Matemática Discreta

Clase 9: Derivaciones estructuradas

Federico Olmedo y Alejandro Hevia
Departamento de Ciencias de la Computación
Universidad de Chile

¿Qué son las derivaciones estructuradas?

Es un formato o estructura para presentar argumentos matemáticos (cálculos, derivaciones, pruebas, etc.)

- Es una extensión (por parte de Ralph-Johan Back) del *estilo de pruebas calculacional* originalmente propuesto por Edsger Dijkstra para razonar sobre la corrección de programas.
- Organiza los argumentos de una manera bien clara y precisa, facilitando su entendimiento (y posible detección de errores).
- Adopta una vista jerárquica, donde el argumento principal puede dividirse en múltiples subargumentos (posiblemente anidados hasta cualquier profundidad).
- Puede utilizarse sobre cualquier área de la matemática.

Motivación

Muchos argumentos matemáticos consiste en demostrar que dos expresiones e_0 y e_n están relacionados por alguna relación $\sim$, es decir,

$$e_0 \sim e_n$$

Para ello se procede incrementalmente, transformando sucesivamente e_1 hasta llegar a e_n:

$$e_0 \sim_1 e_1 \sim_2 \cdots \sim_n e_n$$

Ejemplo:

- Para probar que $e_0 = e_2$ podemos probar que $e_0 = e_1$ y $e_1 = e_2$.
- Para probar que $e_0 \leq e_2$ podemos probar que $e_0 = e_1$ y $e_1 \leq e_2$.
- Para probar que $e_0 \Rightarrow e_2$ podemos probar que $e_0 \Rightarrow e_1$ y $e_1 \Leftrightarrow e_2$.

Motivación

Una derivación estructurada es un argumento de la forma

$$e_0 \sim_1 e_1 \sim_2 \cdots \sim_n e_n$$

para concluir que

$$e_0 \sim e_n \ ,$$

donde cada paso

$$e_i \sim_{i+1} e_{i+1}$$

se justifica explícita y detalladamente.

Estructura

$$
\begin{array}{ll}
\bullet & \text{Vamos a probar que } e_0 \sim e_n \\
 & e_0 \\
\sim_1 & \{ \text{ justificación de porqué } e_0 \sim_1 e_1 \ \} \\
 & e_1 \\
\sim_2 & \{ \text{ justificación de porqué } e_1 \sim_2 e_2 \ \} \\
 & e_2 \\
\vdots & \\
 & e_{n-1} \\
\sim_n & \{ \text{ justificación de porqué } e_{n-1} \sim_n e_n \ \} \\
 & e_n \\
\blacksquare &
\end{array}
$$

1. La primera línea (con el símbolo $\bullet$) especifica el objetivo de la derivación y la última línea (con el símbolo $\blacksquare$) su finalización.
2. Las $\sim_i$ son relaciones binarias:
   - el caso más comun es cuando $\sim = \sim_1 = \cdots = \sim_n$ es transitiva, pero

Ejemplo 1

Determinar las soluciones reales de la ecuación $(x-1)(x^2+1)=0$.

- Vamos a probar que $(x-1)(x^2+1)=0$ sii $x=1$

$$
\begin{array}{ll}
 & (x-1)(x^2+1)=0 \\
\Leftrightarrow & \{\ ab=0 \Leftrightarrow a=0 \vee b=0 \text{ con } a := x-1, b := x^2+1\ \} \\
 & x-1=0\ \vee\ x^2+1=0 \\
\Leftrightarrow & \{\ \text{foco en la subexpresión } x-1=0\text{; aritmética}\ \} \\
 & x=1\ \vee\ x^2+1=0 \\
\Leftrightarrow & \{\ \text{foco en la subexpresión } x^2+1=0\text{; aritmética}\ \} \\
 & x=1\ \vee\ x^2=-1 \\
\Leftrightarrow & \{\ \text{foco en la subexpresión } x^2=-1;\ \forall a \in \mathbb{R}.\ a^2 \geq 0 \text{ con } a := x\ \} \\
 & x=1\ \vee\ \mathit{false} \\
\Leftrightarrow & \{\ \mathit{false} \text{ neutro del } \vee\ \} \\
 & x=1
\end{array}
$$

■

Ejemplo 2

Demostrar que $(x+1)(x+2) > x(x+3)$.

