Capítulo 1: Fundamentos: Lógica y Demostraciones

Clase 2: Lógica de Predicados y Métodos de Demostración

Matemática Discreta - CC3101

Profesor: Pablo Barceló

Predicados

La lógica proposicional no puede expresar adecuadamente el significado de ciertos razonamientos muy usuales en matemática:

- Todo número natural es par o impar.
- Existen números irracionales x, y tal que x^y es racional.

Podemos pensar que un predicado es una proposición que además menciona a ciertas variables:

$$x > 3, \quad x = y + 5, \quad x = y^2$$

Los predicados no son verdaderos ni falsos por si solos; su valor de verdad dependen del valor que tomen las variables.

Cuantificación

Denotamos los predicados por: $P(x), Q(x, y), R_1(x, y, z), \ldots$

La fórmulas de la lógica de predicados se forman desde los predicados, usando los conectivos lógicos $\vee, \wedge, \neg$ y los cuantificadores $\forall$ y $\exists$.

Los cuantificadores son otra forma de crear una proposición a partir de una fórmula con variables. Por ejemplo,

- $\forall x P(x)$ dice que todo elemento del dominio tiene la propiedad P (esto puede ser verdadero o falso);
- $\exists x P(x)$ dice que existe un elemento del dominio que tiene la propiedad P (esto puede ser verdadero o falso).

Pregunta: ¿Existen otros cuantificadores posibles?

El dominio de discurso y las variables ligadas

El valor de verdad de una oración ahora depende del dominio de discurso.

Ejemplo: La oración $\forall x \forall y(x < y \rightarrow \exists z(x < z \wedge z < y))$ es cierta en los número reales pero no en los números enteros.

Si un cuantificador es usado sobre una variable x, entonces decimos que la variable x aparece cuantificada o ligada en la fórmula.

Para que una fórmula tenga un valor de verdad entonces todas sus variables deben estar ligadas.

- Ejemplo: El valor de verdad de $\exists x(x + y = 1)$ depende del valor que tome y.

Equivalencias lógicas

Sean ϕ y ψ dos fórmulas sin variables libres (las llamamos oraciones).

Decimos que ϕ y ψ son equivalentes, si el valor de ambas fórmulas es el mismo, no importa cuál sea el dominio de discurso y cómo interpretemos los predicados en se dominio.

Ejercicio: Demuestre que las oraciones $\forall x(P(x) \wedge Q(x))$ y $\forall x P(x) \wedge \forall x Q(x)$ son equivalentes.

Haga lo mismo para $\exists x(P(x) \vee Q(x))$ y $\exists x P(x) \vee \exists x Q(x)$.

Ejercicio: ¿A qué oración es equivalente la negación de $\forall x P(x)$?

Ejemplo de Lewis Carroll

Podemos representar en el lenguaje lógico algunos elementos importantes del lenguaje natural.

Ejemplo: Considere las siguientes afirmaciones:

- Todos los leones son fieros;
- Algunos leones no toman café;
- Algunas criaturas fieras no toman café.

Podemos representarlas por:

$$\forall x(P(x) \rightarrow Q(x)); \quad \exists x(P(x) \wedge \neg R(x)); \quad \exists x(Q(x) \wedge \neg R(x)).$$

Ejemplo de Lewis Carroll

Podemos representar en el lenguaje lógico algunos elementos importantes del lenguaje natural.

Ejemplo: Considere las siguientes afirmaciones:

- Todos los leones son fieros;
- Algunos leones no toman café;
- Algunas criaturas fieras no toman café.

Podemos representarlas por:

$$\forall x(P(x) \rightarrow Q(x)); \quad \exists x(P(x) \wedge \neg R(x)); \quad \exists x(Q(x) \wedge \neg R(x)).$$

Pregunta: ¿Por qué no podemos escribir la segunda afirmación como $\exists x(P(x) \rightarrow \neg R(x))$?

Ejercicios

Ejercicio: Escriba los axiomas de los grupos conmutativos en lógica de predicados.

Ejercicio: Exprese que $\lim_{x \to a} f(x) = p$ en la lógica de predicados.

Ejercicio: Exprese que el $\lim_{x \to a} f(x)$ no existe en la lógica de predicados.

Ejercicio: ¿Cómo podría expresar que el tamaño de un grupo es par en lógica de predicados?

Reglas válidas de inferencia

Luego, estudiaremos demostraciones. Las demostraciones son argumentos válidos que establecen la verdad de una proposición matemática.

Por argumento nos referimos a las secuencias de afirmaciones que terminan en una conclusión.

Que el argumento sea válido significa que la verdad de la conclusión debe *seguirse* de la verdad de las premisas. i.e. es imposible que las premisas sean verdaderas y la conclusión falsa.

Las reglas lógicas de inferencia son patrones que nos aseguran la validez del argumento. Son los bloques con los que construimos argumentos más complejos.

Reglas de inferencia

Quizás la regla más famosa de inferencia de la lógica proposicional es el modus ponens:

$$\frac{p \quad p \rightarrow q}{q}$$

También tenemos el modus tollens:

$$\frac{\neg q \quad p \rightarrow q}{\neg p}$$

... y el razonamiento transitivo:

$$\frac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}$$

Reglas de inferencia

Tenemos reglas de inferencia, además, para la lógica de predicados. Por ejemplo, la instanciación universal:

$$\frac{\forall x P(x)}{P(c)}$$

... o la generalización universal:

$$\frac{P(c) \quad \text{para un } c \text{ arbitrario}}{\forall x P(x)}$$

... o la generalización existencial:

$$\frac{P(c) \quad \text{para algún } c}{\exists x P(x)}$$

Combinando reglas de inferencia

Nuestros argumentos serán en realidad largas secuencias con variadas combinaciones de las reglas de inferencias.

Por ejemplo, podríamos combinar modus ponens e instanciación universal en una sola regla:

$$\frac{\begin{array}{l}\forall x(P(x) \rightarrow Q(x)) \\ P(a) \quad \text{para algún } a\end{array}}{Q(a)}$$

Métodos de demostración: Introducción

Introduciremos la noción de demostración, y los métodos más utilizados para construir demostraciones.

Una demostración se construye a partir de las hipótesis del teorema a demostrar, los axiomas que sabemos que son verdad, y teoremas previamente demostrados.

A partir de estos se utilizan las reglas de inferencia lógica.

Pregunta: ¿Cuán formal debe ser una demostración?

Los metodos de demostración presentados aquí son relevantes no sólo en matemáticas, sino también en varias aplicaciones computacionales.

¿Qué es un teorema?

Un teorema es una proposición matemática que puede ser demostrada que es verdad.

- Se asume que un teorema es una proposición matemática importante, de otra forma se llama simplemente proposición.
- Resultados intermedios se llaman lemas.
- Un corolario es un teorema que puede ser probado fácilmente de otro teorema probado anteriormente.
- Una conjetura es algo que se piensa que es verdadero, pero para lo cual no existe demostración.

¿Cómo se enuncia un teorema?

Generalmente un teorema es de la forma:

> Todos los elementos de un dominio dado tienen cierta propiedad.

Sin embargo, el cuantificador universal generalmente se omite:

Ejemplo: El enunciado:

- Si x e y son números reales positivos tal que $x > y$, entonces $x^2 > y^2$,

realmente significa:

- Para todo par x, y de números reales positivos, si $x > y$ entonces $x^2 > y^2$.

Metodos de demostración

Muchos teoremas son de la forma $\forall x(P(x) \rightarrow Q(x))$.

Una idea entonces es tomar un objeto c arbitrario en el dominio, y demostrar que $P(c) \rightarrow Q(c)$. Luego, por generalización podemos asumir que el teorema es cierto.

¿Cómo demostrar que $p \rightarrow q$ es cierto?

Sólo nos basta demostrar que q es cierto cuando p es cierto (por la tabla de verdad).

Para demostrar esto es que mostraremos diferentes tipos de técnicas.

Demostraciones directas

Una demostración directa de $p \longrightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas

Una demostración directa de $p \longrightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas

Una demostración directa de $p \longrightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas

Una demostración directa de $p \rightarrow q$ se construye de la siguiente forma:

- Asuma que p es verdadero.
- Deduzca otras proposiciones a partir de p utilizando las reglas de inferencias y los axiomas.
- Deténgase una vez que haya obtenido la proposición q.

Ejemplo: Demuestre directamente que si n es un entero impar entonces n^2 también es un entero impar.

- Tome un entero impar n arbitrario;
- $n = 2k + 1$, para algún entero k (axioma);
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ (inferencia);
- $n^2 = 2(2k^2 + 2k) + 1$ (inferencia);
- n^2 es impar (axioma).

Demostraciones directas: Ejercicios

Ejercicio: Demuestre directamente que si m, n, p son enteros y $(m+n)$ y $(n+p)$ son enteros pares, entonces $m+p$ también es un entero par.

Ejercicio: Demuestre directamente que si m y n son cuadrados perfectos, entonces mn es también cuadrado perfecto.

Recuerde que a es cuadrado perfecto si existe un entero b tal que $a = b^2$.

Demostraciones por contraposición

Muchas veces es difícil encontrar una demostración directa de un resultado (lo veremos luego).

En tales casos podemos intentar demostraciones que no empiecen con p y busquen q por medio de las reglas de inferencias: Buscamos una demostración indirecta.

