*Combinatorics, Probability and Computing* (2005) 15, 627–629. © 2005 Cambridge University Press
doi:10.1017/S096354830500711X Printed in the United Kingdom

# PROBLEM SECTION

# Jaeger's Conjecture

AART BLOKHUIS[†]

Department of Mathematics and Computer Science, Technical University Eindhoven
P.O.Box 513 5600 MB Eindhoven, the Netherlands
aartb@win.tue.nl

*Received May 13th 2005*

The problem we consider here is based on the following question posed by François Jaeger in 1981 at a combinatorics meeting in Eger (Hungary):

**Question 1.1.** *Consider the n-dimensional vector-space over* $GF(5)$. *Is it true that for any two bases* $B_1$, $B_2$ *there exists a hyperplane* $H$ *which is disjoint from* $B_1 \cup B_2$*? The answer is positive if* $M(B_1 \cup B_2)$ *is a regular matroid. The question is equivalent to the following: is it true that for every* $n \times n$ *non-singular matrix* $\mathbf{A}$ *over* $GF(5)$ *there exists a vector* $\mathbf{x}$ *such that neither* $\mathbf{x}$ *nor* $\mathbf{Ax}$ *has any* 0*-components?*

François Jaeger (1947-1997) is mostly known for his work in Knot Theory and in particular his discovery of the connections between link invariants and the Bose-Mesner algebra of certain association schemes. A conference in his honour was held in Grenoble (France) in 1998.

A somewhat more general version of his question deserves the name *Jaeger's Conjecture:*

**Conjecture 1.2.** *Let* $\mathbf{A}$ *be a non-singular matrix defined over the finite field* $GF(q)$, $q > 3$. *Then there exists a vector* $\mathbf{x}$ *such that neither* $\mathbf{x}$ *nor* $\mathbf{Ax}$ *has any* 0*-component.*

For small $q$ the statement is false as can be seen from the matrices $\left(\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 1\\ 1 & 2\end{smallmatrix}\right)$ over $GF(2)$ and $GF(3)$ respectively. A very nice proof of Jaeger's conjecture in the case that

[†] The author was supported by the "Finite Structures" project carried out by Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, in the framework of the European Community's "Structuring the European Research Area" programme.

https://doi.org/10.1017/S096354830500711X Published online by Cambridge University Press

$q$ is a proper prime power was given by Alon and Tarsi [1]; an essentially equivalent version using the idea of a *Rédei polynomial* appears in Ball and Lavrauw [2], and it is this proof we will present here.

Before continuing however let us mention a couple of equivalent formulations of this conjecture. As in Jaeger's original question we may reformulate it as:

**Variation 1.** *Let $V$ be a vector-space over $GF(q)$, $q > 3$, with two bases $A$ and $B$. Then there exists a hyperplane in $V$ disjoint from both.*

Or yet another equivalent version:

**Variation 2.** *Let $V$ be an $n$-dimensional vector space over $GF(q)$, provided with two bases: $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ and $\{\mathbf{b}_1, \ldots, \mathbf{b}_n\}$. Must there exist a vector $\mathbf{c}$ in $V$ all of whose coordinates with respect to both bases are nonzero?*

Here is (my version of) Ball and Lavrauw's version of Alon and Tarsi's proof of Jaeger's Conjecture in the case that $q = p^n$, $n > 1$. Let $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$ be related by

$$X_1\mathbf{a}_1 + \cdots + X_n\mathbf{a}_n = Y_1\mathbf{b}_1 + \cdots + Y_n\mathbf{b}_n.$$

We may define an inner product in such a way that the $\mathbf{a}_i$ form an orthonormal basis. We then consider the dual basis of the $\mathbf{b}_i$, say $\mathbf{b}_i^*$ so $(\mathbf{b}_i, \mathbf{b}_j^*) = \delta_{ij}$. So $X$ and $Y$ are linearly related by $Y_i = (X, \mathbf{b}_i^*)$ and $X_j = \sum_i (\mathbf{b}_i, \mathbf{a}_j) Y_i =: L_j(Y)$.

Suppose a vector $\mathbf{c}$ with the required properties does not exist. Then the 'Rédei-polynomial'

$$R(X) := \prod_i (X, \mathbf{b}_i^*) = \prod_i (X_1\mathbf{b}_{i1}^* + X_2\mathbf{b}_{i2}^* + \cdots + X_n\mathbf{b}_{in}^*),$$

vanishes for all $X$ with $X_1, \ldots, X_n$ non zero, for if we consider:

$$\mathbf{c} = X_1\mathbf{a}_1 + \cdots + X_n\mathbf{a}_n = Y_1\mathbf{b}_1 + \cdots + Y_n\mathbf{b}_n,$$

then all $X_j$ non-zero implies that at least one of the $Y_i$ is zero, but $Y_i = (X, \mathbf{b}_i^*)$. This implies that $R(X)$ is in the ideal $\langle (X_i^{q-1} - 1) \mid i = 1, \ldots, n \rangle$, so we have

$$R(X) := \prod_i (X, \mathbf{b}_i^*) = F_1(X)\big(X_1^{q-1} - 1\big) + \cdots + F_n(X)\big(X_n^{q-1} - 1\big),$$

for certain (homogeneous) polynomials $F_i$ of degree $n - q + 1$. Now consider the change of variables $X \mapsto Y$ and let $F_i(X) =: G_i(Y)$. In terms of $Y$ our equation becomes

$$\prod_i Y_i = G_1(Y)\big(L_1(Y)^{q-1} - 1\big) + \cdots + G_n(Y)\big(L_n(Y)^{q-1} - 1\big).$$

For $q$ a proper prime power this is impossible, because the coefficient of any square free monomial in $L_i(Y)^{q-1}$ is a multiple of $(q-1)!$ which is zero mod $p$.

https://doi.org/10.1017/S096354830500711X Published online by Cambridge University Press

## References

[1] N. Alon and M. Tarsi, A nowhere-zero point in linear mappings, *Combinatorica* **9** (1989) 393–395.
[2] S. Ball and M. Lavrauw, How to use Rédei polynomials in higher dimensional spaces, lecture notes of talk given at Combinatorics 2004 in Catania, Italy.
`http://www-ma4.upc.es/~simeon/listofpapers.html`
[3] F. Jaeger, Problem presented at the *6th Hung. Comb. Coll.*, Eger, Hungary 1981. *Finite and Infinite Sets Vol II (Eger 1981)*, 879, Colloq. Math. Soc. János Bolyai, 37, North Holland, Amsterdam, 1984.

https://doi.org/10.1017/S096354830500711X Published online by Cambridge University Press