An associative block design ABD(8,5)

Citation for published version (APA):

Brouwer, A. E. (1999). An associative block design ABD(8,5). *SIAM Journal on Computing*, 28(6), 1970-1971. <https://doi.org/10.1137/S0097539797316622>

DOI:

[10.1137/S0097539797316622](https://doi.org/10.1137/S0097539797316622)

Document status and date:

Published: 01/01/1999

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

AN ASSOCIATIVE BLOCK DESIGN $ABD(8,5)^*$

A. E. BROUWER[†]

To Maja, on the occasion of her seventeenth birthday.

Abstract. An associative block design is a certain balanced partition of a hypercube into smaller hypercubes. We construct such a design, thus settling the smallest open case.

AMS subject classification. 05B30

PII. S0097539797316622

An $ABD(k, w)$ is a $b \times k$ matrix (where $b = 2^w$) with entries from $\{0, 1, *\}$ such that (i) the stars form a 1-design: each row has $k - w$ stars and each column $b(k - w)/k$ stars, and (ii) the rows represent disjoint subsets of $\{0, 1\}^k$. Here a row represents the set of binary vectors of length k obtained by replacing its stars in all possible ways by 0s and 1s.

This concept was introduced in 1974 by Rivest [4, 5, 6] in order to find a hash function with good worst-case behavior with respect to partial-match queries. For example, the eight rows

00*0	11*1
100*	011*
*100	*011
1*10	0*01

form an $ABD(4, 3)$.

In order to save space, let us extend our alphabet with the minus sign, where a row containing r minus signs stands for the 2^r rows obtained by replacing these minus signs in all possible ways by 0s and 1s. Then the only other $ABD(4, 3)$ is the following:

*000
*111
-*10
-0*1
-10*

The theory is as follows (see [1, 2, 3, 6]).

PROPOSITION 0.1. (i) ([6]) *An $ABD(k, w)$ has exactly $bw/(2k)$ 0s and $bw/(2k)$ 1s in each column. In particular, $bw/(2k)$ is an integer.*

(ii) ([1]) *In an $ABD(k, w)$ with $w > 0$ any given star pattern occurs in an even number of rows. Moreover, among the rows with a given star pattern there are as many with an even number of 1s as with an odd number of 1s.*

(iii) *For $w \leq 4$ the only $ABD(k, w)$ are the trivial ones with $w = 0$ or $w = k$ (represented, respectively, by a single row of stars or minus signs only) and the two examples shown above.*

(iv) ([2]) *If $w > 3$, then $k \leq w(w - 1)/2$.*

*Received by the editors February 2, 1997; accepted for publication July 2, 1997; published electronically June 3, 1999.

<http://www.siam.org/journals/sicomp/28-6/31662.html>

[†]University of Technology, Den Dolech 2, P.O. Box 513, 5600 MB Eindhoven, the Netherlands (aeb@win.tue.nl).

- (v) ([3]) *There is no ABD(10, 5).*
 (vi) ([6]) *If ABD(k_i, w_i) exist for $i = 1, 2$, then there also is an ABD($k_1 k_2, w_1 w_2$).*
 (vii) ([1]) *Suppose that $k \geq w > 0$ and $k' \geq w' > 0$ and $k' \geq k$ and $w'/k' \geq w/k$. Then if an ABD(k, w) exists, and $2^{w'} w' / (2k')$ is an integer, then ABD(k', w') also exists.*

One may use generating function arguments to get more detailed information on the possible star patterns. See [1].

The purpose of this note is to show that an ABD(8, 5) exists:

```

-0000***  *01*10*0
-0001***  -*1*1*11
-001*0**   **11*001
- **1010*  *10*00*0
*0*1*110   *1*0*001
**01*111   *100**11
- **1110*  -1*0*10*
-*1*00*0   *1**0110
*010**01   *1**1000
-*1*0*11   -1**1*10
*010*1*0   *101*0*1

```

Now the smallest open case is the question of whether an ABD(12, 6) exists.

Acknowledgment. This note was inspired by a letter from Knuth, who asked whether there had been any progress on ABDs since 1976 and in particular whether the existence of an ABD(8, 5) was still open.

REFERENCES

- [1] A. E. BROUWER, *On associative block designs*, in Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I, Colloq. Math. Soc. János Bolyai 18, North-Holland, Amsterdam, 1978, pp. 173–184.
- [2] J. A. LA POUTRÉ, *A theorem on associative block designs*, Discrete Math. 58 (1986), pp. 205–208.
- [3] J. A. LA POUTRÉ AND J. H. VAN LINT, *An associative block design ABD(10, 5) does not exist*, Utilitas Math., 31 (1987), pp. 219–225.
- [4] R. L. RIVEST, *On hash-coding algorithms for partial match retrieval*, in Proceedings of the 15th Annual Symposium on Switching and Automata Theory, Long Beach, CA, IEEE Comput. Soc., 1974, pp. 95–103.
- [5] R. L. RIVEST, *Analysis of Associative Retrieval Algorithms*, Laboratoire de recherche en informatique et automatique, IRIA rapport 54, Institut de Recherche d'Informatique et d'Automatique, Domaine de Voluceau, Rocquencourt, Le Chesnay, France, 1974.
- [6] R. L. RIVEST, *Partial-match retrieval algorithms*, SIAM J. Comput., 5 (1976), pp. 19–50.