Las demostraciones por contraposición están basadas en que para demostrar $p \longrightarrow q$ basta demostrar $\neg q \longrightarrow \neg p$ (equivalencia lógica).

En realidad lo que hacemos es construir una demostración directa del contrapositivo de $p \longrightarrow q$.

Demostraciones por contraposición: Ejemplo

Ejercicio: Trate de demostrar directamente que si n es un entero y $3n + 2$ es impar, entonces n es impar.

Ejercicio: Demuéstrelo ahora por contraposición.

Ejercicio: Demuestre por contradicción que si $n = ab$, donde ambos a y b son enteros positivos, entonces $a \leq \sqrt{n}$ o $b \leq \sqrt{n}$.

Pregunta: ¿Cuál parecería entonces ser una estrategia razonable para demostrar una proposición de la forma $p \rightarrow q$?

Demostraciones por contradicción

Asuma que queremos demostrar p. Entonces, si encontráramos una contradicción q tal que $\neg p \rightarrow q$ es cierto, podríamos concluir que p es cierto (¿por qué?).

Esto es lo que llamamos demostración por contradicción.

Ejercicio: Demuestre por contradicción que $\sqrt{2}$ es irracional.

Recuerde que un número x es racional si y sólo si existen dos enteros m y n tal que $n \neq 0$ and $x = m/n$.

$\sqrt{2}$ es irracional

Asuma por contradicción que $\sqrt{2}$ es irracional.

Luego, $\sqrt{2} = a/b$, donde a y b son enteros sin factores en común y $b \neq 0$.

Por tanto, $2 = a^2/b^2$ y $2b^2 = a^2$.

Se sigue, que a^2 es par. Pero entonces, a también es par (demostración por contradicción).

Luego, $a = 2c$, para algún entero c, y $b^2 = 2c^2$.

Por tanto, b^2 es par y, por lo mencionado anteriormente, b también lo es.

Luego, 2 es factor común de a y b. Contradicción.

Contraposición vs contradicción

Una proposición de la forma $p \longrightarrow q$ también puede ser probada por contradicción.

Basta asumir que $p \wedge \neg q$ nos lleva a una contradicción.

Además, toda demostración por contraposición puede convertirse en una demostración por contradicción (¿cómo?).

Bicondicionales

¿Cómo podemos demostrar un teorema de la forma $p \leftrightarrow q$?

Bicondicionales

¿Cómo podemos demostrar un teorema de la forma $p \leftrightarrow q$?

Basta demostrar que $p \rightarrow q$ y que $q \rightarrow p$ (tablas de verdad).

No necesariamente las dos direcciones se demuestran siguiendo el mismo método.

Ejemplo: Sea n un entero positivo. Demuestre que n es impar si y sólo si n^2 es impar.

Pregunta: ¿Cómo podemos demostrar un teorema de la forma $p_1 \leftrightarrow p_2 \leftrightarrow \cdots \leftrightarrow p_n$?

Errores en las demostraciones

Pregunta: ¿Dónde está el error en el siguiente razonamiento?

Sean a y b dos enteros cualesquiera,y asuma que $a = b$. Luego,

1. $a^2 = ab$;
2. $a^2 - b^2 = ab - b^2$;
3. $(a + b)(a - b) = b(a - b)$;
4. $a + b = b$;
5. $2b = b$;
6. $2 = 1$.

Demostraciones por casos

Asumamos que queremos demostrar $p \rightarrow q$, y que sabemos que $p \leftrightarrow (p_1 \vee p_2 \vee \cdots \vee p_n)$.

Algunas veces es más facil demostrar $(p_1 \vee p_2 \vee \cdots \vee p_n) \rightarrow q$. A esto lo llamamos demostración por casos.

Nota: Basta demostrar que $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \cdots \wedge (p_n \rightarrow q)$.

Ejercicio: Demuestre por casos que si n es un entero, entonces $n^2 \geq n$.

Ejercicio:Demuestre por casos que $|xy| = |x||y|$, donde x e y son números enteros.

Demostraciones por casos

A veces utilizamos la frase 'Sin pérdida de generalidad...' en una demostración para referirnos al hecho de que demostrar sólo algunos de los casos es suficiente para demostrar todos los otros.

Ejercicio: Demuestre que para todo par x, y de números reales positivos, y para todo número real $0 < r < 1$, se tiene que $(x + y)^r < x^r + y^r$.

Demostraciones por casos

A veces utilizamos la frase 'Sin pérdida de generalidad...' en una demostración para referirnos al hecho de que demostrar sólo algunos de los casos es suficiente para demostrar todos los otros.

