thm_2Einteger_2EINT__MOD__P (TMHnqpXWFffShQZeSJnAyFMuxriYS4FrHYn)

October 26, 2020

Definition 1 *We define* c_2Emin_2E_3D *to be* $\lambda A.\lambda x \in A.\lambda y \in A.inj\_\_o\ (x = y)$ *of type* $\iota \Rightarrow \iota$.

Definition 2 *We define* c_2Ebool_2ET *to be* $(ap\ (ap\ (\mathsf{c\_2Emin\_2E\_3D}\ (2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1$

Let $ty\_2Einteger\_2Eint : \iota$ be given. Assume the following.

$$nonempty\ ty\_2Einteger\_2Eint \tag{1}$$

Let $c\_2Einteger\_2Eint\_\_div : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Eint\_\_div \in ((ty\_2Einteger\_2Eint^{ty\_2Einteger\_2Eint})^{ty\_2Einteger\_2Eint}) \tag{2}$$

Let $c\_2Einteger\_2Eint\_\_mod : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Eint\_\_mod \in ((ty\_2Einteger\_2Eint^{ty\_2Einteger\_2Eint})^{ty\_2Einteger\_2Eint}) \tag{3}$$

Let $ty\_2Enum\_2Enum : \iota$ be given. Assume the following.

$$nonempty\ ty\_2Enum\_2Enum \tag{4}$$

Let $ty\_2Epair\_2Eprod : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow \forall A1.nonempty\ A1 \Rightarrow nonempty\ (ty\_2Epair\_2Eprod\ A0\ A1) \tag{5}$$

Let $c\_2Einteger\_2Eint\_\_REP\_\_CLASS : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Eint\_\_REP\_\_CLASS \in ((2^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)})^{ty\_2Einteger\_2} \tag{6}$$

Definition 3 *We define* c_2Emin_2E_40 *to be* $\lambda A.\lambda P \in 2^A.$**if** $(\exists x \in A.p\ (ap\ P\ x))$ **then** $(the\ (\lambda x.x \in A \wedge p$ *of type* $\iota \Rightarrow \iota$.

Definition 4 *We define* c_2Ebool_2E_21 *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap\ (\mathsf{c\_2Emin\_2E\_3D}\ (2^{A\_27}$

Definition 5 *We define* c_2Einteger_2Eint__REP *to be* $\lambda V0a \in ty\_2Einteger\_2Eint.(ap$ (c_2Emin_2E_40 $(ty$

Let $c\_2Einteger\_2Etint\_\_lt : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Etint\_\_lt \in ((2^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)})^{(ty\_2Epair\_2Eprod\ ty\_2Enum} \tag{7}$$

Definition 6 *We define* c_2Einteger_2Eint__lt *to be* $\lambda V0T1 \in ty\_2Einteger\_2Eint.\lambda V1T2 \in ty\_2Einteger\_2$

Definition 7 *We define* c_2Ebool_2EF *to be* $(ap$ (c_2Ebool_2E_21 $2)$ $(\lambda V0t \in 2.V0t))$.

Definition 8 *We define* c_2Emin_2E_3D_3D_3E *to be* $\lambda P \in 2.\lambda Q \in 2.inj\_\_o\ (p\ P \Rightarrow p\ Q)$ *of type* ι.

Definition 9 *We define* c_2Ebool_2E_7E *to be* $(\lambda V0t \in 2.(ap\ (ap$ c_2Emin_2E_3D_3D_3E $V0t)$ c_2Ebool_2EF

Definition 10 *We define* c_2Einteger_2Eint__le *to be* $\lambda V0x \in ty\_2Einteger\_2Eint.\lambda V1y \in ty\_2Einteger\_2E$

Let $c\_2Enum\_2EZERO\_\_REP : \iota$ be given. Assume the following.

$$c\_2Enum\_2EZERO\_\_REP \in omega \tag{8}$$

Let $c\_2Enum\_2EABS\_\_num : \iota$ be given. Assume the following.

$$c\_2Enum\_2EABS\_\_num \in (ty\_2Enum\_2Enum^{omega}) \tag{9}$$

Definition 11 *We define* c_2Enum_2E0 *to be* $(ap\ c\_2Enum\_2EABS\_\_num\ c\_2Enum\_2EZERO\_\_REP)$.

Let $c\_2Einteger\_2Eint\_\_of\_\_num : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Eint\_\_of\_\_num \in (ty\_2Einteger\_2Eint^{ty\_2Enum\_2Enum}) \tag{10}$$

Let $c\_2Einteger\_2Etint\_\_mul : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Etint\_\_mul \in (((ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)})^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty} \tag{11}$$

Let $c\_2Einteger\_2Etint\_\_eq : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Etint\_\_eq \in ((2^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)})^{(ty\_2Epair\_2Eprod\ ty\_2Enum} \tag{12}$$

Let $c\_2Einteger\_2Eint\_\_ABS\_\_CLASS : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Eint\_\_ABS\_\_CLASS \in (ty\_2Einteger\_2Eint^{(2^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)}} \tag{13}$$

Definition 12 *We define* c_2Einteger_2Eint__ABS *to be* $\lambda V0r \in (ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_$

Definition 13 *We define* c_2Einteger_2Eint__mul *to be* $\lambda V0T1 \in ty\_2Einteger\_2Eint.\lambda V1T2 \in ty\_2Eintege$

Let $c\_2Einteger\_2Etint\_\_add : \iota$ be given. Assume the following.

$$c\_2Einteger\_2Etint\_\_add \in (((ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty\_2Enum\_2Enum)})^{(ty\_2Epair\_2Eprod\ ty\_2Enum\_2Enum\ ty} \tag{14}$$

Definition 14 *We define* c_2Einteger_2Eint__add *to be* $\lambda V0T1 \in ty\_2Einteger\_2Eint.\lambda V1T2 \in ty\_2Eintege$

Definition 15 *We define* c_2Ebool_2E_3F *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ V0P\ (ap$ (c_2Emin_2E_40

Definition 16 *We define* c_2Ebool_2E_2F_5C *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap$ (c_2Ebool_2E_21 2) $(\lambda V2t \in$

Definition 17 *We define* c_2Ebool_2ECOND *to be* $\lambda A\_27a : \iota.(\lambda V0t \in 2.(\lambda V1t1 \in A\_27a.(\lambda V2t2 \in A\_27a.($

Definition 18 *We define* c_2Ebool_2E_5C_2F *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap$ (c_2Ebool_2E_21 2) $(\lambda V2t \in$

Assume the following.

$$True \tag{15}$$

Assume the following.

$$(\forall V0t1 \in 2.(\forall V1t2 \in 2.(((p\ V0t1) \Rightarrow (p\ V1t2)) \Rightarrow (((p\ V1t2) \Rightarrow (p\ V0t1)) \Rightarrow ((p\ V0t1) \Leftrightarrow (p\ V1t2)))))) \tag{16}$$

Assume the following.

$$(\forall V0t \in 2.(((True \Rightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge ((((p\ V0t) \Rightarrow True) \Leftrightarrow True) \wedge (((False \Rightarrow (p\ V0t)) \Leftrightarrow True) \wedge ((((p\ V0t) \Rightarrow (p\ V0t)) \Leftrightarrow True) \wedge (((p\ V0t) \Rightarrow False) \Leftrightarrow (\neg (p\ V0t)))))))) \tag{17}$$

Assume the following.

$$((\forall V0t \in 2.((\neg(\neg(p\ V0t))) \Leftrightarrow (p\ V0t))) \wedge (((\neg True) \Leftrightarrow False) \wedge ((\neg False) \Leftrightarrow True))) \tag{18}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.(V0x = V0x)) \tag{19}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.(\forall V1y \in A\_27a.((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \tag{20}$$

Assume the following.

