NEAR-RINGS AND BALANCED INCOMPLETE BLOCK DESIGNS

by

Richard Henry Palmer

A Thesis Submitted to the Faculty of the

COMMITTEE ON COMPUTER SCIENCE

In Partial Fulfillment of the Requirements
For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

1 9 7 1

STATEMENT BY AUTHOR

This thesis has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this thesis are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

SIGNED: Richard Allen

APPROVAL BY THESIS DIRECTOR

This thesis has been approved on the date shown below:

J. R. Clay
J. R. CLAY
Associate Professor of Mathematics

17 June 1971
Date

TABLE OF CONTENTS

ABSTRACT

In his paper, Some Algebraic and Geometric Aspects of Planarity, Dr. J. R. Clay described a connection between certain types of near-rings constructed over finite fields of prime order and balanced incomplete block designs. This thesis generalizes Dr. Clay's techniques to all finite fields and describes several computer algorithms related to the generation of these designs.

INTRODUCTION

We begin by describing certain fundamental concepts to be used throughout this thesis.

Special Notation

Because the need occurs so often, we will adopt the convention that the symbol P will always denote a prime number. We will also use the convention $H \lhd G$ to mean that H is a normal subgroup of the group G. To denote a subgroup that is not necessarily normal we will write $H < G$. We also adopt the notation that the expression in parenthesis immediatly following the term being defined in a definition will be used to stand for the term.

Definition I

A field (F) is a triple $(F,+,\cdot)$ where the following conditions hold.

1. $(F,+)$ is an abelian group.
2. $(F^*,\cdot)$ is an abelian group where F^* is the set of non-zero elements of F.
3. The operation $\cdot$ is left and right distributive over the operation $+$.

Definition II

A Near-Ring (N) is a triple, $(N,+,*)$ where the following conditions hold.

1. (N,+) is a group.
2. (N,*) is a semi-group.
3. The operation * is left distributive over the operation +.

We shall make use of the following equivalence relation on the elements of a Near-Ring.

Definition III

Two elements, $\{g_1, g_2\}$ in N are said to be left-equivalent multipliers (written $g_1 \equiv_m g_2$) if $g_1 * x = g_2 * x$ for all x contained in N.

The following specialization of the near-ring concept and its refinement are important to our application.

Definition IV

A Planar Near-Ring (PNR) is a near-ring where the following conditions hold.

1. The equation $g_1 * x = g_2 * x + g_3$ is always solvable for x in N whenever $g_1 \neq_m g_2$.
2. N has at least 3 elements, no two of which are left-equivalent multipliers.

Definition V

Let A be the set of all elements in some PNR which are left-equivalent multipliers to the zero element. If the set A contains only the zero element then the PNR is said to be an Integral Planar Near-Ring (IPNR).

A proof that such structures exist is given by Clay in [2]. The result is stated in this thesis as Theorem IV.

We next define what is meant by a Block and by a Balanced Incomplete Block Design.

Definition VI

Let $\{g_1,g_2\}$ be contained in N where $g_1 \neq 0$. The set

$$B = \{x*g_1 + g_2 \mid x \in N\}$$

is called the Block determined by the pair $\{g_1,g_2\}$.

Definition VII

A Balanced Incomplete Block Design (BIBD) is a set of v objects, sometimes called varieties, and a family of b distinct subsets of these varieties, sometimes called blocks, where

1. each block contains exactly k objects,
2. each variety belongs to exactly r blocks,
3. each pair of distinct varieties belongs to exactly λ blocks.

Example of a BIBD

{0,1,2} {1,3,5} {2,3,6} {0,3,4} {1,4,6} {2,4,5} {0,5,6}

The above are the blocks of a BIBD with parameters:

v=b=7; k=r=3; λ=1

Let (G,+) be a group and let AUT(G) be the automorphism group related to G. Suppose $\Phi < AUT(G)$. It is convenient to define an equivalence relation on the elements of G in terms of Φ.

Definition VIII

Let $\{g_1, g_2\}$ be contained in G. The element g_1 is said to be Φ-equivalent to g_2 (written $g_1 \equiv_\Phi g_2$) if there exists a $\phi \in \Phi$ such that $\phi(g_1) = g_2$. Here equivalence classes induced by Φ are called orbits and an orbit whose cardinality equals the order of Φ is called principal. If each non-identity element of Φ fixes only the zero element of the group G, then Φ is said to be fixed-point free.

The following is theorem 3 in [4] and its proof is given there.

Theorem I

A finite near-ring N is planar if and only if

1. each map, $\phi_a(x) = a * x$ is either an automorphism of N or is the zero map,
2. the multiplication is not trivial; i.e., one of the ϕ_a is distinct from the identity or the zero map,
3. all the orbits of

$$\Phi = \{\phi_a \mid \phi_a(x) = a*x \text{ where } \{a,x\} \subseteq N \text{ and } \phi_a \neq 0\}$$

are either principal or consist of a single element,

4. the group Φ is fixed-point free.

The Φ defined in the theorem above will be called the automorphism group related to the PNR.

The following are denoted as lemma 11 and corollary 12 of [4].

Theorem II

If for some N which is a PNR we have that

$$N * a + b = N * a' + b'$$

then one of the following conditions must be true:

1. $b = b'$ and $a \equiv_{\Phi} a'$;

2. $\{g,g'\} \subseteq N^*a$ implies that $g - g' \in N^*(-a)$.

Theorem III

Suppose N is a PNR with no sub near-field, and suppose the related group of automorphisms has even order. Then

$$N * a + b = N * a' + b'$$

if and only if $b = b'$ and $a \equiv_{\Phi} a'$. Here a near-field is defined to be a near-ring whose non-zero elements form a group with respect to multiplication.

In [4], Ferrero calls a finite PNR fundamental if its related group of automorphisms has even order and if the near-ring has no sub near-fields. If the order of the fundamental near-ring is v and the order of Φ is k - 1 then Ferrero proves that the elements of the near-ring and its blocks form a BIBD with parameters

$$b = \frac{v(v-1)}{k-1}; \qquad r = \frac{k(v-1)}{k-1}; \qquad \lambda = k$$

where k denotes the number of elements in each block. Finally Ferrero shows the concept is not vacuous; such fundamental near-rings exist for each abelian group whose order is relativly prime to six with the resulting BIBD's having the above parameters with k = 3.

Clay extended Ferrero's results by showing BIBD's could be constructed in the same manner from finite PNR's which were not fundamental in the sense described above. The following theorem is in [2]

and is proved there. It defines a class of PNR's which are not fundamental in Ferrero's sense.

Theorem IV

For a finite field, F, of order P^n and for each non-trivial divisor, t, of $P^n - 1$ there is an IPNR

$$(F,+,*_t).$$

Clay gives a constructive proof of the existence of these non-fundamental IPNR's. The construction is described in the following paragraph.

Suppose $t \cdot m = P^n - 1$. Then there exists a subgroup

$$H < F^*$$

where the order of H is t. Let

$$H_1, H_2, \ldots, H_m$$

be the cosets of H. Now, from each H_i choose one element z_i. The z_i are said to represent H_i. Clay now defines the operations of + and $*_t$ in the following way. The operation + is exactly the same as the field operation of +. The operation $*_t$ is defined by the function

$$X_1 *_t X_2 = 0 \text{ if } X_1 = 0$$

$$X_1 *_t X_2 = B \cdot X_2 \text{ where } X_1 \in H_1 \text{ and } X_1 = B \cdot z_i.$$

The following example shows how one goes about this process by exhibiting some non-fundamental IPNR's that can be derived from Z_7, the field of order 7.

Some Non-Fundamental IPNR's Associated With Z_7

Recall that Z_7 is isomorphic to the integers MOD(7) under addition and multiplication.

We seek a subgroup, H, if the multiplicative group of Z_7 where H has odd order. Clearly the elements of H must be {1,2,4} and the elements of the other coset are {3,5,6}.

There are 9 ways to choose representatives from the subgroup and its coset. They are the following:

1. {1,3}	4. {2,3}	7. {4,3}
2. {1,5}	5. {2,5}	8. {4,5}
3. {1,6}	6. {2,6}	9. {4,6}

By definition, all the IPNR's derived in the following have the operation + defined as in the field. The different multiplications are described in Table I.

Table 1. Some IPNR Multiplications on Z_7*

1.	{1,3,1}	2.	{1,5,1}	3.	{1,6,1}
	{2,6,2}		{2,3,2}		{2,5,2}
	{4,5,4}		{4,6,4}		{4,3,4}
4.	{1,5,4}	5.	{1,6,4}	6.	{1,3,4}
	{2,3,1}		{2,5,1}		{2,6,1}
	{4,6,2}		{4,3,2}		{4,5,2}
7.	{1,6,2}	8.	{1,3,2}	9.	{1,5,2}
	{2,5,4}		{2,6,4}		{2,3,4}
	{4,3,1}		{4,5,1}		{4,6,1}

*The table is to be read in the following way. We have sets of triples of the form

$$\begin{array}{ll} k. & \{1,x_1,m_1\} \\ & \{2,x_2,m_2\} \\ & \{4,x_4,m_4\} \end{array}$$

where the following meaning is to be attached to the figure. We are describing the multiplication induced by set k of representatives from the previous page. Here we read that

$$\begin{array}{l} 1 *_t X = x_1 \quad *_t X = m_1 \ . \ X \text{ MOD}(7) \\ 2 *_t X = x_2 \quad *_t X = m_2 \ . \ X \text{ MOD}(7) \\ 4 *_t X = x_4 \quad *_t X = m_4 \ . \ X \text{ MOD}(7) \end{array}$$

Clay then takes a subset of these PNR's; those constructed over the finite fields of prime order and proves (Theorem 3.8 in [2]) the following theorem.

Theorem V

If t is a non-trivial divisor of P - 1, then there exists a BIBD with the following parameters.

$$v = P; \quad b = \frac{v(v-1)}{t}; \quad k = \lambda = t + 1; \quad r = \frac{k(v-1)}{k-1}$$

Clay's method consists of constructing all distinct blocks of the form

$$F *_t g_1 + g_2$$

where 1. F is the field of order P; 2. $*_t$ is an IPNR multiplication defined on F as above; 3. g_1 and g_2 are elements of the field where g_1 is not equal to zero.

It is useful to note that the B's defined in the operation $*_t$ in theorem IV depend only on P, the order of the field, and t, the divisor of P - 1, and not on the choice of representatives. In fact, it is direct to show that the B's are exactly the elements of the subgroup H of F^* whose order is that of the divisor. However, the actual multiplication depends on the choice of representatives. Keeping the above in mind, it is easy to see that the blocks are of the form;

$$\bar{H}_i + g \text{ where } \bar{H}_i = H_i \cup \{0\}$$

and H_i is a coset of H; the order of H is t, the non-trivial divisor of the order of F^*; and g is a member of the field.

A GENERALIZATION OF CLAY'S RESULTS

This section generalizes the results of the previous theorem to finite fields of all orders. The generalization is non-trivial for the method used there does not always yield BIBD's with the same parameters. We prove this in the following lemma.

Lemma I

Let F have order P^n. For each subfield of F there exists a BIBD with parameters

$$v = P^n; \quad b = \frac{v(v-1)}{k(k-1)}; \quad k = P^h; \quad r = \frac{v-1}{k-1}; \quad \lambda = 1$$

where k is the order of the subfield.

Proof:

It is well known that if k is the order of a subfield of a field of order v then h must divide n. This immediately gives us that k - 1 must divide v - 1. Hence there exists a subgroup H of F^* with order k - 1. Denote the cosets of H as

$$H_1, H_2, \ldots, H_r$$

Define the symbol $\bar{H}_i$ to the $H_i \cup \{0\}$ Suppose $g \cdot H = H_i$. Then $g \cdot \bar{H} = \bar{H}_i$ and it is easy to show that the set $\bar{H}_i$ is closed under addition and hence is a subgroup of F.

The blocks are unique. Suppose otherwise; i.e.,

$$\bar{H}_i + g_1 = \bar{H}_j + g_2$$

where $i \neq j$. Then we have that

$$\bar{H}_i = \bar{H}_j + g \qquad g = g_2 - g_1$$

Then we would have g in $\bar{H}_i$ and $(-g)$ in $\bar{H}_j$. But this says that $\bar{H}_1 = \bar{H}_j$, a contradiction.

Furthermore, it is clear that each element of F occurs exactly once in the coset expansion of each $\bar{H}_i$. This gives us r.

If a pair $\{g_1, g_2\}$ occurs, it occurs at most once. For if $\{g_1, g_2\} \subseteq (\bar{H}_i \cap (\bar{H}_j + \bar{g}_3))$ and $i \neq j$ then $g_1 - g_2$ is in $\bar{H}_1 \cap \bar{H}_j = \{0\}$ and hence $g_1 = g_2$. Since g_i is paired with $k - 1$ other elements each time it occurs (and it occurs r times) we get $\lambda = 1$.

We can derive the following interesting corollary from the previous result.

Corollary I

For all P and for all $n \neq 0$ there exists a BIBD with parameters

$$v = b = P^{2n} + P^n + 1; \quad k = r = P^n + 1; \quad \lambda = 1$$

Proof:

If F is a field of order P^{2n} then F has a subfield $\bar{H}$ of order P^n. Define H to be the non-zero elements of $\bar{H}$. Now H is both the multiplicative group of $\bar{H}$ and a subgroup of F^*. Since the order of F^* is $P^{2n} - 1$ and the order of H is $P^n - 1$ we get that H has $P^n + 1$ cosets considered as a subgroup of F^*. Using the same techniques as in the preceeding lemma we note that if H_i is a coset of H; then $H_i \cup \{0\} = \bar{H}_i$ is

a subgroup of F. Therefore we can construct a BIBD with parameters

$$v = P^{2n};\quad b = P^n(P^n + 1);\quad k = P^n;\quad r = P^n + 1;\quad \lambda = 1$$

by the previous lemma.

This design, and in fact all designs constructed as in Lemma I have an interesting property which we shall formally define at this point. A BIBD is said to be group divisible if the family of blocks can be partitioned into pairwise disjoint sub-families of blocks where the union of blocks contained in any such sub-family of blocks contains all the varieties of the design Clearly the blocks described above are group divisible and a subset having this property is of the form;

$$\bar{H}_i, \bar{H}_{i1}, \ldots, \bar{H}_{iP^n}$$

where $\bar{H}_i < F$ and $\bar{H}_{ik}$ is a coset of $\bar{H}_i$. Let us denote these subsets by S_i, $i = 1,2,\ldots P^n + 1$. Then, if we pick $P^n + 1$ new varieties, not already chosen, v_i, $i = 1,2,\ldots,P^n + 1$, and append v_i to each block of S_i then each v_i appears in the design P^n times and appears with each element of the original design once. If we append the block;

$$\{v_1, v_2, \ldots, v_{P^n + 1}\}$$

to the design then each v_i appears $P^n + 1$ times and is paired with each element of the augmented design once. Since this also holds for each element other then the v_i's in the augmented design, we get our desired result.

We can use the observation that our blocks

$$F *_t g_1 + g_2$$

can be written in the form $\bar{H}_i + g_2$ where

$$\bar{H}_i = (\bar{H} \cup \{0\}) \cdot g_i$$

to restate a previous theorem.

Restatement of Theorem II

Suppose blocks $\bar{H}_i + g_2 = \bar{H}_j + g_1$ in an IPNR constructed as in Theorem IV. Then one of the following conditions must be true.

1. $g_2 = g_1$ and $i = j$.
2. If $\{g_2, g_1\} \subseteq \bar{H}_i$ then $g_2 - g_1 \in \bar{H} \cdot (-i)$ where $\bar{H} \cdot i = \bar{H}_i$.

We now prove:

Theorem VI

Let F be a field where the order of F is $P^n = q$. Let d be a non-trivial divisor of $q - 1$ where $d + 1$ is not of the form P^h where h divides n. Then there exists a BIBD with parameters

$$v = q; \quad b = \frac{v(v-1)}{d} \quad k = \lambda = d + 1; \quad r = \frac{k(v-1)}{k-1}.$$

Proof:

We begin by noting that these are the parameters of Theorem V where P is replaced by P^n.

If d divides $q - 1$ then there exists a subgroup H of F^* where the order of H is d. Furthermore, we know that H is not of the form P^h. Define, as before, $\bar{H}$ to be $H \cup \{0\}$ and $\bar{H}_i$ to be $\bar{H}_i \cup \{0\}$ where H_i is a coset of H. Then, using as before the notation

$$\bar{H} + g$$

for blocks, if we have

$$\bar{H}_i + g_1 = \bar{H}_j + g_2$$

and we let $g_3 = g_2 - g_1$ then it follows that

$$\bar{H}_i = \bar{H}_j + g_3 \qquad (1)$$

by subtraction.

Now if we pick some $g \neq 1$ from H then the equation

$$\sum_{x \in H} x = g \sum_{x \in H} x \qquad (2)$$

surely holds since H is closed under multiplication. We subtract the right-hand side of (2) from the left

$$\sum_{x \in H} x\,(1 - g) = 0$$

and it follows that

$$\sum_{x \in H} x = 0 \qquad (3)$$

Clearly (3) holds if we multiply through by any non-zero element of F and we can get

$$\sum_{x \in H_i} x = 0$$

We apply this result to equation (1) and get

$$0 = 0 + (d + 1)g_3.$$

This says that either $(d + 1)$ or g_3 must be equal to zero. Since F is of characteristic P, if $(d + 1)$ were zero then $(d + 1)$ is not of this form. This gives us that g_3 is zero.

But $g_3 = 0$ gives $\bar{H}_i = \bar{H}_j$ from equation (1). Therefore we get $b = v(v - 1)/d$.

It is clear that the family

$$\{\bar{H}_i + x\}$$

where x ranges over the elements of F yields every element d + 1 times. Hence we get

$$r = (d + 1)(v - 1)/d.$$

Since v and k are obvious from the construction, it remains to show that $\lambda = d + 1$. This can be obtained by using a result due to Ferrero (see the discussion following Theorem III). A previous paragraph gives us our re-statement of Theorem II mentioned before this theorem. These hypotheses yield us the results of Corollary 12 in [4] which states that if condition 1 of Theorem II holds in an IPNR then if $x,y \subseteq F$ where $x \neq y$ then the pair $\{x,y\}$ belongs to exactly $\lambda = d + 1$ different blocks. This gives us the theorem.

COMPUTER GENERATION OF BIBD'S

Computer generation of BIBD's involves problems dealing with most of the classical trade-offs of computer programming. Since the type of designs we have described in the first section are intimately connected with finite fields we are, in a sense, dealing with a data base of the abstract elements of a field. Since fields have no direct hardware analog on a digital computer, the programmer must find a method of mapping this concept to representations that a computer can manipulate. Furthermore, there are procedural trade-offs that influence the choice of method. These considerations make the concept of a general algorithm for generating these designs a nebulous one at best. Hence the discussion which follows will be predicated upon other considerations.

Two subproblems are common to constructing the BIBD's which have been described in this paper. The first is finding a subgroup of a given order in the multiplicative group of a field. The second is finding a presentation of a field which is applicable for computer processing.

Clearly the first problem depends upon the second. The second problem can be said to depend in an ultimate sense on the hardware configuration of the machine to be used. This problem has been

considered in a hardware sense by Berlekamp [1] and this thesis will not attempt to review these results. Rather we will discuss the somewhat easier problem of developing a data structure of a field within the confines of the ALGOL programming language. In the following, the computer algorithms to be presented will be written in the ALGOL reference language.

We first examine the problem of finite field representation. The method of field representation divides into two special cases depending upon the order of the field. If we are dealing with a prime field, clearly the simplest representation of this field we can choose is the integers MOD(P) where MOD is defined by the algorithm:

```
integer procedure MOD(a,b); value a,b; integer a,b;
begin MOD:=a-(a-b)*b end MOD;
```

We can calculate in a field of order P with the following procedure.

```
integer procedure PRIMEPM(a,b,op,P); value a,b,op,P;
integer a,b,P; boolean op;
comment compute a+b if op is true -- compute a·b otherwise;
begin PRIMEPM:=if op then MOD(a+b,P) else MOD(a*b,P) end PRIMEPM;
```

Let us complete the case of prime fields by discussing the question of computing subgroups of F* of a given order. Since F* is cyclic we are guaranteed from elementary considerations of the theory of cyclic groups that an element of F* exists whose successive powers generate F*. For our purposes, we can define this element to be an

integer γ such that $\gamma^k \not\equiv 1 (P)$ for all integers k where k is not a multiple of P - 1. The following procedure returns a subgroup of F* of a field or order P in a vector v where the order of the subgroup is h.

```
procedure PRIMESUBGROUP(P,h,v); value P,h;
integer P,h; integer array v;
begin integer i;
integer procedure ROOT(P); value P;
comment finds a generator of F :
begin integer i,j,test;
 for i:=2 step 1 until P do
  begin
   test:=i;
   for j:=P-2 step -1 until 2 do
   begin
    test:=MOD(test*i,P);
    if test=1 then go to outerloop
   end innerloop;
   ROOT:=i; go to exit;
  outerloop:
  end outerloop;
exit:
end ROOT;
 v[1]:=1; if h=1 then go to exit; v[2]:=MOD(ROOT(P) ↑((P-1)/h),P);
  if h=2 then go to exit;
 for i:=3 step 1 until h do
  v[i]:=MOD(v[2]*v[i-1],P);
exit: end PRIMESUBGROUP;
```

Fields of Order P^n

We digress to discuss fields of order $P^n = q$ where n is greater than one. The discussion is informal since proofs of the assertions made herein can be found in most texts on modern algebra. We intend here only to give a general algebraic justification for our choice of representatives for elements of fields of these orders.

Let Z_p be a prime field or order P and let $Z_p[X]$ be the polynomial domain associated with Z_p. It can be proved that for any finite n there exists at least one polynomial Π of order n such that this polynomial is irreducible over Z_p. If we assume that this polynomial has a root θ in some larger field GF we could describe a homomorphic mapping from $Z_p[X]$ onto GF in the following way.

$$\Sigma\zeta_l X^l \quad \rightarrow \quad \Sigma\zeta_l \theta^l$$

The fact that such a homomorphism exists, implies that GF is isomorphic to a residue class ring of $Z_p[X]$. It can be shown that this residue class ring can be represented by the set of all polynomials of degree less than n, the degree of Π. Here addition of polynomials is done by adding the coefficients MOD(P) and multiplication of polynomials is done by considering their products MOD(Π). Since there are exactly q of these polynomial representatives, the residue class ring represents a field of order q.

Another way of looking at it is as follows. If GF is the field of least order which contains θ and Z_p, then it must also contain all powers of θ. By the definition of our homomorphic mapping given above we have that there are only n distinct powers of our root. Also, since GF is a field, it must contain all distinct sums involving powers of our root and elements of Z_p. This gives us our q elements.

Data Representation of Fields of Order P^n

We choose to have two distinct representatives of our field. One, our internal representation, is a vector containing the coefficients of a polynomial in the residue class ring of $Z_p[X]$ defined before.

Note that we assume that Π, our irreducible polynomial of degree n, is given. We do not include here algorithms for generating such polynomials; several are described by Knuth in [5] and [6]. Most such algorithms attempt to derive special side conditions dependent upon the characteristic of the field which limit the combinatorial range of the coefficients of at least one irreducible polynomial. The algorithms then continue with some heuristic search. Another method is to use a variation of Berlekamp's techniques for polynomial factorization in finite fields to get a quick factorization of $X^q - X$ for a factor of the desired order.

We need a cheaper method than that of polynomial vectors for storing the intermediate results of calculations. For this, we choose a map taking our polynomials onto a subset of the integers. Suppose $\zeta(X)$ is a polynomial in our residue class ring. Since the degree of this polynomial is less than n we can map the polynomial onto the integers MOD(P^n) with the following map F;

$$\zeta(X) \quad \rightarrow \quad \zeta(P).$$

Clearly the map is a ring isomorphism. Procedures to translate from internal to external representation and vice-versa are the following.

```
integer procedure INTTOEXT (ζ,P,n,k); value P,n,k;
 integer P,n,k; integer array ζ;
comment computes the function "F" described above
begin integer i;
 INTTOEXT:=0;
 for i:=k step -1 until 1 do
  INTTOEXT:=(INTTOEXT+ζ [i])*P;
 INTTOEXT:=INTTOEXT+ζ [0]
end INTTOEXT;


integer procedure EXTTOINT (ζ,ext,P,n); value ext,P,n;
 integer ext,P,n; integer array ζ;
comment computes the function EXTTOINT:=degree (ζ) and has
        the side effect that ζ contains the internal
        representation of ext upon exit;
begin integer i,j,save;
 save:=ext; i:=-1;
 loop: i:=i+1; j:=save÷P; ζ[i]:=save-j*P; save:=j;
  if save≠0 then go to loop;
 EXTTOINT:=i
end EXTTOINT;
```

