Scan
add to 4
segs

$(2^{4k}+2^{2k+1},2^{4k}+2^{2k+1})$ and order $2^{2k+2}(2^{2k-1}+1+s)$. Note that for $s=0$, this provides two non-trivial sequences of Hadamard matrices.

(ii) Exchange the matrix Q by $I_{2^{2k}}$ in (i).

Corollary 10.

(i) *For each positive integer k, there are orthogonal designs of type* $(2^{2k+1},2^{2k+1},2^{4k+1},2^{4k+1})$, $(2^{4k}+2^{2k},2^{4k}+2^{2k},2^{4k}+2^{2k},2^{4k+2k})$, $(2^{2k+1},2^{2k}+2^{4k},2^{2k}+2^{4k},2^{4k+1})$ *and order* $2^{2k+2}(2^{2k}+1+s)$, $s=0,1,2,\ldots$.

(ii) *For each positive integer k, there are orthogonal designs of type* $(2,2^{2k+1},2^{4k+1},2^{4k+1})$, $(1+2^{4k},1+2^{4k},2^{2k}+2^{4k},2^{2k}+2^{4k})$, $(2,2^{2k}+2^{4k},2^{2k}+2^{4k},2^{4k+1})$, $(2^{2k+1},1+2^{4k},1+2^{4k},2^{4k+1})$ *and order* $2^{2k+2}(2^{2k}+1+s)$, $s=1,2,\ldots$.

Proof. The proof of this part is now predictable.

Remarks: (i) One can change the sign of any block in each of the above designs.

(ii) The designs and the Hadamard matrices (from Corollary 9) in this paper are all new. The closest construction to the above is the method of construction given in Theorem 4.49 of [1]. These are the designs of the type mentioned in Theorem 3, but with A, B, C, D being circulant.

The fact that the block signs could be changed may lead to unequivalent designs (and in particular unequivalent Hadamard matrices).

The research is supported by NSERC Grant A7853.

References.

[1] A.V. Geramita and Jennifer Seberry, *Orthogonal designs, quadratic forms and Hadamard matrices*, "Lecture Notes in Pure and Applied Mathematics," Vol. 45, Marcel Dekker, New York and Basel, 1979.

[2] J.M. Goethals and J.J. Seidel, *A Skew-Hadamard matriz of order 36* , J. Aust. Math. Soc. 11 (1970), 343-344.

[3] H. Kharaghani, *"New class of weighing matrices,"* Ars Combinatoria 19 (1985), 69-72.

[4] H. Kharaghani, *"Some orthogonal designs of order $n \equiv 0$ mod 4,"* preprint.

[5] H. Kharaghani, *"Construction of orthogonal designs,"* Ars Combinatoria (to appear).

Department of Mathematics
University of Alberta
Edmonton, Alberta
T6G 2G1

6167-6170

Association Schemes and Derived PBIB Designs of Prime Power Order

R.A. Hultquist, G.L. Mullen and H. Niederreiter

ABSTRACT

Using the finite field analog of the Euler function in the polynomial ring over a finite field, we construct a class of association schemes of prime power order. Several results are then given concerning the number of nonisomorphic association schemes constructible by our method. For each of our association schemes, we also indicate how to construct a series of cyclic PBIB designs.

1. Introduction.

In [1] Agrawal and Nair used the Euler phi function from elementary number theory to construct an association scheme for each composite integer v. From the association scheme, several classes of partially balanced incomplete block (PBIB) designs, called reduced residue classes cyclic PBIB designs, were then constructed.

In the present paper, for v a prime power, we present a generalization of the Agrawal and Nair construction. In section 2 we construct a class of association schemes by using the finite field analog of the Euler function in the ring of polynomials over a finite field. We also show that for $v=p^n$ with p a prime, the results of Agrawal and Nair can be obtained as a special case of our construction. Section 3 is devoted to obtaining some results concerning the number of nonisomorphic association schemes obtainable from our construction over the field of q elements. In particular, we show that the number of such nonisomorphic association schemes with q^n treatments is closely related to the number of factorization patterns of polynomials of degree n. Finally in section 4, we follow the lead of Agrawal and Nair and indicate how to construct a series of cyclic PBIB designs from each of our association schemes.

For general terminology of association schemes and PBIB designs we refer the reader to Clatworthy [3] and Raghavarao [8].

ARS COMBINATORIA 25(1988), pp. 65-82

2. Construction of Association Schemes.

Let F_q denote the finite field of order $q = p^\delta$ with p a prime and $\delta \geq 1$. Let $F_q[x]$ denote the ring of polynomials in one indeterminate x with coefficients in F_q so that the ring $F_q[x]$ has unique factorization. Moreover, the division and Euclidean algorithms can be used to calculate the greatest common divisor $(\alpha(x),\beta(x))$ of two polynomials $\alpha(x),\beta(x) \in F_q[x]$.

The Euler phi function $\phi(v)$ counts the number of positive integers $\leq v$ that are relatively prime to v. The function $\phi(v)$ has an analog in the ring $F_q[x]$. Let $V \in F_q[x]$ have degree $n \geq 1$ and let $\Phi_q(V)$ denote the number of polynomials in a reduced residue system modulo V, so that $\Phi_q(V)$ counts the number of polynomials over F_q that are of degree $< n$ and relatively prime to V. The function Φ_q is multiplicative, so that if $V_1,V_2 \in F_q[x]$ with $(V_1,V_2) = 1$, then $\Phi_q(V_1V_2) = \Phi_q(V_1)\Phi_q(V_2)$. If V is irreducible of degree n and $e \geq 1$, then $\Phi_q(V^e) = q^{ne} - q^{n(e-1)}$. See [5, p. 122-123] for details.

Let $V \in F_q[x]$ be a monic polynomial of degree $n \geq 1$ and let M_V denote the complete residue system modulo V containing all the q^n polynomials over F_q of degree $< n$. Suppose that V has the canonical factorization $V = V_1^{e_1} \cdots V_r^{e_r}$, where $e_i \geq 1$ and the V_i are distinct monic irreducible polynomials of degree v_i so that $n = \sum_{i=1}^{r} v_i e_i$. Let $T_1 = 1$, $T_2,...,T_s$ be the monic divisors of V except for V itself, so that the total number of monic divisors of V is $s + 1 = \prod_{i=1}^{r} (e_i+1)$.

For $i = 1,...,s$ let $A_i = \{\alpha(x) \in M_V \,|\, (\alpha(x),V(x)) = T_i(x)\}$ and let n_i be the cardinality of the set A_i, so that $n_i = \Phi_q(V/T_i)$. Clearly A_1 is a reduced residue system modulo V and hence A_1 is a group of order $\Phi_q(V)$ under polynomial multiplication modulo V.

