Brief an Ronald Rivest
Massachusetts Institute of Technology

Dear Sirs

I send you some results of my master theisis(Theorem 3, Theorem 4,Theorem 5 and a counterexample).
The correctness of the counterexample was attested by Prof. Rivest from the M.I.T. (see page 8)
If you think the results are worth publishing, please let me know

sincerely C. Barner

Carl-Heinz Barner
steigstr 23
7441 Unterensingen

P.S.

REFERENCES:
see at page 383 of the article:
"On recognizing graph properties from adjacency matrices"
in: Theoretical Computer Science 3 (1976) 371-384

Sufficient Conditions For Exhaustive Boolean Functions

Abstract:

Norbert Illies discovered a counterexample to the generalized Aanderaa-Rosenberg Conjecture.

When we want generalize this counterexample such that(how in the counterexample of Illies)is: $\Gamma(P) \supset C_d = \langle \sigma \rangle$ ($\sigma = (m_1, \dots, m_d)$ is a permutation in cyclic representation that creates the cyclic group C_d) then we have: $d \notin E$

This follows by the main theorem 3 of this work.

Theorem 4 and 5 are sufficient conditions for exhaustive Boolean functions.At last I will still show the incorrectness of a published proof.

The following results,definitions etc refer to the article "On recognizing graph properties from adjacency matrices" in: Theoretical Computer Science 3 (1976) 371-384 (authors: Rivest/Vuillemin) and the article "A counterexample to the generalized Aandera-Rosenberg conjecture",in Informating Processing Letters ,Volume 7,number 3 april 1978

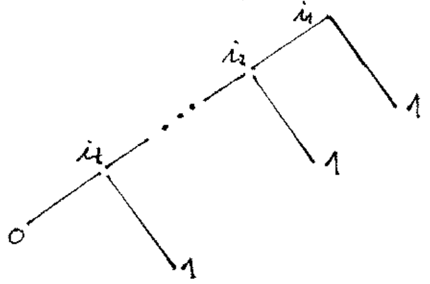
Introduction.

We denote by $P: \{0,1\}^d \to \{0,1\}$ Boolean functions, with $x.=(x_1,\dots,x_d)$ vectors from $\{0,1\}^d$ 0 denotes the vector consisting of d zeros, 1 the vector consisting of d ones.
Σ_d is the set of all permutations on $\{1,2,\dots,d\}$ and is called the symmetric group on $\{1,2,\dots,d\}$
A subgroup Γ of Σ_d is called transitive iff for all $i,j \in \{1,\dots,d\}$ there is a permutation $\sigma \in \Gamma$ with $\sigma(i)=j$. Let $P: \{0,1\}^d \to \{0,1\}$ be a function, $x \in \{0,1\}^d$ a vector and $\sigma(x):=(x_{\sigma(1)},x_{\sigma(2)},\dots,x_{\sigma(d)})$
Then the set of permutations $\Gamma(P):=\{\sigma \in \Sigma_d \mid \forall x \in \{0,1\}^d \; P(x)=P(\sigma(x))\}$ is called the stabilizer of P. $\Gamma(P)$ is a subgroup of Σ_d
The set of vectors $x\Gamma(P):=\{y \in \{0,1\}^d \mid \exists \sigma \in \Gamma(P) \text{ with } \sigma(y)=x\}$ is called the orbit of x under $\Gamma(P)$

Decision trees:
Let T be a binary tree with each node $v \in T$ labelled with $l(v) \in \{1,\dots,d\}$ if v is an internal node and $l(v) \in \{0,1\}$ if v is a leaf.
The function $P(T): \{0,1\}^d \to \{0,1\}$ realized by T is defined in the usual way:

$$P(T)(x)=\begin{cases} P(\text{left subtree of } T)(x) \text{ if } x_{l(\text{root of } T)}=0 \\ P(\text{right subtree of } T)(x) \text{ if } x_{l(\text{root of } T)}=1 \\ l(\text{root of } T) \text{ if } T \text{ consists of a single node} \end{cases}$$

we introduce a shorthand notation for decision trees:
a bracketed leaf $(j_1,\dots,j_s)$ stands for



where $\{i_1,\dots,i_t\}=\{i \in \{1,\dots,d\} \; i \neq j_1,\dots,j_s$ and i is not a lable on the path from the root to the leaf $(j_1,\dots,j_s)\}$.
The weight $w(x)$ of a vector x is the number of ones in x
$W_i(P):=\{x \mid P(x)=1 \wedge w(x)=i\}$ $\quad w_i(P):=|W_i(P)|$

$$P^1(-1):=\sum_{\substack{j \text{ even} \\ 0\le j\le d}} w_j(P) - \sum_{\substack{j \text{ odd} \\ 0\le j\le d}} w_j(P)$$

