GEOMETRY OVER A FINITE FIELD

Donald L. Reisler
Nicholas M. Smith

Research Analysis Corporation
McLean, Virginia 22101

ABSTRACT

The development of certain aspects of a physically interpretable geometry defined over a finite field is presented. The concepts of order, norm, metric, inner product, etc. are developed over a subset of the total field. It is found that the finite discrete space behaves locally, not globally, like the conventional "continuous" spaces. The implications of this behavior for mathematical induction and the limit procedure are discussed, and certain radical conclusions are reached. Among these are: (a) mathematical induction ultimately fails for a finite system and further extension leads to the introduction of formal indeterminancy; (b) finite space-time operations have inherent formal properties like those heretofore attributed to the substantive physical universe, and (c) certain formal properties attributed to continuous spaces cannot be developed from successive embedding in finite space of finer resolution—but must be based on independent axiomatic (non-testable) assumptions. It is suggested that a finite field representation should be used as the fundamental basis of a physical representation.

1. INTRODUCTION

"Mathematics is devised by mathematicians." This tautology contains potentially significant implications. Mathematicians are mortal human beings whose conceptualizing capacity is finite. Acting in a rational mode, or as we shall say, as a "cognitive agent," man communicates at finite rates; employs finite strings of symbols; and has finite data processing and storage capacity. Yet he has devised conceptual mathematical geometries of continuous and infinite spaces. It is reasonable to expect that a man's finiteness qua mathematician will exert a controlling influence on the nature of the concepts he develops. This realization has led us to seek a priori characterizations of these concepts that result from the nature of the cognitive agent who produced them.

Thus, we have set ourselves the task of determining "How do you get there from here." Or more formally, how can a finite cognitive agent develop concepts of continuous spaces and space-time systems as well as the associated mathematical operations. It is necessary to start with the development of numbers—in the finite cognitive system and demonstrate how this leads to operations such as translation and rotation in finite geometries. Then, we examine the meaning of the corresponding processes in continuous spaces in a manner appropriate to the operations admissible to the finite cognitive agent.

The resulting implications of this investigation are in some respects expected;—in other aspects quite radical. The findings of this paper are

in opposition to certain of the conventional conclusions and assumptions of mathematics and we are aware of their heretical nature. Thus we ask the reader to consider the arguments in the context of the philosophical viewpoint upon which they are based.

It is found that there are constraints that limit the cognitive agent in actu and contribute certain formal properties to his admissible concepts. In particular, we look at mathematical induction and the process of going to the limit; examples are presented that are physical illustrations of our ideas. It is proposed that certain of the presumed external physical postulates are in fact formal properties of finite spaces and their reintroduction as physical properties results from our using infinite field mathematics. We suggest, and present examples, to show how these postulates arise to constrain the mathematics of infinite fields to represent "experience."

In this paper, we explore a finite field (Galois Field) representation and attempt to formulate a physically interpretable geometry over this field. Thus we seek to define the basic objects of geometry solely in terms of the finite field concepts. We have developed some formal aspects of a vector space defined over a finite scalar field. Kustaanheimo and Järnefelt[1] did extensive work to formulate such a geometry in order to provide a structure that was consistent with the apparent finiteness and discreteness of the physical universe; since then there have been additional efforts to refine the mathematics.[2]

2. HEURISTICS

The goal of this effort is to establish that one can perform all legitimate arithmetic and algebraic operations solely within the context defined by a primitve commitment to finitism, etc.[3] In order to achieve this demonstration, we must adopt certain mathematical structures that can serve as the foundation of the various operations. In this section we shall present a series of metatheoretical and motivational arguments that seek to establish the concepts and development that are employed. It is clear that uniqueness and necessity of a representation of experience cannot be proven unless the universe of discourse is closed, i.e., uniqueness and necessity are always with respect to a given context. Hence a system purporting to represent or at least be consonant with experience is perforce backed "only" by sufficiency or demonstrable adequacy.

To insure that arithmetic can be carried out we shall require that the two basic operations of addition and multiplication be defined. Also the inverse operations of subtraction and division will be required. To insure that we satisfy the requirement of ontological parity[3] we shall demand that the basic set be closed under the four primary operations. Nonambiguity similarly implies that the results of these operations be unique. We shall also seek as much procedural invariance as we can by requiring associative and commutative multiplication and addition. Furthermore, the combination of these two operations will be such that the appropriate distributive laws are valid. These conditions are sufficient to define a field as the underlying mathematical reservoir

for our primitive operations. Therefore, as an immediate consequence of our commitment to finitism, we are led to consider a finite field (Galois field).[4]

If our mathematical system is to serve as a suitable basis for the many computational operations, then it must admit of many other operations that are to be considered legitimate. There are certain such operations that do not always lead directly to a formal answer because of the severe limitations imposed by the restriction of finite resources and capabilities. However, in any actual calculation one always has finite and greatly limited resources and that never becomes a deterrent or causes termination of the logical procedures. One simply replaces the problem for which there is no formal solution by some solvable problem taken from the given field. Thus, for example, when computing the square root of two, one "truncates" the calculation at the desired level of resolution. Clearly this is tantamount to introducing a replacement problem. If we seek a resolution of one decimal place in the answer, then we look to a neighboring perfect square, 196×10^{-2} that is "close" to 200×10^{-2} and declare the answer to be 14×10^{-1}. In this way, replacement permits our mathematical operations to continue and avoids cessation due to uncomputability or lack of performable instructions. One could also construct his system to reset itself to some arbitrary point—say zero—whenever an impasse is reached. However, the rationale for replacement is clearly preferable because it seeks a "nearby" problem and we shall adopt it.

Let us point out that we have described replacement with a "neighboring" problem or "best" approximation but the bare algebraic structure does not yet have any procedure for determining such a "best" replacement. Thus we need some measure of proximity or closeness in order to determine that which is the appropriate substitute. If we are to define a vector space over the finite field, then a metric can fill this requirement. However, even if some value can be associated with the "distance" between points, we still require a mechanism for comparing different distances. In short, the underlying number field must have some ordering relation. Since our primitive commitments do not demand global operations but merely a suitable local definition, we shall seek—as a minimum—an irreflexive[5] binary relation. Clearly there is no way to define a meaningful transitive order throughout a finite field and still retain the other properties of uniqueness, nonambiguity, irreflexivity, etc.

In defining a metric for a vector space, we will encounter the square root operation. If we restrict ourselves to a ground field GF(p), then there will be formal square roots for half the elements of the multiplicative group, i.e. for $(p - 1)/2$ elements. This behavior is reminiscent of the analogous property of the real number system in which only "half" the elements (positive elements) have square roots in the field. If we wish to institute an extension of GF(p) in order to generate a square root for every element of GF(p), then we may do a

similar thing to that done in conventional analysis, viz. embed our system in a "complex plane" obtained by expanding GF(p) via $x^2 + 1$ as a prime ideal. In this way all "real" numbers (i.e. elements of GF(p)) will have formal square roots. Unfortunately, we have merely set the problem back one stage for only $(p^2 - 1)/2$ elements of $GF(p^2)$ have square roots in $GF(p^2)$. We can establish a replacement technique for these nonsquare elements of $GF(p^2)$, thereby closing our system. This procedure does generate a formally satisfactory system for all elements of the ground field. Actually, we will find that even these hard won formal square roots for GF(p) do not in general behave as desired and we are forced to introduce still another replacement procedure to rectify the situation. This is necessitated by the additional demand that square roots of ordered numbers lie in the same order. With these many qualifications and extensions, we will find that certain general properties of geometry in vector spaces can be realized.

3. AN "ORDERING" RELATION

In this section we shall begin work upon the explicit development of geometry defined in a finite and discrete space. For the early and classical work on this topic see reference 1.

Consider GF(p) with $p = 8\prod_{i=1}^{k} q_i - 1$, where the q_i are the odd primes. We know that in such a field the elements $1,2,\ldots,q_k$ are all square residues and -1 is nonsquare.[1]

Definition(1) Let $x,y \in GF(p)$ with p given above. If $x - y =$ square residue, then x is said to exceed y, in symbols $x > y$. If $x - y =$ nonsquare residue, then x is less than y, $x < y$.[6]

Theorem (1). Let p be as above. If x is square, then -x is nonsquare and vice versa (here -x is the additive inverse of x, i.e. $x + (-x) \equiv 0 \pmod{p}$.

Proof. If p is an odd prime and w a primitive root of GF(p), then $w^{(p-1)/2} \equiv -1 \pmod{p}$.[7] Let $x = w^n$ and $-x = w^m$, where n an even integer and m an integer. We have

$$x + (-x) = w^n + w^m \equiv 0 \pmod{p} .$$

Now, either $n > m$ or $m > n$. Assume, for definiteness, $m < n$. Then

$$w^m(w^{n-m} + 1) \equiv 0 \pmod{p} .$$

Since $w^m \not\equiv 0 \pmod{p}$, we have $w^{n-m} + 1 \equiv 0 \pmod{p}$. From above, this gives $w^{n-m} \equiv w^{(p-1)/2} \pmod{p}$. From this we obtain $n - m \equiv (p - 1)/2 \pmod{p - 1}$. However, for a p in the form given above, we see that

$$(p - 1)/2 = 4 \prod_{i=1}^{k} q_i - 1$$

which is always odd. Therefore n and m have opposite parity.