Let $\alpha(x)A_j = \{\alpha(x)\beta(x) \,|\, \beta(x) \in A_j\}$ and let $[\alpha(x)A_j] = \{\gamma(x) \in M_V \,|\, \gamma(x) \equiv \alpha(x)\beta(x) \bmod V \text{ for some } \beta(x) \in A_j\}$ denote the set of distinct polynomials obtained when $\alpha(x)A_j$ is considered modulo V. If $\alpha_j(x) \in A_j$ then $[\alpha_j(x)A_1] = A_j$ for $j = 1,...,s$ and moreover each polynomial in A_j is represented the same number of times, say f_j, in the set $\alpha_j(x)A_1$ considered modulo V. It follows also that $[\alpha_1(x)A_j] = A_j$ for every $\alpha_1(x) \in A_1$.

Definition 2.1. Two polynomials $\alpha(x)$ and $\beta(x)$ in M_V are said to be i-th associates if $\alpha(x) - \beta(x) \in A_i$.

We note that if $\alpha(x) \in A_i$ then $-\alpha(x) \in A_i$, so the relation is symmetric.

Definition 2.2. If $\alpha(x)$ and $\beta(x)$ are k-th associates, define $p_{ij}^k(\alpha,\beta)$ to be the number of common polynomials among the i-th associates of $\alpha(x)$ and the j-th associates of $\beta(x)$.

Lemma 2.1. *If $\alpha(x)$ and $\beta(x)$ are k-th associates and if $\delta(x)$ and $\gamma(x)$ are k-th associates, then $p_{ij}^k(\alpha,\beta) = p_{ij}^k(\delta,\gamma)$.*

Proof. Since A_1 is indeed a group under polynomial multiplication modulo $V(x)$, Agrawal and Nair's proof of their Lemma 2.1 can be extended to our case. We include a proof here only for the sake of completeness.

Let $\alpha(x) + A_j = \{\alpha(x)+a(x) \,|\, a(x) \in A_j\}$ where all calculations are performed modulo $V(x)$. Suppose $\alpha(x) - \beta(x) = \mu(x)$ and $\delta(x) - \gamma(x) = \omega(x)$, so that if $|S|$ denotes the cardinality of the set S then

$$p_{ij}^k(\alpha,\beta) = |(\alpha(x)+A_i) \cap (\beta(x)+A_j)|.$$

A simple calculation shows that

$$p_{ij}^k(\alpha,\beta) = |(\alpha(x)-\beta(x)+A_i) \cap A_j| = |(\mu(x)+A_i) \cap A_j|$$

and $p_{ij}^k(\delta,\gamma) = |(\omega(x)+A_i) \cap A_j|$.

Since $[a_i(x)A_1] = A_i$ for $i = 1,...,s$ if $a_i(x) \in A_i$, we have $\omega(x) = \mu(x)a_1(x)$ for some $a_1(x) \in A_1$. But since A_1 is a group we have $a_1^{-1}(x) \in A_1$, so

$$\begin{aligned} |(\omega(x)+A_i) \cap A_j| &= |(a_1(x)\mu(x)+A_i) \cap A_j| \\ &= |(\mu(x)+[a_1^{-1}(x)A_i]) \cap [a_1^{-1}(x)A_j]| \\ &= |(\mu(x)+A_i) \cap A_j| \end{aligned}$$

which completes the proof.

Definition 2.3. Given a set of v treatments, a symmetric relation is an association scheme with s association classes if

(a) Any two distinct treatments are i-th associates for a unique $i = 1,...,s$;

(b) Each treatment has n_i i-th associates, the number n_i being independent of the treatment;

(c) If two treatments α and β are k-th associates, then the number p_{ij}^k of treatments which are i-th associates of α and j-th associates of β is independent of α and β.

The numbers v, n_i and p_{ij}^k, $1 \leq i,j,k \leq s$, are the parameters of the

association scheme. Using polynomials to represent treatments, we have now proven.

Theorem 2.2. *For monic* $V = V_1^{e_1} \cdots V_r^{e_r} \in F_q[x]$ *of degree* $n \geq 1$, *the relations defined in Definition 2.1 yield an association scheme with* $s = \prod_{j=1}^{r}(e_j+1) - 1$ *association classes and parameters* $v = q^n$, $n_i = \Phi_q(V/T_i)$ *for* $1 \leq i \leq s$.

We note that if V is irreducible over F_q, then the association scheme has only one association class, so that in general we assume that V is a reducible polynomial over F_q.

We now show that if $v = p^n$ with p a prime, the association scheme of Agrawal and Nair [1] can be obtained as a special case of our construction. Consider the association scheme induced by $V(x) = x^n$ over the field F_p. Clearly there are $s = n$ association classes and $n_i = \Phi_p(x^{n-i+1}) = p^{n-i+1} - p^{n-i}$ for $i = 1,...,s$. Now if $A_i = \{\alpha_{i1}(x), \ldots, \alpha_{in_i}(x)\}$ in the finite field construction, then $B_i = \{\alpha_{i1}(p), \ldots, \alpha_{in_i}(p)\}$ is the corresponding set in the Agrawal and Nair construction, where $\alpha_{ij}(p)$ is calculated modulo $v = p^n$. Hence the two association schemes are indeed equivalent.

These association schemes and the PBIB designs that we will construct in section 4 find application in experimental design. While for such work the required irreducible polynomials are in general of low degree over fields of small order, irreducible polynomials over an arbitrary field F_q are easily constructed by calculating minimal polynomials of elements in extension fields F_{q^k} of F_q where $k \geq 1$ is the degree of the extension. In particular, if $\alpha \neq 0 \in F_{q^k}$ and s is the smallest positive integer such that $\alpha^{q^s} = \alpha$, the elements $\alpha, \alpha^q, \ldots, \alpha^{q^{s-1}}$ are the distinct conjugates of α relative to F_q. The minimal polynomial $f_\alpha(x)$ of α has degree s, is irreducible over F_q, and moreover $f_\alpha(x) = \prod_{i=0}^{s-1}(x - \alpha^{q^i}) \in F_q[x]$. For further theoretical details regarding irreducible polynomials over finite fields, see chapter 2, section 2, and chapter 3, sections 2 and 3, in [5].

Lists of irreducibles over small fields are available in the literature. Table C in [5] lists all monic irreducible polynomials of degree n over F_p for n and p as follows: $p = 2$, $n \leq 11$; $p = 3$, $n \leq 7$; $p = 5$, $n \leq 5$; and $p = 7$, $n \leq 4$.

