Exam questions

10893, Rasmus Bækgaard

Nov. 22th, 2013

Contents

1 Set

Disposition

- Symbols
- Sets/subsets
- Powersets
- Set operations

Symbols

- $\mathbb{N}$ – natural number (positive integers)
- $\mathbb{Z}$ – integers – whole numbers.
- $\mathbb{Q}$ – rational numbers – $\frac{m}{n}$ where $m, n \in \mathbb{Z}$
- $\mathbb{I}$ – irrational numbers – like $\sqrt{2}, \pi$
- $\mathbb{R}$ – real numbers – Everything with and without comma.
- $\mathbb{C}$ – complex numbers – $a + b \cdot i$
- $\emptyset$ – Empty set – nothing

Cardinal number / cardinality

The amount of elements in a set:
$|S| = \{2, -3, \emptyset\} = 3$

1.1 Subset

Basic

- A set within a set: $S = \{a, b, c\}, T = \{a, b\}, U = \{a, b, c\}, V = \{c\}$
- Can be written as $T \subseteq S$
  - Pronounced: "*T is a **proper** subset of S*".
- Can be written as $S \subseteq U$
  - Pronounced: "*S is a subset of U*".
- If a set is not in another set it's written as $T \nsubseteq V$

Intervals

- Open, $(a, b) = \{x \in \mathbb{R} : a < x < b\}$
- Closed, $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- Half open (bottom closed), $[a, b) = \{x \in \mathbb{R} : a \leq x < b\}$
- Half closed (top closed), $(a, b] = \{x \in \mathbb{R} : a < x \leq b\}$

Power set

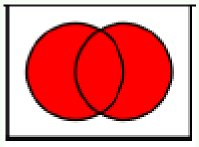
- A combination of all elements as **subsets**:

  $A = \emptyset, B = \{a, b\}, C = \{1, 2, 3\}$
- $\mathcal{P}(A) = \{\emptyset\}$
- $\mathcal{P}(B) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$
- $\mathcal{P}(C) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
- Cardinality: $|\mathcal{P}(A)| = 2^{|A|}$
- $\mathcal{P}(set) = \{subset : subset \subseteq set\}$

1.2 Set operations

Union

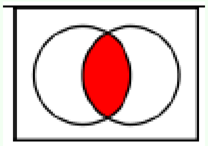
- Means "in total"
- Written as $A \cup B$
- SQL: `SELECT A, B IN Sets`



Intersection

- Means "in common"
- Written as $A \cap B$
- If nothing is in common it's called **disjoint** and written $A \cap B = \emptyset$
- Can be written as $A \cap B = \{x \in A \vee x \in B : x \in A \wedge x \in B\}$
- SQL:

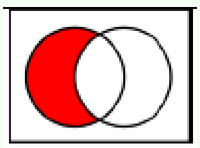
```
SELECT A, B
FROM SetA
INNER JOIN SetB
ON A.a = b.a
```



Difference

- Means "What does A have which B does not"
- Written as $A - B$
- Can also be written as $A \setminus B$
- SQL:

```
SELECT A, B
FROM SetA
INNER JOIN SetB
ON A.a = b.a
```



2 Logic

Disposition

- Basic
- Dis- and con-junction: $\vee, \wedge$
- Implies and biconditional: $\Rightarrow$ & $\Leftrightarrow$
- Logical equivalence: $\equiv$
- De Morgan's laws
- Quantifiers: $\forall, \exists$

Basic

- True or false
- Truth table
- **Open sentence** – 1 or more variables, x, y in a **domain**
- **Open sentence over the domain** – $P(x)$
  - $P(x) : x + 1 \geq 1$ is over the domain $\mathbb{Z}$ (integers)
- **Negation** – means "not"

Disjunctions and conjunctions

- **Disjunction** – "or", written as $P \vee Q$. *Any of them true?*
  - **Exclusive or** – xor
- **Conjunction** – "and", written as $P \wedge Q$. "Are both true?"

