JOURNAL OF COMBINATORIAL THEORY (A) 13, 246–273 (1972)

An Existence Theory for Pairwise Balanced Designs II. The Structure of PBD-Closed Sets and the Existence Conjectures*

RICHARD M. WILSON

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210

Communicated by Bruce Rothschild

Received March 8, 1970

I. INTRODUCTION

We shall use the notation and results of Part I of this article [8]. In [8], we have already remarked that

$$\lambda(v-1) \equiv 0 \pmod{k-1} \tag{1}$$

and

$$\lambda v(v-1) \equiv 0 \pmod{k(k-1)} \tag{2}$$

are necessary conditions for the existence of a (v, k, λ)-BIBD with $v > 0$, and we have mentioned

THE EXISTENCE CONJECTURE. *Given positive integers k and λ, there exists a constant $C = C(k, \lambda)$ such that $v \in B[k; \lambda]$ for every integer $v \geqslant C$ which satisfies the congruences* (1) *and* (2).

The most significant work to date on the Existence Conjecture is that of Hanani [3, 4, 5]. It is shown that the conditions (1) and (2) are both necessary and sufficient for the existence of a (v, k, λ)-BIBD when $k = 3,4$ and for all λ. Hanani also proves that (1) and (2) are sufficient for the existence of a $(v, 5, \lambda)$-BIBD with one exception: namely, no $(15, 5, 2)$-BIBD exists.

Recall that a set K of positive integers is said to be PBD-*closed* (or simply a *closed set*) iff K is equal to its closure $B[K]$. From [8, Proposition 5.2], we have

* This research was supported in part by NSF Research Grant GP 9375 (Ohio State Research Foundation Project Nos. 2548 and 2736).

1.1. LEMMA. *For any K and λ, $B[K; \lambda]$ is a closed set.*

With the Existence Conjecture in mind, this observation suggests the undertaking of the study of the structure of closed sets in general. It is at first surprising that closed sets must necessarily behave very regularly at their "tail ends." Given any set K, we denote by $\beta(K)$ the greatest common divisor of the numbers $\{k(k-1) \mid k \in K\}$ (see Section 2).

MAIN THEOREM. *Every closed set K is eventually periodic with period $\beta(K)$. That is, there exists a constant C such that, for every $k \in K$, $\{v \mid v \geqslant C, v \equiv k \pmod{\beta(K)}\} \subseteq K$.*

An interesting consequence of the Main Theorem is that every closed set K is finitely generated in the sense that there exists a finite set $K_0 \subseteq K$ such that $K = B[K_0]$. Applications to the sets $B[k; \lambda]$ yield

THEOREM. *The Existence Conjecture is valid for a pair k, λ whenever* (i) *$k/(k, \lambda)$ is one or a prime power (in particular, whenever k is a prime power), or* (ii) *$\lambda \geqslant ([\frac{1}{2}k] - 1)([\frac{1}{2}k] - 2)$.*

Partial results can be given in any case and the problem is at least greatly reduced. For example, we prove that all sufficiently large integers $v \equiv 1$ or $6 \pmod{30}$ belong to $B[6]$ and that, if there exists a single $v_0 \in B[6]$ with $v_0 \equiv 16$ or $21 \pmod{30}$, then the Existence Conjecture holds for $k = 6$, $\lambda = 1$.

It is hoped that the theory of closed sets can be applied to other problems concerning pairwise balance of the form of the Existence Conjecture. Indeed, a similar conjecture concerning the sets $B[K; \lambda]$ can be formulated and we give analogous results. The sets $F_K[d]$ can also be described in terms of K.

2. THE EXTENDED EXISTENCE CONJECTURE, THE PARAMETERS α AND β

In this section we will want to consider the greatest common divisor of possibly infinite sets J of integers. We define $gcd(J)$ to be the unique non-negative generator of the ideal in the ring of integers which is generated by J. One sees immediately that $d = gcd(J)$ is the unique non-negative integer satisfying (i) $d \mid k$ for all $k \in J$, and (ii) if $c \mid k$ for all $k \in J$, then $c \mid d$. Clearly, if $J_1 \subseteq J_2$, then $gcd(J_2) \mid gcd(J_1)$. We shall also need

2.1. PROPOSITION. *There is a finite set $J_0 \subseteq J$ such that $gcd(J_0) = gcd(J)$.*

Proof. Since $gcd(J)$ is an element of the ideal generated by J, we have $gcd(J) = a_1k_1 + a_2k_2 + \cdots + a_nk_n$ for some integers a_i and elements $k_i \in J$. Putting $J_0 = \{k_1, k_2, ..., k_n\}$, it easily follows that $gcd(J) = gcd(J_0)$.

Given a set K of positive integers, we define the parameters:

$$\alpha(K) = gcd\{k - 1 \mid k \in K\},$$

$$\beta(K) = gcd\{k(k - 1) \mid k \in K\}.$$

2.2. PROPOSITION. *If* $v \in B[K; \lambda]$, *then*

$$\lambda(v - 1) \equiv 0 \pmod{\alpha(K)}, \tag{3}$$

and

$$\lambda v(v - 1) \equiv 0 \pmod{\beta(K)}. \tag{4}$$

Proof. Given $v \in B[K; \lambda]$, let $(X, \mathscr{L})$ be a (v, K, λ)-PBD, where $\mathscr{L} = (B_i \mid i \in I)$ is the family of blocks. Fix $\theta \in X$. We count the number N of pairs (x, i) such that $x \neq \theta$, $\{x, \theta\} \subseteq B_i$. If we fix an index $i_0 \in I$, then the number of $x \neq \theta$ such that $\{x, \theta\} \subseteq B_{i_0}$ is either 0 or $|B_{i_0}| - 1 \equiv 0 \pmod{\alpha(K)}$. Thus $N \equiv 0 \pmod{\alpha(K)}$. On the other hand, if we fix $x_0 \neq \theta$, then the number of indices $i \in I$ for which $\{x_0, \theta\} \subseteq B_i$ is λ and hence $N = \lambda(v - 1)$. This proves congruence (3).

Now we count the number N' of ordered triples (x, y, i) such that $x \neq y$, $\{x, y\} \subseteq B_i$. If we fix an index $i_0 \in I$, then the number of pairs (x, y), $x \neq y$, $\{x, y\} \subseteq B_{i_0}$, is $|B_{i_0}|(|B_{i_0}| - 1) \equiv 0 \pmod{\beta(K)}$. Thus $N' \equiv 0 \pmod{\beta(K)}$. If we fix an ordered pair (x, y), $x \neq y$, then the number of indices $i \in I$ such that $\{x, y\} \subseteq B_i$ is λ and thus $N' = \lambda v(v - 1)$. This proves congruence (4).

Remark. In some particular cases, it is easy to prove the non-existence of certain PBD's with potentially multiple block sizes. For example, $45 \notin B[\{6, 7\}; 1]$ although the necessary conditions (3) and (4) are satisfied. As in [6], consideration of the dispersion at any point of a hypothetical (45, {6, 7}, 1)-PBD shows that there must be precisely 4 blocks of size 7 which contain that point. But it would then follow that the total number of blocks of size 7 is $45 \cdot 4/7$ which is not an integer.

We generalize the Existence Conjecture:

THE EXTENDED EXISTENCE CONJECTURE. *Given a set K of positive integers and a positive integer λ, there exists a constant $C = C(K, \lambda)$ such that $v \in B[K; \lambda]$ for all integers $v \geqslant C$ satisfying congruences* (3) *and* (4).

Some cases of this conjecture are known to be valid. In his work on BIBD's, Hanani [3] proves that $B[\{3, 4, 6\}]$ consists of those positive integers $v \equiv 0$ or $1 \pmod 3$; $B[\{4, 5, 8, 9, 12\}]$ of those $v \equiv 0$ or $1 \pmod 4$.

We seek to describe a closed set K in terms of $\alpha(K)$ and $\beta(K)$. For a closed set $K = \mathrm{B}[K]$, the Extended Existence Conjecture would assert the existence of a constant C such that $\{v \in K \mid v \geqslant C\}$ consists of precisely those $v \geqslant C$ satisfying

$$v \equiv 1 \pmod{\alpha(K)} \tag{5}$$

and

$$v(v-1) \equiv 0 \pmod{\beta(K)}. \tag{6}$$

2.3. PROPOSITION. *For any set K of positive integers, $\alpha(B[K]) = \alpha(K)$ and $\beta(B[K]) = \beta(K)$.*

Proof. Since $K \subseteq B[K]$, we have $\alpha(B[K]) \mid \alpha(K)$ and $\beta(B[K]) \mid \beta(K)$. On the other hand, Proposition 2.2 asserts that $\alpha(K) \mid v - 1$ and $B(K) \mid v(v-1)$ for every $v \in B[K]$, and hence $\alpha(K) \mid \alpha(B[K])$, $\beta(K) \mid \beta(B[K])$.

Given a set K, we note that $\alpha(K) = 0$ iff $\beta(K) = 0$ iff $K = \varnothing$ or $\{1\}$. Since $\alpha(K) \mid k(k-1)$ for every $k \in K$, we have

$$\alpha(K) \mid \beta(K). \tag{7}$$

Since $2 \mid k(k-1)$ for all $k \in K$,

$$2 \mid \beta(K). \tag{8}$$

We define $\gamma(K) = \beta(K)/\alpha(K)$ if $\alpha(K) \neq 0$ and $\gamma(K) = 1$ if $\alpha(K) = 0$ Note that $\gamma(B[k]) = \gamma(\{k\}) = k$.

2.4. PROPOSITION *For any set K, $\alpha(K)$ and $\gamma(K)$ are relatively prime.*

Proof. If $\alpha(K) = 0$, we are done. Assuming $\alpha(K) \neq 0$, let d be a common divisor of $\alpha(K)$ and $\beta(K)$. Then $d \cdot \alpha(K) \mid k(k-1)$ for each $k \in K$. Now $\alpha(K)$, and hence d, divides each $k - 1$; therefore both $\alpha(K)$ and d are relatively prime to each $k \in K$. Then $d \cdot \alpha(K) \mid k - 1$ for each $k \in K$ and consequently $d \cdot \alpha(K) \mid \alpha(K)$. We conclude $d = \pm 1$ and the proposition is established.

Conditions (7) and (8) and Proposition 2.4 characterize those pairs of integers which occur as $\alpha(K)$ and $\beta(K)$ for some K. Indeed, let a and b be non-negative integers such that $a \mid b$, b is even, and $(a, b/a) = 1$ (admitting $a = b = 0$). To the pair a, b we may attach the "model" closed set $H = H(a, b) = \{v > 0 : a \mid v - 1, b \mid v(v-1)\}$.

