

Ứng dụng của định lý Combinatorial Nullstellensatz

Trương Phước Nhân, 01/08/2017

Xem lại các bài viết “Định lý không điểm tổ hợp”, “Bổ đề Permanet và ứng dụng” và “Định lý Chevalley – Warning”.

Bài toán 1: (Trois-Zannier) Cho p là một số nguyên tố và $S_1, S_2, \dots, S_k$ là tập các số nguyên không âm, mỗi tập đều chứa số 0 và chứa các số nguyên phân biệt theo modulo p . Giả sử $\sum_i (|S_i| - 1) \geq p$. Chứng minh rằng với mọi bộ $(a_1, a_2, \dots, a_k) \in \mathbb{Z}_p^k$ phương trình $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$ luôn có một nghiệm không tầm thường $(x_1, x_2, \dots, x_k) \in S_1 \times S_2 \times \dots \times S_k$.

Chứng minh:

Xét đa thức $P(x_1, x_2, \dots, x_k) = (a_1x_1 + a_2x_2 + \dots + a_kx_k)^{p-1} - 1 + c \prod_{0 \neq s_1 \in S_1} (x_1 - s_1) \prod_{0 \neq s_2 \in S_2} (x_2 - s_2) \dots \prod_{0 \neq s_k \in S_k} (x_k - s_k)$ trong đó c được chọn sao cho $P(0, \dots, 0) = 0$. Nhận thấy: bậc của đa thức $(a_1x_1 + a_2x_2 + \dots + a_kx_k)^{p-1}$ là $p-1$ và bậc của đa thức $c \prod_{0 \neq s_1 \in S_1} (x_1 - s_1) \prod_{0 \neq s_2 \in S_2} (x_2 - s_2) \dots \prod_{0 \neq s_k \in S_k} (x_k - s_k)$ là $\sum_i (|S_i| - 1)$, theo giả thiết ta suy ra bậc của đa thức P là $\sum_i (|S_i| - 1)$. Dễ dàng nhận thấy $c \neq 0$ (nếu ngược lại ta suy ra $P(0, \dots, 0) = -1$) nên hệ số của đơn thức $x_1^{|S_1|-1} x_2^{|S_2|-1} \dots x_k^{|S_k|-1}$ bằng $c \neq 0$.

Áp dụng định lý Combinatorial Nullstellensatz cho đa thức P ta tìm được bộ $(t_1, t_2, \dots, t_k) \in S_1 \times S_2 \times \dots \times S_k$ sao cho $P(t_1, t_2, \dots, t_k) \neq 0$.

Nếu $a_1t_1 + a_2t_2 + \dots + a_kt_k \neq 0$ sử dụng định lý Fermat ta suy ra $(a_1x_1 + a_2x_2 + \dots + a_kx_k)^{p-1} = 1$. Do $P(t_1, t_2, \dots, t_k) \neq 0$ nên vector $(t_1, t_2, \dots, t_k)$ là không tầm thường (hiểu theo nghĩa $\neq (0, \dots, 0)$) nên $c \prod_{0 \neq s_1 \in S_1} (x_1 - s_1) \prod_{0 \neq s_2 \in S_2} (x_2 - s_2) \dots \prod_{0 \neq s_k \in S_k} (x_k - s_k) = 0$, điều này suy ra rằng $(a_1x_1 + a_2x_2 + \dots + a_kx_k)^{p-1} \neq 1$, mâu thuẫn. Từ đây ta suy ra $a_1x_1 + a_2x_2 + \dots + a_kx_k = 0$.

Bài toán 2: (Alon) Cho p là một số nguyên tố và $a_1, a_2, \dots, a_k$ các số nguyên modulo p (không nhất thiết phân biệt). Chứng minh rằng với $b_1, b_2, \dots, b_k$ ($k < p$) là các số nguyên modulo p phân biệt ta luôn tìm được một hoán vị σ sao cho các số $a_1 + b_{\sigma(1)}, a_2 + b_{\sigma(2)}, \dots, a_k + b_{\sigma(k)}$ là phân biệt.

