt einen konstruktiven Tip zu liefern. Man kommt sich in einer solchen Situation ziemlich blöd vor. Die Korrektheit der schriftlichen Formulierung ist Prof. Schmitt sehr wichtig. Er kreidet Fehler sofort an – und seien es nur „ungeschickt gewählte“ Indizes (was bei einer Beweis- oder Herleitungsskizze in einer Prüfungssituation vielleicht schon mal vorkommen kann). Etwas befremdlich fand ich allerdings schon, daß Prof. Schmitt zur Begründung der Note die ca. 4 - 5 Schmierzettel hervorholte, die ich während der Prüfung vollgeschrieben hatte, und zusammenzählte, wo ich überall Fehler gemacht hatte.

Mein Eindruck ist, daß Prof. Schmitt mehr Wert auf eine korrekte schriftliche Formulierung und auf auswendig gelerntes Wissen legt, als auf die Tatsache, daß man die Zusammenhänge verstanden hat und sie anwenden kann. Beweise mußte ich ihm auch erst anbieten, aber vielleicht lag das auch daran, daß er sie mir aufgrund der katastrophalen Anfangsphase nicht mehr zugetraut hat. Obwohl Prof. Schmitt meinte, daß es zum Ende hin besser wurde (was ich auch über seinen Prüfungstil sagen kann), litt wohl die Atmosphäre darunter, daß ich am Anfang der Prüfung „nicht seinen Ball (mit den Linearen Codes) aufgenommen habe“, den er versucht hatte mir zuzuspielen. Ich bin nicht darauf gekommen, daß wenn man von Codierungen spricht, es zwangsläufig auf Lineare Codes hinauslaufen muß...

All diese Einschätzungen beruhen auf meinen persönlichen Eindrücken. Ich bin mir sicher, daß Prof. Schmitt aufgrund der unglücklichen Kommunikation zwischen uns beiden eine ähnliche Einschätzung von mir gewonnen hat und damit aus seiner Sicht die Note gerechtfertigt ist.