$$(\forall V0t \in 2.(((True \Leftrightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge ((((p\ V0t) \Leftrightarrow True) \Leftrightarrow (p\ V0t)) \wedge (((False \Leftrightarrow (p\ V0t)) \Leftrightarrow (\neg (p\ V0t))) \wedge (((p\ V0t) \Leftrightarrow False) \Leftrightarrow (\neg (p\ V0t))))))) \tag{21}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0Q \in 2.(\forall V1P \in (2^{A\_27a}).((\forall V2x \in A\_27a.((p\ (ap\ V1P\ V2x)) \vee (p\ V0Q))) \Leftrightarrow ((\forall V3x \in A\_27a.(p\ (ap\ V1P\ V3x))) \vee (p\ V0Q)))))) \tag{22}$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0P \in 2.(\forall V1Q \in (2^{A\_27a}).((\forall V2x \in A\_27a.((p\ V0P) \vee (p\ (ap\ V1Q\ V2x)))) \Leftrightarrow ((p\ V0P) \vee (\forall V3x \in A\_27a.(p\ (ap\ V1Q\ V3x))))))) \tag{23}$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(\forall V2C \in 2.(((p\ V0A) \vee ((p\ V1B) \wedge (p\ V2C))) \Leftrightarrow (((p\ V0A) \vee (p\ V1B)) \wedge ((p\ V0A) \vee (p\ V2C))))))) \tag{24}$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(\forall V2C \in 2.((((p\ V1B) \wedge (p\ V2C)) \vee (p\ V0A)) \Leftrightarrow (((p\ V1B) \vee (p\ V0A)) \wedge ((p\ V2C) \vee (p\ V0A))))))) \tag{25}$$

Assume the following.

$$(\forall V0q \in ty\_2Einteger\_2Eint.((\neg(V0q = (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))) \Rightarrow (\forall V1p \in ty\_2Einteger\_2Eint.((V1p = (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_add}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_mul}\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_div\ V1p)\ V0q))\ V0q))\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1p)\ V0q))) \wedge (p\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ebool\_2ECOND}\ 2)\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V0q)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0})))\ (ap\ (ap\ \mathsf{c\_2Ebool\_2E\_2F\_5C}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V0q)\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1p)\ V0q)))\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1p)\ V0q))\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))))\ (ap\ (ap\ \mathsf{c\_2Ebool\_2E\_2F\_5C}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1p)\ V0q)))\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1p)\ V0q))\ V0q)))))))) \tag{26}$$

Assume the following.

$$(\forall V0i \in ty\_2Einteger\_2Eint.(\forall V1j \in ty\_2Einteger\_2Eint.(\forall V2m \in ty\_2Einteger\_2Eint.((\exists V3q \in ty\_2Einteger\_2Eint.((V0i = (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_add}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_mul}\ V3q)\ V1j))\ V2m)) \wedge (p\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ebool\_2ECOND}\ 2)\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V1j)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0})))\ (ap\ (ap\ \mathsf{c\_2Ebool\_2E\_2F\_5C}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V1j)\ V2m))\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ V2m)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))))\ (ap\ (ap\ \mathsf{c\_2Ebool\_2E\_2F\_5C}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))\ V2m))\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V2m)\ V1j)))))) \Rightarrow ((ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V0i)\ V1j) = V2m))))) \tag{27}$$

Assume the following.

$$(\forall V0t \in 2.((\neg(\neg(p\ V0t)))\Leftrightarrow(p\ V0t))) \tag{28}$$

Assume the following.

$$(\forall V0A \in 2.((p\ V0A)\Rightarrow((\neg(p\ V0A))\Rightarrow False))) \tag{29}$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(((\neg((p\ V0A)\vee(p\ V1B)))\Rightarrow False)\Leftrightarrow (((p\ V0A)\Rightarrow False)\Rightarrow((\neg(p\ V1B))\Rightarrow False))))) \tag{30}$$

Assume the following.

$$(\forall V0A \in 2.(\forall V1B \in 2.(((\neg((\neg(p\ V0A))\vee(p\ V1B)))\Rightarrow False)\Leftrightarrow ((p\ V0A)\Rightarrow((\neg(p\ V1B))\Rightarrow False))))) \tag{31}$$

Assume the following.