We need a method of constructing subgroups of F* of some order h. We assume a primative polynomial is given. Such polynomials are listed by Knuth in [6]. But first, we must be able to compute modulo (Π) and P. The following procedure accomplishes this.

```
procedure MODIP (ζ,max,Π,P,n); value max,P,n;
comment "ζ" and "Π" are polynomials over Z_P ORDER (ζ)<"max" and
        ORDER (Π)="n". MODIP computes the function MODIP:=ORDER
        (ζMOD (Π,P)) and has the side effect that ζ is replaced
        by ζ MOD (Π,P) in locations 0 - (n-1) of the array ζ;
begin integer i,m,j,k;
 procedure MONIC;
 comment MONIC has the side effect that the coefficients of "Π"
         are replaced by the coefficients of an equivalent
         monic polynomial;
 begin integer reciprocal, i;
  i:=Π [n]; if i=1 then go to out;
  reciprocal:=1;
  loop: reciprocal:=reciprocal+1;
```

```
      if MOD (reciprocal*i,P)≠1 then go to loop;
     for i:=n step -1 until 0 do Π [i] :=MOD(Π[i]*reciprocal,P);
    out:
    end MONIC;
   comment  compute ORDER(u);
    m:=max+1; loop:m=m-1; if  ζ[m]=0 then go to loop;
   comment  see if you are done at this point;
    if m<n then go to exit; MONIC;
   comment  ORDER(u) is greater than or equal to ORDER(index).
            Set ζ to ζ MOD(Π,P);
    for k:=m-n step -1 until 0 do
     for j:=n+k-1 step -1 until k do
      ζ[j]:=ABS (ζ[j]-MOD (ζ[n+k]* Π[j-k],P));
    comment  now compute the order of the residue;
     m:=n;  go to loop;
    exit:  MODIP:=m
   end MODIP:
```

This allows us to compute a + b and a · b in the field. We do this with the following.

```
   integer procedure FIELDCOMP (a,b,P,n,Π,opsw);
    value a,b,P,n,opsw;
     integer a,b,P,n;  boolean opsw;  integer array Π;
   comment  computes the function:
            FIELDCOMP:="a" op "b"
            where a and b are external representations of elements of
            a field of order P^n.  "Π" is an indexing polynomial for
            this field.  Op is to be considered "+" or "*" depending
            upon "opsw";
   begin integer i,j,k,L;
    integer array aa,bb[0:n-1], product [0:2*n-2];
    k:=EXTTOINT(aa,a,P,n); L:=EXTTOINT(bb,b,P,n);
    if opsw then
     begin if k>L then
      begin for i:=L step -1 until 0 do aa[i]:=MOD(aa[i]+bb[i],P);
       FIELDCOMP:=INITTOEXT(aa,P,n,k) end;
      else
      begin for i:=k step -1 until 0 do bb[i]:=MOD(bb[i]+aa[i],P);
       FIELDCOMP:=INITTOEXT(bb,P,n,L)
      end;
      end;
```

```
    else
    begin
     for i:=k+L step -1 until 0 do product [i]:=0;
     for i:=k step -1 until 0 do
      for j:=L step -1 until 0 do
       product [i+j]:=MOD(product[i+j]+MOD(aa[i]*bb[j],P),P);
     FIELDCOMP:=INTTOEXT(product,P,n,MODIP(product,2*n-2,Π,P,n))
    end;
end  FIELDCOMP;
```

We can now write procedures for constructing arbitrary subgroups of F*.

```
procedure SUBGROUPPN(h,P,n,Π,sub,prim);  value h,P,n;
 integer h,P,n;  integer array Π,sub,prim;
comment  A call to the procedure SUBGROUPPN has the effect of
         setting the elements of the array "sub" to external
         representations of the elements of a subgroup of
         order "h" of the multiplicative group of a field of
         order P^n.  "Π" is as before.  The array prim is a
         vector representing a generator polynomial of F*;
begin integer i,ndx;
 integer array x[0:n];
sub [1]:=1;  if h=1 then go to exit;
 for i=n  Step -1 until 0 do  x[i];=prim[i];
sub [2]:=INTTOEXT (x,P,n,MODIP(x,ndx,ΠP,n));
 if h=2 then go to exit;
for i:=3 step 1 until h do
sub [i]:=FIELDCOMP(sub[i-1],P,n,Π,false);
exit:
end  SUBGROUPPN;
```

APPENDIX I.

A COMPUTER GENERATED BIBD

The following is a BIBD with parameters v=64; b=192; k=22; r=66; λ=22. It was computed by a computer program using routines similar to those described in this thesis.

