Extremal Combinatorics
Seminar Sommersemester 2004

Zeugenmengen und Isolation

Azadeh Nikookhesal
18. Juni 2004

Lehr - und Forschungsgebiet Theoretische Informatik
Prof. Dr. P. Rossmanith
RWTH Aachen

Inhaltsverzeichnis

1 Einleitung **2**

2 Das Theorem von Bondy **2**

2.1 Das Theorem 2

3 Durchschnittliche Zeugenmengen **3**

3.1 Das Theorem 3

4 Das Isolationslemma **5**

4.1 Das Lemma 5

5 Das Diktator-Paradox **6**

5.1 Das Theorem von Arrow 6

1 Einleitung

Gegeben sei eine Menge **A** von verschiedenen 0-1-Vektoren und ein Vektor u in **A**, wie viele Bits von u müssen wir kennen, um ihn von anderen Vektoren in **A** unterscheiden zu können? Eine Menge von solchen Bits heißt *Zeuge* für $u \notin A - \{u\}$. In diesem Kapitel werden wir die Größe solchen Zeugenmengen abschätzen. Wir werden auch das s.g "Diktator-Paradoxon" kennen lernen, welches besagt: In einer demokratischen Gesellschaft existiert immer ein Individuum, das seinen Willen gegen alle anderen durchsetzen wird.

2 Das Theorem von Bondy

Bevor wir das Theorem von Bondy erklären, müssen wir zuerst wissen, was ein Zeuge ist.

Was ist ein Zeuge?

Sei $A \subseteq \{0,1\}^n$ eine Menge von m verschiedenen 0-1-Vektoren der Länge n. Eine Menge $S \subseteq \{1, \cdots, n\}$ von Koordinaten ist ein Zeuge für einen Vektor u in **A**, wenn für jeden anderen $v \in A$ eine Koordinate in S existiert, in der sich u von v unterscheidet. Die minimale Größe eines Zeugen für u in **A** wird mit $w_A(u)$ dargestellt. Es ist offensichtlich, dass $w_A(u) \leq |A| - 1$ für alle A und $u \in A$. Man kann die Korrektheit der o.g. Behauptung an Hand eines einfachen Beispiels zeigen: Wenn A den 0-Vektor 0^n und n Vektoren mit nur einer 1 enthält, dann ist $w_A(0^n) = n$.

Beispiel 2.1 *Sei A wie folgt:*

$$A = \{v_1 = (0,0,1,1), v_2 = (0,1,0,1), v_3 = (1,0,0,0), v_4 = (1,1,1,1)\}$$

Jeder Vektor unterscheidet sich von den anderen Elementen in A an den Koordinaten, die der Zeuge des Vektors angibt. Diese müssen jedoch nicht eindeutig sein. Ein beliebiger Zeuge S_i für den Vektor v_i sieht wie folgt aus:

$$v_1 : S_1 = \{1,2\}$$
$$v_2 : S_2 = \{2,3\}$$
$$v_3 : S_3 = \{4\}$$
$$v_4 : S_4 = \{1,4\}$$

2.1 Das Theorem

Das folgende Ergebnis (Bondy 1972) besagt:
wenn wir nur $m \leq n$ Vektoren haben, dann haben alle Vektoren ein und den selben Zeugen mit einer Größe von höchstens $m - 1$. Die Abbildung von einem Vektor $v = (v_1, \cdots, v_k)$ bezüglich einer Menge von Koordinaten $S = \{i_1, \cdots, i_k\}$ ist der Vektor $v \restriction_s \rightleftharpoons (v_{i_1}, \cdots, v_{i_k})$. Genauso wird auch die Abbildung einer Menge von Vektoren A als $A_{\restriction_s} = \{v \restriction_s : v \in A\}$ dargestellt.

Beispiel 2.2 *Sei A wie folgt:*

$$A = \{v_1 = (0,\boxed{0,1},1), v_2 = (0,\boxed{1,0},1), v_3 = (1,\boxed{0,0},0), v_4 = (1,\boxed{1,1},1)\}$$

Wie man sieht, unterscheiden sich die Vektoren $\{v_1, \cdots, v_4\}$ genau an zwei Koordinaten. Dann sieht der Zeuge für A wie folgt aus:

$$S = \{2,3\}$$

und die Abbildung der Vektoren von A bezüglich S ist die Menge

$$A_{\restriction_s} = \{\underbrace{(0,1)}_{v_1\restriction_s}, (1,0), (0,0), (1,1)\}$$

Theorem 2.1 *(Bondy 1972)*
Es existiert für jede Menge A *von* 0-1*-Vektoren eine Menge* S *mit höchstens* $|A| - 1$ *Koordinaten, so dass alle Vektoren* $\{v_{\restriction_s} : v \in A\}$ *verschieden sind.*

Beweis zum Theorem von Bondy:
Annahme: Sei A ein Gegenbeispiel, dann gilt $|A_{\restriction_s}| < |A|$ für jede Menge S mit höchstens $|A| - 1$ Koordinaten. Sei S eine maximale Menge von Koordinaten für die gilt $|A_{\restriction_s}| \geq |S| + 1$. Da $|A_{\restriction_s}| \leq |A| - 1$, werden mindestens zwei Vektoren $u \neq v \in A$ in S übereinstimmen. Wähle eine Koordinate $i \notin S$, in der sich diese zwei Vektoren unterscheiden, und eine Menge $T \rightleftharpoons S \bigcup \{i\}$. Da die Vektoren u,v in S übereinstimmen, aber sich in T unterscheiden, gilt, dass die Abbildung $A_{\restriction_T}$ mindestens einen Vektor mehr als $A_{\restriction_s}$ hat. Dann gilt:

$$|A_{\restriction_T}| \geq |A_{\restriction_s}| + 1 \geq |S| + 2 = |T| + 1$$

Dies ist ein Widerspruch zur maximalen Größe von S.

□

3 Durchschnittliche Zeugenmengen

Da im worst - case die Größe der Zeugenmengen gleich n ist, ist es sinnvoll, sich eine durchschnittliche Größe für die Zeugenmenge zu überlegen:

$$w_{ave}(A) \rightleftharpoons \frac{1}{|A|} \sum_{u \in A} w_a(u) \tag{1}$$

Dasselbe Beispiel wie im letzten Abschnitt zeigt, dass die Differenz zwischen den worst-case und den average-case des Gewichts der Zeugenmengen groß ist: Sei A eine Menge von $n + 1$ Vektoren mit höchstens einer 1, dann ist $w_{ave}(A) = \frac{2n}{(n+1)} \leq 2$. Die $2n$ ergeben sich aus den n 1-Vektoren (Vektoren die nur eine 1 haben), bei denen nur eine Koordinate als Zeuge ausreicht, und dem 0-Vektor, bei dem alle n Koordinate benötigt werden.

3.1 Das Theorem

Wie groß kann $w_{ave}(A)$ als eine Funktion von $|A|$ sein?

Theorem 3.1 *(Kushilevitz, Linial, Rabinovitch und Saks (1996))*
Es gilt, dass für jede Menge A von m 0-1 Vektoren $w_{ave}(A) \leq 2m^{1/2}$ *ist. Für unendlich viele m existiert andererseits eine Menge A von m* 0-1*-Vektoren, so dass* $w_{ave}(A) \geq \frac{1}{2\sqrt{2}} m^{1/2}$.

Beweis zum Theorem 3.1:
Der Beweis zu diesem Theorem besteht aus 2 Teilen, nämlich dem Beweis für die obere Schranke und dem Beweis für die untere Schranke. Hier führen wir nur den Beweis für die obere Schranke.
Obere Schranke:
Sei A eine beliebige Menge von m Vektoren. Ordne die Vektoren $u_1, u_2, \cdots, u_m$ nach abnehmender kleinster Zeugengröße: $w(u_1) \geq w(u_2) \geq \cdots \geq w(u_m)$. Betrachte die Summe der ersten k größten Werte, $\sum_{i=1}^{k} w(u_i)$. Finde eine Menge T mit höchstens $k-1$ Koordinaten laut *Bondys Theorem* (Theorem 2.1), angewendet auf die Menge $\{u_1, \cdots, u_k\}$, und stelle die T - Koordinaten in alle Vektoren von A fest. Mit der Eigenschaft von T sind die Vektoren $u_1, \cdots, u_k$ bereits verschieden. Die T-Koordinaten von jedem Vektor u_j mit $j > k$ unterscheidet u_j von allen $u_1, \cdots, u_k$ bis auf einem Vektor u_i, weil keine zwei Vektoren $u_1, \cdots, u_k$ in T übereinstimmen. Man kann u_i um ein weiteres Bit erweitern, um u_i von u_j unterscheiden zu können. Wendet man diesen Schritt für jeden u_j mit $j > k$, dann ist jeder Vektor aus $u_1, \cdots, u_k$ unterscheidbar von jedem anderen Vektor in A. Man benötigt für den letzten Schritt $m-k$ zusätzliche Bits, so dass folgt:

$$\sum_{i=1}^{k} w(u_i) \leq k(k-1) + m - k = k^2 - 2k + m \tag{2}$$

Wir wissen, dass $w(u_k)$ unter den Gewichten $w(u_1), \cdots, w(u_k)$ minimal ist, weil $w(u_1) \geq w(u_2) \geq \cdots \geq w(u_m)$. Daher gilt:

$$(\sum_{i=1}^{k} w(u_i) \geq k w(u_k)) \leq k^2 - 2k + m \tag{3}$$

und mittels Division durch k auf beiden Seiten der Ungleichung ergibt sich:

$$w(u_k) \leq k - 2 + m/k \tag{4}$$

Aus den Formeln (2) und (4) erhält man:

$$\sum_{i=1}^{m} w(u_i) = \sum_{i=1}^{k} w(u_i) + \sum_{i=k+1}^{m} w(u_i) \leq (k^2 - 2k + m) + \underbrace{(m-k)}_{a} \underbrace{(k - 2 + \frac{m}{k})}_{b} \tag{5}$$

a: Anzahl der übrig gebliebenen Vektoren aus A
b: Da für alle andere Vektoren gilt: $w(u_k) \geq w(u_{k+1}) \geq \cdots \geq w(u_m)$

Setze in der Ungleichung (5) $k = m^{1/2}$:

$$\sum_{i=1}^{m} w(u_i) \leq 2m^{3/2}$$

und aus Formel (1) ergibt sich:

$$w_{ave}(A) \leq 2m^{1/2}$$

□

4 Das Isolationslemma

Bei einer Menge von n Punkten $\mathbf{X}$ sei $\mathcal{F}$ eine Familie von Teilmengen von $\mathbf{X}$. Über die Funktion $w(x)$ wird jedem Punkt $x \in X$ ein Gewicht zugeordnet. Das Gewicht einer Teilmenge E ist definiert durch $w(E) = \sum_{x \in E} w(x)$. Die Funktion w ist isolierend für $\mathcal{F}$, wenn nur eine einzige Teilmenge existiert, die das minimale Gewicht besitzt. Unabhängig davon, wie unsere Familie $\mathcal{F}$ gewählt wurde, kann eine zufällig gewählte Funktion w mit sehr großer Wahrscheinlichkeit *isolierend* für $\boldsymbol{F}$ sein.

4.1 Das Lemma

Lemma 4.1 *(Mulmulex,Vazirani (1987))*
Sei $\mathcal{F}$ eine Familie von Teilmengen von einer n-elementigen Menge X. *Sei $w : X \rightarrow \{1, \cdots, N\}$ eine zufällig ausgewählte Funktion, die gleichmäßig über den Definitionsbereich verteilt ist. Dann gilt:*

$$Prob(w \text{ ist isolierend für } \mathcal{F}) \geq 1 - \frac{n}{N}$$

Beweis zu dem Lemma *(Spencer(1995))*
Setze für einen Punkt $x \in X$,

$$\alpha(x) = \min_{E \in F; x \notin E} w(E) - \min_{E \in F; x \in E} w(E - \{x\}) \tag{6}$$

Da $w(x)$ gleichmäßig über die Menge $\{1, \cdots, N\}$ gewählt wurde, ist $\alpha(x)$ von $w(x)$ unabhängig.

$$Prob(w(x) = \alpha(x)) \leq 1/N \tag{7}$$

(weil $\alpha(x)$ beliebigen Wert, auch $\geq N$, haben kann.)

Da wir wissen wollen, ob ein x existiert, für das $w(x) = \alpha(x)$ gilt, müssen wir die Menge $\mathcal{X}$ für jeden x überprüfen(falls $\mathcal{X}$ n Elementen hat, dann n-mal überprüfen). Also ergibt sich: $n \cdot \frac{1}{N}$:

$$Prob(w(x) = \alpha(x) \text{ für ein beliebiges } x \in X) \leq n/N \tag{8}$$

$$n \cdot (Prob(w(x) = \alpha(x)) \leq 1/N)$$

Die Wahrscheinlichkeit, dass w isolierend ist, ist:

$$Prob(w \text{ isolierend}) = 1 - Prob(w \text{ nicht isolierend}) \tag{9}$$

w ist nicht isolierend, wenn: $\exists A, B \in \mathcal{F} : w(A) = w(B) = \min w(E), E \in \mathcal{F}$ (d.h. wenn zwei Mengen mit minimalem Gewicht existieren).
Um zu zeigen, dass w nicht isolierend ist, wählen wir zwei minimale Mengen $A, B \in F$, so dass $x \in A - B$. Dann gilt:

$$\min_{E \in F; x \notin E} w(E) = w(B) \tag{10}$$

$$\min_{E \in F; x \in E} w(E - \{x\}) = w(A) - w(x) \tag{11}$$

Setzt man (10) und (11) in die Formel (6) ein, erhält man das Ergebnis $w(x) = \alpha(x)$. Wenn w nicht isolierend für $\boldsymbol{F}$ ist, dann ist also $w(x) = \alpha(x)$ für ein beliebiges $x \in X$. Es ist bereits bekannt, dass $w(x) = \alpha(x)$ mit einer Wahrscheinlichkeit von höchstens n/N auftreten kann.

5 Das Diktator-Paradox

Zum Erläutern des Diktator-Paradox betrachten wir als praktisches Beispiel ein Referendum. Sei $I = 1, \cdots, n$ eine Gesellschaft aus n Individuen. Sie haben die Möglichkeit Präferenzordnungen, über eine Menge $\mathcal{X}$ von Optionene, anzugeben. Wir gehen davon aus, dass jedes Individuum i eine Rangliste für die Optionen erstellt. Dies kann man beschreiben als eine totale Ordnung $<_i$ auf X für jedes $i \in I$, wobei $x <_i y$ bedeutet, dass das Individuum i die Option y der Option x vorzieht. Also erhalten wir eine Menge $R = \{<_1, \cdots, <_n\}$ von totalen Ordnungen $<$ auf X. Eine "social choice function" **F** hat als Eingabe eine Menge von solchen totalen Ordnungen und gibt eine "soziale Präferenz" auf X aus. Totale Ordnung heißt: wenn $x < y$ und $y < z$, dann folgt $x < z$.
Nun führen wir den Begriff des Diktators $(i_0 \in I)$ ein. Bei jedem Referendum stimmt seine Präferenz mit dem Ergebnis der sozialen Präferenz überein. Das bedeutet, dass für jede gegebene Menge von totalen Ordnungen $R = \{<_1, \cdots, <_n\}$ die soziale Wahlfunktion die Ordnung $<_{i_0}$ ausgibt, unabhängig davon, welche Präferenzen $<_i$ die anderen Individuen $i \neq i_0$ angeben.

5.1 Das Theorem von Arrow

Das Theorem von Arrow besagt, dass es unter bestimmten Umständen immer einen Diktator gibt. Dazu muss die Wahlfunktion F drei " Demokratie-Axiome" erfüllen. Diese drei Axiome lauten:

(A1) Wenn $x < y$ (in der sozialen Präferenz), dann bleibt diese Aussage wahr, falls die individuellen Präferenzen zu Gunsten y's verändert werden.

(A2) Sei $Y \subseteq X$ eine Menge von Optionen und gegeben, dass zwischen zwei Wahlen keine individuellen Veränderungen in Y stattfinden, dann wird die Gesellschaft ihre Präferenzen innerhalb von Y ebenfalls nicht ändern.

(A3) Für alle verschiedenen Optionen $x, y \in X$ gibt es ein System von individuellen Präferenzen, für die die zugehörige soziale Präferenz $x < y$ erfüllt. Es sollte für eine Gesellschaft möglich sein die Option*y* der Option x vorzuziehen, wenn dies genügend Individuen tun.

Theorem 5.1 *(Theorem von Arrow)*
Für $|X| \geq 3$ *und jede* social choice function, *welche die drei "Demokratie- Axiome" erfüllt, existiert ein Diktator.*

Beweis zum Theorem *(Cameron 1994)*
Sei (x, y) ein geordnetes Paar von verschiedenen Optionen. Wir nennen eine Menge J von Individuen (x, y)-bestimmend, wenn gilt:

$$x <_j y, \forall j \in J \Rightarrow x < y \text{ (soziale Ordnung)}$$

Außerdem bezeichnen wir J als **bestimmend**, wenn es (x, y)-bestimmend für irgendwelche $x, y \in X$ ist. Sei J eine minimal bestimmende Menge. Aus den Axiomen (A1) - (A3) folgt, dass für alle verschiedenen Optionen $x, y \in X$ und jedes Individuum zieht y vor x so gilt auch, dass $x < y$ in der sozialen Ordnung sind. Also ist $J \neq \emptyset$. sei nun J (x, y) - bestimmend und sei $I_0 \in J$

Behauptung 1 $J = \{i_0\}$
Um die Behauptung zu zeigen, nehmen wir das Gegenteil an. Dazu sei $J' \rightleftharpoons J - i_0$ *und* $K \rightleftharpoons I - J$. *Sei v eine Option in X, die sich von x und y unterscheidet (*$|X \geq 3|$*). Betrachten wir nun die individuellen Präferenzen* $<_i$, $i \in I$, *für die gilt:*

$$x <_{i_0} y <_{i_0} v$$
$$v <_i x <_i y, \forall i \in J'$$
$$y <_j v <_j x, \forall j \in K$$

Dann ist $x < y$, *da dies bei allen Elementen der* (x, y)*-bestimmenden Menge* J *zutrifft. Außerdem gilt* $y < v$, *denn wenn* $v < y$ *gelten würde, dann wäre* J' (v, y)*-bestimmend. Dies widerspricht der Minimalität von J. Daher ist* $x < v$. *Aber dann ist* i_0 (x, v)*-bestimmend, da ansonsten niemand mit dieser Ordnung übereinstimmt. Da J minimal sein soll, erhalten wir* $J = \{i_0\}$.

Behauptung 2 i_0 *ist ein Diktator.*
Wir müssen beweisen, dass $\{i_0\}$ (u, v)*-bestimmend ist für alle Paare von unterschiedlichen Optionen* $u \neq v$. *Der Fall* $u = x$ *ist bereits in obiger Behauptung (Behauptung1) behandelt worden, so dass nur noch zwei Möglichkeiten übrig bleiben:*

1. Fall $u \neq x$ *und* $v \neq x$.
Wir betrachten die individuellen Präferenzen mit:

$$u <_{i_0} x <_{i_0} v$$
$$v <_j u <_j x, \forall j \neq i_0$$

Dann ist $u < x$ *(da es bei allen zutrifft),* $x < v$ *(da es bei* i_0 *zutrifft und* i_0 (x, v)*-bestimmend ist, für alle* $v \neq x$ *). Also ist* $u < v$ *, und* i_0 *ist* (u, v)*-bestimmend, da diese Ordnung sonst bei keinem Element zutrifft.*

2. Fall $v = x$
Wähle $z \notin \{u, x\}$, *und betrachte die individuellen Präferenzen, in denen gilt:*

$$u <_{i_0} z <_{i_0} x$$
$$z <_j x <_j u, \forall j \neq i_0$$

Dann ist $u < z$ *(da dies bei* i_0 *gilt und* u, z *sich von x unterscheiden) und* $z < x$ *(da es bei allen zutrifft). Also ist* $u < x$ *und* i_0 *ist* (u, x)*-bestimmend.*

□