Theorem (2). If $x,y \in GF(p)$ with p given above, then $x > y$ iff $y < x$.

Proof. Assume $x > y$. Then $x - y$ = square residue and $y - x$ = -(square residue). In such a GF(p), the additive inverse of a square residue is nonsquare and vice versa. This follows because in such GF(p) -1 is a nonsquare residue and if x is a square residue, then $(-1)(x) = -x$ is a nonsquare residue. (See Theorem (1)). Hence $x > y \Rightarrow y < x$. The converse is proved similarly.

Theorem (3). If $\alpha \in GF(p)$, then $\alpha^2 \equiv (-\alpha)^2 \pmod{p}$.

Proof. From the above theorem, we know that if $\alpha = w^n$ and $-\alpha = w^m$ then $n - m \equiv (p - 1)/2 \pmod{p - 1}$. Hence, since $\alpha^2 = w^{2n}$, $(-\alpha)^2 = w^{2m}$, we have $2n - 2m \equiv (p - 1) \pmod{p - 1} \equiv 0 \pmod{p - 1}$.

Definition (2). Define an "absolute value" function in the following way. If $\alpha \in GF(p)$ with $p = 8 \prod_{i=1}^{k} q_i - 1$, then $|\alpha| = \alpha$ if α is a square residue and $|\alpha| = -\alpha$ if α is a nonsquare residue. Theorem (1) provides the justification for this definition.

Theorem (4). Let $x \in GF(p)$ $(p \neq 2)$ be a square residue. Then there exist two elements $a,b \in GF(p)$ such that $a^2 \equiv b^2 \equiv x \pmod p$. Furthermore, if $p = 8 \prod_{i=1}^{k} q_i - 1$, then a and b are of opposite parity and are additive inverses of each other, $a + b \equiv 0 \pmod p$. One of the two, say a, is square and the other b, is nonsquare. a is called $+\sqrt{x}$.

Proof. Let us first prove there can't be three elements all of which square to the same value. Assume $\exists$ three distinct elements $a,b,c \in GF(p) \ni a^2 \equiv b^2 \equiv c^2 \equiv x \pmod p$. Then $a^2 - b^2 \equiv 0 \pmod p$ and $a^2 - c^2 \equiv 0 \pmod p$, or $(a + b)(a - b) \equiv 0 \pmod p$ and $(a + c)(a - c) \equiv 0 \pmod p$. Since a,b,c are distinct, we have $a + b \equiv 0 \pmod p$ and $a + c \equiv 0 \pmod p$. But in a field, the additive inverse is unique, so $b \equiv c \pmod p$ which violates assumption that a,b,c are distinct.

Now prove $\exists$ two elements $a,b \ni a^2 \equiv b^2 \equiv x \pmod p$. There are $p - 1$ distinct nonzero elements and $(p - 1)/2$ distinct squares in $GF(p)$, $p \neq 2$. Since there aren't three elements having some squared value, there must be two such distinct elements for every square x.

From $a^2 - b^2 \equiv (a + b)(a - b) \equiv 0 \pmod p$ and $a \not\equiv b \pmod p$ we see that a,b are additive inverse. If $p = 8 \prod_{i=1}^{k} q_i - 1$, we may invoke Theorem (1), to conclude they are of opposite parity.

4. LOCAL "ORDER"

Let us consider some arbitrary $x \in GF(p)$. We know that $(x + 1) - x = 1 =$ square residue; hence $x + 1 > x$. Similarly, $x - (x - 1) = 1$, or $x > x - 1$. Also, $(x + 1) - (x - 1) = 2 =$ square residue, so that $x + 1 > x > x - 1$. Clearly this process may be continued for q_k consecutive elements to generate the following order relations:

$$x - (q_k - 1)/2 < x - (q_k - 3)/2 < \ldots < x + (q_k - 1)/2.$$

Let us designate this set of q_k consecutive transitively ordered elements that is centered about x by Toss (x, q_k). We shall consider $x + 1, \ldots, x + (q_k - 1)/2$ as all "positive" with respect to x while $x - 1, \ldots, x - (q_k - 1)/2$ are "negative" with respect to x. It is important to realize that the terms positive and negative express a relation that is referred to some specific point, not necessarily the additive identity 0. In order to perform calculations we must be sure to refer to this central point x. This is done by counting the number of steps "above" or "below" x for any member of Toss (x, q_k). Thus, if $a, b \in$ Toss (x, q_k), we have the sum as $(a - x) + (b - x) + x$, etc. Clearly this is the well-known transformation of linear translation. Thus, with the above identifications and definitions, we see that any point $x \in GF(p)$ may serve as the center of a Toss (x, q_k). Thus whatever "geometry" can be done at one point can be done at any point. Therefore we have shown that

Theorem (5). Any point $x \in GF(p)$ can be the center of a Toss (x, q_x) and "geometry" can be done locally within this set.

To simplify calculations we may assume that $x = 0$ is the chosen center, thereby avoiding the extra terms of $a - x$, etc. However, we must remember that the choice of center point is arbitrary and the geometrical results obtained in one Toss are equivalent to those found in any Toss in the field.

Since we are defining a vector space over GF(p), we may generalize this discussion for n-dimensional vectors and let the center become a vector $x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$. Essentially this is a succinct formulation of n distinct centers, one for each component.

5. EXTENSION OF THE FIELD[8]

Let GF(p) be a Galois field. We know that $(p - 1)/2$ elements are square and $(p - 1)/2$ are nonsquare (see Theorem (4)). The $(p - 1)/2$ square elements all have two square roots in GF(p) whereas the nonsquare elements do not have a square root in GF(p). If $p = 8 \prod_{i=1}^{k} q_i - 1$, then the two roots of the square elements are related by $+\sqrt{x} + (-\sqrt{x}) \equiv 0$ and $+\sqrt{x} > 0$, $-\sqrt{x} < 0$. To obtain square roots for the nonsquare elements we must embed GF(p) in a larger field $GF(p^2)$ which is the extension of GF(p), i.e. we obtain $GF(p^2)$ from GF(p) by adjunction of a root of $x^2 + 1 \equiv 0 (\text{mod } p)$. $GF(p^2)$ becomes isomorphic to the set of first degree polynomials

$a + bx$ where the coefficients $a,b \in GF(p)$. Clearly there are p^2 elements in $GF(p)$. To simplify comparisons with "ordinary" mathematics, let us denote the indeterminant by i. Since $i^2 + 1 \equiv 0$ we have $i^2 \equiv -1$, and $a + ib \in GF(p^2)$. Let us now find square roots of the negative elements of $GF(p)$. Let $x \in GF(p)$ $p = 8 \prod_{i=1}^{k} q_i - 1$ be nonsquare. Assume an element $a + ib \in GF(p^2)$ as the square root of x. Hence $a + ib \equiv \sqrt{x}$ or $x \equiv (a + ib)^2 \equiv a^2 - b^2 + 2iab$. From this we see that $ab \equiv 0 \Rightarrow a \equiv 0$ or $b \equiv 0$. Also have $a^2 - b^2 \equiv x$. If $b \equiv 0$, then $b^2 \equiv 0$ and $x \equiv a^2$ which violates assumption that x is nonsquare. Hence $a \equiv 0$ and $x \equiv -b^2$ and $b^2 \equiv -x$. We know that $x < 0 \Rightarrow -x > 0$ so $b \equiv \pm\sqrt{-x}$. Hence $\sqrt{x} \equiv \pm i\sqrt{-x}$ which conforms to our prior expectations. Thus $\forall\, x \in GF(p)$ $\exists\, z \in GF(p^2) \ni z^2 \equiv x$.[9]

Since $(p^2 - 1)/2$ elements of $GF(p^2)$ are square and $(p^2 - 1)/2$ are nonsquare, we see that a square root for elements of $GF(p^2)$ can be found for some of the elements ($(p^2 - 1)/2$ of them). This can also be seen since there are two square roots for each $x \in GF(p^2)$ $(x \neq 0)$ and this—due to uniqueness properties—implies that only half the nonzero elements can have square roots in $GF(p^2)$. This is yet another way in which the finite field differs radically from the continuous field where every complex number has two square roots in the complex plane. In finite field mathematics we are able to count according to the customary rules without encountering the unusual characteristics of the transfinite arithmetic.

Theorem (6). If $p = 8 \prod_{i=1}^{k} q_i - 1$, then $x^2 + 1$ is irreducible over $GF(p^2)$.

Proof. Assume $x^2 + 1$ is reducible over $GF(p^2)$. Then $\exists\ a,b \in GF(p) \ni$ $x^2 + 1 \equiv (x + a)(x + b) \equiv x^2 + ab + x(a + b)$. For this to hold, we must have

$$ab \equiv 1 \quad \text{and} \quad a + b \equiv 0.$$

This implies $a^2 + ab \equiv a^2 + 1 \equiv 0$. In $GF(p)$ of the above form, there exist no solution to this because -1 is nonsquare and $a^2 \equiv -1$ cannot be solved.