0	1	4	7	10	13	16	19	22	25	28	31	34	37	40	43	46	49	52	55	58	61
1	4	35	6	28	11	50	55	43	21	10	48	18	46	60	22	37	41	62	19	53	32
2	59	55	8	25	51	27	35	26	10	21	36	31	24	54	15	9	32	30	4	39	41
3	56	61	46	47	15	44	49	29	38	17	53	63	6	59	51	7	19	14	41	18	4
4	35	3	38	9	31	14	59	53	46	24	13	51	21	49	63	55	40	44	2	22	3
5	44	62	58	11	23	54	3	38	29	13	24	37	34	27	57	18	12	35	33	7	42
6	7	57	1	49	5	18	47	52	32	41	20	56	3	9	42	54	10	22	17	44	21
7	6	38	7	41	12	34	17	62	61	49	27	16	54	24	52	3	28	43	47	5	25
8	45	47	2	61	14	31	57	33	41	32	16	27	45	37	30	60	21	15	39	36	11
9	24	10	60	4	52	53	21	50	55	35	44	23	59	6	12	2	57	13	25	20	47
10	24	9	41	1	44	10	37	29	2	1	52	30	19	57	27	55	6	31	49	50	8
11	13	44	50	5	1	17	34	60	36	44	35	19	30	43	40	33	63	26	14	41	39
12	58	27	15	63	7	55	56	24	53	58	38	47	26	62	9	15	5	60	16	23	23
13	11	31	12	44	1	47	18	40	23	5	4	55	33	22	60	30	58	9	34	48	53
14	42	16	51	53	6	4	20	37	63	39	47	38	22	33	46	43	36	3	27	31	44
15	20	53	30	10	8	15	58	59	27	56	61	41	50	29	2	12	14	8	64	14	31
16	50	14	34	15	47	1	50	21	43	26	8	7	58	36	25	63	33	61	12	37	62
17	47	45	10	54	55	11	7	23	40	3	42	50	41	25	38	49	46	39	0	32	24
18	34	24	56	33	10	6	13	61	62	30	59	1	44	53	32	5	15	21	11	3	22
19	55	59	17	37	18	50	0	53	24	46	29	11	10	61	39	28	3	36	1	15	40
20	27	58	44	22	57	50	14	10	26	43	6	45	53	44	28	39	52	49	42	9	33
21	25	37	32	59	36	22	9	16	1	2	33	62	4	47	56	35	9	18	24	14	8
22	43	56	62	27	40	21	53	0	56	27	49	32	14	13	1	42	31	6	34	4	18
23	35	30	53	51	25	60	62	17	13	29	46	9	48	56	47	31	42	55	52	45	12
24	9	28	40	35	62	39	25	12	19	4	5	36	2	7	50	59	38	11	21	27	17
25	21	46	61	2	23	43	24	56	0	59	30	52	35	17	16	4	45	34	9	42	7
26	15	39	33	56	54	28	63	2	20	16	32	49	12	51	59	50	34	45	54	55	48
27	26	12	31	43	38	2	42	28	15	22	7	8	39	5	10	53	62	41	14	24	30
28	10	20	49	1	5	26	46	27	54	0	62	33	55	38	20	19	7	48	37	12	45
29	51	18	42	36	59	57	31	3	5	23	19	35	52	15	56	62	53	37	44	61	58
30	33	23	15	34	46	41	8	45	31	18	25	10	11	42	8	13	56	2	44	17	27
31	48	13	27	52	4	9	29	49	30	62	0	2	36	58	41	23	22	10	51	40	15
32	61	54	21	45	39	62	60	34	6	8	26	22	38	55	18	57	2	56	40	51	1
33	37	36	26	14	47	49	44	8	48	34	21	28	13	14	45	11	16	59	5	47	20
34	18	51	16	30	55	7	11	32	52	33	2	0	5	39	61	44	26	25	13	54	43
35	4	1	57	24	48	42	2	63	37	9	11	29	25	41	58	31	60	5	53	43	54
36	23	33	39	29	21	4	52	47	11	51	37	24	31	16	17	46	14	19	62	9	55
37	46	21	54	19	33	58	11	14	35	55	36	5	0	8	42	1	47	29	28	16	57
38	57	7	4	61	27	51	45	5	3	40	12	14	32	28	44	61	24	63	9	62	46
39	53	26	36	42	32	24	43	55	50	14	54	40	27	34	19	20	51	17	22	2	11
40	60	49	24	57	22	36	61	13	17	38	58	39	8	0	11	45	4	50	32	21	10
41	49	60	10	7	63	31	54	48	8	6	43	15	17	35	31	47	1	27	3	11	2
42	14	56	29	39	45	35	27	46	58	53	17	57	43	30	37	22	23	54	20	25	5
43	22	63	52	27	64	25	39	41	16	20	41	61	42	11	0	14	48	7	53	35	34
44	5	52	63	13	10	3	33	57	51	11	9	46	18	20	38	24	50	4	30	6	14
45	8	17	59	32	42	44	38	30	49	61	56	20	60	46	33	40	25	26	57	23	28
46	37	25	3	55	31	63	28	42	4	10	23	44	1	45	14	0	17	51	10	56	38
47	17	8	55	3	16	13	6	36	61	54	14	12	40	21	23	41	37	53	7	33	9
48	31	11	20	62	35	45	51	41	33	52	1	59	23	63	49	36	43	28	29	60	26
49	41	40	28	6	58	33	3	31	45	7	22	26	47	4	48	17	0	29	54	13	59
50	12	29	11	58	6	19	16	9	39	63	57	17	15	52	24	26	44	40	56	10	36
51	29	34	14	23	2	30	48	54	44	36	55	4	62	26	3	52	39	46	31	32	53
52	62	44	43	31	9	61	36	6	34	48	10	25	29	50	7	51	20	0	23	57	15
53	39	15	23	14	61	9	22	19	12	42	3	60	20	18	55	27	29	47	43	59	13
54	3	32	37	17	26	5	41	51	57	47	39	58	7	2	24	6	55	42	49	34	35
55	19	2	47	46	34	12	1	39	9	37	51	13	26	32	53	10	54	23	0	26	60
56	10	42	18	20	17	1	12	25	22	15	45	0	63	23	21	58	30	32	51	46	62
57	38	5	35	40	25	24	0	44	54	60	50	42	61	10	5	32	0	56	45	52	37
58	63	22	8	53	49	37	15	4	42	12	40	54	16	31	35	56	13	57	25	0	29
59	2	14	45	21	24	27	4	15	28	25	18	48	9	3	26	24	61	33	35	53	49
60	40	41	9	38	43	23	32	11	47	57	63	53	45	1	13	8	35	12	61	48	55
61	32	3	25	8	53	52	40	18	7	45	15	43	57	19	34	38	59	16	60	39	0
62	52	5	22	48	24	32	23	7	14	31	28	21	51	12	6	29	27	1	36	48	56
63	56	43	44	12	41	46	26	35	14	50	60	3	55	48	4	16	11	38	15	1	51
0	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44	47	50	53	56	59	62
1	59	44	45	13	42	47	27	36	15	51	61	4	57	49	5	17	12	39	16	2	52
2	0	36	7	29	12	57	56	44	22	11	49	19	47	61	23	38	42	63	20	1	33
3	60	56	9	26	52	24	36	27	11	22	35	32	25	55	16	10	33	31	5	40	42
4	55	62	47	48	10	45	51	30	39	18	54	1	7	60	52	8	20	15	42	19	5
5	36	0	39	10	32	15	60	59	47	25	14	52	22	50	1	26	41	45	3	23	4
6	45	63	59	12	29	55	31	39	30	14	25	38	35	28	58	19	13	36	34	8	43
7	8	58	2	50	51	19	46	53	33	42	21	57	4	10	63	55	11	23	18	45	22
8	7	39	6	42	13	35	18	63	62	50	28	17	55	25	53	4	24	44	48	6	26
9	46	48	3	62	15	32	58	34	42	33	17	28	41	38	31,	61	22	16	39	37	11
10	25	11	61	5	53	54	22	51	56	36	45	24	60	7	13	3	58	14	26	21	44
11	29	10	42	0	45	16	34	21	3	2	53	31	20	58	28	56	7	32	47	51	9
12	14	49	51	6	2	18	35	61	37	45	36	20	31	44	41	34	1	25	19	42	46
13	51	26	14	1	8	56	57	25	54	59	39	48	27	63	10	16	6	61	17	29	24
14	12	32	13	45	0	48	19	41	24	6	5	56	34	23	61	31	59	10	35	50	54
15	43	17	52	54	9	5	21	38	1	40	48	39	23	34	47	44	37	4	28	22	45
16	27	54	31	17	4	11	59	60	23	57	62	42	51	30	3	13	19	9	1	20	32
17	57	15	35	16	48	0	51	22	44	27	9	8	59	37	26	1	34	62	13	38	53
18	48	46	20	55	37	12	8	24	41	4	43	51	42	26	37	50	47	40	7	21	25
19	35	30	57	34	2,	7	14	62	63	31	60	2	46	54	33	6	16	22	12	4	23
20	50	60	18	38	19	61	0	54	25	47	30	12	11	62	40	29	4	37	2	15	41
21	28	51	49	23	56	60	15	11	27	44	7	46	54	45	29	40	53	50	43	10	34
22	26	38	33	50	37	23	10	17	2	3	34	63	5	48	57	36	9	19	25	15	7
23	44	59	63	21	41	22	54	0	57	28	50	33	15	14	2	43	32	7	46	5	19
24	37	31	54	52	20	61	63	18	14	30	47	10	49	57	48	32	43	56	53	46	13
25	10	24	41	30	63	47	20	13	21	5	6	37	3	8	51	60	39	12	22	28	18
26	22	47	62	3	24	44	25	57	0	60	31	53	36	18	17	5	46	35	10	43	8,
27	16	40	34	57	55	29	1	3	21	17	33	50	13	52	60	51	35	46	59	56	49
28	21	13	32	44	39	3	43	29	16	23	8	9	40	6	11	54	53	42	15	25	31
29	11	25	50	2	0	27	47	28	60	0	63	34	56	39	21	20	8	49	34	13	46
30	52	19	43	37	00	58	32	4	6	24	20	30	53	16	55	63	54	38	49	62	59
31	34	24	16	35	47	42	0	46	32	19	26	11	12	43	9	14	57	3	45	18	26

