Anomaly Detection

How To Find Needles In Haystacks

Business Problems

- Is this credit card purchase a fraudulent transaction?
- Should this tax return be audited?
- Is this medical instrument acceptable for hospital use?
- Is this computer file read/write process an indicator of malware?
- Which machine in my production line requires servicing?

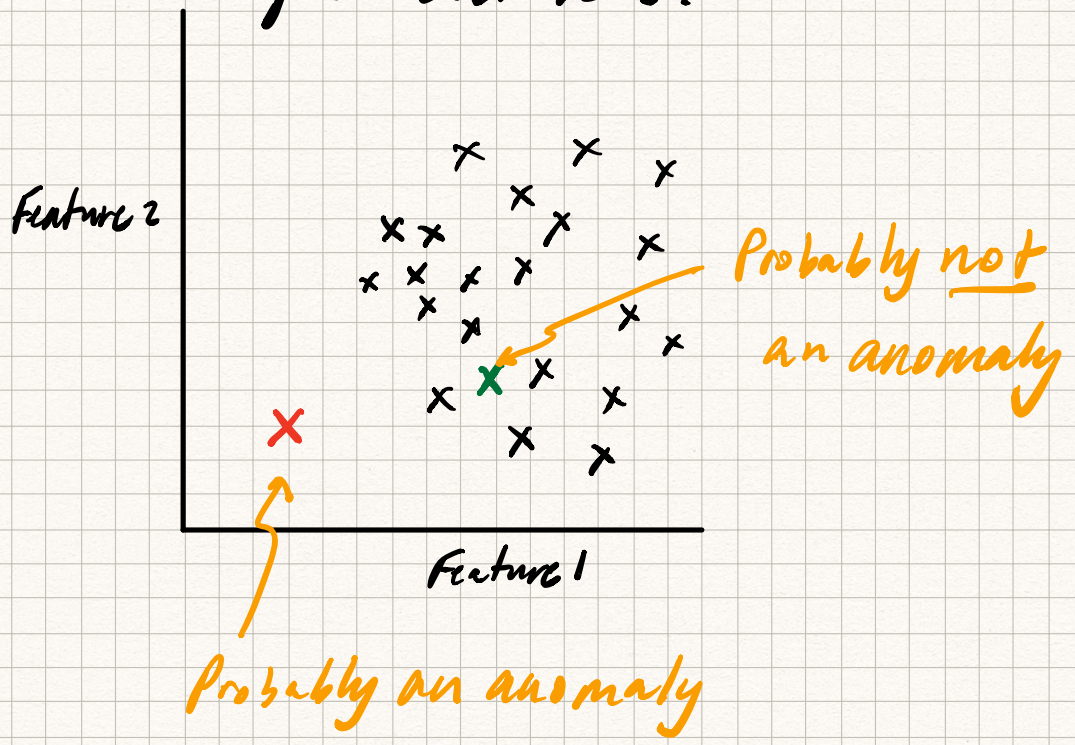
Why Anomaly Detection is Hard

- You know it when you see it... but you don't know what you're looking for.
- What is anomalous can change over time. (Viruses)
- Anomalies can be context dependent (A $2M house next a freeway is an anomaly... unless you're in San Francisco!)

> In general, anomalies are unknown unknowns.

So how do you do it?

→ Define what's normal — then look for outliers.



"Probably", because it all depends on how well you're able to capture normal and how good your definition of onthier is.

Dataset Point of View

	x_1	x_2
Row 1	2.5	1.5
Row 2	6.4	3.8
⋮		
Row m	9.8	2.4

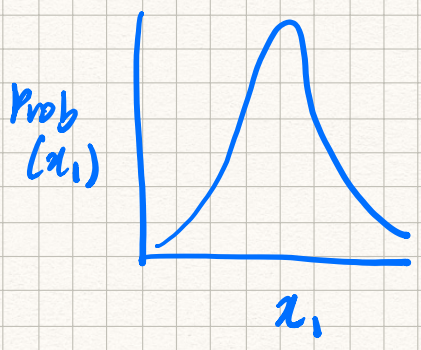
These are all normal values.