Because of their application in algebraic coding theory, more extensive tables of irreducibles have been constructed in the case $p = 2$. For example, Marsh [6] provides an exhaustive list of all irreducibles of degree $n \leq 19$ over F_2 and Peterson and Weldon [7] list one irreducible over F_2 of each possible order for all degrees n with $17 \leq n \leq 34$. Moreover, Table

F of [5] lists one primitive, and hence irreducible, polynomial of each degree $n \geq 2$ over F_p for all $p < 50$ with $p^n < 10^9$.

For irreducibles over fields of prime power order p^δ with $\delta > 1$, Beard and West [2] provide an exhaustive list of irreducibles of degree $n \geq 2$ over F_{p^δ} in each of the following cases: $p = 2$, $\delta = 2$, $n \leq 5$; $p = 2$, $\delta = 3$, $n \leq 4$; $p = 2$, $\delta = 4$, $n \leq 3$; and $p = 3$, $\delta = 2$, $n \leq 4$.

3. Enumeration of Association Schemes.

The Agrawal and Nair construction described in [1] yields one association scheme for each composite integer v. It will be seen that if $v = q^n$, our finite field construction yields a number of nonisomorphic association schemes each with q^n treatments, one of which was shown in section 2 to reduce to the Agrawal and Nair case. In this section we show that if $v = q^n$ with $q \geq n$, then the number of nonisomorphic association schemes constructible with our finite field construction is given by the number of factorization patterns of polynomials of degree n, which as will be seen, is greater than the number of unrestricted partitions of n.

A factorization pattern of a polynomial of degree n is a partition of the form $n = b_1 a_1 + \cdots + b_r a_r$ where

$$b_1 = b_2 = \cdots = b_{k_1} < b_{k_1+1} = b_{k_1+2} = \cdots = b_{k_2} < b_{k_2+1} = b_{k_2+2} = \cdots = b_{k_3} < \cdots < b_{k_{c-1}+1} = b_{k_{c-1}+2} = \cdots = b_{k_c} \tag{3.1}$$

with $k_c = r$ and

$$a_1 \geq a_2 \geq \cdots \geq a_{k_1},\ a_{k_1+1} \geq a_{k_1+2} \geq \cdots \geq a_{k_2},\ \ldots,\ a_{k_{c-1}+1} \geq a_{k_{c-1}+2} \geq \cdots \geq a_{k_c} \tag{3.2}$$

where b_i is the degree of an irreducible occurring with multiplicity a_i. Hence we will write the factorization pattern above in the form

$$n = b_1^{a_1} + \cdots + b_r^{a_r}. \tag{3.3}$$

Since in the form (3.3) if $i \neq j$ we may indeed have $b_i = b_j$, we have called such a partition a factorization pattern to distinguish it from an unrestricted partition of n where one assumes the b_i's to be distinct when using the form (3.3).

We consider for illustrative purposes two factorization patterns of 4, namely $1^2 + 2$ and $1 + 1 + 2$. The factorization pattern $1^2 + 2$ corresponds to one linear factor of multiplicity 2 and one irreducible quadratic while the pattern $1 + 1 + 2$ corresponds to two distinct linear factors each with multiplicity 1 and one irreducible quadratic.

If $q < n$ it will not be possible to construct an association scheme with q^n treatments using our finite field construction for each factorization pattern of n. For example, if we consider the factorization pattern $n = 1 + \cdots + 1$ with $q < n$, then clearly there are only q distinct monic linear polynomials over F_q.

It is possible to write down a criterion in terms of $I_q(t)$, the number of monic irreducible polynomials of degree t over F_q, which gives a necessary and sufficient condition to determine whether from a given factorization pattern of n, it is possible to construct a polynomial $V(x)$ of degree n inducing an association scheme with q^n treatments. It is well known, see [5, p. 93], that

$$I_q(t) = \frac{1}{t}\sum_{d|t}\mu(d)q^{t/d} \tag{3.4}$$

where $\mu(d)$ is the Möbius function from elementary number theory. Consider the factorization pattern of n given by (3.1) and (3.2). Then a polynomial $V = B_1^{a_1}\cdots B_r^{a_r}$ of degree n with B_i irreducible of degree b_i over F_q inducing an association scheme with q^n treatments can be constructed if and only if $I_q(b_{k_i}) \geq k_i - k_{i-1}$ for $1 \leq i \leq c$, where $k_0 = 0$.

If $[\,]$ denotes the greatest integer function and if $q \geq n$, it is easy to check that $I_q(t) \geq [n/t]$. Given any factorization pattern of n, no more than $[n/t]$ irreducibles of degree t will be needed to construct a polynomial $V(x)$ of degree n over F_q with the property that the factorization pattern of $V(x)$ is the given factorization pattern.

The following theorem shows that if V_1 and V_2 induce association schemes with q^n treatments and V_1 and V_2 have distinct factorization patterns, then V_1 and V_2 induce association schemes which have different parameter sets, so that in particular, they are nonisomorphic. To be more precise, let $V = B_1^{a_1}\cdots B_r^{a_r} \in F_q[x]$ with $B_j \in F_q[x]$ a monic irreducible of degree b_j and $a_j \geq 1$ for $j = 1,...,r$, where the b_j's and a_j's satisfy (3.1) and (3.2). Let $T_1,...,T_t$ be the monic divisors of V so that $t = \prod_{j=1}^{r}(a_j+1)$. Here we are considering all divisors of V, even though in the construction of our association schemes in section 2 we considered only divisors $T \neq V$. We also note that as T_i runs through the divisors of V so does V/T_i. Hence if $\ell_i = \Phi_q(T_i)$ for $i = 1,...,t$ and $n_i = \Phi_q(V/T_i)$ for $i = 1,...,s$ as defined in section 2, then the multiset $\{\ell_1,\ldots,\ell_t\}$ is equal to the multiset $\{1,n_1,...,n_s\}$.

For $i = 1,...,t$, ℓ_i can be written uniquely in the form $\ell_i = q^{E(\ell_i)}R(\ell_i)$ with $E(\ell_i) \geq 0$ and $gcd(q,R(\ell_i)) = 1$. We note that if $T_i = B_1^{e_1}\cdots B_r^{e_r}$ with $0 \leq e_j \leq a_j$ for $1 \leq j \leq r$, then

$$E(\ell_i) = \sum_{j=1}^{r}\max(0,e_j-1)b_j,\quad R(\ell_i) = \prod_{\substack{j=1\\ e_j\geq 1}}^{r}(q^{b_j}-1).$$

Consider the multiset $S = \{\ell_1,\ldots,\ell_t\}$, i.e. consider the set of values attained by the ℓ_i, together with the multiplicity with which each value is attained.

Theorem 3.1. *The multiset $S = \{\ell_1,\ldots,\ell_t\}$ determines the tuple $(b_1,...,b_r,a_1,...,a_r)$ uniquely.*

Proof. The proof proceeds in two steps. In the first step the b_j are determined and in the second the a_j.

Step 1.

