Clase demos

Brandwein Eric, Ferreyra Tania

Agosto 2024

1. Qué es una demo? Es solo para convencer a otros matematicos?
   - Existen los demostradores automáticos
   - Mostrar una demo en un paper para ver que estan escritas en lenguaje natural
   - (Cifu, aviso que lo agrego por si es burrada) Enfatizar que si bien las demos deberían garantizar deducción perfecta, al hacerse en lenguaje natural y chequearse a ojo (porque nadie usa los provers) hay chances de error. Para el TM quedó un ejemplo lindo que es el problema de matrix chaining `https://en.wikipedia.org/wiki/Matrix_chain_multiplication`: En la clase pasada conté que el problema se puede resolver en $O(n \log n)$ pero el paper original tiene un error en un paso algebraico hiper boludo (o sea, sería ejemplo de teorema correcto, prueba incorrecta). Aparte, para este problema se propuso un nuevo algoritmo hace poco que está directamente mal (teorema incorrecto, ergo demo incorrecta, menos mal). Link al paper original `https://epubs.siam.org/doi/10.1137/0211028`, link a las correcciones, y donde dicen que el algoritmo más rápido que se sacó después tiene tanto la demo mal como la prueba mal `https://www.cs.huji.ac.il/~odedsc/papers/SICOMP19-Revisiting.pdf`.
   - Si algo cumple una propiedad, existe una definición de esa propiedad. Por ejemplo, si queremos demostrar que algo es mínimo, hay que demostrar que es más chico que cualquier otro de los elementos. Si querés demostrar que dos conjuntos son iguales, demostrás la doble contención. Etc.
2. Definiciones (Teorema, Lemma, Def, etc)
3. Tipos de demos (buscar ejemplos de conjuntos o secuencias en lo posible)
   - Directa
   - Por casos
   - Por contradicción
   - Por construcción (se usan para cuando tenés que probar que algo existe)

- Por contraejemplo (medio lo mismo que por construcción)
- Reducción al absurdo (acá el ejemplo canónico siento que es el de ver que raiz de 2 es irracional).
- Inducción (Probar la fórmula de la geométrica? O que $2^n \leq n + 1!$, lo cual sirve saber para comparar complejidades.)
- etc.

4. Demostraciones mal hechas de cosas falsas

   (Ejemplo de la gúia vieja de demostraciones) Dado un conjunto de caballos, todos son del mismo color (en particular, implica que todos los caballos son del mismo color): Suponemos que vale para $n = 2$, y entonces para el caso inductivo tomás $n \geq 3$ y decís ”para los primeros $n - 1$ caballos vale la hipótesis y son del mismo color, luego para el conjunto formado por el caballo $n - 1$ y n también vale la hipótesis y entonces todos son del mismo color”. Observar que una vez que encuentren el error en la demo, eso no implica que el teorema sea falso (y ahi ponemos una foto con dos caballos de color distinto xD).

5. Demostraciones mal hechas de cosas verdaderas (ver si tenemos tiempo para que la corrijan ellos y la escriban bien, o si es muy pavo el error)

   - razonamiento circular
   - pasas algo por obvio que no es obvio. Enfatizar que se zarpen de verborrágicos

6. Demostración de backtracking o de podas o de algo (ver distintos niveles de formalismo)

   Acá algo que se puede mostrar es que la complejidad de fibonacci sin dinámica es exactametne $\Theta(\phi^n)$ con $\phi = \frac{\sqrt{5}+1}{2}$. La demo sale directo probando que el árbol de recursión cuando llamás con n a la función tiene $2F_n - 1$ nodos donde F_n es el n-ésimo número de fibonacci (que es $\Theta(\phi^n)$ por la fórmula cerrada esa).

