Über die Rivest-Vuillemin Vermutung

Diplomarbeit, August 1985
Universität Stuttgart
Nebenfach Informatik

Betreuer : Dr. Ulrich Hedtstück
Prüfer : Prof. Dr. W. Schwabhäuser
vorgelegt von: Carl - Heinz Barner

INHALTSANGABE

Nach den einleitenden Definitionen und dem Satz 1 über die even-odd-ballance (der das Hilfsmittel ist, um in den späteren Sätzen zu zeigen, daß eine Boolsche Funktion erschöpfend ist) sowie dem Satz 2 von Rivest und Vuillemin werden die Begriffe Periode und Abstandsfolge eingeführt (diese werden gebraucht um später die even-odd-ballance $P^1(-1)$ zu berechnen). Danach wird durch das Gegenbeispiel von Illies die verallgemeinerte Aanderaa-Rosenberg Vermutung widerlegt. Dann wird der Beweis von Theorem 4.10. in [RV] durch ein Gegenbeispiel als nicht korrekt dargestellt. Satz 4 und Satz 5 sind Abschwächungen von Theorem 4.10., wobei Satz 3 für die Beweise von Satz 4 und Satz 5 verwendet wird. Außerdem gibt Satz 3, ähnlich wie Satz 2, hinreichende Bedingungen dafür, daß eine Boolsche Funktion erschöpfend ist, an. Satz 6 ist eine Modifikation von Theorem 4.10..
Danach werden andere Gegenbeispiele zur Aanderaa-Rosenberg Vermutung gesucht, indem versucht wird, das Gegenbeispiel von Illies auf verschiedene Arten zu verallgemeinern.
Im Ausblick wird die Grenze des Hilfsmittels "even-odd-ballance" untersucht.

EINLEITUNG

Ein gegebener Graph G läßt sich auf verschiedene Arten beschreiben, z.B. durch die Adjazenzmatrix, oder dadurch, daß man zu jedem Knoten des Graphen G alle seine benachbarten Knoten angibt. Dadurch läßt sich auch eine Eigenschaft eines Graphen durch verschiedene Arten beschreiben.
Ein fundamentales Problem der Theoretischen Informatik besteht darin, die relative Leistungsfähigkeit von verschiedenen Datenstrukturen zu bestimmen.
Z.B. haben Hopcroft und Tarjan in [HT] erwähnt, daß man $\Omega(v^2)$ Operationen benötigt, aus der Adjazenzmatrix eines Graphen mit v Knoten Planarität bzw. Nichtplanarität zu bestimmen.
Auf ähnliche Weise haben Holt und Reingold in [HR] gezeigt, daß man im schlimmsten Fall $\Omega(v^2-1)/4$ Operationen benötigt, aus der Adjazenzmatrix eines gerichteten Graphen G die Eigenschaft "G enthält einen Kreis bzw. G enthält keinen Kreis" zu bestimmen.
Durch diese Resultate motiviert, vermutete Arnold Rosenberg in [RO] : ob eine beliebige Grapheigenschaft (wobei Graphen als Adjazenzmatrix dargestellt werden) zutrifft oder nicht, wird im schlimmsten Fall von $\Omega(v^2)$ Operationen bestimmt.
Aanderaa widerlegte diese Vermutung, indem er zeigte, daß weniger als 3v Operationen benötigt werden um zu bestimmmen ob ein gerichteter Graph mit v Knoten eine "Senke" enthält.
Aanderaa schlug vor, daß die Grapheigenschaften "monoton" sein sollten, d.h.: wenn die Eigenschaften für einen Graphen $G=(V,E)$ gilt, muß sie auch für alle Graphen $G'=(V,E')$ mit $E \subset E'$ gelten.
Dies schließt das Gegenbeispiel mit der Senke aus und führt zur
Aanderaa - Rosenberg Vermutung (siehe [RO]):
Im schlimmsten Fall sind $\Omega(v^2)$ Operationen nötig, um aus der Adjazenzmatrix eines Graphen G zu bestimmmen, ob der Graph G eine Eigenschaft P hat, die

1) nichttrivial
2) monoton
3) unabhängig von der Numerierung der Knoten
4) unabhängig von der Existenz von "Schlingen" ist

Beim Beweis der Aanderaa - Rosenberg Vermutung wird die folgende Behauptung benutzt:

Behauptung.
P sei eine transitive, d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, d Primzahlpotenz. Dann ist P erschöpfend.

Diese Behauptung motiviert die folgende

Verallgemeinerte Aanderaa – Rosenberg Vermutung:
Sei P eine transitive d-stellige Boolsche Funktion mit
$P(0) \neq P(1)$, d natürliche Zahl.
Dann ist P erschöpfend.

DEFINITIONEN

Eine d-stellige Boolsche Funktion P ist eine Abbildung $P: \{0,1\}^d \longrightarrow \{0,1\}$ $(d \in N_0)$. Wir setzen immer voraus, daß der Definitionsbereich von P die gesamte Menge $\{0,1\}^d$ ist, d.h. P ist für jedes der 2^d d-tupel aus $\{0,1\}^d$ definiert. Die Elemente aus $\{0,1\}^d$ fassen wir als d-bit Vektoren (falls im Kontext klar, sagt man kurz Vektoren) auf. Falls die Stellenzahl d klar ist, bezeichnen wir den Nullvektor $(0,\ldots,0)$ mit 0 und den Einsvektor $(1,\ldots,1)$ mit 1.
Ein d-bit Vektor x heißt Wahr-Vektor von P, falls $P(x)=1$
und Falsch-Vektor von P, falls $P(x)=0$.
Das Gewicht $w(x)$ eines Vektors x ist die Anzahl der Einsen in x.
Die Menge $\sum_d$ aller Permutationen auf $\{1,\ldots,d\}$ bildet eine Gruppe, bzgl. der Hintereinanderausführung, die sogenannte symmetrische Gruppe. Die Untergruppen der symmetrischen Gruppe heißen Permutationsgruppen.
Unter einem Zyklus der Länge K versteht man eine Permutation $(i_1,\ldots,i_k)$, die i_1 nach i_2, i_2 nach $i_3,\ldots,i_{k-1}$ nach i_k, i_k nach i_1 abbildet.
Eine Untergruppe Γ von $\sum_d$ heißt k-fach transitiv, $(1 \le k \le d)$, wenn es zu je zwei geordneten k-tupeln $(i_1,\ldots,i_k)$ und $(j_1,\ldots j_k)$ von Zahlen aus $\{1,\ldots,d\}$ mit $i_\nu \neq i_\mu, j_\nu \neq j_\mu$ für $\nu \neq \mu$ eine Permutation $\sigma \in G$ existiert mit $\sigma(i_\nu)=j_\nu$ für $\nu=1,\ldots,k$.
Eine Untergruppe Γ von $\sum_d$ heißt transitiv, wenn Γ 1-fach transitiv ist.
Ersetzt man bei der Definition von k-fach transitiv "existiert" durch "existiert genau ein", dann spricht man von scharf k-fach transitiv.
Sei G Untergruppe von $\sum_d$. $St_G(i) := \{\sigma \in G \mid \sigma(i)=i\}$.
Ist $St_G(i)=1$ für alle $i \in \{1,\ldots,d\}$, dann heißt G semiregulär

Eine Untergruppe G von $\sum_d$ heißt regulär, wenn G transitiv und semiregulär ist.
Bemerkung:
Ist G Untergruppe von $\sum_d$, dann gilt:
G ist scharf einfach transitiv genau dann wenn G regulär ist.
Sei P eine d-stellige Boolsche Funktion.
Für $x=(x_1,\ldots,x_d) \in \{0,1\}^d$ und $\sigma \in \sum_d$
sei $\sigma(x) := (x_{\sigma(1)},\ldots,x_{\sigma(n)})$.
Die Menge
$\Gamma(P) := \{\sigma \in \sum_d \mid$ für alle $x \in \{0,1\}^d$ gilt $P(x)=P(\sigma(x))\}$
heißt Stabilisator von P.
Sei G Untergruppe von $\sum_d$ und x ein d-bit Vektor, dann heißt $xG := \{\sigma(x) \mid \sigma \in G\}$ die Bahn von x unter G.
Eine d-stellige Boolsche Funktion P heißt
k-fach transitiv, falls $\Gamma(P)$ k-fach transitiv ist.

$P^1(z) := \sum_{0 \le i \le d} w_i(P) \cdot z^i$ ist der Aufzähler einer d-stelligen Boolschen Funktion P, wobei $W_i(P) = \{x \in \{0,1\}^d \mid P(x)=1 \text{ und } w(x)=i\}$, $w_i(P) := |W_i(P)|$. Wenn es im Kontext klar ist, schreibt man w_i statt $w_i(P)$ bzw. W_i statt $W_i(P)$.

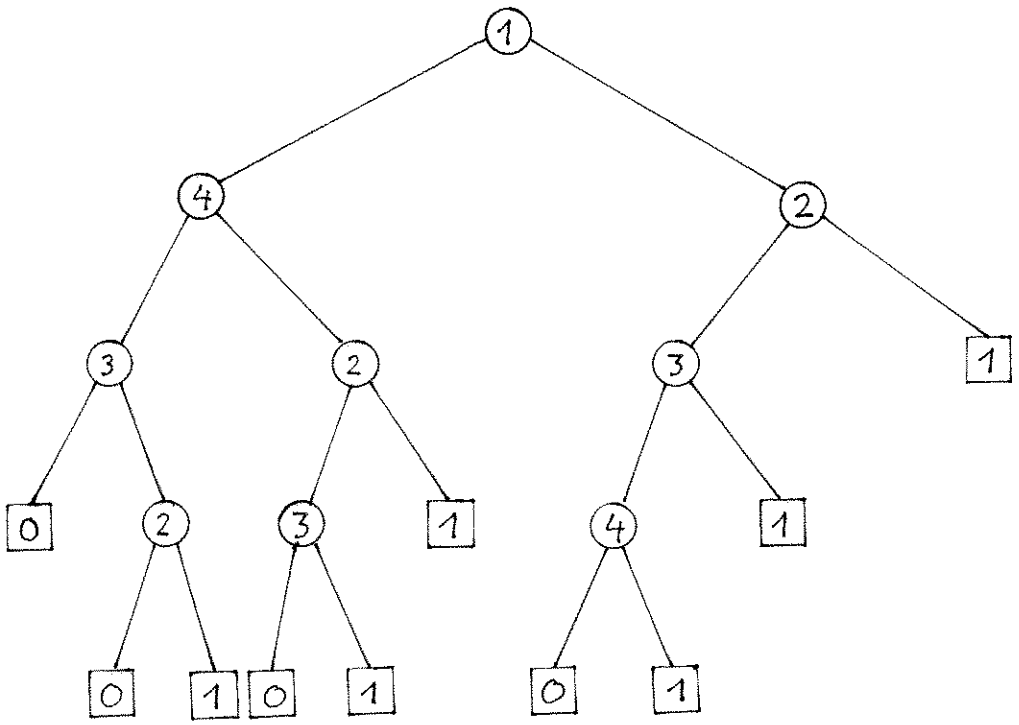
Bemerkung.

$$P^1(-1) = \sum_{\substack{i \text{ gerade} \\ 0 \le i \le d}} w_i - \sum_{\substack{i \text{ ungerade} \\ 0 \le i \le d}} w_i$$

Ein geordneter Baum ist ein (gerichteter) Baum, in dem für jeden Knoten die Menge der Söhne geordnet ist. Ein geordneter Binärbaum ist ein geordneter Baum, in dem jeder Sohn eines Knotens entweder als linker Sohn oder als rechter Sohn ausgezeichnet ist, und in dem jeder Knoten höchstens einen linken und einen rechten Sohn hat.
Der vom linken Sohn eines Knotens K in einem geordneten Binärbaum aufgespannte Unterbaum heißt, falls er überhaupt existiert, der linke Unterbaum von K, entsprechend definiert man den rechten Unterbaum von K.
In einem gerichteten Baum heißt ein Knoten, der mindestens einen Sohn hat, innerer Knoten, ein Knoten, der keinen Sohn hat, heißt Blatt.
Die Höhe eines gerichteten Baums ist die Länge eines längsten Pfades von der Wurzel zu einem Blatt (d.h. die Anzahl der Kanten auf diesem Pfad). Die Tiefe eines Knotens K in einem gerichteten Baum ist die Länge des Pfades von der Wurzel zu K.
Ein geordneter Binärbaum T heißt vollständig, wenn jeder innere Knoten von T zwei Söhne hat und wenn jeder Pfad von der Wurzel zu einem Blatt die Länge h hat, wobei h die Höhe von T ist.
Ein Entscheidungsbaum ist ein geordneter Binärbaum, dessen innere Knoten mit natürlichen Zahlen 1,2,... markiert sind und jeweils genau zwei Söhne haben, und dessen Blätter mit 0 oder 1 markiert sind, so daß auf jedem Pfad von der Wurzel zu einem Blatt jede der Zahlen 1,2,... höchstens einmal als Markierung eines inneren Knotens vorkommt. (Üblicherweise werden Entscheidungsbäume allgemeiner definiert, doch genügt für unsere Betrachtungen diese spezielle Sorte.)
Wenn alle Markierungen der inneren Knoten eines Entscheidungsbaums T aus der Menge $\{1,\dots,n\}$ sind, so bestimmt jeder Vektor $v=(v_1,\dots,v_n) \in \{0,1\}^n$ eindeutig einen Pfad P in T von der Wurzel zu einem Blatt in folgender Weise: Ist n=0, d.h. der Baum besteht nur aus einem Blatt, das zugleich die Wurzel ist, so gibt es nur einen Pfad. Sei $n \ge 1$ und sei i_1 die Markierung der Wurzel. Wähle als nächsten Knoten den linken Sohn, falls $v_{i_1}=0$, andernfalls den rechten Sohn. Ist man bei

einem inneren Knoten mit Markierung i_v angelangt, so wähle wiederum den linken Sohn, falls $v_{i_v}=0$, andernfalls den rechten Sohn. Liegen auf P insgesamt k innere Knoten ($0 \leq k \leq n$), so repräsentiert P (bzw. das zu P gehörende Blatt) auf diese Weise genau 2^{n-k} Vektoren.
Sei T ein Entscheidungsbaum, dessen innere Knoten mit Zahlen aus $\{1,\ldots,n\}$ markiert sind und f eine n-stellige Boolsche Funktion. T berechnet f oder T ist ein Entscheidungsbaum für f, falls für jedes Blatt L in T und die entsprechende Markierung m(L) gilt: Wird ein Vektor v von L repräsentiert, so ist $f(v)=m(L)$. (Dabei ist f durch n und T eindeutig bestimmt.)
Sei f eine n-stellige Boolsche Funktion. Für einen Entscheidungsbaum T für f und einen Vektor $v=(v_1,\ldots,v_n)$ mit $v \in \{0,1\}^n$ sei $c(T,v)$ die Anzahl der Komponenten v_i von v, die T benötigt, um f(v) zu berechnen, m.a.W., $c(T,v)$ ist die Länge des zu v gehörenden Pfades. Sei $c(T):=\max\{c(T,v) \mid v \in \{0,1\}^n\}$, d.h. die Höhe von T. Dann heißt
$C(f):=\min\{c(T) \mid T \text{ ist ein Entscheidunsbaum für } f\}$
die Argumentkomplexität von f. Ist $C(f)=n$, so nennen wir f erschöpfend

Beispiel:
Sei f die 4-stellige Boolsche Funktion mit $f(v)=1$ gdw. $w(v) \geq 2$. Die folgende Abbildung zeigt einen Entscheidungsbaum für f. Die inneren Knoten sind als Kreise gezeichnet, die Blätter als Quadrate. Die Markierungen sind in die Kreise bzw. Quadrate hineingeschrieben.



Satz 1. (even-odd-ballance)
Sei P eine d-stellige Boolsche Funktion, die nicht erschöpfend ist. Dann ist die Anzahl der Wahr-Vektoren von P mit geradem Gewicht gleich der Anzahl der Wahr-Vektoren mit ungeradem Gewicht.

Beweis.
Wenn P nicht erschöpfend ist, so gibt es einen vollständigen Entscheidungsbaum T für P der Höhe d-1. Da jedes Blatt in T genau zwei Vektoren repräsentiert, die denselben Funktionswert haben und deren Gewicht sich um Eins unterscheidet, gilt die Behauptung.

q.e.d.

Bemerkung.
Satz 1. gilt auch entsprechend für die Falsch-Vektoren von P.

Satz 2 (Rivest, Vuillemin).
Sei P eine transitive d-stellige Boolsche Funktion mit $P(0)\neq P(1)$, wobei d eine Primzahlpotenz $d=p^{\alpha}$ ist ($\alpha \in N$).
Dann ist P erschöpfend.

Beweis.
Der Stabilisator $\Gamma(P)$ operiert auf $\{0,1\}^n$ durch $\sigma(v)=(v_{\sigma(1)},\ldots,v_{\sigma(d)})$. Sei $v\Gamma(P)$ die Bahn von v unter $\Gamma(P)$. Es gilt $w(u)=w(v)$ für alle $u\in v\Gamma(P)$. Sei $b_i(v) := |\{u\in v\Gamma(P) \mid u_i=1\}|$, $i=1,\ldots,n$.
Da $\Gamma(P)$ nach Voraussetzung transitiv ist, ist $b_i(v)$ unabhängig von i, wir können also die Bezeichnung b(v) ohne Index verwenden. Schreibt man die Vektoren aus $v\Gamma(P)$ untereinander, dann erhält man durch zwei verschiedene Zählweisen der Einsen in der so entstandenen Matrix die Gleichung.
$w(v)\cdot|v\Gamma(P)| = p^{\alpha} b(v)$.
Dann ist entweder $w(v)=p^{\alpha}$ (d.h. v=1) oder w(v)=0 (d.h. v=0) oder p ist ein Teiler von $|v\Gamma(P)|$.
Wir betrachten nun die Wahr-Vektoren von P. Da alle Bahnen eine Mächtigkeit haben, die durch p teilbar ist, außer den Bahnen $\{0\}$ und $\{1\}$, und da nur einer der beiden Vektoren 0 und 1 ein Wahr-Vektor von P ist, gilt für die Anzahlen G(P) bzw. U(P) der Wahr-Vektoren von P mit geradem bzw. ungeradem Gewicht die Beziehung $G(P) \neq U(P) \pmod p$. Dann ist aber P nach Satz 1 erschöpfend.

Definitionen.

$\sigma = (m_1, \ldots, m_d)$, $C_d := \langle \sigma \rangle$ sei die durch den Zyklus $\sigma = (m_1, \ldots, m_d)$ erzeugte zyklische Gruppe.
$p > 0$ heißt eine Periode des d-bit Vektors x bzgl. C_d genau dann wenn gilt: $\sigma^p(x) = x$

$p_m(x)$ heißt kleinste Periode des d-bit Vektors x bzgl. C_d genau dann wenn gilt:
1) $p_m(x)$ ist Periode von x bzgl. C_d
2) für jede Periode p bzgl. C_d gilt: $p_m(x) \leq p$

Bemerkungen.

1) Falls es im Kontext klar ist läßt man bzgl. C_d oft weg

2) $C_d(x) := \{ \sigma^k(x) \mid k \in N_0 \}$

3) p sei Periode von x bzgl. C_d. Dann gilt
$\sigma^{q \cdot p + r}(x) = \sigma^r(x) \quad q, r \in N_0$
denn
$$\sigma^{q \cdot p + r}(x) = \underbrace{\sigma^p(\sigma^p(\ldots\sigma^p}_{q\text{-mal}}(\sigma^r(x))\ldots) = \sigma^r(x)$$

Behauptung 1.
$\sigma = (m_1, \ldots, m_d)$, $C_d = \langle \sigma \rangle$
Sei x ein d-bit Vektor.
Dann gilt:
$p_m(x) = |C_d(x)|$

Beweis.

1) $C_d(x) = \{ \sigma^k(x) \mid k \in N_0 \}$
$= \{ \sigma^{q \cdot p_m(x) + r}(x) \quad q \in N_0, \quad 0 \leq r < p_m(x) \}$
$= \{ \sigma^r(x) \mid 0 \leq r < p_m(x) \}$

2) Seien $0 \leq r_1 < p_m(x)$, $0 \leq r_2 < p_m(x)$, $r_1 \geq r_2$, $\sigma^{r_1}(x) = \sigma^{r_2}(x)$ dann ist $\sigma^{r_1 - r_2}(x) = x$. Daraus folgt $r_1 = r_2$.
Wäre nämlich $r_1 - r_2 > 0$, dann wäre $r_1 - r_2$ Periode von x und $r_1 - r_2 < p_m(x)$. Widerspruch!

Behauptung 2.
$\sigma=(m_1,\ldots,m_d)$, $C_d=<\sigma>$.
p ist Periode des d-Tupels x bzgl. C_d
genau dann wenn gilt:

$$x_{m_{i\oplus p}} = x_{m_i} \text{ für alle } i \in \{1,\ldots,d\}$$

wobei die Abbildung " $\oplus$ " wie folgt definiert ist:
$\oplus : \{1,\ldots,d\} \times N \longrightarrow \{1,\ldots,d\}$ und
$k \oplus j=r :\Longleftrightarrow k+j=c\cdot d+r$ und $1\leq r\leq d$

Bemerkung.
$(\{1,\ldots,d\}, \oplus)$ bildet ein Gruppe mit der obigen Verknüpfung " $\oplus$ ", die auf $\{1,\ldots,d\} \times \{1,\ldots,d\}$ eingeschränkt ist.
" $\oplus$ " ist dann die Addition auf dem Restklassengruppe mod d.
Im folgenden wird "+" statt " $\oplus$ " geschrieben.

Beweis.
trivial

Behauptung 3.
Für jede natürliche Zahl p gilt:
p ist eine Periode eines d-bit Vektors x bzgl. $C_d=<\sigma>$
$\sigma=(m_1,\ldots,m_d)$ genau dann wenn gilt: $p_m(x) \mid p$

Beweis.
Für alle $p \in N$ existieren $q,r \in N_0$ mit $p=q\cdot p_m(x)+r$ und $0 \leq r<p_m(x)$. p ist eine Periode eines d-bit Vektors x bzgl. C_d gdw $\sigma^{p}(x)=x$ gdw $\sigma^{q\cdot p_m(x)+r}(x)=x$ gdw $\sigma^{r}(x)=x$ gdw $r=0$ gdw $p_m(x) \mid p$ q.e.d.

Da später bei Illies von Abständen die Rede ist, muß dieser Begriff präzisiert werden. Im weiteren kann man mit diesen Abständen die even-odd-ballance $P^1(-1)$ berechnen.

Definition.
Sei $\{i_1,\ldots,i_k\} \subset \{1,\ldots,d\}$, dann bezeichnet $[i_1,\ldots,i_k]$ den d-bit Vektor $(x_1,\ldots,x_d)$
wobei $x_i=1$ gdw $i \in \{i_1,\ldots,i_k\}$, und $i_1<i_2<\ldots<i_k$

Definition.
Die Folge $(a_1,a_2,\ldots,a_k)$ eines d-bit Vektors $x=[i_1,\ldots,i_k]$ heißt Abstandsfolge von x genau dann wenn gilt:
$a_1=i_2-i_1,\ldots,a_{k-1}=i_k-i_{k-1}$, $a_k=i_1-i_k$,
wobei " − " die Subtraktion auf der Restklassengruppe mod d bedeutet.
Beachte: $i_j=i_1+a_1+\ldots+a_{j-1}$ $1\leq j\leq k$

Behauptung 4.
Seien $C_d=\langle(1,2,\ldots,d)\rangle$ und $(a_1,\ldots,a_k)$ die Abstandsfolge eines d-bit Vektors $x=[i_1,\ldots,i_k]$.
Dann gilt: $p_m(x)\in\{a_1,a_1+a_2,\ldots,a_1+\ldots+a_k\}$

Beweis.
Da d Periode von x ist gilt: $1\leq p_m(x)\leq d$
(Man kann sich also nach der vorigen Bemerkung auf die Addition " + " auf der Restklassengruppe mod d beschränken.)
$x_{i_1}=1$. Dann gilt $x_{i_1+p_m(x)}=1$.
Also existiert ein $j\in N$ mit $1\leq j\leq k$ und $i_1+p_m(x)=i_j$.
Dann gilt: $p_m(x)=i_j-i_1=a_1+\ldots+a_{j-1}$,
also $p_m(x)\in\{a_1,\ldots,a_1+a_2+\ldots+a_{k-1}\}$ oder
$p_m(x)=0$ (d.h. $p_m(x)=d$)
(d ist das Nullelement auf der Restklassengruppe mod d)

Behauptung 5.
I)
Seien genau k−1 Abstände der Abstandsfolge $(a_1,\ldots,a_k)$ eines d-bit Vektors $x=[i_1,\ldots,i_k]$ gleich a und ein davon verschiedener Abstand gleich b.
Dann gilt: $p_m(x)=d=(k-1)a+b$

II)
Wenn alle Abstände einer Abstandsfolge $(a_1,\ldots,a_k)$ eines d-bit Vektors $x=[i_1,\ldots,i_k]$ gleich a sind,
dann gilt: $p_m(x)=a$

In I) und II) bezieht sich $p_m(x)$ auf $C_d=\langle(1,\ldots,d)\rangle$

Beweis.
I)
Da d Periode von x ist, gilt: $1\leq p_m(x)\leq d$
(Man kann sich also nach der vorigen Bemerkung auf die Addition " + " auf der Restklassengruppe mod d beschränken.)

Es gilt:
$i_{f\oplus 1}-i_f=b$
$i_{f\oplus 1\oplus j}=i_{f\oplus 1}+j\cdot a \quad 0\leq j<k,$
wobei " $\oplus$ " Addition auf Restklassengruppe mod k,
" + " Addition auf Restklassengruppe mod d ist.
Im weiteren wird zwischen " $\oplus$ " und " + " nicht unterschieden.
Mit Behauptung 5 folgt: $p_m(x)=c\cdot a+b,\ (0\leq c<k)$
oder $p_m(x)=c\cdot a\ (1\leq c<k)$
wäre $p_m(x)<d$, dann gibt es für $p_m(x)$ zwei Fallunterscheidungen.

1. Fall:
$p_m(x)=c\cdot a+b \quad 0\leq c\leq k-2$
definiere $i_j:=i_f-(c+1)a$
es gilt: $i_j\in\{i_1,\ldots,i_k\}$,
denn $i_f=i_{f+1-1}=i_{f+1+k-1}=i_{f+1}+(k-1)a$
(Beachte daß das Inverse von 1 gleich k-1 ist.)
Also $i_j=i_f-(c+1)a=i_{f+1}+(k-1)a-(c+1)a=i_{f+1}+(k-2-c)a$
$=i_{f+1+k-2-c} \quad (0\leq k-2-c<k)$
Es gilt:
$i_j+p_m(x)=i_{f+1}+(k-2-c)a+c\cdot a+b=i_{f+1}+(k-2)\cdot a+b$
Angenommen es existiere ein $i_r\in\{i_1,\ldots,i_k\}$ mit
$i_r=i_j+p_m(x)$, dann ist
$i_r=i_{f+1}+(k-2)a+b$
andererseits ist:
$i_r=i_{f+1}+r\cdot a \quad 0\leq r\leq k-1$
also:
$i_{f+1}+r\cdot a=i_{f+1}+(k-2)a+b$ also
$(k-2-r)a+b=0=(k-1)a+b$ (d ist Nullelement), also
$(1+r)a=0=(k-1)a+b$
wäre $r\leq k-2$, also $1+r\leq k-1$, also $(1+r)a\leq(k-1)a$ also
$(1+r)a<(k-1)a+b$ Widerspruch!
wäre $r=k-1$, also $r+1=k$, also $k\cdot a=(k-1)a+b$ also
$b=a$ Widerspruch!
Damit gilt nun: $i_r\notin\{i_1,\ldots,i_k\}$, also $x_{i_j+p_m(x)}=0\neq 1=x_{i_j}$
Also $x_{i_j+p_m(x)}\neq x_{i_j}$. Also ist $p_m(x)$ keine Periode von x. Widerspruch!

2. Fall:
$p_m(x)=c\cdot a \quad 1\leq c\leq k-1$
definiere $i_j:=i_f-(c-1)a$
es gilt: $i_j\in\{i_1,\ldots,i_k\}$
denn: $i_j=i_f-(c-1)a=i_{f+1}+(k-1)a-(c-1)a=i_{f+1}+(k-c)a$
$=i_{f+1+k-c} \quad (1\leq k-c\leq k-1)$
Es gilt:
$i_j+p_m(x)=i_{f+1}+(k-c)a+c\cdot a=i_{f+1}+k\cdot a$
Angenommen es existiert ein $i_r\in\{i_1,\ldots,i_k\}$
mit $i_r=i_j+p_m(x)$, dann ist $i_r=i_{f+1}+k\cdot a$
aber andererseits:
$i_r=i_{f+1}+r\cdot a \quad 0\leq r\leq k-1$
also:
$i_{f+1}+k\cdot a=i_{f+1}+r\cdot a$ also
$k\cdot a=r\cdot a$ also

$(k-r)a=0=(k-1)a+b$
wäre $r\geq 1$, also $k-r\leq k-1$, also $(k-r)a\leq(k-1)a$ also
$(k-r)a<(k-1)a+b$ Widerspruch!
wäre $r=0$, also $k\cdot a=0$, also $k\cdot a=(k-1)a+b$ also
$a=b$ Widerspruch!
Damit gilt nun: $i_r \notin \{i_1,\ldots,i_k\}$ also $x_{i_j+P_m(x)}=0\neq 1=x_{i_j}$
q.e.d.

Definition.
Ein d-bit Vektor x enthält genau n Einsen im Abstand a genau dann wenn für die Abstandsfolge $(a_1,\ldots,a_n)$ von x gilt:
es existiert ein $i\in N$ mit $1\leq i\leq k$ und
$a_i=a_{i+1}=\ldots=a_{i+n-2}=a$, wobei
" + " Addition auf der Restklassengruppe mod n bedeutet.

Rivest und Vuillemin verallgemeinerten die Aanderaa-Rosenberg Vermutung wie folgt:

Verallgemeinerte Aanderaa-Rosenberg Vermutung:
Sei P eine transitive, d-stellige Boolsche Funktion mit $P(0)\neq P(1)$, $d\in N$.
Dann ist P erschöpfend.

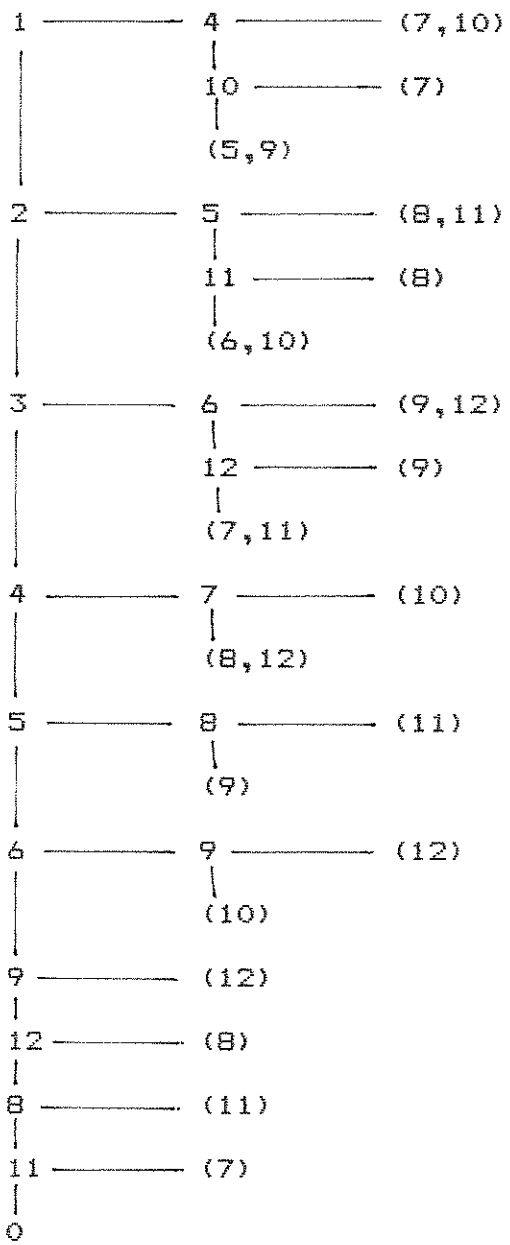
Satz 2. sagt aus, daß diese Vermutung gilt, falls d Primzahlpotenz ist. Der allgemeine Fall wurde aber widerlegt durch das

Gegenbeispiel von Illies
$C_{12}=\langle(1,2,\ldots,12)\rangle$ heißt die von dem Zyklus $(1,2,\ldots,12)$ der Länge 12 erzeugte zyklische Gruppe der Ordnung 12.
Die 12-stellige Boolsche Funktion P sei definiert durch:
$$P^{-1}(1):=\{0\}\cup C_{12}[1]\cup C_{12}[1,4]\cup C_{12}[1,5]\cup C_{12}[1,4,7]\cup C_{12}[1,5,9]\cup C_{12}[1,4,7,10]$$

anders ausgedrückt:
$P(x)=1$ genau dann wenn eine der folgenden Bedingungen erfüllt ist:
1) $x=0$
2) x enthält genau eine Eins
3) x enthält genau zwei Einsen im Abstand 3 oder 4
4) x enthält genau drei Einsen im Abstand 3 oder 4
5) x enthält genau vier Einsen im Abstand 3

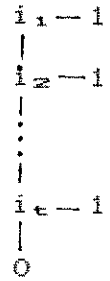
$\Gamma(P)$ ist transitiv, denn $C_{12}\subset\Gamma(P)$,
außerdem gilt: $P(0)\neq P(1)$

Der Entscheidungsbaum T von Illies in abgeändeter systematischer Form:



Ein geklammertes Blatt $(j_1,\ldots,j_m)$ ist die Abkürzung für den Entscheidungsbaum (E):
wobei
$\{i_1,\ldots,i_t\} = \{i \in \{1,\ldots,d\} \mid i \neq j_1,\ldots,j_m;$
i ist keine Markierung auf dem Pfad von der Wurzel zum geklammerten Blatt $(j_1,\ldots,j_m)\}$

(E):



Zuerst ist es notwendig, die später in Theorem 4.10. ungenau formalisierte, angegebene Menge E präzise zu definieren.
Man kann E auf zwei verschiedene aber äquivalente Weisen charakterisieren.

Definition A.
$d \in E$ genau dann wenn eine Folge $d_1,\ldots,d_n=d$ existiert, so daß für alle $i \in N$ mit $1 \leq i \leq n$ gilt:
a.) $d_i=1$ oder
b.) es existiert ein $k \in N$ und eine Primzahl q, so daß:
$d_i=d_{i-1} \cdot q^k$ und $q > 2^{d_{i-1}-1}$

Bemerkung. $d_i \in E$ für $1 \leq i \leq n$

Definition B.
$F \in \mathfrak{E}$ genau dann wenn die folgenden zwei Bedingungen erfüllt sind:
1.) $1 \in F$
2.) aus $n \in F$, q Primzahl, $q > 2^{n-1}$ folgt $n \cdot q^k \in F$, $k \in N$

$\bar{E} := \bigcap_{F \in \mathfrak{E}} F$

Behauptung 6.
$\bar{E}=E$ (d.h. Def.A und Def.B sind äquivalent)

Beweis.

I.) Zeige für alle $F \in \mathfrak{E}$ gilt: $E \subset F$
(d.h. $\bigcap_{F \in \mathfrak{E}} F \supset E$)
$d_1,\ldots,d_n=d$ sei Folge für $d \in E$
Zeige: (mittels vollständiger Induktion)
für alle $j \in N$ mit $j \leq n$ gilt: $d_j \in F$
Ind. Anfang: $d_1=1 \in F$
Ind. Vorauss.: $d_{i-1} \in F$
Fall 1: $d_i=1$ also $d_i \in F$
Fall 2: es existiert ein $k \in N$ und eine Primzahl q
mit: $d_i=\underbrace{d_{i-1}}_{\in F} \cdot q^k$ und $q > 2^{d_{i-1}-1}$ also $d_i \in F$

II.) Zeige $E \in \mathfrak{E}$ (d.h. $\overbrace{F \in \mathfrak{E}}^{\text{}} \; F \subset E$)

Es gilt: $1 \in E$
sei $n \in E$, q Primzahl, $q > 2^{n-1}$
zeige: $n \cdot q^k \in E$ für alle $k \in N$
Da $n \in E$ ist $n_1, \ldots, n_r = n$ Folge für n
$n_1, n_2, \ldots, n_r, n_{r+1}$ mit $n_r = n$, $n_{r+1} = n \cdot q^k$
ist Folge für $n \cdot q^k$
denn:
$n_{r+1} = n_r \cdot q^k$ und $q > 2^{n-1}$ und für alle n_i $(1 \leq i \leq r)$ gilt: Bed. 1.) oder Bed. 2.) Glieder von Def.B. Also $n \cdot q^k \in E$. q.e.d.

In verschiedenen folgenden Beweisen wird die "Induktion über den Aufbau von E" benötigt.

Behauptung 7.
Um zu zeigen, daß für alle $d \in E$ gilt: $\mathfrak{Y}(d)$, genügt es die "Induktion über den Aufbau von E" zu zeigen:
1.) $\mathfrak{Y}(1)$
2.) aus $\mathfrak{Y}(n)$, $n \in E$, q Primzahl, $q > 2^{n-1}$ folgt: für alle $k \in N$ gilt: $\mathfrak{Y}(n \cdot q^k)$

Beweis.
$d_1, \ldots, d_n = d$ sei Folge für d
Zeige: (mittels vollständiger Induktion)
für alle $j \in N$ mit $j \leq n$ gilt: $\mathfrak{Y}(d_j)$
i.) $\mathfrak{Y}(d_1) = \mathfrak{Y}(1)$
ii.) Es gelte: $\mathfrak{Y}(d_{i-1})$
a.) es existiert ein $k \in N$ und eine Primzahl q mit: $d_i = \underbrace{d_{i-1}}_{\in E} \cdot q^k$ und $q > 2^{d_{i-1}-1}$, also $\mathfrak{Y}(d_i)$
b.) $d_i = 1$ also $\mathfrak{Y}(d_i) = \mathfrak{Y}(1)$ q.e.d.

Im folgenden wird das Theorem 4.10. mit Beweis dargestellt. (vgl. [RV]). Danach wird mit einem Gegenbeispiel gezeigt, daß der Beweis nicht korrekt ist. Danach wird das Theorem 4.10. in abgeschwächter Form korrekt bewiesen.

Theorem 4.10.
E ist die kleinste Menge von natürlichen Zahlen, so daß gilt:
a) $1 \in E$
b) aus $n \in E$, q Primzahl, $q > 2^{n-1}$ folgt $n \cdot q^k \in E$ für alle $k \in N$.

P sei eine transitive, abelsche, d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in E$.
Dann ist P erschöpfend.

Beweis. (Induktion über den Aufbau von E)
Um dieses Theorem zu zeigen genügt es nach dem Satz über die even-odd-ballance (Satz 1) folgendes zu zeigen:
P sei eine transitive, abelsche, d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in E$.
Dann gilt: $P^1(-1) \neq 0$

Nun zur Induktion über E:
$\mathfrak{H}(n) :\Longleftrightarrow$
Für jede transitive, abelsche, n-stellige Boolsche Funktion R mit $R(0) \neq R(1)$ gilt: $R^1(-1) \neq 0$

$\mathfrak{H}(1)$: denn aus $R(0) \neq R(1)$ folgt $R^1(-1) \neq 0$
Gelte $\mathfrak{H}(n)$, $n \in E$, q Primzahl, $q > 2^{n-1}$
Zeige: $\mathfrak{H}(n \cdot q^k)$, $k \in N$, $(d := n \cdot q^k)$
Aus $\Gamma(P)$ abelsch und transitiv folgt $|\Gamma(P)| = d$. ← siehe [RV]
Da aus $q > 2^{n-1} \geq n$ folgt: $q > n$, gilt $q \nmid n$
Nach einem Sylowschen Satz existiert also eine Untergruppe Θ der Ordnung q^k.
Da $\Gamma(P)$ abelsch ist, ist dies die einzige Untergruppe der Ordnung q^k.
(denn: Wäre Θ' Untergruppe der Ordnung q^k, dann wäre nach einem Sylowschen Satz Θ und Θ' konjugiert, also würde ein $a \in \Gamma(P)$ existieren mit
$a \cdot \Theta = \Theta' \cdot a = a\,\Theta'$ also $\Theta' = \Theta$)

Definition.
$\Theta(i) := \{\vartheta(i) \mid \vartheta \in \Theta\}$, $i \in \{1, \ldots, d\}$ heißt das von der Untergruppe Θ von Σ_d erzeugte Transitivitätsgebiet.

Behauptung 8.
Das Mengensystem $\{\Theta(i) \mid i \in \{1, \ldots, d\}\}$ ist eine Klasseneinteilung von $\{1, \ldots, d\}$, wobei das Mengensystem aus n Transitivitätsgebieten der Ordnung q^k besteht.

Beweis.
Zeige: aus $\Theta(i) \cap \Theta(j) \neq \emptyset$ folgt $\Theta(i) = \Theta(j)$
sei $\vartheta_1(i) = \vartheta_2(j)$ $\vartheta_1, \vartheta_2 \in \Theta$ also $i = \vartheta_1^{-1} \cdot \vartheta_2(j)$
dann gilt für beliebiges ϑ_3 :
$\vartheta_3(i) = \vartheta_3(\vartheta_1^{-1} \cdot \vartheta_2(j)) = \vartheta_3 \cdot \vartheta_1^{-1} \cdot \vartheta_2(j) \in \Theta(j)$
also gilt: $\Theta(i) \subset \Theta(j)$; analog gilt: $\Theta(j) \subset \Theta(i)$

Zeige: $\bigcup_{i \in \{1,\ldots,d\}} \Theta(i) = \{1,\ldots,d\}$

sei $j \in \{1,\ldots,d\}$.
$j = id(j) \in \Theta(j) \subset \bigcup_{i \in \{1,\ldots,d\}} \Theta(i)$ q.e.d.

Durch die Klasseneinteilung von $M := \{1,\ldots,d\}$ wird eine Äquivalenzrelation auf M erklärt.
$i \sim j$ genau dann wenn ein Transitivitätsgebiet $T \in \{\Theta(i) \mid i \in \{1,\ldots,d\}\}$ existiert mit $i \in T$ und $j \in T$.

Bemerkung.
$i \sim j$ genau dann wenn ein $\sigma \in \Theta$ existiert mit $\sigma(i) = j$

Behauptung 9.
Wenn $q \nmid |x\,\Gamma(P)|$ dann gilt:
aus $i \sim j$ folgt $x_i = x_j$, wobei
$x\,\Gamma(P) := \{\sigma(x) \mid \sigma \in \Gamma(P)\}$

Beweis.
Es gilt: $|x\,\Gamma(P)| = |\Gamma(P)| / |Aut(x)|$
wobei $Aut(x) := \{\vartheta \in \Gamma(P) \mid \vartheta(x) = x\}$ Untergruppe
siehe dazu [RV]
Sei nun $q \nmid |x\,\Gamma(P)|$. Dann gilt: $\Theta \subset Aut(x)$
(denn: aus $|x\,\Gamma(P)| = n \cdot q^k / |Aut(x)|$
folgt $|Aut(x)| = m \cdot q^k$ und $m \mid n$
da $m \mid n$ gilt, folgt $m \leq n < q$ also $q > m$ also $q \nmid m$.
Also besitzt Aut(x) eine Untergruppe Θ der Ordnung q^k. Da $\Gamma(P)$ genau eine Untergruppe der Ordnung q^k besitzt, muß Θ' identisch Θ sein. Also: $\Theta \subset Aut(x)$.
Sei nun $i \sim j$, also existiert ein $\sigma \in \Theta$ mit $\sigma(i) = j$.
Wegen $\Theta \in Aut(x)$ gilt: $x_i = x_{\sigma(i)} = x_j$,
also $x_i = x_j$ q.e.d.

Weil $\ominus$ Normalteiler ($\Gamma(P)$ abelsch) existiert die Faktorgruppe $\Gamma(P)/\ominus$ mit:
$\Gamma(P)/\ominus$ abelsch ($\Gamma(P)$ abelsch)
$\Gamma(p)/\ominus$ transitiv ($\Gamma(P)$ transitiv)

Definiere die n-stellige Boolsche Funktion Q:
$Q(y_1,y_2,\ldots,y_n) := P(x_1,\ldots,x_n)$,
wobei alle Variablen x_j im i-ten Transitivitätsgebiet identisch y_i sind.

Es gilt: $\Gamma(Q) \cong \Gamma(P)/\ominus$

Bemerkung.
Diese Aussage ist im allgemeinen falsch. Siehe dazu später ein Gegenbeispiel.

Mit dem obigen Isomorphismus folgt sofort, daß $\Gamma(Q)$ abelsch und transitiv ist.
Außerdem folgt $Q(0) \neq Q(1)$ $(Q(0)=P(0) \neq P(1)=Q(1))$
Mit Hilfe der Induktionsvoraussetzung $\mathcal{Y}(n)$
folgt $Q^1(-1) \neq 0$

Behauptung 10.
$|Q^1(-1)| \leq 2^{n-1}$

Beweis.
$W_i(Q) := \{x \mid Q(x)=1 \text{ und } w(x)=i\} \subset \{x \mid w(x)=i\}$
$w_i(Q) = |W_i(Q)| \leq \binom{n}{i}$

$$\text{also } 0 \leq \sum_{\substack{i \text{ gerade} \\ 0 \leq i \leq n}} w_i(Q) \leq \sum_{\substack{i \text{ gerade} \\ 0 \leq i \leq n}} \binom{n}{i} = 2^{n-1}$$

$$\text{genauso } 0 \leq \sum_{\substack{i \text{ ungerade} \\ 0 \leq i \leq n}} w_i(Q) \leq \sum_{\substack{i \text{ ungerade} \\ 0 \leq i \leq n}} \binom{n}{i} = 2^{n-1}$$

$$\text{also: } |Q^1(-1)| = \left| \sum_{\substack{i \text{ gerade} \\ 0 \leq i \leq n}} w_i(Q) - \sum_{\substack{i \text{ ungerade} \\ 0 \leq i \leq n}} w_i(Q) \right| \leq 2^{n-1}$$

q.e.d.

Behauptung 11.
$P^1(-1)=Q^1(-1) \mod q$ siehe [RV]
das heißt: $P^1(-1)/q$ und $Q^1(-1)/q$ haben den gleichen Rest

Damit gilt nun:
$0 \neq |Q^1(-1)| \leq 2^{n-1} < q$, also $q \nmid Q^1(-1)$
also hat $P^1(-1)/q$ einen Rest, folglich gilt: $P^1(-1) \neq 0$
q.e.d.

Das im folgenden angegebene Gegenbeispiel zu der Behauptung $\Gamma(Q) \cong \Gamma(P)/\ominus$ zeigt daß $\Gamma(Q)$ im allgemeinen nicht abelsch zu sein braucht. Damit kann aber nicht mehr mit der Induktionvoraussetzung $\mathfrak{A}(n)$ auf $Q^1(-1) \neq 0$ geschlossen werden. Da aber im Beweis die Induktionsvoraussetzung $\mathfrak{A}(n)$ und die Behauptung $\Gamma(Q)$ abelsch und transitiv dazu benutzt werden um auf $Q^1(-1) \neq 0$ zu schließen ($Q^1(-1) \neq 0$ wird im Beweis auch benötigt), sehe ich bei Beibehaltung der Definition der Abbildung Q keine Möglichkeit den Beweis zu reparieren.

Gegenbeispiel zu Behauptung $\Gamma(Q) \cong \Gamma(P)/\ominus$

a)
$d=15 \in E$, denn aus $n=3 \in E$, $q^k=5^1$, 5 Primzahl, $3 \in E$, $5>2^{3-1}$ folgt $15 \in E$.
Definiere nun die 15-stellige Boolsche Funktion P wie folgt
$P^{-1}(1) := C_{15}[1,2] \cup C_{15}[1,2,4,7] \cup C_{15}[1,4,7,10,13] \cup \{0\}$
wobei $C_{15} := \langle (1,2,3,\ldots,15) \rangle$ die durch den Zyklus $(1,2,3,\ldots,15)$ erzeugte zyklische Gruppe ist.
Die 15-bit Vektoren mit Funktionswert 1 sind also:

I)	II)	III)
110000000000000	110100100000000	100100100100100
011000000000000	011010010000000	010010010010010
001100000000000	001101001000000	001001001001001
000110000000000	000110100100000	
000011000000000	000011010010000	
000001100000000	000001101001000	
000000110000000	000000110100100	
000000011000000	000000011010010	
000000001100000	000000001101001	
000000000110000	100000000110100	VI)
000000000011000	010000000011010	
000000000001100	001000000001101	000000000000000
000000000000110	100100000000110	
000000000000011	010010000000011	
100000000000001	101001000000001	

Behauptung 12.
Die Permutation $\sigma \in \Gamma(P)$ hat die Form (1) oder (2)

$$\begin{pmatrix} \ldots,i-1,i,i+1,\ldots \\ \ldots,3,\ 2,\ 1,\ 15,14,\ldots \end{pmatrix} \qquad (1) \quad \text{oder}$$

$$\begin{pmatrix} \ldots,i-1,i,i+1,\ldots \\ \ldots,14,\ 15,1,\ 2\ ,3,\ldots \end{pmatrix} \qquad (2)$$

dies folgt aus folgenden Überlegungen:

Behauptung 13.
Sei $\sigma \in \Gamma(P)$. Dann gilt:
aus $\sigma(j)=i$ folgt $\sigma(j-1)=i+1$ oder $\sigma(j+1)=i+1$

Beweis.
Sei $\sigma(j-1)\neq i+1$ und $\sigma(j+1)\neq i+1$
definiere x so, daß: $x_i=1$, $x_{i+1}=1$,
$x_k=0$ für $k \notin \{i,i+1\}$
Dann gilt: $P(x)=1$
es gilt weiter: $\sigma(x)=(\ldots,x_{\sigma(j-1)},x_{\sigma(j)},x_{\sigma(j+1)},\ldots)$
$=(\ldots,x_{\sigma(j-1)},1,x_{\sigma(j+1)},\ldots) = (\ldots,0,1,0,\ldots)$.
Also $P(\sigma(x))=0\neq i=P(x)$, also $\sigma \notin \Gamma(P)$
q.e.d.

Behauptung 14.
Voraussetzung: $\sigma \in \Gamma(P)$
Dann gilt:
(1) aus $\sigma(j)=i$ und $\sigma(j+1)=i+1$ folgt $\sigma(j+2)=i+2$
(2) aus $\sigma(j)=i$ und $\sigma(j-1)=i+1$ folgt $\sigma(j-2)=i+2$

Beweis.
(1) Sei $\sigma(j+1)=i+1$. Dann folgt mit Beh 13
$\sigma(j+2)=i+2$ oder $\sigma(j)=i+2$;
da $\sigma(j)=i$ folgt $\sigma(j)\neq i+2$ also $\sigma(j+2)=i+2$

(2) Sei $\sigma(j-1)=i+1$. Dann folgt mit Beh 13
$\sigma(j-2)=i+2$ oder $\sigma(j)=i+2$;
da $\sigma(j)=i$ folgt $\sigma(j)\neq i+2$ also $\sigma(j-2)=i+2$
q.e.d.

Behauptung 15.
Für jede Permutation $\sigma \in \sum_d$ gilt:
es existiert ein $k \in N$ mit $\sigma(k)=1$ und $1 \leq k \leq d$

Dann hat man nun:
Da $\sigma(k)=1$ folgt mit Behauptung 13. A) oder B)
A): $\sigma(k+1)=2$
Mit Behauptung 14. gilt: $\sigma(k+2)=3$.
Mit Behauptung 14. gilt: $\sigma(k+3)=4$ u.s.w.

B) $\sigma(k-1)=2$
Mit Behauptung 14. gilt: $\sigma(k-2)=3$.
Mit Behauptung 14. gilt: $\sigma(k-3)=4$ u.s.w.

definiere:
$\gamma_i := \begin{pmatrix} \dots,i,\dots \\ \dots,3,2,1,15,14,\dots \end{pmatrix}$, $y=(1101001000000000)$

Behauptung 16.
$\gamma_i \notin \Gamma(P)$

Beweis.
Da $\gamma_i(y) \notin \Pi)$ gilt: $P(\gamma_i(y))=0 \neq 1=P(y)$ q.e.d.

Damit gilt: $\Gamma(P)=C_{15}$ (abelsch, transitiv)

b)
C_{15} enthält genau eine Untergruppe $\ominus$ der Ordnung 5.
Dies muß die zyklische Gruppe

$$C_5=\left\langle \begin{pmatrix} 1,2,3,4,\dots,15 \\ 4,5,6,7,\dots,3 \end{pmatrix} \right\rangle$$

oder ausführlich:

$$C_5=\left\{ \begin{pmatrix} 1,2,3,4,\dots,15 \\ 1,2,3,4,\dots,15 \end{pmatrix}, \begin{pmatrix} 1,2,3,4,\dots,15 \\ 4,5,6,\dots \end{pmatrix}, \begin{pmatrix} 1,2,3,4,\dots,15 \\ 7,8,9,\dots \end{pmatrix}, \begin{pmatrix} 1, 2, 3,\dots,15 \\ 10,11,12,\dots \end{pmatrix}, \begin{pmatrix} 1, 2, 3,\dots,15 \\ 13,14,15,\dots \end{pmatrix} \right\}$$

Bestimmung der Transitivitätsgebiete:

$T_1=\{1,4,7,10,13\}$ $T_2=\{2,5,8,11,14\}$ $T_3=\{3,6,9,12,15\}$

Definition von Q

Q(000):=P(0000000000000000)=1
Q(001):=P(0010010010010010)=1
Q(010):=P(0100100100100100)=1
Q(011):=P(0110110110110110)=0
Q(100):=P(1001001001001001)=1
Q(101):=P(1011011011011011)=0
Q(110):=P(1101101101101101)=0
Q(111):=P(1111111111111111)=0

3 stellige Vektoren mit Funktionswert 1:
(000) (001) (010) (100)

3 stellige Vektoren mit Funktionswert 0:
(011) (101) (110) (111)

Daraus folgt: $\Gamma(Q)=\sum_3$ (symmetrische Gruppe vom Grad 3)

Da $|\Gamma(Q)| = 6$ und $|\Gamma(P)|/|\Theta| = 15/5 = 3$
folgt $\Gamma(Q) \not\subseteq \Gamma(P)/\Theta$

Bemerkung.
Da $\sum_n$ für $n \geq 3$ nichtabelsch ist, gilt:
$\Gamma(Q)$ nichtabelsch

Satz 3.
Sei P eine d-stellige Boolsche Funktion mit $\Gamma(P) \supset C_d$, $C_d = \langle (m_1, \ldots, m_d) \rangle$, $P(0) \neq P(1)$, $d \in E$.
Dann ist P erschöpfend.

Beweis. (Induktion über den Aufbau von E)
Um Satz 3 zu zeigen, genügt es nach dem Satz über die even-odd-ballance (Satz 1) folgendes zu zeigen:
Sei P eine d-stellige Boolsche Funktion mit $\Gamma(P) \supset C_d$, $C_d = \langle (m_1, \ldots, m_d) \rangle$, $P(0) \neq P(1)$, $d \in E$. Dann gilt: $P^1(-1) \neq 0$
Nun zur Induktion über E:

$\mathcal{Y}(n) :\Longleftrightarrow$
$Q: \{0,1\}^n \longrightarrow \{0,1\}$ n-stellige Boolsche Funktion,
$\Gamma(Q) \supset C_n$, $C_n := \langle (r_1, \ldots, r_n) \rangle$, $Q(0) \neq Q(1) \Longrightarrow Q^1(-1) \neq 0$

Es gilt: $\mathcal{Y}(1)$ (denn aus $Q(0) \neq Q(1)$ folgt $Q^1(-1) \neq 0$)
Es gelte: $\mathcal{Y}(n)$, $n \in E$, q Primzahl, $q > 2^{n-1}$
zeige: $\mathcal{Y}(n \cdot q^k)$, $k \in N$, $(d := n \cdot q^k)$

Es genügt zu zeigen:
aus $\mathcal{Y}(n)$, $n \in E$, q Primzahl, $q > 2^{n-1}$, $q > 2$ folgt:
$\mathcal{Y}(n \cdot q^k)$ für $k \in N$

denn:
1. Fall:
$n=1 \Longrightarrow q > 2^{1-1}=1$ zeige $\mathcal{Y}(q^k)$ für $k \in N$. Dies gilt nach Satz 2
2. Fall:
$n>1 \Longrightarrow q > 2^{2-1}=2 \Longrightarrow q>2$. Zeige $\mathcal{Y}(n \cdot q^k)$ für $q>2$, $k \in N$

Behauptung 17.
Sei $\sigma = (m_1, \ldots, m_d)$, $C_d = \langle \sigma \rangle$ und $C_d \subset \Gamma(P)$. Dann gilt:

1) $$\bigsqcup_{\substack{j \text{ gerade} \\ 0 \le j \le d}} W_j(P) = \bigsqcup_{\{x \mid P(x)=1 \text{ und } w(x) \text{ gerade}\}} C_d(x)$$

2) $$\bigsqcup_{\substack{j \text{ ungerade} \\ 0 \le j \le d}} W_j(P) = \bigsqcup_{\{x \mid P(x)=1 \text{ und } w(x) \text{ ungerade}\}} C_d(x)$$

Beweis. (zu 1))
$z \in$ L.S.:
es existiert j gerade und $0 \le j \le d$ mit $w(z)=j$
und $P(z)=1$. Es gilt: $z \in C_d(z)$

$z \in$ R.S.:
es existieren $x \in R := \{x \mid P(x)=1 \text{ und } w(x) \text{ gerade}\}$,
und $k \in N$ mit $z = \sigma^k(x)$. Es gilt:
$w(z)=w(\sigma^k(x))=w(x)=j$ (gerade), $P(z)=P(\sigma^k(x))=P(x)=1$
q.e.d.

Behauptung 18.
Seien $\sigma = (m_1, \ldots, m_d)$, $C_d = \langle \sigma \rangle$, und $Z_n = \{z \in \{0,1\}^d \mid \sigma^n(z)=z\}$
die Menge der d-bit Vektoren mit Periode n bzgl. C_d,
$Z_n' := \{0,1\}^n$
Dann wird Z_n durch die folgende Abbildung φ bijektiv auf Z_n' abgebildet.
$\varphi : Z_n \to Z_n'$ mit $\varphi(z_1, \ldots, z_d) := (z_{m_1}, \ldots, z_{m_n})$
und $(z_1, \ldots, z_d)' := \varphi(z_1, \ldots, z_d)$

Beweis.
injektiv:
seien $z=(z_1,\dots,z_d)$, $\bar{z}=(\bar{z}_1,\dots,\bar{z}_d)$ Vektoren mit $z\neq\bar{z}$
Dann existiert ein $i\in\{1,\dots,d\}$ mit $z_i\neq\bar{z}_i$
Da $(m_1,\dots m_d)$ Permutation ist, existiert ein $j\in\{1,\dots,d\}$ mit $i=m_j$, also $z_{m_j}\neq\bar{z}_{m_j}$
Es gilt: für alle $j\in N$ existieren $c,r\in N_0$ mit $j=c\cdot n+r$ und $0\leq r\leq n$. Dann ist:
$z_{m_j}=z_{m_{c\cdot n+r}}=z_{m_r}$ und $\bar{z}_{m_j}=\bar{z}_{m_{c\cdot n+r}}=\bar{z}_{m_r}$ also gilt:
$z_{m_r}\neq\bar{z}_{m_r}$ also $z'\neq\bar{z}'$

surjektiv:
sei $x=(x_1,\dots,x_n)\in\{0,1\}^n$

$z_{m_1}:=x_1,\quad z_{m_2}:=x_2,\quad\dots,\quad z_{m_n}:=x_n$
$z_{m_{n+1}}:=x_1,\quad z_{m_{n+2}}:=x_2,\quad\dots,\quad z_{m_{2n}}:=x_n$

$z_{m_{(q^k-1)n+1}}:=x_1,\quad z_{m_{(q^k-1)n+2}}:=x_2,\quad\dots,\quad z_{m_{n\cdot q^k}}:=x_n$

damit: $z_{m_1}=z_{m_{n+1}}=\dots=z_{m_{(q^k-1)n+1}}$
$z_{m_2}=z_{m_{n+2}}=\dots=z_{m_{(q^k-1)n+2}}$

$z_{m_n}=z_{m_{2n}}=\dots=z_{m_{n\cdot q^k}}$

damit: $\sigma^n(z)=z$, also $z\in Z_n$ q.e.d.

Definiere die Abbildung:
$P':Z_n'\longrightarrow\{0,1\}$ mit $P'(z')=P(z)$

Behauptung 19.
Wenn
$\sigma=(m_1,\dots,m_d)$, $\gamma=(m_1,\dots,m_n)$, $C_d=\langle\sigma\rangle$, $C_n=\langle\gamma\rangle$,
$|C_d(x)|\mid n$ dann gilt die Behauptung:
Die Abbildung $\Phi:C_d(x)\longrightarrow\{0,1\}^n$ mit $\Phi=\varphi\big|_{C_d(x)}$
ist eine bijektive Abbildung von $C_d(x)$ auf $C_n(x')$
(daraus folgt: $|C_d(x)|=|C_n(x')|$)

Beweis.
1) Zeige $C_d(x)\subset Z_n$
aus $|C_d(x)|=p_m(x)$ und $|C_d(x)|\mid n$ folgt $p_m(x)\mid n$.
Mit Behauptung 3. folgt n ist Periode von x,
also $x\in Z_n$.
Es gilt: $\sigma^k(x)\in Z_n$ Denn: $\sigma^n(\sigma^k(x))=\sigma^{k+n}(x)=\sigma^k(\sigma^n(x))=\sigma^k(x)$, also $C_d(x)\subset Z_n$

2) Zeige: $\Phi(\sigma^k(x)) \in C_n(x')$

Zeige dazu: $[\sigma^k(x)]' = \gamma^k(x')$

Seien $x=(x_1,\dots,x_d)$, $x'=(x_{m_1},\dots,x_{m_n})$,
$y=(y_1,\dots,y_d)=\sigma^k(x)$, $y'=(y_{m_1},\dots,y_{m_n})$ also gilt
$y_{m_i}=x_{m_{i+k}}$, $y'=(y_{m_1},\dots,y_{m_n})=(x_{m_{1+k}},\dots,x_{m_{n+k}})=$
$\gamma^k(x_{m_1},\dots,x_{m_n})=\gamma^k(x')$ q.e.d.

Behauptung 20.
Sei $C_d=<\sigma>$ und $\sigma=(m_1,\dots,m_d)$. Dann gilt:
$C_d(x)\cap C_d(y)=\emptyset$ oder $C_d(x)=C_d(y)$

Beweis.
Beachte, daß $C_d=<\sigma>$ Untergruppe von $\sum_d$ ist. q.e.d.

Bemerkung.
Wenn $|C_d(z)| \nmid n$, $z\in\{0,1\}^d$, $d=n\cdot q^k$, q Primzahl
dann gilt: $q \mid |C_d(z)|$

Beweis.
Es gilt: $|C_d(z)| \mid n\cdot q^k$
(denn: $|C_d(z)| = p_m(z)$, außerdem ist d eine Periode von z bzgl. C_d. Nach Beh 3 gilt $p_m(z) \mid d$, also $|C_d(z)| \mid d$.)
Die Primfaktorzerlegung (PFZ) von $|C_d(z)|$ besteht also höchstens aus Primzahlen q und Primzahlen aus der PFZ von n. Bestünde die PFZ von $|C_d(z)|$ nur aus Primzahlen aus der PFZ von n, dann muß $|C_d(z)| \mid n$ gelten, was zum Widerspruch zur Voraussetzung steht. Also ist in der PFZ von $|C_d(z)|$ mindestens eine Primzahl q enthalten. Damit gilt $q \mid |C_d(z)|$. q.e.d.

$$P^1(-1) = \sum_{\substack{j \text{ gerade}\\ 0\le j\le d}} w_j(P) - \sum_{\substack{j \text{ ungerade}\\ 0\le j\le d}} w_j(P)$$

$$= \sum_{\substack{j \text{ gerade}\\ 0\le j\le d}} |W_j(P)| - \sum_{\substack{j \text{ ungerade}\\ 0\le j\le d}} |W_j(P)|$$

$$= \Big|\bigsqcup_{\substack{j \text{ gerade}\\ 0\le j\le d}} W_j(P)\Big| - \Big|\bigsqcup_{\substack{j \text{ ungerade}\\ 0\le j\le d}} W_j(P)\Big|$$

$$= \Big| \bigcup_{\substack{\{x \mid P(x)=1 \\ w(x) \text{ gerade}\}}} C_d(x) \Big| - \Big| \bigcup_{\substack{\{x \mid P(x)=1 \\ w(x) \text{ ungerade}\}}} C_d(x) \Big|$$

$$= \Big| \bigcup_{x \in M_1} C_d(x) \cup \bigcup_{x \in M_2} C_d(x) \Big| - \Big| \bigcup_{x \in M_3} C_d(x) \cup \bigcup_{x \in M_4} C_d(x) \Big|$$

$M_1 = \{x \mid P(x)=1, w(x) \text{gerade}, |C_d(x)| \mid n\}$
$M_2 = \{x \mid P(x)=1, w(x) \text{gerade}, |C_d(x)| \nmid n\}$
$M_3 = \{x \mid P(x)=1, w(x) \text{ungerade}, |C_d(x)| \mid n\}$
$M_4 = \{x \mid P(x)=1, w(x) \text{ungerade}, |C_d(x)| \nmid n\}$

es existieren Vektoren $x_m \in M_1$, $m \in \Lambda_1$ so daß:

$$\bigcup_{m \in \Lambda_1} C_d(x_m) = \bigcup_{x \in M_1} C_d(x)$$

und aus m_1, m_2, $m_1 \neq m_2$ folgt $C_d(x_{m_1}) \neq C_d(x_{m_2})$

(analoges gilt für $\Lambda_2, \Lambda_3, \Lambda_4$,)

$$= \Big| \bigcup_{m \in \Lambda_1} C_d(x_m) \cup \bigcup_{m \in \Lambda_2} C_d(x_m) \Big| - \Big| \bigcup_{m \in \Lambda_3} C_d(x_m) \cup \bigcup_{m \in \Lambda_4} C_d(x_m) \Big|$$

$$= \sum_{m \in \Lambda_1} |C_d(x_m)| + \sum_{m \in \Lambda_2} |C_d(x_m)| - \sum_{m \in \Lambda_3} |C_d(x_m)| - \sum_{m \in \Lambda_4} |C_d(x_m)|$$

$$= c \cdot q + \sum_{m \in \Lambda_1} |C_d(x_m)| - \sum_{m \in \Lambda_3} |C_d(x_m)|$$

↑ vorhergehende Bemerkung

$$= c \cdot q + \sum_{m \in \Lambda_1} |C_n(x'_m)| - \sum_{m \in \Lambda_3} |C_n(x'_m)|$$

$$= c \cdot q + \Big| \bigcup_{m \in \Lambda_1} C_n(x'_m) \Big| - \Big| \bigcup_{m \in \Lambda_3} C_n(x'_m) \Big|$$

Behauptung 21.

$$\bigcup_{m \in \Lambda_1} C_n(x'_m) = \bigcup_{\{y \mid P'(y)=1,\ w(y) \text{ gerade}\}} C_n(y)$$

(analoges gilt für Λ_3)

Beweis.

"$\subset$":

$z \in$ L.S. also existiert ein $m \in \Lambda_1$, mit $z \in C_n(x'_m)$, also existiert ein $k \in N$ mit $z = \gamma^k(x'_m)$

Es gilt: 1.) $P'(x'_m)=1$
denn: $P'(x'_m)=P(x_m)=1$ $(x_m \in M_1)$

2.) $w(x'_m)$ gerade
denn: $w(x_m)=w(x'_m)\cdot q^k$
da $q>2$ gilt, folgt: $w(x_m)$ gerade gdw. $w(x'_m)$ gerade. Also $w(x'_m)$ gerade.

aus 1.) und 2.) folgt: $\gamma^k(x'_m) \in$ R.S.

"$\supset$":

$z \in$ R.S. also existiert ein y mit $P'(y)=1$ und $w(y)$ gerade und es existiert ein $k \in N$ mit $z=\gamma^k(y)$. Außerdem existiert mit Behauptung 18. ein $v \in Z_n$ mit $v'=y$.

Es gilt: 1.) $w(v)$ gerade
denn: aus $w(v)$ gerade gdw $w(v')=w(y)$ gerade und $w(y)$ gerade folgt $w(v)$ gerade

2.) $P(v)=1$
denn: $P(v)=P'(v')=P'(y)=1$

3.) $|C_d(v)| \mid n$
denn: v hat eine Periode n, also $p_m(v) \mid n$ und mit $p_m(v)=|C_d(v)|$ folgt: $|C_d(v)| \mid n$

mit 1.), 2.), 3.) folgt $v \in M_1$, also existiert ein $x_m \in M_1$, $m \in \Lambda_1$ mit $C_d(v)=C_d(x_m)$, also $v \in C_d(x_m)$, also existiert ein $r \in N$ mit $v=\sigma^r(x_m)$, also $y=v'=[\sigma^r(x_m)]'=\gamma^r(x'_m)$, damit:
$z=\gamma^k(y)=\gamma^k(\gamma^r(x'_m))=\gamma^{k+r}(x'_m) \in C_n(x'_m)$ q.e.d.

Mit Behauptung 21. gilt damit:

$$P^1(-1) = c\cdot q + \underbrace{\sum_{\substack{j \text{ gerade} \\ 0 \le j \le d}} w_j(P')}_{\in [0,q)} - \underbrace{\sum_{\substack{j \text{ ungerade} \\ 0 \le j \le d}} w_j(P')}_{\in [0,q)} \neq 0$$

$$g := \quad =: u$$

$\neq 0$ (siehe Beh. 22.)

da: $0 \le g \le 2^{n-1} < q$ und $0 \le u \le 2^{n-1} < q$

$\in (-q,q)$

Behauptung 22.
Sei P eine d-stellige Boolsche Funktion
$\sigma=(m_1,\ldots,m_d)$, $\gamma=(m_1,\ldots,m_n)$, $C_d=\langle\sigma\rangle$, $C_n=\langle\gamma\rangle$
$P(0)\neq P(1)$, $\Gamma(P)\supset C_d$, $d\in E$, und es gelte $\mathfrak{H}(n)$.
Dann gilt: $P'^{1}(-1)\neq 0$

Beweis.
1) $P'(0)=P(0)\neq P(1)=P'(1)$, also $P'(0)\neq P'(1)$
2) zeige: $C_n\subset\Gamma(P')$
$P'(\gamma^k(z'))=P'([\sigma^k(z)]')=P(\sigma^k(z))=P(z)=P'(z')$
$\sigma^k\in C_d\subset\Gamma(P)$

Da die Voraussetzungen in $\mathfrak{H}(n)$ erfüllt sind, folgt nun: $P'^{1}(-1)\neq 0$. q.e.d.

Damit ist nun der Satz 3 bewiesen.

Bemerkungen zum Hauptsatz über abelsche Gruppen

Sei $n=n_1\cdot n_2\cdot\ldots\cdot n_r$, wobei die n_i Primzahlpotenzen sind. (n_i werden so geordnet, daß man mit wachsenden Potenzen der kleinsten auftretenden Primzahl beginnt, dann die wachsenden Potenzen der nächstgrößeren Primzahl folgen läßt und so fortfährt bis zum Schluß.)
Wenn $G=Z_{n_1}\otimes\ldots\otimes Z_{n_r}$, dann sagt man G sei vom Typ $(n_1,\ldots,n_r)$. (Z_{n_λ} : zyklische Gruppe) Der Hauptsatz über abelsche Gruppen sagt nun, daß alle abelschen Gruppen der Ordnung n eineindeutig den sämtlichen möglichen Typen zu der Zahl n entsprechen.
z.B.: $24=2^3\cdot 3$. Alle abelschen Gruppen der Ordnung 24 haben die Typen (8,3), (2,4,3), (2,2,2,3).
Wenn $n=p\cdot q$, $p\neq q$, p,q Primzahl, dann gibt es nur den Typ (p,q), also gibt es nur eine abelsche Gruppe der Ordnung $n=p\cdot q$ und die muß zyklisch sein.

Zwar funktioniert der Beweis in Theorem 4.10. wegen des gefundenen Gegenbeispiels nicht, aber man kann für eine Teilmenge von E die Behauptung von Theorem 4.10. zeigen.

Definition.
$E'=\{q\cdot r \mid q,r \text{ Primzahlen und } q>2^{r-1}\}$

Behauptung 23.
$E' \subset E$

Beweis.
Es gilt: Jede Primzahl ist Element von E
($1 \in E$, q Primzahl, $q > 2^{1-1}$, also $q \in E$)
aus $r \in E$, q Primzahl, $q > 2^{r-1}$ folgt $r \cdot q \in E$

Satz 4.
Sei P eine transitive, abelsche, d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in E'$.
Dann ist P erschöpfend.

Beweis.
Sei $d = q \cdot r$, $q > 2^{r-1}$, q,r Primzahlen,
$\Gamma(P)$ abelsch, transitiv, dann ist $|\Gamma(P)| = q \cdot r$ [RV]
Da aus $q > 2^{r-1} \geq r$ folgt $q \neq r$, gilt nach dem Hauptsatz über abelsche Gruppen: $\Gamma(P)$ ist zyklisch.
Da $\Gamma(P)$ transitiv ist, wird $\Gamma(P)$ von einem Zyklus der Länge d erzeugt. (Jede Permutation läßt sich als Produkt elementfremder Zyklen schreiben.)
Damit: $\Gamma(P) = C_d = \langle (m_1, \ldots, m_d) \rangle$. Also gilt mit Satz 3
P ist erschöpfend. q.e.d.

Satz 5.
Sei P eine 2-fach transitive, abelsche d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in E$.
Dann ist P erschöpfend.

Beweis.
Es gilt: wenn $\Gamma(P)$ 2-fach transitiv und abelsch ist, dann muß $\Gamma(P)$ zyklisch sein. (siehe [WI])
Da $\Gamma(P)$ außerdem transitiv ist, existiert ein Zyklus $\mathfrak{G} = (m_1, \ldots, m_d)$ mit $\Gamma(P) = C_d := \langle \mathfrak{G} \rangle$. Also gilt mit Satz 3
P ist erschöpfend. q.e.d.

Satz 6.
Sei P eine transitive, abelsche d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in E'' := \{q \cdot r \mid q,r \text{ Primzahlen}\}$.
Dann ist P erschöpfend.

Beweis.
Fall 1: $q=r$, also ist $d=q^2$ Primzahlpotenz. wende Satz 2. an.
Fall 2: $q \neq r$, also folgt mit dem Hauptsatz über abelsche Gruppen, daß $|\Gamma(P)| = q \cdot r$ zyklisch ist. Da $\Gamma(P)$ außerdem transitiv ist, folgt mit Satz 3., daß P erschöpfend ist. q.e.d.

Da durch das Gegenbeispiel von Illies die verallgemeinerte Aanderaa-Rosenberg Vermutung widerlegt ist, versucht man nun weitere Gegenbeispiele zu finden, um eventuell eine Teilmenge von N angeben zu können, für die die verallgemeinerte Aanderaa-Rosenberg Vermutung richtig wird. (Beachte, daß auf der Suche nach neuen Gegenbeispielen nur Boolsche Funktionen mit $P^1(-1)=0$ von Interesse sind.)
Für alle folgenden d-stelligen Boolschen Funktionen soll (wie bei Illies) gelten: $\Gamma(P) \supset C_d = <(1,2,\ldots,d)>$

Berechnung von $w_i(P)$:

$$W_i(P) = \bigcup_{x \in W_i(P)} C_d(x)$$

es existieren $x_r \in W_i(P)$, $r \in \Lambda_i$, so daß:

$$\bigcup_{x \in W_i(P)} C_d(x) = \bigcup_{r \in \Lambda_i} C_d(x_r)$$

wobei aus $r_1 \in \Lambda_i$, $r_2 \in \Lambda_i$, $r_1 \neq r_2$ folgt $C_d(x_{r_1}) \neq C_d(x_{r_2})$
also:

$$w_i(P) = \sum_{r \in \Lambda_i} |C_d(x_r)| = \sum_{r \in \Lambda_i} p_m(x_r)$$

Zur Berechnung von $p_m(x)$ wird in den folgenden Verallgemeinerungen Behauptung 5. verwendet.

1. Verallgemeinerung:
P sei eine d-stellige Boolsche Funktion ($d=n(n+1)$), für die gilt:
$P(x)=1$ genau dann wenn eine der folgenden Bedingungen erfüllt ist: (vergleiche Definition auf Seite 12)

0.) x=0
1.) x enthält genau 1 Eins
2.) x enthält genau 2 Einsen im Abstand n oder n+1
3.) x enthält genau 3 Einsen im Abstand n oder n+1
⋮
n+1.) x enthält genau n+1 Einsen im Abstand n

Die Verallgemeinerung besteht darin, daß man 3 durch n und 4 durch n+1 ersetzt.

Diese und die folgenden Boolschen Funktionen werden im folgenden durch Tabellen dargestellt:

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_1(P)$
0					1
1	d		d		d
2	n	n+1	d	d	2d
n-1	n	n+1	d	d	2d
n	n	n+1	d	n+1	d+n+1
n+1	n		n		n

wobei jede Zeile (außer der ersten und der zweiten) der Tabelle folgenden zwei Vektortypen entspricht:

a.) Vektoren x_1 mit genau w Einsen im Abstand 1 und kleinster Periode $p_m(x_1)$

b.) Vektoren x_2 mit genau w Einsen im Abstand 2 und kleinster Periode $p_m(x_2)$

Die Zeile mit w=0 entspricht dem Nullvektor.
Die Zeile mit w=1 entspricht Vektoren mit Gewicht 1

In der letzten Spalte steht $w_1(P)$, das zur Berechnung von $P^1(-1)$ benötigt wird.

Die even-odd-ballance der n·(n+1) stelligen Boolschen Funktion in der 1. Verallgemeinerung soll jetzt für einige Werte von n ausführlich berechnet werden.

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_1(P)$	
0					1	
1	12		12		12	d=3·4
2	3	4	12	12	24	$P^1(-1)$=
3	3	4	12	4	16	28-28=0
4	3		3		3	
0					1	
1	20		20		20	d=4·5
2	4	5	20	20	40	$P^1(-1)$=
3	4	5	20	20	40	66-64=2
4	4	5	20	5	25	
5	4		4		4	
0					1	
1	30		30		30	d=5·6
2	5	6	30	30	60	$P^1(-1)$=
3	5	6	30	30	60	126-126=0
4	5	6	30	30	60	
5	5	6	30	6	36	
6	5			5	5	
0					1	
1	42		42		42	d=6·7
2	6	7	42	42	84	$P^1(-1)$=
3	6	7	42	42	84	218-216=2
4	6	7	42	42	84	
5	6	7	42	42	84	
6	6	7	42	7	49	
7	6		6		6	
0					1	
1	56		56		56	d=7·8
2	7	8	56	56	112	$P^1(-1)$=
3	7	8	56	56	112	344-344=0
4	7	8	56	56	112	
5	7	8	56	56	112	
6	7	8	56	56	112	
7	7	8	56	8	64	
8	7		7		7	

Behauptung 24.
P sei eine n·(n+1) stellige Boolsche Funktion, die genauso wie in der 1. Verallgemeinerung definiert ist.
Dann gilt:
$P^1(-1)=0$ genau dann wenn gilt: n ist ungerade

(Im folgenden verwendet man die Abkürzungen:
$g := \sum_{\substack{j \text{ gerade} \\ 0 \le j \le d}} w_j(P)$; $u := \sum_{\substack{j \text{ ungerade} \\ 0 \le j \le d}} w_j(P)$)

Beweis.
1.) Sei n ungerade
$g=1+n+2d(r-1)/2$
$u=d+d+n+1+((r-5)/2+1)2d$
also $g-u=0$
2.) Sei n ungerade
$g=1+d+n+1+((r-4)/2+1)2m$
$u=d+r+((r-4)/2+1)2m$
also $g-u=2$ q.e.d.

Versuche nun den Algorithmus von Illies in analoger Weise auf n(n+1) stellige (wie in der 1. Verallgemeinerung definierte) Boolsche Funktionen (n ungerade) zu übertragen.
Man sieht sofort daß man mit dem übertragenen Algorithmus nicht weiterkommt.

2. Verallgemeinerung
Im Gegenbeispiel von Illies tauchen 2 bzw. 3 bzw. 4 Einsen auf mit Abstand 12/4=3 bzw. 12/3=4.
Nun sollen wieder 2 bzw. 3 bzw. 4 Einsen auftauchen jetzt aber mit Abstand d/4 bzw. d/3 ($d=k\cdot 12$, $k \in N$).
P sei eine $k\cdot 12$ stellige ($k \in N$) Boolsche Funktion, für die gilt:
P(x)=1 genau dann wenn eine der folgenden Bedingungen erfüllt ist:
1.) x=0
2.) x enthält genau 1 Eins
3.) x enthält genau 2 Einsen im Abstand d/4 oder d/3
4.) x enthält genau 3 Einsen im Abstand d/4 oder d/3
5.) x enthält genau 4 Einsen im Abstand d/4

tabellarisch:

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_i(P)$
0					1
1	d		d		d
2	d/4	d/3	d	d	2d
3	d/4	d/3	d	d/3	4/3 d
4	d/4		d/4		d/4

g=1+2d+d/4=9/4 d+1
u=d+4/3 d=7/3 d
also $P^1(-1) \neq 0$ für $d \neq 12$

In den folgenden Verallgemeinerungen wird nur noch die kürzere tabellarische Schreibweise für die Darstellung von $P^{-1}(1)$ und $w_i(P)$ benutzt.

3. Verallgemeinerung
P sei eine d-stellige Boolsche Funktion ($d > 4a$, $a \in N$, $4 \mid d$) mit folgender tabellarischer Darstellung:

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_i(P)$
0					1
1	d		d		d
2	a	d/4	d	d	2d
3	a	d/4	d	d	2d
4		d/4		d/4	d/4

g=1+2d+d/4=1+9/4 d
u=d+2d=3d
$P^1(-1) \neq 0$

Die $w_i(P)$ wurden folgendermaßen berechnet:
In der folgenden Tabelle wird dem Gewicht eines Vektors x_1 (mit $P(x_1)=1$ und x_1 enthält Einsen im Abstand a) seine Abstandsfolge und mit Behauptung 5. seine kleinste Periode zugeordnet.

Gewicht	Abstandsfolge	$P_m(x_1)$
1	(d)	d
2	(a,d-a)	d
3	(a,a,d-2a)	d
4	(a,a,a,d-3a)	d

Die $P_m(x_1)$ wurden folgendermaßen berechnet:
Es gilt: $d-a \neq a$, $d-2a \neq a$ und $d-3a \neq a$.
Denn:
wäre $d-a=a$, dann wäre $d=2a>4a$ Widerspruch!
wäre $d-2a=a$, dann wäre $d=3a>4a$ Widerspruch!
wäre $d-3a=a$, dann wäre $d=4a>4a$ Widerspruch!
Mit Behauptung 5. folgt sofort $P_m(x_1)=d$

Die Berechnung der $P_m(x_2)$ mit $P(x_2)=1$ und x hat Einsen im Abstand d/4 geht genauso mit Behauptung 5.

4. Verallgemeinerung
(fast analog zur 3. Verallgemeinerung)
P sei eine d-stellige Boolsche Funktion ($d>4a$, $a \in N$, $4 \mid d$) mit folgender tabellarischer Darstellung:

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_i(P)$
0					1
1	d		d		d
2	a	d/4	d	d	2d
3	a	d/4	d	d	2d
4		a		d	d

$g=1+2d+d=3d+1$
$u=d+2d=3d$
also $P^1(-1) \neq 0$

5. Verallgemeinerung
Sei P eine d-stellige Boolsche Funktion ($d>4a_1$, $d>4a_2$; $a_1, a_2 \in N$) mit folgender tabellarischer Darstellung:

w	Abst.1	Abst.2	$p_m(x_1)$	$p_m(x_2)$	$w_i(P)$
0					1
1	d		d		d
2	a_1	a_2	d	d	2d
3	a_1	a_2	d	d	2d
4	a_1	a_2	d	d	2d

$g=1+2d+2d=4d+1$
$u=d+2d=3d$
also $P^1(-1) \neq 0$

AUSBLICK

Obwohl durch das Gegenbeispiel von Illies die verallgemeinerte Aanderaa-Rosenberg Vermutung widerlegt wurde, ist es weiter ein interessantes Ziel, die größte Teilmenge M der natürlichen Zahlen zu bestimmen, für die die folgende Behauptung gilt:

Behauptung.
Sei P eine transitive, d-stellige Boolsche Funktion mit $P(0) \neq P(1)$, $d \in M$.
Dann ist P erschöpfend.

Eine Methode um diesem Ziel näher zu kommen, ist die Verwendung des Hilfsmittels "even-odd-balance".
(Benutzt man die "even-odd-balance" nicht, muß man die Algorithmen selbst untersuchen, was im allgemeinen sehr kompliziert ist.)
Durch die Angabe von natürlichen Zahlen $d \in N$ und transitiven, d-stelligen Boolschen Funktionen mit $P(0) \neq P(1)$ und $P^1(-1)=0$ kann man die Grenze dieser Methode erkennen.

Im folgenden werden Boolsche Funktionen angegeben mit der folgenden Eigenschaft:

P ist eine transitive, d-stellige Boolsche Funktion, mit $P(0) \neq P(1)$ und $P^1(-1)=0$.

Behauptung 25.
Es existieren transitive, d- stellige Boolsche Funktionen mit $P(0) \neq P(1)$, $d=k \cdot 12$, ($k \in N$, k ungerade) und $P^1(-1)=0$.

Beweis.
$$P^{-1}(1)=C_d\ \underbrace{[1,4,7,\ldots,k\cdot 12-2]}_{\text{4k-Einsen}} \cup C_d\ \underbrace{[1,5,9,\ldots,k\cdot 12-3]}_{\text{3k-Einsen}} \cup \{0\}$$

$g=1+ |C_d\ [1,4,7,\ldots,k\cdot 12-2]| \quad =4$
$u= |C_d\ [1,5,9,\ldots,k\cdot 12-3]| \quad =4$
also $P^1(-1)=0$ q.e.d.

Behauptung 26.
Es existieren transitive, d-stellige Boolsche Funktionen mit $P(0)\neq P(1)$, $d=k\cdot 35$, ($k\in N$, k ungerade) und $P^1(-1)=0$.

Beweis.
$P^{-1}(1)=C_d$ [1,6,11,...,k·35−4]
(7k-Einsen)

C_d [1,2,3,6,7,8,11,12,13,...,k·35−2]
(3·7k-Einsen)

C_d [1,3,4,6,8,9,11,13,14,...,k·35−1]
(3·7k-Einsen)

C_d [1,2,8,9,15,16,22,23,...,k·35−5]
(2·5k-Einsen)

C_d [1,3,8,10,15,17,...,k·35−4]
(2·5k-Einsen) q.e.d.

g=1+7+7=15
u=5+5+5=15
also $P^1(-1)=0$

Behauptung 27.
Es existieren transitive, d-stellige Boolsche Funktionen $P(0)\neq P(1)$, $d=r(r+1)$, ($r\geq 3$, r ungerade) und $P^1(-1)=0$ (siehe Behauptung 24.)

Eine transitive, d-stellige Boolsche Funktion mit $P(0)\neq P(1)$, $d\in N$ und $\Gamma(P)\supset C_d$, $C_d=\langle(1,2,...,d)\rangle$ läßt sich mittels einer Tabelle darstellen.
In der folgenden Tabelle entspricht jede Zeile einem d-stelligen Vektor x mit Funktionswert $P(x)=1$, Gewicht $w=k\cdot r$ und kleinster Periode $p_m(x)$.
Für den Vektor x gilt: $w(x')=k$, ($x'=\varphi(x)$), $r=d/p_m(x)$
Für je zwei beliebige d-bit Vektoren x,y, denen zwei verschiedene Zeilen entsprechen, gilt: $C_d(x)\cap C_d(y)=\emptyset$
D.h. $x=(x_1,...,x_{p_m(x)},\ x_1,...,x_{p_m(x)},...,x_1,...,x_{p_m(x)},)$
wobei $x_1,...,x_{p_m(x)}$ in x genau $d/p_m(x)$ mal vorkommt und k Einsen enthält.

Transitive, d-stellige Boolsche Funktionen P mit $P(0) \neq P(1)$, $d \in N$ und $P^1(-1)=0$:

d	w	$p_m(x)$
2·12	0	1
	3	8
	6	4
	8	3
4·12	0	1
	3	12
	4	9
	18	2
6·12	0	1
	3	24
	4	18
	24	3
	36	2
8·12	0	1
	3	32
	4	24
	24	4
	32	3
10·12	0	1
	3	40
	4	30
	24	5
	30	4
12·12	0	1
	3	48
	4	36
	16	9
	72	2
14·12	0	1
	3	56
	4	42
	24	7
	28	6
16·12	0	1
	3	64
	4	48
	16	12
	64	3
18·12	0	1
	3	72
	4	54
	24	9
	2·27=54	8
20·12	0	1
	3	80
	4	60
	2·15=30	16
	80	3
22·12	0	1
	3	88
	4	66
	2·33=66	8
	88	3
	44	6
	66	4
24·12	0	1
	3	96
	4	72
	96	3
	36	8
	24	12
26·12	0	1
	3	104
	4	78
	26	12
	52	6
	78	4
	104	3
2·35	0	1
	5	14
	5	14
	7	10
	7	10
	10	7
	2·10=20	7
	2·10=20	7
	2·10=20	7
	4·10=40	7
	5·10=50	7
	14	5

d	w	$p_m(x)$
$4\cdot35$	0	1
	20	7
	35	4
	35	4
$6\cdot35$	0	1
	42	5
	35	6

d	w	$p_m(x)$
$8\cdot35$	0	1
	40	7
	35	8
$10\cdot35$	0	1
	$2\cdot50=100$	7
	$2\cdot50=100$	7
	$2\cdot50=100$	7
	$3\cdot35=105$	10
	$3\cdot35=105$	10
	175	2

Durch diese positiven Ergebnisse wird motiviert:

Vermutung 1:
Für alle natürlichen Zahlen k existieren transitive, d-stellige Boolsche Funktionen P mit $P(0)\neq P(1)$, $d=k\cdot12$ und $P^1(-1)=0$.

Die Konstruktion dieser Boolschen Funktionen läuft auf die Lösung eines zahlentheoretischen Problems hinaus. D.h. wenn man folgende zahlentheoretische Vermutung gelöst hat, ist die Vermutung 1 richtig.

Vermutung 2: (zahlentheoretische Vermutung)
Es sei $d=k\cdot12$, $k\in N$.
Es existiert eine Menge
$M:=\{(g,k,r,s)\in N^4 \mid s\neq1,\ 1\leq k\leq s,\ r\cdot s=d,\ g\leq b_{k,s}$, und aus $(g_1,k_1,r_1,s_1),\ (g_2,k_2,r_2,s_2)\in N^4,\ k_1=k_2,\ r_1=r_2,\ s_1=s_2$ folgt $g_1=g_2\}$

von 4er Tupeln, für die gilt:

$$1+\sum_{\substack{(g,k,r,s)\in M,\\ k\cdot r \text{ gerade}}} g\cdot s = \sum_{\substack{(g,k,r,s)\in M,\\ k\cdot r \text{ ungerade}}} g\cdot s$$

$b_{k,s}=$ Anzahl aller disjunkten Bahnen von d-bit Vektoren x unter $C_d=\langle(1,2,\ldots,d)\rangle$ mit $p_m(x)=s$ und $w(x^i)=k$

Analoge Vemutungen lassen sich für $d=k\cdot35$, $k\in N$ aufstellen.

Wenn Vermutung 1 und die analoge Vermutung für $k \cdot 35$ richtig ist, hat man "viele" transitive d-stellige Boolsche Funktionen P mit $P(0) \neq P(1)$, $d \in N \setminus E$ und $P^1(-1)=0$ gefunden.
($d \in N \setminus E$ folgt aus $\Gamma(P) \supset C_d=\langle(1,2,\ldots,d)\rangle$ und Satz 3).
Dies führt zur folgenden

Frage:
Existieren für alle $d \in N \setminus E$ transitive, d-stellige Boolsche Funktionen P mit $P(0) \neq P(1)$ und $P^1(-1)=0$?

LITERATURVERZEICHNIS

[HE] Ulrich Hedtstück, Über die Argumentkomplexität Boolscher Funktionen. Institut für Informatik der Universität Stuttgart 1985

[HR] R.C. Holt and E.M. Reingold, On The time required to detect cycles and connectivity in graphs, Math. Systems Theory 6 (1972) 103-106.

[HT] J. Hopcroft and R. Tajan, Efficient planarity testing, Cornell University Computer Science Tech. Report TR 73-165 (1973)

[IL] N. Illies, A counterexample to the generalized Aanderaa-Rosenberg Conjecture, Inform. Proc. Lett. 7 (1978), no. 3, 154-155

[RO] A.L. Rosenberg, On the time required to recognize properties of graphs: A problem, SIGACT News 5 (1973) 15-16

[RV] R.L. Rivest and J. Vuillemin, On recognizing graph properties from adjacency matrices, Theor. Comp. Sci. 3 (1976) 371-384

[WI] H. Wielandt, Finite Permutation Groups (Academic Press, 1964)

EIDESSTATTLICHE ERKLÄRUNG:

Ich erkläre ehrenwörtlich, daß ich diese Diplomarbeit nur mit den angegebenen Hilfsmitteln und ohne fremde Hilfe angefertigt habe.

Carl-Heinz Barner