- Vamos a probar que $(x+1)(x+2) > x(x+3)$

$$
\begin{array}{ll}
 & (x+1)(x+2) \\
= & \{\text{ distrib. del } \times \text{ cra la } + \} \\
 & x^2 + 2x + x + 2 \\
= & \{\text{ foco en la subexpresión } 2x + x\text{; aritmética } \} \\
 & x^2 + 3x + 2 \\
> & \{\, a > 0 \Rightarrow b + a > b \text{ con } b := x^2 + 3x, a := 2 \,\} \\
 & x^2 + 3x \\
= & \{\text{ saco factor común } x \} \\
 & x(x+3)
\end{array}
$$

■

Nivel de detalle

La granularidad y el nivel de detalle de las derivaciones pueden variar:

- Vamos a probar que $(x+1)(x+2) > x(x+3)$

$$
\begin{array}{ll}
 & (x+1)(x+2) \\
= & \{\text{distrib. a izq. del } \times \text{ cra la } +\text{: } a(b+c) = ab+ac \\
 & \text{ con } a := x+1, b := x, c := 2\} \\
 & (x+1)x + (x+1)\cdot 2 \\
= & \{\text{foco en la subexpresión } (x+1)x\text{; distrib. a der. del } \times \text{ cra la } +\text{:} \\
 & (a+b)c = ac+bc \text{ con } a := x, b := 1, c := x\} \\
 & x^2 + x + (x+1)\cdot 2 \\
= & \{\text{foco en la subexpresión } (x+1)\cdot 2\text{; distrib. a der. del } \times \text{ cra la } +\text{:} \\
 & (a+b)c = ac+bc \text{ con } a := x, b := 1, c := 2\} \\
 & x^2 + x + 2x + 2 \\
\vdots & \\
\blacksquare &
\end{array}
$$

Nivel de detalle

El nivel de detalle depende de la audiencia destino, aunque en cualquier caso las justificaciones deben ser lo suficientemente detalladas para que el lector las pueda verificar sin tener que hacer cálculos él mismo o recurrir al uso papel y lápiz.

Justificaciones

En su forma más precisa y detallada (y la que se aconseja seguir), la justificación de cada paso tiene la forma

$$\{\ \textit{nombre: formulación formal}, \quad \text{con } \textit{instanciaciones}, \quad \text{donde } \textit{condiciones}\ \}$$

- *nombre* representa el nombre coloquial del argumento que justifica el paso
- *formulación formal* representa su formulación matemática, de manera simbólica
- *instanciaciones* representa cómo se instancia (sustitución de variables por expresiones concretas) para justificar el paso
- *condiciones* representa las restricciones que se cumplen y son necesarias para que la justificación sea válida

Incorporando premisas

Muchas veces el resultado

$$e_0 \sim e_n$$

que queremos probar vale sólo ante la presencia de ciertas premisas o hipotesis.

Ejemplo: Probar que si $a, b, c \geq 0$, entonces

$$(1 + a)(1 + b)(1 + c) \geq 1 + a + b + c$$

Las derivaciones estructuradas permiten también representar argumentos matemáticos que incorporan premisas.

Estructura de las derivaciones con premisas

$$
\begin{array}{ll}
\bullet & \text{Vamos a probar que } e_0 \sim e_n \text{ cuando} \\
- & \text{premisa}_1 \\
\vdots & \\
- & \text{premisa}_m \\
\models & e_0 \\
\sim_1 & \{\, \text{justificación de porqué } e_0 \sim_1 e_1 \,\} \\
 & e_1 \\
\vdots & \\
 & e_{n-1} \\
\sim_n & \{\, \text{justificación de porqué } e_{n-1} \sim_n e_n \,\} \\
 & e_n \\
\blacksquare &
\end{array}
$$

Cuando hay múltiples premisas, se las suele enumerar para poder referirlas de manera precisa.

Ejemplo 3

Probar que $m^2 - n^2 \geq 3$ cuando m, n son enteros positivos con $m > n$.

Para probar el resultado vamos a usar monotonía del producto:

$$b \geq b' \wedge a \geq 0 \implies ab \geq ab'$$

$$\begin{array}{ll}
\bullet & \text{Probamos que } m^2 - n^2 \geq 3 \text{ cuando} \\
- & \mathrm{H}_1 : \quad m, n \in \mathbb{Z}_{>0} \\
- & \mathrm{H}_2 : \quad m > n \\
\models & m^2 - n^2 \\
= & \{\, \text{diferencia de cuadrados} \,\} \\
 & (m-n)(m+n) \\
\geq & \{\, \text{monot. del producto con } a := m-n, b := m+n, b' := 3 \\
 & \text{donde } m+n \geq 3 \text{ y } m-n \geq 0 \text{ por } \mathrm{H}_1 \text{ y } \mathrm{H}_2 \,\} \\
 & (m-n) \cdot 3
\end{array}$$