   En la misma línea se puede pensar el siguiente problema: dado n y k, imprimir todas las secuencias de 0s y 1s de longitud n con k 1s. Creo recordar que el backtracking bien hecho (o sea, que cuenta cuántos 1s pusiste y eso) tiene exactamente $\binom{n}{k}$ nodos. Es decir, al poner las podas bien pasas de 2^n a eso, que es polinomial si $k = O(1)$.

7. Tips

8. Dos Ejercicios en clase, arman grupitos de dos y cada uno resuelve uno y se lo pasa al compañero.

9. Puesta en común de los ejercicios

10. Decir el ejercicio a entregar

1 ¿Qué es una demostración

[Esto es un borrador, dejo lo que tenía de antes por si sirve de punto de partida, pero a priori me parece demasiado formal, creo que no era la idea, no sé qué piensan. Tania]

Una demostración es una justificación de la validez de un enunciado, que debe realizarse mediante una secuencia de enunciados lógicamente conectados. En una demostración se infiere la veracidad de una proposición (tesis) a partir de la veracidad de una proposición dada (hipótesis), siguiendo una sucesión de pasos donde podemos incluir axiomas, teoremas, proposiciones ya demostradas o definiciones ya establecidas.

En el contexto de lógica proposicional, una afirmación solo puede ser verdadera o falsa, de modo que se nos presentan dos alternativas: demostrar la veracidad de la misma o mostrar un ejemplo en donde no sea válida, comúnmente llamado contraejemplo. Discutiremos estas dos posibilidades mencionando múltiples enfoques posibles para las demostraciones.

2 Definiciones

Axioma

Definimos un axioma como todo enunciado que sirve para la construcción de una teoría y que se admite como cierto sin demostrarse. Por ejemplo, los axiomas de números reales, como las propiedades conmutativa y asociativa del producto y la suma. Para que la teoría esté bien definida se requiere que los axiomas no se contradigan y que estén definidos de forma independiente.

Conjetura

Una conjetura es una proposición que se sospecha verdadera, pero que no ha sido demostrada ni se ha encontrado un contraejemplo que permita refutarla. Por ejemplo, la conjetura de Goldbach.

Teorema

Un teorema es un enunciado que se deduce directamente de los axiomas o de axiomas y teoremas precedentes. Debe estar debidamente demostrada su veracidad para que sea un teorema. Por ejemplo, el Último Teorema de Fermat fue una conjetura durante más de tres siglos hasta su demostración en 1994, lo que lo convirtió efectivamente en un teorema.

Lema

Un lema es una proposición cuya demostración antecede a un teorema y que no resulta de especial interés en sí misma, sino que sirve para probar dicho teorema.

Corolario

Un corolario es una proposición que se deduce inmediatamente de un teorema a partir de una demostración inmediata, corta y sencilla.

3 Tipos de Demostraciones

Demostraciones Directas

Demostración Directa

Dada una proposición de la forma $P \implies Q$, se parte asumiendo que P es verdad y se procede a establecer una cadena de implicaciones hasta llegar a la conclusión de que Q debe ser verdadera, haciendo uso para ello de cualquier información disponible, así como teoremas, propiedades o resultados probados con anterioridad. En símbolos:

$$P \implies P_1 \implies P_2 \implies ... \implies P_n \implies Q$$

que nos lleva a ir de P a Q y por lo tanto demuestra la validez de la implicación.

Ejemplo 1: Demuestre que dos cuadrados perfectos consecutivos difieren en un número impar.

Solución: Esta proposición puede reacomodarse como: *Si a y b son cuadrados perfectos consecutivos, entonces $a - b$ es un número impar*, de manera que tiene la forma $P \implies Q$, donde P es: *a y b son cuadrados perfectos consecutivos*, y Q es: *$a - b$ es un número impar.*

Supongamos que a y b son cuadrados perfectos consecutivos, con $a > b$ (el caso $a < b$ es totalmente análogo). Podemos decir que a y b tienen la forma:

$$a = (n + 1)^2 \ y \ b = n^2$$

donde n es algún número entero. Analizamos qué ocurre con la resta:

$$a - b = (n + 1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1$$

Por la forma obtenida podemos asegurar que $a - b$ es un número impar.

Demostración por Casos

Para demostrar $P \implies Q$ descomponemos P en la forma $P = P_1 \vee P_2 \vee ... \vee P_n$, y probamos que $P_i \implies Q$, para $i = 1, 2, ..., n$. Es importante no olvidar ninguno de los casos.

Ilustramos la estrategia con un ejemplo.

Ejemplo 2: Demostrar que si $n \in \mathbb{Z}$, entonces $n(n+1)$ es par.

Solución: Como $n \in \mathbb{Z}$, podemos dividir los casos posibles en dos: n es par o n es impar:

i) Si n es par, $n = 2k$, $k \in \mathbb{Z}$, y entonces $n(n+1) = 2k(2k+1)$ que es un número par, ya que $k(2k+1)$ es un número entero.

ii) Si n es impar, $n = 2k+1$, $k \in \mathbb{Z}$, y entonces $n(n+1) = (2k+1)(2k+2) = (2k+1)(k+1)2$ que es un número par, ya que $(2k+1)(k+1)$ es un número entero.

Como se analizaron todos los casos posibles, se demuestra que $n(n+1)$ es par para todo $n \in \mathbb{Z}$.

Demostraciones Indirectas

Demostración por Contradicción

Para una proposición de la forma $P \implies Q$ una demostración por contradicción supone que la hipótesis P es verdadera, pero que la tesis Q es falsa. De esta forma la estrategia es demostrar que esto no es posible al encontrar una contradicción a la veracidad de P, lo que nos lleva a concluir que si P es verdadera Q ha de serlo también (es decir $P \implies Q$).

Ejemplo 3: Sea n un entero positivo. Demuestre que si n^2 es par, también lo es n.

Solución: En este caso la afirmación a probar es de la forma $P \implies Q$, donde P es: *n es un entero positivo y n^2 es par*, y Q es: *n es par.*

Supongamos que n es un entero positivo tal que n^2 es par. Ahora supongamos que n no es par. Si n no es par, entonces debe ser impar, y si es impar tiene una forma particular: $2k+1$, con $k \in \mathbb{Z}$. En símbolos:

$$n \text{ no es par} \implies n \text{ es impar} \implies n = 2k+1,\ k \in \mathbb{Z}$$

Usando esta información, vemos que:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2) + 1$$

$k \in \mathbb{Z} \implies (2k^2+2) \in \mathbb{Z}$, entonces la expresión hallada para n^2 indica que el número es impar, sin embargo, esto contradice la hipótesis de que n^2 es par. Se concluye entonces que la suposición de que n no era par debe ser falsa, y por lo tanto n debe ser par.

Demostración por Reducción al Absurdo

Esta estrategia es similar a la anterior: para una proposición de la forma $P \implies Q$ suponemos que la hipótesis P es verdadera, pero que la tesis Q es falsa. Nuevamente buscaremos demostrar que esto no es posible al encontrar una contradicción, en este caso no de la veracidad de P, sino de algún resultado previo conocido.

Ejemplo 4: Demuestre que si m y n son enteros tales que $n + n^2 + n^3 = m + m^2$, entonces n es par.

Solución: Supongamos que n es impar. Si n es impar, entonces n^2 y n^3 también lo son, pues su descomposición en factores primos debe tener los mismos números primos que la de n, y por lo tanto no poseen al 2 como factor. La suma de tres números impares es siempre un número impar, entonces $n + n^2 + n^3$ es impar y por lo tanto también lo es $m + m^2$. Sin embargo, $m + m^2 = m(m + 1)$ que, como se probó en el ejemplo 2, es par, de modo que hemos llegado a una contradicción. Se concluye entonces que n debe ser par, que es el resultado que queríamos probar.

