Dear Mr Rivest

In your article "On Recognizing graph properties from adjacency matrices" in Theoretical Computer Science 3 (1976) 371-384

one can find the theorem 4.10:

$P: \{0,1\}^d \rightarrow \{0,1\}$ is such that $P(\mathbf{0}) \neq P(1)$, $\Gamma(P)$ abelian and transitive, $d \in E$ then P exhaustive.

I will send you a counterexample for the following statement in the prove : "We can create an induced function $Q: \{0,1\}^n \longrightarrow \{0,1\}$ such that $\Gamma(Q) = \Gamma(P)/\Theta$ and $Q(y_1, \dots, y_n) = P(x_1, \dots, x_d)$, where all of the variables x_j in the i^{th} block are set equal to y_i"

Is there any possibility to change the prove so that the prove becomes correct.⊗ I would be glad to get an answer of you since I am writing a master theisis which ~~about~~ uses this article. The counterexample can you find on the next sides.

Many thanks, sincerely

Ch. Bamer

⊗ and also the modifiKations of the Theorem at page 382.

Counterexample

Theorem 4.10

$P:\{0,1\}^d \to \{0,1\}$; $P(\mathbf{0}) \neq P(\mathbf{1})$, $\Gamma(P)$ transitive, abelian, $d \in E$ $\Rightarrow$ P exhaustive

① $d = 15$, $n = 3$, $q^k = 5^1$, 5 prime, $3 \in E$, $5 > 2^{3-1}$.

Definition from $P:\{0,1\}^{15} \longrightarrow \{0,1\}$:

$P^{-1}(1)$ consists of the following vectors:

$$\left.\begin{matrix}
101000000000000\\
010100000000000\\
001010000000000\\
000101000000000\\
000010100000000\\
000001010000000\\
000000101000000\\
000000010100000\\
000000001010000\\
000000000101000\\
000000000010100\\
000000000001010\\
000000000000101\\
100000000000010\\
010000000000001
\end{matrix}\right\}\ \mathrm{I}
\qquad
\left.\begin{matrix}
111000000000000\\
011100000000000\\
001110000000000\\
000111000000000\\
000011100000000\\
000001110000000\\
000000111000000\\
000000011100000\\
000000001110000\\
000000000111000\\
000000000011100\\
000000000001110\\
000000000000111\\
100000000000011\\
110000000000001
\end{matrix}\right\}\ \mathrm{II}$$

$$\left.\begin{matrix}
110100100000000\\
011010010000000\\
001101001000000\\
000110100100000\\
000011010010000\\
000001101001000\\
000000110100100\\
000000011010010\\
000000001101001\\
100000000110100\\
010000000011010\\
001000000001101\\
100100000000110\\
010010000000011\\
101001000000001
\end{matrix}\right\}\ \mathrm{III}
\qquad
\left.\begin{matrix}
100100100100100\\
010010010010010\\
001001001001001
\end{matrix}\right\}\ \mathrm{IV}
\qquad
\left.\begin{matrix}
000000000000000
\end{matrix}\right\}\ \mathrm{V}$$

what can we say about permutation $\sigma \in \Gamma(P)$?

$\sigma \in \Gamma(P)$ must be in one of the following two forms:

ⓐ $\begin{pmatrix} \cdots\cdots & i-1 & i & i+1 & \cdots\cdots \\ \cdots 5\ \square\ 3\ \square & 1 & 15 & \square\ 13 & \cdots\cdots \end{pmatrix}$ or $\begin{pmatrix} \cdots\cdots & i-1 & i & i+1 & \cdots\cdots \\ \cdots 13\ \square & 15 & 1 & \square\ 3\ \square\ 5 & \cdots \end{pmatrix}$ ⓑ

[note $x \in \mathrm{I} \Rightarrow \sigma(x) \in \mathrm{I}$ $\qquad \sigma(x) := (x_{\sigma(1)}, \ldots, x_{\sigma(15)})$]

where do we have to place the remaining numbers from ⓐ, ⓑ

ⓐ, ⓑ must be in the following form:

$$\begin{pmatrix} \cdots\cdots & i & \cdots\cdots \\ \cdots 4\,3\,2 & 1 & 15\,14 \cdots \end{pmatrix}, \quad \begin{pmatrix} \cdots\cdots & i & \cdots\cdots \\ \cdots 13\,14\,15 & 1 & 2\,3\,4 \cdots \end{pmatrix}$$

$$\left[\text{note} \quad x \in \mathrm{III} \implies \sigma(x) \in \mathrm{III}\right]$$

but:

$$\gamma_i := \begin{pmatrix} \cdots\cdots & i & \cdots\cdots \\ \cdots 3\,2 & 1 & 15\,14\,13 \cdots \end{pmatrix} \overbrace{(110100100000000)}^{:=y} \notin \mathrm{III} \qquad 1 \le i \le 15$$

$\implies P(\gamma_i(y)) = 0$. with $P(y) = 1$ follows $\gamma_i \notin \Gamma(P)$

$\implies \Gamma(P) = C_{15}$

(c) $C_{15} = \Gamma(P)$ contains exactly one subgroup θ of order 5.

This must be the cyclic group C_5

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

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

$$\begin{aligned}
Q(000) &:= P(000000000000000) = 1 \\
Q(001) &:= P(001001001001001) = 1 \\
Q(010) &:= P(010010010010010) = 1 \\
Q(011) &:= P(011011011011011) = 0 \\
Q(100) &:= P(100100100100100) = 1 \\
Q(101) &:= P(101101101101101) = 0 \\
Q(110) &:= P(110110110110110) = 0 \\
Q(111) &:= P(111111111111111) = 0
\end{aligned}$$

3-bit vectors with value 1:	3-bit vectors with value 0
(0,0,0) (0,0,1) (0,1,0) (1,0,0)	(011) (101) (110) (111)

$\implies \Gamma(Q) = \Sigma_3$, where Σ_3 is the symmetric group of degree 3

since $|\Gamma(Q)| = 6$ and $|\Gamma(P)/\theta| = 3$ follows

$$\Gamma(Q) \neq \Gamma(P)/\theta$$