CDD: 511.3

EL CONCEPTO DE DEMOSTRACIÓN Y ALGUNAS DE SUS PROBLEMÁTICAS

LUIS ROSA FERRARI

Instituto de Filosofía
Facultad de Humanidades y Ciencias de la Educación
Universidad de la Republica
MONTEVIDEO, URUGUAY

luisrferrari@gmail.com

Resumen: En este trabajo analizaremos algunos aspectos involucrados en el concepto de demostración matemática. Comenzaremos con la descripción de Enderton, sobre los requisitos que una demostración debe cumplir, estas son convicción final, finitud y verificabilidad algorítmica, para luego analizar las objeciones que Chateaubriand hace al respecto, y señalar algunas discrepancias con sus planteos. Estas discrepancias no pretenden apoyar la perspectiva de Enderton. En una segunda instancia, procuraremos observar algunas dificultades que surgen, cuando queremos determinar lo que es una demostración. Si bien el concepto de demostración puede ser analizado desde diversas perspectivas, teniendo en cuenta sus múltiples dimensiones, por ejemplo su dimensión retórica, ontológica, me concentrare fundamentalmente en su aspecto epistémico.

Palabras-clave: Demostración. Convicción. Finitud. Verificabilidad. Formal.

THE CONCEPT OF PROOF AND SOME OF ITS PROBLEMS

Abstract: In this paper I analyze some aspects involved in the concept of mathematical proof. I begin with Enderton's description of the requirements that a proof must fulfill, namely, a final conviction, finitude and algorithmic verifiability, and then analyze the objections that Chateaubriand raises on this topic, and indicate some discrepancies in his exposition. These discrepancies are not meant as an argument for Enderton's perspective. Although the concept of proof can be analyzed from different perspectives, i.e., taking into account its several different dimensions, for example its rhetorical, ontological dimension, I will concentrate fundamentally on its epistemic dimension.

Keywords: Proof. Conviction. Finitude. Verifiability. Formal.

1. ALGUNOS INTENTOS DE CARACTERIZACIÓN

1.1. La caracterización de Enderton

Podemos identificar una noción de demostración, que no es claramente atribuible a un pensador en particular, aunque en el texto de Enderton[1], encontramos una clara descripción de esta concepción, la llamaremos noción clásica de demostración.

1) Una demostración debe ser un argumento, que dado una persona, esta debe quedar convencida de la verdad de la aserción, a la cual el argumento se remite.

2) Toda demostración debe ser finita, ya que no se puede dar un objeto infinito a otra persona.

3) Una demostración debe ser verificable, si una persona quiere cerciorarse de la verdad de la aserción, debe poder verificarla, para corroborar que no contiene falacias, sin que esto implique una determinada cualidad de talento o inspiración departe del verificador.

1.2. La convicción en una demostración

Sobre el primer punto Chateaubriand (2005, p. 282), cuestiona que el fin de una demostración deba ser el de convencer a otra persona.

> Why can I not producer proofs for myself without the slightest intention or desire to convince anyone else? I might not even have the intention of convincing myself, since I might be already convinced. I might do it because I want to know if there is a proof of

[1] Véase Enderton (1972, p. 101).

> that assertion in certain context. I might be trying to ascertain something about the context, not de assertion. (Chateaubriand 2005, p. 282)

Por ejemplo tenemos una afirmación que sabemos que es cierta, 2+2=4, podemos querer una demostración de esto, no para convencernos de su validez, sino para sacar conclusiones del sistema axiomático en el cual queremos demostrar dicha afirmación.

Si bien cuesta pensar en hacer una demostración, y no someterla al escrutinio de otras personas, si entendemos a una demostración, como una especie particular de argumento, las características que diferencian a las demostraciones de otros argumentos, deben ser tales que puedan ser potencialmente reconocidas por otras personas distintas al sujeto demostrante, sin que esto implique necesariamente un compromiso de intencionalidad de convencimiento a terceros. Si la demostración la entendemos como los intuicionistas[2] como un proceso mental, podremos catalogar a ese proceso que tuvo lugar en nuestra mente, como una demostración, sin necesidad de que tengamos que reconocerle a dicho proceso características particulares, o en caso contrario podríamos tener una idea de demostración como proceso mental ,pero que por razones normativas ,le exigimos ciertas características, lo cual haría la función de estandarización , es decir una especie de seguridad de que todos tenemos una idea de demostración similar, aunque en ambos casos el punto 1) no solo seria innecesario sino imposible.

Si consideramos que una demostración es un objeto matemático, el cumplimiento del punto 1) parecería crucial, ya que de alguna manera, debería ser accesible a todos, y por lo tanto debería dar convicción final no solo al "constructor del objeto ", sino a todos los que accedan a el.

---

[2] Para una comprensión general de esta filosofía, puede leerse van Stigt (1990).

Cuando demostramos que 2+2=4 en un determinado sistema axiomático, ¿que demostramos? Demostramos que la suma que aprendimos en la escuela es correcta, o demostramos que los números 2 y 4 bajo ese marco teórico cumplen esa relación? Asumir que demostramos que la suma que aprendimos en la escuela es correcta, supone que nuestro marco teórico modela perfectamente esa realidad. Aun así podríamos tener una demostración de una afirmación , en un sistema axiomático ,y querer otra demostración en ese mismo marco teórico, para aclarar otros aspectos conceptuales de la teoría ,igualmente creemos que esto no muestra que el fin de la demostración , no sea establecer la verdad de su tesis, ya que por mas que la motivación de la demostración se aclarar puntos oscuros de los axiomas, este esclarecimiento depende directamente de la convicción que me provee esa demostración de la verdad de mi afirmación en ese marco teórico, de la misma manera que cuando pretendo demostrar la verdad de una afirmación, y me valgo de un lema para demostrarlo.

En el plano de los lenguajes formales tenemos una definición precisa de demostración, definida como una secuencia finita de formulas, pero sabemos que en matemáticas aceptamos como demostraciones textos que están escritos en lenguaje natural, textos que combinan símbolos matemáticos y lenguaje natural.

Llamamos demostraciones a discursos, que aunque eventualmente podríamos escribirlos, no necesitamos escribirlos para que adquieran el estatus de demostración. ¿Como distinguir estas entidades peculiares de otras que al "buen ojo" del matemático nunca serian aceptadas como demostraciones? Una primera cualidad identificatoria, como diría Enderton, es la de producir convicción final, se dice que una demostración debe dar una certeza firme de la veracidad de lo que pretende demostrar, pero cuantas veces nos hemos topado con demostraciones convincentes de afirmaciones falsas, o demostraciones que producían una fuerte convicción de una afirmación, que aunque verdadera, analizando dicha demostración observábamos que no había una conexión entre la demostración y la afirmación que pretendíamos demostrar. En principio una demostración debe ser algo que establezca la verdad de la tesis que queremos demostrar a partir de la verdad de nuestras premisas, esta debe ser una cualidad común a toda cosa que uno pueda considerar demostración, por mas hospitalaria que sea nuestra idea de demostración.

1.3. La finitud en una demostración

En su libro *Logical Forms* Chateaubriand (2005, p. 283) arguenta en contra de la finitud, o mejor dicho a favor de la infinitud.

> Is it true that I can not give an infinite object to someone else? Can I give it myself?
>
> What does it mean to give a proof? Do we literally have to produce it step by step? Are there not proofs in first order logic that would take more matter than there is in the entire universe to produce in this way? How do we give such a proof to someone else?
>
> The answer is simple: we describe it. We say that if you do this and that and that and continue in this way for an enormously large number of steps, then eventually such and such. (And this is a fairly literal description; there are more general ones.) Our description, of course, has to be less than finite; it has to be such that the person will be able to take it in, to understand it. But then, is it not possible to describe in the same way proofs with an infinite structure? Do we not give each other infinite things all the time? Is it not a little odd that I can give someone (or myself) an infinite set of hypotheses, but can only use a finite number of them in a proof? Does the activity of mathematics not consist, most of the time, in the consideration and discussion, including giving, of infinite objects and structures? I can give an infinite proof in exactly the same way in which I give an infinite set of hypotheses; namely, by describing it in an understandable way. It seems to me, therefore, that the communicability of proofs per se imposes no restriction of finiteness on their structure. (Chateaubriand 2005, p. 283)

