

Pascal-F Verifier Internal Design Document “Icode” Interface Control Document

John Nagle

FACC / Palo Alto

1. Introduction

“Icode” is the name given to the intermediate language produced by the first pass of the Pascal-F compiler. As the first pass of the compiler is used both as a component of the compiler and of the Pascal-F Verifier, it is necessary to clearly establish the syntax and semantics of “icode”.

1.1 The Icode Operators

| | |
|-----------|--|
| xch (1) | Working operator. Causes the top two operands on the stack to be exchanged. |
| del (2) | Working operator. Causes the top operand on the stack to be deleted. |
| fix (3) | Working operator. |
| monit (4) | Working operator. Identifies the beginning of a monitor or module. |
| ident (5) | Working operator. Marks an identifier as an object in the icode stream. |
| proc (6) | Working operator. Identifies the beginning of a procedure or function. |
| end (7) | Working operator. Identifies the end of a monitor, module, procedure, function, or main program. |
| null (8) | Statement operator, 0-argument. Represents the null statement. |
| refer (9) | Selector operator, 1-argument, result type pointer, argument type: data. Used when passing data items by address as VAR arguments to procedures. |
| stol (10) | Statement operator, 2-argument, argument types: data, [-32768..32767]. Store operator; stores second argument into first. |
| stor (11) | Unused. |
| stof (12) | Statement operator, 2-argument, argument types: data, fixed point. Store operator for fixed point operands. |
| succ (16) | Expression operator, 1-argument, result type oversize integer, argument type: [-32768..32767]. Successor operator. |
| pred (17) | Expression operator, 1-argument, result type oversize integer, argument type: [-32768..32767]. Predecessor operator. |
| uceq (24) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare equal. |
| ucne (25) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare not equal. |
| ucgt (26) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare greater. |
| ucle (27) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare less than or equal. |
| ucge (28) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare greater than or equal. |
| uclt (29) | Expression operator, 2-argument, result type Boolean, argument types: [0..32767], [0..32767]. Unsigned compare less than. |
| umax (30) | Expression operator, 2-argument, result type [0..32767], argument types: [0..32767], [0..32767]. Unsigned maximum function. |
| umin (31) | Expression operator, 2-argument, result type [0..32767], argument types: [0..32767], [0..32767]. Unsigned minimum function. |
| iadd (32) | Expression operator, 2-argument, result type oversize integer, argument types: [-32768..32767], [-32768..32767]. Integer add. |
| isub (33) | Expression operator, 2-argument, result type oversize integer, argument types: [-32768..32767], [-32768..32767]. Integer subtract. |

| | |
|------------|--|
| imul (34) | Expression operator, 2-argument, result type oversize integer, argument types: [-32768..32767], [-32768..32767]. Integer multiply. |
| idiv (35) | Expression operator, 2-argument, result type [-32768..32767], argument types: [-32768..32767], [-32768..-1, 1..32767]. Integer divide. |
| imod (36) | Expression operator, 2-argument, result type [-32768..32767], argument types: [-32768..32767], [-32768..-1, 1..32767]. Integer remainder. |
| ineg (40) | Expression operator, 1-argument, result type oversize integer, argument type: [-32768..32767]. Integer negation. |
| iabs (41) | Expression operator, 1-argument, result type oversize integer, argument type: [-32768..32767]. Integer absolute value. |
| iodd (42) | Expression operator, 1-argument, result type Boolean, argument type: [-32768..32767]. Integer test for odd. |
| ceil (44) | Expression operator, 1-argument, result type [-32768..32767], argument type: [-32768..32767]. Integer ceiling. |
| floor (45) | Expression operator, 1-argument, result type [-32768..32767], argument type: [-32768..32767]. Integer floor. |
| sadd (48) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point add. |
| ssub (49) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point subtract. |
| smul (50) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point multiply. |
| sdiv (51) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point divide. |
| rescl (53) | Expression operator, 2-argument, result type Unimplemented, argument types: Unimplemented, Unimplemented. Fixed point rescale. |
| iceq (56) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer compare equal. |
| icne (57) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer compare not equal. |
| icgt (58) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer compare greater than. |
| icle (59) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer less than or equal to. |
| icge (60) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer compare greater than or equal to. |
| iclt (61) | Expression operator, 2-argument, result type Boolean, argument types: [-32768..32767], [-32768..32767]. Signed integer compare less than. |
| imax (62) | Expression operator, 2-argument, result type [-32768..32767], argument types: [-32768..32767], [-32768..32767]. Signed integer maximum. |
| imin (63) | Expression operator, 2-argument, result type [-32768..32767], argument types: [-32768..32767], [-32768..32767]. Signed integer minimum. |

| | |
|------------|---|
| fadd (64) | Unused. |
| fsub (65) | Unused. |
| fmul (66) | Unused. |
| fdiv (67) | Unused. |
| fneg (72) | Unused. |
| fabs (73) | Unused. |
| float (74) | Unused. |
| trunc (75) | Unused. |
| round (76) | Unused. |
| fxeq (80) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point compare equal. |
| fxne (81) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point compare not equal. |
| fxgt (82) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point greater than. |
| fxle (83) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point less than or equal to. |
| fxge (84) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point greater than or equal to. |
| fxlt (85) | Expression operator, 2-argument, result type Boolean, argument types: fixed point, fixed point. Fixed point less than. |
| fxmax (86) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point maximum. |
| fxmin (87) | Expression operator, 2-argument, result type fixed point, argument types: fixed point, fixed point. Fixed point minimum. |
| fceq (88) | Unused. |
| fcne (89) | Unused. |
| fcgt (90) | Unused. |
| fcle (91) | Unused. |
| fcge (92) | Unused. |
| fclt (93) | Unused. |
| fmax (94) | Unused. |
| fmin (95) | Unused. |
| not (96) | Expression operator, 1-argument, result type Boolean, argument type: Boolean. Boolean negation. |
| eqv (104) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean equivalence. |
| xor (105) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean exclusive or. |

| | |
|--------------|--|
| nimp (106) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean negative implication. |
| rimp (107) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean reverse implication. |
| imp (108) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean implication. |
| nrimp (109) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean negative reverse implication. |
| or (110) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean or. |
| and (111) | Expression operator, 2-argument, result type Boolean, argument types: Boolean, Boolean. Boolean and. |
| compl (112) | Expression operator, 1-argument, result type set, argument type: set. Set complement. |
| union (113) | Expression operator, 2-argument, result type set, argument types: set, set. Set union. |
| inter (114) | Expression operator, 2-argument, result type set, argument types: set, set. Set intersection. |
| sdiff (115) | Expression operator, 2-argument, result type set, argument types: set, set. Set difference. |
| sgens (117) | Expression operator, 2-argument, result type Unimplemented, argument types: Unimplemented, Unimplemented. |
| sadel (118) | Expression operator, 2-argument, result type Unimplemented, argument types: Unimplemented, Unimplemented. |
| empty (119) | Expression operator, 0-argument, result type set. Empty set constant. |
| sceq (120) | Expression operator, 2-argument, result type Boolean, argument types: set, set. Set compare equal. |
| scne (121) | Expression operator, 2-argument, result type Boolean, argument types: set, set. Set compare unequal. |
| scgt (122) | Unused. |
| scl (123) | Expression operator, 2-argument, result type Boolean, argument types: set, set. Improper subset test. |
| scge (124) | Expression operator, 2-argument, result type Boolean, argument types: set, set. Improper superset test. |
| sclt (125) | Unused. |
| in (126) | Expression operator, 2-argument, result type Boolean, argument types: [0..15], set. Set membership test. |
| sany (127) | Unused. |
| field (131) | Selector operator, 1-argument, result type data, argument type: addr. Specifies a subfield of a word by bit offset and length in bits. |
| offset (132) | Selector operator, 1-argument, result type data, argument type: addr. Specifies a subfield of a record by byte offset and length in bytes. |