Ejercicio: Demuestre que para todo par x, y de números reales positivos, y para todo número real $0 < r < 1$, se tiene que $(x + y)^r < x^r + y^r$.

Asumimos sin pérdida de generalidad que $x + y = 1$.

Sino, asumamos que hemos demostrado el teorema para este caso y que $x + y = t \neq 1$.

Entonces $x/t + y/t = 1$, y por tanto, $(x/t + y/t)^r < (x/t)^r + (y/t)^r$.

Multiplicando a ambos lados por t^r, obtenemos $(x + y)^r < x^r + y^r$.

Demostración por casos

Ahora continuamos la demostración para el caso $x + y = 1$.

Por tanto, $0 < x, y < 1$. Además, dado que $0 < r < 1$, tenemos que $0 < 1 - r < 1$.

Por tanto, $x^{1-r} < 1$ y $y^{1-r} < 1$. Esto implica que $x < x^r$ y $y < y^r$.

Luego, $1 = x + y < x^r + y^r$ y, por tanto, $1 = (x + y)^r < x^r + y^r$. Esto demuestra el teorema.

Demostraciones de existencia

Muchos teoremas enuncian que existe un objeto con cierta propiedad, i.e. son de la forma $\exists x P(x)$.

Las demostraciones de este tipo de teoremas se llaman de existencia.

Existen demostraciones constructivas de existencia. Lo que hacen es encontrar un elemento a tal que $P(a)$.

Ejercicio: Demuestre que existe un entero positivo que puede ser expresado como la suma de cubos de enteros positivos en dos formas diferentes.

Demostraciones de existencia

Muchos teoremas enuncian que existe un objeto con cierta propiedad, i.e. son de la forma $\exists x P(x)$.

Las demostraciones de este tipo de teoremas se llaman de existencia.

Existen demostraciones constructivas de existencia. Lo que hacen es encontrar un elemento a tal que $P(a)$.

Ejercicio: Demuestre que existe un entero positivo que puede ser expresado como la suma de cubos de enteros positivos en dos formas diferentes.

- $1729 = 10^3 + 9^3 = 12^3 + 1^3$

Demostraciones de existencia

Existen también demostraciones no-constructivas de existencia.

Por ejemplo, asuma que no existe elemento a tal que $P(a)$ y obtenga una contradicción.

Ejercicio: Demuestre que existen números irracionales x e y tal que x^y es racional.

Demostraciones de unicidad

Muchos teoremas enuncian que existe un único objeto con cierta propiedad, i.e. son de la forma $\exists x(P(x) \wedge \forall y(P(y) \rightarrow x = y))$.

Tales resultados se prueban en dos partes:

- Existencia: hay un elemento a tal que $P(a)$.
- Univocidad: si $b \neq a$, entonces $\neg P(b)$.

Ejercicio: Demuestre que si a y b son números reales y $a \neq 0$, entonces existe un único número real r tal que $ar + b = 0$.

Estrategias de demostración

Por supuesto, encontrar una demostración a un teorema no es algo que pueda ser formalizado.

Siempre hay algo por atrás que corresponde a la intuición matemática.

Ejemplo: Dados dos reales positivos x e y, demuestre que $(x+y)/2 > \sqrt{xy}$, i.e. la media aritmética es siempre mayor que la media geométrica.

Conjeturas

La historia de la matemática funciona de forma muy distinta a como aparece en los libros.

Primero se exploran conceptos y ejemplos, se formulan conjeturas, se prueban o refutan esas conjeturas, y luego éstas se reformulan.

A veces una conjetura parece verdadera y se busca una demostración. Si esto no funciona se busca un contraejemplo.

La búsqueda de tal contraejemplo, aunque infructuosa, puede proveer de un mejor entendimiento de la dificultad del problema. Esto puede ayudar en una segunda búsqueda de una demostración.

Conjeturas famosas

Las conjeturas han sido muy importantes en la historia de la matemática. Ellas han ayudado a gente que ha tratado de resolverlas a hacer avances inmensos en las matemáticas.

Quizás la conjetura más famosa de la historia de la matemática es la que corresponde al último teorema de Fermat (probado hace muy poco por A. Wiles).

Fermat's last theorem: La ecuación $x^n + y^n = z^n$ no tiene solución en los enteros positivos, para cualquier $n > 2$.

Conjeturas famosas

Otra conjetura famosa es la llamada $3x + 1$.

Sea f una función definida por:

$$f(x) = \begin{cases} x/2 & \text{si } x \text{ es par;} \\ 3x + 1 & \text{si } x \text{ es impar.} \end{cases}$$

Conjetura: Para cualquier entero positivo x, aplicando repetidamente f sobre x nos llevará a 1.

Ejercicio: Pruebe la conjetura para varios enteros positivos.