

thm_2Ewords_2EWORD__NEG__MUL
(TMddNdfkJo8cStyLAyDMRgtJtM5atF7XuLf)

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 $c_2Ebool_2E_T$ to be $(ap (ap (c_2Emin_2E_3D (2^2))) (\lambda V0x \in 2.V0x)) (\lambda V1x \in 2.V1x)$

Let $ty_2Efc_2E_finite_image : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow nonempty (ty_2Efc_2E_finite_image A0) \quad (1)$$

Let $ty_2Ebool_2E_itself : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow nonempty (ty_2Ebool_2E_itself A0) \quad (2)$$

Let $c_2Ebool_2E_the_value : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow c_2Ebool_2E_the_value A_27a \in (ty_2Ebool_2E_itself A_27a) \quad (3)$$

Let $ty_2Eenum_2E_enum : \iota$ be given. Assume the following.

$$nonempty ty_2Eenum_2E_enum \quad (4)$$

Let $c_2Efc_2E_dimindex : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow c_2Efc_2E_dimindex A_27a \in (ty_2Eenum_2E_enum^{(ty_2Ebool_2E_itself A_27a)}) \quad (5)$$

Definition 3 We define $c_2Ebool_2E_21$ to be $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap (ap (c_2Emin_2E_3D (2^{A_27a})))$

Definition 4 We define $c_2Ebool_2E_EF$ to be $(ap (c_2Ebool_2E_21 2)) (\lambda V0t \in 2.V0t)$.

Definition 5 We define $c_2Emin_2E_3D_3D_3E$ to be $\lambda P \in 2.\lambda Q \in 2.inj_o (p \Rightarrow q)$ of type ι .

Definition 6 We define $c_2Ebool_2E_7E$ to be $(\lambda V0t \in 2.(ap (ap c_2Emin_2E_3D_3D_3E V0t) c_2Ebool_2E_EF$

Definition 7 We define $c_Ebool_2E_2F_5C$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap (c_Ebool_2E_21 2) (\lambda V2t \in 2$

Let $c_2Enum_2EREP_num : \iota$ be given. Assume the following.

$$c_2Enum_2EREP_num \in (\omega^{ty_2Enum_2Enum}) \quad (6)$$

Let $c_2Enum_2ESUC_REP : \iota$ be given. Assume the following.

$$c_2Enum_2ESUC_REP \in (\omega^{\omega}) \quad (7)$$

Let $c_2Enum_2EABS_num : \iota$ be given. Assume the following.

$$c_2Enum_2EABS_num \in (ty_2Enum_2Enum^{\omega}) \quad (8)$$

Definition 8 We define c_2Enum_2ESUC to be $\lambda V0m \in ty_2Enum_2Enum.(ap c_2Enum_2EABS_num$

Definition 9 We define $c_2Emin_2E_40$ to be $\lambda A.\lambda P \in 2^A.\mathbf{if} (\exists x \in A.p (ap P x)) \mathbf{then}$ (the $(\lambda x.x \in A \wedge p$ of type $\iota \Rightarrow \iota$).

Definition 10 We define $c_Ebool_2E_3F$ to be $\lambda A.27a : \iota.(\lambda V0P \in (2^{A-27a}).(ap V0P (ap (c_2Emin_2E_40$

Definition 11 We define $c_2Eprim_rec_2E_3C$ to be $\lambda V0m \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum$

Definition 12 We define $c_Ebool_2E_3F_21$ to be $\lambda A.27a : \iota.(\lambda V0P \in (2^{A-27a}).(ap (ap c_Ebool_2E_2F_5C$

Definition 13 We define $c_2Efcf_2Efinite_index$ to be $\lambda A.27a : \iota.(ap (c_2Emin_2E_40 (A.27a^{ty_2Enum_2Enum$

Let $ty_2Efcf_2Ecart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow \forall A1.nonempty A1 \Rightarrow nonempty (ty_2Efcf_2Ecart \quad (9)$$

Let $c_2Efcf_2Edest_cart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A.27a.nonempty A.27a \Rightarrow \forall A.27b.nonempty A.27b \Rightarrow c_2Efcf_2Edest_cart \quad (10)$$

Definition 14 We define $c_2Efcf_2Efcf_index$ to be $\lambda A.27a : \iota.\lambda A.27b : \iota.\lambda V0x \in (ty_2Efcf_2Ecart A.27a$

Let $c_2Enum_2EZERO_REP : \iota$ be given. Assume the following.

$$c_2Enum_2EZERO_REP \in \omega \quad (11)$$

Definition 15 We define c_2Enum_2E0 to be $(ap c_2Enum_2EABS_num c_2Enum_2EZERO_REP)$.

