Mathematical Case Studies: Some Finite and Infinite Combinatorics*

Rob Arthan
rda@lemma-one.com

31 December 2016

Abstract

This document presents some definitions and theorems from elementary finite and infinite combinatorics. The definitions include a "fold" operator for finite sets and the operation that sums a real-valued function on a finite indexed set. The theorems include: more facts about finiteness and the size of finite sets; algebraic properties of indexed sums; induction over finitely-supported functions; the inclusion/exclusion principle; the binomial coefficients and their basic properties, including the formula for the number of combinations and the binomial theorem. The theory is applied to give proofs of Bertrand's ballot theorem and the two-square theorem. The main theorems in infinite combinatorics are the infinite versions of the pigeon-hole principle and of Ramsey's theorem.

Reference: LEMMA1/HOL/WRK073; Current git revision: ce70fda

*First posted 22 November 2005; for full changes history see: `https://github.com/RobArthan/pp-contrib`.

Contents

1 INTRODUCTION

This document is one of a set of documents containing mathematical case studies in ProofPower-HOL. It deals with some finite and infinite combinatorics. Notable results include the inclusion/exclusion principle, the formula for the number of combinations, the binomial theorem, Bertrand's ballot theorem and the infinite version of Ramsey's theorem.

Section 2 and 3 below give an overview of the material on finite and infinite combatorics respectively, including all the specifications and a guide to the theorems proved. Section A and B contain listings of all the theorems proved in the theories. An index to the specifications and the theorems is given at the end of the document.

2 THE THEORY *fincomb*

2.1 Preliminaries

The following commands set up a theory to hold the definitions, theorems, etc., and a proof context that is convenient for the work. The theory is a child of the theory "analysis" (defined in [3]) from which we use several definitions, in particular, the characteristic function χ_A of a set A.

SML

```
force_delete_theory"fincomb" handle Fail _ => ();
open_theory"analysis";
new_theory"fincomb";
new_parent "set_thms";
set_merge_pcs["basic_hol1", "'sets_alg", "'ℤ", "'ℝ"];
```

2.2 Folding Binary Operators over Finite Sets

The following definition of a "fold" operation for finite sets is parametrised by three things: an associative and commutative binary operator, p, with identity element, e, and a "valuation" function v; the operation maps the valuation function over a set combining the resulting values with the product operation.

HOL Constant

```
SetFold : 'a → ('a → 'a → 'a) → ('b → 'a) → 'b SET → 'a
────────────────────────────────────────
∀e p v•
        (∀x• p x e = x)
∧       (∀x y• p x y = p y x)
∧       (∀x y z• p (p x y) z = p x (p y z))
⇒       SetFold e p v {}  = e
∧       ∀x a•  a ∈ Finite ∧ ¬x ∈ a
        ⇒       SetFold e p v ({x} ∪ a) = p (v x) (SetFold e p v a)
```

The parametrisation of *SetFold* is as recommended by Nipkow and Paulson and works nicely. An alternative would be to combine p and v into a single function, say $f = \lambda xy \bullet p(vx)y$ but then the algebraic laws that f must satisfy have an unfamiliar form. The two approaches are interdefinable.

The theorems in the theory begin by with some lemmas about finite sets and their sizes. These are then used to prove two lemmas needed to prove the consistency of the definition of *SetFold*.

∪_finite_thm	*list_finite_size_thm*	*SetFold_consistent*
elems_finite_thm	*set_fold_consistent_lemma1*	*set_fold_def*
list_finite_size_thm1	*set_fold_consistent_lemma2*	

2.3 Further Theorems About Finiteness

The first block of theorems extends the repertoire of lemmas about finite sets and their sizes. The approach to this topic in the ProofPower-HOL library tends to characterise a finite set, A, as one that can be written as $Elems(L)$ for some list L and the size $\#(A)$ as the length $\#(L)$ where L is a list of distinct elements with $Elems(L) = A$.

The first few theorems are aimed at an alternative characterisation of a finite set A as one that is in one-one correspondence with an initial subset of the natural numbers, $\{i|i < m\}$ for some m. *En route* are proved various useful facts, e.g., that finiteness and size are preserved under bijections.

singleton_finite_thm	*range_finite_size_thm*	*distinct_nth_thm*
size_⊆_diff_thm	*length_map_thm*	*bijection_finite_size_thm*
⊆_finite_size_thm	*elems_map_thm*	*bijection_finite_size_thm1*
⊆_size_eq_thm	*map_distinct_thm*	*range_bijection_finite_size_thm*
size_disjoint_∪_thm	*nth_∈_elems_thm*	*surjection_finite_size_thm*
∪_finite_size_≤_thm	*elems_nth_thm*	*range_finite_size_thm1*

The next block of theorems deal with the power set operator. $\mathbb{P}\,a$ is defined in the ProofPower-HOL library by the bi-implication $x \in \mathbb{P}a \iff x \subseteq a$. The first theorem below just recasts this as an equation. There are then two trivial but quite useful lemmas about binary partitions of a power set. This is followed by the theorem that, if a is finite, then so is $\mathbb{P}a$ and $\#(\mathbb{P}a) = 2^{\#(a)}$

ℙ_thm	*ℙ_split_thm1*
ℙ_split_thm	*ℙ_finite_size_thm*

2.4 Sums over Finite Indexed Sets

A useful application of the set fold operation is to define the following indexed sum operation. Given an index set, a, and a function, f, assigning a real number to each member of a, *IndSum* a f is the indexed sum $\sum_{x\in a} f(x)$, and is defined for any set a in which f has finite support.

HOL Constant

$$\textbf{IndSum} : 'a\ SET \to ('a \to \mathbb{R}) \to \mathbb{R}$$

$$\begin{aligned}
&\forall f\bullet\quad IndSum\ \{\}\ f = \mathbb{N}\mathbb{R}\ 0 \\
&\wedge\quad \forall x\ a\bullet\ a \in Finite \wedge \neg x \in a \\
&\qquad \Rightarrow\quad IndSum\ (\{x\} \cup a)\ f = f\ x + IndSum\ a\ f
\end{aligned}$$

We will write $\sum a\ f$ as shorthand for *IndSum a f*.

SML

```
declare_alias("Σ", ⌜IndSum⌝);
```

The consistency proof for *IndSum* is very simple given the set fold operation. As with *SetFold*, the definition is intended to cover the two important cases where a is finite (*ind_sum_def1*) or where f has finite support (*ind_sum_def2*).

IndSum_consistent *ind_sum_def*

We now begin to develop the theory of indexed sums. The first result is an example: if A is finite, then its size $\#(A)$ may be calculated as the indexed sum $\sum_A 1$. The next few theorems show that the indexed sum operator $\sum_A f$ is linear in f (i.e., it respects addition and multiplication by a constant) and give some useful consequences of this.

A principle that is applied almost unconsciously in informal reasoning is that the indexed sum $\sum_A f$ is a local property of f, in the sense that, if f and g are functions that agree on A, then $\sum_A f = \sum_A g$. This block of theorems concludes with one showing how indexed sums behave when the function is composed with a bijection: if b is a bijection on the set A and B is the image of A under b, then $\sum_B f = \sum_A (\lambda x \bullet f(b(x)))$

ind_sum_size_thm	*ind_sum_const_times_thm*	*ind_sum_local_thm*
ind_sum_plus_thm	*ind_sum_0_thm*	*ind_sum_0_bc_thm*
ind_sum_minus_thm	*ind_sum_diff_0_thm*	*bijection_ind_sum_thm*

We now have two lemmas for calculating the indexed sum in two cases where there is at most one non-zero value in the sum:

ind_sum_χ_singleton_thm *ind_sum_singleton_thm*

Now we define the support of a real valued function.

HOL Constant

$$\textbf{Supp} : ('a \to \mathbb{R}) \to 'a\ SET$$

$$\forall\ f \bullet\ Supp\ f = \{x \mid \neg f\ x = \mathbb{N}\mathbb{R}\ 0\}$$

Next comes an induction principle for functions of finite support, i.e., functions f such that $f(x) \neq 0$ for at most finitely many x. If p is any property of functions that is true for the characteristic function, $\chi_{\{x\}}$, of any singleton set, $\{x\}$, and that is preserved under addition and multiplication by a constant (for operands of finite support), then $p(f)$ holds for any function f of finite support.

In working with an indexed sum $\sum_A f$, one can always assume that f has finite support (by adjusting it to be 0 outside A if necessary). This induction principle gives a different line of attack on $\sum_A f$, which can be particularly useful if the internal structure of A is complex.

fin_supp_induction_thm *fin_supp_induction_thm1* *supp_clauses*

We will use the induction principle for functions of finite support to tackle the inclusion/exclusion principle. The inclusion/exclusion principle deals with a family U_i of sets where i range over a finite and non-empty index set I. The inclusion/exclusion principle is the following equation giving the size of the union of the U_i.

$$\#\left(\bigcup_{i\in I} U_i\right) = \sum_{\substack{J \in \mathbb{P}I \\ J \neq \{\}}} (-1)^{\#(J)+1}\#\left(\bigcap_{j\in J} U_j\right) \tag{1}$$

This is a special case of a more general statement about indexed sums and the more general statement is actually rather simpler to prove. The more general statement is the following, which holds for U_i and I above and any real-valued function f:

$$\sum_{x\in\bigcup_{i\in I} U_i} f(x) = \sum_{\substack{J \in \mathbb{P}I \\ J \neq \{\}}} (-1)^{\#(J)+1}\left(\sum_{z\in\bigcap_{j\in J} U_j} f(z)\right) \tag{2}$$

The statement about sizes follows immediately from the statement about indexed sums by applying it to the function $f(x) = 1$. The statement about sums is better understood in the following more symmetric form in which $A = \bigcup_{i\in I} U_i$ is the range of the sum on the left-hand side of the above equation:

$$\sum_{J\in\mathbb{P}I} (-1)^{\#(J)}\left(\sum_{z\in A\cap\bigcap_{j\in J} U_j} f(z)\right) = 0 \tag{3}$$

Here, the intersections with A in the range of the inner sum have no effect except when J is empty. The previous statement thus follows from the above simply by subtracting the sum over the non-empty J from both sides of the equation.

