Joseph Birkner Matrikel-Nr. 2982838	LDS - WS 14/15	Gruppe 5 Tutor: T. Böpple

Klausurvorbereitung

Aussagenlogik

- Umformungsregeln
  - Kommutativität
  - Assoziativität
  - Distributivität
  - Ersetzbarkeitstherorem: Eine Teilformel X in Y kann durch eine erfüllbarkeitsäquivalente Teilformel X' ersetzt werden.
  - De-Morgan: $\neg(A \wedge B) \equiv (\neg A \vee \neg B), \neg(A \vee B) \equiv (\neg A \wedge \neg B)$
  - Doppelnegation
  - Idempotenzgesetz: $a \wedge a \equiv a$, $a \vee a \equiv a$
  - Absorptionsgesetz: $a \vee (a \wedge b) \equiv a$, $a \wedge (a \vee b) \equiv a$
- KNF, DNF
- **Resolution**: Test ob Formel in KNF unerfüllbar (Herleitung einer leeren Klausel):
  Nimm zwei Klauseln, von denen eine A enthält und die andere $\neg A$
  Vereinige diese Klauseln zu einer neuen Klausel, die alle Variablen bis auf A enthält.
  Wiederhole, bis leere Klausel gefunden.
- **Endlichkeitssatz**: Eine (möglicherweise unendliche) Formelmenge X ist genau dann erfüllbar (d. h. hat ein Modell), wenn jede endliche Teilmenge von X erfüllbar ist.
- Hornformeln: KNF, in der jede Klausel maximal ein positives Literal enthält.
- Erfüllbarkeitstest (Markierungsalgorithmus) für Hornformeln:
  1. Bringe Hornformel in Implikationsschreibweise:
     A $\equiv 1 \Rightarrow A$, $\neg A \equiv A \Rightarrow 0$, $A \vee \neg B \vee \neg C \equiv (B \wedge C) \Rightarrow A$
  2. Kommt $A \Rightarrow 1$ vor, markiere A.
  3. Kommt $(B \wedge C) \Rightarrow D$ vor, und B, C sind markiert, markiere D.
  4. Kommt $(E \wedge F) \Rightarrow 0$ vor, und E und F sind markiert: HALT $\Rightarrow$ unerfüllbar.
     Ansonsten wenn möglich weiter bei 2|3. Ansonsten: HALT: $\Rightarrow$ erfüllbar.

Prädikatenlogik

- Atom: $P(t_1, t_2, ..., t_n)$, Literal: Atom oder negiertes Atom, Geschlossene Formel: Ohne freie Variablen
- 'Struktur': Besteht aus 'Universum' und 'Interpretation'. Universum: Wertebreich für Funktionen und Variablen. Interpretation: Belegung von Funktionen und Prädikaten.
- Unifikation: Angleichung von aussagenlogischen Formeln durch Substitutionen:
  1. Seien A, B zwei Formeln. Suche erste Stelle, an der sich A von B unterscheidet.
  2. Seien x, t die Terme an dieser Stelle.
     Wenn weder x noch t eine Variable $\Rightarrow$: HALT $\Rightarrow$ Nicht unifizierbar.
     Ansonsten: Wenn t ein Term ist, und t enthält x: HALT $\Rightarrow$ Nicht unifizierbar.
     Ansonsten: Substituiere x mit t.
  3. Wiederhole (1) bis Formelende erreicht. HALT $\Rightarrow$ Unifikator gefunden.
- (Bereinigte) Pränexform: Keine freien Variablen (freie Variablen mit $\exists$-Quantoren gebunden, Alle Quantoren am Anfang
- Skolemform: Ersetze $\exists$-gebundene Variablen durch neue n-stellige Funktionssymbole $f(a_1, ..., a_n)$, wobei $a_1, ..., a_n$ die in der Formel vorkommenden $\forall$-gebundenen Variablen sind.
- Matrix: Skolemform ohne Quantoren, in KNF. Ist die Matrix erfüllbar, so ist auch die BPNF erfüllbar. Das Erfüllbarkeitsproblem an sich ist aber trotzdem unentscheidbar (Y/?).
- Herbrand-Universum: Universum besteht aus rekursiver Einsetzung von Funktionen für Parameter. Funktionen sind als sie selbst definert. Offen bleibt nur die Interpretation der Prädikate.

Graphentheorie

- Satz: Die Summe aller Knotengrade in einem endlichen Graphen ist immer gerade.
- P_n: Pfad mit n Knoten
- C_n: Kreis durch n Knoten
- K_n: Vollständiger Graph durch n Knoten, Anzahl der Kanten ist $\binom{n}{2}$.
  Sonderfall: "Bipartite Graphen"$K_{m,n}$: Jeder Knoten aus A mit $|A| = m$ ist mit jedem Knoten aus B mit $|B| = n$ verbunden.
- Eulerweg: Jede Kante wird genau einmal durchlaufen. Existiert, wenn maximal 2 Knoten einen ungeraden Grad haben.
- Eulerkreis: Geschlossener Eulerweg. Existiert, wenn alle Knoten graden Grad haben.
- Plättbarkeit:
  - Satz von Kuratowski: Ein Graph ist plättbar, wenn er weder K_5 noch $K_{3,3}$ enthält.
  - Satz von Euler: Ein Graph G mit Knoten V und Kanten E ist genau dann plättbar, wenn $|V| - |E| + f = 2$, wobei f die Anzahl der Facetten des Graphen ist.

Modulare Algebra

- Erweiterter Euklidischer Algorithmus, $\text{ggT}(a, b) = m * a + n * b, m, n \in \mathbb{Z}$
- Lemma von Bezout, "Rückwärts einsetzen"
- Exponentiation großer (modularer) Zahlen:
  $a^e \bmod n \equiv$ while(e>1){ if(e ungerade) ret = ret*a mod n; e /= 2; a = a*a mod n; }
- Direktes Lösen von simultanen Kongruenzen ganzer Zahlen:
  $x \equiv a$ mod n
  $x \equiv b$ mod m
  $d = \text{ggT}(n, m) = y * n + z * m$
  $x \equiv a - y * n * \frac{a-b}{d} \bmod \frac{n*m}{d}$
- Algebraische Strukturen:
  Halbgruppen $\Rightarrow$ .. ist assoziativ.
  Monoide $\Rightarrow$ .. hat ein neutrales Element.
  Gruppen $\Rightarrow$ .. alle Elemente sind invertierbar.
  Abelsche Gruppen $\Rightarrow$ .. ist kommutativ.
  Ringe $\Rightarrow$ .. ist abelsche Gruppe mit + und Monoid mit $*$. Es gelten Distributivgesetze.
  Körper $\Rightarrow$ .. ist abelsche Gruppe mit $*$.
- Chinesischer Restsatz:
  $\text{ggT}(a, b) = 1 \Rightarrow \mathbb{Z}/ab \Leftrightarrow \mathbb{Z}/a * \mathbb{Z}/b$ (Ringisomorphismus)
- Kleiner Satz von Fermat:
  p ist Primzahl $\Rightarrow n^{(p-1)} \equiv 1 \bmod p$
- Satz von Euler-Fermat:
  $ggT(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \bmod n$
- Eulersche phi-Funktion (Anzahl aller Teilerfremden von n kleiner als n):
  $\phi(n) = n * \sum_{\text{p ist Primzahl} \wedge p|n} 1 - \frac{1}{p}$
- Primzahlzertifikat:
  $n \in \mathbb{N}$ ist Primzahl $\Leftrightarrow \forall p|(n-1) : \exists a \in \mathbb{N}$:
  $a^{n-1} \equiv 1 \bmod n \wedge$
  $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$
- RSA:
  1. Bestimme Primzahlen $\{p, q | p \neq q \wedge p, q > 3\}$
  2. Bestimme Öffentlichen Modulo $n = p * q$
  3. Bestimme $\phi(n) = (p-1)(q-1)$
  4. Bestimme Öffentlichen Random Exponent e mit $ggT(e, \phi(n)) = 1$
  5. Veröffentliche öffentliches Schlüsselpaar (n, e)
  6. Bestimme Geheimen Exponenten s mit $e * s \equiv 1 \bmod \phi(n)$
  7. Beweis: $(x^e)^s = x \bmod n$

Wachstumsabschätzungen

- Fakultät:
  (Anzahl der Möglichkeiten, Permutationen aus einer Menge M zu bilden.)
  Stirlingsche Formel: $n! \sim \sqrt{2\pi n}(\frac{n}{e})^n$
- Binomialkoeffizient
- Fibonacci-Zahlen F_n, Goldener Schnitt G
  $G = \frac{1+\sqrt{5}}{2} \sim 1.618$
  $\bar{G} = \frac{1-\sqrt{5}}{2} \sim 0.618$
  $F_n = \frac{1}{\sqrt{5}}(G^n - \bar{G}^n)$
- Ableitungsregeln
- Asymptotik der Primzahldichte nach Gauß:
  $\pi(n) = \frac{n}{\ln(n)}$
- Bertrandtsches Postulat:
  $\forall G \in \{\{n, .., 2n\} | n \in \mathbb{N}\} : \exists p \in G : p$ ist prim.
- kgV

Diskrete Wahrscheinlichkeitsrechnung

- Ereignis
- Zufallsvariable X
- Wichtige Formeln:

Erwartungswert:	$E[X] = \sum_{\omega \in \Omega} X(\omega) * Pr[\omega]$
Varianz:	$\mathrm{Var}[X] = \sum_{x \in X}(x - E[X])^2 Pr[X = x]$
Standardabweichung:	$\sigma_X = \sqrt{\mathrm{Var}[X]}$
Tschebitschevsche Ungleichung:	$Pr[\lvert X - E[X] \rvert \geq \lambda\sigma_X] \leq \frac{1}{\lambda^2} \mid Pr[\lvert X - E[X] \rvert \geq N] \leq \frac{E[X]}{N^2}$
Markovsche Ungleichung:	$Pr[X \geq \lambda E[X]] \leq \frac{1}{\lambda}$

Kombinatorik

- Binomialkoeffizienten-Formeln:

Binomialkoeffizient: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$	**Trinomiale Revision:** $\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$
Additionstheorem: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$	**Obere Summation:** $\binom{n+1}{m+1} = \sum_{k=m}^{n} \binom{k}{m}$
Invertierbarkeit von k: $\binom{n}{k} = \binom{n}{n-k}$	**Parallele Summation:** $\binom{n+k-1}{k} = \sum_{i=0}^{k} \binom{n+k}{k}$
Binomialsatz: $(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$	**Vandermondsche Identität:** $\binom{x+y}{n} = \sum_{k=0}^{x} \binom{x}{k}\binom{y}{n-k}$

- Kombinatorische Formelmatrix:

	Mit Zurücklegen	Ohne Zurücklegen
Mit Reihenfolge	n^k	$\frac{n!}{(n-k)!}$
Ohne Reihenfolge	$\binom{n+k-1}{k}$	$\binom{n}{k}$

- Catalan-Zahlen:
  Anzahl der Dyck-Wörter mit Länge 2n, Anzahl der Binärbäume mit n Knoten, Anzahl der saturierten Binärbäume mit n inneren Knoten:
  $C_n = \frac{1}{n+1}\binom{2n}{n}$