Demostración por Contrarrecíproco

La proposición $\sim Q \implies \sim P$ es equivalente a $P \implies Q$ y se denomina contrarrecíproco de esta. Dado que ambas son equivalentes, se puede demostrar el contrarrecíproco, que en ocasiones es un camino más simple, y de esta forma queda probada la proposición original.

Retomando el ejemplo anterior:

Ejemplo 5: Sea n un entero positivo. Demuestre que si n^2 es par, también lo es n.

Solución: Para este ejemplo el contrarrecíproco resulta:

Para n un número entero positivo, si n no es par, entonces n^2 no es par

o lo que es lo mismo:

Para n un número entero positivo, si n es impar, entonces n^2 es impar

Entonces, partiendo de la nueva hipótesis:

$$n \text{ es impar} \implies n = 2k + 1, \; k \in \mathbb{Z}$$

$$n = 2k + 1 \implies n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

$k \in \mathbb{Z} \implies (2k^2+2) \in \mathbb{Z}$, entonces la expresión hallada para n^2 indica que el número es impar. Así, el contrarrecíproco es verdadero, y por lo tanto también lo es la proposición original.

Demostración por Construcción

[Tania: esto está improvisado, lo pongo como para tener un punto de partida, y el ejemplo es el primero que se me ocurrió, seguro hay mejores]

En el caso particular en que la proposición a demostrar asegure la existencia de un elemento que cumpla una determinada propiedad o condición, bastará encontrar un ejemplo que cumpla la propiedad o condición para probar la veracidad del enunciado. En este caso podemos partir de la propiedad/condición para tratar de construir un ejemplo válido.

Ejemplo 6: Demostrar que existe una función $f : \mathbb{R} \to \mathbb{R}$ par e impar a la vez.

Solución: Sea $f : \mathbb{R} \to \mathbb{R}$ una función. Para que f sea par, se debe cumplir que:

$$f(x) = f(-x) \quad \forall x \in \mathbb{R}$$

mientras que para que f sea impar, se debe cumplir que:

$$f(x) = -f(-x) \quad \forall x \in \mathbb{R}$$

Si forzamos ambas condiciones, obtenemos que $f(x) = 0$ para todo $x \in \mathbb{R}$, con lo cual la función nula es un ejemplo de función par e impar a la vez, y así el enunciado es verdadero.

Aclaración sobre la Doble Implicación

Para el caso de las proposiciones de la forma $P \iff Q$ las estrategias de demostración son las mismas, sin embargo es importante señalar que la demostración de este enunciado requiere demostrar que $P \implies Q$ y que $Q \implies P$. Olvidarse de una de estas dos proposiciones implica **no** haber demostrado el resultado deseado, por lo que se debe prestar especial atención a evitar esto.

Ejemplo 7: Demostrar la siguiente propiedad de valor absoluto:

$$|r| = a,\ a \in \mathbb{R}^+ \iff r = a \vee r = -a$$

Solución: Veamos primero que $|r| = a,\ a \in \mathbb{R}^+ \implies r = a \vee r = -a$.

Usando la definición de valor absoluto:

$$|r| = \begin{cases} r & \text{si } r \geq 0 \\ -r & \text{si } r < 0 \end{cases}$$

tendremos dos casos posibles:

i) Si $r \geq 0$, $|r| = r = a$.

ii) Si $r < 0$, $|r| = -r = a$, lo cual implica $r = -a$.

De este modo $r = a$ o $r = -a$ para todo $r \in \mathbb{R}$.

Ahora probemos que $r = a \ \vee \ r = -a, \ a \in \mathbb{R}^+ \implies |r| = a$. Nuevamente haremos uso de la definición de valor absoluto. Si $r = a$, entonces $r > 0$, ya que $a > 0$, y luego $|r| = r = a$. Si en cambio $r = -a$, entonces $r < 0$, y luego $|r| = -r = -(-a) = a$. En ambos casos se obtiene $|r| = a$, por lo que se prueba el resultado.

Habiendo probado la implicación en uno y otro sentido, queda demostrada la doble implicación.

Existen algunos teoremas que afirman que varios resultados son equivalentes, lo cual significa que cada uno de ellos cumple una doble implicación con todos los restantes. Esto en la práctica no se demuestra así, sino que se arma un anillo de implicaciones. Es decir, si $p_1, p_2, p_3, ..., p_n$ son las proposiciones equivalentes, se demuestra que $p_1 \implies p_2 \implies p_3 \implies ... \implies p_n \implies p_1$. Como se cierra el anillo con la última implicación, si se demuestra que esto es verdadero será posible, usando este resultado, llegar desde la veracidad de cualquier proposición a probar la de todas las otras y desde la veracidad de cualquier otra a la de la proposición.

Demostración por Inducción

Dada una proposición $P(n)$ que depende de una variable $n \in \mathbb{N}$, podemos demostrar que la proposición es válida para todo n si demostramos que:

1. $P(1)$ es verdadera (caso base).
2. $P(i) \implies P(i+1)$ (paso inductivo).

Ejemplo 8: Demostrar que para todo $n \in \mathbb{N}$:

$$2^n \leq (n+1)!$$

Solución: Caso base: Para $n = 1$ nos queda que $2^n = 2$ y $(n+1)! = 2! = 2$, luego $2^n \leq (n+1)!$.

Paso inductivo: Suponemos que la proposición vale hasta n y demostramos que vale para $n+1$. Podemos reacomodar $2^{n+1} = 2^n \ 2$ y

$(n+2)! = (n+2)(n+1)!$. Por hipótesis inductiva, $2^n \leq (n+1)!$, luego:

$$2^{n+1} = 2\ 2^n \leq 2\ (n+1)!$$

Como $(n+2) \geq 2$,

$$2\ (n+1)! \leq (n+2)(n+1)! = (n+2)!$$

luego $2^{n+1} \leq (n+2)!$.

La definición puede extender a demostrar que una proposición $P(n)$ vale para todo $n \in \mathbb{Z}/n \geq a$ cambiando el caso base a $P(a)$.

Contraejemplos

Si tenemos la sospecha de que una afirmación cuya veracidad queremos determinar es falsa, podemos intentar encontrar algún ejemplo que lo demuestre. Si la proposición es falsa para un caso particular, es en general falsa, de modo que esto basta para demostrar el valor de verdad.

Ejemplo 9: Evaluar la veracidad de la proposición: $a \in \mathbb{R} \implies \frac{a}{a} = 1$.

Solución: Si bien esta proposición puede parecer cierta a simple vista, podemos encontrar un valor para el cual la proposición no se cumple. Consideremos $a = 0$: $a \in \mathbb{R}$, sin embargo $\frac{a}{a}$ no está definido y por lo tanto no puede ser igual a 1. Como la proposición no se cumple para todos los valores posibles de a (no se cumple para 0), entonces es falsa.

En este el contraejemplo dado es el único posible. Veamos un ejemplo con mayores posibilidades:

Ejemplo 10: Evaluar la veracidad de la siguiente proposición:

$$\text{Sean } A, B \in M_{n\times n},\ AB = \Theta_{n\times n} \implies A = \Theta_{n\times n} \vee B = \Theta_{n\times n}.$$

Solución: La proposición en este caso representaría una extensión a matrices de una propiedad de números reales, sin embargo esta supuesta extensión no es válida. Para ello, consideremos el ejemplo:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad y \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Este ejemplo demuestra que no es necesario que una de las matrices sea la matriz nula para que el resultado dé la matriz nula, por lo que $AB = \Theta_{n\times n}$ no me permite determinar los valores de A o B.

En este caso se obtendría el mismo resultado usando el ejemplo con A y B invertidos, o cambiando el valor no nulo de las matrices por cualquier otro número distinto de cero, por lo que hay infinitas elecciones posibles del contraejemplo. Siempre es recomendable empezar buscando una opción simple.

