stichting

mathematisch

centrum

$\sum$

MC

DEPARTMENT OF PURE MATHEMATICS   ZW 49/76   JUNE

A.E. BROUWER

ON ASSOCIATIVE BLOCK DESIGNS

2e boerhaavestraat 49 amsterdam
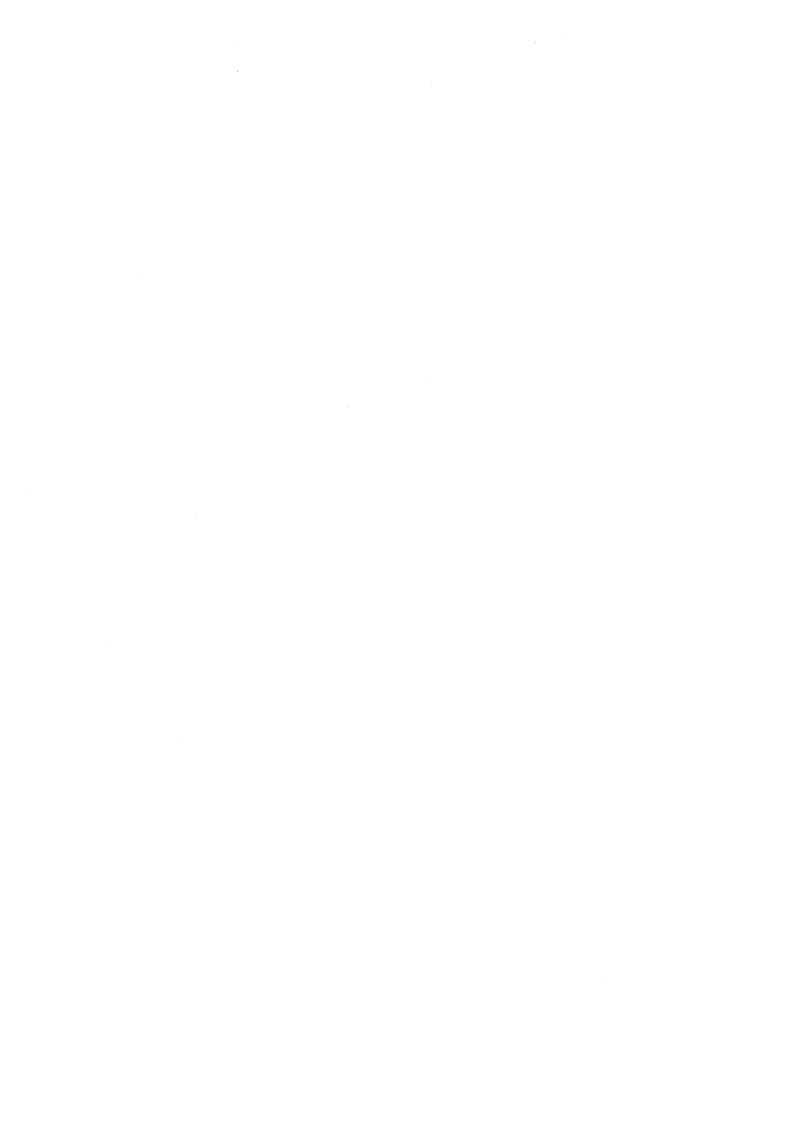
On associative block designs

by

A.E. Brouwer

ABSTRACT

We give a review of the known results on associative block designs.
Also a monotonicity theorem is proved.

0. INTRODUCTION

Recently Ronald L. Rivest in his paper "On hash-coding algorithms for partial-match retrieval", introduced the concept of an associative block design, abbreviated ABD. In order to find a hash-function with good worst-case behaviour with respect to partial-match queries he requires the following:

Let k and w be integer, $0 \leq w \leq k$, $k > 0$. An ABD (k,w) is a rectangular array with $b = 2^w$ rows and k columns with entries from $\{0,1,*\}$ such that:

(i)   each row has w digits and $(k-w)$ stars,

(ii)   each column contains the same number $\dfrac{b(k-w)}{k}$ of stars,

(iii) the rows represent disjoint subsets of $\{0,1\}^k$. That is, given any

two rows there is a column in which they contain differing digits. [a row is said to represent the subset of $\{0,1\}^k$ obtained by replacing the stars it contains in all possible ways by zeroes and ones.]

