Phát hện gian lận bằng mô hình Markov ẩn

Mô hình ngẫu nhiên

Nguyễn Thanh Hải-20170734
Nguyễn Tiến Thành-20173374
Phạm Tiến Duật-2017349

7/2020

Nội dung

Giới thiệu

Thẻ tín dụng được phân thành hai loại:

- Thẻ vậy lý. Thẻ vật lý dùng để thanh toán tại các cửa hàng (quẹt thẻ) hoặc thanh toán trực tuyến.
- Thẻ điện tử. Thẻ điện tử không có ở dạng vật lý, nó là một công cụ thanh toán kỹ thuật số.

Gian lận thẻ tín dụng là hình thức gian lận sử dụng công nghệ cao để đánh cắp thông tin thẻ tín dụng (Visa, MasterCad, ATM...) của người sử dụng thuộc về lĩnh vực tài chính, ngân hàng. Các hình thức gian lận:

- Bị thanh toán hay quẹt thẻ tại một cửa hàng nào đó khi mua hàng trong trường hợp bạn bị trộm thẻ.
- Sử dụng công nghệ cao qua mạng Internet đánh cắp thông tin thẻ tín dụng của người dùng.
- Bị rút trộm tiền mặt qua máy ATM.
- Làm giả thẻ Visa, MasterCad.

Thiệt hại từ các vụ gian lận thẻ tín dụng là rất lớn

Vì vậy, các ngân hàng đã phải xây dựng các hệ thống ngăn ngừa và phát hiện gian lận trong các giao dịch thẻ tín dụng. Hệ thống này hoạt động theo quy tắc chung:

- Lưu trữ thông tin giao dịch của khách hàng.
- Phân tích dữ liệu giao dịch và khoanh vùng phạm vi sử dụng thẻ.
- Khi một giao dịch được tiến hành, hệ thống dựa vào dữ liệu trong quá khứ để phỏng đoán xem giao dịch có gì bất thường không, từ đó đưa ra các cảnh báo cần thiết.

Nhiều kỹ thuật để phát hiện gian lân thẻ tín dụng: phát hiện gian lận dựa vào cây quyết định; sử dụng mạng Nơ ron để phán đoán các giao dịch bất thường; kỹ thuật sử dụng cây quyết đinh...
Trong báo cáo này, chúng em giới thiệu và tập trung phân tích kỹ thuật sử dụng mô hình Markov ẩn (Hidden Markov Model – HMM) để phát hiện gian lận thẻ tín dụng.

Một số định nghĩa mở đầu và Mô hình Markov

1. Một số định nghĩa
2. Mô hình Markov

Một số định nghĩa

Định nghĩa 2.1: *(Tính Markov). Một dãy trạng thái ngẫu nhiên được gọi là có tính Markov nếu xác suất chuyển trạng thái tiếp theo chỉ phụ thuộc vào trạng thái hiện tại và quá khứ.*

Định nghĩa 2.2: *(Tính thuần nhất). Một trạng thái ngẫu nhiên được gọi là có tính thuần nhất nếu xác suất chuyển trạng thái chỉ phụ thuôc vào độ lớn khoảng thời gian mà không phụ thuộc vào thời điểm.*

Định nghĩa 2.3: *(Xích Markov). Dãy biến ngẫu nhiên $(X_n)_{n\geq 0}$ được gọi là một xích Markov với phân phối ban đầu λ và ma trận chuyển P nếu:*

i, *X_0 có phân phối λ tức là:*

$$P(X_0 = i) = \lambda_i \qquad \forall i \in I$$

ii, *Với mọi $n \geq 0$ phân phối của X_{n+1} với điều kiện $X_n = i_n$ là $(P_{i_n j})_{j\in I}$ và độc lập với $X_0, \ldots, X_{n-1}$. Tức là:*

$$P(X_{n+1} = i_{n+1} \mid X_n = i_n, \ldots, X_0 = i_0) = P(X_{n+1} = i_{n+1} \mid X_n = i_n)$$
$$= P_{i_n i_{n+1}} \forall n \geq 0, i_0, \ldots, i_{n+1} \in I$$

Một số định nghĩa

Định nghĩa 2.4: *(Quá trình Markov). Quá trình ngẫu nhiên* $(X_t)_{t\geq 0}$ *được gọi là quá trình ngẫu nhiên Markov nếu* $\forall t_0 < t_1 < \ldots < t_{n-1} < t_n < \ldots \in T$ *thì* $X_n = X(t_n), n = 0, 1, 2, \ldots$ *là xích Markov. Tức thỏa mãn:*

$$P(X(t_{n+1}) = j \mid X(t_n) = i_n, X(t_{n-1}) = i_{n-1}, \ldots, X(t_0) = i_0) = P(X(t_{n+1}) = j \mid X(t_n) = i_n)$$

Định nghĩa 2.5: *(Quá trình Markov thuần nhất). Nếu xác suất chuyển chỉ phụ thuộc khoảng thời gian từ* $s \to t$*,tức là:*

$$p(s, i, t, j) = p(s + h, i, t + h, j)$$

thì quá trình Markov được gọi là thuần nhất.

