```
prod_fin_is_fin  THM

⊢  ∀t:T. Fin(T) ⇒ Fin(T×T)  by Unfold ‘finite‘ 0 THEN ExRepD
|
1. T : Type
2. T
3. n : ℕ
4. f : ℕn→T
5. Bij(ℕn; T; f)
⊢  ∃n:ℕ, f:(ℕn→T×T). Bij(ℕn; T×T; f)  by Assert (n>0)
|
|\
| .....assertion .....
| ⊢  n>0  by Assert (¬n = 0)
| |
| |\
| | .....assertion .....
| | ⊢  ¬n = 0  by (Analyze 0) THEN (Unfold ‘biject‘ -2)
| | |
| | 5. Inj(ℕn; T; f) & Surj(ℕn; T; f)
| | 6. n = 0
| | ⊢  False  by Unfold ‘surject‘ 5 THEN Analyze 5
| | |
| | 5. Inj(ℕn; T; f)
| | 6. ∀b:T. ∃a:ℕn. f(a) = b
| | 7. n = 0
| | ⊢   by (InstHyp [t] -2) THEN (Analyze -1)
| |
| .\
| . 6. ¬n = 0
| . ⊢   by Auto
|
.\
. 6. n>0
. ⊢   by InstConcl [n·n;λx.<f(x ÷ n),f(x rem n)>]
. |
. |\
. | .....set predicate .....
. | ⊢  0≤n·n  by BackThru Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a}
. |
. |\
. | 7. x : ℕ(n·n)
. | ⊢  0≤(x ÷ n)
. |   by Inst Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1} [x;n]
. |
. |\
. | 7. x : ℕ(n·n)
. | ⊢  (x ÷ n)<n
. |   by BackThru Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
. |
. |\
. | 7. x : ℕ(n·n)
. | ⊢  0≤(x rem n)
. |   by (Inst
. |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n    {rem_bounds_1}
```

```
. |       [x;n])
. |      THEN
. |      ProveProp
. |
. |\
. | 7. x : ℕ(n·n)
. | ⊢  (x rem n)<n
. |   by (Inst
. |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n    {rem_bounds_1}
. |       [x;n])
. |      THEN
. |      ProveProp
. |
. .\
. . ⊢  Bij(ℕ(n·n); T×T; λx.<f(x ÷ n),f(x rem n)>)
. . | by Analyze 5 THEN Analyze 0
. . |
. . |\
. . | 5. Inj(ℕn; T; f)
. . | 6. Surj(ℕn; T; f)
. . | 7. n>0
. . | ⊢  Inj(ℕ(n·n); T×T; λx.<f(x ÷ n),f(x rem n)>)
. . | | by Unfold ‘inject‘ 0 THEN Unfold ‘inject‘ 5
. . | |
. . | 5. ∀a1,a2:ℕn. f(a1) = f(a2) ⇒ a1 = a2
. . | 6. Surj(ℕn; T; f)
. . | 7. n>0
. . | ⊢  ∀a1,a2:ℕ(n·n).
. . | |  (λx.<f(x ÷ n),f(x rem n)>)(a1)
. . | |  =
. . | |  (λx.<f(x ÷ n),f(x rem n)>)(a2)
. . | |  ⇒
. . | |  a1 = a2  by Reduce 0 THEN RepD
. . | |
. . | |\
. . | | 8. a1 : ℕ(n·n)
. . | | 9. a2 : ℕ(n·n)
. . | | 10. <f(a1 ÷ n),f(a1 rem n)> = <f(a2 ÷ n),f(a2 rem n)>
. . | | ⊢  a1 = a2  by (Analyze -1) THEN (Reduce -1) THEN (Reduce -2)
. . | | |
. . | | 10. f(a1 ÷ n) = f(a2 ÷ n)
. . | | 11. f(a1 rem n) = f(a2 rem n)
. . | | ⊢
. . | | | by (InstHyp [a1 ÷ n;a2 ÷ n] 5)
. . | | |    THEN
. . | | |    (InstHyp [a1 rem n;a2 rem n] 5)
. . | | |

. . | | |\
. . | | | ⊢  0≤(a1 ÷ n)
. . | | |   by BackThru Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1}
. . | | |
. . | | |\
. . | | | ⊢  (a1 ÷ n)<n
. . | | |   by BackThru
. . | | |      Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
```

```
. . | | |
. . | | |\
. . | | | ⊢  0≤(a2 ÷ n)
. . | | |   by BackThru Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1}
. . | | |
. . | | |\
. . | | | ⊢  (a2 ÷ n)<n
. . | | |   by BackThru
. . | | |      Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
