

Ma trận Hadamard

Trương Phước Nhân, 10/02/2018

Một ma trận H cấp $n \times n$ có tất cả các phần tử là ± 1 được gọi là Hadamard bậc n nếu $HH^T = H^T H = nI$.

Chú ý rằng điều kiện $HH^T = nI$ nói lên rằng H là ma trận khả nghịch với ma trận nghịch đảo $\frac{1}{n}H^T$. Bởi vì

một ma trận sẽ giao hoán với ma trận nghịch đảo của nó, nên một trong hai điều kiện $HH^T = nI$ hoặc $H^T H = nI$ sẽ suy ra điều kiện còn lại. Một điểm lưu ý nữa đó là hệ thức $HH^T = nI$ có nghĩa là hai hàng khác nhau bất kì của ma trận H sẽ trực giao (tích vô hướng của chúng bằng 0), và tương tự $H^T H = nI$ tương đương với việc hai cột khác nhau bất kì của ma trận H cũng trực giao.

Nhận xét rằng nếu ta có một ma trận Hadamard thì bằng cách nhân một hàng (hoặc một cột) bất kì cho -1 thì kết quả thu được vẫn là một ma trận Hadamard; tính trực giao của các hàng và các cột được bảo toàn. Do đó chúng ta luôn luôn có thể chuẩn hóa một ma trận Hadamard, tức là ta luôn có thể giả thiết rằng tất cả các phần tử ở hàng đầu tiên (hoặc cột đầu tiên) bằng 1.

Kết quả 1: Nếu tồn tại một ma trận Hadamard H có bậc $n > 2$, thì n là một bội số của 4

Chứng minh:

Giả sử rằng H đã được chuẩn hóa, có nghĩa là tất cả các phần tử ở hàng đầu tiên bằng 1. Do các hàng trực giao nhau, hàng thứ hai phải có cùng số các số 1 và -1 ; do đó ta phải có $\frac{n}{2}$ số 1 và $\frac{n}{2}$ số -1 , nên n phải là một số chẵn. Bằng cách sắp xếp lại thứ tự các cột nếu cần thiết (việc làm này không làm thay đổi tính trực giao giữa các hàng), ta có thể giả sử ma trận H có hai hàng đầu là

$$1 \ 1 \ \dots \ 1 \ 1 \ 1 \ \dots \ 1$$

$$1 \ 1 \ \dots \ 1 \ -1 \ -1 \ \dots \ -1$$

Nếu $n > 2$, ta xét hàng thứ ba của ma trận H . Giả sử rằng có h vị trí trong đó $\frac{n}{2}$ vị trí đầu tiên là 1, và có

k vị trí trong số $\frac{n}{2}$ vị trí sau là 1. Khi đó có $\frac{n}{2} - h$ vị trí trong số $\frac{n}{2}$ vị trí đầu tiên là -1 , và có $\frac{n}{2} - k$ vị trí trong số $\frac{n}{2}$ vị trí sau là -1 .

Do hàng thứ nhất và thứ ba trực giao với nhau nên: $h - \left(\frac{n}{2} - h\right) + k - \left(\frac{n}{2} - k\right) = 0 \Rightarrow h + k = \frac{n}{2}$ (*)

Do hàng thứ hai và thứ ba trực giao với nhau nên: $h - \left(\frac{n}{2} - h\right) - k + \left(\frac{n}{2} - k\right) = 0 \Rightarrow h = k$ (**)

Từ (*) và (**) ta suy ra $h = k = \frac{n}{4}$, hay nói cách khác n là một bội số của 4.

Nếu như tồn tại một ma trận Hadamard bậc $4m$ thì ta có thể thu được một design từ ma trận này. Ý tưởng cơ bản của việc xây dựng nằm ở chỗ là xét một ma trận đã chuẩn hóa và xây đó xóa đi hàng và cột đầu tiên của ma trận này, thay các số -1 bởi số 0, và xem ma trận thu được như một ma trận liên thuộc của một design.

Kết quả 2: Nếu tồn tại một ma trận Hadamard bậc $4m$ thì sẽ tồn tại một $(4m-1, 2m-1, m-1)$ - design

Chứng minh:

Giả sử H là một ma trận Hadamard chuẩn hóa bậc $4m$. Với lối lập luận tương tự như trong kết quả 1) mỗi hàng và mỗi cột của ma trận H , ngoài trừ hàng và cột đầu tiên, sẽ luôn có $2m$ số 1 và $2m$ số -1 .

Bằng cách xóa đi hàng đầu tiên và cột đầu tiên của ma trận H , và tiến hành thay thế các số -1 bởi các số 0. Ma trận thu được là một $(0,1)$ - ma trận A có cấp $(4m-1) \times (4m-1)$ sao cho mỗi hàng và mỗi cột có chính xác $2m$ số 0 và $2m-1$ số 1.

Ta xem xét A như là ma trận liên thuộc của một design như sau: Nó có $4m-1$ khối và $4m-1$ phần tử; mỗi khối chứa chính xác là $2m-1$ phần tử và mỗi phần tử nằm trong chính xác $2m-1$ khối. Với hai phần tử phân biệt bất kì. Các cột của A tương ứng với hai phần tử này có $m-1$ số 1 chung (bằng phương pháp tương tự như trong kết quả 1) ta có thể chứng minh được rằng hai cột bất kì của ma trận H có chung nhau chính xác m số 1, ngoài trừ cột đầu tiên ra), nghĩa là hai phần tử này cùng nằm chung trong chính xác $m-1$ khối, nên $\lambda = m-1$.

Một $(4m-1, 2m-1, m-1)$ - design được gọi là Hadamard design. (xem bài viết “**Cấu hình đối xứng**”)

Nhận xét rằng phép xây dựng trình bày trong kết quả 2) có thể được đảo ngược như sau: Cho trước một Hadamard design, ta tiến hành thay thế các số 0 trong ma trận liên thuộc bằng số -1 và bổ sung thêm hàng và cột đầu gồm tất cả các phần tử bằng 1. Ma trận thu được là một ma trận Hadamard. Do đó ta có kết quả mạnh hơn sau :

Kết quả 3: Một ma trận Hadamard bậc $4m$ tồn tại $\Leftrightarrow$ Một $(4m-1, 2m-1, m-1)$ - design tồn tại

Tài liệu tham khảo :

- [1]. Ian Anderson, A First Course in Discrete Mathematics, 1st.
- [2]. Trương Phước Nhân, Cấu hình đối xứng, 06/02/2018