Mô hình Markov

Tập trạng thái quan sát $\{q_1, q_2, \ldots, q_n\}$.

$$P(q_n \mid q_{n-1}, \ldots, q_2, q_1) = P(q_n \mid q_{n-1}) \tag{1}$$

Phương trình 1 được gọi là *Giả thuyết Markov bậc 1*.
Định nghĩa 2.6: *(Mô hình Markov bậc 1). Một hệ thống mà thỏa mãn giả thuyết Markov bậc 1 thì được gọi là mô hình Markov (bậc 1) và chuỗi trạng thái quan sát $\{q_i\}$ của hệ được gọi là chuỗi Markov (bậc 1).*
Xác suất của một chuỗi trạng thái quan sát $\{q_1, q_2, \ldots, q_n\}$ dùng giả thuyết Markov có thể được biểu diễn như sau:

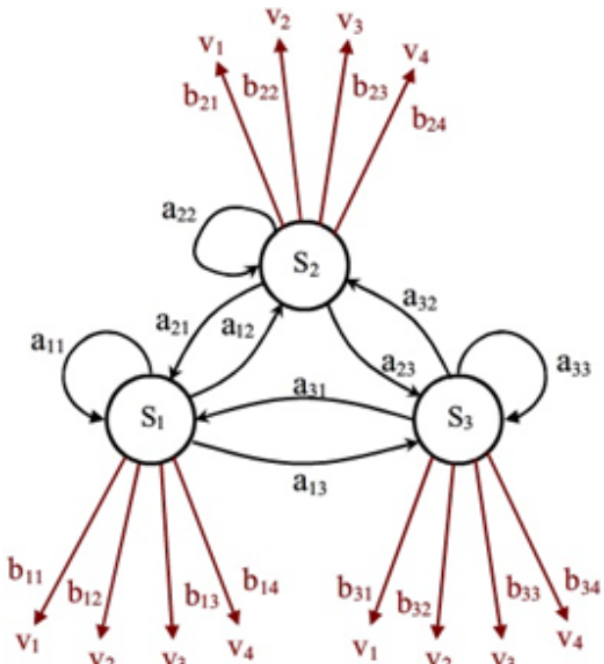
$$P(q_1, q_2, \ldots, q_n) = \prod_{i=1}^{n} P(q_i \mid q_{i-1}) \tag{2}$$

Mô hình Markov ẩn

1. Định nghĩa mô hình Markov ẩn
2. Các thành phần và hoạt động của mô hình Markov ẩn
3. Ba bài toán của mô hình Markov ẩn
4. Ứng dụng của mô hình Markov ẩn

Định nghĩa mô hình Markov ẩn

Mô hình Markov ẩn (Hidden Markov Model - HMM) là kết quả mở rộng của khái niệm Mô hình Markov rời rạc và thuần nhất bằng cách mỗi trạng thái được gắn với một hàm quan sát.
Tập các quan sát $O = \{O_1, O_2, ...\}$ được sinh ra bởi dãy các trạng thái $s_1, s_2, ..., s_N$ của mô hình, mà dãy các trạng thái này không thấy được.
Như vậy trong mô hình Markov ẩn có một quá trình ngẫu nhiên kép
Ví dụ một mô hình Markov ẩn 3 trạng thái



Ví dụ

Có hai người bạn A và B liên lạc với nhau qua tin nhắn điện thoại, A ở Việt Nam còn B ở Mỹ. B là người có tâm trạng dễ thay đổi theo thời tiết. Thường B sẽ kể cho A biết tâm trạng của mình vui hay buồn qua các tin nhắn, nhưng không cho biết về tình hình thời tiết tại nơi B ở. Vậy A có thể đoán được trạng thái thời tiết ở Mỹ nếu chỉ biết xác suất thay đổi thời tiết của 2 ngày liên tiếp tại Mỹ và các khả năng để B cảm thấy vui hay buồn dựa trên thời tiết tại đó được không?
Giả sử xác suất chuyển trạng thái của thời tiết (nắng, mưa, râm) tại Mỹ được cho trong Bảng 1 và giả sử B cho biết sự thay đổi tâm trạng của mình (vui, buồn) dựa trên thời tiết được cho trong bảng sau:

	Vui	Buồn
Nắng	0.9	0.1
Mưa	0.2	0.8
Râm	0.6	0.4

Các thành phần và hoạt động mô hình Markov ẩn

1. Các thành phần của HMM
2. Hoạt động của HMM
3. Các công thức sử dụng trong HMM

Các thành phần của HMM I

Một mô hình Markov ẩn được đặc trưng bởi 5 thành phần cơ bản sau

i) N - số trạng thái trong mô hình. $S = \{s_1, ..., s_N\}$ là tập các trạng thái.

ii) M - số ký hiệu quan sát có thể. $V = \{v_1, ..., v_M\}$ là tập các ký hiệu quan sát có thể.

iii) $A = \{a_{ij}\}$ - xác suất chuyển trạng thái

$$a_{ij} = P(q_{t+1} = s_j | q_t = s_i)$$

$$\begin{cases} \sum_{j=1}^{N} a_{ij} = 1 & i = \overline{1, N} \\ a_{ij} \geq 0 & i, j = \overline{1, N} \end{cases}$$

iv) $B = b_j(k)$ - xác suất phát xạ quan sát trong mỗi trạng thái. $b_j(k)$ là xác suất của quan sát v_k tại trạng thái s_j ở thời điểm t

Các thành phần của HMM II

$$b_j(k) = P(v_k) \text{ tại thời điểm } t | q_t = s_j$$

$$\begin{cases} \sum_{k=1}^{M} b_j(k) = 1 & j = \overline{1, N} \\ b_j(k) \geq 0 & i, j = \overline{1, N}; k = \overline{1, M} \end{cases}$$

v) $\pi = \{\pi_1, ..., \pi_N\}$ là tập các phân bố xác suất cho trạng thái khởi đầu, π_i là xác suất để trạng thái s_i được chọn tại thời điểm khởi đầu $t = 1$

$$\pi_i = P(q_1 = s_i)$$

$$\begin{cases} \sum_{i=1}^{N} \pi_i = 1 & i = \overline{1, N} \\ \pi_i \geq 0 & i, i = \overline{1, N} \end{cases}$$

Hoạt động của HMM

1. Chọn một trạng thái khởi đầu $q_1 = s_i$ tương ứng với xác suất cho trạng thái khởi đầu π
2. Gán $t = 1$.
3. Chọn $O_t = v_k$ tương ứng với xác suất quan sát tại trạng thái s_i , tức là $b_i(k)$.
4. Chuyển sang trạng thái mới $q_{t+1} = s_j$ tương ứng với xác suất chuyển trạng thái a_{ij} .
5. Gán $t = t + 1$ và quay lại bước 3 nếu $t < T$. Nếu ngược lại thì kết thúc.

