A Design by Contract Library for C

Brandon Koepke

February 12, 2016

Contents

Abstract

Design by contract is a software correctness methodology. The intention is to define a formal interface for abstract data types using preconditions, postconditions, and invariants. This library can be used to ensure that certain properties are always satisfied at runtime.

1 Motivation

Design by contract is normally used both as a form of runtime contracts (to ensure that an object doesn't invalidate it's invariants) and as a form of documentation. By forcing software developers to explicitly state method contracts we can make it much easier to understand what an implementation of a method should be doing.

Testing is another method that can be used in conjunction with design by contract to ensure that certain software properties hold. The difference with design by contract is that we can ensure that *all* implementations of a method satisfy certain properties.

In the formal methods hierarchy, design by contract sits close to the bottom (between formal specification and formal development). Since the contracts specified by a design by contract system are evaluated at runtime there is a performance penalty to using them; however, they take significantly less time during development than other formal method systems (refinement types, dependent types, theorem provers, etc) at this time.

2 Contract System

2.1 Common

We start off with the common contract definition which will be used by the implementation of many of the other contracts. We take in an expression as well as a string representation of that same expression so we can pretty-print the contract violation. We also take in the file name, line number, the function name, and a format string. Within this contract we then check whether the expression is satisfied. If it is not then we print the error, assert failure (to aid with debugging), and finally exit with failure status. The reason that we are failing hard and fast with these contract violations is because we do not know

whether the program still has valid state after a contract violation. In theory, none of these contracts should ever be violated in release code.

2a ⟨*contract-c* 2a⟩≡ (6b)

```
void contract(bool expr, const char *expr_s, const char *file,
              int line, const char *func, const char *format) {
  if (!expr) {
    fprintf(stderr, format, file, line, func, expr_s);
    assert(false), exit(EXIT_FAILURE);
  }
}
```

We also define a generic contract that asserts that it's input is non-null and also returns it's argument to the caller.

2b ⟨*contract-non-null-c* 2b⟩≡ (6b)

```
void *contract_non_null(const void *x, const char *x_s,
                        const char *file, int line,
                        const char *func, const char *format) {
  if (x == NULL) {
    fprintf(stderr, format, file, line, func, x_s);
    assert(false), exit(EXIT_FAILURE);
  }
  return void_cast(x);
}
```

Finally, we have a generic contract that asserts equailty between two values and returns the first argument to the caller.

2c ⟨*contract-equal-c* 2c⟩≡ (6b)

```
void *contract_equal(const void *a, const void *b,
                     const char *a_s, const char *b_s,
                     const char *file, int line, const char *func,
                     const char *format) {
  if (a != b) {
    fprintf(stderr, format, file, line, func, a_s, b_s);
    assert(false), exit(EXIT_FAILURE);
  }
  return void_cast(a);
}
```

2.2 Strong

Strong contracts are contracts that should be left in release code (in other words, they are part of the public API).

We start off by defining a simple contract that will always fail when reached. This enables us to make failure cases explicit. We use *#define* here so we can get references to the point in the source code where the contract was violated. We are failing hard in all of our contracts because contract failures indicate programmer errors, not situations that can be recovered from.

2d ⟨*contract-fail-h* 2d⟩≡ (6a)

```
#define contract_fail() _contract_fail(__FILE__, __LINE__, __func__)
void _contract_fail(const char *file, int line, const char *func);
```

2e ⟨*contract-fail-c* 2e⟩≡ (6b)

```
void _contract_fail(const char *file, int line, const char *func) {
  fprintf(stderr, "%s:%d: %s: Fail.\n", file, line, func);
  assert(false), exit(EXIT_FAILURE);
}
```

We also define a contract that ensures a value is not null before proceeding with the body of a method. In order to facilitate more compact code we also return a reference to the value that was passed in. Also note that we have a defined 'function' as well as the actual function itself. Do not use the function declaration directly, the *#define* is the intended function call and the function declaration is only exposed in order to facilitate the defined function.

3a ⟨*contract-requires-non-null-h* 3a⟩≡ (6a)

```
#define contract_requires_non_null(x)                                          \
  _contract_requires_non_null((x), #x, __FILE__, __LINE__, __func__)
void *_contract_requires_non_null(const void *x, const char *x_s,
                                  const char *file, int line, const char *func);
```

3b ⟨*contract-requires-non-null-c* 3b⟩≡ (6b)

```
void *_contract_requires_non_null(const void *x, const char *x_s,
                                  const char *file, int line,
                                  const char *func) {
  return contract_non_null(x, x_s, file, line, func,
                           "%s:%d: %s: Requires ‘%s’ != NULL failed.\n");
}
```

It is also useful to be able to assert equality between two values.

