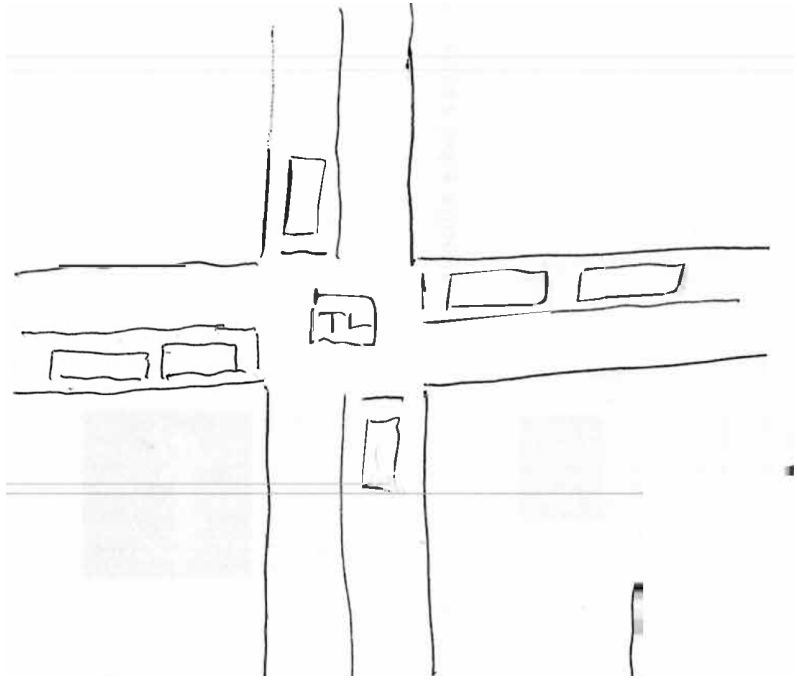
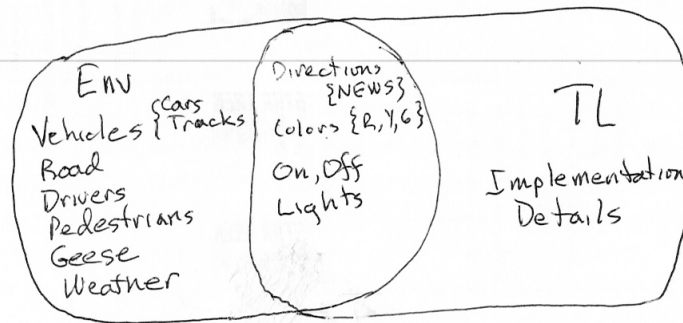
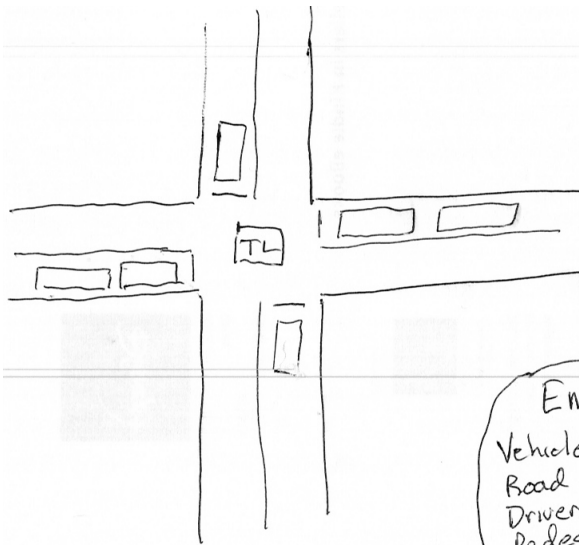


Traffic Light Example

Daniel Berry





Where is time?

$R = R_1 \& R_2 \& \dots \& R_r$

$S = S_1 \& S_2 \& \dots \& S_s$

$D = D_1 \& D_2 \& \dots \& D_d$

Let's focus on one particular conjunct (feature) of R:

$R_i =$ Vehicles going in perpendicular directions do not collide

R_i = Vehicles going in perpendicular directions do not collide

We determine that one particular conjunct (feature) of S is relevant:

S_j = No two perpendicular directions show a green light at the same time.

(Note that if one had temporal logic expression of this as "Henceforth, ...", he/she could conceivably PROVE that the code satisfies S_j)

But does $S \models R$?

But does $S \models R$?

In terms of R_i , the key part of the validation $S \models R$ is

$S_j \models R_i$

Is S_j enough to guarantee R_i ?

Hint: the fact that I am asking this question in a lecture is a strong indication that it is NOT :-)

No

So what more is needed? in particular from D?

Dk = Whenever a vehicle driver sees a red light, he/she orders the vehicle to stop
(i.e. he/she hits the brakes)

Is this enough?

No

So what more is needed? in particular from D?

DI = Whenever a vehicle is ordered to stop, it stops within 2 seconds

So we can validate

$D_k \ \& \ D_l, S_j \mid - R_i$

Can we strengthen (i.e., add a feature) S to make some of the D conjuncts unnecessary?

Yes!

What can we do to get rid of

Dk = Whenever a vehicle driver sees a red light, he/she orders the vehicle to stop

?

If we have self-driving vehicles that can be controlled by a radio signal from traffic lights, then if we have

S_t = when a direction changes to yellow, send out a radio signal that tells all vehicles coming toward the direction to stop within 2 seconds

then we do not need

D_k = Whenever a vehicle driver sees a red light, he/she orders the vehicle to stop

if we have

St = when a direction changes to yellow, send out a radio signal that tells all vehicles coming toward the direction to stop within 2 seconds

can we then get rid of

DI = Whenever a vehicle is ordered to stop, it stops within 2 seconds

?

Not easily...

vehicles can break down!!

Maybe could have a yellow light trigger that something in the road physically blocks each vehicle coming toward it, e.g., a steel wall that pops out of the road or hooks that come out of the road and grab the vehicles.

But even these could fail.

Many times we choose to live with Ds that are NOT true in the real world, because we have no choice or the probability of its not holding is low enough or the consequences if its not holding are small enough.