For example an ABD$(2,1)$ does not exist, since

$*0$

$*1$

satisfies (i) and (iii) but not (ii), and

$*0$

$1*$

satisfies (i) and (ii) but not (iii).

On the other hand an ABD$(4,3)$ exists (even in two nonisomorphic types).

It seems difficult to determine in general for which parameters k,w an ABD(k,w) exists; we can give however a few existence and non existence theorems. In the following pages all results known to us and some useful methods are described.

Convention: a roman letter stands for a positive integer, a greek letter for a real number.

1. RESTRICTIONS ON ABD's .

In this section some restrictions and non-existence results are given.

PROPOSITION 1. [Rivest] *An* ABD(k,w)

(i) *has exactly* $\frac{bw}{2k}$ *zeroes and* $\frac{bw}{2k}$ *ones in each column. In particular* $\frac{bw}{2k}$ *is an integer.*

(ii) *has exactly* $\binom{w}{u}$ *rows which agree in exactly* u *positions with any word* $x \in \{0,1\}^k$.

(iii) *satisfies*

$$k\left(\frac{bw}{2k}\right)^2 \geq \binom{b}{2}$$

that is

$$w^2 \geq 2k(1-\frac{1}{b}).$$

PROOF.

(i) There are $\frac{bw}{k}$ digits in each column. Since there are as many words $x \in \{0,1\}^k$ that contain a one as words containing a zero in a given column, and each row containing a digit in that column contributes the same number of words (namely 2^{k-w}) it follows that each column contains the same number of zeros and ones.

(ii) Let k(u) be the number of rows which agree in exactly u positions with a given word $x \in \{0,1\}^k$. Then by writing down the weight enumerator (counting differences with u) we find:

$$(1+X)^k = (1+X)^{k-w} \cdot \sum_{u=0}^{w} k(u) \cdot X^u,$$

hence

$$k(u) = \binom{w}{u}.$$

(iii) Count differences between rows: in each column there are $\left(\frac{bw}{2k}\right)^2$ differences, hence in the entire array $k\left(\frac{bw}{2k}\right)^2$ differences. But each of the $\binom{b}{2}$ pairs of rows must contain at least one difference. □

PROPOSITION 2. [v. Emde Boas] *Let* w > 0. *A given star-pattern occurs in an even number of rows.*

This proposition can be greatly generalized using generating function arguments as in the proof of proposition 1 (ii) above.

For example: let us divide the columns of an ABD(k,w) into two nonempty sets K_1 and K_2 and count the differences with a fixed word, say 0^k, in K_1 and K_2 separately.

If r is a row index and K is a set of column indices we will write $N_r(*,K)$ for the number of stars in row r and some column of K. $N_r(0,K)$ and $N_r(1,K)$ are defined similarly. Hoping that no confusion will arise we suppress the subscript r most of the time.

Put $\qquad a = |K_1|, \qquad b = |K_2| \qquad$ (so that a+b=k).

Now we find

$$(1+X)^a(1+Y)^b = \sum_{\text{rows}} (1+X)^{N(*,K_1)}X^{N(1,K_1)}(1+Y)^{N(*,K_2)}Y^{N(1,K_2)}.$$

Putting X = −1 we get

$$0 = \sum_{\substack{\text{rows with} \\ N(*,K_1)=0}} (-1)^{N(1,K_1)}(1+Y)^{k-w}Y^{N(1,K_2)}$$

hence (after dividing by $(1+Y)^{k-w}$: for each fixed j:

$$(1) \qquad 0 = \sum_{\substack{N(*,K_1)=0 \\ N(1,K_2)=j}} (-1)^{N(1,K_1)} .$$

In particular: (if K is the set of all columns) let $|K_1| = w$, $|K_2| = k - w$.

$$0 = \sum_{\substack{\text{rows with a} \\ \text{fixed star pattern}}} (-1)^{N(1,K)} .$$

This implies proposition 2: the number of rows with a fixed star pattern is even, but also: among the rows with a given star pattern as many rows have an odd number of ones, as there are rows with an even number of ones.

Of course instead of splitting up the set of columns into two parts, any other partition gives similar equations.

PROOF. There are 2^w words in $\{0,1\}^k$ which have zeroes on the positions of the star pattern. Each row with the given star pattern contributes 1, while each other row contributes an even number of words to this set of 2^w words. Since 2^w is even, the number of times that the contribution is 1 must be even. $\square$

PROPOSITION 3. *Let w > 3.*

(i) *If two rows agree in all but one position then $\binom{w}{2} \geq k$.*

(ii) *Otherwise $w^2 > 2k$*

[note that this improves slightly on proposition 1 (iii).]

PROOF.

(i) Suppose two rows are equal except at the i-th column where one has a zero and the other a one. The remaining b-2 rows must differ from both rows so that there must be a difference with each of them not in the i-th column.

That is: $b-2 \leq (w-1) \cdot \dfrac{bw}{2k}$ or $\binom{w}{2} \geq k(1 - \dfrac{2}{b})$.

A. $\qquad (w-1) \cdot \dfrac{bw}{2k} = b - 2$

Since b is divisible by 4 both sides are $\equiv 2 \bmod 4$. $2^w | b$ hence $2^{w-1} | k$ so $2^{w-1} \leq k \leq \dfrac{2}{3} w^2$ by proposition 1. iii. The only solutions are $w = 4$ and $w = 5$ which give

$$\dfrac{6 \cdot 2^4}{k} = 2^4 - 2 \Rightarrow k = \dfrac{3 \cdot 2^4}{7} \notin \mathbb{Z}$$

and

$$\dfrac{10 \cdot 2^5}{k} = 2^5 - 2 \Rightarrow k = \dfrac{2^5}{3} \notin \mathbb{Z}.$$

[Note: k=4, w=3 gives a solution]

B. $\qquad (w-1) \cdot \dfrac{bw}{2k} = b - 1$.

The right side is odd, so w is even and $\frac{bw}{2k}$ is odd hence $2^w | k$ so $2^w \le k \le \frac{2}{3} w^2$ which is impossible.

Therefore $(w-1) \cdot \frac{bw}{2k} \ge b$ or $\binom{w}{2} \ge k$.

(ii) By proposition 2 the rows can be paired such that two rows in a pair have the same star pattern. By hypothesis they differ in more than one position i.e. counting differences:

$$(b-2) + 2 \le w \cdot \frac{bw}{2k} \quad \text{i.e.} \quad w^2 \ge 2k.$$

Now suppose equality holds, then each row differs in exactly 2 positions from its companion row (with the same star pattern) and in exactly 1 position from each other row. That is, we have

```
*....*00..000
*....*00..011
          01  (bw/2k -1 times)
          10  (bw/2k -1 times)
```

(If the first two rows have 00 and 11 in the last two columns, then all other rows with a 1 in the last column must have only stars and zeroes in the remaining last w-1 columns, and in order to differ from the second row a zero in the last column but one.) Since pairing should be unique we must have $\frac{bw}{2k} = 2 \to 2^w = 2w$, impossible for $w \ge 3$. $\square$

[It is probably to a proposition of this type that Rivest refers when he says that by a slight extension of proposition 1 (iii) it can be seen that an ABD(8,4) does not exist.]

In order to save space we extend our notation for an ABD as follows: a row containing r "-"'s will represent 2^r rows of the actual ABD obtained by independently replacing each - by a 0 or a 1.
For instance the row -- represents the ABD(2,2):

```
00
01
10
11
```

Now proposition 3 (i) can be rephrased as:

"If an ABD(k,w) contains a - then $\binom{w}{2} \geq k$".

The following proposition classifies all ABD's with $w \leq 4$. Two ABD's are considered the same when one is obtained from the other by permuting rows & columns and possibly interchanging all zeroes and ones in some columns.

PROPOSITION 4.

(i)   *For each* $k > 0$ *there exists a unique* ABD(k,0) *nl.* $*^k$.

(ii)   *An* ABD(k,1) *exists only for* $k = 1$:   -

(iii) *An* ABD(k,2) *exists only for* $k = 2$:   - -

(iv)   *There are three types* ABD(k,3):

     One with $k = 3$:   - - -

     Two with $k = 4$:

*000		00*0
*111		100*
-*10	and	*100
-0*1		1*10
-10*		11*1
		011*
		*011
		0*01

(v)   *An* ABD(k,4) *exists only for* $k = 4$:   ----.

PROOF. Of course for any $w > 0$ a unique ABD(w,w) exists, nl $-^w$. Now assume $0 \leq w < k$.

(i)   Obvious

(ii) $\frac{bw}{2k} = \frac{1}{k} \in Z$ implies $k = 1$.

(iii) $\frac{bw}{2k} = \frac{4}{k} \in Z$ implies $k \in \{1,2,4\}$. Since we assumed $w < k$ we have only to check for an ABD(4,2). This ABD necessarily starts

     **00   (by normalizing)

     ..01   (two rows with exactly one 1

     ..1.   must differ somewhere)

     ....

But now the third column cannot contain 2 stars.

(iv) $\frac{bw}{2k} = \frac{12}{k} \in Z$ and $k > w$ implies $k \in \{4,6,12\}$.

$k = 12$ is impossible since $12 \cdot (1)^2 \neq \binom{8}{2}$.

$k = 6$ is impossible since $6 \cdot (2)^2 \neq \binom{8}{2}$.

Therefore $k = 4$.

If we start

    *000

    *111

then the other six rows form two groups like

    d10*

    d*10   (d=0,1)

    d0*1

These two groups can be oriented in two ways with respect to each other, thus giving the two examples quoted above:

*000	and	*000
*111		*111
010*		010*
0*10		0*10
00*1		00*1
110*		101*
1*10		1*01
10*1		11*0.

If we start *000 and do not allow two complementary rows,

        *011

then we get

    *000

    *011

    *010

since there are three. zeroes in each column. But now the first column contains too many stars. Finally if we start *000 then we get

*001

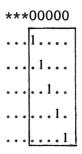| *000 | | *000 |
*001		*001
001*		001*
01*0	or	01*0
101*		1*10
11*0		110*
0*0		01*1
1*		1*11

The first one cannot be completed and the second one is isomorphic to the first type mentioned in the proposition.

(v)   w is a power of 2 implies k is a power of 2. But $w^2 = 16 > 2k$, k < 8 & k > w = 4 is impossible.   □

In the checking of small examples like the ABD(4,3) above we often use the following arguments:

Let x be a word in $\{0,1\}^k$ represented by the i-th row in an ABD(k,w). Look at the k words in $\{0,1\}^k$ which have Hamming distance 1 to x. k-w of these words are again represented by the i-th row of the ABD (namely those words that differ from x in a position where the i-th row has a star). The remaining w words are represented by w different rows of the ABD (for if $x+e_j$ and $x+e_k$ (j ≠ k) are represented by the same row then this row has stars in the j-th and k-th positions i.e. it also represents x).

For example if the first row of an ABD(8,5) is ***00000 then we may write immediately:

```
***00000
...|1....|
...|.1...|
...|..1..|
...|...1.|
...|....1|
```
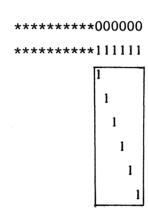
where the next five rows are just those rows which contain only one 1. Furthermore, all $\binom{5}{2}$ pairs of these rows must contain a difference, so the square indicated contains at least $\binom{5}{2} = 10$ zeroes. In fact from two positions symmetric w.r.t. the diagonal at least one must contain a zero.

Reasoning this way we get for instance:

LEMMA. *An* ABD(16,6) *does not contain two rows differing in all 6 digit positions.*

PROOF. We get

```
**********000000
**********111111
```

$$
\begin{array}{|cccccc|}
\hline
1 &   &   &   &   &   \\
  & 1 &   &   &   &   \\
  &   & 1 &   &   &   \\
  &   &   & 1 &   &   \\
  &   &   &   & 1 &   \\
  &   &   &   &   & 1 \\
\hline
\end{array}
$$

The ABD contains $2^6 = 64$ rows, each column contains 40 stars and 12 ones and 12 zeroes. Therefore there are $6.12 = 72$ differences with the second row to be divided among 63 rows, that is, at most 9 differences may be spoiled. Now the first row spoils 5 differences (it has 6 while only 1 is needed) and the six rows containing only one 1 spoil at least $\binom{6}{2} - 6 = 9$ differences, which is too much. $\square$

LEMMA. *An* ABD(10,5) *does not contain two rows differing in all 5 digit positions.*

PROOF. We get

```
*****00000
*****11111
```

$$\begin{bmatrix} 1 & & & & \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & 1 \end{bmatrix}$$