2.5. PROPOSITION. $\alpha(H) = a$, $\beta(H) = b$, and H is a closed set.

Proof. Clearly $a \mid \alpha(H)$ and $b \mid \beta(H)$. For any $n > 0$, $nb + 1 \in H$, and hence $\beta(H) \mid nb(nb + 1)$. If $\beta(H) = 0$, it follows $b = a = 0$, $H = \{1\}$. Otherwise we may take $n \equiv 1, -1 \pmod{\beta(H)}$ successively to find $\beta(H) \mid b(b + 1)$ and $\beta(H) \mid b(b - 1)$. Since b is even, $(b - 1, b + 1) = 1$, from which it follows that $\beta(H) \mid b$. Hence $\beta(H) = b$.

Since $(a, c) = 1$, where $c = b/a$, we can select $v > 0$ such that $v \equiv 0 \pmod{c}$ and $v \equiv 1 \pmod{a}$. Then $v \in H$, hence $\alpha(H) \mid v - 1$, and consequently $(\alpha(H), c) = 1$. But then, $a \mid \alpha(H) \mid \beta(H) = ac$ implies $\alpha(H) = a$.

By 2.2, $v \in B[H]$ implies $\alpha(H) \mid v - 1$ and $\beta(H) \mid v(v - 1)$. From what we have proved above, this means $v \in H$. Thus H is closed.

It is easy to see that $\{k \in K \mid k = 1 \text{ or } k \geqslant M\}$ is a closed set for any closed set K. We say that two sets S and T *eventually coincide* iff there exists a constant M such that $\{s \in S \mid s \geqslant M\} = \{t \in T \mid t \geqslant M\}$. The Extended Existence Conjecture for $\lambda = 1$ is equivalent to the assertion that for any closed set K, $H(\alpha(K), \beta(K))$ and K eventually coincide.

3. EVENTUAL PERIODICITY AND FIBERS

Z will denote the ring of integers and for any integer π, $Z/(\pi)$ is to be the ring of residue classes modulo π. Let J be a set of integers. A *π-fiber* of J is a residue class $f \in Z/(\pi)$ for which there exists $k \in J$ with $k \equiv f \pmod{\pi}$. Thus the set of all π-fibers of J is just the image of J under the canonical epimorphism $Z \to Z/(\pi)$. A π-fiber f of J is said to be *complete* iff there exists a constant M such that $\{v \mid v \geqslant M, v \equiv f \pmod{\pi}\} \subseteq J$. Finally, we say that J is *eventually periodic with period π* iff all π-fibers are complete. Loosely speaking, then, this requires that the "tail end" of J be the union of arithmetic progressions to the modulus π and that each progression that has been "started" somewhere in J must eventually be completed.

The 0-fibers of a set J are precisely the elements of J, for $Z/(0) = Z$. If $\pi \neq 0$, then there can be only finitely many π-fibers of J, and thus the assertion that J is eventually periodic with period π is equivalent to the existence of a constant M such that for every $k \in J$, $\{v \mid v \geqslant M, v \equiv k \pmod{\pi}\} \subseteq J$. (This equivalence also holds for $\pi = 0$.)

Essential to our proof of the Main Theorem is

3.1. PROPOSITION. *The eventual periods of a set J form an ideal in Z.*

Proof. Every set J is eventually periodic with period 0. Now let π_1 and π_2 be two eventual periods of J and let $\pi = s\pi_1 + t\pi_2$ where $s, t \in Z$. We

assume $\pi_2 \neq 0$. There are constants M_1, M_2 such that for any $k \in J$, $\{v \mid v \geqslant M_i, v \equiv k \pmod{\pi_i}\} \subseteq J$, $i = 1, 2$. Put $M = \max(M_1, M_2)$ and let $k_0 \in J$ be given.

Suppose $v \geqslant M$ and $v \equiv K_0 \pmod{\pi}$, say $v - k_0 = n\pi = ns\pi_1 + nt\pi_2$. Select an integer m such that $M_2 \leqslant v - ns\pi_1 + m\pi_1\pi_2 = l$, say. (Any m will suffice if $\pi_1 = 0$.) Now $l \equiv K_0 \pmod{\pi_2}$ and $l \geqslant M_2$, so $l \in J$. And $v = l \pmod{\pi_1}$, $v \geqslant M_1$, so $v \in J$. In summary, $\{v \mid v \geqslant M, v \equiv k_0 \pmod{\pi}\} \subseteq J$. We have established that π is an eventual period of J and this proves the proposition.

The unique non-negative generator of the ideal of eventual periods of a set J will be called the *primitive* eventual period.

Let K be a closed set. We refer to the $\beta(K)$-fibers of K simply as the fibers of K. The assertion that an integer is a fiber of K will mean that that integer, when read modulo $\beta(K)$, is a fiber of K. The Extended Existence Conjecture in conjunction with 2.2 would assert that the fibers of K are precisely those $f \in Z/(\beta(K))$ satisfying $f - 1 \equiv 0 \pmod{\alpha(K)}$ and $f(f-1) \equiv 0 \pmod{\beta(K)}$, and that every fiber is complete. This latter assertion is precisely the Main Theorem. After it is proved, we will know that either $\beta(K)$ or $\frac{1}{2}\beta(K)$ is the primitive period in view of

3.2. PROPOSITION. *Let K be a closed set which is eventually periodic with period $\pi > 0$. If π is even, then $\beta(K) \mid \pi$, and if π is odd, then $\beta(K) \mid 2\pi$.*

Proof. Recall that every closed set K contains 1. If $\beta(K) = 0$, then $K = \{1\}$ and has only the eventual period 0. Assuming $\beta(K) > 0$, we note that, since $1 \in K$, we have $1 + n\pi \in K$ for all sufficiently large integers n. Then, of course, $\beta(K) \mid n\pi(1 + n\pi)$. Taking $n \equiv \pm 1 \pmod{\beta(K)}$, we find $\beta(K) \mid \pi(1 + \pi)$ and $\beta(K) \mid \pi(1 - \pi)$. If π is even, then $(1 + \pi, 1 - \pi) = 1$ and hence $\beta(K) \mid \pi$. If π is odd, then $(1 + \pi, 1 - \pi) = 2$ and hence $\beta(K) \mid 2\pi$.

COROLLARY. *If the closed set K has an odd eventual period, then $\beta(K) \equiv 2 \pmod 4$ and K contains elements congruent to 2 or 3 modulo 4.*

Proof. Since $\beta(K)$ divides twice the eventual period, it is clear that $\beta(K) \equiv 2 \pmod 4$. Necessarily then, there is some $k \in K$ with $k(k-1) \not\equiv 0 \pmod 4$. This is the case iff $k \equiv 2$ or $3 \pmod 4$.

Every closed set K has at least one fiber, namely, 1. Since $k \in B[k]$, k is a fiber of the closed set $B[k]$. From the congruences (1) and (2), all fibers f of $B[k]$ are solutions of the system

$$\begin{aligned} f - 1 &\equiv 0 \pmod{k-1}, \\ f(f-1) &\equiv 0 \pmod{k(k-1)}. \end{aligned} \tag{9}$$

If k is a prime power, then $\{1, k\}$ is the complete set of fibers of $B[k]$, for these are the only solutions modulo $k(k-1) = \beta(B[k])$ to the system (9). If k has two distinct prime divisors, then (9) has more than two solutions (see below). But, unfortunately, the author knows of no other fibers of any set $B[k]$ besides 1 and k.

3.3. PROPOSITION. *The number of residue classes f modulo $\beta(K)$ satisfying*

$$\begin{aligned} f - 1 &\equiv 0 \pmod{\alpha(K)}, \\ f(f-1) &\equiv 0 \pmod{\beta(K)} \end{aligned} \tag{10}$$

is 2^r where r is the number of distinct prime divisors of $\gamma(K)$.

Proof. Since $(\alpha(K), \gamma(K)) = 1$, f satisfies the congruences iff $f - 1 \equiv 0 \pmod{\alpha(K)}$ and $f(f-1) \equiv 0 \pmod{\gamma(K)}$. Writing $\gamma(K) = P_1^{\nu_1} P_2^{\nu_2} \cdots P_r^{\nu_r}$ as the product of powers of distinct primes, the latter system is equivalent to

$$\begin{aligned} f - 1 &\equiv 0 \pmod{\alpha(K)} \\ f(f-1) &\equiv 0 \pmod{P_1^{\nu_1}} \\ &\vdots \qquad\qquad \vdots \\ f(f-1) &\equiv 0 \pmod{P_r^{\nu_r}}. \end{aligned}$$

There is a unique solution modulo $\alpha(K)$ to $f - 1 \equiv 0 \pmod{\alpha(K)}$ while there are two solutions modulo $P_i^{\nu_i}$ to $f(f-1) \equiv 0 \pmod{P_i^{\nu_i}}$. Since $\alpha(K), P_1^{\nu_1}, \ldots, P_r^{\nu_r}$ are pairwise prime, the Chinese remainder theorem asserts that the number of solutions modulo $\beta(K)$ to the system is 2^r.

The sets $H(a, b)$ introduced in Section 2 are examples of closed sets where every solution of (10) is a fiber. If $\gamma(K) = 1$ for some closed set K then, by 3.3, 1 is the only fiber of K. If $\gamma(K) > 1$ then, as we shall see later, K has at least two fibers. We are not able to verify the part of the Extended Existence Conjecture which asserts that all solutions of (10) are fibers of K, but we will prove that the number of fibers is always a power of 2.

4. LEMMAS ON BIBD'S AND CLOSED SETS

If we are to construct PBD's by recursive composition techniques, then clearly it is necessary to have something to start with. The following result of the author's paper [7, Lemma 1 and Theorem 5] is thus of utmost importance here:

4.1. LEMMA. *Let $k \geqslant 2$, $\lambda \geqslant 1$ be given and let q be a prime power, $q > \{\frac{1}{2}k(k-1)\}^{k(k-1)}$. If $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$, then $q \in B[k; \lambda]$.*

We shall make several references to Dirichlet's famous theorem on primes in arithmetic progressions, which we now state.

4.2. LEMMA (Dirichlet). *If $(a, m) = 1$, then the arithmetic progression $tm + a$, $t = 1, 2, \ldots$, contains infinitely many prime numbers.*

The only part of 4.1 we will need for the proof of the Main Theorem is

4.3. PROPOSITION. *Every closed set $K \neq \{1\}$ is infinite.*

Proof. Take $k \in K$, $k \geqslant 2$. By 4.2, there are infinitely many primes $p \equiv 1 \pmod{k(k-1)}$ and all such, which are sufficiently large, belong to $B[k]$ by 4.1. Since K is closed, $B[k] \subseteq K$.

