A page in Number Theory

Andrea Asperti

Dipartimento di Scienze dell'Informazione
Università degli Studi di Bologna

1/12/2006

A page in Number Theory

A Classical Introduction to Modern Number Theory
Kenneth Ireland
Michael Rosen
Graduate Texts in Mathematics, Springer Verlag
pp.19-20

Content

Content

Content

Content

Content

Content

Content

Outline

Möbius function

"... We now introduce a very important arithmetic function, the Möbius μ function.
For $n \in Z^+$, $\mu(1) = 1$, $\mu(n) = 0$ if n is not square-free, and $\mu(p_1 p_2 \dots p_l) = (-1)^l$, where the p_i are distinct positive primes."

Möbius function in Matita

```
let rec moebius_aux p n : Z \def
  match p with
  [ O \Rightarrow pos O
  | (S p1) \Rightarrow
    match p_ord n (nth_prime p1) with
    [ (pair q r) \Rightarrow
      match q with
      [ O \Rightarrow moebius_aux p1 r
      | (S q1) \Rightarrow
        match q1 with
        [ O \Rightarrow Zopp (moebius_aux p1 r)
        | (S q2) \Rightarrow OZ
        ]
      ]
    ]
  ].

definition moebius : nat \to Z \def
\lambda n.
  let p \def (max n (\lambda p:nat.eqb (n \mod (nth_prime p)) O)) in
  moebius_aux (S p) n.
```

Outline

$\Sigma_{d|n}\mu(d) = 0$

Proposition. If $n > 1$, $\Sigma_{d|n}\mu(d) = 0$.

Proof. If $n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$, then

$$\Sigma_{d|n}\mu(d) = \Sigma_{(\epsilon_1,\ldots,\epsilon_l)}\mu(p_1^{\epsilon_1} \ldots p_l^{\epsilon_l})$$

where the ϵ_i are zero or one. Thus

$$\Sigma_{d|n}\mu(d) = 1 - l + \binom{l}{2} - \binom{l}{3} + \cdots + (-1)^l = (1-1)^l = 0$$

$\square$

$\Sigma_{d|n}\mu(d) = 0$

Proposition. If $n > 1$, $\Sigma_{d|n}\mu(d) = 0$.

Proof. If $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$, then

$$\Sigma_{d|n}\mu(d) = \Sigma_{(\epsilon_1,\dots,\epsilon_l)}\mu(p_1^{\epsilon_1} \dots p_l^{\epsilon_l})$$

where the ϵ_i are zero or one. Thus

$$\Sigma_{d|n}\mu(d) = 1 - l + \binom{l}{2} - \binom{l}{3} + \dots + (-1)^l = (1-1)^l = 0$$

□

$\Sigma_{d|n}\mu(d) = 0$

A different approach:
Let $n = p^a r$, where $p \nmid r$ (ord p in n is a).

$$\Sigma_{d|p^a r}\mu(d) = \Sigma_{d|r}\Sigma_{i \le a}\mu(p^i d)$$

Since $p \nmid r$ then $p \nmid d$ and hence $\mu(pd) = -\mu(d)$.
Moreover, for any $i > 1$, $\mu(p^i d) = 0$ since it is not square free.
Hence, for any d,

$$\Sigma_{i \le a}\mu(p^i d) = \mu(d) + \mu(pd) + \Sigma_{2 \le i \le a}\mu(p^i d) = 0$$

□

Nested summations

$$\Sigma_{i<n:p_1(i)}\Sigma_{j<m:p_2(j)}g(i,j) = \Sigma_{k<n\times m:p_1(k\ div\ m)\wedge p_2(k\ mod\ m)}(g(k\ div\ m, k\ mod\ m),)$$

```
theorem sigma_p2 :
\forall n,m:nat.
\forall p1,p2:nat \to bool.
\forall g: nat \to nat \to Z.
sigma_p (n*m)
  (\lambda x.andb (p1 (div x m)) (p2 (x mod m)))
  (\lambda x.g (div x m) (mod x m)) =
sigma_p n p1
  (\lambda x.sigma_p m p2 (g x)).
```