Si decimos que las demostraciones, son su comunicación lingüística, entonces deben ser más que finitas, muy finitas. Chateaubriand critica el hecho que pedirles a las demostraciones que sean finitas, supone una idealización tal, que no cabria una diferencia sustancial considerarlas infinitas, ya que pedir la finitud a secas, supone demostraciones de tamaño tan grande como se quiera, según él estas observaciones no conducen a elegir entre dos caminos, o decimos que las secuencias lingüísticas, usadas en la comunicación de las demostraciones son las demostraciones, o decimos que ellas comunican las demostraciones. En el primer caso debemos aceptar un finitismo muy estricto, en el segundo caso debemos aceptar que las secuencias lingüísticas comunican demostraciones, que pueden ser solo representadas matemáticamente por estructuras infinitas.¿ Pero cuando decimos que una demostración es finita que queremos decir?, parece claro que esta denominación viene de la idea sintactista de demostración, en la cual uno identifica demostración con una secuencias de fórmulas, de lo cual se desprende que cuando hablamos de finitud, estamos diciendo que las formulas son finitas. En un plano no formal[3] podríamos decir que la finitud en una demostración esta dada por los "pasos" de la demostración, en el caso de considerar a las demostraciones como cosas que tiene un significado, aun si no estamos en un lenguaje formal, postura a la que adherimos. En el caso no formal de demostración surge un problema ¿Qué son los pasos en una demostración? Una conjetura es decir que los pasos, son, los "eslabones deductivos", instancias en las cuales la verdad de las premisas se trasmite a otras afirmaciones, y de esas afirmaciones a otras afirmaciones hasta llegar a nuestra conclusión. Esa es una idea a la que llamaremos, idea clásica de que son los pasos en una demostración. Tomando esta caracterización, podemos hacernos ahora la siguiente pregunta ¿Qué es una demostración infinita?,

[3] Esta denominación es tomada de Seoane (2006).

evidentemente que una demostración infinita ,si ah de tener un enriquecimiento epistémico, debe ser algo que en donde antes predicábamos la finitud ahora predicamos la infinitud– un candidato natural serán lo pasos– llamémosles a esto "conservación del comportamiento de los pasos en un sentido fuerte" (CCPF), o siendo mas permisivos, en el lugar donde antes predicábamos la finitud ahora tenemos algo que conserva ciertos aspectos fundamentales de lo anterior, y a ese algo le predicamos la infinitud; Llamémosle "Conservación del comportamiento de los pasos en un sentido débil" (CCPD).

Tenemos pues la tarea de identificar, cual es el comportamiento de los pasos en una demostración, vimos anteriormente una aproximación, decíamos que eran como eslabones deductivos, en los cuales se trasmitía la verdad de las premisas a afirmaciones y eventualmente de estas a otras afirmaciones hasta llegar a la conclusión.

Esta idea que podríamos llamar comportamiento de los pasos clásico (CPC), esta íntimamente conectada a una idea de chequeabilidad de las demostraciones, cuando hablamos de pasos de una demostración, – y si distinguimos, demostración con expresión de la demostración–, hablamos de los pasos en la expresión de la demostración, ya que sea cual sea nuestra idea de demostración, cuando decimos estos son los pasos de la demostración, nos referimos a algo ya dado, algo que a sido expresado, estos pasos son indicadores de momentos muy particulares a la hora de verificar una demostración, nos dicen paso *K:* Cerciórese de la veracidad de la afirmación *K*, como es verdadera, entonces la afirmación $K+1$ es verdadera.

Esta es una concepción clásica del comportamiento de los pasos en una demostración. Chateaubriand (2005, p. 285) presenta la siguiente demostración como candidata a demostración infinita:

Sea al siguiente conjunto de hipótesis

i) $\forall x \forall y \forall z((Rxy \,\&\, Ryz) \rightarrow Rxz)$
ii) $\forall x \neg Rxx$
iii) Rc_1c_2
iv) Rc_2c_3
.
.
.
Teorema: R tiene dominio infinito.
Demostración: $c_1 \neq c_2$ porque que $\forall x \neg Rxx$, $c_2 \neq c_3$ nuevamente porque $\forall x \neg Rxx$, $c_3 \neq c_1$, porque si $c_3 = c_1$ y tenemos que $Rc_1c_2 \,\&Rc_2c_3$ entonces Rc_1c_3 absurdo por ii), $c_3 \neq c_4$ por ii), $c_4 \neq c_2$ porque si $c_4 = c_2$, y tenemos que $Rc_2c_3 \,\&Rc_3c_4$ entonces Rc_2c_4, absurdo por ii), ídem $c_1 \neq c_4$.
Y así sucesivamente ...
Entonces R tiene dominio infinito.

