Anhang B

Konservative Erweiterungen der Typentheorie und ihre Gesetze

Achtung: Dieser Teil wurde relativ zügig aus einer alten Quelle zusammengestellt und könnte divese kleine Fehler enthalten. Für Hinweise bin ich dankbar.

B.1 Endliche Mengen

Der Typ der endlichen Mengen ist ein generischer Datentyp, der auf der Basis der Konzepte Set, =, $\emptyset$, + und $\in$ eingeführt werden kann. Die einfachste Form einer Implementierung ist eine Simulation durch Listen modulo einer neuen Definition der Gleichheit.

BASISKONZEPTE

Definition B.1.1 (Beschränkte Boole'sche Quantoren)

$\forall x \in S.p_x \equiv \texttt{list\_ind}(S;\texttt{true};\texttt{a,\_,pS'.pS'}\wedge p_x\texttt{[a/}x\texttt{]})$

$\exists x \in S.p_x \equiv \texttt{list\_ind}(S;\texttt{false};\texttt{a,\_,pS'.pS'}\vee p_x\texttt{[a/}x\texttt{]})$

Definition B.1.2 (Implementierung endlicher Mengen)

$\emptyset \equiv \texttt{[]}$

$+ \equiv \lambda\texttt{a,S. a.S}$

$\in_\alpha \equiv \lambda\texttt{a,S. }\exists\texttt{x}\in\texttt{S.x}\underset{\alpha}{=}\texttt{a}$

$\underset{\texttt{Set}(\alpha)}{=} \equiv \lambda\texttt{S,T. (}\forall\texttt{a}\in\texttt{S. a}\in_\alpha\texttt{T)} \wedge \texttt{(}\forall\texttt{a'}\in\texttt{T. a'}\in_\alpha\texttt{S)}$

$\texttt{Set}(\alpha) \equiv \texttt{(S,T):}\alpha\,\texttt{list // S}\underset{\texttt{Set}(\alpha)}{=}\texttt{T}$

Der Index α zeigt an, daß eine Operation von der Gleichheit auf dem Typ α abhängt und somit nur dann berechenbar ist, wenn es hierfür eine boolesche Entscheidungsfunktion gibt. Der Übersichtlichkeit halber wird er ab sofort unterdrückt.

Lemma B.1.3 Axiome endlicher Mengen

$\forall\alpha\texttt{:TYPES. }\forall\texttt{S:Set}(\alpha)\texttt{. }\forall\texttt{x,a:}\alpha\texttt{. }\forall\texttt{P:PROP(Set}(\alpha)\texttt{)}.$

1. $\texttt{Set}(\alpha) \in \texttt{TYPES}$
2. $\emptyset \in \texttt{Set}(\alpha)$
3. $+ \in \texttt{Set}(\alpha)\times\alpha\to\texttt{Set}(\alpha)$
4. $\in \;\in \alpha\times\texttt{Set}(\alpha)\to\mathbb{B}$
5. $\texttt{a}\notin\emptyset$
6. $\texttt{x}\in\texttt{(S+a)} \Leftrightarrow \texttt{(x=a} \vee \texttt{x}\in\texttt{S)}$
7. $\texttt{(S+a)+x = (S+x)+a}$
8. $\texttt{(S+a)+a = S+a}$
9. $\texttt{(P(}\emptyset\texttt{)} \wedge \forall\texttt{S:Set}(\alpha)\texttt{.}\forall\texttt{a:}\alpha\texttt{.P(S)}\Rightarrow\texttt{P(S+a))} \Rightarrow \forall\texttt{S:Set}(\alpha)\texttt{.P(S)}$

Lemma B.1.4 Finite Constructability and Extensionality

$\forall\alpha$:TYPES.$\forall$S,S':Set(α).
1. S=$\emptyset$ $\vee$ $\exists$a:α.$\exists$S':Set(α).(a$\notin$S' $\wedge$ S=S'+a)
2. S=S' $\Leftrightarrow$ $\forall$a:α.(a$\in$S $\Leftrightarrow$ a$\in$S')

ABGELEITETE KONZEPTE

Die weiteren Operationen auf endlichen Mengen hängen von der oben gegebenen speziellen Implementierung nicht ab, da sie sich i.w. durch $\emptyset$, +, $\in$, Gleichheit und den Induktionsoperator list_ind beschreiben lassen.

Definition B.1.5 (Set Notation)

if S=$\emptyset$ then t else t'	$\equiv$	list_ind(S; t; _,_,_,t')
let S=S'+a $\in$ exp	$\equiv$	list_ind(S; ∞; a,S',_,exp)
let S=$\{a\}$ $\in$ exp	$\equiv$	let S=S'+a $\in$ if S'=$\emptyset$ then exp else ∞
let S=$\{a,a'\}$ $\in$ exp	$\equiv$	let S=S'+a' $\in$ let S'=$\{a\}$ $\in$ exp
let S=$\{a,a',a''\}$ $\in$ exp	$\equiv$	let S=S'+a'' $\in$ let S'=$\{a,a'\}$ $\in$ exp
$\lambda\{a\}$.exp	$\equiv$	λS.let S=$\{a\}$ $\in$ exp
$\lambda\{a,a'\}$.exp	$\equiv$	λS.let S=$\{a,a'\}$ $\in$ exp
$\lambda\{a,a',a'\}$.exp	$\equiv$	λS.let S=$\{a,a',a'\}$ $\in$ exp

Definition B.1.6 (Set Operations)

empty?	$\equiv$	λS. if S=$\emptyset$ then true else false
$\subseteq$	$\equiv$	λS,S'. $\forall$x$\in$S.x$\in$S'
$\{$*list-exp*$\}$	$\equiv$	*list-exp*.nil
$\{i..j\}$	$\equiv$	ind(j-i; _,_.$\emptyset$; $\{j\}$; diff,j-set.j-set+(j-diff))
$\{f_x \mid x\in S\wedge p_x\}$	$\equiv$	list_ind(S; $\emptyset$; a,_,GSF. if p_x[a/x] then GSF+f_x[a/x] else GSF
$\{f_x \mid x\in S\}$	$\equiv$	$\{f_x \mid x\in S$ $\wedge$ true$\}$
$\mid S\mid$	$\equiv$	list_ind(S; 0; a,S',card. if a$\in$S' then card else card+1)
-	$\equiv$	λS,a. $\{$x$\mid$x$\in$S$\wedge$x$\neq$a$\}$
$\cup$	$\equiv$	λS,S'. list_ind(S'; S; a,_,union.union+a)
$\cap$	$\equiv$	λS,S'. $\{$x$\mid$x$\in$S$\wedge$x$\in$S'$\}$
$\setminus$	$\equiv$	λS,S'. $\{$x$\mid$x$\in$S$\wedge$x$\notin$S'$\}$
$\bigcup$	$\equiv$	λFAMILY. list_ind(FAMILY; $\emptyset$; S,FAM,Union.Union$\cup$S)
$\bigcap$	$\equiv$	λFAMILY. list_ind(FAMILY; ∞; S,FAM,inter. if empty?(FAM) then S else inter$\bigcap$S)
arb	$\equiv$	λS. list_ind(S; ∞; a,_,_. a)
map	$\equiv$	λf,S. $\{$f(x)$\mid$x$\in$S$\}$
reduce	$\equiv$	λop,S. list_ind(S; ∞; a,S',redS'. if empty?(S') then a else if a$\in$S' then redS' else op(redS',a))
T= $S\uplus S'$	$\equiv$	T= $S\cup S'$ $\wedge$ empty?($S\cap S'$)

Die unten angegebenen Lemmata beschreiben die Grundgesetze der soeben definierten Operationen. Im wesentlichen zeigen sie, wie eine Operation über diverse andere distributiert. Sie können daher zur Vereinfachung eingesetzt werden. Wir gruppieren sie gemäß der jeweils äußersten Operation.

Lemma B.1.7 Operation Signatures

$\forall\alpha,\beta$:TYPES. $\forall$p:$\alpha\to\mathbb{B}$. $\forall$f:$\alpha\to\beta$.

1. empty? $\in$ Set(α)$\to\mathbb{B}$
2. λS. $\exists$x$\in$S.p(x) $\in$ Set(α)$\to\mathbb{B}$
3. λS. $\forall$x$\in$S.p(x) $\in$ Set(α)$\to\mathbb{B}$
4. $\subseteq$ $\in$ Set(α)$^2\to\mathbb{B}$
5. λi,j. {i..j} $\in$ $\mathbb{Z}^2\to$Set($\mathbb{Z}$)
6. λS.{f(x)|x$\in$S $\wedge$ p(x)} $\in$ Set(α)$\to$Set(β)
7. λS. |S| $\in$ Set(α)$\to\mathbb{N}$
8. - $\in$ Set(α)$\times\alpha\to$Set(α)
9. $\cup$ $\in$ Set(α)$^2\to$Set(α)
10. $\cap$ $\in$ Set(α)$^2\to$Set(α)
11. $\setminus$ $\in$ Set(α)$^2\to$Set(α)
12. $\bigcup$ $\in$ Set(Set(α))$\to$Set(α)
13. $\bigcap$ $\in$ Set(Set(α))$\not\to$Set(α
14. arb $\in$ Set(α)$\to\alpha$
15. map $\in$ ($\alpha\to\beta$)$\times$Set(α)$\to$Set(β)
16. reduce $\in$ ($\alpha^2\to\alpha$)$\times$Set(α)$\not\to\alpha$

Lemma B.1.8 Element addition

$\forall\alpha$:TYPES.$\forall$S:Set(α).$\forall$a:α.

1. (S+a)$\neq\emptyset$
2. a$\in$S $\Rightarrow$ S+a=S
3. a$\notin$S $\Rightarrow$ S+a$\neq$S
4. a$\in$S $\Rightarrow$ (S-a)+a = S

Lemma B.1.9 Membership

$\forall\alpha,\beta$:TYPES.$\forall$a,a':α.$\forall$S,S':Set(α).$\forall$FAM:Set(Set(α)).$\forall$p:$\alpha\to\mathbb{B}$.$\forall$f:$\alpha\to\beta$.$\forall$b:β. $\forall$i,j,k:$\mathbb{Z}$.

