Appendix

A Detailed Algorithm of Alg. 1

Algorithm 4 Detailed Algorithm of Alg. 1

1: **function** ***MDP***(S_0)
▷ ObserveFromEnv: run agent-env interaction for M steps
2: r, $\{S_t\}_{t\in[M-1]} \leftarrow$ ObserveFromEnv(S_0)
3: **return** r, $\{S_t\}_{t\in[M-1]}$
4: **function** ***Fuzzing***$()$
▷ τ: state sequence freshness threshold
5: $\mathcal{C} \leftarrow$ Sampling(N) ▷*Sample seed corpus with N initial states*
6: $Params^s, Params^c \leftarrow$ Init$()$ ▷*Initialize key parameters*
7: **for** $S_0^i \in \mathcal{C}$ **do**
8: $E_i \leftarrow$ ***Sensitivity***(S_0^i)
9: r_i, $\{S_t^i\}_{t\in[M-1]} \leftarrow$ ***MDP***(S_0^i)
10: $p_i \leftarrow$ ***Seq_fresh***$(\{S_t^i\}_{t\in[M-1]}, Params^s, Params^c, \tau)$
11: **while** passed time $<$ 12 hours **do**
12: Select S_0^k from $\mathcal{C}$ with probability $E_k/\sum_{i=1}^{N} E_i$
13: $S_0^{\Delta,k} \leftarrow$ Mutate_Validate(S_0^k)
14: r_k^Δ, $\{S_i^{\Delta,k}\}_{i\in[M-1]} \leftarrow$ ***MDP***$(S_0^{\Delta,k})$
15: $p_k^\Delta \leftarrow$ ***Seq_fresh***$(\{S_i^{\Delta,k}\}_{i\in[M-1]}, Params^s, Params^c, \tau)$
16: **if** $Crash(\{S_i^{\Delta,k}\}_{i\in[M-1]})$ **then** ▷*Testing oracles. See Sec. 6 for details.*
17: Add $S_0^{\Delta,k}$ to $\mathcal{R}$
18: **else if** $r_k^\Delta < r_k$ **or** $p_k^\Delta < \tau$ **then** ▷*Feedback. See Sec. 5.3 for details.*
19: Add $S_0^{\Delta,k}$ to $\mathcal{C}$
20: $E_k^\Delta \leftarrow$ ***Sensitivity***$(S_0^{\Delta,k})$
21: Maintain $r_k^\Delta, E_k^\Delta, p_k^\Delta$ for $S_0^{\Delta,k}$
22: **return** $\mathcal{R}$
23: **function** ***Init***$()$
▷ $\mathcal{K}$: the component number of the GMM
▷ Sampling$(\mathcal{K}+1)$: sample $\mathcal{K}+1$ states from state space $\mathcal{P}$
24: $\{S_0^k\}_{k\in[\mathcal{K}]} \leftarrow$ Sampling$(\mathcal{K}+1)$
25: **for** $k \in [\mathcal{K}-1]$ **do**
26: $\mathcal{G}_{s,0}^k \leftarrow 1/\mathcal{K}$, $\mathcal{G}_{c,0}^k \leftarrow 1/\mathcal{K}$
27: $\mathcal{G}_{s,1}^k \leftarrow S_0^k$, $\mathcal{G}_{c,1}^k \leftarrow S_0^k||S_0^{k+1}$
28: $\mathcal{G}_{s,2}^k \leftarrow \mathcal{G}_{s,1}^k \times \mathcal{G}_{s,1}^{k\,T}$, $\mathcal{G}_{c,2}^k \leftarrow \mathcal{G}_{c,1}^k \times \mathcal{G}_{c,1}^{k\,T}$
29: $Params^s \leftarrow \{\mathcal{G}_{s,0}^k, \mathcal{G}_{s,1}^k, \mathcal{G}_{s,2}^k\}_{k\in[\mathcal{K}-1]}$
30: $Params^c \leftarrow \{\mathcal{G}_{c,0}^k, \mathcal{G}_{c,1}^k, \mathcal{G}_{c,2}^k\}_{k\in[\mathcal{K}-1]}$
31: **return** $Params^s, Params^c$
32: **function** ***ObserveFromEnv***(S_0)
▷ π, T, R: the target model, transaction function, and reward function
33: $r \leftarrow 0$, $t \leftarrow 0$ ▷*r is the accumulated reward, t is the time step*
34: **while** $t < M$ **do** ▷*M is the maximum length of the state sequence*
35: $a_t \leftarrow \pi(S_t)$
36: $S_{t+1} \leftarrow T(S_t, a_t)$
37: $r \leftarrow r + R(S_t, a_t)$
38: $t \leftarrow t + 1$
39: **return** r, $\{S_t\}_{t\in[M-1]}$

In this section, we present the detailed algorithms of functions ***Init*** and ***ObserveFromEnv*** in Alg. 1.

Init is called before fuzzing (line 6 in Alg. 4), and it randomly initializes the parameters $Params^s$ and $Params^c$ of ***DynEM***. Specifically, $\mathcal{K}+1$ states are randomly sampled from state space $\mathcal{P}$ (line 24 of Alg. 4), and then the initial C-S statistics parameters $Params^s$ and $Params^c$ are calculated based on these randomly selected states (lines 25–28 of Alg. 4).

ObserveFromEnv describes the interactions between the MDP environment and the model-controled agent. The cumulative rewards r and the state sequence $\{S_t\}_{t\in[M-1]}$ are returned. We note that the state sequence length M can be arbitrarily long.

B Illustration of Alg. 2

Fig. 11 illustrates the intuition behind Alg. 2, where states with higher sensitivity are less stable and more sensitive to permutations (i.e., ΔS_0 and ΔS_1 in Fig. 11. We pay greater attention to the state with higher sensitivity, which is S_0^k in Fig. 11.

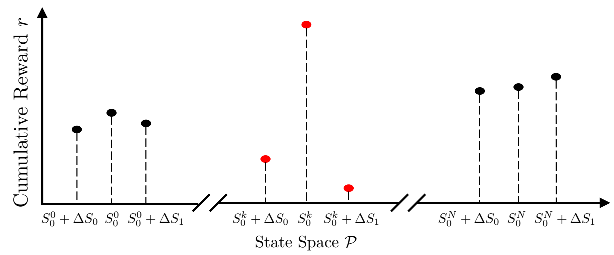

Figure 11: Illustration of the local sensitivity.

C Detailed Algorithm of Alg. 3

In this section, we present the detailed algorithms of functions ***GMM*** and ***DynEM*** in Alg. 3.

GMM is used to calculate the probability density function returned by the Gaussian Mixture Models parameterized by the GMM parameters derived from the C-S statistics parameters of ***DynEM***, *Params* (line 10 of Alg. 5). As we mentioned in Sec. 5.2, the C-S statistics parameters *Params* contain all the information we need to estimate the GMM parameters. The GMM parameters $\{\phi_k, \mu_k, \Sigma_k\}_{k\in[\mathcal{K}-1]}$ are calculated by function ***Get_GMM_Params*** with input *Params* (lines 14–16 in Alg. 5). Then the pdf of input state X can be naturally calculated with these GMM parameters (line 11 of Alg. 5).

Get_CS_Stat computes the C-S statistics with the current input X and the current C-S statistics parameters of ***DynEM*** *Params*. The C-S statistics contain all the information of the GMMs' parameters, which is defined as following:

Definition 3 (C-S Statistics of Gaussian distribution)**.** *Statistic H is complete and sufficient for some pdf parameterized by θ, if H isn't missing any information about θ and doesn't provide any irrelevant information. Such C-S statistic of Gaussian distribution is $(\bar{X}, \hat{\Sigma})$, where $\bar{X} = \frac{1}{n}\sum_{i=0}^{n-1} X_i$, $\hat{\Sigma} = \frac{1}{n}\sum_{i=0}^{n-1}(X_i-\bar{X})(X_i-\bar{X})^T = \overline{XX^T} - \bar{X}\bar{X}^T$, and n is the size of the dataset used to estimate the distribution.*

The density estimation for each of the $\mathcal{K}$ GMM components are calculated (line 19–20 of Alg. 5). Then the C-S statistics are calculated with the input state X and the GMMs results $\{w_k\}_{k\in[\mathcal{K}-1]}$ (line 21 of Alg. 5). Recall that in Definition 3, we only need to calculate $\bar{X}$ and $\overline{XX^T}$ to get the C-S statistics and then compute the Gaussian parameters. Thus, for GMMs, we only need to maintain and update $\bar{X}$, $\overline{XX^T}$, and the weights $\{w_k\}_{k\in[\mathcal{K}-1]}$ to compute the GMMs parameters (line 21 of Alg. 5).

The C-S statistics are maintained by the parameters of ***DynEM***. More specifically, $\mathcal{G}_{s,0}^k$ and $\mathcal{G}_{c,0}^k$ maintain and update the weight parameter ϕ_k^s and ϕ_k^c of the k^{th} GMM component, respectively. $\mathcal{G}_{s,1}^k$ and $\mathcal{G}_{c,1}^k$ maintain and update the first weighted C-S statistics $\overline{S_t}$ and $\overline{S_t||S_{t-1}}$, and $\mathcal{G}_{s,2}^k$ and $\mathcal{G}_{c,2}^k$ maintain and update the second weighted

Algorithm 5 Detailed Algorithm of Alg. 3

1: **function** ***SEQ_FRESH***$(\{S_t\}_{t\in[M-1]}, Params^s, Params^c, \tau)$
2: **for** $t \in [M-2]$ **do**
3: $p(S_t) \leftarrow \text{GMM}(S_t, Params^s)$
4: $p(S_t, S_{t+1}) \leftarrow \text{GMM}(S_t||S_{t+1}, Params^c)$
5: $p \leftarrow p(S_0) \times \prod_{t=0}^{M-2} \frac{p(S_t,S_{t+1})}{p(S_t)}$
6: **if** $p < \tau$ **then**
7: $Params^s, Params^c \leftarrow \text{DYNEM}(\{S_t\}_{t\in[M-1]}, Params^s, Params^c)$
8: **return** p
9: **function** ***GMM***$(X, Params)$
10: $\{\phi_k, \mu_k, \Sigma_k\}_{k\in[\mathcal{K}-1]} \leftarrow$ ***GET_GMM_PARAMS***$(Params)$
11: $p(X) \leftarrow \sum_{k=0}^{\mathcal{K}-1} \phi_k \mathcal{N}(X \mid \mu_k, \Sigma_k)$
12: **return** $p(X)$
13: **function** ***GET_GMM_PARAMS***$(Params)$
14: $\{\mathcal{G}_0^k, \mathcal{G}_1^k, \mathcal{G}_2^k\}_{k\in[\mathcal{K}-1]} \leftarrow Params$
15: **for** $k \in [\mathcal{K}-1]$ **do**
16: $\phi_k \leftarrow \mathcal{G}_0^k, \mu_k \leftarrow \mathcal{G}_{s1}^k/\mathcal{G}_0^k, \Sigma_k \leftarrow (\mathcal{G}_2^k - \mu_k \times \mathcal{G}_1^{k^T})/\mathcal{G}_0^k$
17: **return** $\{\phi_k, \mu_k, \Sigma_k\}_{k\in[\mathcal{K}-1]}$
18: **function** ***GET_CS_STAT***$(X, Params)$
19: $\{\phi_k, \mu_k, \Sigma_k\}_{k\in[\mathcal{K}-1]} \leftarrow$ ***GET_GMM_PARAMS***$(Params)$
20: $\{w_k\}_{k\in[\mathcal{K}-1]} \leftarrow \{\phi_k \mathcal{N}(X \mid \mu_k, \Sigma_k)\}_{k\in[\mathcal{K}-1]}$
21: $CS\_Stat \leftarrow \{w_k, w_k X, w_k XX^T\}_{k\in[\mathcal{K}-1]}$
22: **return** CS_Stat
23: **function** ***UPDATE_PARAMS***$(CS\_Stat, Params)$
▷ γ: update weight parameter
24: $\{\mathcal{G}_0^k, \mathcal{G}_1^k, \mathcal{G}_2^k\}_{k\in[\mathcal{K}-1]} \leftarrow Params$
25: $\{w_k, w_k X, w_k XX^T\}_{k\in[\mathcal{K}-1]} \leftarrow CS\_Stat$
26: $\{\mathcal{G}_0^k\}_{k\in[\mathcal{K}-1]} \leftarrow \{\gamma w_k + (1-\gamma)\mathcal{G}_0^k\}_{k\in[\mathcal{K}-1]}$
27: $\{\mathcal{G}_1^k\}_{k\in[\mathcal{K}-1]} \leftarrow \{\gamma w_k X + (1-\gamma)\mathcal{G}_1^k\}_{k\in[\mathcal{K}-1]}$
28: $\{\mathcal{G}_2^k\}_{k\in[\mathcal{K}-1]} \leftarrow \{\gamma w_k XX^T + (1-\gamma)\mathcal{G}_2^k\}_{k\in[\mathcal{K}-1]}$
29: $Params \leftarrow \{\mathcal{G}_0^k, \mathcal{G}_1^k, \mathcal{G}_2^k\}_{k\in[\mathcal{K}-1]}$
30: **return** $Params$
31: **function** ***DYNEM***$(\{S_t\}_{t\in[M-1]}, Params^s, Params^c)$
▷ GET_CS_STAT: Compute C-S statistics in Definition 3.
▷ UPDATE_PARAMS: Update corresponding parameters using C-S statistics.
32: **for** $S_t \in \{S_t\}_{t\in[M-1]}$ **do**
33: $CS\_Stat^s \leftarrow \text{GET\_CS\_STAT}(S_t, Params^s)$
34: $Params^s \leftarrow \text{UPDATE\_PARAMS}(CS\_Stat^s, Params^s)$
35: **for** $S_t||S_{t+1} \in \{S_t||S_{t+1}\}_{t\in[M-2]}$ **do**
36: $CS\_Stat^c \leftarrow \text{GET\_CS\_STAT}(S_t||S_{t+1}, Params^c)$
37: $Params^c \leftarrow \text{UPDATE\_PARAMS}(CS\_Stat^c, Params^c)$
38: **return** $Params^s, Params^c$

C-S statistics $\overline{S_t S_t^T}$ and $\overline{(S_t||S_{t-1})(S_t||S_{t-1})^T}$. With the updated parameters of ***DYNEM***, the information of the GMMs parameters is also updated. So we can calculate the updated parameters of the GMMs by function ***GET_GMM_PARAMS***.

UPDATE_PARAMS updates the C-S statistics parameters of ***DYNEM*** *Params* with the current C-S statistics *CS_Stat* derived from the current input state. The parameters of ***DYNEM*** are updated by a factor of γ (lines 24–29 of Alg. 5).

The convergence of Dynamic EM is guaranteed, which has the asymptotic equivalence to the EM algorithm. We refer the interested readers to the proof presented in Sec. 3.2 of [21].