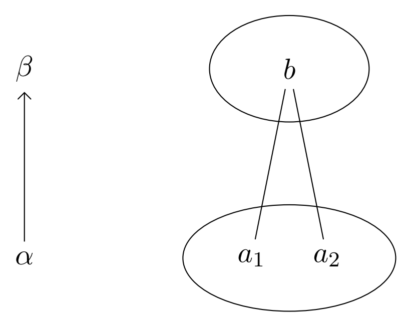
Пусть B некоторое множество. Через P^+B обозначим множество всех непустых подмножеств B.
Функцию $c\colon P^+B \to B$ назовём функцией выбора для B, если
$c(X) \in X$ для любого $X \in P^+B$
Аксиома выбора утверждает, что для любого множества есть функция выбора. Докажем, что из аксиомы выбора следует закон исключённого третьего (в интуиционистской теории множеств). Пусть дана некоторая формула ϕ, докажем $\phi \vee \neg\phi$
Возьмём множество $B = \{0,1\} = \{x \mid x = 0 \vee x = 1\}$
Возьмём два его подмножества
$B_0 = \{x \mid x = 0 \vee (x = 1 \wedge \phi)\}$
$B_1 = \{x \mid (x = 0 \wedge \phi) \vee x = 1\}$
Если для множества B есть функция выбора, применим её к B_0 и B_1.
Если результаты равны
$c(B_0) = c(B_1)$ то верна ϕ. В самом деле, если
$c(B_0) = c(B_1) = 0$
то множество B_1 содержит 0, из чего следует ϕ. Если же
$c(B_0) = c(B_1) = 1$
то множество B_0 содержит 1, из чего следует ϕ.
Если же
$c(B_0) \neq c(B_1)$ то $\neg\phi$. В самом деле, если ϕ верна, то
$B_0 = B_1 = \{0,1\}$ и поэтому должно быть $c(B_0) = c(B_1)$.

Линейно упорядоченное множество B называется вполне упорядоченным, если в каждом его непустом подмножестве есть наименьший элемент. На самом деле линейность, а также рефлексивность и транзитивность порядка следуют из наличия наименьших элементов. Рефлексивность $x \leqslant x$ следует из наличия наименьшего элемента во множестве $\{x\}$. Линейность $x \leqslant y \vee y \leqslant x$ следует из наличия наименьшего элемента во множестве $\{x,y\}$. Транзитивность следует из наличия наименьшего элемента во множестве $\{x,y,z\}$ (упражнение). Таким образом, нужна только антисимметричность $x \leqslant y \wedge y \leqslant x \Rightarrow x = y$ и принцип наименьшего элемента.
Ясно, что для вполне упорядоченного множества есть функция выбора. Цермело доказал обратное - если для множества есть функция выбора, то его можно вполне упорядочить. Интересно, что вполне упорядочиваемость множества равносильна наличию функции выбора с дополнительным свойством
$c(B_1 \cup B_2) = c\{c(B_1), c(B_2)\}$
Тогда можно определить $x \leqslant y$ как $x = c\{x,y\}$ и доказать, что получается

линейный порядок и $c(B_1) \leqslant y$ для любого $y \in B_1$ (упражнение).
Вернёмся к теореме Цермело. Есть глобальный её вариант "если для каждого множества есть функция выбора, то каждое множество можно вполне упорядочить". В такой форме его можно доказать и в интуиционистской теории множеств, поскольку из аксиомы выбора следует закон исключённого третьего и проходит классическое доказательство. Но есть локальный вариант "если для некоторого множества B есть функция выбора, то это множество B можно вполне упорядочить". В этом случае у нас, вообще говоря, нет функции выбора для $\{0, 1\}$ и мы не можем доказать закон исключённого третьего. Заметим, что если во множестве B есть два разных элемента (обозначим их 0 и 1), мы можем взять множество $\{x \in B \mid x = 0 \vee x = 1\}$ и доказать закон исключённого третьего. Поэтому все проблемы связаны с множествами, в которых нет двух разных элементов. Классически из $\neg\exists x, y \in B\,(x \neq y)$ следует
$\forall x, y \in B\,(x = y)$. Такое множество одноэлементно или пусто и вполне упорядочено отношением равенства. Но в интуиционистском случае мы можем вывести только $\forall x, y \in B\,(\neg\neg x = y)$. Множества с таким свойством могут быть очень хитро устроены (вот простая модель Крипке с двумя моментами времени)



Заметим также, что вполне упорядочиваемость с интуиционистской точки зрения свойство очень сильное. Например, натуральный ряд им не обладает (в интуиционистской теории множеств нельзя доказать, что в каждом непустом множестве натуральных чисел есть наименьший элемент).

Идея классического доказательства такова. Пусть множество B непусто (если пусто, то оно уже вполне упорядочено). Применим к нему функцию выбора

$b_0 = c(B)$ и это будет наименьший элемент. Выбросим его
$B' = B - \{b_0\}$
Если B' не пусто, применим функцию выбора снова

$b_1 = c(B')$ и это будет следующий элемент. Выбросим его
$B'' = B' - \{b_1\} = B - \{b_0, b_1\}$
и так далее выбираем элемент за элементом, пока они не кончатся. Если выбрали уже бесконечно много элементов $b_0, b_1, b_2 \ldots$, выбросим их все
$B^\omega = B - \{b_0, b_1, b_2 \ldots\} = B \cap B' \cap B'' \cap \ldots$ и продолжаем применять функцию выбора
$b_\omega = c(B^\omega)$
пока все элементы не кончатся. Заметим, что относительно полученного порядка $b_0 < b_1 < b_2 < \ldots < b_\omega < \ldots$ множества $B, B', B'', \ldots B^\omega \ldots$ являются верхними сегментами
$B = \{b_0, b_1, b_2, \ldots b_\omega \ldots\}$
$B' = \{b_1, b_2, \ldots b_\omega \ldots\}$
$B'' = \{b_2, \ldots b_\omega \ldots\}$
и т.д., то есть каждое из них вместе с любым своим элементом содержит все большие его.

Формализуем это доказательство. Пусть $M \subseteq PB$ есть наименьшее семейство подмножеств B со следующими свойствами
(a) $B \in M$
(b) если $X \in M$ и X не пусто, то $X' \in M$, где
$X' = X - \{c(X)\} = \{x \in X \mid x \neq c(X)\}$
(c) если $N \subseteq M$ и N не пусто, то $\cap N \in M$
Условие (b) мы сразу перепишем так, чтобы оно годилось и для пустых подмножеств (иначе будут трудности при интуиционистском доказательстве, потому что нельзя эффективно проверить, пусто некоторое множество или нет). По функции выбора
$c\colon P^+B \to B$
определим функцию
$\hat{c}\colon PB \to PB$
$\hat{c}(X) = \{x \in X \mid x = c(X)\}$
это множество состоит из одного элемента $\{c(X)\}$ если X не пусто и равно $\emptyset$ в противном случае. Перепишем условие (b) так
(b) если $X \in M$, то $X' \in M$, где
$X' = \{x \in X \mid x \notin \hat{c}(X)\}$

Поскольку M определяется как наименьшее семейство, порождённое некоторыми операциями, для него верен соответствующий принцип индукции. А именно, если $L \subseteq PM$ обладает теми же свойствами замкнутости
(a) $B \in L$
(b) если $X \in L$, то $X' \in L$, где $X' = \{x \in X \mid x \notin \hat{c}(X)\}$

(c) если $N \subseteq L$ и N не пусто, то $\cap N \in L$
то $M \subseteq L$.
Теперь мы докажем некоторый принцип индукции, на первый взгляд более сильный (на самом деле нет), который Todd Wilson называет "индукцией Смальяна". Пусть дано отношение $R \subseteq M \times M$ с такими свойствами
(a) $R(X, B)$ для всех $X \in M$
(b) если $R(X, Y)$ и $R(Y, X)$, то $R(X, Y')$ для любых $X, Y \in M$
(c) для всякого $X \in M$ и всякого непустого семейства $N \subseteq M$ из $\forall Y \in N\, R(X, Y)$ следует $R(X, \cap N)$
тогда $R = M \times M$, то есть верно $R(X, Y)$ для любых $X, Y \in M$.
Для доказательства предположим, что верны посылки (a),(b),(c) индукции Смальяна. Обозначим L семейство таких $Y \in M$, что $\forall X \in M\, R(X, Y)$.
Докажем обычной индукцией, что $M \subseteq L$. Посылки (a),(c) обычной индукции непосредственно следуют из посылок (a),(c) индукции Смальяна, которые мы предположили верными. Чтобы доказать посылку (b) обычной индукции (если $Y \in L$, то $Y' \in L$), докажем сначала, что для всякого $Y \in M$ из $\forall X \in M\, R(X, Y)$ следует $\forall X \in M\, R(Y, X)$
Мы предположим, что $\forall X \in M\, R(X, Y)$ и $X \in M$ и докажем $R(Y, X)$ простой индукцией по X
(a) $R(Y, B)$ в силу первой посылки индукции Смальяна
(b) если $R(Y, X)$ то $R(Y, X')$, поскольку $R(X, Y)$ тоже верно (мы предположили $\forall X \in M\, R(X, Y)$) и можно использовать вторую посылку индукции Смальяна
(c) в силу третьей посылки индукции Смальяна
Будем считать, что индукция Смальяна обоснована.