Aside from 4.1 and the fact the sets $B[K; \lambda]$ are closed (Lemma 1.1), the only other information concerning $\lambda > 1$ we require is furnished by

4.4. PROPOSITION. *If $\lambda = a_1\lambda_1 + a_2\lambda_2 + \cdots + a_n\lambda_n$ for integers $a_i \geqslant 0$, $\lambda_i \geqslant 1$, then $\bigcap_{i=1}^{n} B[K; \lambda_i] \subseteq B[K; \lambda]$.*

Proof. Given $v \in \bigcap_{i=1}^{n} B[K; \lambda_i]$, there exists a (v, K, λ_i)-PBD $(X, \mathscr{L}_i)$, $i = 1, 2, \ldots, n$. Put $\mathscr{L} = a_1\mathscr{L}_1 + \cdots + a_n\mathscr{L}_n$ (this is the family of blocks obtained by counting each block B with a multiplicity $m = a_1m_1 + \cdots + a_nm_n$, where m_i is the number of times B occurs in the family $\mathscr{L}_i$). The design $(X, \mathscr{L})$ is then a (v, K, λ)-PBD and hence $v \in B[K; \lambda]$.

COROLLARY. *If $\lambda_0 \mid \lambda$, then $B[K; \lambda_0] \subseteq B[K; \lambda]$.*

Remark. Let K be any set and put $\lambda_0 = (\lambda, \beta(K))$. Keeping in mind the fact that $\alpha(K) \mid \beta(K)$, it is easily verified that $\lambda(v-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda v(v-1) \equiv 0 \pmod{\beta(K)}$ iff $\lambda_0(v-1) \equiv 0 \pmod{\alpha(K)}$ and $\lambda_0 v(v-1) \equiv 0 \pmod{\beta(K)}$. Thus, since $B[K; \lambda_0] \subseteq B[K; \lambda]$, if the Extended Existence Conjecture is valid for the pair K, λ_0, then it is valid for K, λ. So the Conjecture is valid for a fixed set K and all λ iff it is valid for those λ which divide $\beta(K)$. In particular, if it is valid, then the constant $C(K, \lambda)$ may be chosen to be independent of λ.

Another result of utmost importance to us is that of Chowla, Erdös, and Straus [2], which in our terminology reads

4.5. LEMMA. *There exists a constant $oa(k)$ such that $m \in 0A[k]$ for all $m > oa(k)$.*

We use $oa(k)$ to denote the minimum such constant so that $oa(k+1) \geqslant oa(k)$.

All other necessary preliminary results are furnished by [8]. The GDD Composition Theorem [8, Theorem 11.2] and Hanani's observation that R_k is a closed set [8, Theorem 10.1] will be instrumental. We state below several variations of assertions of [8] which will be used often:

4.6. LEMMA. *If e, $e+1$, m, and t are elements of a closed set K (or $t = 0$) and $0 \leqslant t \leqslant m$, $m > oa(e+1)$, then $em + t \in K$.*

Proof. By [8, Lemma 10.2], $em + t \in B[\{e, e+1, m, t\}]$. But, since K is closed, this latter set is contained in K.

4.7. LEMMA. *Let K be a closed set. If $J \subseteq K$, then $G_K[J] \subseteq K$. If $j+1 \in K$ for every $j \in J$, then $w+1 \in K$ for every $w \in G_K[J]$.*

Proof. These are special cases of the Adjunction theorem [8, Theorem 11.1] with $d = 0,1$.

4.8. LEMMA. *If $v \in B[k]$ and $v - 1 > oa(k)$, then*

$$kv,\ k(v-1)+1 \in B[k].$$

Proof. In Lemma 4.7, take $K = B[k]$, $J = \{v\}$ and then $J = \{v-1\}$. This is also a special case of [8, Theorem 9.1].

4.9. LEMMA. *If $v \in F_K[u]$, $v > u$, then there exists a GDD with block sizes from K and group type $\{u\} + (v-u)\{1\}$ ($v\{1\}$ if $u = 0$).*

Proof. Let $(X, \mathcal{A})$ be a $(v, K, 1)$-PBD with a flat F of order u. Then $(X, \{F\} \cup \{\{x\} \mid x \in X - F\}, \mathcal{A} - \mathcal{A} \mid F)$ is the required GDD (omit F as a group if $u = 0$).

5. THE FIBER 1 OF $B[k]$ IS COMPLETE

5.1. THEOREM. *Let $k \geqslant 2$ be given. There exists a constant $C = C(k)$ such that $v \in B[k]$ for all integers $v \geqslant C$ satisfying $v \equiv 1 \pmod{k(k-1)}$.*

The proof is broken up into several steps in order to emphasize the main points. It is convenient to work within the closed set

$$R_k = \{r > 0 \mid r(k-1)+1 \in B[k]\}$$

and we note here that the theorem is equivalent to the assertion of the

existence of a constant C' such that $r \in R_k$ for all $r \geqslant C'$ satisfying $r \equiv 0 \pmod{k}$. k is to remain fixed throughout this section. By 4.3, $B[k]$, and hence R_k, is infinite.

5.2. STEP 1. There exists a positive integer r^* such that $r^* \equiv 0 \pmod{k}$ and r^*, $r^* + 1$, $r^* + k$, $r^* + k + 1 \in R_k$.

Proof. Select $u \in B[k]$ with $u - 1 > oa(k)$. By 4.8,

$$ku,\ k(u-1) + 1 \in B[k].$$

Again by 4.8, (with $v = k(u-1) + 1$, ku), we find that $k(k(u-1)) + 1$, $k(k(u-1) + 1)$, $k(ku - 1) + 1$, $k(ku)$ are all elements of $B[k]$. We take

$$r^* = k^2 \frac{u-1}{k-1}.$$

The above four elements of $B[k]$ establish, respectively, that r^*, $r^* + 1$, $r^* + k$, $r^* + k + 1$ all belong to R_k.

5.3. STEP 2. For every $\epsilon > 1$, there is a sequence $r_1, r_2, r_3, \ldots$ of elements of R_k such that $1 < r_{i+1}/r_i < \epsilon$, $i = 1, 2, 3, \ldots$.

Proof. Take any $t_1, t_2 \in R_k$ with $t_1 < t_2$ and let r^* be as in Step 1. By Lemma 4.6, if $m \in R_k$ and $m > \max(oa(r^* + 1), t_2)$, then $mr^* + t_1$ and $mr^* + t_2 \in R_k$. Select and fix an m as above which in addition is large enough so that

$$1 < \frac{mr^* + t_2}{mr^* + t_1} < \epsilon,$$

and put $u = mr^* + t_1$, $v = mr^* + t_2$. Thus we have found $u, v \in R_k$ with $1 < v/u < \epsilon$.

Let n be the least integer for which $(\frac{v}{u})^n \geqslant u$ so that $1 < u^n/v^{n-1} < \epsilon$. Every positive integer i can be written uniquely as $i = sn + t$ where $s \geqslant 0$, $1 \leqslant t \leqslant n$, and we define

$$r_i = r_{sn+t} = u^{s+n-t}v^t.$$

Now $u, v \geqslant m > oa(r^* + 1) \geqslant oa(k)$, so by [8, corollary to 11.6] used inductively, $r_i \in R_k$. If $i = sn + t$, where $t < n$, then

$$\frac{r_{i+1}}{r_i} = \frac{u^{s+n-t-1}v^{t+1}}{u^{s+n-t}\ v^t} = \frac{v}{u},$$

and, if $i = sn + n$, then

$$\frac{r_{i+1}}{r_i} = \frac{u^{s+1+n-1}v}{u^s v^n} = \frac{u^n}{v^{n-1}}.$$

In either case, $1 < r_{i+1}/r_i < \epsilon$ as required.

5.4. STEP 3. There exists a positive integer M and a sequence $s_1, s_2, s_3, \ldots$ of elements of R_k such that $0 < s_{i+1} - s_i \leqslant M$, $i = 1, 2, 3, \ldots$.

Proof. Let r^* be as in Step 1 and by Step 2, select and fix a sequence $r_1, r_2, \ldots$ of elements of R_k such that $1 < r_{i+1}/r_i < \epsilon = (r^* + 1)/r^*$. By omitting the first few elements if necessary, we may assume that $r_1 > oa(r^* + 1)$. Then, by Lemma 4.6, we observe: if for some i we have $t \in R_k$ (or $t = 0$) and $t \leqslant r_i$, then $r_i r^* + t \in R_k$.

We take $M = r_1 r^*$ and define the sequence $s_1, s_2, \ldots$ inductively. Put $s_1 = r_1 r^*$, $s_2 = r_1 r^* + r_1$. Then $s_1, s_2 \in R_k$ by our above observation. Assume that we have defined $s_1, s_2, \ldots, s_n \in R_k (n \geqslant 2)$ such that $0 < s_{i+1} - s_i \leqslant M$ for $i = 1, 2, \ldots, n - 1$. Let l be the least integer such that $(r^* + 1)r_l > s_n$ (note $l \geqslant 2$). Then, of course, $(r^* + 1)r_{l-1} \leqslant s_n$ and, since $r_l/r_{l-1} < (r^* + 1)/r^*$, we have $r_l r^* < s_n$. Now $0 < s_n - r_l r^* < s_n$, so surely we can find some element s_j, $1 \leqslant j \leqslant n$, of the partial sequence so far defined such that $0 < s_j - (s_n - r_l r^*) \leqslant M$. We put $t = \min(r_l, s_j)$ and define $s_{n+1} = r_l r^* + t$. Then $s_{n+1} \in R_k$ by the observation of the previous paragraph, and in either case for t, $0 < s_{n+1} - s_n \leqslant M$.

5.5. STEP 4. Let r^* be as in Step 1. There exists a positive integer $h \equiv 0 \pmod{k}$ and GDD's with block sizes from R_k and group types

(i) $h\{1\}$,

(ii) $(h + 1)\{1\}$,

(iii) $h\{1\} + \{r^*\}$,

(iv) $(h + 1)\{1\} + \{r^*\}$,

(v) $h\{1\} + \{r^* + k\}$,

(vi) $(h + 1)\{1\} + \{r^* + k\}$.

Proof. Select $m \in B[r^* + k]$ such that $m > \max(oa(r^* + 1), r^* + k + 1)$. Since $r^* + k \in R_k$ and R_k is closed, $m \in R_k$. We take $h = mr^*$. Recalling that $r^* \equiv 0 \pmod{k}$, $h \equiv 0 \pmod{k}$. By Lemma 4.6, $h = mr^*$ and $h + 1 = mr^* + 1$ belong to $R_k \subseteq F_{R_k}[0]$, and, by Lemma 4.9, the GDD's (i) and (ii) exist. Let $(X, \{G_0, G_1, \ldots, G_{r^*}\}, \mathcal{A})$ be a GD $(r^* + 1, m)$ so that $|G_i| = m$, $|A| = r^* + 1$ for $A \in \mathcal{A}$. Let H_1, H_2, H_3, H_4 be subsets of G_0 of cardinalities r^*, $r^* + 1$, $r^* + k$, $r^* + k + 1$,

respectively. The PBD's $X_i = (X_i, \{H_i, G_1, ..., G_{r^*}\} \cup \mathscr{A} \mid X_i)$, where $X_i = H_i \cup G_1 \cup ... \cup G_{r^*}$, have block sizes from R_k and orders $h + r^*$, $h + r^* + 1$, $h + r^* + k$, $h + r^* + k + 1$ according as $i = 1, 2, 3, 4$. Now the PBD's X_1 and X_2 have at least one block of size r^*. Thus $h + r^*$, $h + r^* + 1 \in F_{R_k}[r^*]$. By 4.9, GDD's (iii) and (iv) exist. The PBD X_3 has a block of size $r^* + k$, namely, H_3. Thus $h + r^* + k \in F_{R_k}[r^* + k]$ and 4.9 yields the GDD (v). The PBD X_4 has a block (any G_i) of size m and thus $h + r^* + k + 1 \in F_{R_k}[m]$. But $m \in B[r^* + k]$ and $m > r^* + k$, so $m \in F_{R_k}[r^* + k]$. We may conclude by [8, Proposition 3.7] that $h + r^* + k + 1 \in F_{R_k}[r^* + k]$ and then Lemma 4.9 gives the GDD (vi).

5.6. STEP 5. For every positive integer n, there exists an integer $d \equiv 0 \pmod{k}$ such that $d, d + k, d + 2k, ..., d + nk \in R_k$.

Proof. We proceed by induction. The assertion is valid for $n = 1$ where we may take $d = r^*$ as in 5.2. Fix n and assume we have found $d \equiv 0 \pmod{k}$ such that $d, d + k, ..., d + nk \in R_k$.

Let r^* and h be as in Step 4. Select $m \in R_k$, $m > \max(oa(h + 2), d + nk)$ and put $d^* = mh + d + r^*$. We claim that $d^*, d^* + k, ..., d^* + (n + 1)k \in R_k$. Note that $d^* \equiv 0 \pmod{k}$ since $h \equiv d \equiv r^* \equiv 0 \pmod{k}$.

Let l be given, $0 \leqslant l \leqslant n$, and let $(X, \{G_{-1}, G_0, G_1, ..., G_h\}, \mathscr{A})$ be a GD$(h + 2, m)$. We define a weighting w of X by assigning the value 1 to all points of $G_1 \cup G_2 \cup \cdots \cup G_h$, weighting $d + lk$ points of G_0 with 1 and the remaining points of G_0 with 0, and weighting one point of G_{-1} with r^* and the remaining points with 0. Now for each block $A \in \mathscr{A}$ (which meets each group in one point), the list $(w(x) \mid x \in A, w(x) \neq 0)$ is one of the lists (i) through (iv) of 5.5 and thus ingredient GDD's with blocks sizes from R_k exist. We apply the GDD Composition Theorem [8, Theorem 8.1] to construct a GDD with block sizes from R_k and group type $h\{m\} + \{d + lk\} + \{r^*\}$. Since all group sizes belong to R_k, the canonically associated PBD has block sizes from R_k and order

$$hm + d + lk + r^* = d^* + lk.$$

But R_k is closed and hence $d^* + lk \in R_k$. This holds for $l = 0, 1, ..., n$.

It remains only to show that $d^* + (n + 1)k \in R_k$. We use the same recipe GDD X with the weighting w defined by assigning 1 to each point of $G_1 \cup \cdots \cup G_n$, weighting $d + nk$ points of G_0 with 1 and the rest with 0, and weighting 1 point of G_{-1} with $r^* + k$ and the remaining with 0. For each block $A \in \mathscr{A}$, the list $(w(x) \mid x \in A, w(x) \neq 0)$ is one of the lists (i), (ii), (v), or (vi) of 5.5. By [8, Theorem 8.1] we may construct a GDD with block sizes from R_k and group type $h\{m\} + \{d + nk\} + \{r^* + k\}$. Again since all group sizes belong to R_k, we conclude $d^* + (n + 1)k =$

$hm + d + nk + r^* + k \in R_k$. This completes the proof of 5.6 by induction.

Proof of Theorem 5.1. We assert the existence of a constant C' such that the conditions $r \equiv 0 \pmod{k}$ and $r \geqslant C'$ imply $r \in R_k$. By 5.4, we have an integer M and a sequence $s_1, s_2, s_3 \ldots$ of elements of R_k such that $0 < s_{i+1} - s_i \leqslant M$. Using 5.6, we select $d \equiv 0 \pmod{k}$ such that d, $d + k$, $d + 2k, \ldots, d + Mr^* \in R_r$, where $r^* \equiv 0 \pmod{k}$ is as in 5.2. By dropping the first few elements of the sequence, if necessary, we may assume $s_1 \geqslant d + Mr^*$. With this understanding, we put

$$C' = \max(d + (oa(r^* + 1) + M)r^*, d + s_1 r^*).$$

Given $r \equiv 0 \pmod{k}$, $r \geqslant C'$, choose the largest integer m such that $d + s_m r^* \leqslant r$. Then $d + s_m r^* + Mr^* \geqslant d + s_{m+1} r^* > r \geqslant C'$, so that $s_m > oa(r^* + 1)$ and $r = d + lk + s_m r^*$, where $0 \leqslant lk \leqslant Mr^*$. Now r^*, $r^* + 1$, $d + lk$, and s_m all belong to the closed set R_k and $d + lk \leqslant d + Mr^* \leqslant s_1 \leqslant s_m$, $s_m > oa(r^* + 1)$. Thus, by Lemma 4.6, $r = s_m r^* + d + lk \in R_k$ and Theorem 5.1 is now proved.

6. The Eventual Periodicity of Closed Sets

6.1. Main Theorem. *Every closed set K is eventually periodic with period $\beta(K)$.*

We again proceed by steps. K is to be a fixed closed set throughout this discussion.

6.2. Step 1. In order to prove 6.1, it will be sufficient to show that, whenever $2 < k \in K$, $1 < v \in B[k]$, and $v \equiv 1 \pmod{k(k-1)}$, then K is eventually periodic with period $v - 1$.

Proof. Assume that this statement has been shown. Given $k \in K$, $k \geqslant 2$, if p_1 and p_2 are sufficiently large distinct primes, then by Theorem 5.1, $p_1 k(k-1) + 1$ and $p_2 k(k-1) + 1$ belong to $B[k]$. We could then conclude that K is eventually periodic with periods $p_1 k(k-1)$ and $p_2 k(k-1)$. By Proposition 3.1, the eventual periods of K from an ideal. Then, in particular, $k(k-1) = (p_1 k(k-1), p_2 k(k-1))$ would be an eventual period of K. This holds for each $k \in K$ (even $k = 1$) and, again by 3.1, K would be eventually periodic with period $\beta(K) = gcd\{k(k-1) \mid k \in K\}$.

We now fix some $k \in K$, $k \geqslant 2$, fix $v \in B[k]$, $v > 1$, $v \equiv 1 \pmod{k(k-1)}$, and let $f \in Z/(v-1)$ be an arbitrary $(v-1)$-fiber of K.

6.3. STEP 2. There exists $u^* \in K$ with $u^* \equiv f \pmod{v-1}$ and $u^* - 1 > oa(v)$.

Proof. Since f is a $(v-1)$-fiber of K, we have by definition some $u \in K$ with $u \equiv f \pmod{v-1}$. Since $v - 1 \equiv 0 \pmod{k(k-1)}$, Theorem 5.1 says that $t(v-1)+1 \in B[k] \subseteq K$ for all sufficiently large t. Select and fix such a t large enough so that in addition $t(v-1)+1 > oa(u)$ and $u(t(v-1)+1)-1 > oa(v)$. Put $u^* = u(t(v-1)+1)$. Clearly $u^* \equiv f \pmod{v-1}$ and $u^* - 1 > oa(v)$. The PBD canonically associated to a GD$(u, t(v-1)+1)$, which exists since $t(v-1)+1 > oa(u)$, has order u^* and block sizes from $\{u, t(v-1)+1\} \subseteq K$. But K is closed, so $u^* \in K$.

6.4. STEP 3. Let u^* be as in Step 2. There exist GDD's with block sizes from K and group types

(i) $\{u^*-1\} + u^*\{v-1\}$,

(ii) $\{u^*-1\} + (u^*-1)\{v-1\}$.

Proof. From 6.3, $u^* - 1 > oa(v)$. First let $(X, \mathscr{G}, \mathscr{A})$ be a GD(v, u^*) and select a point $\theta \in X$. In the PBD $X = (X, \mathscr{G} \cup \mathscr{A})$ there will be one block of size u^* containing θ; all other blocks through θ have size v. Thus the dispersion X_θ at θ is a GDD with one group of size $u^* - 1$, other groups of size $v-1$, and block sizes from $\{u^*, v\} \subseteq K$. Since the order is $vu^* - 1$, the number of groups of size $v-1$ is necessarily u^*, and the GDD has group type $\{u^*-1\} + u^*\{v-1\}$ as in (i).

Now let $(Y, \{G_1, G_2, \ldots, G_v\}, \mathscr{B})$ be a GD(v, u^*-1). Let z be a new point and consider the PBD $Y \cup \{z\} = (Y \cup \{z\}, \{G_1 \cup \{z\}, \ldots, G_v \cup \{z\}\} \cup \mathscr{B})$, which has block sizes from $\{u^*, v\} \subseteq K$. Through a point $\theta \in Y$, there is one block of size u^*; the other blocks have size v. Thus the dispersion $(Y \cup \{z\})_\theta$ is a GDD with group type $\{u^*-1\} + (u^*-1)\{v-1\}$ and block sizes from K as claimed in (ii).

Select and fix an integer M (by increasing the constant of Theorem 5.1 if necessary) which has the properties $M \geqslant v(u^*-1)$, $M \geqslant oa(u^*+1)$ and such that $w \geqslant M$, $w \equiv 1 \pmod{k(k-1)}$ assures $w \in B[k]$.

6.5. STEP 4. If $m \equiv 1 \pmod{k(k-1)}$ and $M \leqslant t \leqslant m$, then $(u^*-1)vm + (v-1)t + 1 \in K$.

Proof. Given t and m as above, let $(X, \{G_0, G_1, \ldots, G_{u^*}\}, \mathscr{A})$ be a GD(u^*+1, m). We define a weighting w of X by assigning the weight $v-1$ to t points of G_0 and 0 to the remaining points of G_0, u^*-1 to all points of G_1, and $v-1$ to all points of $G_2 \cup G_3 \cup \cdots \cup G_{u^*}$. For every block $A \in \mathscr{A}$, the list $(w(x) \mid x \in A, w(x) \neq 0)$ is either $\{u^*-1\} + u^*\{v-1\}$

or $\{u^* - 1\} + (u^* - 1)\{v - 1\}$. In 6.4 we have seen that ingredient GDD's with these group types and block sizes from K exist. By the GDD Composition Theorem [8, Theorem 8.1], we may construct a GDD with block sizes from K and group type $\{m(u^* - 1)\} + (u^* - 1)\{m(v - 1)\} + \{t(v - 1)\}$. Now, if $\{m(u^* - 1) + 1, m(v - 1) + 1, t(v - 1) + 1\} \subseteq K$, we may adjoin a point and conclude by Lemma 4.7 that $m(u^* - 1) + (u^* - 1)m(v - 1) + t(v - 1) + 1 = (u^* - 1)vm + (v - 1)t + 1 \in K$, as required.

