Ứng dụng đại số tuyến tính

Đại học Khoa học Tự Nhiên, ĐHQG Thành phố Hồ Chí Minh

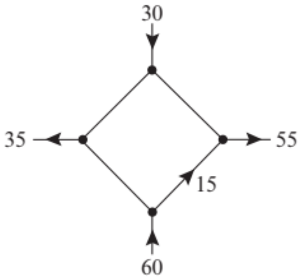
Ngày 23 tháng 2 năm 2023

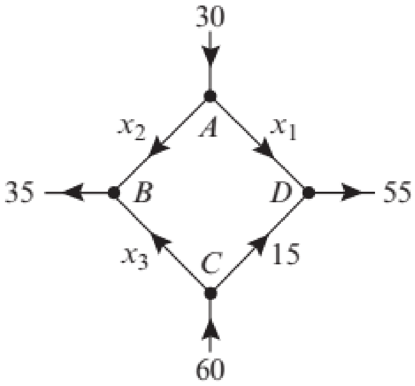
1. Ứng dụng HPTTT
2. Ứng dụng ĐSTT trong mật mã học - Cryptography
3. Ứng dụng ĐSTT trong đồ họa máy tính

Outlines

Hệ PTTT trong bài toán điều tiết lưu lượng

Hình bên dưới minh họa cho hệ thống của lưu lượng đi qua 4 điểm, tại từng điểm ta có số lượng dịch chuyển và hướng của các dòng chảy tại. Hãy tìm chiều dịch chuyển và tìm lưu lượng dịch chuyển trên các cạnh tương ứng.





Gọi x_1, x_2, x_3, x_4 là lưu lượng từng cạnh tương ứng trên hình. Hướng của dòng chảy trên từng cạnh được đặt như trên và hướng của dòng chảy có thể thay đổi phụ thuộc theo kết quả của lưu lượng được tìm ra.

Hệ PTTT trong bài toán lưu lượng

Từ mô hình của lưu lượng tại node A, ta có

$$x_1 + x_2 = 30$$

Tương tự, tại các nodes khác ta có

$$\begin{aligned} x_2 + x_3 &= 30 \\ x_3 + 15 &= 60 \\ x_1 + 15 &= 55 \end{aligned}$$

Giải hệ phương trình trên, ta có

$$x_1 = 40, x_2 = -10, x_3 = 45$$

Do $x_2 = 40$ là một số âm nên kết quả này cho thấy hướng của lưu lượng tại x_2 là ngược lại với giả thuyết đặt ra từ đầu bài.

Hệ PTTT trong bài toán cân bằng hóa học

Một phương trình hóa học được gọi là cân bằng nếu mỗi nguyên tố trong phương trình có cùng số nguyên tử ở mỗi bên. Xét ví dụ về phương trình đã cân bằng

$$CH_4 + 2O_2 \longrightarrow CO_2 + 2H_20$$

Với phương trình trên, ta có thể nhân thêm các hằng số nguyên dương vào 2 về phương trình, tuy nhiên trong lý thuyết sẽ dùng hằng số nguyên dương nhỏ nhất cho việc cân bằng.
Với một phương trình hóa học, ta có thể áp dụng hệ phương trình tuyến tính cho việc giải tìm hệ số cân bằng.

Ví dụ

Gọi x_1, x_2, x_3, x_4 lần lượt là hệ số cân bằng của CH_4, O_2, CO_2, H_20 trong phương trình hóa học

$$x_1 CH_4 + x_2 O_2 \longrightarrow x_3 CO_2 + x_4 H_2 0$$

Või mỗi nguyên tố trong phương trình hóa học, tổng số nguyên tử nguyên tố đó ở 2 về bằng nhau, ta có

$$\begin{aligned} x_1 &= x_3 \text{ với nguyên tố Carbon} \\ 4x_1 &= 2x_4 \text{ với nguyên tố Hydro} \\ 2x_2 &= 2x_3 + x_4 \text{ với nguyên tố Oxy} \end{aligned}$$

Từ đó, ta có hệ phương trình

$$x_1 - x_3 = 0$$
$$4x_1 - 2x_4 = 0$$
$$2x_2 - 2x_3 - x_4 = 0$$

Ma trận hóa hệ phương trình trên

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 4 & 0 & 0 & -2 \\ 0 & 2 & -2 & -1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & -1/2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1/2 \end{pmatrix}$$

$$x_1 = \alpha/2, x_2 = \alpha, x_3 = \alpha/2, x_4 = \alpha, \alpha \in \mathbb{R}$$

Hệ số tối giản nhất khi $t = 2$, do đó phương trình được cân bằng lần lượt $x_1 = 1, x_2 = 2, x_3 = 1, x_4 = 2$

Ví dụ - SV tự giải

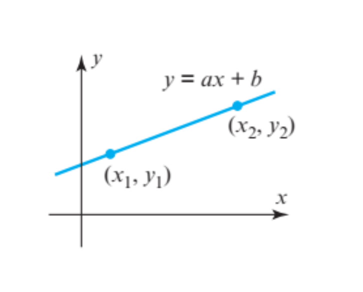
Cân bằng phương trình hóa học sau

$$HCl + Na_3PO_4 \longrightarrow H_3PO_4 + NaCl$$

Nội suy đa thức

Hệ phương trình tuyến tính có ứng dụng trong việc nội suy, với bài toán tìm một đa thức mà đồ thị đi qua các điểm đã có trước trên mặt phẳng.

Tìm một hàm số bậc nhất đi qua các điểm trên mặt phẳng tọa độ hình sau



Nội suy đa thức

Đồ thị trên hình là của đa thức có dạng $y = ax + b$, và do đồ thị đi qua 2 điểm $(x_1, y_1), (x_2, y_2)$ nên ta có

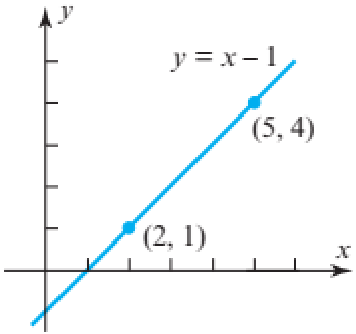
$$y_1 = ax_1 + b$$
$$y_2 = ax_2 + b$$

Giải hệ phương trình trên tìm được a, b và do đó nhận được đa thức cần tìm.

Nội suy đa thức

Ví dụ

Tìm đa thức $y = ax + b$, biết đồ thi đi qua 2 điểm trên hình sau



Giải

Do hàm số $y = ax + b$ đi qua 2 điểm $A(2,1), B(5,4)$, thay tọa độ lần lượt vào hàm số ta có

$$1 = 2a + b$$
$$4 = 5a + b$$

Giải hệ phương trình trên, ta có $a = 1, b = -1$, vậy hàm số cần tìm có dạng $y = x - 1$.

Nội suy đa thức

Định lý

Với n điểm cho trước trên mặt phẳng Oxy mà các tọa độ x_i khác nhau, khi đó sẽ có duy nhất 1 đa thức có bậc nhỏ hơn hay bằng $n-1$ mà đồ thị sẽ đi qua các điểm trên.

Ví dụ

Tìm đa thức có đồ thị đi qua các điểm sau

$$(1,3) \quad (2,-2) \quad (3,-5) \quad (4,0)$$

Giải

Vì đồ thị đi qua 4 điểm, nên ta sẽ sử dụng nội suy đa thức với 1 đa thức có bậc là $n = 3$.

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$$

Với 4 điểm đã có trước trên hệ trục tọa độ, ta có hệ phương trình

$$\begin{cases} a_0 + a_1 + a_2 + a_3 = 3 \\ a_0 + 2a_1 + 4a_2 + 8a_3 = -2 \\ a_0 + 3a_1 + 9a_2 + 27a_3 = -5 \\ a_0 + 4a_1 + 16a_2 + 64a_3 = 0 \end{cases}$$

Ma trận hóa hệ phương trình trên

$$\tilde{A} = \left(\begin{array}{cccc|c} 1 & 1 & 1 & 1 & 3 \\ 1 & 2 & 4 & 8 & -2 \\ 1 & 3 & 9 & 16 & -5 \\ 1 & 4 & 16 & 64 & 0 \end{array}\right) \longrightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & -5 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

Giải

Giải hệ trên và nhận được các hệ số của đa thức là

$$a_0 = 4, a_1 = 3, a_2 = -5, a_3 = 1$$

Do đó đa thức cần tìm có dạng

$$p(x) = 4 + 3x - 5x^2 + x^3$$

Ví dụ

Tìm tích phân sau

$$\int_0^1 \sin\left(\frac{\pi x^2}{2}\right) dx$$

Giải

Để tìm tích phân trên, ta không thể áp dụng các phương pháp cơ bản. Một phương pháp được áp dụng là nội suy đa thức xấp xỉ với hàm số cần tìm tích phân và tính tích phân của hàm số đó. Để nội suy đa thức, ta có thể chọn 5 điểm với tọa độ x lần lượt

$$x_0 = 0 \quad x_1 = 0.25 \quad x_2 = 0.5 \quad x_3 = 0.75 \quad x_4 = 1$$

Với hàm $f(x) = \sin\left(\frac{\pi x^2}{2}\right)$, giá trị hàm số $f(x)$ lần lượt được tìm

$$f(x_0) = 0 \quad f(x_1) = 0.098017 \quad f(x_2) = 0.382683 \quad f(x_3) = 0.77301 \quad f($$

Do đồ thị của đa thức đi qua 5 điểm nên ta có thể chọn đa thức bậc 4 có dạng

$$p(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$$

Ứng dụng hệ phương trình tuyến tính để giải, ta có đa thức cần tìm có dạng

$$p(x) = 0.098796x + 0.762356x^2 + 2.14429x^3 - 2.00544x^4$$

Do đó, để tìm tích phân của hàm $f(x)$ ban đầu, ta có thể tính tích phân của hàm $p(x)$

$$\int_0^1 \left(0.098796x + 0.762356x^2 + 2.14429x^3 - 2.00544x^4\right) dx \approx 0.438501$$

Ví dụ - SV tự giải

Tìm tích phân sau

$$\int_0^1 e^{x^2} dx$$

Ứng dụng hệ PTTT từ thời Ai Cập cổ đại

Giấy cói Ahmes (hoặc Rhind) là nguồn cung cấp hầu hết thông tin của chúng ta về Toán học Ai Cập. Tờ giấy cói dài 5 mét này chứa 84 bài toán ngắn, cùng với lời giải của chúng, và có niên đại từ khoảng năm 1650 trước Công nguyên.

Ứng dụng hệ PTTT từ thời Ai Cập cổ đại

Bài toán 40 trong Giấy cói Ahmes.

Chia 100 hecta lúa mạch cho 5 người đàn ông theo cấp số cộng sao cho tổng là hai người nhận được ít nhất bằng một phần bảy tổng của ba người nhận nhiều nhất.

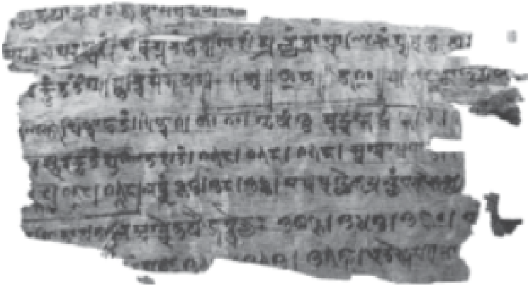
Ta có thể lập được hệ phương trình biểu diễn cho bài toán

$$\begin{cases} 5a + 10d = 100 \\ 11a - 2d = 0 \end{cases}$$

Phương pháp giải được mô tả trong giấy cói được gọi là phương pháp định vị sai hoặc giả định.
Nó bắt đầu bằng cách giả sử một số giá trị thuận tiện của a (trong trường hợp của chúng ta $a = 1$), thay giá trị đó vào phương trình thứ hai, và nhận được $d = 11/2$. Thay $a = 1$ và $d = 11/2$ vào vế trái của phương trình đầu tiên ta được 60, ngược lại vế phải là 100.
Điều chỉnh dự đoán ban đầu cho a bằng cách nhân nó với $100/60$ dẫn đến giá trị đúng $a = 5/3$. Thay $a = 5/3$ vào phương trình thứ hai thì cho $d = 55/6$, do đó số lượng lúa mạch mà năm người đàn ông nhận được là $10/6$, $65/6$, $120/6$, $175/6$ và $230/6$ hecta.
Kỹ thuật đoán giá trị của một ẩn số và sau này điều chỉnh nó đã được sử dụng bởi nhiều nền văn hóa trong suốt các thời đại.

Bản thảo Bakhshali là một tác phẩm cổ của toán học Ấn Độ. Hình ảnh sau được lưu trữ tại Thư viện Bodleian, Đại học của Oxford. Nó bao gồm khoảng 70 lá hoặc tấm vỏ cây bạch dương có chứa các vấn đề toán học và các bài pháp của chúng. Nhiều bài toán của nó được gọi là bài toán cân bằng dẫn đến hệ phương trình tuyến tính. Một trong những bài toán như sau

Thương gia thứ nhất có bảy con ngựa asava, thương gia thứ hai có chín con ngựa haya, và thương gia thứ ba có mười con lạc đà. Nếu mỗi người cho hai người còn lại 1 con vật của mình thì giá trị của những con vật mỗi người có sẽ như nhau. Tìm giá của mỗi con vật và tổng giá trị của các con vật sở hữu bởi từng người.



Fragment III-5-3v of the Bakhshali Manuscript

[Image: Bodleian Library, University of Oxford, MS. Sansk. d. 14, fragment III 5 3v.]

Outlines

Trong phần này, chúng ta tìm hiểu phương pháp mã hóa và giải mã tin nhắn.
Nghiên cứu mã hóa và giải mã các tin nhắn bí mật được gọi là mật mã học. Trong thời buổi hiện nay, sự quan tâm đối với chủ đề mật mã học tăng cao vì nhu cầu duy trì quyền riêng tư của thông tin truyền qua các đường dây liên lạc công cộng.
Trong ngôn ngữ mật mã, thư không được mã hóa được gọi là bản văn và thư được mã hóa được gọi là bản mã. Quá trình chuyển đổi từ văn bản thuần túy sang mã hóa được gọi là mã hóa, và quá trình đảo ngược chuyển đổi từ mật mã sang văn bản thuần túy được gọi là giải mã.

Mật mã Hill

Mật mã Hill do Lester S. Hill giới thiệu trên 2 bài báo "Cryptography in an Algebraic Alphabet," American Mathematical Monthly, 36 (June– July 1929), pp. 306–312; and "Concerning Certain Linear Transformation Apparatus of Cryptography," American Mathematical Monthly, 38 (March 1931), pp. 135–154.]

Trong phương pháp này, ta sẽ gán mỗi ký tự trong bản văn và mỗi ký tự trong bản mã bằng một số cụ thể, trong đó Z sẽ được gán giá trị là 0.

Table 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Mật mã Hill

Ngoài ra, mỗi cặp ký tự trong bản văn sẽ được mã hóa thành các ký tự trong bản mã như sau

- Chọn 1 ma trận vuông cấp 2 với các hệ số nguyên

  $$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

  để thực hiện mã hóa
- Nhóm mỗi 2 ký tự trên bản văn thành 1 nhóm và thêm 1 ký tự giả bằng cách lập lại ký tự cuối cùng nếu số lượng ký tự là lẻ.

- Gán mỗi ký tự thành một số hạng theo thứ tự trong bảng trên. Do đó ta có được từng cặp ký tự trong bản văn là một vector cột có dạng

$$p = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

- Từng cặp ký tự trong bảng mật mã được tìm bằng tích giữa ma trận A và p, Ap.
- Biểu diễn lại từng số trong mật mã đã được mã hóa thành các ký tự chữ cái tương ứng.

Mật mã học

Ví dụ

Sử dụng ma trận mã hóa sau

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$$

để mã hóa bản văn sau IAMHIDING

Mã hóa

- Nhóm từng cặp ký tự trong bản văn, do số lượng ký tự là 9 nên ta sẽ có 1 ký tự giả GG

  IA MH ID IN GG

- Sử dụng chữ số thay thế cho các ký tự ở bảng trên, ta có

  91 138 94 914 77

Với từng cặp ký tự trong bản văn đã biểu diễn dưới dạng số, ta mã hóa lần lượt. Ví dụ với IA,

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} 9 \\ 1 \end{pmatrix} = \begin{pmatrix} 11 \\ 3 \end{pmatrix}$$

Từ bảng trên ta có ký tự IA sau khi được mã hóa sẽ trở thành KC. Thực hiện mã hóa toàn bộ ta nhận được bảng mật mã từ bản văn ban đầu

KCCXQLKPUU

Mật mã học

Ví dụ

Mã hóa văn bản DARKNIGHT với ma trận mã hóa

$$A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$$

Ví dụ

Giải mã bản mã GTNKGKDUSK với ma trận mã hóa

$$A = \begin{pmatrix} 5 & 6 \\ 2 & 3 \end{pmatrix}$$

Ví dụ

Giải mã bản mã SAKNOXAOJX với ma trận mã hóa

$$A = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix}$$

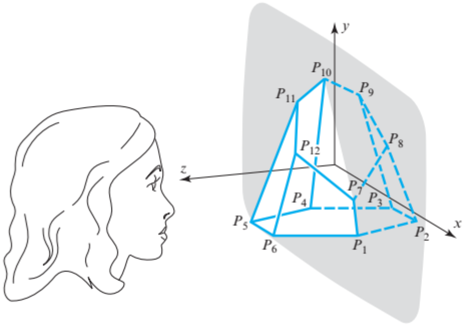
Ví dụ

Giải mã bản mã IOSBTGXESPXHOPDE biết những ký tự đầu tiên là DEAR.

Outlines

Ứng dụng ĐSTT trong đồ họa máy tính

Với mỗi vật thể trong không gian 3 chiều $\mathbb{R}^3$, các điểm mà mắt nhìn thấy được sẽ được gán với các điểm tọa độ P_i như hình minh họa sau.



Ứng dụng ĐSTT trong đồ họa máy tính

Với các điểm P_1 đến P_{12} ở hình trên, ta đã gán các tọa độ cho các điểm của hình khối mà mắt thường quan sát được.

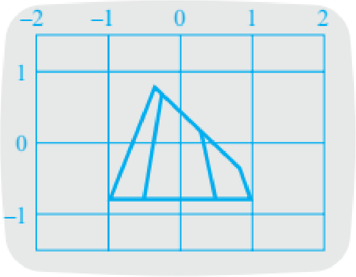
P_1: (1.000, −.800, .000), P_2: (.500, −.800, −.866),
P_3: (−.500, −.800, −.866), P_4: (−1.000, −.800, .000),
P_5: (−.500, −.800, .866), P_6: (.500, −.800, .866),
P_7: (.840, −.400, .000), P_8: (.315, .125, −.546),
P_9: (−.210, .650, −.364), P_{10}: (−.360, .800, .000),
P_{11}: (−.210, .650, .364), P_{12}: (.315, .125, .546)

Tổng quát, với n điểm biểu diễn của một hình khối trong không gian 3 chiều, ta có thể ma trận hóa các điểm trên bằng ma trận có dạng

$$P = \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \\ z_1 & z_2 & \cdots & z_n \end{bmatrix}$$

Ứng dụng ĐSTT trong đồ họa máy tính

Bằng cách giữ lại các thành phần x, y của các điểm và biểu diễn n điểm trên mặt phẳng tọa độ Oxy ta có hình phẳng mô hình cho hình khối ban đầu.



View 1

Ứng dụng ĐSTT trong đồ họa máy tính

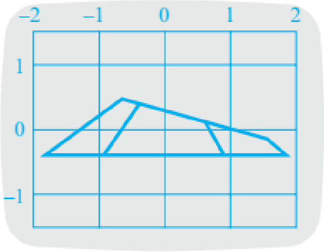
Một trong những bài toán quan tâm đó là thu phóng hình dáng của hình khối ban đầu và biểu diễn hình minh họa sau khi thu phóng trên không gian Oxy.

Để thực hiện việc thu phóng này, ta gọi α là hệ số thu phóng theo chiều Ox, β là hệ số thu phóng theo chiều Oy và γ là hệ số thu phóng theo chiều Oz, do các điểm biểu diễn của hình khối ban đầu là môt ma trận với 3 dòng và n cột, nên ta đặt ma trận S là ma trận hệ số thu phóng theo yêu cầu và ta có

$$S = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix}$$

Ứng dụng ĐSTT trong đồ họa máy tính

Hình dưới đây minh họa cho việc thu phóng hình khối ban đầu với hệ số $\alpha = 1.8, \beta = 0.5, \gamma = 3$



