

thm_2Ewords_2EWORD_LEFT_SUB_DISTRIB (TMMT2Hp816zPiE1hEuN1SL5onE3gLhg6hdP)

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

Let $ty_2EfcP_2Efinite_image : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow nonempty (ty_2EfcP_2Efinite_image A0) \quad (1)$$

Let $ty_2Ebool_2Eitself : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow nonempty (ty_2Ebool_2Eitself A0) \quad (2)$$

Let $c_2Ebool_2Ethe_value : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow c_2Ebool_2Ethe_value A_27a \in (ty_2Ebool_2Eitself A_27a) \quad (3)$$

Let $ty_2EEnum_2Enum : \iota$ be given. Assume the following.

$$nonempty ty_2EEnum_2Enum \quad (4)$$

Let $c_2EfcP_2Edimindex : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow c_2EfcP_2Edimindex A_27a \in (ty_2EEnum_2Enum^{(ty_2Ebool_2Eitself A_27a)}) \quad (5)$$

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_2EF 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 $\lambda P \in 2.\lambda Q \in 2.inj_o (p P \Rightarrow p Q)$ of type ι .

Definition 6 We define $c_Ebool_2E_7E$ to be $(\lambda V0t \in 2.(ap (ap c_Emin_2E_3D_3D_3E V0t) c_Ebool_2E_7E))$

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 $c_Emin_2E_40$ to be $\lambda A.\lambda P \in 2^A.$ **if** $(\exists x \in A.p (ap P x))$ **then** *(the $(\lambda x.x \in A \wedge P x)$ of type $\iota \Rightarrow \iota$).*

Definition 10 We define $c_Ebool_2E_3F$ to be $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap V0P (ap (c_Emin_2E_40$

Definition 11 We define $c_Eprim_rec_2E_3C$ 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 $c_Efcp_2Efinite_index$ to be $\lambda A_27a : \iota.(ap (c_Emin_2E_40 (A_27a^{ty_2Enum_2Enum}))$

Let $ty_2Efcp_2Ecart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty A0 \Rightarrow \forall A1.nonempty A1 \Rightarrow nonempty (ty_2Efcp_2Ecart A0 A1) \quad (9)$$

Let $c_2Efcp_2Edest_cart : \iota \Rightarrow \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow \forall A_27b.nonempty A_27b \Rightarrow c_2Efcp_2Edest_cart A_27a A_27b \in ((A_27a^{(ty_2Efcp_2Efinite_image A_27b)})^{(ty_2Efcp_2Ecart A_27a A_27b)}) \quad (10)$$

Definition 14 We define $c_Efcp_2Efcp_index$ to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0x \in (ty_2Efcp_2Ecart A_27a A_27b)$

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 $c_Earithmetic_2E_2B : \iota$ be given. Assume the following.

$$c_Earithmetic_2E_2B \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (12)$$

Definition 17 We define $c_Earithmetic_2EBIT2$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_Earithmetic_2E_2B))$

Definition 18 We define $c_Earithmetic_2ENUMERAL$ to be $\lambda V0x \in ty_2Enum_2Enum.V0x$.

Let $c_Earithmetic_2EEXP : \iota$ be given. Assume the following.

$$c_Earithmetic_2EEXP \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (13)$$

Definition 19 We define c_Ebool_2ECOND to be $\lambda A_27a : \iota.(\lambda V0t \in 2.(\lambda V1t1 \in A_27a.(\lambda V2t2 \in A_27a.(c_Ebool_2ECOND A_27a t1 t2))))$

Definition 20 We define c_Ebit_2ESBIT to be $\lambda V0b \in 2.\lambda V1n \in ty_2Enum_2Enum.(ap (ap (ap c_Ebool_2ECOND A_27a)))$

Let $c_Esum_num_2ESUM : \iota$ be given. Assume the following.

$$c_Esum_num_2ESUM \in ((ty_2Enum_2Enum^{(ty_2Enum_2Enum^{ty_2Enum_2Enum})})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (14)$$

Definition 21 We define c_Ewords_2Ew2n to be $\lambda A_27a : \iota.\lambda V0w \in (ty_2Enum_2Enum^{(ty_2EfcP_2Ecart 2 A_27a)}).(ap (ap c_Esum_num_2ESUM A_27a w))$

Let $c_Ewords_2Edimword : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty A_27a \Rightarrow c_Ewords_2Edimword A_27a \in (ty_2Enum_2Enum^{(ty_2Ebool_2Eitself A_27a)})^{ty_2Enum_2Enum} \quad (15)$$

Let $c_Earithmetic_2E_2D : \iota$ be given. Assume the following.

$$c_Earithmetic_2E_2D \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (16)$$

Definition 22 We define $c_Earithmetic_2EBIT1$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_Earithmetic_2E_2D))$