1. a'$\in${a} $\Leftrightarrow$ a'=a
2. k$\in${i..j} $\Leftrightarrow$ (i$\leq$k $\wedge$ k$\leq$j)
3. b$\in${f(x)|x$\in$S$\wedge$p(x)} $\Leftrightarrow$ $\exists$x$\in$S. p(x) $\wedge$ b=f(x)
4. a$\in${x|x$\in$S$\wedge$p(x)} $\Leftrightarrow$ a$\in$S $\wedge$ p(a)
5. a$\in$S-a' $\Leftrightarrow$ a$\in$S $\wedge$ a$\neq$a'
6. a$\in$S$\cup$S' $\Leftrightarrow$ a$\in$S $\vee$ a$\in$S
7. a$\in$S$\cap$S' $\Leftrightarrow$ a$\in$S $\wedge$ a$\in$S'
8. a$\in$S$\setminus$S' $\Leftrightarrow$ a$\in$S $\wedge$ a$\notin$S'
9. a$\in\bigcup$FAM $\Leftrightarrow$ $\exists$S$\in$FAM. a$\in$S
10. a$\in\bigcap$FAM $\Leftrightarrow$ $\forall$S$\in$FAM. a$\in$S
11. arb(S)$\in$S
12. b$\in$map(f,S) $\Leftrightarrow$ $\exists$x$\in$S.b=f(x)

Lemma B.1.10 empty?

$\forall\alpha,\beta$:TYPES.$\forall$a:α.$\forall$S,S':Set(α).$\forall$FAM:Set(Set(α)).$\forall$p:$\alpha\to\mathbb{B}$.$\forall$f:$\alpha\to\beta$.

1. empty?(S) $\Leftrightarrow$ S=$\emptyset$
2. empty?(S) $\Leftrightarrow$ |S|=0
3. S$\subseteq$S' $\Rightarrow$ empty?(S') $\Rightarrow$ empty?(S)
4. $\neg$empty?(S+a)
5. $\neg$empty?({a})
6. empty?({f(x)|x$\in$S$\wedge$p(x)}) $\Leftrightarrow$ empty?(S) $\vee$ $\forall$x$\in$S.$\neg$p(x))
7. empty?(S-a) $\Leftrightarrow$ empty?(S) $\vee$ S={a}
8. empty?(S$\cup$S') $\Leftrightarrow$ empty?(S) $\wedge$ empty?(S')
9. empty?(S) $\vee$ empty?(S') $\Rightarrow$ empty?(S$\cap$S')
10. empty?(S) $\Rightarrow$ empty?(S$\setminus$S')
11. empty?($\bigcup$FAM) $\Leftrightarrow$ $\forall$S$\in$FAM. empty?(S)
12. $\exists$S$\in$FAM. empty?(S) $\Rightarrow$ empty?($\bigcap$FAM)

Lemma B.1.11 Limited Universal Quantifier

$\forall\alpha,\beta$:TYPES.$\forall$a:α.$\forall$S,S':Set(α).$\forall$FAM:Set(Set(α)).$\forall$p,q:$\alpha\rightarrow\mathbb{B}$.$\forall$f:$\alpha\rightarrow\beta$.

1. $\forall$x$\in\emptyset$. p(x)
2. $\forall$x$\in$S+a. p(x) $\Leftrightarrow$ p(a) $\wedge$ $\forall$x$\in$S.p(x)
3. $\forall$x$\in$\{a\}. p(x) $\Leftrightarrow$ p(a)
4. S$\subseteq$S' $\Rightarrow$ $\forall$x$\in$S'. p(x) $\Rightarrow$ $\forall$x$\in$S. p(x)
5. $\forall$x$\in$\{f(y)|y$\in$S$\wedge$q(y)\}. p(x) $\Leftrightarrow$ $\forall$y$\in$S. q(y) $\Rightarrow$ p(f(y))
6. $\forall$x$\in$S-a. p(x) $\wedge$ p(a) $\Rightarrow$ $\forall$x$\in$S.p(x)

6a. a$\in$S $\Rightarrow$ $\forall$x$\in$S-a. p(x) $\wedge$ p(a) $\Leftrightarrow$ $\forall$x$\in$S.p(x)

7. $\forall$x$\in$S$\cup$S'. p(x) $\Leftrightarrow$ $\forall$x$\in$S.p(x) $\wedge$ $\forall$x$\in$S'.p(x)
8. $\forall$x$\in$S$\cap$S'. p(x) $\Leftarrow$ $\forall$x$\in$S.p(x) $\vee$ $\forall$x$\in$S'.p(x)
9. $\forall$x$\in$S\S'. p(x) $\wedge$ $\forall$x$\in$S'.p(x) $\Rightarrow$ $\forall$x$\in$S.p(x)
10. $\forall$x$\in\bigcup$FAM. p(x) $\Leftrightarrow$ $\forall$S$\in$FAM. $\forall$x$\in$S.p(x)
11. $\forall$x$\in\bigcap$FAM. p(x) $\Leftarrow$ $\exists$S$\in$FAM. $\forall$x$\in$S.p(x)

Lemma B.1.12 Limited Existential Quantifier

$\forall\alpha,\beta$:TYPES.$\forall$a:α.$\forall$S,S':Set(α).$\forall$FAM:Set(Set(α)).$\forall$p,q:$\alpha\rightarrow\mathbb{B}$.$\forall$f:$\alpha\rightarrow\beta$.

1. $\neg\exists$x$\in\emptyset$. p(x)
2. $\exists$x$\in$S+a. p(x) $\Leftrightarrow$ p(a) $\vee$ $\exists$x$\in$S.p(x)
3. $\exists$x$\in$\{a\}. p(x) $\Leftrightarrow$ p(a)
4. S$\subseteq$S' $\Rightarrow$ $\exists$x$\in$S. p(x) $\Rightarrow$ $\exists$x$\in$S'. p(x)
5. $\exists$x$\in$\{f(y)|y$\in$S$\wedge$q(y)\}. p(x) $\Leftrightarrow$ $\exists$y$\in$S. q(y) $\wedge$ p(f(y))
6. $\exists$x$\in$S-a. p(x) $\Leftarrow$ $\neg$p(a) $\wedge$ $\exists$x$\in$S.p(x)
7. $\exists$x$\in$S$\cup$S'. p(x) $\Leftrightarrow$ $\exists$x$\in$S.p(x) $\vee$ $\exists$x$\in$S'.p(x)
8. $\exists$x$\in$S$\cap$S'. p(x) $\Leftrightarrow$ $\exists$x$\in$S.p(x) $\wedge$ $\exists$x$\in$S'.p(x)
9. $\exists$x$\in$S\S'. p(x) $\Leftarrow$ $\exists$x$\in$S.p(x) $\wedge$ $\nexists$x$\in$S'.p(x)
10. $\exists$x$\in\bigcup$FAM. p(x) $\Leftrightarrow$ $\exists$S$\in$FAM. $\exists$x$\in$S.p(x)
11. $\exists$x$\in\bigcap$FAM. p(x) $\Leftrightarrow$ $\exists$x:α. p(x) $\wedge$ $\forall$S$\in$FAM.x$\in$S

Lemma B.1.13 Subset

$\forall\alpha,\beta$:TYPES.$\forall$a:α.$\forall$S,S',S'':Set(α).$\forall$FAM:Set(Set(α)).$\forall$p:$\alpha\rightarrow\mathbb{B}$.$\forall$f:$\alpha\rightarrow\beta$.$\forall$i,j,k,l:$\mathbb{Z}$.

1. $\emptyset\subseteq$S
2. S$\subseteq\emptyset$ $\Leftrightarrow$ empty?(S)
3. S+a$\subseteq$S' $\Leftrightarrow$ S$\subseteq$S' $\wedge$ a$\in$S'
4. \{a\}$\subseteq$S $\Leftrightarrow$ a$\in$S
5. \{i..j\}$\subseteq$\{k..l\} $\Leftrightarrow$ k$\leq$i$\wedge$j$\leq$l
6. S$\subseteq$S' $\Rightarrow$ \{f(x)|x$\in$S$\wedge$p(x)\}$\subseteq$\{f(x)|x$\in$S'$\wedge$p(x)\}
7. S-a$\subseteq$S
8. S$\subseteq$S$\cup$S'

8a. S$\cup$S'$\subseteq$S'' $\Leftrightarrow$ S$\subseteq$S'' $\wedge$ S'$\subseteq$S''

9. S$\cap$S'$\subseteq$S
10. S\S'$\subseteq$S
11. S$\subseteq$S
12. S$\subseteq$S' $\wedge$ S'$\subseteq$S'' $\Rightarrow$ S$\subseteq$S''
13. S$\subseteq$S' $\wedge$ S'$\subseteq$S $\Leftrightarrow$ S=S'

Lemma B.1.14 Integer Subset

$\forall$i,j:$\mathbb{Z}$.

1. i>j $\Rightarrow$ empty?(\{i..j\})
2. \{i..i\} = \{i\}
3. \{i+1..j\} = \{i..j\}-i
4. i-1$\leq$j $\Rightarrow$ \{i-1..j\} = \{i..j\}+(i-1)
5. \{i..j-1\} = \{i..j\}-j
6. i$\leq$j+1 $\Rightarrow$ \{i..j+1\} = \{i..j\}+(j+1)
7. \{i+1..j+1\} = \{k+1|k$\in$\{i..j\}\}

Lemma B.1.15 General Set Former

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$S,S':Set($\alpha$).$\forall$a:$\alpha$.$\forall$FAM:Set(Set($\alpha$)).$\forall$f,f':$\alpha\to\beta$.$\forall$p,q:$\alpha\to\mathbb{B}$.$\forall$g:$\beta\to\gamma$.$\forall$q:$\beta\to\mathbb{B}$.