El argumento de la infinitud es el siguiente; Podríamos decir que R tiene dominio infinito es consecuencia lógica de las hipótesis. Si bien la comunicación de la demostración es finita, la demostración tiene estructura infinita, si le damos esta demostración a cualquier estudiante quedara convencido de la verdad de la conclusión, sin necesidad de una cuota de inspiración particular, y sin necesidad de seguir los pasos uno a uno, aunque necesitamos todas las hipótesis para convencernos de la verdad de la afirmación. La concepción clásica de demostración nos exigiría recorrer todos los pasos, pero esta concepción permite demostraciones de largo finito, es decir demostraciones de largo, tan largo como se quiera, según Chateaubriand este esfuerzo de idealización, es tal, que supone la existencia de un individuo capaz de verificar una prueba paso por paso, aunque estos sean infinitos, entonces no habría porque no permitir que una demostración tenga pasos infinitos, ya que de permitir demostraciones de cualquier largo, a permitir demostraciones de largo infinito, no existe un esfuerzo adicional de idealización significativo.

> We can give the proof to the student, and they are completely convinced by it. In a very natural sense they can even effectively check that the proof is correct (without brilliant flashes of insight), although they cannot go every step, one by one.
>
> It seems, therefore, that the question of finiteness of proofs is not as cut and dried as we would be led to believe by looking at standard discussions of proof. (Chateaubriand 2005, p. 286)

Parece claro que la exigencia de CCPF es imposible de satisfacer ya que CPC está, como señalamos anteriormente ligada a una idea de verificación, que nos demandaría un tiempo infinito chequear la demostración, entonces la alternativa es pedir CCPD.

Debemos ser capaces de conservar en un sentido sustancial CPC, pero abandonar en un sentido muy fuerte la relación entre los pasos y la verificación, ya que tenemos pasos infinitos ,pero nuestra capacidad de verificar sigue siendo extremadamente finita.¿Es esto posible?. ¿Son los pasos en una demostración tan caracterizadores de estas, que predicar su infinitud, nos obligue a considerar como demostraciones, lo que antes desechábamos como tales? Chateaubriand no deja claro, cuales son las características de lo que el llama "pasos", ni su relación con los otros componentes de una demostración.

No creemos posible que romper la relación clásica entre pasos y verificación, no suponga una degeneración de CPC tal, que cuando decimos demostraciones infinitas sea tan arbitrario, que el decir que una demostración que utilice conjuntos infinitos es infinita. Ahora bien ¿Cuáles son esos momentos en el verificar de la demostración anterior – si es que son identificables – de los cuales los pasos pretenden dar cuenta?. Es decir si en el verificar de la demostración, identificamos pasos en la demostración, que tienen una conexión fuerte con esos momentos, entonces la demostración en cuestión seria parte de nuestra "fauna" conocida, y no seria valida como "hallazgo zoológico".

¿A que nos referimos cuando decimos que usamos todas las hipótesis en la demostración anterior?, evidentemente no esta referido a recorrerlas todas, ya que esto es imposible, pero de alguna manera todas deberán ser necesarias para establecer la verdad de la afirmación, R tiene dominio infinito. Ahora esto se parece mucho a usar un conjunto infinito como hipótesis. Tanto la hipótesis i) como la hipótesis ii) son claramente utilizadas individualmente, pero las hipótesis de la iii) en adelante no parecen ser usadas individualmente sino como un todo, ya que uno de los puntos clave de la demostración es dar cuenta que para cualquier n todos las c_i, con $i \leq n$ son distintos entre si. Esto parece depender mas que de considerar a k) como hipótesis, $\forall k \geq iii$, considerar todo ese conjunto como una hipótesis, ya que lo que nos da esa seguridad esta garantizado no por considerar a k) con $k \geq iii$ como hipótesis, sino la propiedad que genera ese conjunto, esta propiedad, que es necesaria para determinar el conjunto de hipótesis de iii) en adelante, junto con las hipótesis i) y ii), son las que nos dan esa convicción final acerca de la infinitud de la relación R.

1.4. La verificabilidad algorítmica en una demostración

Otro punto analizado por Chateaubriand es el 3). Según este filosofo, existen muchas razones por las cuales no llegamos a una convicción final en una demostración. Una razón es que no entendimos algunos pasos en la demostración, no vemos porque se puede derivar tal cosa de otra. También puede ocurrir que si bien estamos convencidos de la corrección de los pasos individuales, no entendemos porque la afirmación es cierta.