Implies and biconditional

- $P \Rightarrow Q$ – politician logic.
- P is also called a **hypothesis / premesis**
- Q is the **conclusion**
- $Q \Rightarrow P$ is a **converse**
- **Biconditional**, written as $P \Leftrightarrow Q$ and said "P is equivalent to Q" or "If and only if"

P	Q	$P \Rightarrow Q)$
T	T	T
T	F	F
F	T	T
F	F	T

Logical equivalence and fundamental properties

- $P \vee Q \equiv Q \vee P$ (Commutative law)
- $P \vee (Q \vee R) \equiv (P \vee Q \vee R)$ (Associative law)
- $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ (Distributive law)

De Morgan's laws

- Proof by truth table
- $\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$
- $\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$

P	Q	$\neg(P \wedge Q)$	$(\neg P) \vee (\neg Q)$
T	T	F	F
T	F	T	T
F	T	T	T
F	F	T	T

Quantifiers

- **Universal quantifier** – $\forall$ – $\forall x \in \mathbb{N}, x \geq 0$
- **Existential quantifier** – $\exists$ – $\exists x \in \mathbb{N}, x < 2$
- Can be written as: $\exists x \in \mathbb{Z}, P(x)$, where $P(x) : x^2 < 1$

3 Proofs techniques

Disposition

- Basic
- Conjecture
- Trivial proof
- Vacuous proof
- Direct proof
- Indirect / contrapositive
- Proof by cases

Basic

- **Axiom** – statement whose truth is accepted without proof.
- **Theorem** – statement which can be verified.
- **Corollary** – a consequence of some earlier result and to be deduced from.
- **Lemma** –a result used as help for another statement.

Conjecture

- A conjecture is something we **believe to be true**, normally based on examples.

$1 = 1$,
$1 + 2 = 3$,
$1 + 2 + 3 = 6$.
Conjecture: $1 + \ldots + n = \sum_{k=1}^{n} n = \frac{n(n+1)}{2}$

Trivial proof

- Something that is true – no need to prove it.
- Let $n \in \mathbb{Z}$. If $n^3 > 0$ then 3 is odd

Vacuous proof

- If something is always proven wrong:
- Let $n \in \mathbb{Z}$. If **3 is even**, then $n^3 > 0$

  Clearly wrong!

Direct proof

- Show only what needs to be shown
- $\forall x \in S, P(x) \Rightarrow Q(x)$

  Show only that this is true also when Q is false.
- Is shown from lemmas and other proofs.

Politician statement

P	Q	P $\Rightarrow$ Q
T	T	T
T	F	F
F	T	T
F	F	T

Indirect proof / proof by contrapositive

- Reverse the result and means.
- Let $x \in S$. If $Q(x)$, then $P(x) \Rightarrow$

  Let $x \in S$. If $\neg Q(x)$, then $\neg P(x)$

Politician statement

P	Q	$\neg P \Rightarrow \neg Q$
T	T	T
T	F	F
F	T	T
F	F	T

Proof by cases

- Do subcases and show they span the result.
- Case 1: n is even (U). Case 2: n is odd (L). $\mathbb{Z} = U \cup L$
- Case 1: $n \geq 0$ (U). Case 2: $n < 0$ (L). $\mathbb{Z} = U \cup L$

Contradiction

$P \Rightarrow \neg Q$
"Assume there's no smallest number" – flip it:
"Assume there's a smallest number called r – what about $0 < \frac{r}{2} < r$"

Induction

- Base case $P(1)$, assuming $P(k)$ sticks
- Induction, $P(k+1)$

Counter example

$P(k) \not\Rightarrow Q$
$\forall x \in \mathbb{N}, n > 2 \rightarrow n = 1 \not> 2$

4 Direct and contrapositive proof techniques

Disposition

- Basic
- Deduction
- Direct proof
- Counter example

Basic

- **Axiom** – statement whose truth is accepted without proof.
- **Theorem** – statement which can be verified.
- **Corollary** – a consequence of some earlier result and to be deduced from.
- **Lemma** –a result used as help for another statement.

Direct proof

- Show only what needs to be shown
- $\forall x \in S, P(x) \Rightarrow Q(x)$

  Show only that this is true also when Q is false.
- Is shown from lemmas and other proofs.

Politician statement

P	Q	P ⇒ Q
T	T	T
T	F	F
F	T	T
F	F	T

Deduction

- given P show Q

- Direct proof $P \Rightarrow Q$
- Proof by cases $P(1) \Rightarrow Q, P(2) \Rightarrow Q$
- Proof by contrapositive $\neg Q \Rightarrow \neg P$

Indirect proof / proof by contrapositive

- Reverse the result and means.
- Let $x \in S$. If $Q(x)$, then $P(x) \Rightarrow$

  Let $x \in S$. If $\neg Q(x)$, then $\neg P(x)$

Politician statement

P	Q	$\neg P \Rightarrow \neg Q$
T	T	T
T	F	F
F	T	T
F	F	T

4.1 Her mangler

5 Counterexamples and contradictive proof techniques

Disposition

- Counterexample
- Contradiction
- Existence proof
- Existence disproof

Counterexample

- A counterexample is **one case** that proves a statement **wrong**
- Example
  $\forall x \in \mathbb{N}, x < x^2$
  $x = 1 \Leftrightarrow 1 < 1^2 \Leftrightarrow 1 \not< 1$

Proof by contradiction

- A contradiction, $\neg Q$, is assumed to be false so that Q is true.

  $(P \Rightarrow Q) = true$ becomes $(P \Rightarrow \neg Q) = false$

  $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

- Example:

  Let $x, y \in \mathbb{R}^+$. Use a proof by contradiction to prove that if $x < y$ then $\sqrt{x} < \sqrt{y}$

  Lets rewrite the statement:

$$\begin{aligned}
&\forall x, y \in \mathbb{R}^+, P \Rightarrow Q && P = x < y \text{ and } Q = \sqrt{x} < \sqrt{y} && (1)\\
&\exists x, y \in \mathbb{R}^+, P \Rightarrow \neg Q && && (2)\\
&\neg Q = \neg(\sqrt{x} < \sqrt{y}) && && (3)\\
&\neg\sqrt{x} < \neg\sqrt{y} && && (4)\\
&\sqrt{x} \geq \sqrt{y} && \text{Remove negation} && (5)\\
&x \geq y && \text{Square both sides} && (6)
\end{aligned}$$

  Since $x < y$ and $x \geq y$ is clearly not the same, the statement is proven.

Existence proofs

There are two kinds:

- **Witness**: A single example

  Example: $\exists x \in \mathbb{R}, x > 0$ and pick $x = 1$

- **General/abstract**:

  Example: $\exists p \in \text{room}, \forall p' \in \text{room}, \text{Hairlenght}(p) \geq \text{Hairlenght}(p')$

  Someone in the room has longer or equal long hair than everyone else – remember more than 1 in room.

Existence Disproofs

- Just like a contradiction, but for existential it's a property that never holds:
- $\neg\big(\exists x \in S, R(x)\big) \equiv \forall x \in S, \neg R(x)$

6 Induction proof techniques

Well-ordered

- Nonempty subset with a least element
  - The smallest element in a subset of a set.
  - If all numbers in the set can be listed, you can find a least element
  - If you do not have, $x \in \mathbb{Q}, x < 0$ can have a subset $(0, 10]$ and that has no listed minimum.

<u>Disposition</u>

- Well-ordered
- Basic
- Induction hypothesis
- Strong induction
- Minimum counterexample

Basic

- Proves a statement $P(n)$ holds for $P(n+1)$.
- Make **base step**: $p(1)$ is true

  This is also called **the induction hypothesis**.
- Make **induction step**: $\forall k \in \mathbb{N}, P(k) \Rightarrow P(k+1)$ is true.
- Make conclusion: $P(n)$ is true for all natural numbers, n.

Induction hypothesis

- Induction step is $P(k) \Rightarrow P(k+1)$
- Remember to depend on $P(k)$
- Without this – no induction
  - $\forall n \in \mathbb{Z}^+, 2^n \geq n$ (For every nonnegative integer $n \ldots$)
  - Base step: $n = 0$ is true since $2^0 > 0$. Assume $2^k > k$ gives the same.
  - Induction Step: $2^{k+1} = k+1$. When $k = 0$, we have $2^{0+1} = 2 > 0 + 1 = 1$. Assume $k \geq 1$.
  - Then $2^{k+1} = 2 \cdot 2^k > 2k = k + k \geq k + 1$.