Definition 16 We define $c_2Earithmetic_2EZERO$ to be c_2Enum_2E0 .

Let $c_2Earithmetic_2E_2B : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2B \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (12)$$

Definition 17 We define $c_2Earithmetic_2EBIT2$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic$

Definition 18 We define $c_2Earithmetic_2ENUMERAL$ to be $\lambda V0x \in ty_2Enum_2Enum.V0x$.

Let $c_2Earithmetic_2EEXP : \iota$ be given. Assume the following.

$$c_2Earithmetic_2EEXP \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (13)$$

Definition 19 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 20 We define c_2Ebit_2ESBIT to be $\lambda V0b \in 2.\lambda V1n \in ty_2Enum_2Enum.(ap (ap (ap (c_2Ebo$

Let $c_2Esum_num_2ESUM : \iota$ be given. Assume the following.

$$c_2Esum_num_2ESUM \in ((ty_2Enum_2Enum^{(ty_2Enum_2Enum^{ty_2Enum_2Enum})})^{ty_2Enum_2Enum}) \quad (14)$$

Definition 21 We define $c_2Ewords_2Ew2n$ to be $\lambda A_27a : \iota.\lambda V0w \in (ty_2EfcP_2Ecart\ 2\ A_27a).(ap (ap$

Definition 22 We define $c_2Earithmetic_2EBIT1$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic$

Let $c_2Earithmetic_2EDIV : \iota$ be given. Assume the following.

$$c_2Earithmetic_2EDIV \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (15)$$

Definition 23 We define $c_2Ebit_2EDIV_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum$

Let $c_2Earithmetic_2E_2D : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2D \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (16)$$

Let $c_2Earithmetic_2EMOD : \iota$ be given. Assume the following.

$$c_2Earithmetic_2EMOD \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (17)$$

Definition 24 We define $c_2Ebit_2EMOD_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum$

Definition 25 We define c_2Ebit_2EBITS to be $\lambda V0h \in ty_2Enum_2Enum.\lambda V1l \in ty_2Enum_2Enum.\lambda V$

Definition 26 We define c_2Ebit_2EBIT to be $\lambda V0b \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap$

Definition 27 We define c_2EfcP_2EFCP to be $\lambda A_27a : \iota.\lambda A_27b : \iota.(\lambda V0g \in (A_27a^{ty_2Enum_2Enum}).(ap$

Definition 28 We define $c_2Ewords_2En2w$ to be $\lambda A_27a : \iota.\lambda V0n \in ty_2Enum_2Enum.(ap (c_2EfcP_2EFC$

Definition 29 We define $c_2Ewords_2Eword_add$ to be $\lambda A_27a : \iota.\lambda V0v \in (ty_2EfcP_2Ecart\ 2\ A_27a).\lambda V$

Let $c_2Earithmetic_2E_2A : \iota$ be given. Assume the following.

$$c_2Earithmetic_2E_2A \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (18)$$

Definition 30 We define $c_2Ewords_2Eword_mul$ to be $\lambda A_27a : \iota. \lambda V0v \in (ty_2Efc_2Ecart\ 2\ A_27a). \lambda V$

Let $c_2Ewords_2Edimword : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a. nonempty\ A_27a \Rightarrow c_2Ewords_2Edimword\ A_27a \in (ty_2Enum_2Enum^{(ty_2Ebool_2Eitself\ A_27a)}) \quad (19)$$

Definition 31 We define $c_2Ewords_2Eword_2comp$ to be $\lambda A_27a : \iota. \lambda V0w \in (ty_2Efc_2Ecart\ 2\ A_27a).$

Assume the following.

$$True \quad (20)$$

Assume the following.

$$\forall A_27a. nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a. ((V0x = V0x) \Leftrightarrow True)) \quad (21)$$

Assume the following.