Bộ ba $\lambda = (A, B, \pi)$ được coi là bộ ký pháp gọn để biểu diễn một mô hình Markov ẩn. A, B, π được gọi là *các tham số* của mô hình λ.

Công thức sử dụng trong HMM I

- Xác suất của một dãy trạng thái: Xác xuất của một dãy trạng thái $q = \{q_1, ..., q_N\}$ từ mô hình HMM với các tham số λ tương ứng là tích của các xác suất chuyển tiếp của mỗi trạng thái cho bởi công thức sau

$$P(q|\lambda) = \pi_{q_1} \prod_{n-1}^{N-1} a_{q_n q_{n+1}} = \pi_{q_1} a_{q_1 q_2} \dots a_{q_{N-1} q_N}$$

- Khả năng của một dãy quan sát sinh bởi dãy trạng thái tương ứng: Cho dãy quan sát $O = \{O_1, ..., O_N\}$ và dãy các trạng thái $q = \{q_1, ...q_N\}$ được xác định bởi mô hình HMM với các tham số λ khả năng của dãy O với điều kiện q được cho bởi

$$P(O|q, \lambda) = \prod_{n=1}^{N} P(O_n|q_n, \lambda) = b_{q_1 O_1} \dots b_{q_N O_N}$$

là một tích các xác suất xạ quan sát.

Công thức sử dụng trong HMM II

- Khả năng chung của một dãy quan sát O và dãy trạng thái q tương ứng đó là xác suất để O và q xảy ra đồng thời

$$P(O, q|\lambda) = P(O|q, \lambda)P(q|\lambda) \qquad \text{(Bayes)}$$

- Khả năng của một dãy quan sát $O = \{O_1, ..., O_N\}$ có mối liên hệ với một HMM với các tham số λ xác định bởi

$$P(O|\lambda) = \sum_{\forall q} P(O, q|\lambda)$$

đó là tổng của các khả năng chung của dãy tất cả các dãy trạng thái có thể của q cho bởi mô hình.

Ba bài toán của mô hình Markov ẩn

1. Bài toán 1: Bài toán ước lượng (Likelihood Computation)
2. Bài toán 2: Bài toán giải mã (Decoding Computation)
3. Bài toán 3: Bài toán huấn luyện (Training HMM)

Bài toán 1: Bài toán ước lượng (Likelihood Computation) I

Bài toán: Cho mô hình Markov ẩn $\lambda = (A, B, \pi)$ và một dãy quan sát $O = \{O_1, O_2...\}$, cần tính xác suất $P(O|\lambda)$.
Giả sử ta có dãy quan sát $O = \{O_1, O_2, ..., O_T\}$ độ dài T và dãy các trạng thái tương ứng của mô hình Markov ẩn $q = \{q_1, q_2, ..., q_T\}$. Khi đó, xác suất để dãy quan sát O được sinh ra bởi mô hình λ là:

$$\begin{aligned} P(O|\lambda) &= \sum_{\forall q} P(O, q|\lambda) \\ &= \sum_{\forall q} P(O|q, \lambda).P(q|\lambda) \\ &= \sum_{\forall q} \left[\prod_{t=1}^{T} P(O_t|q_t, \lambda).\lambda_{q_1} \prod_{t=1}^{T-1} a_{q_t q_{t+1}} \right] \end{aligned}$$

Tính xác suất này bằng cách liệt kê tất cả các khả năng có thể của dãy trạng thái q .Cách này có độ phức tạp tính toán rất lớn.

Bài toán 1: Bài toán ước lượng (Likelihood Computation) II

Khắc phục trong thuật toán tiến - lùi sau đây.

- **Thuật toán tiến**
  Gọi biến tiến $\alpha_t(i) = P(O_1, O_2, ..., O_t, q_t = s_i|\lambda)$ là xác suất biến quan sát O tới thời điểm t : $O = O_1, ..., O_t$, tại trạng thái s_i được sinh bởi mô hình λ.
  Các giá trị $\alpha_t(i)$ được tính bằng thuật toán đệ quy sau

  B1. Khởi tạo

$$\alpha_1(i) = \pi_i b_i(O_1), 1 \leq i \leq N \tag{2}$$

  B2. Tính các $\alpha_{t+1}(j)$ bằng phương pháp đệ quy

$$\alpha_{t+1}(j) = \left[\sum_{i=1}^{N} \lambda_t(i) a_{ij}\right] b_j(O_{t+1}) 1 \leq t \leq T-1; 1 \leq j \leq N \tag{3}$$

Bài toán 1: Bài toán ước lượng (Likelihood Computation) III

B3. Kết thúc

$$P(O|\lambda) = \sum_{i=1}^{N} \alpha_T(i). \tag{4}$$

Thuật toán dừng lại ở $B3$ khi $t = T$.

- **Thuật toán lùi**
  Gọi biến lùi $\beta_t(i) = P(O_{t+1}, O_{t+2}, ..., O_T|q_t = s_i, \lambda)$ là xác suất cảu dãy quan sát O từ thời điểm $t+1$ đến thời điểm $T : O = O_{t+1}, O_{t+2}, ..., O_T$ với điều kiện là mô hình ở trạng thái s_i tại thời điểm t. Các $\beta_t(i)$ được tính bằng thuật toán đệ quy sau

  B1. Khởi tạo

$$\beta_T(i) = 1, 1 \leq i \leq N \tag{5}$$

Bài toán 1: Bài toán ước lượng (Likelihood Computation) IV

B2. Tính các $\beta_t(j)$ bằng phương pháp đệ quy

$$\beta_t(j) = \sum_{j=1}^{N} a_{ij} b_j(O_{t+1}) \beta_{t+1}(j) \tag{6}$$

$$t = T-1, T-2, \ldots, 1; 1 \leq i \leq N$$

B3. Kết thúc

$$P(O|\lambda) = \sum_{i=1}^{N} \pi_i b_i(O_1) \beta_1(i) \tag{7}$$

Bằng thuật toán tiến-lùi, ta có thể tính xác suất

$$P(O|\lambda) = \sum_{i=1}^{N} \alpha_T(i) = \sum_{i=1}^{N} \pi_i b_i(O_1) \beta_1(i) = \sum_{i=1}^{N} \alpha_t(i) \beta_t(i). \tag{8}$$

Bài toán 2: Bài toán giải mã (Decoding Computation) I

Bài toán: Với dãy quan sát $O = \{O_1, O_2, ...\}$ và mô hình Markov ẩn $\lambda = (A, B, \pi)$. Làm thể nào để có thể tìm được dãy trạng thái tương ứng $q = \{q_1, q_2, ..., \}$ tối ưu nhất theo một tiêu chuẩn nào đó?
Phương pháp thông dụng là dùng thuật toán tìm kiếm Viterbi để tìm ra một dãy các trạng thái tối ưu duy nhất.
Đặt $\delta_t(i) = \max_{q_1,q_2,...,q_{t-1}} P(q_1 q_2 ... q_{t-1} q_t = s_i, O_1 O_2 ... O_t|\lambda)$ là biến cố xác suất cao nhất tại mọi thời điểm t tương ứng với dãy trạng thái $q_1, q_2, ..., q_{t-1}$ kết thúc tại trạng thái $q_i = s_i$. Các biến $\delta_{t+1}(j)$ được tính bằng phương pháp đệ quy dựa trên các tính toán trước đó

$$\delta_{t+1}(j) = \left[\max_{a \le i \le N} \delta_t(i) a_{ij}\right] b_j(O_{t+1}) \tag{9}$$

Để lưu vết các trạng thái của dãy các trạng thái tối ưu ta dùng mảng $\psi_t(j)$, khi thuật toán kết thúc các phần tử trong mảng chính là các trạng thái của dãy q cần tìm. Thuật toán tìm kiếm Viterbi mô tả như sau

Bài toán 2: Bài toán giải mã (Decoding Computation) II

B1. Khởi tạo

$$\delta_1(i) = \pi_i b_i(O_i), 1 \leq i \leq N \tag{10}$$

B2. Đệ quy

$$\delta_t(j) = \left[\max_{1\leq i\leq N} \delta_{t-1}(i)a_{ij}\right] b_j(O_t), \quad 2 \leq t \leq T; 1 \leq j \leq N \tag{11}$$

$$\psi_t(j) = \arg\max_{1\leq i\leq N} \left[\delta_{t-1}(i)a_{ij}\right], \quad 2 \leq t \leq T; 1 \leq j \leq N \tag{12}$$

B3. Kết thúc

$$P^*(O|\lambda) = \max_{1\leq i\leq N} [\delta_T(i)]$$

B4. Truy hồi các trạng thái

$$q_t^* = \psi_{t+1}(q_{t+1}^*, \qquad t = T-1, T-2, ..., 1 \tag{13}$$

Kết thúc thuật toán, các q_t^* chính là các trạng thái của dãy cần tìm.

Bài toán 3: Bài toán huấn luyện (Training HMM) I

Bài toán: Bài toán tối ưu các tham số của mô hình. Tìm cách nào để điều chỉnh các tham số A, B, π để được xác suất $P(O|\lambda)$ lớn nhất? Giải pháp cho bài toán này là thủ tục huấn luyện lặp Baum-Welch. Chọn biến $\gamma_t(i) = P(q_t = s_i|O, \lambda)$ là xác suất để mô hình ở trạng thái s_i tại thời điểm t với dãy quan sát O và mô hình λ đã cho. Với định nghĩa trên, biến $\gamma_t(i)$ được biểu diễn thông qua hai biến tiến và lùi như sau

$$\gamma_t(i) = \frac{P(q_t = s_i|O, \lambda)}{P(O|\lambda)} = \frac{\alpha_t(i)\beta_t(i)}{P(O|\lambda} = \frac{\alpha_t(i)\beta_t(i)}{\sum_{i=1}^{N} \alpha_t(i)\beta_t(i)} \tag{14}$$

Từ công thức 14 rút ra được $\sum \gamma_t(i) = 1$.

Với $\gamma_t(i)$ có thể tìm được tại thời điểm t xác suất lớn nhất của dãy $\{O_1, O_2, ..., O_t\}$ là

$$q_t = \arg\max\left[\gamma_t(i)\right], \qquad 1 \leq i \leq N; 1 \leq t \leq T \tag{15}$$

Bài toán 3: Bài toán huấn luyện (Training HMM) II

Chọn biến $\xi_t(i,j)$ là xác suất mô hình ở trạng thái s_i tại thời điểm t và ở trạng thái s_j tại thời điểm $t+1$ với mô hình λ và dãy quan sát O cho trước, tức là

$$\xi_t(i,j) = P(q_t = s_i, q_{t+1} = j|O,\lambda) \tag{16}$$

Với biến tiến $\alpha_t(i)$ và biến lùi $\beta_t(j)$ được định nghĩa như trên, $\xi_t(i,j)$ có thể biểu diễn như sau

$$\begin{aligned}\xi_t(i,j) &= \frac{P(q_t = s_i, q_{t+1} = j|O,\lambda}{P(O|\lambda} = \frac{\alpha_t(i)a_{ij}b_j(O_{t+1}\beta_{t+1}(j)}{P(O|\lambda} \\ &= \frac{\alpha_t(i)a_{ij}b_j(O_{t+1}\beta_{t+1}(j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_t(i)a_{ij}b_j(O_{t+1}\beta_{t+1}(j)}\end{aligned} \tag{17}$$

Bài toán 3: Bài toán huấn luyện (Training HMM) III

Từ định nghĩa của $\gamma_t(i)$ ta có

$$\gamma_t(i) = \sum_{j=1}^{N} \xi_t(i,j) \tag{18}$$

Từ các công thức trên có thể nhận thấy:

$\sum_{t=1}^{T-1} \xi_t(i,j)$ = khả năng để mô hình chuyển trạng thái từ s_i sang s_j.

$\sum_{t=1}^{T-1} \gamma_t(i)$ = khả năng để mô hình chuyển trạng thái từ s_i.

Từ các công thức trên ta có tập các công thức dùng để điều chỉnh (re-estimation) các tham số của mô hình Markov ẩn như sau:

Bài toán 3: Bài toán huấn luyện (Training HMM) IV

$\overline{\pi_i}$ = khả năng mô hình ở trạng thái s_i tại thời điểm $(t = 1)$

$$\overline{\pi_i} = \gamma_1(i) \tag{19}$$

$\overline{a_{ij}}$= (khả năng chuyển trang thái từ s_i sang s_j)/(khả năng chuyển từ trạng thái s_i)

$$\Rightarrow \overline{a_{ij}} = \frac{\sum_{t=1}^{T-1} \xi_t(i,j)}{\sum_{t=1}^{T-1} \gamma_t(i)} \tag{20}$$

Bài toán 3: Bài toán huấn luyện (Training HMM) V

$\overline{b_j(v_k)}$ = (khả năng ở tại trạng thái s_i với ký hiệu quan sát v_k)/(khả năng ở tại trạng thái v_i)

$$\Rightarrow \overline{b_j(v_k)} = \frac{\sum_{t=1, O_t=v_k}^{T} \gamma_t(j)}{\sum_{t=1}^{T} \gamma_t(j)} \tag{21}$$

Với một mô hình $\lambda = (A, B, \pi)$ đầu tiên, sử dụng các công thức, 19, 20 và 21 để tính toán bộ tham số mới $\lambda = (A, B, \pi)$. Theo [7] ta đã chứng minh được rằng:

- Hoặc là mô hình khởi điểm λ được định nghĩa chính xác là mô hình hội tụ và do đó $\lambda = \overline{\lambda}$.
- Hoặc là mô hình mới có $P(O|\overline{\lambda}) > P(O|\lambda)$.

Bài toán 3: Bài toán huấn luyện (Training HMM) VI

Dựa vào chứng minh này, dùng $\overline{\lambda}$ thay thể cho λ và lặp lại các tính toán (19), (20), (21) sẽ cải thiện được xác suất $P(O|\lambda)$ cho tới thời điểm thuật toán hội tụ.
Trong quá trình tính toán, sau mỗi lần lặp các biểu thức sau đây luôn được thỏa mãn

$$\sum_{i=1}^{N} \overline{\pi_i} = 1, \sum_{j=1}^{N} \overline{a_{ij}} = 1, \sum_{k=1}^{N} \overline{b_j}(k) = 1 \quad (22)$$

$$1 \leq i \leq N, 1 \leq j \leq N$$

Ứng dụng mô hình Markov ẩn

Mô hình Markov ẩn có rất nhiều ứng dụng trong thực tế:

- Các bài toán dự báo: dự báo thời tiết, dự đoán biến động thị trường chứng khoán,. . .
- Các bài toán nhận dạng: Nhận dạng tiếng nói, nhận dạng thực thể, nhận dạng chữ viết tay, . . .
- Tin sinh học và hệ gene học: Dự đoán vùng mang mã trên một trình từ gene, xác định các họ gene hoặc họ protein liên quan, mô phỏng cấu trúc không gian của protein từ trình tự aminoacid, . . .
- Xử lí tín hiệu, phân tích dữ liệu và nhận dạng mẫu.

Phát hiện gian lận thẻ tín dụng bằng HMM

1. Phát hiện gian lận thẻ tín dụng bằng HMM
2. Áp dụng phương pháp
3. Nhận xét

Phát hiện gian lận thẻ tín dụng bằng HMM I

Dựa trên mô hình Markov ẩn, việc phát hiện gian lận không sử dụng xác minh thông tin cá nhân, chữ ký... mà chỉ sử dụng thói quen chi tiêu của khách hàng.
Hệ thống sẽ sử dụng các thông tin trong lịch sử giao dịch của khách hàng trước đó như loại mặt hàng, số lượng, tần suất giao dịch, số tiền giao dịch, địa điểm mua hàng ... để so sánh với giao dịch hiện tại xem có sự bất thường nào không.
Nếu có, hệ thống sẽ đưa ra cảnh báo và yêu cầu người dùng xác minh danh tính hoặc yêu cầu nhập một mã xác nhận nào đó. Nếu xác nhận thành công, hệ thống sẽ cho tiếp tục giao dịch.
Ngược lại, đó được coi như là một giao dịch gian lận.

Phát hiện gian lận thẻ tín dụng bằng HMM II

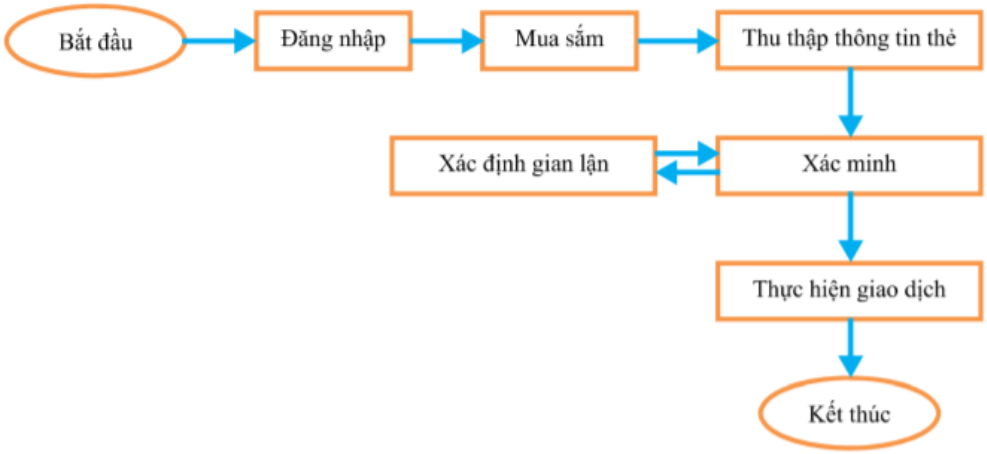


Figure: Xác định gian lận sử dụng HMM[6]

Phát hiện gian lận thẻ tín dụng bằng HMM III

Trong phần này, ta áp dụng các thuật toán của bài toán ước lượng và bài toán giải mã trình bày trong chương trước. Một mô hình Markov ẩn được ký hiệu là $\lambda = (A, B, \pi)$. Với A, B, π là các tham số đã được xác định ở chương trước.
Trong thực tế, mỗi khách hàng mua rất nhiều loại mặt hàng khác nhau và khó có thể dự đoán. Mặt khác, số tiền giao dịch của khách hàng là rõ ràng. Vì vậy ta có thể tiếp cận bài toán phát hiện gian lận thẻ tín dụng như sau:

- Phân cụm các loại mặt hàng thành N cụm. Đối với mỗi khách hàng có một cách phân cụm khác nhau.
- Đối với số tiền chi tiêu cho mỗi giao dịch, ta lại phân cụm số tiền chi tiêu thành M cụm. Ta coi mỗi cụm là một ký hiệu quan sát v_i. Với mỗi trạng thái s_i ta có xác suất phát xạ quan sát B tương ứng với M ký hiệu quan sát.
- Kết hợp với một phân phối ban đầu phù hợp của các trạng thái ta có mô hình Markov ẩn $\lambda = (A, B, \pi)$ tướng ứng.

Phát hiện gian lận thẻ tín dụng bằng HMM IV

Mô hình trên được xây dựng dựa trên việc giao dịch của khách hàng. Giả sử ta có một dãy quan sát số tiền của các giao dịch là $O = \{O_1,\ O_2, \ldots, O_R\}$. Xác suất của dãy quan sát đó là:

$$\alpha_1 = P(O_1, O_2, \ldots, O_R|\lambda)$$

Khi khách hàng thực hiện giao dịch tiếp theo, ta có quan sát O_{R+1}, ta loại bỏ quan sát O_1 và được dãy quan sát $O = \{O_2, O_3, \ldots, O_{R+1}\}$. Xác suất của dãy quan sát này là:

$$\alpha_2 = P\left(O_2, O_3, \ldots, O_{R+1}|\lambda\ \right)$$

Và ta ký hiệu: $\Delta\alpha = \alpha_1 - \alpha_2$
Nếu $\Delta\alpha \leq 0$ thì giao dịch có quan sát O_{R+1} được coi là giao dịch bình thường.

Phát hiện gian lận thẻ tín dụng bằng HMM V

Nếu $\Delta\alpha > 0$ thì giao dịch có thể là một giao dịch gian lận. Giao dịch đó là gian lận nếu với một ngưỡng sai khác cho phép kí hiệu là Z và

$$\frac{\Delta\alpha}{\alpha_1} \geq Z$$

Tuy nhiên, trong thực tế các trường hợp gian lận có đặc điểm thực hiện nhiều giao dịch trong một khoảng thời gian ngắn. Vì vậy ta có thể xác định gian lận bằng nhiều giao dịch sau giao dịch có quan sát O_R như sau:
Ta ký hiệu: $\beta_2 = P(O_{R+1},\ O_{R+2}, \ldots, O_{2R}|\lambda)$ và

$$\Delta\beta = \alpha_1 - \beta_2$$

Tương tự như trên, nếu $\Delta\beta > 0$ và $\frac{\Delta\beta}{\alpha_1} \geq Z$ thì hệ thống sẽ đưa ra cảnh báo các giao dịch là gian lận.

Áp dụng phương pháp

Phương pháp gồm 3 phần chính:

- Phân cụm dữ liệu
- Đào tạo dữ liệu
- Phát hiện gian lận

Cụ thể như sau:

Thuật toán phân cụm

Sử dụng thuật toán phân cụm K-mean (K-mean clustering) [8] để nâng cao hiệu quả của hệ thống. Ý tưởng thuật toán như sau:
Bước 1: Khởi tạo K điểm dữ liệu trong bộ dữ liệu và tạm thời coi nó là tâm của các cụm dữ liệu của chúng ta.
Bước 2: Với mỗi điểm dữ liệu trong bộ dữ liệu, tâm cụm của nó sẽ được xác định là 1 trong K tâm cụm gần nó nhất.
Bước 3: Sau khi tất cả các điểm dữ liệu đã có tâm, tính toán lại vị trí của tâm cụm để đảm bảo tâm của cụm nằm ở chính giữa cụm.
Bước 4: Bước 2 và bước 3 sẽ được lặp đi lặp lại cho tới khi vị trí của tâm cụm không thay đổi hoặc tâm của tất cả các điểm dữ liệu không thay đổi.

Thuật toán đào tạo I

Vấn đề tiếp theo là nếu giao dịch là bình thường, thì dữ liệu đó được đưa vào dùng để tính toán trong các lần giao dịch tiếp theo. Vì vậy, chúng ta cần có một bước gọi là đào tạo dữ liệu (training data). Với *thuật toán đào tạo* được thể hiện bằng sơ đồ bên dưới.

Thuật toán đào tạo II

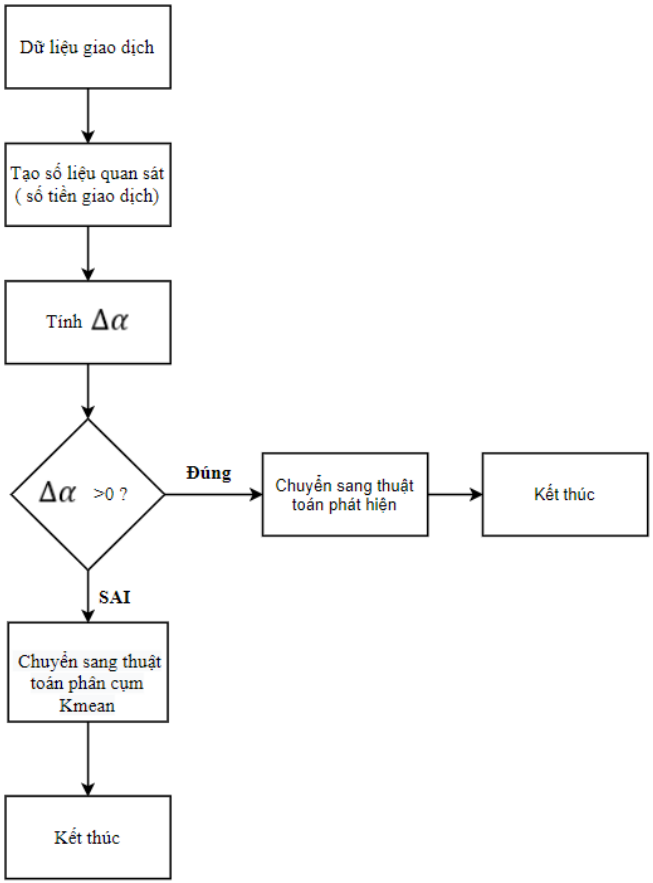


Figure: Thuật toán đào tạo

Thuật toán đào tạo III

Các bước cụ thể như sau:
Bước 1: Từ dữ liệu giao dịch, xác định các tham số của mô hình và ký hiệu quan sát Q_{R+1}.
Bước 2: Tính α_1, α_2 và $\Delta\alpha$
Bước 3:

- Nếu $\Delta\alpha \leq 0$ thì giao dịch là bình thường, thêm dữ liệu và sử dụng thuật toán phân cụm K-mean để phân cụm với dữ liệu mới.
- Nếu $\Delta\alpha > 0$ thì giao dịch có thể là gian lân và chuyển sang thuật toán phát hiện.

Thuật toán phát hiện I

Khi $\Delta\alpha > 0$ ta thực hiện *thuật toán phát hiện* như sau:
Bước 1: Nhập ngưỡng cho phép Z.
Bước 2 : Tính $\frac{\Delta\alpha}{\alpha_1}$
Bước 3:

- Nếu $\frac{\Delta\alpha}{\alpha_1} < Z$ thì sai khác là chấp nhận được và thêm dữ liệu vào để sử dụng thuật toán phân cụm K-mean.
- Nếu $\frac{\Delta\alpha}{\alpha_1} \geq Z$ thì hệ thống đưa ra cảnh báo giao dịch là gian lận.

Chú ý: Trong một số thử nghiệm với R trong khoảng từ 5 đến 25, với R =15 mang lại hiệu quả cao nhất [7]. Vì vậy, trong các phần tiếp theo, ta mặc định các số liệu có được khi áp dụng với R=15.
/CODE như sau:/

Nhận xét

1. Hiệu quả của phương pháp
2. Cách khắc phục và phương hướng phát triển

Hiệu quả của phương pháp I

Đánh giá hiệu quả của phương pháp dựa trên việc chọn ngưỡng chấp nhận Z.
Ta thấy khi chọn Z càng nhỏ, số lượng các giao dịch bị cảnh báo gian lận càng nhiều. Tuy nhiên khi đó tỷ lệ chính xác sẽ rất thấp. Nếu chọn Z quá lớn sẽ dẫn tới việc một số giao dịch là gian lận nhưng không bị cảnh báo. Vì vậy chúng ta phải chọn ngưỡng chấp nhận Z sao cho hiệu quả.
Ta tham khảo dữ liệu từ các thử nghiệm sau đây [9]
Trong đó:
$p =$ (số gian lận phát hiện được)/(số gian lận thực tế)
$q =$ Độ chính xác = (số gian lận)/(số cảnh báo gian lận)

Hiệu quả của phương pháp II

Ngưỡng chấp nhận Z	$p(\%)$	$q(\%)$
0.3	92	39
0.4	88	43
0.5	77	53
0.6	70	60
0.7	59	70

