Ghosts and Demons: Undefined Behavior in the C2Y Core Language (Status Update)

Martin Uecker, Graz University of Technology, uecker@tugraz.at

This is a preliminary analysis of all UB in the core language listed as item 1 to 87 in Annex J.2 in N3220 (corresponding to C23). The color in the left column has the following meaning: Green are items which could be defined or made a constraint violation. For 26 items a change was voted into C2Y as of 2025/02. Light green items require (type) checking across translation units which is not currently done by most implementations. Orange items can be detected at runtime for existing code. Red items refer to memory safety issues that are difficult or expensive to detect without breaking existing ABIs. Those will require new annotations or an opt-in memory safety mode. The right column proposes solutions and lists related documents. The color indicates where mainstream compilers already provide a (partial) implementation of well-defined safe behavior.

	Undefined Behavior	**Status / Plan**
1	Shall outside of constraints	Work in progress..., ghost (N3484, 2025/02)
2	~~Does not end with newline~~	defined behavior (N3411, 2025/02)
3	~~Token concat produces universal character name~~	constraint (N3479, 2025/02)
4	Non-standard or missing main	constraint N3480 (WIP, target: 2025/08)
5	Data race	**opt-in memory safety (lifetime)**
6	Character not in base source char set	(WIP, target: 2025/08)
7	Invalid multibyte character in source	(WIP, target: 2025/08)
8	~~Both internal and external linkage~~	constraint (N3410, 2025/02)
9	Access outside life-time	**opt-in memory safety (lifetime)**
10	Value of pointer outside life-time	**opt-in memory safety (lifetime)**
11	Automatic object is used which has indet. representation	**opt-in memory safety (initialization)**
12	A non-value representation is read via non-char. lvalue	type safety in opt-in memory safety mode
13	A non-value representation produced via non-char. lvalue	**trap**
14	Declarations which are not compatible	**linker constraint**
15	Composite type with unevaluated sizes	**constraint / defined, N3397, N3432**
16	Range error in conversion from to integer	trap (floating point exception)
17	Range error floating point	trap (floating point exception)
18	Lvalue does not designate object	**opt-in memory safety mode (lifetime)**
19	~~Conversion of incomplete lvalues~~	constraint (N3481, 2025/02)
20	Automatic not address taken.	**opt-in memory safety mode (initialization)**
21	~~Pointer conversion of arrays with register~~	implementation-defined (N3244, 2024/06)
22	~~Use of void expression~~	ghost (N3409, 2025/02)
23	Range, conversion pointer to integer	constraint
24	Conversion pointers, alignment	trap (UBSan: alignment)
25	Function call via incompat. pointer	type safety in opt-in memory safety mode
26	Unmatched single or double quote	(WIP, target: 2025/08)
27	Reserved keyword used incorrectly	constraint
28	Invalid character in identifier	(WIP, target: 2025/08)
29	Identifier starts with digit	(WIP, target: 2025/08)
30	Two identifier differ only in non-significant character	(WIP, target: 2025/08)
31	__func_ explicitly declared	special case of 27
32	Program attempts to modify string literal	**type safety in opt-in memory safety mode**
33	Various token issues	constraint / defined behavior
34	Sequencing of side effects	**defined order, N3203**
35	Exceptional condition during evaluation	trap (UBSan: signed-integer-overflow)
36	Object accessed via wrong type	type safety in opt-in memory safety mode
37	Function call via wrong type	type safety in opt-in memory safety mode
38	Member of atomic structure or union	constraint

	Undefined Behavior	Status / Plan
39	Operand of * has invalid value	trap (UBSan: null), **opt-in memory-safety**
40	~~Weird pointer conversion~~	constraint (N3340, 2024/10)
41	Division / modulo by zero	trap (UBSan: integer/float-divide-by-zero)
42	Non-reprs. Result for divsion / modulo	trap (UBSan: signed-integer-overflow)
43	OOB pointer arithmetic	**constraint / trap in opt-in memory safety mode**
44	Indirection of one-after pointer	**constraint / trap in opt-in memory safety mode**
45	Subtraction of unrelated pointers	implementation-defined behavior
46	OOB array subscription	trap (UBSan: bounds), N3395
47	Pointer subtraction not representable in ptrdiff	trap
48	Shift by neg. our too much	trap (UBSan: shift-exponents)
49	Signed left shift	trap (UBSan: shift)
50	Rel. comparison of unrelated pointers	implementation-defined behavior
51	Overlapping assignment	**defined behavior**
52	~~Integer constant expression~~	ghost (N3447, 2025/02)
53	~~Constant expression in initializer~~	ghost (N3447, 2025/02)
54	~~Arithmetic constant expression~~	ghost (N3447, 2025/02)
55	~~Object accessed in address constant~~	ghost (N3447, 2025/02)
56	~~Completeness after declaration for an object with no linkage~~	constraint (N3244, 2024/06)
57	~~Block scope function decl. with storage class~~	constraint (N3244, option 1, 2024/06)
58	~~Structure / union with no named members~~	implementation defined (N3341, 2024/10)
59	OOB FAM access or pointer arithmetic	**constraint in opt-in memory safety mode**
60	~~Tagged type not completed when needed.~~	ghost (N3244, 2024/06)
61	Modification of const-qualified object	type safety in opt-in memory safety mode
62	Access to volatile object via non-vol.	type safety in opt-in memory safety mode
63	~~Function types includes qualifier~~	implementation defined (N3342, 2024/10)
64	Two qualified types	ghost (WIP, target 2025/08)
65	Restrict, access rules	**constraint in opt-in memory safety mode**
66	Restrict, assignment	**constraint**
67	~~Inline function not also defined.~~	constraint (N3244, 2024/10)
68	_Noreturn function returns	trap (UBSan: unreachable)
69	Inconsistency of alignment specifiers	**constraint (N3244, alternative, 2024/10)** **linker constraint**
70	Different alignment across TU	**linker constraint**
71	Pointers required to be compatible	ghost (WIP, target: 2025/08)
72	VLA with non-positive size	trap (UBSan: vla-bound)
73	Arrays compatible including run-time	trap (GCC patch exists)
74	Static in array parameter	**trap + opt-in memory safety (bounds), N3395**
75	~~Storage classifier or qual. for void as parmareter~~	constraint (N3344, alternative 1, 2024/10)
76	Incompatible function types	type safety in opt-in memory safety mode
77	~~Inferred type extensions~~	moved to J.3
78	~~Inferred type extensions~~	moved to J.3
79	~~Value of unnamed member used~~	ghost (N3245, 2024/10)
80	~~Initializer UB~~	constraint (N3346, 2024/10)
81	~~Initializer UB~~	constraint (N3346, 2024/10)
82	~~Initializer UB~~	constraint (N3346, 2024/10)
83	Call of function via unsequenced etc.	**unspecified result**
84	Unequal to one external definitions	**linker constraint**
85	~~A function with variable type without ...~~	ghost (N3482, 2025/02)
86	Function reaches } and return value is used	**constraint / trap N3483**
87	~~Tentative def. with internal linkage and incomplete type~~	constraint (N3347 + RM 26758, 2024/10)

Acknowledgments: The Undefined Behavior Study Group for discussions. All errors are my own.