. . | | |
. . | | |\
. . | | | 12. (a1 ÷ n) = (a2 ÷ n)
. . | | | ⊢  0≤(a1 rem n)
. . | | |   by (Inst
. . | | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | | |       {rem_bounds_1}
. . | | |       [a1;n])
. . | | |      THEN
. . | | |      ProveProp
. . | | |
. . | | |\
. . | | | 12. (a1 ÷ n) = (a2 ÷ n)
. . | | | ⊢  (a1 rem n)<n
. . | | |   by (Inst
. . | | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | | |       {rem_bounds_1}
. . | | |       [a1;n])
. . | | |      THEN
. . | | |      ProveProp
. . | | |
. . | | |\
. . | | | 12. (a1 ÷ n) = (a2 ÷ n)
. . | | | ⊢  0≤(a2 rem n)
. . | | |   by (Inst
. . | | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | | |       {rem_bounds_1}
. . | | |       [a2;n])
. . | | |      THEN
. . | | |      ProveProp
. . | | |
. . | | |\
. . | | | 12. (a1 ÷ n) = (a2 ÷ n)
. . | | | ⊢  (a2 rem n)<n
. . | | |   by (Inst
. . | | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | | |       {rem_bounds_1}
. . | | |       [a2;n])
. . | | |      THEN
. . | | |      ProveProp
. . | | |
. . | | .\
. . | | . 12. (a1 ÷ n) = (a2 ÷ n)
. . | | . 13. (a1 rem n) = (a2 rem n)
. . | | . ⊢
. . | | . | by (Inst
```

```
. . | | . |     Thm* ∀a:ℤ, n:ℤ^-0. a = (a ÷ n)·n+(a rem n)
. . | | . |     {div_rem_sum}
. . | | . |     [a1;n])
. . | | . |    THEN
. . | | . |    (Inst
. . | | . |     Thm* ∀a:ℤ, n:ℤ^-0. a = (a ÷ n)·n+(a rem n)
. . | | . |     {div_rem_sum}
. . | | . |     [a2;n])
. . | | . |
. . | | . 14. a1 = (a1 ÷ n)·n+(a1 rem n)
. . | | . 15. a2 = (a2 ÷ n)·n+(a2 rem n)
. . | | . ⊢   by Analyze
. . | |
. . | |\
. . | | 8. a1 : ℕ(n·n)
. . | | 9. ℕ(n·n)
. . | | ⊢  0≤(a1 ÷ n)
. . | |   by BackThru Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1}
. . | |
. . | |\
. . | | 8. a1 : ℕ(n·n)
. . | | 9. ℕ(n·n)
. . | | ⊢  (a1 ÷ n)<n
. . | |   by BackThru
. . | |      Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
. . | |
. . | |\
. . | | 8. a1 : ℕ(n·n)
. . | | 9. ℕ(n·n)
. . | | ⊢  0≤(a1 rem n)
. . | |   by (Inst
. . | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | |       {rem_bounds_1}
. . | |       [a1;n])
. . | |      THEN
. . | |      ProveProp
. . | |

. . | |\
. . | | 8. a1 : ℕ(n·n)
. . | | 9. ℕ(n·n)
. . | | ⊢  (a1 rem n)<n
. . | |   by (Inst
. . | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | |       {rem_bounds_1}
. . | |       [a1;n])
. . | |      THEN
. . | |      ProveProp
. . | |
. . | |\
. . | | 8. ℕ(n·n)
. . | | 9. a2 : ℕ(n·n)
. . | | ⊢  0≤(a2 ÷ n)
. . | |   by BackThru Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1}
. . | |
. . | |\
```

```
. . | | 8. ℕ(n·n)
. . | | 9. a2 : ℕ(n·n)
. . | | ⊢  (a2 ÷ n)<n
. . | |   by BackThru
. . | |      Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
. . | |
. . | |\
. . | | 8. ℕ(n·n)
. . | | 9. a2 : ℕ(n·n)
. . | | ⊢  0≤(a2 rem n)
. . | |   by (Inst
