From: Frank Farance
Organization: Farance Inc.
Telephone: +1 212 486 4700
Fax: +1 212 759 1605
E-mail: frank@farance.com
Date: 1995-12-22
Document Number: WG14/N527 X3J11/95-128
Subject: DR on Variable Length Structures

Question:

It the following conforming?

```
struct x
{
        char y[1];
};
struct x *z;

z = (struct x *) malloc(sizeof(*z)+100);
z->y[5] = '?';
```

In defect report 051, we state that this isn't conforming behavior because the pointer arithmetic for the larger structure might not be compatible with a smaller structure. Thus, we recommend the ''safer'' idiom:

```
#define HUGE_ARR

struct x
{
        char y[HUGE_ARR];
};
struct x *z;

z = (struct x *) malloc(sizeof(*z)-HUGE_ARR+100);
z->y[5] = '?';
```

However, in defect report 073, we state that the ''safer'' idiom is undefined behavior because it is possible implement the "->" operator as first fetching all of "*z", then selecting "y[5]" from it. This approach would cause access to unallocated memory, thus, the operation produces undefined behavior.

Our responses to the question have been inconsistent. At the 1995-10 meeting in Nashua, WG14 indicated that it wanted to designate this as undefined behavior.