Consider those ℓ_i with $E(\ell_i) = 0$. There are exactly 2^r of those, corresponding to the r-tuples $(e_1,...,e_r)$ with $0 \leq e_j \leq 1$ for $1 \leq j \leq r$. Thus r is determined. Delete the value $\ell_i = 1$ corresponding to $T_i = 1$. Among the remaining $2^r - 1$ values ℓ_i the smallest one is $q^{b_1} - 1$, thus b_1 is determined, and the second smallest is $q^{b_2} - 1$, thus b_2 is determined. From the $2^r - 1$ values ℓ_i above delete the values $q^{b_1} - 1$, $q^{b_2} - 1$, $(q^{b_1}-1)(q^{b_2}-1)$. Among the remaining $2^r - 4$ values ℓ_i the smallest one is $q^{b_3} - 1$, thus b_3 is determined. From these $2^r - 4$ values ℓ_i delete the values $q^{b_3} - 1$, $(q^{b_1}-1)(q^{b_3}-1)$, $(q^{b_2}-1)(q^{b_3}-1)$, $(q^{b_1}-1)(q^{b_2}-1)(q^{b_3}-1)$. Among the remaining $2^r - 8$ values ℓ_i the smallest one is $q^{b_4} - 1$, thus b_4 is determined. Continuing in this way, the values of $b_1,...,b_r$ are determined. Since $\Phi_q(T)$ does not depend on the specific form of the B_j, but only on the degrees of the B_j, we may choose arbitrary monic irreducible $B_j \in F_q[x]$ with the degree of B_j equal to b_j for $1 \leq j \leq r$.

Step 2.

Case $q > 2$. We first determine $a_1,a_2,...,a_{k_1}$. Consider those ℓ_i with $R(\ell_i) = q^{b_1} - 1$. The corresponding $E(\ell_i)$ are exactly all values $(e_j-1)b_1$ with $1 \leq e_j \leq a_j$, $1 \leq j \leq k_1$. For these ℓ_i write $E_1(\ell_i) = 1 + E(\ell_i)b_1^{-1}$. Since $a_1 \geq a_2 \geq \cdots \geq a_{k_1}$, the largest value of $E_1(\ell_i)$ is a_1, thus a_1 is determined. If the largest value of $E_1(\ell_i)$ occurs with multiplicity m_1, this means that a_1 is repeated m_1 times, i.e. $a_1 = a_2 = \cdots = a_{m_1}$. If $m_1 = k_1$, then we are done. If $m_1 < k_1$, let d_1 be the largest positive integer such that d_1 is attained more than m_1 times by $E_1(\ell_i)$, say it is attained $m_2 > m_1$ times. Then $a_{m_1+1} = a_{m_1+2} = \cdots = a_{m_2} = d_1$. If $m_2 = k_1$, then we are done. If $m_2 < k_1$, let d_2 be the largest positive

integer such that d_2 is attained more than m_2 times by $E_1(\ell_i)$, say it is attained $m_3 > m_2$ times. Then $a_{m_2+1} = a_{m_2+2} = \cdots = a_{m_3} = d_2$. Continuing in this way, the values of $a_1,a_2,...,a_{k_1}$ are determined.

If $k_1 = r$, then we are done. Otherwise delete from S the $(a_1+1)...(a_{k_1}+1)$ values $\Phi_q(T)$ with

$$T|\prod_{j=1}^{k_1} B_j^{a_j}.$$

Among the remaining ℓ_i consider those with $R(\ell_i) = q^{b_{k_2}} - 1$. The corresponding $E(\ell_i)$ are exactly all values $(e_j-1)b_{k_2}$ with $1 \le e_j \le a_j$, $k_1+1 \le j \le k_2$. For these ℓ_i write $E_2(\ell_i) = 1 + E(\ell_i)b_{k_2}^{-1}$. By considering the values of $E_2(\ell_i)$, we can determine $a_{k_1+1},...,a_{k_2}$ by the same method as before. If $k_2 = r$, then we are done. Otherwise, delete from S the $(a_1+1)...(a_{k_2}+1)$ values $\Phi_q(T)$ with

$$T|\prod_{j=1}^{k_2} B_j^{a_j}.$$

Among the remaining ℓ_i consider those with $R(\ell_i) = q^{b_{k_3}} - 1$. Continuing in this way, the values of $a_1,...,a_r$ are determined.

Case $q = 2$. The method for the case $q > 2$ does not work here since we can have $q^{b_j} - 1 = 1$. If $b_1 \ge 2$, this does not occur, and so we can proceed as above. Now let $b_1 = 1$, hence $b_1 = b_2 = \cdots = b_{k_1} = 1$. Consider those ℓ_i with $R(\ell_i) = 1$. The corresponding $E(\ell_i)$ are exactly all values

$$\max(0,e_1-1) + \cdots + \max(0,e_{k_1}-1),\ 0 \le e_j \le a_j,\ 1 \le j \le k_1.$$

For any $h \ge 0$ we can therefore determine the number $N(h)$ of solutions of

$$\max(0,e_1-1) + \cdots + \max(0,e_{k_1}-1) = h$$

with $0 \le e_j \le a_j$, $1 \le j \le k_1$. Now we have in the ring of polynomials with integer coefficients

$$G(x) = \sum_{h=0}^{\infty} N(h)x^h = \prod_{j=1}^{k_1}\Big(\sum_{e_j=0}^{a_j} x^{\max(0,e_j-1)}\Big) = \prod_{j=1}^{k_1}(1+\frac{x^{a_j}-1}{x-1})$$

$$= 2^{\#\{1\le j\le k_1 | a_j=1\}} \prod_{\substack{j=1\\ a_j>1}}^{k_1}(1+\frac{x^{a_j}-1}{x-1}).$$

Thus the leading coefficient of $G(x)$ is 2^{k_1-m}, where $m = k_1 - \#\{1\le j\le k_1 | a_j=1\}$, and so m is determined. Since $a_1 \ge a_2 \ge \cdots \ge a_{k_1}$, this means that $a_j = 1$ for $m+1 \le j \le k_1$. If $m = 0$, then $a_1,...,a_{k_1}$ are determined. Otherwise consider

$$F_1(x) = (x-1)^{m}2^{m-k_1} G(x) = \prod_{j=1}^{m}(x-1)(1+\frac{x^{a_j}-1}{x-1}) = \prod_{j=1}^{m}(x^{a_j}+x-2),$$

where we have $a_1 \ge a_2 \ge \cdots \ge a_m > 1$. After expanding the last product, the largest exponent is $a_1 + \cdots + a_m$ (with corresponding coefficient 1) and the second largest exponent is $a_1 + \cdots + a_{m-1} + 1$ (with corresponding coefficient being positive). The difference between these exponents is $a_m - 1$, thus a_m is determined by $F_1(x)$. Now form

$$F_2(x) = \frac{F_1(x)}{x^{a_m}+x-2} = \prod_{j=1}^{m-1}(x^{a_j}+x-2)$$

and apply the same procedure to it, thus determining a_{m-1}. Continue in this way until $F_m(x) = x^{a_1} + x - 2$ determines a_1. Altogether, we have determined $a_1,a_2,...,a_{k_1}$.