Let $c_Earithmetic_2EDIV : \iota$ be given. Assume the following.

$$c_Earithmetic_2EDIV \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (17)$$

Definition 23 We define $c_Ebit_2EDIV_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap (ap c_Earithmetic_2EDIV A_27a))$

Let $c_Earithmetic_2EMOD : \iota$ be given. Assume the following.

$$c_Earithmetic_2EMOD \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum})^{ty_2Enum_2Enum} \quad (18)$$

Definition 24 We define $c_Ebit_2EMOD_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap (ap c_Earithmetic_2EMOD A_27a))$

Definition 25 We define c_Ebit_2EBITS to be $\lambda V0h \in ty_2Enum_2Enum.\lambda V1l \in ty_2Enum_2Enum.\lambda V2n \in ty_2Enum_2Enum.(ap (ap (ap c_Ebit_2ESBIT A_27a)))$

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 $\lambda A_27a : \iota.\lambda V0n \in ty_2Enum_2Enum.(ap (c_2EfcP_2EFCP$

Definition 29 We define $c_2Ewords_2Eword_2comp$ to be $\lambda A_27a : \iota.\lambda V0w \in (ty_2EfcP_2Ecart\ 2\ A_27a).$

Definition 30 We define $c_2Ewords_2Eword_2add$ to be $\lambda A_27a : \iota.\lambda V0v \in (ty_2EfcP_2Ecart\ 2\ A_27a).\lambda V$

Definition 31 We define $c_2Ewords_2Eword_2sub$ 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.

$$c_2Earithmetic_2E_2A \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (19)$$

Definition 32 We define $c_2Ewords_2Eword_2mul$ to be $\lambda A_27a : \iota.\lambda V0v \in (ty_2EfcP_2Ecart\ 2\ A_27a).\lambda V$

Assume the following.

$$True \quad (20)$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0t \in 2.((\forall V1x \in A_27a.(p\ V0t)) \Leftrightarrow (p\ V0t))) \quad (21)$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a.((V0x = V0x) \Leftrightarrow True)) \quad (22)$$

Assume the following.

$$\begin{aligned} & \forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0v \in (ty_2EfcP_2Ecart\ 2\ A_27a).(\forall V1w \in (ty_2EfcP_2Ecart\ 2\ A_27a).(\forall V2x \in \\ & (ty_2EfcP_2Ecart\ 2\ A_27a).((ap\ (ap\ (c_2Ewords_2Eword_2mul\ A_27a) \\ & V0v)\ (ap\ (ap\ (c_2Ewords_2Eword_2add\ A_27a)\ V1w)\ V2x)) = (ap\ (ap\ (\\ & c_2Ewords_2Eword_2add\ A_27a)\ (ap\ (ap\ (c_2Ewords_2Eword_2mul \\ & A_27a)\ V0v)\ V1w))\ (ap\ (ap\ (c_2Ewords_2Eword_2mul\ A_27a)\ V0v)\ V2x)))))) \end{aligned} \quad (23)$$

Assume the following.

$$\begin{aligned} & \forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0v \in (ty_2EfcP_2Ecart\ 2\ A_27a).(\forall V1w \in (ty_2EfcP_2Ecart\ 2\ A_27a).((ap\ (c_2Ewords_2Eword_2comp \\ & A_27a)\ (ap\ (ap\ (c_2Ewords_2Eword_2mul\ A_27a)\ V0v)\ V1w)) = (ap\ (ap \\ & (c_2Ewords_2Eword_2mul\ A_27a)\ V0v)\ (ap\ (c_2Ewords_2Eword_2comp \\ & A_27a)\ V1w)))))) \end{aligned} \quad (24)$$

Theorem 1

$$\forall A_{27a}. \text{nonempty } A_{27a} \Rightarrow (\forall V0v \in (\text{ty_2EfcP-2Ecart } 2 \ A_{27a}). (\forall V1w \in (\text{ty_2EfcP-2Ecart } 2 \ A_{27a}). (\forall V2x \in (\text{ty_2EfcP-2Ecart } 2 \ A_{27a}). ((\text{ap } (\text{ap } (\text{c_2Ewords_2Eword_mul } A_{27a}) \ V0v) (\text{ap } (\text{ap } (\text{c_2Ewords_2Eword_sub } A_{27a}) \ V1w) \ V2x)) = (\text{ap } (\text{ap } (\text{c_2Ewords_2Eword_sub } A_{27a}) (\text{ap } (\text{ap } (\text{c_2Ewords_2Eword_mul } A_{27a}) \ V0v) \ V1w)) (\text{ap } (\text{ap } (\text{c_2Ewords_2Eword_mul } A_{27a}) \ V0v) \ V2x))))))$$