Diskrete Strukturen und Logik

WiSe 2006/07 in Trier

Henning Fernau
Universität Trier
fernau@informatik.uni-trier.de

$\boxed{\textbf{Diskrete Strukturen und Logik}}$ Gesamtübersicht

- Organisatorisches
- Einführung
- Logik & Mengenlehre
- Beweisverfahren
- Kombinatorik: Die Kunst des Zählens
- algebraische Strukturen

$\boxed{\textbf{Beweisverfahren}}$ — Eine Übersicht

Direkter Beweis

Beweis durch Umkehrschluss

Widerspruchsbeweis (Indirekter Beweis)

Fallunterscheidungen

Schubfachprinzip

Induktion

Exkurs — Spieltheorie

Hier: Zweipersonenspiele mit vollständiger Information

Wichtig: Spielbeschreibung mit Regelwerk (kann man logisch spezifizieren); wann gilt das Spiel für wen als beendet / gewonnen ?

Fragestellungen:
Wie sollten Spieler $\mathbb{A}$ (macht ersten Zug) oder Spieler $\mathbb{B}$ ziehen ?
Gesucht: Vorschrift (*Strategie*), die jeder *Spielkonfiguration* einen Zug zuordnet.
Besitzt Spieler $\mathbb{A}$ (oder Spieler $\mathbb{B}$) eine Gewinnstrategie ?

Exkurs — Spieltheorie

Strategie, lokale Sicht: B sucht "Antwort" auf Zug von A und umgekehrt.

Wie gelangt man zu einer guten Strategie ? *Minimax-Ansatz*

A denkt darüber nach, einen Zug α zu machen.
Dazu überlegt sich A, was B auf α antworten könnte.
Um zu gewinnen, muss A für jede Antwort β von B einen "Gewinnzug" α' usw.
Etwas formaler (c Anfangskonfiguration, C_A Menge der Endkonfigurationen, in denen A gewonnen hat): A besitzt *Gewinnstrategie* gdw.

$$\exists\alpha\forall\beta\exists\alpha'\forall\beta'\ldots(c\alpha\beta\alpha'\beta'\ldots)\in C_A$$

Exkurs — Spieltheorie

Strategie, lokale Sicht: B sucht “Antwort” auf Zug von A und umgekehrt.

Wie gelangt man zu einer guten Strategie ?

Entsprechend besitzt B eine Gewinnstrategie gdw.

$$\forall\alpha\exists\beta\forall\alpha'\exists\beta'\ldots(c\alpha\beta\alpha'\beta'\ldots)\in C_B$$

Satz: Gibt es in Zweipersonenspielen mit vollständiger Information kein Unentschieden, so hat entweder Spieler A oder Spieler B eine Gewinnstrategie. (Einer-Wird-Gewinnen)

Beweis: . . . de Morgan. . .

Exkurs — Spieltheorie: ein Beispiel

Satz: Spieler A hat eine Gewinnstrategie für "Vier gewinnt".

Beweis: ist konstruktiv, siehe folgende Diplomarbeit von 1988

Exkurs — Spieltheorie ein weiteres Beispiel

 Rekonstruktion eines antiken Mühle-Spiels

Satz: Es gibt weder für A noch für B eine Gewinnstrategie bei “Mühle”.

Beweis: besteht aus einer 17 GB großen Datei . . .

Ebenfalls Ergebnis einer Diplomarbeit (von 1993)

Exkurs — Spieltheorie Motivation

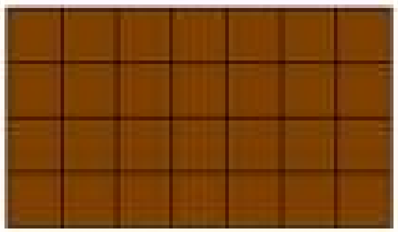
Schwerpunkt Spieleprogrammierung bei Prof. Sturm

Für Wirtschaftsinformatiker insbesondere: Historischer Ausgangspunkt der Spieltheorie ist die Analyse von Gesellschaftsspielen durch Joh(an)n von Neumann (ungarisch: Neumann János) im Jahre 1928.
Anwendbarkeit des von ihm entwickelten Ansatzes zur Analyse wirtschaftlicher Fragestellungen $\leadsto$
"Spieltheorie und wirtschaftliches Verhalten" (Theory of Games and Economic Behavior; JvN und Oskar Morgenstern, 1944):
Startpunkt der modernen Spieltheorie

John von Neumann — einer der ersten Informatiker ?

Spieltheorie
Grundkonzeption der Architektur heutiger Rechner
Zelluläre Automaten (hochparallele Systeme)
aber auch: Atom- & Wasserstoffbombenpolitik

Chomp: Das Feld links unten auf der $n \times m$-Tafel ist vergiftet !