32	49	14	28	53	5	9	30	50	31	63	0	3	37	59	42	24	23	11	52	41	16
33	62	55	22	46	40	63	61	35	7	9	27	23	39	56	19	58	3	57	41	52	2
34	31	37	27	19	38	50	45	9	49	35	22	29	14	15	46	12	17	60	6	48	21
35	19	52	17	31	56	8	12	33	53	34	3	0	6	40	62	45	27	26	14	55	44
36	5	2	54	25	49	43	3	1	38	10	12	30	24	42	59	22	61	6	60	44	55
37	24	34	40	35	22	41	53	48	12	52	38	25	32	17	18	49	15	20	63	9	51
38	47	22	55	29	34	59	11	15	36	56	37	6	0	9	63	2	44	30	29	17	58
39	56	8	5	61	28	52	46	6	4	41	13	15	33	29	45	62	25	1	9	63	47
40	54	27	37	43	33	20	44	56	51	10	55	41	28	35	30	21	52	18	23	3	12
41	61	50	25	58	23	37	62	14	18	39	59	40	9	0	12	46	5	51	38	32	26
42	50	61	11	8	1	31	55	49	9	7	44	16	18	36	32	48	2	28	4	12	3
43	15	57	30	40	46	36	28	47	59	54	18	58	44	31	38	33	24	55	21	26	6
44	23	1	53	28	61	25	43	2	17	21	42	62	43	12	0	15	49	8	54	36	35
45	6	53	1	14	11	4	34	58	52	12	10	47	19	21	39	35	51	5	31	7	15
46	9	18	60	33	43	49	39	31	50	62	57	21	61	47	34	41	26	27	58	24	29
47	38	26	4	56	31	1	29	43	5	20	24	45	2	46	15	9	18	52	11	57	39
48	18	9	56	4	17	14	7	37	61	55	15	13	50	22	24	42	38	54	8	34	10
49	32	12	21	63	36	46	52	42	34	53	2	60	26	1	50	37	44	29	30	61	27
50	42	41	24	7	59	34	4	32	46	8	23	27	48	5	49	18	0	21	55	14	60
51	13	21	12	59	7	20	17	10	40	1	58	18	16	53	25	27	45	41	57	11	37
52	30	35	15	24	3	39	49	55	45	37	56	5	63	27	4	53	40	47	32	33	1
53	63	45	44	32	10	62	37	7	35	49	11	26	30	51	8	52	21	0	24	58	17
54	40	16	24	15	62	10	23	20	13	43	4	61	21	19	56	28	30	48	44	60	14
55	4	33	36	18	27	6	42	52	58	48	40	59	8	3	30	7	56	43	50	35	36
56	20	3	48	47	35	13	2	40	10	38	52	14	29	33	54	11	55	24	0	27	61
57	17	43	19	27	18	2	13	26	23	16	46	7	1	24	22	59	31	33	51	47	63
58	39	7	36	41	21	30	9	45	55	61	51	43	62	11	6	33	10	59	46	53	38
59	1	23	6	51	54	38	16	5	43	13	41	55	17	32	36	57	14	58	27	0	30
60	3	20	46	22	31	21	5	16	29	26	19	49	10	4	27	25	62	34	36	54	50
61	41	42	10	39	44	24	33	12	48	58	1	54	46	2	14	9	36	13	62	49	56
62	33	4	26	9	54	53	41	19	8	46	16	44	58	20	35	39	60	17	61	30	0
63	53	6	23	49	25	33	24	8	19	32	29	22	52	13	7	30	28	2	37	39	57
0	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63
1	54	7	24	50	26	34	25	9	20	33	30	23	53	14	8	31	29	3	38	40	58
2	60	45	46	14	43	48	28	37	16	52	62	5	58	50	6	18	13	40	17	3	53
3	0	37	8	30	13	58	57	45	23	12	50	20	48	62	24	39	43	1	21	2	34
4	61	57	10	27	53	29	37	28	12	23	36	33	26	56	17	11	34	32	6	41	43
5	56	63	48	49	17	46	51	31	40	19	55	2	8	61	53	9	21	16	43	20	6
6	37	0	40	11	33	16	61	60	48	26	15	53	23	51	2	27	42	46	4	24	5
7	46	1	60	13	30	56	32	40	31	15	26	39	36	29	59	20	14	37	35	9	44
8	9	59	3	51	52	20	49	54	34	43	22	58	5	11	1	56	12	24	19	46	23
9	8	40	0	43	14	35	19	1	63	51	29	18	56	26	54	5	30	45	49	7	27
10	47	49	4	63	16	33	59	35	43	34	18	29	42	39	32	62	23	17	40	38	12
11	26	12	62	6	54	55	23	52	57	37	46	25	61	8	14	4	59	15	27	22	49
12	30	11	43	0	46	17	39	22	4	3	54	32	21	59	29	57	8	33	48	52	10
13	15	50	52	7	3	19	36	62	38	46	37	21	32	45	42	35	2	26	20	43	41
14	52	29	15	2	9	57	58	26	55	60	40	49	28	1	11	17	7	62	18	30	25
15	13	33	14	46	9	49	20	42	25	7	6	57	35	24	62	32	60	11	36	51	55
16	44	18	53	55	10	6	22	39	2	41	49	40	24	35	48	45	38	5	29	23	46
17	28	55	32	18	5	12	60	61	29	58	63	43	52	31	4	14	20	10	2	21	33
18	58	16	36	17	49	0	52	23	45	28	10	9	60	38	27	2	35	63	14	39	54
19	49	47	21	56	58	13	9	25	42	5	44	52	43	27	38	61	48	41	8	32	26
20	36	31	58	35	21	8	15	63	1	32	61	3	46	55	34	7	17	23	13	5	24
21	57	61	19	39	20	52	0	55	26	48	31	13	12	63	41	30	5	38	3	17	42
22	29	52	50	24	59	61	16	12	28	45	8	47	55	46	30	41	54	51	44	11	35
23	27	39	34	61	38	24	11	18	3	4	35	1	6	49	58	37	10	20	26	16	8
24	45	60	1	22	42	23	55	0	58	29	51	34	16	15	3	44	33	8	41	6	20
25	38	32	55	53	27	62	1	19	15	31	48	11	50	58	49	33	44	57	54	47	14
26	11	30	42	37	1	41	27	14	21	6	7	38	4	9	52	61	40	13	23	29	19
27	23	48	63	4	25	45	26	58	0	61	32	54	37	19	18	6	47	36	11	44	9
28	17	41	35	58	56	30	2	4	22	18	34	51	14	53	61	52	36	47	60	57	50
29	22	14	33	45	40	4	44	30	17	24	9	10	41	7	12	55	1	43	16	26	32
30	12	26	51	3	7	28	48	29	61	0	1	35	57	40	22	21	9	50	39	14	47
31	53	20	44	38	61	59	33	5	7	25	21	37	54	17	56	1	55	39	50	63	60
32	35	25	17	36	48	43	7	47	33	20	27	12	13	44	10	15	58	4	46	19	29
33	50	15	29	54	6	10	31	51	32	1	0	4	38	60	43	25	24	12	53	42	17
34	63	56	23	47	41	1	62	36	8	10	28	24	40	57	20	59	4	58	42	53	3
35	32	38	28	20	39	51	46	10	50	36	23	30	15	16	47	13	18	61	7	49	22
36	20	53	18	32	57	9	13	34	54	35	4	0	7	41	63	46	28	27	15	56	45
37	6	3	59	26	50	44	4	2	39	11	13	31	27	43	60	23	62	7	61	45	56
38	25	35	41	31	23	42	54	49	13	53	39	26	33	18	19	50	16	21	1	10	52
39	48	23	56	21	35	60	12	16	37	57	38	7	0	10	44	3	40	31	30	18	59
40	59	9	6	62	29	53	47	7	5	42	14	16	34	30	46	63	26	2	10	1	48
41	55	28	38	44	34	26	45	57	52	16	56	42	29	36	21	22	53	19	24	4	13
42	62	51	26	59	24	38	63	15	19	40	60	41	10	0	13	47	6	52	34	33	21
43	51	62	12	9	2	32	56	50	10	8	45	17	19	37	33	49	3	29	5	13	4
44	16	58	31	41	47	37	29	48	60	55	19	59	45	32	39	24	25	56	22	27	7
45	24	2	54	29	62	27	41	3	18	22	43	63	44	13	0	16	50	9	55	37	36
46	7	54	2	15	12	5	35	59	53	13	11	48	20	22	40	36	52	6	32	8	16
47	10	19	61	34	44	50	40	32	51	63	58	22	62	48	35	42	27	28	59	25	30
48	39	27	5	57	32	2	30	44	6	21	25	46	3	47	16	0	19	53	12	58	40
49	19	10	57	5	18	15	8	36	62	56	16	14	51	23	25	43	39	55	9	35	11
50	33	13	22	1	37	47	53	43	35	54	3	61	25	2	51	38	45	30	31	62	28
51	43	42	30	8	60	35	5	33	47	9	24	28	49	6	50	19	0	22	56	15	61
52	14	22	13	60	8	21	18	11	41	2	59	19	17	54	26	28	46	42	58	12	38
53	31	36	16	25	4	40	50	56	46	38	57	6	1	28	5	64	41	48	33	34	2
54	1	46	45	33	11	63	38	8	36	50	12	27	31	52	9	53	22	0	25	59	18
55	41	17	25	16	63	11	24	21	14	44	5	62	22	20	57	29	31	49	45	61	15
56	5	34	39	19	28	7	43	53	59	49	41	60	9	4	31	8	57	44	51	36	37
57	21	4	49	48	36	14	3	41	11	39	53	15	30	34	55	12	56	25	0	28	62
58	18	44	20	28	19	3	14	27	24	17	47	8	2	25	23	60	32	34	52	48	1
59	46	8	37	42	22	31	15	46	56	62	52	44	63	12	7	34	11	60	47	54	39
60	2	24	7	52	51	39	17	6	44	14	42	56	18	33	37	58	15	59	28	0	31
61	4	21	47	23	31	22	6	17	30	27	20	50	11	5	28	26	63	35	37	55	51
62	42	43	11	40	45	25	34	13	49	59	2	55	47	3	15	10	37	14	63	50	57
63	34	5	27	10	55	54	42	20	9	47	17	45	59	21	36	40	61	18	62	31	0

LIST OF REFERENCES

1. Berlekamp, Elwyn, R., Algebraic Coding Theory, New York, McGraw-Hill, 1968

2. Clay, James R., Some Algebraic and Geometric Aspects of Planarity, Proceedings of the Conference of Combinatorial Geometry and its Applications, Perugia, Italy (1970)

3. Ferrero, G., Classificazione e costruzione degli stems p-singolari, Istituto Lombardo (Ren. Sc.) 102 (1968), pp. 597-613

4. Ferrero, G., Stems planari e BIB-desegni, Riv. Mat. Univ. Parma (2), 11, (1970) pp. 1-18

5. Knuth, Donald E., Semi-Numerical Algorithms, New York, Addison-Wesley, 1969, pp. 381-395

6. Knuth, Donald E., Sankhyā, Ser. A, 26 (1964), pp. 305-328