Strong induction

- We don't have to start at 1 or natural numbers.
- We have a base (proved elsewhere), a gap where some example should be, and a *prior*, k which will imply $k+1$.
- Base set: $\forall n \in \mathbb{N}, P(n)$ where $n \geq 10$. This gives us $P(10)$ as base case.
- Induction step: If $P(i)$ for every integer i with $10 \leq i \leq k$, then $P(k+1)$ is true for every positive integer k above or equal to 10.
  - Not just $P(10)$ and $P(k)$ but also all in between:
    $P(i), P(i+1), P(i+2) \ldots$
- Conclusion: $P(k+1)$ is true.

Minimum counterexample

- Assume a statement is false.
- Make it a contradiction, showing it is **not** false.
- A way of getting more information for the proof.

7 Functions

Basic

- $f : A \to B$ – "Function f from A to B"
- Domain: $dom(f)$ – Entire input
- Codomain: $codom(f)$ – Entire output
- Image and map: $b = f(a)$ – b is the image and f maps a **into** b.
- Inverse image: $b = f(a)$ – a can be the output, but not necessarily.
- Range: $range(f)$ – What is output (not all)
- Onto: $range(f) = codom(f)$
- One-to-one: Every element n the target is only hit once

Onto and one-to-one

- Onto or **surjective**: Multiple $f(x)$ gives $f(y)$
- One-one or **injective**: Straight over.
- One-one is also called **bijective** or **one-to-one correspondence** if it is both one-to-one *and* onto (If range and codomain is equal)

Identity function

- If R is equivalence relation it's, reflective, symmetric and transitive
- If the function is $A \to A$ it's called **Identity**.
- this means $R : \{(a, a), (b, b), (c, c) \dots\}$
  - This is only used *once* on each side

Composition

- $A \to f \to B \to g \to C$
- $(g \circ f)(x) : A \to C$
- $(g \circ f)(x) = g\big(f(x)\big) \forall a \in A$

Inverse function

- A set with pairs where the pairs are inverted.
- $R = \{(a, 1), (b, 2)\}$
  $R^{-1} = \{(1, a), (2, b)\}$
- $R^{-1} = \{(b, a) : (a, b) \in R\}$

8 Relations

Disposition

- Basic
- Reflection
- Symmetric
- Transitive
- Distance
- Equivalence relation and -class
- Congruence modulon

Basic

- R is a **relation** from A to B: $R \subseteq A \times B$
  - $A = \{x, y, z\}, B = \{1, 2\}$
    $R = \{(x, 2), (y, 1), (y, 2)\}$
- If $(a, b) \in R$ then a is **related** to b
- **Domain**: $R - dom(R)$ is the subset of A
  - $dom(R) = \{a \in A : (a, b) \in R \text{ for some } b \in B\}$
- **Range**: $R - range(R)$ is a subset of B.
  - $range(R) = \{b \in B : (a, b) \in R \text{ for some } a \in A\}$
- Inverse relation: $R = R^{-1}$
  - $R^{-1} = \{(b, a) : (a, b) \in R\}$
  - **Example**: $R = \{(x, 2), (y, 1), (y, 2)\} \rightarrow R^{-1} = \{(2, x), (1, y), (2, y)\}$
- **Relation on a set**: If $A = \{1, 2\}$ then $A \times A = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$

Reflection

- Reflection: $\forall x, a \in A : xRa \Rightarrow aRx$

Symmetric

- Symmetric: $\forall x, y \in A, xRy \Rightarrow yRx$

Transitive

- Transitive: $\forall x, y, z \in A, xRy \land yRz \Rightarrow xRz$
  - $A = \{1\}$ is also transitive, since $(1, 1)$ and $(1, 1)$ you can go to $(1, 1)$.

Distance

- The distance between two numbers: $|a - b|$ is the numeric value.

Equivalence-relation and -class

- A relation is equivalence when *reflexive, symmetric and transitive* is all applied.
- Write up R and write a class as

  $[a] = \{x \in A : xRa\}$

  Example: $[a] = \{a, b\}$
- If a set has already been described, it is written:

  $[b] = [a]$

  $[c] = \{c\}$

Congruence Modulon

- Like modulus with modifications
- For a, b where $n \geq 2$, a is **congruent to** b **modulo** n.

  Example: $24 \equiv 6 \pmod 9$

  $\{0, 9, 18\} + 6 = 24$

  Example: