15-122: Principles of Imperative Computation

R10: From C1 to Shining C

Andrew Benson, Tom Cortina

Header Files

In C0 and C1, we usually wrote the interface and implementation of our data structures in the same file. Unfortunately, this means that if we want to show clients our data structure's interface, we end up showing them our implementation too! C solves this by separating the interface and implementation respectively into a header file and a source file. A header file for BST's is shown below:

```
1  #ifndef _BST_H_
2  #define _BST_H_
3
4  typedef struct bst_header *bst;
5  typedef int compare_fn(void* e1, void* e2);
6  typedef void free_fn(void* e);
7
8  bst bst_new(compare_fn* elem_compare, free_fn* elem_free);
9  void bst_insert(bst B, void* e); /* e cannot be NULL! */
10 void* bst_lookup(bst B, void* e); /* return NULL if not in tree */
11 void bst_free(bst B);
12
13 #endif
```

Header files usually only contain type and function declarations for the client and no actual code.

Aside: the `#ifndef`, `#define`, and `#endif` lines are known as header guards, and they prevent the header file from being included too many times in a file.

Contracts

Contracts are a core part of the C0 and C1 languages. Unfortunately, we don't have the power to build contracts into C. Don't lose hope, though! We provide you with a supplemental contracts library so you can continue to program with contracts. To use it, you'll need to put `#include "path to contracts.h"` at the top of your C file. Also, you'll need to pass the `-DDEBUG` flag instead of `-d` when you compile with gcc if you want contracts to be checked.

`contracts.h` provides you with `REQUIRES`, `ENSURES`, and `ASSERT`. You can treat these as C functions* that replace our contracts in the following way:

(a) `//@requires` can be replaced by `REQUIRES` at the very beginning of the function.

(b) `//@ensures` can be replaced by `ENSURES` before every return statement and/or at the end of the function.

(c) `//@loop_invariant` can be replaced by `ASSERT` before the loop runs and at the end of each loop iteration.

(d) `//@assert` can be replaced by `ASSERT`.

*To be precise, these are actually C macros that preprocessing reduces to native C `assert` statements during compilation. Shhh, don't tell.

Checkpoint 0

Rewrite the following C0 function into C. Only the contracts will need to be changed.

```
1  int length(list* start, list* end)
2  //@requires is_segment(start, end);
3  //@ensures \result > 0;
4  {
5    int length = 0;
6    while (start != end)
7    //@loop_invariant is_segment(start, end);
8    {
9      length++;
10     start = start->next;
11   }
12   return length;
13 }
```

Memory Allocation

In C0 and C1, we had the functions `alloc`, which allocated enough memory for a singleton of some type, and `alloc_array`, which allocated enough memory for an array of some type. In C, there is only* `malloc`, which takes one argument - the amount of memory you want.

For example, in equivalent of `alloc(struct list_node)` in C is `malloc(sizeof(int))`, and the equivalent of `alloc_array(int, 3)` in C is `malloc(3*sizeof(int))`.

However, `malloc` can return `NULL` in certain high-memory cases. Usually you would have to check the return value to see if it is `NULL`, but we provide you with a replacement for `malloc` that does this check for you: `xmalloc`. To use it, put `#include "path to xalloc.h"` at the beginning of your C file.

*Note that `malloc` does not initialize the memory it allocates to 0. If you require this, there is a variant of `malloc` called `calloc` (and a corresponding `xcalloc`) that does this.

Freeing Memory

After you are done using any memory referenced by a pointer returned by `malloc` or `calloc`, you must free it or your program will have "memory leaks" (in C0 and C1, something called a garbage collector does this automatically. We might discuss this more in depth later in the semester.) You can free such memory by passing a pointer to it to `free`. Once you free it, it is undefined to access that memory. Also, don't free memory that was previously freed. That also results in undefined behavior.

When we design libraries for data structures like stacks and BST's, it's important to specify whether the client or library is responsible for freeing each piece of memory that is `malloc`ed. Usually, whoever allocates the memory "owns" it and is responsible for freeing it, but in data structures like BST's, we may want to transfer ownership of the memory to the data structure. Thus, we ask the client to supply a "freeing" function in `bst_new` for BST elements, so that when the client calls `bst_free`, we can call their "freeing" function on every element in the BST. If the function pointer the client gives us is `NULL`, then we don't free the BST elements.

Checkpoint 1

Rewrite `bst_new` (which should take in a pointer to a "freeing function") and `bst_insert` into C, and write the function `bst_free`, which frees all the memory that the BST is responsible for.

```
1 typedef int compare_fn(void* e1, void* e2);
2
3 typedef struct tree_node tree;
4 struct tree_node {
5   void* data;
6   tree* left;
7   tree* right;
8 };
9
10 typedef struct bst_header bst;
11 struct bst_header {
12   tree* root;
13   compare_fn* compare;
14 };
15
16 bst* bst_new(compare_fn* compare)
17 //@requires compare != NULL;
18 //@ensures is_bst(\result);
19 {
20   bst* B = alloc(struct bst_header);
21   B->root = NULL;
22   B->compare = compare;
23   return B;
24 }
25
26 tree* tree_insert(tree* T, void* e, compare_fn* compare)
27 //@requires e != NULL && compare != NULL && is_tree(T, compare);
28 //@ensures is_tree(\result, compare);
29 {
30   if (T == NULL) {
31     /* create new node and return it */
32     T = alloc(struct tree_node);
33     T->data = e;
34     T->left = NULL; T->right = NULL;
35     return T;
36   }
37   int r = (*compare)(e, T->data);
38   if (r == 0) {
39     T->data = e;        /* modify in place */
40   } else if (r < 0) {
41     T->left = tree_insert(T->left, e, compare);
42   } else {
43     //@assert r > 0;
44     T->right = tree_insert(T->right, e, compare);
45   }
46   return T;
47 }
48
49
```

```
50 void bst_insert(bst* B, void* e)
51 //@requires is_bst(B);
52 //@requires e != NULL;
53 //@ensures is_bst(B);
54 {
55   B->root = tree_insert(B->root, e, B->compare);
56   return;
57 }
```

Write `bst_free` here: