Height and Excess of Pythagorean Triples

DARRYL McCULLOUGH
University of Oklahoma
Norman, OK 73019
dmccullough@math.ou.edu

Does the world really need another article about Pythagorean triples? Here is why we think so. The set of Pythagorean triples has a lot of interesting structure, which has intrigued both amateur and professional mathematicians. It is the topic of an extensive mathematical literature, almost all of which relies on an enumeration of primitive Pythagorean triples that has been known since ancient times. But it is not widely known that there is a different enumeration, based on two simple geometric parameters that we call the *height* and the *excess*. In this article, we will use these parameters to make some known results about Pythagorean triples more transparent. And we will use them to achieve a better understanding of one natural group structure on the set of primitive Pythagorean triples, and to discover another one.

Recall that a *Pythagorean triple* (PT) is an ordered triple (a, b, c) of positive integers such that $a^2 + b^2 = c^2$. When a and b are relatively prime, the triple is a *primitive* PT (PPT). Each PT is a positive integer multiple of a uniquely determined PPT.

The height and excess parameters are shown in FIGURE 1. For a PT (a, b, c), the *height* h is just $c - b$, and the *excess* e is $a + b - c$. The term *excess* arises from the fact that e is simply the extra distance one must travel when going along the two legs instead of the hypotenuse.

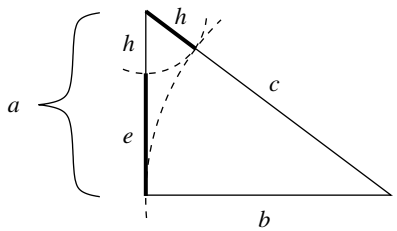

Figure 1 Height and excess of a Pythagorean triangle

Not all combinations of h and e can occur in an integer-sided triangle. We will see that, for a given h, the possible values of e are *exactly the integer multiples of a certain integer* d. The integer d is called the *increment,* and it is related to h in a simple way: d is the smallest positive integer whose square is divisible by $2h$. Since e is a multiple of d, we can write $e = kd$ for a positive integer k. As will be verified in Theorem 1, associating k and h to (a, b, c) sets up a one-to-one correspondence of the PTs with the pairs of positive integers (k, h). For example, everybody's favorite PT $(3, 4, 5)$ corresponds to the pair $(1, 1)$, and $(4, 3, 5)$ and $(5, 12, 13)$ correspond to $(1, 2)$ and $(2, 1)$ respectively, while the nonprimitive PTs $(48, 189, 195)$ and $(459, 1260, 1341)$ correspond to $(7, 6)$ and $(21, 81)$. We call this correspondence the *height-excess enumeration.*

In the rest of this article, we will see various uses of the height and excess parameters. The overarching goal is *to find structure on the set of Pythagorean triples.* To best understand a particular structure on the set of PTs, we need to *view it with the*

right coordinates. The classical enumeration, which we will detail later, assigns a pair of relatively prime integer coordinates (m, n) to each PPT. The height and excess parameters lead to several other systems of coordinates, and we will use whichever of these systems of coordinates seems best for viewing the structure that we are trying to understand. Besides the *k-h* coordinates coming from the height-excess enumeration, and a closely-related kind of coordinates on PPTs, called *k-q* coordinates, we will use *a-h* coordinates, in which $(3, 4, 5)$ is $[3, 1]$, and *e-h* coordinates, in which $(3, 4, 5)$ is $\langle 2, 1\rangle$. Each of these coordinate systems reveals some of the structure of the set of PTs that is hidden when the PTs are written in the conventional way. In fact, it sometimes seems to me that (a, b, c) is the most unenlightening way to think about a PT.

The height-excess enumeration

Our first theorem will establish the height-excess enumeration of PTs. It actually enumerates *all* the triples of (not necessarily positive) integers satisfying the Pythagorean relation $a^2 + b^2 = c^2$. These are called *generalized Pythagorean triples* (GPTs). A GPT (a, b, c) is called primitive when a and b are relatively prime. Each GPT is a positive integer multiple of a uniquely determined primitive GPT.

The PTs (a, b, c) and (b, a, c) both correspond to the same geometric right triangle. We make the arbitrary choice of thinking of the one with $a < b$ as representing this right triangle, so we use the term *Pythagorean triangle* to mean a PT with $a < b$. Theorem 1 will identify, in terms of k and h, the PTs that are triangles, and the PTs that are primitive.

In the statement of Theorem 1, the symbol e does not appear explicitly. The excess is the number dk. Also, a nonzero integer is called *square-free* if it is not divisible by the square of any prime.

THEOREM 1. (THE HEIGHT-EXCESS ENUMERATION) *For any (k, h) in the set $\mathbb{Z} \times \mathbb{Z}$ of pairs of integers, define $P(k, h)$ as follows: If h is nonzero, write it as pq^2 with p square-free and q positive, and associate with it the number d equal to $2pq$ if p is odd, and to pq if p is even. Put*

$$P(k, h) = \left(h + dk, dk + \frac{(dk)^2}{2h}, h + dk + \frac{(dk)^2}{2h}\right),$$

if $h \neq 0$, and put $P(k, 0) = (0, k, k)$. Then P is a bijection from $\mathbb{Z} \times \mathbb{Z}$ to the set of all GPTs (a, b, c). Moreover,

1. *$P(k, h)$ is primitive if and only if k and h are relatively prime and either $h = \pm q^2$ with q odd, or $h = \pm 2q^2$.*
2. *$P(k, h)$ is a PT if and only if both k and h are positive, and is a Pythagorean triangle when in addition $k > \sqrt{2}h/d$.*

Theorem 1 gives a recipe for finding the parameters k and h for any GPT (a, b, c). If $b = c$, then the triple is $(0, k, k) = P(k, 0)$. Otherwise, k and h are calculated as follows.

To find (k, h) from (a, b, c)

1. Put $h = c - b$.
2. Write $h = pq^2$ with p square-free and positive.
3. Put $d = 2pq$ if p is odd, and $d = pq$ if p is even.
4. Put $k = (a - h)/d$.

For example, for $(459, 1260, 1341)$, we have $h = 1341 - 1260 = 81$, so $p = 1$ and $q = 9$, giving $d = 18$, and $k = (459 - 81)/18 = 21$, so $(459, 1260, 1341)$ is $P(21, 81)$.

The proof of Theorem 1 uses only the basic properties of prime factorization and relatively prime integers, and some college algebra. It could be skipped on a first reading, in order to get on to some of the flashier applications of height and excess.

The first step of the proof is to develop the key properties of d. As usual, the notation $x \mid y$ means that the integer y is evenly divisible by the integer x.

LEMMA 1. *Let h be a nonzero integer with associated increment d, as defined in Theorem 1. Then $2h \mid d^2$. If D is any integer for which $2h \mid D^2$, then $d \mid D$.*

Proof. The first assertion is immediate from the definition of d. For the second, we may assume that D is nonzero. Considering prime factorizations, we see that if $2h = 2pq^2$ divides D^2, then $q \mid D$, so $D = D_1 q$ and $2p \mid D_1^2$. Since p has distinct prime factors, it follows that $p \mid D_1$, and if p is odd then $2p \mid D_1$, so $d \mid D$. ∎

Now for the actual proof of Theorem 1. For $h = 0$, all its assertions are straighforward to check, so we assume that $h \neq 0$. By Lemma 1, every expression $P(k, h)$ has integer entries, and algebra shows that it is Pythagorean. Using $h = c - b$, $e = a + b - c$, and the Pythagorean relation, more algebra shows that for all GPTs,

$$(a, b, c) = \left(h + e, e + \frac{e^2}{2h}, h + e + \frac{e^2}{2h}\right).$$

The Pythagorean relation implies that $e^2 = 2(c - a)(c - b)$, so $2h \mid e^2$. By Lemma 1, e is divisible by d, say $e = dk$. So every GPT has the form $P(k, h)$. Since the GPT determines h, e, and d uniquely, k is also determined, showing that P is injective.

Next we identify the primitive GPTs. We use the notation $\gcd(x, y)$ to denote the greatest common divisor of two integers x and y, not both 0. For $h = 0$, $P(k, 0) = (0, k, k)$ is primitive exactly when $k = \pm 1$, and $(\pm 1, 0)$ are exactly the pairs with $h = 0$ that satisfy the given conditions. Suppose that $h \neq 0$. When (a, b, c) is a primitive PT, $c - a$ and $c - b$ must be relatively prime. For suppose that both were divisible by some prime r. Then r divides the sum $(c - a)^2 + (c - b)^2 = (3c - 2a - 2b)c$. Now r could not divide c, since then it would divide both a and b. So r divides $3c - 2a - 2b = 2(c - a) + 2(c - b) - c$. Again we have the contradiction that r divides c. We conclude that $c - a = (k^2 d^2)/(2h)$ and $c - b = h$ are relatively prime. For p odd, these are $2pk^2$ and pq^2, so $p = \pm 1$, q is odd, and $\gcd(2k, q) = 1$. For p even, they are $k^2 p/2$ and pq^2, so $p = \pm 2$ and $\gcd(k, 2q) = 1$. Thus $\gcd(k, h) = 1$ in both cases. Conversely, suppose that h and k satisfy the given conditions. For $h = \pm q^2$, (a, b) is $\pm(q(q + 2k), 2k(q + k))$. If r is a prime dividing both entries, then $r \neq 2$ since the first entry is odd. So r must divide q or $q + 2k$, and must divide k or $q + k$. Any of the four possible combinations leads to r dividing both q and k, a contradiction. For $h = \pm 2q^2$, (a, b) is $\pm(2q(k + q), k(q + 2k))$ and the reasoning is similar.

For the additional remarks, suppose first that $P(k, h) = (a, b, c)$ is a PT, that is, that all three of a, b, and c are positive. Since $P(k, 0) = (0, k, k)$, we must have $h \neq 0$. Since $c = (h^2 + (e + h)^2)/(2h)$, c is positive exactly when $h > 0$. For $h > 0$, $b = dk + (dk)^2/(2h)$ is positive exactly when $(h + dk)^2 > h^2$, that is, either $h + dk < -h$ or $h + dk > h$. In the first case, $a < 0$ and in the second case $a > 0$. We conclude that $P(k, h)$ is a PT exactly when both h and k are positive. For PTs, the form given in Theorem 1 is a triangle exactly when $h + dk < dk + (dk)^2/(2h)$, which says that $k > \sqrt{2}h/d$. ∎

We will now list some properties of the height-excess enumeration. Except for the description of the excess as twice the inradius, they are not used in this article, but some might be of interest in other contexts. We will finish this section with some history of the enumeration.

The number k equals $4A/(dP)$, where A is the area $ab/2$ and P is the perimeter $a+b+c$. This can be seen using the identity $eP = 4A$, which follows from the Pythagorean property. For a right triangle, e is twice the inradius, that is, twice the radius of the largest circle that can be inscribed in the triangle. To see this, just draw the radii from the center of this circle to the three points where it meets the sides and use the definition of excess.

When $h > 0$ and $k > 0$, k is the ordinal of (a, b, c) in the sequence of PTs of height h, in order of increasing values of any one of: a, b, b/a, A, P. This illustrates what I like most about the height-excess enumeration: unlike the classical enumeration (which we will discuss later), it brings order to the apparent chaos of nonprimitive triples, and puts them on an equal footing with the overprivileged primitive triples.

For $h > 0$, d satisfies $2\sqrt{h} \le d \le 2h$, with the lower bound achieved when $p = 1$ and the upper bound when $q = 1$. Thus, the size of d relative to $2\sqrt{h}$ is a rough measure of how far h is from being a perfect square. In fact, the expression $d^2/(2h)$ that appears in Theorem 1 is exactly $p/2$, when p is even, or $2p$, when p is odd.

As far as we can determine, the first version of the height-excess enumeration for PTs is due to M. G. Teigan and D. W. Hadwin [**23**]. The parameters used there are $x = h$, $y = e^2/(2h)$ (which, being $c - a$, is the height of (b, a, c)), and $z = e$. It was noted that (1) z is even, and (2) $2xy = z^2$, and conversely that any triple of positive integers (x, y, z) satisfying (1) and (2) determines a PT, which is primitive exactly when $\gcd(x, y) = 1$. The height-excess enumeration was also found by H. Klostergaard [**16**]. The integer n in [**16**] is our $e/2$, and the integer called d there is our h. Klostergaard observed that h divides $e^2/2$, and used this to describe an enumeration of all Pythagorean triangles by finding the possible heights associated to each increasing integer value of $e/2$; also, $e/2$ is described as twice the area-perimeter ratio.

More explicit renderings of the height-excess enumeration were given by B. Dawson [**7**] and M. Wójtowicz [**26**]. For positive h, Dawson's parameterization is (r, h) where $r = a/d$ if h is even and $r = a/d - 1/2$ if h is odd [**7**]. This shifts the first coordinate so that $(0, h)$ corresponds to the GPT of height h with the smallest nonnegative value of a. Wójtowicz [**26**, Theorem 6] gave a formula equivalent to the one in Theorem 1. Also, A. Grytczuk [**9**] obtained a ring structure (without unit) on the set $\mathcal{P}_h$ of GPTs of height h by transferring the usual structure on the subring $d\mathbb{Z}$ of $\mathbb{Z}$ to $\mathcal{P}_h$ via the bijection sending $P(k, h)$ to e, and this was elaborated upon by Wójtowicz [**25**].

The height-excess enumeration for PTs is implicit as well in an article written by the father-and-son combination of P. W. Wade and W. R. Wade [**24**]. They found the number d, developed a recursion formula that produces all PTs of height h, and used the classical enumeration to give a full verification that the recursion produces all PTs in the cases $h = q^2$ and $h = 2q^2$. In an article that I wrote with Elizabeth Wade [**18**], we proved Theorem 1 for the case of PTs, and used it to give a quick verification of the Wade-Wade recursion for all positive h. In fact, the recursion gives $P(k+1, h)$ in terms of $P(k, h)$.

Elizabeth is not related to P. W. and W. R.

PTs of a given excess The problem of finding all PPTs and PTs (a, b, c) with a equal to a given number has been solved several times in the literature [**1, 4, 14**]. In fact, there is currently a website where one can enter a value of a and receive a list of the PTs [**5**]. As an application of Theorem 1, we are going to obtain a similar count of the number of PTs with a given excess. Our result gives the exact counts both of PTs

and PPTs, and, as we will explain, its proof provides an effective procedure for listing them. We remark that e is always even, since (among many possible reasons) $e = dk$ and d is always even.

THEOREM 2. *For an even positive integer E, write E as $2^{\alpha_0} p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ for distinct odd primes p_i, with all $\alpha_i > 0$. Then the number of PTs of excess E is*

$$2\alpha_0 \prod_{i=1}^{n} (2\alpha_i + 1),$$

of which exactly 2^{n+1} are primitive.

The PTs in Theorem 2 occur in pairs (a, b, c) and (b, a, c), so to obtain the number of Pythagorean triangles of excess E we divide the number of PTs by 2.

Proof. We first find the PPTs $P(k, h)$ with excess E. By statement 1 of Theorem 1, there are two cases. If $h = q^2$, then $d = 2q$, q is odd, and $\gcd(k, q) = 1$. Thus we need to factor $E = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ as $2qk$. Since q and k can have no prime factors in common, when q has some powers of a prime it must have them all. Thus, the choices for q are the 2^n products of the form $p_{i_1}^{\alpha_{i_1}} \cdots p_{i_r}^{\alpha_{i_r}}$, where $i_1 < \cdots < i_r$. This yields the PPTs $P(E/2q, q^2)$ with $d = 2q$ and excess E. Similarly, if $h = 2q^2$, then again $d = 2q$, but $\gcd(k, 2q) = 1$, so k must be odd. In this case there are 2^n choices for k and so 2^n PPTs of the form $P(E/2q, 2q^2)$. Thus we have a total of 2^{n+1} choices for PPTs of excess E.

To include nonprimitive triples, we need to count 2^{r+1} triples for each divisor of E of the form $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$ (with all exponents positive). These are the PPTs of excess D, and multiplied by E/D they give triples of excess E. Each term in the product $2\alpha_0 \prod_{i=1}^{n} (2\alpha_i + 1)$ has the form $2^{r+1}\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$. To obtain a divisor D of the form $2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$, one has α_0 choices for β_0 and α_{i_j} choices for each β_{i_j}, giving $\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$ possibilities. Each such choice produces 2^{r+1} triples, so the number of triples arising from the divisors of the form $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$ is exactly $2^{r+1}\alpha_0\alpha_{i_1} \cdots \alpha_{i_r}$. ∎

The proof of Theorem 2 gives a procedure to find the PTs or Pythagorean triangles of excess E. Take each even divisor D of E, written as $D = 2^{\beta_0} p_{i_1}^{\beta_{i_1}} \cdots p_{i_r}^{\beta_{i_r}}$. For each of the 2^r choices of $\{j_1, \ldots, j_k\} \subset \{i_1, \ldots, i_r\}$, write $D = xy$ with $y = p_{j_1}^{\beta_{j_1}} \cdots p_{j_k}^{\beta_{j_k}}$. Each such factorization gives two PTs $\frac{E}{D} P(x/2, y^2)$ and $\frac{E}{D} P(y, x^2/2)$ of excess E. They have the same values of a and b, but in reverse order. The one with smaller a gives the Pythagorean triangle.

For example, for $E = 36 = 2^2 \cdot 3^2$ there are ten triangles, including two primitives. The procedure finds them to be

$$\begin{array}{llll} (37, 684, 685), & (38, 360, 362), & (39, 252, 255), & (40, 198, 202), \\ (42, 144, 150), & (44, 117, 125), & (45, 108, 117), & (48, 90, 102), \\ & (54, 72, 90), \quad \text{and} & (60, 63, 87). & \end{array}$$

FIGURE 2 shows these ten triangles, with the two primitive ones, (37, 684, 685) and (44, 117, 125), emphasized. The hypotenuses of these ten triangles do not actually intersect in a single point, as the figure may seem to suggest. In fact, for no three triangles of the same excess (Pythagorean or not, positioned as in FIGURE 2 in the first quadrant with their right angles at the origin) do the hypotenuses intersect in a common point; for as we noted in the previous section, the excess equals the diameter of the

incircle, so the hypotenuses of the three triangles T_1, T_2, T_3 would be tangent to their common incircle at distinct points p_1, p_2, and p_3. Selecting notation so that p_1, p_2, and p_3 have increasing x-coordinate, we see that the intersections of the hypotenuses of T_1 and T_2 and of T_2 and T_3 lie on opposite sides of p_2 in the hypotenuse of T_2. So there is no common point.

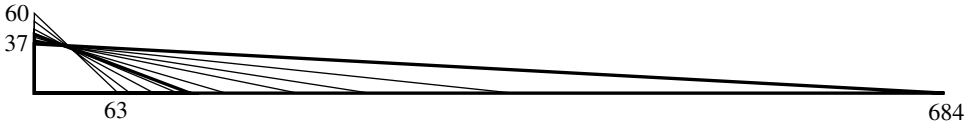

Figure 2 The ten Pythagorean triangles of excess 36

If we do not restrict to triangles with the same excess, then arbitrarily large numbers of Pythagorean triangles, positioned as in FIGURE 2, may have hypotenuses sharing a common point. For if p/q is a rational number greater than 1, the triangle with vertices $(p/q, 0)$, $(0, 0)$, and $(0, p/(p-q))$ will have hypotenuse passing through $(1, 1)$. The length of its hypotenuse is the square root of $p^2((p-q)^2+q^2)/(q^2(p-q)^2)$, which will be rational provided that $p-q$ and q form the first two entries of a PT. Selecting n such numbers $p_1/q_1, \ldots, p_n/q_n$, then multiplying by the number $Q = q_1 \cdots q_n(p_1 - q_1) \cdots (p_n - q_n)$ to clear the denominators of the fractions, we obtain n Pythagorean triangles whose hypotenuses pass through the point (Q, Q). Can this happen with primitive Pythagorean triangles?

The classical enumeration of primitive PTs We mentioned that most articles on PTs rely on the *classical enumeration*, which dates to antiquity [**4, 6**]. It appears in almost every text on elementary number theory, and goes like this. For any pair (m, n) of positive integers with $m > n$, the triples $(m^2 - n^2, 2mn, m^2 + n^2)$ and $(2mn, m^2 - n^2, m^2 + n^2)$ are Pythagorean and correspond to a single Pythagorean triangle. If m and n are relatively prime and not both odd, then these PTs are primitive. Conversely, an argument using prime factorization shows that every PPT has one of these two forms, with m and n relatively prime and not both odd. So, taking these triples for all relatively prime pairs (m, n) with $m > n$ and not both odd produces each PPT exactly once, while taking all their integer multiples gives each PT once. As explained in [**4**], there is a slightly nicer *refined classical enumeration.* Start instead with all relatively prime (m, n) with $m > n$, and write $(m^2 - n^2, 2mn, m^2 + n^2)$ if one of m or n is even (that is, when a is odd), and

$$\left(\frac{m^2 - n^2}{2}, mn, \frac{m^2 + n^2}{2}\right)$$

if m and n are both odd (when a is even). This gives a list of PPTs, with each one appearing exactly once.

For PPTs, the height-excess enumeration gives the following enumeration.

COROLLARY 1. *Let (a, b, c) be a PPT.*

1. *If a is odd, then (a, b, c) can be expressed uniquely as $P(k, q^2) = (q^2 + 2qk, 2qk + 2k^2, q^2 + 2qk + 2k^2)$ for some (k, q) with $\gcd(2k, q) = 1$.*
2. *If a is even, then (a, b, c) can be expressed uniquely as $P(k, 2q^2) = (2q^2 + 2qk, 2qk + k^2, 2q^2 + 2qk + k^2)$ for some (k, q) with $\gcd(k, 2q) = 1$.*

Proof. From Theorem 1, the $P(k, q^2)$ with $\gcd(2k, q) = 1$ are exactly the PPTs with a odd, while the $P(k, 2q^2)$ with $\gcd(k, 2q) = 1$ are exactly those with a even. ∎

How are the refined classical m-n coordinates related to the k-q coordinates coming from Corollary 1? Starting from (m, n), we can use the recipe for finding (k, h) from (a, b, c) to find that $(k, h) = (n, (m-n)^2)$ when one of m or n is even, and $(k, h) = (n, (m-n)^2/2)$ when both are odd. So, $k = n$ in either case, and (using the fact that $m > n$) we have $q = m - n$ when one of m or n is even, and $q = (m-n)/2$ when both are odd. Suppose, on the other hand, that we start from (k, q). Then $q = m - n$ and $(m, n) = (k + q, k)$ when a is odd, while $q = (m-n)/2$ and $(m, n) = (k + 2q, k)$ when a is even.

Corollary 1 is similar to the reparameterization of the classical enumeration obtained in [**6**] by putting $m = i + j$ and $n = i$.

The Barning tree

A very different approach to enumerating the PPTs appears in works of a number of authors [**3, 10, 11, 13, 15, 17, 21**]. We believe that the original version is due to F. J. M. Barning [**3**]. He considered the set of PPTs with a even, regarding them as column vectors. In (a, b, c) coordinates, the statement is quite striking:

THEOREM 3. *Consider the following transformations, each having determinant* 1:

$$A_1 = \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}.$$

Every PPT (a, b, c) *with* a *even can be obtained in exactly one way starting from* $(4, 3, 5)$ *and applying a sequence of the transformations* A_i.

In terms of *structure* on the set of PPTs, this can be interpreted as saying that the PPTs with even a form the vertices of a directed tree with three edges leaving each vertex, and one entering every vertex except $(4, 3, 5)$, in such a way that multiplication of a PPT by an A_i sends it to one of the three vertices to which it leads in the tree. Because of this interpretation, we call this enumeration the *Barning tree.* The PPTs with odd a have a corresponding structure, as we will see near the end of this section.

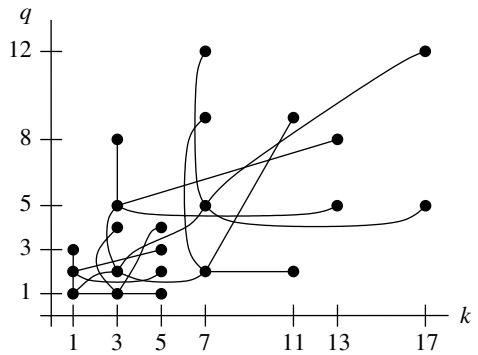

Figure 3 A portion of the Barning tree, viewed in k-q coordinates

Our proof of Barning's theorem uses the k-q coordinates on PPTs given in part 2 of Corollary 1 (we have not been able to obtain a copy of Barning's article, but our proof is surely just a recasting of the original).

FIGURE 3 shows a portion of the Barning tree in k-q coordinates. The vertices are some of the (k, q) pairs that correspond to PPTs, and the edges connect each vertex to the three PPTs obtained from it by multiplying by one of the three matrices. Notice that each vertex and its three offspring form a rectangle. The proof uses a clever process for starting at any vertex and descending through the tree down to the vertex $(1, 1)$, which is the PT $(4, 3, 5)$ in k-q coordinates. We call this process the *Barning descent.*

Proof of Theorem 3. For positive k and q with $\gcd(k, 2q) = 1$, write $T(k, q)$ to denote the PPT $P(k, 2q^2) = (2q^2 + 2qk, 2qk + k^2, 2q^2 + 2qk + k^2)$ (when necessary in calculations, assume that $T(k, q)$ is a column vector rather than a row vector). In particular, $T(1, 1) = (4, 3, 5)$. Corollary 1 shows that these are exactly the PPTs with a even. We calculate

$$A_2\, T(k, q) = \begin{pmatrix} 6q^2 + 10qk + 4k^2 \\ 8q^2 + 10qk + 3k^2 \\ 10q^2 + 14qk + 5k^2 \end{pmatrix}.$$

Calling this vector (A, B, C), we use our usual recipe to write it as $T(K, Q)$ by computing that $H = C - B = 2(q + k)^2$, so $Q = q + k$, $D = 2(q + k)$, and $K = (A - H)/D = (4q^2 + 6qk + 2k^2)/2(q + k) = k + 2q$. Carrying out similar calculations for A_1 and A_3, we find:

$$\begin{aligned} A_1\, T(k, q) &= T(k, q + k), \\ A_2\, T(k, q) &= T(k + 2q, k + q), \\ A_3\, T(k, q) &= T(k + 2q, q). \end{aligned}$$

Notice that when we write $A_i\, T(k, q)$ as $T(K, Q)$, we have $K < Q$ in the first case, $Q < K < 2Q$ in the second, and $2Q < K$ in the third.

In k-q coordinates, the matrices of A_1, A_2, and A_3 are

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}.$$

Inverting these matrices, and, as before, denoting $A_i\, T(k, q)$ by $T(K, Q)$, we find that:

$$\begin{aligned} A_1^{-1} T(K, Q) &= T(K, Q - K), \\ A_2^{-1} T(K, Q) &= T(2Q - K, K - Q), \\ A_3^{-1} T(K, Q) &= T(K - 2Q, Q). \end{aligned}$$

These three cases are illustrated in FIGURE 4, where P_i denotes $A_i^{-1}\, T(K, Q)$.

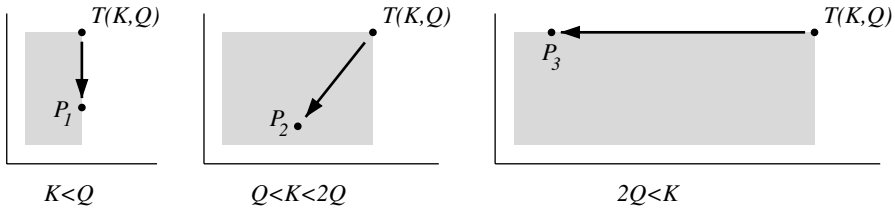

Figure 4 The three cases in the Barning descent

We are now set up for the Barning descent. Given any $T(K, Q)$ with $K > 1$ or $Q > 1$, the condition that $\gcd(K, 2Q) = 1$ shows that either $K < Q$, $Q < K < 2Q$, or $2Q < K$. Applying A_1^{-1}, A_2^{-1}, or A_3^{-1} in the respective cases produces a $T(k, q)$ with $k + q < K + Q$. Repeating with this new PPT, we find a composition $A_{i_n}^{-1} \cdots A_{i_1}^{-1}$ sending $T(K, Q)$ to $T(1, 1)$. The composition $A_{i_1} \cdots A_{i_n}$ moves $T(1, 1)$ to $T(K, Q)$. This is the only possible such composition, for any other one would lead to a case where $A_i\, T(k', q') = A_j\, T(k'', q'')$ with $i \neq j$, but this resulting element $T(K', Q')$ would have to satisfy two of the mutually exclusive conditions $K' < Q'$, $Q' < K' < 2Q'$, and $2Q' < K'$. ∎

The Barning tree for the PPTs with a odd is essentially the same as the version for a even, but we need not repeat the entire argument. Notice that for the matrix

$$M = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

one has (as usual thinking of (a, b, c) as a column vector) that $M(a, b, c) = (b, a, c)$. Since in a PPT, exactly one of a or b is even, multiplication by M converts the PPTs with a odd into the PPTs with a even, and converts the even ones back into odds. So, the exact statement of Theorem 3 holds after replacing each A_i by MA_iM and replacing $(4, 3, 5)$ by $(3, 4, 5)$.

Two articles by L. Palmer, M. Ahuja, and M. Tikoo [**19, 20**] contain some additional information about the form of a matrix A that preserves the set of PTs.

Operations on PTs

In the remainder of this article, we will be examining algebraic operations on sets of GPTs. There are many meaningless operations—for example, we could just make a list of all the GPTs in some random order, associate the nth GPT to the natural number n, and "add" the PTs according to the way that their associated numbers add. An operation is meaningful only when it reflects geometric or algebraic information about the GPTs.

When developing algebraic structures, one often uses a procedure called *projectivization.* This is actually a familiar process from everyday arithmetic. Start with the set of ordered pairs of positive integers (m, n). Let us write this pair as $m/\!\!/n$, and consider the simple operation defined by $m_1/\!\!/n_1 * m_2/\!\!/n_2 = m_1m_2/\!\!/n_1n_2$. This makes the set into a *semigroup,* that is, a set with an associative operation. In this case, the operation has an identity element, since $1/\!\!/1 * m/\!\!/n = m/\!\!/n$, so the semigroup is called a *monoid.* But it fails to be a *group,* since some elements (in fact, all elements other than $1/\!\!/1$) do not have inverses. Now, we projectivize by declaring that $m/\!\!/n$ and $r/\!\!/s$ are equivalent if they have integer multiples that are equal (that is, if there are positive integers t and u so that $tm/\!\!/tn = ur/\!\!/us$). We write m/n for the set of pairs equivalent to $m/\!\!/n$. For example, $3/6 = \{1/\!\!/2, 2/\!\!/4, 3/\!\!/6, 4/\!\!/8, \ldots\} = 1/2$. The equivalence relation has the property that if $m_1/n_1 = m_2/n_2$ and $r_1/s_1 = r_2/s_2$, then $m_1r_1/n_1s_1 = m_2r_2/n_2s_2$, so the star operation induces a multiplication operation on the equivalence classes defined by $m/n * r/s = mr/ns$. This operation still has an identity element, $1/1$, but now every element has an inverse, since $a/b * b/a = ab/ba = 1/1$. The equivalence classes form the group $\mathbb{Q}_{>0}$ of positive rational numbers. One can think of this process as erasing a lot of inessential structure on the fractions—the structure that makes $2/\!\!/4$ different from $3/\!\!/6$—and after eliminating this unnecessary structure, the higher-level algebraic structure of a group can exist on the set $\mathbb{Q}_{>0}$ of equivalence classes.

For the rational numbers, each equivalence class m/n contains exactly one fraction in lowest terms, and two fractions are equivalent exactly when they are both multiples of the same fraction in lowest terms. In everyday life, we often identify a rational number with the unique fraction in lowest terms that it contains, as when we write $(2/3)(9/4) = 3/2$. What we are really doing is multiplying the fractions $2/\!\!/3$ and $9/\!\!/4$ to obtain $18/\!\!/12$, then writing the equivalence class $18/12$ as $3/2$.

Another way to think of this equivalence relation is that the underlying meaning of a fraction is a *ratio,* and $1/\!\!/2$ and $2/\!\!/4$ just represent the same ratio by different sizes of numbers. In the same way, we can think of the PTs (3, 4, 5) and (6, 8, 10) as the same *shape* (similarity class) of right triangles, just being represented by different sizes of triangles. The PPT (3, 4, 5) is the triple in "lowest terms" that represents this shape (just as $1/2$ is the "primitive" fraction that represents its ratio).

Using the analogous projectivization process on PTs, complex multiplication has been used to construct a well-known operation on the set of PPTs (together with (1, 0, 1)) [**8, 22**]. We call it the Taussky-Eckert operation. One treats the first two entries of (a, b, c) as $a + bi$ and mimics complex multiplication. If the product lies in the second quadrant, multiply by $-i$ to move it into the first quadrant. In formulas, $(a_1, b_1, c_1) \otimes (a_2, b_2, c_2)$ equals $(a_1a_2 - b_1b_2, a_1b_2 + a_2b_1, c_1c_2)$ if $a_1a_2 - b_1b_2 > 0$, and equals $(a_1b_2 + a_2b_1, b_1b_2 - a_1a_2, c_1c_2)$ if $a_1a_2 - b_1b_2 \leq 0$. This defines an operation on the set of PTs, plus the GPTs of the form $(n, 0, n)$ with $n > 0$. The operation is meaningful because it is *multiplicative with respect to the c-coordinate.*

The $\otimes$ operation has an identity element (1, 0, 1), but elements other than (1, 0, 1) do not have inverses, and a product of two PPTs need not be primitive. Again we save the day by declaring that two of these GPTs are equivalent when they have integer multiples that are equal. The operation respects the equivalence relation, so there is an induced operation on the equivalence classes. Also, each equivalence class contains exactly one primitive triple, so the equivalence classes can be identified with the PPTs (along with (1, 0, 1)). At the level of PPTs, this means carrying out the operation, then dividing out by the greatest common divisor to obtain a new PPT. For the equivalence classes, (b, a, c) is the inverse of (a, b, c), because $(a, b, c) \otimes (b, a, c) = (a^2 + b^2, 0, c^2)$, which is equivalent to (1, 0, 1). So just as with fractions and rational numbers, the equivalence classes have the higher-level algebraic structure of a group. Eckert [**8**] showed that with this operation, the PTs form a free abelian group generated by the triples (a, b, p) with $a > b$ and p a prime of the form $4n + 1$ (Hlawka [**12**] gives a discussion of this and other more advanced topics on PTs).

The Beauregard-Suryanarayan group

R. Beauregard and E. Suryanarayan [**4**] studied the operation on the set of GPTs defined by $(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2)$. This operation is meaningful because it is multiplicative for a. By projectivizing, they obtained a group structure on the set of primitive GPTs with $a > 0$ and $c > 0$, and identified the resulting group with the group $\mathbb{Q}_{>0}$ of positive rational numbers.

We are going to analyze the Beauregard-Suryanarayan operation using a-h coordinates. That is, we write a GPT (with $h \neq 0$) as $[a, h]$, where a is the a from (a, b, c) and h is the height. We will see that, in these coordinates, the operation behaves as coordinatewise multiplication $[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2]$. This allows a simplified treatment of the theory developed in [**4**]. The projectivized object obtained from the set of all GPTs with $h \neq 0$ is naturally identified with the monoid $\{1, -1\} \times \mathbb{Q}$, the Beauregard-Suryanarayan group being the subset identified with $\{1\} \times \mathbb{Q}_{>0}$. The PPTs correspond to the semigroup $\{1\} \times \mathbb{Q}_{>1}$.

To get started, observe that the Pythagorean identity implies that for any GPT with $h \neq 0$,

$$(a, b, c) = \left(a, \frac{a^2 - h^2}{2h}, \frac{a^2 + h^2}{2h}\right).$$

Thus, a and h determine a GPT, provided of course that a has the form $a = h + kd$. We denote this GPT by $[a, h]$, and call these the *a-h coordinates* of the GPT. It is a PT exactly when $a > h > 0$, since this is exactly when both h and k are positive. Some interesting examples of GPTs in a-h coordinates are:

1. $[1, 1] = (1, 0, 1)$, $[1, -1] = (1, 0, -1)$, $[-1, 1] = (-1, 0, 1)$, and $[-1, -1] = (-1, 0, -1)$.
2. $[3, 1] = (3, 4, 5)$ and $[4, 2] = (4, 3, 5)$, while $[2, 1]$ does not represent a GPT since for $h = 1$ we have $d = 2$.
3. For q odd, $[q, 1] = (q, (q^2 - 1)/2, (q^2 + 1)/2)$.
4. For q odd, $[q, q^2] = (q, (1 - q^2)/2, (q^2 + 1)/2)$.
5. For $s > 1$, $[2^s, 2] = (2^s, 2^{2s-2} - 1, 2^{2s-2} + 1)$.
6. For $s > 1$, $[2^s, 2^{2s-1}] = (2^s, 1 - 2^{2s-2}, 2^{2s-2} + 1)$.

The result of the Beauregard-Suryanarayn operation,

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1a_2, b_1c_2 + b_2c_1, b_1b_2 + c_1c_2),$$

has height

$$b_1b_2 + c_1c_2 - (b_1c_2 + b_2c_1) = (c_1 - b_1)(c_2 - b_2),$$

so written in a-h coordinates, the operation takes the form

$$[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2],$$

as claimed.