| | |
|-------------|---|
| indir (133) | Selector operator, 1-argument, result type data, argument type: pointer. Indirect address operator; used in referencing VAR formal arguments to routines. |
| index (134) | Selector operator, 2-argument, result type data, argument types: addr, [0..32767]. Array subscript operator. |
| movem (135) | Statement operator, 2-argument, argument types: addr, addr. Data move operator; used for record and array assignments. |
| invok (138) | Unused. |
| rtemp (140) | Selector operator, 0-argument, result type pointer. Used to refer to temporary variables created with the “dtemp” operator. |
| dtemp (141) | Statement operator, 2-argument, argument types: ind, statement. Declares a temporary variable for the duration of one statement; used in the implementation of WITH statements. |
| if (144) | Statement operator, 3-argument, argument types: Boolean, statement, statement. IF statement operator. |
| case (145) | Statement operator, N-argument, argument types: [-32768..32767], [-32768..32767], statement, [-32768..32767]. CASE statement operator. |
| entry (146) | Unused. |
| loop (147) | Statement operator, N-argument, argument types: statement. Loop operator; used for LOOP, WHILE, and REPEAT statements. |
| exit (148) | Statement operator, 2-argument, argument types: Boolean, statement. Exit from loop operator; used within loop constructs. |
| for (149) | Statement operator, 5-argument, argument types: data, [-32768..32767], i8, [-32768..32767], statement. FOR statement operator. |
| seq (152) | Statement operator, N-argument, argument types: statement. Represents a sequence of statements. |
| wait (154) | Statement operator, 1-argument, argument type: signal. WAIT statement operator. |
| send (155) | SEND statement operator. Statement operator, 1-argument, argument type: signal. |
| tsig (156) | Expression operator, 1-argument, argument type: signal. |
| lock (157) | Expression operator, 1-argument, result type data, argument type: data. |
| enabl (158) | Unused. |
| litsc (160) | Literal operator, 0-argument, result type set. Set constant operator. |
| liter (162) | Literal operator, 0-argument, result type [-32768..32767]. Numeric literal operator. |
| rdata (163) | Selector operator, 0-argument, result type data. Used to specify addresses in VALUE data space. |
| litd (164) | Literal operator, 0-argument, result type [-32768..32767]. |
| raise (165) | Statement operator, 1-argument. |
| vceq (168) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |

| | |
|-------------|--|
| vcne (169) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |
| vcgt (170) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |
| vcle (171) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |
| vcge (172) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |
| vclt (173) | Expression operator, 2-argument, result type Boolean, argument types: Unimplemented, Unimplemented. |
| dvad (174) | Selector operator, 0-argument, result type data. Used to specify addresses in device space. |
| varbl (176) | Selector operator, 0-argument, result type data. Used to specify addresses in absolute data space or stack-relative data space. |
| param (192) | Selector operator, 0-argument, result type data. Used to specify addresses in routine parameter space. |
| call (208) | Statement operator, N-argument, argument types: statement. Used to call procedures and functions. |
| icall (224) | Expression operator, 0-argument. Used to call monitors and modules. |
| defnd (249) | Expression operator, 1-argument, result type Boolean, argument type: data. Verifier only. Boolean test for definedness. |
| old (250) | Selector operator, 1-argument, result type data, argument type: data. Verifier only. Used only in EXIT declarations to refer to the value of a variable at entry to the routine. |
| vdecl (252) | Declaration operator, 1-argument, argument type: Boolean. Verifier only. Used only in the specification part of the icode for a routine; indicates each declaration assertion. |
| vhead (253) | Declaration operator, 2-argument. Verifier only. This is always the top operator in the tree for the verifier. The first argument is a sequence of verifier assertions, and the second are the program statements. |
| asert (254) | Statement operator, N-argument, argument type: Boolean. Verifier only. Used to represent statement-type assertions (STATE, ASSERT, and SUMMARY) in icode. |
| linen (255) | Working operator. Verifier only. Used to express source line number information in icode. |