

# COMP 597: Assignment #1

Instructor: Xujie Si, TA: Breandan Considine

September 20, 2021

This is the first assignment of COMP 597: Automated Reasoning with ML.

## 1 SAT Encoding

The following solutions can be obtained using a solver of your choice. Please show all work. Only solutions obtained with a SAT solver will receive credit.

**Palindromic primes** (20 points): A prime palindrome is a natural number with exactly two factors which are the same written forwards or backwards. Let  $1802201963_{10} = PQR$ . What are its factors in base-2? What is the largest  $M = PQR$  whose factors are all distinct binary palindromes you can find in an hour? Please describe your solution and its SAT encoding.

**Bonus question** (10 points): Every alphanumeric character in the following ciphertext maps to a single case-insensitive letter in the English alphabet. Every plaintext word can be found in the English 10k dictionary.<sup>1</sup>

```
1W9G9 QL U 5U30 I91RM0Y JWM PY3GZULQYT 3SC6AMOP1K 2X 1W0 LKLJZCB R9 I4QAN HYN 24G UIPAP1K 12 NZEM826 QDJ08A0314HA
722AL XS5 4DN95L1UDNPD7 7WUJ 3SC6A90P1K. PX 7W0 5H3M QB RSD IK S4G J228L, 7WZD BKL1MCL RPVA 9EOY14UVVK IZ3SC9 MHLPOG
1S 4BM HYN CS5M G98QUIA9. PX DS1, 1W9K RP8V 32DJPD40 JS IZ3SCZ WHGNM5 7S 4B0 UDN VOBL 5M8PUI80 X2G UVA I4J H GOVUJQE98K
BCHVV B01 SX 3SCC2Y 7UBFL. TPEOD W2R WHGN 1WQYFPYT QL, QX 1W2B9 QDJM8AM314U8 7228L UG9 JS L433ZZN, 1WMK RPAV WUEZ
7S B4IL1QJ47M 3UA34VU1PSD X25 JW24TW7.
```

What is the plaintext and who originally wrote this? Please describe how you solved it, provide the key and SAT encoding in a language of your choice.

---

<sup>1</sup><https://github.com/first20hours/google-10000-english/blob/master/google-10000-english.txt>

## 2 Problem 2: DIY SAT Solving

**Programming exercise** (40 points): Choose one of the following two options, write about it, and submit your source code. Give instructions for how to run it and a few test cases.

1. Implement your own solver. Either DPLL, UP or two-watched literals.
2. Hack into MiniSat/Kissat. Make improvement. Report your findings.

## 3 Problem 3: Uninterpreted function equivalence

**SMT exercise** (40 points): Implement an uninterpreted function solver and test it on the following questions:

1.  $a * (b + c + d) \stackrel{?}{=} a * b + a * c + a * d$
2. ...