

thm_2Ewords_2EWORD__BITS__EXTRACT
(TM-
duk12Bn6LAFPvPXkWnb8XphbyYuKUT7MB)

October 26, 2020

Definition 1 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 2 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 3 We define $c_2Ebool_2E_2T$ to be $(ap (ap (c_2Emin_2E_3D (2^2)) (\lambda V0x \in 2.V0x)) (\lambda V1x \in 2.V1x))$

Definition 4 We define $c_2Ebool_2E_21$ to be $\lambda A.\lambda a : \iota.(\lambda V0P \in (2^{A-27a}).(ap (ap (c_2Emin_2E_3D (2^{A-27a}))$

Definition 5 We define $c_2Ebool_2E_5C_2F$ to be $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap (c_2Ebool_2E_21 2) (\lambda V2t \in 2.V2t))$

Definition 6 We define $c_2Ebool_2E_2F$ to be $(ap (c_2Ebool_2E_21 2) (\lambda V0t \in 2.V0t))$.

Definition 7 We define $c_2Ebool_2E_7E$ to be $(\lambda V0t \in 2.(ap (ap c_2Emin_2E_3D_3D_3E V0t) c_2Ebool_2E_2F$

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

$$c_2Enum_2EZERO_REP \in \omega \tag{1}$$

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

$$nonempty\ ty_2Enum_2Enum \tag{2}$$

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

$$c_2Enum_2EABS_num \in (ty_2Enum_2Enum^{\omega}) \tag{3}$$

Definition 8 We define c_2Enum_2E0 to be $(ap c_2Enum_2EABS_num c_2Enum_2EZERO_REP)$.

Definition 9 We define $c_2Earithmic_2EZERO$ to be c_2Enum_2E0 .

Definition 20 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 21 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.

$$\forall A0.nonempty A0 \Rightarrow \forall A1.nonempty A1 \Rightarrow nonempty (ty_2Efcp_2Ecart A0 A1) \quad (12)$$

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

$$\forall A_27a.nonempty A_27a \Rightarrow \forall A_27b.nonempty A_27b \Rightarrow c_2Efcp_2Edest_cart A_27a A_27b \in ((A_27a^{(ty_2Efcp_2Efinite_image A_27b)})^{(ty_2Efcp_2Ecart A_27a A_27b)}) \quad (13)$$

Definition 22 We define $c_2Efcp_2Efcp_index$ to be $\lambda A_27a : \iota. \lambda A_27b : \iota. \lambda V0x \in (ty_2Efcp_2Ecart A_27a$

Definition 23 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 24 We define $c_2Ewords_2Eword_bits$ to be $\lambda A_27a : \iota. \lambda V0h \in ty_2Enum_2Enum. \lambda V1l \in ty_2$

Definition 25 We define $c_2Ecombin_2Eo$ to be $\lambda A_27a : \iota. \lambda A_27b : \iota. \lambda A_27c : \iota. \lambda V0f \in (A_27b^{A_27c}). \lambda V1$

Definition 26 We define $c_2Earithmetic_2EBIT2$ to be $\lambda V0n \in ty_2Enum_2Enum. (ap (ap c_2Earithmetic$

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

$$c_2Earithmetic_2EEXP \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (14)$$

Definition 27 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.

$$c_2Esum_num_2ESUM \in ((ty_2Enum_2Enum^{(ty_2Enum_2Enum^{ty_2Enum_2Enum})})^{ty_2Enum_2Enum}) \quad (15)$$

Definition 28 We define $c_2Ewords_2Ew2n$ to be $\lambda A_27a : \iota. \lambda V0w \in (ty_2Efcp_2Ecart 2 A_27a). (ap (ap$

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

$$c_2Earithmetic_2EDIV \in ((ty_2Enum_2Enum^{ty_2Enum_2Enum})^{ty_2Enum_2Enum}) \quad (16)$$

Definition 29 We define $c_2Ebit_2EDIV_2EXP$ to be $\lambda V0x \in ty_2Enum_2Enum. \lambda V1n \in ty_2Enum_2Enum$

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

Definition 31 We define `c_2Ebit_2EBITS` to be $\lambda V0h \in ty_2Enum_2Enum.\lambda V1l \in ty_2Enum_2Enum.\lambda V$

Definition 32 We define `c_2Ebit_2EBIT` to be $\lambda V0b \in ty_2Enum_2Enum.\lambda V1n \in ty_2Enum_2Enum.(ap$

Definition 33 We define `c_2Ewords_2En2w` to be $\lambda A_27a : \iota.\lambda V0n \in ty_2Enum_2Enum.(ap (c_2Efc_2EFC$

Definition 34 We define `c_2Ewords_2Ew2w` to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0w \in (ty_2Efc_2Ecart\ 2\ A_27$

Definition 35 We define `c_2Ewords_2Eword_extract` to be $\lambda A_27a : \iota.\lambda A_27b : \iota.\lambda V0h \in ty_2Enum_2Enum$

Assume the following.

$$\begin{aligned}
& (\forall V0n \in ty_2Enum_2Enum.(\forall V1m \in ty_2Enum_2Enum.(\\
& \quad \forall V2p \in ty_2Enum_2Enum.(((p (ap (ap c_2Earithmetic_2E_3C_3D \\
& (ap (ap c_2Earithmetic_2EMIN V1m) V0n)) V2p)) \Leftrightarrow ((p (ap (ap c_2Earithmetic_2E_3C_3D \\
& \quad V1m) V2p)) \vee (p (ap (ap c_2Earithmetic_2E_3C_3D V0n) V2p)))) \wedge ((\\
& \quad p (ap (ap c_2Earithmetic_2E_3C_3D V2p) (ap (ap c_2Earithmetic_2EMIN \\
& \quad V1m) V0n))) \Leftrightarrow ((p (ap (ap c_2Earithmetic_2E_3C_3D V2p) V1m)) \wedge (p \\
& \quad (ap (ap c_2Earithmetic_2E_3C_3D V2p) V0n)))))))))
\end{aligned} \tag{18}$$

Assume the following.

$$True \tag{19}$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0t \in 2.((\forall V1x \in A_27a.(p\ V0t)) \Leftrightarrow (p\ V0t))) \tag{20}$$

Assume the following.

$$\begin{aligned}
& (\forall V0t \in 2.(((True \wedge (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge (((p\ V0t) \wedge True) \Leftrightarrow \\
& (p\ V0t)) \wedge (((False \wedge (p\ V0t)) \Leftrightarrow False) \wedge (((p\ V0t) \wedge False) \Leftrightarrow False) \wedge \\
& \quad (((p\ V0t) \wedge (p\ V0t)) \Leftrightarrow (p\ V0t))))))
\end{aligned} \tag{21}$$

Assume the following.

$$\begin{aligned}
& (\forall V0t \in 2.(((True \Rightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \wedge (((p\ V0t) \Rightarrow True) \Leftrightarrow \\
& True) \wedge (((False \Rightarrow (p\ V0t)) \Leftrightarrow True) \wedge (((p\ V0t) \Rightarrow (p\ V0t)) \Leftrightarrow True) \wedge ((\\
& \quad (p\ V0t) \Rightarrow False) \Leftrightarrow \neg (p\ V0t))))))
\end{aligned} \tag{22}$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a.((V0x = V0x) \Leftrightarrow True)) \tag{23}$$

Assume the following.

$$\forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0x \in A_27a.(\forall V1y \in A_27a.((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \tag{24}$$

Assume the following.

$$\begin{aligned}
& (\forall V0t \in 2.(((True \Leftrightarrow (p V0t)) \Leftrightarrow (p V0t)) \wedge (((p V0t) \Leftrightarrow True) \Leftrightarrow \\
& (p V0t)) \wedge (((False \Leftrightarrow (p V0t)) \Leftrightarrow \neg(p V0t)) \wedge (((p V0t) \Leftrightarrow False) \Leftrightarrow \neg(\\
& p V0t))))))
\end{aligned} \tag{25}$$

Assume the following.

$$\begin{aligned}
& (\forall V0t1 \in 2.(\forall V1t2 \in 2.(\forall V2t3 \in 2.(((p V0t1) \Rightarrow \\
& ((p V1t2) \Rightarrow (p V2t3))) \Leftrightarrow (((p V0t1) \wedge (p V1t2)) \Rightarrow (p V2t3))))))
\end{aligned} \tag{26}$$

Assume the following.

$$\begin{aligned}
& (\forall V0x \in 2.(\forall V1x_{.27} \in 2.(\forall V2y \in 2.(\forall V3y_{.27} \in \\
& 2.(((p V0x) \Leftrightarrow (p V1x_{.27})) \wedge ((p V1x_{.27}) \Rightarrow ((p V2y) \Leftrightarrow (p V3y_{.27})))) \Rightarrow \\
& (((p V0x) \Rightarrow (p V2y)) \Leftrightarrow ((p V1x_{.27}) \Rightarrow (p V3y_{.27}))))))
\end{aligned} \tag{27}$$

Assume the following.