. . | |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | |       {rem_bounds_1}
. . | |       [a2;n])
. . | |      THEN
. . | |      ProveProp
. . | |
. . | .\
. . | . 8. ℕ(n·n)
. . | . 9. a2 : ℕ(n·n)
. . | . ⊢  (a2 rem n)<n
. . | .   by (Inst
. . | .       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . | .       {rem_bounds_1}
. . | .       [a2;n])
. . | .      THEN
. . | .      ProveProp
. . |
. . .\
. . . 5. Inj(ℕn; T; f)
. . . 6. Surj(ℕn; T; f)
. . . 7. n>0
. . . ⊢  Surj(ℕ(n·n); T×T; λx.<f(x ÷ n),f(x rem n)>)
. . . | by Unfold ‘surject‘ 6 THEN Analyze 0
. . . |
. . . 6. ∀b:T. ∃a:ℕn. f(a) = b
. . . 7. n>0
. . . 8. b : T×T
. . . ⊢  ∃a:ℕ(n·n). (λx.<f(x ÷ n),f(x rem n)>)(a) = b  by Analyze 8
. . . |
. . . 8. b1 : T
. . . 9. b2 : T
. . . ⊢  ∃a:ℕ(n·n). (λx.<f(x ÷ n),f(x rem n)>)(a) = <b1,b2>
. . . | by (InstHyp [b1] 6) THEN (Analyze -1) THEN (InstHyp [b2] 6)
. . . |    THEN
. . . |    (Analyze -1)
. . . |
. . . 10. a : ℕn
. . . 11. f(a) = b1
. . . 12. a1 : ℕn
. . . 13. f(a1) = b2
. . . ⊢   by InstConcl [a·n+a1]
. . . |
. . . |\
. . . | ⊢  0≤a·n+a1
```

```
. . . |   by Inst Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a} [a;n]
. . . |
. . . |\
. . . | ⊢  a·n+a1<n·n  by Assert (a·n≤(n-1)·n)
. . . | |
. . . | |\
. . . | | .....assertion .....
. . . | | ⊢  a·n≤(n-1)·n
. . . | |   by Inst
. . . | |      Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b    {mul_preserves_le}
. . . | |      [a;n-1;n]
. . . | |
. . . | .\
. . . | . 14. a·n≤(n-1)·n
. . . | . ⊢   by Assert (n+(n-1)·n = n·n)
. . . | . |
. . . | . 15. n+(n-1)·n = n·n
. . . | . ⊢   by Auto
. . . |
. . . |\
. . . | ⊢  (λx.<f(x ÷ n),f(x rem n)>)(a·n+a1) = <b1,b2>
. . . | | by (Reduce 0) THEN Analyze
. . . | |
. . . | |\
. . . | | ⊢  f((a·n+a1) ÷ n) = b1  by Assert (a = ((a·n+a1) ÷ n))
. . . | | |
. . . | | |\
. . . | | | .....assertion .....
. . . | | | ⊢  a = ((a·n+a1) ÷ n)  by Analyze
. . . | | | |
. . . | | | ⊢  a = ((a·n+a1) ÷ n)
. . . | | | | by (Thin 11 THEN Analyze 10) THEN (IntInd 10)
. . . | | | |
. . . | | | |\
. . . | | | | 10. a1 : ℕn
. . . | | | | 11. f(a1) = b2
. . . | | | | 12. 0≤0
. . . | | | | 13. 0<n
. . . | | | | ⊢  0 = ((0·n+a1) ÷ n)
. . . | | | |   by Inst
. . . | | | |      Thm* ∀a:ℕ, n:ℕ+. a<n ⇒ (a ÷ n) = 0
. . . | | | |      {div_base_case}
. . . | | | |      [a1;n]
. . . | | | |
. . . | | | .\
. . . | | | . 10. a1 : ℕn
. . . | | | . 11. f(a1) = b2
. . . | | | . 12. a : ℤ
. . . | | | . 13. 0<a
. . . | | | . 14. 0 ≤ a-1 < n ⇒ a-1 = (((a-1)·n+a1) ÷ n)
. . . | | | . 15. 0≤a
. . . | | | . 16. a<n
. . . | | | . ⊢
. . . | | | . | by (Analyze 14)
. . . | | | . |    THEN
```

```
. . . | | | . |    (Inst
. . . | | | . |     Thm* ∀a:ℕ, n:ℕ+. a≥n ⇒ (a ÷ n) = ((a-n) ÷ n)+1
. . . | | | . |     {div_rec_case}
. . . | | | . |     [a·n+a1;n])
. . . | | | . |
. . . | | | . |\
. . . | | | . | .....set predicate .....