Chứng minh: Đặt $B = \{b_1, b_2, \dots, b_k\}$. Giả sử phản chứng, với mọi cách chọn $b_{\sigma(1)}, b_{\sigma(2)}, \dots, b_{\sigma(k)}$ thì luôn có ít nhất là hai phần tử trong số các phần tử $a_1 + b_{\sigma(1)}, a_2 + b_{\sigma(2)}, \dots, a_k + b_{\sigma(k)}$ trùng nhau. Điều đó có nghĩa là nếu $x_1, x_2, \dots, x_k$ là các phần tử phân biệt thuộc B thì $\prod_{1 \leq i < j \leq k} (x_i + a_i - x_j - a_j) = 0$ trên $\mathbb{Z}_p$.

Xét đa thức: $P(x_1, x_2, \dots, x_k) = \prod_{1 \leq i < j \leq k} (x_i - x_j)(x_i + a_i - x_j - a_j)$.

$$\Rightarrow P(x_1, x_2, \dots, x_k) = \prod_{1 \leq i < j \leq k} (x_i - x_j)^2 + Q(x_1, x_2, \dots, x_k)$$

trong đó Q là một đa thức có bậc nhỏ hơn $\prod_{1 \leq i < j \leq k} (x_i - x_j)^2$. Do đó $\deg P = k(k-1)$.

Từ nhận xét trên ta suy ra đa thức $P(x_1, x_2, \dots, x_k)$ triệt tiêu với mọi $(x_1, x_2, \dots, x_k) \in B^k$.

Ta cần xác định các bộ $(t_1, t_2, \dots, t_k)$ với $t_1 + t_2 + \dots + t_k = k(k-1)$, $t_i < k-1$ và hệ số của đơn thức $x_1^{t_1} x_2^{t_2} \dots x_k^{t_k}$ không triệt tiêu trên $\mathbb{Z}_p$. Nhận thấy là từ hai điều kiện đầu ta suy ra $t_1 = t_2 = \dots = t_k = k-1$. Ta cần xác định hệ số của đơn thức $x_1^{k-1} x_2^{k-1} \dots x_k^{k-1}$. Do $\deg Q < k(k-1)$ nên ta chỉ cần tính hệ số của đơn thức $x_1^{k-1} x_2^{k-1} \dots x_k^{k-1}$ trong đa thức $\prod_{1 \leq i < j \leq k} (x_i - x_j)^2$.

Chú ý rằng bằng kỹ thuật xử lý định thức ta thu được :
$$\prod_{1 \leq i < j \leq k} (x_i - x_j)^2 = (-1)^{\frac{k(k-1)}{2}} (x_1 x_2 \dots x_k)^{k-1} \prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)$$

Do đó vấn đề trở thành xác định hệ số tự do trong khai triển của biểu thức $\prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)$. Ta cần đến kết quả phụ mạnh mẽ sau đây :

Bổ đề : Cho $a_1, a_2, \dots, a_k$ là các số nguyên không âm. Nếu kí hiệu $f(a_1, a_2, \dots, a_k)$ là số hạng tự do của “đa thức” $\prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$ thì $f(a_1, a_2, \dots, a_k) = \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! a_2! \dots a_k!}$.

Chứng minh bổ đề : Đặt $g(a_1, a_2, \dots, a_k) := \frac{(a_1 + a_2 + \dots + a_k)!}{a_1! a_2! \dots a_k!}$.

Ta chứng minh bằng qui nạp theo $a_1 + a_2 + \dots + a_k$ đẳng thức $f(a_1, a_2, \dots, a_k) = g(a_1, a_2, \dots, a_k)$.

Với $a_1 = a_2 = \dots = a_k = 0$ thì hệ thức là hiển nhiên. Ta có 2 nhận xét cơ bản sau về đại lượng $g(a_1, a_2, \dots, a_k)$:

1) $g(a_1, a_2, \dots, a_k) = g(a_1 - 1, a_2, \dots, a_k) + g(a_1, a_2 - 1, \dots, a_k) + \dots + g(a_1, a_2, \dots, a_k - 1)$ nếu tất cả các a_i đều dương

2) $g(a_1, \dots, a_l, 0, a_{l+1}, \dots, a_k) = g(a_1, \dots, a_l, a_{l+1}, \dots, a_k)$

Do vậy ta chỉ cần chứng minh $f(a_1, a_2, \dots, a_k)$ cũng thỏa mãn các hệ thức truy hồi tương tự :

1') $f(a_1, a_2, \dots, a_k) = f(a_1 - 1, a_2, \dots, a_k) + f(a_1, a_2 - 1, \dots, a_k) + \dots + f(a_1, a_2, \dots, a_k - 1)$ nếu tất cả các a_i đều

dương. Thật vậy, đẳng thức trên suy ra từ sự kiện $\prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)^{a_i} = \sum_{i=1}^n \left(\prod_{j \neq i} \left(1 - \frac{x_i}{x_j}\right)^{a_i} \prod_{j \neq i} \left(1 - \frac{x_i}{x_j}\right)^{-1} \right)$

(sử dụng công thức nội suy Lagrange cho đa thức $P(x) = 1$ với các mốc nội suy $x_1, x_2, \dots, x_n$ ta thu được hệ

thức $1 = \sum_{i=1}^n \prod_{j \neq i} \left(1 - \frac{x_i}{x_j}\right)^{-1}$ và xét tại giá trị $x = 0$)

2') $f(a_1, \dots, a_{l-1}, 0, a_{l+1}, \dots, a_k) = f(a_1, \dots, a_{l-1}, a_{l+1}, \dots, a_k)$. Thật vậy, nếu $a_l = 0$ thì

$\prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)^{a_i} = \prod_{\substack{1 \leq i \neq j \leq k \\ i, j \neq l}} \left(1 - \frac{x_i}{x_j}\right)^{a_i}$ nên $f(a_1, \dots, a_{l-1}, 0, a_{l+1}, \dots, a_k) = f(a_1, \dots, a_{l-1}, a_{l+1}, \dots, a_k)$.

Từ đây ta suy ra điều phải chứng minh.

Từ bổ đề trên ta nhận thấy hệ số tự do trong khai triển của biểu thức $\prod_{1 \leq i \neq j \leq k} \left(1 - \frac{x_i}{x_j}\right)$ là $\frac{(1+1+\dots+1)!}{1!1!\dots1!} = k!$

nên hệ số của đơn thức $x_1^{k-1} x_2^{k-1} \dots x_k^{k-1}$ trong khai triển của biểu thức $\prod_{1 \leq i < j \leq k} (x_i - x_j)^2$ là

$(-1)^{\frac{k(k-1)}{2}} k! \neq 0$ ($0 < k < p$) trên $\mathbb{Z}_p$. Theo định lý Combinatorial Nullstellensatz ta tìm được một vector

$(\overline{x_1}, \overline{x_2}, \dots, \overline{x_k}) \in B^k$ sao cho $P(\overline{x_1}, \overline{x_2}, \dots, \overline{x_k}) \neq 0$, mâu thuẫn. Kết thúc chứng minh.

Tài liệu tham khảo

- [1]. Titu Andreescu, Gabriel Dospinescu, Problems from the book, Second Editon.
- [2]. Trương Phước Nhân, Định lý không điểm tổ hợp, 30/07/2017
- [3]. Trương Phước Nhân, Bổ đề Permanet và ứng dụng, 30/07/2017
- [4]. Trương Phước Nhân, Định lý Chevalley – Warning , 31/07/2017