Now $v - 1 \equiv 0 \pmod{k(k - 1)}$, so both $t(v - 1) + 1$ and $m(v - 1) + 1$ are congruent to 1 modulo $k(k - 1)$ and in addition, both exceed the constant M. So by the definition of M, we have $t(v - 1) + 1, m(v - 1) + 1 \in B[k] \subseteq K$. It remains only to show that $m(u^* - 1) + 1 \in K$ to complete the proof of 6.5. By hypothesis, $M \leqslant m \equiv 1 \pmod{k(k - 1)}$, so $m \in B[k]$. From 6.3, $u^* - 1 > oa(v) \geqslant oa(k)$ (surely $v > k$) and thus a GD$(k, u^* - 1)$ exists. In particular, $k \in \mathrm{NG}[u^* - 1, K]$. But $m \in B[k]$ and NG$[u^* - 1, K]$ is a closed set by [8, Proposition 11.4], so $m \in \mathrm{NG}[u^* - 1, K]$. Finally, since $(u^* - 1) + 1 \in K$, Lemma 4.7 asserts that $m(u^* - 1) + 1 \in K$.

Proof of Theorem 6.1. In view of 6.2, it suffices to show that the arbitrary $(v - 1)$-fiber f of K is complete. Let u^* and M be as above and put $C = (v - 1)[M + (u^* - 1) + Mv(u^* - 1)] + u^*$. We claim $\{w \mid w \geqslant C, w \equiv f \pmod{v - 1}\} \subseteq K$.

Given such a w, we note that

$$\frac{w - u^*}{v - 1} - M - (u^* - 1) - Mv(u^* - 1)$$

is a non-negative integer and hence can be written as $a + bv(u^* - 1)$, where $b \geqslant 0$ and $0 \leqslant a < v(u^* - 1) \leqslant M$. Putting $t = a + M$ and $m = (b + M)(v - 1) + 1$, we have $M \leqslant t \leqslant 2M \leqslant m$ (surely $v \geqslant 3$) and $m \equiv 1 \pmod{k(k - 1)}$. After checking that $w = (v - 1)t + (u^* - 1)vm + 1$, we have $w \in K$ by 6.5. Thus the claim is verified, f is complete, and the Main Theorem is established.

6.6. THEOREM. *Every closed set K is finitely generated, i.e., there is a finite subset $K_0 \subseteq K$ such that $K = B[K_0]$.*

Proof. In view of Proposition 2.1, there is a finite set $K_1 \subseteq K$ such that $\beta(K_1) = \beta(K)$. Let $K_2 \subseteq K$ be a set of representatives for the fibers of K, i.e. for each fiber f of K, choose some $k_f \in K$ with $k_f \equiv f \pmod{\beta(K)}$ and put $K_2 = \{k_f \mid f \text{ fiber of } K\}$. Since there are only finitely many fibers of K (even when $\beta(K) = 0$, i.e., $K = \{1\}$), K_2 is finite.

We have $B[K_1 \cup K_2] \subseteq B[K] = K$. Now $B[K_1 \cup K_2]$ and K are both

closed sets, $\beta(B[K_1 \cup K_2]) = \beta(K)$, and both have the same set of $\beta(K)$-fibers. Necessarily then, by the Main Theorem, they eventually coincide and we can find a constant C such that for $v \geqslant C$, $v \in K$ iff $v \in B[K_1 \cup K_2]$. With $K_0 = K_1 \cup K_2 \cup \{k \in K \mid k < C\}$, it follows that $B[K_0] = K$.

7. Illustrations and an Application

Presented with a closed set, our first interest is in the determination of β, for then 6.1 yields much information. In particular, since 1 is a fiber of any closed set K, K will contain all sufficiently large integers congruent to 1 modulo $\beta(K)$. Our second interest is the determination of the fibers. If all fibers are known, then we have completely described the "tail end" of our closed set. If the Extended Existence Conjecture is valid, then the determination of $\alpha(K)$ would suffice to describe all the fibers.

If a closed set K is presented as $K = B[K_0]$ for a finite set K_0, then we may easily calculate $\beta(K) = \beta(K_0)$, $\alpha(K) = \alpha(K_0)$ (by Proposition 2.3), and the elements of K_0 are all fibers of K. For example, let $K = B[\{8, 9\}]$. We have $\alpha(K) = (7, 8) = 1$, $\beta(K) = (8 \cdot 7, 9 \cdot 8) = 8$, and hence $\gamma(K) = 8$. 8 and 9 are elements of K and hence 0 and 1 (mod 8) are fibers of K. Since γ is a prime power, there can be no other fibers of K (Proposition 3.3). Thus the "tail end" of K is known; if v is "large," then $v \in K$ iff $v \equiv 0$ or 1 (mod 8). A similar example is $B[8]$. Here $\beta = 56$, $\alpha = 7$, $\gamma = 8$. 1 and 8 are the fibers of $B[8]$; the "tail end" of $B[8]$ consists of those $v \equiv 1$ or 8 (mod 56).

It is not always this easy. Consider the sets $H_1 = \{6, 9, 10\}$, $H_2 = \{6, 9\}$, $H_3 = \{3, 4\}$, $H_4 = \{6, 7\}$. Put $K_i = B[H_i]$, $i = 1, 2, 3, 4$. In each case $\alpha(K_i) = 1$, $\beta(K_i) = \gamma(K_i) = 6$. 1 is a fiber of each K_i and for each there can be at most 4 fibers: the solutions 0, 1, 3, 4 (mod 6) to $f - 1 \equiv 0 \pmod 1$ and $f(f-1) \equiv 0 \pmod 6$. By inspection of the sets H_i, we see that 0, 3, 4 are fibers of K_1, 0 and 3 are fibers of K_2, 3 and 4 are fibers of K_3, and 0 is a fiber of K_4. Actually, K_1, K_2, and K_3 have the complete set $\{0, 1, 3, 4\}$ as fibers. This can be established by the composition theorem of [8]; for example, the existence of a GD(3, 4) implies $12 \in K_3$ so that 0 is a fiber of K_3. In Section 8 we give a "composition theorem" (8.1) for fibers to take care of such cases without having to construct PBD's in each instance. Indeed, that 0 must also be a fiber of K_3 is an immediate consequence of 8.5 which asserts that a closed set K cannot have precisely 3 fibers.

The set K_4 is an exception in the sense that we are not able to show that 3 and 4 are fibers. If 0 and 1 were the only fibers of K_4, then the Extended Existence Conjecture would be false. A similar example is

$B[6]$. Here $\alpha(B[6]) = 5$, $\beta(B[6]) = 30$, $\gamma(B[6]) = 6$. 1 and 6 are fibers of $B[6]$ and, by the Main Theorem, these fibers are complete. But the structure of $B[6]$ is not described until we know if there are any other fibers. The only other possibilities, i.e., solutions of the necessary conditions, are 16 and 21 (mod 30). But this author knows of no elements $v \in B[6]$ with $v \equiv 16$ or 21 (mod 30). However, as we shall see in Section 8, if either of 16 or 21 is a fiber, then the other is also.

Before we make a more detailed investigation of fibers, we consider the existence of PBD's having flats of a given order. An opportunity to apply the Main Theorem is presented by

7.1. PROPOSITION. *$F_K[u] \cup \{1\}$ is a closed set.*

Proof. Let $v \in B[F_K[u] \cup \{1\}]$ be given and assume $v > 1$. Then there exists a PBD X of order v and with block sizes from $F_K[u]$. Since $v > 1$, this PBD has at least one block B, say $| B | = w \in F_K[u]$. B is a flat of X, so $v \in F_K[w]$. By [8, Proposition 3.7], we conclude $v \in F_K[u]$. Thus $B[F_K[u] \cup \{1\}] \subseteq F_K[u] \cup \{1\}$ and this proves the assertion.

7.2. THEOREM. *Let u be an element of a closed set K. Then $F_K[u]$ and K eventually coincide.*

Proof. We have $F_K[u] \subseteq K$, so $\beta(K) \mid b$ where $b = \beta(F_K[u])$. If $\beta(K) = 0$ or $u = 1$, the assertion is obvious. Assuming $u > 1$, we have $b > 0$ since $u \in F_K[u]$ and therefore $b \mid u(u - 1)$.

Now 1 mod b is a fiber of the closed set $F_K[u] \cup \{1\}$ and by 6.1 this fiber is complete. In particular, there are infinitely many $w \in F_K[u]$ with $w \equiv 1 \pmod{b}$. Let $f \in Z/(b)$ be a b-fiber of K and select $v \in K$ with $v \equiv f \pmod{b}$. Taking any $w \in F_K[u]$ with $w > oa(v)$ and $w \equiv 1 \pmod{b}$, we have a GD(v, w) and hence a PBD of order vw and block sizes $\{v, w\}$. Therefore, $vw \in F_K[w] \subseteq F_K[u]$ using [8, Proposition 3.7]. But $vw \equiv f \pmod{b}$, so f is also a b-fiber of $F_K[u] \cup \{1\}$. Conversely, since $F_K[u] \cup \{1\} \subseteq K$, every b-fiber of $F_K[u] \cup \{1\}$ is a b-fiber of K.

In summary, the two closed sets $F_K[u] \cup \{1\}$ and K have the same b-fibers. Every $k \in K$ is congruent modulo b to some $j \in F_K[u]$. But $b \mid j(j - 1)$ and hence $b \mid k(k - 1)$. It follows that $b \mid \beta(K)$ and hence $\beta(K) = b = \beta(F_K[u] \cup \{1\})$. And $F_K[u] \cup \{1\}$ and K have the same fibers. Consequently, in view of 6.1, they eventually coincide.

Theorem 7.2 answers many questions one might ask concerning the occurence of certain configurations in PBD's. For instance, for what integers v does there exist a $(v, K, 1)$-PBD with 37 disjoint flats of order u? By 7.2, the set of all such v either is empty or eventually coincides with

$B[K]$. For if there exists a single such PBD $(X, \mathcal{A})$ of order v_0, then $v_0 \in B[K]$ and hence $F_K[v_0] = F_{B[K]}[v_0]$ eventually coincides with $B[K]$. And given a PBD with a flat of order v_0, we may unplug it and replace it with $(X, \mathcal{A})$ [8, Proposition 3.6]. If $u \in B[K]$, the existence of such a PBD is easily established using transitive GD(u, m)'s, $m \in B[K]$.