$$\begin{aligned} & \forall A_27a. nonempty\ A_27a \Rightarrow (\forall V0v \in (ty_2Efc_2Ecart\ 2\ A_27a). (\forall V1w \in (ty_2Efc_2Ecart\ 2\ A_27a). (((ap\ (ap\ (\\ & \quad c_2Ewords_2Eword_mul\ A_27a)\ (ap\ (c_2Ewords_2En2w\ A_27a)\ c_2Enum_2E0)) \\ V0v) = (ap\ (c_2Ewords_2En2w\ A_27a)\ c_2Enum_2E0)) \wedge (((ap\ (ap\ (c_2Ewords_2Eword_mul \\ & \quad A_27a)\ V0v)\ (ap\ (c_2Ewords_2En2w\ A_27a)\ c_2Enum_2E0)) = (ap\ (c_2Ewords_2En2w \\ & \quad A_27a)\ c_2Enum_2E0)) \wedge (((ap\ (ap\ (c_2Ewords_2Eword_mul\ A_27a) \\ & \quad (ap\ (c_2Ewords_2En2w\ A_27a)\ (ap\ c_2Earithmetic_2ENUMERAL\ (ap \\ & \quad c_2Earithmetic_2EBIT1\ c_2Earithmetic_2EZERO))))\ V0v) = V0v) \wedge \\ & \quad (((ap\ (ap\ (c_2Ewords_2Eword_mul\ A_27a)\ V0v)\ (ap\ (c_2Ewords_2En2w \\ & \quad A_27a)\ (ap\ c_2Earithmetic_2ENUMERAL\ (ap\ c_2Earithmetic_2EBIT1 \\ & \quad c_2Earithmetic_2EZERO)))) = V0v) \wedge (((ap\ (ap\ (c_2Ewords_2Eword_mul \\ & \quad A_27a)\ (ap\ (ap\ (c_2Ewords_2Eword_add\ A_27a)\ V0v)\ (ap\ (c_2Ewords_2En2w \\ & \quad A_27a)\ (ap\ c_2Earithmetic_2ENUMERAL\ (ap\ c_2Earithmetic_2EBIT1 \\ & \quad c_2Earithmetic_2EZERO))))\ V1w) = (ap\ (ap\ (c_2Ewords_2Eword_add \\ & \quad A_27a)\ (ap\ (ap\ (c_2Ewords_2Eword_mul\ A_27a)\ V0v)\ V1w))\ V1w)) \wedge \\ & \quad (((ap\ (ap\ (c_2Ewords_2Eword_mul\ A_27a)\ V0v)\ (ap\ (ap\ (c_2Ewords_2Eword_add \\ & \quad A_27a)\ V1w)\ (ap\ (c_2Ewords_2En2w\ A_27a)\ (ap\ c_2Earithmetic_2ENUMERAL \\ & \quad (ap\ c_2Earithmetic_2EBIT1\ c_2Earithmetic_2EZERO)))) = (ap\ (\\ & \quad ap\ (c_2Ewords_2Eword_add\ A_27a)\ V0v)\ (ap\ (ap\ (c_2Ewords_2Eword_mul \\ & \quad A_27a)\ V0v)\ V1w)))))))))) \quad (22) \end{aligned}$$

Assume the following.

$$\forall A_27a. nonempty\ A_27a \Rightarrow (\forall V0w \in (ty_2Efc_2Ecart\ 2\ A_27a). ((ap\ (c_2Ewords_2Eword_2comp\ A_27a)\ (ap\ (c_2Ewords_2Eword_2comp\ A_27a)\ V0w)) = V0w)) \quad (23)$$

Assume the following.

$$\begin{aligned} & \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow (\forall V0w \in (ty_2EfcP_2Ecart \\ & 2\ A_{.27a}).(\forall V1v \in (ty_2EfcP_2Ecart\ 2\ A_{.27a}).(((ap\ (c_2Ewords_2Eword_2comp \\ & A_{.27a})\ V1v) = V0w) \Leftrightarrow (V1v = (ap\ (c_2Ewords_2Eword_2comp\ A_{.27a})\ V0w)))))) \end{aligned} \quad (24)$$

Assume the following.

$$\begin{aligned} & \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow (\forall V0v \in (ty_2EfcP_2Ecart \\ & 2\ A_{.27a}).(\forall V1w \in (ty_2EfcP_2Ecart\ 2\ A_{.27a}).((ap\ (c_2Ewords_2Eword_2comp \\ & A_{.27a})\ (ap\ (ap\ (c_2Ewords_2Eword_mul\ A_{.27a})\ V0v)\ V1w)) = (ap\ (ap \\ & (c_2Ewords_2Eword_mul\ A_{.27a})\ (ap\ (c_2Ewords_2Eword_2comp \\ & A_{.27a})\ V0v))\ V1w)))))) \end{aligned} \quad (25)$$

Theorem 1

$$\begin{aligned} & \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow (\forall V0w \in (ty_2EfcP_2Ecart \\ & 2\ A_{.27a}).((ap\ (c_2Ewords_2Eword_2comp\ A_{.27a})\ V0w) = (ap\ (ap\ (\\ & c_2Ewords_2Eword_mul\ A_{.27a})\ (ap\ (c_2Ewords_2Eword_2comp\ A_{.27a}) \\ & (ap\ (c_2Ewords_2En2w\ A_{.27a})\ (ap\ c_2Earithmetic_2ENUMERAL\ (ap \\ & c_2Earithmetic_2EBIT1\ c_2Earithmetic_2EZERO))))))\ V0w))) \end{aligned}$$