Nested summations

$$\Sigma_{i<n:p_1(i)}\Sigma_{j<m:p_2(j)}g(i,j) = \Sigma_{k<n\times m:p_1(k\ div\ m)\wedge p_2(k\ mod\ m)}(g(k\ div\ m, k\ mod\ m),)$$

```
theorem sigma_p2 :
\forall n,m:nat.
\forall p1,p2:nat \to bool.
\forall g: nat \to nat \to Z.
sigma_p (n*m)
  (\lambda x.andb (p1 (div x m)) (p2 (x mod m)))
  (\lambda x.g (div x m) (mod x m)) =
sigma_p n p1
  (\lambda x.sigma_p m p2 (g x)).
```

Bijection

From

$$\Sigma_{d|p^a r}\mu(d) = \Sigma_{d|r}\Sigma_{i\leq a}\mu(p^i d)$$

to

$$\Sigma_{d|p^a r}\mu(d) = \Sigma_{k\leq r\times a:(k\ div\ a)|r}\mu(p^{k\ mod\ a}(k\ div\ a))$$

Bijection:
If $d|p^a r$ then $d = p^i s$ where $i \leq a$ and $s|r$. Map d into $sa + i$, so that $sa + i\ div\ a = s$ and $sa + i\ mod\ a = i$.

Bijection

From

$$\Sigma_{d|p^a r}\mu(d) = \Sigma_{d|r}\Sigma_{i\leq a}\mu(p^i d)$$

to

$$\Sigma_{d|p^a r}\mu(d) = \Sigma_{k\leq r\times a:(k\ div\ a)|r}\mu(p^{k\ mod\ a}(k\ div\ a))$$

Bijection:
If $d|p^a r$ then $d = p^i s$ where $i \leq a$ and $s|r$. Map d into $sa + i$, so that $sa + i\ div\ a = s$ and $sa + i\ mod\ a = i$.

Independence under permutations

$$\Sigma_{x<n1:p1(x)}g(h(x)) = \Sigma_{x<n2:p2(x)}g(x))$$

```
theorem eq_sigma_p_gh:
\forall g: nat \to Z.
\forall h,hinv: nat \to nat.\forall n1,n2.
\forall p1,p2:nat \to bool.
(\forall i. i < n1 \to p1 i = true \to p2 (h i) = true) \to
(\forall i. i < n1 \to p1 i = true \to hinv (h i) = i) \to
(\forall i. i < n1 \to p1 i = true \to h i < n2) \to
(\forall j. j < n2 \to p2 j = true \to p1 (hinv j) = true) \to
(\forall j. j < n2 \to p2 j = true \to h (hinv j) = j) \to
(\forall j. j < n2 \to p2 j = true \to hinv j < n) \to
sigma_p n1 p1 (\lambda x.g(h x)) =
  sigma_p n2 (\lambda x.p2 x) g.
```

Independence under permutations

$$\Sigma_{x<n1:p1(x)}g(h(x)) = \Sigma_{x<n2:p2(x)}g(x))$$

```
theorem eq_sigma_p_gh:
\forall g: nat \to Z.
\forall h,hinv: nat \to nat.\forall n1,n2.
\forall p1,p2:nat \to bool.
(\forall i. i < n1 \to p1 i = true \to p2 (h i) = true) \to
(\forall i. i < n1 \to p1 i = true \to hinv (h i) = i) \to
(\forall i. i < n1 \to p1 i = true \to h i < n2) \to
(\forall j. j < n2 \to p2 j = true \to p1 (hinv j) = true) \to
(\forall j. j < n2 \to p2 j = true \to h (hinv j) = j) \to
(\forall j. j < n2 \to p2 j = true \to hinv j < n) \to
sigma_p n1 p1 (\lambda x.g(h x)) =
  sigma_p n2 (\lambda x.p2 x) g.
```