Ejemplo 3

Para probar el resultado vamos a usar monotonía del producto:

$$b \geq b' \wedge a \geq 0 \implies ab \geq ab'$$

$$
\begin{array}{ll}
 & (m - n) \cdot 3 \\
= & \{ \text{ conmutatividad del prod. } \} \\
 & 3 \cdot (m - n) \\
\geq & \{ \text{ monot. del producto con } a := 3, b := m - n, b' := 1 \\
 & \text{donde } m - n \geq 1 \text{ por } H_1 \text{ y } H_2 \text{, y } 3 \geq 0 \} \\
 & 3 \cdot 1 \\
= & \{ \text{ 1 neutro del prod. } \} \\
 & 3
\end{array}
$$

■

Ejemplo 3

Retomemos el segundo paso de la derivación:

$$
\begin{array}{lll}
\bullet & \text{Probamos que } m^2 - n^2 \geq 3 \text{ cuando} & \\
- & \mathrm{H}_1: & m, n \in \mathbb{Z}_{>0} \\
- & \mathrm{H}_2: & m > n \\
\vdots & & \\
 & (m-n)(m+n) & \\
\geq & \{\text{ monot. del producto con } a := m-n, b := m+n, b' := 3 & \\
 & \text{donde } m+n \geq 3 \text{ y } m-n \geq 0 \text{ por } \mathrm{H}_1 \text{ y } \mathrm{H}_2\} & \\
 & (m-n) \cdot 3 &
\end{array}
$$

Al aplicar la monotonía del producto no es tan trivial que $m + n \geq 3$ y $m - n \geq 0$ siguen de H_1 y H_2.

Para justificar su validez de mejor manera, podemos apelar a derivaciones estructuradas.

Ejemplo 3

- Probamos que $m - n \geq 0$

$$
\begin{array}{ll}
 & true \\
\Leftrightarrow & \{\text{ premisa H}_2\ \} \\
 & m > n \\
\Leftrightarrow & \{\text{ aritmética }\} \\
 & m - n > 0 \\
\Rightarrow & \{\ a \Rightarrow a \vee b \text{ con } a := m - n > 0, b := m - n = 0\ \} \\
 & m - n > 0 \ \vee\ m - n = 0 \\
\Leftrightarrow & \{\text{ def. } \geq \} \\
 & m - n \geq 0
\end{array}
$$

■

- Observe cómo introdujimos la premisa H_2 en la derivación
- La corrección de la derivación se basa en que $p \equiv true \Rightarrow p$

Ejemplo 3

- Probamos que $m + n \geq 3$

$$
\begin{array}{ll}
 & \mathit{true} \\
\Leftrightarrow & \{ \text{premisas } \mathrm{H}_1 \text{ y } \mathrm{H}_2 \} \\
 & m > n \ \wedge \ m, n \in \mathbb{Z}_{>0} \\
\Rightarrow & \{ \text{foco en subexpresión } m > n;\ m, n \in \mathbb{Z} \} \\
 & m \geq n + 1 \ \wedge \ m, n \in \mathbb{Z}_{>0} \\
\Rightarrow & \{ \text{foco en subexpresión } m, n \in \mathbb{Z}_{>0} \} \\
 & m \geq n + 1 \ \wedge \ n \geq 1 \\
\Rightarrow & \{ \text{foco en subexpresión } m \geq n + 1;\ n \geq 1 \} \\
 & m \geq n + 1 \geq 2 \ \wedge \ n \geq 1 \\
\Rightarrow & \{ \text{sumando m.a.m. } m \geq 2 \text{ y } n \geq 1 \} \\
 & m + n \geq 3
\end{array}
$$

■

Derivaciones anidadas

En vez de escribir derivaciones separadas, podemos anidarlas en la derivación original (indentándolas a la derecha):

$$\vdots$$

$(m - n)(m + n)$

$\geq$ $\{$ monot. del producto con $a := m - n, b := m + n, b' := 3$ donde $m + n \geq 3$ y $m - n \geq 0$ por H_1 y $H_2\}$

- Probamos que $m + n \geq 3$

  $\vdots$

  ■

- Probamos que $m - n \geq 0$

  $\vdots$

  ■

$(m - n) \cdot 3$

$$\vdots$$

Incorporando métodos de prueba

Cuando utiliza algún método de prueba (inducción, análisis de casos, contrarecíproco, etc.) para establecer la relación $e_0 \sim e_n$, debe explicitarlo en forma de justificación la derecha del símbolo $\models$.

Ejemplo 4

Probar que $|x+1| > 1$ cuando x está fuera del intervalo $[-2, 0]$.

$\bullet$ Probamos que $|x+1| > 1$ cuando
$-$ $x < -2 \lor x > 0$

$\models$ $\{$ procedemos por análisis de casos sobre $x > 0 \lor x < -2$ $\}$

- $\bullet$ Probamos que $|x+1| > 1$ cuando
- $-$ $x < -2$

  $\vdots$

  $\blacksquare$

- $\bullet$ Probamos que $|x+1| > 1$ cuando
- $-$ $x > 0$

  $\vdots$

  $\blacksquare$