$$\begin{aligned}
& \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow \forall A_{.27b}.nonempty\ A_{.27b} \Rightarrow \forall A_{.27c}. \\
& nonempty\ A_{.27c} \Rightarrow (\forall V0f \in (A_{.27b}^{A_{.27a}}).(\forall V1g \in (A_{.27a}^{A_{.27c}}). \\
& (\forall V2x \in A_{.27c}.((ap\ (ap\ (ap\ (c_{.2Ecombin_2Eo}\ A_{.27c}\ A_{.27b}\ A_{.27a}) \\
& V0f)\ V1g)\ V2x) = (ap\ V0f\ (ap\ V1g\ V2x))))))
\end{aligned} \tag{28}$$

Assume the following.

$$\begin{aligned}
& \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow \forall A_{.27b}.nonempty\ A_{.27b} \Rightarrow (\\
& \forall V0x \in (ty_{.2EfcP_2Ecart}\ A_{.27a}\ A_{.27b}).(\forall V1y \in (ty_{.2EfcP_2Ecart} \\
& A_{.27a}\ A_{.27b}).((V0x = V1y) \Leftrightarrow (\forall V2i \in ty_{.2Enum_2Enum}.((p\ (ap \\
& (ap\ c_{.2Eprim_rec_2E_3C}\ V2i)\ (ap\ (c_{.2EfcP_2Edimindex}\ A_{.27b})\ (\\
& c_{.2Ebool_2Ethe_value}\ A_{.27b})))) \Rightarrow ((ap\ (ap\ (c_{.2EfcP_2EfcP_index} \\
& A_{.27a}\ A_{.27b})\ V0x)\ V2i) = (ap\ (ap\ (c_{.2EfcP_2EfcP_index}\ A_{.27a}\ A_{.27b}) \\
& V1y)\ V2i))))))
\end{aligned} \tag{29}$$

Assume the following.

$$\begin{aligned}
& \forall A_{.27a}.nonempty\ A_{.27a} \Rightarrow \forall A_{.27b}.nonempty\ A_{.27b} \Rightarrow (\\
& \forall V0g \in (A_{.27a}^{ty_{.2Enum_2Enum}}).(\forall V1i \in ty_{.2Enum_2Enum}. \\
& ((p\ (ap\ (ap\ c_{.2Eprim_rec_2E_3C}\ V1i)\ (ap\ (c_{.2EfcP_2Edimindex}\ A_{.27b}) \\
& (c_{.2Ebool_2Ethe_value}\ A_{.27b})))) \Rightarrow ((ap\ (ap\ (c_{.2EfcP_2EfcP_index} \\
& A_{.27a}\ A_{.27b})\ (ap\ (c_{.2EfcP_2EFCP}\ A_{.27a}\ A_{.27b})\ V0g))\ V1i) = (ap\ V0g \\
& V1i))))))
\end{aligned} \tag{30}$$

Assume the following.

$$\begin{aligned}
& \forall A_27a.nonempty\ A_27a \Rightarrow \forall A_27b.nonempty\ A_27b \Rightarrow (\\
& \quad \forall V0w \in (ty_2Efc_2Ecart\ 2\ A_27a). (\forall V1i \in ty_2Enum_2Enum. \\
& \quad ((p\ (ap\ (ap\ c_2Eprim_rec_2E_3C\ V1i)\ (ap\ (c_2Efc_2Edimindex\ A_27b) \\
& \quad (c_2Ebool_2Ethe_value\ A_27b)))) \Rightarrow ((p\ (ap\ (ap\ (c_2Efc_2Efc_index \\
& \quad 2\ A_27b)\ (ap\ (c_2Ewords_2Ew2w\ A_27a\ A_27b)\ V0w))\ V1i)) \Leftrightarrow ((p\ (ap \\
& \quad (ap\ c_2Eprim_rec_2E_3C\ V1i)\ (ap\ (c_2Efc_2Edimindex\ A_27a)\ (\\
& \quad c_2Ebool_2Ethe_value\ A_27a)))) \wedge (p\ (ap\ (ap\ (c_2Efc_2Efc_index \\
& \quad 2\ A_27a)\ V0w)\ V1i))))))
\end{aligned} \tag{31}$$

Theorem 1

$$\begin{aligned}
& \forall A_27a.nonempty\ A_27a \Rightarrow (\forall V0h \in ty_2Enum_2Enum. (\\
& \quad \forall V1l \in ty_2Enum_2Enum. (\forall V2w \in (ty_2Efc_2Ecart\ 2 \\
& \quad A_27a). ((ap\ (ap\ (ap\ (c_2Ewords_2Eword_bits\ A_27a)\ V0h)\ V1l)\ V2w) = \\
& \quad (ap\ (ap\ (ap\ (c_2Ewords_2Eword_extract\ A_27a\ A_27a)\ V0h)\ V1l)\ V2w))))))
\end{aligned}$$