X,Y,Z:PNat (∀x,y,z∈PNAT) 省略

Theorem1 結合則

Xに対して帰納法を適用し以下を証明する。

(∀x:PNat)(∀y,z:PNat) ((x+y)+z = x+(y+z))

① 基底ケース (x=0の時,(0+y)+z=0+(y+z))

左辺 (0+y)+z → y+z ‥by(+1)

右辺 0+(y+z) → y+z ‥by(+1) QED

② 帰納ケース ((S(x)+y)+z=S(x)+(y+z)) (仮定 (x+y)+z = x+(y+z) ‥(IH))

左辺 (S(x)+y)+z → S(x+y)+z ‥by(+2)

→ S((x+y)+z) ‥by(+2)

→ S(x+(y+z)) ‥by(IH)

右辺 S(x)+(y+z) → S(x+(y+z)) ‥by(+2) QED

Theorem2 交換則 (X+Y = Y+X) (∀X,Y:PNAT)

Xに対して帰納法を適用し、X+Y = Y+Xを証明する。

① Base case (X=0の時)

左辺 0+Y → Y ‥by(+1)

右辺 Y+0 → Y ‥by(rz+)

② 帰納ケース (仮定 x+Y = Y+x ‥IH)

左辺 S(x)+Y → S(x+Y) ‥by(+2)

→ S(Y+x) ‥by(rs+)

右辺 Y+S(x) → S(Y+x) ‥by(rs+) QED

Theorem3 [_*_の結合律]

(X*Y)*Z = X*(Y*Z)

Xに対して構造帰納法を適用しこれを証明する

① Base Case

左辺 (0*Y)*Z → 0*Z by(*1)

→ 0 by(*1)

右辺 0*(Y*Z) → 0 by(*1)

② Induction Case (仮定 (x*Y)*Z = x*(Y*Z) ‥(IH))

左辺 (S(x)*Y)*Z → ((x*Y)+Y)*Z ‥by(*2)

→ ((x*Y)*Z)+(Y*Z) ‥by(d*+) (X+Y)*Z = (X*Z)+(Y*Z)

→ (x*(Y*Z))+(Y*Z) ‥by(IH)

右辺 S(x)*(Y*Z) → (x*(Y*Z))+(Y*Z) ‥by(*2)

QED

Theorem4 [Commutativity of _*_ (comm*)]

X*Y = Y*X

Xに対して構造帰納法を適用しこれを証明する

① Base Case

左辺 0*Y → 0 ‥by(*1)

右辺 Y*0 → 0 ‥by(rz*)

② Induction Case (仮定 x*Y=Y*x ‥(IH))

左辺 S(x)*Y → (x*Y)+Y ‥by(*2)

→ (Y*x)+Y ‥by(IH)

右辺 Y*S(x) → (Y*x)+Y by(rs*)

QED

Theorem5 [規再帰のコレクトネス]

Xに対して構造帰納法を適用しこれを証明する

fact1(X) = fact2(X)

① Base case

左 fact1(0) → S(0) ‥by(f1-1)

右 fact2(0) → sfact2(0,S(0)) ‥by(f2)

→ S(0) ‥by(sf2-1)

② induction case (fact1(x) = fact2(x) ‥IH)

左 fact1(S(x)) → S(x)*fact1(x) ‥by(f1-2)

→ S(x)*fact2(x) ‥by(IH)

→ S(x)*sfact2(x,S(0)) ‥by(f2)

→ sfact2(x,S(x)*S(0)) ‥by(P-sf2)

右 fact2(S(x)) → sfact2(S(x),S(0)) ‥by(f2)

→ sfact2(x,S(x)*S(0)) by(sf2-2)

QED

Lemma1 [Right Zero of _+_ (rz+)] X+0 = X (∀X:PNat)

Xに対して構造帰納法を適用しこれを証明する

① Base case

0+0 → 0 by(+1)

② 帰納ケース (x+0 = x ‥(IH))

左辺 S(x)+0 → S(x+0) ‥(+2)

→ S(x) ‥(IH)

右辺 S(x)

QED

Lemma2 X+S(Y) = S(X+Y) (∀X,Y:PNat)

Xに対して構造帰納法を適用しこれを証明する

① Base Case

左辺 0+S(Y) → S(Y) by(+1)

右辺 S(0+Y) → S(Y) by(+1)

② 帰納ケース (仮定 x+S(Y) = S(x+Y) ‥(IH))

左辺 S(x)+S(Y) → S(x+S(Y)) ‥by(+2)

→ S(S(x+Y)) ‥by(IH)

右辺 S(S(x)+Y) → S(S(x+Y)) ‥by(+2)

QED

Lemma3 [Distributive law of _*_ over _+_ (d*+)]

(X+Y)*Z = (X*Z)+(Y*Z)

Xに対して構造帰納法を適用しこれを証明する

① Base Case (x=0)

左辺 (0+Y)*Z → Y*Z by(+1)

右辺 (0*Z)+(Y*Z) → 0+(Y*Z) by(*1)

→ Y*Z by(+1)

② Induction Case (仮定: (x+Y)*Z = (x*Z)+(Y*Z) ‥(IH))

左辺 (S(x)+Y)*Z → S(x+Y)*Z ‥by(+2)

→ ((x+Y)*Z)+Z ‥by(*2)

→ ((x*Z)+(Y*Z))+Z by(IH)

→ (x*Z)+((Y*Z)+Z) by(assoc+)

→ (x*Z)+(Z+(Y*Z)) by(comm+)

右辺 (S(x)*Z)+(Y*Z) → ((x*Z)+Z)+(Y*Z) by(*2)

→ (x*Z)+(Z+(Y*Z)) by(assoc+)

QED

Lemma4 [Right Zero of _*_ (rz*)]

X*0 = 0

Xに対して構造帰納法を適用しこれを証明する

① Base Case

0*0 → 0 ‥by(*1)

② Induction case (x*0 = 0 ‥(IH))

左辺 S(x)*0 → (x*0)+0 ‥by(*2)

→ 0+0 ‥by(IH)

→ 0 ‥by(+1)

右辺 0

QED

Lemma5 [Right Successor _*_ (rs*)]

X*S(Y) = (X*Y)+X (∀X,Y:PNat)

Xに対して構造帰納法を適用しこれを証明する

① Base Case

左辺 0*S(Y) → 0 ‥by(*1)

右辺 (0*Y)+0 → 0+0 by(*1)

→ 0 by(+1)

② Induction Case (x*S(Y) = (x*Y)+x ‥(IH))

左辺 S(x)*S(Y) → (x*S(Y))+S(Y) ‥by(*2)

→ ((x*Y)+x)+S(Y) ‥by(IH)

→ S(Y)+((x*Y)+x) ‥by(comm+)

→ S(Y+((x*Y)+x)) ‥by(+2)

右辺 (S(x)*Y)+S(x) → ((x*Y)+Y)+S(x) ‥by(*2)

→ S(x)+((x*Y)+Y) ‥by(comm+)

→ S(x+((x*Y)+Y)) by(+2)

→ S(((x*Y)+Y)+x) by(comm+)

→ S((Y+(x*Y))+x) by(comm+)

→ S(Y+((x*Y)+x)) by(assoc+)

QED

Lemma6 [Property of sfact2 (P-sf2)]

Y*sfact2(X,Z) = sfact2(X,Y*Z)

Xに対して構造帰納法を適用しこれを証明する

① Base Case

左 Y*sfact2(0,Z) → Y*Z ‥by(sf2-1)

右 sfact2(0,Y*Z) → Y*Z ‥by(sf2-1)

② Induction Case (Y*sfact2(S(x),Z) = sfact2(S(x),Y*Z) ‥(IH))

左 Y*sfact2(S(x),Z) → Y*sfact2(x,S(x)*Z) by(sf2-2)

→ sfact2(x,Y*(S(x)*Z)) by(IH)

右 sfact2(S(x),Y*Z) → sfact2(x,S(x)*(Y*Z)) ‥by(sf2-2)

→ sfact2(x,(S(x)*Y)*Z) ‥by(assoc*)

→ sfact2(x,(Y*S(x))*Z) ‥by(comm*)

→ sfact2(x,Y*(S(x)*Z)) ‥by(assoc*)

QED