The Annals of Mathematical Statistics
1970, Vol. 41, No. 5, 1763–1767

GENERALIZED COMBINING OF ELEMENTS FROM FINITE FIELDS[1]

By B. L. Raktoe[2]

University of Guelph and Cornell University

0. Introduction and summary. In a recent paper Raktoe [1969] has presented a new approach and also a generalized technique of combining elements from distinct finite fields. The results however were related only to distinct prime fields, i.e. each of the Galois fields in question consisted of residue classes modulo a prime. This paper solves the problem of combining elements for the most general case, i.e. the fields are not necessarily based on distinct primes and they can be prime powered.

1. Preliminaries and background. Let $GF(p_1^{n_{11}})$, $GF(p_1^{n_{12}})$, $\cdots$, $GF(p_1^{n_{1t_1}})$, $GF(p_2^{n_{21}})$, $GF(p_2^{n_{22}})$, $\cdots$, $GF(p_2^{n_{2t_2}})$, $\cdots$, $GF(p_k^{n_{k1}})$, $GF(p_k^{n_{k2}})$, $\cdots$, $GF(p_k^{n_{kt_k}})$ be $\alpha(=\sum_{j=1}^k t_j)$ Galois fields, based on k distinct primes $p_1, p_2, \cdots, p_k$. As is well known, each $GF(p_j^{n_{ji}})$ consists of residue classes of polynomials over the ring of integers modulo an n_{ji}-degree polynomial $P_{ji}(x)$ over $GF(p_j)$ and modulo the prime p_j, $i = 1, 2, \cdots, t_j$, $j = 1, 2, \cdots, k$. First, White and Hultquist [1965] and more recently Raktoe [1969] have solved the problem of combining elements from the fields for the case $t_j = 1$ and $n_{ji} = 1$ for all $j = 1, 2, \cdots, k$, i.e. for the case of k distinct prime fields. In this paper we assume that $t_j \geqq 1$ and $n_{ji} \geqq 1$, i.e. we may have more than one field based on the same prime and the fields may be prime powered. This is the general combining problem, so that White and Hultquist's [1965] and Raktoe's [1969] results will be special cases.

In order to facilitate the ensuing developments for the reader, we summarize in the form of definitions, lemmas and theorems the main results obtained by Raktoe [1969]. Thus, when $R(p)$, $(p = \prod_{j=1}^k p_j$, p_j's distinct), denotes the ring of residue classes modulo p and $I(w)$ denotes the ideal generated by the arbitrary element w of $R(p)$, then he has proved eight lemmas and two theorems and has stated two definitions. These results are numbered alphabetically:

Lemma a. *The elements of the form* $a_j = \prod_{i\neq j}^k p_i - p_j = c_j - p_j$, (*where* $c_j = \prod_{i\neq j}^k p_i$) *in the ring* $R(p)$ *are prime to the number* p *and hence* a_j^{-1} *exists in* $R(p)$, *for* $j = 1, 2, \cdots, k$.

Lemma b. *The elements of the form* $b_j = c_j \cdot a_j^{-1} = 1 + p_j \cdot a_j^{-1}$, $j = 1, 2, \cdots, k$ *in* $R(p)$ *are idempotent.*

Received March 4, 1969; revised January 6, 1970.

[1] Paper No. BU-191 of the Biometrics Unit and No. 579 of the Department of Plantbreeding and Biometry, Cornell University.

[2] Visiting Associate Professor of Biological Statistics, Cornell University, January 1–September 1, 1969.

LEMMA c. *The product $b_j \cdot b_{j^*} = 0$ in the ring $R(p)$ if $j \neq j^*$, j and j^* taking on the values* $1, 2, \cdots, k$.

LEMMA d. *The element b_j of Lemma* b *generates the ideal $I(b_j)$ in the ring $R(p)$, which annihilates the ideal $I(b_{j^*})$ if $j \neq j^*$, j and j^* taking on the values* $1, 2, \cdots, k$.

LEMMA e. *The ideal generated by the element p_j in $R(p)$ annihilates the ideal $I(b_j)$,* $j = 1, 2, \cdots, k$.

LEMMA f. *The multiplicative identity element of the ideal $I(b_j)$ of Lemma* d *is* $b_j, j = 1, 2, \cdots, k$.