Let $\mathcal{D}$ denote the set of GPTs with $h \neq 0$. If $[a, h] = (a, b, c)$ is a GPT and n is a nonzero integer, then $n[a, h] = (na, nb, nc) = [na, nh]$. So just as for the Taussky-Eckert operation, we can projectivize $\mathcal{D}$ by declaring that two GPTs are equivalent if they have positive integer multiples that are equal. For example, the equivalence class of $(4, 3, 5)$ is $\{[4, 2], [8, 4], [12, 6], \ldots\}$. Each equivalence class contains one primitive GPT, so the resulting set of equivalence classes $\mathcal{G}$ can be identified with the set of primitive GPTs of nonzero height. The main result is:

THEOREM 4. *Define $\phi: \mathcal{G} \to \{1, -1\} \times \mathbb{Q}$ by sending $[a, h]$ to $(\sigma(h), a/h)$, where $\sigma(h) = 1$ if h is positive and is -1 if h is negative. Then ϕ is an isomorphism.*

Proof. If $n_1[a_1, h_1] = n_2[a_2, h_2]$, then $\phi([a_1, h_1]) = (\sigma(n_1h_1), n_1a_1/(n_1h_1)) = (\sigma(n_2h_2), n_2a_2/(n_2h_2)) = \phi([a_2, h_2])$, so ϕ is well-defined on equivalence classes. The homomorphism condition $\phi([a_1, h_1] * [a_2, h_2]) = \phi([a_1a_2, h_1h_2])$ is also immediate. For surjectivity, it is enough to note that $\phi(\pm[1, 1]) = (\pm 1, 1)$, $\phi(\pm[1, -1]) = (\pm 1, -1)$, $\phi([0, 1]) = (1, 0)$, $\phi([4, 2]) = (1, 2)$, $\phi([2, 4]) = (1, 1/2)$, and for q an odd prime, $\phi([q, 1]) = (1, q)$ and $\phi([q, q^2]) = (1, 1/q)$, since products of these elements produce all elements of $\{1, -1\} \times \mathbb{Q}$. For injectivity, suppose that $\phi([a_1, h_1]) = \phi([a_2, h_2])$. Then h_1 and h_2 have the same sign, so replacing both $[a_i, h_i]$ by $[-a_i, -h_i]$, if necessary, we may assume that both h_1 and h_2 are positive. Since

$$\frac{1}{h}[a, h] = \left(\frac{a}{h}, \frac{(a/h)^2 - 1}{2}, \frac{(a/h)^2 + 1}{2}\right),$$

we have $h_2[a_1, h_1] = h_1[a_2, h_2]$. That is, $[a_1, h_1]$ and $[a_2, h_2]$ are projectively equivalent, so they represent the same element of $\mathcal{G}$. ∎

Since $\mathbb{Q}_{>0}$ is the free abelian group on the set of primes, this shows that the projectivization of the submonoid consisting of all $[a, h]$ with $a > 0$ and $h > 0$ (that is, the (a, b, c) with $a > 0$ and $c > 0$) is an abelian group that is free on the set $\{[4, 2]\} \cup \{[p, 1] \mid p \text{ is an odd prime}\}$. This is the Beauregard-Suryanarayan group. It has an elegant geometric interpretation, which is explained in [**4**]. Finally, from the formula for (a, b, c) in terms of a and h, we observe that $[a, h]$ is a PT exactly when $a > 0$, $h > 0$, and $a > h$, so the PPTs correspond to the semigroup $\{1\} \times \mathbb{Q}_{>1}$.

The Beauregard-Suryanarayan monoid

To obtain the Beauregard-Suryanarayan group, we projectivized the Beauregard-Suryanarayan monoid, thereby erasing the structure that was preventing it from being a group. In fact, that lost structure is rather interesting, so we will now backtrack and analyze the Beauregard-Suryanarayan monoid itself. This is a good example of how a complicated algebraic object can be understood by studying it "at each prime."

Recall that the Beauregard-Suryanarayan monoid $\mathcal{D}$ was the set of all GPTs $[a, h]$ with $h \neq 0$, with the operation $[a_1, h_1] * [a_2, h_2] = [a_1a_2, h_1h_2]$. We emphasize that the operation is commutative, and remind the reader that a semigroup is a set with an associative operation, while a monoid is a semigroup with an identity element.

The structure we will find involves a direct sum of monoids. The books that I have checked either do not define a direct sum of monoids, or define it in a very abstract setting using the language of categories. Here is a straightforward definition for the countable commutative monoids that we will be using. Suppose you have monoid S and a (finite or infinite) collection of submonoids $S_1, S_2, \ldots$ of S (a submonoid is a subset of S that contains the identity element of S and itself forms a monoid under the operation of S). When we say that S is the direct sum $\oplus S_n = S_1 \oplus S_2 \oplus \cdots$ of these submonoids, we will mean that every nonidentity element of S can be written in a unique way (up to order of the factors) as a product of nonidentity elements from finitely many of the different submonoids. A good example to keep in mind is the counting numbers $S = \{1, 2, \ldots\}$, with the operation of multiplication. Let $\mathcal{P}$ denote the set of prime numbers, and for each $p \in \mathcal{P}$, let S_p be the submonoid $\{1, p, p^2, p^3, \ldots\}$ of S. The fact that each counting number factors uniquely into a product of prime factors says exactly that $S = \oplus_{p \in \mathcal{P}} S_p = S_2 \oplus S_3 \oplus S_5 \oplus \cdots$.

We begin by determining how to identify the primitive GPTs from their a-h coordinates.

PROPOSITION 1. *For $h \neq 0$, $[a, h]$ is primitive exactly when either*

1. *a is odd and $h = \pm q^2$ with q odd and* $\gcd(a, h) = q$, *or*
2. *a is even and $h = \pm 2q^2$ with* $\gcd(a, h) = 2q$.

Proof. Since $[a, h] = -[-a, -h]$, we may assume that $h > 0$. Suppose that $[a, h]$ is primitive. If $h = q^2$, then according to Corollary 1, $a = q(q + 2k)$ with $\gcd(2k, q) = 1$, so $\gcd(a, h) = q$. If $h = 2q^2$, then $a = 2q(q + k)$ with $\gcd(2q, k) = 1$, so $\gcd(a, h) = 2q$.

Conversely, suppose that $[a, h]$ is not primitive. If h is not of the form q^2 with q odd or $2q^2$, then neither condition holds. Suppose that $h = q^2$. Since the triple is not primitive, statement 1 of Theorem 1 shows that k and h are divisible by an odd prime p. Since $a = q(q + 2k)$, pq divides both a and h. This shows that $\gcd(a, h)$ must be greater than q. The case of $h = 2q^2$ is similar. ∎

Recall that if $[a, h]$ is a GPT and n is a nonzero integer, then $n[a, h] = [na, nh]$. Consequently, if a product of PTs is primitive, each factor must be primitive (although a product of PPTs need not be primitive, for example $(4, 3, 5) * (4, 3, 5) = 2(8, 15, 17)$). Beauregard and Suryanarayan [**4**] proved the following unique factorization theorem for the monoid $\mathcal{D}$.

THEOREM 5. *Let $[a, h] \in \mathcal{D}$ be primitive. Write a as $\pm 2^r p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$, where $r \geq 0$, all r_i and s_j are positive, and $\{p_1, \ldots, p_m, q_1, \ldots, q_n\}$ are distinct odd primes, with the q_j being the odd prime factors of a that are also factors of h. Then $[a, h]$ factors uniquely as $S_0 * P_0 * (\prod_{i=1}^{m} [p_i, 1]^{r_i}) * (\prod_{j=1}^{n} [q_j, q_j^2]^{s_j})$, where S_0 is one of the four GPTs $[\pm 1, \pm 1]$, and*

(i) $P_0 = [1, 1]$ *if h is odd,*

(ii) $P_0 = [2^r, 2]$ *if $h \equiv 2 \mod 4$, and*

(iii) $P_0 = [2^r, 2^{2r-1}]$ *if $h \equiv 0 \mod 4$.*

In the latter two cases, $r \geq 2$.

We will now use a-h coordinates to give a proof of this result. Our proof will not use Theorem 4. While Theorem 5 can be deduced as a corollary of Theorem 4, this does not seem to shorten the proof if one wants the precise information about how the form of P_0 depends on h. Theorem 4 can be deduced from Theorem 5 [**4**].

Proof. Factoring out S_0 allows us to assume that both a and h are positive. We first prove the existence of the factorization. Suppose first that a is odd; by Proposition 1, $h = q^2$ with q odd and $\gcd(a, h) = q$. So we can write $h = q_1^{2s_1} \cdots q_n^{2s_n}$ and $a = p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$, with all r_i and s_j positive, and $p_1, \ldots, p_m, q_1, \ldots, q_n$ distinct odd primes. This give the desired factorization with P_0 chosen as in (i).

Now suppose that a is even; by Proposition 1, $h = 2q^2$ with $\gcd(a, h) = 2q$. So we can write $h = 2^{2s_0+1} q_1^{2s_1} \cdots q_n^{2s_n}$ and $a = 2^r p_1^{r_1} \cdots p_m^{r_m} q_1^{s_1} \cdots q_n^{s_n}$. If $s_0 = 0$, then we obtain a factorization of $[a, h]$ with P_0 as in (ii). In this case, $r \geq 2$, since a factor of $[2, 2]$ would prevent $[a, h]$ from being primitive. If $s_0 > 0$, then since $\gcd(a, h) = 2^{s_0+1} q_1^{s_1} \cdots q_n^{s_n}$, we must have $r = s_0 + 1$ giving a factorization with P_0 as in (iii), with $r \geq 2$.

For the uniqueness of the factorization, we observe that the product of the first entries must be a, and the only way that the second entries can have product equal to h is for the factor of h that is a power of 2 to be paired with the factor 2^r of a, and for each of the $q_{s_i}^2$ factors of h to be paired with one of the q_{s_i} factors of a that appears in a term of the form $[q_{s_i}, q_{s_i}^2]$. ∎

COROLLARY 2. *Let $[a, h] \in \mathcal{D}$. Then $[a, h]$ can be written uniquely in the form $S_0 * [2^s, 2^t] * (\prod_{i=1}^{m} [p_i^{s_i}, p_i^{t_i}])$, where the p_i are distinct odd primes, $s, t \geq 0$, each $s_i, t_i \geq 0$ and $s_i + t_i > 0$, and S_0 is one of the four GPTs $[\pm 1, \pm 1]$. In this form, each $t_i \leq 2s_i$, and either $s = t = 0$ or $1 \leq t < 2s$.*

Proof. Write $[a, h]$ as $[N, N] * [a_1, h_1]$, where N is a positive integer and $[a_1, h_1]$ is primitive. Using the factorization for $[a_1, h_1]$ given in Theorem 5, we obtain a factorization for $[a, h]$ of the desired form. It is unique, since the product of the first entries of the factors is a and the product of the second entries is h. ∎

Now, we can develop the precise structure of the monoid $\mathcal{D}$. First, note that $\mathcal{D}$ is the union of two nonintersecting semigroups: $\mathcal{D}_0$, the set of $[0, h]$, and $\mathcal{D}_{\neq 0}$, the monoid consisting of the $[a, h]$ with $a \neq 0$. When $a = 0$, h must be even, so $\mathcal{D}_0$ is isomorphic to the semigroup $2\mathbb{Z} - \{0\}$ under multiplication. The rule $[0, h_1] * [a, h_2] = [0, h_1 h_2]$ shows exactly how to multiply an element of $\mathcal{D}_0$ by an element of $\mathcal{D}_{\neq 0}$, so to understand the multiplicative structure of $\mathcal{D}$, it remains only to understand $\mathcal{D}_{\neq 0}$. Let $\mathcal{A}$ be the

monoid consisting of the $[a, h]$ with a and h both positive. Since each $[a, h]$ in $\mathcal{D}_{\neq 0}$ can be written uniquely as $[\epsilon_1, \epsilon_2] * [a_1, h_1]$, with $[\epsilon_1, \epsilon_2] \in \{[\pm 1, \pm 1]\}$ and $[a_1, h_1] \in \mathcal{A}$, $\mathcal{D}_{\neq 0}$ is the direct sum $\{[\pm 1, \pm 1]\} \oplus \mathcal{A}$. So it remains only to understand $\mathcal{A}$. In the process, we will determine exactly which elements of $\mathcal{D}$ can be written as products of primitive GPTs.

Begin with an $[a, h]$ in $\mathcal{A}$. By Corollary 2, $[a, h]$ can be factored uniquely as $\prod_{i=1}^{m} [p_i^{s_i}, p_i^{t_i}]$, where the p_i are distinct primes and the exponents are all nonnegative, and for each i, $s_i + t_i > 0$ and $t_i \leq 2s_i$, and moreover if $p_i = 2$ then $1 \leq t_i < 2s_i$. So we can write $\mathcal{A}$ as the direct sum $\bigoplus_{p \in \mathcal{P}} \mathcal{A}_p$, where $\mathcal{P}$ is the set of primes and

1. For p an odd prime, $\mathcal{A}_p$ is the set of GPTs of the form $[p^s, p^t]$ with $s, t \geq 0$ and $t \leq 2s$.
2. $\mathcal{A}_2$ is the set of GPTs of the form $[2^s, 2^t]$, where $s, t \geq 0$ and either $s = t = 0$ or $1 \leq t < 2s$.

We will see that the $\mathcal{A}_p$ with p odd are rather easy to describe and are all essentially the same, while $\mathcal{A}_2$ is quite a bit more complicated.

We first analyze the $\mathcal{A}_p$ for an odd p. Since $t \leq 2s$, any element $[p^s, p^t]$ of $\mathcal{A}_p$ can be written as $[p, p]^u * [p, 1]^v * [p, p^2]^w$, with u, v, and w nonnegative and at least one of them positive. We identify $[p^s, p^t]$ with the vector (s, t), so that the operation becomes vector addition. This identifies $\mathcal{A}_p$ with the submonoid $\mathbb{M}$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ generated by the vectors $(1, 1)$, $(1, 0)$, and $(1, 2)$. The latter two vectors generate a submonoid that we call $\mathcal{B}_p$; for each $(s, t) \in \mathcal{B}_p$, t is even.

The first coordinate system in FIGURE 5 shows a picture of $\mathcal{A}_p$, with the solid dots indicating the elements of $\mathcal{B}_p$. One sees, either by calculation or by noticing that in FIGURE 5, adding the vector $(1, 1)$ moves the solid dots to the open circles, that every element of $\mathcal{A}_p$ can be written uniquely as $[p, 1]^u * [p, p^2]^v * [p, p]^\epsilon$ with ϵ equal to 0 or 1, and an element lies in $\mathcal{B}_p$ if and only if $\epsilon = 0$, that is, when it has the form $[p^s, p^t]$ with t even. Thus $\mathcal{B}_p$ consists exactly of the elements of $\mathcal{A}_p$ that are products of PPTs.

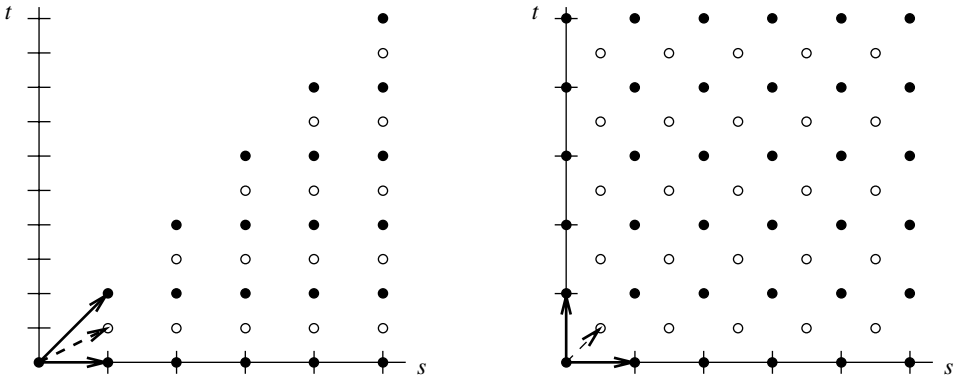

Figure 5 $\mathcal{A}_p$ and $\mathcal{B}_p$ for p an odd prime

Algebraically, $\mathcal{A}_p$ is generated as a semigroup by three generators $\gamma_1 = [p, 1]$, $\gamma_2 = [p, p^2]$, and $\gamma_3 = [p, p]$, subject to the relation that $\gamma_1 * \gamma_2 = \gamma_3 * \gamma_3$, and $\mathcal{B}_p$ is the submonoid generated by γ_1 and γ_2. In fact, $\mathcal{B}_p$ is isomorphic to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$. An explicit isomorphism is given by multiplication by the matrix

$$\begin{pmatrix} 1 & -1/2 \\ 0 & 1/2 \end{pmatrix}$$

(as usual, we regard (s, t) as a column vector and multiply on the left by this matrix). The second coordinate system of FIGURE 5 shows the result of multiplying the vectors of $\mathcal{A}_p$ by this matrix. This carries $\mathcal{B}_p$ to $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$, and $\mathcal{A}_p - \mathcal{B}_p$ to the vectors of the form $(1/2, 1/2) + (s, t)$ for $(s, t) \in \mathcal{B}_p$.

Now we analyze $\mathcal{A}_2$. By Corollary 2, $\mathcal{A}_2$ consists of $[1, 1]$ and the $[2^s, 2^t]$ with $1 \leq t < 2s$. Again changing to vector notation, we identify $\mathcal{A}_2$ with the submonoid $\mathbb{M}_2$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{\geq 0}$ consisting of $(0, 0)$ and all (s, t) with $1 \leq t < 2s$. There is no finite generating set for $\mathcal{A}_2$. For the angles of inclination of the nonzero vectors in the span of any finite subset of $\mathbb{M}_2$ are bounded away from 0, but 0 is a limit point for the set of angles of inclination of elements of M_2.

Define the submonoid $\mathcal{B}_2$ of $\mathcal{A}_2$ to consist of the products of primitive GPTs. Let $\mathcal{S}_2^+ = \{(s, 1) \mid s \geq 2\}$ and $\mathcal{S}_2^- = \{(s, 2s - 1) \mid s \geq 2\}$. Theorem 5 shows that $\mathcal{S}_2 = \{(0, 0)\} \cup \mathcal{S}_2^+ \cup \mathcal{S}_2^-$ is the collection of all primitive GPTs in $\mathcal{A}_2$, so $\mathcal{B}_2$ is the submonoid generated by $\mathcal{S}_2$. In a previous version of this article, we gave a proof that $\mathcal{B}_2$ contains all but finitely many elements of $\mathcal{A}_2$. We thank the referee for improvements that give the following sharper result.

THEOREM 6. *The set* $\mathcal{A}_2 - \mathcal{B}_2$ *consists of* $(1, 1)$, $(2, 2)$, $(3, 2)$, $(3, 3)$, $(3, 4)$, $(4, 3)$, $(4, 5)$, $(5, 3)$, $(5, 5)$, *and* $(5, 7)\}$; *these are exactly the PTs* $2^n(1, 0, 1)$ *for* $n = 1, 2, 3,$ *and* 5, $2(4, \pm 3, 5)$, $4(4, \pm 3, 5)$, *and* $4(8, \pm 15, 17)$.

Proof. In our proof, all variables will represent positive integers. First, consider the region L in FIGURE 6, which consists of all nonzero $(s, t) \in \mathcal{A}_2$ having $1 \leq t \leq s/2$. We claim that $L \subset \mathcal{B}_2$, as we will show by induction on t. If $t = 1$, then $(s, t) \in \mathcal{S}_2^+$. If $t > 1$, then $(s, t) = (2, 1) + (s - 2, t - 1)$, with $(s - 2, t - 1) \in L$. By the induction hypothesis, $(s - 2, t - 1) \in \mathcal{B}_2$, so $(s, t) \in \mathcal{B}_2$.

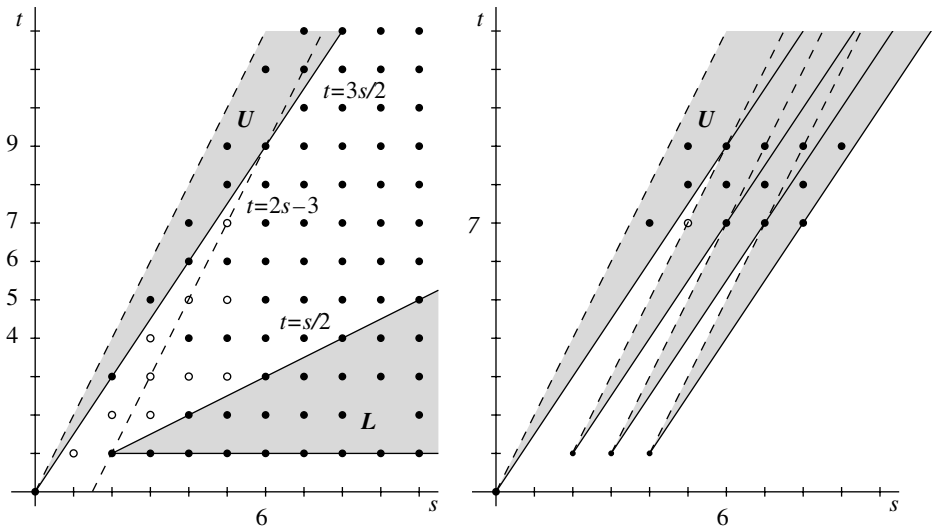

Figure 6 Finding $\mathcal{A}_2 - \mathcal{B}_2$

Next, we claim that $U \subset \mathcal{B}_2$, where, as shown in FIGURE 6, U is the set of (s, t) satisfying $3 \leq 3s/2 \leq t < 2s$. Let M be the matrix

$$\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}.$$

Notice that $M = M^{-1}$, and M carries integer lattice points to integer lattice points. As usual, thinking of vectors as column vectors when necessary, we have $M(s, 1) = (s, 2s - 1)$, so M interchanges the sets $\mathcal{S}_2^+$ and $\mathcal{S}_2^-$. Also, M interchanges the s-axis with the line $t = 2s$ and interchanges the line $t = s/2$ with the line $t = 3s/2$. That is, M interchanges the sets U and L. Since multiplication by M is a homomorphism with respect to vector addition, and every element of L is a sum of elements of $\mathcal{S}_2^+$, this shows that every element of U is a sum of elements of $\mathcal{S}_2^-$, so $U \subset \mathcal{B}_2$.

We note that

1. For $s \geq 4$, $(s, 4) = (s - 2, 1) + (2, 3) \in \mathcal{B}_2$.
2. For $s \geq 6$, $(s, 5) = (s - 2, 4) + (2, 1) \in \mathcal{B}_2$.
3. For $s \geq 5$, $(s, 6) = (3, 5) + (s - 3, 1) \in \mathcal{B}_2$.

Now, write $(s, t) + U$ to mean the set of all points of the form $(s, t) + (u, v)$ with $(u, v) \in U$. The second graph in FIGURE 6 shows the sets $(2, 1) + U$, $(3, 1) + U$, and $(4, 1) + U$, and makes it clear that the union of all $(n, 1) + U$ for $n \geq 2$ contains all (s, t) with $s \geq 6$ and $t \geq 7$. Since each $(n, 1) + U \subset \mathcal{B}_2$, all of these points are in $\mathcal{B}_2$.

Combining the observations made so far shows that all the solid dots in the first graph in FIGURE 6 are in $\mathcal{B}_2$, leaving only the points listed in the statement of the theorem, shown as hollow dots, as candidates for the points of $\mathcal{A}_2 - \mathcal{B}_2$.

To check that these ten points are not in $\mathcal{B}_2$, we induct on s. Each element of $\mathcal{S}_2$ other than $(0, 0)$ has s-coordinate at least 2, so $(1, 1)$ is not in $\mathcal{B}_2$. Since $(2, 2)$ is not one of the primitives $(2, 1)$ or $(2, 3)$, it is not in $\mathcal{B}_2$. To be in $\mathcal{B}_2$, each of $(3, 2)$, $(3, 3)$ and $(3, 4)$ would have to be $(2, 1) + (1, t)$ or $(2, 3) + (1, t)$, which is impossible since no $(1, t)$ is primitive. Each of $(4, 3)$ and $(4, 5)$ would have to be either $(2, 1) + (2, t)$ or $(2, 3) + (2, t)$, for $t = 1$ or $t = 3$, again giving no posssibilites. Finally, $(5, 3)$, $(5, 5)$, or $(5, 7)$ would have to be $(2, 1) + (3, t)$ or $(2, 3) + (3, t)$, for $t = 1$ or $t = 5$. ■

As was the case for $\mathcal{A}_p$, multiplication by the matrix

$$\begin{pmatrix} 1 & -1/2 \\ 0 & 1/2 \end{pmatrix}$$

clarifies the picture. FIGURE 7 shows the result of multiplying the vectors of $\mathcal{A}_2$ by this matrix. The nonzero primitives are carried to the points $(n + 1/2, 1/2)$ and $(1/2, n + 1/2)$ for $n \geq 1$.

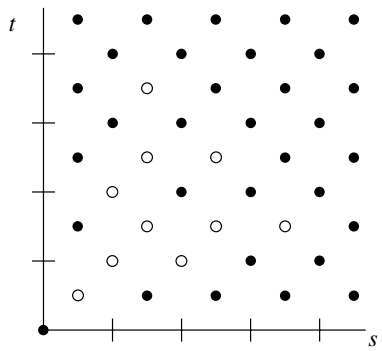

Figure 7 A better view of $\mathcal{A}_2$ and $\mathcal{B}_2$

We still need to identify which elements of $\mathcal{D}_0$ are products of primitives. We denote this subsemigroup by $\mathcal{B}_0$. For any product of elements of $\mathcal{D}$ that lies in $\mathcal{D}_0$, one of the

factors must have $a = 0$. The only primitives in $\mathcal{D}_0$ are $[0, \pm 2]$, so the only products of primitive elements from $\mathcal{D}_0$ are the $[0, \pm 2^n]$ with $n \geq 1$. The h-coordinates of the other primitive factors, up to sign, all have the form q^2 with q odd, or $2q^2$ with $q \neq 0$. So the h-coordinate of the product must have the form $\pm Q^2$ with Q even, or $\pm 2Q^2$, and any number of this form can be achieved.

Summarizing, we have the complete monoid structure.

THEOREM 7. *The Beauregard-Suryanarayan monoid $\mathcal{D}$ is a disjoint union $\mathcal{D}_0 \cup \mathcal{D}_{\neq 0}$, where $\mathcal{D}_0$ consists of all $[0, h]$ with h even, and is isomorphic to $2\mathbb{Z} - \{0\}$. There is a direct sum decomposition*

$$\mathcal{D}_{\neq 0} = \{[\pm 1, \pm 1]\} \oplus \mathcal{A}_2 \oplus \left(\bigoplus_{p \in \mathcal{P} - \{2\}} \mathcal{A}_p \right),$$

with each $\mathcal{A}_p$ isomorphic to the 3-generator monoid $\mathbb{M}$, and $\mathcal{A}_2$ isomorphic to the non-finitely-generated monoid $\mathbb{M}_2$. The submonoid of products of primitive GPTs is a disjoint union $\mathcal{B}_0 \cup \mathcal{B}_{\neq 0}$, where $\mathcal{B}_0$ consists of all $[0, h]$ with h of the form $\pm q^2$ with q even, or $\pm 2q^2$, and

$$\mathcal{B}_{\neq 0} = \left\{[\pm 1, \pm 1]\right\} \oplus \mathcal{B}_2 \oplus \left(\bigoplus_{p \in \mathcal{P} - \{2\}} \mathcal{B}_p \right),$$

where each $\mathcal{B}_p$ consists of the $[p^s, p^t]$ in $\mathcal{A}_p$ with t even, and $\mathcal{B}_2$ consists of all but the ten elements of $\mathcal{A}_2$ specified in Theorem 6.

The *e*-operation

In this final section, we adapt our approach to the Beauregard-Suryanarayan operation to develop a new operation on GPTs (with $h \neq 0$), which is multiplicative with respect to e and to h. We will see that as with the Beauregard-Suryanarayan operation, the group obtained by projectivization can be naturally identified with $\{1, -1\} \times \mathbb{Q}$, but this time the subgroup corresponding to $\{1\} \times \mathbb{Q}_{>0}$ *is exactly the set of PPTs.*

Since $e = kd$, Theorem 1 shows that e-h coordinates on the set $\mathcal{D}$ of GPTs with $h \neq 0$ can be defined by putting

$$\langle e, h \rangle = \left(h + e, e + \frac{e^2}{2h}, h + e + \frac{e^2}{2h} \right).$$

Theorem 1 and Lemma 1 show that $\langle e, h \rangle$ represents a GPT exactly when h and e are integers such that $h \neq 0$ and $2h$ divides e^2, and $\langle e, h \rangle$ is a PT exactly when both e and h are positive. Some examples are:

1. $\langle 2, 1 \rangle = (3, 4, 5)$, $\langle 2, 2 \rangle = (4, 3, 5)$, $\langle 2, -2 \rangle = (0, 1, -1)$.
2. $\langle 2p, 1 \rangle = (1 + 2p, 2p + 2p^2, 1 + 2p + 2p^2)$.
3. $\langle 2p, 2 \rangle = (2 + 2p, 2p + p^2, 2 + 2p + p^2)$.
4. $\langle 2q, q^2 \rangle = (q^2 + 2q, 2q + 2, q^2 + 2q + 2)$.
5. $\langle 2^s, 2^{2s-1} \rangle = (2^s + 2^{2s-1}, 1 + 2^s, 1 + 2^s + 2^{2s-1})$ with $s \geq 1$.

The relation between e-h coordinates and a-h coordinates is just that $\langle e, h \rangle = [e + h, h]$, so the condition to identify primitive GPTs is exactly that of Proposition 1:

PROPOSITION 2. *For $h \neq 0$, $\langle e, h\rangle$ is primitive exactly when either*

1. $h = \pm q^2$ *with q odd and* $\gcd(e, h) = q$, *or*
2. $h = \pm 2q^2$, *and* $\gcd(e, h) = 2q$.

We define an operation by the simple rule

$$\langle e_1, h_1\rangle \langle e_2, h_2\rangle = \langle e_1 e_2, h_1 h_2\rangle$$

and call it the *e-operation.* Notice that $\langle e_1 e_2, h_1 h_2\rangle$ does represent a GPT, since if $2h_1 \mid e_1^2$ and $2h_2 \mid e_2^2$, then $2h_1 h_2 \mid (e_1 e_2)^2$. In (a, b, c)-coordinates (obviously the wrong ones for viewing it), the operation takes the form

$$\begin{aligned}(a_1, b_1, c_1)(a_2, b_2, c_2) = \\ (a_1a_2 + a_1b_2 - a_1c_2 + b_1a_2 + 2b_1b_2 - 2b_1c_2 - c_1a_2 - 2c_1b_2 + 2c_1c_2,\\ 3a_1a_2 + a_1b_2 - 3a_1c_2 + b_1a_2 + b_1b_2 - b_1c_2 - 3c_1a_2 - c_1b_2 + 3c_1c_2,\\ 3a_1a_2 + a_1b_2 - 3a_1c_2 + b_1a_2 + 2b_1b_2 - 2b_1c_2 - 3c_1a_2 - 2c_1b_2 + 4c_1c_2),\end{aligned}$$

and in a-h coordinates it is $[a_1, h_1][a_2, h_2] = [a_1a_2 - a_1h_2 - a_2h_1 + 2h_1h_2, h_1h_2]$. Here are a couple of sample calculations.

$$\begin{aligned}(3, 4, 5)\,(3, 4, 5) &= \langle 2, 1\rangle \langle 2, 1\rangle \\ &= \langle 4, 1\rangle = (5, 12, 13)\\ (4, 3, 5)\,(a, b, c) &= \langle 2, 2\rangle \langle a + b - c, c - b\rangle \\ &= \langle 2(a + b - c), 2(c - b)\rangle = (2a, 2b, 2c)\end{aligned}$$

For $\langle e, h\rangle = (a, b, c)$ and any nonzero integer n, we have $n\langle e, h\rangle = (na, nb, nc) = \langle ne, nh\rangle$, and we will declare all these equivalent. Denote the set of equivalence classes with $h \neq 0$ by $\mathcal{E}$.

THEOREM 8. *Define $\phi\colon \mathcal{E} \to \{1, -1\} \times \mathbb{Q}$ by sending $\langle e, h\rangle$ to $(\sigma(h), e/h)$, where $\sigma(h) = 1$ if h is positive and is -1 if h is negative. Then ϕ is an isomorphism.*

Proof. As in Theorem 4, it is straightforward to check that ϕ is a well-defined homomorphism. It is surjective, since $\phi(\pm\langle 2, 2\rangle) = (\pm 1, 1)$, $\phi(\pm\langle 2, -2\rangle) = (\pm 1, -1)$, $\phi(\langle 0, 1\rangle) = (1, 0)$, $\phi(\langle 2, 1\rangle) = (1, 2)$, $\phi(\langle 4, 8\rangle) = (1, 1/2)$, and $\phi(\langle 4, 8\rangle\langle 2q, 1\rangle) = (1, q)$ and $\phi(\langle 4, 8\rangle\langle 2q, q^2\rangle) = (1, 1/q)$, when q is an odd prime. For injectivity, suppose that $\phi(\langle e_1, h_1\rangle) = \phi(\langle e_2, h_2\rangle)$. Then h_1 and h_2 have the same sign, so replacing each $\langle e_i, h_i\rangle$ by $\langle -e_i, -h_i\rangle$ if necessary, we may assume that both h_1 and h_2 are positive. Since

$$\frac{1}{h}\langle e, h\rangle = \left(1 + \frac{e}{h}, \frac{e}{h} + \frac{1}{2}\left(\frac{e}{h}\right)^2, 1 + \frac{e}{h} + \frac{1}{2}\left(\frac{e}{h}\right)^2\right),$$

we have $h_2\langle e_1, h_1\rangle = h_1\langle e_2, h_2\rangle$. Thus $\langle e_1, h_1\rangle$ and $\langle e_2, h_2\rangle$ are projectively equivalent and represent the same element of $\mathcal{E}$. ∎

Under this isomorphism, the PPTs correspond exactly to $\mathbb{Q}_{>0}$, so they form an abelian group free on the generators $\{\langle 2, 1\rangle\} \cup \{\langle 2p, 2\rangle \mid p \text{ is prime}\}$. It is also free on the set of height-1 PPTs $\{\langle 2, 1\rangle\} \cup \{\langle 2p, 1\rangle \mid p \text{ is prime}\}$.

Unlike the Beauregard-Suryanarayan operation, the *e*-operation is not well-behaved at the level of PTs. For example, it has no identity element, and appears to have poor

factorization properties, since no GPT $\langle e, h\rangle$ with $e \equiv 2 \mod 4$ can be factored into a product of two GPTs. But perhaps there is still some nice structure hiding there.

Acknowledgment. The author was supported in part by NSF grant DMS-0102463. He thanks the referees for many suggestions that improved this article.

REFERENCES

1. R. Amato, On the determination of Pythagorean triples, (Italian, English summary) *Atti Soc. Peloritana Sci. Fis. Mat. Natur.* **27** (1981), 3–8.
2. P. J. Arpaia, A generating property of Pythagorean triples, this MAGAZINE **44** (1971), 26–27.
3. F. J. M. Barning, On Pythagorean and quasi-Pythagorean triangles and a generation process with the help of unimodular matrices, (Dutch) *Math. Centrum Amsterdam Afd. Zuivere Wisk,* ZW-011 (1963) 37 pp.
4. R. Beauregard and E. Suryanarayan, Pythagorean triples: the hyperbolic view, *College Math. J.* **27** (1996), 170–181.
5. H. Becker, http://home.foni.net/~heinzbecker/pythagoras.html
6. J. Buddenhagen, C. Ford, and M. May, Nice cubic polynomials, Pythagorean triples, and the law of cosines, this MAGAZINE **65** (1992), 244–249.
7. B. Dawson, The ring of Pythagorean triples, *Missouri J. Math. Sci.* **6** (1994), 72–77.
8. E. Eckert, The group of primitive Pythagorean triangles, this MAGAZINE **57** (1984), 22–27.
9. A. Grytczuk, Note on a Pythagorean ring, *Missouri J. Math. Sci.* **9** (1997), 83–89.
10. J. Gollnick, H. Scheid, J. Zöllner, Rekursive Erzeugung der primitiven pythagoreischen Tripel, (German) [Recursive generation of primitive Pythagorean triples], *Math. Semesterber.* **39** (1992), 85–88.
11. A. Hall, Genealogy of Pythagorean triads, *Mathematical Gazette* **54:390** (1970), 377–379.
12. E. Hlawka, Pythagorean triples, in *Number Theory* (ed. R. P. Bambaugh, V. C. Dumir, and R. J. Hans-Gill), in series *Trends in Mathematics*, Birkhäuser, Basel (2000), 141–155.
13. J. Jaeger, Pythagorean number sets (Danish, English summary), *Nordisk Mat. Tidskr.* **24** (1976), 56–60, 75.
14. T. A. Jenkyns and D. McCarthy, Integers in Pythagorean triples, *Bull. Inst. Combin. Appl.* **4** (1992), 53–57.
15. Kanga, A. R., The family tree of Pythagorean triples, *Bull. Inst. Math. Appl.* **26** (1990), 15–17.
16. H. Klostergaard, Tabulating all Pythagorean triples, this MAGAZINE **51** (1978), 226–227.
17. E. Kristensen, Pythagorean number sets and orthonormal matrices, (Danish, English summary) *Nordisk Mat. Tidskr.* **24** (1976), 111–122, 135.
18. D. McCullough and E. Wade, Recursive enumeration of Pythagorean triples, *College Math. J.* **34** (2003), 107-111.
19. L. Palmer, M. Ahuja, and M. Tikoo, Finding Pythagorean triple preserving matrices, *Missouri J. Math. Sci.* **10** (1998), 99–105.
20. ———, Constructing Pythagorean triple preserving matrices, *Missouri J. Math. Sci.* **10** (1998), 159–168.
21. Préau, Paul, Un graphe ternaire associé à l'équation $X^2 + Y^2 = Z^2$, (French, English summary) [A ternary graph associated with the equation $X^2 + Y^2 = Z^2$], *C. R. Acad. Sci. Paris Sér. I Math.* **319** (1994), 665–668.
22. O. Taussky, Sums of squares, *Am. Math. Monthly* **77** (1970), 805–830.
23. M. G. Teigan and D. W. Hadwin, On generating Pythagorean triples, *Amer. Math. Monthly* **78** (1971), 378–379.
24. P. W. Wade and W. R. Wade, Recursions that produce Pythagorean triples, *College Math. J.* **31** (2000), 98–101.
25. M. Wójtowicz, Algebraic structures of some sets of Pythagorean triples, I, *Missouri J. Math. Sci.* **12** (2000), 31–35.
26. ———, Algebraic structures of some sets of Pythagorean triples, II, *Missouri J. Math. Sci.* **13** (2001), 17–23.

A Note from the Problems Editor

John Cobb and Martin Tangora each noted that there is an even quicker solution to Quickie 943 (October 2004). Because the metric space (X, d) is compact, $d(x, y)$ assumes its maximum on $X \times X$. Thus $d(f(x), f(y)) > d(x, y)$ cannot be true for every pair (x, y) with $x \neq y$. Hence X must consist of a single point.