The ABD contains $2^5 = 32$ rows, each column contains 16 stars and 8 ones and 8 zeroes. At most $5.8 - 31 = 9$ differences may be spoiled. Now the first row spoils 4 and the five rows containing only one 1 spoil at least $\binom{5}{2} - 5 = 5$ differences with the second row which means that all other rows have exactly one 0 in the last five columns. Now look at the five rows differing in one of the last five columns from the word 1111100000. These five rows again have at least $\binom{5}{2}$ zeroes in their last five columns which is impossible unless at least two of them coincide with one of the earlier rows:

```
*****00000
*****11111
*****10000
*****01000
.......1..
........1.
.........1
```

But now we've spoiled $4 + 3 + 3 > 9$ differences, again too much. □

LEMMA. *An* ABD(16,6) *does not contain two rows differing in 5 digit positions.*

PROOF. Let the first row be $*^{10}0^6$, and the second row be in $\{0,1,*\}^{11}1^5$. Consider for each choice of $d \in \{0,1\}^{10}$ the five rows differing in one of the last five columns from $d.0^6$. For each d we spoil 5 differences while we have $9 - 4 = 5$ differences to spoil, that is, we get each time the same rows, all starting with $*^{10}$. But one such a row spoils 4 differences and

we need at least two, thus spoiling 4 + 2*4 > 9 differences with the 2nd row. □

LEMMA. *An ABD(16,6) does not contain two rows with the same star pattern differing in exactly 2 digit positions.*

PROOF. Let the first two rows be $*^{10} 0^6$ and $*^{10} 0^4 1^2$. These are both rows with an even number of ones, and by the argument after proposition 2 it follows that there are at least two rows of the form $*^{10} d^6$ with an odd number of ones. By the previous lemma and proposition 3 (i) these rows cannot differ at 1 or 5 positions from the first two rows, hence they differ at exactly 3 positions from both, i.e., they look like $*^{10}(0011)(01)$.

In columns 11-14 we have a total of $4 \times 12 = 48$ ones, and, as we just saw, at least two of these ones are on the same row; hence there are at most 46 rows containing one of these ones. The remaining rows (at least 64-2-46= = 16) differ from the first two rows only in the last two columns, i.e., they look like $\cdot^{14}01$ or $\cdot^{14}10$. Since a column contains 12 ones, both of these types must occur and one, say $\cdot^{14}01$, occurs at least 8 times. Now fix one row of the other type; it has 9 differences to spoil, and the 8 rows of type $\cdot^{14}01$ each spoil one difference; but the four rows differing from the fixed row in exactly one position but not at one of the last two columns spoil at least $\binom{4}{2} - 4 = 2$ differences. Noting that these four rows are others than the eight rows found earlier, and that $8 + 2 > 9$ we arrive at a contradiction. □

LEMMA. *An ABD(16,6) does not contain two rows with the same star pattern differing in exactly 4 digit positions.*

PROOF. Let the first two rows be $*^{10}0^6$ and $*^{10}0^2 1^4$. As before it follows that these are two rows of the form $*^{10}d^6$ with an odd number of ones. Both must differ from the first two rows in 3 positions and from each other in 4 positions. Therefore, there are only two essentially different possibilities:

A. $\qquad *^{10} 1\ 00011$

$\qquad\qquad *^{10} 1\ 01100$

and

B. $*^{10}$ 0 10011

$*^{10}$ 1 00101.

Divide the columns into three subsets: $K_1 := \{\text{cols. 1-10}\}$, $K_2 := \{\text{col. 11}\}$ and $K_3 := \{\text{cols. 12-16}\}$. Writing down the appropriate weight enumerator we find

$$(1+X)^{10}(1+Y)(1+Z)^5 =$$

$$= \sum (1+X)^{N(*,K_1)} X^{N(1,K_1)} (1+Y)^{N(*,K_2)} Y^{N(1,K_2)} (1+Z)^{N(*,K_3)} Z^{N(1,K_3)}$$

Putting $Y = 0$ and $Z = -1$ we get

$$\sum_{\substack{N(1,K_2)=0 \\ N(*,K_3)=0}} (-1)^{N(1,K_3)} (1+X)^{N(*,K_1)} X^{N(1,K_1)} = 0 .$$

Since the first row has spoiled already $3 + 2 + 2 = 7$ differences it cannot afford to spoil $3 + 2 = 5$ more, i.e., there cannot be more rows of type $*^{10}d^6$. The contribution of the first four rows to this sum is $2(1+X)^{10}$ in case A and $(1+X)^{10}$ in case B. All further rows contribute either 0 or $(-1)^{N(1,K_3)}(1+X)^9 X^{N(1,K_1)}$ to this sum. Looking at the coefficient of X^{10} we find in case A at least 2 rows and in case B at least 1 row of the type $(1*^9)*d^5$ with an odd number of ones among the d^5; by symmetry we find as many of the type $(0*^9)*d^5$. Since the first row has spoiled already 7 differences we cannot have $d^5 = 1^5$ and we can have at most once $d^5 = (0^2 1^3)$. Likewise because of the second row we can have at most once $d^5 = (0^4 1)$. Therefore we are in case B and may assume that the fifth row looks like $(1*^9)*0(0^3 1)$. Now look at the row compatible with $1^{11} 0^5$. It has a 1 in the 11th column and a 0 in one of the columns 13-15 (since it must differ from the first and from the fifth row). But this means that it spoils a tenth difference with the 2nd row. Contradiction. □

Conclusion: If an ABD(16,6) exists, it consists of 32 pairs of rows with the same star pattern, where each time the rows forming a pair differ in exactly 3 positions.

It has not yet been possible to rule out the existence of an ABD(8,5) or ABD(10,5) or ABD(16,6) with these methods. In fact we do not have an example of parameters k,w such that $w^2 > 2k$ and $2k|bw$ for which we can prove the non-existence of ABD(k,w).

2. CONSTRUCTION OF ABD's

In this section some construction methods will be given to make new ABD's out of a given one. It appears that all known ABD's can be constructed in this way from the known ABD(k,0), ABD(k,k), ABD(4,3).

THEOREM 1. [Rivest] *Suppose that an* ABD(k_i,w_i) *exists* (i=1,2). *Then an* ABD(k_1k_2,w_1w_2) *exists.*

PROOF. We may suppose $w_2 \neq 0$. Partition the rows of an ABD(k_2,w_2) in two disjoint sets R_0 and R_1 such that $|R_0| = |R_1|$. Now replace in the given ABD(k_1,w_1) each star by $*^{k2}$, each 0 in all possible ways by a row in R_0 and each 1 in all possible ways by a row in R_1. It is readily verified that the array thus obtained is an ABD(k_1k_2,w_1w_2). □

COROLLARY. *For each* t *an* ABD($4^t,3^t$) *exists. In particular* ABD(16,9) *and* ABD(64,27) *do exist.*

THEOREM 2. *Suppose that*
(i) $k \geq w > 0$,
(ii)   ABD(k,w) *exists,*
(iii) $k' \geq w' > 0$,
(iv) $\frac{w'}{k'} \geq \frac{w}{k}$, (v) $k' \geq k$,
(vi) $\frac{2^{w'} \cdot w'}{2k'} \in Z$.

Then ABD(k',w') *exists.*

COROLLARY 2. *If for some* w > 0 ABD(2^e,w) *exists, then for each* z *with* $w \leq z \leq 2^e$ *an* ABD(2^e,z) *exists.*

More generally:

COROLLARY 3. *If for some* $w > 0$ *ABD(k,w)* *exists and* $k = k_0 \cdot 2^e$, k_0 *odd then*
$ABD(k, w+ik_0)$ *exists for* $0 \le i \le \dfrac{k-w}{k_0}$

COROLLARY 4. *If* ABD(k,w) *exists and* α *is such that* $\alpha \ge 1$ *and* $\alpha k \in Z$,
$\alpha w \in Z$ *then* ABD($\alpha k, \alpha w$) *exists.*

COROLLARY 5. *For* $k \ge 32$ *ABD(2k,k)* *exists.*

PROOF. ABD(64,27) exists, hence ABD(64,32) exists. Now apply the previous corollary.

PROOF of theorem 2:

We will prove corollaries 3 and 4. Then the theorem follows:

> If $w_1 = \dfrac{w'}{k'} \cdot k$ is an integer then
>
> ABD(k,w) exists $\Rightarrow$
> ABD(k,w_1) exists $\Rightarrow$
> ABD(k',w') exists.
>
> If $w_2 = \dfrac{w}{k} \cdot k'$ is an integer then
> ABD(k,w) exists $\Rightarrow$
> ABD(k',w_2) exists $\Rightarrow$
> ABD(k',w') exists.