proof

$$\Sigma_{x<S(n2):p2(x)}g(x) =$$
$$= g(n2) + \Sigma_{x<n2:p2(x)}g(x)$$
$$= g(h(hinv(n2))) + \Sigma_{x<n2:p2(x)}g(x))$$
$$= g(h(hinv(n2))) + \Sigma_{x<(Sn1):p1(x)\wedge x\neq hinv(n2)}g(h(x))$$
$$= \Sigma_{x<S(n1):p1(x)}g(h(x)))$$

```
lemma sigma_p_gi: \forall g: nat \to Z.
\forall n,i.\forall p:nat \to bool.
i < n \to p i = true \to
sigma_p n p g =
  g i + sigma_p n (\lambda x. andb (p x) (notb (eqb x i))) g.
```

Outline

Dirichlet product

"The full significance of the Möbius μ function can be understood most clearly when its connection with Dirichlet multiplication is brought to light.
Let f and g be complex valued functions on Z^+. The Dirichlet product of f and g is defined by the formula $f \otimes g(n) = \Sigma f(d_1)g(d_2)$ where the sum is over all pairs (d_1, d_2) of positive integers suche that $d_1 d_2 = n$."

Dirichlet product in Matita

```
definition dirichlet_product:
  (nat \to Z) \to (nat \to Z) \to nat \to Z \def
\lambda f,g.\lambda n.
  sigma_p (S n)
   (\lambda d.divides_b d n)
   (\lambda d. (f d)*(g (div n d))).
```

Dirichlet product is associative

"This product is associative, as one can see by checking that $f \otimes (g \otimes h)(n) = (f \otimes g) \otimes h(n) = \Sigma f(d_1)g(d_2)h(d3)$ *where the sum is over all 3-tuples* (d_1, d_2, d_3) *of positive integers such that* $d_1 d_2 d_3 = n$*."*

Dirichlet product is associative

By definition $f \otimes g(n) = \Sigma_{d|n} f(d) g(n \ div \ d)$

$$
\begin{aligned}
f \otimes (g \otimes h)(n) = & \\
&= \Sigma_{d1|n} f(d1) g \otimes h(n \ div \ d1) \\
&= \Sigma_{d1|n} f(d1)(\Sigma_{d2|n \ div \ d1} g(d2) h((n \ div \ d1) \ div \ d2)) \\
&= \Sigma_{d1|n} \Sigma_{d2|n \ div \ d1} f(d1) g(d2) h((n \ div \ d1) \ div \ d2) \\
(f \otimes g) \otimes h(n) = & \\
&= \Sigma_{d1|n} f \otimes g(d1) h(n \ div \ d1) \\
&= \Sigma_{d1|n} (\Sigma_{d2|d1} f(d2) g(d1 \ div \ d2)) h(n \ div \ d1) \\
&= \Sigma_{d1|n} \Sigma_{d2|d1} f(d2) g(d1 \ div \ d2)) h(n \ div \ d1)
\end{aligned}
$$

A not so trivial bijection

$\{(d_1, d2) \leq (n, n) : d_1 | n, d_2 | (n \; div \; d1)\}$
$\{(d_1, d2) \leq (n, n) : d_1 | n, d_2 | d1\}$

$h(d_1, d_2) = (d_1 d_2, d_1)$
$hinv(d_1, d_2) = (d_2, d_1 \; div \; d_2)$

$hinv(h(d_1, d_2)) = hinv(d_1 d_2, d_1) = (d_1, d_1 d_2 \; div \; d_1) = (d_1, d_2)$
$h(hinv(d_1, d_2)) = h(d_2, d_1 \; div \; d_2) = (d_2(d_1 \; div \; d_2), d_2)) = (d_1, d_2)$

Everything complicated by the fact that that we must first reduce everything to a single summmation:

$h(i) = (i \; div \; n)(i \mod n) \times n + i \; div \; n$
$hinv(j) = j \; mod \; n * n + ((j \; divn) \; div \; (j \; mod \; n))$

A not so trivial bijection

$$\{(d_1, d2) \leq (n, n) : d_1|n, d_2|(n\ div\ d1)\}$$
$$\{(d_1, d2) \leq (n, n) : d_1|n, d_2|d1\}$$

$$h(d_1, d_2) = (d_1 d_2, d_1)$$
$$hinv(d_1, d_2) = (d_2, d_1\ div\ d_2)$$

$$hinv(h(d_1, d_2)) = hinv(d_1 d_2, d_1) = (d_1, d_1 d_2\ div\ d_1) = (d_1, d_2)$$
$$h(hinv(d_1, d_2)) = h(d_2, d_1\ div\ d_2) = (d_2(d_1\ div\ d_2), d_2)) = (d_1, d_2)$$

Everything complicated by the fact that that we must first reduce everything to a single summmation:

$$h(i) = (i\ div\ n)(i \mod n) \times n + i\ div\ n$$
$$hinv(j) = j\ mod\ n * n + ((j\ divn)\ div\ (j\ mod\ n))$$

A not so trivial bijection

$\{(d_1, d2) \leq (n, n) : d_1 | n, d_2 | (n\ div\ d1)\}$
$\{(d_1, d2) \leq (n, n) : d_1 | n, d_2 | d1\}$

$h(d_1, d_2) = (d_1 d_2, d_1)$
$hinv(d_1, d_2) = (d_2, d_1\ div\ d_2)$

$hinv(h(d_1, d_2)) = hinv(d_1 d_2, d_1) = (d_1, d_1 d_2\ div\ d_1) = (d_1, d_2)$
$h(hinv(d_1, d_2)) = h(d_2, d_1\ div\ d_2) = (d_2(d_1\ div\ d_2), d_2)) = (d_1, d_2)$

Everything complicated by the fact that that we must first reduce everything to a single summmation:

$h(i) = (i\ div\ n)(i \mod n) \times n + i\ div\ n$
$hinv(j) = j\ mod\ n * n + ((j\ divn)\ div\ (j\ mod\ n))$

Independence under permutation 2

State directly permutation invariance for nested sums.

```
theorem sigma_p2_eq:
\forall g: nat \to nat \to Z.
\forall h11,h12,h21,h22: nat \to nat \to nat.
\forall n,m.
\forall p11,p21:nat \to bool.
\forall p12,p22:nat \to nat \to bool.
(\forall i,j. i < n \to j < m \to p21 i = true \to p22 i j = true \to
  p11 (h11 i j) = true \land p12 (h11 i j) (h12 i j) = true
  \land h21 (h11 i j) (h12 i j) = i \land h22 (h11 i j) (h12 i j) = j
  \land h11 i j < n \land h12 i j < m) \to
(\forall i,j. i < n \to j < m \to p11 i = true \to p12 i j = true \to
  p21 (h21 i j) = true \land p22 (h21 i j) (h22 i j) = true
  \land h11 (h21 i j) (h22 i j) = i \land h12 (h21 i j) (h22 i j) = j
  \land (h21 i j) < n \land (h22 i j) < m) \to
sigma_p n p11 (\lambda x:nat .sigma_p m (p12 x) (\lambda y. g x y)) =
sigma_p n p21 (\lambda x:nat .sigma_p m (p22 x) (\lambda y. g (h11 x y) (h12 x y))).
```

More functions

"Define the function T by $T(1) = 1$ and $T(n) = 0$ for $n > 1$. Then $f \otimes T = T \otimes f = f$."

$$
\begin{aligned}
f \otimes T(n) &= \\
&= \Sigma_{d|n} f(d) T(n \text{ div } d) \\
&= f(n) T(n \text{ div } n) + \Sigma_{d|n, d<n} f(d) T(n \text{ div } d) \\
&= f(n) + \Sigma_{d|n, d<n} 0 \\
&= f(n)
\end{aligned}
$$

Remarks:

- intensional vs extensional equality.
- commutativity of dirichlet product not even mentioned, but again not entirely trivial (you have to pass through a permutation).