. . . | | | . | 14. 0≤a
. . . | | | . | 15. a<n
. . . | | | . | 16. a-1 = (((a-1)·n+a1) ÷ n)
. . . | | | . | ⊢  0≤a·n+a1
. . . | | | . |   by Inst Thm* ∀a,b:ℕ. 0≤a·b    {mul_bounds_1a} [a;n]
. . . | | | . |
. . . | | | . .\
. . . | | | . . .....antecedent .....
. . . | | | . . 14. 0≤a
. . . | | | . . 15. a<n
. . . | | | . . 16. a-1 = (((a-1)·n+a1) ÷ n)
. . . | | | . . ⊢  a·n+a1≥n  by Assert (a·n≥n)
. . . | | | . . |
. . . | | | . . |\
. . . | | | . . | .....assertion .....
. . . | | | . . | ⊢  a·n≥n  by Assert (a≥1)
. . . | | | . . | |
. . . | | | . . | 17. a≥1
. . . | | | . . | ⊢
. . . | | | . . |   by Inst
. . . | | | . . |      Thm* ∀a,b:ℤ, n:ℕ. a≤b ⇒ n·a≤n·b
. . . | | | . . |      {mul_preserves_le}
. . . | | | . . |      [1;a;n]
. . . | | | . . |
. . . | | | . . .\
. . . | | | . . . 17. a·n≥n
. . . | | | . . . ⊢   by Auto
. . . | | |
. . . | | .\
. . . | | . 14. a = ((a·n+a1) ÷ n)
. . . | | . ⊢   by RWH (HypC -1) 11
. . . | |
. . . | .\
. . . | . ⊢  f((a·n+a1) rem n) = b2
. . . | . | by (Inst
. . . | . |     Thm* ∀a,b:ℕ, n:ℕ+. ((a+b·n) rem n) = (a rem n)
. . . | . |     {rem_invariant}
. . . | . |     [a1;a;n])
. . . | . |    THEN
. . . | . |    (Inst
. . . | . |     Thm* ∀a:ℕ, n:ℕ+. a<n ⇒ (a rem n) = a
. . . | . |     {rem_base_case}
. . . | . |     [a1;n])
. . . | . |
. . . | . 14. ((a1+a·n) rem n) = (a1 rem n)
. . . | . 15. (a1 rem n) = a1
. . . | . ⊢   by ArithSimp 0
. . . | . |
```

```
. . . | . ⊢  f((a1+a·n) rem n) = b2
. . . | . | by Assert (a1 = ((a1+a·n) rem n))
. . . | . |
. . . | . |\
. . . | . | .....assertion .....
. . . | . | ⊢  a1 = ((a1+a·n) rem n)  by Analyze
. . . | . |
. . . | . .\
. . . | . . 16. a1 = ((a1+a·n) rem n)
. . . | . . ⊢   by RWH (HypC -1) 13
. . . |
. . . .\
. . . . 14. a2 : ℕ(n·n)
. . . . ⊢  (λx.<f(x ÷ n),f(x rem n)>)(a2) ∈ T×T  by Reduce 0
. . . . |
. . . . |\
. . . . | ⊢  0≤(a2 ÷ n)
. . . . |   by BackThru Thm* ∀a:ℕ, n:ℕ+. 0≤(a ÷ n)    {div_bounds_1}
. . . . |
. . . . |\
. . . . | ⊢  (a2 ÷ n)<n
. . . . |   by BackThru
. . . . |      Thm* ∀n:ℕ+, x:ℕ(n·n). (x ÷ n)<n    {div_bounds_2}
. . . . |
. . . . |\
. . . . | ⊢  0≤(a2 rem n)
. . . . |   by (Inst
. . . . |       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . . . |       {rem_bounds_1}
. . . . |       [a2;n])
. . . . |      THEN
. . . . |      ProveProp
. . . . |
. . . . .\
. . . . . ⊢  (a2 rem n)<n
. . . . .   by (Inst
. . . . .       Thm* ∀a:ℕ, n:ℕ+. 0≤(a rem n) & (a rem n)<n
. . . . .       {rem_bounds_1}
. . . . .       [a2;n])
. . . . .      THEN
. . . . .      ProveProp
END
```