8. The Lattice of Fibers

8.1. Theorem. *If $f, g, h \in Z/(\beta(K))$ are fibers of the closed set K, then $f(g - h) + h$ is also a fiber of K.*

Proof. The theorem is immediate for $K = \{1\}$, so we may assume $\beta = \beta(K) > 0$. Select $v, u \in K$ with $v \equiv f \pmod{\beta}$ and $u \equiv h \pmod{\beta}$. The fiber g of K is complete and, by Theorem 7.2, K and $F_K[u]$ eventually coincide. So we can find some $w \in F_K[u]$ with $w \equiv g \pmod{\beta}$ and $w - u > o\alpha(v)$. By the Adjunction Theorem [8, Theorem 11.1], we can adjoin a flat of order u to a GD$(v, w - u)$ to obtain a PBD with order $v(w - u) + u$ and block sizes from K. Since K is closed, $v(w - u) + u \in K$. Noting that $f(g - h) + h \equiv v(w - u) + u \pmod{\beta}$ completes the proof.

Corollary 1. *If f and g are fibers of the closed set K, then fg is a fiber of K.*

Proof. Since $f(f - 1) \equiv 0$, we have $fg \equiv f(g - f) + f$.

Corollary 2. *If f is a fiber of $B[k]$, then $1 + k - f$ is also a fiber of $B[k]$.*

Proof. Since $f \equiv 1 \pmod{k - 1}$, we have $fk \equiv k \pmod{k(k - 1)}$. 1 and k are fibers of $B[k]$, and $1 + k - f \equiv f(k - 1) + 1 \pmod{k(k - 1)}$.

Thus if either 16 or 21 is a fiber of $B[6]$, then the other is also.

Given a closed set K, we call 1 the *minimum* fiber of K for reasons which will become apparent later. The fiber of K are all idempotent elements of the ring $Z/(\beta(K))$ (another way of phrasing the necessary condition $f(f - 1) \equiv 0 \pmod{\beta(K)}$ and all are congruent to 1 modulo $\alpha(K)$. Since $\alpha(K)$ and $\gamma(K)$ are relatively prime, two fibers are equal in $Z/(\beta(K))$ iff they are congruent modulo $\gamma(K)$.

8.2. Theorem. (i) *If K_0 is a finite set of positive integers, then $\gamma(K_0) \mid \operatorname{lcm}(K_0)$ (the least common multiple of elements of K_0).* (ii) *Let K be a closed set. Then the unique element $f \in Z/(\beta(K))$ with $f \equiv 1 \pmod{\alpha(K)}$ and $f \equiv 0 \pmod{\gamma(K)}$ is a fiber of K.*

Proof. For (i) we write $K_0 = \{k_1, k_2, ..., k_n\}$ and proceed by induction on n. If $K_0 = \{k\}$, we have $\gamma(K_0) = k = \text{lcm}(K_0)$. Assuming the validity of (i) for sets of $n-1$ elements, put $l_0 = \text{lcm}\{k_1, k_2, ..., k_{n-1}\}$, $\alpha_0 = \alpha\{k_1, ..., k_{n-1}\}$, $\beta_0 = \beta\{k_1, ..., k_{n-1}\}$. Our induction hypothesis then asserts that $\beta_0 \mid \alpha_0 l_0$. We have $\beta(K_0) = (\beta_0, k_n(k_n - 1))$, $\alpha(K_0) = (\alpha_0, k_n - 1)$, and $\text{lcm}(K_0) = \text{lcm}\{l_0, k_n\} = l_0 k_n/(l_0, k_n)$. Then

$$\alpha(K_0) \cdot \text{lcm}(K_0) = \left(\alpha_0 l_0 \frac{k_n}{(l_0, k_n)}, \frac{l_0}{(l_0, k_n)} k_n(k_n - 1)\right).$$

Now $\beta(K_0) \mid \beta_0 \mid \alpha_0 l_0$ and $\beta(K_0) \mid k_n(k_n - 1)$. Consequently, $\beta(K_0) \mid \alpha(K_0) \cdot \text{lcm}(K_0)$. Equivalently, $\gamma(K_0) \mid \text{lcm}(K_0)$.

To prove (ii), let the closed set K be given and, by Theorem 6.6, select a finite subset $K_0 \subseteq K$ such that $K = B[K_0]$. By 3.3, $\gamma(K) = \gamma(K_0)$. By Corollary 1 to 8.1, the product m of the elements of K_0 is a fiber of K. We have $\gamma(K_0) \mid \text{lcm}(K_0) \mid m$, so that the fiber m represents the unique residue class f modulo $\beta(K)$ with $f \equiv 0 \pmod{\gamma(K)}$ and $f \equiv 1 \pmod{\alpha(K)}$.

The fiber of a closed set K which is divisible by $\gamma(K)$ will be called the *maximum* fiber of K. The maximum fiber of $B[k]$ is k.

8.3. THEOREM. *A closed set K has precisely one fiber iff $\gamma(K) = 1$. If $\gamma(K)$ is a prime power, then K has precisely two fibers.*

Proof. If $\gamma(K) = 1$, then 1 is the only solution modulo $\beta(K) = \alpha(K)$ to $f - 1 \equiv 0 \pmod{\alpha(K)}$. If $\gamma(K) > 1$, then the maximum and minimum fibers of K are incongruent modulo $\beta(K)$ and hence are two distinct fibers of K. If $\gamma(K)$ is a prime power, then K cannot have more than two fibers by Proposition 3.3.

Thus if $\gamma(K)$ is one or a prime power, the "tail end" of a closed set K is completely described.

The set of fibers of a closed set K is a subset of idempotent elements of the ring $Z/(\beta(K))$ and is closed under the operation $f(g - h) + h$. More generally, let I be any finite non-empty set of idempotents of a commutative ring R which is closed under the operation $a(b - c) + c$. For $x, y \in I$, we define $x \sqcup y = x(y - x) + x = xy \in I$ and $x \sqcap y = x(x - y) + y = x + y - xy \in I$. One readily verifies that, under these operations, I becomes a distributive lattice (see [1] for the terminology). (The underlying partial ordering is $a \leqslant b$ if $a \mid b$ in the ring R, or equivalenty, iff $ba = b$.) Since I is finite, there is a minimum element z and a maximum element m. (In the lattice of fibers of a closed set K, 1 is the minimum element and the maximum element is the unique fiber divisible by $\gamma(K)$.) For $a \in I$, we define $a' = a(m - z) + z = a \sqcup m - a \sqcup z + z = m + z - a \in I$ and observe that $a \sqcup a' = a(m + z - a) = a \sqcup m + a \sqcup z - a = m$ and

$a \sqcap a' = a + (m + z - a) - a \sqcup a' = z$. Thus the lattice is also complemented, i.e., I is a Boolean lattice. Being finite, I has finite length n. But it is well known [1, p. 159, Theorem 6] that every Boolean lattice of finite length n is isomorphic to the lattice of all subsets of its n points. In particular, we have

8.4. LEMMA. *Let R be a commutative ring and let I be a finite subset of idempotent elements closed under the operation $a(b - c) + c$. Then $|I| = 2^n$ for some non-negative integer n.*

(It is interesting to note the set of all idempotents of R is closed under $a(b - c) + c$.) Immediately, from 8.1 and 3.3, we conclude

8.5. THEOREM. *The number of fibers of a closed set K is 2^n, for some $n \geqslant 0$, which does not exceed the number of distinct prime divisors of $\gamma(K)$.*

By 3.2, the primitive eventual period of a closed set K is either $\beta(K)$ or $\frac{1}{2}\beta(K)$, and the latter alternative is possible only if $\beta(K) \equiv 2 \pmod 4$.

8.6. THEOREM. *If K is a closed set and there exists a single pair of distinct fibers f, $g \in Z/(\beta(K))$ such that $f \equiv g \pmod{\frac{1}{2}\beta(K)}$, then K is eventually periodic with period $\frac{1}{2}\beta(K)$.*

Proof. The set $I \subseteq Z/(\frac{1}{2}\beta(K))$ of $(\frac{1}{2}\beta(K))$-fibers of K is the image of the set of fibers of K under the canonical epimorphism $Z/(\beta(K)) \to Z/(\frac{1}{2}\beta(K))$. Therefore I is a set of idempotent elements of $Z/(\frac{1}{2}\beta(K))$ which is closed under the operation $a(b - c) + c$. By 8.4, $|I| = 2^n$, for some n, while the number of fibers of K is 2^m, for some m. Now each element of I has at most two fibers of K as pre-image and hence $n \leqslant m \leqslant n + 1$. However, at least one element does have two pre-images, f and g. Thus we must have $m = n + 1$ and every element of I must have two pre-images. We have shown that, if h is a fiber of K, then $h + \frac{1}{2}\beta(K)$ must also be a fiber and it follows that K is eventually periodic with period $\frac{1}{2}\beta(K)$.

9. THE SETS $B[K; \lambda]$

We apply the theory of the previous sections to $B[K; \lambda]$, which by Lemma 1.1 is a closed set.

Given an integer n, we define

$$\epsilon(n) = \begin{cases} n, & \text{if } n \text{ is even,} \\ 2n, & \text{if } n \text{ is odd.} \end{cases}$$

Note that, if $n \mid m$ and m is even, then $\epsilon(n) \mid m$. Also note $\epsilon(gcd(J)) = gcd\{\epsilon(j) \mid j \in J\}$.

9.1. PROPOSITION. *Let $k \geqslant 2$, $\lambda \geqslant 1$ be given. Then*

$$\beta(B[k; \lambda]) = \epsilon\left(\frac{k(k-1)}{(\lambda, k(k-1))}\right).$$

Proof. By Proposition 2.2, $\lambda v(v-1) \equiv 0 \pmod{k(k-1)}$ for every $v \in B[k; \lambda]$. Equivalenty,

$$v(v-1) \equiv 0 \left(\mathrm{mod}\ \frac{k(k-1)}{(\lambda, k(k-1))}\right),$$

and thus

$$\frac{k(k-1)}{(\lambda, k(k-1))} \Big| \beta,$$

where $\beta = \beta(B[k; \lambda])$. Then $b \mid \beta$ where

$$b = \epsilon\left(\frac{k(k-1)}{(\lambda, k(k-1))}\right),$$

say $\beta = mb$.