Теперь с помощью индукции Смальяна мы докажем важную лемму. Пусть $X, Y \in M$ и X не пусто. Тогда из $c(X) \in Y$ следует $X \subseteq Y$. Содержательно, потому что элементы M – это верхние сегменты, а $c(X)$ – наименьший элемент X (но мы порядок ещё не определили). Для $X, Y \in M$ определим отношение
$R(X, Y) := (X \in P^+B \wedge c(X) \in Y) \Rightarrow X \subseteq Y$
и докажем для него посылки индукции Смальяна
(a) $R(X, B)$ есть $(X \in P^+B \wedge c(X) \in B) \Rightarrow X \subseteq B$
и оно верно, поскольку $X \subseteq B$
(c) в качестве упражнения
(b) а вот это трудно. Из $R(X, Y)$ и $R(Y, X)$ надо вывести $R(X, Y')$, которое выглядит так
$(X \in P^+B \wedge c(X) \in Y') \Rightarrow X \subseteq Y'$
Пишем вывод в виде таблицы (Фитча)

1	$(X \in P^{+}B \wedge c(X) \in Y) \Rightarrow X \subseteq Y$	посылка $R(X,Y)$
2	$(Y \in P^{+}B \wedge c(Y) \in X) \Rightarrow Y \subseteq X$	посылка $R(Y,X)$
3	$X \in P^{+}B$	
4	$c(X) \in Y'$	
5	$x \in X$	гипотеза, сейчас докажем $x \in Y'$
6	$c(X) \in Y$	из 4 с учётом $Y' \subseteq Y$
7	$X \subseteq Y$	из 1,3,6
8	$x \in Y$	из 5,7
9	$x = c(Y)$	новая гипотеза, сейчас приведём к противоречию
10	$Y \in P^{+}B$	из 8 (или 6)
11	$c(Y) \in X$	из 5,9
12	$Y \subseteq X$	из 2,10,11
13	$X = Y$	из 7,12
14	$c(X) = c(Y)$	из 13
15	$c(Y) \in Y'$	из 4,14 противоречие с $Y' = Y - \{c(Y)\}$
16	$x \neq c(Y)$	9-15
17	$x \in Y'$	из 8,16
18	$X \subseteq Y'$	из 5-17

Лемма доказана. Сейчас ещё одна лемма и можно определять порядок.
Определим операцию на подмножествах B
$R\colon PB \to PB$
$R(X) = \cap\{Y \in M \mid X \subseteq Y\}$
(не очень разумно опять использовать букву R в совершенно новом смысле, но я сохраняю обозначения Тодда Вилсона).
Содержательно, $R(X)$ есть пересечение всех верхних сегментов, содержащих X (наименьший верхний сегмент, содержащий X). Видимо, очевидно (или постигается минутным размышлением), что $X \subseteq R(X)$
Также $R(X) \in M$ как пересечение непустого семейства элементов M (непустое, потому что содержит B). Докажем, что если $R(X)$ не пусто, то $c(R(X)) \in X$. Доказывать будем от противного.
Предположим, что $R(X)$ не пусто и $c(R(X)) \notin X$.
Тогда $X \subseteq R(X) - \{c(R(X))\}$ то есть $X \subseteq R(X)'$
Поскольку $R(X)' \in M$ и при этом $R(X)$ является наименьшим элементом M, содержащим X в качестве подмножества, получаем
$R(X) \subseteq R(X)'$
Из этого и $c(R(X)) \in R(X)$ получаем противоречие
$c(R(X)) \in R(X)'$
От противного заключаем, что $c(R(X)) \in X$

Определяем порядок на B
$x \leqslant y \Leftrightarrow \forall Z \in M\,(x \in Z \Rightarrow y \in Z)$

Докажем, что в каждом непустом подмножестве есть наименьший элемент.
Пусть $X \in P^+B$. Докажем, что $c(R(X)) \leqslant x$ для любого $x \in X$.
Надо доказать, что для любого $x \in X$
$\forall Z \in M\,(c(R(X)) \in Z \Rightarrow x \in Z)$
Но у нас есть "важная лемма", что из $c(R(X)) \in Z$ следует $R(X) \subseteq Z$ и поэтому $X \subseteq Z$, поэтому $x \in Z$.

Наконец, докажем антисимметричность. Если $x \leqslant y$ и $y \leqslant x$ то
$\forall Z \in M(x \in Z \Leftrightarrow y \in Z)$
Предположим, что $x \neq y$ (от противного). Возьмём множество $Z = R(\{x, y\})$, применим к нему функцию выбора
$c(Z) \in \{x, y\}$ то есть $c(Z)$ равен x или y, делаем разбор случаев.
Если $c(Z) = x \neq y$ то $y \in Z - \{c(Z)\}$, то есть $y \in Z'$
Но тогда и $x \in Z'$, поскольку $x \in Z' \Leftrightarrow y \in Z'$
Получили противоречие, поскольку $Z' = Z - \{x\}$
Если $c(Z) = y \neq x$ то $x \in Z - \{c(Z)\}$, то есть $x \in Z'$

Но тогда и $y \in Z'$, поскольку $x \in Z' \Leftrightarrow y \in Z'$
Получили противоречие, поскольку $Z' = Z - \{y\}$

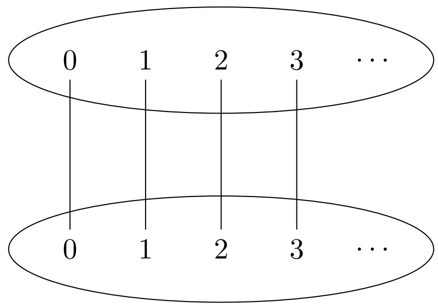
Всё, классическое доказательство локальной теоремы Цермело закончено. Дважды мы что-то доказывали от противного. Теперь мы внесём в доказательство небольшие изменения и оно станет чисто интуиционистским.
Вместо одной операции
$X' = \{x \in X \mid x \neq c(X)\}$
мы будем рассматривать семейство операций
$X^\theta = \{x \in X \mid x = c(X) \Rightarrow \theta\}$
для каждого значения истинности θ. Значения истинности можно понимать как элементы множества $P\{*\}$ (множество подмножеств одноэлементного множества $\{*\}$). Каждому подмножеству $u \in P\{*\}$ соответствует формула $* \in u$ и каждой формуле θ соответствует подмножество $\{x \mid \theta\}$, эти операции взаимно обратны (упражнение). Заметим, что
$X' = X^\perp = \{x \in X \mid x = c(X) \Rightarrow \perp\}$
Опять же, чтобы не делать разницы между пустыми и непустыми подмножествами, мы будем писать
$X^\theta = \{x \in X \mid x \in \hat{c}(X) \Rightarrow \theta\}$
Семейство $M \subseteq PB$ определяем как наименьшее семейство со следующими свойствами замкнутости
(a) $B \in M$
(b) если $X \in M$, то $X^\theta \in M$ для любого θ
(c) если $N \subseteq M$ и N не пусто, то $\cap N \in M$
Вторая посылка индукции Смальяна выглядит так
(b) если $R(X, Y)$ и $R(Y, X)$, то $R(X, Y^\theta)$ для любых $X, Y \in M$ и любого θ
Доказательство "важной леммы" почти не меняется (добавляется одна строчка в конце). Мы выводим из посылок
$(X \in P^+B \wedge c(X) \in Y) \Rightarrow X \subseteq Y$
$(Y \in P^+B \wedge c(Y) \in X) \Rightarrow Y \subseteq X$
следствие
$(X \in P^+B \wedge c(X) \in Y^\theta) \Rightarrow X \subseteq Y^\theta$

1	$(X \in P^+B \wedge c(X) \in Y) \Rightarrow X \subseteq Y$	посылка $R(X, Y)$
2	$(Y \in P^+B \wedge c(Y) \in X) \Rightarrow Y \subseteq X$	посылка $R(Y, X)$
3	$X \in P^+B$	
4	$c(X) \in Y^\theta$	
5	$x \in X$	гипотеза, сейчас докажем $x \in Y^\theta$
6	$c(X) \in Y$	из 4 с учётом $Y^\theta \subseteq Y$
7	$X \subseteq Y$	из 1,3,6
8	$x \in Y$	из 5,7
9	$x = c(Y)$	новая гипотеза, сейчас выведем θ
10	$Y \in P^+B$	из 8 (или 6)
11	$c(Y) \in X$	из 5,9
12	$Y \subseteq X$	из 2,10,11
13	$X = Y$	из 7,12
14	$c(X) = c(Y)$	из 13
15	$c(Y) \in Y^\theta$	из 4,14
16	θ	из 15 с учётом $Y^\theta = \{y \in Y \mid y = c(Y) \Rightarrow \theta\}$
17	$x = c(Y) \Rightarrow \theta$	9-16
18	$x \in Y^\theta$	из 8,17
19	$X \subseteq Y^\theta$	из 5-18