If $k_1 = r$, then we are done. Otherwise delete from S the $(a_1+1)...(a_{k_1}+1)$ values $\Phi_2(T)$ with

$$T|\prod_{j=1}^{k_1} B_j^{a_j}.$$

Among the remaining ℓ_i consider those with $R(\ell_i) = 2^{b_{k_2}} - 1$. The corresponding divisors T are of the form

$$T = UB_w^{e_w} \text{ with } U|\prod_{j=1}^{k_1} B_j^{a_j}$$

and $1 \le e_w \le a_w$ for some $k_1 + 1 \le w \le k_2$. The corresponding $E(\ell_i)$ are exactly all values

$$\max(0,e_1-1) + \cdots + \max(0,e_{k_1}-1) + (e_w-1)b_{k_2}$$

with $0 \le e_j \le a_j$ for $1 \le j \le k_1$ and $1 \le e_w \le a_w$ for some $k_1 + 1 \le w \le k_2$. Let $M(h)$ be the multiplicity of $h \ge 0$ in this system of values $E(\ell_i)$, let $N(h)$ be as above, and let $L(h)$ be the number of solutions of $(e_w-1)b_{k_2} = h$ with $1 \le e_w \le a_w$ for some $k_1 + 1 \le w \le k_2$.

Then in the ring of polynomials with integer coefficients

$$H(x) = \sum_{h=0}^{\infty} M(h)x^h = (\sum_{h=0}^{\infty} N(h)x^h)(\sum_{h=0}^{\infty} L(h)x^h) = G(x)\sum_{h=0}^{\infty} L(h)x^h,$$

where $G(x)$ is as above. Now $H(x)$ and $G(x)$ are known, thus the polynomial $\sum_{h=0}^{\infty} L(h)x^h$ is determined. In other words, we know exactly which values are attained by $(e_w-1)b_{k_2}$, $1 \le e_w \le a_w$, $k_1+1 \le w \le k_2$, and with which multiplicity each value is attained. Therefore the method in the case $q > 2$ can be applied and determines all a_w for $k_1+1 \le w \le k_2$.

If $k_2 = r$, then we are done. Otherwise delete from S the $(a_1+1)...(a_{k_2}+1)$ values $\Phi_2(T)$ with

$$T \mid \prod_{j=1}^{k_2} B_j^{a_j}.$$

Among the remaining ℓ_i consider those with $R(\ell_i) = 2^{b_{k_3}} - 1$. The corresponding divisors T are of the form

$$T = UB_w^{e_w} \text{ with } U \mid \prod_{j=1}^{k_1} B_j^{a_j}$$

and $1 \le e_w \le a_w$ for some $k_2+1 \le w \le k_3$. The corresponding $E(\ell_i)$ are exactly all values

$$\max(0,e_1-1) + \cdots + \max(0,e_{k_1}-1) + (e_w-1)b_{k_3}$$

with $0 \le e_j \le a_j$ for $1 \le j \le k_1$ and $1 \le e_w \le a_w$ for some $k_2+1 \le w \le k_3$. Thus we can proceed as above to determine a_w for $k_2+1 \le w \le k_3$. Continuing in this way, the values of $a_1,...,a_r$ are determined.

Let $F_q(n)$ represent the number of factorization patterns of n of the form (3.1) and (3.2) with the property that there exists a monic polynomial V of degree n over F_q such that V factors over F_q into one of the $F_q(n)$ factorization patterns. For example if $n = 4$, there are 11 distinct factorization patterns of 4 given by $1+1+1+1$, 1^2+1+1, 1^2+1^2, 1^3+1, 1^4, $1+1+2$, 1^2+2, $1+3$, $2+2$, 2^2, and 4. Hence $F_2(4) = 8$ since by (3.4) there are no monic polynomials of degree 4 over F_2 which have the factorization patterns $1+1+1+1$, 1^2+1+1, or $2+2$. Similarly $F_3(4) = 10$ and $F_q(4) = 11$ if $q \ge 4$.

Corollary 3.2. *For each prime power q and each $n \ge 1$ there are $F_q(n)$ nonisomorphic association schemes with q^n treatments constructible by the method of section 2.*

As factorization patterns of the form (3.1) and (3.2) now have combinatorial significance, a study of such patterns would indeed be of interest. For the moment however, we prove only the following theorem which provides a generating function that allows the computation of $F_q(n)$ for any prime power q and $n \ge 1$.

Theorem 3.3. *The generating function for $F_q(n)$ is given by*

$$1 + \sum_{n=1}^{\infty} F_q(n)z^n = \prod_{n=1}^{\infty} (1-z^n)^{-B_q(n)} \qquad (3.5)$$

where $B_q(n)$ is the number of positive divisors d of n with $d \le I_q(n/d)$ and $I_q(n/d)$ is defined in (3.4).

Proof. We first show that if $p(m,n)$ denotes the number of ordinary partitions of n into at most m parts, then

$$F_q(n) = \sum p(I_q(b_1),a_1)...p(I_q(b_r),a_r) \qquad (3.6)$$

where the sum is over all ordinary partitions $b_1^{a_1} + \cdots + b_r^{a_r}$ of n. It is clear from the discussion in the middle of page 6 that each part $b_j^{a_j}$ of an ordinary partition can be decomposed over F_q into exactly $p(I_q(b_j),a_j)$ distinct factorization patterns of $b_j^{a_j}$. Hence each ordinary partition $b_1^{a_1} + \cdots + b_r^{a_r}$ of n can be decomposed over F_q into exactly $p(I_q(b_1),a_1)...p(I_q(b_r),a_r)$ distinct factorization patterns of n from which (3.6) follows. Hence if we set $p(m,n) = 1$ if $n = 0$, we get

$$1 + \sum_{n=1}^{\infty} F_q(n)z^n = 1 + \sum_{n=1}^{\infty} \left(\sum_{b_1^{a_1}+...+b_r^{a_r}=n} p(I_q(b_1),a_1)...p(I_q(b_r),a_r) \right) z^n$$

$$= 1 + \sum_{n=1}^{\infty} \left(\sum_{n_1+2n_2+3n_3+...=n} p(I_q(1),n_1)p(I_q(2),n_2)p(I_q(3),n_3)... \right) z^n$$