De manera formal, los contraejemplos sirven para refutar proposiciones de la forma $\forall x \in S, P(x) \implies Q(x)$ al hallar un valor específico de S que no verifica la implicación. Cuando la proposición no sigue de forma explícita esta estructura, es importante verificar el lenguaje usado para asegurarnos que el ejemplo efectivamente implique que la proposición no se cumple. Por ejemplo, si tuviéramos la proposición *"existe una función que es par e impar a la vez"*, que también podría enunciarse como *"es posible hallar una función que es par e impar a la vez"*, no bastaría con mostrar una función que no sea par e impar de forma simultánea, ya que la proposición no dice que todas las funciones lo cumplan, sino solo que existe alguna. En este caso no podríamos usar la estrategia del contraejemplo.

Aclaraciones Finales

Si bien hasta ahora se han discutido algunas estrategias comunes, las formas de demostrar son muy variadas y dependiendo del resultado a probar pueden ser simples o sumamente complejas. Es importante cuando nos encontremos con una demostración desafiante no quedarnos con la hoja en blanco, sino intentar todo lo que se nos ocurra. En particular, el uso de dibujos y diagramas puede ser una herramienta poderosa, y en algunos casos necesaria.

Para ilustrar la utilidad del uso de gráficos, consideremos la demostración del Teorema de Pitágoras.

Ejemplo 11: Demostrar el Teorema de Pitágoras: *Para todo triángulo rectángulo la suma del cuadrado de sus catetos es igual al cuadrado de su hipotenusa.*

Solución: Para realizar esta deducción realizamos una construcción geométrica, válida para cualquier triángulo rectángulo, según se ve en la figura 1.

En este caso, denominando a y b a los catetos y c a la hipotenusa, vemos que las área totales y del cuadrado del centro resultan:

$$A_{total} = (a+b)^2 \ , \ A_{centro} = c^2$$

La diferencia de estas áreas debe dar la suma de las áreas de los triángulos, que son todos iguales:

$$A_{total} - A_{centro} = 4A_{triangulo}$$

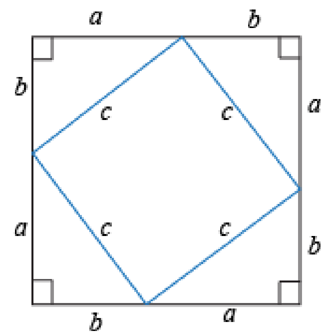

Figure 1: Construcción geométrica para demostrar el Teorema de Pitágoras.

Por otra parte, usando la fórmula del área de un triángulo $A_{triangulo} = \frac{ab}{2}$. Reemplazando:

$$A_{total} - A_{centro} = (a+b)^2 - c^2 = 4A_{triangulo} = 4\frac{ab}{2}$$

$$(a+b)^2 - c^2 = 4\ \frac{ab}{2} = 2ab$$

$$a^2 + 2ab + b^2 - c^2 = 2ab$$

$$a^2 + 2ab + b^2 - c^2 - 2ab + c^2 = 2ab - 2ab + c^2$$

$$a^2 + b^2 = c^2$$

4 Ejemplos

4.1 Posible Ejemplo: Ejercicio 3c de la guía

3) Dada una matriz simétrica M de $n \times n$ números naturales y un número k, queremos encontrar un subconjunto I de $\{1, \ldots, n\}$ con $|I| = k$ que maximice $\sum_{i,j \in I} M_{ij}$. c) Proponer una poda por optimalidad y mostrar que es correcta.

Empecemos por pensar el problema. ¿Qué sería podar por optimalidad? En este caso, sería que dada una solución parcial nos diéramos cuenta que es imposible que ésta sea mejor que la mejor solución que teníamos hasta ahora. ¿Qué sería "ser mejor" en este contexto? Sería que la sumatoria $\sum_{i,j \in I} M_{ij}$ sea mayor.