> Take a beginning student who know little mathematics and prove to him by mathematical induction that $1+2+3\ldots n = \frac{n^2+n}{2}$. After a few runs he may accept it, accepting that each step is correct, but he may not be entirely convinced. The reason he is not entirely convinced is that he does not see why the result is true. He understands the formulas "$1+2+3\ldots n$" and "$\frac{n^2+n}{2}$", and can manipulate them, but the steps by mathematical induction do not relate them meaningfully to him; he cannot relate them to something that he can understand clearly. To further expand the proof into long sequence of algorithmically checkable steps by means of the rules of proof of first order logic and the axioms of first order arithmetic, will certainly make things worse. He may again accept that each step is undoubtedly correct, but he still reductant to accept the result. (Chateaubriand 2005, p. 288)

Luego presenta la siguiente demostración alternativa:

Sean los *n* primeros números representados por unidades

●
● ●
● ● ●
.
.
.
● ● ● . . . ●

¿Cuántas unidades hay? Si completamos el cuadrado tenemos n^2 unidades, entonces $\frac{n^2}{2}$ es casi la figura, porque falta la mitad de la diagonal, entonces en la figura hay $\frac{n^2}{2}+\frac{n}{2}$ unidades.

Esta prueba "Léase Chateaubriand (2005)", es enteramente convincente, aunque los pasos no son algorítmicamente verificables en el sentido usual. Sustituir esta demostración, por la demostración por inducción, mostrara algo sobre la inducción, sobre el mecanismo de demostración por inducción, pero no agregara más convencimiento.

> It may be argued that fallacious proofs can be given by means of such methods. I agree. And it may also be argued that fallacious proofs can be given using induction. (Chateaubriand 2005, p. 289)

Chateaubriand no esta convencido, de que la convicción final en una prueba, tenga que ser dada, o garantizada por la verificabilidad algorítmica. Según él, así como la verdad de las premisas se pueden derivar de varias fuentes, también la corrección de nuestras inferencias intermedias, por ejemplo, cuando reconocemos una inferencia como una instancia del modus ponens, o usamos una analogía.

2. LA DIFICULTAD DE CARACTERIZAR EL CONCEPTO DE DEMOSTRACIÓN MATEMÁTICA

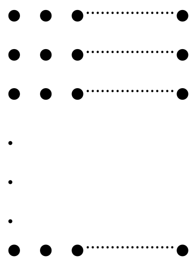
2.1. Una demostración "rival"

Analicemos ahora algunos de los argumentos de Chateaubriand acerca del punto 3).

En la prueba que presenta Chateaubriand – formulada por Polya –, surge un problema. ¿Que es la mitad de la diagonal? Si estamos trabajando con unidades, que representan el 1 y n es la cantidad de unidades de la diagonal, entonces la expresión la mitad de la diagonal, en el caso de que n sea impar carecerá de sentido, en realidad ese problema se presenta antes cuando decimos que $\frac{n^2}{2}$ es casi el número que estamos buscando. ¿Si le damos alguien esta demostración, captará este problema inmediatamente? Si no lo hace, podemos decir que la convicción llego por malas razones?, podríamos argumentar que esto no es un problema, trabajando con media unidad, pero esto no esta explicito en la demostración – lo cual no seria grave, en cuanto la demostración apela a argumentos gráficos y no tanto senténciales –, pero tampoco parece ser una consideración implícita. Entonces tenemos dos caminos, o trabajamos con objetos en la demostración que no tienen una semántica – media unidad –, o le damos una semántica compatible con los números naturales, por ejemplo considerar que estamos trabajando con los racionales. Si elegimos la primera opción, y consideramos objetos que no tiene significado en la demostración, estaríamos trabajando con $\frac{n^2}{2}$ y $\frac{n}{2}$ como dos símbolos sin significado, pero que al sumarlos, o mejor dicho, al concatenarlos con el símbolo $+$, adquieren el significado esperado, lo cual nos podría llevar a sospechar del resultado, ya que habría una especie de "salto semántico", es decir queremos corroborar una afirmación acerca de ciertos objetos , para lo cual nos valemos de ciertos símbolos, que no tiene una conexión establecida con dichos objetos, no tiene una relación de significado con ellos. La segunda opción parece ser un agregado a la demostración, ya que no esta implícito en la demostración considerar otra semántica para las unidades que no sea la de representar unidades indivisibles, por lo cual llevaría a considerar esta demostración como otra distinta, la demostración anterior más el agregado.

Consideremos ahora la siguiente demostración alternativa:

Tomemos la misma disposición de unidades que en la demostración de Polya, y completemos de la misma manera para formar un cuadrado



Si observamos las dos zonal separadas por la diagonal, vemos claramente que tienen la misma cantidad de unidades, y además si X es el número de unidades de esas zonas, tenemos que $X+n$ es el número que estamos buscando.