1. $\{$f(x)|x$\in\emptyset\wedge$ p(x)$\}$ = $\emptyset$
2. $\neg$p(a) $\Rightarrow$ $\{$f(x)|x$\in$S+a $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$
3. p(a) $\Rightarrow$ $\{$f(x)|x$\in$S+a $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$+f(a)
4. $\neg$p(a) $\Rightarrow$ $\{$f(x)|x$\in\{$a$\}\wedge$ p(x)$\}$ = $\emptyset$
5. p(a) $\Rightarrow$ $\{$f(x)|x$\in\{$a$\}\wedge$ p(x)$\}$ = $\{$f(a)$\}$
6. $\{$g(y) | y$\in\{$f(x)|x$\in$S$\wedge$p(x)$\}\wedge$ q(y)$\}$ = $\{$g(f(x))|x$\in$S$\wedge$p(x)$\wedge$q(f(x))$\}$
7. $\neg$p(a) $\Rightarrow$ $\{$f(x)|x$\in$S-a $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$
8. p(a) $\Rightarrow$ $\{$f(x)|x$\in$S-a $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$-f(a)
9. $\{$f(x)|x$\in$S$\cup$S' $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}\cup\{$f(x)|x$\in$S' $\wedge$ p(x)$\}$
10. $\{$f(x)|x$\in$S$\cap$S' $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}\cap_\beta\{$f(x)|x$\in$S' $\wedge$ p(x)$\}$
11. $\{$f(x)|x$\in$S$\setminus$S' $\wedge$ p(x)$\}$ = $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$ $\setminus$ $\{$f(x)|x$\in$S' $\wedge$ p(x)$\}$
12. $\{$f(x)|x$\in\bigcup$FAM $\wedge$ p(x)$\}$ = $\bigcup\{$ $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$ | S$\in$FAM$\}$
13. $\{$f(x)|x$\in\bigcap$FAM $\wedge$ p(x)$\}$ = $\bigcap\{$ $\{$f(x)|x$\in$S $\wedge$ p(x)$\}$ | S$\in$FAM$\}$
14. $\{$x|x$\in$S $\wedge$ x$\neq$a$\}$ = S-a
15. $\{$x|x$\in$S $\wedge$ x$\in$S'$\}$ = S$\cap$S'
16. $\{$x|x$\in$S $\wedge$ x$\notin$S'$\}$ = S$\setminus$S'
17. $\forall$x$\in$S.p(x)$\Rightarrow$f(x)=f'(x) $\Rightarrow$ $\{$f(x)|x$\in$S$\wedge$p(x)$\}$=$\{$f'(x)|x$\in$S$\wedge$p(x)$\}$
18. $\forall$x$\in$S. p(x)$\Leftrightarrow$q(x) $\Rightarrow$ $\{$f(x)|x$\in$S$\wedge$p(x)$\}$=$\{$f(x)|x$\in$S$\wedge$q(x)$\}$

Lemma B.1.16 Cardinality

$\forall\alpha,\beta$:TYPES.$\forall$S,S',T:Set(α).$\forall$a:α.$\forall$f:$\alpha\to\beta$.$\forall$i,j:$\mathbb{Z}$.

1. |$\emptyset$| = 0
2. a$\notin$S $\Rightarrow$ |S+a| = |S|+1
3. |$\{$a$\}$| = 1
4. S$\subseteq$S' $\Rightarrow$ |S|$\leq$|S'|
5. i$\leq$j $\Rightarrow$ |$\{$i..j$\}$| = j-i+1
6. a$\in$S $\Rightarrow$ |S-a| = |S|-1
7. T=S$\uplus$S' $\Rightarrow$ |T| = |S|+|S'|
8. |map(f,S)| = |S|

Lemma B.1.17 Element Deletion

$\forall\alpha,\beta$:TYPES.$\forall$S,S':Set(α).$\forall$a,a':α.

1. $\emptyset$-a = $\emptyset$
2. a$\notin$S $\Rightarrow$ ((S+a)-a = S)
3. a$\neq$a' $\Rightarrow$ ((S+a)-a' = (S-a')+a)
4. $\{$a$\}$-a = $\emptyset$
5. a$\neq$a' $\Rightarrow$ $\{$a$\}$-a' = $\{$a$\}$
6. a$\notin$S $\Rightarrow$ S-a = S

Lemma B.1.18 Union

$\forall\alpha,\beta$:TYPES.$\forall$S,S',S'':Set(α).$\forall$a,a':α.$\forall$FAM,FAM':Set(Set(α)).$\forall$f:$\alpha\to\beta$.$\forall$p,q:$\alpha\to\mathbb{B}$.$\forall$i,j,k:$\mathbb{Z}$.

1. S$\cup\emptyset$ = S
2. S$\cup$(S'+a) = (S$\cup$S')+a
3. S$\cup\{$a$\}$ = S+a
4. i$\leq$j$\wedge$j<k $\Rightarrow$ $\{$i..j$\}\cup\{$j+1..k$\}$ = $\{$i..k$\}$
5. $\{$f(x)|x$\in$S$\wedge$p(x)$\}$ $\cup$ $\{$f(x)|x$\in$S$\wedge$q(x)$\}$ = $\{$f(x)|x$\in$S$\wedge$ p(x)$\vee$q(x)$\}$
6. S$\cup$(S'$\cap$S'') = (S$\cup$S')$\cap$(S$\cup$S'')
7. $\bigcup$FAM $\cup$ $\bigcup$FAM' = $\bigcup$(FAM$\cup$FAM')
8. S$\cup$S = S
9. S$\cup$S' = S'$\cup$S
10. S$\cup$(S'$\cup$S'') = (S$\cup$S')$\cup$S''
11. S$\cup$(S$\cap$S') = S

Lemma B.1.19 Intersection

$\forall\alpha,\beta:\mathtt{TYPES}.\forall S,S',S'':\mathtt{Set}(\alpha).\forall a,a':\alpha.\forall FAM,FAM':\mathtt{Set}(\mathtt{Set}(\alpha)).\forall f:\alpha\to\beta.\forall p,q:\alpha\to\mathbb{B}.\forall i,j,k:\mathbb{Z}.$

1. $S\cap\emptyset = \emptyset$
2. $a\in S \Rightarrow (S\cap(S'+a) = (S\cap S')+a)$
3. $a\notin S \Rightarrow S\cap(S'+a) = S\cap S'$
4. $a\in S \Rightarrow (S\cap\{a\} = \{a\})$
5. $a\notin S \Rightarrow S\cap\{a\} = \emptyset$
6. $(i\leq j \wedge j\leq k \wedge k\leq j') \Rightarrow \{i..k\}\cap\{j..j'\} = \{j..k\}$
7. $\{f(x)\,|\,x\in S\wedge p(x)\} \cap \{f(x)\,|\,x\in S\wedge q(x)\} = \{f(x)\,|\,x\in S\wedge p(x)\wedge q(x)\}$
8. $S\cap(S'\cup S'') = (S\cap S')\cup(S\cap S'')$

8a $S\cap(S'-a) = (S\cap S')-a$

9. $\bigcap FAM \cap \bigcap FAM' = \bigcap(FAM\cup FAM')$
10. $S\cap S = S$
11. $S\cap S' = S'\cap S$
12. $S\cap(S'\cap S'') = (S\cap S')\cap S''$
13. $S\cap(S\cup S') = S$

Lemma B.1.20 Set Difference

$\forall\alpha,\beta:\mathtt{TYPES}.\forall S,S',S'':\mathtt{Set}(\alpha).\forall a,a':\alpha.\forall FAM,FAM':\mathtt{Set}(\mathtt{Set}(\alpha)).\forall f:\alpha\to\beta.\forall p,q:\alpha\to\mathbb{B}.\forall i,j,k:\mathbb{Z}.$

1. $S\setminus\emptyset = S$
2. $S\setminus(S'+a) = (S\setminus S')-a$
3. $S\setminus\{a\} = S-a$
4. $\emptyset\setminus S' = \emptyset$
5. $a\notin S' \Rightarrow ((S+a)\setminus S' = (S\setminus S')+a)$
6. $a\in S' \Rightarrow ((S+a)\setminus S' = S\setminus S')$
7. $a\notin S \Rightarrow (\{a\}\setminus S = \{a\})$
8. $a\in S \Rightarrow (\{a\}\setminus S = \emptyset)$
9. $\{f(x)\,|\,x\in S\wedge p(x)\} \setminus \{f(x)\,|\,x\in S\wedge q(x)\} = \{f(x)\,|\,x\in S\wedge p(x)\wedge\neg q(x)\}$
10. $S\setminus(S'\cup S'') = (S\setminus S')\setminus S''$
11. $S\setminus S = \emptyset$
12. $S\subseteq S' \Rightarrow S\setminus S' = \emptyset$

Lemma B.1.21 Union of a family of sets

$\forall\alpha,\beta,\gamma:\mathtt{TYPES}.\forall FAM:\mathtt{Set}(\mathtt{Set}(\alpha)).\forall S:\mathtt{Set}(\alpha).\forall T:\mathtt{Set}(\beta).\forall F:\alpha\to\mathtt{Set}(\beta).\forall g:\beta\to\gamma.$
$\forall p:\alpha\to\mathbb{B}.\forall q:\beta\to\mathbb{B}.\forall S:\mathtt{Set}(\alpha).\forall c:\gamma.$

1. $\bigcup\emptyset = \emptyset$
2. $\bigcup(FAM+S) = \bigcup FAM\cup S$
3. $\bigcup(\{S\}) = S$
4. $\bigcup\{\ \{g(y)\,|\,y\in F(x)\wedge q(y)\}\ |\,x\in S\wedge p(x)\} = \{g(y)\,|\,y\in\bigcup\{F(x)\,|\,x\in S\wedge p(x)\}\ \wedge\ q(y)\})$
5. $c\in\bigcup\{\ \{g(y)\,|\,y\in F(x)\ \wedge\ q(y)\}\ |\ x\in S\wedge p(x)\} \Leftrightarrow \exists x\in S.\,p(x)\ \wedge\ \exists y\in F(x).\,q(y)\wedge c=g(y)$
6. $S\in FAM \Rightarrow \bigcup(FAM-S) = \bigcup FAM\setminus S$
7. $\bigcup\{\ \bigcup\{f(x,y)\,|\,x\in S\wedge p(x)\}\,|\,y\in T\ \wedge\ q(y)\} = \bigcup\{\ \bigcup\{f(x,y)\,|\,y\in T\wedge q(y)\}\,|\,x\in S\ \wedge\ p(x)\}$
8. $\bigcup\{\ \{G(y)\,|\,y\in F(x)\wedge q(y)\}\ |\,x\in S\wedge p(x)\} = \{\ \bigcup\{G(y)\,|\,y\in F(x)\wedge q(y)\}\ |\,x\in S\wedge p(x)\}$

Lemma B.1.22 Intersection of a family of sets

$\forall\alpha,\beta,\gamma:\mathtt{TYPES}.\forall F:\alpha\to\mathtt{Set}(\beta).\forall FAM:\mathtt{Set}(\mathtt{Set}(\alpha)).\forall g:\beta\to\gamma.\forall p:\alpha\to\mathbb{B}.\forall q:\beta\to\mathbb{B}.\forall S:\mathtt{Set}(\alpha).$

1. $\bigcap\{S\} = S$
2. $\bigcap(FAM+S) = \bigcap FAM\cap S$
3. $\bigcap\{\ \{g(y)\,|\,y\in F(x)\wedge q(y)\}\ |\,x\in S\wedge p(x)\} = \{g(y)\,|\,x\in\bigcap\{F(x)\,|\,x\in S\wedge p(x)\}\ \wedge\ q(y)\})$

Lemma B.1.23 Arbitrary Selection

$\forall\alpha:\mathtt{TYPES}.\forall a:\alpha.$

1. $\mathtt{arb}(\{a\}) = a$

Lemma B.1.24 map-operation

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\to$Set($\beta$).$\forall$g:$\beta\to\gamma$.$\forall$p:$\alpha\to\mathbb{B}$.$\forall$S,S':Set($\alpha$).$\forall$a:$\alpha$.

1. map(f,$\emptyset$) = $\emptyset$
2. map(f,S+a) = map(f,S)+f(a)
3. map(f,{a}) = {f(a)}
4. map(g,{f(x)|x$\in$S $\wedge$ p(x)}) = {g(f(x))|x$\in$S $\wedge$ p(x)})
5. map(f,S-a) = map(f,S)-f(a)
6. map(f,S$\cup$S') = map(f,S)$\cup$map(f,S')
7. map(f,S$\cap$S') = map(f,S)$\cap$map(f,S')
8. map(f,S\S') = map(f,S)\map(f,S')

Lemma B.1.25 Reduce operation

$\forall\alpha$:TYPES.$\forall$bop:$\alpha^2\to\alpha$.$\forall$S:Set(α).$\forall$a:α.$\forall$FAM:Set(Set(α)).

1. reduce(bop,{a}) = a
2. $\neg$empty?(S) $\wedge$ a$\notin$S $\Rightarrow$ reduce(bop,S+a) = bop(reduce(bop,S),a)
3. $\neg$empty?(FAM) $\Rightarrow$ reduce($\cup$,FAM) = $\bigcup$FAM
4. $\neg$empty?(FAM) $\Rightarrow$ reduce($\cap$,FAM) = $\bigcap$FAM

B.2 Endliche Folgen

Der Typ der endlichen Mengen ist ein generischer Datentyp, der auf der Basis der Konzepte `Seq`, `=`, `[]`, `cons`, `first` und `rest` eingeführt werden kann. Bis auf kleine Erweiterungen entspricht der dem NuPRL Listenkonstruktor.

BASISKONZEPTE

Definition B.2.1 (Implementierung endlicher Folgen)

`[]`	$\equiv$ `nil`
`cons`	$\equiv$ λ`a,L. (a.L)`
`list_ind`$(L;t_b;a,L',FL'.t_{ind})$	$\equiv$ `list_ind`$(L;t_b;a,L',FL'.t_{ind})$
`first`	$\equiv$ λ`L.list_ind(L;`∞`;a,_,_.a)`
`rest`	$\equiv$ λ`L.list_ind(L;[];_,L',_.L')`
`=`	$\equiv$ λ`L,L'.(list_ind(L;`λ`L.list_ind(L;true;_,_,_.false);` `a,_,EQ.`λ`L1.a=first(L1)` $\wedge$ `EQ(rest(L1))) (L'))`
`Seq`(α)	$\equiv$ α `list`

Lemma B.2.2 Axioms of Finite Sequences

$\forall\alpha$:`TYPES`.$\forall$`L,L':Seq`(α).$\forall$`a,a':`α. $\forall$`P:PROP(Seq`(α)`)`.

1. `Seq`(α) $\in$ `TYPES`
2. `[]` $\in$ `Seq`(α)
3. `cons` $\in$ $\alpha\times$`Seq`$(\alpha)\to$`Seq`(α)
4. `first` $\in$ `Seq`$(\alpha)\not\to\alpha$
5. `rest` $\in$ `Seq`$(\alpha)\to$`Seq`(α)
6. `[]`$\neq$`a.L`
7. `a.L=a'.L'` $\Leftrightarrow$ `(a=a'` $\wedge$ `L=L' )`
8. `first(a.L)=a`
9. `rest(a.L)=L`
10. $\forall$`g:`β.$\forall$`h:(`$\beta\times$`Seq`$(\alpha)\times\alpha)\to\beta$.$\exists$`f:Seq`$(\alpha)\to\beta$.
    `f([])=g` $\wedge$ $\forall$`L:Seq`(α).$\forall$`a:`α. `f(a.L)=h(f(L),L,a)`
11. `(P([])` $\wedge$ $\forall$`L:Seq`(α).$\forall$`a:`α`.P(L)`$\Rightarrow$`P(a.L))` $\Rightarrow$ $\forall$`L:Seq`(α)`.P(L)`

Lemma B.2.3 Finite Constructability and Sequence Equality

$\forall\alpha$:`TYPES`.$\forall$`L,L':Seq`(α).

1. $\forall\alpha$:`TYPES`.$\forall$`L:Seq`(α). `L=[]` $\vee$ $\exists$`a:`α.$\exists$`L':Seq`(α). `L=a.L'`
2. `L=L'` $\Leftrightarrow$ `first(L)=first(L')` $\wedge$ `rest(L)=rest(L')`

ABGELEITETE KONZEPTE

Definition B.2.4 (Sequence Notation)

`if` L`=[] then` t `else` t'	$\equiv$ `list_ind`$(L;\ t;\ \_,\_,\_,t')$
`let` L`=`$a.L'$ $\in$ exp	$\equiv$ `list_ind`$(L;\ \infty;\ a,L',\_,exp)$
`let` L`=[`a`]` $\in$ exp	$\equiv$ `let` L`=`a`.L'` $\in$ `if L'=[] then` exp `else` ∞
`let` L`=[`a,a'`]` $\in$ exp	$\equiv$ `let` L`=`a'`.L'` $\in$ `let L'=[`a`]` $\in$ exp
`let` L`=[`a,a',a''`]` $\in$ exp	$\equiv$ `let` L`=`a''`.L'` $\in$ `let L'=[`a,a'`]` $\in$ exp
λ`[`a`]`.exp	$\equiv$ λ`L.let L=[`a`]` $\in$ exp
λ`[`a,a'`]`.exp	$\equiv$ λ`L.let L=[`a,a'`]` $\in$ exp
λ`[`a,a',a'`]`.exp	$\equiv$ λ`L.let L=[`a,a',a'`]` $\in$ exp

Definition B.2.5 (Sequence Operations)

null?	$\equiv$ λL. list_ind(L; true; _,_,_.false)
[*list-exp*]	$\equiv$ *list-exp*.nil
[i..j]	$\equiv$ ind(j-i; _,_.[]; [j]; diff,j-seq. (j-diff).j-seq)
[f_x | $x \in L \wedge p_x$]	$\equiv$ list_ind(L; []; a,_,GSF. if p_x[a/x] then f_x[a/x].GSF else GSF)
[f_x | $x \in L$]	$\equiv$ [f_x | $x \in L \wedge$true]
|L|	$\equiv$ list_ind(L; 0; _,_,card. card+1)
L[i]	$\equiv$ list_ind(L; λj.∞; a,_,jth-of. λj. if j=1 then a else jth-of(j-1)) (i)
last	$\equiv$ λL. L[|L|]
$\cdot$	$\equiv$ λL,a. list_ind(L; [a]; a',_.app. a'.app)
ins	$\equiv$ λL,j,a. [if i<j then L[i] else if i=j then a else L[i-1] | i $\in$ [1..|L|+1]]
del	$\equiv$ λL,j. [if i<j then L[i] else L[i+1] | i $\in$ [1..|L|-1]]
$\circ$	$\equiv$ λL,L'. list_ind(L; L'; a,_,conc. a.conc)
rev	$\equiv$ λL. [L[|L|-i] | i $\in$ [0..|L|-1]]
domain	$\equiv$ λL. {1..|L|}
range	$\equiv$ λL. {L[i] | i $\in$ domain(L)}
map	$\equiv$ λf,L. [f(x) | x $\in$ L]
reduce	$\equiv$ λop,L. list_ind(L; ∞; a,L',redL'.if null?(L') then a else op(redL',a))
$L_{[i..j]}$	$\equiv$ [L[k] | k $\in$ [i..j]]
$\in$	$\equiv$ λa,L. $\exists$x $\in$ range(L).x=a
$\sqsubseteq$	$\equiv$ λL,L'. |L| $\leq$ |L'| $\wedge$ $\forall$i $\in$ domain(L). L[i]=L'[i]
$L_{<g}$	$\equiv$ [x | x $\in L \wedge$ x<g]
$L_{\geq g}$	$\equiv$ [x | x $\in L \wedge$ x$\geq g$]
find	$\equiv$ λg,L. min{j | j $\in$ domain(L) $\wedge$ L[j]=g}
-	$\equiv$ λL,g.del(L,find(g,L))
nodups	$\equiv$ λL. $\forall$i $\in$ domain(L).$\forall$j $\in$ {i+1..|L|}. L[i]$\neq$L[j]
perm	$\equiv$ λL,S. nodups(L) $\wedge$ range(L)=S
rearranges	$\equiv$ λL,L'. $\exists$I:Seq($\mathbb{Z}$).perm(I,domain(L)) $\wedge$ L'=[L[k] | k $\in$ I]
insert	$\equiv$ λL,g.$L_{<g}$ $\circ$ g.L
Seq$^+$(α)	$\equiv$ {L:Seq(α) | $\neg$empty?(L)}
arb	$\equiv$ λL. first(L)

Lemma B.2.6 Operation Signatures

$\forall\alpha,\beta$:TYPES.$\forall$f:$\alpha\to\beta$.$\forall$p:$\alpha\to\mathbb{B}$.

1. null? $\in$ Seq(α)$\to\mathbb{B}$
2. $\in$ $\in$ $\alpha\times$Seq(α)$\to\mathbb{B}$
3. $\sqsubseteq$ $\in$ Seq(α)$^2\to\mathbb{B}$
4. λi,j. [i..j] $\in$ $\mathbb{Z}^2\to$Seq($\mathbb{Z}$)
5. λL. [f(x) \| x $\in$ L $\wedge$ p(x)] $\in$ Seq(α)$\to$Seq(β)
6. λL. \|L\| $\in$ Seq(α)$\to\mathbb{N}$
7. λL,i.L[i] $\in$ Seq(α)$\times\mathbb{Z}\to\alpha$
8. last $\in$ Seq(α)$\to\alpha$
9. $\cdot$ $\in$ Seq(α)$\times\alpha\to$Seq(α)
10. ins $\in$ Seq(α)$\times\mathbb{N}\times\alpha\to$Seq($\alpha$)
11. del $\in$ Seq(α)$\times\mathbb{N}\to$Seq(α)
12. $\circ$ $\in$ Seq(α)$^2\to$Seq(α)
13. rev $\in$ Seq(α)$\to$Seq(α)
14. domain $\in$ Seq(α)$\to$Set(α)
15. range $\in$ Seq(α)$\to$Set(α)
16. map $\in$ ($\alpha\to\beta$)$\times$Seq(α)$\to$Seq(β)
17. reduce $\in$ ($\alpha^2\to\alpha$)$\times$Seq(α) $\not\to$ α
18. λL,i,j. $L_{[i..j]}$ $\in$ Seq(α)$\times\mathbb{Z}^2\to$Seq(α)
19. nodups $\in$ Seq(α)$\to\mathbb{B}$
20. perm $\in$ Seq(α)$\times$Set(α)$\to\mathbb{B}$
21. rearranges $\in$ PROP(Seq(α)^2)

Lemma B.2.7 Prepend

$\forall\alpha\mathtt{:TYPES.}\forall\mathtt{L:Seq(}\alpha\mathtt{).}\forall\mathtt{a:}\alpha\mathtt{.}$

1. $\mathtt{a.L}\neq\mathtt{[]}$
2. $\mathtt{a.L}\neq\mathtt{L}$

Lemma B.2.8 null?

$\forall\alpha,\beta\mathtt{:TYPES.}\forall\mathtt{f:}\alpha\to\beta\mathtt{.}\forall\mathtt{p:}\alpha\to\mathbb{B}\mathtt{.}\forall\mathtt{L,L':Seq(}\alpha\mathtt{).}\forall\mathtt{a:}\alpha\mathtt{.}\forall\mathtt{i:}\mathbb{N}\mathtt{.}$

1. $\mathtt{null?(L)} \Leftrightarrow \mathtt{L=[]}$
2. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{null?(L')}\Rightarrow\mathtt{null?(L)}$
3. $\neg\mathtt{null?(a.L)}$
4. $\neg\mathtt{null?([a])}$
5. $\mathtt{null?([f(x)|x}\in\mathtt{L}\wedge\mathtt{p(x)])} \Leftrightarrow \mathtt{null(L)}\vee\forall\mathtt{x}\in\mathtt{L.}\neg\mathtt{p(x))}$
6. $\mathtt{null?(L)} \Rightarrow \mathtt{|L|=0}$
7. $\neg\mathtt{null?(L\cdot a)}$
8. $\mathtt{i}\leq\mathtt{|L|+1} \Rightarrow \neg\mathtt{null?(ins(L,i,a))}$
9. $\mathtt{null?(del(L,i))} \Leftrightarrow \mathtt{null?(L)}\vee\mathtt{L=[L[i]]}$
10. $\mathtt{null?(L}\circ\mathtt{L')} \Leftrightarrow \mathtt{null?(L)}\wedge\mathtt{null?(L')}$
11. $\mathtt{null?(rev(L))} \Leftrightarrow \mathtt{null?(L)}$
12. $\mathtt{null?(L)} \Leftrightarrow \mathtt{empty?(domain(L))}$
13. $\mathtt{null?(L)} \Leftrightarrow \mathtt{empty?(range(L))}$

Lemma B.2.9 Membership

$\forall\alpha,\beta\mathtt{:TYPES.}\forall\mathtt{f:}\alpha\to\beta\mathtt{.}\forall\mathtt{p:}\alpha\to\mathbb{B}\mathtt{.}\forall\mathtt{L,L':Seq(}\alpha\mathtt{).}\forall\mathtt{a,a':}\alpha\mathtt{.}\forall\mathtt{b:}\beta\mathtt{.}\forall\mathtt{i,j,k:}\mathbb{Z}\mathtt{.}$

1. $\mathtt{a}\notin\mathtt{[]}$
2. $\mathtt{a'}\in\mathtt{a.L} \Leftrightarrow \mathtt{a'=a}\vee\mathtt{a'}\in\mathtt{L}$
3. $\mathtt{a}\in\mathtt{L} \Leftrightarrow \mathtt{a=first(L)}\vee\mathtt{a}\in\mathtt{rest(L)}$
4. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{a}\in\mathtt{L} \Rightarrow \mathtt{a}\in\mathtt{L'}$
5. $\mathtt{a'}\in\mathtt{[a]} \Leftrightarrow \mathtt{a=a'}$
6. $\mathtt{k}\in\mathtt{[i..j]} \Leftrightarrow \mathtt{i}\leq\mathtt{k}\wedge\mathtt{k}\leq\mathtt{j}$
7. $\mathtt{b}\in\mathtt{[f(x)|x}\in\mathtt{L}\wedge\mathtt{p(x)]} \Leftrightarrow \exists\mathtt{x}\in\mathtt{L.\,p(x)}\wedge\mathtt{b=f(x)}$
8. $\mathtt{a'}\in\mathtt{L\cdot a} \Leftrightarrow \mathtt{a'=a}\vee\mathtt{a'}\in\mathtt{L}$
9. $\mathtt{i}\leq\mathtt{|L|+1} \Rightarrow \mathtt{a'}\in\mathtt{ins(L,i,a)} \Leftrightarrow \mathtt{a'=a}\vee\mathtt{a'}\in\mathtt{L}$
10. $\mathtt{0<i} \wedge \mathtt{i}\leq\mathtt{|L|} \wedge \mathtt{a}\neq\mathtt{L[i]} \Rightarrow \mathtt{a}\in\mathtt{del(L,i)}\Leftrightarrow\mathtt{a'}\in\mathtt{L}$
11. $\mathtt{a}\in\mathtt{L}\circ\mathtt{L'} \Leftrightarrow \mathtt{a}\in\mathtt{L}\vee\mathtt{a}\in\mathtt{L'}$
12. $\mathtt{a}\in\mathtt{rev(L)} \Leftrightarrow \mathtt{a}\in\mathtt{L}$
13. $\mathtt{i}\in\mathtt{domain(L)} \Leftrightarrow \mathtt{1}\leq\mathtt{i}\wedge\mathtt{i}\leq\mathtt{|L|}$
14. $\mathtt{a}\in\mathtt{L} \Leftrightarrow \mathtt{a}\in\mathtt{range(L)}$

Lemma B.2.10 Prefix

$\forall\alpha,\beta\mathtt{:TYPES.}\forall\mathtt{f:}\alpha\to\beta\mathtt{.}\forall\mathtt{p:}\alpha\to\mathbb{B}\mathtt{.}\forall\mathtt{L,L':Seq(}\alpha\mathtt{).}\forall\mathtt{a,a':}\alpha\mathtt{.}\forall\mathtt{b:}\beta\mathtt{.}\forall\mathtt{i,j,k,l:}\mathbb{Z}\mathtt{.}$

1. $\mathtt{[]}\sqsubseteq\mathtt{L}$
2. $\mathtt{L}\sqsubseteq\mathtt{[]} \Leftrightarrow \mathtt{null?(L)}$
3. $\mathtt{a.L}\sqsubseteq\mathtt{L'} \Leftrightarrow \mathtt{a=first(L')}\wedge\mathtt{L}\sqsubseteq\mathtt{rest(L')}$
4. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{first(L)=first(L')}$
5. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{rest(L)}\sqsubseteq\mathtt{rest(L')}$
6. $\mathtt{[a]}\sqsubseteq\mathtt{L} \Leftrightarrow \mathtt{a=first(L)}$
7. $\mathtt{[i..j]}\sqsubseteq\mathtt{[k..l]} \Leftrightarrow \mathtt{i=j} \wedge \mathtt{j}\leq\mathtt{l}$
8. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{[f(x)|x}\in\mathtt{L}\wedge\mathtt{p(x)]}\sqsubseteq\mathtt{[f(x)|x}\in\mathtt{L'}\wedge\mathtt{p(x)]}$
9. $\mathtt{L}\sqsubseteq\mathtt{L\cdot a}$
10. $\mathtt{L}\sqsubseteq\mathtt{L}\circ\mathtt{L'}$
11. $\mathtt{L}\sqsubseteq\mathtt{L'} \Leftrightarrow \exists\mathtt{L'':Seq(}\alpha\mathtt{).\ L}\circ\mathtt{L''=L'}$
12. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{domain(L)}\subseteq\mathtt{domain(L')}$
13. $\mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{range(L)}\subseteq\mathtt{range(L')}$
14. $\mathtt{L}\sqsubseteq\mathtt{L}$
15. $\mathtt{L}\sqsubseteq\mathtt{L'} \wedge \mathtt{L'}\sqsubseteq\mathtt{L''} \Rightarrow \mathtt{L}\sqsubseteq\mathtt{L''}$
16. $\mathtt{L}\sqsubseteq\mathtt{L'} \wedge \mathtt{L'}\sqsubseteq\mathtt{L} \Leftrightarrow \mathtt{L=L'}$
17. $\mathtt{i}\leq\mathtt{|L|} \wedge \mathtt{L}\sqsubseteq\mathtt{L'} \Rightarrow \mathtt{L[i]=L'[i]}$

Lemma B.2.11 Integer sequence

$\forall i,j{:}\mathbb{Z}.$

1. $i>j \Rightarrow \mathtt{null?}([i..j])$
2. $[i..i] = [i]$
3. $i\leq j \Rightarrow \mathtt{first}([i..j]) = i$
4. $[i{+}1..j] = \mathtt{rest}([i..j])$
5. $i{-}1\leq j \Rightarrow [i{-}1..j] = (i{-}1).[i..j]$
6. $i\leq j{+}1 \Rightarrow [i..j{+}1] = [i..j]\cdot(j{+}1)$
7. $[i{+}1..j{+}1] = [\,k{+}1 \mid k\in[i..j]\,]$
8. $i\leq j \Rightarrow \mathtt{last}([i..j]) = j$

Lemma B.2.12 General sequence former

$\forall\alpha,\beta,\gamma{:}\mathtt{TYPES}.\forall L,L'{:}\mathtt{Seq}(\alpha).\forall a{:}\alpha.\forall f,f'{:}\alpha\to\beta.\forall g{:}\beta\to\gamma.\forall p,p'{:}\alpha\to\mathbb{B}.\forall q{:}\beta\to\mathbb{B}.\forall i{:}\mathbb{N}.$

