

Homework 10

Jiří Klepl

a) The modified program:

```
char mybuf[256];

void concatenate(
    char buf1[], unsigned len1,
    char buf2[], unsigned len2) {
    if (len1 + len2 > 256) return; // len1 + len2 <= 256

    { unsigned i = 0;
      if (i != len1) {
          assert(i < len1); // and we don't need (i >= 0)
          i = *;
          assume(i < len1);

          asssert(i < 256); // subsumed by (i < len1)
          asssert(i < len1); // assumed
          mybuf[i] = buf1[i];
          i++;
          assert(i != len1 -> i < len1);
      }
    }

    { unsigned i = 0;
      if (i != len2) {
          assert(i < len2);
          i = *;
          assume(i < len2);

          assert(i + len1 <= 256); // subsumed by:
              // (i < len2 && len1 + len2 < 256)
          assert(i < len2); // assumed
          mybuf[len1 + i] = buf2[i];
          i++;
          assert(i != len2 -> i < len2);
      }
    }
}
```

b) see a)

c) They do not hold. Under bit-vector arithmetics, it is possible that $len1 + len2 < 256 \wedge \exists i : 0 \leq i < len2 \rightarrow len1 + i \geq 256$.