2.Формални системи(ФС), логика и доказателства, използвани в Z нотацията - Резюме

Логика в Z нотацията:

- Базира се на **математич. логика и теория на множествата**;
- Използва **схеми** за описание на типове данни, състояния на с-мата и операции, начините за промяна на състояние;

Пропозиционна логика: Работи с твърдения. **Твърдението** е **изявление** за предполагаем факт. То е или вярно или невярно, но никога и двете. Използват се логически оператори (¬ not, ∧ and/конюнкция, ∨ or/дизюнкция, ⇒ Импликация (ако-то), ⇔ Еквивалентност/тогава и само тогава/) и изреч.(p, q, r...). Семантика: Стойността на истинност се определя чрез таблици на истинност. Значението на пропозиционното изречение (wff) се дефинира като: **а)** Всеки примитивен символ (p, q, r, ...) се интерпретира чрез твърдение, което се свързва със съответната си стойност на истинност: истина (t) или лъжа (f). Пр.: p - Днес е сряда. **b)** Истинността на сложните твърдения се дефинира единствено от истинността на отделните съставящи твърдения.

Методи за доказателства:

Дедукция: Доказателство чрез **естествено умозаключение**.

Доказателство чрез опровергаване: Д-тво чрез противоречие.

Доказателство чрез анализ на случаи: Разделяне на доказателството на подслучаи.

Разсъждение чрез равенства: Д-тва чрез еквивалентности (пр. закони на **Де Морган** ¬(A∧B)≡¬A∨¬B, двойно отрицание ¬(¬A)≡A.

Предикатна логика: Универсални твърдения ∀- описват характеристики на всеки обект от разглежданото множество - всички елементи от дад. множество S удовлетворяват свойство P

$\forall x : S \bullet \text{Stooge}(x)$
$\text{Stooge}(x1) \land \text{Stooge}(x2) \land \text{Stooge}(x3) \land \ldots$
Stooge( ) се нарича ПРЕДИКАТ

Екзистенциални твърдения ∃: съществуването на елемент от множество S, който притежава свойство P:

$\exists x : S \bullet P(x)$ или $P(x1) \lor P(x2) \lor P(x3) \lor \ldots$

Свойствата (предикатите) могат да се разглеждат като **булеви** функции: когато се приложат към аргумент връщат стойност истина или лъжа. Предикатите могат да имат n-аргумента: P(x,y,z)

символът ● обикновено служи като **разделител** или **ограничител на обхвата** - „**такова, че**“ или „**където**“.

-Описва свойства на обекти от дад. множество чрез предикати.

-Синтаксисът вкл. допълн. символи и обхвати на променливите.

One-point rule -**Опростява** екзистенциални изрази чрез **замяна на променливи** със стойности.

тавтология (tautology)- твърдения винаги верни

противоречие (contradiction) - твърдения винаги неверни

(contingency) – напр.случайност **-** нито истина, нито лъжа

доказателството- Повишава качеството на софтуера**:**

-изясняване на изискванията: доказателството помага в изясняването на с-мата и идентифицира скритите допускания

- доказател. показва, че проектът е верен и оясннява защо е верен

-в етапа на изпълнение: осигурява факта, че имплементираната част от кода се “държи” като нейната спецификация

Доказателство: **P |= W** , W е истина, когато твърденията от списъка P са истина. **W е семантично следствие на P**.

Дедукция: Пропозиционни изчисления: **правила за извод**: **Ако можем да докажем тези факти/ Можем да направим заключение за тези факти или Истинността на заключението е следствие на истинността на предпоставката**

Modus Ponens: P→Q (Ако P, тогава Q)

Modus Tollens /proof by contradiction**/**: **p ⇒ q is true** and **q is false** then **p is false**.

Case Analysis/ v-elimination**/** (p ⇒r) ∧ (q ⇒ r) ≡ (p v q ⇒ r)

Simple Case Analysis (p ⇒ r) ∧ (¬ p ⇒ r) ≡ r

Доказателство чрез равенство/еквивалентност - Две изречения са еквивалентни (≡), ако имат равна стойност на истинност при всяка интерпретация: ¬ (p ∧ ¬q) ≡ (q v ¬p)

Пропозиционното изчисление е **последователно** ако: Всичко, което може да се докаже, е вярно: P |- W, то P |= W

Пропоз. изчисление е **пълно** ако: всичко, което е валидно, може да бъде доказано чрез правила за извод: Ако P |= W, то P |- W

⇔ е като ≡ : = два обекта са еднакви

|-P ≡ Q (синтактична доказуемост)- можем да **докажем логическата еквивалентност P≡Q** в дад. ФС, използвайки **правила на дедукция -форм. доказване** -правила и аксиоми.

|=P ≡ Q (семантична истинност) - логическата еквивалентност P≡Q е вярна във всички модели т.е. при всяка възм. интерпретация P и Q имат една и съща ст-ст (верни/ неверни).

Определители и декларации в Z нотацията:

Ξ x: a | p • q **Ξ** значи (∀ **или** ∃)

x ограничена промен.; **a** обхват на x; **p** ограничение; **q** предикат

Заместване (Substitution rule): Ако m=n, то валидното за n е валидно и за m.

The one-point rule: е концепция в Z-нотацията, която се използва за опростяване на изрази, свързани с квантори (например ∀ и ∃)