1 Correctness of Recursive Algorithms

Consider an algorithm of integer multiplication (multiply an m-bit number a and an n-bit number b).

Preconditions:

- m, n are positive integers
- $-2^m < a < 2^m$ and $-2^n < b < 2^n$ for any $a, b \in \mathbb{Z}$.

Postconditions: return $a \times b$.

Suppose that n and m are even.

Let a', a'' be such that $a = a' \times 2^{m/2} + a''$.

Similarly, let b', b'' be such that $b = b' \times 2^{n/2} + b''$.

Let $T(m, n)$ be the worst case time to perform this algorithm.

Then $a \times b = (a' \times 2^{m/2} + a'') \times (b' \times 2^{n/2} + b'')$, and hence $T(m, n) = 4T(m/2, n/2) + c(m+n)$ for some constant c.

When $m = n$, we obtain that $T(n, n) = 4T(n/2, n/2) + 2cn$.

By Master Theorem, $T(n/2, n/2) \in \Omega(n^2)$.

Consider now another algorithm:

F(a, b, m, n)

```
if n = 1
    then if b = 0 then return 0
            b = −1 then return − a
         else return a
            fi
            fi
              if m = 1
                  then if a = 0 then return 0
                          a = −1 then retu
                       else return b
                          fi
                          fi
                          n′ ← n ÷ 2
                          a′ ← a ÷ 2^{n′}
                          a′′ ← a mod 2^{n′}
                          m′ ← m ÷ 2
                          b′ ← b ÷ 2^{m′}
                          b′′ ← b mod 2^{m′}
                          c ← F(a′, b′, n −
                          d ← F(a′′, b′′, n′,
                          e ← F(a′ − a′′, b′
                          return c × 2^{n′+m′}
```

Let $P(m, n)$ = "$\forall a \in \mathbb{Z} \forall b \in \mathbb{Z}$ if $-2^n < a < 2^n$ and $-2^m < b < 2^m$ then $F(a, b, m, n)$ halts and returns $a \times b$".

Proof:

Let $(m, n) \in \mathbb{Z}^m \times \mathbb{Z}^n$ be arbitrary. Assume $P(u, v)$ is true for all $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ such that $u < m$ and $v < n$.

If $n = 1$, then b is a $*$-bit integer, $b \in$

If $b = 0$, then $a \times b = 0$ which is return on line 2. If b$= -1$ then $a \times b = -a$, which is returned on line 3.

If $b = 1$, then $a \times b = a$, which is returned on line 4.

When $m = 1$, there is a similar argument. Therefore, $P(1, 1)$ is satisfied.

Suppose $m, n > 1$.

Then $1 \leq \lfloor n/2 \rfloor \leq \lceil n/2 \rceil < n$ and $1 \leq \lfloor m2 \rfloor \leq m2 < m$.

Note that $n' = \lfloor n/2 \rfloor$ and $m - m' = \lceil m/2 \rceil$, so $P(m', n')$ and $P(m'', n'')$ are true.

Let a, b be arbitrary integers with $-2^m < a < 2^m$ and $-2^n < b < 2^n$.

Then $a = a' \times 2^{m'} + a''$ and $b = b' \times 2^{n'} + b''$, while $-2^{m'} < a'' < 2^{m'}$ and $-2^{n'} < b' < 2^{n'}$.

Similarly, we obtain that $-2^{m-m'} < a' < 2^{n-m'}$ and $-2^{n-n'} < b' < 2^{n-n'}$.

Thus, $-2^{m-m'} < a' - a'' < 2^{m-m'}$ and $-2^{n-n'} < b' - b'' < 2^{n-n'}$.

Then $c = a'b'$ by $P(m - m', n - n')$ and line 15 and $d = a'' \times b''$ by $P(m', n')$ and line 16.

We also have $e = (a' - a'') \times (b' - b'')$ by $P(m - m', n - n')$ and line 17.

Exercise: Continue the proof.