More functions

> *"Define the function T by $T(1) = 1$ and $T(n) = 0$ for $n > 1$. Then $f \otimes T = T \otimes f = f$."*

$$
\begin{aligned}
f \otimes T(n) = & \\
&= \Sigma_{d|n} f(d) T(n \; div \; d) \\
&= f(n) T(n \; div \; n) + \Sigma_{d|n, d<n} f(d) T(n \; div \; d) \\
&= f(n) + \Sigma_{d|n, d<n} 0 \\
&= f(n)
\end{aligned}
$$

Remarks:

- intensional vs extensional equality.
- commutativity of dirichlet product not even mentioned, but again not entirely trivial (you have to pass through a permutation).

More functions

"Define the function T by $T(1) = 1$ and $T(n) = 0$ for $n > 1$. Then $f \otimes T = T \otimes f = f$."

$$
\begin{aligned}
f \otimes T(n) = & \\
& = \Sigma_{d|n} f(d) T(n \; div \; d) \\
& = f(n) T(n \; div \; n) + \Sigma_{d|n, d<n} f(d) T(n \; div \; d) \\
& = f(n) + \Sigma_{d|n, d<n} 0 \\
& = f(n)
\end{aligned}
$$

Remarks:

- intensional vs extensional equality.
- commutativity of dirichlet product not even mentioned, but again not entirely trivial (you have to pass through a permutation).

More functions

"Define the function T by $T(1) = 1$ and $T(n) = 0$ for $n > 1$. Then $f \otimes T = T \otimes f = f$."

$$
\begin{aligned}
f \otimes T(n) = & \\
& = \Sigma_{d|n} f(d) T(n \textit{ div } d) \\
& = f(n) T(n \textit{ div } n) + \Sigma_{d|n, d<n} f(d) T(n \textit{ div } d) \\
& = f(n) + \Sigma_{d|n, d<n} 0 \\
& = f(n)
\end{aligned}
$$

Remarks:

- intensional vs extensional equality.
- commutativity of dirichlet product not even mentioned, but again not entirely trivial (you have to pass through a permutation).

More functions

> *"Define the function T by $T(1) = 1$ and $T(n) = 0$ for $n > 1$. Then $f \otimes T = T \otimes f = f$."*

$$
\begin{aligned}
f \otimes T(n) = & \\
&= \Sigma_{d|n} f(d) T(n \; div \; d) \\
&= f(n) T(n \; div \; n) + \Sigma_{d|n, d<n} f(d) T(n \; div \; d) \\
&= f(n) + \Sigma_{d|n, d<n} 0 \\
&= f(n)
\end{aligned}
$$

Remarks:

- intensional vs extensional equality.
- commutativity of dirichlet product not even mentioned, but again not entirely trivial (you have to pass through a permutation).

More functions: I

"Define I by $I(n) = 1$ for all n. Then $f \otimes I(n) = I \otimes f(n) = \Sigma_{d|n} f(d)$."

Prove that $f \otimes I(n) = f(n)$ (for a time, easy), then use commutativity. Proving directly $I \otimes f(n) = f(n)$ is far more complex.

More functions: I

"Lemma. $I \otimes \mu = \mu \otimes I = T$.

Proof. $\mu \otimes I(1) = \mu(1)I(1) = 1$. *If* $n > 1$, $\mu \otimes I(n) = \Sigma_{d|n}\mu(d) = 0$.

Easy.