▲ View 2 View 1 scaled by $\alpha = 1.8,\ \beta = 0.5,\ \gamma = 3.0.$

$$SP = \begin{bmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{bmatrix} \begin{bmatrix} x_1 & x_2 & \cdots & x_n \\ y_1 & y_2 & \cdots & y_n \\ z_1 & z_2 & \cdots & z_n \end{bmatrix}$$

$$= \begin{bmatrix} \alpha x_1 & \alpha x_2 & \cdots & \alpha x_n \\ \beta y_1 & \beta y_2 & \cdots & \beta y_n \\ \gamma z_1 & \gamma z_2 & \cdots & \gamma z_n \end{bmatrix} = P'$$

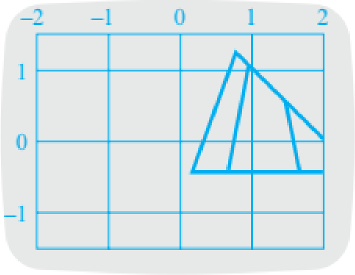
Dời hình ảnh

Một vấn đề được quan tâm tiếp theo là dời hình ảnh hoặc biểu diễn hình ảnh tại một vị trí khác trên màn hình. Gọi x_0, y_0, z_0 là sự thay đổi lần lượt theo Ox, Oy, Oz mà các điểm biểu diễn mới của hình ảnh sẽ thay đổi so với tọa độ gốc. Khi đó mỗi điểm P_i' là các điểm biểu diễn mới của P_i, ta có tọa độ của $P_i' = (x_i + x_0, y_i + y_0, z_i + z_0)$ và tất cả các điểm biểu diễn mới của hình trên màn hình đều thay đổi theo quy tắc trên. Vì thế, ta đặt ma trận T

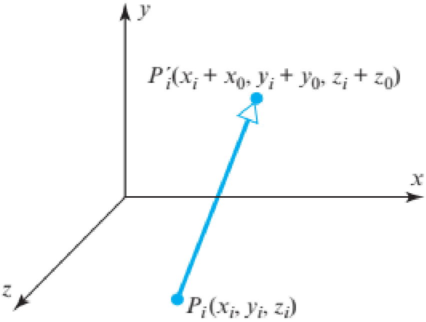
$$T = \begin{pmatrix} x_0 & x_0 & \dots & x_0 \\ y_0 & y_0 & \dots & y_0 \\ z_0 & z_0 & \dots & z_0 \end{pmatrix}$$

Với tọa độ lúc sau của mỗi điểm biểu diễn thỏa điều kiện $P' = P + T$

Dời hình ảnh

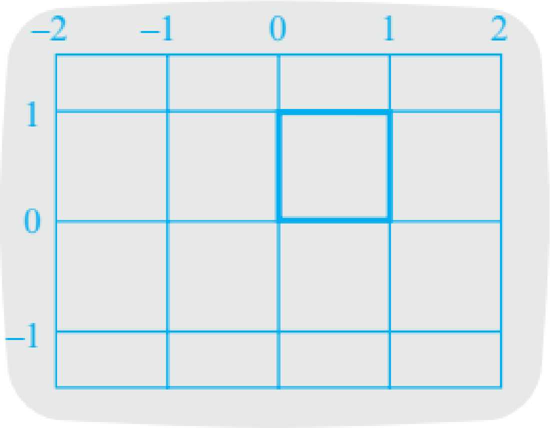


▲ View 3 View 1 translated by $x_0 = 1.2, \quad y_0 = 0.4, \quad z_0 = 1.7.$



Ví dụ

Cho một hình vuông được vẽ trên hình sau



Ví dụ

a) Tìm ma trận biểu diễn tọa độ 4 đỉnh của hình vuông trên hình,

b) Tìm tọa độ biểu diễn 4 đỉnh của hình vuông nếu thực hiện thu phóng theo tỷ lệ $\alpha = 1.5, \beta = 0.5$ và vẽ hình biểu diễn hình vuông sau khi thu phóng,

c) Tìm tọa độ biểu diễn 4 đỉnh của hình vuông nếu thực hiện phép dời hình với vector biểu diễn sự thay đổi của Ox, Oy, Oz lần lượt là $(-2, -2, 3)$ và vẽ hình biểu diễn của hình vuông sau khi dời hình.