k-linear unabhängige Mengen

Paul Reichert

16. September 2020

1 Einführung

Definition 1
Sei $n \in \mathbb{N}$. Eine Menge $M \subseteq \mathbb{F}_2^n$ heißt k-linear unabhängig, wenn jede Teilmenge von M mit höchstens k Elementen linear unabhängig ist. Die Kardinalität der größten solchen Menge M wird mit $x_k(n) \coloneqq |M|$ bezeichnet. ◊

Beispiel 1
$n+1$ verschiedene Elemente sind immer linear abhängig. Wenn $n < k$ ist, folgt daraus, dass $x_k(n) = n$ ist. Dazu wähle man M als Basis von $\mathbb{F}_2^n$. ◊

Beispiel 2
Jede Teilmenge von $\mathbb{F}_2^n$ ist 2-linear unabhängig, solange sie nicht den Nullvektor enthält.◊

2 Der Fall $k = 3$

Satz 1
Es sei $n \in \mathbb{N}$. Dann ist $x_3(n) = 2^{n-1}$. ◊

Beweis. Zuerst bemerken wir, dass die Aussage sich mit Beispiel 1 verträgt.

Es sei N eine beliebige Untergruppe von $\mathbb{F}_2^n$, die Index 2 hat. (Beispielsweise können wir die Untergruppe aller Vektoren mit einer geraden Anzahl an Einsen betrachten.)

Nun zeigen wir, dass $M \coloneqq N^c$ eine 3-linear unabhängige Menge ist. Keine nichttriviale $\mathbb{F}_2$-Linearkombination von einem oder zwei Elementen aus M kann 0 ergeben. Wir müssen also nur noch Linearkombinationen dreier Elemente $m_1, m_2, m_3 \in M$ betrachten.

Nun sind aber $m_1 + N, m_2 + N$ und $m_3 + N$ in $F_2^n/N \cong \mathbb{Z}/2\mathbb{Z}$ ein und dasselbe von $0+N$ verschiedene Element der Ordnung 2. Also ist $m_1+m_2+m_3+N$ von N verschieden, weshalb $m_1 + m_2 + m_3$ insbesondere nicht 0 ergeben kann.

Damit ist M tatsächlich 3-linear unabhängig. Wegen $|M| = 2^{n-1}$ ist $x_3(n) \geq 2^{n-1}$.

Wenn eine noch größere 3-linear unabhängige Menge M' in $\mathbb{F}_2^n$ existierte, dann wähle ein $m \in M'$. Wir erhalten durch Addition von $m' \in M' \setminus \{m\}$ noch $|M'| - 1$ paarweise verschiedene Vektoren, die sich als Summe genau zweier (von 0 verschiedener) Vektoren aus M' schreiben lassen.

Wir unterscheiden nun zwei Fälle, um beide zum Widerspruch zu führen.

Zuerst nehmen wir an, es gäbe ein solches m', sodass $m+m'$ in M' liegt. Dann ist aber $m+m'+(m+m')=0$, im Widerspruch dazu, dass M' 3-linear unabhängig ist.

Es bleibt also nur noch der Fall, dass alle oben genannten $|M'|-1$ Vektoren außerhalb von M' liegen. Dann gilt aber

$$\left|M'\right| - 1 + \left|M'\right| \leq \mathbb{F}_2^n,$$

was aber nicht sein kann, weil M' mehr als halb so groß wie $\mathbb{F}_2^n$ ist. Widerspruch. □

3 Der Fall $k > 3$

Für diesen Fall kenne ich keine allgemeine Formel, aber immerhin eine erste Abschätzung nach unten. Zunächst aber ein erstes Beispiel für eine interessante k-linear unabhängige Menge.

Beispiel 3
Die Vektoren $1000, 0100, 0010, 0001, 1111$ in $\mathbb{F}_2^4$ sind 4-linear unabhängig. Das lässt sich leicht mit einer Fallunterscheidung danach machen, ob die Teilmenge mit höchstens vier Elementen 1111 enthält oder nicht. Besser geht nicht, $x_4(4) = 5$. ◊

Satz 2
Es seien $m, n \in \mathbb{N}$ und $k \in \mathbb{N}$. Dann gilt:

$$x_k(m+n) \geq x_k(m) + x_k(n). \qquad \text{◊}$$

Beweis. Sind $M \subseteq \mathbb{F}_2^m, N \subseteq \mathbb{F}_2^n$ zwei k-linear unabhängige Teilmengen, dann ist

$$\{(w,0),(0,v) \in \mathbb{F}_2^{m+n} \mid w \in M, v \in N\}$$

eine k-linear unabhängige Menge mit $|M|+|N|$ Elementen. □

Satz 3
Es seien $m, n \in \mathbb{N}$, $k \in \mathbb{N}$ und $M \subseteq \mathbb{F}_2^m$ und $N \subseteq \mathbb{F}_2^n$ k-linear unabhängige Teilmengen. Definiere für $v \in N, w \in M$

$$vw \coloneqq \{(v_1 w, v_2 w, \ldots, v_n w) \in \mathbb{F}_2^{mn}.$$

Dann ist MN eine k-linear unabhängige Teilmenge und bezeugt (wenn $|M| = x_k(m)$), dass

$$x_k(mn) \geq x_k(m) x_k(n). \qquad \text{◊}$$

Beweis. Wenn MN nicht k-linear unabhängig wäre, würden sich in MN höchstens k verschiedene Vektoren $v^{(i)}w^{(i)}$ zu Null aufaddieren. Für alle als $w^{(i)}$ vorkommenden $w \in M$ gilt aufgrund der k-linearen Unabhängigkeit von N:

$$\sum_{w^{(j)}=w} v^{(j)}w^{(j)} = \underbrace{\left(\sum_{w^{(j)}=w} v^{(j)}\right)}_{\neq 0} w \neq 0.$$

Für $w = w^{(1)}$ existiert zum Beispiel eine Stelle l mit

$$\sum_{w^{(j)}=w^{(1)}} v_l^{(j)} = 1.$$

Dann gilt für den l-ten m-Bit-Block in $\sum v^{(i)}w^{(i)}$:

$$\sum v_l^{(i)}w^{(i)} = \sum_{w\in M}\left(\sum_{w^{(j)}=w} v_l^{(j)}\right) w = \sum_{w\in A} w,$$

wobei

$$A \coloneqq \left\{ w \in M \mid \sum_{w^{(j)}=w} v_l^{(j)} = 1 \right\}.$$

A enthält mindestens $w^{(1)}$, aber höchstens k verschiedene Elemente. Weil M k-linear unabhängig ist, ist also $\sum_{w\in A} w \neq 0$.

Damit ist gezeigt, dass der l-te m-Bit-Block von $\sum v^{(i)}w^{(i)}$ von 0 verschieden sein muss, und wir folgern, dass MN tatsächlich k-linear unabhängig ist. □

4 Cliquen

Wie schon oben angedeutet wurde, gibt es eine eindeutige maximale k-linear unabhängige Teilmenge von $\mathbb{F}_2^k$. Diese ist gegeben durch eine Basis, zu der man noch die Summe aller Basisvektoren hinzunimmt. Diese Menge hat eine sehr interessante Symmetrieeigenschaft: Jede Permutation dieser $k+1$ Vektoren kann zu einem Vektorraumautomorphismus fortgesetzt werden.

Bemerkung/Definition 1
Für jede Teilmenge $M \subseteq \mathbb{F}_2^n$ mit $k+1$ Elementen ($k \in \mathbb{N}_0$) sind folgende Aussagen äquivalent:

1. M ist eine maximale k-linear unabhängige Teilmenge der k-dimensionalen linearen Hülle $\langle M\rangle$ von M.
2. $\sum M = 0$ und es gibt $m \in M$, sodass $M \setminus \{m\}$ linear unabhängig ist.

3. $\sum M = 0$ und für alle $m \in M$ ist $M \setminus \{m\}$ linear unabhängig.

4. M ist eine minimal linear abhängige Menge.

Eine solche Menge nennen wir $k+1$-Clique, Clique der Größe $k+1$ oder Clique der Dimension k.

Hier ergibt sich eine Analogie zu affinen und projektiven Räumen. So, wie es in einem projektiven Raum vom Auge des Betrachters abhängt, welche Punkte affin sind und welche im Unendlichen liegen, ist hier die Aufteilung von M in eine linear unabhängige Teilmenge und einen zusätzlichen Punkt m willkürlich. ◊

An der letzten Charakterisierung sehen wir etwas weiteres Interessantes. Eine Menge ist genau dann k-linear, wenn sie nur Cliquen einer Dimension größer als k enthält. Außerdem ist eine Menge genau dann linear unabhängig, wenn sie keine Clique enthält.

Die letztere Beobachtung ist interessant, denn sie stellt einen Zusammenhang zwischen der Anzahl an Cliquen (keine) und der Anzahl an Elementen einer linear unabhängigen Menge $M \subseteq \mathbb{F}_2^n$ (entspricht der Dimension von $\langle M \rangle$) her. Außerdem lässt sich jede Menge $M \subseteq \mathbb{F}_2^n$ durch wiederholtes Entfernen eines Punktes in einer beliebigen Clique zu einer linear unabhängigen Menge mit gleicher linearer Hülle verkleinern. Wie viele Punkte müssen wir entfernen? Naja, eben so viele, bis keine Cliquen mehr übrig sind. Vielleicht überschneiden sich einige Cliquen auch, sodass wir durch eine geschickte Auswahl die Zahl der entfernten Punkte manipulieren könnten.

Oder auch nicht, denn andererseits wissen wir, dass wir am Ende immer bei einer linear unabhängigen Menge mit genau $\dim \langle M \rangle$ Elementen ankommen, sodass wir in jedem Fall genau $|M| - \dim \langle M \rangle$ Elemente entfernen werden müssen!

Das ist interessant. Was passiert dann, wenn sich zwei Cliquen überschneiden (das nenne ich verquickte Cliquen)? Die Zahl der zu entfernenden Punkte scheint nämlich sehr wohl davon davon abzuhängen, ob ein Punkt in der Schnittmenge entfernt wird (womit zwei Cliquen mit einer Klappe geschlagen würden) oder jeweils ein Punkt aus jeder Clique, der nicht im Schnitt liegt.

Um zu verstehen, was passiert, hier ein Beispiel.

Beispiel 4
Wir betrachten die Menge $M \subseteq \mathbb{F}_2^5$, die aus zwei verquickten 5-Cliquen besteht:

- 10000, 01000, 00100, 11100 und
- 00001, 00010, 00100, 00111.

Die Cliquen überschneiden sich in 00100.

Wird 00100 aus M entfernt, so bleiben $10000, 01000, 11100, 00111, 00010, 00001$ übrig. Es stellt sich heraus, dass diese sechs Vektoren keineswegs linear unabhängig sind, sondern eine große 6-Clique bilden, die beim Design unserer verquickten 5-Cliquen als Nebenprodukt entstanden ist. ◊

Immer, wenn zwei Cliquen verquickt sind, muss mindestens eine weitere Clique existieren, damit die Zahl der zu entfernenden Punkte von der konkreten Wahl dieser Punkte unabhängig ist.

Ich vermute hier tiefe Einsichten in die Struktur der Cliquen k-linear unabhängiger Mengen. Es gibt viele Fragen, die man anknüpfend an obige Ideen untersuchen könnte:

- (Für welche n) Gibt es 5-linear unabhängige Mengen, die als 4-linear unabhängige Mengen in $\mathbb{F}_2^n$ maximal sind?
- Welche Gesetzmäßigkeiten gelten für den Schnitt von Cliquen?
- Lässt sich aus der Invarianz der Zahl zu entfernender Punkte etwas Interessantes über die Überlagerungsstruktur von Cliquen folgern, ähnlich den Sylowsätzen für Gruppen?
- Welche Kombinationen von Cliquen können in welchen Dimensionen auftreten?
- Wie groß können Teilmengen werden, deren Cliquengröße durch k nach oben statt nach unten eingeschränkt ist?
- ...