Outline

Möbius Inversion Theorem

"Theorem (Möbius Inversion Theorem).
Let $F(n) = \Sigma_{d|n} f(d)$*. Then* $f(n) = \Sigma_{d|n}\mu(d)F(n/d)$*.*
Proof. $F = f \otimes I$*. Thus*
$F \otimes \mu = (f \otimes I) \otimes \mu = f \otimes (I \otimes \mu) = f \otimes T = f$*.*
This shows that $f(n) = F \otimes \mu(n) = \Sigma_{d|n}\mu(d)F(n/d)$*.*

Formal proof not as elegant, mostly due to extensionality problems.
For instance, we only know $F(n) = f \otimes I(n)$, so we cannot just rewrite $F \otimes \mu$ into $(f \otimes I) \otimes \mu$.
You should define a lemma of the kind

$$f \equiv f' \to g \equiv g' \to f \otimes g \equiv f' \otimes g'$$

Möbius Inversion Theorem

"Theorem (Möbius Inversion Theorem).
Let $F(n) = \Sigma_{d|n} f(d)$. *Then* $f(n) = \Sigma_{d|n} \mu(d) F(n/d)$.
Proof. $F = f \otimes I$. *Thus*
$F \otimes \mu = (f \otimes I) \otimes \mu = f \otimes (I \otimes \mu) = f \otimes T = f$.
This shows that $f(n) = F \otimes \mu(n) = \Sigma_{d|n} \mu(d) F(n/d)$.

Formal proof not as elegant, mostly due to extensionality problems.
For instance, we only know $F(n) = f \otimes I(n)$, so we cannot just rewrite $F \otimes \mu$ into $(f \otimes I) \otimes \mu$.
You should define a lemma of the kind

$$f \equiv f' \to g \equiv g' \to f \otimes g \equiv f' \otimes g'$$

Outline

Euler ϕ function

"... The Möbius inversions has many applictions. We shall use it to obtain formula for yet another arithmetic function, the Eler ϕ function. For $n \in Z^+$, $\phi(n)$ is defined to be the number of integers between 1 and n relatively prime to n. For example, $\phi(1) = 1$, $\phi(5) = 4$, $\phi(6) = 2$, and $\phi(9) = 6$. If p is a prime, it is clear that $\phi(p) = p - 1$."

Euler ϕ function in Matita

```
definition totient: nat \to nat \def
\lambda n.
  sigma_p n
    (\lambda m. eqb (gcd m n) (S O))
    (\lambda m.S O).
```

Outline

$\Sigma_{d|n}\phi(d) = n$

"Proposition. $\Sigma_{d|n}\phi(d) = n$*.*

Proof. Consider the n rational numbers $1/n, 2/n, 3/n, \ldots (n-1)/n, n/n$*. Reduce each to lowest terms; i.e. express each number as a quotient of relatively prime integers. The denominators will all be divisors of n. If* $d|n$*, exactly* $\phi(d)$ *of our numbers will have d in the denominator after reducing to lowest terms. Thus* $\Sigma_{d|n}\phi(d) = n$*.* □"

$\Sigma_{d|n}\phi(d) = n$, formally

$$\Sigma_{d|n}\phi(d) = \Sigma_{d|n}\Sigma_{i:gcd(i,d)=1}1$$

Get rid of the nested sum.
A dependency problem: the bound of the inner sum is d, that is the index of the outermost sum. Change the bound modifying the boolean condition:

$$\Sigma_{d|n}\Sigma_{i:gcd(i,d)=1}1 = \Sigma_{d|n}\Sigma_{i\leq n:gcd(i,d)=1}1$$

Formally:

```
sigma_p d
  (\lambda i. eqb (gcd i d) (S O))
  (\lambda i.S O) =
sigma_p n
  (\lambda i. (leb i d) andb (eqb (gcd i d) (S O)))
  (\lambda i.S O)
```

$\Sigma_{d|n}\phi(d) = n$, formally (2)

$$\Sigma_{d|n}\Sigma_{i<S(n):gcd(i,d)=1} 1 =$$
$$= \Sigma_{\langle d,i\rangle<S(n)\times S(n):(d|n)\wedge i\leq d\wedge gcd(i,d)=1} 1$$
$$= \Sigma_{k<S(n)\times S(n):(k/(Sn)|n)\wedge(k\ mod\ S(n)\leq d)\wedge gcd(k/S(n),k\ mod\ S(n))=1} 1$$