3c ⟨*contract-requires-equal-h* 3c⟩≡ (6a)

```
#define contract_requires_equal(a, b)                                          \
  _contract_requires_equal((a), (b), #a, #b, __FILE__, __LINE__, __func__)
void *_contract_requires_equal(const void *a, const void *b, const char *a_s,
                               const char *b_s, const char *file, int line,
                               const char *func);
```

3d ⟨*contract-requires-equal-c* 3d⟩≡ (6b)

```
void *_contract_requires_equal(const void *a, const void *b, const char *a_s,
                               const char *b_s, const char *file, int line,
                               const char *func) {
  return contract_equal(a, b, a_s, b_s, file, line, func,
                        "%s:%d: %s: Requires ‘%s’ == ‘%s’ failed.\n");
}
```

We can also assert arbitrary expressions.

3e ⟨*contract-requires-h* 3e⟩≡ (6a)

```
#define contract_requires(expr)                                                \
  _contract_requires((expr), #expr, __FILE__, __LINE__, __func__)
void _contract_requires(bool expr, const char *expr_s, const char *file,
                        int line, const char *func);
```

3f ⟨*contract-requires-c* 3f⟩≡ (6b)

```
void _contract_requires(bool expr, const char *expr_s, const char *file,
                        int line, const char *func) {
  contract(expr, expr_s, file, line, func,
           "%s:%d: %s: Requires ‘%s’ failed.\n");
}
```

We also define these contracts as postconditions. While you could use the requires contracts for postconditions as well (they do the same thing), using ensures signifies intent.

3g ⟨*contract-ensures-h* 3g⟩≡ (6a)

```
#define contract_ensures(expr)                                                 \
  _contract_ensures((expr), #expr, __FILE__, __LINE__, __func__)
void _contract_ensures(bool expr, const char *expr_s, const char *file,
                       int line, const char *func);
```

4a ⟨*contract-ensures-c* 4a⟩≡ (6b)

```
void _contract_ensures(bool expr, const char *expr_s, const char *file,
                       int line, const char *func) {
  contract(expr, expr_s, file, line, func, "%s:%d: %s: Ensures ‘%s’ failed.\n");
}
```

4b ⟨*contract-ensures-non-null-h* 4b⟩≡ (6a)

```
#define contract_ensures_non_null(x)                                          \
  _contract_ensures_non_null((x), #x, __FILE__, __LINE__, __func__)
void *_contract_ensures_non_null(const void *x, const char *x_s,
                                 const char *file, int line, const char *func);
```

4c ⟨*contract-ensures-non-null-c* 4c⟩≡ (6b)

```
void *_contract_ensures_non_null(const void *x, const char *x_s,
                                 const char *file, int line, const char *func) {
  return contract_non_null(x, x_s, file, line, func,
                           "%s:%d: %s: Ensures ‘%s’ != NULL failed.\n");
}
```

4d ⟨*contract-ensures-equal-h* 4d⟩≡ (6a)

```
#define contract_ensures_equal(a, b)                                          \
  _contract_ensures_equal((a), (b), #a, #b, __FILE__, __LINE__, __func__)
void *_contract_ensures_equal(const void *a, const void *b, const char *a_s,
                              const char *b_s, const char *file, int line,
                              const char *func);
```

4e ⟨*contract-ensures-equal-c* 4e⟩≡ (6b)

```
void *_contract_ensures_equal(const void *a, const void *b, const char *a_s,
                              const char *b_s, const char *file, int line,
                              const char *func) {
  return contract_equal(a, b, a_s, b_s, file, line, func,
                        "%s:%d: %s: Ensures ‘%s’ == ‘%s’ failed.\n");
}
```

Finally we define the same contracts as invariants.