"Zugteile":  

Die zwei Spieler wählen abwechselnd ein Schokoladenstück und essen nicht nur das gewählte Stück, sondern alles, was sich rechts und oberhalb davon befindet. Der letzte Biss legt somit die gesamte verbleibende Schokolade fest.
Der Spieler, der das vergiftete Stückchen essen muss(!), hat verloren.

Chomp: Das Feld links unten auf der $n \times m$-Tafel ist vergiftet !
Aber manche schert das nicht !

Chomp: Das Feld links unten auf der $n \times m$-Tafel ist vergiftet !

Chomp: Das Feld links unten auf der $n \times m$-Tafel ist vergiftet !

Satz: Spieler A hat eine Gewinnstrategie, falls $n = m$.

Beweis: konstruktiv (!)

Im ersten Zug isst A alles bis auf die erste Zeile und die erste Spalte.

Isst nun B k Stückchen von der Zeile, isst A k Stückchen von der Spalte und umgekehrt.

Zum Schluss bleibt das Eck links unten für B übrig. $\rightsquigarrow$ A gewinnt.

Ebenso konstruktiv: Satz: Spieler A hat eine Gewinnstrategie, falls $n = 2$.

Wie geht's ?

Chomp: Das Feld links unten auf der $n \times m$-Tafel ist vergiftet !

Satz: Spieler A hat eine Gewinnstrategie.

Beweis: Eingangs gibt es $n \times m$ Schokoladenstücke, und bei jedem Biss verringert sich die Zahl der Schokoladenstückchen um wenigstens Eins.

$\leadsto$ Das Spiel endet stets mit Spieler A oder B als Gewinner.

Annahme: A hat keine Gewinnstrategie.

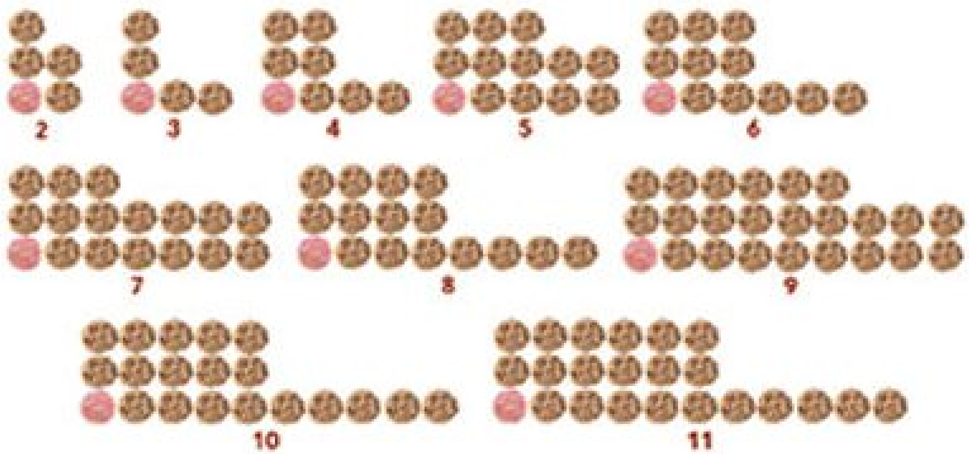
$\leadsto$ B hat eine Gewinnstrategie. (Einer-Wird-Gewinnen)

Auf einen beliebigen Zug α hat also B eine richtige Antwort β, um stets zu gewinnen.

Aufgrund der Struktur des Spiels hätte aber auch A den Biss β bereits ausführen können und hätte so eine Gewinnstrategie. Widerspruch !

Diplomarbeit (oder mehr. . .): Finde einen konstruktiven Beweis !

Chomp: Das Feld links unten auf der $3 \times m$-Tafel ist vergiftet !



Fallunterscheidungen

Erinnerung: Tautologie $p \equiv (q \implies p) \land (\neg q \implies p)$.

$\rightsquigarrow$ Fallunterscheidung: 1. q ist wahr; 2. q ist falsch.

Lemma: Sei $a \in \mathbb{Z}$.
a^2 geteilt durch vier lässt entweder den Rest Eins oder den Rest Null.

Beweis: 1. Fall: a ist gerade. $\rightsquigarrow \exists k(a = 2k)$. $\rightsquigarrow a^2 = (2k)^2 = 4k^2$. $\rightsquigarrow 4 \mid a^2$.

2. Fall: a ist ungerade. $\rightsquigarrow \exists k(a = 2k + 1)$. $\rightsquigarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. $\rightsquigarrow 4 \mid (a^2 - 1)$.

Fallunterscheidungen: noch eine Anwendung in der Zahlentheorie

Lemma: Sei $a \in \mathbb{Z}$.
Ist a nicht durch drei teilbar, so lässt a^2 beim Teilen durch drei den Rest Eins.

Beweis: "a ist nicht durch drei teilbar." $\iff$ $(3|(a-1)) \vee (3|(a-2))$.
"a^2 lässt beim Teilen durch drei den Rest Eins." $\iff$ $3|(a^2-1)$.

1. Fall: $(3|(a-1))$, $\rightsquigarrow \exists k(a = 3k+1)$. $\rightsquigarrow$

$$a^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

$\rightsquigarrow 3|(a^2-1)$.

2. Fall: $(3|(a-2))$, $\rightsquigarrow \exists k(a = 3k+2)$. $\rightsquigarrow$

$$a^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

$\rightsquigarrow 3|(a^2-1)$.

Fallunterscheidungen: Die allgemeine Sicht

Betrachte die Tautologie:

$$((p_1 \vee p_2 \vee \cdots \vee p_n) \implies q) \equiv [(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q)]$$

Fallunterscheidungen können also mehr als zwei Fälle umfassen.

Beweise mit vielen Fallunterscheidungen sind aber in der Regel nicht sehr elegant (und eignen sich nicht für eine Grundvorlesung).

Das Schubfachprinzip von Dirichlet 

Falls man n Gegenstände auf m Fächer ($n > m > 0$) verteilt, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Beweis: Falls das Prinzip nicht stimmt, dann landet in jedem Schubfach höchstens ein Gegenstand.

Damit gibt es höchstens soviele Gegenstände wie Schubfächer.

$\rightsquigarrow$ Widerspruch zur Annahme, dass es mehr Gegenstände als Schubfächer gibt.

Schubfachprinzip: Eine spielerische Anwendung

In einer Gruppe von acht Leuten haben (mindestens) zwei am gleichen Wochentag Geburtstag.

n Gegenstände: 8 Leute
m Schubfächer: 7 Wochentage
Verteilung wird vorgenommen über die Geburtstage (aber das ist <u>unwesentlich</u> für das Prinzip)

Schubfachprinzip: Etwas mit Logik

Lemma: Es seien p_1, p_2, p_3 Aussagen. Unter ihnen gibt es zwei, die logisch äquivalent sind.

Beweis: n Gegenstände: 3 Aussagen

m Schubfächer: 2 Wahrheitswerte

Also kommt wenigstens zwei Aussagen derselbe Wahrheitswert zu.

Schubfachprinzip: Eine zahlentheoretische Anwendung

Satz: Jede Folge von n^2+1 verschiedenen Zahlen enthält eine monoton fallende oder eine monoton wachsende Unterfolge der Länge $n+1$.

Beispiel: ($n = 3$) Die Folge $7, 6, 11, 13, 5, 2, 4, 1, 9, 8$ enthält die fallende Folge $7, 6, 5, 2, 1$.

Beweis: Sei $a(1), \ldots, a(n^2+1)$ eine Zahlenfolge. Ordne $a(k)$ das Paar $(\sigma(k), \phi(k))$ zu mit:
$\sigma(k)$: Länge der längsten monoton steigenden Unterfolge, die bei $a(k)$ beginnt
$\phi(k)$: Länge der längsten monoton fallenden Unterfolge, die bei $a(k)$ beginnt

Wenn die Behauptung falsch wäre, so gölte $\forall k((\sigma(k) \leq n) \wedge (\phi(k) \leq n))$.
Schubfachprinzip $\leadsto$ es gibt $s < t$ mit $\sigma(s) = \sigma(t)$ und $\phi(s) = \phi(t)$.

1. Fall: $a(s) < a(t)$: Dann gibt es eine aufsteigende Folge der Länge $\sigma(t) + 1$; betrachte $a(s)$ gefolgt von der bei $a(t)$ beginnenden steigenden Folge $\leadsto \sigma(s) \geq \sigma(t) + 1$.
2. Fall: $a(s) > a(t)$ analoge Verlängerung der bei $a(s)$ beginnenden fallenden Folge.

$\lceil x \rceil$: kleinste ganze Zahl n mit $n \geq x$ (Aufrundefunktion; ceiling)

Das **Schubfachprinzip**: Eine Verallgemeinerung

Satz: Werden $n > k$ Gegenstände auf k Fächer verteilt, so gibt es mindestens ein Fach, das $\lceil \frac{n}{k} \rceil$ Gegenstände enthält.

Beweis: Wäre das nicht der Fall, so können die Fächer insgesamt nicht mehr als

$$k\left(\left\lceil \frac{n}{k} \right\rceil - 1\right) < k\left(\left(\frac{n}{k} + 1\right) - 1\right) = n$$

Gegenstände enthalten; Widerspruch !