We want to prove that this quantity is equal to $n = \Sigma_{k<S(n)} 1$.
Hence we must provide a bijection between

$$\{k < S(n)\times S(n) : (k/(Sn)|n)\wedge(k\ mod\ S(n) \leq d)\wedge gcd(k/S(n), k\ mod\ S(n)) = 1\}$$

and

$$\{k < S(n)\}$$

$\Sigma_{d|n}\phi(d) = n$, formally (3)

$$\{k < S(n) \times S(n) : (k/(Sn)|n) \wedge (k \ mod \ S(n) \leq d) \wedge gcd(k/S(n), k \ mod \ S(n)) = 1\}$$

$$\{k < S(n)\}$$

The bijection:

$$\frac{i}{d} = \frac{i(n/d)}{n} = \frac{in/d}{n}$$

so $h(k) = (k \ modS(n))n/(k/S(n))$
$h^-1(j) = \langle d, i \rangle$ where $\frac{i}{d} = \frac{j}{n}$
So, $d = n/gcd(j, n)$ and $i = j/gcd(j, n)$, and
$h^{-1}(j) = (n/gcd(j, n))S(n) + j/gcd(j, n)$

You are "just" left to prove that h and h^{-1} define indeed a bijection bewteen the above sets.

Outline

Conclusions

- 1850 script lines vs 36 lines in the mathematical text: a DeBruijn factor of 50!
- about 150 hours work. Extrapolating, working 6 hours a day for 240 days a year, we could formalize the whole book in 38 years.
- formalization effort looks independent of the system
- better libraries and a more confortable environment

Conclusions

- 1850 script lines vs 36 lines in the mathematical text: a DeBruijn factor of 50!
- about 150 hours work. Extrapolating, working 6 hours a day for 240 days a year, we could formalize the whole book in 38 years.
- formalization effort looks independent of the system
- better libraries and a more confortable environment

Conclusions

- 1850 script lines vs 36 lines in the mathematical text: a DeBruijn factor of 50!
- about 150 hours work. Extrapolating, working 6 hours a day for 240 days a year, we could formalize the whole book in 38 years.
- formalization effort looks independent of the system
- better libraries and a more confortable environment

Conclusions

- 1850 script lines vs 36 lines in the mathematical text: a DeBruijn factor of 50!
- about 150 hours work. Extrapolating, working 6 hours a day for 240 days a year, we could formalize the whole book in 38 years.
- formalization effort looks independent of the system
- better libraries and a more confortable environment

Conclusions

- 1850 script lines vs 36 lines in the mathematical text: a DeBruijn factor of 50!
- about 150 hours work. Extrapolating, working 6 hours a day for 240 days a year, we could formalize the whole book in 38 years.
- formalization effort looks independent of the system
- better libraries and a more confortable environment

Beyond formal checking

- added value: having expressed knowledge in a machine-understandable (higly structured) format.
- checking is just one possible applications (probably not the most relevant one)
- big challenge: study other potential applications (MKM).

Beyond formal checking

- added value: having expressed knowledge in a machine-understandable (higly structured) format.
- checking is just one possible applications (probably not the most relevant one)
- big challenge: study other potential applications (MKM).

Beyond formal checking

- added value: having expressed knowledge in a machine-understandable (higly structured) format.
- checking is just one possible applications (probably not the most relevant one)
- big challenge: study other potential applications (MKM).

Beyond formal checking

- added value: having expressed knowledge in a machine-understandable (higly structured) format.
- checking is just one possible applications (probably not the most relevant one)
- big challenge: study other potential applications (MKM).

Beyond formal checking

- added value: having expressed knowledge in a machine-understandable (higly structured) format.
- checking is just one possible applications (probably not the most relevant one)
- big challenge: study other potential applications (MKM).