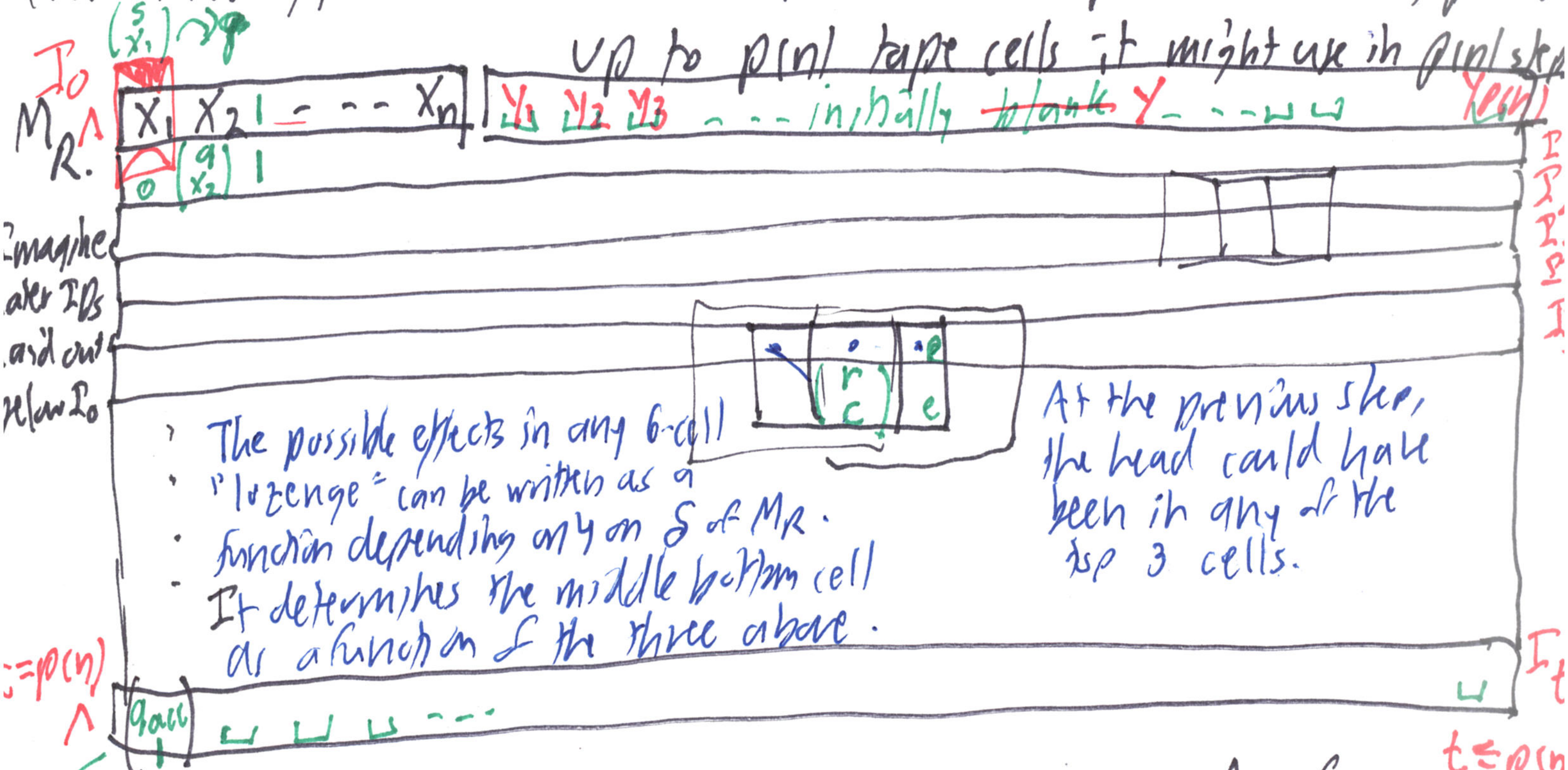
CSE596 Lecture Fri 10/26 Fall 2018

Theorem: [Steve Cook 1970–71, Leonid Levin 1970–1973]
SAT is <u>NP-complete</u>, i.e. SAT $\in$ NP (already seen) and for all $A \in NP$, $A \leq_m^p$ SAT. [We will prove a reduction to a subcase of SAT]

Proof: By $A \in NP$, there is a polynomial $p(n)$ and a single-tape TM $M_R(x,y)$ that computes a witness predicate $R(x,y)$ with $|y| \leq p(|x|)$.
From Monday, we saw that $R(x,y)$ can be the computation checking predicate.



preserve if M_R halts before p(n) steps.

output write wo

$x \in A \equiv$ the write is 1.

Each lozenge has the same function Δ of six characters (3 inputs, 1 output) over $\Gamma \cup Q \times \Gamma$.

We can re-code those over binary and write the finite Δ function as a Boolean function, using NAND gates only. $\therefore$ M_R can be simulated by $p(n) \times p(n)$ sized circuits. [Can get $O(p(n) \log p(n))$.]

We have abstracted this to a circuit C_n s.t. $x \in A \iff \exists y\ M_R$ acc (x, y)
$\iff \exists y\ C_n(x, y) = 1$

$x_1 - x_i - \ x_n \quad y_1 - - - - y_j - - - y_{p(n)}$

• • • ... • •   • • ... • ... •

We can "stamp out" C_n in $O(p(n)^2)$ time.

(u and/or v can be wires from inputs x_i or guesses y_j)

g

Gate g functions correctly on bits u, v giving output w if and only if ϕ_g is made true, where

$$\phi_g = (u \vee w) \wedge (v \vee w) \wedge (\bar{u} \vee \bar{v} \vee \bar{w}).$$

$|w_0$

Final ϕ_x is:

$$\left(\bigwedge_{\text{NAND gates } g \text{ in } C} \phi_g \right) \wedge (w_0) \wedge$$

Only part that depends on x not just $n = |x|$: Singleton clauses (x_i) or $(\bar{x}_i)$ to set those vars to the actual bits of x. E.g. $x = 011$: $(\bar{x}_1) \wedge (x_2) \wedge (x_3)$

Thus ϕ_x is computed by an $\tilde{O}(p(n)^2)$ time function of x, and for all $x \in \Sigma^*$:

$x \in A \iff (\exists y : |y| \leq p(n))\ R(x, y)$
$\iff (\exists y)\ C_n(x, y) = 1 \iff \exists (y, \vec{w})\ \phi_x(x, y, w) = 1$ (wires u, v, w.)
$\iff \phi_x \in SAT.$ ☒

Observe: Every clause has at most 3 literals, all of the same sign, and ϕ_x is a conjunction of these clauses. <u>3SAT</u>.