$$= \prod_{j=1}^{\infty} \left(\sum_{n=0}^{\infty} p(I_q(j),n)z^{jn} \right).$$

Since $\prod_{n=1}^{\infty} (1-z^n)^{-1}$ is the generating function for the ordinary partition function, for any $m \ge 1$ we have

$$\sum_{n=0}^{\infty} p(m,n)z^n = \prod_{i=1}^{m}(1-z^i)^{-1}.$$

Applying this with $m = I_q(j)$ and substituting z^j for z, we get

$$\sum_{n=0}^{\infty} p(I_q(j),n)z^{jn} = \prod_{i=1}^{I_q(j)}(1-z^{ij})^{-1}.$$

Therefore

$$1 + \sum_{n=1}^{\infty} F_q(n)z^n = \prod_{j=1}^{\infty}\prod_{i=1}^{I_q(j)}(1-z^{ij})^{-1} = \prod_{n=1}^{\infty}(1-z^n)^{-B_q(n)},$$

where $B_q(n)$ is the number of ordered pairs (i,j) of integers with $ij = n$ and $1 \le i \le I_q(j)$. Hence $B_q(n)$ is the number of positive divisors d of n with $d \le I_q(n/d)$ which completes the proof.

Let $F(n)$ denote the total number of factorization patterns of n of the form (3.1) and (3.2). As indicated in the middle of page 6, if $q \ge n$ then $I_q(t) \ge [n/t]$ so that the condition $d \le I_q(n/d)$ is satisfied for all positive divisors d of n. Thus for $q \ge n$ we have $B_q(n) = d(n)$, the number of positive divisors of n. We also have $F_q(n) = F(n)$ for $q \ge n$. Hence we may state

Corollary 3.4. *The generating function for $F(n)$ is given by*

$$1 + \sum_{n=1}^{\infty} F(n)z^n = \prod_{n=1}^{\infty}(1-z^n)^{-d(n)},$$

where $d(n)$ is the number of positive divisors of n.

For the sake of completeness, we list in Table 1 some values of $F_q(n)$ for small q and n. In Table 2 we also list some values of $F(n)$.

Table 1
$F_q(n)$

q\n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	3	4	8	11	20	27	45	61	95	128	193	257	374	497	703	927	1287	1663	2297
3	1	3	5	10	15	29	42	72	107	170	246	383	542	810	1145	1662	2311	3305	4537	6353
4	1	3	5	11	16	32	47	84	124	208	299	481	687	1068	1505	2255	3163	4638	6444	9258
5	1	3	5	11	17	33	50	89	135	223	332	551	776	1194	1730	2591	3700	5429	7660	11035
7	1	3	5	11	17	34	52	93	143	239	360	582	861	1338	1963	2908	4288	6354	9069	13182
8	1	3	5	11	17	34	52	94	144	242	365	593	878	1372	2015	3002	4432	6595	9434	13775
9	1	3	5	11	17	34	52	94	145	243	368	598	889	1389	2049	3114	4595	6741	9677	14143
11	1	3	5	11	17	34	52	94	145	244	370	602	897	1405	2077	3165	4612	6887	9916	14532
13	1	3	5	11	17	34	52	94	145	244	370	603	899	1409	2085	3181	4640	6938	10002	14678
16	1	3	5	11	17	34	52	94	145	244	370	603	899	1410	2087	3186	4649	6957	10035	14740
17	1	3	5	11	17	34	52	94	145	244	370	603	899	1410	2087	3186	4650	6958	10038	14745
19	1	3	5	11	17	34	52	94	145	244	370	603	899	1410	2087	3186	4650	6959	10040	14749

Table 2

n	$F(n)$	n	$F(n)$	n	$F(n)$
1	1	11	370	21	21077
2	3	12	603	22	30479
3	5	13	899	23	43120
4	11	14	1410	24	61574
5	17	15	2087	25	86308
6	34	16	3186	26	121785
7	52	17	4650	27	169336
8	94	18	6959	28	236475
9	145	19	10040	29	326201
10	244	20	14750	30	451402

If $v = q^n$, for some factorization patterns of n one can construct an association scheme with a particular set of n_i's in several different ways. In particular, consider the factorization pattern $n = b_1^{a_1} + \cdots + b_r^{a_r}$ where a positive integer $m > 1$ divides each b_j, so that $b_j = md_j$ for $j = 1,\ldots,r$. Let $V = B_1^{a_1} \cdots B_r^{a_r}$ where B_j is monic irreducible of degree b_j over F_q. Then we obtain an association scheme where if $T_i \ne V$ is a monic divisor of V, then $n_i = \Phi_q(V/T_i)$.

A second approach to constructing an association scheme with the same set of n_i's, is to consider polynomials over the extension field F_{q^m}. Here we use the well-known result that an irreducible polynomial of degree $m\ell$ over F_q factors over F_{q^m} into m irreducible polynomials each of degree ℓ, see [5, Theorem 3.46]. Hence for $j = 1,\ldots,r$ the irreducible B_j of degree

$b_j = md_j$ over F_q factors over F_{q^m} into m irreducible factors each of degree d_j. For $j = 1,...,r$ choose D_j to be a monic irreducible factor of B_j of degree d_j over F_{q^m}. Let $V_1 = D_1^{a_1} \cdots D_r^{a_r}$ over F_{q^m}, and if $T_i' \neq V_1$ is a monic divisor of V_1 then $n_i' = \Phi_{q^m}(V_1/T_i')$, so that upon reordering, $n_i' = n_i$ for all i. Hence both methods induce association schemes with the same set of n_i's. While the association schemes constructed by these methods may be isomorphic, there may, however, be computational advantages in using one method over the other.

The most important advantage of working in extension fields is, however, that for some cases where we can not construct an association scheme with q^n treatments over F_q because of an insufficient number of irreducible polynomials over F_q of particular degrees, it may be possible, by using the extension field method, to indeed construct such schemes with q^n treatments. We now consider several examples of such situations.

Let $v = 2^4$ and consider the factorization pattern $4 = 2 + 2$. By (3.4) there is only one irreducible quadratic over F_2, that being $x^2 + x + 1$. Hence over F_2 it is not possible to construct a polynomial $V(x)$ of degree 4 with factorization pattern $2 + 2$. Over the field F_{2^2} let $V(x) = x(x+1)$, so that $V(x)$ induces an association scheme with $s = 3$ association classes and moreover, $n_1 = 9$ and $n_2 = n_3 = 3$. Other examples that do not exist over F_2 but that do exist over F_{2^2} are easily constructed. In the case $v = 2^6$, consider the factorization pattern $6 = 2 + 2 + 2$ and let $V_1(x) = x(x+1)(x+\alpha)$ over F_{2^2} where $\alpha \neq 0$, $1 \in F_{2^2}$ and for the factorization pattern $6 = 2^2 + 2$ let $V_2(x) = x^2(x+1)$ over F_{2^2}, so that $V_1(x)$ and $V_2(x)$ both induce association schemes. Of course similar examples could also be given for cases where $q > 2$.