Antes de seguir, veamos que estamos hablando de dos conceptos importantes: solución parcial y extensión de una solución parcial. Definamos entonces estos conceptos para formalizar lo que estamos pensando y no cometer errores:

Definición 1: I_j es una solución parcial hasta j si $I_j \subseteq \{1, \ldots, n\}$.

Definición 2: I extiende I_j si $I_j \subseteq I$ y además si $a \in I \setminus I_j$ entonces $j < a \leq n$, o lo que es lo mismo, $I \setminus I_j \subseteq \{j+1, \ldots, n\}$.

Habiendo definido esto, volvamos al problema de encontrar una poda. Queremos encontrar una lógica que nos permita decir que una solución parcial I_j no puede extenderse a una solución mejor que la mejor hasta ahora. Teniendo en cuenta cómo definimos extensión de I_j, una opción de poda sería la idea de que si al conjunto I_j le agrego "todo lo que puedo agregar" y aún así la suma no es mayor al mejor hasta ahora, entonces no va a extenderse a una mejor solución. ¿Qué sería "todo lo que puedo agregar"? Serían números en el conjunto $\{j+1, \ldots, n\}$. Esto no toma en cuenta que una solución factible debe tener exactamente k elementos, con lo cual es posible que en realidad no se puedan agregar todos los elementos de ese conjunto, pero como ya tenemos verificaciones de factibilidad, no es necesario que la poda las tenga en cuenta.

Entonces, la poda a proponer sería: Si la mejor solución hasta ahora es un conjunto I_{mejor} tal que $\sum_{i,j \in I_{mejor}} M_{ij} = q$, y la solución parcial I_j cumple que:

$$\sum_{i,j \in I_j \cup \{j+1,\ldots,n\}} M_{ij} \leq q \tag{1}$$

entonces no existe solución I que extienda a I_j tal que $\sum_{i,j \in I} M_{ij} > q$ (es decir, I_j no puede extenderse a una solución mejor que I_{mejor}).

Expresado de esta forma, más allá de que vemos que la condición 1 nos define el criterio para la poda a usar en nuestro algoritmo, tenemos bien expresado qué es lo que debemos demostrar matemáticamente. Entonces los pasos de la demostración serían:

Sea I una solución cualquiera que extiende a I_j. El costo de esta función es:

$$\sum_{i,j \in I} M_{ij} = \sum_{i,j \in I_j} M_{ij} + \sum_{i,j \in I \setminus I_j} M_{ij}$$

Como sabemos que $I \setminus I_j \subseteq \{j+1, \ldots, n\}$ (por definición de extención de la solución parcial I_j), y además los elementos de $\{j+1, \ldots, n\}$ son todos números naturales, si agregáramos todos los elementos de $\{j+1, \ldots, n\}$ que NO estén en $I \setminus I_j$ obtendríamos una suma mayor o igual (porque estamos agregando números positivos), luego:

$$\sum_{i,j \in I \setminus I_j} M_{ij} \leq \sum_{i,j \in \{j+1,\ldots,n\}} M_{ij}$$

Reemplazando:

$$\sum_{i,j \in I} M_{ij} = \sum_{i,j \in I_j} M_{ij} + \sum_{i,j \in I \setminus I_j} M_{ij} \leq \sum_{i,j \in I_j} M_{ij} + \sum_{i,j \in \{j+1,\ldots,n\}} M_{ij} = \sum_{i,j \in I_j \cup \{j+1,\ldots,n\}} M_{ij} \leq q$$

Donde la última desigualdad sale por hipótesis. Así, hemos llegado a que cualquier extensión I de la solución I_j cumple que $\sum_{i,j \in I} M_{ij} \leq q$, y luego ninguna cumple que $\sum_{i,j \in I} M_{ij} > q$, por lo que ninguna puede ser mejor que la mejor hasta ahora, y así la poda por optimalidad es correcta.