1. $[f(x)|x\in[]\wedge p(x)] = []$
2. $\neg p(a) \Rightarrow [f(x)|x\in a.L\wedge p(x)] = [f(x)|x\in L\wedge p(x)]$
3. $p(a) \Rightarrow [f(x)|x\in a.L\wedge p(x)] = f(a).[f(x)|x\in L\wedge p(x)]$
4. $p((\mathtt{first}(L)) \Rightarrow \mathtt{first}([f(x)|x\in L\wedge p(x)]) = f(\mathtt{first}(L))$
5. $p((\mathtt{first}(L)) \Rightarrow \mathtt{rest}([f(x)|x\in L\wedge p(x)]) = [f(x)|x\in \mathtt{rest}(L)\wedge p(x)]$
6. $\neg p(a) \Rightarrow [f(x)|x\in[a]\wedge p(x)] = []$
7. $p(a) \Rightarrow [f(x)|x\in[a]\wedge p(x)] = [f(a)]$
8. $[g(y) \mid y\in[f(x)|x\in L\wedge p(x)] \wedge q(y)] = [g(f(x))|x\in L\wedge p(x)\wedge q(f(x))]$
9. $\forall a{:}\alpha.\ \neg p(a) \Rightarrow [f(x)|x\in L\cdot a\wedge p(x)] = [f(x)|x\in L\wedge p(x)]$
10. $p(a) \Rightarrow [f(x)|x\in L\cdot a\wedge p(x)] = [f(x)|x\in L\wedge p(x)]\cdot f(a)$
11. $i\leq|L|{+}1 \Rightarrow \neg p(a) \Rightarrow [f(x)|x\in \mathtt{ins}(L,i,a)\wedge p(x)] = [f(x)|x\in L\wedge p(x)]$
12. $\neg p(L[i]) \Rightarrow [f(x)|x\in \mathtt{del}(L,i)\wedge p(x)] = [f(x)|x\in L\wedge p(x)]$
13. $[f(x)|x\in L\circ L'\wedge p(x)] = [f(x)|x\in L\wedge p(x)]\circ[f(x)|x\in L'\wedge p(x)]$
14. $[f(x)|x\in \mathtt{rev}(L)\wedge p(x)] = \mathtt{rev}([f(x)|x\in L\wedge p(x)])$
15. $\forall x\in L.p(x)\Rightarrow f(x)=f'(x) \Rightarrow [f(x)|x\in L\wedge p(x)]=[f'(x)|x\in L\wedge p(x)]$
16. $\forall x\in L.\ p(x)\Leftrightarrow p'(x) \Rightarrow [f(x)|x\in L\wedge p(x)]=[f(x)|x\in L\wedge p'(x)]$

Lemma B.2.13 Cardinality

$\forall\alpha,\beta{:}\mathtt{TYPES}.\forall f{:}\alpha\to\beta.\forall p{:}\alpha\to\mathbb{B}.\forall L,L'{:}\mathtt{Seq}(\alpha).\forall a{:}\alpha.\forall i,j{:}\mathbb{Z}.$

1. $|[]| = 0$
2. $|a.L| = |L|{+}1$
3. $\neg\mathtt{null?}(L) \Rightarrow |\mathtt{rest}(L)| = |L|{-}1$
4. $|[a]| = 1$
5. $L\sqsubseteq L' \Rightarrow |L|\leq|L'|$
6. $|[f(x)|x\in L\wedge p(x)]|=|[x|x\in L\wedge p(x)]|$
7. $\forall i,j{:}\mathbb{Z}.\ i\leq j \Rightarrow |[i..j]| = j{-}i{+}1$
8. $|L\cdot a| = |L|{+}1$
9. $i\leq|L|{+}1 \Rightarrow |\mathtt{ins}(L,i,a)| = |L|{+}1$
10. $0<i \wedge i\leq|L| \Rightarrow |\mathtt{del}(L,i)| = |L|{-}1$
11. $|L\circ L'| = |L|{+}|L'|$
12. $|\mathtt{rev}(L)| = |L|$
13. $|L| = |\mathtt{domain}(L)|$

Lemma B.2.14 Selecting the i-th element

$\forall\alpha,\beta$:TYPES.$\forall$f:$\alpha\to\beta$.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i,j:$\mathbb{N}$.

1. L[1]=first(L)
2. L[i+1]=rest(L)[i]
3. ins(L,i,a)[i]=a
4. [f(x)|x$\in$L][i]=f(L[i])
5. i$\leq$|L| $\Rightarrow$ L·a[i]=L[i]
6. L·a[|L|+1]=a
7. i<j $\Rightarrow$ ins(L,j,a)[i]=L[i]
8. i>j $\Rightarrow$ ins(L,j,a)[i]=L[i-1]
9. i<j $\Rightarrow$ del(L,j)[i]=L[i]
10. i$\geq$j $\Rightarrow$ del(L,j)[i]=L[i+1]
11. i$\leq$|L| $\Rightarrow$ L$\circ$L'[i]=L[i]
12. i>|L| $\Rightarrow$ L$\circ$L'[i]=L'[i-|L|]
13. i$\leq$|L| $\Rightarrow$ rev(L)[i]=L[|L|-i+1]

Lemma B.2.15 last

$\forall\alpha,\beta$:TYPES.$\forall$f:$\alpha\to\beta$.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{N}$.

1. last[a]=a
2. last(L·a)=a
3. last([f(x)|x$\in$L])=f(last(L))
4. i$\leq$|L| $\Rightarrow$ last(ins(L,i,a))=last(L)
5. last(ins(L,|L|+1,a)=a
6. i<L $\Rightarrow$ last(del(L,i))=last(L)
7. last(del(L,|L|))=L[|L|-1]
8. $\neg$null?(L') $\Rightarrow$ last(L$\circ$L')=last(L')
9. null?(L') $\Rightarrow$ last(L$\circ$L')=last(L)
10. last(rev(L))=first(L)

Lemma B.2.16 Append

$\forall\alpha$:TYPES.$\forall$L:Seq(α).$\forall$a,a':α.

1. []·a= [a]
2. (a'.L)·a=a'.(L·a)

Lemma B.2.17 Insert

$\forall\alpha$:TYPES.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{N}$.

1. ins(L,1,a)=a.L
2. ins(L,i+1,a)=first(L).ins(rest(L),i,a)
3. ins(L,|L|+1,a)=L·a
4. i$\leq$|L| $\Rightarrow$ ins(del(L,i),i,L[i])=L
5. i$\leq$|L| $\Rightarrow$ ins(L$\circ$L',i,a)=ins(L,i,a)$\circ$L'
6. i>|L| $\Rightarrow$ ins(L$\circ$L',i,a)=L$\circ$ins(L',i-|L|,a)

Lemma B.2.18 Delete

$\forall\alpha$:TYPES.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{N}$.

1. del(L,1)=rest(L)
2. del(L,i+1)=first(L).del(rest(L),i)
3. del(L·a,|L|+1)=L
4. i$\leq$|L|+1 $\Rightarrow$ del(ins(L,i,a),i)=L
5. i$\leq$|L| $\Rightarrow$ del(L$\circ$L',i)=del(L,i)$\circ$L'
6. i>|L| $\Rightarrow$ del(L$\circ$L',i)=L$\circ$del(L',i-|L|)
7. i$\leq$|L| $\Rightarrow$ del(rev(L),i)=rev(del(L,|L|-i+1))

Lemma B.2.19 Concat

$\forall\alpha$:TYPES.$\forall$L,L',L'':Seq(α).$\forall$a:α.$\forall$i,j,k:$\mathbb{Z}$.

1. L$\circ$[]=L
2. []$\circ$L=L
3. (a.L)$\circ$L'=a.(L$\circ$L')
4. [a]$\circ$L=a.L
5. L$\circ$[a]=L·a
6. i$\leq$j$\wedge$j<k $\Rightarrow$ [i..j]$\circ$[j+1..k]=[i..k]
7. L$\circ$(L'$\circ$L'')=(L$\circ$L')$\circ$L''

Lemma B.2.20 Reverse

$\forall\alpha,\beta$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$p:$\alpha\rightarrow\mathbb{B}$.$\forall$L,L':Seq($\alpha$).$\forall$a:$\alpha$.

1. rev([])=[]
2. rev(a.L)=rev(L)·a
3. rev([a]=[a]
4. rev([f(x)|x$\in$L$\wedge$p(x)])=[f(x)|x$\in$rev(L)$\wedge$p(x)]
5. rev(L·a)=a.rev(L)
6. rev(L$\circ$L')=rev(L')$\circ$rev(L)
7. rev(rev(L))=L

Lemma B.2.21 Domain

$\forall\alpha$:TYPES.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{N}$.

1. domain([])=$\emptyset$
2. domain(a.L)=domain(L)+(|L|+1)
3. domain([a])=$\{$1$\}$
4. L$\sqsubseteq$L' $\Rightarrow$ domain(L)$\subseteq$domain(L')
5. domain(L·a)=domain(L)+(|L|+1)
6. i$\leq$|L| $\Rightarrow$ domain(ins(L,i,a))=domain(L)+(|L|+1)
7. i$\leq$|L| $\Rightarrow$ domain(del(L,i))=domain(L)-|L|
8. domain(L$\circ$L') = domain(L)+domain(L')
9. domain(rev(L))=domain(L)

Lemma B.2.22 Range

$\forall\alpha,\beta$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$p:$\alpha\rightarrow\mathbb{B}$.$\forall$L,L':Seq($\alpha$).$\forall$a:$\alpha$.$\forall$i,j:$\mathbb{Z}$.

1. range([])=$\emptyset$
2. range(a.L)=range(L)+a
3. range([i..j])=$\{$i..j$\}$
4. L$\sqsubseteq$L' $\Rightarrow$ range(L)$\subseteq$range(L')
4. range([f(x)|x$\in$L$\wedge$p(x)])=$\{$f(x)|x$\in$range(L)$\wedge$p(x)$\}$
5. range(L·a)=range(L)+a
6. i$\leq$|L|+1 $\Rightarrow$ range(ins(L,i,a))=range(L)+a
7. range(L$\circ$L') = range(L)$\cup$range(L')
8. range(rev(L)) = range(L)

Lemma B.2.23 Reduce

$\forall\alpha$:TYPES.$\forall$bop:$\alpha^2\rightarrow\alpha$.$\forall$L:Seq($\alpha$).$\forall$a:$\alpha$.

1. reduce(bop,[a]) = a
2. $\neg$null?(L) $\Rightarrow$ reduce(bop,a.L) = bop(reduce(bop,L),a)

Lemma B.2.24 Nodups

$\forall\alpha$:TYPES.$\forall$L,L':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{Z}$.

1. nodups([])
2. nodups(a.L) $\Leftrightarrow$ nodups(L) $\wedge$ a$\notin$L
3. L$\sqsubseteq$L' $\Rightarrow$ nodups(L') $\Rightarrow$ nodups(L)
4. nodups[i..j]
5. nodups(L) $\Leftrightarrow$ |L| = |range(L)|
6. nodups(L·a) $\Leftrightarrow$ nodups(L) $\wedge$ a$\notin$L
7. i$\leq$|L| $\Rightarrow$ nodups(ins(L,i,a)) $\Leftrightarrow$ nodups(L) $\wedge$ a$\notin$L
8. nodups(L$\circ$L') $\Leftrightarrow$ nodups(L) $\wedge$ nodups(L') $\wedge$ $\forall$x$\in$L.x$\notin$(L')
9. nodups(rev(L)) $\Leftrightarrow$ nodups(L)

Lemma B.2.25 Difference

$\forall\alpha$:TYPES.$\forall$L:Seq(α).$\forall$a:α.

1. []-a=[]
2. a.L-a=L
3. a$\in$L $\Rightarrow$ $\exists$k$\in$domain(L).L=$\mathtt{L}_{[1..k-1]}\circ$a.$\mathtt{L}_{[k+1..|L|]}$

Lemma B.2.26 Rearranges

$\forall\alpha,\beta$:TYPES.$\forall$L,L',S,S':Seq(α).$\forall$a:α.$\forall$i:$\mathbb{N}$.$\forall$f:$\alpha\to\beta$.$\forall$p:$\alpha\to\mathbb{B}$.$\forall$g:$\mathbb{Z}$

1. rearranges([],S) $\Leftrightarrow$ S=[]
2. rearranges(a.L,S) $\Leftrightarrow$ a$\in$S $\wedge$ rearranges(L,S-a)
3. rearranges(L,S) $\Rightarrow$ $\forall$x$\in$L.x$\in$S
4. rearranges(L,S) $\Leftrightarrow$ |L| = |S|
5. rearranges(L·a,S) $\Leftrightarrow$ a$\in$S $\wedge$ rearranges(L,S-a)
6. i$\leq$|L| $\Rightarrow$ rearranges(ins(L,i,a),S) $\Leftrightarrow$ a$\in$S $\wedge$ rearranges(L,S-a)
7. rearranges(L,S) $\wedge$ rearranges(L',S')) $\Rightarrow$ rearranges(L$\circ$L',S$\circ$S')
8. rearranges(L,S) $\Rightarrow$ domain(L)=domain(S)
9. rearranges(L,S) $\Rightarrow$ range(L)=range(S)
10. rearranges(L,rev(L))
11. rearranges(L,L)
12. rearranges(L,S) $\Leftrightarrow$ rearranges(S,L)
13. rearranges(L,L') $\wedge$rearranges(L',S)) $\Rightarrow$ rearranges(L,S)
14. rearranges($\mathtt{L}_{<g}\circ\mathtt{L}_{\geq g}$,L)
15. rearranges(L,S) $\Leftrightarrow$ $\forall$a$\in$L. a$\in$S $\wedge$ rearranges(L-a,S-a)
16. rearranges(L,S) $\Rightarrow$ rearranges([f(x)|x$\in$L$\wedge$p(x)],[f(x)|x$\in$S$\wedge$p(x)])

B.3 Endliche Abbildungen

Der Typ der endlichen Abbildungen ist ein generischer Datentyp, der auf der Basis der Konzepte `Map`, `=`, $\{\!|\,|\!\}$, `extend`, `apply` und `domain` eingeführt werden kann. Die einfachste Form einer Implementierung ist die Verwendung von Listen von Paaren (Tabellen).

BASISKONZEPTE

Definition B.3.1 (Theory Implementation of Finite Maps)

$$
\begin{array}{ll}
\{\!|\,|\!\} & \equiv \texttt{[]} \\
\mapsto\! ab & \equiv \langle a,b\rangle \\
\texttt{extend} & \equiv \lambda\texttt{M,a,b. }(\mapsto\!\texttt{ab.M}) \\
\texttt{mapind}(M;t_b;a,b,M',FM'.t_{ind}) & \equiv \texttt{list\_ind}(M;t_b;\texttt{ ab},M',FM'.\texttt{ let ab=}\langle a,b\rangle\texttt{ in }t_{ind}) \\
\texttt{apply} & \equiv \lambda\texttt{M,y.mapind(M;}\infty\texttt{;a,b,M',appM'.} \\
 & \qquad\qquad \lambda\texttt{x.if x=a then b else appM'(x)) (y)} \\
M(a) & \equiv \texttt{apply}(M,a) \\
\texttt{domain} & \equiv \lambda\texttt{M. }\{\texttt{x.1}\,|\,\texttt{x}\in\texttt{range(M)}\} \\
\texttt{=} & \equiv \lambda\texttt{M,M'. domain(M)=domain(M')} \wedge \forall\texttt{x}\in\texttt{domain(M).M(x)=M'(x)} \\
\texttt{Map}(\alpha,\beta) & \equiv \texttt{M,M':Seq}(\alpha\times\beta)\texttt{//M=M'}
\end{array}
$$

Lemma B.3.2 Axioms of Finite Maps

$\forall\alpha,\beta,\gamma\texttt{:TYPES.}\forall\texttt{M,M':Map}(\alpha,\beta)\texttt{.}\forall\texttt{a,a':}\alpha\texttt{.}\forall\texttt{b:}\beta\texttt{.}\forall\texttt{P:PROP(Map}(\alpha,\beta)\texttt{)}.$

1. $\texttt{Map}(\alpha,\beta) \in \texttt{TYPES}$
2. $\{\!|\,|\!\} \in \texttt{Map}(\alpha,\beta)$
3. $\texttt{apply} \in \texttt{Map}(\alpha,\beta)\times\alpha\not\to\beta$
4. $\texttt{extend} \in \texttt{Map}(\alpha,\beta)\times\alpha\times\beta\to\texttt{Map}(\alpha,\beta)$
5. $\texttt{domain} \in \texttt{Map}(\alpha,\beta)\to\texttt{Set}(\alpha)$
6. $\texttt{extend(M,a,b)(a)=b}$
7. $\texttt{a'}\neq\texttt{a} \Rightarrow \texttt{extend(M,a,b)(a')=M(a')}$
8. $\texttt{domain}(\{\!|\,|\!\})=\emptyset$
9. $\texttt{domain(extend(M,a,b))=domain(M)+a}$
10. $\texttt{M=M'} \Leftrightarrow \texttt{domain(M)=domain(M')} \wedge \forall\texttt{x}\in\texttt{domain(M).M(x)=M'(x)}$
11. $\forall\texttt{g:}\gamma\texttt{.}\forall\texttt{h:}(\gamma\times\texttt{Map}(\alpha,\beta)\times\alpha)\to\beta\texttt{.}\exists\texttt{f:Map}(\alpha,\beta)\to\beta\texttt{.}$
    $\texttt{f}(\{\!|\,|\!\})\texttt{ = g} \wedge \forall\texttt{M:Map}(\alpha,\beta)\texttt{.}\forall\texttt{a:}\alpha\texttt{.}\forall\texttt{b:}\beta\texttt{. a}\notin\texttt{domain(M)} \Rightarrow \texttt{f(extend(M,a,b)) = h(f(M),M,a,b)}$
12. $(\texttt{P}(\{\!|\,|\!\}) \wedge \forall\texttt{M:Map}(\alpha,\beta)\texttt{.}\forall\texttt{a:}\alpha\texttt{.}\forall\texttt{b:}\beta\texttt{.P(M)}\Rightarrow\texttt{P(extend(M,a,b))}) \Rightarrow \forall\texttt{M:Map}(\alpha,\beta)\texttt{.P(M)}$

Lemma B.3.3 Finite Constructability

$\forall\alpha,\beta\texttt{:TYPES.}\forall\texttt{M:Map}(\alpha,\beta).$

1. $\texttt{M=}\{\!|\,|\!\} \vee \exists\texttt{a:}\alpha\texttt{.}\exists\texttt{b:}\beta\texttt{.}\exists\texttt{M':Map}(\alpha,\beta)\texttt{. a}\notin\texttt{domain(M)} \wedge \texttt{M=extend(M,a,b)}$

ABGELEITETE KONZEPTE

Definition B.3.4 (Map Vocabulary)

$$
\begin{array}{ll}
\{\!|\,\textit{map-list-exp}\,|\!\} & \equiv \textit{map-list-exp}\texttt{.nil} \\
\texttt{let }M\texttt{=extend}(M',a,b)\texttt{ in }e & \equiv \texttt{mapind}(M;\ \infty;\ a,b,M',\_,e) \\
\sqsubseteq & \equiv \lambda\texttt{M,M'. }\forall\texttt{x}\in\texttt{domain(M).M(x)=M'(x)} \\
\texttt{range} & \equiv \lambda\texttt{M.}\{\texttt{M(x)}\,|\,\texttt{x}\in\texttt{domain(M)}\} \\
\{\!|\mapsto\! f_x g_x\,|\,x\in S \wedge p_x\,|\!\} & \equiv \texttt{setind}(S;\ \{\!|\,|\!\};\texttt{ a,\_,GSF.} \\
 & \qquad \texttt{if }p_x\texttt{[a/}x\texttt{] then extend(GSF,}f_x\texttt{[a/}x\texttt{],}g_x\texttt{[a/}x\texttt{]) else GSF)} \\
\{\!|\mapsto\! f_x g_x\,|\,x\in S\,|\!\} & \equiv \{\!|\mapsto\! f_x g_x\,|\,x\in S\wedge\texttt{true}\,|\!\} \\
\circ & \equiv \lambda\texttt{M,M'.}\{\!|\mapsto\!\texttt{xM'(M(x))}\,|\,\texttt{x}\in\texttt{domain(M)}\wedge\texttt{M(x)}\in\texttt{domain(M')}\,|\!\} \\
|M| & \equiv |\texttt{domain}(M)|
\end{array}
$$

Lemma B.3.5 Operator Signatures

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$g:$\alpha\rightarrow\gamma$.$\forall$p:$\alpha\rightarrow$Bool.

1. $\sqsubseteq$ $\in$ Map(α,β)$^2\rightarrow$Bool
2. range $\in$ Map(α,β)$\rightarrow\beta$
3. λS. {\|$\mapsto$f(x)g(x)\|x$\in$S $\wedge$ p(x)\|} $\in$ Set(α)$\rightarrow$Map(β,γ)
4. $\circ$ $\in$ Map(α,β)$\times$Map(β,γ)$\rightarrow$Map(α,γ)
5. λM. \|M\| $\in$ Map(α,β)$\rightarrow\mathbb{N}$

Lemma B.3.6 extend

$\forall\alpha,\beta$:TYPES.$\forall$M:Map(α,β).$\forall$a:α.$\forall$b:β.

