# Problem-set 04 

Mostafa Touny

## Contents

Ex. 1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
a . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
b . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
Ex. 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
Ex. 3 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
a . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
b . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
Ex. 4 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
a . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
b . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
c . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3
d . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
lectures 8,9 (skimmed) Sipser Ch. 1.2; and, 3.2, 3.3 on nondeterminism. Sipser first half of Ch. 7.4 (and also Ch. 5.3 if it helps).

## Ex. 1

a
Obviously the problem has a polynomial-time verifier by specifying the range of the subsequence common among all $w_{i}$. It's easy to loop on that range $k$, Checking whether corresponding positions of all $w_{j}$ are the same.

## b

Obviously a verifier is some input $x_{0}$ such that $C_{1}\left(x_{0}\right) \neq C_{2}\left(x_{0}\right)$. It's easy to compute both circuits and check their unequal output.

## Ex. 2

Intuitively, If a problem has some varifier, Then we can brute-force all possible verifiers. Observe we can choose the greatest branching factor $c_{\max }$ so that time is upper-bounded by $c_{\max }^{\operatorname{poly(n)}}$. Alternatively, Our argument might be seen through the perspective of a tree of an $N P$ problem, where $\operatorname{poly}(n)$ is the time required of the longest path of the tree.
I am not aware of any more rigorous proof.

## Ex. 3

a
For clarity and brevity we list all cases:

- unit clause $x_{i}$
- delete any clause containing $x_{i}$
- delete $\neg x_{i}$ from any clase
- unit clause $\neg x_{i}$
- delete any clause containing $\neg x_{i}$
- delete $x_{i}$ from any clause

Due to symmetry we mention only the case of unit clause $x_{i}$.
We prove the new propagated $C^{\prime}$ is satisfiable if and only if the given $C$ is satisfiable.
$(\leftarrow)$ Necessarily $x_{i}=$ True. Hence any clause containing $x_{i}$ is immediately evaluated to True as well. Since $\neg x_{i}=$ False one of the remaining units of the clause containing $\neg x_{i}$ must be evaluated to True.
$(\rightarrow)$ Following the same reasoning, Since $x_{i}=$ True, adding any clause containig $x_{i}$ is still going to be true regardless of other units boolean values. Also adding
$\neg x_{i}=$ False to any clause evaluated to True won't change the whole clause's boolean value.
b
We give a constructive polynomial-time algorithm. We follow the hint mentioned in the problem statement.

For case (ii), Loop on clauses, and for each:

- If no negative literal is assigned any value, Conveniently pick-up the first negative literal $\neg x_{k}$ and assign $x_{k}=$ False.
- If a negative literal $\neg x_{k}$ is assigned $x_{k}=$ False, Continue to the next clause.

Observe we only assign $x_{k}=$ False. As a result, the case of a negative literal $\neg x_{k}$ assigned $x_{k}=$ True won't ever be encountered.

For case (i), Keep applying the process of $a$, Until all unit-clauses are eliminated. If any clause is empty, It's concluded the given $C$ is unsatisfiable. Now we know every clause contains at least two literals, Including a negative literal. Case (i) is now reduced to case (ii).

## Ex. 4

## a

Clearly, If literals $x_{i}$ which are assigned to 1 are even, Then they can re-arranged as pairs, Each yielding 0 , and in turn all pairs yield 0 . Observe for an even number, $2 k \bmod 2=0$.

Similarly, if literals $x_{i}$ which are assigned to 1 are odd, Then we obtain 1 XOR $0=1$, by separating one literal from the remaining even literals.
b
We define summation as, $\epsilon_{1}+\epsilon_{2}=c_{1}+c_{2}+1$ where are $\sum_{i} x_{1 i}=c_{1} \bmod 2$ and $\sum_{i} x_{2 i}=c_{2} \bmod 2$. Note if $c_{1}=c_{2}=1$, Then $c_{1}+c_{2}+1=1+1+1=1 \bmod 2$ and hence $\left(\epsilon_{1}+\epsilon_{2}\right)(x)=1$. On the other hand, If $1+c_{2}+1=1 \bmod 2$, Then $c_{2}=-1=1 \bmod 2$. Hence, $\epsilon_{2}(x)=1$.
c
Consider $k_{1}$ to be the number of equations in which $x_{11}$ appreas.

$$
\text { Update } x_{11} \text { to }\left\{\begin{array}{lr}
0, & \text { if } k_{1} \text { is even }  \tag{1}\\
k_{1} x_{11}, & \text { if } k_{1} \text { is odd }
\end{array}\right\}
$$

Remark in case $k_{1}=2 m$ is even, Then $\sum_{j=1}^{2 m} x_{1 j}=2\left(m x_{11}\right)=0 \bmod 2$. That, Regardless of $x_{1 j}$ values, as we would always obtain an even number.

Now consider the whole system of equations by summing all equations as we defined in $b$. In case $k_{1}$ is even, Then we know $x_{1 j}$ evaluates to zero, and hence their removal from the system doesn't affect. In case $k_{1}$ is odd, Then $k_{1} x_{11}$ is exactly equivalent to $x_{11}+x_{12}+\cdots+x_{1 n}$. Think of redistributing $x_{1 j}$ to reconstruct the original equations before the transformation, which clarifies why the new system is equivalent to the original one.

## d

If at any stage $0=1$ is concluded, Then no matter what $x$ is inputted, The system won't be satisfied. Since the transformed system is equivalent to the original one, It's trivial why the original system is unsatisfiable.
Observe in modulus 2, the only possible evaluation outcomes are 0 or 1 . So if $L H S \neq R H S$, then necessarily we get $0=1$. If we don't get $0=1$, then all equations' evaluations are satisfied.
Observe also if $k_{i i} x_{i i}=c \bmod 2$ then by our definitions we know $k_{i i}$ is odd. It follows there's exactly one unique solution for $x_{i} i$.

As the instructor hinted, back-substitution can be applied recursively to compute $x_{n n}, x_{n-1 n-1}, . ., x_{11}$ where once $x_{i i}$ is computed, For all the above equations, Their number of variables are reduced by one. Only one literal $x_{i-1 i-1}$ is left for the next equation.

As a valid assignment $x$ for the transformed system is constructed, The original system is satisfied by $x$ also.