It is quite natural to attempt to prove equation (3) by induction on I (or on the size of I). This works, but the proof is somewhat complicated. Somewhat simpler is to work by induction on A, but it it still quite complex. Instead, our proof of the inclusion/exclusion principle implements the above remarks together with the proof of equation (3) sketched below which works by induction on the structure of f.

Changing it to be identically 0 outside A if necessary, we may assume f has finite support, and, as the left-hand side of (3) is easily seen to be linear in f, the principle of induction for functions of finite support means it is sufficient to prove (3) when $f = \chi_{\{x\}}$ is the characteristic function of a singleton set $\{x\}$. For $f = \chi_{\{x\}}$, the summand $f(z)$ on the left-hand side of (3) is 1 or 0 according as $z = x$ or not. Thus the inner sum is 1 if $x \in U_j$ for all $j \in J$ and vanishes otherwise.

So, if x is not in any U_j, the left-hand side of (3) vanishes and we are done, and, if x is in some U_j, (3) reduces to:

$$\sum_{J\in\mathbb{P}\{j\in I|x\in U_j\}} (-1)^{\#(J)} = 0 \tag{4}$$

(Formally, we are appealing here to the special case of the inclusion/exclusion principle when $\#(I) = 2$, which states that $\sum_{B\cup C} f = \sum_B f + \sum_C f - \sum_{B\cap C} f$, with $B = \mathbb{P}\{j \in I|x \in U_j\}$ and $C = \mathbb{P}I\backslash B$.)

But now I claim that $\sum_{J\in\mathbb{P}K}(-1)^{\#(J)} = 0$ for any non-empty indexed set K, which, taking $K = \{j \in I|x \in U_j\}$ in (4) will complete the proof.

To see that $\sum_{J \in \mathbb{P}K}(-1)^{\#(J)} = 0$ for any non-empty indexed set K, pick $k \in K$, then, as J ranges over $\mathbb{P}(K \backslash \{k\})$, the sets J and $J \cup \{i\}$ range over $\mathbb{P}K$ (with every member of $\mathbb{P}K$ appearing exactly once). As $(-1)^{\#(J)} = -(-1)^{\#(J \cup \{i\})}$, the contributions of J and $J \cup \{i\}$ cancel out and the sum is zero. (Formally, we are again using the special case of the principle for $\#(I) = 2$ together with the result about indexed sums composed with a bijection.)

The above proof is captured in the following series of theorems, which give the main steps in the above argument in bottom-up order:

ind_sum_∪_thm	*ind_⋃_finite_thm*	*ind_sum_inc_exc_thm*
ind_sum_ℙ_thm	*ind_sum_inc_exc_sym_thm*	*size_inc_exc_thm*

A final block of theorems in this section are useful facts about supports and indexed sums of use elsewhere.

supp_χ_thm	*ind_sum_supp_thm*	*ind_sum_singleton_×_thm*
supp_plus_thm	*ind_sum_transfer_thm*	*ind_sum_×_thm*

2.5 Binomial Coefficients

We define the binomial coefficient C^n_m by recursion equations in the usual way. The consistency of the definition is proved automatically.

HOL Constant

Binomial : ℕ → ℕ → ℕ

```
      Binomial 0 0 = 1
∧     (∀m•Binomial 0 (m+1) = 0)
∧     (∀n•Binomial (n+1) 0 = 1)
∧     (∀n m• Binomial (n+1) (m+1) = Binomial n m + Binomial n (m+1))
```

After the inclusion/exclusion principle, we turn to something a little simpler, proving that if A is a set of size n, then A has C^n_m subsets of size m. In a related vein we also prove the binomial theorem (but apart from the algebraic facts about the binomial function that are used, the proofs are separate).

We then have a couple of useful lemmas about the factorial function which are used to prove the formula $C^{m+n}_m = (n+m)!/m! * n!$.

binomial_0_clauses	*combinations_finite_size_thm*	*factorial_not_0_recip_thm*
binomial_less_0_thm	*binomial_thm1*	*factorial_times_thm*
binomial_eq_thm	*binomial_thm*	*binomial_factorial_thm*

2.6 Sampling

If A is a finite set of size s say, there are s^n ways of taking an ordered sample of m not necessarily distinct elements of A ("sampling with replacement"). If the samples are required to be distinct, then there are no samples unless $s = m+n \geq n$, say, and then the number of samples is $(m+n)(m+n-1)\ldots(m+1)$ ("sampling without replacement"). The following function gives this quantity as a function of m and n.

HOL Constant

$$\boldsymbol{DistinctSamples} : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$$

$$(\forall n \bullet\ DistinctSamples\ n\ 0 = 1)$$
$$\land \quad (\forall m\ n \bullet\ DistinctSamples\ n\ (m+1) = (n+m+1) * DistinctSamples\ n\ m)$$

The following block of theorems help deal with sampling and provide some further useful combinatorial facts. The first in the block proves the existence of a polymorphic enumeration function assigning to each finite set A, a function $\mathsf{enumerate}_A$ which maps the set of natural numbers less than $\#(A)$ bijectively onto A. This is used to prove a theorem about "coverings": let us say a set B *covers* another set A, if there is a function f and a natural number m mapping B to A such that the inverse images $f^{-1}(y)$ as y ranges over A are all finite and of size m; in these circumstances, then if A is finite, so is B and $\#(B) = m \times \#(A)$.

These facts (together with earlier counting principles) are then used to prove the statements made above about sampling, in which we use lists to represent ordered samples. This representation fits in nicely with earlier results connecting lists and finite sets.

enumerate_thm	*distinct_samples_rw_thm*
covering_finite_size_thm	*distinct_samples_up_thm*
samples_finite_size_thm	*distinct_samples_finite_size_thm*

Determining probabilities in finite sample spaces is "simply" a matter of counting: if S is finite sample space with $\#(S) \neq 0$ and X is a subset of S, then the probability that an event in S belongs to X is $\#(X)/\#(S)$.

The next theorem gives the well-known calculation that in a group of 23 people, the probability that at least two people have the same birthday is greater than 1/2. This is a simple consequence of the above theorems on sampling (S and $S\ X$ being the set of samples of size 23 out of a set of size 365 with and without replacement respectively). In section 2.7, we do a harder example.

birthdays_thm

2.7 Application: Bertrand's Ballot Theorem

In Bertrand's ballot problem a ballot is held between two candidates, North and South, say. North beats South, the votes being counted one at a time by a single clerk. The problem is to calculate the probability that at all times during the count, North had a majority over South.

The answer is the result of dividing the North's final majority by the total number of votes cast. I.e., if the North receives M votes and South N, the probability is $(M-N)/(M+N)$.

Following Feller [2], we represent the ballot problem using *walks* (also called "paths" in [2]). We define a *walk* of length n starting at x is a sequence of integers s_i such that $s_0 = x$, $|s_{m+1} - s_m| = 1$ for $0 \leq i < n$ and (for definiteness) $s_{m+1} = s_n$ for $m \geq n$.

HOL Constant

$$\textbf{\textit{Walk}} : \mathbb{N} \to \mathbb{Z} \to (\mathbb{N} \to \mathbb{Z})\ SET$$

$$\begin{array}{ll} \forall n\ x\ s \bullet & \\ & s \in Walk\ n\ x \\ \Leftrightarrow & s\ 0 = x \\ \wedge & (\forall m \bullet m < n \Rightarrow Abs(s(m{+}1) - s(m)) = \mathbb{N}\mathbb{Z}\ 1) \\ \wedge & (\forall m \bullet n \leq m \Rightarrow s\ m = s\ n) \end{array}$$

In talking about walks, we often identify a walk s_i with the polygonal path obtained by joining the points (i, s_i) in the plane. Under this identification a walk starting at x of length n begins at $(0, x)$, takes n diagonal north-east or south-east steps and then heads directly east indefinitely. The following definition captures the final y-value taken on by a walk.

HOL Constant

$$\textbf{\textit{WalkTo}} : \mathbb{N} \to \mathbb{Z} \to \mathbb{Z} \to (\mathbb{N} \to \mathbb{Z})\ SET$$

$$\begin{array}{ll} \forall n\ x\ y\ s \bullet & \\ & s \in WalkTo\ n\ x\ y \\ \Leftrightarrow & s \in Walk\ n\ x \wedge s\ n = y \end{array}$$

Walks satisfy a discrete version of the intermediate value theorem: if x, y and z are integers such that z lies between x and y then any walk from x to y takes the value z at some stage.

In the ballot problem, define t_i to be the (possibly zero or negative) majority of North over South when the i-th vote is counted. Then t_i is a walk of length $M + N$ from 0 to $M - N$ and any such walk corresponds to exactly one possible order in which to count the votes.

HOL Constant

$$\textbf{\textit{BallotCounts}} : \mathbb{N} \to \mathbb{N} \to (\mathbb{N} \to \mathbb{Z})\ SET$$

$$\forall m\ n \bullet\ BallotCounts\ m\ n = WalkTo\ (m + n)\ (\mathbb{N}\mathbb{Z}\ 0)\ (\mathbb{N}\mathbb{Z}\ m - \mathbb{N}\mathbb{Z}\ n)$$

Thus the probability we have to calculate is x/s, where s is the total number of walks, t_i, of length $M + N$ from 0 to $M - N$, and where x is the number of these that are *favourable*, i.e., that are such that $t_i > 0$ for $i > 0$. For any Q, a walk of length $M + N$ from Q to $Q + M - N$ is uniquely determined by the set of indices i for which $t_{i+1} - t_i = 1$. Thus the number of such walks is the number of ways of choosing M numbers less than $M + N$, i.e., $s = C_M^{M+N}$.

To calculate the number of favourable walks, we use what Feller calls the *reflection principle*. This says that, if i and j are positive integers, then there is a one-to-one correspondence between walks of length $M + N$, s_i, from i to j which cross the x-axis and arbitrary walks of length $M + N$ from $-i$ to j. To see this one observes that, by the intermediate value theorem for walks, a walk, t_i, of the second sort must have $t_i = 0$ for some i; reflecting the initial negative segment of t_i in the x-axis gives a walk s_i of the first sort. This reflection defines the required one-to-one correspondence.

Now if t_i is a favourable walk of length $M + N$ from 0 to $M - N$ then $u_i = t_{i+1}$ defines a walk from 1 to $M - N > 0$ which does not cross the x-axis. From the reflection principle, we have that the number of such walks is $a = C^{M+N-1}_{M-1} - C^{M+N-1}_{M}$. It then follows from a calculation using the expression of the binomial function in terms of factorials, that $x/s = (M - N)/(M + N)$.

The following block of theorems implements the proof sketched above.

walk_thm	*walk_to_minus_thm*
walk_to_thm	*walk_to_intermediate_value_thm*
walk_finite_size_thm	*walk_to_reflection_thm*
walk_to_finite_size_thm	*ballot_lemma1*
walk_to_empty_thm	*ballot_lemma2*
walk_to_finite_thm	*ballot_lemma3*
walk_walk_to_thm	*ballot_lemma4*
walk_shift_thm	*ballot_lemma5*
walk_minus_thm	*ballot_thm*

2.8 Involutions

Involutions give some useful counting principles.

HOL Constant

$\boldsymbol{Involution} : {}'a\ SET \to ({}'a \to {}'a)\ SET$

$\forall f\ A\bullet\ f \in Involution\ A \Leftrightarrow (\forall x\bullet\ x \in A \Rightarrow f\ x \in A \land f(f\ x) = x)$

Fixed points are important:

HOL Constant

$\boldsymbol{Fixed} : ({}'a \to {}'a) \to {}'a\ SET$

$\forall x\ f\bullet\ x \in Fixed\ f \Leftrightarrow f\ x = x$

We prove that every involution f on a set X has a fundamental region: i.e., a subset A such that X decomposes as the disjoint union of A, $f(A)$ and the fixed point set of f. We use Zorn's lemma for this in the special case where the ordered set comprises sets and inclusion. The formulation of this case of Zorn's lemma in some versions of ProofPower is hard to use directly, so we provide a more convenient formulation. After a few convenience lemmas, we then give the main counting principles for involutions on finite sets: if a set admits an involution with no fixed points, its size is even; an involution on a set with an odd size has at least one fixed point; if a set admits an involution with a unique fixed point, its size is odd.

zorn_thm2	*involution_def_thm2*	*involution_odd_size_thm*
fund_region_thm	*involution_size_thm*	*involution_set_dif_fixed_thm*
involution_one_one_thm	*involution_even_size_thm*	*involution_fixed_singleton_thm*
involution_def_thm1		

2.9 Application: the Two Squares Theorem

We apply the theorems on involutions to do the combinatorial part of Heath-Brown's ingenious proof of the theorem that every prime congruent to 1 modulo 4 is the sum of two squares. This requires a few preliminary lemmas on integer arithmetic. Apart from variable names, the proof then follows closely the presentation of [1] (our sets A, B and C are Aigner & Günter's S, T and U). At each stage, rather than assume primality, we make the exact assumptions the combinatorial arguments require. The proof is completed in [4] where prime numbers are defined.

ℤ_interval_finite_thm
ℤ_0_≤_square_thm
ℤ_0_less_0_less_times_thm
ℤ_0_less_times_thm
ℤ_0_less_times_thm1
ℤ_≤_square_thm
a_finite_thm
f_involution_a_thm
size_a_size_b_thm
size_a_size_c_thm
size_c_size_c_thm
g_involution_c_thm
size_c_thm
h_involution_b_thm
h_fixed_in_b_thm
two_squares_lemma

3 THE THEORY *infcomb*

SML

```
force_delete_theory "infcomb" handle Fail _ => ();
open_theory "fincomb";
new_theory "infcomb";
set_merge_pcs["basic_hol1", "'sets_alg"];
```

The only definition we need is that of the class of infinite sets (which is simply to be the complement of the class of finite sets):

HOL Constant

```
Infinite : 'a SET SET
──────────────────────────────
Infinite = ~Finite
```

The theorems begin with a simple refactoring of the definition that characterizes infinite sets as those admitting a one-to-one endofunction. This is used to show that a set difference $a \setminus b$ where a is infinite and b is finite is infinite and that a one-to-one image of an infinite set is infinite. We then has some theorems about the natural numbers: they are infinite, the minimum of an infinite subset of natural numbers is well-defined, an infinite set of natural numbers is unbounded and an infinite set of natural numbers is the range of an order-preserving function on the natural numbers. With all this in hand we prove the infinite vefsions of the pigeon hole theorem and of Ramsey's theorem.

infinite_thm
infinite_diff_finite_thm
infinite_one_one_image_thm
ℕ_*infinite_thm*
min_infinite_thm
infinite_unbounded_thm
ordered_enumeration_thm
infinite_pigeon_hole_thm
infinite_ramsey_thm

References

[1] Martin Aigner and Günter. M. Ziegler. *Proofs from the Book*. Springer-Verlag, 2000.

[2] William Feller. *An Introduction to Probability Theory and its Applications*. John Wiley & Sons, Inc., third edition, 1968.

[3] LEMMA1/HOL/WRK066. *Mathematical Case Studies: Basic Analysis*. R.D. Arthan, Lemma 1 Ltd., `rda@lemma-one.com`.

[4] LEMMA1/HOL/WRK074. *Mathematical Case Studies: Some Number Theory*. R.D. Arthan, Lemma 1 Ltd., `rda@lemma-one.com`.

A THEOREMS IN THE THEORY fincomb

$\mathbb{NR}$_$\mathbb{N}$_***exp_thm*** $\vdash \forall\ m\ n \bullet\ \mathbb{NR}\ (m \mathbin{\hat{}} n) = \mathbb{NR}\ m \mathbin{\hat{}} n$

$\mathbb{Z}$_***abs_eq_1_thm***

$$\vdash \forall\ x \bullet\ Abs\ x = \mathbb{NZ}\ 1 \Leftrightarrow x = \mathbb{NZ}\ 1 \lor x = \sim (\mathbb{NZ}\ 1)$$

walk_def1

$$\begin{array}{l}
\vdash \forall\ n\ x\ s \\
\quad \bullet\ s \in Walk\ n\ x \\
\qquad \Leftrightarrow s\ 0 = x \\
\qquad\quad \land (\forall\ m \\
\qquad\quad \bullet\ m < n \\
\qquad\qquad \Rightarrow s\ (m + 1) + \sim (s\ m) = \mathbb{NZ}\ 1 \\
\qquad\qquad\quad \lor\ s\ (m + 1) + \sim (s\ m) = \sim (\mathbb{NZ}\ 1)) \\
\qquad\quad \land (\forall\ m \bullet\ n \le m \Rightarrow s\ m = s\ n)
\end{array}$$

$\cup$_***finite_thm*** $\vdash \forall\ A\ B \bullet\ A \cup B \in Finite \Leftrightarrow A \in Finite \land B \in Finite$

min_$\in$_thm $\vdash \forall\ n\ a \bullet\ n \in a \Rightarrow Min\ a \in a$

min_$\le$_thm $\vdash \forall\ n\ a \bullet\ n \in a \Rightarrow Min\ a \le n$

elems_finite_thm

$$\vdash \forall\ list \bullet\ Elems\ list \in Finite$$

list_finite_size_thm1

$$\begin{array}{l}
\vdash \forall\ a \\
\quad \bullet\ a \in Finite \\
\qquad \Leftrightarrow (\exists\ list \\
\qquad \bullet\ list \in Distinct \\
\qquad\quad \land Elems\ list = a \\
\qquad\quad \land \#\ list = \#\ a)
\end{array}$$

list_finite_size_thm

$$\begin{array}{l}
\vdash \forall\ a\ m \\
\quad \bullet\ a \in Finite \land \#\ a = m \\
\qquad \Leftrightarrow (\exists\ list \\
\qquad \bullet\ list \in Distinct \land Elems\ list = a \land \#\ list = m)
\end{array}$$

set_fold_consistent_lemma1

$$\begin{array}{l}
\vdash \forall\ x\ list1\ n \\
\quad \bullet\ x \in Elems\ list1 \\
\qquad\quad \land list1 \in Distinct \\
\qquad\quad \land \#\ list1 = n + 1 \\
\qquad \Rightarrow (\exists\ list2 \\
\qquad \bullet\ list2 \in Distinct \\
\qquad\quad \land Elems\ list2 = Elems\ list1 \setminus \{x\} \\
\qquad\quad \land \#\ list2 = n)
\end{array}$$

set_fold_consistent_lemma2

$$\begin{array}{l}
\vdash \forall\ e\ p\ v \\
\quad \bullet\ (\forall\ x \bullet\ p\ x\ e = x) \\
\qquad\quad \land (\forall\ x\ y \bullet\ p\ x\ y = p\ y\ x) \\
\qquad\quad \land (\forall\ x\ y\ z \bullet\ p\ (p\ x\ y)\ z = p\ x\ (p\ y\ z)) \\
\qquad \Rightarrow (\forall\ n\ list1\ list2 \\
\qquad \bullet\ list1 \in Distinct \\
\qquad\qquad \land list2 \in Distinct \\
\qquad\qquad \land \#\ list1 = n \\
\qquad\qquad \land Elems\ list1 = Elems\ list2 \\
\qquad\quad \Rightarrow Fold\ (\lambda\ x\ y \bullet\ p\ (v\ x)\ y)\ list1\ e \\
\qquad\qquad = Fold\ (\lambda\ x\ y \bullet\ p\ (v\ x)\ y)\ list2\ e)
\end{array}$$

SetFold_consistent

$\vdash$ *Consistent*
$(\lambda\ SetFold'$
$\bullet\ \forall\ e\ p\ v$
$\bullet\ (\forall\ x \bullet\ p\ x\ e = x)$
$\land\ (\forall\ x\ y \bullet\ p\ x\ y = p\ y\ x)$
$\land\ (\forall\ x\ y\ z \bullet\ p\ (p\ x\ y)\ z = p\ x\ (p\ y\ z))$
$\Rightarrow SetFold'\ e\ p\ v\ \{\} = e$
$\land\ (\forall\ x\ a$
$\bullet\ a \in Finite \land \neg\ x \in a$
$\Rightarrow SetFold'\ e\ p\ v\ (\{x\} \cup a)$
$= p\ (v\ x)\ (SetFold'\ e\ p\ v\ a)))$

set_fold_def $\vdash \forall\ e\ p\ v$
$\bullet\ (\forall\ x \bullet\ p\ x\ e = x)$
$\land\ (\forall\ x\ y \bullet\ p\ x\ y = p\ y\ x)$
$\land\ (\forall\ x\ y\ z \bullet\ p\ (p\ x\ y)\ z = p\ x\ (p\ y\ z))$
$\Rightarrow SetFold\ e\ p\ v\ \{\} = e$
$\land\ (\forall\ x\ a$
$\bullet\ a \in Finite \land \neg\ x \in a$
$\Rightarrow SetFold\ e\ p\ v\ (\{x\} \cup a)$
$= p\ (v\ x)\ (SetFold\ e\ p\ v\ a))$

IndSum_consistent

$\vdash$ *Consistent*
$(\lambda\ IndSum'$
$\bullet\ \forall\ f$
$\bullet\ IndSum'\ \{\}\ f = 0.$
$\land\ (\forall\ x\ a$
$\bullet\ a \in Finite \land \neg\ x \in a$
$\Rightarrow IndSum'\ (\{x\} \cup a)\ f$
$= f\ x + IndSum'\ a\ f))$

ind_sum_def $\vdash \forall\ f$
$\bullet\ \Sigma\ \{\}\ f = 0.$
$\land\ (\forall\ x\ a$
$\bullet\ a \in Finite \land \neg\ x \in a$
$\Rightarrow \Sigma\ (\{x\} \cup a)\ f = f\ x + \Sigma\ a\ f)$

singleton_finite_thm

$\vdash \forall\ x \bullet\ \{x\} \in Finite$

size_⊆_diff_thm

$\vdash \forall\ a\ b \bullet\ a \in Finite \land b \subseteq a \Rightarrow \#\ a = \#\ (a \setminus b) + \#\ b$

⊆_finite_size_thm

$\vdash \forall\ a\ b \bullet\ a \in Finite \land b \subseteq a \Rightarrow b \in Finite \land \#\ b \leq \#\ a$

⊆_size_eq_thm

$\vdash \forall\ a\ b \bullet\ a \in Finite \land b \subseteq a \land \#\ b = \#\ a \Rightarrow b = a$

size_disjoint_∪_thm

$\vdash \forall\ a\ b\ c$
$\bullet\ a \in Finite \land a = b \cup c \land b \cap c = \{\}$
$\Rightarrow \#\ a = \#\ b + \#\ c$

∪_finite_size_≤_thm

$\vdash \forall\ a\ b$
$\bullet\ a \in Finite \land b \in Finite$
$\Rightarrow a \cup b \in Finite \land \#\ (a \cup b) \leq \#\ a + \#\ b$

range_finite_size_thm

$$\vdash \forall\ m \bullet\ \{i | i\ <\ m\}\ \in\ Finite\ \wedge\ \#\ \{i | i\ <\ m\}\ =\ m$$

length_map_thm

$$\vdash \forall\ f\ list \bullet\ \#\ (Map\ f\ list)\ =\ \#\ list$$

elems_map_thm

$$\vdash \forall\ f\ list \bullet\ Elems\ (Map\ f\ list) = \{y | \exists\ x \bullet\ x\ \in\ Elems\ list\ \wedge\ y\ =\ f\ x\}$$

map_distinct_thm

$$\vdash \forall\ f\ list \bullet\ (\forall\ x\ y \bullet\ x\ \in\ Elems\ list\ \wedge\ y\ \in\ Elems\ list\ \wedge\ f\ x\ =\ f\ y \Rightarrow\ x\ =\ y)\ \wedge\ list\ \in\ Distinct \Rightarrow\ Map\ f\ list\ \in\ Distinct$$

nth_∈_elems_thm

$$\vdash \forall\ list\ i \bullet\ i\ <\ \#\ list\ \Rightarrow\ Nth\ list\ (i\ +\ 1)\ \in\ Elems\ list$$

elems_nth_thm

$$\vdash \forall\ list \bullet\ Elems\ list = \{x | \exists\ i \bullet\ i\ <\ \#\ list\ \wedge\ Nth\ list\ (i\ +\ 1)\ =\ x\}$$

distinct_nth_thm

$$\vdash \forall\ list\ i\ j \bullet\ list\ \in\ Distinct\ \wedge\ i\ <\ \#\ list\ \wedge\ j\ <\ \#\ list\ \wedge\ Nth\ list\ (i\ +\ 1)\ =\ Nth\ list\ (j\ +\ 1) \Rightarrow\ i\ =\ j$$

bijection_finite_size_thm

$$\vdash \forall\ a\ b\ f \bullet\ a\ \in\ Finite\ \wedge\ (\forall\ x\ y \bullet\ x\ \in\ a\ \wedge\ y\ \in\ a\ \wedge\ f\ x\ =\ f\ y\ \Rightarrow\ x\ =\ y)\ \wedge\ b\ =\ \{z | \exists\ x \bullet\ x\ \in\ a\ \wedge\ z\ =\ f\ x\} \Rightarrow\ b\ \in\ Finite\ \wedge\ \#\ b\ =\ \#\ a$$

***bijection_finite_size_thm*1**

$$\vdash \forall\ a\ b\ f \bullet\ a\ \in\ Finite\ \wedge\ (\forall\ x\ y \bullet\ x\ \in\ b\ \wedge\ y\ \in\ b\ \wedge\ f\ x\ =\ f\ y\ \Rightarrow\ x\ =\ y)\ \wedge\ a\ =\ \{z | \exists\ x \bullet\ x\ \in\ b\ \wedge\ z\ =\ f\ x\} \Rightarrow\ b\ \in\ Finite\ \wedge\ \#\ b\ =\ \#\ a$$

range_bijection_finite_size_thm

$$\vdash \forall\ a\ m \bullet\ a\ \in\ Finite\ \wedge\ \#\ a\ =\ m \Leftrightarrow (\exists\ f \bullet\ (\forall\ i\ j \bullet\ i\ <\ m\ \wedge\ j\ <\ m\ \wedge\ f\ i\ =\ f\ j\ \Rightarrow\ i\ =\ j)\ \wedge\ a\ =\ \{x | \exists\ i \bullet\ i\ <\ m\ \wedge\ f\ i\ =\ x\})$$

surjection_finite_size_thm

$$\vdash \forall\ a\ b\ f \bullet\ a\ \in\ Finite\ \wedge\ b\ \subseteq\ \{z | \exists\ x \bullet\ x\ \in\ a\ \wedge\ z\ =\ f\ x\} \Rightarrow\ b\ \in\ Finite\ \wedge\ \#\ b\ \leq\ \#\ a$$

***range_finite_size_thm*1**

$\vdash \forall\ m$
$\bullet\ \{i | 1\ \leq\ i\ \land\ i\ \leq\ m\}\ \in\ Finite$
$\land\ \#\ \{i | 1\ \leq\ i\ \land\ i\ \leq\ m\}\ =\ m$

***range_bijection_finite_size_thm*1**
$\vdash \forall\ a$
$\bullet\ a\ \in\ Finite$
$\Leftrightarrow\ (\exists\ f$
$\bullet\ (\forall\ i\ j \bullet\ i\ <\ \#\ a\ \land\ j\ <\ \#\ a\ \land\ f\ i\ =\ f\ j\ \Rightarrow\ i\ =\ j)$
$\land\ a\ =\ \{x | \exists\ i \bullet\ i\ <\ \#\ a\ \land\ f\ i\ =\ x\})$

$\mathbb{P}$*_thm* $\vdash \forall\ a \bullet\ \mathbb{P}\ a\ =\ \{b | b\ \subseteq\ a\}$

$\mathbb{P}$*_split_thm* $\vdash \forall\ x\ a$
$\bullet\ \mathbb{P}\ a\ =\ \{b | b\ \subseteq\ a\ \land\ x\ \in\ b\}\ \cup\ \{b | b\ \subseteq\ a\ \land\ \neg\ x\ \in\ b\}$
$\land\ \{b | b\ \subseteq\ a\ \land\ x\ \in\ b\}\ \cap\ \{b | b\ \subseteq\ a\ \land\ \neg\ x\ \in\ b\}\ =\ \{\}$

$\mathbb{P}$*_split_thm*1 $\vdash \forall\ a\ b$
$\bullet\ b\ \subseteq\ a$
$\Rightarrow\ \mathbb{P}\ a\ =\ \mathbb{P}\ b\ \cup\ \{c | c\ \subseteq\ a\ \land\ (\exists\ x \bullet\ x\ \in\ c\ \land\ \neg\ x\ \in\ b)\}$
$\land\ \mathbb{P}\ b\ \cap\ \{c | c\ \subseteq\ a\ \land\ (\exists\ x \bullet\ x\ \in\ c\ \land\ \neg\ x\ \in\ b)\}\ =\ \{\}$

$\mathbb{P}$*_finite_size_thm*
$\vdash \forall\ a \bullet\ a\ \in\ Finite\ \Rightarrow\ \mathbb{P}\ a\ \in\ Finite\ \land\ \#\ (\mathbb{P}\ a)\ =\ 2\ \hat{}\ \#\ a$

$\times$*_finite_size_thm*
$\vdash \forall\ a\ b$
$\bullet\ a\ \in\ Finite\ \land\ b\ \in\ Finite$
$\Rightarrow\ (a\ \times\ b)\ \in\ Finite\ \land\ \#\ (a\ \times\ b)\ =\ \#\ a\ *\ \#\ b$

ind_sum_size_thm
$\vdash \forall\ A \bullet\ A\ \in\ Finite\ \Rightarrow\ \Sigma\ A\ (\lambda\ x \bullet\ 1.)\ =\ \mathbb{N}\mathbb{R}\ (\#\ A)$

ind_sum_plus_thm
$\vdash \forall\ A\ f\ g$
$\bullet\ A\ \in\ Finite\ \Rightarrow\ \Sigma\ A\ (\lambda\ x \bullet\ f\ x\ +\ g\ x)\ =\ \Sigma\ A\ f\ +\ \Sigma\ A\ g$

ind_sum_minus_thm
$\vdash \forall\ A\ f \bullet\ A\ \in\ Finite\ \Rightarrow\ \Sigma\ A\ (\lambda\ x \bullet\ \sim\ (f\ x))\ =\ \sim\ (\Sigma\ A\ f)$

ind_sum_const_times_thm
$\vdash \forall\ A\ f\ c \bullet\ A\ \in\ Finite\ \Rightarrow\ \Sigma\ A\ (\lambda\ x \bullet\ c\ *\ f\ x)\ =\ c\ *\ \Sigma\ A\ f$

ind_sum_0_thm
$\vdash \forall\ A\ f \bullet\ A\ \in\ Finite\ \Rightarrow\ \Sigma\ A\ (\lambda\ x \bullet\ 0.)\ =\ 0.$

ind_sum_diff_0_thm
$\vdash \forall\ A\ f\ g$
$\bullet\ A\ \in\ Finite\ \land\ \Sigma\ A\ (\lambda\ x \bullet\ f\ x\ -\ g\ x)\ =\ 0.$
$\Rightarrow\ \Sigma\ A\ f\ =\ \Sigma\ A\ g$

ind_sum_local_thm
$\vdash \forall\ A\ f\ g$
$\bullet\ A\ \in\ Finite\ \land\ (\forall\ x \bullet\ x\ \in\ A\ \Rightarrow\ f\ x\ =\ g\ x)$
$\Rightarrow\ \Sigma\ A\ f\ =\ \Sigma\ A\ g$

ind_sum_0_bc_thm
$\vdash \forall\ A\ f$
$\bullet\ A\ \in\ Finite\ \land\ (\forall\ x \bullet\ x\ \in\ A\ \Rightarrow\ f\ x\ =\ 0.)\ \Rightarrow\ \Sigma\ A\ f\ =\ 0.$

bijection_ind_sum_thm
$\vdash \forall\ A\ f\ b$
$\bullet\ A\ \in\ Finite$
$\land\ (\forall\ x\ y \bullet\ x\ \in\ A\ \land\ y\ \in\ A\ \land\ b\ x\ =\ b\ y\ \Rightarrow\ x\ =\ y)$
$\Rightarrow\ \Sigma\ \{z | \exists\ x \bullet\ x\ \in\ A\ \land\ z\ =\ b\ x\}\ f$
$=\ \Sigma\ A\ (\lambda\ x \bullet\ f\ (b\ x))$

ind_sum_χ_singleton_thm

$\vdash \forall\ A\ x$
$\quad \bullet\ A \in \mathit{Finite}$
$\qquad \Rightarrow \Sigma\ A\ (\chi\ \{x\}) = (\mathit{if}\ x \in A\ \mathit{then}\ 1.\ \mathit{else}\ 0.)$

ind_sum_singleton_thm

$\vdash \forall\ x\ f \bullet\ \Sigma\ \{x\}\ f = f\ x$

fin_supp_induction_thm1

$\vdash \forall\ p$
$\quad \bullet\ (\forall\ x \bullet\ p\ (\chi\ \{x\}))$
$\qquad \wedge (\forall\ f\ c$
$\qquad \bullet\ \{x | \neg\ f\ x = 0.\} \in \mathit{Finite} \wedge p\ f$
$\qquad\quad \Rightarrow p\ (\lambda\ x \bullet\ c * f\ x))$
$\qquad \wedge (\forall\ f\ g$
$\qquad \bullet\ \{x | \neg\ f\ x = 0.\} \in \mathit{Finite}$
$\qquad\qquad \wedge \{x | \neg\ g\ x = 0.\} \in \mathit{Finite}$
$\qquad\qquad \wedge p\ f$
$\qquad\qquad \wedge p\ g$
$\qquad\quad \Rightarrow p\ (\lambda\ x \bullet\ f\ x + g\ x))$
$\qquad \Rightarrow (\forall\ f \bullet\ \{x | \neg\ f\ x = 0.\} \in \mathit{Finite} \Rightarrow p\ f)$

fin_supp_induction_thm

$\vdash \forall\ p$
$\quad \bullet\ (\forall\ x \bullet\ p\ (\chi\ \{x\}))$
$\qquad \wedge (\forall\ f\ c$
$\qquad \bullet\ \mathit{Supp}\ f \in \mathit{Finite} \wedge p\ f \Rightarrow p\ (\lambda\ x \bullet\ c * f\ x))$
$\qquad \wedge (\forall\ f\ g$
$\qquad \bullet\ \mathit{Supp}\ f \in \mathit{Finite} \wedge \mathit{Supp}\ g \in \mathit{Finite} \wedge p\ f \wedge p\ g$
$\qquad\quad \Rightarrow p\ (\lambda\ x \bullet\ f\ x + g\ x))$
$\qquad \Rightarrow (\forall\ f \bullet\ \mathit{Supp}\ f \in \mathit{Finite} \Rightarrow p\ f)$

supp_clauses $\vdash \mathit{Supp}\ (\lambda\ x \bullet\ 0.) = \{\}$
$\quad \wedge (\forall\ f \bullet\ \mathit{Supp}\ (\lambda\ x \bullet\ \sim (f\ x)) = \mathit{Supp}\ f)$
$\quad \wedge (\forall\ f\ g \bullet\ \mathit{Supp}\ (\lambda\ x \bullet\ f\ x + g\ x) \subseteq \mathit{Supp}\ f \cup \mathit{Supp}\ g)$
$\quad \wedge (\forall\ c\ f \bullet\ \mathit{Supp}\ (\lambda\ x \bullet\ c * f\ x) \subseteq \mathit{Supp}\ f)$

ind_sum_∪_thm

$\vdash \forall\ A\ B\ f$
$\quad \bullet\ A \in \mathit{Finite} \wedge B \in \mathit{Finite}$
$\qquad \Rightarrow \Sigma\ (A \cup B)\ f = \Sigma\ A\ f + \Sigma\ B\ f - \Sigma\ (A \cap B)\ f$

ind_sum_ℙ_thm

$\vdash \forall\ K$
$\quad \bullet\ K \in \mathit{Finite} \wedge \neg\ K = \{\}$
$\qquad \Rightarrow \Sigma\ (\mathbb{P}\ K)\ (\lambda\ J \bullet\ \sim 1.\ \hat{}\ \#\ J) = 0.$

ind_⋃_finite_thm

$\vdash \forall\ I\ U\ A\ f$
$\quad \bullet\ I \in \mathit{Finite}$
$\qquad \wedge (\forall\ i \bullet\ i \in I \Rightarrow U\ i \in \mathit{Finite})$
$\qquad \wedge A = \bigcup\ \{B | \exists\ i \bullet\ i \in I \wedge B = U\ i\}$
$\qquad \Rightarrow A \in \mathit{Finite}$

ind_sum_inc_exc_sym_thm

$\vdash \forall\ I\ U\ A\ f$
$\quad \bullet\ I \in \mathit{Finite}$
$\qquad \wedge \neg\ I = \{\}$
$\qquad \wedge (\forall\ i \bullet\ i \in I \Rightarrow U\ i \in \mathit{Finite})$

$$
\begin{array}{l}
\quad\quad \land\ A = \bigcup\ \{B | \exists\ i \bullet\ i \in I \land B = U\ i\} \\
\quad \Rightarrow \Sigma \\
\quad\quad\quad (\mathbb{P}\ I) \\
\quad\quad\quad (\lambda\ J \\
\quad\quad\quad\quad \bullet \sim 1.\ \hat{}\ \#\ J \\
\quad\quad\quad\quad\quad * \Sigma\ (A \cap \bigcap\ \{B | \exists\ j \bullet\ j \in J \land B = U\ j\})\ f) \\
\quad\quad = 0.
\end{array}
$$

ind_sum_inc_exc_thm

$$
\begin{array}{l}
\vdash \forall\ I\ U\ A\ f \\
\quad \bullet\ I \in Finite \\
\quad\quad\quad \land \neg\ I = \{\} \\
\quad\quad\quad \land (\forall\ i \bullet\ i \in I \Rightarrow U\ i \in Finite) \\
\quad\quad\quad \land\ A = \bigcup\ \{B | \exists\ i \bullet\ i \in I \land B = U\ i\} \\
\quad\quad \Rightarrow \Sigma\ A\ f \\
\quad\quad\quad = \Sigma \\
\quad\quad\quad\quad (\mathbb{P}\ I \setminus \{\{\}\}) \\
\quad\quad\quad\quad (\lambda\ J \\
\quad\quad\quad\quad\quad \bullet \sim 1.\ \hat{}\ (\#\ J + 1) \\
\quad\quad\quad\quad\quad\quad * \Sigma\ (\bigcap\ \{B | \exists\ j \bullet\ j \in J \land B = U\ j\})\ f)
\end{array}
$$

size_inc_exc_thm

$$
\begin{array}{l}
\vdash \forall\ I\ U\ A \\
\quad \bullet\ I \in Finite \\
\quad\quad\quad \land \neg\ I = \{\} \\
\quad\quad\quad \land (\forall\ i \bullet\ i \in I \Rightarrow U\ i \in Finite) \\
\quad\quad\quad \land\ A = \bigcup\ \{B | \exists\ i \bullet\ i \in I \land B = U\ i\} \\
\quad\quad \Rightarrow \mathbb{NR}\ (\#\ A) \\
\quad\quad\quad = \Sigma \\
\quad\quad\quad\quad (\mathbb{P}\ I \setminus \{\{\}\}) \\
\quad\quad\quad\quad (\lambda\ J \\
\quad\quad\quad\quad\quad \bullet \sim 1.\ \hat{}\ (\#\ J + 1) \\
\quad\quad\quad\quad\quad\quad * \mathbb{NR}\ (\#\ (\bigcap\ \{B | \exists\ j \bullet\ j \in J \land B = U\ j\})))
\end{array}
$$

supp_χ_thm $\vdash \forall\ A \bullet\ Supp\ (\chi\ A) = A$

supp_plus_thm

$$
\begin{array}{l}
\vdash \forall\ f\ g \\
\quad \bullet\ Supp\ (\lambda\ x \bullet\ f\ x + g\ x) \\
\quad\quad = (Supp\ f \cup Supp\ g) \setminus \{x | f\ x = \sim (g\ x)\}
\end{array}
$$

ind_sum_supp_thm

$$\vdash \forall\ A\ f \bullet\ A \in Finite \Rightarrow \Sigma\ A\ f = \Sigma\ (A \cap Supp\ f)\ f$$

ind_sum_transfer_thm

$$
\begin{array}{l}
\vdash \forall\ A\ B\ f\ g\ h \\
\quad \bullet\ A \in Finite \\
\quad\quad\quad \land\ B \in Finite \\
\quad\quad\quad \land (\forall\ x \\
\quad\quad\quad \bullet\ x \in A \land \neg\ f\ x = 0. \Rightarrow h\ x \in B \land f\ x = g\ (h\ x)) \\
\quad\quad\quad \land (\forall\ y \\
\quad\quad\quad \bullet\ y \in B \land \neg\ g\ y = 0. \\
\quad\quad\quad\quad \Rightarrow (\exists_1\ x \bullet\ x \in A \land h\ x = y \land f\ x = g\ y)) \\
\quad\quad \Rightarrow \Sigma\ A\ f = \Sigma\ B\ g
\end{array}
$$

ind_sum_singleton_×_thm

$$
\begin{array}{l}
\vdash \forall\ x\ B\ f \\
\quad \bullet\ B \in Finite \Rightarrow \Sigma\ (\{x\} \times B)\ f = \Sigma\ B\ (\lambda\ y \bullet\ f\ (x, y))
\end{array}
$$

ind_sum_×_thm

$\vdash \forall f\ A\ B$
$\quad \bullet A \in Finite \land B \in Finite$
$\quad\quad \Rightarrow \Sigma\ A\ (\lambda\ x \bullet\ \Sigma\ B\ (\lambda\ y \bullet\ f\ (x,\ y))) = \Sigma\ (A \times B)\ f$

binomial_0_clauses

$\vdash \forall\ n \bullet\ Binomial\ n\ 0 = 1 \land Binomial\ 0\ (n + 1) = 0$

binomial_less_0_thm

$\vdash \forall\ n\ m \bullet\ n < m \Rightarrow Binomial\ n\ m = 0$

binomial_eq_thm

$\vdash \forall\ n \bullet\ Binomial\ n\ n = 1$

combinations_finite_size_thm

$\vdash \forall\ A\ n\ m$
$\quad \bullet A \in Finite \land \#\ A = n$
$\quad\quad \Rightarrow \{X | X \subseteq A \land \#\ X = m\} \in Finite$
$\quad\quad\quad \land \#\ \{X | X \subseteq A \land \#\ X = m\} = Binomial\ n\ m$

***binomial_thm*1**

$\vdash \forall\ x\ n$
$\quad \bullet (1. + x)\ \hat{}\ n$
$\quad\quad = Series\ (\lambda\ m \bullet\ \mathbb{NR}\ (Binomial\ n\ m) * x\ \hat{}\ m)\ (n + 1)$

binomial_thm

$\vdash \forall\ x\ y\ n$
$\quad \bullet (x + y)\ \hat{}\ n$
$\quad\quad = Series$
$\quad\quad\quad (\lambda\ m \bullet\ \mathbb{NR}\ (Binomial\ n\ m) * x\ \hat{}\ m * y\ \hat{}\ (n - m))$
$\quad\quad\quad (n + 1)$

factorial_not_0_thm

$\vdash \forall\ m \bullet\ \neg\ \mathbb{NR}\ (m\ !) = 0.$

factorial_times_thm

$\vdash \forall\ m$
$\quad \bullet \mathbb{NR}\ (m\ !) * \mathbb{NR}\ (m\ !)\ ^{-1} = 1.$
$\quad\quad \land \mathbb{NR}\ (m\ !)\ ^{-1} * \mathbb{NR}\ (m\ !) = 1.$

binomial_factorial_thm

$\vdash \forall\ m\ n$
$\quad \bullet \mathbb{NR}\ (Binomial\ (m + n)\ m)$
$\quad\quad = \mathbb{NR}\ ((m + n)\ !) * \mathbb{NR}\ (m\ !)\ ^{-1} * \mathbb{NR}\ (n\ !)\ ^{-1}$

enumerate_thm

$\vdash \exists\ enumerate$
$\quad \bullet \forall\ a$
$\quad\quad \bullet a \in Finite$
$\quad\quad\quad \Leftrightarrow (\forall\ i\ j$
$\quad\quad\quad\quad \bullet i < \#\ a$
$\quad\quad\quad\quad\quad \land j < \#\ a$
$\quad\quad\quad\quad\quad \land enumerate\ a\ i = enumerate\ a\ j$
$\quad\quad\quad\quad \Rightarrow i = j)$
$\quad\quad\quad \land a = \{x | \exists\ i \bullet\ i < \#\ a \land enumerate\ a\ i = x\}$

covering_finite_size_thm

$\vdash \forall\ a\ b\ f\ m$
$\quad \bullet a \in Finite$
$\quad\quad \land (\forall\ x \bullet\ x \in b \Rightarrow f\ x \in a)$
$\quad\quad \land (\forall\ y$
$\quad\quad \bullet y \in a$
$\quad\quad\quad \Rightarrow \{x | x \in b \land y = f\ x\} \in Finite$

$$\land \# \{x | x \in b \land y = f\ x\} = m) \Rightarrow b \in \mathit{Finite} \land \# b = m * \# a$$

samples_finite_size_thm

$$\vdash \forall a\ n \bullet a \in \mathit{Finite} \Rightarrow \{L | \mathit{Elems}\ L \subseteq a \land \# L = n\} \in \mathit{Finite} \land \# \{L | \mathit{Elems}\ L \subseteq a \land \# L = n\} = \# a \mathbin{\hat{}} n$$

distinct_samples_rw_thm

$$\vdash \forall n\ m \bullet \mathit{DistinctSamples}\ n\ m = (\mathit{if}\ m = 0\ \mathit{then}\ 1\ \mathit{else}\ (n + m) * \mathit{DistinctSamples}\ n\ (m - 1))$$

distinct_samples_up_thm

$$\vdash \forall n\ m \bullet \mathit{DistinctSamples}\ n\ (m + 1) = (n + 1) * \mathit{DistinctSamples}\ (n + 1)\ m$$

distinct_samples_finite_size_thm

$$\vdash \forall a\ n \bullet a \in \mathit{Finite} \land n \leq \# a \Rightarrow \{L | \mathit{Elems}\ L \subseteq a \land \# L = n \land L \in \mathit{Distinct}\} \in \mathit{Finite} \land \# \{L | \mathit{Elems}\ L \subseteq a \land \# L = n \land L \in \mathit{Distinct}\} = \mathit{DistinctSamples}\ (\# a - n)\ n$$

birthdays_thm

$$\vdash \mathit{let}\ S = \{L | \mathit{Elems}\ L \subseteq \{i | 1 \leq i \land i \leq 365\} \land \# L = 23\}\ \mathit{in}\ \mathit{let}\ X = \{L | L \in S \land \neg L \in \mathit{Distinct}\}\ \mathit{in}\ S \in \mathit{Finite} \land \neg \# S = 0 \land X \subseteq S \land \# X / \# S > 1 / 2$$

walk_thm

$$\vdash \forall n\ x \bullet \mathit{Walk}\ n\ x = \{s | \exists a \bullet (\forall m \bullet m \in a \Rightarrow m < n) \land (\forall m \bullet s\ m = x + \mathbb{NZ}\ (\# (\{k | k < m \land k < n\} \cap a)) - \mathbb{NZ}\ (\# (\{k | k < m \land k < n\} \setminus a)))\}$$

walk_to_thm

$$\vdash \forall n\ x\ y \bullet \mathit{WalkTo}\ n\ x\ y = \{s | \exists a \bullet (\forall m \bullet m \in a \Rightarrow m < n) \land (\forall m \bullet s\ m = x + \mathbb{NZ}\ (\# (\{k | k < m \land k < n\} \cap a)) - \mathbb{NZ}\ (\# (\{k | k < m \land k < n\} \setminus a)))$$

$$\land\ s\ n = y\}$$

walk_finite_size_thm

$$\vdash \forall\ n\ x \bullet\ Walk\ n\ x \in Finite \land \#\ (Walk\ n\ x) = 2\ \hat{}\ n$$

walk_to_finite_size_thm

$$\begin{array}{l}
\vdash \forall\ x\ m\ n \\
\quad \bullet\ WalkTo\ (m + n)\ x\ (x + \mathbb{NZ}\ m - \mathbb{NZ}\ n) \in Finite \\
\qquad \land\ \#\ (WalkTo\ (m + n)\ x\ (x + \mathbb{NZ}\ m - \mathbb{NZ}\ n)) \\
\qquad\quad = Binomial\ (m + n)\ m
\end{array}$$

walk_to_empty_thm

$$\begin{array}{l}
\vdash \forall\ n\ x\ y \\
\quad \bullet\ (\forall\ p\ q \bullet\ \neg\ (p + q = n \land y = x + \mathbb{NZ}\ p - \mathbb{NZ}\ q)) \\
\qquad \Leftrightarrow WalkTo\ n\ x\ y = \{\}
\end{array}$$

walk_to_finite_thm

$$\vdash \forall\ n\ x\ y \bullet\ WalkTo\ n\ x\ y \in Finite$$

walk_walk_to_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ x\ s \\
\quad \bullet\ m \le n \land s \in Walk\ n\ x \\
\qquad \Rightarrow (\lambda\ k \bullet\ if\ k \le m\ then\ s\ k\ else\ s\ m) \\
\qquad\quad \in WalkTo\ m\ x\ (s\ m)
\end{array}$$

walk_shift_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ x \\
\quad \bullet\ s \in Walk\ (m + n)\ x \\
\qquad \Rightarrow (\lambda\ k \bullet\ s\ (k + m)) \in Walk\ n\ (s\ m)
\end{array}$$

walk_minus_thm

$$\vdash \forall\ s\ n\ x \bullet\ s \in Walk\ n\ x \Rightarrow (\lambda\ k \bullet\ \sim (s\ k)) \in Walk\ n\ (\sim x)$$

walk_to_minus_thm

$$\begin{array}{l}
\vdash \forall\ s\ n\ x\ y \\
\quad \bullet\ s \in WalkTo\ n\ x\ y \\
\qquad \Rightarrow (\lambda\ k \bullet\ \sim (s\ k)) \in WalkTo\ n\ (\sim x)\ (\sim y)
\end{array}$$

walk_to_intermediate_value_thm

$$\begin{array}{l}
\vdash \forall\ n\ x\ y\ s\ z \\
\quad \bullet\ s \in WalkTo\ n\ x\ y \land (x \le z \land z \le y \lor y \le z \land z \le x) \\
\qquad \Rightarrow (\exists\ k \bullet\ k \le n \land s\ k = z)
\end{array}$$

walk_to_reflection_thm

$$\begin{array}{l}
\vdash \forall\ m\ n\ k\ z \\
\quad \bullet\ \mathbb{NZ}\ 0 < z \land 0 < k \land n < k + m \\
\qquad \Rightarrow \#\ (WalkTo\ (m + n)\ (\sim (\mathbb{NZ}\ k))\ z) \\
\qquad\quad = \# \\
\qquad\qquad \{s \\
\qquad\qquad\quad | s \in WalkTo\ (m + n)\ (\mathbb{NZ}\ k)\ z \\
\qquad\qquad\qquad \land\ (\exists\ i \bullet\ s\ i = \mathbb{NZ}\ 0)\}
\end{array}$$

***ballot_lemma*1**

$$\begin{array}{l}
\vdash \forall\ m\ n\ y \\
\quad \bullet\ \# \\
\qquad\quad \{s \\
\qquad\qquad | s \in WalkTo\ (m + n + 1)\ (\mathbb{NZ}\ 0)\ y \\
\qquad\qquad\quad \land\ (\forall\ i \bullet\ \mathbb{NZ}\ 0 < s\ (i + 1))\} \\
\qquad = \# \\
\qquad\quad \{s \\
\qquad\qquad | s \in WalkTo\ (m + n)\ (\mathbb{NZ}\ 1)\ y \\
\qquad\qquad\quad \land\ (\forall\ i \bullet\ \mathbb{NZ}\ 0 < s\ i)\}
\end{array}$$

ballot_lemma2

$$\begin{array}{l}
\vdash \forall\ m\ n \\
\quad \bullet\ 0 < n \land n < m + 1 \\
\qquad \Rightarrow \mathbb{NR} \\
\qquad\quad (\# \\
\qquad\qquad \{s \\
\qquad\qquad\ \ | s \\
\qquad\qquad\qquad \in WalkTo \\
\qquad\qquad\qquad\quad (m + n + 1) \\
\qquad\qquad\qquad\quad (\mathbb{NZ}\ 0) \\
\qquad\qquad\qquad\quad (\mathbb{NZ}\ (m + 1) - \mathbb{NZ}\ n) \\
\qquad\qquad\qquad \land (\forall\ i \bullet\ \mathbb{NZ}\ 0 < s\ (i + 1))\}) \\
\qquad\ = \mathbb{NR}\ (Binomial\ (m + n)\ m) \\
\qquad\quad - \mathbb{NR}\ (Binomial\ (m + n)\ (m + 1))
\end{array}$$

ballot_lemma3

$$\begin{array}{l}
\vdash \forall\ m\ n \\
\quad \bullet\ 0 < n \land n < m + 1 \\
\qquad \Rightarrow (\mathbb{NR}\ (Binomial\ (m + n)\ m) \\
\qquad\qquad - \mathbb{NR}\ (Binomial\ (m + n)\ (m + 1))) \\
\qquad\quad * \mathbb{NR}\ (Binomial\ (m + n + 1)\ (m + 1))\ ^{-1} \\
\qquad\ = ((m + 1) - n) / ((m + 1) + n)
\end{array}$$

ballot_lemma4

$$\vdash \forall\ m\ n \bullet\ \lnot\ \#\ (WalkTo\ (m + n)\ (\mathbb{NZ}\ 0)\ (\mathbb{NZ}\ m - \mathbb{NZ}\ n)) = 0$$

ballot_lemma5

$$\begin{array}{l}
\vdash \forall\ m \\
\quad \bullet\ (let\ S = WalkTo\ m\ (\mathbb{NZ}\ 0)\ (\mathbb{NZ}\ m) \\
\qquad in\ let\ X = \{s | s \in S \land (\forall\ i \bullet\ \mathbb{NZ}\ 0 < s\ (i + 1))\} \\
\qquad\ in\ 0 < m \Rightarrow X = S)
\end{array}$$

ballot_thm

$$\begin{array}{l}
\vdash \forall\ m\ n \\
\quad \bullet\ (let\ S = BallotCounts\ m\ n \\
\qquad in\ let\ X = \{s | s \in S \land (\forall\ i \bullet\ \mathbb{NZ}\ 0 < s\ (i + 1))\} \\
\qquad\ in\ S \in Finite \\
\qquad\quad \land \lnot\ \#\ S = 0 \\
\qquad\quad \land X \subseteq S \\
\qquad\quad \land (n < m \Rightarrow \#\ X / \#\ S = (m - n) / (m + n)))
\end{array}$$

zorn_thm2

$$\begin{array}{l}
\vdash \forall\ u \\
\quad \bullet\ \lnot\ u = \{\} \\
\qquad\ \land (\forall\ v \bullet\ \lnot\ v = \{\} \land v \subseteq u \land Nest\ v \Rightarrow \bigcup\ v \in u) \\
\qquad \Rightarrow (\exists\ a \bullet\ Maximal_{\subseteq}\ u\ a)
\end{array}$$

fund_region_thm

$$\begin{array}{l}
\vdash \forall\ f\ X \\
\quad \bullet\ f \in Involution\ X \\
\qquad \Rightarrow (\exists\ A \\
\qquad \bullet\ A \subseteq X \\
\qquad\quad \land (\forall\ x \\
\qquad\quad \bullet\ (x \in A \Rightarrow \lnot\ f\ x \in A) \\
\qquad\qquad \land (x \in X \land \lnot\ x \in A \land \lnot\ f\ x \in A \\
\qquad\qquad\quad \Rightarrow x \in Fixed\ f)))
\end{array}$$

involution_one_one_thm

$$\begin{array}{l}
\vdash \forall\ f\ X\ x\ y \\
\quad \bullet\ f \in Involution\ X \land x \in X \land y \in X \land f\ x = f\ y
\end{array}$$

$\Rightarrow x = y$

involution_def_thm1

$\vdash \forall f\ X\ x \bullet f \in Involution\ X \land x \in X \Rightarrow f\ (f\ x) = x$

involution_def_thm2

$\vdash \forall f\ X\ x \bullet f \in Involution\ X \land x \in X \Rightarrow f\ x \in X$

involution_size_thm

$\vdash \forall f\ X$
$\bullet f \in Involution\ X$
$\land X \in Finite$
$\land A \subseteq X$
$\land (\forall x \bullet x \in A \Rightarrow \neg f\ x \in A)$
$\land (\forall x \bullet x \in X \Rightarrow x \in A \lor f\ x \in A)$
$\Rightarrow \#\ X = 2 * \#\ A$

involution_even_size_thm

$\vdash \forall f\ X$
$\bullet f \in Involution\ X \land X \in Finite \land X \cap Fixed\ f = \{\}$
$\Rightarrow (\exists k \bullet \#\ X = 2 * k)$

involution_odd_size_thm

$\vdash \forall f\ X\ k$
$\bullet f \in Involution\ X \land X \in Finite \land \#\ X = 2 * k + 1$
$\Rightarrow \neg X \cap Fixed\ f = \{\}$

involution_set_dif_fixed_thm

$\vdash \forall f\ X\ k$
$\bullet f \in Involution\ X \Rightarrow f \in Involution\ (X \setminus Fixed\ f)$

involution_fixed_singleton_thm

$\vdash \forall f\ X\ x$
$\bullet f \in Involution\ X \land X \in Finite \land X \cap Fixed\ f = \{x\}$
$\Rightarrow (\exists k \bullet \#\ X = 2 * k + 1)$

ℤ_interval_finite_thm

$\vdash \forall m\ n \bullet \{i | m \leq i \land i \leq n\} \in Finite$

ℤ_0_≤_square_thm

$\vdash \forall i \bullet \mathbb{NZ}\ 0 \leq i * i$

ℤ_0_less_0_less_times_thm

$\vdash \forall i\ j \bullet \mathbb{NZ}\ 0 < i \land \mathbb{NZ}\ 0 < j \Rightarrow \mathbb{NZ}\ 0 < i * j$

ℤ_0_less_times_thm

$\vdash \forall i\ j \bullet \mathbb{NZ}\ 0 < i \land \mathbb{NZ}\ 0 < j \Rightarrow j \leq i * j$

ℤ_0_less_times_thm1

$\vdash \forall i\ j \bullet \mathbb{NZ}\ 0 < i \land \mathbb{NZ}\ 0 < j \Rightarrow j \leq j * i$

ℤ_≤_square_thm

$\vdash \forall i \bullet i \leq i * i$

a_finite_thm $\vdash \forall p\ A$
$\bullet A$
$= \{(x, y, z)$
$| \mathbb{NZ}\ 0 < x$
$\land \mathbb{NZ}\ 0 < y$
$\land \mathbb{NZ}\ 4 * x * y + z * z = p\}$
$\Rightarrow A \in Finite$

f_involution_a_thm

$\vdash \forall p\ A\ f$
$\bullet A$
$= \{(x, y, z)$

$$
\begin{array}{l}
\quad |\mathbb{N}\mathbb{Z}\ \mathit{0} < x \\
\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{0} < y \\
\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{4} * x * y + z * z = p\} \\
\Rightarrow (\lambda\ (x,\ y,\ z)\bullet\ (y,\ x,\ \sim z)) \in \mathit{Involution}\ A
\end{array}
$$

size_a_size_b_thm

$$
\begin{array}{l}
\vdash \forall\ p\ m\ A\ B \\
\quad \bullet\ p = \mathbb{N}\mathbb{Z}\ \mathit{4} * m + \mathbb{N}\mathbb{Z}\ \mathit{1} \\
\qquad \wedge\ A \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |\mathbb{N}\mathbb{Z}\ \mathit{0} < x \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{0} < y \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{4} * x * y + z * z = p\} \\
\qquad \wedge\ B = \{(x,\ y,\ z) | (x,\ y,\ z) \in A \wedge z > \mathbb{N}\mathbb{Z}\ \mathit{0}\} \\
\quad \Rightarrow \#\ A = \mathit{2} * \#\ B
\end{array}
$$

size_a_size_c_thm

$$
\begin{array}{l}
\vdash \forall\ p\ A\ C \\
\quad \bullet\ (\forall\ i\bullet\ \neg\ p = i * i) \\
\qquad \wedge\ A \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |\mathbb{N}\mathbb{Z}\ \mathit{0} < x \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{0} < y \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{4} * x * y + z * z = p\} \\
\qquad \wedge\ C \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |(x,\ y,\ z) \in A \wedge x - y + z > \mathbb{N}\mathbb{Z}\ \mathit{0}\} \\
\quad \Rightarrow \#\ A = \mathit{2} * \#\ C
\end{array}
$$

size_b_size_c_thm

$$
\begin{array}{l}
\vdash \forall\ p\ m\ A\ B\ C \\
\quad \bullet\ p = \mathbb{N}\mathbb{Z}\ \mathit{4} * m + \mathbb{N}\mathbb{Z}\ \mathit{1} \\
\qquad \wedge\ (\forall\ i\bullet\ \neg\ p = i * i) \\
\qquad \wedge\ A \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |\mathbb{N}\mathbb{Z}\ \mathit{0} < x \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{0} < y \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{4} * x * y + z * z = p\} \\
\qquad \wedge\ B = \{(x,\ y,\ z) | (x,\ y,\ z) \in A \wedge z > \mathbb{N}\mathbb{Z}\ \mathit{0}\} \\
\qquad \wedge\ C \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |(x,\ y,\ z) \in A \wedge x - y + z > \mathbb{N}\mathbb{Z}\ \mathit{0}\} \\
\quad \Rightarrow \#\ B = \#\ C
\end{array}
$$

g_involution_c_thm

$$
\begin{array}{l}
\vdash \forall\ p\ A\ C \\
\quad \bullet\ A \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |\mathbb{N}\mathbb{Z}\ \mathit{0} < x \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{0} < y \\
\qquad\qquad \wedge\ \mathbb{N}\mathbb{Z}\ \mathit{4} * x * y + z * z = p\} \\
\qquad \wedge\ C \\
\qquad\quad = \{(x,\ y,\ z) \\
\qquad\quad |(x,\ y,\ z) \in A \wedge x - y + z > \mathbb{N}\mathbb{Z}\ \mathit{0}\} \\
\quad \Rightarrow (\lambda\ (x,\ y,\ z)\bullet\ (x - y + z,\ y,\ \mathbb{N}\mathbb{Z}\ \mathit{2} * y - z))
\end{array}
$$

$\in Involution\ C$

size_c_thm $\vdash \forall\ p\ m\ A\ C$

$\bullet\ p = \mathbb{NZ}\ 4 * m + \mathbb{NZ}\ 1$
$\land\ \mathbb{NZ}\ 1 < p$
$\land\ (\forall\ a\ b$
$\bullet\ \mathbb{NZ}\ 0 < a \land \mathbb{NZ}\ 0 < b \land p = (\mathbb{NZ}\ 4 * a + b) * b$
$\Rightarrow b = \mathbb{NZ}\ 1)$
$\land\ A$
$= \{(x,\ y,\ z)$
$| \mathbb{NZ}\ 0 < x$
$\land\ \mathbb{NZ}\ 0 < y$
$\land\ \mathbb{NZ}\ 4 * x * y + z * z = p\}$
$\land\ C$
$= \{(x,\ y,\ z)$
$|(x,\ y,\ z) \in A \land x - y + z > \mathbb{NZ}\ 0\}$
$\Rightarrow (\exists\ k \bullet\ \#\ C = 2 * k + 1)$

h_involution_b_thm

$\vdash \forall\ p\ A\ B$
$\bullet\ A$
$= \{(x,\ y,\ z)$
$| \mathbb{NZ}\ 0 < x$
$\land\ \mathbb{NZ}\ 0 < y$
$\land\ \mathbb{NZ}\ 4 * x * y + z * z = p\}$
$\land\ B = \{(x,\ y,\ z)|(x,\ y,\ z) \in A \land z > \mathbb{NZ}\ 0\}$
$\Rightarrow (\lambda\ (x,\ y,\ z) \bullet\ (y,\ x,\ z)) \in Involution\ B$

h_fixed_in_b_thm

$\vdash \forall\ p\ m\ A\ B$
$\bullet\ p = \mathbb{NZ}\ 4 * m + \mathbb{NZ}\ 1$
$\land\ \mathbb{NZ}\ 1 < p$
$\land\ (\forall\ i \bullet\ \neg\ p = i * i)$
$\land\ (\forall\ a\ b$
$\bullet\ \mathbb{NZ}\ 0 < a \land \mathbb{NZ}\ 0 < b \land p = (\mathbb{NZ}\ 4 * a + b) * b$
$\Rightarrow b = \mathbb{NZ}\ 1)$
$\land\ A$
$= \{(x,\ y,\ z)$
$| \mathbb{NZ}\ 0 < x$
$\land\ \mathbb{NZ}\ 0 < y$
$\land\ \mathbb{NZ}\ 4 * x * y + z * z = p\}$
$\land\ B = \{(x,\ y,\ z)|(x,\ y,\ z) \in A \land z > \mathbb{NZ}\ 0\}$
$\Rightarrow \neg\ B \cap Fixed\ (\lambda\ (x,\ y,\ z) \bullet\ (y,\ x,\ z)) = \{\}$

two_squares_lemma

$\vdash \forall\ p\ m$
$\bullet\ p = \mathbb{NZ}\ 4 * m + \mathbb{NZ}\ 1$
$\land\ \mathbb{NZ}\ 1 < p$
$\land\ (\forall\ i \bullet\ \neg\ p = i * i)$
$\land\ (\forall\ a\ b$
$\bullet\ \mathbb{NZ}\ 0 < a \land \mathbb{NZ}\ 0 < b \land p = (\mathbb{NZ}\ 4 * a + b) * b$
$\Rightarrow b = \mathbb{NZ}\ 1)$
$\Rightarrow (\exists\ a\ b \bullet\ p = a * a + b * b)$

B THEOREMS IN THE THEORY infcomb

infinite_thm $\vdash \forall\ a\bullet\ a \in \mathit{Infinite} \Leftrightarrow (\exists\ f\bullet\ \mathit{OneOne}\ f \land (\forall\ i\bullet\ f\ i \in a))$

infinite_non_empty_thm

$\vdash \forall\ a\bullet\ a \in \mathit{Infinite} \Rightarrow (\exists\ x\bullet\ x \in a)$

ℕ***_infinite_thm***

$\vdash \mathit{Universe} \in \mathit{Infinite}$

infinite_diff_finite_thm

$\vdash \forall\ a\ b\bullet\ a \in \mathit{Infinite} \land b \in \mathit{Finite} \Rightarrow a \setminus b \in \mathit{Infinite}$

min_infinite_thm

$\vdash \forall\ a$
$\bullet\ a \in \mathit{Infinite} \Rightarrow \mathit{Min}\ a \in a \land (\forall\ i\bullet\ i \in a \Rightarrow \mathit{Min}\ a \le i)$

infinite_diff_singleton_thm

$\vdash \forall\ a\ x\bullet\ a \in \mathit{Infinite} \Rightarrow a \setminus \{x\} \in \mathit{Infinite}$

infinite_unbounded_thm

$\vdash \forall\ a\ i\bullet\ a \in \mathit{Infinite} \Rightarrow (\exists\ j\bullet\ j \in a \land i < j)$

infinite_one_one_image_thm

$\vdash \forall\ a\ f$
$\bullet\ a \in \mathit{Infinite} \land \mathit{OneOne}\ f$
$\Rightarrow \{y | \exists\ x\bullet\ x \in a \land y = f\ x\} \in \mathit{Infinite}$

ordered_enumeration_thm

$\vdash \forall\ a$
$\bullet\ a \in \mathit{Infinite}$
$\Rightarrow (\exists\ f$
$\bullet\ a = \{i | \exists\ m\bullet\ f\ m = i\}$
$\land (\forall\ m\ n\bullet\ m < n \Rightarrow f\ m < f\ n))$

infinite_pigeon_hole_thm

$\vdash \forall\ a\ b\ f$
$\bullet\ a \in \mathit{Infinite} \land b \in \mathit{Finite} \land (\forall\ x\bullet\ x \in a \Rightarrow f\ x \in b)$
$\Rightarrow (\exists\ y\bullet\ y \in b \land \{x | x \in a \land f\ x = y\} \in \mathit{Infinite})$

infinite_ramsey_thm

$\vdash \forall\ n\ X\ C\ m$
$\bullet\ X \in \mathit{Infinite} \land (\forall\ a\bullet\ C\ a < m)$
$\Rightarrow (\exists\ Y\ c$
$\bullet\ Y \subseteq X$
$\land\ Y \in \mathit{Infinite}$
$\land\ c < m$
$\land (\forall\ a$
$\bullet\ a \subseteq Y \land a \in \mathit{Finite} \land \#\ a = n \Rightarrow C\ a = c))$

INDEX