If P is a sufficiently large prime, $P \equiv 1 \pmod{b}$, then by Lemma 4.1, $P \in B[k; \lambda]$. Thus $\beta \mid P(P-1)$; and assuming $P > \beta$, we have $\beta \mid P - 1$. Since b is even, $b - 1$ and $b(b+1)$ are relatively prime. Thus, by Dirichlet's Theorem, Lemma 4.2, we can find large primes $P = b(b+1)l + (1-b)$. Thus, for some l, $\beta \mid b(b+1)l - b$, and hence $m \mid (b+1)l - 1$. In particular, $(m, b+1) = 1$, whence $(\beta, b+1) = 1$. Again, by 4.2, we can find large primes $P = \beta t + (b+1)$. Hence, for some t, $\beta \mid \beta t + b$. Thus $\beta \mid b$ and then $\beta = b$ as claimed.

9.2. PROPOSITION. *Let K be a set of positive integers and λ a positive integer. Then*

$$\beta(B[K; \lambda]) = \epsilon\left(\frac{\beta(K)}{(\lambda, \beta(K))}\right)$$

and

$$\alpha(\beta[K; \lambda]) = \frac{\alpha(K)}{(\lambda, \alpha(K))}.$$

Proof. By 2.2, $\lambda v(v-1) \equiv 0 \pmod{\beta(K)}$ for every $v \in B[K; \lambda]$. Thus $\beta(K)/(\lambda, \beta(K)) \mid \beta(B[K; \lambda])$; hence

$$\epsilon\left(\frac{\beta(K)}{(\lambda, \beta(K))}\right) \Big| \beta(B[K; \lambda]).$$

Now, for each $k \in K$, $B[k; \lambda] \subseteq B[K; \lambda]$, and thus $\beta(B[K; \lambda]) \mid \beta(B[k; \lambda])$. Using 9.1,

$$\beta(B[K; \lambda]) \Big| \epsilon\left(\frac{k(k-1)}{(\lambda, k(k-1))}\right) \Big| \epsilon\left(\frac{k(k-1)}{(\lambda, \beta(K))}\right),$$

and hence $\beta(B[K; \lambda])$ divides

$$gcd\left\{\epsilon\left(\frac{k(k-1)}{(\lambda, \beta(K))}\right) \Big| k \in K\right\},$$

which is equal to

$$\epsilon\left(\frac{\beta(K)}{(\lambda, \beta(K))}\right).$$

Consequently,

$$\beta(B[K; \lambda]) = \epsilon\left(\frac{\beta(K)}{(\lambda, \beta(K))}\right).$$

By 2.2, $\lambda(v-1) \equiv 0 \pmod{\alpha(K)}$ for every $v \in B[K; \lambda]$ and hence $(\alpha(K)/(\lambda, \alpha(K)) \mid \alpha(B[K; \lambda])$. Since $B[K] \subseteq B[K; \lambda]$, we have $\alpha(B[K; \lambda]) \mid \alpha(K)$. Since $(\alpha(K), \gamma(K)) = 1$, it follows that $\alpha(B[K; \lambda])$ is relatively prime to $\gamma(K)$ and hence to $\gamma(K)/(\lambda, \gamma(K))$. Finally, we know

$$\alpha(B[K; \lambda]) \mid \beta(B[K; \lambda]) = \epsilon\left(\frac{\beta(K)}{(\lambda, \beta(K))}\right) = \epsilon\left(\frac{\alpha(K) \cdot \gamma(K)}{(\lambda, \alpha(K))(\lambda, \beta(K))}\right).$$

If $\beta(K)/(\lambda, \beta(K))$ is even, we have shown

$$\frac{\alpha(K)}{(\lambda, \alpha(K))} \mid \alpha(B[K; \lambda]) \mid \frac{\alpha(K)}{(\lambda, \alpha(K)} \cdot \frac{\gamma(K)}{(\lambda, \gamma(K))}$$

from which we may conclude $\alpha(B[K; \lambda]) = \alpha(K)/(\lambda, \alpha(K))$. If $\beta(K)/(\lambda, \beta(K))$ is odd, then we may only conclude

$$\frac{\alpha(K)}{(\lambda, \alpha(K))} \mid \alpha(B[K; \lambda]) \mid 2\frac{\alpha(K)}{(\lambda, \alpha(K))}.$$

To complete the proof in this case, it will suffice to show that $\alpha(B[K; \lambda])$ is odd or, equivalenty, that $B[K; \lambda]$ contains some even number. But

$$\frac{\beta(K)}{(\lambda, \beta(K))} = gcd\left\{\frac{k(k-1)}{(\lambda, \beta(K))} \,\middle|\, k \in K\right\},$$

so necessarily there is some $k \in K$ for which $k(k-1)/(\lambda, \beta(K))$ is odd. Then $k(k-1)/(\lambda, k(k-1))$ is also odd and, if n is any multiple of the order of 2 modulo

$$\frac{k(k-1)}{(\lambda, k(k-1))},$$

then

$$2^n \equiv 1 \left(\mathrm{mod}\ \frac{k(k-1)}{(\lambda, k(k-1))}\right), \qquad \lambda(2^n - 1) \equiv 0 \ (\mathrm{mod}\ k(k-1)).$$

If n is chosen sufficiently large, then $2^n \in B[k; \lambda] \subseteq B[K; \lambda]$ by Lemma 4.1, and this completes the proof.

9.3. THEOREM. *$B[K; \lambda]$ is eventually periodic with period $\beta(K)/(\lambda, \beta(K))$.*

Proof. If $\beta(K)/(\lambda, \beta(K))$ is even, then $\beta(B[K; \lambda] = \beta(K)/(\lambda, \beta(K))$ by 9.2 and the conclusion is just the statement of the Main Theorem. If $\beta(K)/(\lambda, \beta(K))$ is odd, then

$$\beta(B[K; \lambda]) = 2\frac{\beta(K)}{(\lambda, \beta(K))}.$$

In this case, it will be sufficient to exhibit an element $v_0 \in B[K; \lambda]$ with

$$v_0 \equiv 1 + \frac{\beta(K)}{(\lambda, \beta(K))} \left(\mathrm{mod}\ 2\frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

for then 1 and $1 + \beta(K)/(\lambda, \beta(K))$ are two distinct fibers of $B[K; \lambda]$ which differ by $\frac{1}{2}\beta(B[K; \lambda])$ and the conclusion follows from Theorem 8.6. But, as in the proof 9.2, we can find some integer n such that $2^n \in B[K, \lambda]$. From $\lambda\, 2^n(2^n - 1) \equiv 0 \ (\mathrm{mod}\ \beta(K))$, or from the congruence $\lambda(2^n - 1) \equiv 0 \ (\mathrm{mod}\ k(k-1))$ of the proof of 9.2, we deduce that

$$2^n \equiv 1 \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right).$$

Clearly

$$2^n \not\equiv 1 \left(\mathrm{mod}\ 2\frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

so it must be that

$$2^n \equiv 1 + \frac{\beta(K)}{(\lambda, \beta(K))} \left(\mathrm{mod}\ 2\,\frac{\beta(K)}{(\lambda, \beta(K))}\right).$$

In view of the above theorem, it is more natural to work with the $(\beta(K)/(\lambda, \beta(K)))$-fibers of $B[K; \lambda]$ rather than the fibers, i.e., $\beta(B[K; \lambda])$-fibers. The former will be called *-fibers of $B[K; \lambda]$. An integer d will be called a *-fiber of $B[K; \lambda]$ iff when read modulo $\beta(K)/(\lambda, \beta(K))$, d is a *-fiber, i.e.,

$$d \equiv v \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right)$$

for some $v \in B[K; \lambda]$. By 2.2, every *-fiber f of $B[K; \lambda]$ is a solution of

$$\begin{aligned} f &\equiv 1 \quad \left(\mathrm{mod}\ \frac{\alpha(K)}{(\lambda, \alpha(K))}\right), \\ f(f-1) &\equiv 0 \quad \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right), \end{aligned} \tag{11}$$

and the Extended Existence Conjecture, in view of Theorem 9.3, is equivalent to the assertion that all solutions are in fact *-fibers.

9.4. LEMMA. *Let d be a integer which is a *-fiber of $B[K; \lambda_i]$, $i = 1, 2, \ldots, n$. Then d is a *-fiber of $B[K; \lambda]$ whenever $\lambda = a_1\lambda_1 + \cdots + a_n\lambda_n$ for non-negative integers a_i.*

Proof. If v is a sufficiently large integer, $v \equiv d \pmod{\beta(K)}$, then

$$v \equiv d \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda_i, \beta(K))}\right),$$

so by Theorem 9.3 v simultaneously belongs to all $B[K; \lambda_i]$, $i = 1, 2, \ldots, n$. By Proposition 4.4, $v \in B[K; \lambda]$. Since

$$d \equiv v \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

d is a *-fiber of $B[K; \lambda]$.

COROLLARY. *If d is a fiber of $B[K]$, then d is a *-fiber of $B[K; \lambda]$.*

Given a set K, let m be an integer with $m \equiv 1 \pmod{\alpha(K)}$ and $m \equiv 0 \pmod{\gamma(K)}$. Then, by 8.2 m is, a fiber (the maximum fiber) of $B[K]$ and

hence m is a *-fiber of any $B[K; \lambda]$. 1 is also a *-fiber of $B[K; \lambda]$ so an application of Theorem 9.3 yields

9.5. THEOREM. *Let K and λ be given and put $\beta_0 = \beta(K)/(\lambda, \beta(K))$. There exists a constant C such that $\{v \mid v \geqslant C, v \equiv 1 \text{ or } m \pmod{\beta_0}\} \subseteq B[K; \lambda]$. Moreover, if there exists a single $v_0 \in B[K; \lambda]$ with $v_0 \equiv f \pmod{\beta_0}$ (i.e., if f is a *-fiber of $B[K; \lambda]$), then there exists a constant C' such that $\{v \mid v \geqslant C', v \equiv f \pmod{\beta_0}\} \subseteq B[K; \lambda]$.*

9.6. THEOREM. *The Extended Existence Conjecture is valid for a pair K, λ whenever $\gamma(K)/(\lambda, \gamma(K))$ is one or a prime power.*

Proof. It suffices to show that every solution f modulo $\beta(K)/(\lambda, \beta(K))$ to the system (12) is a *-fiber of $B[K; \lambda]$. The second congruence of (12) implies

$$f(f-1) \equiv 0 \left(\mod \frac{\gamma(K)}{(\lambda, \gamma(K))}\right)$$

and, if the modulus is one or a prime power, then either $f \equiv 1$ or 0

$$\left(\mod \frac{\gamma(K)}{(\lambda, \gamma(K))}\right).$$

Since

$$f \equiv 1 \left(\mod \frac{\alpha(K)}{(\lambda, \alpha(K))}\right)$$

and $(\alpha(K), \gamma(K)) = 1$, the first case implies

$$f \equiv 1 \left(\mod \frac{\beta(K)}{(\lambda, \beta(K))}\right)$$

and the second implies

$$f \equiv m \left(\mod \frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

But we know 1 and m are *-fibers of $B[K; \lambda]$ and the theorem is proved.

Since $\gamma(\{k\}) = k$, we have the

COROLLARY. *The Existence Conjecture is valid for a pair k, λ whenever $k/(\lambda, k)$ is one or a prime power. In particular, whenever k is a prime power or $k = \lambda$.*

9.7. LEMMA. *Let a and c be relatively prime integers. If $\lambda(v-1) \equiv 0 \pmod{ac}$, then there exists an integer d such that $\lambda(d-v) \equiv 0 \pmod{ac}$, $d-1 \equiv 0 \pmod{a}$, and $d(d-1) \equiv 0 \pmod{ac}$.*

Proof. Write

$$c = P_1^{\mu_1} P_2^{\mu_2} \cdots P_n^{\mu_n} \quad \text{and} \quad \frac{c}{(\lambda, c)} = P_1^{\nu_1} P_2^{\nu_2} \cdots P_r^{\nu_r}$$

as the product of powers of distinct primes where $0 \leqslant r \leqslant n$, $1 \leqslant \nu_i \leqslant \mu_i$ for $i = 1, 2, \ldots, r$, and $1 \leqslant \mu_i$ for $i = r+1, \ldots, n$. Now

$$v(v-1) \equiv 0 \left(\mathrm{mod}\ \frac{c}{(\lambda, c)}\right),$$

so $v \equiv \epsilon_i \pmod{P_i^{\nu_i}}$ where $\epsilon_i = 0$ or 1, $i = 1, 2, \ldots, r$. Put $\epsilon_i = 0$, say, for $i = r+1, \ldots, n$. Select an integer t such that $t \equiv \epsilon_i - v \pmod{P_i^{\mu_i}}$ and $t \equiv 1 - v \pmod{a}$. We may take $d = v + t$.

By the choice of t, $d \equiv 0$ or $1 \pmod{P_i^{\mu_i}}$ and $d \equiv 1 \pmod{a}$. Thus $d(d-1) \equiv 0 \pmod{c}$ and then $d(d-1) \equiv 0 \pmod{ac}$. By the choice of ϵ_i, $t \equiv 0 \pmod{P_i^{\mu_i}}$, $i = 1, \ldots, r$, and hence $t \equiv 0 \pmod{c/(\lambda, c)}$, $\lambda t \equiv 0 \pmod{c}$. Also $\lambda t \equiv \lambda(1-v) \equiv 0 \pmod{a}$, so $\lambda t \equiv \lambda(d-v) \equiv 0 \pmod{ac}$.

9.8. THEOREM. *If the Extended Existence Conjecture is valid for a set K and $\lambda = 1$, then it is valid for K and all $\lambda \geqslant 1$.*

Proof. Assuming validity for $B[K]$, let λ be given and let f be a solution of the system (12). Taking $a = \alpha(K)$ and $c = \gamma(K)$ in Lemma 9.7, select an integer d,

$$d \equiv f \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

$d - 1 \equiv 0 \pmod{\alpha(K)}$, $d(d-1) \equiv 0 \pmod{\beta(K)}$. By our assumption, d is a fiber of $B[K]$ and hence, by Lemma 9.4, d is a *-fiber of $B[K; \lambda]$. But then so is f, and this proves the theorem.

9.9. THEOREM. *If the Existence Conjecture is valid for pairs k, $\lambda = 1$ with $k \geqslant M$ (M is any constant), then the Extended Existence Conjecture holds in general.*

Proof. In view of 9.8, it will suffice to show that the Extended Conjecture holds for the sets $B[K]$. Let K be given and let f be a solution of $f - 1 = 0 \pmod{\alpha(K)}$ and $f(f-1) \equiv 0 \pmod{\beta(K)}$. It remains to show that f is a fiber of $B[K]$.

Select $k \in B[K]$ which represents the maximum fiber of $B[K]$, so $k \equiv 1 \pmod{\alpha(K)}$ and $k \equiv 0 \pmod{\gamma(K)}$, and such that $k \geqslant M$. Put $l = k(k-1)/\beta(K)$. Then $l(f-1) \equiv 0 \pmod{k-1}$ and $lf(f-1) \equiv 0 \pmod{k(k-1)}$. By Lemma 9.7, there exists an integer d such that $l(d-f) \equiv 0 \pmod{k(k-1)}$, $d-1 \equiv 0 \pmod{k-1}$, and $d(d-1) \equiv 0 \pmod{k(k-1)}$. Assuming the Existence Conjecture for $B[k]$, d is a fiber of $B[k] \subseteq B[K]$ and hence a fiber of $B[K]$. But $d \equiv f \pmod{\beta(K)}$ so that f is a fiber of $B[K]$ as required.

9.10. THEOREM. *The Extended Existence Conjecture is valid for a pair K, λ whenever $\lambda \geqslant ([\frac{1}{2}\gamma(K)] - 1)([\frac{1}{2}\gamma(K)] - 2)$. (Here $[x]$ denotes the greatest integer in x.)*

Proof. For λ as above, we must show that every solution f of (11) is a *-fiber of $B[K; \lambda]$. Fix such a solution f and by Lemma 9.7, choose an integer d such that

$$d \equiv f \left(\mathrm{mod}\ \frac{\beta(K)}{(\lambda, \beta(K))}\right),$$

$d - 1 \equiv 0 \pmod{\alpha(K)}$, $d(d-1) \equiv 0 \pmod{\beta(K)}$.

Now the set of *-fibers of $B[K; \lambda]$ is closed under the operation $a(b-c) + c$; for the *-fibers either coincide with the fibers or are their image under $Z/(\beta(B[K; \lambda)) \to Z/(\frac{1}{2}\beta(B[K; \lambda]))$ (recall Theorem 8.1). Let m be an integer such that $m \equiv 1 \pmod{\alpha(K)}$ and $m \equiv 0 \pmod{\gamma(K)}$, so that m is a *-fiber of $B[K; \lambda]$. If $d' = 1 + m - d$ is a *-fiber of $B[K; \lambda]$, then so is $d'(m-1) + 1$. But $d'm \equiv m \pmod{\beta(K)}$, so $d \equiv d'(m-1) + 1 \pmod{\beta(K)}$. Thus, to show that f is a *-fiber of $B[K; \lambda]$, it will suffice to show that either d or d' is.

Now $d + d' \equiv 0 \pmod{\gamma(K)}$, so we may select an integer t, $0 \leqslant t \leqslant [\frac{1}{2}\gamma(K)]$, such that $t \equiv d'' \pmod{\gamma(K)}$ where d'' is either d or d'. If $t \equiv 0$ or 1, then, since $d'' \equiv 1 \pmod{\alpha(K)}$, we would have $d'' \equiv 1$ or $m \pmod{\beta(K)}$. Then d'' would be a fiber of $B[K]$ and hence a *-fiber of $B[K; \lambda]$ as required.

Otherwise, $1 < t \leqslant [\frac{1}{2}\gamma(K)]$. Then we can verify that $d''(d''-1) \equiv t(d''-1) \equiv (d''-m)(t-1) \equiv 0 \pmod{\gamma(K)}$. And, since $d'' \equiv 1 \equiv m \pmod{\alpha(K)}$, we conclude $t(d''-1) \equiv (d''-m)(t-1) \equiv 0 \pmod{\beta(K)}$. Equivalently,

$$d'' \equiv 1 \left(\mathrm{mod}\ \frac{\beta(K)}{(t, \beta(K))}\right) \quad \text{and} \quad d'' \equiv m \left(\mathrm{mod}\ \frac{\beta(K)}{(t-1, \beta(K))}\right),$$

and we see that d'' is a *-fiber of $B[K; t]$ and also a *-fiber of $B[K; t-1]$. Now every integer $l \geqslant (t-1)(t-2)$ may be written as $l = at + b(t-1)$ for some $a, b \geqslant 0$ (this is readily verified by induction on l, for $t \geqslant 2$). In

particular, since $\lambda \geqslant ([\frac{1}{2}\gamma(K)] - 1)([\frac{1}{2}\gamma(K)] - 2) \geqslant (t-1)(t-2)$, we have $\lambda = at + b(t-1)$ for some $a, b \geqslant 0$. Appealing to Lemma 9.4, d'' is a *-fiber of $B[K; \lambda]$ and this completes the proof.

COROLLARY. *The Existence Conjecture is valid for a pair k, λ whenever* $\lambda \geqslant ([\frac{1}{2}k] - 1)([\frac{1}{2}k] - 2)$.

Theorem 9.10 does not exhaust the power of Lemma 9.4. By the Corollaries to 9.6 and 9.10, the Existence Conjecture has been verified for all pairs k, λ with $k \leqslant 11$ with the exception of $k = 6$, $\lambda = 1$ and $k = 10$, $\lambda = 1, 3, 7, 9, 11$. We close by verifying it for $k = 10$, $\lambda = 7, 9, 11$. The Existence Conjecture would assert that the *-fibers of $B[10; 7]$ and $B[10; 11]$ are 1, 10, 46, and 55 (mod 90); the *-fibers of $B[10; 9]$ are 0, 1, 5, and 6 (mod 10). But, by Theorem 9.6, we know that the *-fibers of $B[10; 2]$ are 1 and 10 (mod 45); the *-fibers of $B[10; 5]$ are 1, 10 (mod 18). The integers 1, 10, 45 and 55 are thus *-fibers of $B[10; 2]$ and $B[10; 5]$, and hence by Lemma 9.4 are *-fibers of $B[10; 7]$, $B[10; 9]$, and $B[10; 11]$.

ACKNOWLEDGMENT

The author is indebted to Professor D. K. Ray-Chaudhuri (who supervised the preparation of the author's Ph.D. dissertation, on which this paper is based) for his advice, encouragement, and many stimulating discussions.

REFERENCES

1. G. BIRKHOFF, "Lattice Theory," 2nd ed., *Amer. Math. Soc. Colloq. Publ.* **25** (1948).
2. S. CHOWLA, P. ERDÖS, AND E. G. STRAUS, On the maximal number of pairwise orthogonal Latin squares of a given order, *Canad. J. Math.* **12** (1960), 204–208.
3. H. HANANI, The existence and construction of balanced incomplete block designs, *Ann. Math. Statist.* **32** (1961), 361–386.
4. H. HANANI, A balanced incomplete block design, *Ann. Math. Statist.* **36** (1965), 711.
5. H. HANANI, On balanced incomplete block designs and related designs, unpublished manuscript, Technion, Israel Institute of Technology, Haifa, 1968.
6. R. M. WILSON, An Existence Theory for Pairwise Balanced Designs, Ph.D. dissertation, Department of Mathematics, The Ohio State University, 1969.
7. R. M. WILSON, Cyclotomy and difference families in elementary Abelian groups, *J. Number Theory* **4** (1972), 17–47.
8. R. M. WILSON, An existence theory for pairwise balanced designs. I. Composition theorems and morphisms, *J. Combinatorial Theory* **A13** (1971), 220–245.