$$(\forall V0A \in 2.(((\neg(p\ V0A))\Rightarrow False)\Rightarrow(((p\ V0A)\Rightarrow False)\Rightarrow False))) \tag{32}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(((p\ V0p)\Leftrightarrow((p\ V1q)\Leftrightarrow(p\ V2r)))\Leftrightarrow(((p\ V0p)\vee((p\ V1q)\vee(p\ V2r)))\wedge(((p\ V0p)\vee((\neg(p\ V2r))\vee(\neg(p\ V1q))))\wedge(((p\ V1q)\vee((\neg(p\ V2r))\vee(\neg(p\ V0p))))\wedge((p\ V2r)\vee ((\neg(p\ V1q))\vee(\neg(p\ V0p))))))))))) \tag{33}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(((p\ V0p)\Leftrightarrow((p\ V1q)\wedge(p\ V2r)))\Leftrightarrow(((p\ V0p)\vee((\neg(p\ V1q))\vee(\neg(p\ V2r))))\wedge(((p\ V1q)\vee (\neg(p\ V0p)))\wedge((p\ V2r)\vee(\neg(p\ V0p))))))))) \tag{34}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(((p\ V0p)\Leftrightarrow((p\ V1q)\vee(p\ V2r)))\Leftrightarrow(((p\ V0p)\vee(\neg(p\ V1q)))\wedge(((p\ V0p)\vee(\neg(p\ V2r)))\wedge ((p\ V1q)\vee((p\ V2r)\vee(\neg(p\ V0p)))))))))) \tag{35}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(((p\ V0p)\Leftrightarrow((p\ V1q)\Rightarrow(p\ V2r)))\Leftrightarrow(((p\ V0p)\vee(p\ V1q))\wedge(((p\ V0p)\vee(\neg(p\ V2r)))\wedge((\neg(p\ V1q))\vee((p\ V2r)\vee(\neg(p\ V0p)))))))))) \tag{36}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(((p\ V0p)\Leftrightarrow(\neg(p\ V1q)))\Leftrightarrow(((p\ V0p)\vee (p\ V1q))\wedge((\neg(p\ V1q))\vee(\neg(p\ V0p))))))) \tag{37}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.(\forall V2r \in 2.(\forall V3s \in 2.(((p\ V0p) \Leftrightarrow (p\ (ap\ (ap\ (ap\ (\mathsf{c\_2Ebool\_2ECOND}\ 2)\ V1q)\ V2r)\ V3s))) \Leftrightarrow (((p\ V0p) \lor ((p\ V1q) \lor (\neg (p\ V3s)))) \land (((p\ V0p) \lor ((\neg (p\ V2r)) \lor (\neg (p\ V1q)))) \land (((p\ V0p) \lor ((\neg (p\ V2r)) \lor (\neg (p\ V3s)))) \land (((\neg (p\ V1q)) \lor ((p\ V2r) \lor (\neg (p\ V0p)))) \land ((p\ V1q) \lor ((p\ V3s) \lor (\neg (p\ V0p))))))))))))) \tag{38}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.((\neg ((p\ V0p) \Rightarrow (p\ V1q))) \Rightarrow (p\ V0p)))) \tag{39}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.((\neg ((p\ V0p) \Rightarrow (p\ V1q))) \Rightarrow (\neg (p\ V1q))))) \tag{40}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.((\neg ((p\ V0p) \lor (p\ V1q))) \Rightarrow (\neg (p\ V0p))))) \tag{41}$$

Assume the following.

$$(\forall V0p \in 2.(\forall V1q \in 2.((\neg ((p\ V0p) \lor (p\ V1q))) \Rightarrow (\neg (p\ V1q))))) \tag{42}$$

Assume the following.

$$(\forall V0p \in 2.((\neg (\neg (p\ V0p))) \Rightarrow (p\ V0p))) \tag{43}$$

Theorem 1

$$(\forall V0P \in (2^{ty\_2Einteger\_2Eint}).(\forall V1x \in ty\_2Einteger\_2Eint.(\forall V2c \in ty\_2Einteger\_2Eint.((\neg (V2c = (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))) \Rightarrow ((p\ (ap\ V0P\ (ap\ (ap\ c\_2Einteger\_2Eint\_\_mod\ V1x)\ V2c))) \Leftrightarrow (\exists V3k \in ty\_2Einteger\_2Eint.(\exists V4r \in ty\_2Einteger\_2Eint.((V1x = (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_add}\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_mul}\ V3k)\ V2c))\ V4r)) \land ((((p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V2c)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))) \land ((p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V2c)\ V4r)) \land (p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ V4r)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))))) \lor ((\neg (p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V2c)\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0})))) \land ((p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_le}\ (ap\ c\_2Einteger\_2Eint\_\_of\_\_num\ \mathsf{c\_2Enum\_2E0}))\ V4r)) \land (p\ (ap\ (ap\ \mathsf{c\_2Einteger\_2Eint\_\_lt}\ V4r)\ V2c))))) \land (p\ (ap\ V0P\ V4r))))))))))$$