Theorem 1(even-odd-ballance)
If P is not exhaustive then $P^1(-1)=0$

Theorem 2(Rivest-Vuillemin)
Any transitive Boolean function $P: \{0,1\}^d \to \{0,1\}$ such that p is a primepower $d=p^\alpha$ and $P(0)\neq P(1)$ is exhaustive
(any decision tree that realizes P has at least depth d)

$\sigma=(m_1,\ldots,m_d)$, where $m_i \in \{1,\ldots,d\}$, is a permutation in cyclic representation. It generates the group $C_d=\langle\sigma\rangle$. We say $p>0$ is a period of a d-bit vector x via σ iff $\sigma^p(x)=x$
$p_m(x)$ denotes the smallest period of the d-bit vector x via σ

Theorem 3
Let E denote the smallest set of natural numbers such that
(i) $1 \in \mathbf{E}$ and
(ii) if $n \in E$ and q prime and $q > 2^{n-1}$,
then $n \cdot q^K \in \mathbf{E}$ for all natural numbers k

If $P:\{0,1\}^d \rightarrow \{0,1\}$, $d \in E$, is a Boolean function with $\Gamma(P) \supset C_d$, $C_d=\langle(m_1,\ldots,m_d)\rangle$, $P(0)\neq P(1)$, then **P** is exhaustive.

proof:

We have to show $P^1(-1)\neq \mathbf{0}$ (even odd ballance)
We prove the following statement $\mathcal{S}(n), n \in E$

$\mathcal{S}(n): \Longleftrightarrow$
If $Q:\{0,1\}^n \rightarrow \{0,1\}$ is a Boolean function and $\Gamma(Q) \supset C_n$, $C_n := \langle(r_1,\ldots,r_n)\rangle$, $Q(0)\neq Q(1)$ then $Q^1(-1)\neq 0$

by induction

inductive basis : $\mathcal{S}(1)$ trivial

by inductive basis we have : $\mathcal{S}(n), n \in \mathbf{E}$, q prime, $q > 2^{n-1}$

inductive statement : $\mathcal{S}(n \cdot q^K), k \in \mathbf{N}, (d := n \cdot q^K)$

it is enough to show:

If $\mathcal{S}(n), n \in E$, q prime, $q > 2^{n-1}$, $q > 2$ then $\mathcal{S}(n \cdot q^k), k \in N$

The following statements are easy to show:

① If $\sigma=(m_1,\ldots,m_d)$, $C_d=\langle\sigma\rangle$, and x is a d-bit vector then $p_m(x)=|C_d(x)|$

② p is a period of a d-bit vector x via σ iff $p_m(x) \mid p$

③ If $\sigma=(m_1,\dots,m_d)$, $C_d=\langle\sigma\rangle$ and $C_d\subset\Gamma(P)$, then

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

similar we have for w(x) odd

④ If $\sigma=(m_1,\dots,m_d)$, $C_d=\langle\sigma\rangle$, and $Z_n=\{z\in\{0,1\}^d\mid\sigma^n(z)=z\}$
$Z_n' :=\{0,1\}^n$, $d=n\cdot q^k$
then

$\varphi: Z_n\longrightarrow Z_n'$ with $\varphi(z_1,\dots,z_d):=(z_{m_1},\dots,z_{m_n})$
and $(z_1,\dots,z_d)' := \varphi(z_1,\dots,z_d)$,
is bijective

we define : $P': Z_n'\longrightarrow\{0,1\}$ with $P'(z')=P(z)$

⑤ If $C_d=\langle\sigma\rangle$ and $\sigma=(m_1,\dots,m_d)$ then
$C_d(x)\cap C_d(y)=\emptyset$ or $C_d(x)=C_d(y)$

⑥ If $|C_d(z)|\nmid n$, $z\in\{0,1\}^d$, $d=n\cdot q^k$, q prime
then $q \mid |C_d(z)|$

⑦ If
$\sigma=(m_1,\dots,m_d)$, $\gamma=(m_1,\dots,m_n)$, $C_d=\langle\sigma\rangle$, $C_n=\langle\gamma\rangle$,
$|C_d(x)| \mid n$ then $|C_d(x)| = |C_n(x')|$

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

Now we prove that $P^1(-1)\neq 0$

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

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

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

$$= \left| \bigsqcup_{\substack{\{x \mid P(x)=1 \\ w(x)\ \text{even}}} C_d(x) \right| - \left| \bigsqcup_{\substack{\{x \mid P(x)=1 \\ w(x)\ \text{odd}}} C_d(x) \right|$$

$$= \left| \bigsqcup_{x\in M_1} C_d(x) \cup \bigsqcup_{x\in M_2} C_d(x) \right| - \left| \bigsqcup_{x\in M_3} C_d(x) \cup \bigsqcup_{x\in M_4} C_d(x) \right|$$

$$\begin{aligned}
M_1 &= \{x \mid P(x)=1, w(x)\ \text{even}\ , |C_d(x)| \mid n\} \\
M_2 &= \{x \mid P(x)=1, w(x)\ \text{even}\ , |C_d(x)| \nmid n) \\
M_3 &= \{x \mid P(x)=1, w(x)\ \text{odd}\ , |C_d(x)| \mid n\} \\
M_4 &= \{x \mid P(x)=1, w(x)\ \text{odd}\ , |C_d(x)| \nmid n\}
\end{aligned}$$

there exist vectors $x_m \in M_1,\ m \in \Lambda_1$ such that

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

and if $m_1,\ m_2,\ m_1 \neq m_2$ then $C_d(x_{m_1}) \neq C_d(x_{m_2})$

similar we have for $\Lambda_2, \Lambda_3, \Lambda_4,)$

$$= \left| \bigsqcup_{m\in\Lambda_1} C_d(x_m) \cup \bigsqcup_{m\in\Lambda_2} C_d(x_m) \right| - \left| \bigsqcup_{m\in\Lambda_3} C_d(x_m) \cup \bigsqcup_{m\in\Lambda_4} C_d(x_m) \right|$$

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

$$\underset{⑥}{=} c\cdot q + \sum_{m\in\Lambda_1} |C_d(x_m)| - \sum_{m\in\Lambda_3} |C_d(x_m)|$$

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

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

The following 2 statements are easy to show

⑧ $$\bigsqcup_{m\in\Lambda_1} C_n(x'_m) = \bigsqcup_{\substack{\{y\mid P'(y)=1\\ w(y)\ \text{even}\}}} C_n(y)$$ (similar we have for Λ_3

notice: $w(x_m)=w(x'_m)\cdot q^K$. Since $q>2$ we have:
$w(x_m)$ even iff $w(x'_m)$ even

⑨ If P is a Boolean function
$\sigma=(m_1,\ldots,m_d)$, $\gamma=(m_1,\ldots,m_n)$, $C_d=\langle\sigma\rangle$, $C_n=\langle\gamma\rangle$
$P(0)\neq P(1)$, $\Gamma(P)\supset C_d$, $d\notin E$, and $\mathfrak{F}(n)$
then $P'^{1}(-1)\neq 0$

Now we have

$$P^{1}(-1)=c\cdot q+\overbrace{\underbrace{g=\underbrace{\sum_{\substack{j\ \text{even}\\0\le j\le d}} w_j(P')}_{\in[0,q)}-\underbrace{\sum_{\substack{j\ \text{odd}\\0\le j\le d}} w_j(P')}_{\in[0,q)}=:U}_{\substack{\text{since }0\le g\le 2^{n-1}<q\text{ and }0\le u\le 2^{n-1}<q\\ \in(-q,q)}}}^{\neq 0\ \text{see}\ ⑨}\neq 0$$

qed

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Laboratory for Computer Science

M.L. Dertouzos, Director   R.L. Rivest and A. Vezza, Associate Directors   545 Technology Square, Cambridge, Massachusetts 02139
(617) 253-

1 April 1985

Mr. Carl-Heinz Barner
Steigstr. 23
7441 Unterensinger
WEST GERMANY

Dear Mr. Barner:

In your example we have

$$\Gamma(Q) \ncong \Gamma(P)/\Theta$$

an interesting oversight on our part. I don't know if it is possible to show that $\Gamma(Q)$ will still be transitive and abelian in all cases; perhaps not.

Please let me know what you discover, and thanks for pointing out this oversight.

Sincerely,

Ronald L. Rivest

Ronald L. Rivest,
Professor of Electrical Engineering
and Computer Science

RLR/jdm