

thm_2Ewords_2EWORD_EXTRACT_BITS_COMP (TMYeVdFHU377DDnHWc1kByy4kdTYScocjJv)

October 26, 2020

Let $ty_2Efc_2Efinite_image : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A0.nonempty\ A0 \Rightarrow nonempty\ (ty_2Efc_2Efinite_image\ A0) \quad (1)$$

Definition 1 We define c_2Emin_2E3D to be $\lambda A.\lambda x \in A.\lambda y \in A.inj_o\ (x = y)$ of type $\iota \Rightarrow \iota$.

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 $ty_2Enum_2Enum : \iota$ be given. Assume the following.

$$nonempty\ ty_2Enum_2Enum \quad (4)$$

Let $c_2Efc_2Edimindex : \iota \Rightarrow \iota$ be given. Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow c_2Efc_2Edimindex\ A_27a \in (ty_2Enum_2Enum^{(ty_2Ebool_2Eitself\ A_27a)}) \quad (5)$$

Definition 2 We define c_2Ebool_2ET to be $(ap\ (ap\ (c_2Emin_2E3D\ (2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1x))$

Definition 3 We define c_2Ebool_2E21 to be $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap\ (ap\ (c_2Emin_2E3D\ (2^{A_27a}))$

Definition 4 We define c_2Ebool_2EF to be $(ap\ (c_2Ebool_2E21\ 2)\ (\lambda V0t \in 2.V0t))$.

Definition 5 We define $c_2Emin_2E3D_3D_3E$ 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 $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap V0P (ap (c_Emin_2E_40 A_27a))))$

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 $\lambda A_27a : \iota.(\lambda V0P \in (2^{A_27a}).(ap (ap c_Ebool_2E_2F_5C A_27a P)))$

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

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

Definition 17 We define $c_2Earithmetic_2EBIT2$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic_2E_2B))$

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.

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

Definition 19 We define c_2Ebool_2ECOND to be $\lambda A_27a : \iota.(\lambda V0t \in 2.(\lambda V1t1 \in A_27a.(\lambda V2t2 \in A_27a.(ap (ap c_2Ebool_2EBIT2))))))$

Definition 20 We define c_2Ebit_2ESBIT to be $\lambda V0b \in 2.\lambda V1n \in ty_2Enum_2Enum.(ap (ap (ap c_2Ebool_2EBIT2)))$

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

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

Definition 21 We define $c_2Ewords_2Ew2n$ to be $\lambda A_27a : \iota.\lambda V0w \in (ty_2Efc_2Ecart\ 2\ A_27a).(ap (ap c_2Esum_num_2ESUM))$

Definition 22 We define $c_2Earithmetic_2EBIT1$ to be $\lambda V0n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic_2EBIT2))$

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

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

Definition 23 We define $c_2Ebit_2EDIV_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic_2EDIV))$

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

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

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

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

Definition 24 We define $c_2Ebit_2EMOD_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap (ap c_2Earithmetic_2EMOD))$

Definition 25 We define c_2Ebit_2EBITS to be $\lambda V0h \in ty_2Enum_2Enum.\lambda V1l \in ty_2Enum_2Enum.\lambda V2n \in ty_2Enum_2Enum.(ap (ap c_2Ebit_2EBIT2))$

Definition 26 We define c_2Ebit_2EBIT to be $\lambda V0b \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap (ap c_2Ebit_2EBIT2))$

Definition 27 We define c_2Efc_2EFCP to be $\lambda A_27a : \iota.\lambda A_27b : \iota.(\lambda V0g \in (A_27a^{ty_2Enum_2Enum}).(ap (ap c_2Efc_2EFCP)))$

Definition 28 We define $c_2Ewords_2En2w$ to be $\lambda A_27a : \iota.\lambda V0n \in ty_2Enum_2Enum.(ap (c_2Efc_2EFCP))$

Definition 29 We define c_Ewords_2Ew2w to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0w \in (ty_2EfcP_2Ecart\ 2\ A_27a$

Definition 30 We define $c_Ecombin_2Eo$ to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda A_27c : \iota.\lambda V0f \in (A_27b^{A_27c}).\lambda V1g \in$

Definition 31 We define $c_Earithmetic_2EMIN$ to be $\lambda V0m \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum$

Definition 32 We define $c_Ebool_2E_5C_2F$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (c_Ebool_2E_21\ 2)\ (\lambda V2t \in$

Definition 33 We define $c_Earithmetic_2E_3C_3D$ to be $\lambda V0m \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum$

Definition 34 We define $c_Ewords_2Eword_bits$ to be $\lambda A_27a : \iota.\lambda V0h \in ty_2Enum_2Enum.\lambda V1l \in ty_2Enum_2Enum$

Definition 35 We define $c_Ewords_2Eword_extract$ to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0h \in ty_2Enum_2Enum$

Assume the following.

$$\begin{aligned} \forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a. (\forall V1y \in \\ A_27a. ((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \end{aligned} \quad (18)$$

Assume the following.

$$\begin{aligned} \forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow (\\ \forall V0f \in (A_27b^{A_27a}). (\forall V1g \in (A_27b^{A_27a}). ((V0f = \\ V1g) \Leftrightarrow (\forall V2x \in A_27a. ((ap\ V0f\ V2x) = (ap\ V1g\ V2x)))))) \end{aligned} \quad (19)$$

Assume the following.

$$\begin{aligned} \forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow \forall A_27c. \\ nonempty\ A_27c \Rightarrow (\forall V0f \in (A_27b^{A_27a}). (\forall V1g \in (A_27a^{A_27c}). \\ (\forall V2x \in A_27c. ((ap\ (ap\ (ap\ (c_Ecombin_2Eo\ A_27c\ A_27b\ A_27a) \\ V0f)\ V1g)\ V2x) = (ap\ V0f\ (ap\ V1g\ V2x)))))) \end{aligned} \quad (20)$$

Assume the following.

$$\begin{aligned} \forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0h1 \in ty_2Enum_2Enum. \\ (\forall V1l1 \in ty_2Enum_2Enum. (\forall V2h2 \in ty_2Enum_2Enum. \\ (\forall V3l2 \in ty_2Enum_2Enum. (\forall V4w \in (ty_2EfcP_2Ecart \\ 2\ A_27a). ((ap\ (ap\ (ap\ (c_Ewords_2Eword_bits\ A_27a)\ V2h2)\ V3l2) \\ (ap\ (ap\ (ap\ (c_Ewords_2Eword_bits\ A_27a)\ V0h1)\ V1l1)\ V4w)) = (\\ ap\ (ap\ (ap\ (c_Ewords_2Eword_bits\ A_27a)\ (ap\ (ap\ c_Earithmetic_2EMIN \\ V0h1)\ (ap\ (ap\ c_Earithmetic_2E_2B\ V2h2)\ V1l1)))\ (ap\ (ap\ c_Earithmetic_2E_2B \\ V3l2)\ V1l1))\ V4w)))))) \end{aligned} \quad (21)$$

Theorem 1

$$\begin{aligned} \forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow (\\ \forall V0n \in (ty_2EfcP_2Ecart\ 2\ A_27a). (\forall V1l \in ty_2Enum_2Enum. \\ (\forall V2k \in ty_2Enum_2Enum. (\forall V3j \in ty_2Enum_2Enum. (\\ \forall V4h \in ty_2Enum_2Enum. ((ap\ (ap\ (ap\ (c_Ewords_2Eword_extract \\ A_27a\ A_27b)\ V3j)\ V2k)\ (ap\ (ap\ (ap\ (c_Ewords_2Eword_bits\ A_27a) \\ V4h)\ V1l)\ V0n)) = (ap\ (ap\ (ap\ (c_Ewords_2Eword_extract\ A_27a\ A_27b) \\ (ap\ (ap\ c_Earithmetic_2EMIN\ V4h)\ (ap\ (ap\ c_Earithmetic_2E_2B \\ V3j)\ V1l)))\ (ap\ (ap\ c_Earithmetic_2E_2B\ V2k)\ V1l))\ V0n)))))) \end{aligned}$$