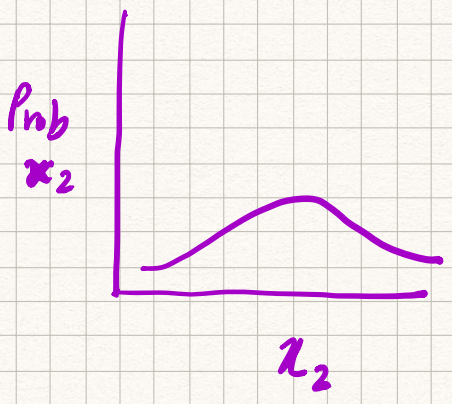
ASSUME

x_1 is independent of x_2.

Prob(x_1)

Prob(x_2)





These curves are based on the actual values that x_1 and x_2 take.

Because x_1 is independent of x_2

(think of x_1 and x_2 as 2 different many-sided dies),

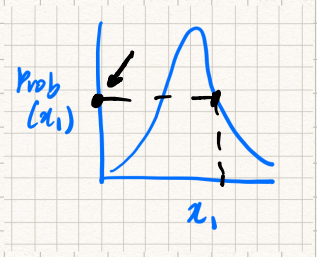
$$\text{Prob}(x_1 = 9.8 \text{ and } x_2 = 2.4) =$$

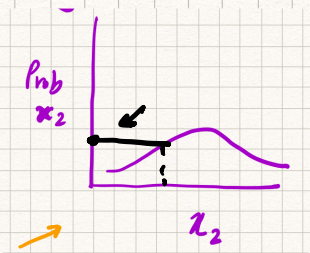
Normal Event

$$\text{prob}(x_1 = 9.8) * \text{prob}(x_2 = 2.4)$$

↓ Can read this off of $\text{prob}(x_1)$

↓ Can read this off of $\text{prob}(x_2)$

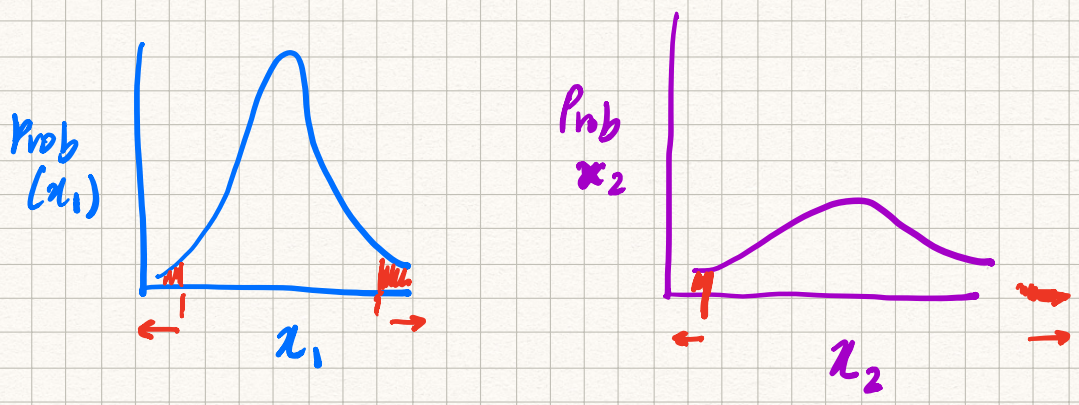




Anomaly Detection Scheme

Construct $prob(x_1)$ and $prob(x_2)$ in such a way that for normal events n_1, n_2 $prob(n_1) * prob(n_2)$ is large while for anomalous events, a_1, a_2,

$prob(a_1) * prob(a_2)$ is small.



For the scheme to work, anomalous values must be very improbable - they must fall in the regions marked in red.

→ Picking the right features is critical for anomaly detection.

Is anomaly detection a machine learning problem?

- What's being optimized?
- What are the parameters being learned?
- What are the hyperparameters?

None of these things are really being done. At least not in the sense that we're used to seeing in the models that we've constructed so far.