Pero sabemos que $X+n+X = n^2$ entonces $X = \dfrac{n^2-n}{2}$ si le sumamos n tenemos $\dfrac{n^2+n}{2}$, y este es el número que estábamos buscando.

Observemos que esta demostración no tiene los problemas de significados marcados a la demostración anterior, pero conserva muchas de sus virtudes de claridad, con un componente algebraico adicional.

2.2. La demostración por inducción

Veamos la demostración por inducción.

Queremos demostrar que $1+2+3...n = \dfrac{n^2+n}{2}$, tomemos a los naturales sin el cero, debemos demostrar que la igualdad es valida en el caso de $n = 1$. $\dfrac{1^2}{2} + \dfrac{1}{2} = 1$ se cumple.

Ahora si demostramos que si se cumple para $n = k$ entonces se cumple para $n = k + 1$, habremos demostrado por el principio de inducción en los naturales, que la afirmación se cumple para todo natural.

Por hipótesis de inducción, sabemos que $1+2+3...k = \dfrac{k^2+k}{2}$.

Entonces $1+2+3...k + 1 = \dfrac{k^2+k}{2} + k + 1$, tomando común denominador, tenemos $1+2+3...k + 1 = \dfrac{k^2+k+2(k+1)}{2} =$

$$\frac{k(k+1)+2(k+1)}{2} = \frac{(k+2)(k+1)}{2} = \frac{(k+1+1)(k+1)}{2} = \frac{(k+1)^2+(k+1)}{2}$$

con lo que hemos demostrado el teorema.

Esta demostración es convincente, ya que esta respaldada por el principio de inducción en los naturales, y por operaciones aritméticas, y estamos convencidos de la valides de ese principio, por lo cual podemos decir que cumple con el punto 1) de Enderton.

Parece no haber una diferencia significativa entre la demostración, y su expresión – si es que esta diferencia cabe – por lo que podemos decir que es finita, y que cumple con CCPF. Si escribiéramos esta demostración en un lenguaje formal, nadie diría que es otra demostración, por lo que es algorítmicamente verificable, por lo tanto cumple con el punto 2) y el punto 3) de la lista de Enderton.

2.3. La demostración de Polya "vs" La demostración por inducción

Ahora si quisiéramos encontrar una relación del mismo tipo para $1^2+2^2+3^2+..n^2$, podríamos proceder de la misma manera que en la demostración de Polya, para encontrar una disposición de unidades, y encontrar una nueva formula. Esta demostración no solo nos dice que la afirmación es verdadera, sino que nos provee de herramientas conceptuales para encontrar otras relaciones. No así la demostración por inducción, si bien me da seguridad de la verdad de la relación, no parece proporcionarme un método que me ayude a encontrar otras igualdades. En las demostraciones que usaban las disposiciones de unidades, vemos que no necesitamos saber el resultado de antemano para llegar a establecer la igualdad, de alguna manera construimos la igualdad en la demostración, podríamos no saber a que es igual $1+2+3+..n$, y ver la demostración como el descubrimiento de una relación, sin embargo cuando demuestro por inducción necesito saber la relación para probarlo en el caso base, y también para ver que si se cumple para k, entonces debe cumplirse para $k + 1$.

En la demostración por inducción vemos a los naturales como un conjunto inductivo, y usamos su principio de inducción asociado para demostrar propiedades, aunque trabajamos con los números naturales mucho antes de verlos como un conjunto inductivo. Es claro que toda esta "tecnología" puede conspirar contra la claridad, pero es necesaria cuando la representación grafica aporta más confusión que claridad.

La demostración por inducción me aporta una mayor capacidad de verificación algorítmica, pero esto no significa que una demostración por inducción pueda ser vista como una simple ejecución de un algoritmo, ya que en muchas demostraciones no somos capaces de reducir todo el argumento a un algoritmo, ya que nos valemos de procedimientos que no fueron "declarados" previamente, nos valemos de imágenes mentales o analogías, que nos son necesarias para entender ciertos pasos.

2.4. La demostración combinatoria

Veamos una demostración más de que $\sum_{j=1}^{j=n} j = \frac{n^2+n}{2}$.

