Formal Methods in Systems Engineering

Block 2 – WS 2025

Mini Project for Block 2
Due November 21, 2025

Note: The deadline for submitting your solution of the project is November 21, 2025. Please upload your solution as a zip-file, containing a Dafny-file named `bezout_<surname>_<matrnr>.dfy` **to TUWEL.**

The assignment requires you to verify total correctness of a given program using Dafny.

1 Installing and Running Dafny

Install Dafny `4.11.*` or versions above, as described on `https://dafny.org/latest/Installation`. The usual steps required are

1. installing .NET 8.0, and
2. installing the VSCode extension[1] (**recommended**), or downloading and running the binaries.

VSCode. Once the extension is installed and you open the Dafny-file, the verification is performed as you make changes and verification errors are shown in the editor. On successful verification, a green check mark will appear next to the method. Additionally, you can activate `Dafny: Show verification trace` through the command palette, or by right-clicking in the file, which can help identify the reason for verification failures.

CLI. Run `dafny verify bezout.dfy` to verify the program. The flag `--extract-counterexample` can help identify the reason for verification failure.

2 Assignment

The file `bezout.dfy` contains a method implementing the extended euclidean algorithm with the following method signature.

```
method bezout(a: int, b: int) returns (g: int, x: int, y: int)
    requires a >= 0
    requires b >= 0
    ensures g >= 0
    ensures a * x + b * y == g
{
...
```

Given two integers a and b, the algorithm computes g, x, y, such that:

- g is the greatest common divisor of a and b, i.e. $g = gcd(a, b)$
- x and y are the Bézout coefficients[2] of a and b, which means that $ax + by = g$.

Your task is to verify the total correctness of this method with respect to the given annotations: you should verify that the g returned is positive and that the return values x and y are in fact the Bézout coefficients. You are not required to prove that g is in fact $gcd(a, b)$. **Hint:** For termination of the outer loop, try to find a decreasing expression using `a'` and `b'`. You can also use branching with `if...then...else...` within such expressions.

To complete this assignment, you should **add invariants** using the `invariant` keyword for the while loops and **add decreasing terms** using the `decreases` keyword as needed. Additionally, you can add `assert` statements, which can help identify the cause of verification failures, and can help against verification timeouts. Do not modify the implementation, as well as the pre- and postconditions.

Make sure that your solution is verified reliably within the (default) verification timeout of 20 seconds. If it takes longer to verify your solution, or you require additional arguments being passed to Dafny, make sure to indicate that at the top of your submitted file (add it as a Dafny comment).

3 Submission

Submit a zip-file containing a Dafny file named `bezout_<surname>_<matrnr>.dfy` with the original code and the annotations you added to TUWEL before **November 21, 2025**.

[1] `https://marketplace.visualstudio.com/items?itemName=dafny-lang.ide-vscode`

[2] `https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity`