Artificial Intelligence Assignment 3

Parth Sandeep Rastogi,2022352

Section A) Theory
Q 1)

Q1@	Direct	Regection	Gibbs
1)	randomly select any point from dataset	we first propose a distribution and Sample using it and reject them based on target distribution	Markov chain method that iteratively select based on CPT
Strenth	unbiased estimate of the population parameter so it is good at estimating general probabilities like travel mode, travel purpose	we can estimate probability of specific parts or small subset of data that we want by selecting general than removing unnecessary points something like buyers who travel in train and travel for leasure	we can estimate Joint probability and complex distribution like given low stress and for liesure What travel mode would you prefer
Weakness	cant compute on highly complicated relations	to many computes done that gets rejected	being iterative and complicated it will be a

b) P (Train ∩ liesure)

= P(liesure | train) * P (train)

= 0.4 × 0.3

= 0.12

now

Count = P * Count population/sample

= 0.12 × 100

= 12

c) P(Air ∩ business)

= P(Air | business) * P(Air)

= 0.2 × 0.8

= 0.16

classmate
Date
Page

d) If the Sample size increased the sample proportion converges to the true population so larger the sample size smaller bias from true distribution (law of large numbers)

Precision is also increased because as sample size increased the std error decreases

With larger sample size ~~~~ the estimation in the numbers is much more close to actual value like what proportion prefer air what prefer train and etc.

Q2)

Q2.

a) ~~1)~~ Variables

J → access Journal
B → read book
C → go to book club

1) $P(J \cup B) = 0.91$
2) $P(J|B) = 0.4$ and $P(\neg J|B) = 0.6$
3) $P(C|B,J) = 0.32$ and $P(C|B,\neg J) = 0.32$
4) $P(J \land \neg B) = 0.227$
5) $P(\neg J \land \neg B) = 0.09$
6) $P(J|\neg B) = 0.716$
7) $P(C \land J) = 0.088$
8) $P(C \lor J) = 0.631$
9) $P(J|C) = 0.4$
10) $P(J) = 0.5$
11) $P(C|\neg B, J) = 0.0044$
$P(C|\neg B, \neg J) = 0.0044$

b) for P(b)

$$P(\neg B) = \frac{P(J \land \neg B)}{P(J|\neg B)}$$

$$= \frac{0.222}{0.716} = 0.317$$

$$P(B) = 1 - P(\neg B) = 0.683$$

for P(C)

$$P(C) = \frac{P(J \wedge C)}{P(J | C)}$$

$$= \frac{0.088}{0.4} = 0.22$$

now taking pairwise

$$P(J \wedge B) = P(J | B)\, P(B)$$
$$= 0.4 \times 0.683$$
$$= 0.2732$$

$$P(\neg J \wedge B) = P(\neg J | B)\, P(B)$$
$$= 0.683 \times 0.6$$
$$= 0.4098$$

using these 2 and eq 4 and 5 we can find

$$P(B \wedge C \wedge J) = P(C | B, J)\, P(B \wedge J)$$
$$= 0.32 \times 0.2732$$
$$= 0.0874$$

$$P(C \wedge \neg B \wedge J) = P(C | \neg B, J)\, P(\neg B \wedge J)$$
$$= 0.0044 \times 0.227$$
$$= 0.000998$$

$$P(C \wedge B \wedge \neg J) = P(C | B, \neg J)\, P(B \wedge \neg J)$$
$$= 0.32 \times 0.4098$$
$$= 0.131$$

$P(C \wedge \neg B \wedge \neg J) = P(C | \neg B, \neg J)\ P(\neg B \wedge \neg J)$
$= 0.0044 \times 0.09$
$= 0.000396$

$P(\neg C \wedge B \wedge J) = P(B \wedge J) - P(C \wedge B \wedge J)$
$= 0.2732 - 0.0874$
$= 0.1858$

$P(\neg C \wedge \neg B \wedge J) = P(\neg B \wedge J) - P(C \wedge \neg B \wedge J)$
$= 0.227 - 0.000998$
$= 0.226$

$P(\neg C \wedge B \wedge \neg J) = P(B \wedge \neg J) - P(C \wedge B \wedge \neg J)$
$= 0.4098 - 0.131$
$= 0.2788$

$P(\neg C \wedge \neg B \wedge \neg J) = P(\neg B \wedge \neg J) - P(C \wedge \neg B \wedge \neg J)$
$= 0.09 - 0.000396$
$= 0.0896$

for validity

$$\sum_{j \in J} \sum_{b \in B} \sum_{c \in C} P(j, b, c) = 1$$

$= 0.0874 + 0.000998 + 0.131 + 0.000396 + 0.1858$
$+ 0.226 + 0.2788 + 0.0896$
$= 0.999994 \simeq 1$

hence valid

c)

Second validity suffice that all probability should be more than 0

c)

C	B	J	P
T	T	T	0.0874
T	T	F	0.131
T	F	T	0.000498
T	F	F	0.000396
F	T	T	0.1858
F	T	F	0.2788
F	F	T	0.226
F	F	F	0.0488

full Joint Probability table

d for conditional indipendence

$P(B \mid C, J) = P(B)$

$P(C \mid B, J) = P(C)$

$P(J \mid B, C) = P(J)$

$$P(B \mid C, J) = \frac{P(B \wedge C \wedge J)}{P(C \wedge J)}$$

$$= \frac{0.0874}{0.088}$$

$$= 0.993 \neq P(B)$$

$$P(C \mid B, J) = 0.32 \neq P(C)$$

$$P(J \mid B, C) = P(J \wedge B \wedge C)\, P(B \wedge C)$$

$$= P(J \wedge B \wedge C)\left(P(B \wedge C \wedge J) + P(B \wedge C \wedge \neg J)\right)$$

$$= 0.0874\,(0.0874 + 0.131)$$

$$= 0.019 \neq P(J)$$

[illegible] of other

$$P(C \mid J) = \frac{P(C \land J)}{P(J)} = \frac{0.088}{0.5}$$

$$= 0.176 \neq P(C)$$

$$P(J \mid B) = \frac{P(J \land B)}{P(B)} = \frac{0.2732}{0.683}$$

$$= 0.4 \neq P(J)$$

$$P(B \mid C) = \frac{P(B \land C)}{P(C)} = \frac{0.2184}{0.22}$$

$$= 0.99$$

$$\neq P(B)$$

hence no conditional independency

Q3)

Q3

a) Problem Formulation

A → adversarial perturbation attack
B → backdoor attack

M → Misclassification Alarm

Given A and B are independent

$P(A \cap B) = P(A)\,P(B)$

B increases

Given this initial condition
likelihood of adversarial perturbation
causing the misclassification
is $= P(A|M)$

$$= \frac{P(M|A)\,P(A)}{P(M)}$$

Bayesian Network

$$\begin{tikzcd} A \arrow[dr] & \\ & M \\ B \arrow[ur] & \end{tikzcd}$$

b) Prior Probabilities → $P(A)$, $P(B)$, $P(M)$

Likelihood probabilities → $P(M|A)$, $P(M|B)$

Posterior Probabilities → $P(A|M)$, $P(B|M$

Priors → Initial probability of an event happening

Likelihood → Probability that Misclassificat alarm has rang ~~due to~~ given A or B (Seperat occured classmate

Date

Page

Posterior probabilities → after observing a misclassification alarm what is updated probability that Adversarial perturbation ~~or~~/Backdoor attack has caused misclassi-fication

$$P(A|M) = \frac{P(M|A)P(A)}{P(M)}$$

$$P(B|M) = \frac{P(M|B)P(B)}{P(M)}$$

c) Probability of Misclassification

$$P(M) = P(M|A)P(A) + P(M|B)P(B)$$

from this we can see increase in $P(B)$ will cause increase in $P(M)$

So when backdoor triggers increased Misclassification alarm probability increases

now using this

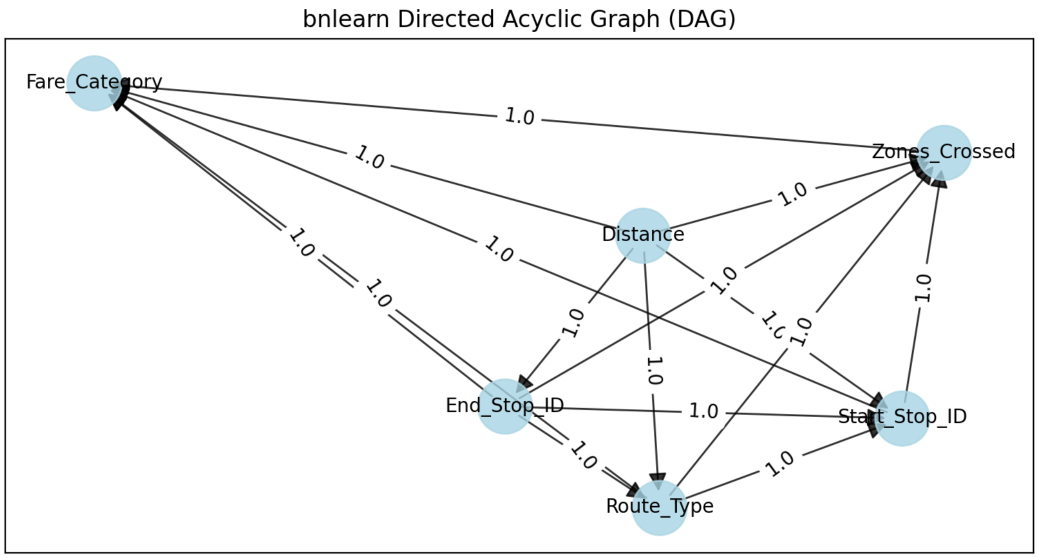
$$P(A|M) = \frac{P(M|A)P(A)}{P(M)}$$

here as $P(M)\uparrow$ rest of ~~fact~~ probability remain same then $P(A|M)$ decreases showing that this shows that likelihood that when misclassification happen that it is less likely due to Adversarial Perturbation

Section B) Bayesian network

Task 1) The structure includes dependencies between all possible feature pairs.

Basic plot

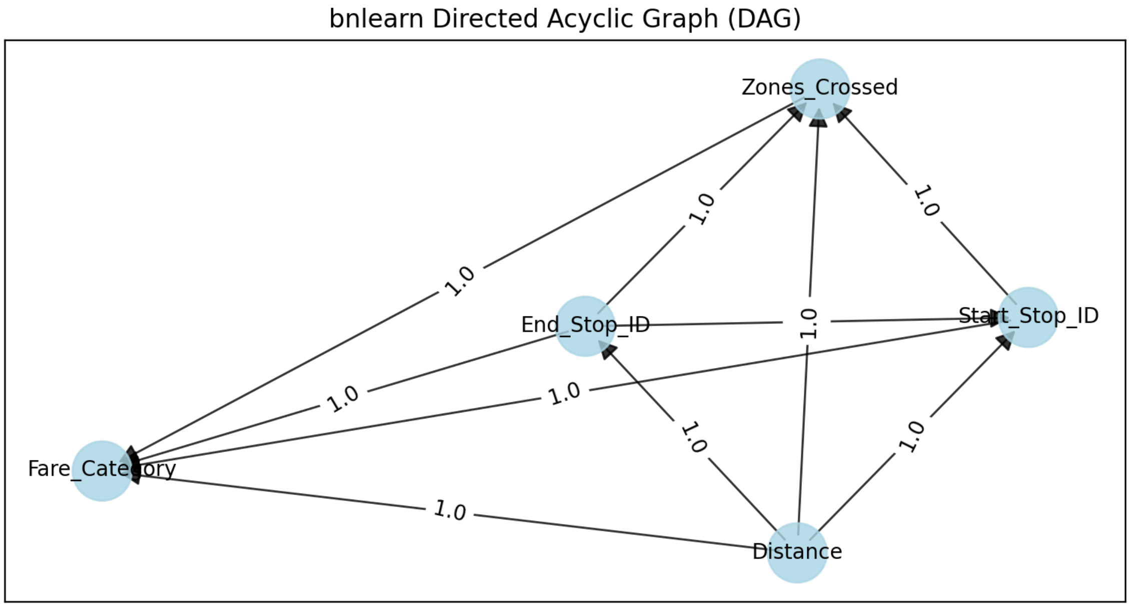


Task 2)
Pruned_network : -

Pruning was applied to the model using the Chi-square independence test with a p-value threshold of 0.05. This statistical method evaluates the independence of variables, and edges or nodes with weak associations (p > 0.05) were removed. As a result, the pruning process eliminated 5 edges and the node route_type, simplifying the model structure.

This pruning improves the model's efficiency by reducing the complexity of computations during inference, as fewer edges and nodes mean fewer operations. For inference, the original model required 52 seconds, while the pruned model achieved the same task in 50 seconds, demonstrating a measurable improvement in runtime efficiency without compromising accuracy.

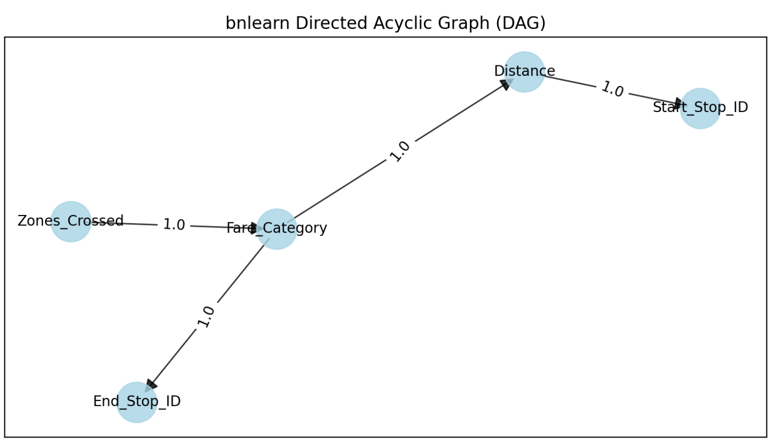
```
[bnlearn] >5 edges are removed with P-value > 0.05 based on chi_square
```



Task 3)

The Bayesian Network was optimized using a hill-climbing algorithm, which iteratively searches for the best structure by removing, or reversing edges to maximize a given evaluation function. This optimization reduced the number of edges to just 4 from 15, significantly simplifying the network structure.

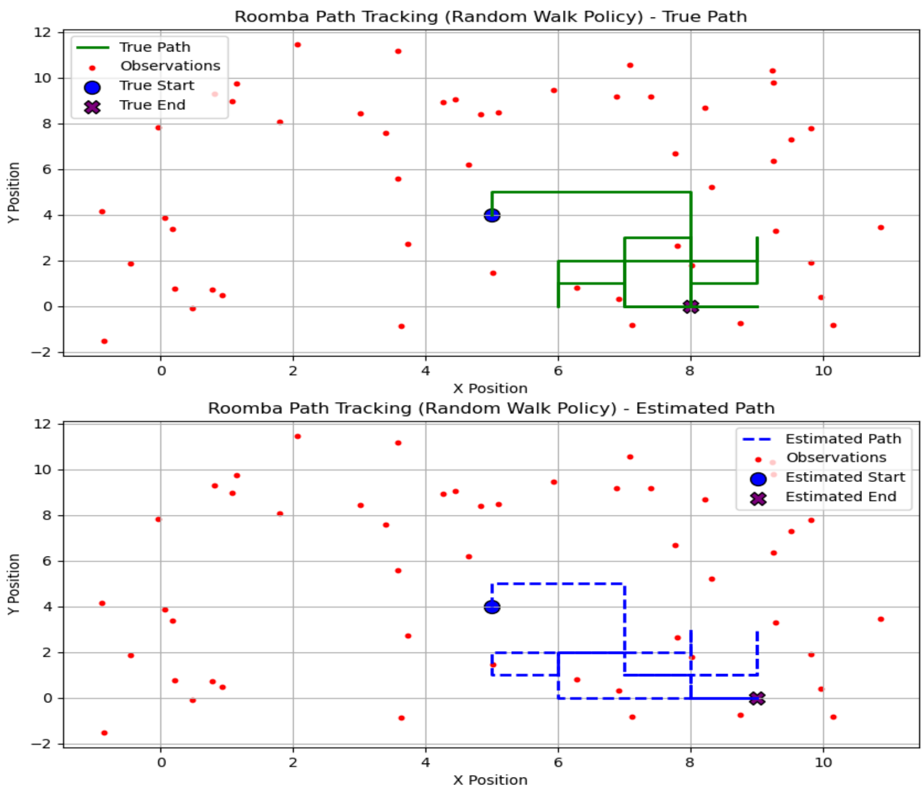
The reduced complexity had a profound impact on performance. The evaluation time dropped dramatically from 52 seconds to merely 1.5 seconds, showing the effectiveness of the hill-climbing approach in achieving a simpler and more efficient model without sacrificing its predictive capabilities.

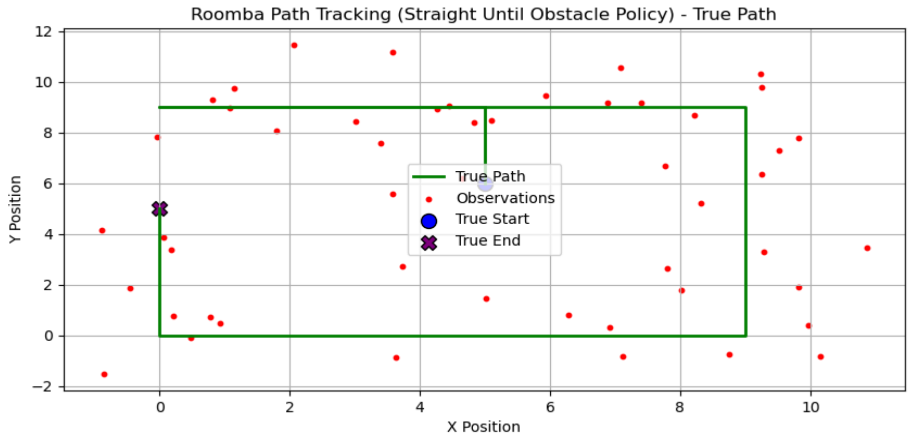


Section C) HMM model

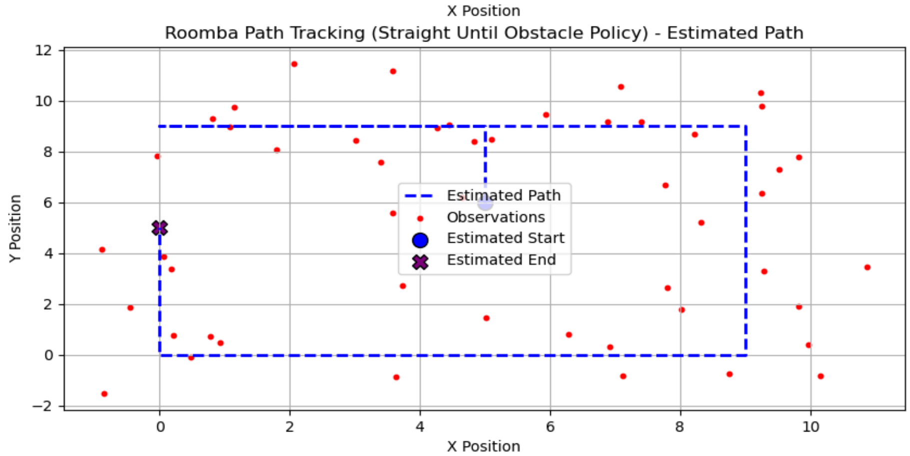
Seed 42)
Processing policy: random_walk
Tracking accuracy for random walk policy: 62.00%

Processing policy: straight_until_obstacle
Tracking accuracy for straight until obstacle policy: 100.00%





Roomba Path Tracking (Straight Until Obstacle Policy) - True Path
True Path
Observations
True Start
True End
Y Position
X Position

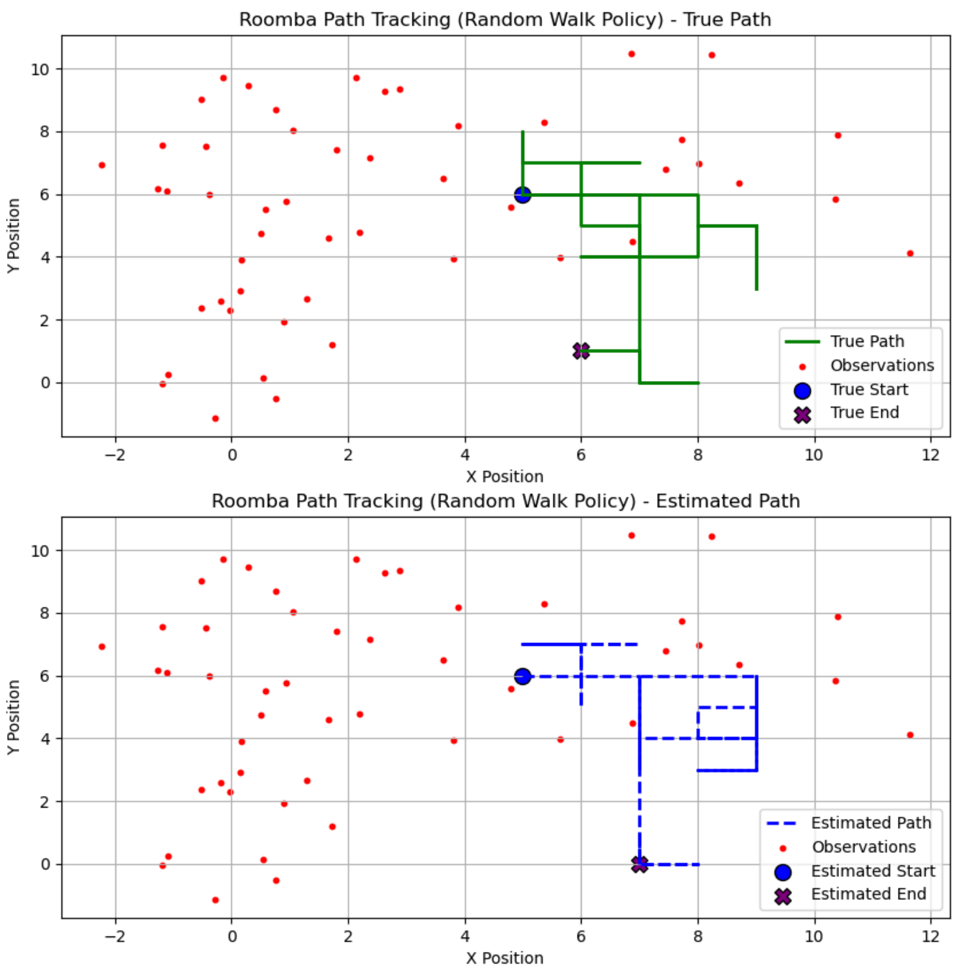


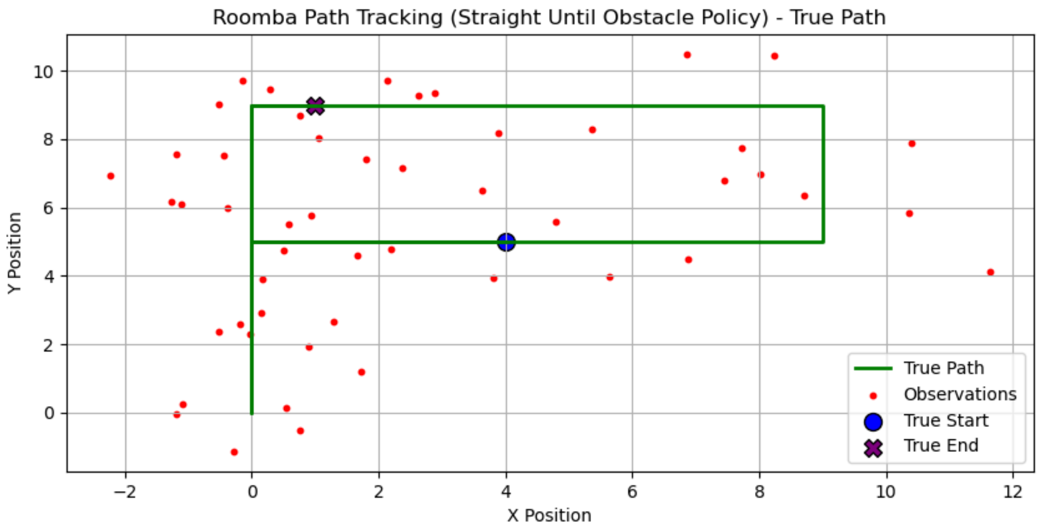
Roomba Path Tracking (Straight Until Obstacle Policy) - Estimated Path
Estimated Path
Observations
Estimated Start
Estimated End
Y Position
X Position

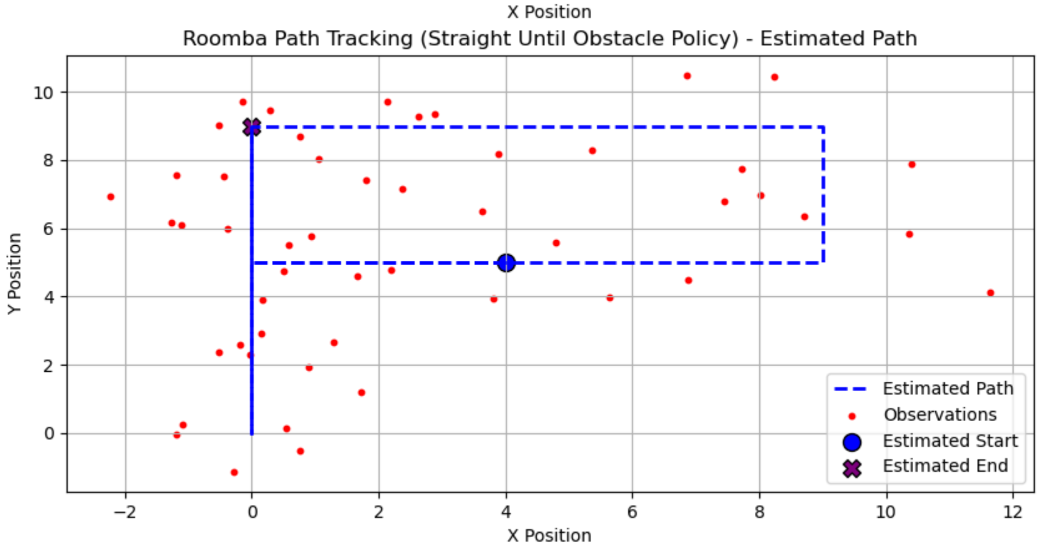
Seed 60)

