Euler's Partition Theorem

Lukas Bulwahn

October 11, 2017

Abstract

Euler's Partition Theorem states that the number of partitions with only distinct parts is equal to the number of partitions with only odd parts. The combinatorial proof follows John Harrison's pre-existing HOL Light formalization [1]. To understand the rough idea of the proof, I read the lecture notes of the MIT course 18.312 on Algebraic Combinatorics [2] by Gregg Musiker. This theorem is the 45th theorem of the Top 100 Theorems list.

Contents

1 Euler's Partition Theorem

theory *Euler-Partition*
imports
Main
Card-Number-Partitions.Number-Partition
begin

1.1 Preliminaries

1.1.1 Additions to Divides Theory

lemma *power-div-nat*:
  assumes $c \leq b$
  assumes $a > 0$
  shows $(a :: nat)\ \hat{}\ b\ div\ a\ \hat{}\ c = a\ \hat{}\ (b - c)$
$\langle proof \rangle$

1.1.2 Additions to Groups-Big Theory

lemma *sum-div*:
  assumes *finite A*
  assumes $\bigwedge a.\ a \in A \Longrightarrow (b::'b::semiring\text{-}div)\ dvd\ f\ a$
  shows $(\sum a{\in}A.\ f\ a)\ div\ b = (\sum a{\in}A.\ (f\ a)\ div\ b)$
$\langle proof \rangle$

lemma *sum-mod*:
  assumes *finite A*
  assumes $\bigwedge a.\ a \in A \Longrightarrow f\ a\ mod\ b = (0::'b::\{semiring\text{-}div\})$
  shows $(\sum a{\in}A.\ f\ a)\ mod\ b = 0$
$\langle proof \rangle$

1.1.3 Additions to Set-Interval Theory

lemma *geometric-sum-2nat*:
  $(\sum i{<}n.\ (2::nat)\ \hat{}\ i) = (2\ \hat{}\ n - 1)$
$\langle proof \rangle$

1.1.4 Additions to Nat Theory or Power Theory

lemma *n-leq-2-pow-n*:
  $n \leq 2\ \hat{}\ n$
$\langle proof \rangle$

1.1.5 Additions to Finite-Set Theory

lemma *finite-exponents*:
  $finite\ \{i.\ 2\ \hat{}\ i \leq (n::nat)\}$
$\langle proof \rangle$

1.2 Binary Encoding of Natural Numbers

definition $bitset :: nat \Rightarrow nat\ set$
where
  $bitset\ n = \{i.\ odd\ (n\ div\ (2\ \hat{}\ i))\}$

lemma *in-bitset-bound*:
  $b \in bitset\ n \Longrightarrow 2\ \hat{}\ b \leq n$
$\langle proof \rangle$

lemma *in-bitset-bound-weak*:
  $b \in bitset\ n \Longrightarrow b \leq n$
$\langle proof \rangle$

lemma *finite-bitset*:
  $finite\ (bitset\ n)$
$\langle proof \rangle$

lemma *bitset-0*:
  $bitset\ 0 = \{\}$
$\langle proof \rangle$

lemma *binary-induct* [*case-names zero even odd*]:
  assumes $P\ (0 :: nat)$
  assumes $\bigwedge n.\ P\ n \Longrightarrow P\ (2 * n)$
  assumes $\bigwedge n.\ P\ n \Longrightarrow P\ (2 * n + 1)$
  shows $\bigwedge n.\ P\ n$
$\langle proof \rangle$

lemma *bitset-2n*: $bitset\ (2 * n) = Suc\ `\ (bitset\ n)$
$\langle proof \rangle$

lemma *bitset-Suc*:
  assumes $even\ n$
  shows $bitset\ (n + 1) = insert\ 0\ (bitset\ n)$
$\langle proof \rangle$

lemma *bitset-2n1*:
  $bitset\ (2 * n + 1) = insert\ 0\ (Suc\ `\ (bitset\ n))$
$\langle proof \rangle$

lemma *sum-bitset*:
  $(\sum i{\in}bitset\ n.\ 2\ \hat{}\ i) = n$
$\langle proof \rangle$

lemma *binarysum-div*:
  assumes $finite\ B$
  shows $(\sum i{\in}B.\ (2{::}nat)\ \hat{}\ i)\ div\ 2\ \hat{}\ j = (\sum i{\in}B.\ if\ i < j\ then\ 0\ else\ 2\ \hat{}\ (i - j))$
  (**is** $\text{-} = (\sum i{\in}\text{-}.\ ?f\ i)$)
$\langle proof \rangle$

lemma *odd-iff*:
  assumes $finite\ B$
  shows $odd\ (\sum i{\in}B.\ if\ i < x\ then\ (0{::}nat)\ else\ 2\ \hat{}\ (i - x)) = (x \in B)$ (**is** $odd\ (\sum i{\in}\text{-}.\ ?s\ i) = \text{-}$)
$\langle proof \rangle$

lemma *bitset-sum*:
  assumes *finite B*
  shows $bitset\ (\sum i{\in}B.\ 2\ \hat{}\ i) = B$
⟨*proof*⟩

1.3 Decomposition of a Number into a Power of Two and an Odd Number

function (*sequential*) *index* :: $nat \Rightarrow nat$
where
  $index\ 0 = 0$
| $index\ n = (if\ odd\ n\ then\ 0\ else\ Suc\ (index\ (n\ div\ 2)))$
⟨*proof*⟩

termination
⟨*proof*⟩

function (*sequential*) *oddpart* :: $nat \Rightarrow nat$
where
  $oddpart\ 0 = 0$
| $oddpart\ n = (if\ odd\ n\ then\ n\ else\ oddpart\ (n\ div\ 2))$
⟨*proof*⟩

termination
⟨*proof*⟩

lemma *odd-oddpart*:
  $odd\ (oddpart\ n) \longleftrightarrow n \neq 0$
⟨*proof*⟩

lemma *index-oddpart-decomposition*:
  $n = 2\ \hat{}\ (index\ n) * oddpart\ n$
⟨*proof*⟩

lemma *oddpart-leq*:
  $oddpart\ n \leq n$
⟨*proof*⟩

lemma *index-oddpart-unique*:
  assumes $odd\ (m :: nat)\ odd\ m'$
  shows $(2\ \hat{}\ i * m = 2\ \hat{}\ i' * m') \longleftrightarrow (i = i' \wedge m = m')$
⟨*proof*⟩

lemma *index-oddpart*:
  assumes *odd m*
  shows $index\ (2\ \hat{}\ i * m) = i\ oddpart\ (2\ \hat{}\ i * m) = m$
⟨*proof*⟩

1.4 Partitions With Only Distinct and Only Odd Parts

definition *odd-of-distinct* :: $(nat \Rightarrow nat) \Rightarrow nat \Rightarrow nat$
where
  odd-of-distinct $p = (\lambda i.\ if\ odd\ i\ then\ (\sum j \mid p\ (2\ \hat{}\ j * i) = 1.\ 2\ \hat{}\ j)\ else\ 0)$

definition *distinct-of-odd* :: $(nat \Rightarrow nat) \Rightarrow nat \Rightarrow nat$
where
  distinct-of-odd $p = (\lambda i.\ if\ index\ i \in bitset\ (p\ (oddpart\ i))\ then\ 1\ else\ 0)$

lemma *odd*:
  odd-of-distinct $p\ i \neq 0 \Longrightarrow odd\ i$
⟨*proof*⟩

lemma *distinct-distinct-of-odd*:
  distinct-of-odd $p\ i \leq 1$
⟨*proof*⟩

lemma *odd-of-distinct*:
  assumes *odd-of-distinct* $p\ i \neq 0$
  assumes $\bigwedge i.\ p\ i \neq 0 \Longrightarrow i \leq n$
  shows $1 \leq i \wedge i \leq n$
⟨*proof*⟩

lemma *distinct-of-odd*:
  assumes $\bigwedge i.\ p\ i * i \leq n$ $\bigwedge i.\ p\ i \neq 0 \Longrightarrow odd\ i$
  assumes *distinct-of-odd* $p\ i \neq 0$
  shows $1 \leq i \wedge i \leq n$
⟨*proof*⟩

lemma *odd-distinct*:
  assumes $\bigwedge i.\ p\ i \neq 0 \Longrightarrow odd\ i$
  shows *odd-of-distinct* (*distinct-of-odd* p) $= p$
⟨*proof*⟩

lemma *distinct-odd*:
  assumes $\bigwedge i.\ p\ i \neq 0 \Longrightarrow 1 \leq i \wedge i \leq n$ $\bigwedge i.\ p\ i \leq 1$
  shows *distinct-of-odd* (*odd-of-distinct* p) $= p$
⟨*proof*⟩

lemma *sum-distinct-of-odd*:
  assumes $\bigwedge i.\ p\ i \neq 0 \Longrightarrow 1 \leq i \wedge i \leq n$
  assumes $\bigwedge i.\ p\ i * i \leq n$
  assumes $\bigwedge i.\ p\ i \neq 0 \Longrightarrow odd\ i$
  shows $(\sum i{\leq}n.\ distinct\text{-}of\text{-}odd\ p\ i * i) = (\sum i{\leq}n.\ p\ i * i)$
⟨*proof*⟩

lemma *leq-n*:
  assumes $\forall i.\ 0 < p\ i \longrightarrow 1 \leq i \wedge i \leq (n{::}nat)$
  assumes $(\sum i{\leq}n.\ p\ i * i) = n$

shows $p\ i * i \leq n$
⟨*proof*⟩

lemma *distinct-of-odd-in-distinct-partitions*:
assumes $p \in \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \neq 0 \longrightarrow \mathit{odd}\ i)\}$
shows $\mathit{distinct\text{-}of\text{-}odd}\ p \in \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \leq 1)\}$
⟨*proof*⟩

lemma *odd-of-distinct-in-odd-partitions*:
assumes $p \in \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \leq 1)\}$
shows $\mathit{odd\text{-}of\text{-}distinct}\ p \in \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \neq 0 \longrightarrow \mathit{odd}\ i)\}$
⟨*proof*⟩

1.5 Euler's Partition Theorem

theorem *Euler-partition-theorem*:
$\mathit{card}\ \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \leq 1)\} = \mathit{card}\ \{p.\ p\ \mathit{partitions}\ n \wedge (\forall\, i.\ p\ i \neq 0 \longrightarrow \mathit{odd}\ i)\}$
(**is** $\mathit{card}\ ?\mathit{distinct\text{-}partitions} = \mathit{card}\ ?\mathit{odd\text{-}partitions}$)
⟨*proof*⟩

end

References

[1] J. Harrison. Euler's partition theorem and other elementary partition theorems. https://github.com/jrh13/hol-light/blob/master/100/euler.ml.

[2] G. Musiker. Course 18.312: Algebraic combinatorics, 2009. http://ocw.mit.edu/courses/mathematics/18-312-algebraic-combinatorics-spring-2009/readings-and-lecture-notes/MIT18_312S09_lec10_Patitio.pdf.