Quadratic Axioms
Harvey M. Friedman
1/3/00

We axiomatize EFA in strictly mathematical terms, involving only the ring operations, without extending the language by either exponentiation, finite sets of integers, or polynomials.

The two axioms beyond commutative rings with unit, are essentially the least element and least common multiple principles for certain quadratics in, respectively, two and four variables.

Strictly speaking, one cannot point to a specific place in the literature where these statements are made, even though they are very elemental and implicit in the literature. So in this sense they are impeachable.

In contrast, our axiomatizations that use finite sets of integers are almost entirely immune to this objection.

We conjecture that an axiomatization can be given entirely within the ring axioms which consists of a finite set of sentences all of which are well known facts stated explicitly in the literature.

Let PQV (positive quadratic values) be the system

1. Axioms for commutative ring with unit.
2. For every a,b,c,d,e,f, the values of axy + bx + cy + d, |x| <= e, |y| <= f, have a least positive upper bound.
3. For every a,b,c,d,e,f,g,h,i,j,k,m, the values of axy + bzw + cx + dy + ez + fw + g in [1,h], with |x| <= i, |y| <= j, |z| <= k, |w| <= m, have a least positive common multiple.

In 2, we use the most common definition of least upper bound. In partciular, if there are positive values, then the least positive upper bound is the max. If there are no positive values, then the least positive upper bound is 1.

In 3, we use the most common definition of common multiple. In particular, if there are no such values then the least positive common multiple is 1.

LEMMA 1. The interval (0,1) is empty.

Proof: Suppose 0 < x < 1. Let x be the least nonzero value of x in [0,1], for 0 < x < 1. I.e., x is least such that 0 < x. But then 0 < x^2 < x, which is a contradiction. QED

LEMMA 2. Let a,b,c,d,e,f,g,h,i be given. Then axy + bx + cy + d assumes a least value >= e on the rectangle [f,g]dot[h,i], provided there is such a value.

Proof: By translation, we can assume that the rectangle is of the form [-j,j+alpha]dot[-k,k+beta], where alpha,beta in {0,1}. But then we only have to handle the cases where the rectangle is [-j,j]dot[-k,k], {j+1}dot[-k,k], [-j,j]dot{k+1}. By translation, the last two cases can be redued to the first case. So we need only prove that axy + bx + cy + d assumes a least value >= e with |x| <= p and |y| <= q, assuming that it assumes some such value. But by axiom 2, axy + bx + cy + d - e + 1 assumes a least positive value with |x| <= p and |y| <= q, assuming that it assumes some such value. But positive values of axy + bx + cy + d - e + 1 correspond exactly to values of axy + bx + cy + d that are >= e. They are the same up to translation. QED

LEMMA 3. For every a,b,c,d,e,f,g,h,i,j,k,m,n,p,q,r, the values of axy + bzw + cx + dy + ez + fw + g in [1,h], with i <= x <= j, k <= y <= m, n <= z <= p, q <= w <= r, have a least positive common multiple, assuming i-j, m-k, p-n, r-q are even.

Proof: By translation, it suffices to get the least positive common multiple of the axy + bzw + cx + dy + ez + fw + g in [1,h], over [-i,i]dot[-j,j]dot[-k,k]dot[-p,p]. But this is just axiom 3. QED

LEMMA 4. Let a,b > 0. The least common multiple lcm(a,b) exists.

Proof: The positive values of ax + b(x-1) for 0 <= x <= max(a,b) are a,b. QED

LEMMA 5. Let a,b > 0. The greatest common divisor gcd(a,b) exists. gcd(a,b)lcm(a,b) = ab.

Proof: Throughout this proof, all letters represent positive integers.

Let x be a common divisor of a,b. Then ab/x = (a/x)b = (b/x)a is a common multiple of a,b. Let y be a common multiple of a,b. Then ab/y is a common divisor of a,b since we can write ab/y = ab/ac = ab/bd = b/c = a/d.

Hence ab/lcm(a,b) is a common divisor of a,b. We claim that it is the greatest common divisor of a,b. To see this, let t be a common divisor of a,b. Then ab/t is a common multiple of a,b, and so ab/t >= lcm(a,b). Hence ab/lcm(a,b) >= t. QED

LEMMA 6. Let x,d be given where d > 0. There exists unique q,r such that x = dq + r and 0 <= r < d.

Proof: First we prove existence. Let r be the least positive value of dy - x for 0 <= y <= x^2. Then r is the least positive value of dy - x. Let r = dy - x. Suppose r > d. Then d(y-1)-x is a smaller positive value. Hence 1 <= r <= d. We can obviously adjust r.

For uniqueness, let x = dq + r = dp + s, where 0 <= q,p < d. Then d(q-p) = s-r. So |d(q-p)| = |s-r| < d. Hence q-p = 0, or p = q as required. QED

LEMMA 7. Let a,b > 0 be relatively prime. There exists x,y such that ax + by = 1.

Proof: Let m be the least positive value of ax + by for -ab <= x,y <= ab. Let m = ax + by, -ab <= x,y <= ab.

Suppose m does not divide a. By Lemma 6, write a = mq + r, 0 <= r < m. Then r = a - mq = a - (ax + by)q = a(1-xq) + byq.

Write r = az + bw. Write z = bq + s, 0 <= s < b. Then r = a(bq + s) + bw = as + bu. Hence bu = r - as > -as > -ab. So u > -a. Now r < m < a,b. Hence as + bu < a,b. Since s >= 0, we see that u < a. In particular, r = as + bu and s,u have magnitudes at most ab.

So m divides a, and by symmetry, m divides b. Hence m = 1. QED

LEMMA 8. Let a,b > 0. There exists x,y such that ax + by = gcd(a,b).

Proof: Note that a/gcd(a,b) and b/gcd(a,b) are relatively prime. Write (a/gcd(a,b))x + (b/gcd(a,b))y = 1. QED

LEMMA 9. Let a,b,c > 0 and a|bc. Suppose a,b are relatively prime. Then a|c.

Proof: By Lemma 7, write ax + by = 1, and so acx + bcy = c. Since a divides the left side, a|c. QED

LEMMA 10. Every n > 1 is divisible by a prime.

Proof: We can assume that n is a composite greater than 2. Look at the values of

8n(xy - n) + x,

that lie in [2,n-1], where 2 <= x,y < n. Such a value must be x, where x divides n and lies in [2,n-1]. The least such value must be the least divisor of n where n is composite. Hence the least such value is a prime divisor of n. QED

LEMMA 11. Let n > 0 and every 1 <= i <= n divides c. Then c+1,2c+1,...,nc+1 are relatively prime in pairs.

Proof: Suppose ic+1 and jc+1 are not relatively prime, i not= j. Let d|ic+1 and d|jc+1, d > 1. By Lemma 10 applied to d, we can assume that d is prime. So d|(i-j)c, and By Lemma 9, d|i-j or d|c. If d|c then d cannot divide ic+1. Hence d|i-j. Therefore 2 <= d < n. But then d|c which is a contradiction. QED

For the next six lemmas, we let phi(i,x1,...,xk) and psi(i,y1,...,ys) be formulas in the language of ordered rings with at most the k+1 and s+1 free variables shown. Let n,c > 0 and every 1 <= i <= n divides c. Let x1,...,xk,y1,...,ys be given. Let z be the least positive common multiple of the ic+1 such that phi(i,x1,...,xk) and 1 <= i <= n. Let w is the least positive common multiple of the ic+1 such that psi(i,y1,...,ys) and 1 <= i <= n.

NOTE: We cannot infer that z,w exist in PQV. We are assuming that z,w exist.

LEMMA 12. For all 1 <= i <= n, ic+1 divides z if and only if phi(i,x1,...,xk).

Proof: Suppose phi(i,x1,...,xk) and 1 <= i <= n. Then ic+1 divides z.

Suppose ic+1 divides z. Then z/ic+1 cannot be a common multiple of the ic+1 such that phi(i,x1,...,xk) and 1 <= i <= n. Let jc+1 not divide z/ic+1, where phi(j,x1,...,xk) and 1 <= j <= n. Then jc+1 divides z. I.e., jc+1 divides ic+1(z/ic+1).

If i not= j then ic+1 and jc+1 are relatively prime, and hence jc+1 divides z/ic+1, which is a contradiction. Hence i = j. Hence phi(i,x1,...,xk). QED

LEMMA 13. Suppose that for all 1 <= i <= n, phi(i,x1,...,xk) implies psi(i,y1,...,ys). Then z|w.

Proof: Suppose gcd(z,w) < z. Then gcd(z,w) is not a common multiple of the ic+1 such that phi(i,x1,...,xk) and 1 <= i <= n. Let 1 <= i <= n be such that phi(i,x1,...,xk) and ic+1 does not divide gcd(z,w). Then ic+1 divides z, ic+1 divides w, and so ic+1 is a common divisor of z,w. By Lemma 8, ic+1 divides gcd(z,w). QED

LEMMA 14. Suppose 1 <= i <= n and ic+1 divides z. Then ic+1 does not divide z/ic+1.

Proof: Fix i as given. We claim that for all 1 <= j <= n with j not= i, if phi(j,x1,...,xk) then jc+1 divides z/ic+1. This follows from jc+1|(ic+1)(z/ic+1) and Lemmas 9 and 11.

So if ic+1 divides z/ic+1 then z/ic+1 is a smaller common multiple of the 1 <= i <= n such that phi(i,x1,...,xk). QED

LEMMA 15. Suppose that for all 1 <= i <= n, phi(i,x1,...,xk) implies psi(i,y1,...,ys). Then for all 1 <= i <= n, ic+1 divides z/y if and only if phi(i,x1,...,xk) and notpsi(i,y1,...,ys).

Proof: Suppose ic+1 divides z/y. Then ic+1 divides z and so phi(i,x1,...,xk).

It suffices to show that ic+1 does not divide y. Suppose the contrary, and write y = u(ic+1). Then ic+1 divides z/u(ic+1), and hence ic+1 divides z/ic+1, contradicting Lemma 14. QED

LEMMA 16. For all 1 <= i <= n, ic+1 divides gcd(y,z) if and only if phi(i,x1,...,xk) and psi(i,y1,...,ys).

Proof: It suffice to show that for all 1 <= i <= n, ic+1 divides gcd(y,z) if and only if ic+1 is a common divisor of y,z. But this follows from Lemma 8. QED

To complete the proof, we just have to interpret the key axioms of the second theory used in posting #77:

15. Finite intervals.
16. Boolean difference.
17. Set addition.
18. Least elements.
19. Common multiples.
20. Scalar set multiplication.
21. Squares.

A code is a triple (n,c,t) where

i) n,c,t > 0;
ii) every 1 <= i <= 2n+1 divides c.

The idea is that the set coded by (n,c,t) is {i in [-n,n]: c(i+n+1)+1 divides t}. These are the finite sets.

LEMMA 17. Every nonempty finite set has a least element.

Proof: Let (n,c,t) be a code for a nonempty finite set. c(t-(c(x+n+1)+1)(y)) + x+n+1, for -n <= x <= n and 1 <= y <= t, has a least positive value. It must be achieved when (c(x+n+1)+1)(y) = t; i.e., when c(x+n+1)+1 divides t. Therefore the least positive value must be achieved when x is least such that c(x+n+1)+1 divides t. QED

LEMMA 18. For all n > 0 there exists c > 0 such that for all 1 <= i <= n, i divides c.

Proof: Take the least positive common multiple of the values of x lying in [1,n], such that |x| <= n. QED

LEMMA 19. Let A be a finite set contained in [-n,n] and assume that for all 1 <= i <= 2n+1, i divides c > 0. Then A has a code (n,c,t).

Proof: Let (m,d,p) be a code for A. Let q be such that for all 1 <= i <= 2n+1, ic+1 divides q. Look at

q(p-(d(x+m+1)+1)(y)) + c(x+n+1)+1

lying in [1,c(2n+1)+1], for |x| <= n.

Because q is so large, these values must be of the form c(x+n+1)+1 where d(x+m+1)+1 divides p. So these values are the c(x+n+1)+1, where x in A.

Let t be the least positive common multiple of these values. By Lemma 12, for all -n <= i <= n, c(i+n+1)+1 divides t if and only if x in A. Hence (n,c,t) codes A. QED

LEMMA 20. Let A,B be finite sets, where B is contained in A. Then A\B is a finite set. Also A intersect B is a finite set.

Proof: Let A,B be contained in [-n,n] and assume that for all 1 <= i <= 2n+1, i divides c > 0. By Lemma 19, let (n,c,s) and (n,c,t) code A,B, respectively. By Lemmas 13 and 15, (n,c,t/s) codes A\B. By Lemma 16, (n,c,gcd(s,t)) codes A intersect B. QED

LEMMA 21. Let A,B be finite sets. Then A\B is a finite set.