LEMMA g. *The multiplicative identity element* 1 *of the ring $R(p)$ is the sum of the multiplicative identities of the $I(b_j)$*'s, *i.e.* $1 = \sum_{j=1}^{k} b_j$.

THEOREM a. *The ring $R(p)$ is the direct sum of the ideals $I(b_j)$*'s *i.e.* $R(p) = \sum_{j=1}^{k} \oplus I(b_j)$.

LEMMA h. *The field $GF(p_j)$ is isomorphic to the ideal $I(b_j)$, $j = 1, 2, \cdots, k$, via the map $\sigma(x) = b_j \cdot x = y$, for $x \in GF(p_j)$ and $y \in I(b_j)$.*

DEFINITION a. Define addition and multiplication of elements from distinct prime fields, i.e. $x \in GF(p_j)$ and $x^* \in GF(p_{j^*})$, $j \neq j^*$ by the rules:

$$x + x^* = \sigma(x) + \sigma(x^*)$$
$$x \cdot x^* = \sigma(x) \cdot \sigma(x^*).$$

DEFINITION b. If $r \in R(p)$ and $x \in GF(p_j)$, then we define the addition and multiplication of x and r by:

$$x + r = \sigma(x) + r$$
$$x \cdot r = \sigma(x) \cdot r.$$

THEOREM b. *The ring $R(p)$ is the direct sum of the $GF(p_j)$*'s, *i.e.* $R(p) = \sum_{j=1}^{k} \oplus GF(p_j)$.

2. Combining elements from arbitrary prime powered fields. Let $GF(p_1^{n_{11}})$, $GF(p_1^{n_{12}}), \cdots, GF(p_1^{n_{1t_1}})$, $GF(p_2^{n_{21}})$, $GF(p_2^{n_{22}}), \cdots, GF(p_2^{n_{2t_2}}), \cdots, GF(p_k^{n_{k1}})$, $GF(p_k^{n_{k2}}), \cdots, GF(p_k^{n_{kt_k}})$ be our $\alpha (= \sum_{j=1}^{k} t_j)$ finite fields, based on k distinct primes $p_1, p_2, \cdots, p_k$. Further let n_j be the least common multiple of $\{n_{j1}, n_{j2}, \cdots, n_{jt_j}\}$, and consider the Galois fields $GF(p_1^{n_1}), GF(p_2^{n_2}), \cdots, GF(p_k^{n_k})$. Then each $GF(p_j^{n_j})$ consists of residue classes of polynomials over $GF(p_j)$. As before, let $R(p)$, $p = \prod_{j=1}^{k} p_j$, be the residue class ring modulo p and consider the ring $R(x, p)$ of polynomials over $R(p)$, then we are ready to prove the following:

LEMMA 2.1. *The ring $R(p)$ is a subring of $R(x, p)$.*

PROOF. See any standard text in modern algebra.

THEOREM 2.1. *The eight lemmas and two theorems under the definitions of Section* 1 *are all true for the subring $R(p)$ of $R(x, p)$.*

PROOF. The proof follows immediately from Lemma 2.1.

LEMMA 2.2. *To each prime polynomial $P_j(x)$ of degree n_j over $GF(p_j)$, there corresponds a polynomial $P_j{}^*(x)$ of degree n_j over $I(b_j)$ of $R(p)$.*

PROOF. Follows from Lemma h of Section 1, with $P_j{}^*(x) = b_j \cdot P_j(x)$.

LEMMA 2.3. *The ring of polynomials over $I(b_j)$ is a subring of $R(x, p)$, for each $j = 1, 2, \cdots, k$. Call these subrings $R(x, b_j)$'s.*

PROOF. The proof follows immediately from Lemma d of Section 1.

LEMMA 2.4. *The residue classes of the ring $R(x, b_j)$ modulo $P_j{}^*(x)$ form a commutative ring for each $j = 1, 2, \cdots, k$. Call these rings $R(x, b_j, P_j{}^*(x))$'s.*

PROOF. Noting that any element in $R(x, b_j, P_j{}^*(x))$ can be written as: $f_j(x) + P_j{}^*(x) \cdot Q_j(x)$, where $f_j(x)$ is a polynomial over $I(b_j)$ of degree $\leqq (n_j - 1)$ and $Q_j(x)$ is a polynomial with coefficients in $I(b_j)$, the ring properties can be easily verified.

LEMMA 2.5. *The multiplicative identity element of $R(x, b_j, P_j{}^*(x))$ is b_j.*

PROOF. The proof follows from Lemma 2.4 and Lemma f of Section 1.

LEMMA 2.6. *The ring $R(x, b_j, P_j{}^*(x))$ annihilates the ring $R(x, b_{j^*}, P_{j^*}^*(x))$ for $j \neq j^*$.*

PROOF. The proof follows from Lemma 2.4 and Lemma d of Section 1.

THEOREM 2.2. *The ring $R(x, b_j, P_j{}^*(x))$ is isomorphic to $GF(p_j{}^{n_j})$.*

PROOF. The proof follows from Lemma 2.4, Lemma 2.5 and Lemma h of Section 1.

DEFINITION 2.1. If $\mu \in GF(p_j{}^{n_j})$ and $\mu^* \in GF(p_{j^*}^{n_{j^*}})$ with $j \neq j^*$, then we define addition and multiplication of elements from distinct finite fields by the rules:

$$\mu + \mu^* = \sigma(\mu) + \sigma(\mu^*)$$

$$\mu \cdot \mu^* = \sigma(\mu) \cdot \sigma(\mu^*)$$

where σ is the coefficient isomorphism defined by Lemma h of Section 1.

DEFINITION 2.2. If $\mu \in GF(p_j{}^{n_j})$ and $r \in R(x, p)$, then we define the addition and multiplication of μ and r by:

$$\mu + r = \sigma(\mu) + r$$

$$\mu \cdot r = \sigma(\mu) \cdot r$$

where σ is again defined by Lemma h of Section 1.

Now, consider an element $g(x)$ of $R(x, p)$, then this element may in virtue of Theorem a of Section 1 be written as $g(x) = \sum_{j=1}^{k} g_j(x)$, where $g_j(x)$ is a polynomial over $I(b_j)$. Setting $g_j(x) = h_j(x) + q_j(x) \cdot P_j{}^*(x)$, where $h_j(x)$ is a polynomial of degree $\leqq (n_j-1)$ over $I(b_j)$ and $q_j(x)$ is a polynomial with coefficients in $I(b_j)$, we have as a consequence that $g(x)=\sum_{j=1}^k h_j(x)+q_j(x)\cdot P_j^*(x)$. Hence it follows that $g(x)=\sum_{j=1}^k [h_j(x)\,(\operatorname{mod} P_j^*(x))]$ and letting $h(x)=\sum_{j=1}^k h_j(x)$, we have in conventional notation $g(x)=h(x)\,(\operatorname{mod} P_1^*(x), \operatorname{mod} P_2^*(x),\cdots, \operatorname{mod} P_k^*(x))$. Denote the set of $h(x)$'s by $R(x,p,P_1^*(x), P_2^*(x),\cdots, P_k^*(x))$ then this set may be given the interpretation of consisting of residue classes of the ring $R(x,p)$ modulo $P_1^*(x)$, modulo $P_2^*(x),\cdots$, modulo $P_k^*(x)$. This leads us to the following lemma and additional results:

LEMMA 2.7. *The set* $R(x,p,P_1^*(x), P_2^*(x),\cdots, P_k^*(x))$ *is a commutative ring.*

LEMMA 2.8. *The ring* $R(x,p,P_1^*(x), P_2^*(x),\cdots, P_k^*(x))=\sum_{j=1}^k \oplus R(x,b_j, P_j^*(x))$.

PROOF. From Theorem a of Section 1, we know that $R(p)=\sum_{j=1}^k \oplus I(b_j)$, which implies the unique decomposition of $g(x)$ above as $g(x)=\sum_{j=1}^k \oplus h_j(x)$ $(\operatorname{mod} P_1^*(x), \operatorname{mod} P_2^*(x),\cdots, P_k^*(x))$, so that by Lemma 2.4 the desired result follows.

THEOREM 2.3. *The ring* $R(x,p,P_1^*, P_2^*(x),\cdots, P_k^*(x))=\sum_{j=1}^k \oplus GF(p_j^{n_j})$.

PROOF. The proof of this theorem follows directly from Theorem 2.2, Definition 2.1, Definition 2.2, and Lemma 2.8.

Let us now return to the beginning of this section and dispose of the problem of combining elements of fields based on the same prime. Noting the definition of the n_j's as least common multiples of the $\{n_{j1}, n_{j2},\cdots, n_{jt_j}\}$'s, the problem is resolved in the following lemma and theorem:

LEMMA 2.9. *The finite field* $GF(p_j^{n_j})$ *contains as subfields all the fields* $GF(p_j^{n_{j1}})$, $GF(p_j^{n_{j2}}),\cdots, GF(p_j^{n_{jt_j}})$.

PROOF. Follows from the definition of n_j and Theorem XXIV on page 160 of Carmichael [1956].

THEOREM 2.4. *The ring* $R(x,b_j,P_j^*(x))$ *contains subrings to which each of the fields* $GF(p_j^{n_{j1}}), GF(p_j^{n_{j2}}),\cdots, GF(p_j^{n_{jt_j}})$ *are isomorphic, so that combining elements from these fields with other arbitrary fields is a solved problem.*

PROOF. Follows immediately from Lemma 2.9, Theorem 2.2 and Theorem 2.3.

3. An example. Consider the fields $GF(2)$, $GF(2^2)$ and $GF(3)$. Here, $n_1=2$ and $n_2=1$ so that $P_1(x)=x^2+x+1$ and $P_2(x)=x+1$. Hence we have:

$$R(p)=R(6)=\{0,1,2,3,4,5\}$$

$$I(b_1)=I(3)=\{0,3\}$$

$$I(b_2)=I(4)=\{0,4,2\}$$

$$R(x,p)=\{e_tx^t+e_{t-1}x^{t-1}+\cdots+e_1x+e_0,\ e_i\in R(6)\}.$$

Lemma 2.1: $R(6) \subset R(x, 6)$.

Lemma 2.2: $P_1{}^*(x = 3 \cdot (x^2+x+1) = 3x^2+3x+3$,
$P_2{}^*(x) = 4(x+1) = 4(x+1) = 4x+4$.

Lemma 2.3: $R(x, 3) \subset R(x, 6)$, $R(x, 4) \subset R(x, 6)$.

Lemma 2.4: $R(x, 3, 3x^2+3x+3) = \{0, 3, 3x, 3x+3\}$;
$R(x, 4, 4x+4) = \{0, 4, 2\}$.

Lemma 2.5: Identity element of $R(x, 3, 3x^2+3x+3)$ is 3.
Identity element of $R(x, 4, 4x+4)$ is 4.

Lemma 2.6: $v \in \{0, 3, 3x+3\}$, $v^* \in \{0, 4, 2\}$ then clearly
$v \cdot v^* = 0$.

Lemma 2.7: $R(x, 6, 3x^2+3x+3, 4x+4) = \{0, 1, 2, 3, 4, 5, 3x, 3x+1, 3x+2, 3x+3, 3x+4, 3x+5\}$.

Lemma 2.8: $R(x, 6, 3x^2+3x+3, 4x+4) = R(x, 3, 3x^2+3x+3) \oplus R(x, 4, 4x+4)$.

Theorem 2.3: $R(x, 6, 3x^2+3x+3, 4x+4) = GF(2^2) \oplus GF(3)$.

Lemma 2.9: $GF(2^2)$ contains $GF(2)$.

Theorem 2.4: $R(x, 3, 3x^2+3x+3)$ contains the subring $I(3)$ which is isomorphic to $GF(2)$.

4. Discussion. In actual manipulations of elements from finite fields one needs only to multiply the elements of the fields with their respective b's before performing the addition or multiplication operation. This remark shows the simplicity in practice. The results obtained through application of our technique to the construction of confounded mixed factorial and mixed lattice designs has already been set forth in a paper by Raktoe and Federer [1969].

Acknowledgment. The author wishes to thank the associate editor and the referee for their efficient handling of the paper and for their remarks which made the paper more concise.

REFERENCES

[1] Carmichael, R. D. (1956). *Introduction to the Theory of Groups of Finite Order*. Dover, New York. (First published 1937.)

[2] Raktoe, B. L. (1969). Combining elements from distinct finite fields in mixed factorials. *Ann. Math. Statist.* **40** 498–504.

[3] Raktoe, B. L. and Federer, W. T. (1969). Construction of confounded mixed lattice designs. Paper No. BU-193 in the Biometrics Unit Series, Cornell Univ. Submitted to *Austral. J. Statistics*.

[4] White, B. and Hultiquist, R. A. (1965). Construction of confounding plans for mixed factorial designs. *Ann. Math. Statist.* **36** 1256–1271.