Theorem (7). If $p = 8 \prod_{i=1}^{k} q_i - 1$, then $x^2 + 1$ is not primitive in $GF(p^2)$.

Proof. For such a p, we always have $p^2 > 4$, yet $x^2 + 1$ divides $x^4 - 1$; hence $x^2 + 1$ cannot be primitive because its order is less than p^2.

Beltrametti and Blasi[10] have shown that for a p of the above form, $i^p = -i$; if $a,b \in GF(p^2)$, then $(a + b)^p = (a^p + b^p)$. Therefore if $a,b \in GF(p)$, then $(a + ib)^p = a - ib$; hence complex conjugation can be associated with the p^{th} power of a "complex number." Define Z^* such that $\forall\ z \in GF(p^2),\ z^* = z^p$.
We follow reference 4 and define the absolute value in an obvious way, viz. $\forall\ z \in GF(p^2)$, $|z| = \sqrt{z^* z} = \sqrt{z^{p+1}}$. If $z = a + ib$, $a,b \in GF(p)$, then $|z| = \sqrt{a^2 + b^2}$ and we see that $\forall\ z \in GF(p^2)\ \exists\ |z| \in GF(p^2)$. This is somewhat unfortunate because the absolute value function is generally considered to be a mapping from the complex plane onto the positive real line. In our case, this becomes a mapping from $GF(p^2)$ onto the square residues of $GF(p)$. As before, we can achieve such a condition over a subset. Let $S(x,q_k) = \{y : y \in \text{Toss } (x,q_k) \text{ and } 2y^2 \in \text{Toss } (x,q_k)\}$ (remember $2y^2$ to be performed with respect to the center, x). For simplicity, consider $S(0,q_k)$. Define $C(S(0,q_k)) = \{z : z = a + ib$, $a,b \in S(0,q_k)\}$. Then $\forall\ z \in C(S(0,q_k))$ $|z| \in GF(p)$ and $|z| =$ square residue. We may generalize our definition to include the

replacement square roots to find (see section 7).

$$|z|_R = \left(\sqrt{z^* z}\right)_R .$$

In terms of this definition, $|z|_R$ is ordered, etc. over an appropriate subset. Thus, we can introduce a length notion over part of $GF(p^2)$.

6. SQUARE ROOTS AND INCOMPLETENESS

We have seen that for any GF(p), there are $(p - 1)/2$ elements that do not have square roots in GF(p). If you embed GF(p) in $GF(p^2)$, then each of these $(p - 1)/2$ elements has a square root in $GF(p^2)$. However, in $GF(p^2)$, there are $(p^2 - 1)/2$ elements without square roots in $GF(p^2)$. This process continues for all finite fields, the richest always failing to contain square roots for about half its members. This is a form of incompleteness that is somewhat reminiscent of the Godel type incompleteness. Godel showed that within any formal system at least as rich as arithmetic, there always exist statements whose truth or falsity depends entirely upon the truth or falsity of a meta statement.[11] Hence the status of certain statements cannot be determined within the system. The square root situation is much the same, for every system (field) is dependent upon the embedding field (meta field) for its square root completion. It should be noted that an infinite field is not considered to display such behavior. In fact the complex plane is purported to contain the square root of every one of its elements. This is another example of the curious counting results one encounters when dealing with infinities of numbers. However, if the infinite field is obtained from a limiting process of successive imbedding, of finite fields, the cited property of the continuous complex plane will not appear for any finite part of the limiting process.

7. REPLACEMENT TECHNIQUE FOR SQUARE ROOTS

Let us concentrate our attention upon the ordered subset centered about 0, i.e. Toss $(0,q_k)$. We are going to be concerned with those elements in Toss $(0,q_k)$ that in conventional number theory are known as perfect squares, viz. 0, 1, 4, 9, 16, ... Let $\text{Toss}^+(0,q_k) = \{0,1,2,\ldots,(q_k-1)/2\}$, i.e. the "positive" elements of Toss $(0,q_k)$.

Let us construct a set $\Gamma(q_k)$ as follows. Let $0 \in \Gamma(q_k)$. Then let $(0+1)^2 \in \Gamma(q_k)$ if $(0+1)^2 \in \text{Toss}^+(0,q_k)$. Continue in this until the first time that $(\underbrace{0+1+\cdots+1}_{n+1 \text{ times}})^2 \notin \text{Toss}^+(0,q_k)$. Then the n elements

$0^2, 1^2, 2^2, \ldots, n^2$ will constitute $\Gamma(q_k)$. Let us arrange and number the elements of $\Gamma(q_k)$ so that $\gamma_0 = 0^2$, $\gamma_1 = 1^2$, etc. Then we have $\gamma_0 < \gamma_1 < \gamma_2 < \cdots < \gamma_n$ where γ_n is the largest "perfect square" in $\text{Toss}^+(0,q_k)$. Let $S(q_k) = \{x : x \in \text{Toss}^+(0,q_k) \text{ and } x \leq \gamma_n\}$. Thus for the elements of $\Gamma(q_k)$ we have the square roots lying in the same order as the squares, clearly a desirable situation. Unfortunately the formal square roots of the elements of $S(q_k)$ not in $\Gamma(q_k)$ do not exhibit this property. We shall impose the additional condition that the squares and square roots of $S(q_k)$ lie in the same order. Since we cannot obtain an acceptable solution—acceptable with respect to the criteria established above—we shall replace the problem by one that we can solve within the framework.

Let $x \in S(q_k)$, $x \notin \Gamma(q_k)$. Problem (1) is to find $y \in S(q_k) \ni y^2 \sim x$. If $x \in S(q_k)$ and $x \notin \Gamma(q_k)$, then $\exists\, i$ $(i \in \{0,1,2,\ldots,n-1\}) \ni \gamma_i < x < \gamma_{i+1}$. We shall replace problem (1) with $\sqrt{\gamma_{i+1}} \in S(q_k)$ and designate the replacement by $(\sqrt{x})_R$. Clearly, if $x \in \Gamma(q_k)$, then $(\sqrt{x})_R = \sqrt{x}$ (where $\sqrt{x}$ has its ordinary definition.).

We have replaced problem (1), which does not have an acceptable solution in GF(p), by another problem that does admit of solution. We again see that going beyond $\text{Toss}(0,q_k)$ leads us into a realm of uniterpretable results. In effect, this corresponds to going beyond the capabilities or resources of the given GF(p).

Theorem (8). 1. $\forall\, x \in S(q_k)$, $(\sqrt{x})_R \in S(q_k)$

2. If $x,y \in S(q_k)$ and $x \leq y$, then $(\sqrt{x})_R \leq (\sqrt{y})_R$

3. If $x,y \in S(q_k)$ and $(\sqrt{x})_R < (\sqrt{y})_R$, then $x < y$.

Proof. Property 1. follows immediately since the γ_i were chosen to be those elements for which $\sqrt{\gamma_i} \in S(q_k)$. For property 2., let $\gamma_i = \min_{\gamma \in \Gamma(q_k)} \gamma \geq x$. Then $\gamma_{i-1} < x \leq \gamma_i$, and $(\sqrt{x})_R = \gamma_i$. Since $y \geq x$ we know that either $x \leq y \leq \gamma_i$ or $y > \gamma_i$. If $x \leq y \leq \gamma_i$, then $(\sqrt{x})_R = (\sqrt{y})_R = \sqrt{\gamma_i}$. If $y > \gamma_i$, then $(\sqrt{y})_R = \sqrt{\gamma_j}$ where $\gamma_j > \gamma_i$; hence, $x \leq y$ implies $(\sqrt{x})_R \leq (\sqrt{y})_R$. For property 3., let $\sqrt{\gamma_i} = (\sqrt{x})_R$ and $\sqrt{\gamma_j} = (\sqrt{y})_R$. Since $(\sqrt{x})_R < (\sqrt{y})_R$, we have $\gamma_i < \gamma_j$. We also have $\gamma_{i-1} < x \leq \gamma_i$ and $\gamma_{j-1} < y \leq \gamma_j$. Now, $\gamma_i < \gamma_j$ implies $\gamma_i \leq \gamma_{j-1}$; hence $x \leq \gamma_i \leq \gamma_{j-1} < y$ and $x < y$.

Note that $(\sqrt{x})_R \leq (\sqrt{y})_R$ does not imply $x \leq y$.

Theorem (9). Let $x, x^2 \in S(q_k)$ with $x \neq 0$. Then $(\sqrt{x^2 - y})_R = x$ if and only if $y \in [0, 2x - 2]$ (here $[\ ]$ has usual definition).

Proof. If $(\sqrt{x^2 - y})_R = x$, then $(x - 1)^2 < x^2 - y \leq x^2$. This implies that $y \in [0, 2x - 2]$. Conversely, assume $y \in [0, 2x - 2]$. Since $(x - 1)^2 = x^2 - (2x - 1) < x^2 - y \leq x^2$, we have $x = (\sqrt{x^2 - y})_R$.

Theorem (10). $\forall\, x \in S(q_k)$, $[(\sqrt{x})_R]^2 \geq x$.

Proof. Let $\sqrt{\gamma_i} = (\sqrt{x})_R$. Then, if $x \neq 0$, $\gamma_{i-1} < x \leq \gamma_i = (\sqrt{\gamma_i})^2 = [(\sqrt{x})_R]^2$. If $x \equiv 0$, the theorem is obvious.

Theorem (11). $\forall\, x, y \in S(q_k) \ni xy \in S(q_k)$, $(\sqrt{xy})_R \leq (\sqrt{x})_R (\sqrt{y})_R$.

Proof. Let $\sqrt{\gamma_i} = (\sqrt{x})_R$ and $\sqrt{\gamma_j} = (\sqrt{y})_R$. Then, if $x \neq 0$, $y \neq 0$, $\gamma_{i-1} < x \leq \gamma_i$ and $\gamma_{j-1} < y \leq \gamma_j$. Hence, $\gamma_{i-1}\gamma_{j-1} < xy \leq \gamma_i \gamma_j$. Therefore, $(\sqrt{xy})_R \leq \sqrt{\gamma_i \gamma_j} = \sqrt{\gamma_i}\ \sqrt{\gamma_j} = (\sqrt{x})_R (\sqrt{y})_R$. Once again, if $x \equiv y \equiv 0$, the theorem is obvious.

8. EMBEDDING

If we wish to find another problem that gives a "better" answer to replace Problem (1), we must expand our field by embedding $GF(p_k)$ in a field $GF(p_{k'})$ where $k' > k$. Because of its greater richness $GF(p_{k'})$ can provide substitute problems that "more closely approach" Problem (1).

Let us choose $p_{k'}$ such that $p_{k'}/p_k = 100 + R$ where $R > 0$. Then we shall identify every 100^{th} element (up to $100q_k$) of $S(q_{k'})$ with the elements of $S(q_k)$, i.e. if $x' \in S(q_{k'})$ and if $x' \equiv 0 \pmod{100}$, then $\exists\, x \in S(q_k) \ni x \to x'$. Now we can pose Problem (1′) which is to find $\sqrt{x'} \in S(q_{k'})$, $(x' \leftarrow x \in S(q_k))$. Again replace Problem (1′) by finding $\gamma_{i'} \in \Gamma(q_{k'}) \ni \gamma_{i-1} < x' \leq \gamma_i$. Again introduce the replacement problem and a soluable problem in $GF(p_{k'})$. Then, using the relation $x \to x'$, we associate a solution, say γ_i, with Problem (1) by the decimal version of $\frac{\gamma_i}{10}$. And if greater resolution is sought repeat this process to $GF(p_{k''})$, etc.

Example. $S(11) = \{0,1,2,\ldots,9\}$. Find $\sqrt{7}$. Replacement problem yields $(\sqrt{7})_R \to 3$. Go to richer field with $S(1109)$. Then $676 < 700 < 729 \Rightarrow (\sqrt{7})_R \to 2.7$.

In this way we have established a procedure that serves to define acceptable square roots to within any desired "resolution" or order of refinement. Let us point out that embedding is a form of replacement and the identification of 1.0 with 1.00 is a matter of pure and arbitrary convention. We could—in principle—associate 1.0 with any number, say 6.25, but that would violate standard practice. The only theoretical requirement is that every element in the coarse field be mapped nonabiguously onto an element of the finer field.

9. ALTERNATIVE REPLACEMENT TECHNIQUE

Instead of "rounding up" as we have done, one could "round to closest neighbor." This changes the form of the theorems and the triangle inequality is lost; however, there are certain aspects that are quite desirable. In this section, we shall just present the definition.

Let $x \in S(q_k) \ni x \notin \Gamma(q_k)$. Then $\exists\, i \in \{0,1,\ldots,n-1\} \ni \gamma_i < x < \gamma_{i+1}$. Form the differences $d^+ = \gamma_{i+1} - x$ and $d^- = x - \gamma_i$. Clearly d^+ and $d^- \in S(q_k)$ so are unambiguously comparable with our order relation. Let us designate the replacement square root of x by $(\sqrt{x})_R$. Then, the following will serve as the definition of $(\sqrt{x})_R$. Let $\sqrt{x}$ designate the positive Galois field square root.

Definition. If $d^+ > d^-$, then $(\sqrt{x})_R = \sqrt{\gamma_i}$; if $d^+ < d^-$, then $(\sqrt{x})_R = \sqrt{\gamma_{i+1}}$.

Since $(N + 1)^2 - N^2 = 2N + 1$, there can be no $x \in S(q_k)$ such that $d^+ = d^-$ and we have an unambiguous formulation. If $x \in \Gamma(q_k)$, then $(\sqrt{x})_R = \sqrt{x}$.

In the subsequent development we shall restrict our attention to the computationally simple "rounding up". However, we must first demonstrate that this choice does not unnecessarily prejudice the conclusions. Thus let us show that the three possible replacement techniques lead to essentially equivalent results.

See Appendix I.

10. GALOIS FIELD GEOMETRY

A vector space defined over a Galois field[12] cannot have an inner product with all of the customary properties because of the lack of transitive order in GF(p). However we shall generalize this notion to what will be called a Galois product in the hopes of introducing a concept of direction.

Definition (3). Let V be a vector space of columns defined over GF(p). Let $[x,y] = x^T y$ define a Galois product $\forall\, x, y \in V$. If $[x,y] \equiv 0$ we shall call x,y orthogonal.

Theorem (12). The Galois product satisfies the following conditions:

1. $[x,y] \in GF(p) \quad \forall\, x,y \in V$;
2. $[x,y] = [y,x] \quad \forall\, x,y \in V$;
3. $[x,\alpha y + \beta z] = \alpha [x,y] + \beta [x,z] \quad \forall\, x,y,z \in V, \forall\, \alpha,\beta \in GF(p)$.

Proof.

Let $x = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$, $y = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$, $z = \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{bmatrix}$ where

the α_i , β_i , $\gamma_i \in GF(p)$. Then $[x,y] = \sum_{i=1}^{n} \alpha_i \beta_i$, etc. Hence 1. follows from closure of GF(p) under multiplication and addition. Similarly 2. follows from commutativity of multiplication in GF(p). Finally 3. follows since multiplication is also distributive in GF(p).

Let us now study the relationships between linear independence and the Galois product.

Theorem (13). If $[x,x] \not\equiv 0$ and $\alpha x \equiv y$, $\alpha \not\equiv 0$ where $x,y \in V$ and $\alpha \in GF(p)$, then $[x,y] \not\equiv 0$. Thus linear dependence implies a nonzero Galois product.

Proof. $[x,y] \equiv [x,\alpha x] \equiv \alpha[x,x] \not\equiv 0$.

Theorem (14). If $[x,y] \equiv 0$ and $[x,x] \not\equiv 0$, $[y,y] \not\equiv 0$, $x,y \in V$, then x and y are linearly independent.

Proof. Let us seek two scalars $\alpha,\beta \in GF(p)$ such that $\alpha x + \beta y \equiv 0$. Operate on this equation with x^T to obtain $\alpha x^T x + \beta x^T y \equiv \alpha [x,x] + \beta [x,y] \equiv \alpha [x,x] \equiv 0$. Hence, since $[x,x] \not\equiv 0$, $\alpha \equiv 0$. Operate similarly with y^T to find $\beta \equiv 0$. Therefore x and y are linearly independent.

11. NORM AND METRIC

Let us now combine the above results and define a region over which an inner product and norm can be identified. Let $E(q_k) = \text{Toss}\ (0, q_k)$ be the transitive ordered subset of GF(p). Let V be an n-dimensional vector space defined over GF(p). Define a subset of $E(q_k)$ as

$$F(q_k) = \{\alpha: \alpha \in E(q_k) \text{ and } n\alpha^2 < q_k\}.$$

Define a region of V by

$$F = \{x: x \in V,\ x = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix},\ \alpha_1, \alpha_2, \ldots, \alpha_n \in F(q_k)\}.$$

<u>Theorem (15)</u>. $\forall\ x \in F,\ [x,x] \geq 0;\ = 0$ iff $x = 0$.

<u>Proof</u>. Let $x = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$; $\alpha_1, \alpha_2, \ldots, \alpha_n \in F(q_k)$. Then we have

$[x,x] = \sum_{i=1}^{n} (\alpha_i)^2$. Let $F^+(q_k) = \{\alpha: \alpha \in F(q_k) \text{ and } \alpha \geq 0\}$.

Clearly $(\alpha_i)^2 \in F^+(q_k)$ $(i = 1,2,\ldots,n)$. Since $n(\alpha_i)^2 < q_k$, the sum of $\sum_{i=1}^{n} (\alpha_i)^2$ is still in $F^+(q_k)$, i.e. transitivity holds and we can sum the inequalities $0 \leq n(\alpha_i)^2 < q_k$ to obtain the theorem.

The set F is not a subspace of V because it is not closed under vector addition or scalar multiplication. Thus when formulating certain theorems additional restrictions are needed to insure that operations do not carry beyond the limits of F into the set V-F. Thus, for example, the condition $[\alpha x,x] = \alpha[x,x]$ is valid over V and GF(p) but the condition $[\alpha x,\alpha x] \geq 0$ is valid only for those $\alpha \in GF(p)$, $x \in F \ni \alpha x \in F$.

Theorem (16). If $\alpha \in GF(p)$, $x \in F$ and $\alpha x \in F$, then $[\alpha x,\alpha x] \geq 0; \equiv 0$ iff $x = 0$ or $\alpha = 0$.

Proof. Follows immediately from Theorem (1) with αx replacing x.

Theorem (17). If we restrict ourselves to operations involving elements of F that do not produce results out of F, then the Galois product becomes an inner product over F.

Proof. From Theorem (12), we know that the Galois product satisfies all but the condition that $(x,x) \geq 0, = 0$ iff $x = 0$ of the definition of an inner product. Theorems (15) and (16) insure that this condition is also satisfied.

Let $H(q_k) = \{\alpha: \alpha \in E(q_k)$ and $4n^2\alpha^4 < q_k\}$.

Let $H = \{x: x \in V , x = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix} , \alpha_1,\alpha_2,\ldots,\alpha_n \in H(q_k)\}$.

Theorem (18). If $x,y \in H$, then $[x,y]^2 \leq [x,x][y,y]$.

Proof. Let $x = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix}$, $y = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{bmatrix}$, $\alpha_i,\beta_i, \in H(q_k)$ $(i = 1,2,\ldots,n)$.

We have that $0 \leq \sum_{i=1}^{n} \sum_{j=1}^{n} (\alpha_i \beta_j - \alpha_j \beta_i)^2$. This inequality holds because by the definition of $H(q_k)$, each term is nonnegative and their sum stays within $E(q_k)$. We may expand this inequality to obtain

$$\left[\sum_{i=1}^{n} \alpha_i \beta_i\right]^2 \leq \sum_{i=1}^{n} (\alpha_i)^2 \sum_{i=1}^{n} (\beta_i)^2.$$

In terms of x and y, this is equivalent to $[x,y]^2 \leq [x,x]\,[y,y]$.

Theorem (19). If $x,y \in H$, then $[x,y] \leq (\sqrt{[x,x]})_R\ (\sqrt{[y,y]})_R$.

Proof. From theorems (8), (9), and (18), we find $[x,y] \leq (\sqrt{[x,x][y,y]})_R$ and from theorem (8) $(\sqrt{[x,x][y,y]})_R \leq (\sqrt{[x,x]})_R\ (\sqrt{[y,y]})_R$.

Definition (.4). Define a mapping from F into GF(p) as follows: $\forall\ x \in F$, $\| x \| = (\sqrt{[x,x]})_R$.

Theorem (20). $\| x \| \geq 0$; $\equiv 0$ iff $x \equiv 0$, $\forall\ x \in F$.

Proof. The proof follows from theorem (15) and the definition of $(\sqrt{\ })_R$.

Theorem (21). $\| \alpha x \| \geq | \alpha | \cdot \| x \|$ $\forall\ x \in F$, $\forall\ \alpha \in GF(p)\ \ni\ \alpha x \in F$.

Proof. $\| \alpha x \| = (\sqrt{[\alpha x, \alpha x]})_R = (\sqrt{\alpha^2 [x,x]})_R \geq (\sqrt{\alpha^2})_R\,(\sqrt{[x,x]})_R$

$= | \alpha | \cdot \| x \|$.

Theorem (22). $\forall\ x,y \in H\ \ni\ x + y \in F$, $\| x + y \| \leq \| x \| + \| y \|$.

Proof. $(\| x \| + \| y \|)^2 = (\sqrt{[x,x]})_R + (\sqrt{[y,y]})_R^2 + 2(\sqrt{[x,x]})_R\,(\sqrt{[y,y]})_R$

Theorem (10) $\Rightarrow$ $\geq [x,x] + [y,y] + 2(\sqrt{[x,x]})_R\,(\sqrt{[y,y]})_R$

Theorem (11) $\Rightarrow$ $\geq [x,x] + [y,y] + 2(\sqrt{[x,x][y,y]})_R$

Theorem (18) $\Rightarrow$ $\geq [x,x] + [y,y] + 2(\sqrt{[x,y]^2})_R$

Theorem (9) $\Rightarrow$ $= [x,x] + [y,y] + 2[x,y]$

$= [x+y, x+y]$.

Therefore, $(\| x \| + \| y \|)^2 \geq [x+y, x+y]$ which implies--from theorem (8) that

$$(\sqrt{(\|x\| + \|y\|)^2})_R \geq (\sqrt{[x+y, x+y]})_R .$$

From theorem (9) and definition (4), we have

$$\| x \| + \| y \| \geq \| x + y \|.$$

Definition (5). Let $\rho(x,y) = \| x - y \|$ $\forall\, x,y \in F \ni x-y \in F$.

Theorem (23). 1. $\rho(x,y) \geq 0$; $\equiv 0$ iff $x \equiv y$.

2. $\rho(x,y) = \rho(y,x)$

Proof. Property 1. follows immediately from theorem (20) with $x - y$ identified with x. Property 2. follows since $\rho(x,y) = \| x - y \| = (\sqrt{[x-y, x-y]})_R = (\sqrt{[y-x, y-x]})_R = \rho(y,x)$.

Theorem (24). $\rho(x,y) + \rho(y,z) \geq \rho(x,z)$ $\forall\, x,y,z \in H \ni x - y,$ $x - z,\ y - z \in H$.

Proof. We shall use the results of theorem (22). $\rho(x,z) = \| x - z \| = \| x - y + y - z \| \leq \| x - y \| + \| y - z \| = \rho(x,y) + \rho(y,z)$.

Thus we see that $\rho(x,y)$ satisfies the definition of a metric over the set H.

12. ROTATION

In addition to the basic metrical properties of geometry that have already been presented, we shall seek a mechanism for generating a concept of rotation. There has been prior work in this direction, generally by introducing finite groups of transformations that preserve some appropriate quadratic form 13. For example, if dealing with a four-dimensional space, one can introduce a metric tensor of the form

$$g = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} ; \qquad 0,1 \in GF(p)$$

and define a bilinear form $x \cdot y = x^T g y$. This is in direct analogy with the conventional formalism of modern physics. However, this procedure does not directly consider the problem of interpretability, especially that associated with the ordered subsets that play such an important role in our development of finite geometry. Hence we impose an additional condition that a subset of all such transformations be found that transforms vectors from $F(q_k)$ into vectors of $F(q_k)$ (we might further restrict to $H(q_k)$, depending on the context).

We have devised a finite algorithm that generates transformations that "rotate" vectors of the ordered grid into other such vectors.[14] Since it is a constructive procedure, it offers immediate insight into the structure and consequences of a finite and discrete geometry.

The rotation technique consists of adjoining integer sided right triangles[15] about some common vertex so that the hypoteneuse of one and a leg of the other are colinear. The common vertex is generally considered

to be the origin. If the triangles are suitably chosen, then the vertices are always realized at points of the discrete grid. Clearly this is a necessary condition. In order to guarantee that this is satisfied, one must have the grid sufficiently rich, i.e. with sufficiently many points. The adjunction is viewed conceptually as being performed via successive embedding in richer, i.e. more "closely" packed fields. Thus, if h is the number of counts of the hypotenuse of the first triangle as seen in field F^1, then this same "segment" should be h^n counts when referred to the field F^n which is required after n adjunctions. In other words, we require an ever richer field to perform every subsequent rotation. By repeated application of this procedure, we may generate rational expressions of arbitrary rotations. If we let our "unit" triangle be thin, i.e. if the ratio of the legs is small, then we can approach any "angle" of ordinary rotation by repeated adjunction of this one triangle. In this case when the same triangle is used, then the sum of the squares of the coordinates, when referred to the richest field, is a conserved quantity. This case fits into the format of the above described systems. Hence we have generated a subset of the formal and global definitions of rotation. As has so often happened in the development of finite field geometry, one can introduce interpretable objects locally, not globally.

Another interesting and potentially far-reaching point to mention is the following. It is found that each successive adjunction requires a richer field if one is to refer the results back to the original orientation. Obviously, this process can continue only so long before one exhausts his capacity to further enrich the field. At this stage, one must either cease or drop the requirement of remembering exactly what the original orientation was. In the latter case, one can either eliminate the record of the original state entirely or introduce a probabilistic formulation that enables one to go further, although without a deterministic description. The probabilistic method does enable one to further extend his capabilities. However, both solutions ultimately lead to complete renunciation of strict determinism in description; hence, the predictative capability is likewise lost. It is conjectured that this failure to achieve a purely and exhaustively deterministic description might be the source of the quantum mechanical behavior so well known in the realm of atomic phenomena.

When the numerical capacity is exceeded, there are ways to retain some control and information by reducing the resolution requirements. This can be done by introducing a hierarchy of counting that no longer carries the lowest decimal. For example, an automobile odometer can register more than 10^5 miles if, after reaching 99,999, we change the gear ratio by a factor of ten. We forgo knowledge of the tenths place but obtain capacity to count hundred thousands. And this hierarchical embedding can be repeated.

13. MATHEMATICAL INDUCTION AND PASSAGE TO THE LIMIT

One of the many implications of the local ordering concept is the distinction between "for any" and "for every." We can declare an origin at any point in the space and do geometry locally; however, this does not imply that we can do geometry at every point referred to this one origin. Mathematical induction asks if the validity of $P(n + 1)$[16] follows from the assumed validity of $P(n)$ and the demonstrable validity of $P(1)$ $P(n)$ assumed true and implying the validity of $P(n + 1)$ is a local

demonstration that can be performed anywhere, i.e., at any n. However, from this local property the conventional assumption is global validity. On the other hand, since this entire process is highly similar to our local order concept, we are led to inquire whether mathematical induction is also limited by the local vs. global distinction. If so, then the principle of mathematical induction must be reevaluated to incorporate the results of a local ordering relation in a finite field.

We have found that any demonstration (from the finite context of the view taken in this paper) of the validity of mathematical induction requires an additional axiom regarding the existence of a "continuous" field. This is consistent with the findings in the early 20th century about the necessity of an axiom of infinity.[17]

In order to develop these ideas more fully, we must first examine an extralogical requirement.

This paper begins with a primitive commitment to finitism and we have attempted to demonstrate the theoretical possibility of performing certain operations wholly within a finite context. Now we must invoke another primitive commitment and can only briefly motivate its introduction. Procedural invariance is an extralogical requirement (see reference 18) that is essentially a generalization of the Einstein principle requiring invariance of physical laws under appropriate transformations. A rational system that leads to a prediction or prescription that is not invariant under the arbitrary procedures of analysis and computation is inherently ambiguous, i.e., the system should not have its results depend upon the computational path that is chosen. The choice of convention should not determine the answer. If it does then

the results cannot be unique. In general, the preservation of consistency under alternative, arbitrary procedures is a categorical requirement, i.e., a system which does not preserve consistency under arbitrary procedural convention is a fortiori inadmissible as a rational paradigm.

We shall now consider "passage to the limit" and mathematical induction to see what effects the demand for procedural invariance brings. In general, there are different limiting procedures that are not in agreement because a discrete grid, no matter how fine, is qualitatively different from a continuous line. There is no gradual transition which transforms all of the properties of the finite system smoothly into the properties of a continuous system; some of the properties of the continuum appear abruptly only when the embedding reaches the ultimate transfinite stage.

Consider three alternative conventions to govern mathematical induction. Let $P(n_p,p)$ be a proposition that is consistent with a set of axioms, G, where $n_p \in GF(p)$. Let $n_{max}(p)$ denote the largest count in GF(p), i.e., starting with 1, $n_{max}(p)$ is the element such that the successor to $n_{max}(p)$ is zero, i.e., p - 1. Let $n_{max}(Toss(p))$ be the number of elements or size of Toss(p). We shall look at $P(n_p,P)$ as n_p and p increase.

(I) Conventional or Customary Mathematics: Let $p \to "\infty" \Rightarrow \forall p$, $n_p < n_{max}(Toss(P))$. This corresponds to the construction of a continuum by indefinite embedding and generates a countably infinite set of trantitively ordered numbers.

The validity of the proposition P is then investigated by conventional logic in the context of continuous space. This procedure generates the well-known (and sometime counter intuitive) results of mathematics.

(II) Fixed Cognitive Agent: Keep $n_p \in GF(p)$ but let $n_p > n_{max}(Toss(p))$. In this case induction on $P(n_p,p)$ leads to results which are not interpretable within the context of the fixed cognitive agent i.e., the results are relatively indeterminably and chaotic. We describe this result by $P(n_p,p) \rightarrow X$ where X is some unexpect d proposition not necessarily consistent with G.

(III) Indefinite Finite Embedding: Let n_p and p increase so that $n_p \in Toss(p)$; then perform induction. In this case the resultant proposition is determinable and consistent with G. Unfortunately, this procedure is limited to the resources that can generate ever larger p's. Hence, when the "largest" p is reached, i.e., when the capacity of the system is exhausted, then case (III) → case (II). We observe that prediction in any substantive system (including that of the physical universe) ultimately exhausts its numerical resource.

Of these procedures, case (I) is the conventional one; case (II) is more appropriate to any actual finite system, and case (III) is arbitrarily constrained to remain within system of adequate numerical resources and thereby investigate only the determinable properties of mathematics.

Illustrative Examples

Example A: Convergence to a Point

Consider the function $P(m) = 1/m$. We desire to define the limiting process designed by

$$\lim_{m \to} P(m),$$

where $m \to$ indicates that m increases under that appropriate condition of the respective procedure.

Under procedure I we have

$$\lim_{m \to \infty} P(m) = 0;$$

Under procedure III we have a two-stage process

$$\lim_{m \to n(\text{Toss}(p))} P(m) = \epsilon(p)$$

$$\lim_{p \to} \epsilon(p) = \delta > 0$$

We note that δ moves arbitrarily close to zero i.e., $\delta < \frac{1}{M}$, where M is any number from any Toss(p); however great.

We may say that "δ convergences toward zero" and may be made to lie within any arbitrarily small neighborhood of zero, i.e., the limit is not a member of the sequence (cf. definition of a Banach Space and the closure requirement).

Under procedure II

We execute the first stage as above in procedure II; then carry the limiting process through the transitivity ordered numbers:

$$\lim_{n \to n_{max}(\text{Toss}(p))} p(m) = \epsilon\,(n_{max})$$

During the limiting process ϵ (n) decreases to a minimum value $1/n_{max}(\text{Toss}(p))$. Next we execute the second stage by replacing n by the successors.

Then "increase" $n_{max}\text{Toss}(p))$ by successive steps defined by the process:

$$n' = n + 1$$

Since n + 1 and subsequent numbers are outside of Toss(p), ϵ (n′) suddenly escapes the neighborhood of zero. If limited to the numerical resources of a fixed Toss(p) of GF(p) the value of ϵ (n′) is undeterminable and may be any number. Here the limiting process, as n increases, behaves in a determinable manner and the value is restricted to a smoothly decreasing neighborhood until n exceeds n_{max}. The value then takes on unpredictable values including some of which are not interpretable.

Example B: Relativistic Properties of a Random Walk in Finite Space*

Consider a one-dimensional discrete space and a point executing a random walk. The probability of moving one space position to a contiguous position of higher index is p, converse q, p + q = 1. Let k designate the index of the point, and let n be the number of steps. Let P(k,n) be the probability that the point is at the k^{th} position after the n^{th} transition.

---

* This example is taken from an earlier work by one of us (NMS) reference 19 and is a simplified version of a more general viewpoint in which the embedded discrete space points are implicit. In order to preserve consistence under a velocity formation it was demonstrated in the reference that it was necessary to introduce an imaginary component of transition probability in order to achieve 6-dimensional rotational transformations (one time dimension for each space dimension). The resulting transformation was shown to be the Lorentz-Fitzgerald transformation of relativistic physics.

Given

$$P(0,0) = 1, \text{ we may show that}$$

$$P(n,k) = \begin{bmatrix} \frac{n+k}{2} \\ \frac{n-k}{2} \end{bmatrix} p^{\frac{n+k}{2}} q^{\frac{n-k}{2}} \; ; \; \sum_k P(n,k) = 1,$$

is a binomial distribution which extends $\pm$ n either side of k = 0.

We may also show that the first moment, $\bar{k} = \Sigma k P(k,n)$ is:

$$\bar{k} = n(p - q); \tag{1}$$

and that the variance is

$$\sigma^2(k,n) = \sum_k (k - \bar{k})^2 = 4npq. \tag{2}$$

Furthermore, since p - q = constant $\equiv \beta$ and p + q = 1, we have

$$\sigma^2(k,n) = n(1-\beta^2); \tag{3}$$

the ratio of $\sigma(k,n)$ for $\beta \neq 0$ to $\sigma_{00}(k,n)$ for $\beta = 0$ is

$$\frac{\sigma}{\sigma_{00}} = (1-\beta^2)^{\frac{1}{2}}. \tag{4}$$

We interpret the transition to result in the change of one space quanta and the corresponding time to change one time quanta. In terms of measures from some much finer embedding, one space quanta represents a change in a distance of Δ, and of time, τ. The mean position of the point is given by

$$\bar{x} = \bar{k}\Delta = n\beta\Delta$$

and the time t, by

$$t = n\tau.$$

The speed of the expected position, v, is given by

$$v = \frac{\bar{x}}{t} = \frac{\beta\Delta}{\tau} \; ; \text{ and } \sigma^2(x) = n(1-\beta^2)\Delta^2.$$

The random walk exhibits relativistic properties, under the interpretation that $\bar{k}$ determines the position of $P(k,n)$ and that σ determines its size. We note that the speed is limited to a maximal quantity, and that the size contracts in the direction of motion as in the Lorentz-Fitzgearld contraction. The maximum velocity, v_{max}, is given by

$$\beta = 1, \text{ i.e., by } v_{max} \equiv c = \frac{n\Delta}{n\tau} = \frac{\Delta}{\tau}$$

and the size, σ, becomes 0 at $\beta = 1$ for all n.

We now examine these relativistic properties as the embedding of finite spaces becomes a continuum by permitting $\Delta \to 0$. This is not a uniquely determinable procedure. We can at most, preserve three properties (since P is a function of k, n, and β) of the distribution, $P(k,n)$. It is not possible to preserve all of its properties. The properties we select for presentation are:

(a) the "size" σ is maintained finite and nonzero;

(b) the time measure (and space measure) are held constant, and

(c) the speed v, is held constant.

Condition (a) is satisfied if for $\sigma^2 = n\Delta^2(1-\beta^2)$ we require $n\Delta^2 = n_0\Delta_0^2$ (where the subscript refers to the values in the initial discrete space).

From above we have

$$n = \frac{n_0\Delta_0^2}{\Delta^2} \qquad (A)$$

From condition (b) we have $t = n\tau = n_0\tau_0 = \text{const.}$ On combining with Condition(a) we have

$$\tau = \frac{\tau_0\,\Delta^2}{\Delta_0^2}. \qquad (B)$$

From condition (c) we have

$$v = \frac{\beta\Delta}{\tau} = \frac{\beta_0\Delta_0}{\tau_0} = \text{const} = \frac{\beta}{\beta_0}\frac{\Delta_0}{\Delta}\frac{\beta_0\Delta_0}{\tau_0} = \frac{\beta}{\beta_0}\frac{\Delta_0}{\Delta}\, v$$

or

$$\frac{\beta}{\beta_0}\frac{\Delta_0}{\Delta} = 1,$$

$$\beta = \beta_0\frac{\Delta}{\Delta_0}. \quad (c)$$

We now let $\Delta \to 0$, having required v and t to remain constant.

$$\lim_{\Delta \to 0} \beta = 0$$

$$\lim_{\Delta \to 0} \sigma = n_0\Delta_0^2 = \sigma_{00}$$ (i.e., the initial standard deviation for $\beta = 0$, i.e., zero velocity).

$$\lim_{\Delta \to 0} c = \lim_{\Delta \to 0}\frac{\Delta}{\tau} = \lim_{\Delta \to 0}\frac{\Delta_0^2}{\tau_0\Delta} = \infty .$$

We note that the Lorentz-like contraction is lost; that the maximum velocity increases without bound—in short, that the natural relativistic properties of the discrete space are lost in going to the continuum as a limiting process. Having destroyed these formal properties in going to the continuum, we may reintroduce them as additional restraints appropriate to the substantitive problem encountered. For example, in the special theory of relativity one imposes the constancy of the velocity of light. The point made herein is that this property is a natural formal property of the discrete space—and that finite cognitive agents are constrained to cognize in the context of discrete spaces. Hence any admissible model of substantive finite space will, perforce, have the relativistic properties.

Example C: Numerousness of the Even, Odd Numbers

In conventional number theory following process I it is shown that the even (odd) numbers are equally as numerous as the transtitive-ordered set of all numbers.

Following procedure III we note that for any finite model of size n the evens are as numerous as $\frac{n}{2}$, n even (or as $\frac{n-1}{2}$ if n is odd) and the odds as numerous as $\frac{n}{2}$, n even or $\frac{n+1}{2}$, n odd. As n is increased this ratio of evens to n remains, or converges toward $\frac{1}{2}$—for any n. Thus the limiting ratio is not one of equally numerous to the total set of integers (unless one maintain that $\frac{1}{2}$ of ∞ is "as numerous" as ∞).

Procedure II conforms to procedure III until $n_{max}(\text{Toss}(p))$ is exceeded—at which time the odds and evens appear in random order and statistically the ratio becomes one-half.

Example D: Trisecting the Angle

In conventional geometry it is agreed that by using an idealized compass and ruler, any given angle may be bisected, but that it is not possible to trisect an angle. It is explicitly forbidden, under the terms of the exercise, to permit infinitc interative algorithms even though they may converge to a trisection of an angle. However, by the nature of the exercise, an infinite algorithm has been implicitly admitted by the supposition that one may place the idealized point of the compass exactly on top of a given point on the idealized paper. One can devise algorithms which enable one point to be placed within any ϵ-neighborhood of a given point with a finite number of operations; however, they are of the nature explicitly forbidden.

The result of these observations is that if infinite procedures are ruled out an angle can neither be bisected nor trisected. On the other hand, if infinitely converging algorithms are admitted, then one may construct, within any tolerable variance, the bisected and the trisected angle. Under procedure III, the variance is decreased indefinitely. Under procedure II [and the ultimate fate of procedure III] the variance can be decreased progressively until the transitively ordered numbers are exhausted; further operations result in random results added to the initial determinable results.

The behavior of determination under case II is more nearly in conformity to actual physical behavior. We are led to surmise that this property—as a natural property of these finite spaces—may be more appropriately associated with the finiteness of the finite cognizing agent itself.

One may regard procedure III as an interim one admitting of embedding one finite field in a larger one (i.e., greater p) in such a manner as to preserve pro tem the determinable character of calculation. This process may be iteratively advanced until some secondary requirement is met (i.e., the uncertainties are balanced or the error is admissible)—or until the process must halt for lack of additional numerical resources. Procedure II identifies the resulting characteristic when such resources are exceeded—and any fixed system must necessarily sooner or later face the consequent introduction of indeterminancy (i.e., all systems are finite).

The use of continuous mathematics to represent finite space-time under the problem conditions imposed here is admissible as an expedient only if it is kept in mind that (1) some inconsistency may inadvertently be introduced, and (2) it may be necessary to introduce additional side

constraints ostensibly as "properties" of the substantive problem in order to preserve some of the characteristics of the finite spaces which have been lost in the conventional limiting processes (e.g., the constant finite speed of light in vacuo).

If one does not admit the existence of a continuous space, even as an additional axiomatic input, he is led to define a concept "infinity" and a "limit" in terms of algorithms which are in every case necessarily truncated by limiting the sequential process to a finite number of operations. Statements about the continuum are then shorthand statements of more exactly definable finite procedures. Some such statements are inadmissible (e.g., "all complex numbers have square roots").

Let us also point out that there are profound generic differences between finite fields and infinite fields and the one does not gradually grow into the other. So long as a field is finite, no matter how large p becomes, it is categorically different from an infinite set. The transition occurs not during the finite approach to the limit, but abruptly "over the horizon" when the limit is reached (e.g., the relative numerousness of evens and odds cannot be understood via a gradual transition from finite to infinite sets). Thus, we must reexamine our understanding of limits, etc., in light of these results. We as finite cognitive agents, are constrained to reach all of our conclusions by finite procedures. Hence, since we can infer an infinite set as a finite sequence of finite sets, one must ask about the status of these infinite sets. Or, if we assume their existence, how do we work with them since they are not finitely attainable or realizable?

APPENDIX I

Given $x \notin \Gamma(q_k)$ we know there exist two perfect squares between which x lies, say

$$(N_0)^2 < x < (N_0 + 1)^2 . \qquad (1)$$

Hence $(\sqrt{x})_R$ will equal N_0 or $N_0 + 1$, depending on whether we assume round-up, round-down, or round nearest. To increase resolution, we may add a decimal place to the root by forming

$$(\sqrt{x})_R \to \frac{1}{10} (\sqrt{100x})_R . \qquad (2)$$

Now, inequality (1) implies

$$100(N_0)^2 < 100x < 100(N_0 + 1)^2 . \qquad (3)$$

Theorem (1). There are nine perfect squares between $100N^2$ and $100(N + 1)^2$, not counting the end points.

Proof. Consider $[10N + \alpha]^2$ where α is a nonnegative integer. Clearly $[10N + \alpha]^2 \in [100N^2, 100(N + 1)^2]$ for $\alpha \in [0,10]$.

Using Theorem (1) on inequality (3), we see that 100x lies between two perfect squares as follows:

$$(10N_0 + \alpha_1)^2 < 100x < (10N_0 + \alpha_1 + 1)^2 \qquad \alpha_1 \in [0,9] \qquad (4)$$

Let us define $N_1 = 10N_0 + \alpha_1$ and rewrite (4) as

$$(N_1)^2 < 100x < (N_1 + 1)^2 \qquad (4)'$$

Let us now consider still another embedding which requires

$$100(N_1)^2 < 10^4 x < 100(N_1 + 1)^2 . \qquad (5)$$

As before, we use Theorem (1) to find $\alpha_2 \in [0,9]$ such that

$$(10N_1 + \alpha_2)^2 < 10^4 x < (10N_1 + \alpha_2 + 1)^2 \tag{6}$$

and so forth. After n embeddings we have

$$(N_n)^2 < 10^{2n} x < (N_n + 1)^2 \tag{7}$$

where $N_n = 10N_{n-1} + \alpha_n = 10(10N_{n-2} + \alpha_{n-1}) + \alpha_n$

$$= 10(10[10N_{n-3} + \alpha_{n-2}] + \alpha_{n-1}) + \alpha_n$$

$$= 10^n N_0 + \sum_{i=0}^{n-1} 10^i \alpha_{n-i} \ . \tag{8}$$

Define $$(\sqrt{x})_{R_n} = \frac{1}{10^n} (\sqrt{10^{2n} x})_R \ . \tag{9}$$

Clearly $(\sqrt{10^{2n} x})_R \in [N_n, N_{n+1}]$ holds for any of the three replacement alternatives.

Thus from Equation (9) we obtain

$$(\sqrt{x})_{R_n} \in \left[\frac{N_n}{10^n} , \frac{N_n + 1}{10^n}\right] \ . \tag{10}$$

From Equation (10) we obtain by squaring that

$$\left((\sqrt{x})_{R_n}\right)^2 \in \left[\left(\frac{N_n}{10^n}\right)^2 , \left(\frac{N_n + 1}{10^n}\right)^2\right] \tag{11}$$

Define $$\left[\left(\frac{N_n}{10^n}\right)^2 , \left(\frac{N_n + 1}{10^n}\right)^2\right] = \Delta_n \ . \tag{12}$$

From inequality (7) we find

$$x \in \Delta_n \tag{13}$$

Consider the length of Δ_n, viz. $|\Delta_n|$. We have

$$|\Delta_n| = \frac{2N_n + 1}{10^{2n}} = \frac{2\left(10^n N_0 + \sum_{i=0}^{n-1} 10^i \alpha_{n-i}\right) + 1}{10^{2n}} \ . \tag{14}$$

Thus for large n, $|A_n|$ behaves according to $2R_0/10^n$. In the limit as $n \to \infty$, $|A_n|$ becomes infinitesimal and we represent this symbolically as

$$\lim_{n \to \infty} |A_n| = 0 \quad . \tag{15}$$

From Equations (11) and (13), we see that both x and $((\sqrt{x})_{R_n})^2$ are in A_n and from (15) we see that $|A_n| \to 0$. Hence

$$\lim_{n \to \infty} ((\sqrt{x})_{R_n})^2 = x \tag{16}$$

and we see that the embedding procedure converges to the appropriate limit to justify its definition and claim for acceptance. Note, this formulation is valid for all three replacement techniques.

Finally, it must be mentioned that the above proofs presuppose that all values be within the appropriate region of some Toss. As the embedding becomes richer and therefore more demanding of resources, the size of the Toss and—at an exponential rate—the size of the GF(p) become increasingly large. There are serious questions about the limiting size of these fields before they become so large as to violate our primitive commitments regarding numerousness and scope, etc.

REFERENCES

1. G. Järnefelt, Suomen Geodecttisen Laitoksen Jalkaisuja Veröffentlichungen Des Finnischen Geodätischen Institutes, Helsinki, 36 (1949) 71.

   G. Järnefelt, Annales Academiae Scientiarum Fennicae, Series A, I., No. 96 (1951).

   G. Järnefelt, Congr. Math. Scand., Helsinki, XIII (1957) 118.

   G. Jarnefelt, and Kustaanheimo, P., Den 11te Skandinaviske Mateematiker-Kongress, I Trondheim (1949) Oslo (1952) 166.

   P. Kustaanheimo, Societas Scientiarum Fennica., Commentationes Physico-Mathematicae, XV, 19 (1950).

   P. Kustaanheimo, Annales Academiae Scientiarum Fennicae, Helsinki, 129 (1952) 128.

   P. Kustaanheimo, Math. Scand., 5 (1957) 197-201.

   P. Kustaanheimo, Societas Scientiarum Fennica., Commentationes Physico-Mathematicae, XX, 8 (1957).

2. Y. Ahmavaara, Journal of Math. Phys., 6 (1965) 87; Journal of Math. Phys., 6 (1965) 220; Journal of Math. Phys. 7 (1966) 197; Journal of Math. Phys. 7 (1966) 201.

   E. Beltrametti, and A. Blasi, Journal of Mathematical Physics, 9 (1968) 1027.

   H. Coish, Phys. Rev., 114 (1959) 383.

   I. Shapiro, Nuclear Physics, 21 (1960) 474.

3. For a full discussion of the philosophical committments, see M. Smith and M. Marney, Foundations of the Prescriptive Sciences, in preparation.

4. For the detailed development of a Galois Field, see E. Beltrametti, and A. Blasi, Journal of Mathematical Physics, 9 (1968) 1027, R. Carmichael, Introduction to the Theory of Groups of Finite Order, Dover Publications, Inc., New York, 1937, L. Dickson, Linear Groups Dover Publications, Inc., New York, 1958, and W. Peterson, Error-Correcting Codes, The M.I.T. Press, Cambridge, Massachusetts, 1961.

5. Irreflexivity is required to avoid ambiguity.

6. This notion of an order relation is based upon that developed by Kustaanheimo, et. al., however, we have generalized the concept to more fully incorporate the principle of local ordering. Let us point out that there are alternative methods for defining an irreflexive binary relation and we have not yet fully developed the rationale for choosing among them. For instance, one could locally order by letting $x > y$ if it requires fewer "counts" to reach y by successive unit subtractions than by successive unit additions.

(However, such a convention fails to order the reciprocals.)

Nevertheless, the geometry is still locally defined for $(p + 1)/2$ consecutive elements. For a general discussion of ordering a set, both finite and infinite, see G. Cantor, Contributions to the Founding of the Theory of Transfinite Numbers, Dover Publications, Inc., New York, 1915, P. Halmos, Naive Set Theory, D. Van Nostrand Company, Inc., Princeton, N. J., 1960, F. Hausdorff, Set Theory, second edition Chelsea Publishing Company, N. Y., 1957, E. Kamke, Theory of Sets, Dover Publications, Inc., New York, 1950.

7. This follows from Euler's Criterion because all primitive roots in GF(p), $p \neq 2$, are odd. See J. Uspensky and M. Heaslet, Elementary Number Theory, McGraw-Hill Book Company, Inc., New York, 1939.

8. To see a discussion of this topic in its more general algebraic framework, see A. Albert, Fundamental Concepts of Higher Algebra, The University of Chicago Press, Chicago, 1956, and B. van der Waerden, Modern Algebra, Volume I, Frederick Ungar Publishing Co., New York, 1949.

9. V should read "for any." The distinction between "for every" and "for any" will play an important role in our examination of mathematical induction.

10. E. Beltrametti, and A. Blasi, Journal of Mathematical Physics, 9 (1968) 1027.

11. K. Godel, On Formally Undecidable Propositions, Basic Books, New York, 1962.

12. See reference 8 for a proof that a vector space can be defined over a Galois Field.

13. E. Beltrametti, and A. Blasi, Journal of Mathematical Physics, 9 (1968) 1027, H. Coish, Phys. Rev., 114 (1959) 383, and I. Shapiro, Nuclear Physics, 21 (1960) 474.

14. N. Smith and D. Reisler "On the Generation of Pythagorean Numbers," to be submitted for publication.

15. One must introduce a purely finite field formulation of plane geometry. For instance we may define a triangle as follows. Let V be a two-dimensional vector space over GF(p). Definition. Let $x^1, x^2, x^3 \in V$ be a set of pairwise linearly independent vectors.

Define the "object" determined by the three differences $x^3 - x^2$, $x^2 - x^1$, $x^3 - x^1$ —called sides—to be a triangle. Denote this triangle by $\Delta(x^1, x^2, x^3)$. In this way one can develop a plane geometry with many familiar theorems. For example, if $\Delta(x^1, x^2, x^3)$ is a triangle with no side of zero "length," then there can be at most one orthogonal intersection of sides.

16. Here P(n) denotes some proposition at the n^{th} iteration.

17. A. Fraenkel, and Y. Bar-Hillel, Foundations of Set Theory, North-Holland Publishing Company, Amsterdam, 1958, and A. Fraenkel, Abstract Set Theory, North-Holland Publishing Company, Amsterdam, 1961.

18. Procedural invariance is a generalization of the Einstein principle of relativity that is required to avoid ambiguity of convention—in the most general sense. See Foundations of Prescriptive Sciences, N. Smith and M. Mannoy, in preparation.

19. N. Smith, Behavioral Science, 1 (1956) 111.

20. Here the "number" η will represent the size or scope of a given cognitive system. In some broad sense it is the largest number of counts that can be conceived of by cognitive agents from within this system. Traditional mathematics has used the symbol as in an unrestricted and unqualified sense that does not take the capabilities of the system into account. Thus, η is the largest count not the largest number. For a further examination of this point, see our earlier discussion.