Sabemos[4]:

$$\frac{n^2+n}{2}=\frac{(n+1)n}{2}=\frac{(n+1)!}{2((n-1)!)}=\frac{(n+1)!}{2(((n+1)-2)!)}=C_2^{n+1}.$$

Supongamos que tenemos $n + 1$ elementos, y las numeramos 1, 2, 3,..., $n + 1$, y queremos saber, de cuantas formas posibles podemos agruparlas de a dos, es decir cuantos subconjuntos de dos elementos, podemos formar con $n + 1$ elementos distintos, esto ya sabemos que es C_2^{n+1}. Utilizaremos los subíndices para ayudarnos a contar. Tomemos una pareja cualquiera i, j, la podemos ordenar de tal forma que $i \prec j$, ¿Cuantas parejas empiezan con 1, $1 \prec 2$, $1 \prec 3$,..., $1 \prec n + 1$ esto es n parejas empiezan con 1. ¿Cuántas empiezan con 2? $2 \prec 3$, $2 \prec 4$,..., $2 \prec n + 1$, esto es $n - 1$, y así hasta la pregunta. ¿Cuantas empiezan con n, $n \prec n + 1$, esto es 1, es claro que ninguna empieza con $n + 1$, entonces $1+2+3...+ n$ es el numero de parejas que se pueden formar con las $n + 1$ elementos, con lo que hemos demostrado el teorema[5].

La prueba es enteramente convincente, por lo que podemos afirmar que cumple con el punto 1) de Enderton.

En cuanto al punto 2), podemos ver que tiene una forma similar a la primera demostración que vimos –" R tiene dominio finito" –, posee un argumento del tipo así sucesivamente, con la diferencia, que si bien n es tan grande como queramos, siempre es finito, de manera similar podemos decir que es el reconocimiento de la relación que genera esa sucesión, lo que me provee la seguridad necesaria para convencerme de la corrección del argumento, por lo tanto la demostración es finita, cumpliendo entonces con el punto 2).

---

[4] Véase apéndice.

[5] Para un estudio mas detallado de la teoría de conteo, ver Grimaldi (1997).

2.5. Buscando similitudes

Tomemos ahora la siguiente disposición

$n, n+1$
$n-1, n \quad n-1, n+1$
.
.
.
$2{,}3 \quad 2{,}4 \quad 2{,}5 \ldots 2, n+1$
$1{,}2 \quad 1{,}3 \quad 1{,}4 \ldots 1, n \qquad 1, n+1$

Notemos que es una disposición similar a la que teníamos en la prueba de Polya. Con la ayuda de esa disposición vemos claramente que el número de parejas de un conjunto de $n + 1$ elementos es igual a $\sum_{j=1}^{j=n} j$, ahora ¿podemos decir que es otra demostración?

El esquema anterior tiene una virtud similar a el de la demostración de Polya, es como un condensador de información, nos ayuda a acceder a una especie de estructura ulterior de la demostración, pero esto no significa que la demostración sea algo que pueda caracterizarse totalmente con una estructura matemática, la forma en la cual yo accedo a esa estructura, es mas que importante.

Podemos reconocer un núcleo argumental en las dos descripciones, este es:

Véase que el número de parejas de un conjunto de $n + 1$ *elementos es* $\sum_{j=1}^{j=n} j$, no podemos decir que son la misma demostración, ya que una no es una simple traducción de la otra, pero reconocemos que utilizan una misma estructura argumental.

2.6. La necesidad de flexibilizar algunos puntos de vista

Ver las demostraciones solamente como una secuencia finita de formulas, nos proporciona un gran conocimiento de muchos de los aspectos que están en juego en una demostración, pero no nos dice todo. Cuando estudiamos una demostración, no leemos una secuencia finita de signos sin significado, también interpretamos, hacemos pausas para explicar ciertas estructuras, es un juego entre lenguaje e interpretación. Si vemos a las demostraciones como algo que debe ser estudiado solamente en el marco de los lenguajes formales, nos perdemos un aspecto importante de estas, pero si vemos a las demostraciones solamente como estructuras matemáticas, nos sucede algo parecido a lo que señalábamos en la demostración anterior, reconocemos una estructura en común, pero la forma por la cual accedemos a esa estructura parece jugar un rol importante. Tenemos por una lado la demostración por inducción, en la cual lenguaje e interpretación parecen fusionarse, hay una especie de función biyectiva entre la secuencia simbólica y su significado, no siempre esto es posible como señalamos anteriormente, y por otro lado la demostración de Polya, en la cual, es mas complicado reconocer una función de interpretación, consecuentemente la verificación algorítmica en estos casos se torna dificultosa, ya que si bien puedo recorrer algorítmicamente la secuencia lingüística de una demostración, también interpreto, me valgo de imágenes mentales para reconocer ciertas estructuras, por lo tanto, pedir verificabilidad algorítmica, es un requisito difícil de satisfacer, por muchos argumentos que consideramos demostraciones.

3 CONSIDERACIONES FINALES

Existe una forma tradicional de ver a las demostraciones como argumentos que pueden ser traducibles a un lenguaje formal, esto tiene como consecuencia pedir verificación algorítmica a las demostraciones, vimos que los tres puntos de Enderton parecen compatibles con esta visión. Chateaubriand crítica estos tres puntos, y parece estar a favor de ver a las demostraciones como una estructura matemática más, como consecuencia, las demostraciones pueden ser tan infinitas como cualquier estructura matemática, en el primer ejemplo que vimos se predicaba la infinitud en los pasos, dimos nuestra opinión discrepante al respecto.

Chateaubriand critica la verificación algorítmica, con lo que estamos de acuerdo ya que creemos que en las demostraciones nos valemos de herramientas que no son claramente traducibles a un lenguaje formal, lo que permitiría su verificación algorítmica. Vimos una ejemplo sobre como podemos ver una misma estructura argumental en dos demostraciones, pero que el acceso a esa estructura argumental merece ser parte constitutiva de la que llamamos demostración. Si bien podemos reconocer una estructura argumental, con cierta independencia de su comunicación lingüística, la forma por la cual yo accedo a esta estructura es relevante, ya sea para asimilar con mayor claridad dicha estructura, o como para verificar algorítmicamente los pasos en la expresión de la demostración, que como defendimos con anterioridad, están íntimamente conectados a ciertos momentos a la hora de verificar la demostración, claro está encontrar una expresión de la demostración que sea lo mas representativa de esa estructura argumental, podrá contribuir a que la verificación algorítmica me de un mayor poder de corroboración, aunque dicha corroboración no podrá, en muchos casos reducirse de manera sustancial a esto.

APENDICE: ALGUNOS ELEMENTOS BÁSICOS DE CONTEO

Definimos el factorial de n, si $n \neq 0$ como $n! := n \times (n-1) \times (n-2)\ldots 1$.

Si $n = 0$, $n! = 1$.

Supongamos que tenemos m elementos distintos, y queremos saber cuantas listas ordenadas podemos construir con ellos. Para el primer lugar podemos elegir m elementos, para el segundo lugar podemos elegir $m - 1$, es decir todos menos el que ya elegimos para el primer lugar, para el tercero $m - 2$, y así para el último tenemos un elemento para elegir. Esto es $m \times (m - 1)(m - 2)\ldots 1$. Definimos entonces la cantidad de permutaciones de m elementos distintos como $P_m := m!$.

Si ahora queremos saber cuantas filas podemos construir con m elementos distintos, pero de largo k, con $k \leq m$. Entonces para el primer lugar tenemos m elecciones, para el segundo lugar tenemos $m - 1$, y así hasta que para el lugar k, tenemos $m - (k - 1)$ elecciones, esto es $m \times (m - 1)(m - 2)\ldots(m - (k - 1))$.

Definimos ahora, arreglos de m elementos tomados de a k elementos como, $A_k^m := m \times (m - 1)(m - 2)\ldots(m - (k - 1))$, entonces $A_k^m = \dfrac{m!}{(m-k)!}$.

Ahora queremos saber cuantos subconjuntos de tamaño k, con $k \leq m$, podemos formar de un conjunto de m elementos. A esto lo llamaremos, combinaciones de m elementos tomados de a k, notación C_k^m. Si a cada subconjunto de tamaño k, lo multiplicamos por $k!$, tenemos la cantidad de listas de m elementos de largo k, esto es A_k^m, entonces tenemos que $k! \times C_k^m = A_k^m$, entonces $C_k^m = \dfrac{A_k^m}{k!}$, por lo que tenemos la siguiente formula $C_k^m = \dfrac{m!}{k!(m-k)!}$.

REFERENCIAS

CHATEAUBRIAND, O. *Logical Forms. Part II: Logic, Language and Knowledge*. Campinas: UNICAMP, 2005. (Coleção CLE, v. 42, pp. 282-289)

ENDERTON, H. B. *A Mathematical Introduction to Logic.* Academic Press, 1972.

GRIMALDI, R. P. *Matemáticas discreta y combinatoria.* Wilmington, Delaware: Addison-Wesley Iberoamericana, 1997. (Tercera edición)

SEOANE, J. "The Concept of Mathematical Elucidation: theory and problems". *CLE e-prints (Section Logic)*, vol. 6, n. 4, pp. 1-21, 2006.

VAN STIGT, W. P. *Brouwer's Intuitionism.* Amsterdam: Elsevier Science Publishers B.V., 1990.