Processing policy: random_walk
Tracking accuracy for random walk policy: 70.00%

Processing policy: straight_until_obstacle
Tracking accuracy for straight until obstacle policy: 90.00%

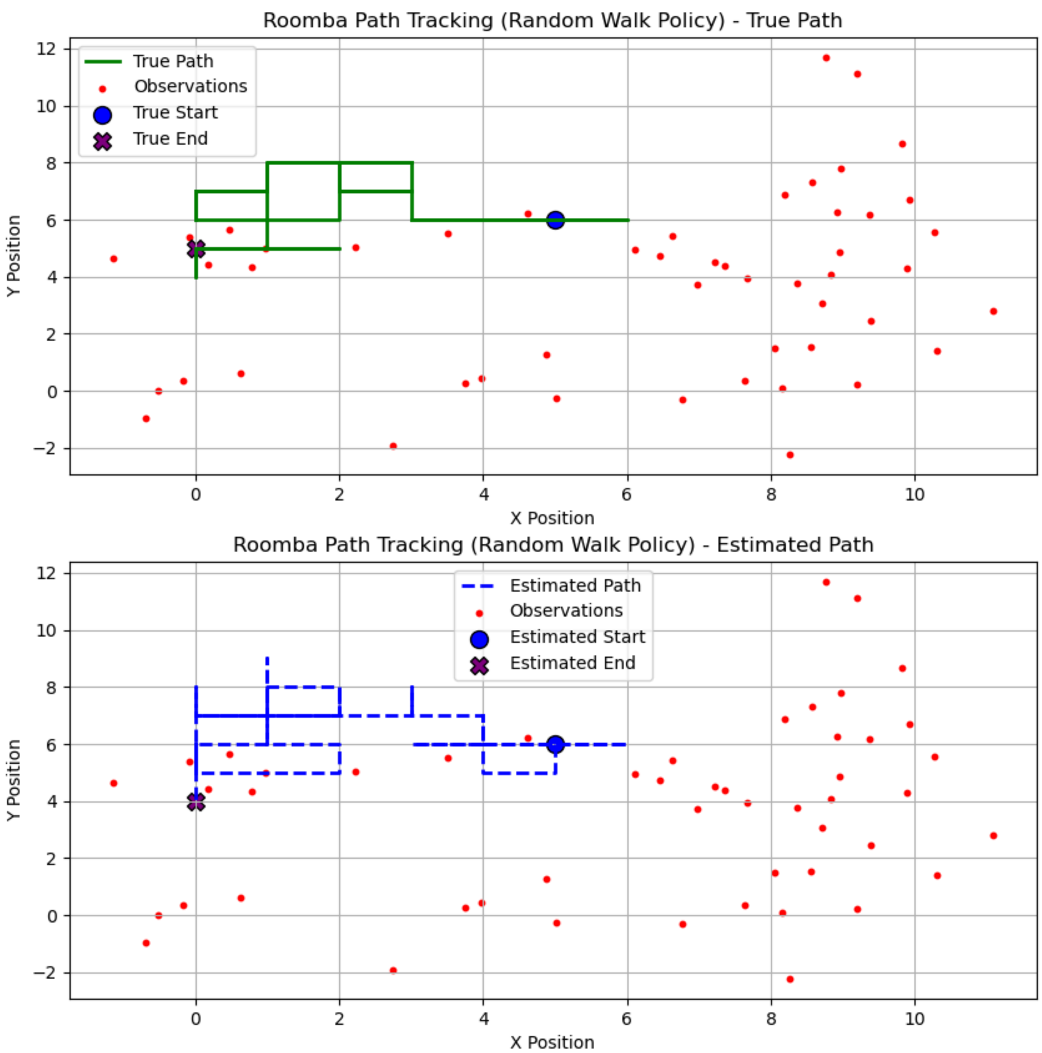


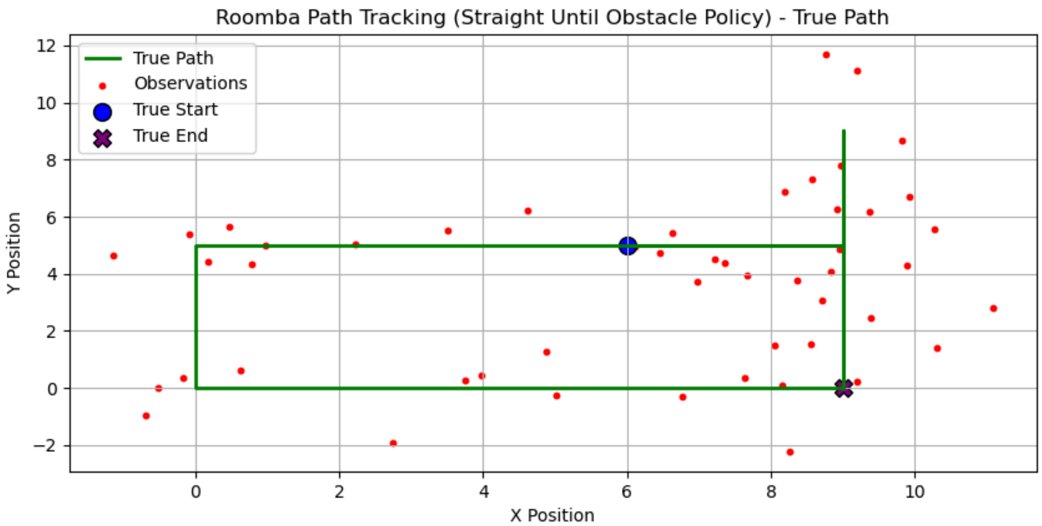

Roomba Path Tracking (Straight Until Obstacle Policy) - True Path
True Path
Observations
True Start
True End
X Position
Y Position

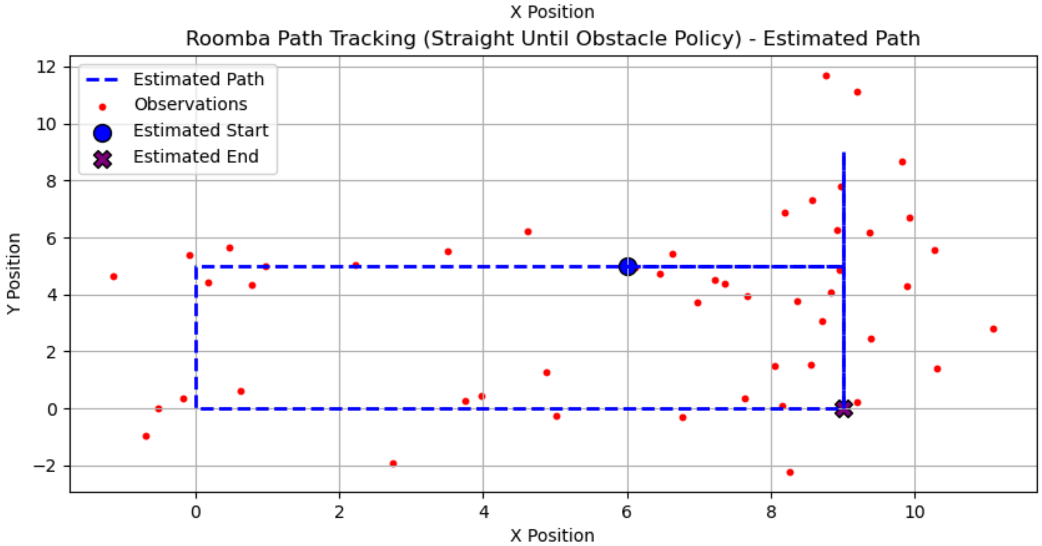

Roomba Path Tracking (Straight Until Obstacle Policy) - Estimated Path
Estimated Path
Observations
Estimated Start
Estimated End
X Position
Y Position

Seed 111) Processing policy: random_walk
Tracking accuracy for random walk policy: 42.00%

Processing policy: straight_until_obstacle
Tracking accuracy for straight until obstacle policy: 100.00%
‘




Roomba Path Tracking (Straight Until Obstacle Policy) - True Path
True Path
Observations
True Start
True End
X Position
Y Position


Roomba Path Tracking (Straight Until Obstacle Policy) - Estimated Path
Estimated Path
Observations
Estimated Start
Estimated End
X Position
Y Position

Straight until obstacle strategy consistently demonstrates better tracing accuracy compared to random walk across all seeds due to its systematic and efficient approach. By following a direct path until encountering an obstacle, this method minimizes unnecessary movements and reduces deviations, leading to improved accuracy. In contrast, the random walk approach introduces significant variability and inefficiency through its stochastic nature, resulting in less reliable tracing performance. This highlights the advantage of a structured strategy in achieving consistent and accurate outcomes.