But at least one of w_1 and w_2 must be an integer: Let $k = k_0 \cdot 2^e$, $k' = k_0' \cdot 2^{e'}$ with k_0 and k_0' odd. $\dfrac{w}{k_0}$ and $\dfrac{w'}{k_0'}$ are integers so if $e \ge e'$ then $w_1 \in Z$ and if $e \le e'$ then $w_2 \in Z$.

PROOF of corollary 3:

It is sufficient to construct from an ABD(k,w) an ABD(k,$w+k_0$) (provided that $0 < w < k$). If we can replace k_0 stars in each row and
$\dfrac{2^w \cdot k_0}{k} = 2^{w-e}$ stars in each column by a minus then we're through. But this can always be done:

PROPOSITION. *Let the rectangular* m $\times$ n *array* A *with entries in* $\{0,1\}$ *have constant row sums* p *and constant column sums* q *(thus mp=nq). If* $p_0 \le p$ *and* $q_0 \le q$ *and* $mp_0 = nq_0$ *then* A *is the sum of two 0-1 matrices with constant row and column sums:* $A = A_0 + A_1$ *where* A_0 *has row sums* p_0 *and column sums* q_0.

PROOF. (communicated by A. Schrijver)

We use a "flow in networks" argument
as follows:

Make a bipartite graph on the rows
and columns of A as follows:

Let $G = \{s, t, r_i(1 \leq i \leq m), c_j(1 \leq j \leq n)\}$ with edges
$\{(r_i, c_j) | A(i,j) = 1\} \cup \{(s, r_i) | i \leq m\} \cup \{(c_j, t) | j \leq n\}$.

If all edges (r_i, c_j) have capacity 1, (s, r_i) have capacity p and edges
(c_j, t) have capacity q then obviously there is a flow with value pm = qn
from s to t. Reducing the capacities of (s, r_i) to p_0 and of (c_j, t) to q_0 we
have a flow $p_0 m = q_0 n$. But as is well known if all capacities are integers
and the total flow is an integer then the flow through each edge can be
chosen to be an integer. In our case this gives flow 0 or 1 through each
(r_i, c_j), thus specifying the matrix A_0. $\square$

PROOF of corollary 4:

It is sufficient to construct from an ABD(k,w) an ABD(k+ℓ,w+v) where
$\frac{v}{\ell} = \frac{w}{k}$ and (v,ℓ) = 1. If $k = k_0 \cdot 2^e$ (k_0 odd) and $w = w_0 \cdot k_0$ then $\frac{v}{\ell} = \frac{w}{k} = \frac{w_0}{2^e}$,
so ℓ is a power of 2.

If σ is a cyclic shift on ℓ symbols then add to the i-th row of the
given ABD(k,w) the symbols $\sigma(*^{\ell-v}\_^v)$. ℓ is a divisor of b hence each of the
ℓ adjoined columns contains the same number $\frac{\ell-v}{\ell} \cdot b = \frac{k-w}{k} \cdot b$ of stars. There-
fore in this way we obtain an ABD(k+ℓ,w+v).
This completes the proof of theorem 2. $\square$

Note: Rivest gave a weak form of corollary 4 by stating:
If ABD(k,w) and ABD(k',w') exist and $\frac{w}{k} = \frac{w'}{k'}$ then ABD(k+k',w+w') exists.

3. PARAMETERS OF POSSIBLE ABD's WITH k ≤ 20; 0 < w < k:

k	w	*'s per column	0's and 1's per column	examples known
4	3	2	3	2 types
8	5	12	10	-
	6	16	24	yes
	7	16	56	yes
10	5	16	8	-
12	6	32	16	-
14	7	64	32	-
16	6	40	12	-
	7	72	28	-
	8	128	64	-
	9	224	144	yes
	10	384	320	yes
	11	640	704	yes
	12	1024	1536	yes
	13	1536	3328	yes
	14	2048	7168	yes
	15	2048	15360	yes
18	9	256	128	-
20	10	512	256	-
	15	8192	12288	yes

REFERENCES

[1] P.v. EMDE BOAS, *Oral communication*.

[2] R.L. RIVEST, *On hash-coding algorithms for partial-match retrieval*, Proceedings of the 15th annula symposium on Switching and Automata theory, october 1974, p. 95-103.

[3] R.L. RIVEST, *Analysis of associative retrieval algorithms*, Laboratoire de recherche en informatique et automatique, IRIA rapport no. 54, février 1974.

[4] A. SCHRIJVER, *Oral communication*.