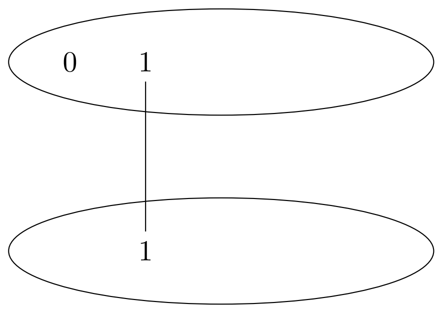
И теперь два места, которые мы доказывали от противного, мы докажем от приятного. Напомню, что операция R определялась так
$R\colon PB \to PB$
$R(X) = \cap\{Y \in M \mid X \subseteq Y\}$
и это наименьший элемент M (верхний сегмент), содержащий X.
Докажем, что если $R(X)$ не пусто, то $c(R(X)) \in X$.
Предположим, что $R(X)$ не пусто. Возьмём в качестве θ формулу $c(R(X)) \in X$, мы хотим доказать θ.
Напомним, что $R(X)^\theta = \{x \in R(X) \mid x = c(R(X)) \Rightarrow \theta\}$
Поскольку для любого $x \in X$ из $x = c(R(X))$ следует θ, мы имеем $X \subseteq R(X)^\theta$
Поскольку $R(X)^\theta \in M$ и при этом $R(X)$ является наименьшим элементом M, содержащим X в качестве подмножества, получаем
$R(X) \subseteq R(X)^\theta$
Из этого и $c(R(X)) \in R(X)$ получаем $c(R(X)) \in R(X)^\theta$ и из этого θ.

Наконец, докажем антисимметричность. Если $x \leqslant y$ и $y \leqslant x$ то
$\forall Z \in M (x \in Z \Leftrightarrow y \in Z)$
Возьмём множество
$Z = R(\{x, y\})$, применим к нему функцию выбора
$c(Z) \in \{x, y\}$
В качестве θ возьмём формулу $x = y$, мы хотим доказать θ.
$c(Z)$ равен x или y, делаем разбор случаев.
Если $c(Z) = x$ то $y = c(Z) \Rightarrow \theta$, поэтому $y \in \{z \in Z \mid z = c(Z) \Rightarrow \theta\}$, то есть $y \in Z^\theta$
Но тогда и $x \in Z^\theta$, поскольку $x \in Z^\theta \Leftrightarrow y \in Z^\theta$
Из $x \in Z^\theta$ следует θ, поскольку $Z^\theta = \{z \in Z \mid z = x \Rightarrow \theta\}$
Если $c(Z) = y$ то $x = c(Z) \Rightarrow \theta$, поэтому $x \in \{z \in Z \mid z = c(Z) \Rightarrow \theta\}$, то есть $x \in Z^\theta$
Но тогда и $y \in Z^\theta$, поскольку $x \in Z^\theta \Leftrightarrow y \in Z^\theta$
Из $y \in Z^\theta$ следует θ, поскольку $Z^\theta = \{z \in Z \mid z = y \Rightarrow \theta\}$

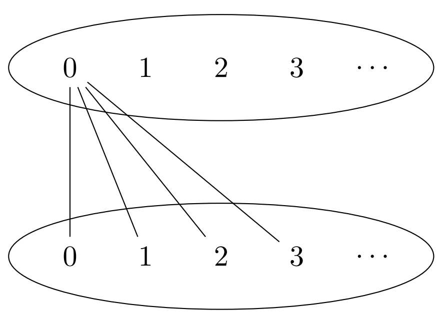
Напоследок пара примеров с моделями Крипке. Возьмём простейшую шкалу из двух моментов времени, объект натуральных чисел выглядит так



Возьмём в нём такой подобъект (подмножество)



Оно не пусто (в каждый момент времени), но в нём нет наименьшего элемента. Наименьший (единственный) элемент 1 в нижний момент времени перестаёт быть наименьшим в верхний. Итого, множество натуральных чисел не вполне упорядочено в этой модели Крипке (что не удивительно, потому что в нём есть два разных элемента, а закон исключённого третьего для этой шкалы не верен). Все вполне упорядоченные множества для этой шкалы выглядят примерно так



Снизу может быть любое вполне упорядоченное множество и сверху любое (не обязательно то же самое), но все элементы нижнего множества должны переходить в наименьший элемент верхнего.