

What is Decidable about String Constraints with the ReplaceAll Function

Strings are a generic but error-prone data type

Vision: a rich string constraint language & fast string solver

prog.js

```
from z3 import *
def main():
    s = Solver()
    A = Bool('A')
    B = Bool('B')
    P = Not(Implies( And(Implies(A,B), A), B ))
    s.add(P)
    # Note that sat and unsat below are constants defined in z3
    if s.check() == sat:
        print('Satisfiable')
    else:
        print('Unsatisfiable')
```

String constraint

φ

supported operations:

- concatenation
- length
- regex matching

This paper: adding **replaceAll** to string constraints

e.g. **replaceAll**("I eat meat", "eat", "slice") = "I slice mslice"

Can model functions important in analysis of XSS vulnerabilities!