Proof: A intersect B is contained in A. Hence A\(A intersect B) = A\B is a finite set. QED

LEMMA 22. Let A,B be finite sets. Then A+B is a finite set.

Proof: By Lemma 19, let (2n,c,s) and (2n,c,t) code A,B, respectively, where A,B are contained in [-n,n]. Let p be a common multiple of c+1,2c+1,...,c(4n+2)+1. Look at

-p(t-(x+n+1)cz) - p(t-(y+n+1)cw) + c(x+y+2n+1)+1

lying in [1,c(4n+1)+1], where |x|,|y| <= n and |z|,|w| <= t.

Since p is so large, these values must be of the form c(x+y+2n+1)+1, where c(x+n+1)+1 divides s and c(y+n+1)+1 divides t. Hence these values are the c(x+y+2n+1)+1, where x in A and y in B.

Let u be the least positive common multiple of these values. By Lemma 12, for all -2n <= i <= 2n, c(i+2n+1)+1 divides u if and only if i in A+B. Hence (2n,c,u) codes A+B. QED

LEMMA 23. For all a,b, [a,b] is a finite set.

Proof: Let a,b in [-n,n], b-a even. Let c be such that for all 1 <= i <= 2n+1, i divides c. By Lemma 3, let t be the least common multiple of the values of c(x+n+1)+1 lying in [1,c(2n+1)+1] for a <= x <= b. Then (n,c,t) codes [a,b].

We now have to handle the case a < b, b-a odd. Since [a,b] = [a,b-1] union {b}, we have merely to show that {b} is a finite set. This is left to the reader. QED

LEMMA 24. Let A be a finite set and n be given. Then nA is a finite set.

Proof: We can assume that n is nonzero. Let nA containedin [-m,m], and c > 0 be such that for all 1 <= i <= m, i divides c. Let (m,c,t) code A. Let p be such that for all 1 <= i <= c, i divides p. Look at

-p(t-(x+m+1)cy) + c(nx+m+1)+1,

lying in [1,c(2m+1)+1], where |x| <= m. Since p is so large, these values must be of the form c(nx+m+1)+1, where x+m+1 divides t. Hence the values are the c(nx+m+1)+1 where x in A. We obtain a code for nA by taking the least positive common multiple. QED

LEMMA 25. For all n > 0, {1^2,...,n^2} is a finite set.

Proof: It suffices to assume that n > 0 is odd since we can union with a singleton. Let c > 0 be such that for all 1 <= i <= n^2 +n+1, i divides c. Let p be such that for all 1 <= i <= c, i divides p. Look at

-p(x-y) + c(xy+n+1)+1,

lying in [1,c(n^2 +n+1)+1], where 1 <= x,y <= n. Since p is so large, these values must be of the form c(xy+n+1)+1 where 1 <= x = y <= n. So these values are the c(x^2 +n+1)+1, 1 <= x <= n. From this we obtain a code of the desired set. QED

THEOREM. The theorems of PQV are exactly the theorems of Isigma0(exp) in the language of ordered rings.

Proof: We have interpreted the system of section 2 of posting #77. QED

NOTE: The applications of axiom 3 use the [1,h] in order to chop off the products of relatively prime numbers involved. If we didn't use the [1,h] then we would get perhaps some big terms in the products that have small factors, screwing up the stuff below. But we still have a high bound on what these terms are, even if we only want an initial segment of them. So we can transfer this higher up so that everything involved, even if higher than we are interested in, is relatively prime. Then we can chop such products down by taking the gcd with the product of all factors up to the point we are interested in. This is like intersecting with intervals, which is OK, although the very first time we do this is before the Boolean stuff.

So I am confident that axiom 3 can be simplified corerspondingly.

And since axiom 3 is only used to code finite sets - i.e., only used to multiply relatively prime numbers ic+1, we can make sure that the variables range over the same intervals.

Similar ideas can uniformize the two intervals in axiom 2.

So we can use

1. Axioms for commutative ring with unit.
2. For every a,b,c,d,e, the values of axy + bx + cy + d, |x| <= e, have a least positive upper bound.
3. For every a,b,c,d,e,f,g,h, the values of axy + bzw + cx + dy + ez + fw + g, with |x|,|y|,|z|,|w| <= h, have a least positive common multiple.