1. extend(M,a,b)$\neq${\| \|}
2. M(a)=b $\Rightarrow$ extend(M,a,b)=M
3. M(a)$\neq$b $\Rightarrow$ extend(M,a,b)$\neq$M

Lemma B.3.7 Domain

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$g:$\alpha\rightarrow\gamma$.$\forall$p:$\alpha\rightarrow$Bool.$\forall$S:Set($\alpha$).$\forall$M:Map($\alpha$,$\beta$).$\forall$M':Map($\beta$,$\gamma$).

1. domain({\|$\mapsto$f(x)g(x)\|x$\in$S$\wedge$p(x)\|}) = {f(x)\|x$\in$S$\wedge$p(x)}
2. domain(M$\circ$M')={x\|x$\in$domain(M)$\wedge$M(x)$\in$domain(M')}
3. domain(M$\circ$M')$\subseteq$domain(M)

Lemma B.3.8 Range

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$g:$\alpha\rightarrow\gamma$.$\forall$p:$\alpha\rightarrow$Bool.$\forall$M:Map($\alpha$,$\beta$).$\forall$M':Map($\beta$,$\gamma$).$\forall$a:$\alpha$.$\forall$b:$\beta$.$\forall$S:Set($\alpha$).

1. range({\| \|}) = $\emptyset$
2. a$\notin$domain(M) $\Rightarrow$ range(extend(M,a,b))=range(M)+b
3. range({\|$\mapsto$f(x)g(x)\|x$\in$S$\wedge$p(x)\|})={g(x)\|x$\in$S$\wedge$p(x)}
4. range(M$\circ$M')={M'(M(x))\|x$\in$domain(M)$\wedge$M(x)$\in$domain(M')}
5. range(M$\circ$M')$\subseteq$range(M')

Lemma B.3.9 Submap

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$g:$\alpha\rightarrow\gamma$.$\forall$p:$\alpha\rightarrow$Bool.$\forall$M,M',M'':Map($\alpha$,$\beta$).$\forall$a:$\alpha$.$\forall$b:$\beta$.$\forall$S,S':Set($\alpha$).

1. {\| \|}$\sqsubseteq$M
2. M$\sqsubseteq${\| \|} $\Leftrightarrow$ M={\| \|}
3. extends(M,a,b)$\sqsubseteq$M' $\Leftrightarrow$ M$\sqsubseteq$M' $\wedge$ a$\in$domain(M') $\wedge$ M'(a)=
4. a$\notin$domain(M') $\wedge$ M$\sqsubseteq$M' $\Rightarrow$ M$\sqsubseteq$extends(M',a,b)
5. S$\subseteq$S' $\Rightarrow$ {\|$\mapsto$f(x)g(x)\|x$\in$S$\wedge$p(x)\|}$\sqsubseteq${\|$\mapsto$f(x)g(x)\|x$\in$S'$\wedge$p(x)\|}
6. M$\sqsubseteq$M' $\Rightarrow$ domain(M)$\subseteq$main(M')
7. M$\sqsubseteq$M' $\Rightarrow$ range(M)$\subseteq$range(M)
8. M$\sqsubseteq$M
9. M$\sqsubseteq$M' $\wedge$ M'$\sqsubseteq$M $\Leftrightarrow$ M=M'
10. M$\sqsubseteq$M' $\wedge$ M'$\sqsubseteq$M'' $\Rightarrow$ M$\sqsubseteq$M''

Lemma B.3.10 General Map Former

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$f:$\alpha\rightarrow\beta$.$\forall$g:$\alpha\rightarrow\gamma$.$\forall$p:$\alpha\rightarrow$Bool.$\forall$S:Set($\alpha$).$\forall$a:$\alpha$.

1. Map$\mapsto$f(x)g(x)\|x$\in\emptyset$ $\wedge$ p(x)={\| \|}
2. p(a) $\Rightarrow$ {\|$\mapsto$f(x)g(x)\|x$\in$(S+a)$\wedge$p(x)\|}=extend({\|$\mapsto$f(x)g(x)\|x$\in$S$\wedge$p(x)\|},f(a),g(a))
3. $\neg$p(a) $\Rightarrow$ {\|$\mapsto$f(x)g(x)\|x$\in$(S+a)$\wedge$p(x)\|}={\|$\mapsto$f(x)g(x)\|x$\in$S$\wedge$p(x)\|}
4. $\forall$a$\in$S. p(a) $\Rightarrow$ {\|$\mapsto$f(x)g(x)\|x$\in$S $\wedge$ p(x)\|}(f(a)) = g(a)

Lemma B.3.11 Map Composition

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$M:Map($\alpha$,$\beta$).$\forall$M':Map($\beta$,$\gamma$).$\forall$a:$\alpha$.$\forall$b:$\beta$.$\forall$c:$\gamma$.

1. {| |}∘M= {| |}
2. b ∈ domain(M') ⇒ extend(M,a,b)∘M' = extend(M∘M',a,M'(b))
3. b ∉ domain(M') ⇒ extend(M,a,b)∘M' = M∘M'
4. M∘{| |}= {| |}
5. b ∉ rangeαM ⇒ M∘extend(M',b,c) = M∘M'

Lemma B.3.12 Map size

$\forall\alpha,\beta,\gamma$:TYPES.$\forall$M:Map($\alpha$,$\beta$).$\forall$M':Map($\beta$,$\gamma$).$\forall$a:$\alpha$.$\forall$b:$\beta$.

1. |{| |}| = 0
2. a ∈ domain(M) ⇒ |extends(M,a,b)| = |M|
3. a ∉ domain(M) ⇒ |extends(M,a,b)| = |M|+1
4. M⊑M' ⇒ |M| ≤ |M'|
5. |M∘M'| ≤ |M|
6. |M∘M'| ≤ |M'|

B.4 Costas Arrays

Die folgende Erweiterung der Theorie der endlichen Folgen ist nötig, um das Costas-Arrays Problem lösen zu können. Wie immer beschreiben die Lemmata Distributivgesetze, die zur Vereinfachung verwendet werden.

Definition B.4.1 (dtrow: Reihe in der Differenzentafel)

$\texttt{dtrow}(L,j) \equiv \texttt{[}L\texttt{[i]-}L\texttt{[i+}j\texttt{] | i} \in \texttt{[1..|}L\texttt{|-}j\texttt{]]}$

Lemma B.4.2 dtrow

∀L,L':Seq(ℤ).∀i:ℤ.∀j:ℕ.

1. dtrow([],j) = []
2. j≤|L| ⇒ dtrow(i.L,j) = (i-L[j]).dtrow(L,j)
3. j≠0 ⇒ dtrow([i],j) = []
4. L⊑L' ⇒ dtrow(L,j) ⊑ dtrow(L',j)
5. j≥|L| ⇒ dtrow(L,j) = []
6. j≤|L| ⇒ dtrow(L·i,j) = dtrow(L,j)·(L[|L|+1-j]-i)

B.5 Integer Segmente

Die folgende Erweiterung der Theorie der endlichen Folgen ist nötig, um das Problem der Maximalen Segmentsumme lösen zu können.

Definition B.5.1 (Segmentsummen und Maxima)

$\sum_{i=p}^{q} L\texttt{[i]} \equiv \texttt{reduce(+,[}L\texttt{[i]|i} \in \texttt{[}p..q\texttt{]])}$

$\{f_{pq} \,|\, q \in S \wedge p \in S_q\} \equiv \bigcup\{\ \{f_{pq} \,|\, p \in S_q\}\ \mid\ q \in S\}$

$m = \texttt{MAX}(S) \equiv m \in S \ \wedge\ \forall \texttt{x} \in S.\ \texttt{x} \leq m$

Man beachte, daß die Segmentsumme $\sum_{i=p}^{q}\texttt{L[i]}$ nur für $L\neq[]$ und $1\leq p\leq q\leq |L|$ definiert ist.

Lemma B.5.2 Segmentsumme

∀L:Seq(ℤ).∀a:ℤ.

1. $\sum_{i=1}^{1}\texttt{a.L[i]} = \texttt{a}$
2. ∀q∈domain(L). $\sum_{i=1}^{q+1}\texttt{a.L[i]} = \sum_{i=1}^{q}\texttt{L[i]+a}$
3. ∀q∈domain(L).∀p∈{1..q}. $\sum_{i=p+1}^{q+1}\texttt{a.L[i]} = \sum_{i=p}^{q}\texttt{L[i]}$
4. ∀q∈domain(L).∀p∈{1..q}. $\sum_{i=p}^{q}\texttt{L·a[i]} = \sum_{i=p}^{q}\texttt{L[i]}$
5. ∀p∈domain(L). $\sum_{i=p}^{|L|+1}\texttt{L·a[i]} = \sum_{i=p}^{|L|}\texttt{L[i]+a}$

Lemma B.5.3 Set Formers and Integer Ranges

∀f:ℤ→ℤ.∀g:ℤ×ℤ→ℤ.∀j,k:ℤ.

1. {f(x)|x∈{j+1..k+1}} = {f(x+1)|x∈{j..k}}
2. {g(x,y)|x∈{j+1..k+1} ∧ y∈{j+1..x}} = {g(x+1,y)|x∈{j..k} ∧ y∈{j+1..x+1}}
3. {g(x+1,y)|x∈{j..k}∧y∈{j+1..x+1}} = {g(x+1,y+1)|x∈{j..k}∧y∈{j..x}}
4. {f(x)|x∈{j..k}} = {f(x)|x∈{j+1..k}}+f(j)
5. {g(x,y)|x∈{j..k}∧y∈{j..x}} = {g(x,y)|x∈{j+1..k}∧y∈{j+1..x}} ∪ {g(x,j)|x∈{j+1..k}} + g(j,j)
6. {f(x)|x∈{j..j}} = {f(j)}
7. {g(x,y)|x∈{j..j} ∧ y∈{j..x}} = {g(j,j)}

Lemma B.5.4 Maximum

∀m,m',a:ℤ. ∀S,S':Set(ℤ).

1. ¬(m = MAX(∅))
2. m=MAX(S) ∧ m'=MAX(S) ⇒ m=m'
3. m=MAX(S) ⇒ max(a,m)=MAX(S+a)
4. a=MAX({a})
5. m=MAX(S) ∧ m'=MAX(S') ∧ S⊆S' ⇒ m≤m'
6. m=MAX(S) ⇒ m+a=MAX({x+a|x∈S})
7. m=MAX(S) ∧ m'=MAX(S') ⇒ max(m,m')=MAX(S∪S')