4. Construction of Cyclic PBIB Designs.

For each association scheme constructed by the method of section 2, we now explain how to construct a series of cyclic PBIB designs. We begin with

Definition 4.1. A PBIB design, based on an association scheme with s association classes, is a collection of v treatments arranged in b blocks so that:

(a) Each block contains k distinct treatments;

(b) Each treatment is contained in r blocks;

(c) If two treatments α and β are j-th associates for some $j = 1,...,s$, then they occur together in λ_j blocks, the number λ_j being independent of the particular pair of j-th associates α and β.

The numbers v,r,b,k and λ_j $(1 \leq j \leq s)$ are known as design parameters.

In the first of two methods, blocks are cyclically developed from a single initial block B taken to be one of the sets A_i where

$$A_i = \{\alpha(x) \in M_V | (\alpha(x), V(x)) = T_i(x)\} \quad (i = 1,...,s) \tag{4.1}$$

Specifically, we build a collection of $b = q^n$ blocks by constructing the blocks $\beta(x) + A_i = \{\beta(x) + a_i(x) | a_i(x) \in A_i\}$, where $\beta(x)$ runs through the q^n polynomials of the complete residue system M_V.

If $V(x)$ is irreducible over F_q, then the association scheme described in section 2 has exactly one association class and the design developed from A_1 is then a balanced incomplete block (BIB) design. If $V(x)$ is reducible over F_q, then the resulting design will be a PBIB design.

Theorem 4.1. *Let $V(x)$ be a monic polynomial of degree $n \geq 1$ over F_q. Let $A_i = \{\alpha(x) \in M_V | (\alpha(x), V(x)) = T_i(x)\}$ for $i = 1,...,s$. Consider the association scheme defined in section 2 with scheme parameters $v = q^n$, $n_i = \Phi_q(V/T_i)$ for $i = 1,...,s$ and p_{ij}^k with $1 \leq i,j,k \leq s$. Let $B = A_i$ for some particular i. The design whose blocks are $\beta(x) + B$, $\beta(x) \in M_V$, obtained by cyclic development of B is a PBIB design with parameters $b = v = q^n$, $r = k = n_i$ and $\lambda_j = p_{ii}^j$ for $j = 1,...,s$.*

Remark. While the λ_j are functions of i as well as j, for simplicity of notation we omit writing the i since we are working with a fixed A_i.

Proof. By construction $b = v = q^n$ and $r = k = n_i$. This leaves us with the problem of showing that $\lambda_j = p_{ii}^j$ for $j = 1,...,s$.

By definition, λ_j denotes the number of times two j-th associates appear together in blocks of the design developed from A_i. Let $\alpha(x)$ and $\beta(x)$ be j-th associates. Now because of the cyclic development of the design starting with A_i, λ_j is also the number of times the difference $\alpha(x) - \beta(x)$ appears among the $n_i(n_i-1)$ differences arising from the set A_i.

By definition, p_{ii}^j is the number of i-th associates of $\alpha(x)$ which are also i-th associates of $\beta(x)$. Suppose $p_{ii}^j = c$ and suppose the c common i-th associates are $\tau_h(x)$ for $h = 1,...,c$. Then $\alpha(x) - \tau_h(x) \in A_i$ and $\beta(x) - \tau_h(x) \in A_i$. Hence $\alpha(x) - \beta(x)$ is then a difference arising from A_i and it arises for each $h = 1,...,c$. But $\alpha(x) - \beta(x) \in A_j$ and hence for each of the $n_i(n_i-1)$ differences arising from A_i, every element of A_j occurs p_{ii}^j times. Therefore $\lambda_j = p_{ii}^j$ which completes the proof.

Remark. Since we cannot cyclically develop a design from A_i if $|A_i| = n_i = 1$, we must eliminate such A_i as potential initial blocks. If $q = 2$, let θ denote the number of distinct linear factors in $V(x)$. Then $s - \theta - \delta_{2g}$ is the number of sets A_i with $|A_i| > 1$, where δ_{2g} is the Kronecker delta symbol. If $q > 2$, then there are no A_i with $|A_i| = 1$.

This procedure for creating PBIB designs is not restricted to developing on only one of the sets A_i. The following corollaries, whose proofs we omit, provide the basis for creating many other designs.

Corollary 4.2. *The design consisting of the blocks $\beta(x) + B$, $\beta(x) \in M_V$, obtained by cyclic development of a set $B = \{0\} \cup A_i$ is a PBIB design with parameters $v = b = q^n$, $r = k = n_i + 1$ and*

$$(\lambda_1,\lambda_2,\ldots,\lambda_i,\ldots,\lambda_s) = (p_{ii}^1, p_{ii}^2, \ldots, p_{ii}^i+2, \ldots, p_{ii}^s).$$

Corollary 4.3. *The design consisting of the blocks $\beta(x) + B$, $\beta(x) \in M_V$, obtained by cyclic development of a set $B = A_i \cup A_j$, $i \neq j$, is a PBIB design with parameters $v = b = q^n$, $r = k = n_i + n_j$ and $\lambda_h = p_{ii}^h + p_{jj}^h + 2p_{ij}^h$ for $h = 1,\ldots,s$.*

The procedures of Corollaries 4.2 and 4.3 can be combined in order to state

Corollary 4.4. *The design consisting of the blocks $\beta(x) + B$, $\beta(x) \in M_V$, obtained by cyclic development of a set $B = \{0\} \cup A_i \cup A_j$ for $i \neq j$ is a PBIB design with parameters $v = b = q^n$, $r = k = n_i + n_j + 1$ and*

$$\lambda_h = p_{ii}^h + p_{jj}^h + 2p_{ij}^h \qquad h \neq i,\ h \neq j$$
$$\lambda_i = (p_{ii}^i+2) + p_{jj}^i + 2p_{ij}^i$$
$$\lambda_j = p_{ii}^j + (p_{jj}^j+2) + 2p_{ij}^j.$$

We also note that although one cannot develop a design from a set A_i where $n_i = 1$, such a set A_i can be used in conjunction with $\{0\}$ or with another set A_j to develop a design.