4f ⟨*contract-invariant-h* 4f⟩≡ (6a)

```
#define contract_invariant(expr)                                              \
  _contract_invariant((expr), #expr, __FILE__, __LINE__, __func__)
void _contract_invariant(bool expr, const char *expr_s, const char *file,
                         int line, const char *func);
```

4g ⟨*contract-invariant-c* 4g⟩≡ (6b)

```
void _contract_invariant(bool expr, const char *expr_s, const char *file,
                         int line, const char *func) {
  contract(expr, expr_s, file, line, func,
           "%s:%d: %s: Invariant ‘%s’ failed.\n");
}
```

4h ⟨*contract-invariant-non-null-h* 4h⟩≡ (6a)

```
#define contract_invariant_non_null(x)                                        \
  _contract_invariant_non_null((x), #x, __FILE__, __LINE__, __func__)
void *_contract_invariant_non_null(const void *x, const char *x_s,
                                   const char *file, int line,
                                   const char *func);
```

5a ⟨*contract-invariant-non-null-c* 5a⟩≡ (6b)

```
void *_contract_invariant_non_null(const void *x, const char *x_s,
                                   const char *file, int line,
                                   const char *func) {
  return contract_non_null(x, x_s, file, line, func,
                           "%s:%d: %s: Invariant ‘%s’ != NULL failed.\n");
}
```

5b ⟨*contract-invariant-equal-h* 5b⟩≡ (6a)

```
#define contract_invariant_equal(a, b)                                  \
  _contract_invariant_equal((a), (b), #a, #b, __FILE__, __LINE__, __func__)
void *_contract_invariant_equal(const void *a, const void *b, const char *a_s,
                                const char *b_s, const char *file, int line,
                                const char *func);
```

5c ⟨*contract-invariant-equal-c* 5c⟩≡ (6b)

```
void *_contract_invariant_equal(const void *a, const void *b, const char *a_s,
                                const char *b_s, const char *file, int line,
                                const char *func) {
  return contract_equal(a, b, a_s, b_s, file, line, func,
                        "%s:%d: %s: Invariant ‘%s’ == ‘%s’ failed.\n");
}
```

2.3 Weak

The weak contracts are implemented in the same way as the strong contracts, the only difference is that we can compile these out without impacting the API of the application.

5d ⟨*contract-weak-h* 5d⟩≡ (6a)

```
#define contract_weak_requires(expr)                                    \
  _contract_requires((expr), #expr, __FILE__, __LINE__, __func__)
#define contract_weak_requires_non_null(x)                              \
  _contract_requires_non_null((x), #x, __FILE__, __LINE__, __func__)
#define contract_weak_requires_equal(a, b)                              \
  _contract_requires_equal((a), (b), #a, #b, __FILE__, __LINE__, __func__)

#define contract_weak_ensures(expr)                                     \
  _contract_ensures((expr), #expr, __FILE__, __LINE__, __func__)
#define contract_weak_ensures_non_null(x)                               \
  _contract_ensures_non_null((x), #x, __FILE__, __LINE__, __func__)
#define contract_weak_ensures_equal(a, b)                               \
  _contract_ensures_equal((a), (b), #a, #b, __FILE__, __LINE__, __func__)
```

6a ⟨*contract.h* 6a⟩≡

```
#pragma once
#include <stdbool.h>
⟨contract-fail-h 2d⟩

⟨contract-requires-non-null-h 3a⟩
⟨contract-requires-equal-h 3c⟩
⟨contract-requires-h 3e⟩

⟨contract-ensures-non-null-h 4b⟩
⟨contract-ensures-equal-h 4d⟩
⟨contract-ensures-h 3g⟩

⟨contract-invariant-non-null-h 4h⟩
⟨contract-invariant-equal-h 5b⟩
⟨contract-invariant-h 4f⟩

⟨contract-weak-h 5d⟩
```

6b ⟨*contract.c* 6b⟩≡

```
#include "contract.h"
#include "unsafe.h"

#include <assert.h>
#include <stdio.h>
#include <stdlib.h>

⟨contract-c 2a⟩

⟨contract-fail-c 2e⟩
⟨contract-non-null-c 2b⟩
⟨contract-equal-c 2c⟩

⟨contract-requires-non-null-c 3b⟩
⟨contract-requires-equal-c 3d⟩
⟨contract-requires-c 3f⟩

⟨contract-ensures-non-null-c 4c⟩
⟨contract-ensures-equal-c 4e⟩
⟨contract-ensures-c 4a⟩

⟨contract-invariant-non-null-c 5a⟩
⟨contract-invariant-equal-c 5c⟩
⟨contract-invariant-c 4g⟩
```

3 Unsafe

Definition for unsafe methods, i.e. methods that may be used only with extreme caution. For the moment we only define a void cast operator. This way we can find all void casts in our code easily and quickly and also easily find void casts that have not been checked for consistency. By using this method you are signifying that you know that the void cast is safe.

6c ⟨*unsafe.h* 6c⟩≡

```
#pragma once
#define void_cast(p)((void *) p)
```