Exercises 11 January 20, 2023

$\boxed{1}$ Use the Nelson-Oppen procedure to determine satisfiability of the following formulas (you can choose either the deterministic or the non-deterministic version):

[2] (a) The following formula combines uninterpreted functions and linear real arithmetic:

$$z = 0 \wedge y \leq x \wedge x \leq y + z \wedge \mathsf{f}(y) = \mathsf{f}(z) \wedge \mathsf{f}(y) = 1 \wedge \mathsf{f}(z) = 2$$

[2] (b) The following formula combines uninterpreted functions and linear real arithmetic:

$$x = y + 1 \wedge y \leq z \wedge x \geq z + 1 \wedge \mathsf{f}(y) = \mathsf{a} \wedge \mathsf{f}(z) = \mathsf{b}$$

[2] (c) The following formula combines uninterpreted functions and linear *integer* arithmetic:

$$1 \leq x \wedge x \leq 2 \wedge \mathsf{f}(1) = \mathsf{a} \wedge \mathsf{f}(x) = \mathsf{b} \wedge \mathsf{a} = \mathsf{b} + 2 \wedge \mathsf{f}(2) = \mathsf{f}(1) + 3$$

[2] $\boxed{2}$ Is the theory of bit vectors convex? Give a proof or a counterexample.

$\boxed{3}$ Consider the following hash functions and try to find hash collisions.

[2] (a) For the following Bernstein hash, is there a hash collision for strings of length 8?

```
unsigned bernstein(char *s, int len){
    unsigned h = 0;
    for (int i = 0; i < len; i++)
        h = (h * 33) + s[i];
    return h;
}
```

[2] ⋆ (b) For the following FNV hash, is there a hash collision for strings of length 3?

```
unsigned fnv(char *s, int len){
    unsigned h = 14695981039346656037;
    for (int i = 0; i < len; i++)
        h = (h * 1099511628211) ^ s[i];
    return h;
}
```

[2] ⋆ $\boxed{4}$ Let T be the theory over a signature with a binary function symbol f and unary function symbols g and h, and equality, and with the axioms of equality together with the two sentences

$$\forall x\, y.\, x = \mathsf{f}(\mathsf{g}(x), \mathsf{g}(y))) \qquad\qquad \forall x\, y.\, y = \mathsf{f}(\mathsf{g}(x), \mathsf{h}(y)).$$

Is T stably infinite?