The second method of constructing cyclic PBIB designs is based upon a procedure of Das and Kulshreshtha [4]. Let V be a monic polynomial of degree $n \geq 1$ over F_q with q odd, so that $n_1 = \Phi_q(V)$ is even. Let E be a subset of A_1 of cardinality $n_1/2$ with the property that $A_1 = E \cup (-E)$. If $t = n_1/2$, let vt blocks, each of cardinality k, be constructed by cyclic development of t initial blocks $B_1,\ldots,B_t$. The initial blocks are generated from a basic initial block $B_0 = \{\beta_1(x), \ldots, \beta_k(x)\}$ and a set $E = \{\epsilon_1(x), \ldots, \epsilon_t(x)\}$, where the $\beta_i(x)$ are k distinct elements

from M_V and the $\epsilon_i(x)$ are distinct nonzero elements of M_V. For $j = 1,\ldots,t$ let

$$B_j = \epsilon_j(x)\, B_0 = \{\epsilon_j(x)\beta_1(x), \ldots, \epsilon_j(x)\beta_k(x)\},$$

where all products are calculated modulo $V(x)$. We now prove

Theorem 4.5. *Let V be a monic polynomial of degree $n \geq 1$ over F_q with q odd and consider the association scheme with parameters $v = q^n$, n_i for $i = 1,\ldots,s$ and p_{jh}^i with $1 \leq i,j,h \leq s$ constructed in section 2. For $i = 1,\ldots,s$ let r_i denote the number of differences arising from B_0 which belong to the set A_i given in (4.1). The design constructed by cyclically developing the sets $B_1,\ldots,B_t$ is a PBIB design with parameters $v = q^n$, $b = n_1v/2$, k, $r = n_1k/2$, and $\lambda_i = r_in_1/(2n_i)$.*

Proof. There are r_i differences $\beta(x) - \alpha(x) \in A_i$ that arise also in B_0. Each of the t initial blocks has the same number of differences contained in B_0. In developing blocks, each block will have the same number of differences in A_i since the same element is added to each element of B_0, i.e., if $\beta(x) - \alpha(x) \in A_i$ then $(\beta(x)+\delta(x)) - (\alpha(x)+\delta(x)) \in A_i$ for all $\delta(x)$. Therefore there are vr_it differences among all blocks which are in A_i.

On the other hand there are v choices for $\alpha(x)$, n_i choices for $\beta(x)$, and since in the i-th class each ordered pair occurs λ_i times, we have $vn_i\lambda_i$ differences among all blocks which are in A_i. Thus $vr_it = vn_i\lambda_i$ and $\lambda_i = r_it/n_i = r_in_1/(2n_i)$.

Acknowledgment. The authors would like to thank the referee for his helpful comments. We would also like to express our sincere appreciation to Professor Ashok K. Agarwal for his very helpful comments regarding the generating function given in Corollary 3.4, Professor Nilotpal Ghosh for his computations which generated the values in Tables 1 and 2, and Professor Kenneth W. Johnson for several helpful comments.

References.

[1] H.C. Agrawal and C.R. Nair, *Reduced residue classes cyclic PBIB designs*, Austral. J. Statist. 26 (1984), 298-309.

[2] J.T.B. Beard, Jr. and K.I. West, *Prime and primitive polynomials of degree n over GF(p^d)*, unpublished table, edited from exhaustive factorization tables obtained by computer.

[3] W.H. Clatworthy, *"Tables of Two Associate Class Partially Balanced Incomplete Block Designs"*, Nat. Bur. Stand., Appl. Math. Ser. 63 (1973).

[4] M.N. Das and A.C. Kulshreshtha, *On derivation of initial blocks of BIB designs with more than one initial block*, Austral. J. Statist. 10 (1968), 75-82.

[5] R. Lidl and H. Niederreiter, *"Finite Fields"*, Encyclopedia of Mathematics and its Applications, Vol. 20, Addison-Wesley, Reading, Mass., 1983.

[6] R.W. Marsh, *Table of irreducible polynomials over GF(2) through degree 19*, Office of Techn. Serv., U.S. Dept. of Commerce, Washington, D.C., 1957.

[7] W.W. Peterson and E.J. Weldon, Jr., *"Error-Correcting Codes"*, second edition, M.I.T. Press, Cambridge, Mass., 1972.

[8] D. Raghavarao, *"Constructions and Combinatorial Problems in Design of Exzperiments"*, John Wiley and Sons, Inc., New York, New York, 1971.

Department of Statistics
The Pennsylvania State University
University Park, PA 16802
U.S.A.

Department of Mathematics
The Pennsylvania State University
University Park, PA 16802
U.S.A.

Austrian Academy of Sciences
Dr. Ignaz-Seipel-Platz 2
A-1010 Vienna
Austria

Ballot Sequences and Restricted Permutations

Dana Richards

University of Virginia
Charlottesville, VA 22903

1. Introduction

The distribution of the length of the longest ascending subsequence of a permutation of $\{1, 2, \cdots, n\}$, $\pi = (\pi_0, \pi_1, \ldots, \pi_{n-1})$, has been much studied (e.g., [1,3]). An ascending subsequence is $\pi_{i_1} < \pi_{i_2} < \cdots < \pi_{i_k}$, where $i_1 < i_2 < \cdots < i_k$, and the length of the subsequence is k. The principal result in this area is that the expected length of the longest subsequence is $2\sqrt{n}$, over all permutations [1]. Another intriguing result concerns the number, $p(n, l)$, of permutations with no ascending subsequence of length greater than l. Let the set of all such permutations be $P(n, l)$. It is known [2] that

$$p(n, 2) = \frac{1}{n+1}\binom{2n}{n}$$

which is a Catalan number. Of course $p(n, 1) = 1$. The appearance of the Catalan number reveals an association with a great number of other well known combinatorial problems in which the Catalan numbers play a role. Often these problems are related by explicit bijections between their domains. Rogers [2] states that a "direct proof would be welcome as it might suggest other ways of calculating" $p(n, l)$ and related quantities. In this note we give a direct proof. In the sequel if we refer to a permutation we assume it is in $P(n, 2)$, unless otherwise specified.

Of all the combinatorial objects counted by the Catalan numbers perhaps the canonical example is the set of ballot sequences $B(n)$ (e.g., [4]). A ballot sequence $B = (B_0, B_1, \cdots, B_{2n-1})$ is a sequence of n 0's and n 1's such that, left to right, the 1's are never outnumbered by the 0's, that is $\sum_{i=0}^{k} B_i \geq \lceil k/2 \rceil$. Many techniques are known for ranking and unranking ballot sequences (e.g., [5]) and, given a bijection between $B(n)$ and $P(n, 2)$, these provide a way to rank and unrank the permutations of $P(n, 2)$. We now exhibit such a bijection.

2. Mapping $B(n)$ into $P(n, 2)$

Consider a permutation π from $P(n, 2)$ and suppose that $\pi_i = 1$. It is clear that $\pi_{i+1} > \pi_{i+2} > \cdots > \pi_{n-1}$. In particular if $\pi_j = 2$ and $j > i$ then $j = n-1$, if $j < i$ then there is no restriction.

ARS COMBINATORIA 25(1988), pp. 83-86