Bảng 4.1: Hiệu quả phương pháp dựa trên ngưỡng chấp nhận

Hiệu quả của phương pháp III

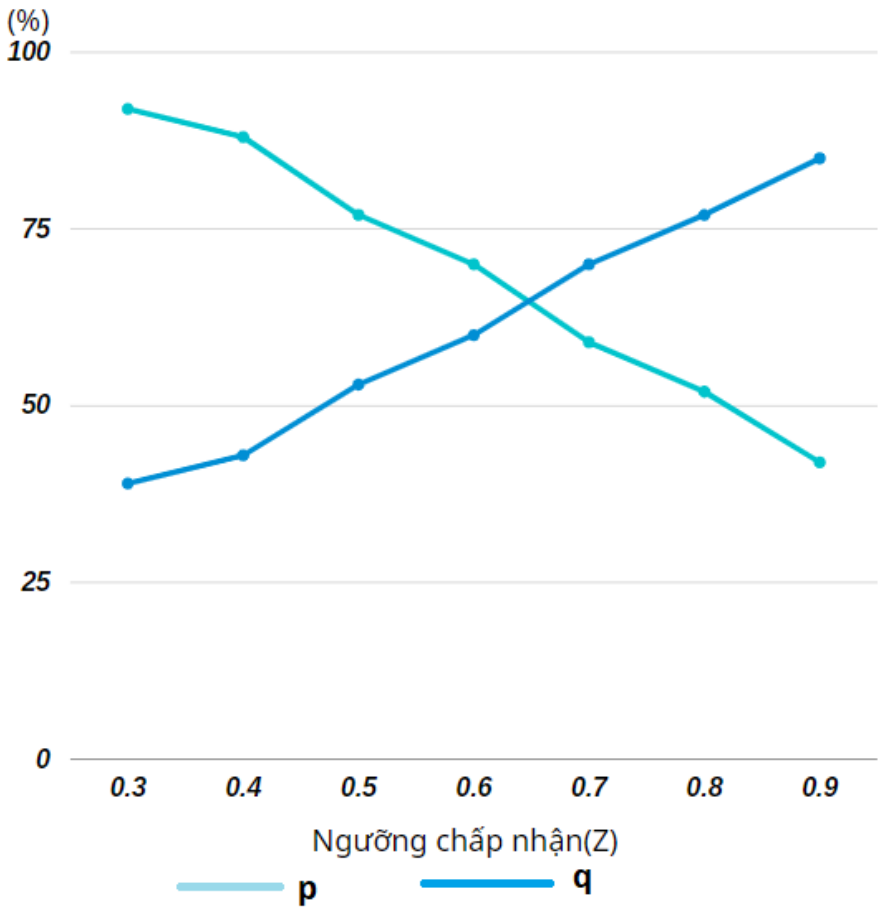


Figure: Hiệu quả phương pháp phụ thuộc ngưỡng chấp nhận Z

Hiệu quả của phương pháp IV

Dựa vào biểu đồ, ta thấy tùy thuộc vào mục tiêu và chiến lược trong thực tế, ta có thể chọn ngưỡng chấp nhận sao cho hợp lý. Ở đây chúng ta có thể chọn Z = 0,5 hoặc 0,6.
Độ chính xác thay đổi theo lượng dữ liệu giao dịch.
Cũng theo dữ liệu tham khảo từ những thử nghiệm[9] ta có bảng dữ liệu sau (với ngưỡng chấp nhận Z=0.5):

Số bộ dữ liệu	100	200	300	400	500	600
Độ chính xác	0.87	0.77	0.69	0.58	0.51	0.48

Bảng 4.2: Sự thay đổi của độ chính xác theo lượng dữ liệu giao dịch.

Ta thấy với lượng dữ liệu lớn, hiệu quả của phương pháp chưa cao.

Hiệu quả của phương pháp V

Ta có một số nhận xét sau:

- Ưu điểm của phương pháp là đưa ra phán đoán nhanh vì các bước phân cụm dữ liệu, đào tạo dữ liệu đã được thực hiện trước khi giao dịch mới phát sinh.
- Nhược điểm của phương pháp: độ chính xác chưa cao, khả năng làm việc với dữ liệu lớn còn kém.

Cách khắc phục và phương hướng phát triển

- Thêm bước chọn k trong thuật toán phân cụm K-mean sao cho hiệu quả nhất.
- Thử nghiệm với dữ liệu thực tế để đưa ra ngưỡng chấp nhận hợp lý.
- Kết hợp và mở rộng với một số phương pháp khác như:
  + Sử dụng mô hình Markov ẩn phân kỳ[7].
  + Sử dụng mô hình bán Markov ẩn (SHMM) kết hợp với các nhân tố thông tin tiêu chuẩn (factorized information criterion – FIC) [9].
  + Sử dụng mô hình Markov ẩn đa phối cảnh (multi-perspective HMMs)[10]

Kết luận

Trong bài báo cáo, chúng ta đã trình bày được một số vấn đề sau:

1. Nhắc lại và trình bày một số kiến thức về xích Markov, quá trình Markov, mô hình Markov.
2. Trình bày định nghĩa và một số tính chất đặc trưng của mô hình Markov ẩn cùng ví dụ minh họa.
3. Trình bày ba bài toán cơ bản của mô hình Markov ẩn và một số ứng dụng trong thực tế.
4. Trình bày phương pháp phát hiện gian lận thẻ tín dụng bằng cách sử dụng mô hình Markov ẩn bao gồm: các thuật toán, nhận xét hiệu quả phương pháp cùng phương hướng khắc phục, phát triển.